Host Security

Module 06

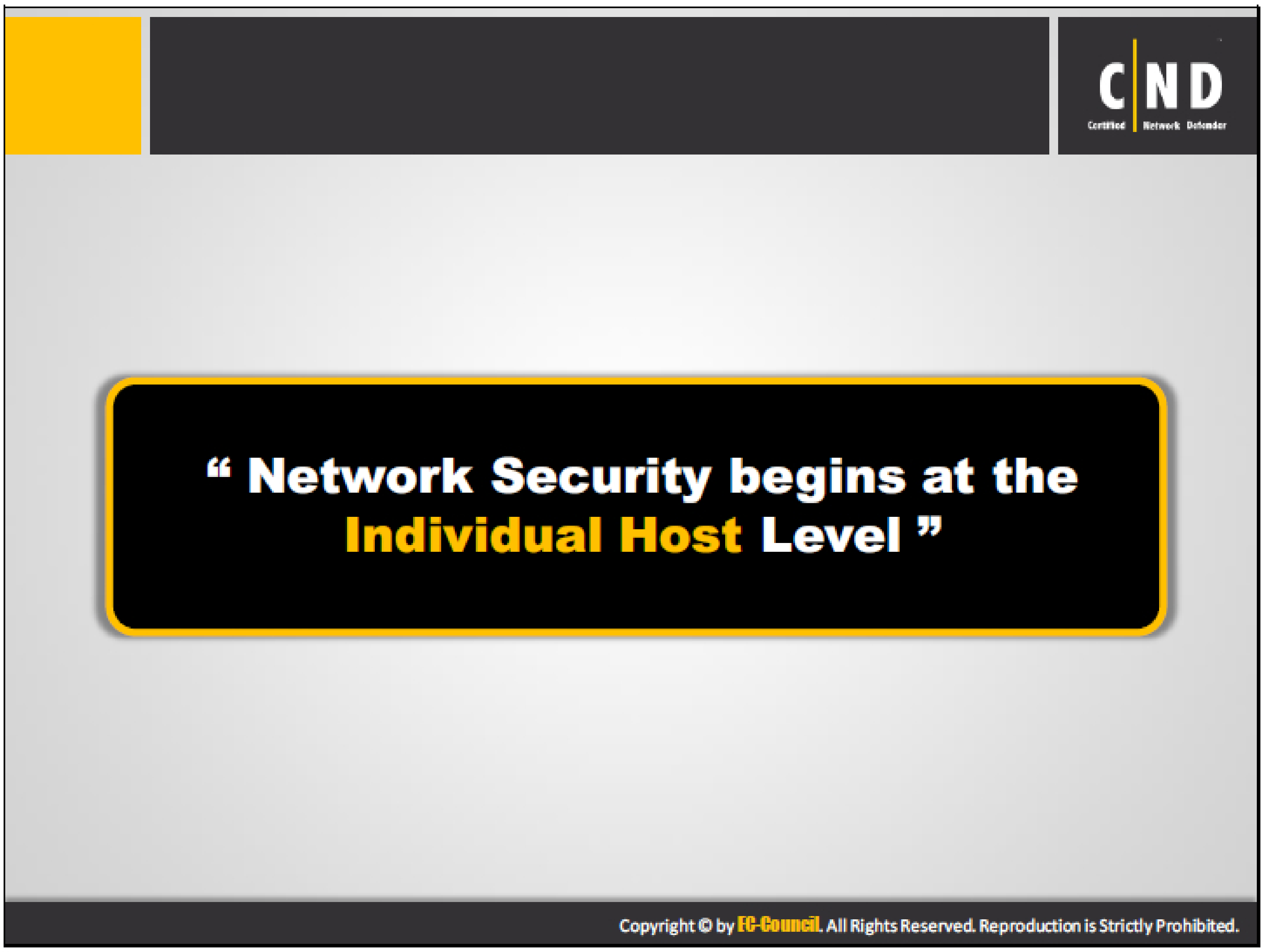
Host Security

Module 06

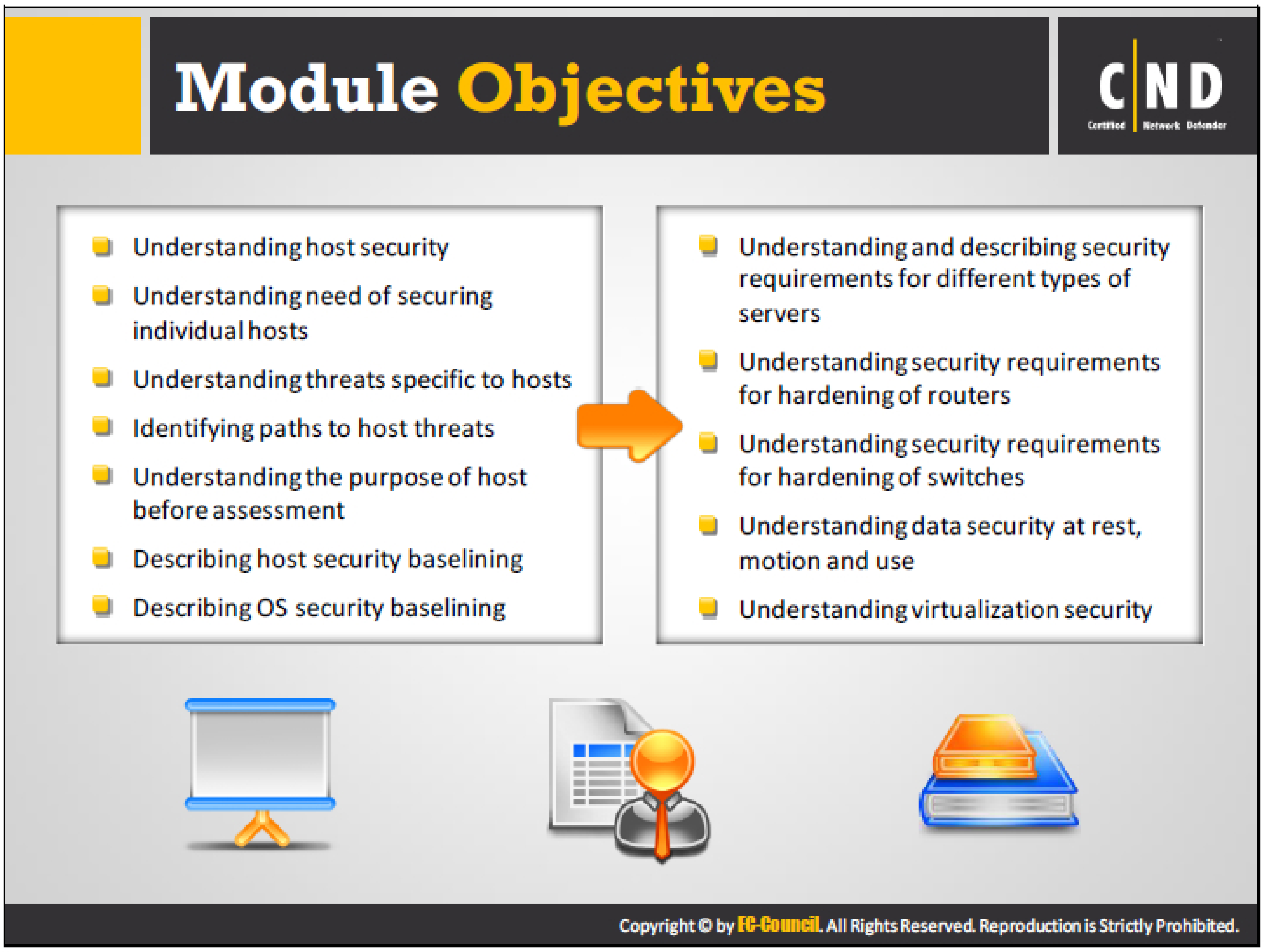
Certified Network Defender

Module 06: Host Security

Exam 312-38



“ Network Security begins at the **Individual Host** Level ”

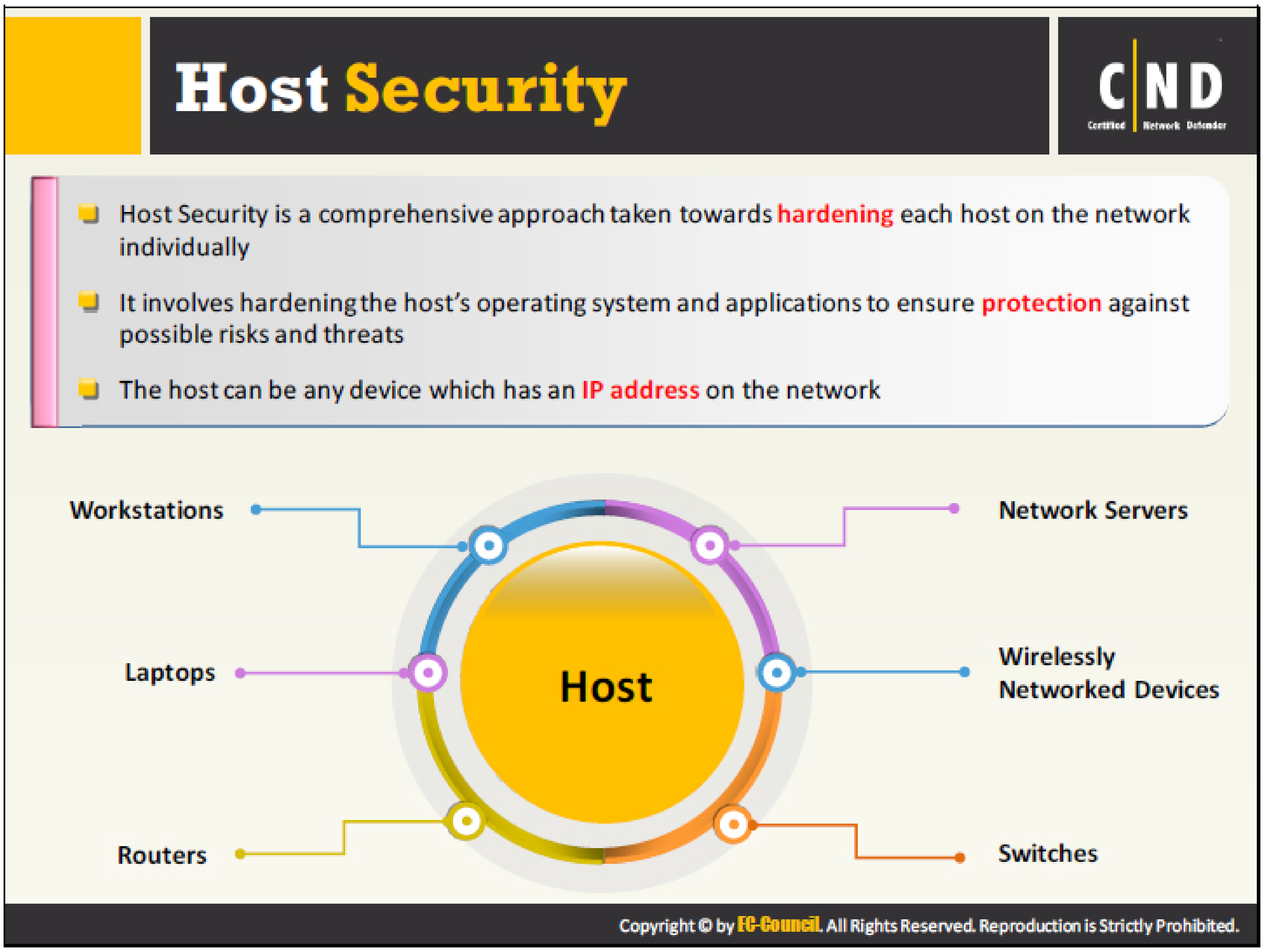


Module Objectives

CND
Certified Network Defender

- Understanding host security
- Understanding need of securing individual hosts
- Understanding threats specific to hosts
- Identifying paths to host threats
- Understanding the purpose of host before assessment
- Describing host security baselining
- Describing OS security baselining
- Understanding and describing security requirements for different types of servers
- Understanding security requirements for hardening of routers
- Understanding security requirements for hardening of switches
- Understanding data security at rest, motion and use
- Understanding virtualization security

Network security starts with securing the individual host on the network. Host security is the next layer of security in defense-in-depth that should be taken care of. This module focuses on security measures and techniques required for securing individual hosts. The module covers all the security tools, techniques, best practices and recommendations required for securing and hardening various types of hosts in the network. The module also provides a brief overview of virtualization security, application security, and data loss prevention techniques that help you in attaining a complete host security.



Host Security

CND Certified Network Defender

- Host Security is a comprehensive approach taken towards hardening each host on the network individually
- It involves hardening the host's operating system and applications to ensure protection against possible risks and threats
- The host can be any device which has an IP address on the network

Host

Workstations

Network Servers

Laptops

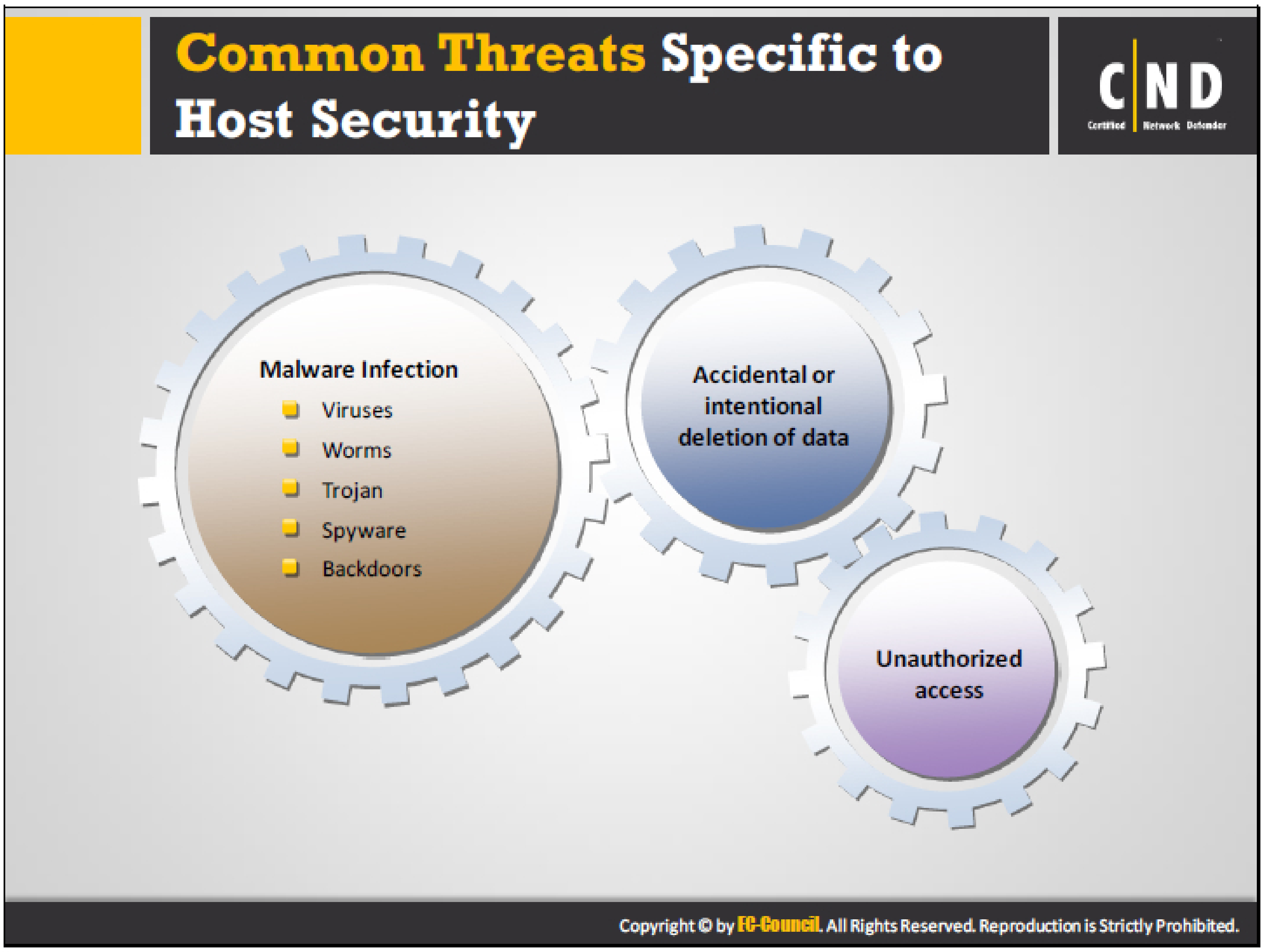
Wirelessly Networked Devices

Routers

Switches

Any device with an IP address connected to the network is considered a host. A host is an important and integral part of any network in the organization. Host security plays a vital role in securing organization network activities since the host can be the major conduit. If the host is compromised, all devices and services risk being compromised as well. Host security refers to the protection of hardware, software, information stored and services running on these computers from any kind of theft or damage. The organization should ensure the confidentiality, availability and integrity of the host and the data they hold. An insecure configuration of a host can put the entire network at a security risk. Even though proper host security measures are taken into consideration while installing host in the network, the host can still be insecure through its use. Over time, the hardware and software installed on the host get outdated and are prone to various types of threats inherent to poor patch management methodologies. Thus, it is important to address and ensure the security of the host during its lifecycle.

The organization needs to systematically monitor the hosts in order to check for the chances of attacks and to identify the various possibilities of attacks on the hosts. Understanding the areas of compromise can help the administrators come up with solutions to prevent those attacks. They can put forward various policies and regulations in strengthening the security of the hosts and thereby providing negligible or no impact to the business of the organization. Appropriate training and awareness can help administrators maintain the security of the host in an organization.



Common Threats Specific to Host Security

Malware Infection
- Viruses
- Worms
- Trojan
- Spyware
- Backdoors

Accidental or intentional deletion of data

Unauthorized access

Hosts can be at risk of both internal and external threats. The internal threats mainly occur within an organization and the damage caused by these threats can lead to a great loss to the assets of an organization. These threats include malware attacks, information theft, unauthorized access, illegal use of corporate resources etc. Any sort of attack on the host internally can affect the end users and the business of an organization. Administrators should evaluate their host against possible internal as well as external threats.

To ensure host security, you should be aware of different threats that the host is vulnerable to. The host can be at risk of being exploited by the following major threats.

Malware Attack

- **Viruses**: Viruses are programs that replicate by reproducing itself to infect the host system. These make changes in the host by deleting files, reformatting hard drive etc. A virus infected system cannot operate again as before.
- **Worms**: They are viruses that repeat itself without much human interaction. They have the ability to spread and infect systems as they travel through the network or the internet.
- **Trojans**: Trojan is considered one of the most complex threats and creates damage to the host. They hide the payload part of the data packet while travelling through the network, thereby allowing file corruption, remote access, interrupting firewalls and anti-virus etc. Another impact of a Trojan is its ability to steal data. This makes it easier for the attackers to gather sensitive information.

- **Spyware**: Spyware is a malware that is used for spying on the actions performed by a user on the system. This gathers the information of all activities performed by a user on the system. For example, Keylogger is a type of spyware that is used to capture the keystrokes.
- **Backdoor**: A backdoor is planted to skip all the authentication steps required and gain unauthorized access to remote computers.

Accidental or intentional deletion of data

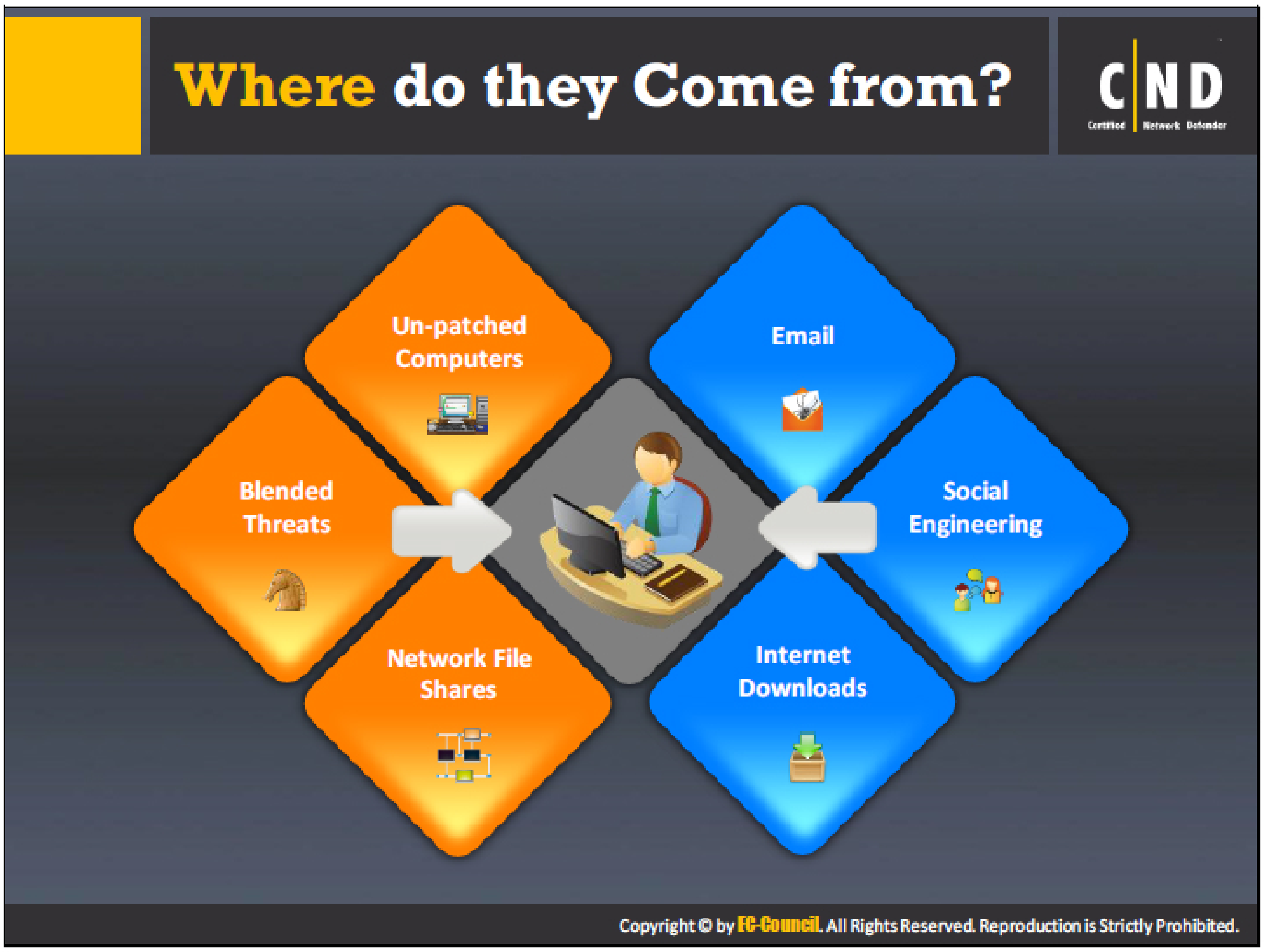
Users can sometimes delete any confidential data intentionally or accidentally that affects the security of the host.

The deletion or removal of data can affect the host security:

- A person gaining access to the host can perform intentional or unintentional deletion or modification of data present in the system.
- Acquire the information present in the system.
- Compromises the availability, confidentiality and integrity of the data stored.

Unauthorized Access

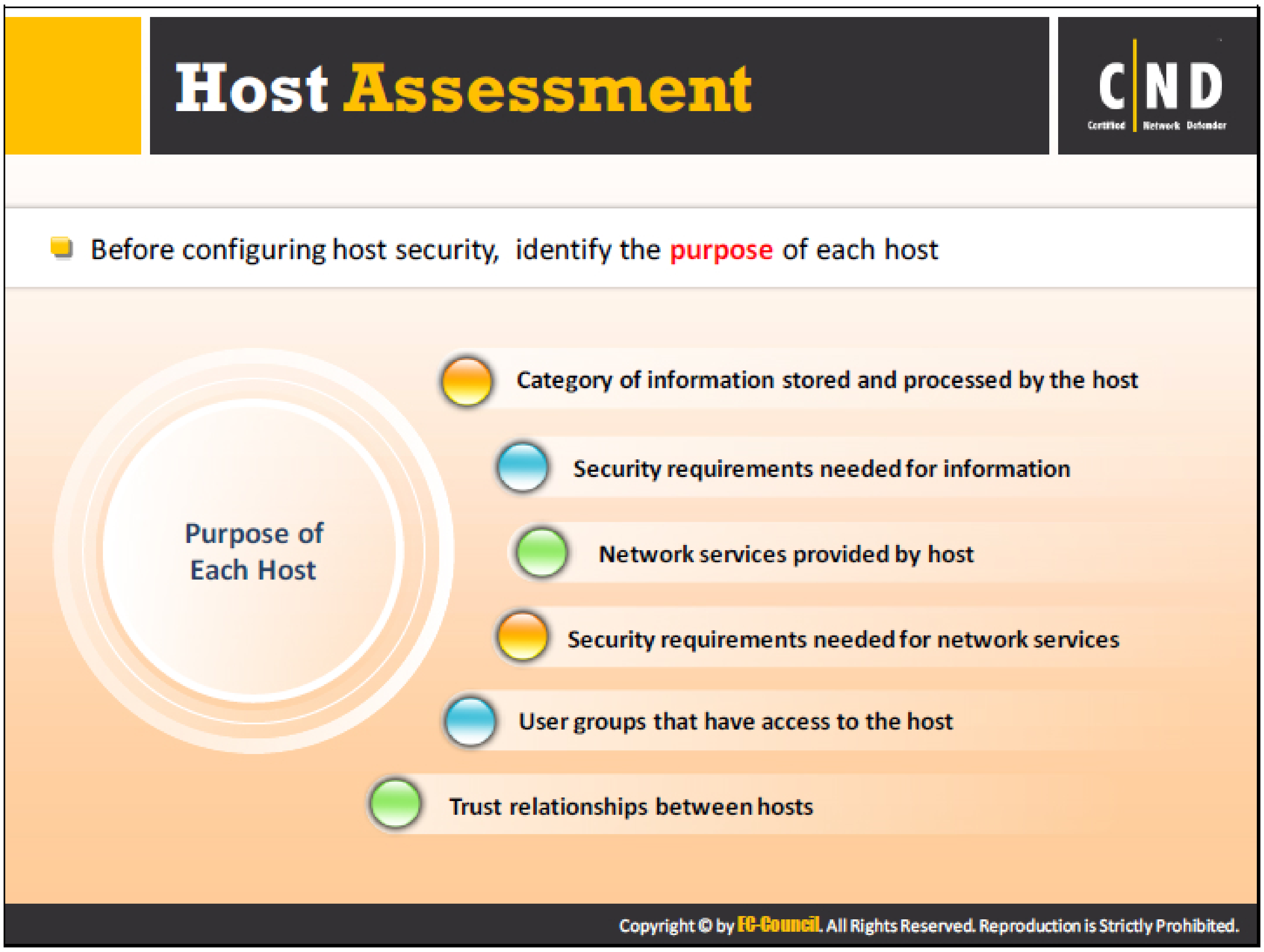
Unauthorized access refers to gaining unauthorized access to restricted files, data, operation, services, etc. running on host. An attacker, if successful in gaining unauthorized access to the system, can perform any malicious action, which will affect the security of the hosts in the network. The unauthorized access can result in stealing, accessing sensitive files, installing a virus in the system, among other actions.



Where do they Come from?

An attacker can take advantages of various vulnerabilities, which exist in order to compromise the specific host. Threats of exploiting vulnerabilities on a host can take various ways to get into the system and infect it. The lack of sufficient knowledge, skills, and insecure configurations on host security opens the network to different types of the security threats:

- **Un-patched Computers:** The majority of attacks on a host are due to the lack of proper patching or the use of outdated software installed on the host. The unpatched computer can create security loopholes and gives attackers a path to compromise it.
- **E-mail:** Host system security can be compromised through sending unsolicited emails such as phishing, malicious attachments, and spam e-mails etc.
- **Network File Sharing:** Network file sharing permits the users to share files between their individual systems over the internet. Even though it makes things easier for users to share files, it paves the way for many threats such as Malware infections, Exposure of sensitive or important information, etc.
- **Internet Downloads:** Internet downloads from untrusted sources can lead the users in downloading malware onto their systems.
- **Social Engineering:** Attackers use social engineering techniques to gain sensitive information which may help them further to gain unauthorized access, malware infection etc.
- **Blended Threats:** Attacker uses a combination of multiple techniques to attack or infect the system.



Host **Assessment**

- Before configuring host security, identify the purpose of each host

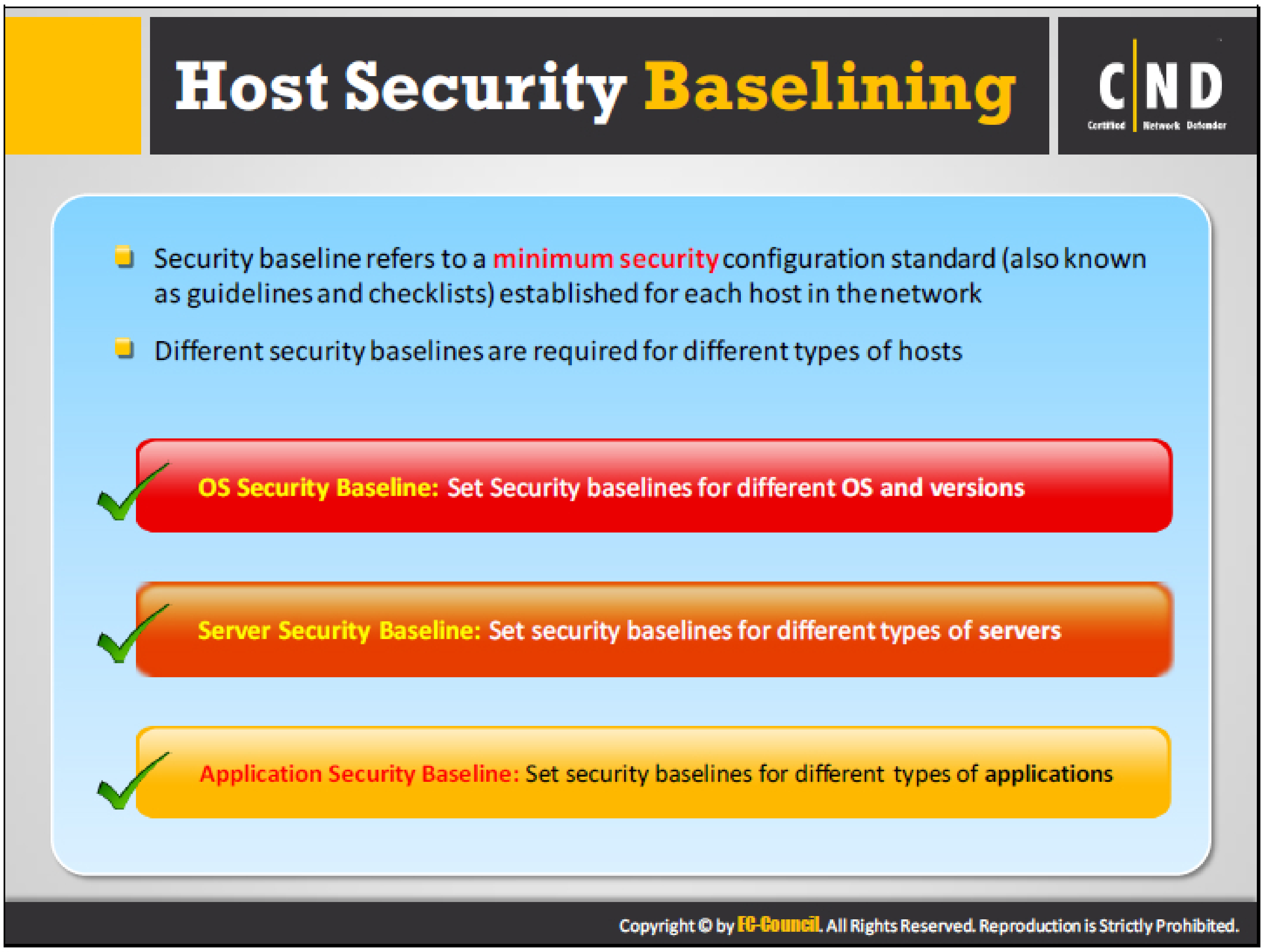
Purpose of Each Host

- Category of information stored and processed by the host
- Security requirements needed for information
- Network services provided by host
- Security requirements needed for network services
- User groups that have access to the host
- Trust relationships between hosts

Hosts in the network are configured or dedicated to perform certain functions. These hosts store and handle various types of sensitive information and provide various services of the organization. Different types of hosts require different levels of security based on the data or services it handles.

For example, the hosts that act as servers in the network, storing sensitive information and performing critical functions, require more security than a normal host or workstation.

A prior host assessment is required to assess the existing level of security and to determine the level of security required for a particular host based on its criticality, the level of sensitive information it stores, network services provided by them, and security requirements specified for them.



Host Security Baselining

- Security baseline refers to a minimum security configuration standard (also known as guidelines and checklists) established for each host in the network
- Different security baselines are required for different types of hosts

✓ **OS Security Baseline:** Set Security baselines for different OS and versions

✓ **Server Security Baseline:** Set security baselines for different types of servers

✓ Application Security Baseline: Set security baselines for different types of **applications**

Host security baselining plays an important role in enhancing the host security of the organizations. Administrators must define and establish a security baseline for hosts in the network depending upon their purpose, criticality, etc. The establishing of security baselines depends on the needs of the organization. Defining any security baseline requires active involvement of management and various departments of an organization to include their preferences.

Host security baselines help you easily identify the hosts with configurations that do not match as stated in the baseline.

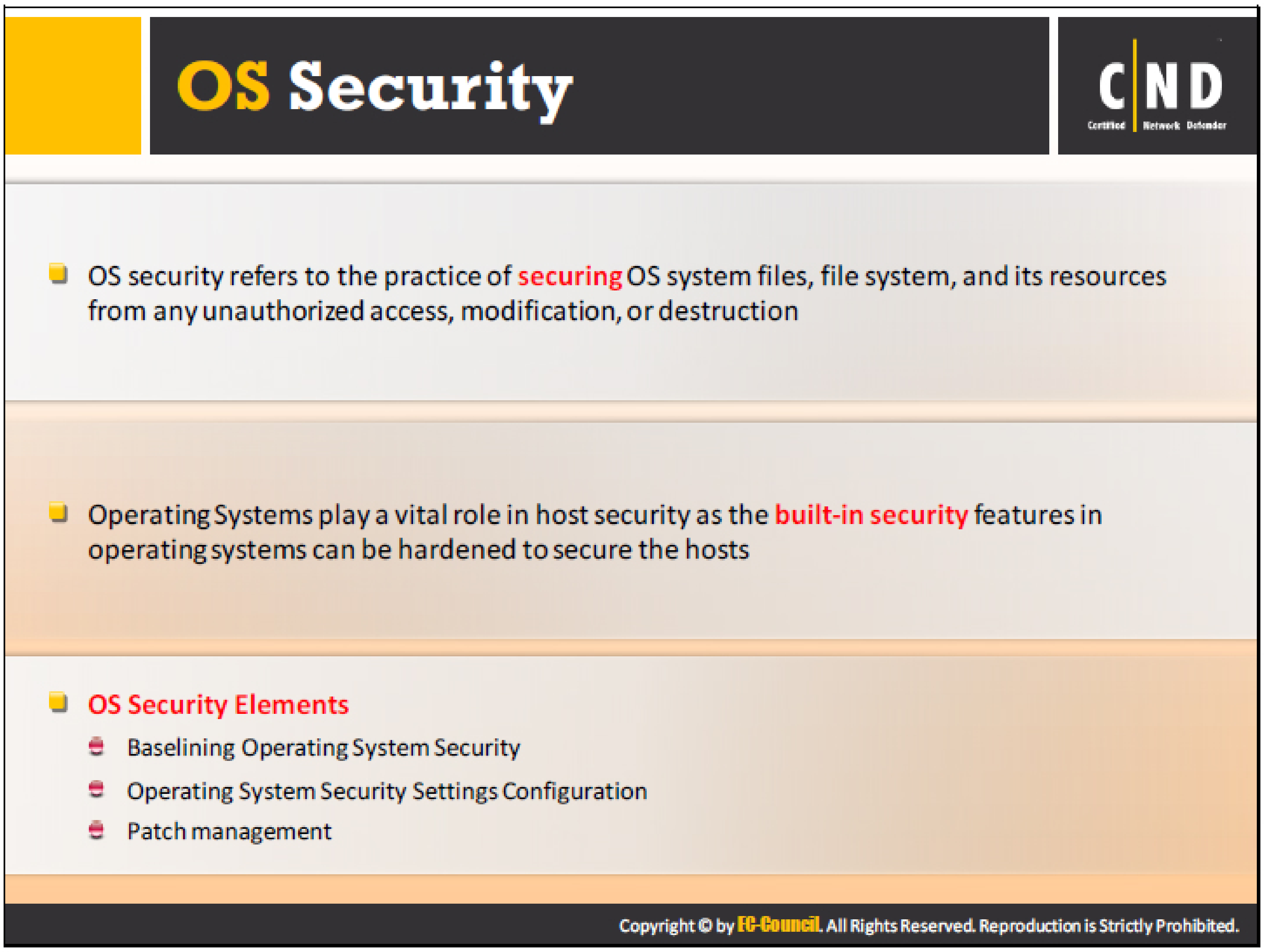
A Host security baseline sets a security objective, standards, guidelines, checklists, etc., which must be met to attain a high level of host security for organizations. It specifies the reference points for installation, hardening, placing of new hosts in the network and all activities performed on the host. Baselining facilitates more protection of the host and helps in determining the actions taken for further security. The baselines should undergo a regular update and monitoring.

The baselines help you to determine:

- The way the host performs in the network.
- Type of data the host uses to communicate across the network.
- Identify the services and resources associated with each host.
- The type of connectivity required for each host.
- A clear picture regarding the working of each host.

The baselines are different from the security policies in a way that the baselines define the structure of the security policies. There are two types of security structures for the baselines: High-level and technical. The execution of these two standards depends on the requirements of the organization. The high-level standards are independent of operating system and depend on the security policies of the organization. The technical baseline consists of statements for each operating system configured in the system and the functions carried out by them. The best method to implement a baseline is to create a simple baseline first and then increase the complexity of the baselines as moving forward with the configurations.

The host security largely depends on the OS and applications installed on the host. Establishing a host security baseline also requires establishing security baselines for the OS, user accounts, and applications to be installed on the hosts.



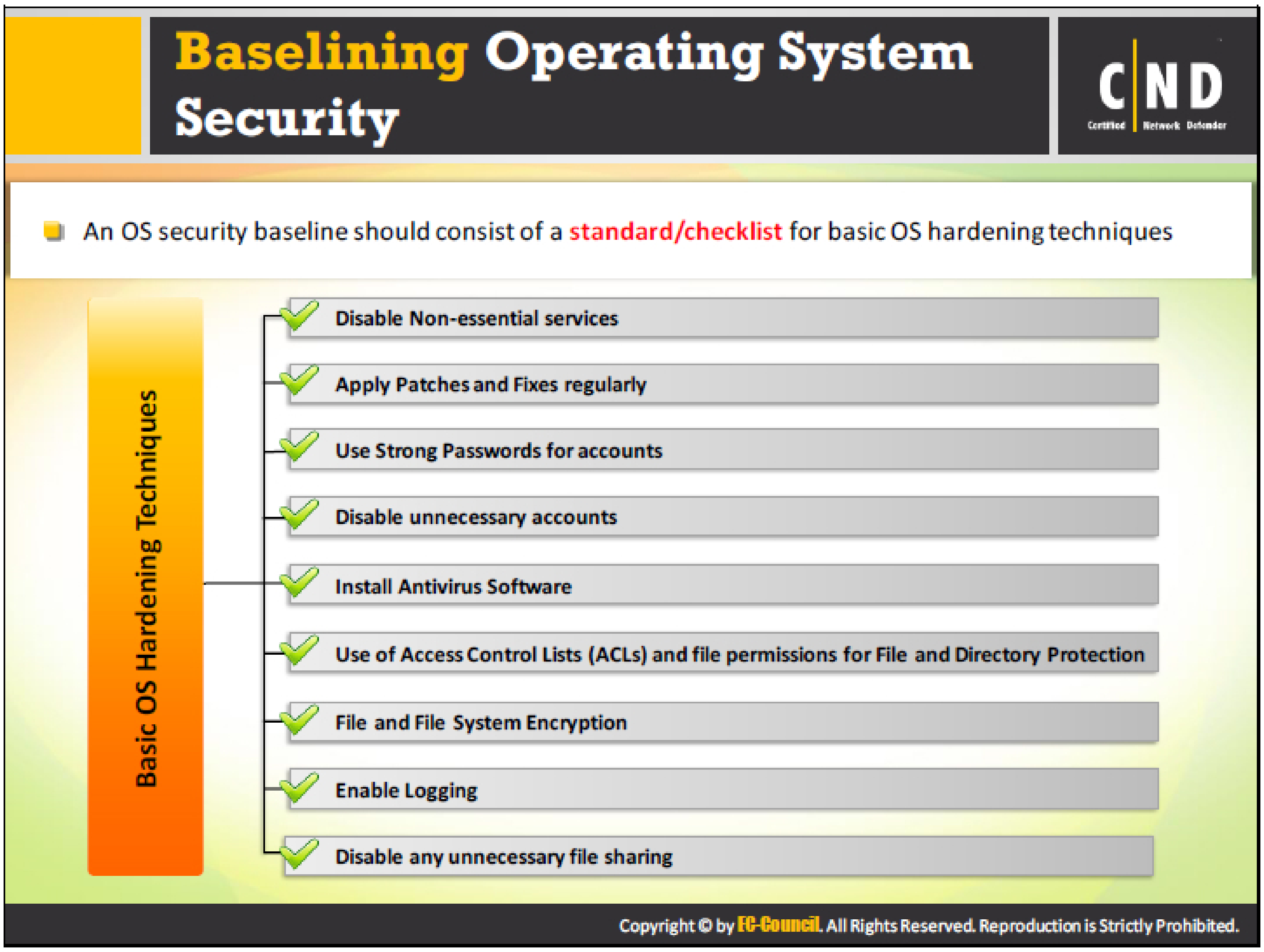
OS Security

- OS security refers to the practice of securing OS system files, file system, and its resources from any unauthorized access, modification, or destruction
- Operating Systems play a vital role in host security as the built-in security features in operating systems can be hardened to secure the hosts
- OS Security Elements
  - Baselining Operating System Security
  - Operating System Security Settings Configuration
  - Patch management

Operating system security refers to securing three components: OS integrity, confidentiality and availability. Each host in the network has a specific OS installed and running. Typical functions of an OS are managing security, system, communication, Input/Output, and hardware and software services for the host on which it is installed. OS security has a direct impact on host security. OS-level protection is required to attain host security. Each OS provides a number of built-in security features in it. The security features help administrators in hardening the security of the host, if configured appropriately based on the OS security baseline established by the organization. The OS security puts forth certain steps to protect the hosts from malware or hacker invasions.

As the operating systems are large and complex, it may come across many security issues. The chances of a virus or a worm invading the system are more when there are not adequate security policies. Also, the operating system provides many services that are critical to the functioning of the operating system. The OS security features must include measures that can take control of these services running on the OS.

The overall security of the host or the computer depends on the security of the operating system. The organization can provide OS security through user authentication, access control mechanisms, separation of kernel and user spaces, managing system resources. Securing the operating system is an integral part of the security policy in an organization. A corrupted OS or malware attacked OS cannot perform any desired task. One of the most commonly used methods for OS security is the least privilege method that each user and program can perform only the assigned task. This helps in controlling the users within a limit. The OS can also confirm that the applications and services running in a system include only required resources in order to perform the desired actions.



Baselining Operating System Security

- An OS security baseline should consist of a standard/checklist for basic OS hardening techniques

Basic OS Hardening Techniques

- ✓ Disable Non-essential services
- ✓ Apply Patches and Fixes regularly
- ✓ Use Strong Passwords for accounts
- ✓ Disable unnecessary accounts
- ✓ Install Antivirus Software
- ✓ Use of Access Control Lists (ACLs) and file permissions for File and Directory Protection
- ✓ File and File System Encryption
- ✓ Enable Logging
- ✓ Disable any unnecessary file sharing

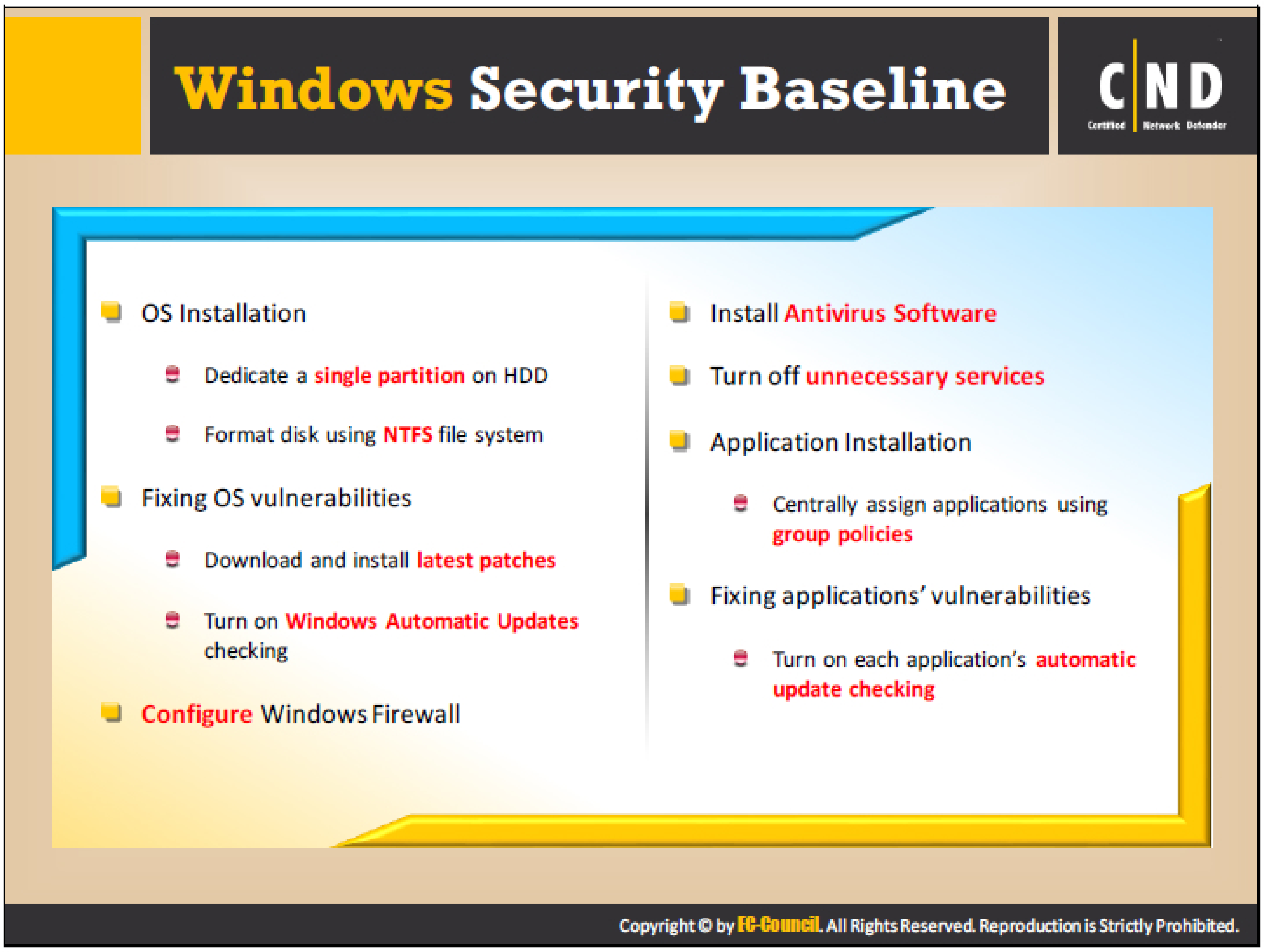
The organization establishes OS security baselines to implement a standard for installing and configuring the operating system. The setting up of the baseline varies from one organization to another. The administrators should take immense care while creating the baseline for an operating system and confirm that it meets the company requirements. The baseline for the OS needs to include the configuration of various operation system settings as well as recording each step, so that it helps for future configurations. The baseline for the OS should also include the actions performed on the system.

The organization decides on the security baselines required for the OS and implement all the settings based on it. An organization can use several security templates to decide the OS security baselines required for their organization. The process of baselining the operating system includes hardening the key components of the system architecture in order to reduce risk of attack.

The OS security baseline should address the following security configurations at a minimum:

- **Non-essential Services**: Only essential services should be enabled on the OS. Enabling unnecessary services on OS can give a path to an attacker to compromise the host through OS security flaws. For example, if a host is not functioning as a web server or a mail server, it should be disabled immediately.
- **Patch Management**: The operating system should undergo patch management regularly in order to ensure that the OS is updated with all the latest updates and fixes.

- **Password Management**: Operating systems need to persuade the users to use complex and strong passwords based on the organization's policy. Password management should also urge the users to change the password after a certain period of time and implement user lockout after a certain fixed number of attempts.
- **Unnecessary Accounts**: Organizations need to monitor the account details of the users. They may remove or delete all unwanted and guest user accounts.
- **File and Directory Protection**: Organizations should control the file and directory permissions using Access control lists.
- **File and File System Encryption:** Encryption of files and folders, formatting disk partitions with a file system with the help of encryption features provided by the OS.
- **Enable Logging:** Tracking all log activities of an operating system.
- **File Sharing:** Disabling unwanted file sharing applications running on the operating system.



Windows Security Baseline

- OS Installation
  - Dedicate a single partition on HDD
  - Format disk using NTFS file system
- Fixing OS vulnerabilities
  - Download and install latest patches
  - Turn on Windows Automatic Updates checking
- Configure Windows Firewall
- Install Antivirus Software
- Turn off unnecessary services
- Application Installation
  - Centrally assign applications using group policies
- Fixing applications' vulnerabilities
  - Turn on each application's automatic update checking

Microsoft announces the security baseline settings for their desktop and server OS products periodically. With each release, Microsoft reevaluates older settings to determine whether they address contemporary threats or not and adds updated baseline settings to address newly discovered vulnerabilities and misconfigurations.

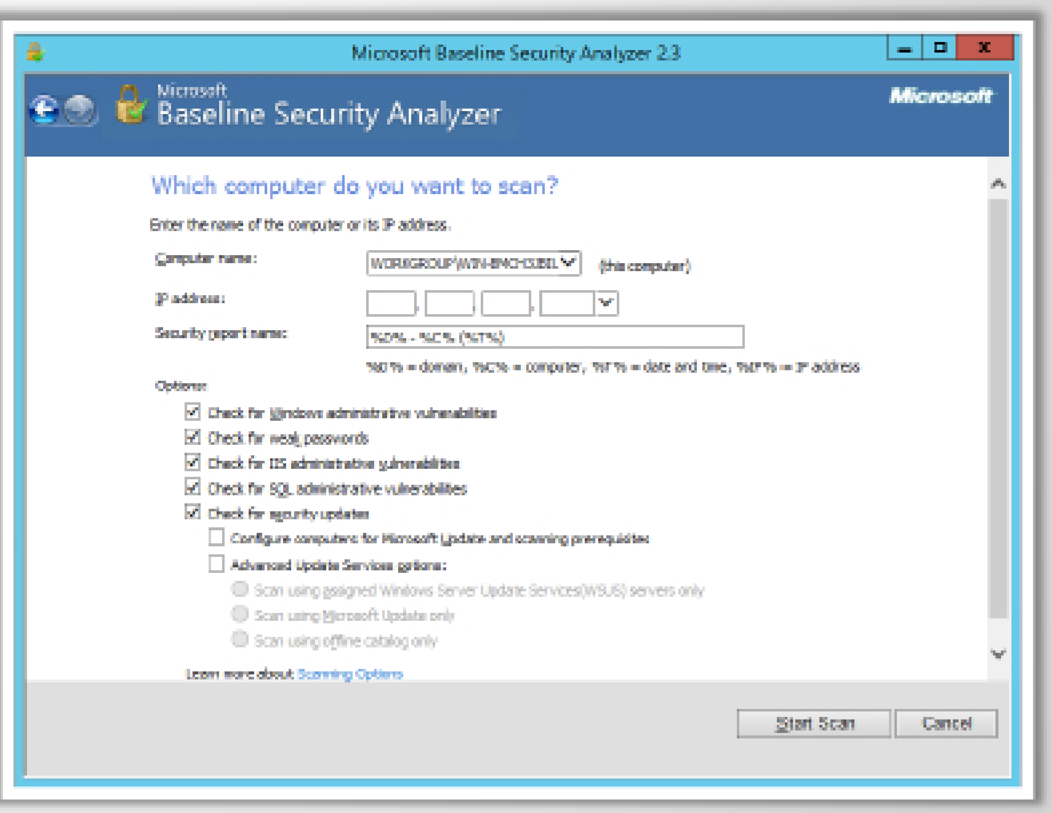
It generally includes guidelines and checklists for:

- Installing software.
- Disabling unnecessary services.
- Applying Windows OS security updates and patches.
- Applying local security policy settings.
- Configuring automatic update settings.
- Managing user accounts.
- Managing passwords.

The Windows security baseline defines the steps for identifying the security updates and configuration changes required. The baselines compare and measure the scheduling, construction methods, management and results in the operating system.

Microsoft Baseline Security Analyzer (MBSA)

- The Microsoft Baseline Security Analyzer provides a streamlined method to identify missing security updates and common security misconfigurations of a Windows OS
- It performs local or remote scans of Microsoft Windows systems



Microsoft Baseline Security Analyzer 2.3

Microsoft Baseline Security Analyzer

Which computer do you want to scan?

Enter the name of the computer or its IP address.

Computer name: WORKGROUP\WIN-8NCH3J3IL (this computer)

IP address:

Security report name: %D% - %C% (%T%)

%D% = domain, %C% = computer, %T% = date and time, %IP% = IP address

Options:

☑ Check for Windows administrative vulnerabilities
☑ Check for weak passwords
☑ Check for IIS administrative vulnerabilities
☑ Check for SQL administrative vulnerabilities
☑ Check for security updates
☐ Configure computers for Microsoft Update and scanning prerequisites
☐ Advanced Update Services options:
○ Scan using assigned Windows Server Update Services(WSUS) servers only
○ Scan using Microsoft Update only
○ Scan using offline catalog only

Learn more about Scanning Options

https://www.microsoft.com

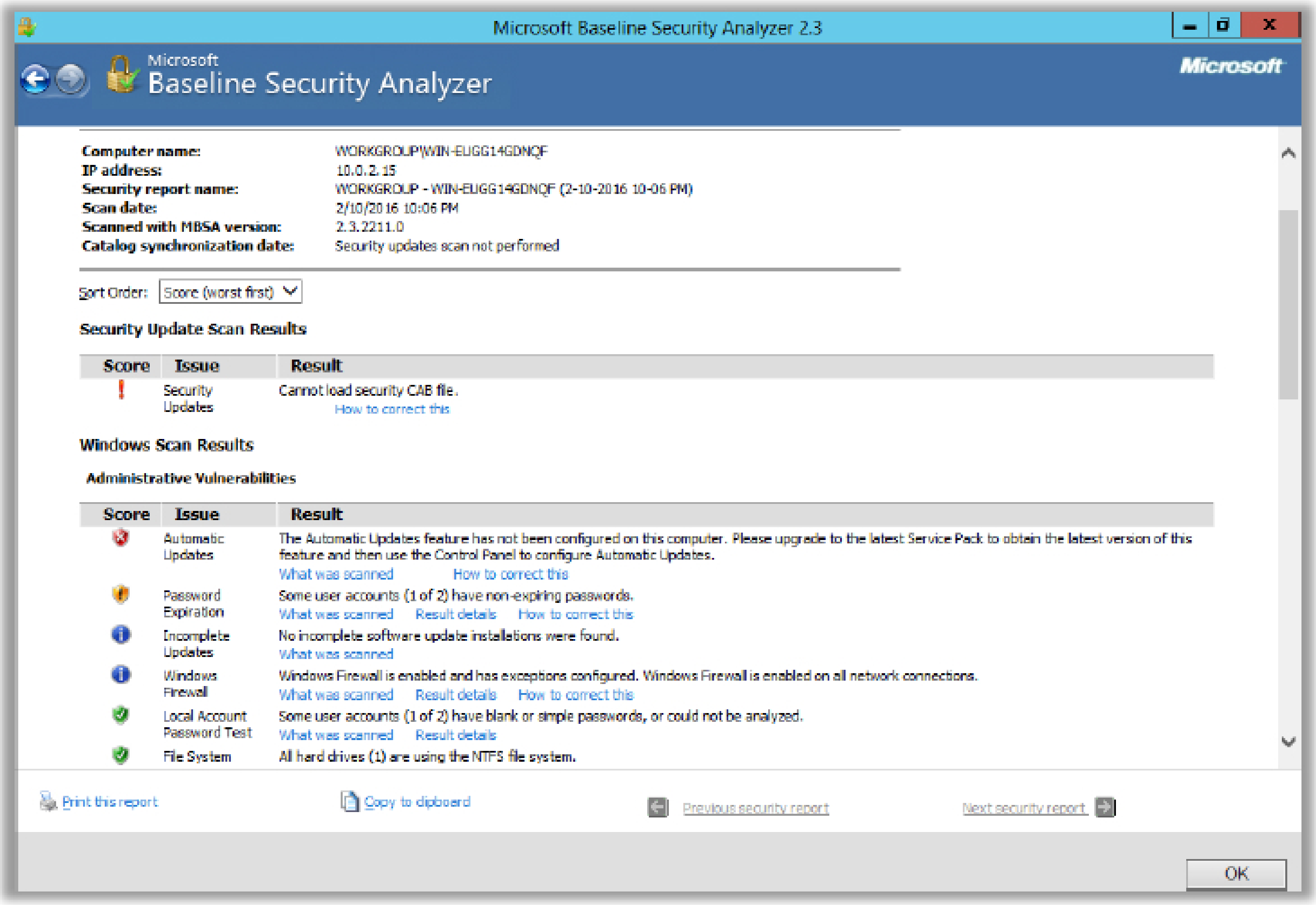
Microsoft Baseline Security Analyzer (MBSA) lets administrators scan local and remote systems for missing security updates as well as common security misconfigurations. Microsoft baseline security analyzer is used to analyze the security standards for the organization by identifying the updates required by the organization and rectifying the weaker settings of Microsoft Windows.

MBSA helps small and medium sized business organizations analyze the security status and standards and check whether it is compatible with the Microsoft security recommendations.

All the scan results produced by MBSA check for critical issues, non-critical issues and best methods that describe the remedies that can be taken for securing the operating system.

Understanding the scan report

After the MBSA tool is ran successfully on the system, it generates a report in the %userprofile% directory of the scanned system. MBSA generates the output in the form of different categories that are represented by different icons depending on the severity of the vulnerability. Below are the details of the icons.



Microsoft Baseline Security Analyzer 2.3
Microsoft
Baseline Security Analyzer
Microsoft

Computer name: WORKGROUP\WIN-EUGG14GDNQF
IP address: 10.0.2.15
Security report name: WORKGROUP - WIN-EUGG14GDNQF (2-10-2016 10-06 PM)
Scan date: 2/10/2016 10:06 PM
Scanned with MBSA version: 2.3.2211.0
Catalog synchronization date: Security updates scan not performed

Sort Order: Score (worst first)

Security Update Scan Results

Score	Issue	Result
!	Security Updates	Cannot load security CAB file. How to correct this

Windows Scan Results

Administrative Vulnerabilities

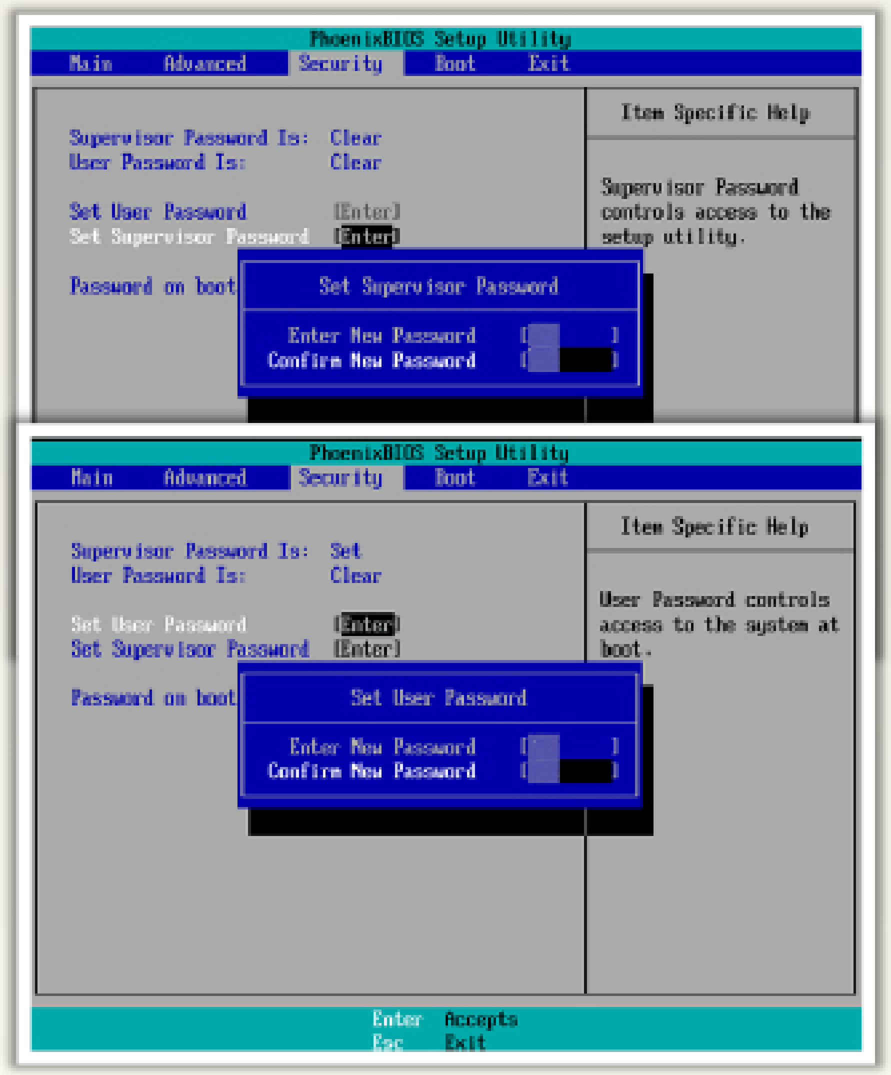
Score	Issue	Result
✗	Automatic Updates	The Automatic Updates feature has not been configured on this computer. Please upgrade to the latest Service Pack to obtain the latest version of this feature and then use the Control Panel to configure Automatic Updates. What was scanned How to correct this
!	Password Expiration	Some user accounts (1 of 2) have non-expiring passwords. What was scanned Result details How to correct this
i	Incomplete Updates	No incomplete software update installations were found. What was scanned
i	Windows Firewall	Windows Firewall is enabled and has exceptions configured. Windows Firewall is enabled on all network connections. What was scanned Result details How to correct this
✓	Local Account Password Test	Some user accounts (1 of 2) have blank or simple passwords, or could not be analyzed. What was scanned Result details
✓	File System	All hard drives (1) are using the NTFS file system.

FIGURE 6.1: Microsoft Baseline Security Analyzer

Source: https://www.microsoft.com

Setting up **BIOS Password**

- Setting up a BIOS Password is the first protection layer of the computer
- It helps you maintain OS security at a low-level
- Steps:
  1. Enter BIOS Setup Utility interface
  2. Select Security and set Supervisor Password. It will control the access to the setup utility
  3. Now, set User Password



```
Supervisor Password Is:  Clear
User Password Is:        Clear

Set User Password        [Enter]
Set Supervisor Password  [Enter]

Password on boot

        Set Supervisor Password

   Enter New Password    [    ]
 Confirm New Password    [    ]

Item Specific Help

Supervisor Password
controls access to the
setup utility.
```

```
Supervisor Password Is:  Set
User Password Is:        Clear

Set User Password        [Enter]
Set Supervisor Password  [Enter]

Password on boot

        Set User Password

   Enter New Password    [    ]
 Confirm New Password    [    ]

Item Specific Help

User Password controls
access to the system at
boot.

Enter  Accepts
Esc    Exit
```

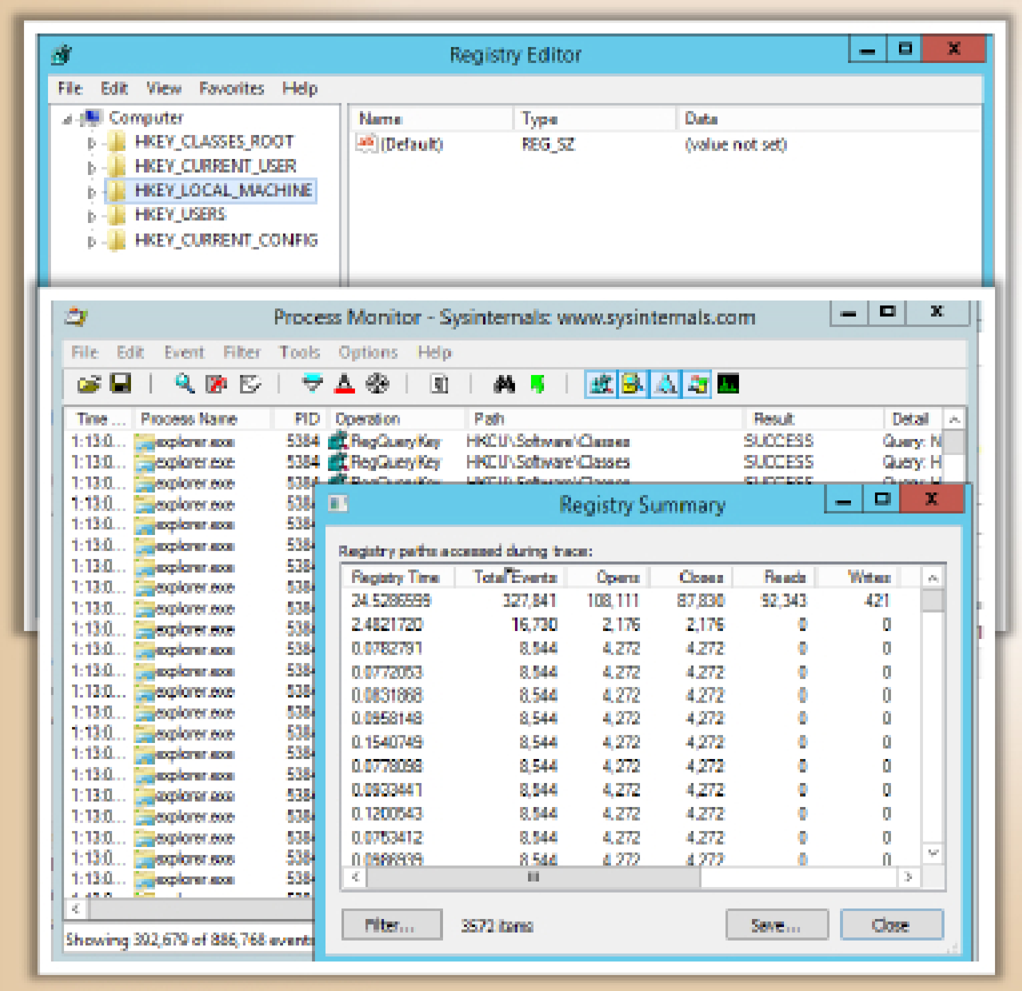
Setting up a BIOS password helps you in controlling the access of the system from external users. The BIOS of an operating system provides the feature of setting up a password that in turn prevents other users from:

- Accessing the system.
- Booting the computer.
- Booting from removable devices.
- Changing BIOS settings.

BIOS passwords are most suitable for systems in public places or a workplace that disables other users from installing another operating system over an existing one. A BIOS setup program can be used for setting a BIOS password. This is easily done by clicking any key before the booting of the operating system. Clicking on "Press F2 to enter set up" message helps the user to go the BIOS settings page. Every computer has documentation available that helps in the easy setting of the BIOS password.

The BIOS provides an extra layer of security by starting even before the operating system and other hardware starts. This allows the user to enter the password and prevents many password-cracking applications to run. It is a complex task to retain the BIOS password when compared to operating the password. Hence, users need to remember the BIOS password because if the user is unable to remember the BIOS password, then the user will be locked out. The users can always try resetting the BIOS password, but most of the time all the attempts are in vain, as it requires more time and provides only less chances of changing it.

Auditing Windows Registry



Registry Editor

File Edit View Favorites Help

- Computer
  - HKEY_CLASSES_ROOT
  - HKEY_CURRENT_USER
  - HKEY_LOCAL_MACHINE
  - HKEY_USERS
  - HKEY_CURRENT_CONFIG

Name	Type	Data
(Default)	REG_SZ	(value not set)

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
1:13:0...	explorer.exe	5384	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: N
1:13:0...	explorer.exe	5384	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: H

Showing 392,679 of 886,768 events

Registry Summary

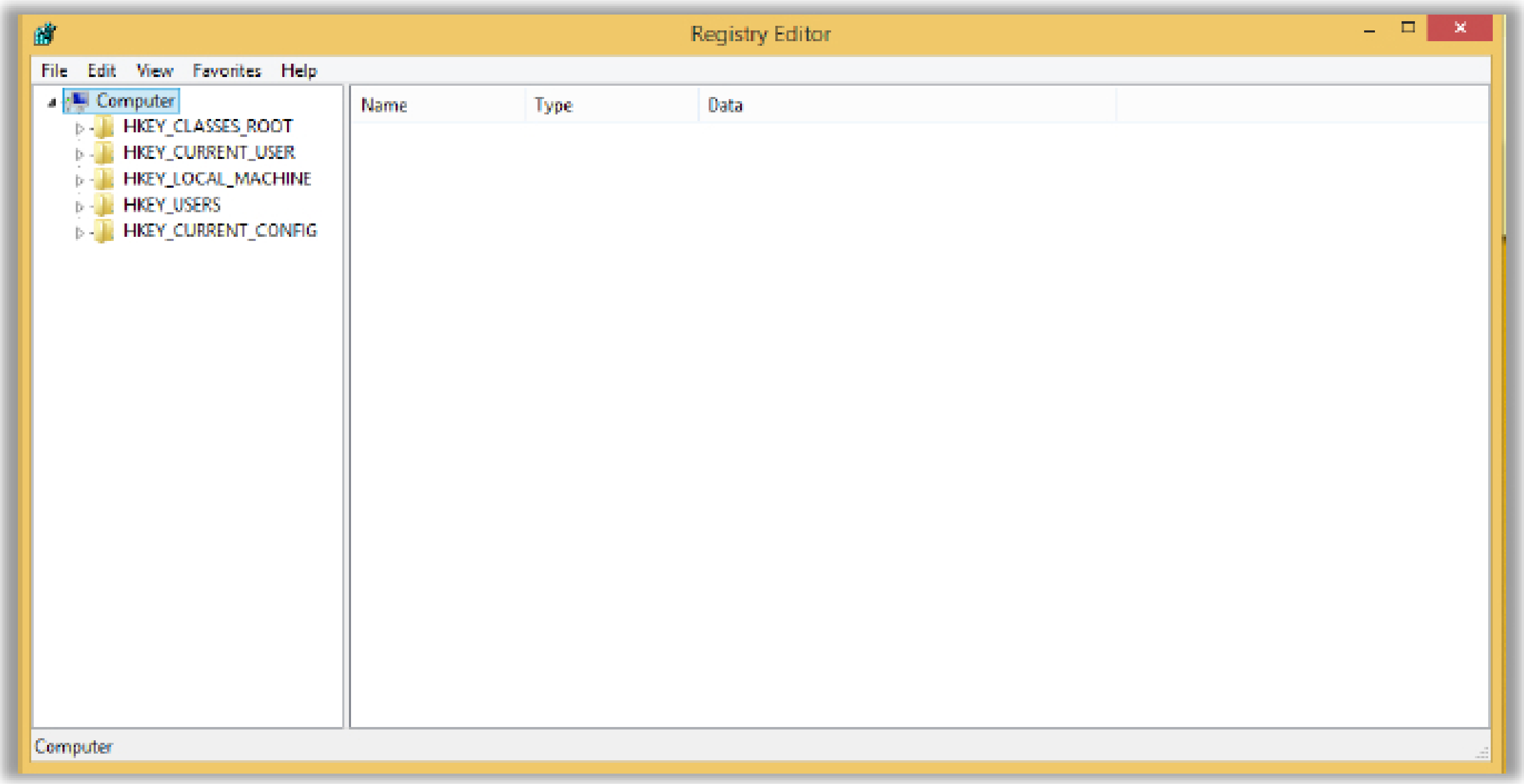
Registry paths accessed during trace:

Registry Time	Total Events	Opens	Closes	Reads	Writes
24.5286599	327,841	108,111	87,830	92,343	421
2.4821720	16,730	2,176	2,176	0	0
0.0782791	8,544	4,272	4,272	0	0
0.0772053	8,544	4,272	4,272	0	0
0.0831868	8,544	4,272	4,272	0	0
0.0958148	8,544	4,272	4,272	0	0
0.1540749	8,544	4,272	4,272	0	0
0.0778098	8,544	4,272	4,272	0	0
0.0933441	8,544	4,272	4,272	0	0
0.1200543	8,544	4,272	4,272	0	0
0.0753412	8,544	4,272	4,272	0	0
0.0986939	8,544	4,272	4,272	0	0

https://technet.microsoft.com

- Windows registry stores all the **configuration settings** of the applications and systems
- OS **records** every action taken by the user in the registry
- It maintains the **registry keys** for various user actions in terms of Log, Autorun Locations, MRU lists, UserAssist, etc.
- Organizations usually do not audit the registry of the workstations
- **Regular Monitoring and Auditing** of the registry can help you detect traces of malicious activity on the system
- Use the **Process Monitor** utility to monitor registry activity in real time

Windows registry, otherwise known as registry, is a database of all the configurational settings of Microsoft Windows. Windows registry stores details like settings for software programs, hardware devices, user preferences, OS configurations etc. At a glance, windows registry consists of all details regarding the operating system. Accessing windows registry requires the user to execute the **regedit** command in the command prompt. The windows registry window is as follows:



Registry Editor

- Computer
  - HKEY_CLASSES_ROOT
  - HKEY_CURRENT_USER
  - HKEY_LOCAL_MACHINE
  - HKEY_USERS
  - HKEY_CURRENT_CONFIG

Name	Type	Data

Computer

FIGURE 6.2: Registry Editor

A registry key is similar to folders. Folders contain files, whereas registry keys contain registry values and other sub keys. Registry Hives are the group of registry keys found at the top of the hierarchy. The registry keys are as follows:

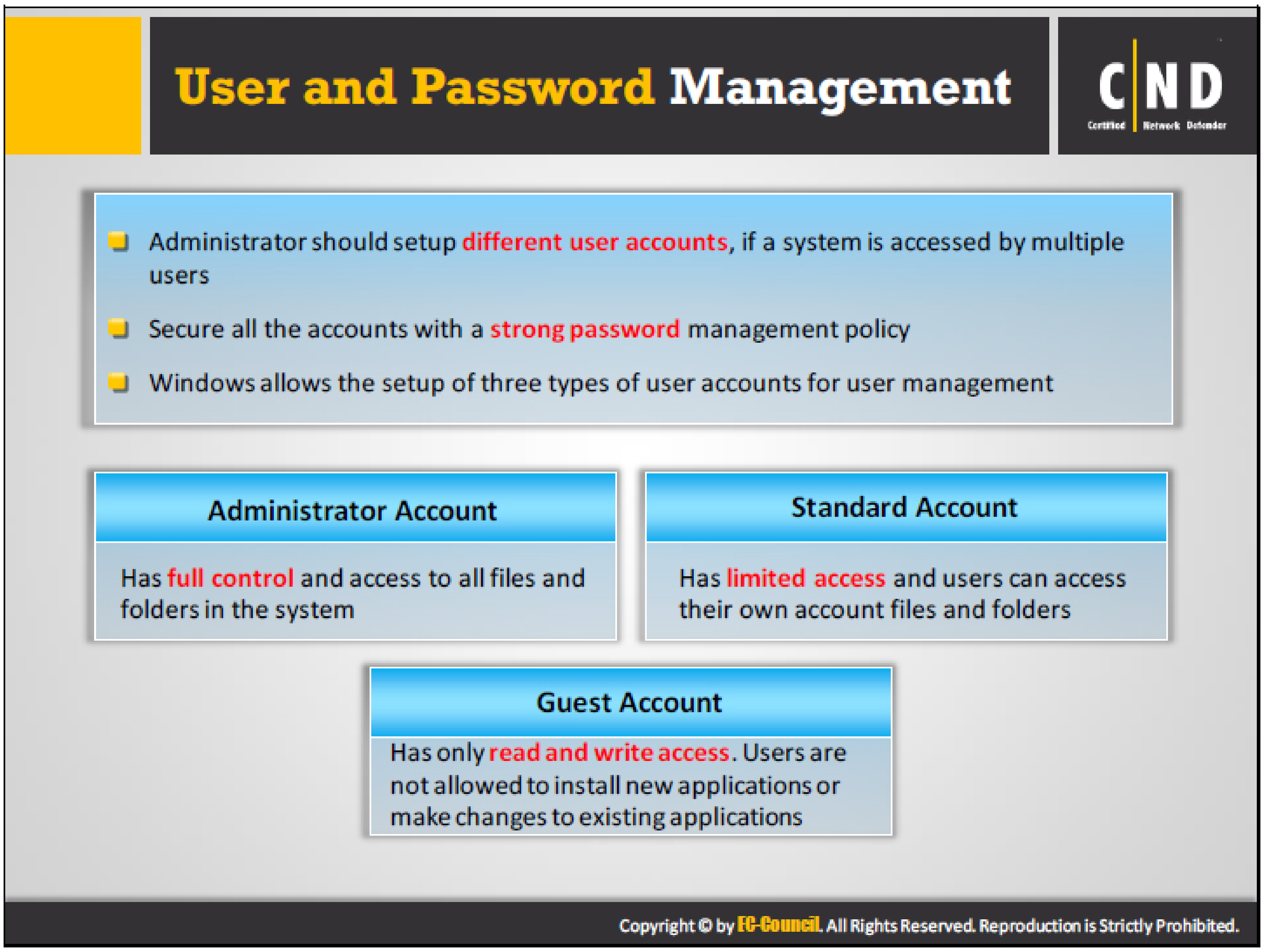
- **HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT**: Here, HKEY_LOCAL_MACHINE is the registry hive and software and Microsoft groups under this registry hive. Microsoft falls under the Software registry key.
- **HKEY_CURRENT_ CONFIG**: This registry key contains information regarding the currently used hardware profile.
- **HKEY_CURRENT_USER**: This registry gives all details regarding the users that are currently present on the computer. The user details include: desktop settings, network connections, printers, application preferences, personal program groups. A new HKEY_CURRENT_USER sub key is created every time a user logs in.
- **HKEY_CLASSES_ROOT**: This key contains the file name extensions and COM class registration information.

Process Monitor Tool

Source: *https://technet.microsoft.com*

Process monitor (Procmon) tool is one of the monitoring tools that help administrators monitor and audit the registry, file system and the network. It captures specific types of input/output operations, which might occur through the registry, file system or network. It combines the features of Filemon and Regmon, thus, giving real-time results related to file system and registry.

- **Some of the features of Process Monitor include**:
  - Captures input and output data.
  - Allows setting up filters as per the user requirement. Reducing the loss of data.
  - Gathers accurate information of process details.
  - Relationship among the processes can be traced.
  - Native log format stores all data in one location.



User and Password Management

- Administrator should setup different user accounts, if a system is accessed by multiple users
- Secure all the accounts with a strong password management policy
- Windows allows the setup of three types of user accounts for user management

Administrator Account

Has full control and access to all files and folders in the system

Standard Account

Has limited access and users can access their own account files and folders

Guest Account

Has only read and write access. Users are not allowed to install new applications or make changes to existing applications

The Windows operating system has a different view in managing the user accounts and passwords.

User management in Windows helps administrators identify and control the users logged in the system. This management includes identifying people logged into the network, managing the user login and logout times. User management provides a better authentication and authorizations of users accessing the network. Monitor user permissions before granting permission to access the network and analyze the logging details. The administrators have the benefit of analyzing the user details and activities. They can filter the user details by IP address or by user, thereby enabling easy management for the users. The whole concept of user management is based on user logging in and logging out of the system. A user trying to access the system is first authenticated and allowed access to the system. There are certain policies for user management that define certain rules for managing the user accounts.

A user can have multiple accounts or a single account. Multiple accounts in a single computer allow multiple users to store data and files in the same system, apply background themes according to each user's preference etc.

Users can create three types of accounts in Windows:

- **Administrator Account:** These account users have the complete privilege of performing any action on the system. These users can install and uninstall programs make configurational changes to the system, add or remove other user accounts in the system etc.

- **Standard Account:** Standard account users are users that have a limited access to the systems. They can access only those files and folders saved in their user account. They do not have the permission to change or delete any configurations of other users.
- **Guest Account:** These types of users do not have the access to any of the files and folders on the system. These users can only check their e-mails on the system.

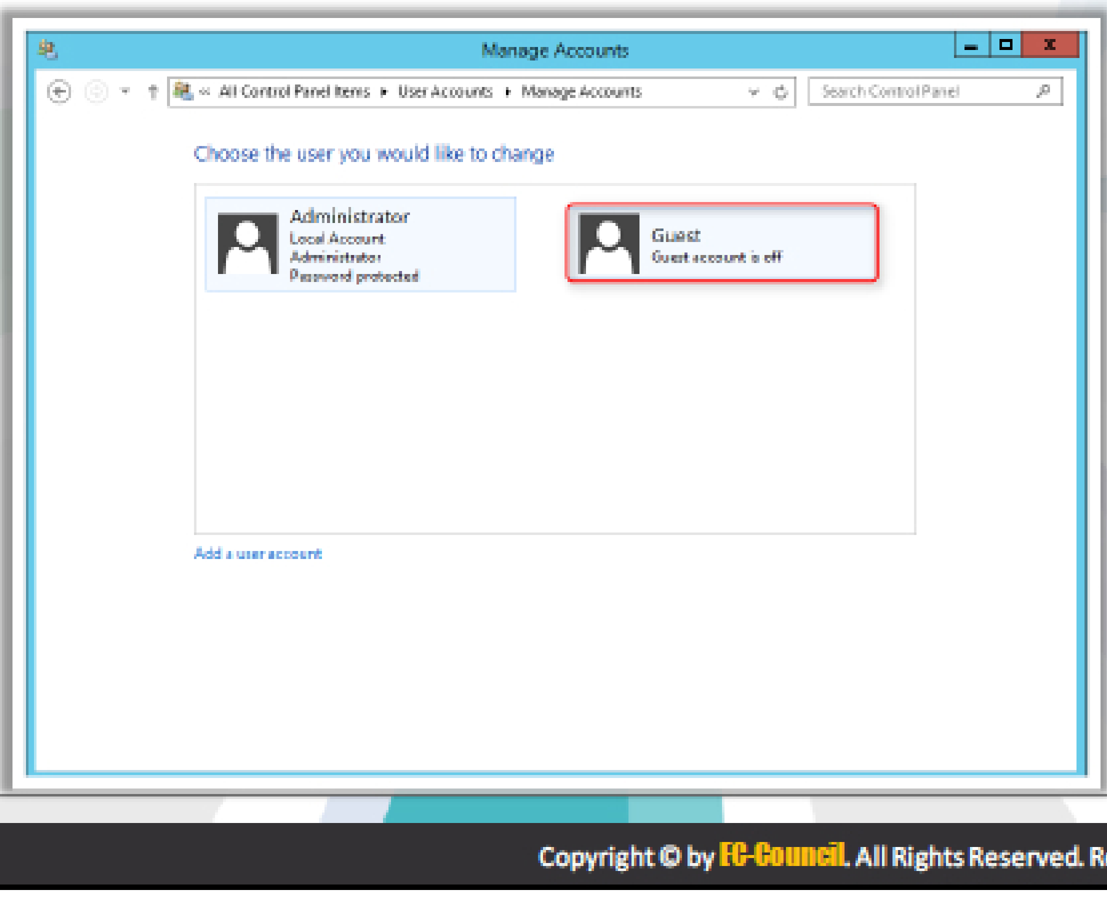
The password management in windows proceeds with the authentication of the user trying to access the system. In other words, all user accounts should be efficiently secured with passwords.

An organization should have a well-defined and effective password policy that helps in minimizing the risks of password compromise during authentication. The policies created need to ensure the availability, confidentiality and integrity of the passwords. Allowing access to only authorized users and preventing unauthorized access. Several access controls assist in maintaining the integrity and availability of passwords, whereas, maintaining the confidentiality of the passwords always remain a challenge to the organization. Maintaining the confidentiality of the password includes several security controls and decisions.

- Some of the **guidelines** for creating strong and complex passwords are:
  - Ensure that the password created does not include the user name.
  - Construct it using a combination of uppercase characters, lowercase characters, digits, special characters.
  - Avoid using the password used previously.
  - Change the passwords periodically.
  - The passwords need to be a minimum of eight characters in length.
  - The password should not be a word from a dictionary.
  - Always set a length for the passwords.
  - Avoid storing the passwords at any location. If you need to store it, do so in an encrypted form.
  - Do not share the password.
- **Best practices** for using passwords in a better way are:
  - Train users on the best ways to protect the passwords.
  - Make them aware of the various forms of attacks on passwords.
  - Use encryption techniques in order to securely store the password.
  - Properly define the password security policies followed throughout the organization.

Disabling Unnecessary User Accounts

1. Go to Control Panel → User Accounts → Manage Accounts
2. Turn Off The Guest Account, if it is ON
3. The guest account users can make unauthenticated access to the Internet



Manage Accounts

All Control Panel Items ▸ User Accounts ▸ Manage Accounts

Search Control Panel

Choose the user you would like to change

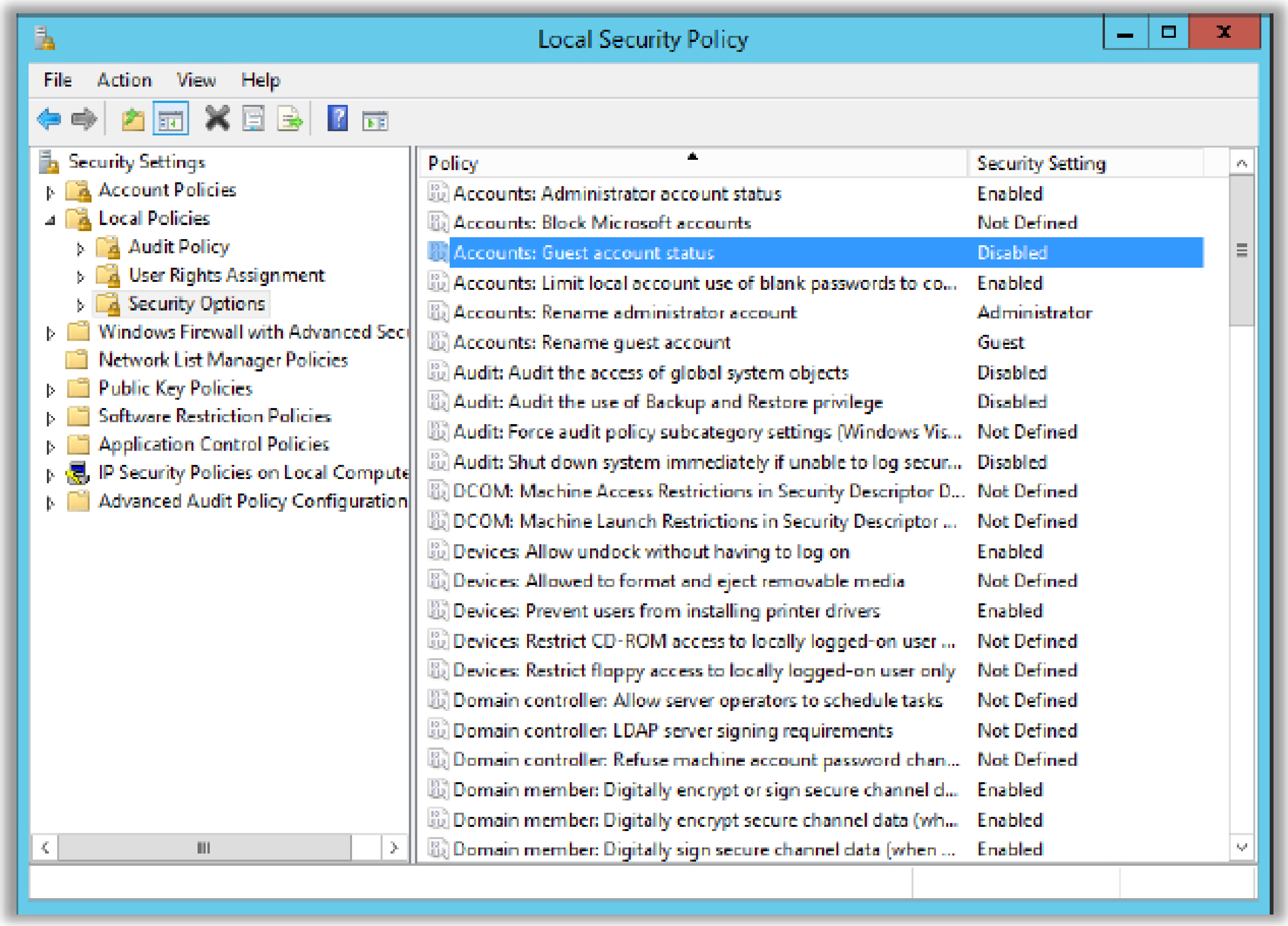
Administrator
Local Account
Administrator
Password protected

Guest
Guest account is off

Add a user account

Administrators should disable unwanted accounts by deactivating them. Deleting a user account is entirely different from disabling an account. Disabled user accounts can be restored, whereas deleted user accounts cannot be restored. Here are the steps for disabling a user account in Windows:

- Go to **Control Panel** and press **Enter**
- Select the option **Administrative Tools**
- Click on **Local Security Policy**
- Click on **Local Policies** option on the left side of the pane and click on **Security Options** under it. Find the option **'User Account Control'** from the list of options in the results pane. **Disable the user account** option

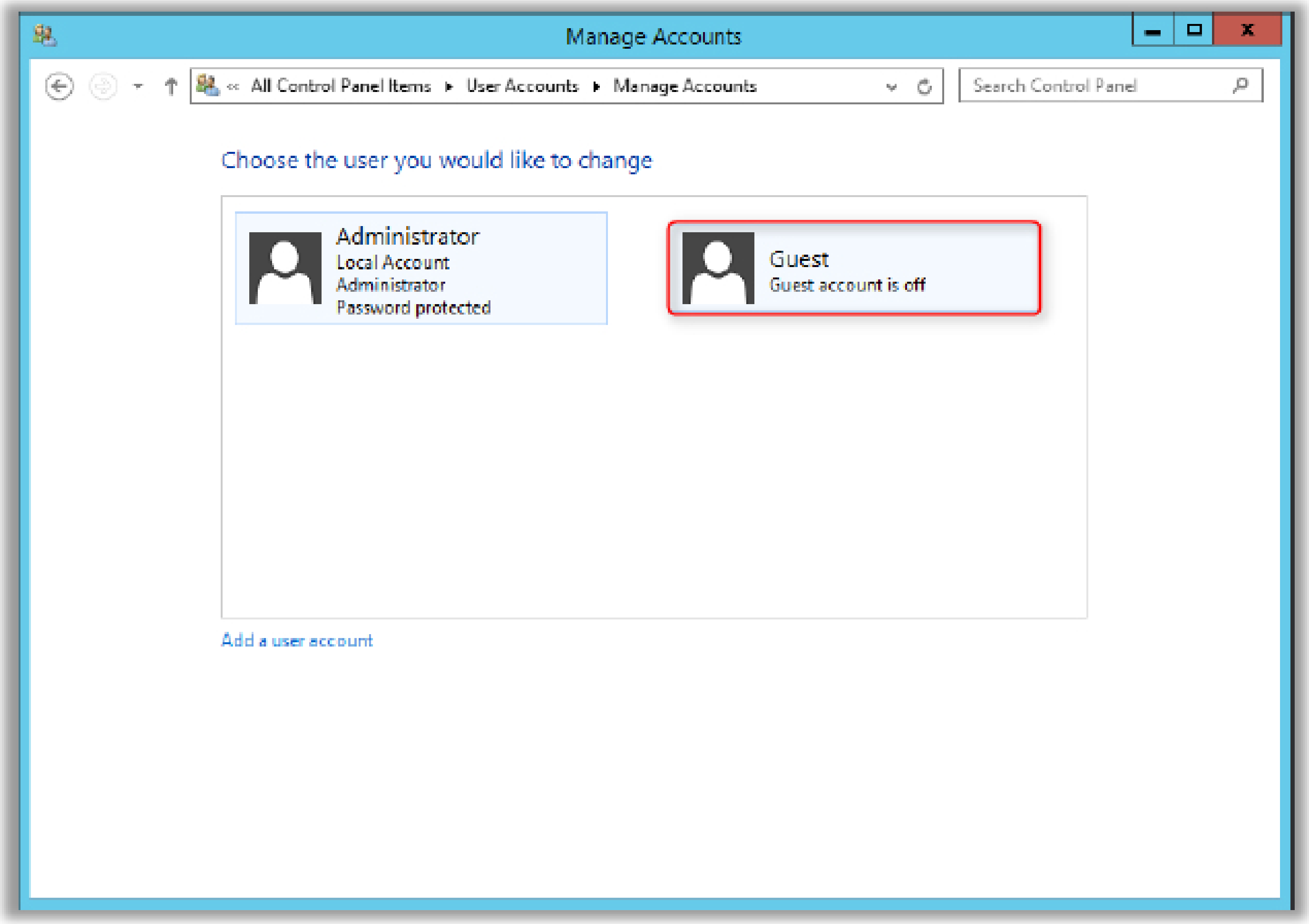

Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Sec
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Accounts: Administrator account status	Enabled
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to co...	Enabled
Accounts: Rename administrator account	Administrator
Accounts: Rename guest account	Guest
Audit: Audit the access of global system objects	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled
Audit: Force audit policy subcategory settings (Windows Vis...	Not Defined
Audit: Shut down system immediately if unable to log secur...	Disabled
DCOM: Machine Access Restrictions in Security Descriptor D...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor ...	Not Defined
Devices: Allow undock without having to log on	Enabled
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Enabled
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password chan...	Not Defined
Domain member: Digitally encrypt or sign secure channel d...	Enabled
Domain member: Digitally encrypt secure channel data (wh...	Enabled
Domain member: Digitally sign secure channel data (when ...	Enabled

FIGURE 6.3: Disabling Unwanted Accounts

An alternative method for the above mentioned step is as follows:

1. Go to **Control Panel → User Accounts → Manage Accounts**
2. Turn Off the Guest Account if it is **On**



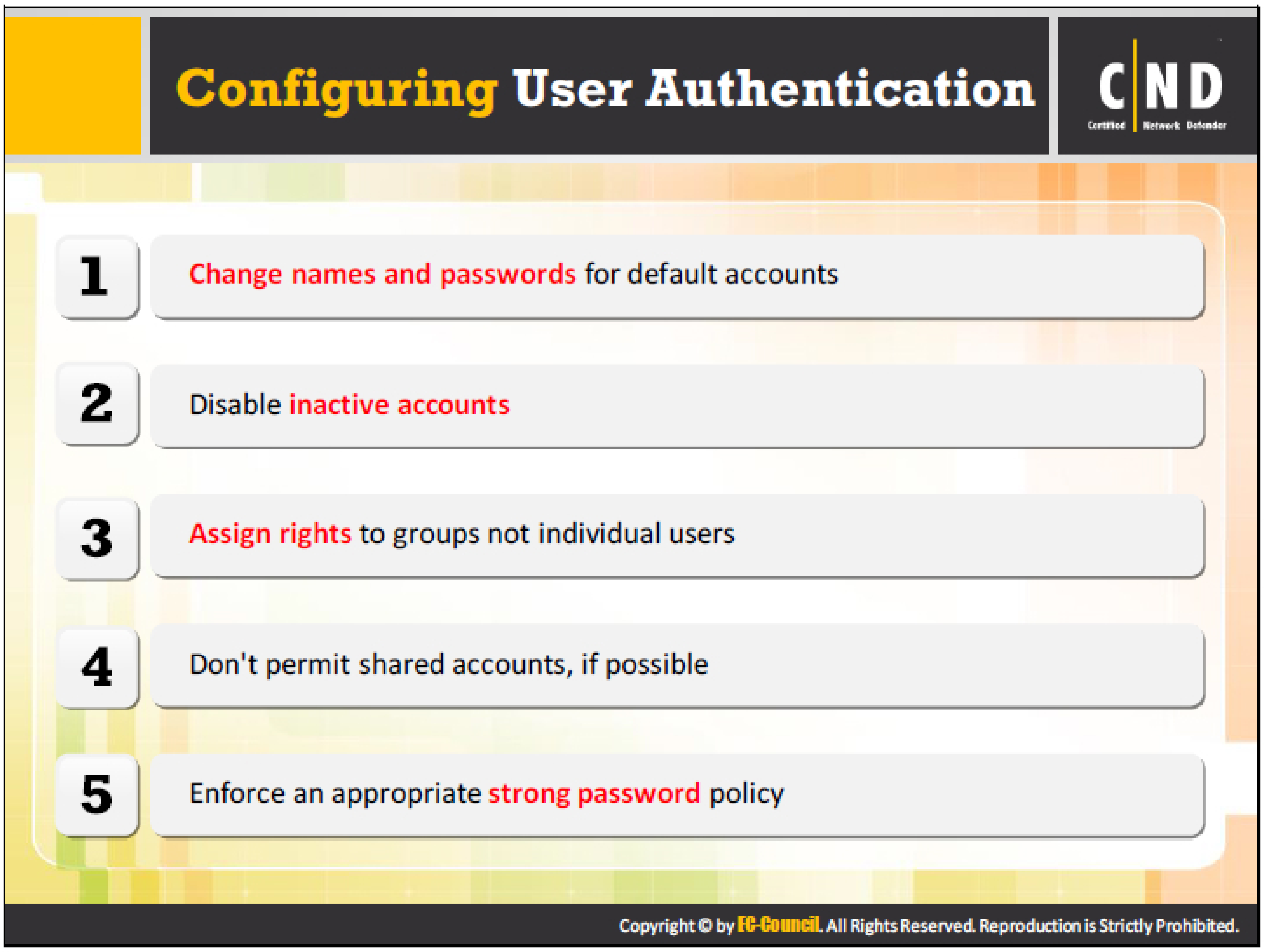
Choose the user you would like to change

Administrator
Local Account
Administrator
Password protected

Guest
Guest account is off

Add a user account

FIGURE 6.4 Managing Accounts

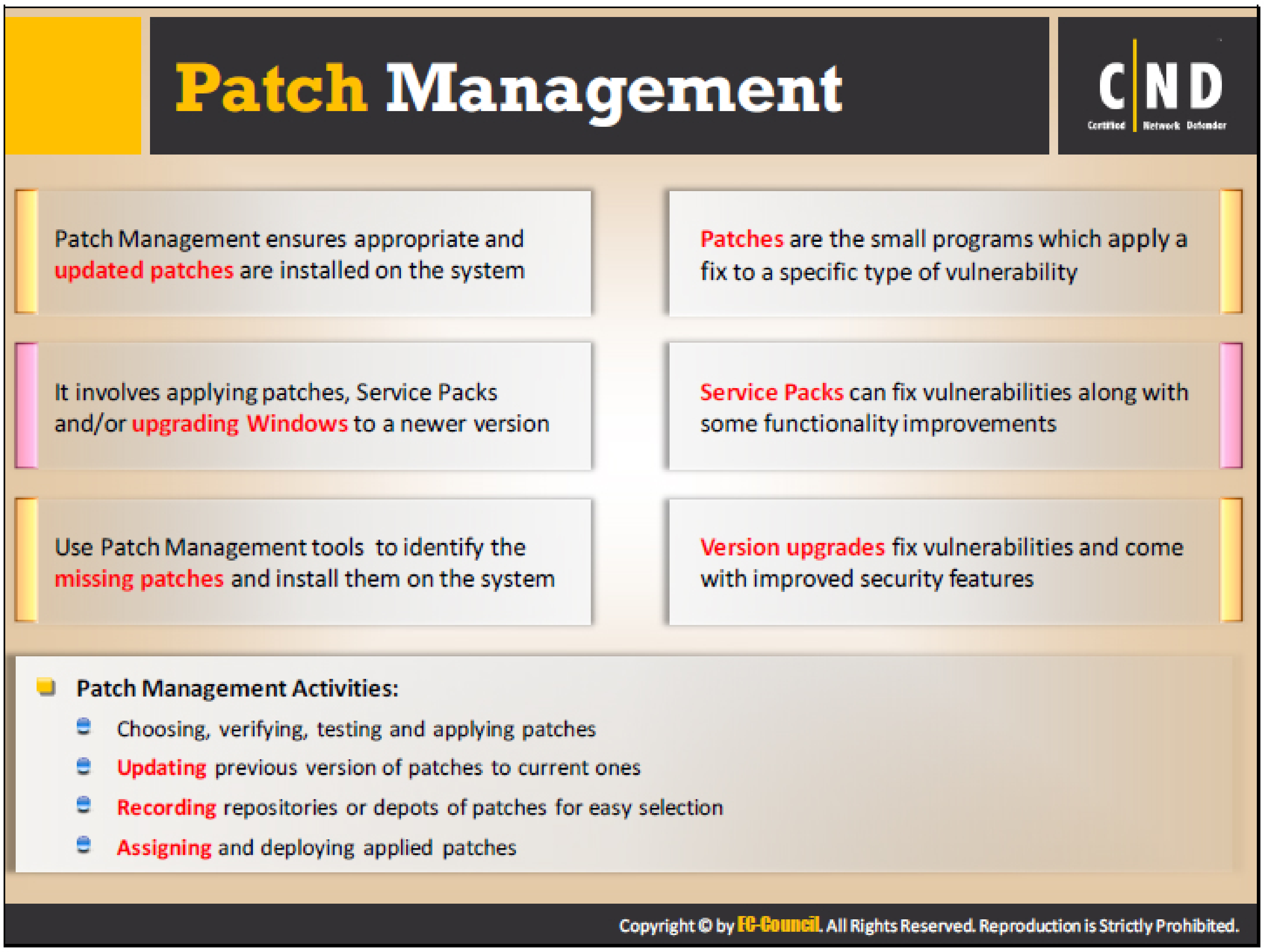


Configuring User Authentication

1. Change names and passwords for default accounts
2. Disable inactive accounts
3. Assign rights to groups not individual users
4. Don't permit shared accounts, if possible
5. Enforce an appropriate strong password policy

Authentication validates and identifies the users accessing the application. It defines whether the user trying to access the system has user permissions to access and to perform actions.

- **Change names and passwords for default accounts:** Systems which have multiple accounts should maintain different usernames and passwords.
- **Disable inactive accounts:** If an employee leaves the company it is the role of the administrator to disable/delete all the accounts of the employee. Timely action can save the resources of the system from intrusion.
- **Assign rights to groups not individual users:** Administrators should deploy and implement group policy in the organization. Group policies allow the administrators to assign rights to specific users. Implementation of group policies makes it easy for administrators to monitor the user activities.
- **Do not permit shared accounts**: Avoid shared accounts in a network. Accounts shared by users act as an open invitation to intruders.
- **Enforce appropriate strong password policy:** Administrators should encourage users to create strong passwords for their accounts. Easy passwords are more vulnerable to threats.



Patch Management

Patch Management ensures appropriate and updated patches are installed on the system

Patches are the small programs which apply a fix to a specific type of vulnerability

It involves applying patches, Service Packs and/or upgrading Windows to a newer version

Service Packs can fix vulnerabilities along with some functionality improvements

Use Patch Management tools to identify the missing patches and install them on the system

Version upgrades fix vulnerabilities and come with improved security features

- **Patch Management Activities:**
  - Choosing, verifying, testing and applying patches
  - Updating previous version of patches to current ones
  - Recording repositories or depots of patches for easy selection
  - Assigning and deploying applied patches

Patch management is an integral part of OS security. Patch management enhances the security of the system with regular updates. In an IT infrastructure, patch management needs to be efficient in order to maintain the security of the system. Patch management involves applying patches, service packs or upgrading the OS to a newer version. Patch management facilitates a consistent configured environment that is secure against the vulnerabilities and threats on an operating system.

- **Patch Management Process:**
  - **Detect**: Install tools that can automatically detect updates and initiate the patch management process.
  - **Assess**: Identify the severity of the vulnerabilities and the amount of patch required to remove the error.
  - **Acquire**: Take the patch for testing if proper security measures are not taken for the detected vulnerabilities.
  - **Test**: Conduct a patch on a test system.
  - **Deploy**: Deployment of all the patches to other systems.
  - **Maintain**: Maintain all other systems by sending notifications regarding the detected vulnerabilities.

- The patch management process can be implemented in two ways on the user machines:
  - Distribute a written process among the employees that can be implemented on their host machines.
  - Implement an auto patch management system that allows the administrators to control the deployment of the patches on host machines.
- **Patch Management Processes:**
  - **Written Process:** In this process, the organization trusts their employees by allowing them to install patches and keep their system updated. In such scenarios, organizations randomly check the systems of the users to make sure, if employees adhere to the patch management policy. However, following this process in an organization is not safe and can easily expose the IT infrastructure to intrusions.
  - **Automated Process:** Automated process is more reliable in terms of keeping the security of the organization. Once the vendors release the security updates, it becomes the responsibility of the administrators to apply those patches in time. These updates can fix the security vulnerabilities of the system that may occur in the systems or in the network. Installation of security patches reduces the risk of data loss.
- **Patch Management Principles:**
  - Every patch management strategy should have a service pack.
  - Product lifecycle can be a key element in the patch management strategy.
  - Perform risk assessment.
  - Use mitigating factors for determining applicability and priority.
  - Use only workarounds for deployment.
  - Use only methods available for the detection and deployment.

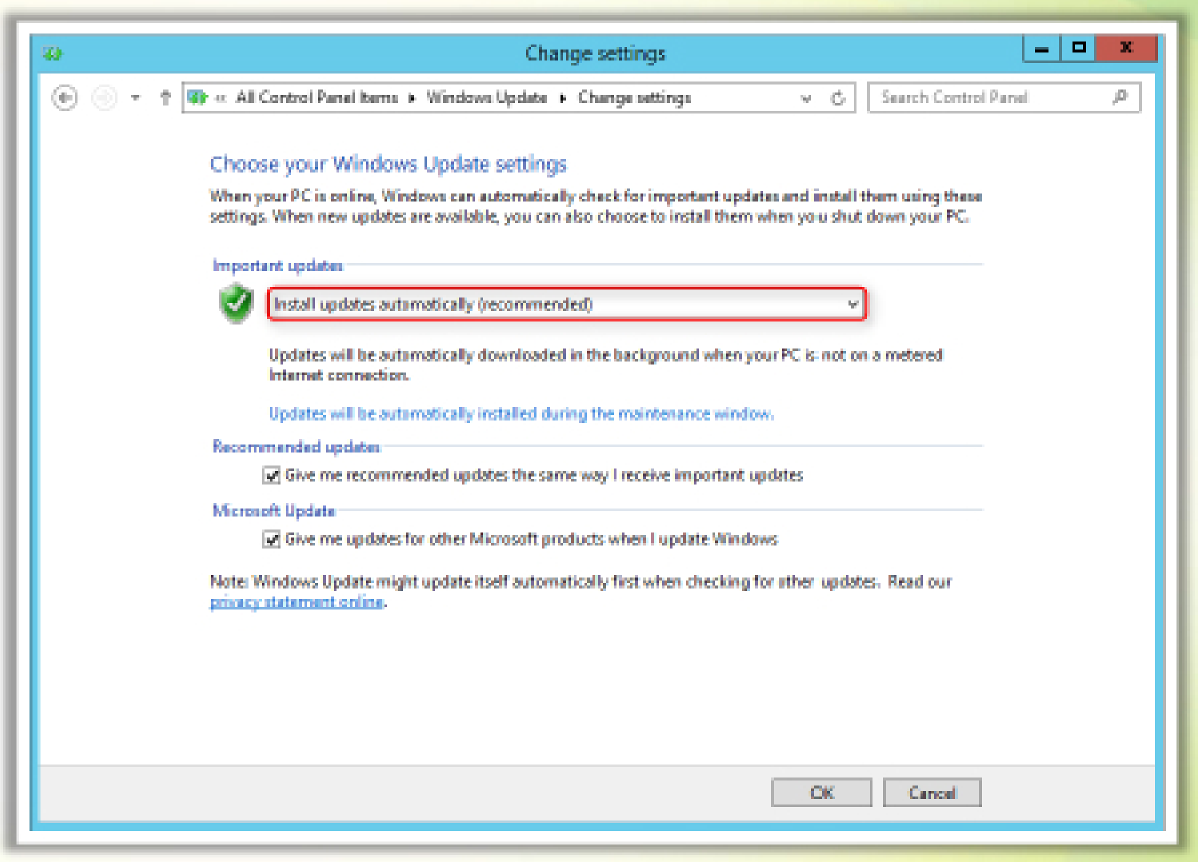
Administrators should be aware of the security requirements of their organization and ensure that patch management is based on those requirements. They can also inform other users regarding the security patch and updates. Several scheduling and prioritizing is required in performing patch management in windows. Every patch management needs to have a patch cycle that provides a standard application for the patches and updates.

Configuring an Update Method for Installing Patches

1. Go to Start → Control Panel → System and click Windows Updates and select option Install update automatically
2. You can also use a third-party Windows update tool for remote-desktop patch management

Advantages of automated patching

- You can force updates to install by specific date
- Computers not on the Internet can receive updates
- Users cannot disable or circumvent updates



Choose your Windows Update settings

When your PC is online, Windows can automatically check for important updates and install them using these settings. When new updates are available, you can also choose to install them when you shut down your PC.

Important updates

Install updates automatically (recommended)

Updates will be automatically downloaded in the background when your PC is not on a metered Internet connection.

Updates will be automatically installed during the maintenance window.

Recommended updates

☑ Give me recommended updates the same way I receive important updates

Microsoft Update

☑ Give me updates for other Microsoft products when I update Windows

Note: Windows Update might update itself automatically first when checking for other updates. Read our privacy statement online.

The Windows OS provides users the option of automated updates. Turning on the windows automatic updates in the control panel enables Windows to download and install all the updates. The process can take place automatically without much interaction from the user. However, the user must respond on time to the alerts that occur during the update process. Missing out on any alert can actually stop any important updates.

- **Windows Update Requirements:**
  - Windows 8: Update to Windows 8.1 or Windows 10.
  - Windows 7: The device should include service pack 1 in order to receive security fixes through windows update.

The user must ensure there is enough disk space available before performing a Windows update. Windows can configure updates properly if around ten percent of the system partition capacity is free.

There are situations wherein the automatic windows update is turned off for a very long time. Here, the user needs to perform an anti-virus scan before even applying the updates. The scanning can ensure that no malware is present in the system.

Accessing Windows Update Configuration

- **Windows 10:**
  - Open **Start** Menu
  - Type **Advanced** or **Update** in the search box
  - Click **Advanced Windows Update options** under settings category

At times, the window for Advanced Windows Update option might open and close immediately. The user needs to repeat the same process until the window opens properly.

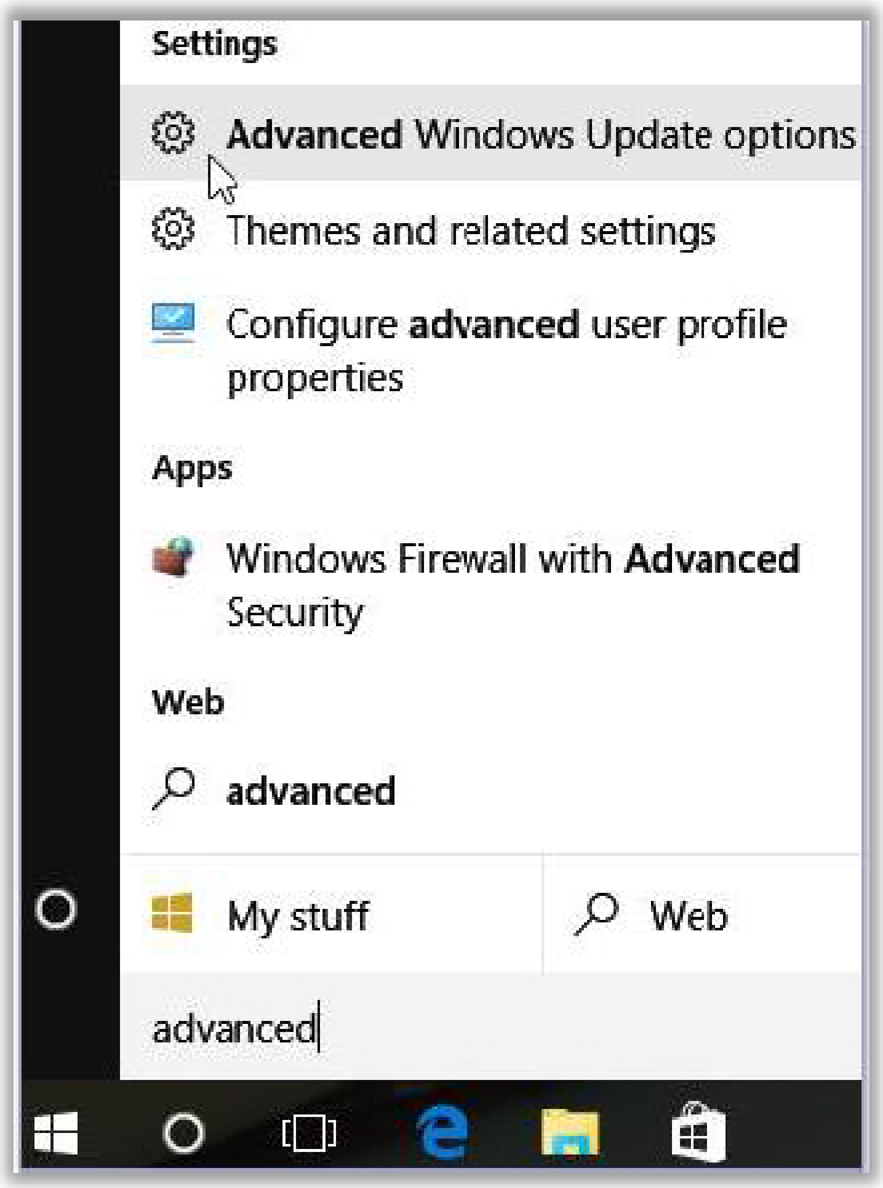

Settings
Advanced Windows Update options
Themes and related settings
Configure advanced user profile properties
Apps
Windows Firewall with Advanced Security
Web
advanced
My stuff
Web
advanced

FIGURE 6.5: Advanced Windows Update options in Windows 10

- **Windows 8:**
  - Open **Start** Menu
  - Type **Advanced** or **Update** in the search box
  - Click on **Optional Updates**

In Windows 8, the user may find another option Windows Update. This update option does not provide any configuration option and hence the users must be careful while selecting the option for update in Windows 8

- **Windows 8.1**
  - Open **Start** Menu
  - Type **Advanced** or **Update** in the search box

- Click on **Windows Updates**

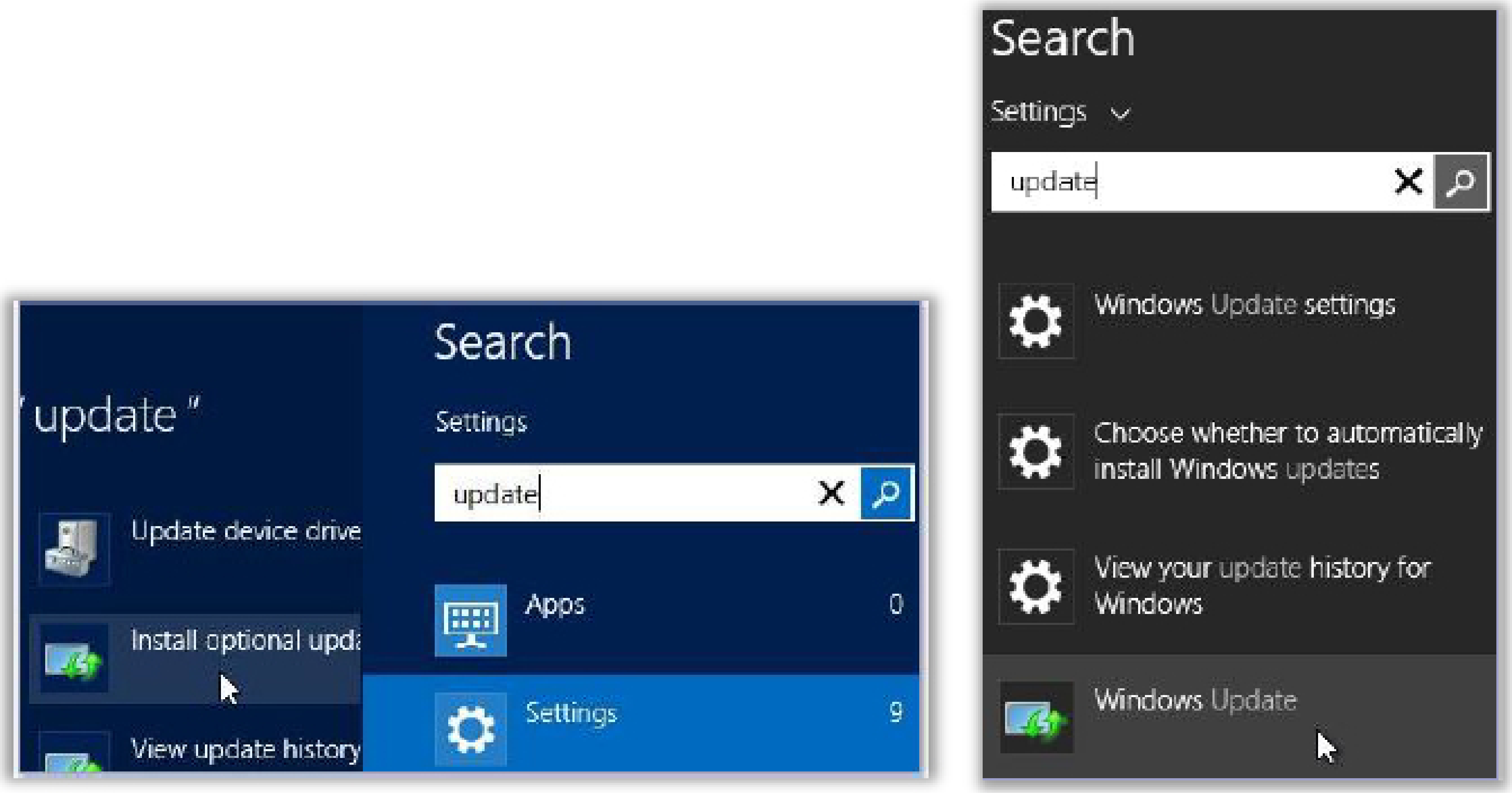
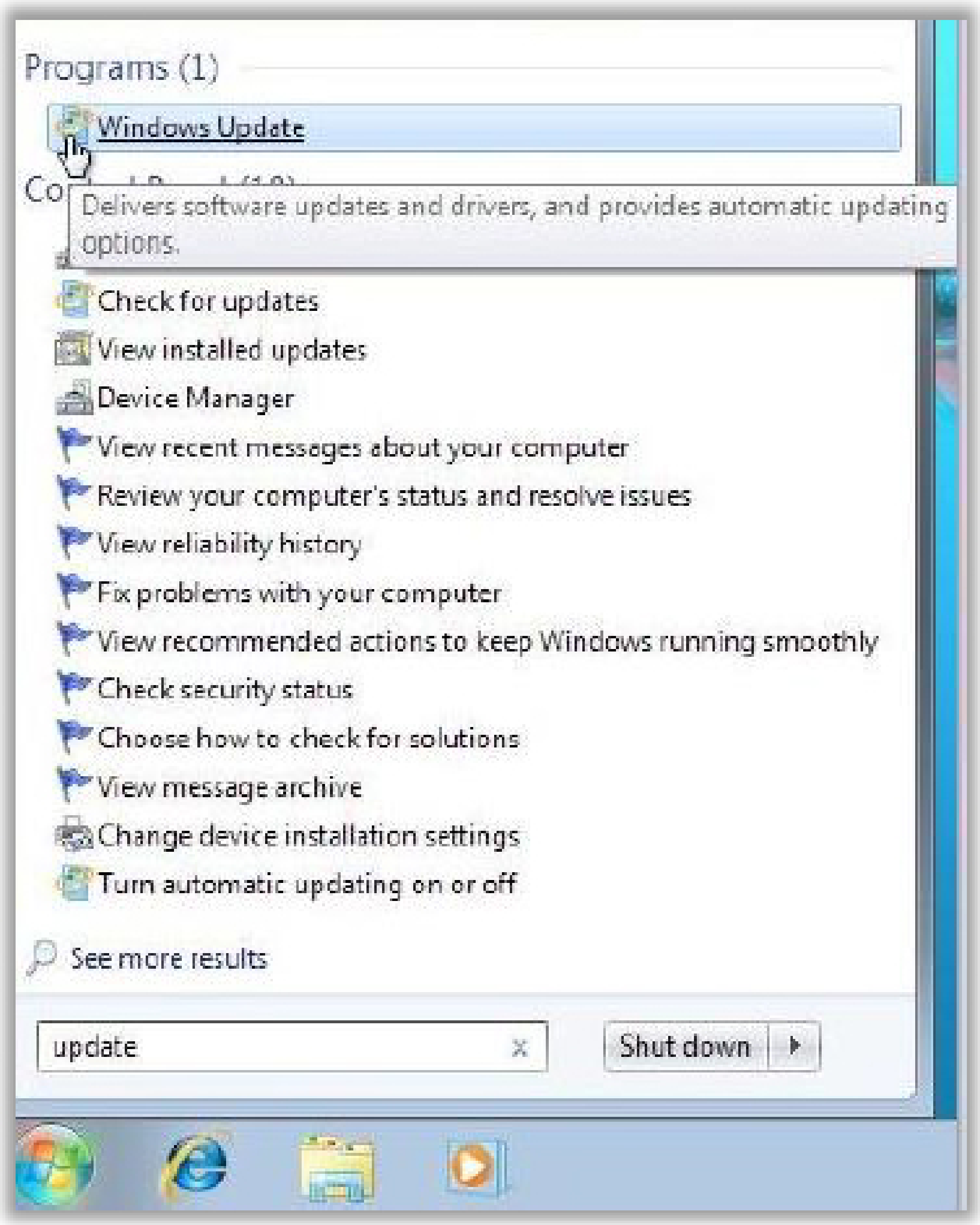


FIGURE 6.6: Windows Update option in Windows 8 and 8.1

- **Windows 7:**
  - Open **Start** Menu
  - Type **Update** in the search box
  - Click **Windows Update**


Programs (1)
Windows Update
Co
Check for updates
View installed updates
Device Manager
View recent messages about your computer
Review your computer's status and resolve issues
View reliability history
Fix problems with your computer
View recommended actions to keep Windows running smoothly
Check security status
Choose how to check for solutions
View message archive
Change device installation settings
Turn automatic updating on or off
See more results
update
Shut down

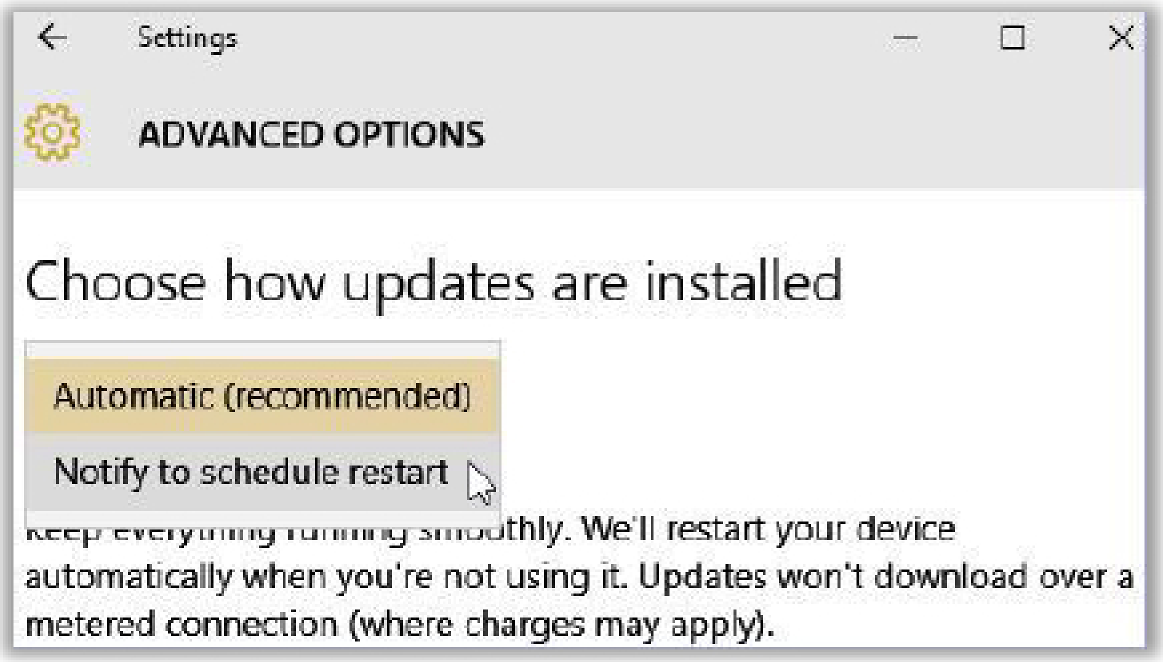
Delivers software updates and drivers, and provides automatic updating options.

FIGURE 6.7: Windows Update option in Windows 7

Enabling and Scheduling Windows Update

Windows may release the updates, service packs, fixes after the scheduled date. Windows checks for all updates the next time the user turns on the computer and connects to the network. The recommended update settings for **Windows 10** are as follows:

- In Windows 10, the configuration updates are available in Modern UI/ Metro style settings app. The user can actually schedule the restart after Windows update in the Choose how updates are installed screen. There are two options in the drop-down – Automatic (Recommended) and Notify to schedule restart. Clicking on **Notify to schedule restart** allows the user to know if there is a need for a reboot or restart of the device



Choose how updates are installed

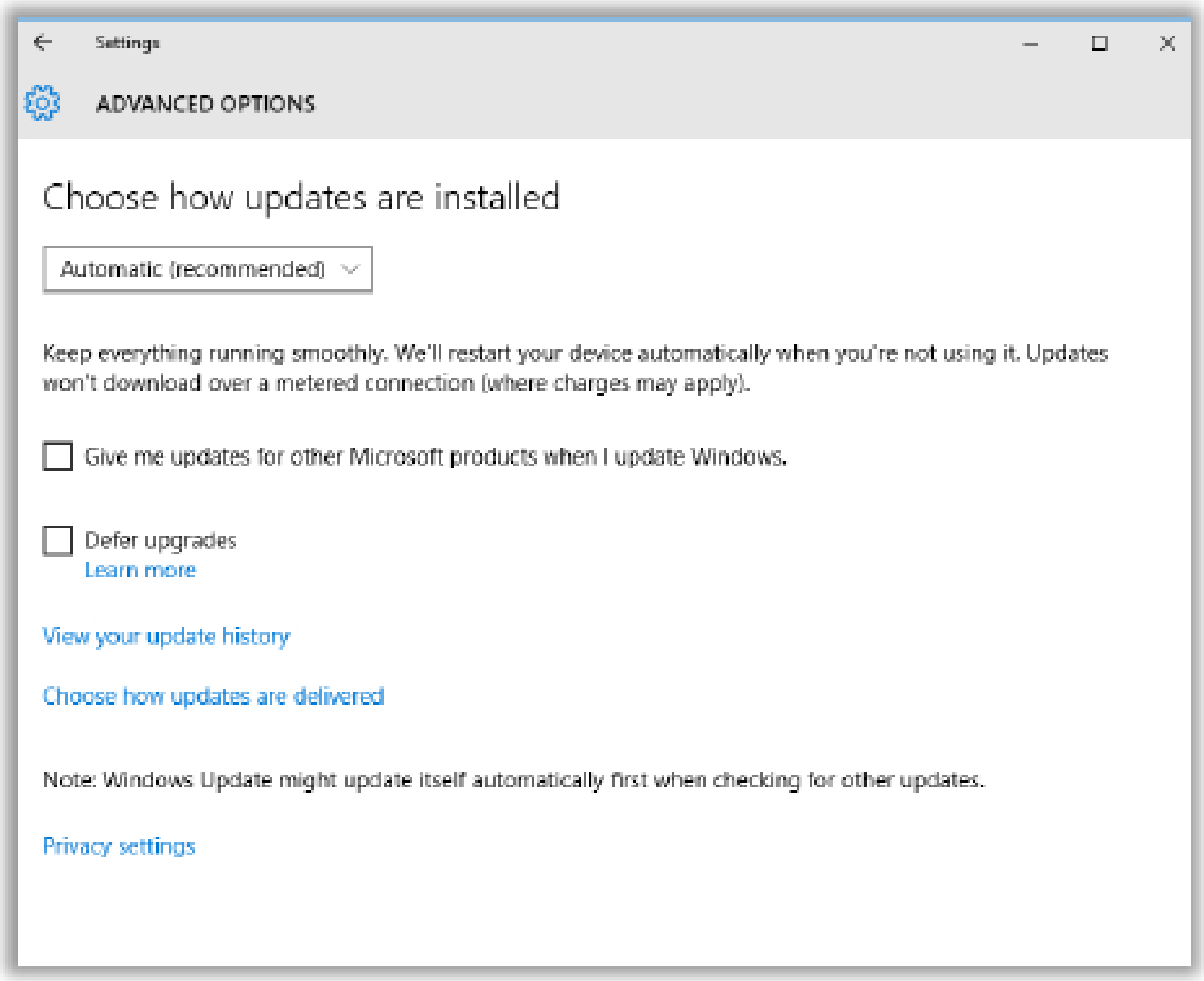
Automatic (recommended)

Notify to schedule restart

Keep everything running smoothly. We'll restart your device automatically when you're not using it. Updates won't download over a metered connection (where charges may apply).

FIGURE 6.8: Selecting the method of installing updates (Step 1)

- Select the check box for the option **Give me updates for other Microsoft products when I update Windows**. This provides updates to Microsoft products
- Make sure the users do not select the option Defer Updates as it postpones large feature upgrades



Choose how updates are installed

Automatic (recommended)

Keep everything running smoothly. We'll restart your device automatically when you're not using it. Updates won't download over a metered connection (where charges may apply).

□ Give me updates for other Microsoft products when I update Windows.

□ Defer upgrades
Learn more

View your update history

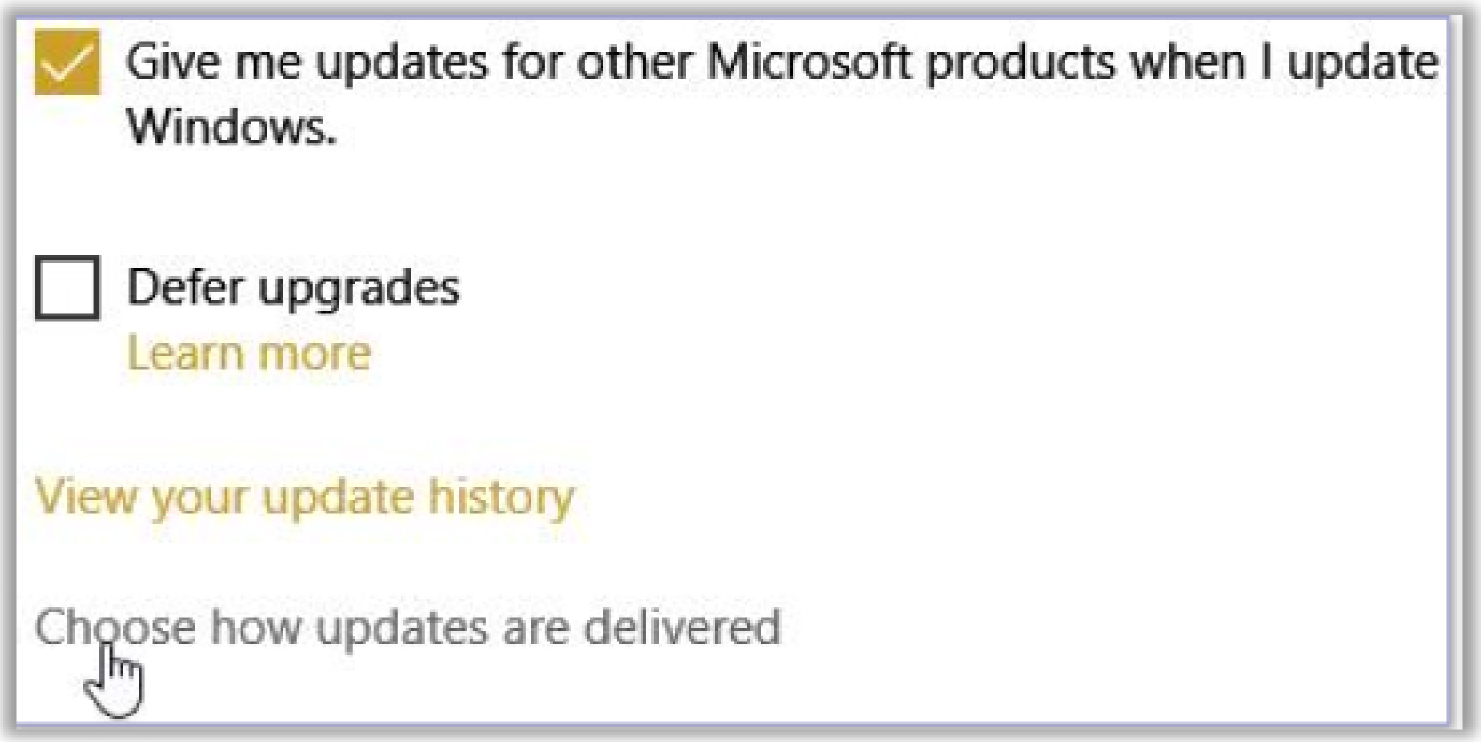
Choose how updates are delivered

Note: Windows Update might update itself automatically first when checking for other updates.

Privacy settings

FIGURE 6.9: Options to select for Automatic (recommended) update installation (Step 2)

- The user can now click on **Choose how updates are delivered**



☑ Give me updates for other Microsoft products when I update Windows.

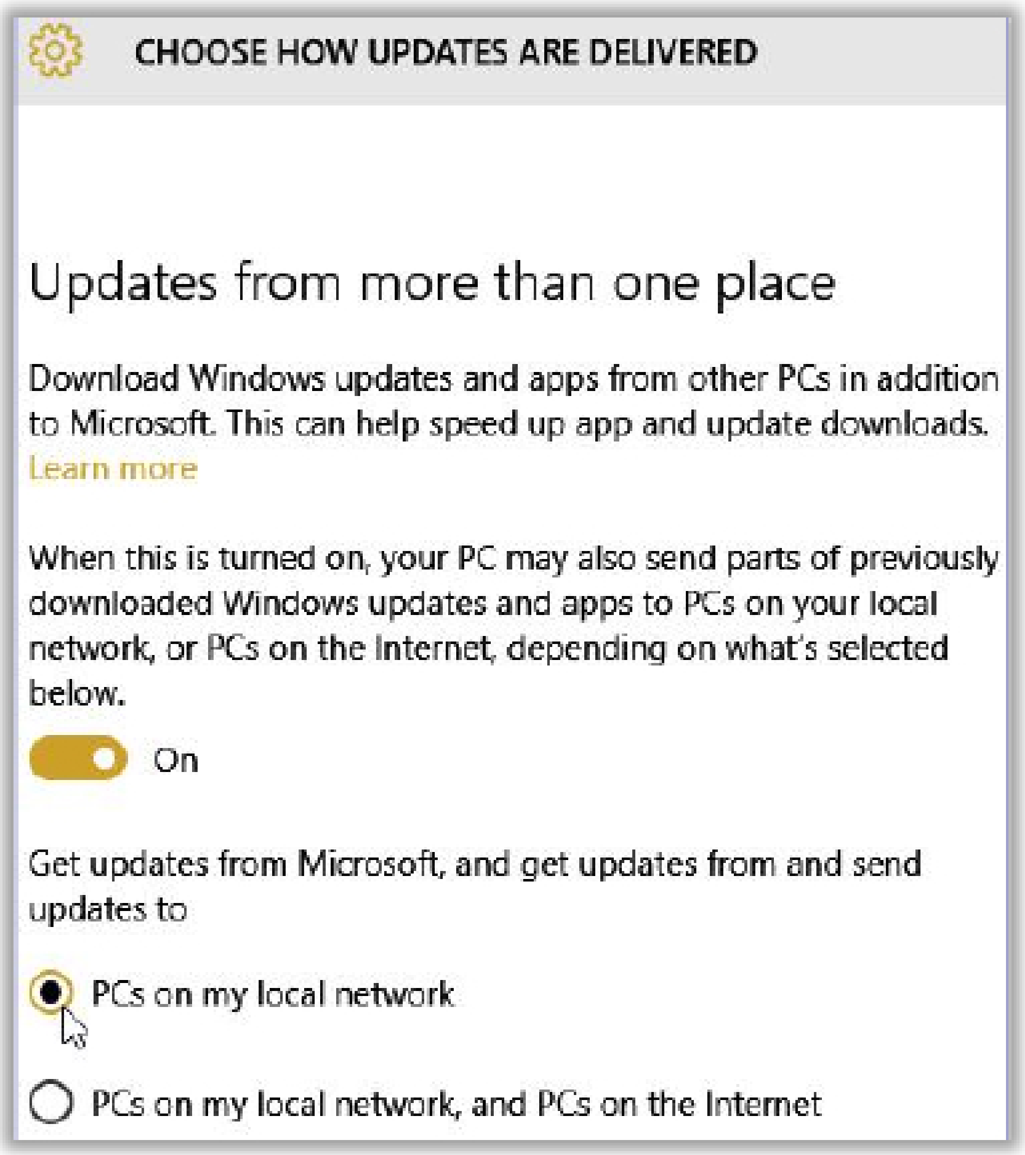
□ Defer upgrades
Learn more

View your update history

Choose how updates are delivered

FIGURE 6.10: Selecting the option for when to receive updates (Step 3)

- Updates from more than one place allows applying the same updates to many Windows 10 devices
- The slider option can be turned off if there is only one Windows 10 device
- If there are several Windows 10 devices, turn the slider on and enable the option **Updates from more than one place**
- Select the option **PC's on my local network**
- Make sure the users do not select the option PC's on my local network and PC's on the internet. This option can allow attackers to achieve a connection to the device



CHOOSE HOW UPDATES ARE DELIVERED

Updates from more than one place

Download Windows updates and apps from other PCs in addition to Microsoft. This can help speed up app and update downloads.
Learn more

When this is turned on, your PC may also send parts of previously downloaded Windows updates and apps to PCs on your local network, or PCs on the Internet, depending on what's selected below.

On

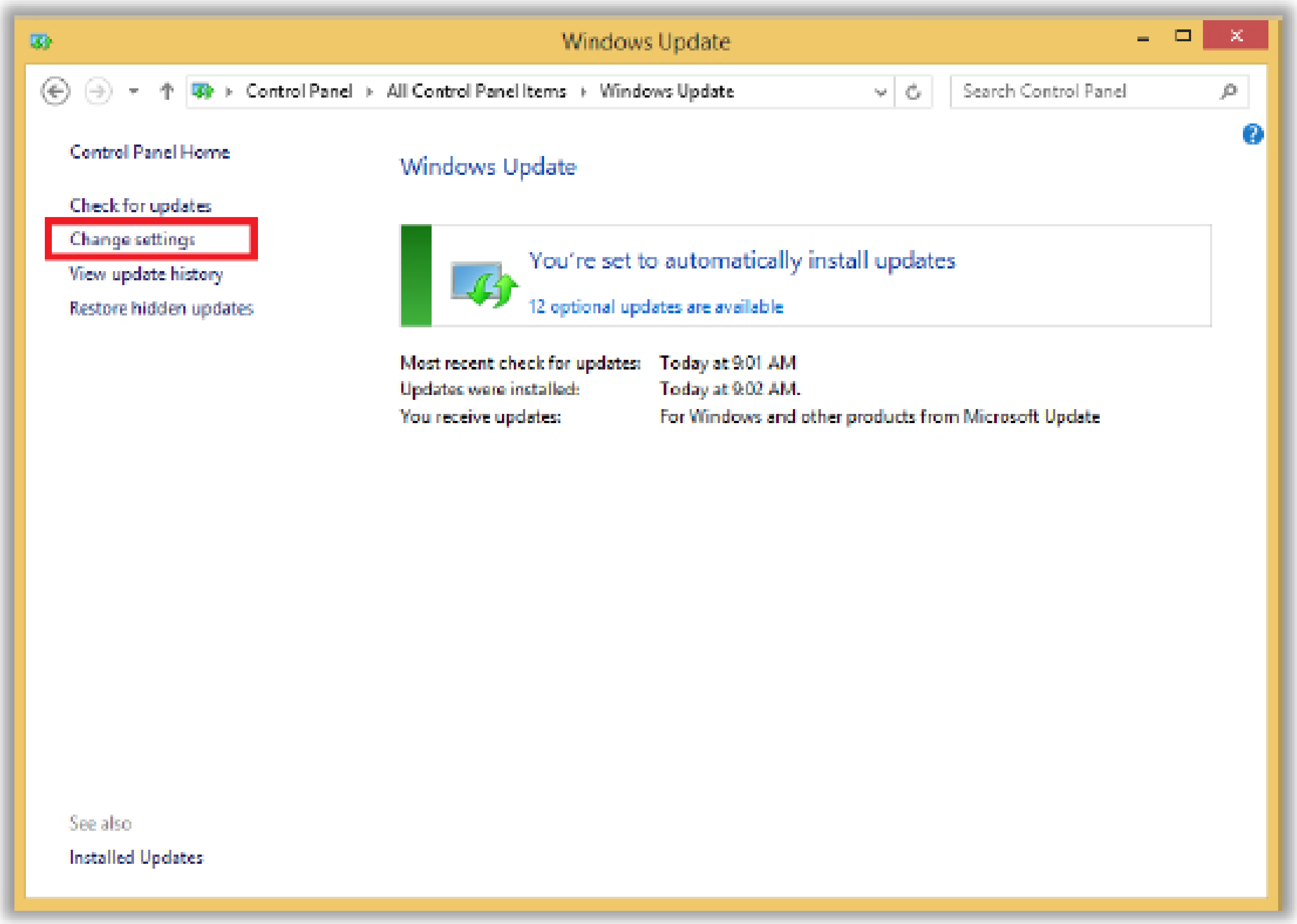
Get updates from Microsoft, and get updates from and send updates to

● PCs on my local network

○ PCs on my local network, and PCs on the Internet

FIGURE 6.11: Selecting the option to install updates for more than one Windows 10 machine (Step 4)

- The recommended update settings for **Windows 8, 8.1 and 7**
    - Open **Start** Menu
    - Type **Advanced** or **Update** in the search box
    - Click on **Windows Updates**
    - Click on **Change settings** option



Windows Update

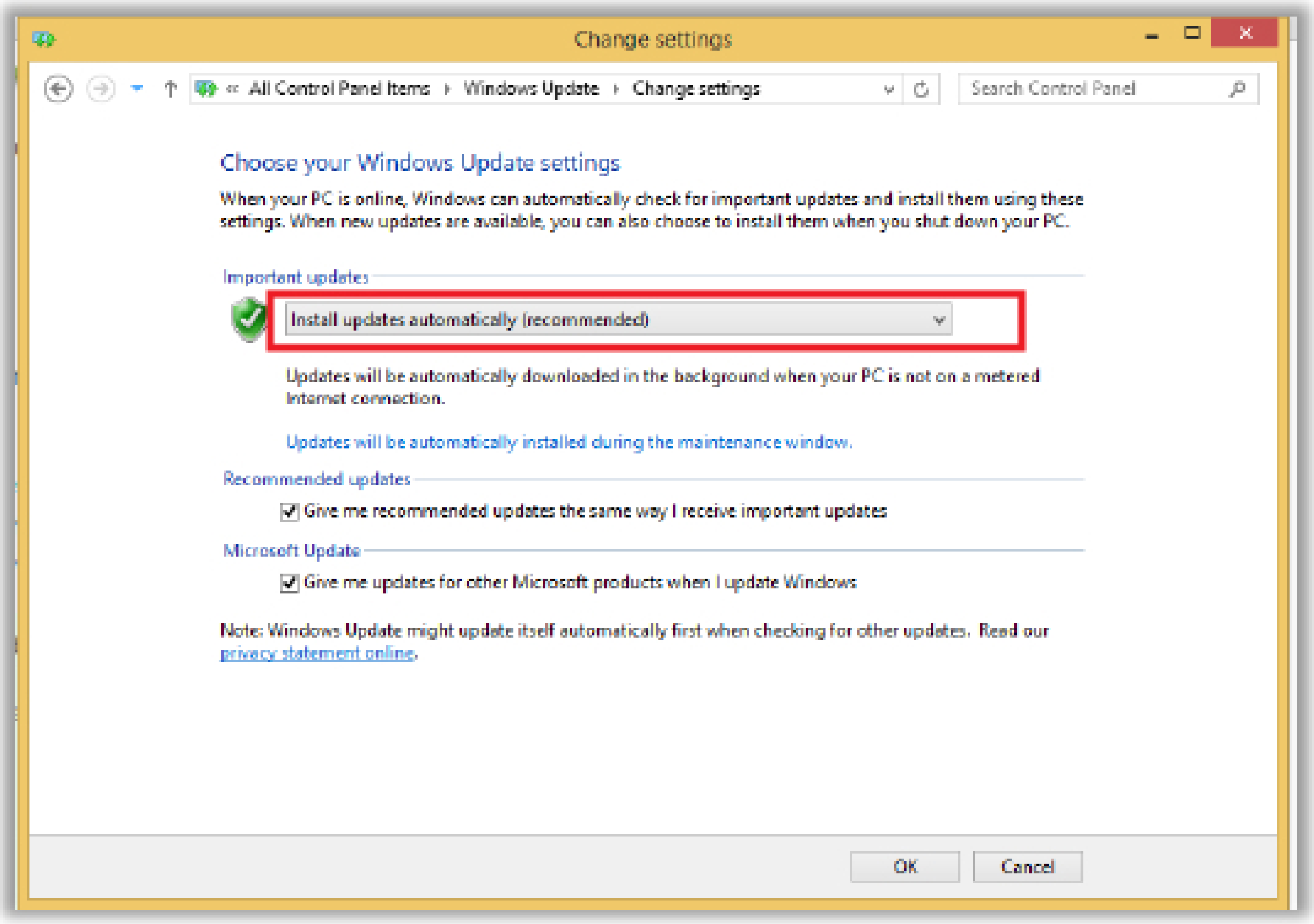
You're set to automatically install updates

12 optional updates are available

Most recent check for updates: Today at 9:01 AM
Updates were installed: Today at 9:02 AM.
You receive updates: For Windows and other products from Microsoft Update

FIGURE 6.12: Change settings option

- Select the default option to **Install updates automatically (recommended)**


Change settings
« All Control Panel Items › Windows Update › Change settings
Search Control Panel
OK
Cancel

Choose your Windows Update settings

When your PC is online, Windows can automatically check for important updates and install them using these settings. When new updates are available, you can also choose to install them when you shut down your PC.

Important updates

Install updates automatically (recommended)

Updates will be automatically downloaded in the background when your PC is not on a metered Internet connection.

Updates will be automatically installed during the maintenance window.

Recommended updates

☑ Give me recommended updates the same way I receive important updates

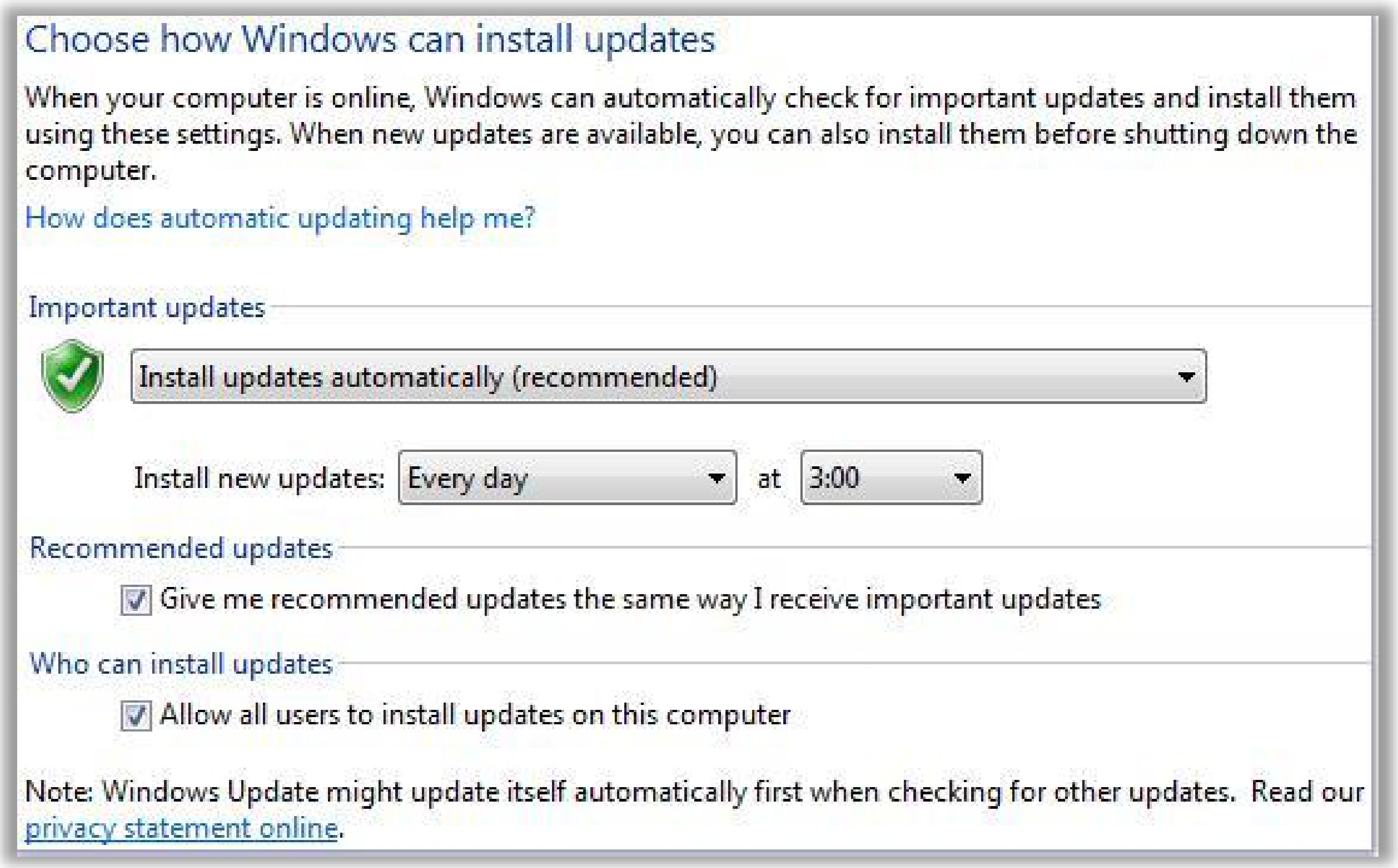
Microsoft Update

☑ Give me updates for other Microsoft products when I update Windows

Note: Windows Update might update itself automatically first when checking for other updates. Read our privacy statement online.

FIGURE 6.13: Install updates automatically (recommended)

- Make sure that the options: **Give me recommended updates the same way I receive important updates** and **Allow all users to install updates on this computer** are enabled
- In Windows 7, the user gets an option to **schedule the installation of new updates**



Choose how Windows can install updates

When your computer is online, Windows can automatically check for important updates and install them using these settings. When new updates are available, you can also install them before shutting down the computer.

How does automatic updating help me?

Important updates

Install updates automatically (recommended)

Install new updates: Every day at 3:00

Recommended updates

☑ Give me recommended updates the same way I receive important updates

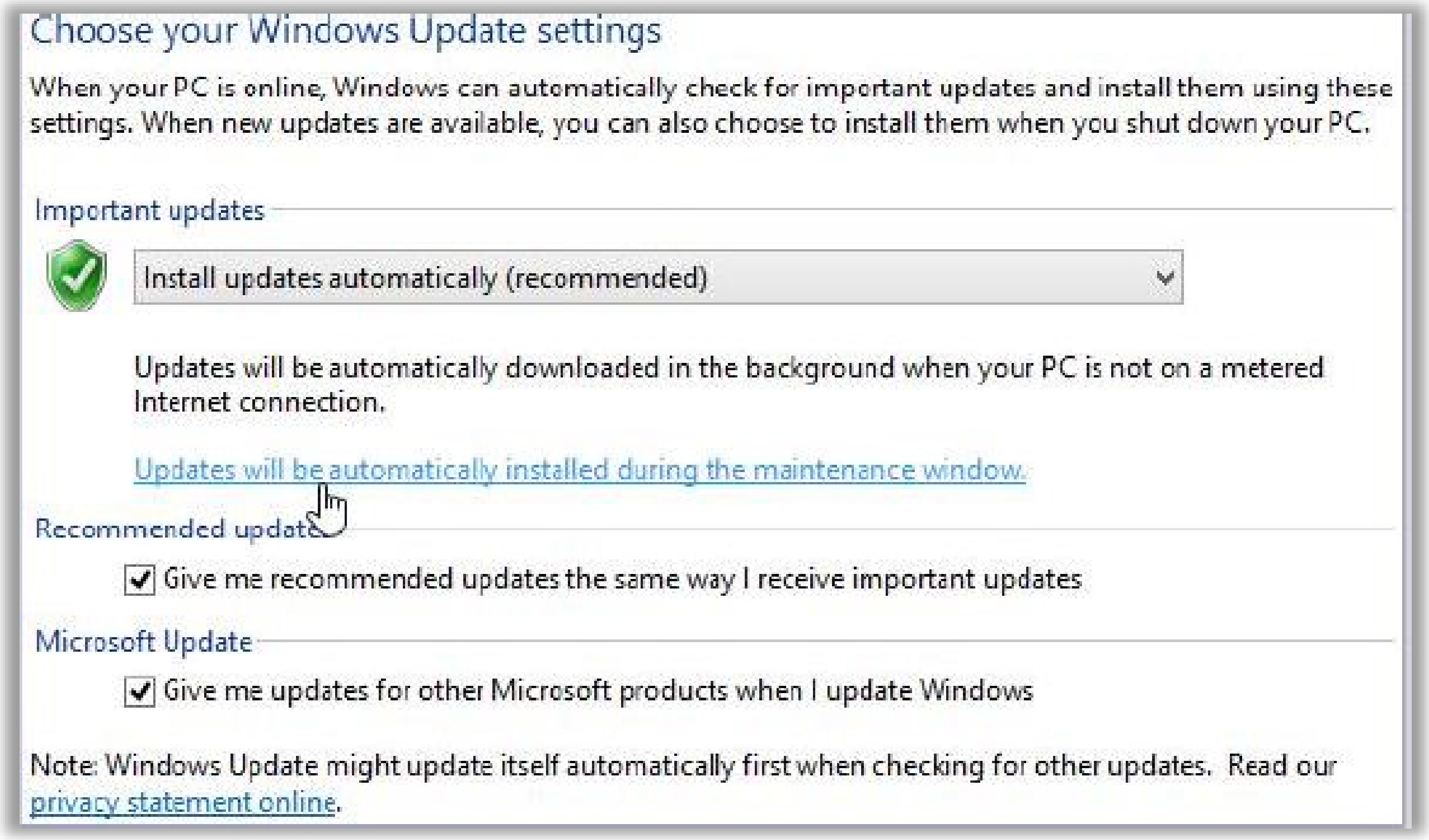
Who can install updates

☑ Allow all users to install updates on this computer

Note: Windows Update might update itself automatically first when checking for other updates. Read our privacy statement online.

FIGURE 6.14: Scheduling the installation for new updates in Windows 7

- In Windows 8 and 8.1, Click on the link: **Updates will be automatically installed during the maintenance window**



Choose your Windows Update settings

When your PC is online, Windows can automatically check for important updates and install them using these settings. When new updates are available, you can also choose to install them when you shut down your PC.

Important updates

Install updates automatically (recommended)

Updates will be automatically downloaded in the background when your PC is not on a metered Internet connection.

Updates will be automatically installed during the maintenance window.

Recommended updates

☑ Give me recommended updates the same way I receive important updates

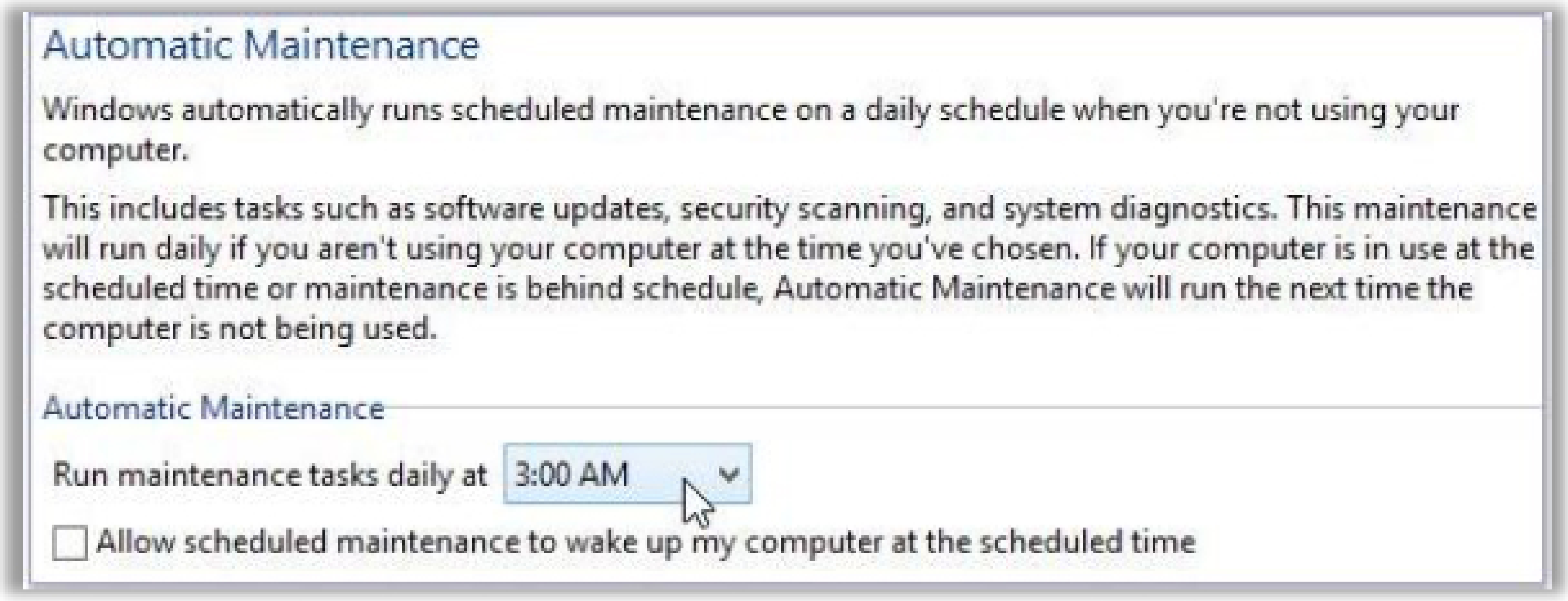
Microsoft Update

☑ Give me updates for other Microsoft products when I update Windows

Note: Windows Update might update itself automatically first when checking for other updates. Read our privacy statement online.

FIGURE 6.15: Automatic Update Installation for Windows 8 and 8.1

- The **Automatic Maintenance** window opens



Automatic Maintenance

Windows automatically runs scheduled maintenance on a daily schedule when you're not using your computer.

This includes tasks such as software updates, security scanning, and system diagnostics. This maintenance will run daily if you aren't using your computer at the time you've chosen. If your computer is in use at the scheduled time or maintenance is behind schedule, Automatic Maintenance will run the next time the computer is not being used.

Automatic Maintenance

Run maintenance tasks daily at 3:00 AM

☐ Allow scheduled maintenance to wake up my computer at the scheduled time

FIGURE 6.16: Scheduling the time in Automatic Maintenance for Windows 8 and 8.1

- The user can set the time for daily schedule

Administrators can also use various third party tools such as ManageEngine's Desktop Central to install or uninstall patches/service packs from a central location.

You can click on Install Patch and select the OS that you wanted to deploy patches/service packs to.

Steps to remotely install and uninstall patches for Windows using Desktop Central

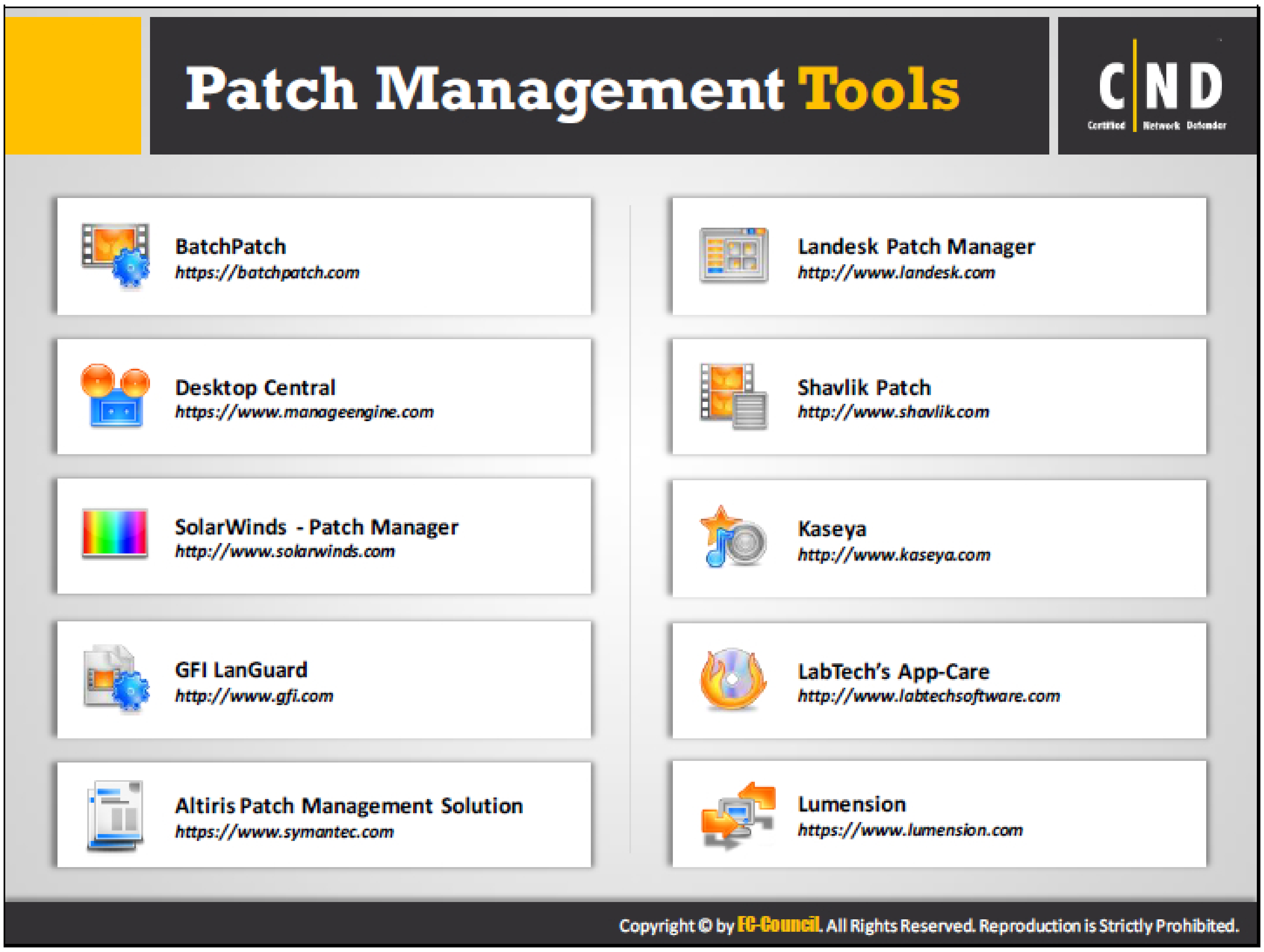
Source: *https://www.manageengine.com*

1. Click **Patch Management**
2. Under **Deployment** select Install/uninstall Patch
3. Choose the operating system as **Windows** and then create a configuration that needs to be deployed
4. Provide a **name** and a **description** for the Install/uninstall Patches Configuration
5. Define Configuration and Specify the Add the Patches, operation type, Scheduler Settings, Deployment Settings, etc. as **Install to install the patches/service packs**
6. Define **Target**

- You can deploy the configuration to any of the following:
  - **Site** - to deploy the configuration to all the users/computers of that site.
  - **Domain** - to deploy the configuration to all the users/computers of that domain.
  - **Organizational Unit** - to deploy the configuration to all the users/computers of that OU.
  - **Group** - to deploy the configuration to all the users/computers of that Group.
  - **User/Computer** - to deploy the configuration to the specified users/computers.

- **IP Addresses** - to deploy the configuration to the specified IP Addresses. You can also specify a range of IP Addresses to deploy a configuration by selecting the IP Range option and specifying the starting and ending IP. This option is available only for the computer configurations.
- **Custom Group** - to deploy the configuration to all the users/computers of the selected Custom Group.

7. Click the **Deploy** button to deploy the defined Install Patches Configuration in the defined targets



Patch Management Tools

BatchPatch
https://batchpatch.com

Desktop Central
https://www.manageengine.com

SolarWinds - Patch Manager
http://www.solarwinds.com

GFI LanGuard
http://www.gfi.com

Altiris Patch Management Solution
https://www.symantec.com

Landesk Patch Manager
http://www.landesk.com

Shavlik Patch
http://www.shavlik.com

Kaseya
http://www.kaseya.com

LabTech's App-Care
http://www.labtechsoftware.com

Lumension
https://www.lumension.com

BatchPatch

Source: *https://batchpatch.com*

BatchPatch is Windows Update & WSUS Patch Management Software used to remotely initiate Windows Update, WSUS, software deployments, and reboots on many computers.

Desktop Central

Source: *https://www.manageengine.com*

Desktop Central is patch management tool used to install/uninstall patches and service packs for Windows operating systems from a central location. It not only manages patch deployment, but also scans for network vulnerabilities, identifies missing security patches and hotfixes, applies them immediately and mitigates risk.

SolarWinds - Patch Manager

Source: *http://www.solarwinds.com*

SolarWinds Patch Manager makes it easy to perform third party patch management across tens of thousands of servers and workstations and enables you to leverage and extend the capabilities of Microsoft WSUS or SCCM to report, deploy, and manage third-party patches as well as Microsoft patches.

GFI LanGuard

Source: http://www.gfi.com

GFI LanGuard patches Microsoft, Mac OS X, Linux and more than 60 third-party applications, and deploys both security and non-security patches. GFI LanGuard scans your operating systems, virtual environments and installed applications through vulnerability check databases.

Altiris Patch Management Solution

Source: https://www.symantec.com

Altiris Patch Management Solution allows you to proactively manage patches and software updates by automating the collection, analysis, and delivery of patches across your enterprise.

Landesk Patch Manager

Source: http://www.landesk.com

LANDESK Patch Manager evaluates, tests, and applies patches across the enterprise easily and automatically to drastically simplify your efforts. It maintains patches for Microsoft Windows and other vital operating systems by downloading patches automatically and streamlining patch testing and deployment.

Shavlik Patch

Source: http://www.shavlik.com

With Shavlik Patch you leverage a single Configuration Manager workflow for publishing updates for both Microsoft and non-Microsoft products.

Kaseya

Source: http://www.kaseya.com

Kaseya provides the tools and infrastructure to enforce policies and to easily address the complexities of software and security patch deployment and simultaneously deploys all required patches across machines.

LabTech's App-Care

Source: http://www.labtechsoftware.com

The App-Care patch management solution extends LabTech's Microsoft update patching to third party applications with seamless integration to close security holes and guard against attacks. It automatically downloads third party patches from the manufacturer and pushes them to computers automatically to close security gaps in third party applications.

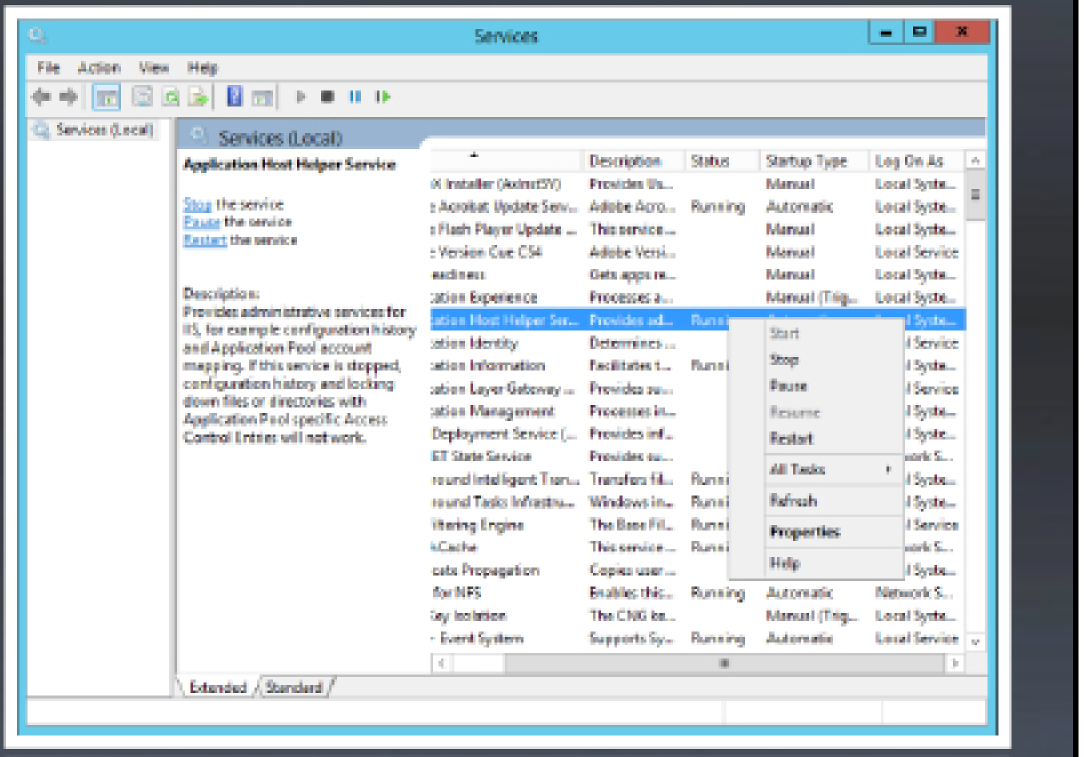
Lumension

Source: https://www.lumension.com

Lumension patch management software helps IT professionals uncover security vulnerabilities and deploy security patches across an entire network to eliminate them. This patch management software can be used on Windows, Mac OS X, UNIX and Linux platforms as well as third-party applications and infrastructure devices.

Disabling Unused System Services

- Go to Control Panel → Administrative Tools → Services
- Disable the following service on any machine other than a server
  - IIS
  - FTP
  - SQL Server
  - Proxy services
  - Telnet
  - Universal Plug And Play on any machine



Application Host Helper Service

Stop the service
Pause the service
Restart the service

Description:
Provides administrative services for IIS, for example configuration history and Application Pool account mapping. If this service is stopped, configuration history and locking down files or directories with Application Pool specific Access Control Entries will not work.

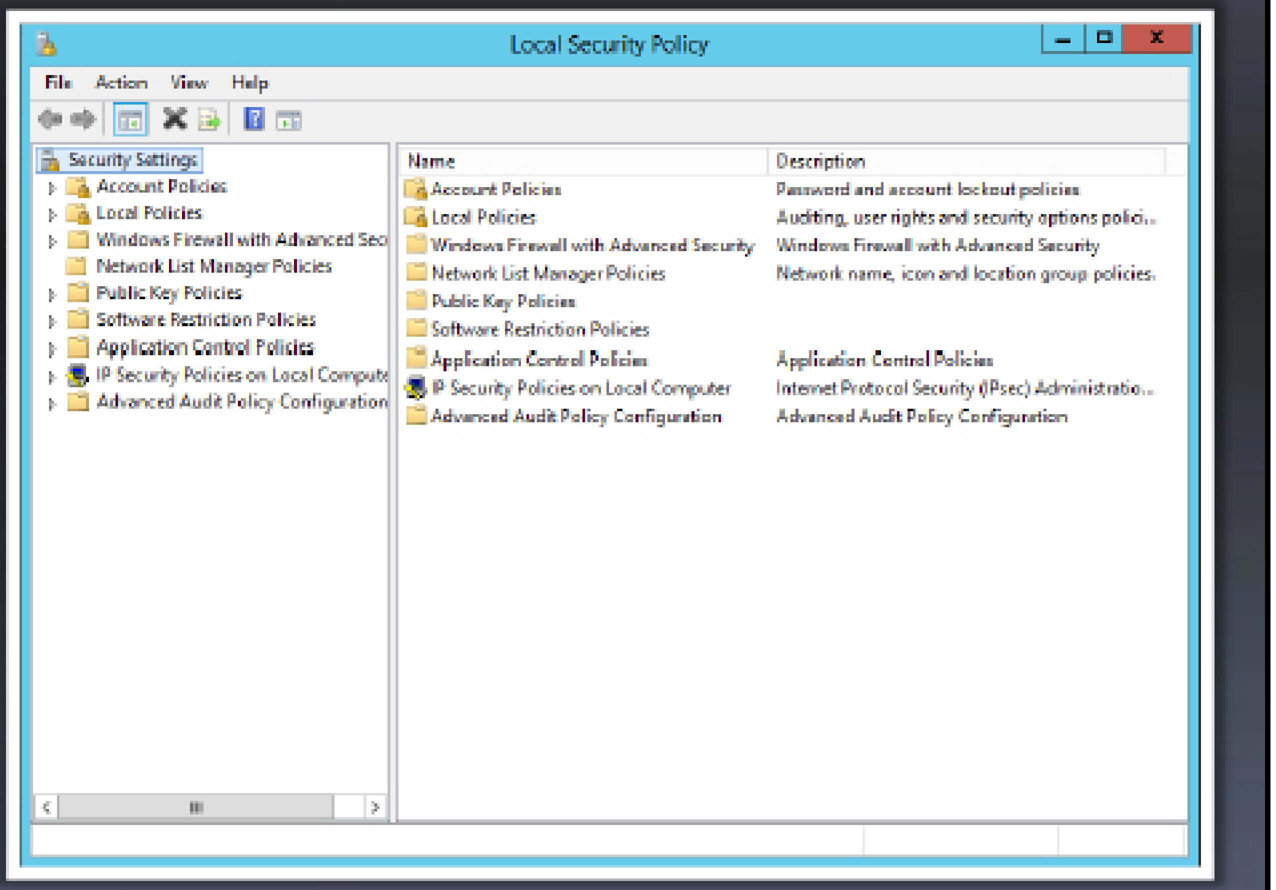
	Description	Status	Startup Type	Log On As
X Installer (AxInstSV)	Provides Us...		Manual	Local Syste...
Acrobat Update Serv...	Adobe Acro...	Running	Automatic	Local Syste...
Flash Player Update ...	This service ...		Manual	Local Syste...
Version Cue CS4	Adobe Versi...		Manual	Local Service
eadiness	Gets apps re...		Manual	Local Syste...
ation Experience	Processes a...		Manual (Trig...	Local Syste...
ation Host Helper Ser...	Provides ad...	Runni		l Syste...
ation Identity	Determines ...			l Service
ation Information	Facilitates t...	Runni		l Syste...
ation Layer Gateway ...	Provides su...			l Service
ation Management	Processes in...			l Syste...
Deployment Service (...	Provides inf...			l Syste...
ET State Service	Provides su...			ork S...
round Intelligent Tran...	Transfers fil...	Runni		l Syste...
round Tasks Infrastru...	Windows in...	Runni		l Syste...
ltering Engine	The Base Fil...	Runni		l Service
Cache	This service ...	Runni		ork S...
cate Propagation	Copies user ...			l Syste...
for NFS	Enables thi...	Running	Automatic	Network S...
ey Isolation	The CNG ke...		Manual (Trig...	Local Syste...
Event System	Supports Sy...	Running	Automatic	Local Service

Unnecessary services run in the background on the systems the user is not aware of. Leaving these services enabled can give a path to the attacker to compromise the system as some of them can be vulnerable to different types of attacks. Administrators can find unnecessary services running on the system based on an organization policy. The policy statement may include lists of necessary services that should be allowed to run on the system and unnecessary services that should be not allowed to run. An administrator can create, pause, stop and restart a service as per the system and user requirement. On the user machine, administrators can disable a service which is not required. Disabling unnecessary services is important as it reduces the chances of system exploitation. Services like IIS, FTP, SQL Server, Proxy services and Telnet are usually not required by the users. Administrator privileges are required to enable and disable services on a particular host.

Set Appropriate Local Security Policy Settings

Check if security policies are set based on the policies designed for your local network

Go to **Control Panel** → **Administrative Tools** → **Local Security Policy**


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Windows Firewall with Advanced Sec
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options polici...
Windows Firewall with Advanced Security	Windows Firewall with Advanced Security
Network List Manager Policies	Network name, icon and location group policies.
Public Key Policies	
Software Restriction Policies	
Application Control Policies	Application Control Policies
IP Security Policies on Local Computer	Internet Protocol Security (IPsec) Administratio...
Advanced Audit Policy Configuration	Advanced Audit Policy Configuration

Local policy settings allow enforcing many systems, users, and security related settings in Microsoft Windows. These policy settings include Password Policy, Audit Policy, and User Permissions. There are default policy settings available; however, the administrator needs to configure more policies in order to confirm security. An administrator should define and set the policies as per organization's security policies.

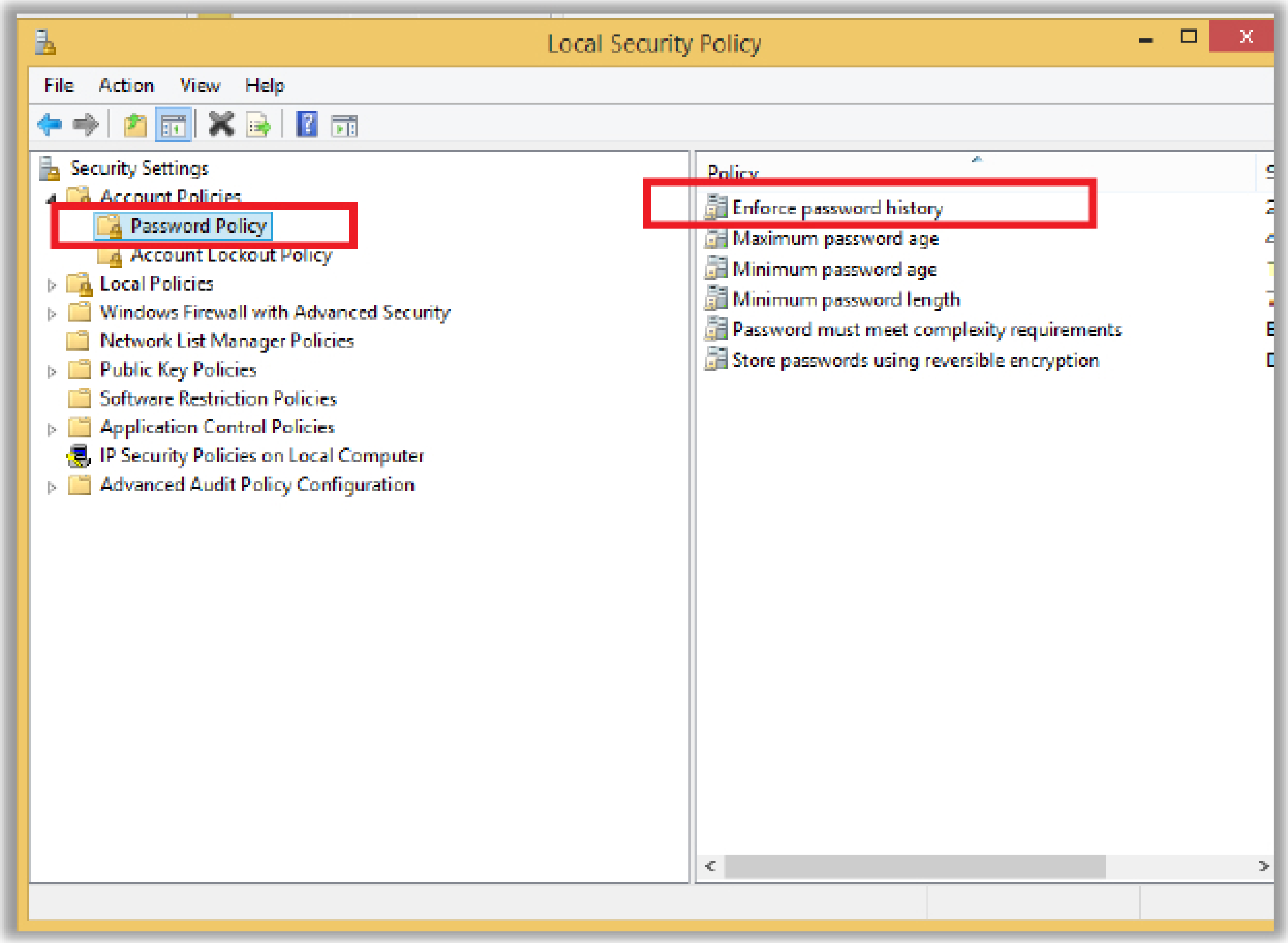
Steps for configuring the Local Policy Settings for the computer:

1. Go to **Control Panel**
2. Click **Administrative Tools** -> Local Security Policy
3. In the security settings, perform one of the following actions:
   a. Click **Account Policies** in order to edit password policy and Account lockout policy
   b. Click **Local Policies** in order to edit Audit policy, User rights assignment and security options
4. Double – click on the **policies** in order to modify or edit the policies
5. Click **OK** after performing the desired action

Every organization should enforce their employees to change the password after a specified time of interval. This urges the need for employing certain policies that outline the requirements for setting a password. The changes in password policy affect only the local computer. However, the configuration of the policies depends on the policies for each organization.

For instance, an organization can edit or configure the local password policies as follows:

- Click on **Account Policies → Password Policy** in the left pane
- Double click on **Enforce password history** in the right pane



- Security Settings
  - Account Policies
    - Password Policy
    - Account Lockout Policy
  - Local Policies
  - Windows Firewall with Advanced Security
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
  - IP Security Policies on Local Computer
  - Advanced Audit Policy Configuration

Enforce password history
Maximum password age
Minimum password age
Minimum password length
Password must meet complexity requirements
Store passwords using reversible encryption

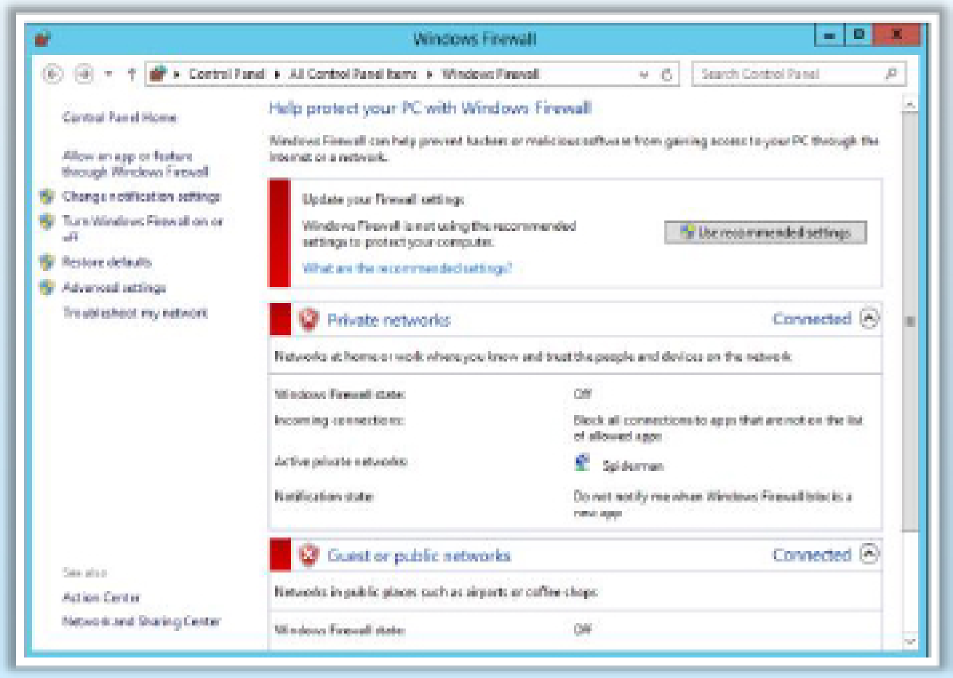
FIGURE 6.17: Enforcing Password Policy

- **Maximum password age:** Determines the time period for using a password. Default value is 42.
- **Minimum password age:** Determines the minimum number of days the user needs to use the password.
- **Minimum password length:** Determines the length of the passwords. Usually the minimum value is '8'.
- **Password must meet complexity requirements:** Determines the criteria for creating a password. This option is enabled and includes upper and lower case letters, numbers and special characters.
- **Store passwords using reversible encryption:** Always "Disabled", as it allows the attacker to crack the password easily.

Configuring Windows Firewall

C|ND Certified Network Defender

Go to Control Panel → Windows Firewall and click Turn Windows Firewall on or off



Windows Firewall

Control Panel ▸ All Control Panel Items ▸ Windows Firewall

Search Control Panel

Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

See also
Action Center
Network and Sharing Center

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Update your Firewall settings

Windows Firewall is not using the recommended settings to protect your computer.

Use recommended settings

What are the recommended settings?

Private networks — Connected

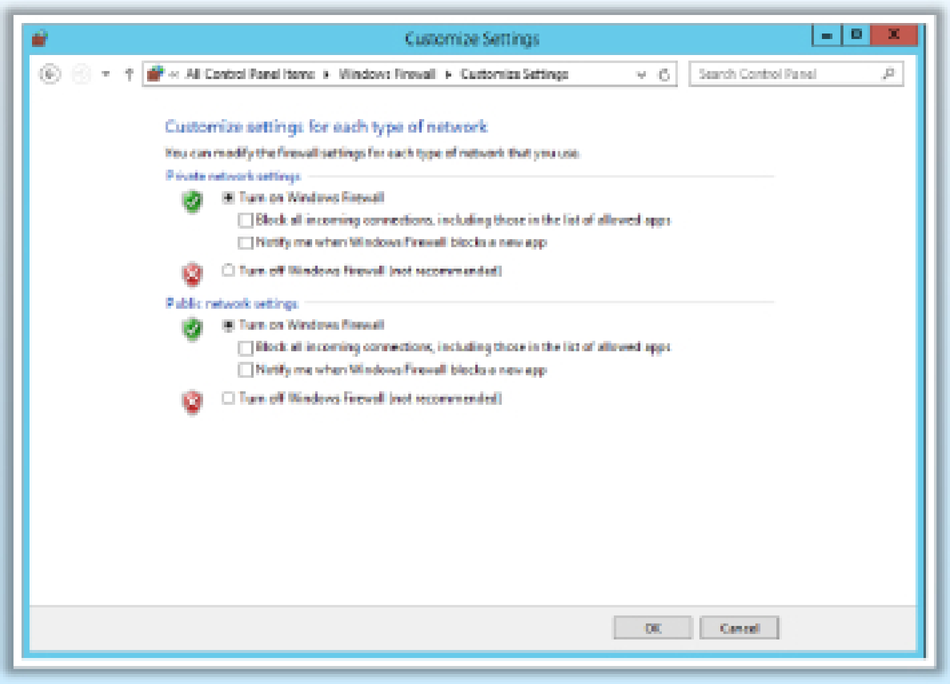
Networks at home or work where you know and trust the people and devices on the network

Windows Firewall state:	Off
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active private networks:	Spiderman
Notification state:	Do not notify me when Windows Firewall blocks a new app

Guest or public networks — Connected

Networks in public places such as airports or coffee shops

Windows Firewall state:	Off



Customize Settings

All Control Panel Items ▸ Windows Firewall ▸ Customize Settings

Search Control Panel

Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

● Turn on Windows Firewall
□ Block all incoming connections, including those in the list of allowed apps
□ Notify me when Windows Firewall blocks a new app
○ Turn off Windows Firewall (not recommended)

Public network settings

● Turn on Windows Firewall
□ Block all incoming connections, including those in the list of allowed apps
□ Notify me when Windows Firewall blocks a new app
○ Turn off Windows Firewall (not recommended)

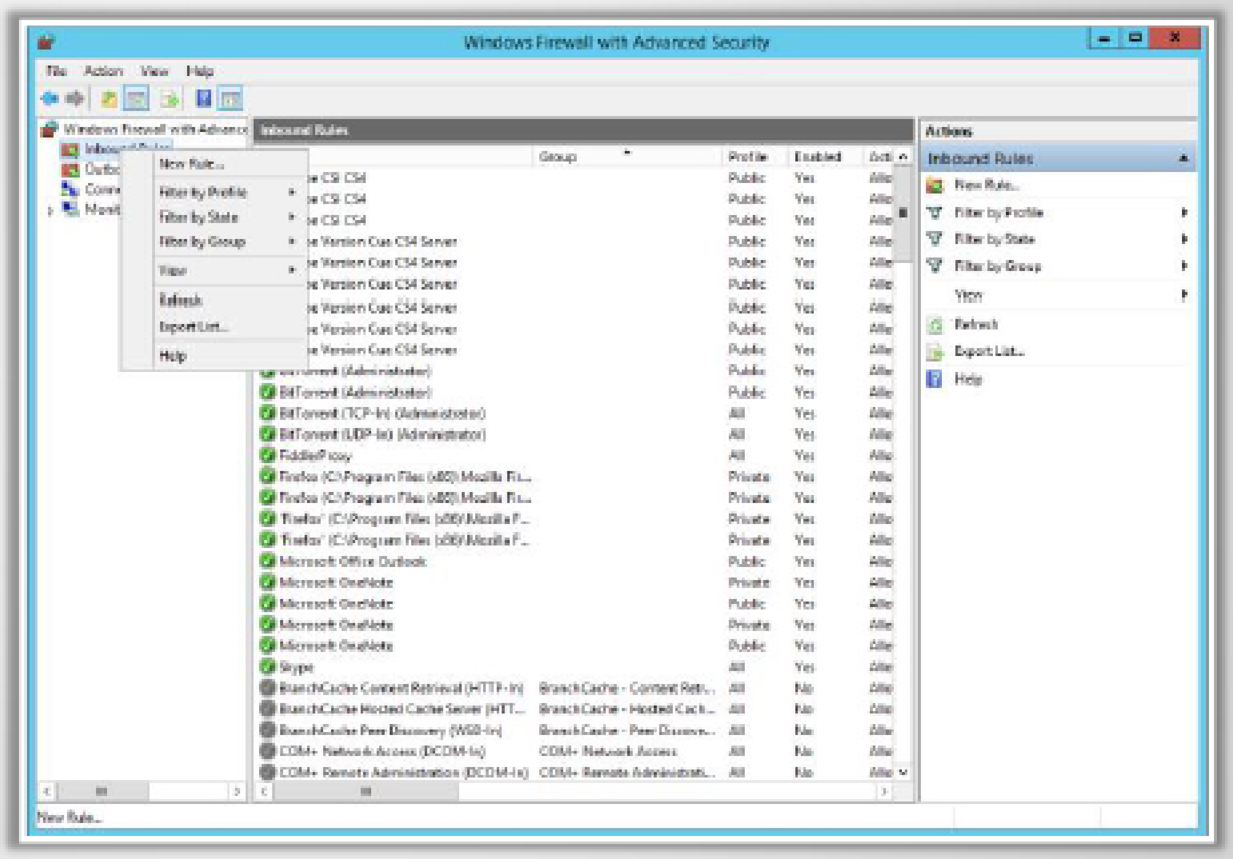
OK Cancel

Configuring Windows Firewall (Cont'd)

C|ND Certified Network Defender

Configuring Inbound and Outbound rules

- Click Advanced Settings and configure inbound/outbound rule for your firewall restrictions
- Click Monitoring to active firewall rules, active Connection security rules, Security Associations, etc.



Windows Firewall with Advanced Security

Inbound Rules

	Group	Profile	Enabled	Acti
...e CS3 CS4		Public	Yes	Allo
...e CS3 CS4		Public	Yes	Allo
...e CS3 CS4		Public	Yes	Allo
...e Version Cue CS4 Server		Public	Yes	Allo
...e Version Cue CS4 Server		Public	Yes	Allo
...e Version Cue CS4 Server		Public	Yes	Allo
...e Version Cue CS4 Server		Public	Yes	Allo
...e Version Cue CS4 Server		Public	Yes	Allo
...e Version Cue CS4 Server		Public	Yes	Allo
...Torrent (Administrator)		Public	Yes	Allo
BitTorrent (Administrator)		Public	Yes	Allo
BitTorrent (TCP-In) (Administrator)		All	Yes	Allo
BitTorrent (UDP-In) (Administrator)		All	Yes	Allo
FiddlerProxy		All	Yes	Allo
Firefox (C:\Program Files (x86)\Mozilla Fi...		Private	Yes	Allo
Firefox (C:\Program Files (x86)\Mozilla Fi...		Private	Yes	Allo
'Firefox' (C:\Program Files (x86)\Mozilla F...		Private	Yes	Allo
'Firefox' (C:\Program Files (x86)\Mozilla F...		Private	Yes	Allo
Microsoft Office Outlook		Public	Yes	Allo
Microsoft OneNote		Private	Yes	Allo
Microsoft OneNote		Public	Yes	Allo
Microsoft OneNote		Private	Yes	Allo
Microsoft OneNote		Public	Yes	Allo
Skype		All	Yes	Allo
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allo
BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...	All	No	Allo
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	Allo
COM+ Network Access (DCOM-In)	COM+ Network Access	All	No	Allo
COM+ Remote Administration (DCOM-In)	COM+ Remote Administrati...	All	No	Allo

Windows Firewall is a built-in feature that governs the security of Windows. It helps in preventing intrusions internally or externally. Windows Firewall has the ability to monitor the incoming and outgoing traffic. Rules and exceptions in the Windows firewall maintain the logs of the traffic. Administrators can apply rules and exceptions based on the type of the network and location of the machine.

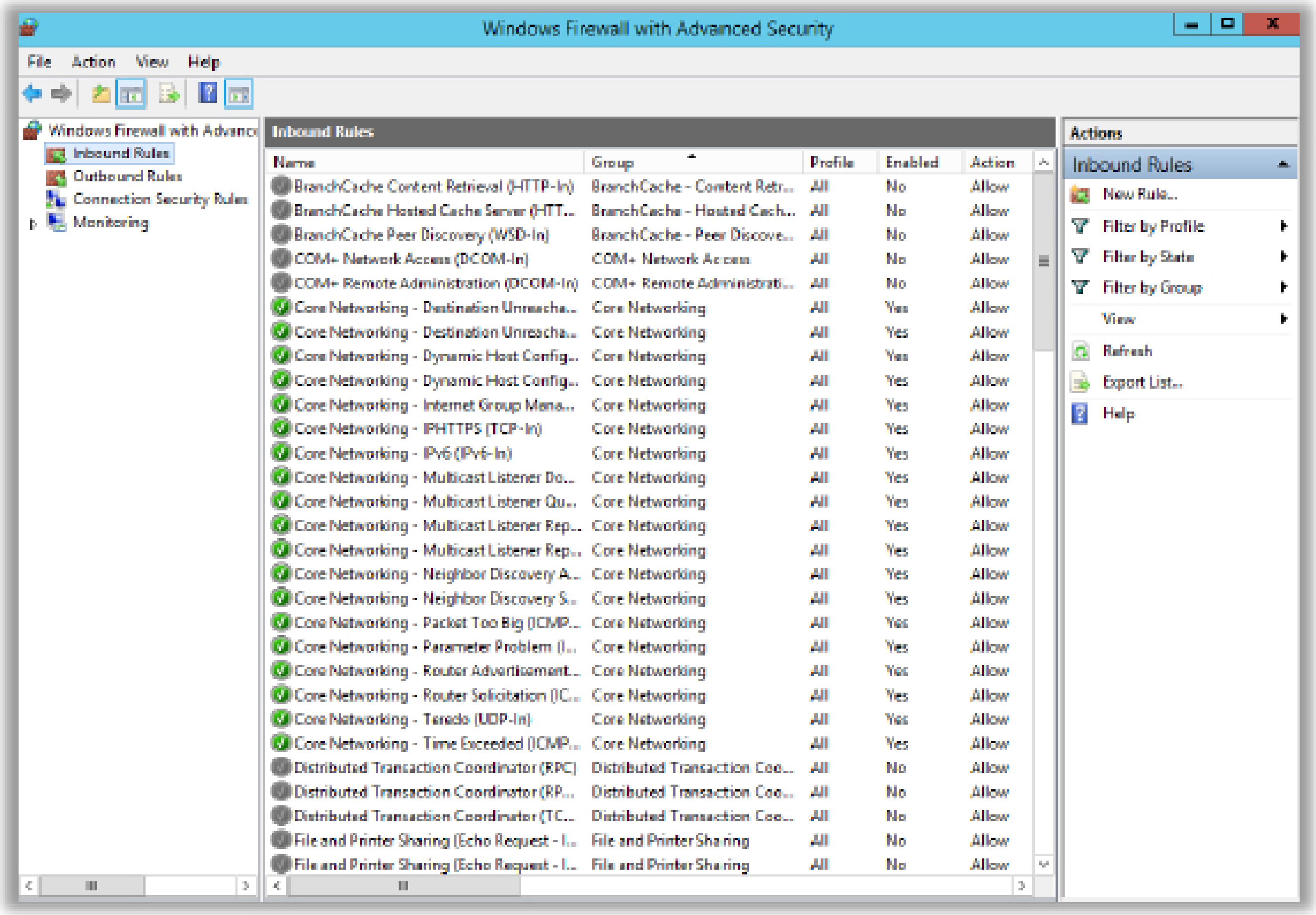
Turning the Firewall ON can stop filter communication passing through it. Administrator privileges are required to turn ON the Windows firewall feature.

- The following steps define how to turn ON the Firewall:
  1. **Start → Control Panel → Windows Firewall**
  2. Click Turn Windows Firewall **ON** or **OFF**

Beside traffic filtering and blocking, The Windows firewall also maintains additional information such as:

1. **Windows Firewall state:** Informs if the firewall is ON or OFF.
2. **Incoming connections:** Notifies, the action the firewall will take for incoming connections.
3. **Active private network:** Displays the name of the active private network.
4. **Notification state:** Notifies the action taken by the firewall for applications.

Configuration of Windows Firewall is done through the option Advanced Security. Windows Firewall with Advanced Security displays the detail functioning of the firewall. It helps in the implementation of rules and exceptions for the firewall. The snap-in displays the rules and exceptions for inbound and outbound traffic.



Inbound Rules

Name	Group	Profile	Enabled	Action
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow
BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...	All	No	Allow
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	Allow
COM+ Network Access (DCOM-In)	COM+ Network Access	All	No	Allow
COM+ Remote Administration (DCOM-In)	COM+ Remote Administrati...	All	No	Allow
Core Networking - Destination Unreacha...	Core Networking	All	Yes	Allow
Core Networking - Destination Unreacha...	Core Networking	All	Yes	Allow
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow
Core Networking - Internet Group Mana...	Core Networking	All	Yes	Allow
Core Networking - IPHTTPS (TCP-In)	Core Networking	All	Yes	Allow
Core Networking - IPv6 (IPv6-In)	Core Networking	All	Yes	Allow
Core Networking - Multicast Listener Do...	Core Networking	All	Yes	Allow
Core Networking - Multicast Listener Qu...	Core Networking	All	Yes	Allow
Core Networking - Multicast Listener Rep...	Core Networking	All	Yes	Allow
Core Networking - Multicast Listener Rep...	Core Networking	All	Yes	Allow
Core Networking - Neighbor Discovery A...	Core Networking	All	Yes	Allow
Core Networking - Neighbor Discovery S...	Core Networking	All	Yes	Allow
Core Networking - Packet Too Big (ICMP...	Core Networking	All	Yes	Allow
Core Networking - Parameter Problem (I...	Core Networking	All	Yes	Allow
Core Networking - Router Advertisement...	Core Networking	All	Yes	Allow
Core Networking - Router Solicitation (IC...	Core Networking	All	Yes	Allow
Core Networking - Teredo (UDP-In)	Core Networking	All	Yes	Allow
Core Networking - Time Exceeded (ICMP...	Core Networking	All	Yes	Allow
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo...	All	No	Allow
Distributed Transaction Coordinator (RP...	Distributed Transaction Coo...	All	No	Allow
Distributed Transaction Coordinator (TC...	Distributed Transaction Coo...	All	No	Allow
File and Printer Sharing (Echo Request - I...	File and Printer Sharing	All	No	Allow
File and Printer Sharing (Echo Request - I...	File and Printer Sharing	All	No	Allow

FIGURE 6.18: Setting Inbound and Outbound Rules in Windows Firewall

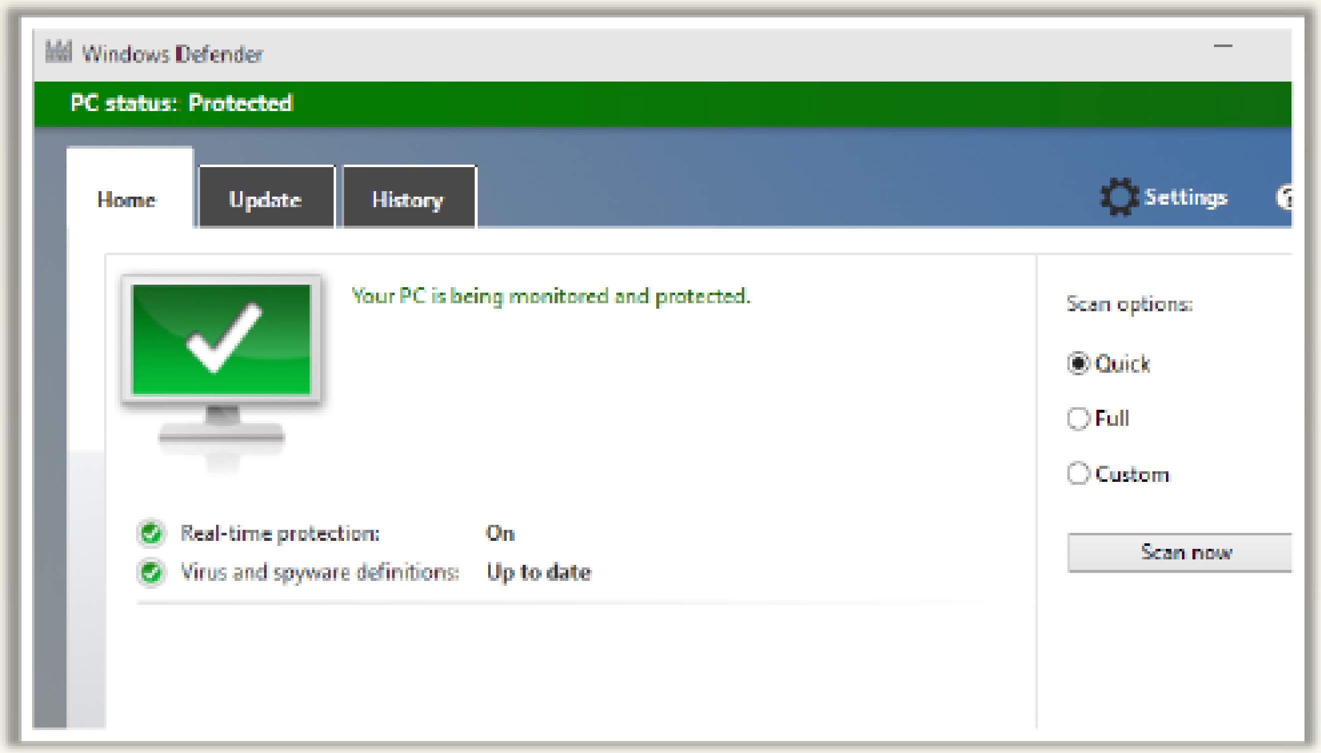
- **Inbound Rules:** They apply to traffic that is coming from the network or the Internet to your Windows computer or device. For example, if you are downloading a file through BitTorrent, the download of that file is filtered through an inbound rule.
- **Outbound Rules:** These rules apply to traffic that is originating from your computer and going to the network and the Internet. For example, your request to load a website in your web browser, that is outbound traffic and is filtered through an outbound rule.
- **Connection security rules**: Less common rules that are used to secure the traffic between two specific computers while it crosses the network. This type of rule is used in very controlled environments with special security requirements. Unlike inbound and outbound rules which are applied only to your computer or device, connection security rules require both computers involved in the communication to have the same rules applied.

All the rules can be configured so that they are specific to certain computers, user accounts, programs, apps, services, ports, protocols, or network adapters. You can display the rules of a certain type by selecting the appropriate category in the column on the left.

- **Creating an Inbound/Outbound Rule:**
  1. Go to **Outbound Rule** → In the Actions pane, click **New Rule**
  2. Select the **Type of Rule** you want to create → **Next**
  3. Type the **pathname** of the program → **Next**
  4. Select the **Action** you want to take → **Next**
  5. Select the **Network Location** for implementing the rule → **Next**
  6. Enter the **Name** of the rule and **Description** if necessary → **Finish**
  7. The new rule created, will appear in the Actions pane

Install Antivirus Software

- Install **up-to-date antivirus** software to protect your system from virus infections
- You can either use **built-in antivirus** or **third-party antivirus** software
- Built-in Antivirus for Windows 10 /Windows 8 - **Windows Defender**



PC status: Protected

Your PC is being monitored and protected.

Real-time protection: On
Virus and spyware definitions: Up to date

Scan options:
● Quick
○ Full
○ Custom

Keeping the system away from virus infections is an important task for host security. Securing the system from viruses is the utmost need of the administrators and the users working on the system. By installing updated antivirus software, you can keep your system from virus infected files, system crash, unwanted pop-ups and damage to the operating system caused by a malware infection. Administrators can also use various third party antivirus solutions for better protection.

Windows has a built-in antivirus solution called Windows Defender to protect the system from virus infection. Windows Defender runs in the background and notifies you when you need to take specific action. However, you can use it anytime to scan for malware if your computer isn't working properly or if you clicked a suspicious link online or in an email message.

Windows Defender is malware protection software used in order to detect and mitigate viruses and other malicious programs.

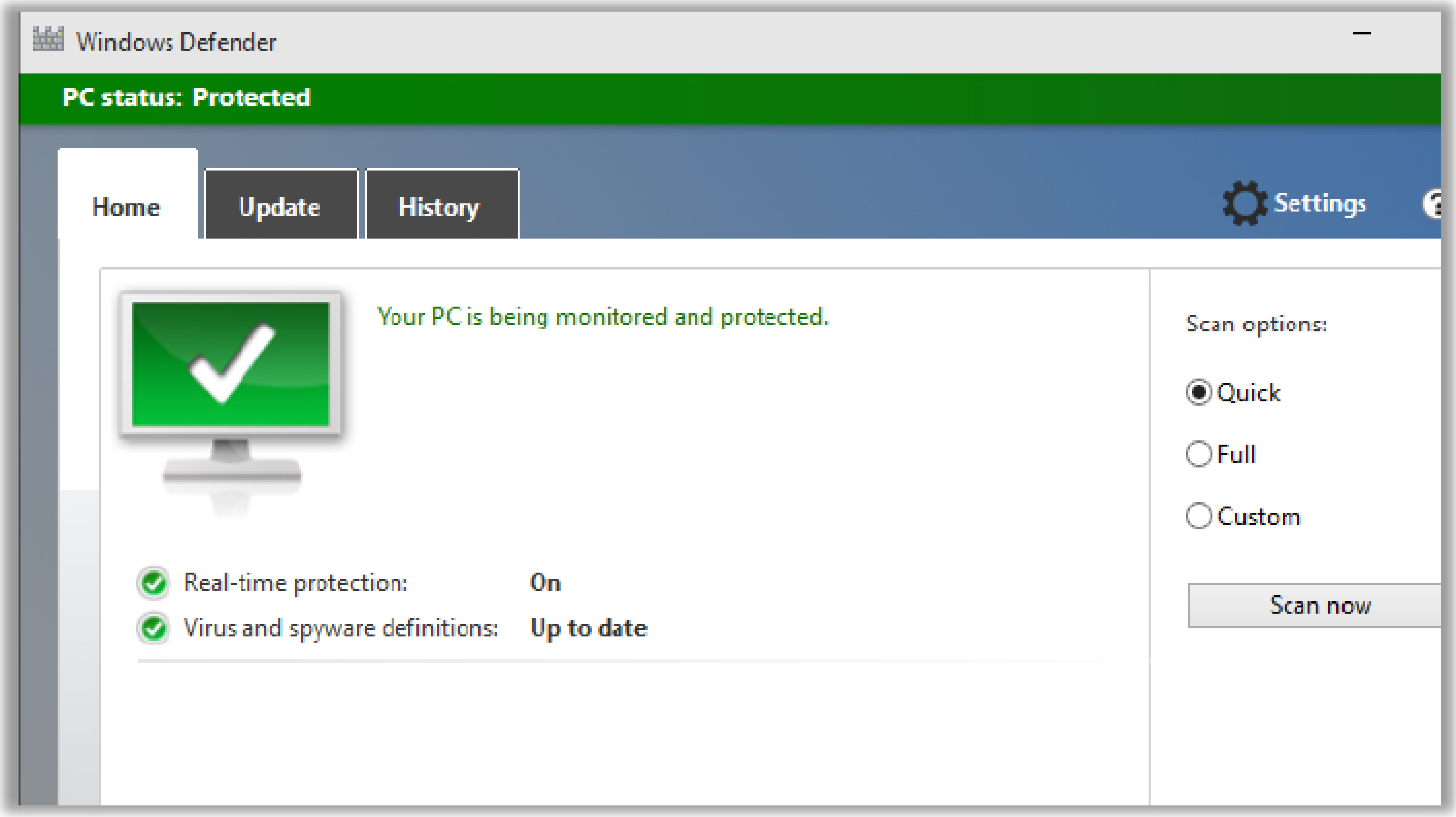
Windows defender scans process:

1. Search for **Windows Defender** in the search bar
2. Open windows defender
3. Select the **Type of Scan** of choice:
   I. Quick scan: Scans only those areas of the computer, wherein those areas are more prone to virus attacks.

II. Full Scan: Scans all files and folders present in the system. This process may be a time consuming process.

III. Custom Scan: Scans only those files or folders as provided by the user.

4. Click **Scan Now**



PC status: Protected

Your PC is being monitored and protected.

Real-time protection: On

Virus and spyware definitions: Up to date

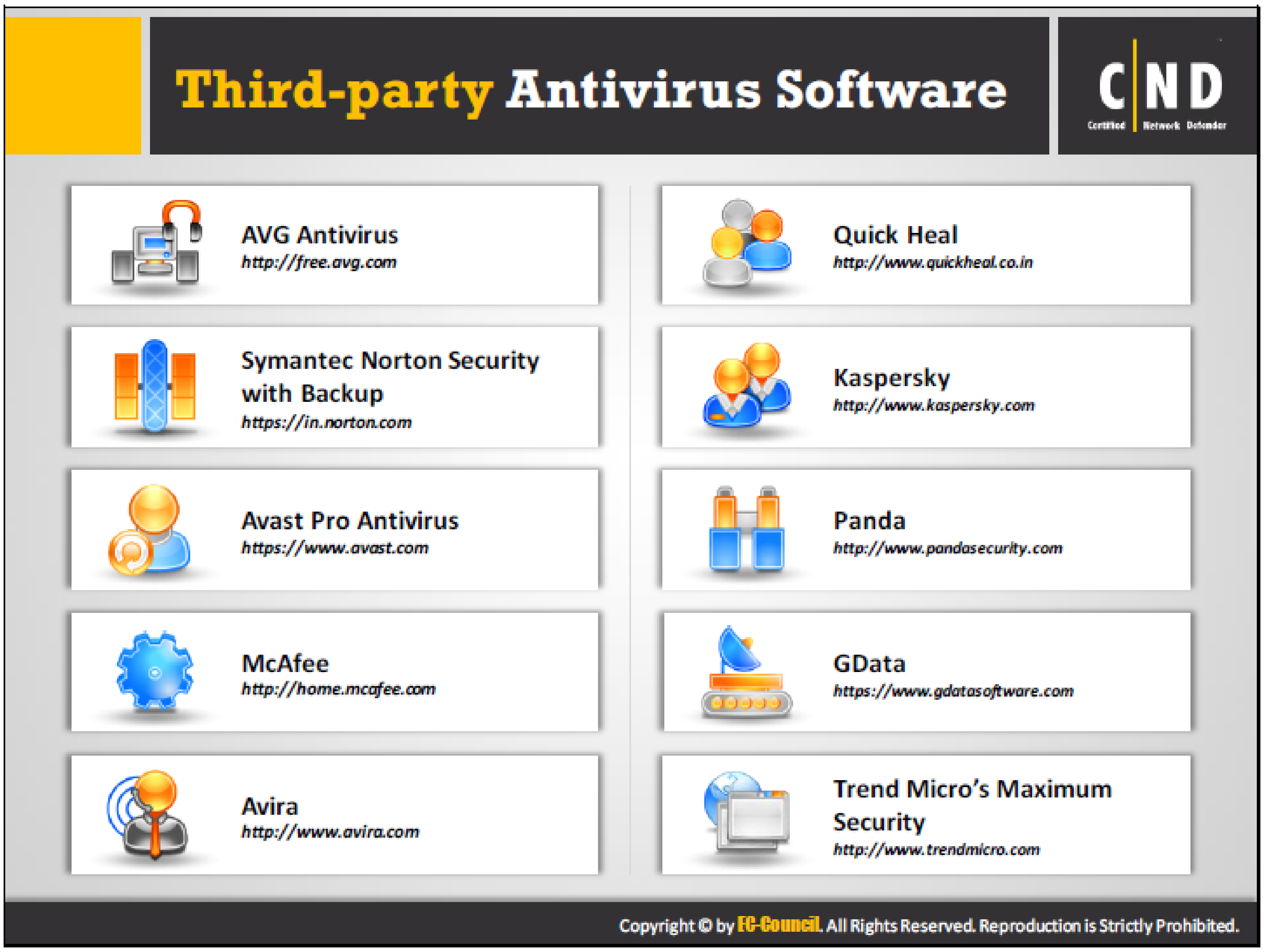
Scan options:

● Quick

○ Full

○ Custom

FIGURE 6.19: Windows Defender



Third-party Antivirus Software

AVG Antivirus
http://free.avg.com

Symantec Norton Security with Backup
https://in.norton.com

Avast Pro Antivirus
https://www.avast.com

McAfee
http://home.mcafee.com

Avira
http://www.avira.com

Quick Heal
http://www.quickheal.co.in

Kaspersky
http://www.kaspersky.com

Panda
http://www.pandasecurity.com

GData
https://www.gdatasoftware.com

Trend Micro's Maximum Security
http://www.trendmicro.com

Below is the list of some third-party antivirus software which can be used to protect you host from malware infections.

AVG Antivirus

Source: http://free.avg.com

AVG Antivirus helps stop, remove and prevent the spreading of viruses, worms, and Trojans. It protects you from malware on your PC and helps stop anything that's infected.

Symantec Norton Security with Backup

Source: https://in.norton.com

Norton Security Scan to determine if your system has been infected with viruses, malware, spyware, or other threats. It checks for suspicious or dangerous cookies and remove those that raise a concern.

Avast Pro Antivirus

Source: https://www.avast.com

Avast Pro Antivirus scans for all the files being downloaded through torrents, servers or flash drive. The files are first tested before being saved in the system. The software has the feature of securing the DNS settings, preventing from hijacking of DNS, fake-password attacks etc. The anti-virus pre-determines the malicious packet/data travelling towards the user's router device or network and dumps it, before exploitation.

McAfee

Source: *http://home.mcafee.com*

McAfee antivirus software tool scans the core components of the system and maintains it up-to-date. The software timely installs the updates in the background without affecting the productivity of the system. The tool has the feature to diagnose malware, worms or Trojans hiding in the backend of the processes and modules. McAfee has the feature to maintain schedule scans on the host machine.

Avira

Source: *http://www.avira.com*

Avira antivirus tool protects the system from viruses, worms and Trojans. It scans unknown files in real time for malware and exploits, blocks harmful websites before they load and identifies potentially unwanted applications hidden within legitimate software.

Quick Heal

Source: *http://www.quickheal.co.in*

Quick Heal is antivirus software used to protect your system from viruses, worms, Trojans, spyware and other such threats.

Kaspersky

Source: *http://www.kaspersky.com*

Kaspersky antivirus delivers essential protection against all types of malware. It safeguards you from the latest viruses, spyware, worms and more.

Panda

Source: *http://www.pandasecurity.com*

Panda provides real-time protection against the latest release malware. It protects PC, Mac or Android device against all types of threats.

GData

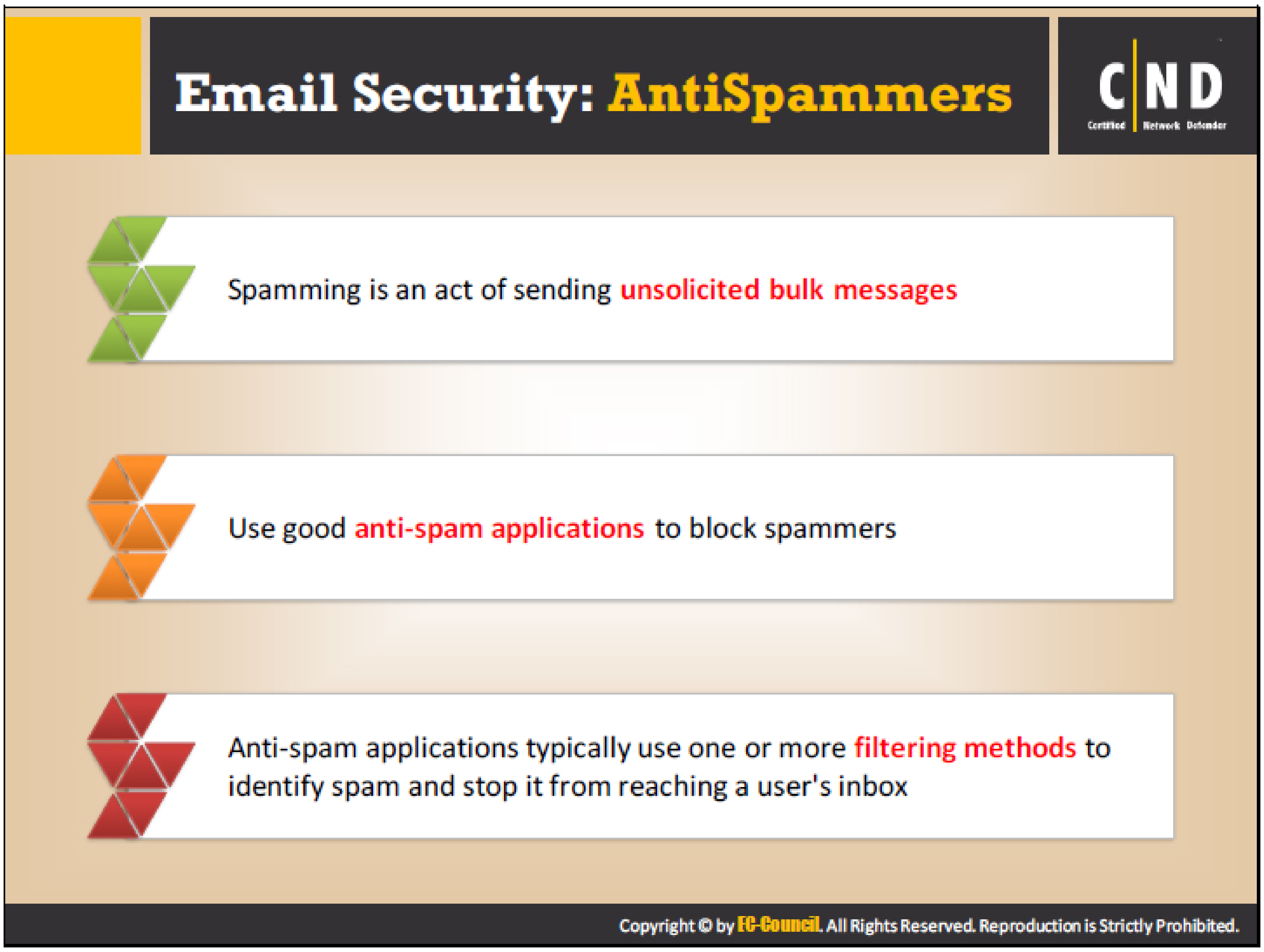
Source: *https://www.gdatasoftware.com*

GData has the feature of proactively detecting the malware from the system. It scans SSL encrypted emails for malicious attachments and suspicious content.

Trend Micro's Maximum Security

Source: *http://www.trendmicro.com*

Trend Micro's Maximum Security helps you to prevent identity theft by blocking phishing emails. It scans privacy settings on social media accounts and provides a secure browser for safe online banking.



Email Security: AntiSpammers

CND
Certified Network Defender

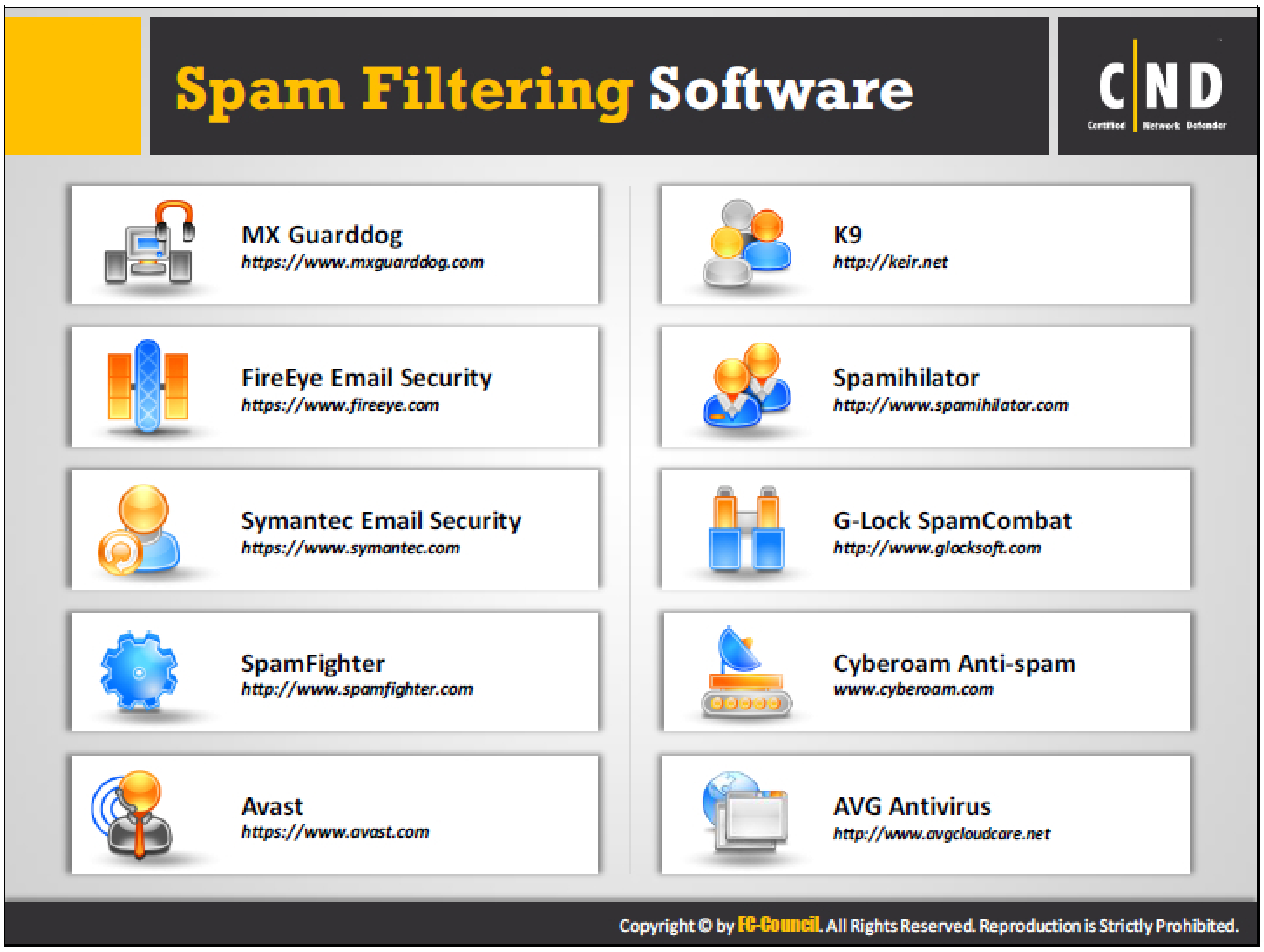
- Spamming is an act of sending unsolicited bulk messages
- Use good anti-spam applications to block spammers
- Anti-spam applications typically use one or more filtering methods to identify spam and stop it from reaching a user's inbox

Email threats have rapidly evolved as one of the major concerns for cyber users. Spamming is one such threat to email security. Spamming involves sending unsolicited bulk email (UBE), junk mail, or unsolicited commercial email (UCE) frequently to individual users or group of users. These email spams typically cost users money out-of-pocket to receive. Spam mail sent via virus infected networks can install a backdoor that allows the spammer to access the computer and use it for malicious purposes.

Anti-spam is a method of denying spam e-mails in the user's e-mail. Generally, antispam methods scan the computers IP address, e-mail signatures and data. This can minimize users from receiving spam emails. There are many types of anti-spam systems used together with many e-mail systems and internet service providers (ISP).

There are various **benefits** for using e-mail security:

- Provides complete security from any kind of cyber-attacks through e-mail by preventing unwanted bulk e-mails and viruses.
- Identify unknown malware and other malicious links in the e-mails.
- Helps in reacting to the detected spam e-mails.



Spam Filtering Software

CND Certified Network Defender

- MX Guarddog https://www.mxguarddog.com
- FireEye Email Security https://www.fireeye.com
- Symantec Email Security https://www.symantec.com
- SpamFighter http://www.spamfighter.com
- Avast https://www.avast.com
- K9 http://keir.net
- Spamihilator http://www.spamihilator.com
- G-Lock SpamCombat http://www.glocksoft.com
- Cyberoam Anti-spam www.cyberoam.com
- AVG Antivirus http://www.avgcloudcare.net

The below is a list of anti-spammer tools for email security.

MX Guarddog

Source: https://www.mxguarddog.com

MX Guarddog offers complete email security, with no software to install and no changes to your email clients. The tool protects user emails against, viruses, malware, phishing emails, DoS attacks etc.

FireEye Email Security

Source: https://www.fireeye.com

FireEye Email Security products detonate and analyze suspicious email attachments and embedded URLs and block malicious activity to enhance email security. With these capabilities, organizations can prevent, detect, and respond to email-based cyber-attacks. AV and anti-spam protection are available to handle casual attacks and nuisance traffic. Customers can select Email Threat Prevention Cloud (ETP) for a complete, off-premise email security solution with no hardware or software to install.

Symantec Email Security

Source: https://www.symantec.com

Symantec Email Security effectively blocks unwanted email. It is a cable of blocking spear-phishing and targeted attack malicious URLs with Real Time Link. It analyzes the email body, subject, and headers, as well as text within document attachments, to identify and prevent loss of confidential data.

SpamFighter

Source: *http://www.spamfighter.com*

SpamFighter protects all the email accounts on your PC. It protects against phishing, identity theft, and other email fraud. Blacklist and block emails and domains.

Avast

Source: *https://www.avast.com*

Avast Internet Security has anti-spam features which allow the so you can stay safe from phishing and do not have to waste your time with junk emails.

K9

Source: *http://keir.net*

K9 is an email filtering application that works in conjunction with the regular POP3 email program. It automatically classifies incoming emails as spam (junk email) or non-spam without the need for maintaining dozens of rules or constant updates to be downloaded. It uses intelligent statistical analysis that can result in extremely high accuracy over time. K9 is for standard POP3 email accounts only. It does not support IMAP nor does it support Hotmail, AOL or any other kind of webmail type systems. It does not natively support SSL or secure authentication.

Spamihilator

Source: *http://www.spamihilator.com*

Spamihilator works between the email client and the Internet and examines every incoming message. It filters the spam and non-spam mails. The Spamihilator uses a number of filters in order to identify spam present on the user network. The program works with almost every email client, such as Outlook, Mozilla Thunderbird, Eudora, IncrediMail, Pegasus Mail, Phoenix Mail, Opera, etc.

G-Lock SpamCombat

Source: *http://www.glocksoft.com*

SpamCombat removes the spam, virus, and junk emails from the inbox. It eliminates all unwanted messages at the server level without receiving them with the email client. G-Lock SpamCombat uses filters like: Complex Filter, Whitelist, Blacklist, HTML Validator, DNSBL filter, and the Bayesian filter in order to avoid spam in the inbox.

Cyberoam Anti-spam

Source: *https://www.cyberoam.com*

Cyberoam Anti-Spam solution provides real-time spam protection over SMTP, POP3, IMAP protocols, protecting organizations from zero-hour threats and blended attacks that involve spam, malware, botnets, phishing, Trojans.

AVG Antivirus

Source: *http://www.avgcloudcare.net*

AVG anti-virus is a cloud-based email security service that delivers comprehensive protection against spam, viruses, phishing attacks, and other email-borne threats. It performs an automatic update and identifies the spam before it affects the user's network.

Enabling Pop-up Blockers

C|ND Certified Network Defender

- Malware may come through unwanted Pop-ups on the site that users are visiting
- Enable Pop-up Blockers feature to prevent unwanted windows from opening

1 Internet Explorer

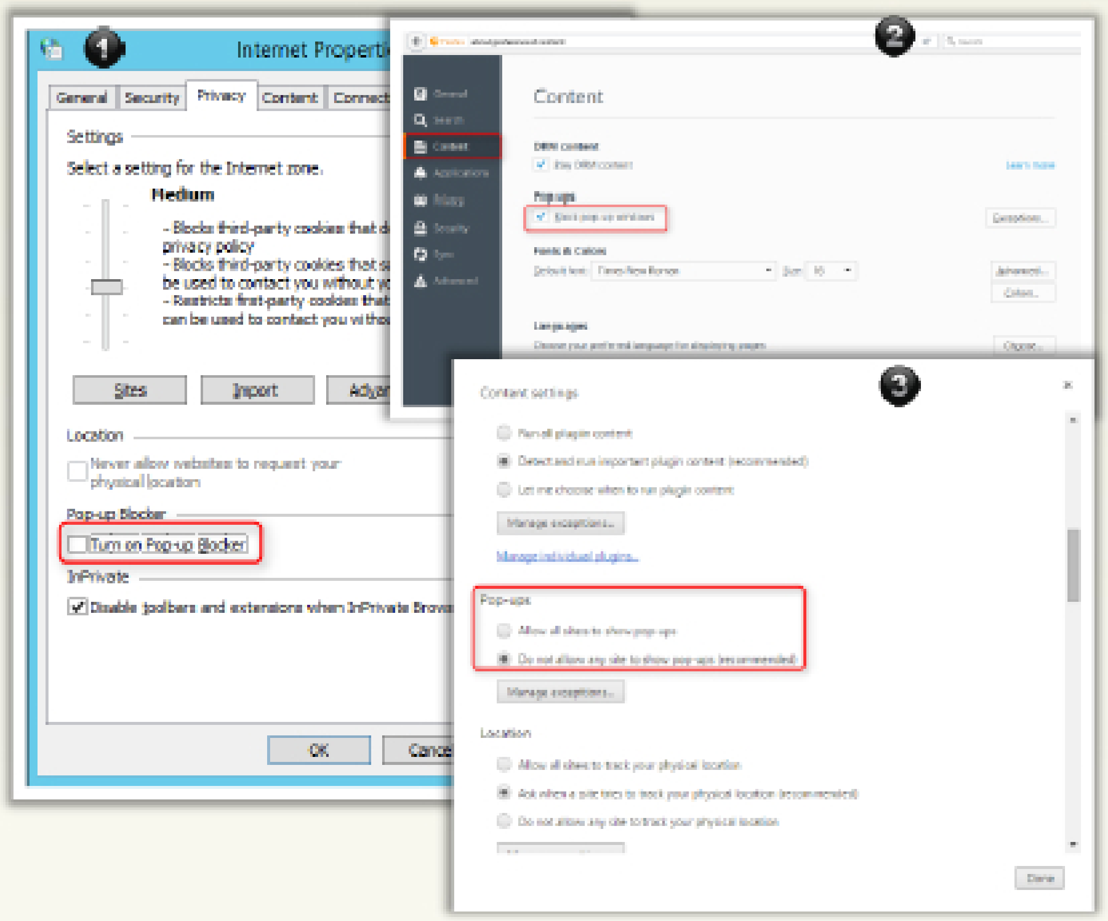
Go to Control Panel → Internet Options → Privacy tab

2 Mozilla Firefox

Go to Options → Content and Check Block pop-up windows checkbox

3 Google Chrome

- Go to Settings, Click Show advanced settings.
- Under "Privacy," click Content settings.
- Under "Pop-ups," select Do not allow any site to show pop-ups (recommended) or Allow all sites to show pop-ups.



Settings
Select a setting for the Internet zone.
Medium
- Blocks third-party cookies that d… privacy policy
- Blocks third-party cookies that s… be used to contact you without y…
- Restricts first-party cookies that can be used to contact you witho…

Sites | Import | Advan…

Location
□ Never allow websites to request your physical location

Pop-up Blocker
□ Turn on Pop-up Blocker

InPrivate
☑ Disable toolbars and extensions when InPrivate Brows…

OK | Cancel

DRM content
☑ Play DRM content

Pop-ups
☑ Block pop-up windows

Fonts & Colors

Languages

○ Run all plugin content
● Detect and run important plugin content (recommended)
○ Let me choose when to run plugin content

Manage exceptions…

Manage individual plugins…

Pop-ups
○ Allow all sites to show pop-ups
● Do not allow any site to show pop-ups (recommended)

Manage exceptions…

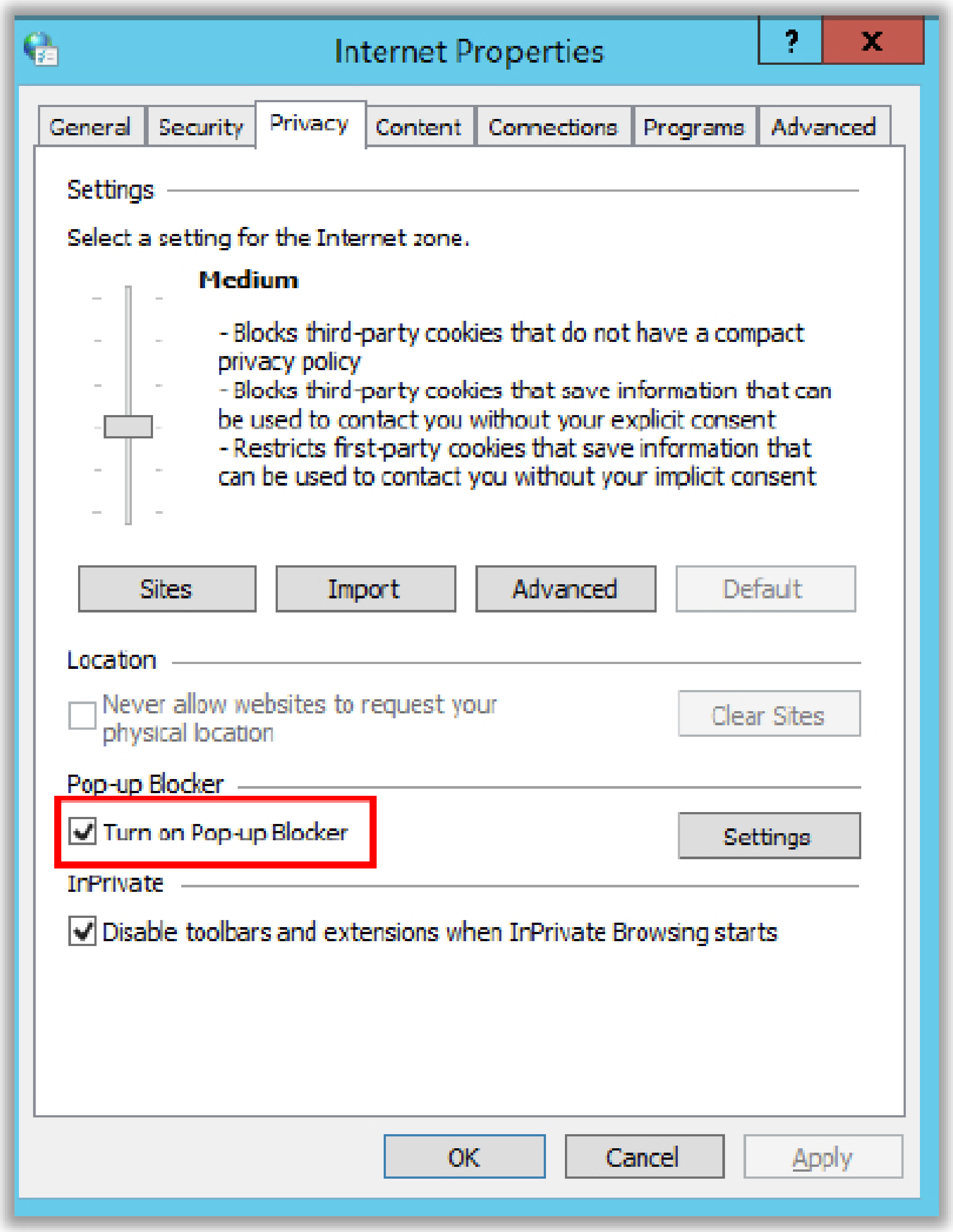
Location
○ Allow all sites to track your physical location
● Ask when a site tries to track your physical location (recommended)
○ Do not allow any site to track your physical location

Pop-up blocker is a feature that automatically prevents websites from opening windows that aren't the main browser window. Pop-up blockers allow you to control what happens as you travel the web and prevent sites from filling your desktop with pop-up windows you do not want or need. Now all modern browsers have pop-up blockers.

It prevents the unnecessary webpages and their pop-ups to store in the system. Usually, sites add pop-ups so that users can get extra information about their search. However, it is advisable to turn on the pop-up blocker, to avoid any intrusion on the system.

Follow the below steps to enable pop-up blocker feature to prevent unwanted windows from opening:

- **Internet Explorer:**
  1. Click on Start → **Control Panel**
  2. Select Internet Options → **Privacy tab**
  3. To enable the pop-up blocker, check on the box "**turn on pop-up blocker**"
  4. Click on **Settings** option, to provide exceptions to the websites
  5. Enter the name of the websites in the textbox "**Address of website to allow**" →Allow
  6. Select the "**Blocking Level**" as per the requirement
  7. Close → **Apply** → **OK**



Internet Properties

General | Security | Privacy | Content | Connections | Programs | Advanced

Settings

Select a setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that save information that can be used to contact you without your explicit consent
- Restricts first-party cookies that save information that can be used to contact you without your implicit consent

Sites | Import | Advanced | Default

Location

□ Never allow websites to request your physical location — Clear Sites

Pop-up Blocker

☑ Turn on Pop-up Blocker — Settings

InPrivate

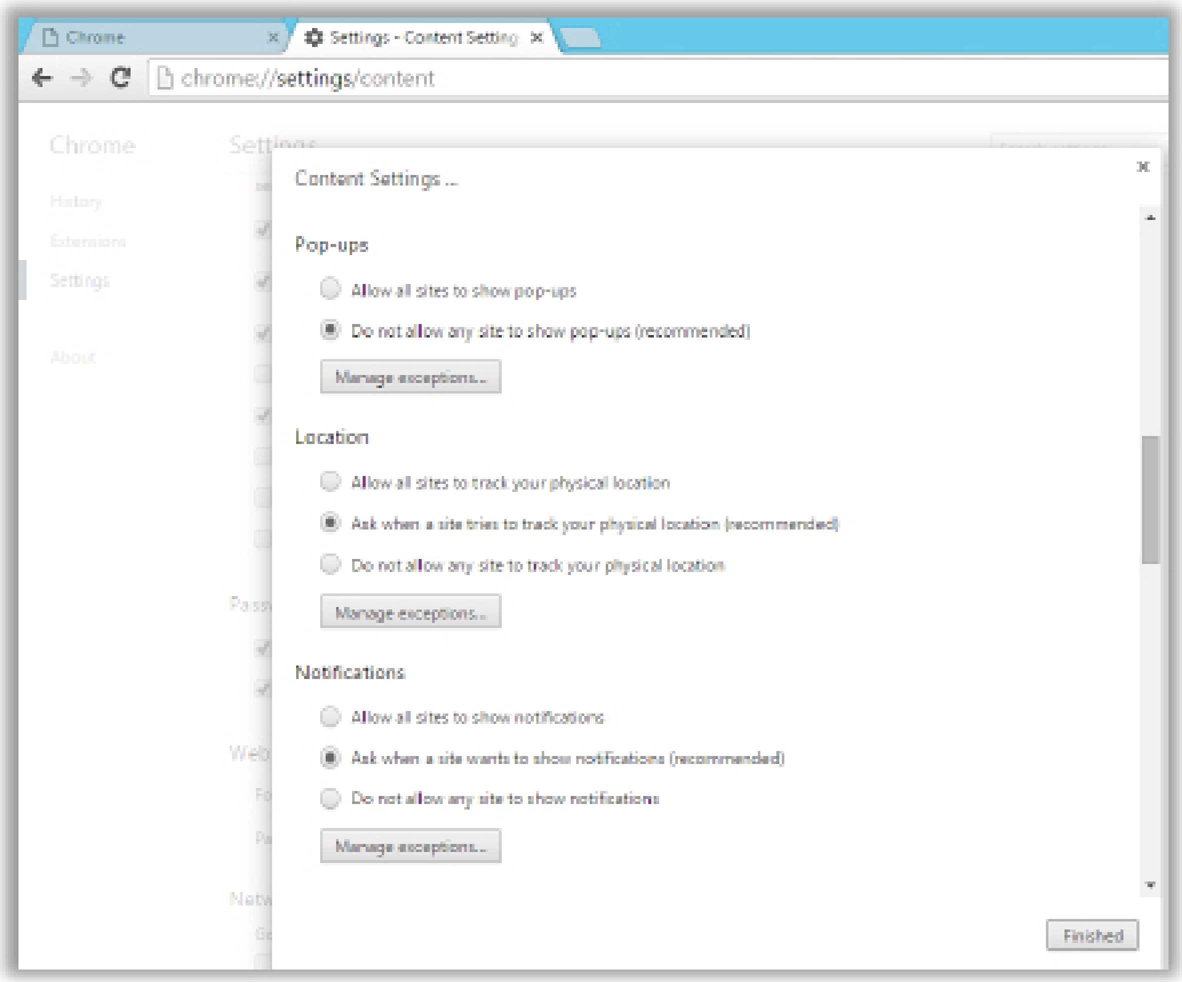
☑ Disable toolbars and extensions when InPrivate Browsing starts

OK | Cancel | Apply

FIGURE 6.20: Enabling Pop-up Blocker in Internet Explorer

- **Google Chrome:**

1. In Google Chrome, ≡ Click → **Settings**
2. Go to Show advanced Settings → Privacy → **Content Settings**
3. In Pop-ups → Do not allow any site to show pop-ups → **Finished**



Settings - Content Settings

chrome://settings/content

Content Settings ...

Pop-ups

○ Allow all sites to show pop-ups
● Do not allow any site to show pop-ups (recommended)

Manage exceptions...

Location

○ Allow all sites to track your physical location
● Ask when a site tries to track your physical location (recommended)
○ Do not allow any site to track your physical location

Manage exceptions...

Notifications

○ Allow all sites to show notifications
● Ask when a site wants to show notifications (recommended)
○ Do not allow any site to show notifications

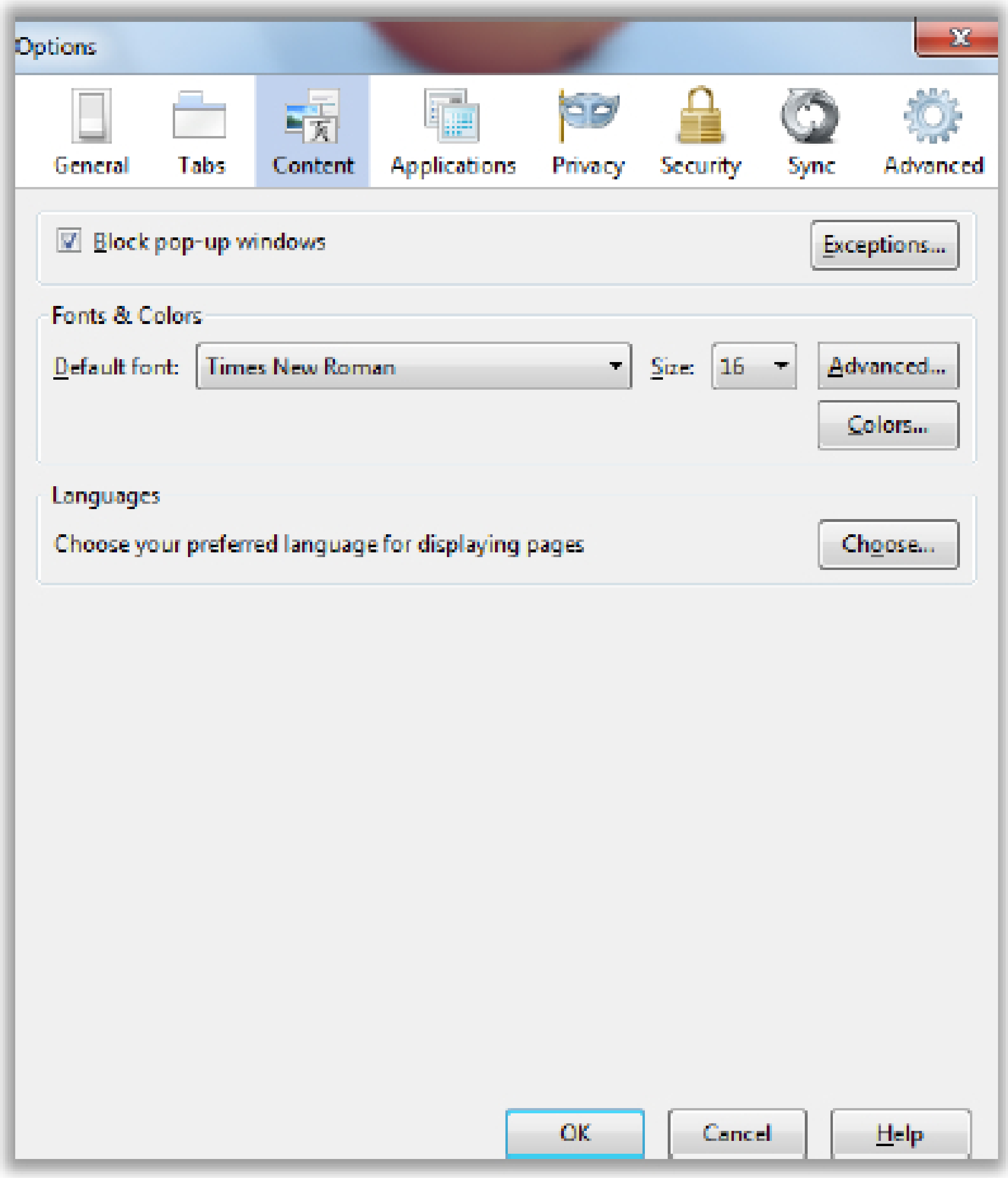
Manage exceptions...

Finished

FIGURE 6.21: Pop-ups settings in Google Chrome

- **Mozilla Firefox:**

1. In Mozilla Firefox, click ≡ → **Options**
2. Go to Content →Check the box "**Block pop-up windows**"
3. **Exceptions tab** will allow adding the URL which exclude from pop-up block rule
4. Click **OK**



Options

☑ Block pop-up windows

Fonts & Colors

Default font: Times New Roman Size: 16

Languages

Choose your preferred language for displaying pages

FIGURE 6.22: Enabling pop-up windows in Mozilla Firefox

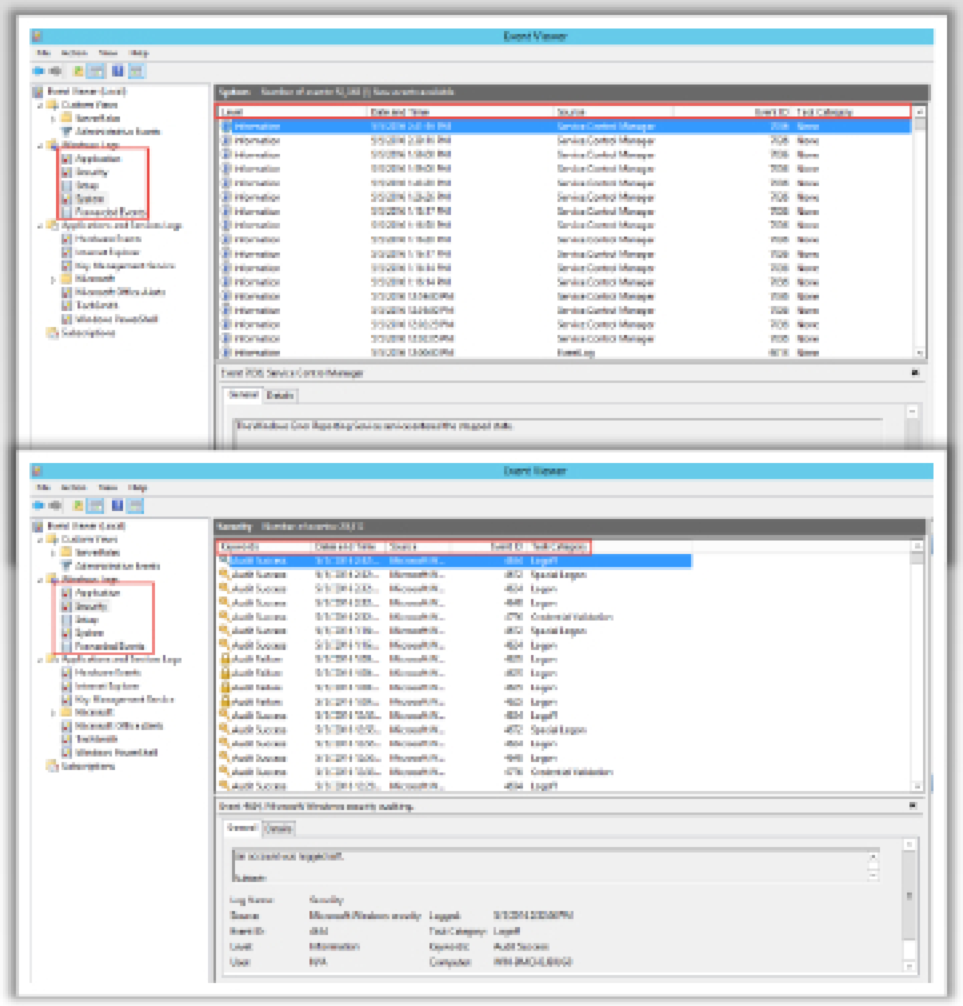
Windows Logs Review and Audit

- Conduct peer log review and audit periodically to look for any suspicious activity and respond to the security incidents
- You need to have administrative access privileges to conduct a log review and audit
- Event Viewer provides a quick overview of when, where, and how an event occurred
- Navigate to Control Panel, go to Administrative Tools, and then double-click Event Viewer
- Check Windows Event Log for various types of logs
  - System log
  - Security logs
  - Setup logs
  - Application logs

- Typical log entries contain following types of information about the events:
  - **Level:** It defines the severity of event. Various types of severity levels are Information, Warning, Error, Critical. and component
  - **Keywords:** It defines type of event occurred. Various types of events are AuditFailure, AuditSuccess, Classic, Correlation Hint, Response Time, SQM, WDI Context and WDI Diag
  - **Date and Time:** It defines date of events occurred
  - **Source:** It defines the source of event
  - **Event ID:** An unique event ID is assigned for each type of event.
  - **Task Category:** It defines task categories

Note: Critical systems require at least a daily log review

Windows Logs Review and Audit (Cont'd)



Conduct a Windows Event log review based on the Event ID, source, date and time of events and its severity levels

Some log entries for suspicious behavior can be:

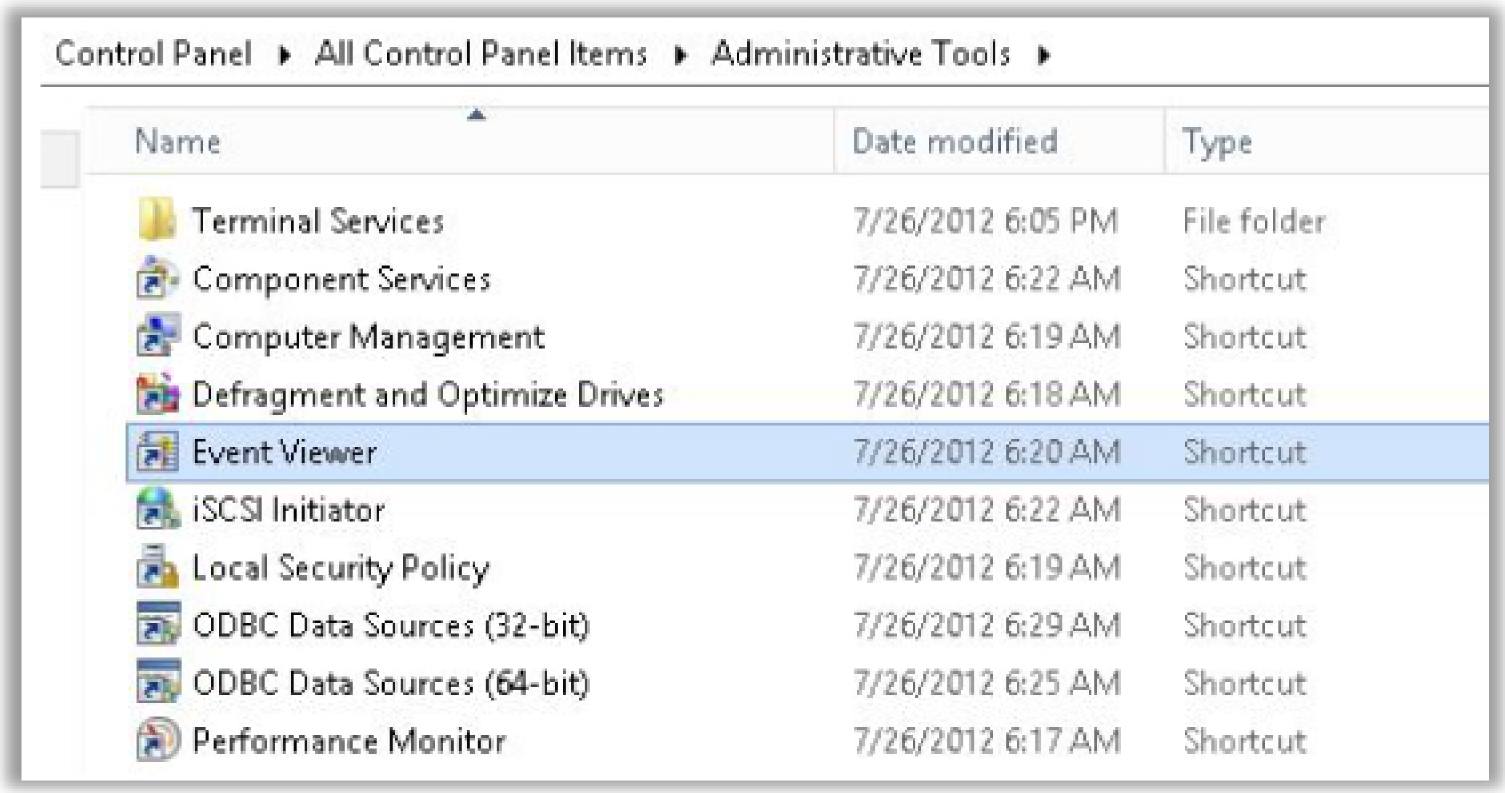
- Consecutive login failure attempts
- Login in attempts in non office hours
- Authority change, addition and removal attempts
- Account unlocked/password reset attempts

Note: CND Resource Kit contains detailed list of Event IDs for corresponding log events.

Windows Log review and Audit involve monitoring and analyzing the log entries for suspicious behavior. Administrators find the log review and audit helpful in troubleshooting problems with Windows and other programs as well as detecting signs of the malicious activities or attempts such as unauthorized login attempts made on the computer.

All the activities of a user on a Windows computer is recorded and stored in a file called Windows Event Log. Administrators can view these log entries with the help of Event Viewer. Event Viewer tracks information in several different logs.

- **Event Viewer:**
  1. Go to Control Panel → **Administrative Tools**
  2. In the Administrative Tools window, double click on **Event Viewer**

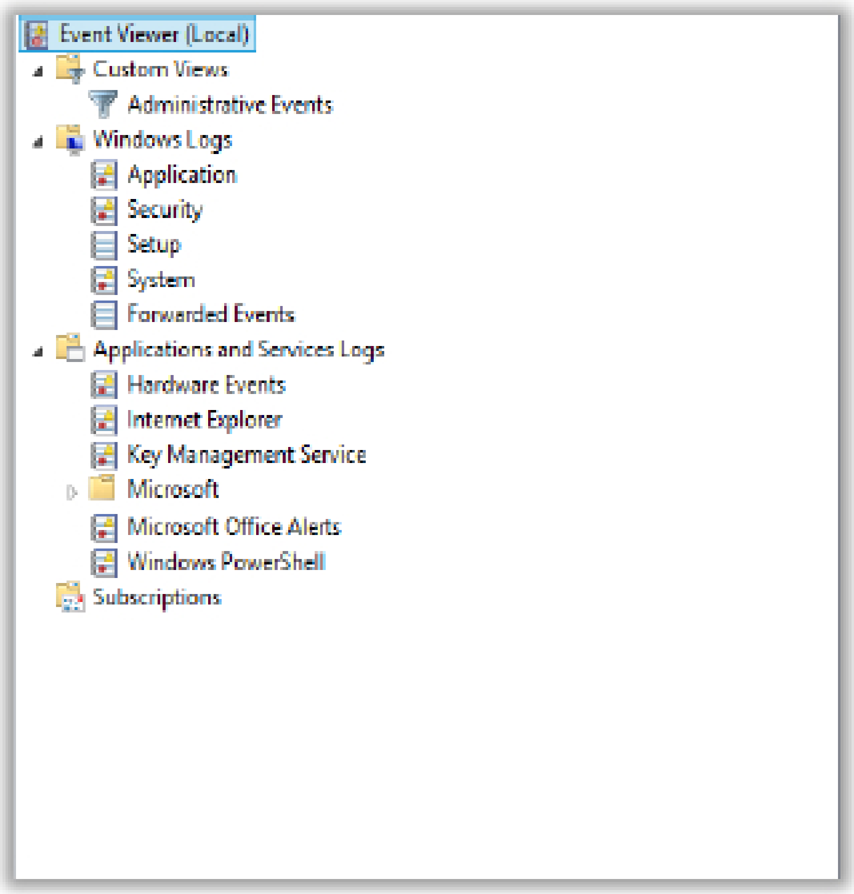


Control Panel ▸ All Control Panel Items ▸ Administrative Tools ▸

Name	Date modified	Type
Terminal Services	7/26/2012 6:05 PM	File folder
Component Services	7/26/2012 6:22 AM	Shortcut
Computer Management	7/26/2012 6:19 AM	Shortcut
Defragment and Optimize Drives	7/26/2012 6:18 AM	Shortcut
Event Viewer	7/26/2012 6:20 AM	Shortcut
iSCSI Initiator	7/26/2012 6:22 AM	Shortcut
Local Security Policy	7/26/2012 6:19 AM	Shortcut
ODBC Data Sources (32-bit)	7/26/2012 6:29 AM	Shortcut
ODBC Data Sources (64-bit)	7/26/2012 6:25 AM	Shortcut
Performance Monitor	7/26/2012 6:17 AM	Shortcut

FIGURE 6.23: Event Viewer

- The main screen of the Event Viewer is divided into three parts:
  - **Navigation Pane:** It displays the various types of logs and their related features.



Event Viewer (Local)
- Custom Views
  - Administrative Events
- Windows Logs
  - Application
  - Security
  - Setup
  - System
  - Forwarded Events
- Applications and Services Logs
  - Hardware Events
  - Internet Explorer
  - Key Management Service
  - Microsoft
  - Microsoft Office Alerts
  - Windows PowerShell
- Subscriptions

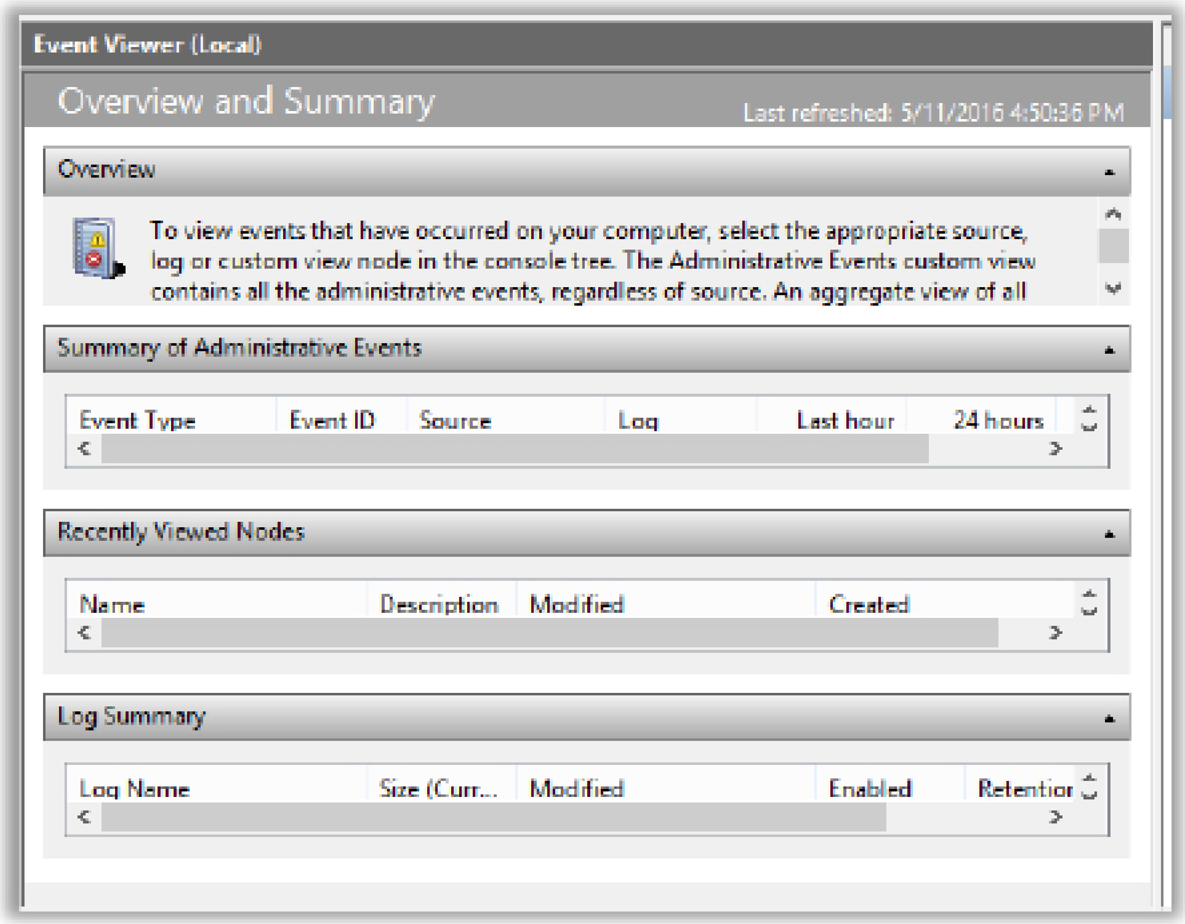
FIGURE 6.24: Navigation Pane in Event Viewer

- **Detail Pane:** In the detail pane, event entries are listed in chronological order.

Clicking on any event entry will show the event's detailed information in the bottom half of the pane.

Each of these events also includes a level which indicates its severity. There are three levels:

1. **Information messages**: These are shown with icons with an "i" in a white circle, which depicts the system performed the task successfully.
2. **Warning messages**: These are shown with a yellow triangular icon, which depicts that an event occurred which, might create a problem later.
3. **Error and critical messages:** These are shown with an exclamation mark inside a red circle, which depicts that a significant problem occurred.



To view events that have occurred on your computer, select the appropriate source, log or custom view node in the console tree. The Administrative Events custom view contains all the administrative events, regardless of source. An aggregate view of all

Event Type	Event ID	Source	Log	Last hour	24 hours

Name	Description	Modified	Created

Log Name	Size (Curr...	Modified	Enabled	Retentior

FIGURE 6.25: Summary window of an Event

- **Action Pane:** The action menu items on the right pane include many of the options available from the main menu bar. This includes saving event entries to a file, opening a saved event file, exporting or filtering events, etc.

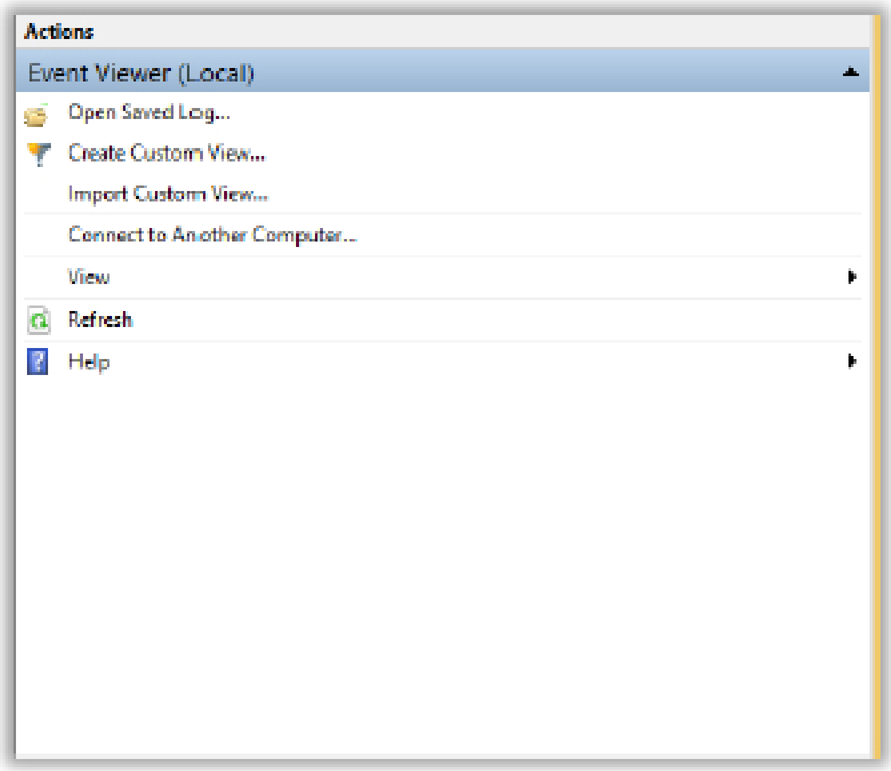
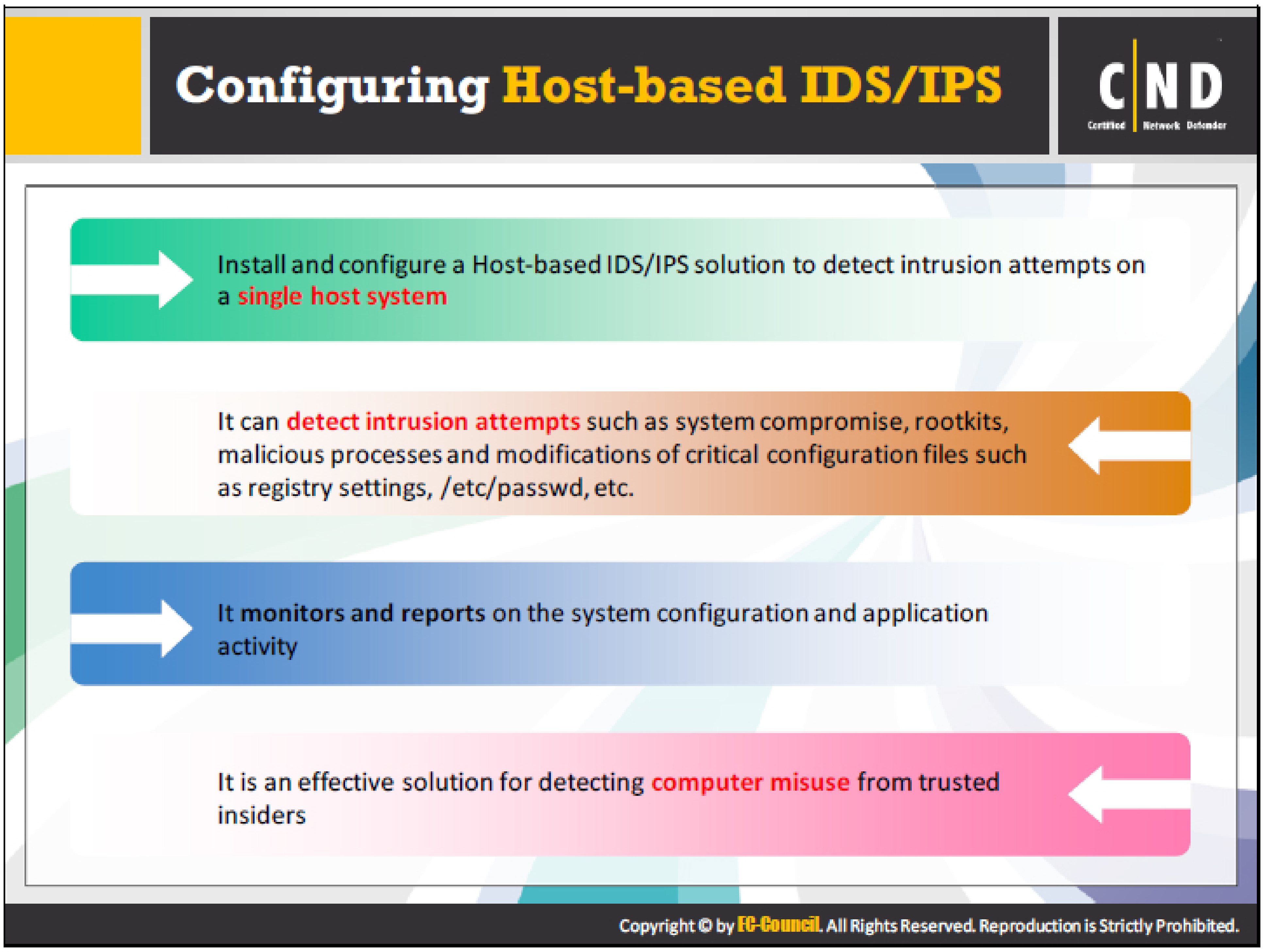


FIGURE 6.26: Action Pane in Event Viewer

- **Windows Event Logs consists of five types of logs:**
  1. Application Log: It stores logs of applications installed on the computer.
  2. Security Log: It stores information related to login attempts, user account privileges, etc.
  3. Setup Log: It stores the information captured during the time of OS installation.
  4. System Log: It stores the information of the messages sent by the OS.
  5. Forwarded Events: Other host machines in the network send these events when the local machine is acting as a central domain for them.
- **Each event in a log contains the following information:**
  - Date: The date of the occurrence of the event.
  - Time: The time of the occurrence of the event.
  - User: The name of the user logged in at the time of the occurrence of the event.
  - Computer: Name of the computer.
  - Event ID: The identification number that states the event type.
  - Source: The source for the occurrence of the event.
  - Type: The type of event occurred.
  - Level: Represents the severity of the events. The different levels are as follows:
    - Information: Informs regarding the change in the application.
    - Warning: Informs that an issue occurred can impact the services of the system.
    - Error: Informs that an error has occurred.
    - Critical: Informs that an error that occurred in the application cannot be rectified.
  - Keywords: Used to search for events.
  - Log: The name of the log where the event was created.

In an organization, an administrator should have the practice of monitoring and auditing the log files. Example of some of the suspicious activities on the computer may include:

- Log entries for suspicious behavior can be:
  - Consecutive login failure attempts.
  - Login in attempts in non-office hours.
  - Authority change, addition and removal attempts.
  - Account unlocked/password reset attempts.



Configuring Host-based IDS/IPS

Install and configure a Host-based IDS/IPS solution to detect intrusion attempts on a single host system

It can detect intrusion attempts such as system compromise, rootkits, malicious processes and modifications of critical configuration files such as registry settings, /etc/passwd, etc.

It **monitors and reports** on the system configuration and application activity

It is an effective solution for detecting computer misuse from trusted insiders

The host-based IDS analyzes and identifies the presence of any malicious activity in a computer system on which the IDS works. It analyzes all the parts of the computer system, especially the resources used by each application, the current state of the system, the storage information that includes RAM, log files, file system, and checks for any changes in the application.

The host-based IDS detects for:

- System compromise.
- Unwanted or unused applications.
- Any kind of modification in the critical configuration files like registry settings.
- Malware.
- Rootkits.
- Rogue processes.
- Any important services that paused in between.
- User access to systems and applications.

The host-based IDS analyze the internal and external of a computer system and checks whether all applications and programs in the computing system follow the security policies. The host-based IDS can work in combination with NIDS, which means that host-based IDS can detect any malfunction missed by network-based IDS. The administrator can compare the analysis done by host-based IDS and network-based IDS in order to confirm the presence of any changes in the system performed by the intruders.

However, the network administrator should consider implementing both network-based IDS and host-based IDS to secure their network.

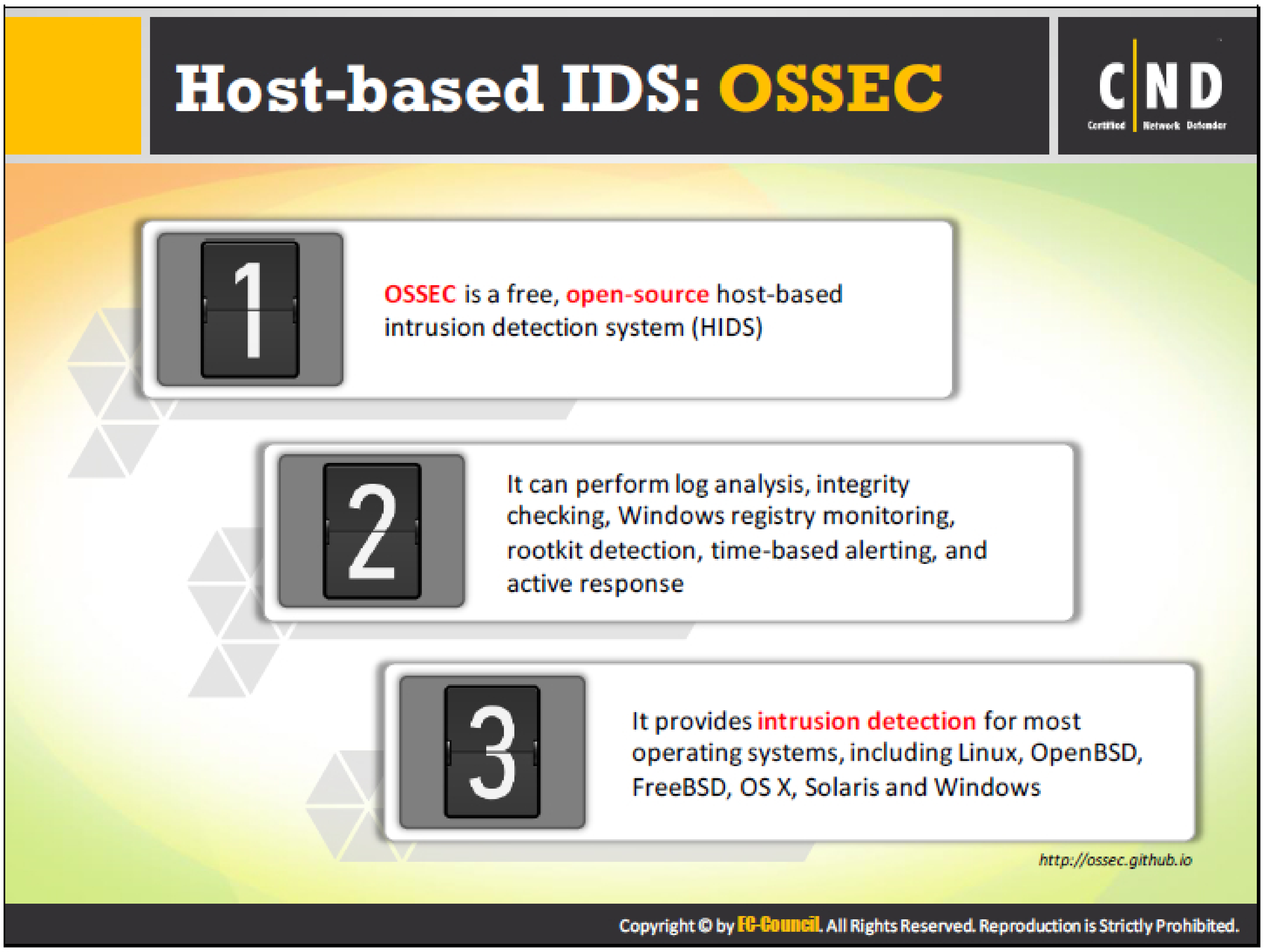
Certain differences between the NIDS and HIDS are:

Difference	Host-based IDS	Network-based IDS
Analysis	Analyze the log files and contains all information regarding the status of the system	Network based analyze the network traffic
Protection	Protects even when LAN is off	Protects only when LAN is ON
Versatility	More Versatile	Less versatile
Affordability	More affordable	Cheaper to implement and needs less administration

TABLE 6.1: NIDS vs HIDS

Advantages of host-based IDS:

- Very low false positives: The host-based IDS perform analysis directly on the host, thereby analyzing all the log files. This reduces the number of false positives.
- Narrow operating system focus: Host-based IDS function only on certain operating systems which in turn minimizes the number of drawbacks.
- Non-network based attacks: Identifies the attacks on the physical machine as well.



Host-based IDS: OSSEC

1. OSSEC is a free, open-source host-based intrusion detection system (HIDS)

2. It can perform log analysis, integrity checking, Windows registry monitoring, rootkit detection, time-based alerting, and active response

3. It provides intrusion detection for most operating systems, including Linux, OpenBSD, FreeBSD, OS X, Solaris and Windows

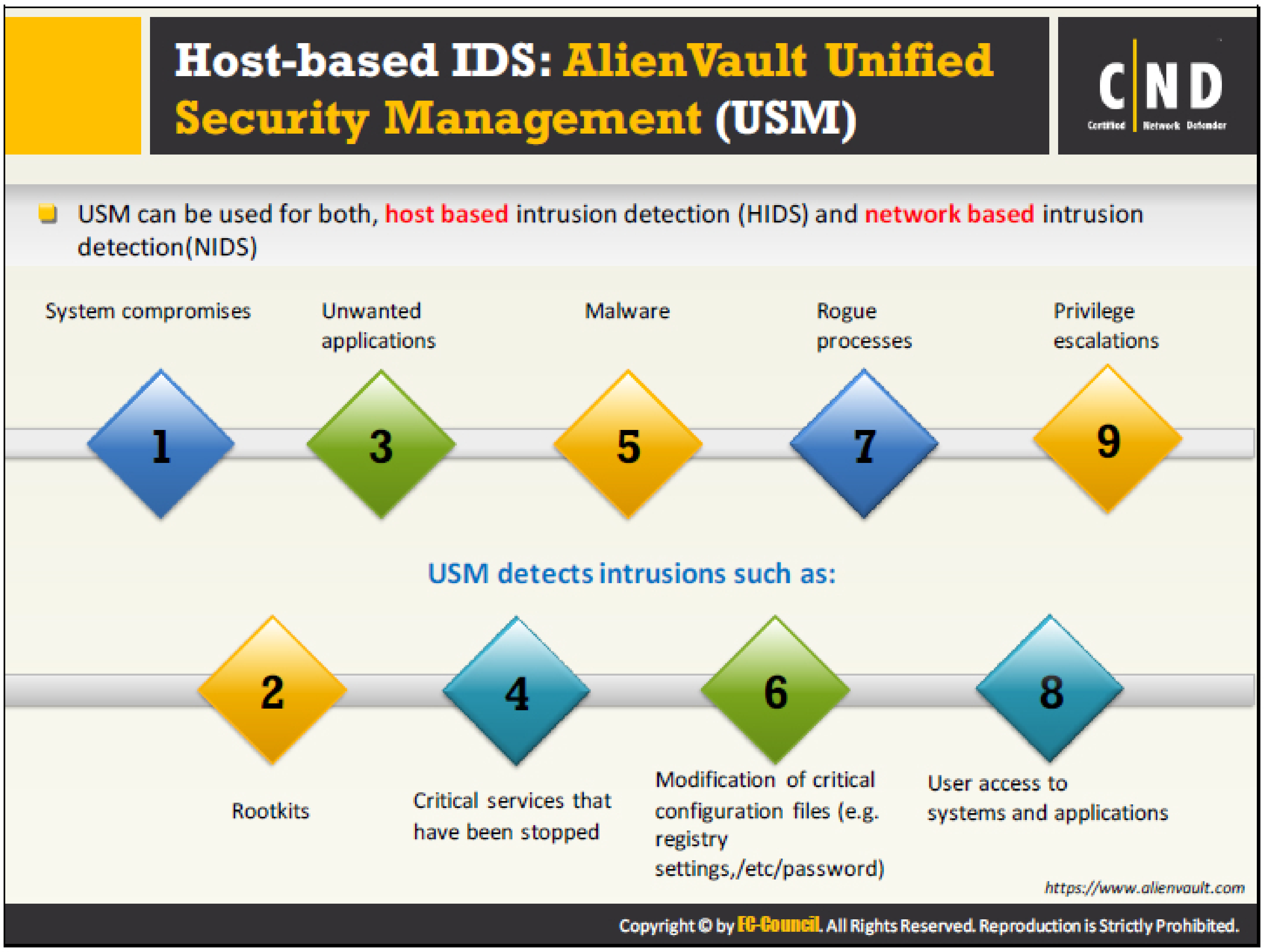
http://ossec.github.io

OSSEC is a platform to monitor and control your systems. It mixes together all the aspects of HIDS (host-based intrusion detection); log monitoring, Security Incident Management (SIM)/Security Information and Event Management (SIEM). It runs on most operating systems, including Linux, OpenBSD, FreeBSD, Mac OS X, Solaris and Windows.

Key Features:

- File Integrity checking: The goal of file integrity checking (or FIM - file integrity monitoring) is to detect these changes and alert you when they happen. It can be an attack, or a misuse by an employee or even a typo by an admin, any file, directory or registry change will be alerted to you.
- Log Monitoring: Every operating system, application, and device on your network generates logs (events) to let you know what is happening. OSSEC collects, analyzes and correlates these logs to let you know if something suspicious is happening (attack, misuse, errors, etc.).
- Rootkit Detection: Criminal hackers want to hide their actions, but when using rootkit detection you can be notified when the system is modified in a way common to rootkits.
- Active Response: Active response allows OSSEC to take immediate action when specified alerts are triggered. This may prevent an incident from spreading before an administrator can take action.

Source: *http://ossec.github.io*



Host-based IDS: AlienVault Unified Security Management (USM)

- USM can be used for both, host based intrusion detection (HIDS) and network based intrusion detection(NIDS)

USM detects intrusions such as:

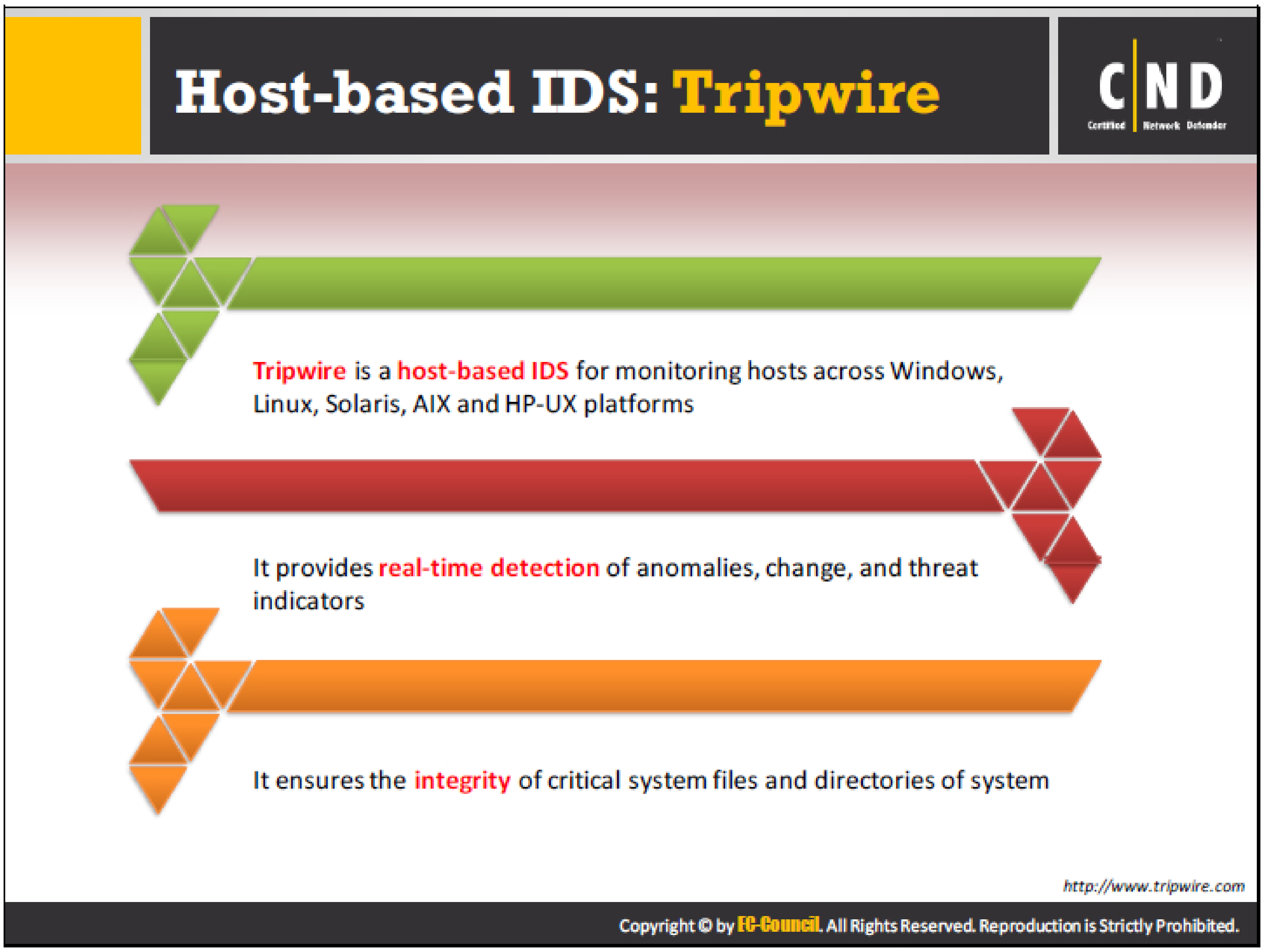
1. System compromises
2. Rootkits
3. Unwanted applications
4. Critical services that have been stopped
5. Malware
6. Modification of critical configuration files (e.g. registry settings,/etc/password)
7. Rogue processes
8. User access to systems and applications
9. Privilege escalations

https://www.alienvault.com

AlienVault's Unified Security Management™ (USM™) platform accelerates and simplifies threat detection, incident response and compliance management for IT teams with limited resources. With essential security controls and integrated threat intelligence built-in, AlienVault USM puts complete security visibility of threats affecting your network and how to mitigate them within fast and easy reach.

- Its intrusion detection capability includes:
    - Network IDS
    - Host IDS
    - File Integrity Monitoring (FIM)

Source: https://www.alienvault.com



Host-based IDS: Tripwire

Tripwire is a host-based IDS for monitoring hosts across Windows, Linux, Solaris, AIX and HP-UX platforms

It provides real-time detection of anomalies, change, and threat indicators

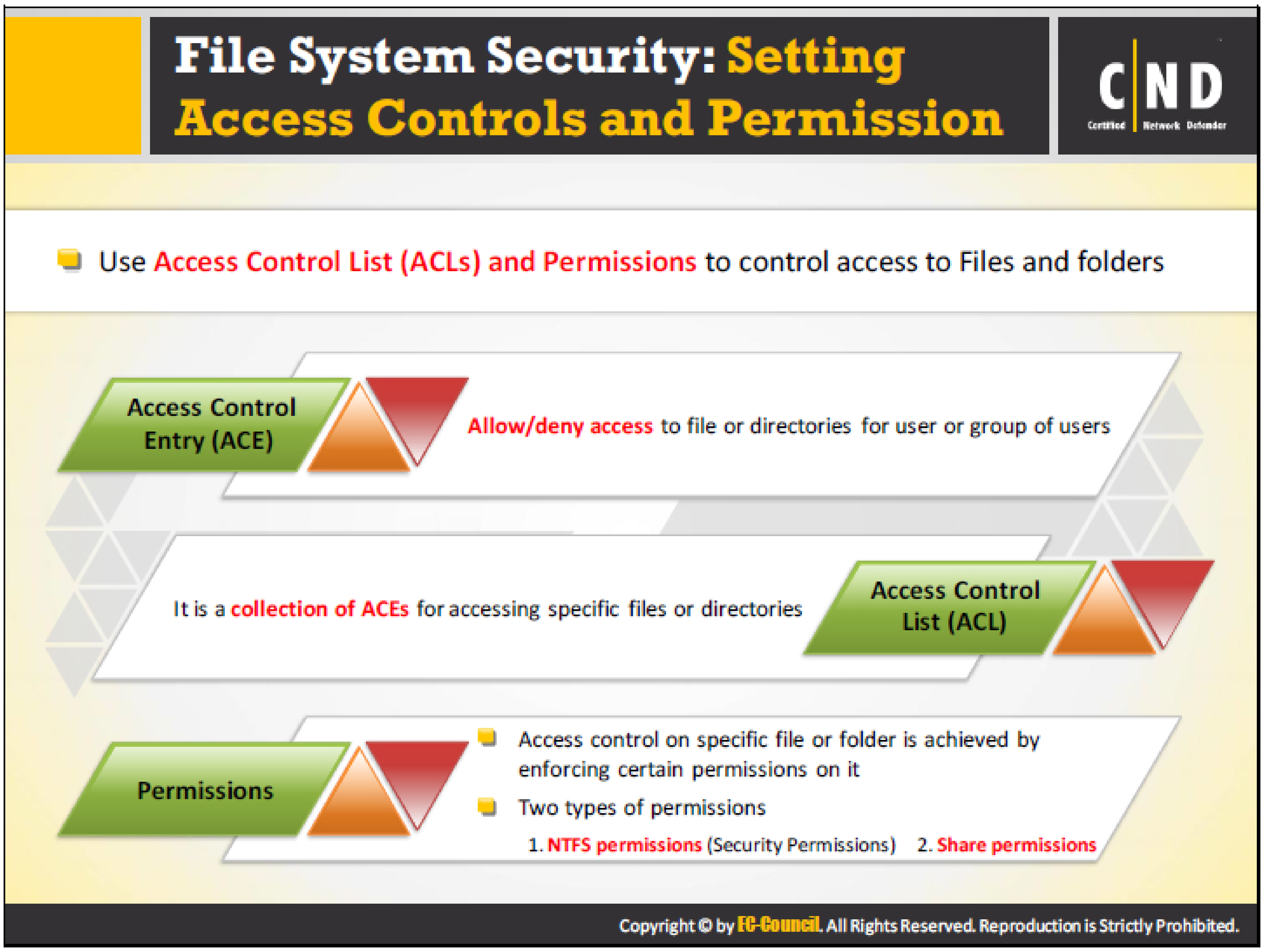
It ensures the integrity of critical system files and directories of system

http://www.tripwire.com

Tripwire software can help to ensure the integrity of critical system files and directories by identifying all changes made to them. Tripwire configuration options include the ability to receive alerts via email if particular files are altered and automated integrity checking via a *cron* job. Using Tripwire for intrusion detection and damage assessment helps you keep track of system changes and can speed the recovery from a break-in by reducing the number of files you must restore to repair the system.

Tripwire compares files and directories against a baseline database of file locations, dates modified, and other data. It generates the baseline by taking a snapshot of specified files and directories in a known secure state. (For maximum security, Tripwire should be installed and the baseline created before the system is at risk from intrusion.) After creating the baseline database, Tripwire compares the current system to the baseline and reports any modifications, additions, or deletions.

Source: http://www.tripwire.com



File System Security: Setting Access Controls and Permission

- Use Access Control List (ACLs) and Permissions to control access to Files and folders

Access Control Entry (ACE): Allow/deny access to file or directories for user or group of users

Access Control List (ACL): It is a collection of ACEs for accessing specific files or directories

Permissions:

- Access control on specific file or folder is achieved by enforcing certain permissions on it
- Two types of permissions

  1. NTFS permissions (Security Permissions) 2. Share permissions

Access controls can provide the authority to users, groups and computers to access files and folders in the computer. When a user or an application requests for an access to the operating system resources, they need to submit their credentials to the operating system. The credentials are access tokens created every time a user or an application tries to log in. The operating system verifies whether the access token created as the permission to access the objects before permitting the user or the application to access the objects. Here, the OS compares the details contained in the access tokens with the Access Control Entries (ACE) for verification. The ACE's can block or permit the services depending on the type of the object. For example, the ACE's available for a Printer are Print, Manage Printing and Manage Documents. The ACL's contain a combination of the ACE's of an object.

- **Access Control Principles:**
  - Least amount of access of objects to users or user groups, thereby allowing them to perform only needed functions.
  - The owner of an object is the one who created that object.
  - Proper permissions are set up for files and folders while installing the operating system. Upgrade the level of permissions from least privilege to the desired level during installation itself.
  - The files and other documents included in a folder can inherit the permitted privileges assigned to that folder.

- Appropriate tools can help in managing the permissions of any folders.
- Event viewer helps in viewing the security logs associated with any object.

- **Access Control Entries**: An ACL can have zero or more ACE's wherein each ACE has the access to an object. Overall, there are six types of ACE's out of which securable objects support three (Generic types) and the other three are directory service objects (Object-specified types).
- The three **generic types of ACE's** are:
    - Access denied ACE: Used in the discretionary access control list in order to prevent access to any user.
    - Access allowed ACE: Used in the discretionary access control list in order to allow access to any user.
    - System Audit ACE: Used in the system-access control list in order to create an audit log for each attempt by a user while accessing the objects.
- The three types of **object-specified** types are:
    - Access denied, object specific: Used in the discretionary access control list to block access to a property or property set. It can even stop the inheritance level of a specified type of a child object.
    - Access allowed, object specific: Used in the discretionary access control list to permit access to a property or property set. It can even stop the inheritance level of a specified type of a child object.
    - System audit, object specific: Used in the system-access control list in order to create an audit log when a user attempts to access the child object.

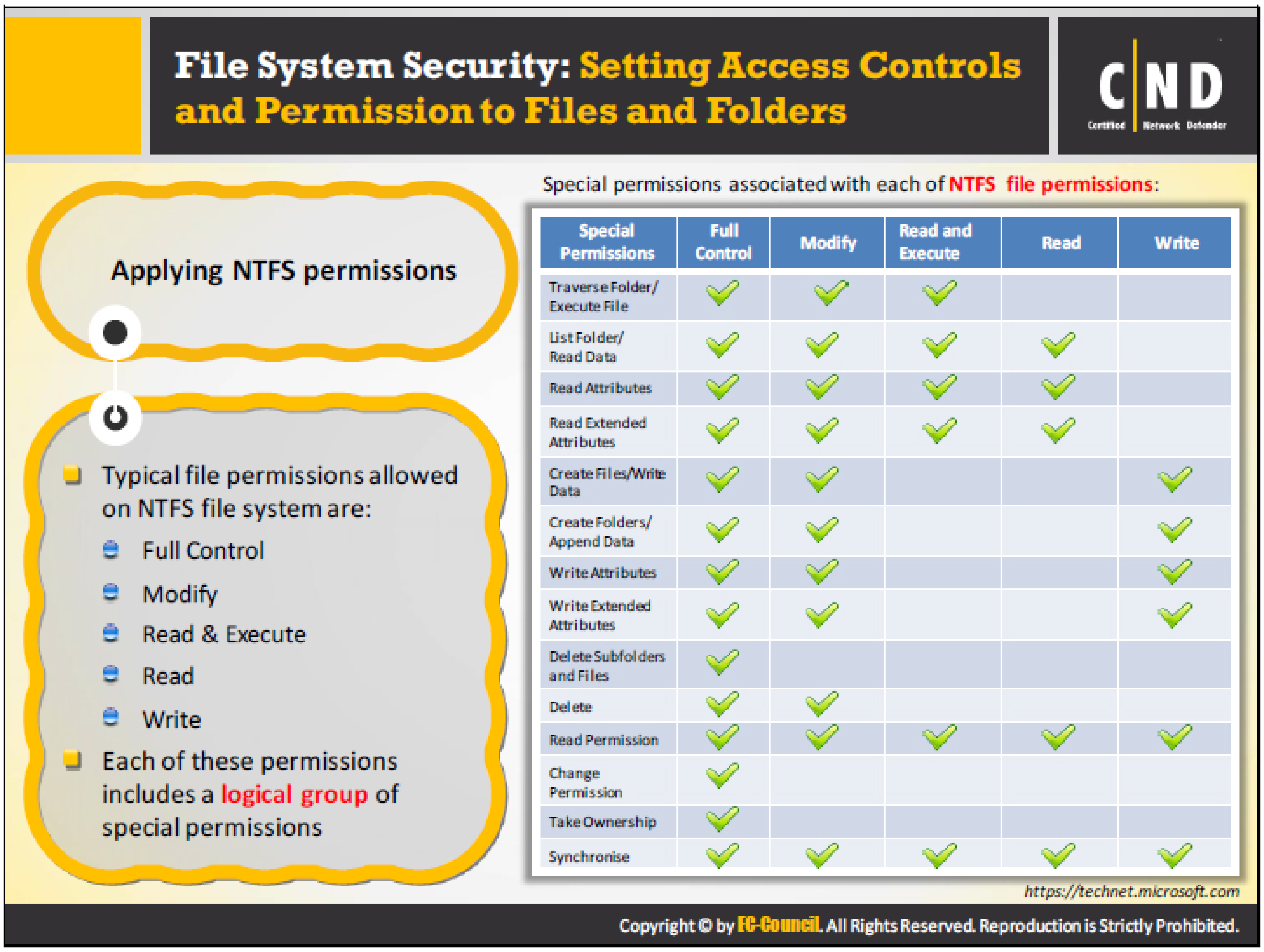
The object-specific types and generic types differ only in the design of the inheritance level.

- **Access Control Lists**: An access control list is a table that provides a detailed description of the access rights of the users towards accessing objects. Every object has an access control list that contains the details of the user rights and privileges for accessing that object. Each OS system has specific ACL's. The ACL's has one or more ACE's that contains the details of the users.
- **Permissions**: Each container or object has a security descriptor attached to itself. This security descriptor contains a detailed description regarding the user access rights. The security descriptor is created along with the container or object. An ACE represents the permission to users or user groups and the whole list or set of permissions is contained in an access control list (ACL). There are two types of permissions:
    - Explicit permission: Permissions that set by default upon creation.
    - Inherited permission: These are permissions achieved from the parent object to the child object.

For example, any files and folders in a folder can inherit the permissions applicable to that particular parent folder. Here, the parent folder has explicit permission, whereas the files and folders have inherited permissions.

- There are two sets of permission entries for accessing a folder on a file server:
  - Share Permission on a folder: Used for files and folders shared across the network or many user accounts. The permissions can be either denied or allowed depending on the users or user accounts. The most commonly used shared permissions are: Full control, Change and Read.
  - NTFS permission on a folder: Controls the permissions over network and local computers. The most commonly used NTFS permissions are: Full control, Modify, read and execute, Read, Write.

Each are independent of each other, however, the final decision on confirming the access permission depends on either of the two.



File System Security: Setting Access Controls and Permission to Files and Folders

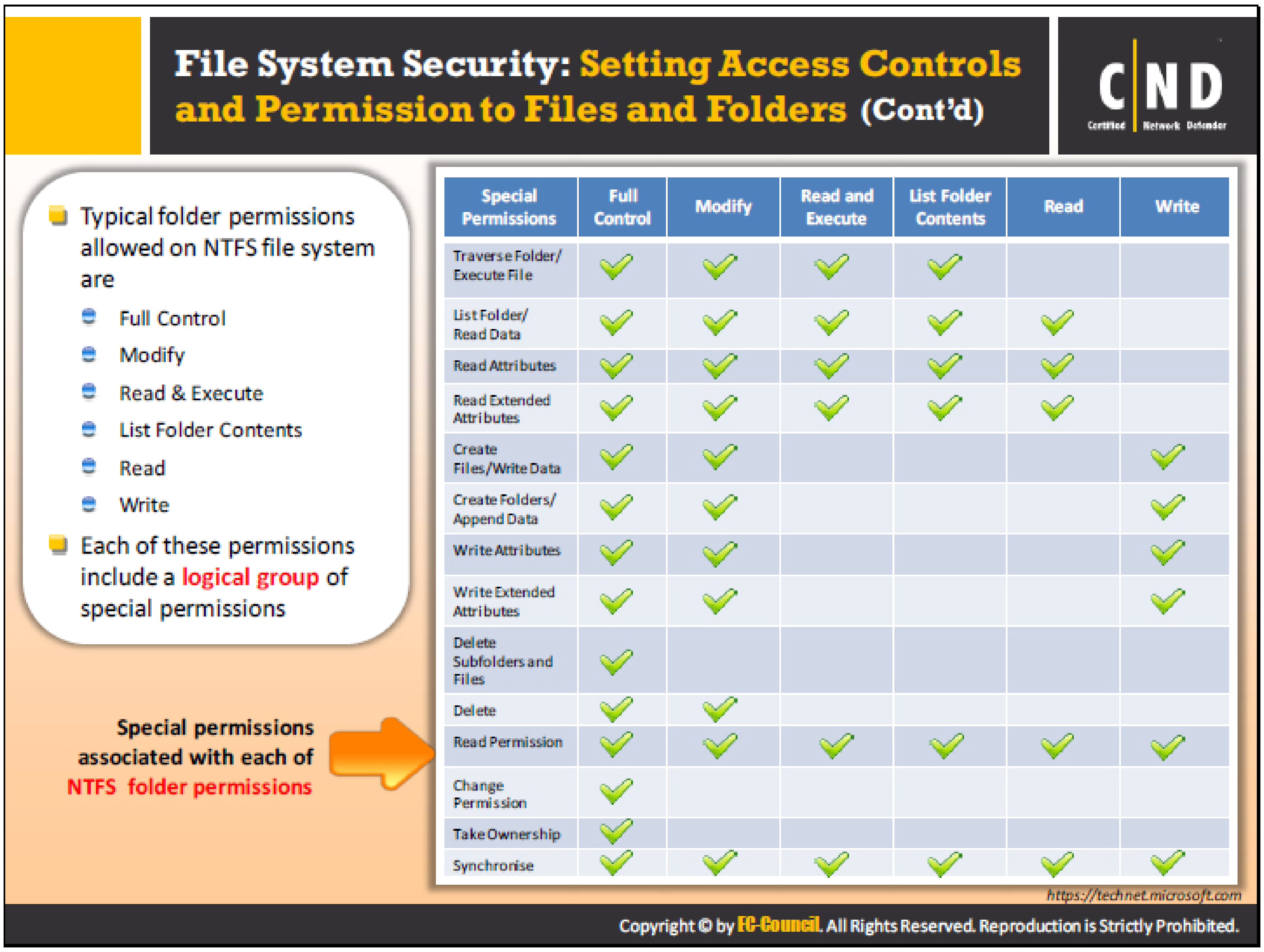
Applying NTFS permissions

- Typical file permissions allowed on NTFS file system are:
  - Full Control
  - Modify
  - Read & Execute
  - Read
  - Write
- Each of these permissions includes a logical group of special permissions

Special permissions associated with each of NTFS file permissions:

Special Permissions	Full Control	Modify	Read and Execute	Read	Write
Traverse Folder/ Execute File	✓	✓	✓		
List Folder/ Read Data	✓	✓	✓	✓	
Read Attributes	✓	✓	✓	✓	
Read Extended Attributes	✓	✓	✓	✓	
Create Files/Write Data	✓	✓			✓
Create Folders/ Append Data	✓	✓			✓
Write Attributes	✓	✓			✓
Write Extended Attributes	✓	✓			✓
Delete Subfolders and Files	✓				
Delete	✓	✓			
Read Permission	✓	✓	✓	✓	✓
Change Permission	✓				
Take Ownership	✓				
Synchronise	✓	✓	✓	✓	✓

https://technet.microsoft.com



File System Security: Setting Access Controls and Permission to Files and Folders (Cont'd)

- Typical folder permissions allowed on NTFS file system are
  - Full Control
  - Modify
  - Read & Execute
  - List Folder Contents
  - Read
  - Write
- Each of these permissions include a logical group of special permissions

Special permissions associated with each of NTFS folder permissions

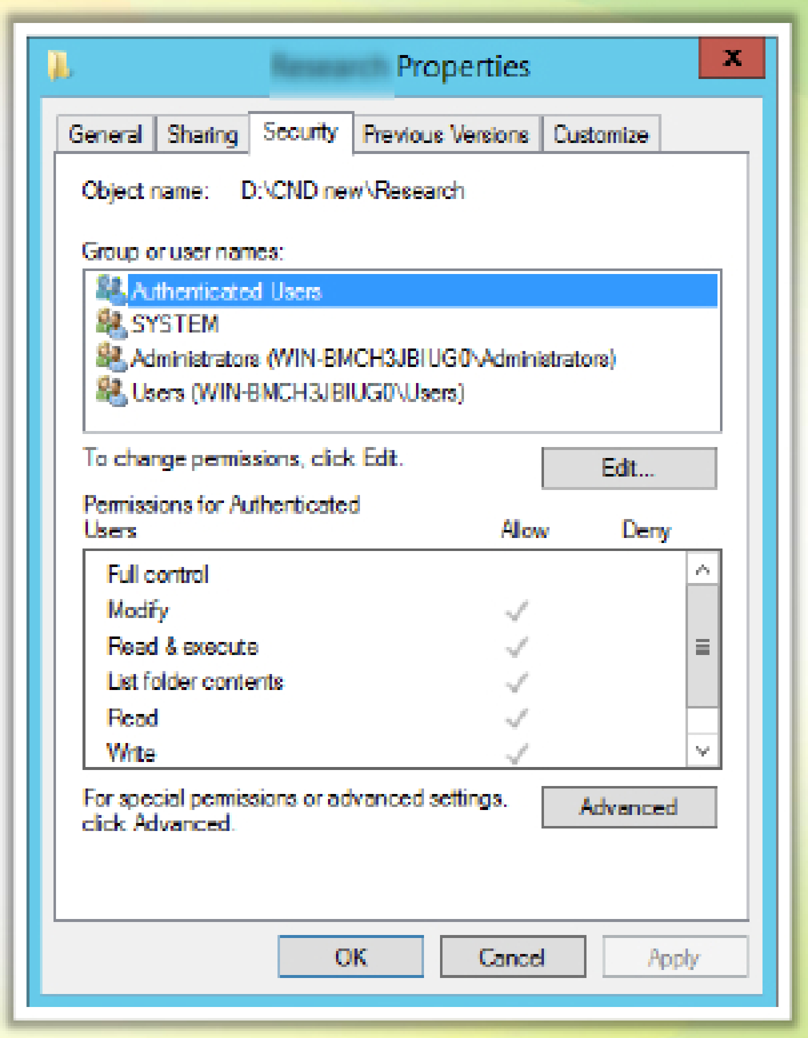
Special Permissions	Full Control	Modify	Read and Execute	List Folder Contents	Read	Write
Traverse Folder/ Execute File	✓	✓	✓	✓		
List Folder/ Read Data	✓	✓	✓	✓	✓	
Read Attributes	✓	✓	✓	✓	✓	
Read Extended Attributes	✓	✓	✓	✓	✓	
Create Files/Write Data	✓	✓				✓
Create Folders/ Append Data	✓	✓				✓
Write Attributes	✓	✓				✓
Write Extended Attributes	✓	✓				✓
Delete Subfolders and Files	✓					
Delete	✓	✓				
Read Permission	✓	✓	✓	✓	✓	✓
Change Permission	✓					
Take Ownership	✓					
Synchronise	✓	✓	✓	✓	✓	✓

https://technet.microsoft.com

File System Security: Setting Access Controls and Permission to Files and Folders (Cont'd)

- To set, view, edit, or remove special permissions:

  1. Go to specific file or folder on which you want to set special permission
  2. Right-click the file or folder, click Properties, and then click the Security tab
  3. Click Advanced
  4. Click Add to set special permissions for a new group or user in Permission Entry Window



Object name: D:\CND new\Research

Group or user names:

Authenticated Users
SYSTEM
Administrators (WIN-BMCH3JBIUG0\Administrators)
Users (WIN-BMCH3JBIUG0\Users)

To change permissions, click Edit.

Permissions for Authenticated Users	Allow	Deny
Full control		
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced.

Applying NTFS permissions to Files and Folders

Setting access controls to files and folders can specify which users and user groups can have the access permissions. NTFS files and folder permissions allow users to access files stored on the local computer and also access files stored in a shared folder over the network. NTFS also allow sharing permissions on shared folders in accordance with file and folder permissions.

- **NTFS permissions for file**:
  - Full Control: Specifies whether a user has all permissions to files. Users having full control have a complete access right to any file even if he/she is denied permission.
  - Modify: This allows the user to read, write, execute and traverse.
  - Read and Execute – Allows the users to go through each directory, read all files.
  - Read: This allows the users to list folders, read files, read attributes and read permissions.
  - Write: Allows users to create files, write data, create folders and set attributes.
- **NTFS permissions for the folder**:
  - Full Control: Specifies whether the user has complete access to folders.
  - Modify: This allows the user to read, write, execute and traverse.

- Read & Execute: This allows the users to list folders, read files, read attributes and read permissions.
- List Folder Contents: Specifies if the user can access the folders and sub folders included.
- Read: This allows the users to list folders, read files, read attributes and read permissions.
- Write: Allows users to create files, write data, create folders and set attributes.

List Folder contents permissions can be set only when these are inherited by folders and not files whereas, the read and execute can appear for files and folders.

It is possible to back up and restore data on NTFS files. However, with FAT files, it is not possible to set permissions to individual files and folders.

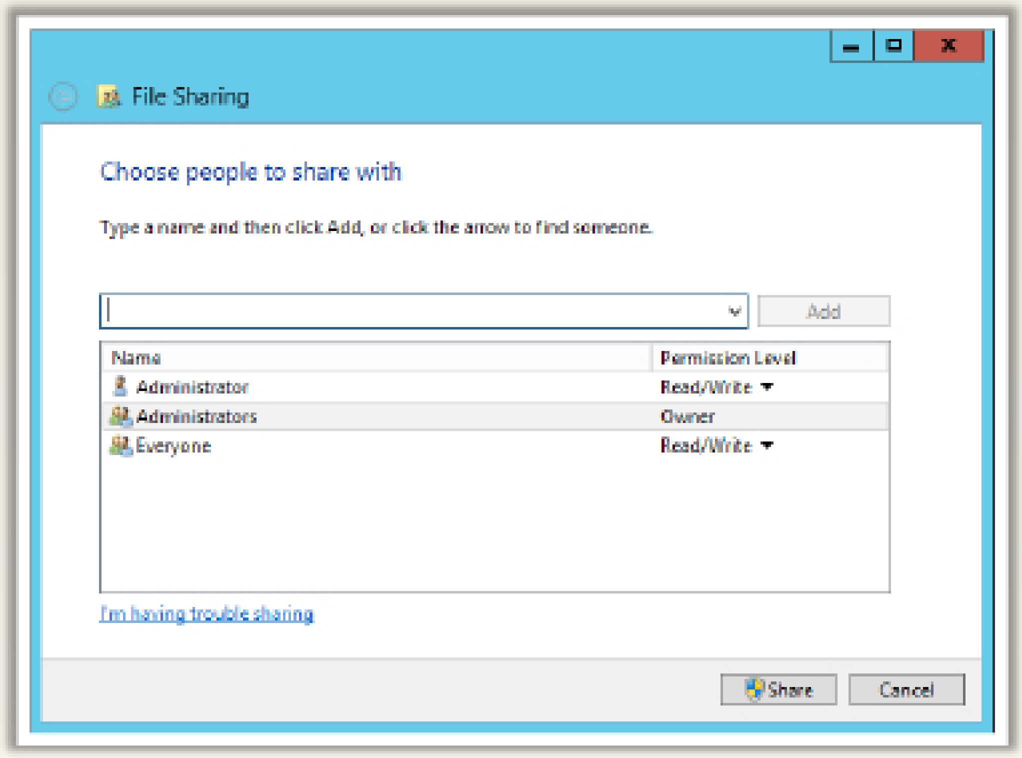
To set, view, change, or remove special permissions for files and folders, go to a specific file or folder on which you want to set special permission.

1. **Right-click** the file or folder, click **Properties**, and then click the **Security tab**
2. Click **Advanced**
3. Click **Add** to set special permissions for a new group or user in the Permission Entry Window

File System Security: Setting Access Controls and Permission to Files and Folders (Cont'd)

Applying Share Permissions

- Share permissions are applied when you need to provide access to a shared folder over the network
- With Share permission, you can restrict access to share folders
  1. Go to the specific file or folder on which you want to set Share Permissions
  2. Right-click the folder, and click Share with option
  3. Select specific user or group to whom you want to assign share permission such as Read, Read/Write



File Sharing

Choose people to share with

Type a name and then click Add, or click the arrow to find someone.

Name	Permission Level
Administrator	Read/Write ▾
Administrators	Owner
Everyone	Read/Write ▾

I'm having trouble sharing

Note: Use NTFS Permission in addition to shared permissions to provide more restriction to shared folders

Applying Share Permissions to Folders

The Shared folders can be accessed over the network. Only users with access permission to any particular folder have the rights to access folders over the network.

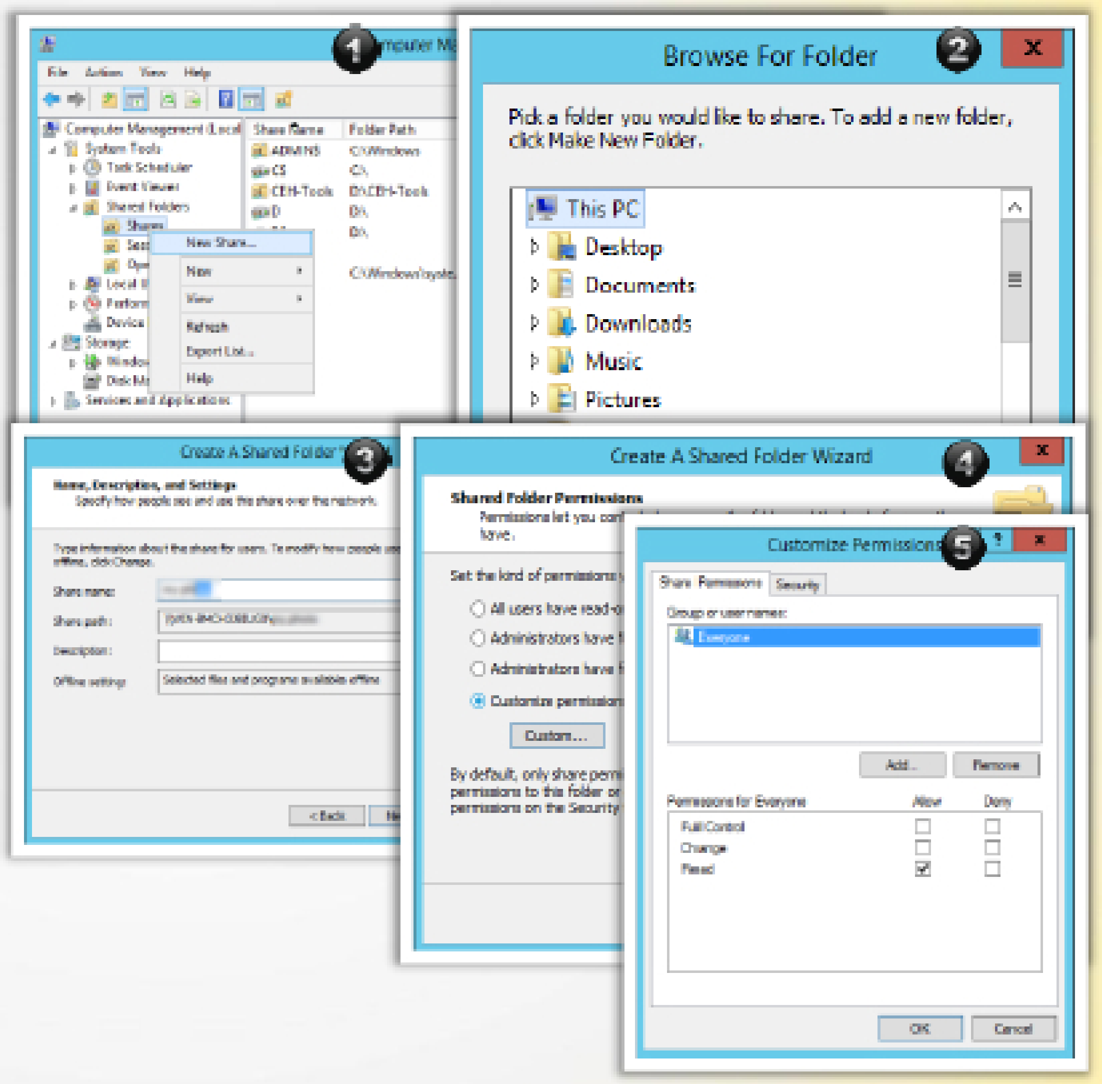
The shared folders can contain personal information, application, etc. Hence, configuring shared permission depends on the type of data contained in a particular folder.

- The **principals** involved in a shared folder are as follows:
  - Shared folder permissions are applicable only to folders and not individual files.
  - Shared folders do not ask for access permission to users accessing the folder from the system where the folder is stored. The access permission is asked for those users who access the folder over the internet.

Creating and Securing a Windows File Share

Creating New File Share

- Go to Computer Management
  1. Click System Tools, right-click Shares and click New Share
  2. Browse the folder that you to share
  3. Enter the [Share Name]
  4. Select Customize permissions and click Custom to customize the Share Folder Permissions
  5. Add the correct Active Directory User(s) &/or Group(s)
     - The Share Permissions only allow Users and/or Group of users to access to a specific shared Folder
     - The User(s) and/or Group(s) must also have the appropriate NTFS Permissions to access the files



Pick a folder you would like to share. To add a new folder, click Make New Folder.

Name, Description, and Settings
Specify how people see and use this share over the network.

Type information about the share for users. To modify how people use the content while offline, click Change.

Offline setting: Selected files and programs available offline

Set the kind of permissions

○ All users have read-o

○ Administrators have f

○ Administrators have f

● Customize permission

By default, only share perm permissions to this folder or permissions on the Security

Permissions for Everyone	Allow	Deny
Full Control	□	□
Change	□	□
Read	☑	□

The windows environment puts forward the concept of shared folders that allow all the users to access the resources contained in that particular shared folder. Shared folder enables every user to view and access the contents of the folder without any restriction. However, the organization needs to employ certain restrictions or permissions that can protect the contents in the shared folder.

A shared folder can contain applications, personal data or any other data. The permissions set on the data depend on the type of content included in the shared folder. Certain features of a shared folder are:

- The shared folder permissions apply only to folders and not files.
- The shared permissions do not apply even to the files and folders contained in the shared folder.
- The permission to access the folder applies to all users who gain access to connect to the folder.
- Resources using FAT use shared folder permissions for protection.
- Permission applied to a group includes permission for each and every user in that particular group.

There are certain **best practices** followed while providing shared folder permissions:

- Assign folder permission to group accounts and not user accounts: Assigning permission to group accounts is much easier than applying to user accounts. A user in a user account can be a part of different shared folders. And, each folder can have different share folder permissions. This leads to a combination of user and group folder permissions. Whereas in the case of group permissions, it is just a matter of addition or removal of users from the group and no need to reassign the permission to the users.
- Assign certain restrictions on the permissions applied to the users in such way that the users can still perform their task.
- Consolidate all the application and other resources in one location.
- Do not explicitly deny permission to a shared resource: if there are any denied shared folder permissions to a user, then that user cannot have that permission, even if they are allowed permission to another group.
- Set NTFS file system permissions for users logging locally: Shared folder permissions apply to those resources that are shared through the network and not locally. Also, shared folder applies to those files and folders in FAT volume.
- Ensure that the copied or moved share folder possess the shared folder permissions.

These steps will show how to create and secure a Windows file share.

1. Click on **Start** Menu and in the search box, type **"Computer Management"**
2. Click System tools → **Share Folders**
3. Right click Shares → **New Shares**
4. **Create A Shared Folder Wizard** will launch → **Next**
5. In "**Folder path**" textbox, enter the path of the folder to be shared → **Next**
6. In "**Share name**" enter the name of the folder to be shared → **Next**
7. As per the requirement administrators can select the option from set the kind of permissions
8. **Finish**

Data and File System Encryption

C|ND Certified Network Defender

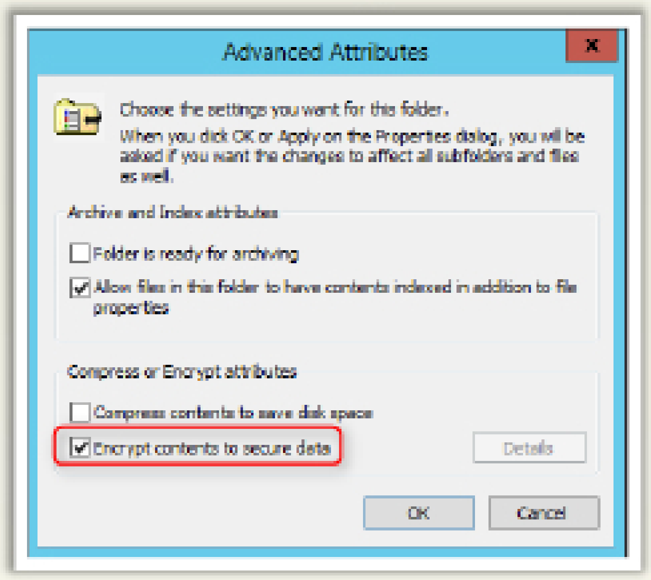
- You can use the Windows built-in or third-party **encryption utilities** to encrypt your data
- Windows Operating has a built-in encryption mechanism called **Encrypted File Systems** (EFS) and **BitLocker** to encrypt your data or volume
- EFS is part of **Microsoft Windows** file system (NTFS)
- It uses **public key encryption** technology and can be used with either workstation or server
- **EFS Limitations**
  - It works only for NTFS file system
  - Loses encryption when encrypted data copies to non-NTFS system
  - Risk of data loss

Encrypting a Folder in Windows

1. Right click on the folder that you want to encrypt and click **Properties**
2. Click **Advanced**
3. Select **Encrypt contents to secure data** check box and click **OK**
4. Click **Apply**

BitLocker

- BitLocker is a full-disk encryption solution that encrypts an **entire volume**
- Install and use BitLocker to perform **full- disk encryption**



Advanced Attributes

Choose the settings you want for this folder.

When you click OK or Apply on the Properties dialog, you will be asked if you want the changes to affect all subfolders and files as well.

Archive and Index attributes

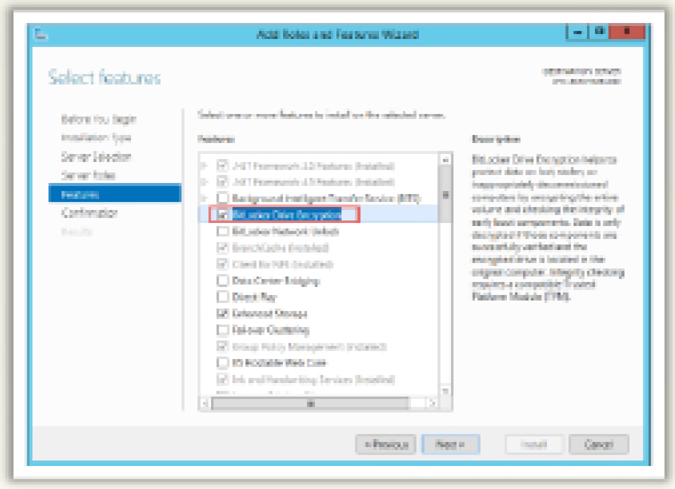
□ Folder is ready for archiving

☑ Allow files in this folder to have contents indexed in addition to file properties

Compress or Encrypt attributes

□ Compress contents to save disk space

☑ Encrypt contents to secure data



Add Roles and Features Wizard

Select features

☑ .NET Framework 3.5 Features (Installed)
☑ .NET Framework 4.5 Features (Installed)
□ Background Intelligent Transfer Service (BITS)
☑ BitLocker Drive Encryption
□ BitLocker Network Unlock
☑ BranchCache (Installed)
☑ Client for NFS (Installed)
□ Data Center Bridging
□ Direct Play
☑ Enhanced Storage
□ Failover Clustering
☑ Group Policy Management (Installed)
□ IIS Hostable Web Core
☑ Ink and Handwriting Services (Installed)

BitLocker Drive Encryption helps to protect data on lost, stolen, or inappropriately decommissioned computers by encrypting the entire volume and checking the integrity of early boot components. Data is only decrypted if those components are successfully verified and the encrypted drive is located in the original computer. Integrity checking requires a compatible Trusted Platform Module (TPM).

Note: Always use full-disk encryption instead of encrypting specific files or folders

Data encryption is used to prevent intercepting and altering or misusing. The Windows operating system provides a built-in encryption mechanism such as EFS and Bit locker to encrypt specific file, folder or entire drive.

EFS (Encryption File System)

EFS (Encryption File System) is a built-in mechanism in Windows operating system. EFS uses the standard DESX algorithm that depends on a 128-bit encryption key.

- **EFS Features:**
  - Enabling encryption is an easy task.
  - Helps in deciding the users that can access files and folders.
  - Enables easy opening and closing of encrypted files.
  - Easy to disable the encryption applied to a folder.
- **EFS Limitations:**
  - It works only for NTFS file system.
  - Lose encryptions when encrypted data copies to non-NTFS system.
  - Risk of data loss.

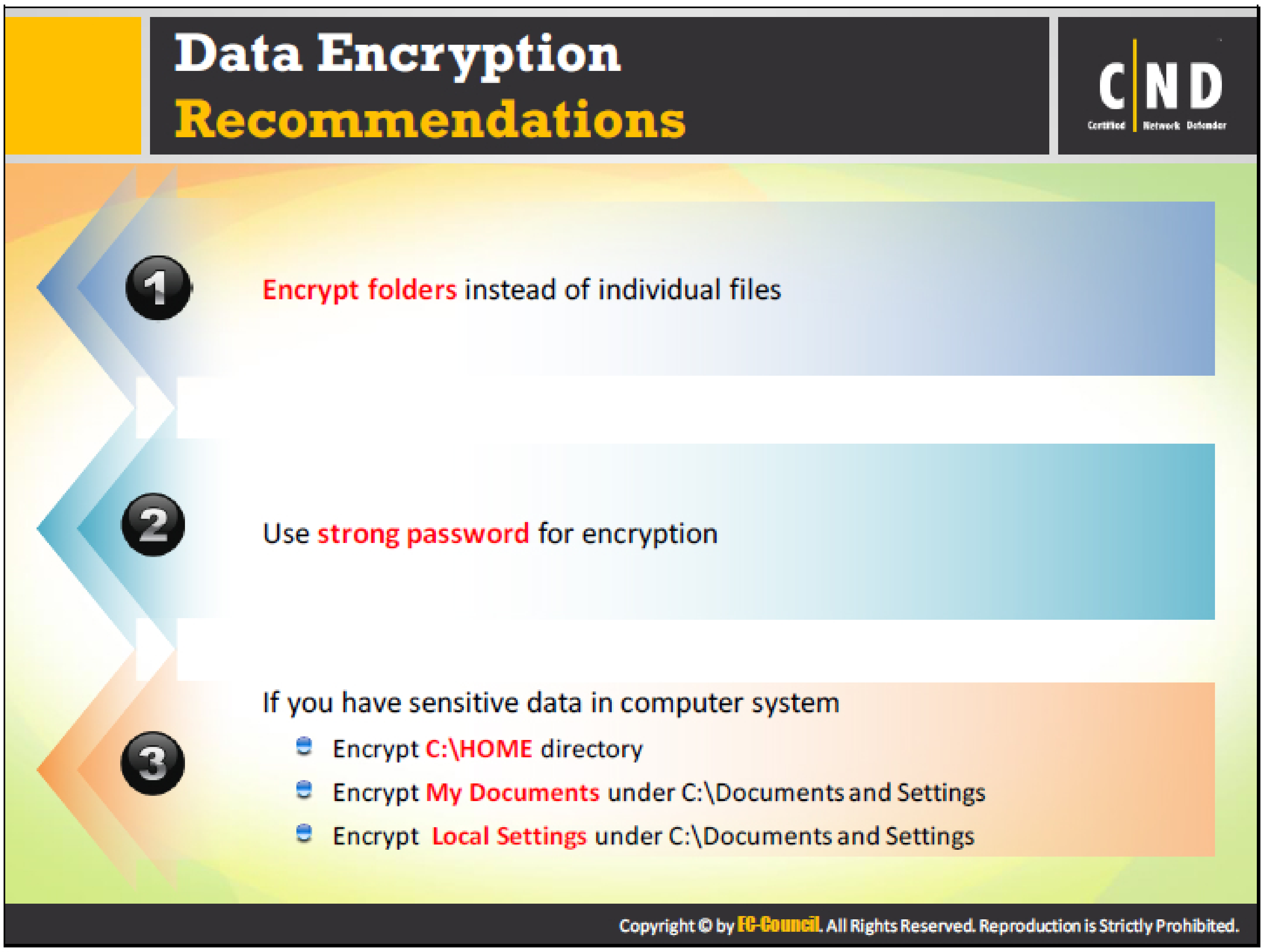
BitLocker

BitLocker extends the level of protection to the disk level. All the sensitive and important documents on the drive can be easily protected using the BitLocker. It prevents the attackers from achieving the system password or documents even after removing the hard drive and placing it on another PC. The main feature of the BitLocker is that it encrypts any new file added to the drive. But, copying files to another drive or PC keeps the files in the decrypted form. The BitLocker finds its application in encrypting:

- The operating system drive
- The internal hard drives
- The external hard drives

The BitLocker checks for any security changes during the system start-up. If it finds any kind of change in the BIOS, it locks the operating system and prevents it from performing further actions. The BitLocker use TPM (Trusted Platform Module), a microchip built into the computer that helps in storing the encryption keys. The TPM assists the BitLocker to keep the system away from attacks and theft.

- **Benefits of Bitlocker:**
  - Provide protection by encrypting the hard disk. Thus providing protection to the information stored in a physically damaged and irreversible hard drive.
  - As BitLocker offers boot time inspection, it prevents the chances of any unauthorized changes.
  - It helps protect data even in the case of a system theft as the attacker cannot access the encrypted files.
  - Provide better protection for files and other sensitive documents at an offline. While being online, the user needs to configure NTFS permission or use EFS.



Data Encryption Recommendations

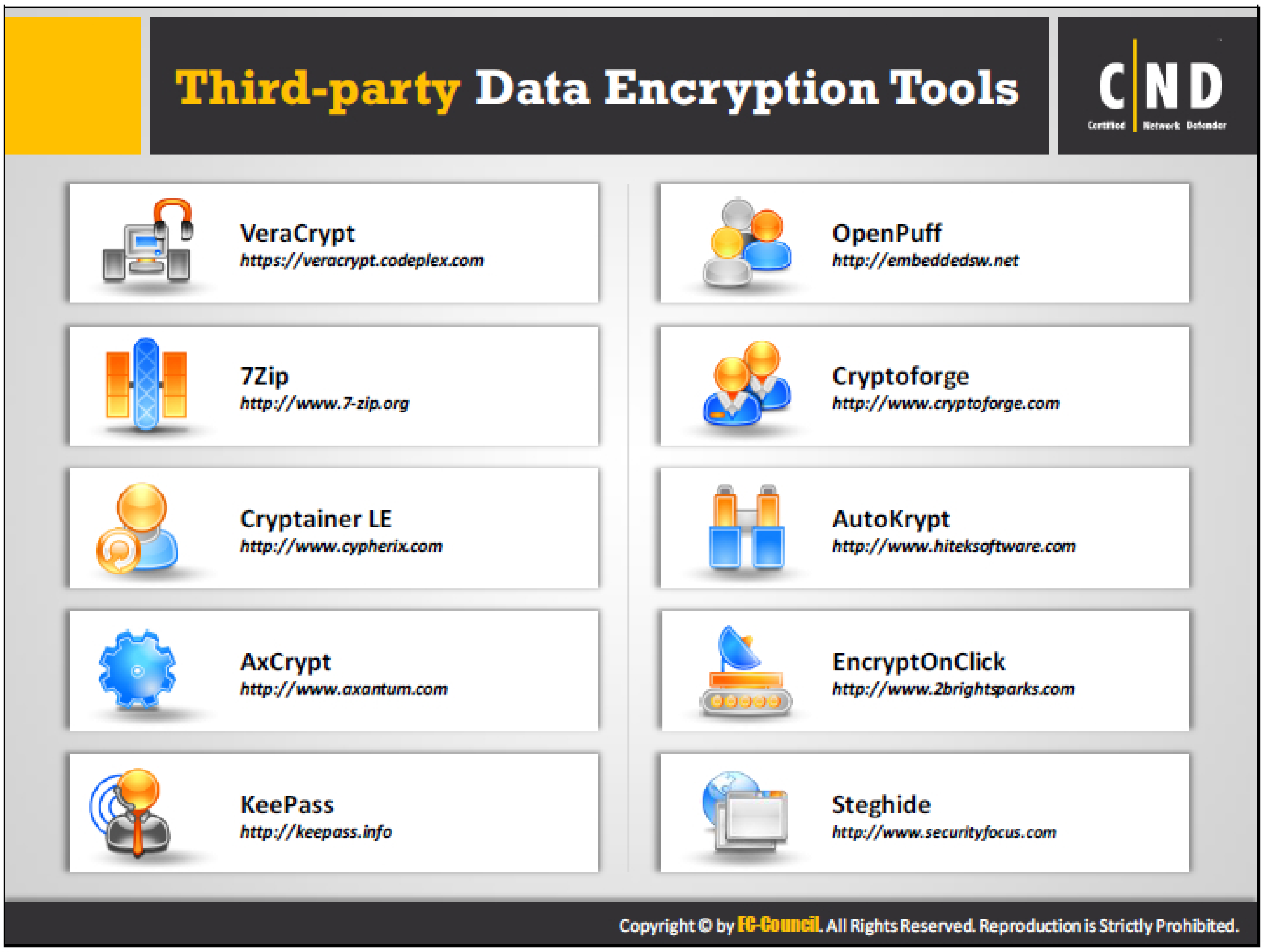
1. Encrypt folders instead of individual files

2. Use strong password for encryption

3. If you have sensitive data in computer system
   - Encrypt C:\HOME directory
   - Encrypt My Documents under C:\Documents and Settings
   - Encrypt Local Settings under C:\Documents and Settings

The organization should consider encrypting important and sensitive data related to Business information or "secrets"/intellectual property. It may include messages, financial reports, legal docs, patents, product releases, research and development data, etc. Data is protected from prying eyes even if the computer gets stolen.

- You should consider encrypting sensitive information stored in following locations:
  - Encrypt **C:\HOME** directory.
  - Encrypt **My Documents** under C:\Documents and Settings.
  - Encrypt **Local Settings** under C:\Documents and Settings.
- **Data Encryption Recommendations:**
  - Prefer Full disk encryption on drive to protect all your data.
  - Encrypt folder instead of individual files.
  - Encrypt folder that contains sensitive information.
  - Use strong password for encryption.
  - Use third party encryption tools to encrypt your sensitive data, if required.



Third-party Data Encryption Tools

VeraCrypt
https://veracrypt.codeplex.com

7Zip
http://www.7-zip.org

Cryptainer LE
http://www.cypherix.com

AxCrypt
http://www.axantum.com

KeePass
http://keepass.info

OpenPuff
http://embeddedsw.net

Cryptoforge
http://www.cryptoforge.com

AutoKrypt
http://www.hiteksoftware.com

EncryptOnClick
http://www.2brightsparks.com

Steghide
http://www.securityfocus.com

VeraCrypt

Source: https://veracrypt.codeplex.com

VeraCrypt is used for on-the-fly encryption (OTFE). It can create a virtual encrypted disk within a file or encrypt a partition.

7Zip

Source: http://www.7-zip.org

7-Zip is open source software which performs encryption with high compression.

Cryptainer LE

Source: http://www.cypherix.com

Cryptainer LE can encrypt every kind of file format, whether it is textual, tabular, graphical, organized in a database, audio or video. It also allows users to password protect files and folders on CD ROMs, DVD's etc.

AxCrypt

Source: http://www.axantum.com

AxCrypt integrates seamlessly with Windows to compress, encrypt, decrypt, store, send and work with individual files. Password Protect any number of files using strong encryption.

KeePass

Source: *http://keepass.info*

KeePass supports the Advanced Encryption Standard (AES, Rijndael) and the Twofish algorithm to encrypt its password databases.

Steghide

Source: *http://www.securityfocus.com*

Steghide is a steganography program, which hides bits of a data file in some of the least significant bits of another file in such a way that the existence of the data file is not visible and cannot be proven.

OpenPuff

Source: *http://embeddedsw.net*

OpenPuff securely encrypts and hides files inside of other files. It supports many file formats like Images (BMP, JPG, PCX, PNG, TGA), Audio support (AIFF, MP3, NEXT/SUN, WAV), Video support (3GP, MP4, MPG, VOB), Flash-Adobe support (FLV, SWF, PDF).

Cryptoforge

Source: *http://www.cryptoforge.com*

CryptoForge is file encryption software for personal and professional data security. It allows protecting the privacy of sensitive files, folders, or emailing messages. After encrypting the information, one can store it on insecure media or transmit it on an insecure network—like the Internet—and still keep it secret. Later, it decrypts the information into its original form. Internet- and still remain secret. Later, the information can be decrypted into its original form.

AutoKrypt

Source: *http://www.hiteksoftware.com*

AutoKrypt is data encryption software designed for automation. It automatically encrypts or decrypts files and folders on a schedule.

EncryptOnClick

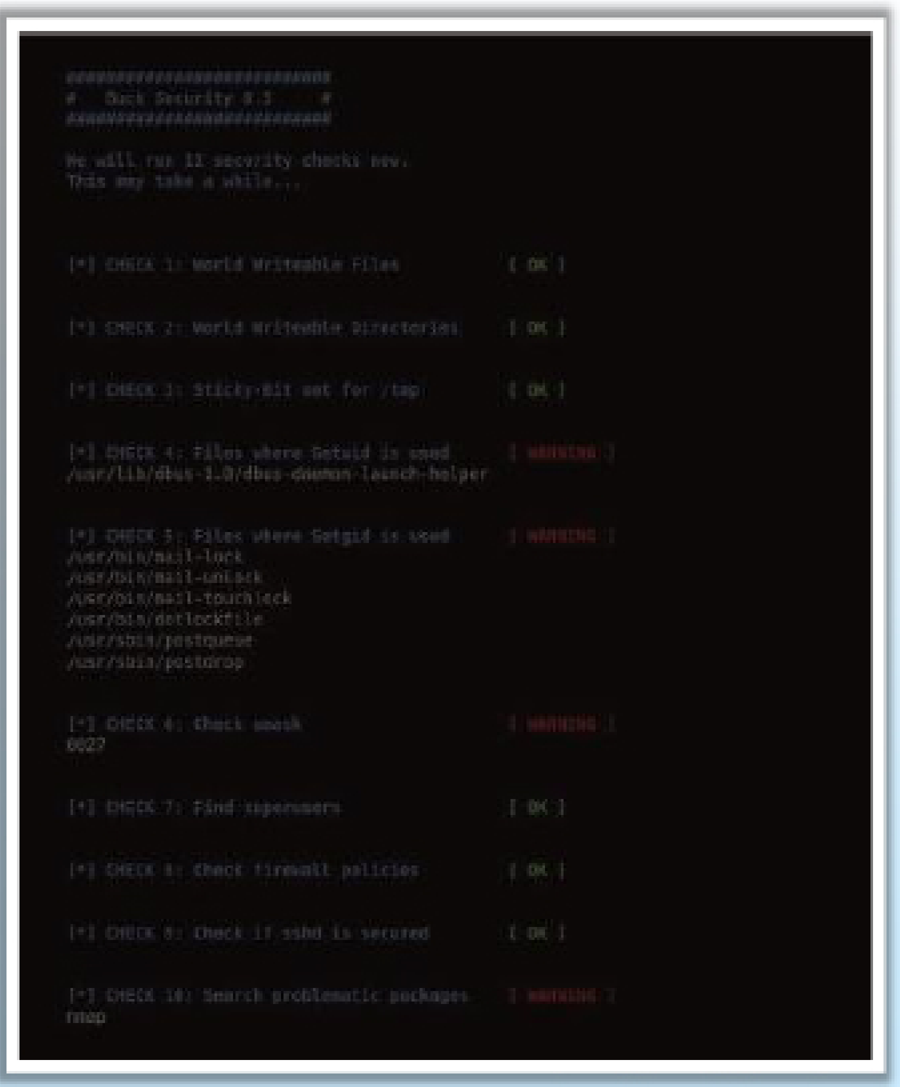
Source: *http://www.2brightsparks.com*

EncryptOnClick helps to encrypt and protect sensitive files.

- **Features:**
  - Secure encryption and decryption method is used (256-bit AES encryption).
  - Files are both compressed & encrypted, which results in a smaller file.
  - Password protected.
  - Encrypt single files or all files in a folder.
  - Unicode enabled so filenames in any language can be encrypted.
  - Encrypt, decrypt, compress, and un-compress files, which can also be opened and decrypted using third party programs like WinZip 9 (provided the correct password is used).

Linux Baseline Security Checker: buck-security

- buck-security allows you to get a quick overview of the security status of your system
- It conducts a security check against the baseline
  - Searching for worldwriteable files
  - Searching for worldwriteable directories
  - Searching for programs where the setuid is set
  - Searching for programs where the setgid is set
  - Checking your umask
  - Checking if the sticky-bit is set for /tmp
  - Searching for superusers
  - Checking firewall policies
  - Checking if sshd is secured
  - Searching for listening services
  - Creating and checking checksums of system programs
  - Searching for installed attack tool packages



```
##############################
#   Buck Security 0.1        #
##############################

We will run 11 security checks now.
This may take a while...


[*] CHECK 1: World Writeable Files          [ OK ]


[*] CHECK 2: World Writeable Directories    [ OK ]


[*] CHECK 3: Sticky-Bit set for /tmp        [ OK ]


[*] CHECK 4: Files where Setuid is used     [ WARNING ]
/usr/lib/dbus-1.0/dbus-daemon-launch-helper


[*] CHECK 5: Files where Setgid is used     [ WARNING ]
/usr/bin/mail-lock
/usr/bin/mail-unlock
/usr/bin/mail-touchlock
/usr/bin/dotlockfile
/usr/sbin/postqueue
/usr/sbin/postdrop


[*] CHECK 6: Check umask                    [ WARNING ]
0022


[*] CHECK 7: Find superusers                [ OK ]


[*] CHECK 8: Check firewall policies        [ OK ]


[*] CHECK 9: Check if sshd is secured       [ OK ]


[*] CHECK 10: Search problematic packages   [ WARNING ]
nmap
```

http://www.buck-security.net

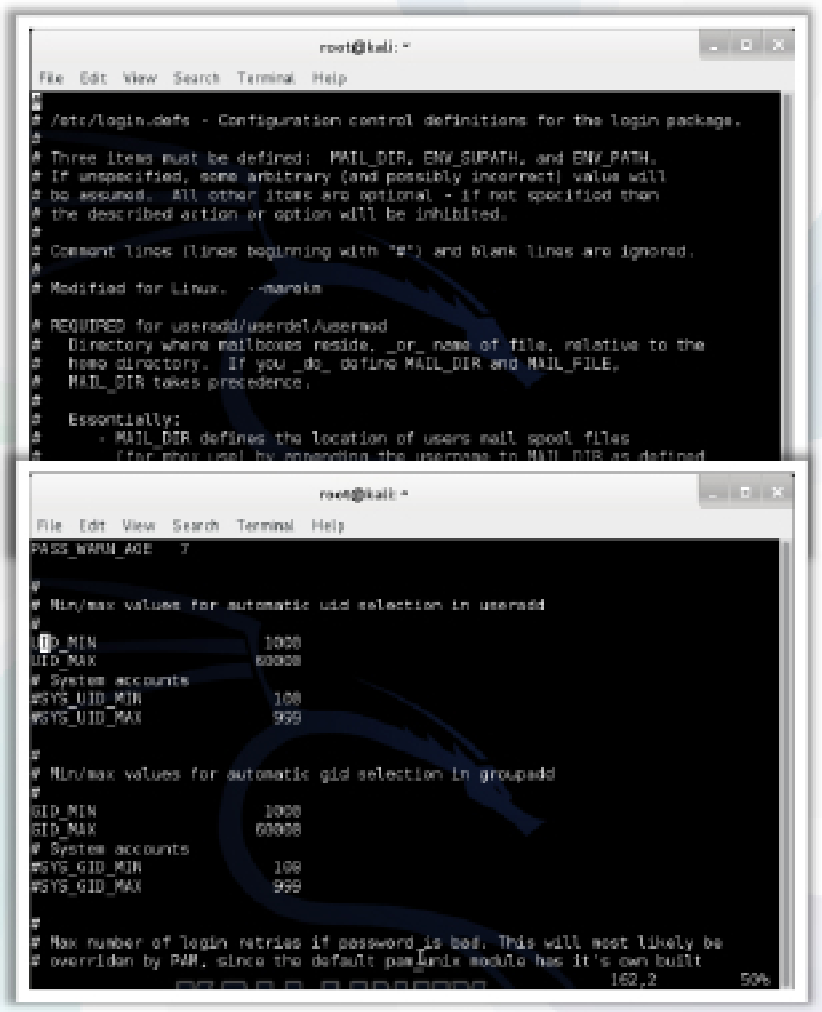
buck-security is a security scanner for Debian and Ubuntu Linux. It runs a couple of important checks and helps you harden your Linux system. This enables you to quickly overview the security status of your Linux system. As a system administrator, you often get into situations where you have to take care of a server that has been maintained by other people. In this situation, it is useful to get an idea of the security status of the system immediately. Buck Security was designed exactly for this. It runs a few important checks and returns the results. It was designed to be extremely easy to install, use and configure.

Source: http://www.buck-security.net

Password Management

- Use strong "root" passwords according to the organization's policy
- The default system password policy should match your organization's password policy
- Go to the /etc/login.defs file to view and change the default password policy settings per the organization's password policy
- Use following command to view and change the default password policy settings

```
# sudo vi /etc/logins.defs
```



```
#
# /etc/login.defs - Configuration control definitions for the login package.
#
# Three items must be defined:  MAIL_DIR, ENV_SUPATH, and ENV_PATH.
# If unspecified, some arbitrary (and possibly incorrect) value will
# be assumed.  All other items are optional - if not specified then
# the described action or option will be inhibited.
#
# Comment lines (lines beginning with "#") and blank lines are ignored.
#
# Modified for Linux.  --marekm

# REQUIRED for useradd/userdel/usermod
#   Directory where mailboxes reside, _or_ name of file, relative to the
#   home directory.  If you _do_ define MAIL_DIR and MAIL_FILE,
#   MAIL_DIR takes precedence.
#
#   Essentially:
#      - MAIL_DIR defines the location of users mail spool files
#        (for mbox use) by appending the username to MAIL_DIR as defined
```

```
PASS_WARN_AGE   7

#
# Min/max values for automatic uid selection in useradd
#
UID_MIN                  1000
UID_MAX                 60000
# System accounts
#SYS_UID_MIN              100
#SYS_UID_MAX              999

#
# Min/max values for automatic gid selection in groupadd
#
GID_MIN                  1000
GID_MAX                 60000
# System accounts
#SYS_GID_MIN              100
#SYS_GID_MAX              999

#
# Max number of login retries if password is bad. This will most likely be
# overriden by PAM, since the default pam_unix module has it's own built
                                                             162,2         50%
```

The /etc/login.defs file defines the site-specific configuration for password management in Linux. The users in an organization need to ensure that the default password policy matches the organization's password policy.

The "root" account is the most privileged account in Linux. The root account gives access to administrators to add accounts, change user passwords, audit and monitor log files etc. The root account does not have any security features imposed on it. Administrators can easily perform their tasks with a root account.

If an administrator wants to change the password on behalf of a user, they have to log in to the "root" account.

The user and group accounts can change their own passwords using the commands below:

- An individual user can change their password using the command: **`$ passwd`**. This prompts the user to change the password by asking for the current and the new password.
- An administrator can change the password for an individual user from his end using the command: **`# passwd user name`**. This prompts the admin to provide the new password.
- The administrator can change the password of any group accounts by the command: **`# passwd -g group name`**.

Change password for a user account

- `$ passwd`

Output

- Changing the password
- (current) UNIX password:
- Enter new UNIX password:
- Retype new UNIX password:
- passwd: password updated successfully

Change Group Password

When the -g option is used, the password for the named group is changed.

```
#passwd -g marketing
```

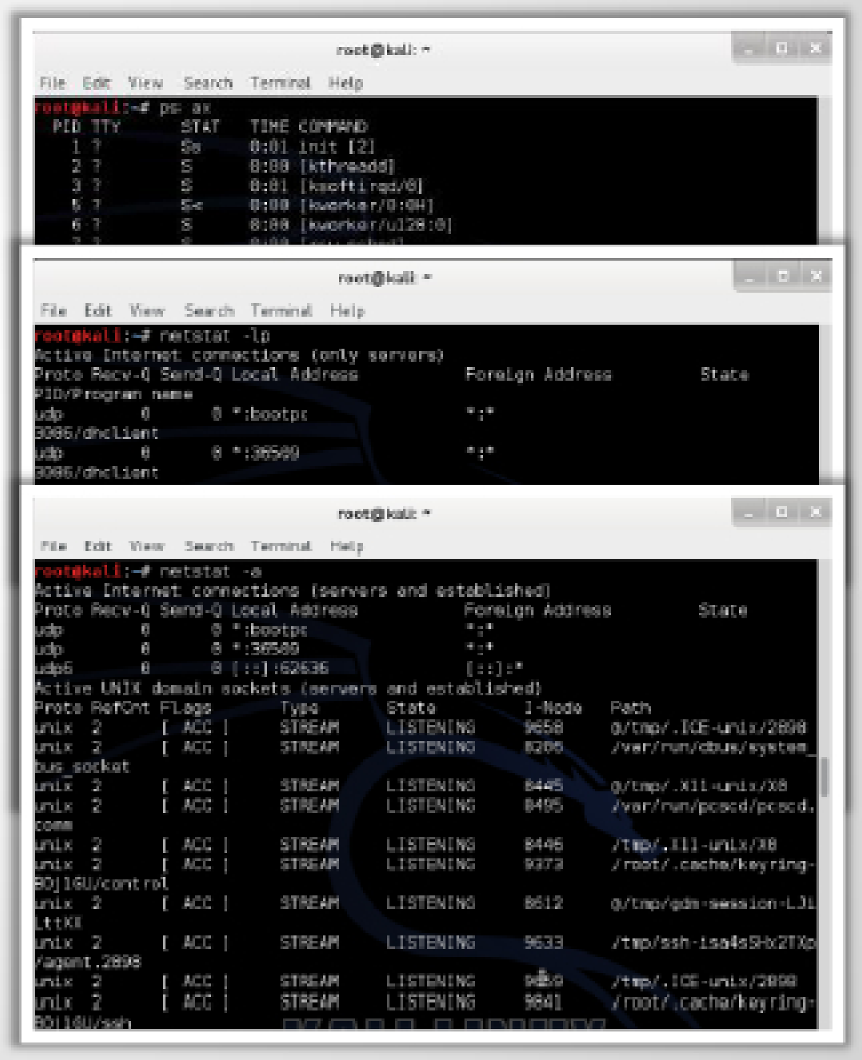
Using the above command will change the password of the users in the Marketing group.

With the help of /etc/login.defs, you can set common best practices for password management in Linux such as:

- Use strong 'root' passwords
- Avoid using old passwords
- Always set a minimum password length
- Provide complex passwords
- Set an expiration period

Disabling Unnecessary Services

- Know what type of services is running on your system
  - `#ps ax`
- Know the processes that are accepting connections and a list of open ports
  - `# netstat –lp`
  - `# netstat –a`
- Use the following commands to disable unwanted services on Red Hat, Fedora, and Red Hat based Linux distributions
  - `# chkconfig [service name]off`
  - `# chkconfig [service name] –del`
  - `# service [service name] stop`
- Use the following commands to disable unwanted services on Debian, Ubuntu, and other Debian based Linux distributions
  - `# update-rc.d -f [service name] remove`


root@kali: ~
File Edit View Search Terminal Help

```
root@kali:~# ps ax
  PID TTY      STAT   TIME COMMAND
    1 ?        Ss     0:01 init [2]
    2 ?        S      0:00 [kthreadd]
    3 ?        S      0:01 [ksoftirqd/0]
    5 ?        S<     0:00 [kworker/0:0H]
    6 ?        S      0:00 [kworker/u128:0]
```

root@kali: ~
File Edit View Search Terminal Help

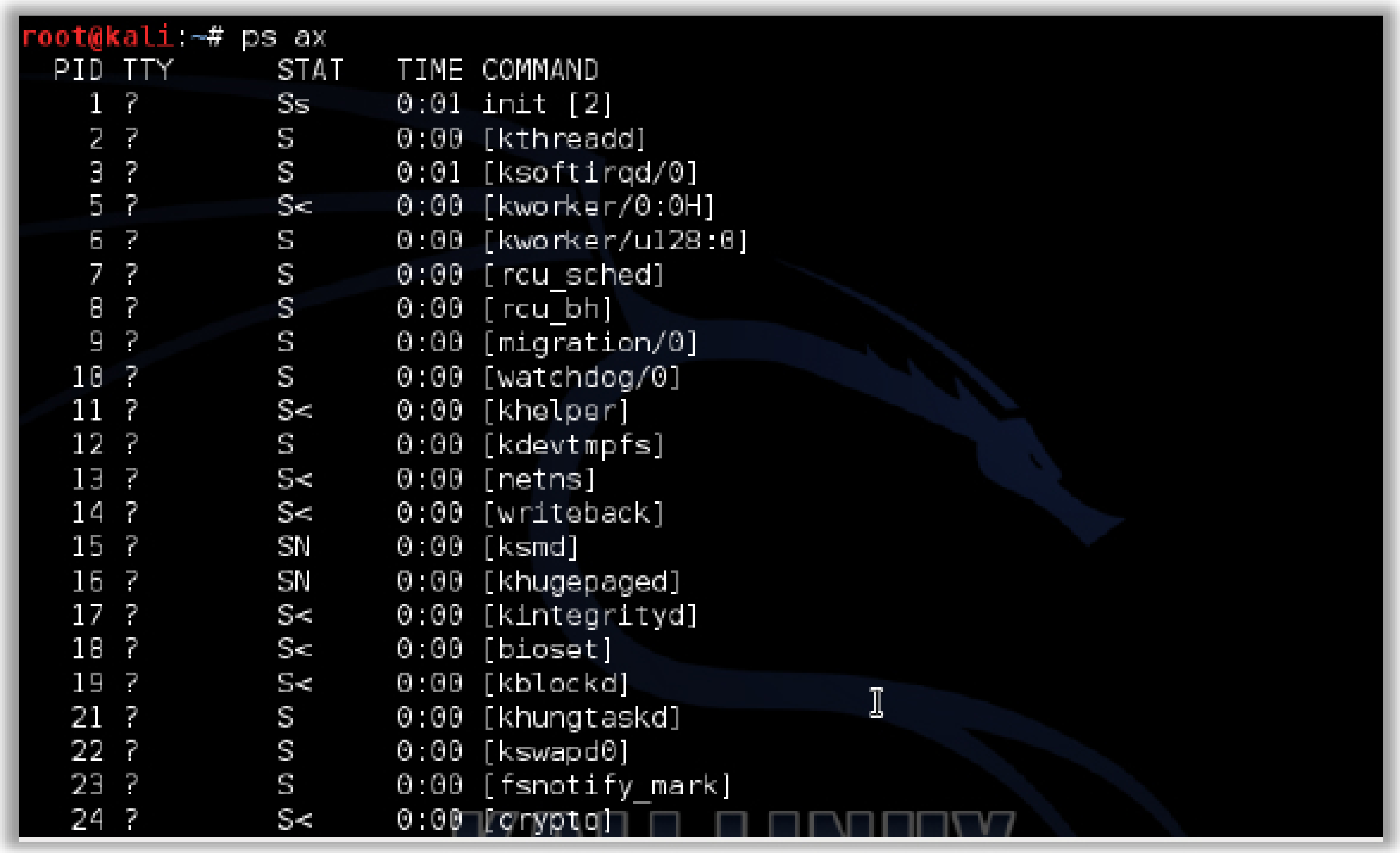
```
root@kali:~# netstat -lp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
udp        0      0 *:bootpc                *:*
3086/dhclient
udp        0      0 *:36580                 *:*
3086/dhclient
```

root@kali: ~
File Edit View Search Terminal Help

```
root@kali:~# netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 *:bootpc                *:*
udp        0      0 *:36580                 *:*
udp6       0      0 [::]:62636              [::]:*
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     9658     @/tmp/.ICE-unix/2898
unix  2      [ ACC ]     STREAM     LISTENING     8286     /var/run/dbus/system_
bus_socket
unix  2      [ ACC ]     STREAM     LISTENING     8445     @/tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     8495     /var/run/pcscd/pcscd.
comm
unix  2      [ ACC ]     STREAM     LISTENING     8446     /tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     9373     /root/.cache/keyring-
8OJ16U/control
unix  2      [ ACC ]     STREAM     LISTENING     8612     @/tmp/gdm-session-LJi
LttKX
unix  2      [ ACC ]     STREAM     LISTENING     9633     /tmp/ssh-isa4sSHx2TXp
/agent.2898
unix  2      [ ACC ]     STREAM     LISTENING     9659     /tmp/.ICE-unix/2898
unix  2      [ ACC ]     STREAM     LISTENING     9841     /root/.cache/keyring-
8OJ16U/ssh
```

The user needs to be completely sure about the services running on their Linux system and they should be based on the organizational policy. Normally, installing an operating system installs many services and packages automatically. These packages will automatically be installed without the user’s knowledge. The installation of many unnecessary services create security threats to hosts. The unnecessary services which are not required or against the organization security policy should be disabled. Administrators should check if their Linux system is running unnecessary services and disable them periodically.

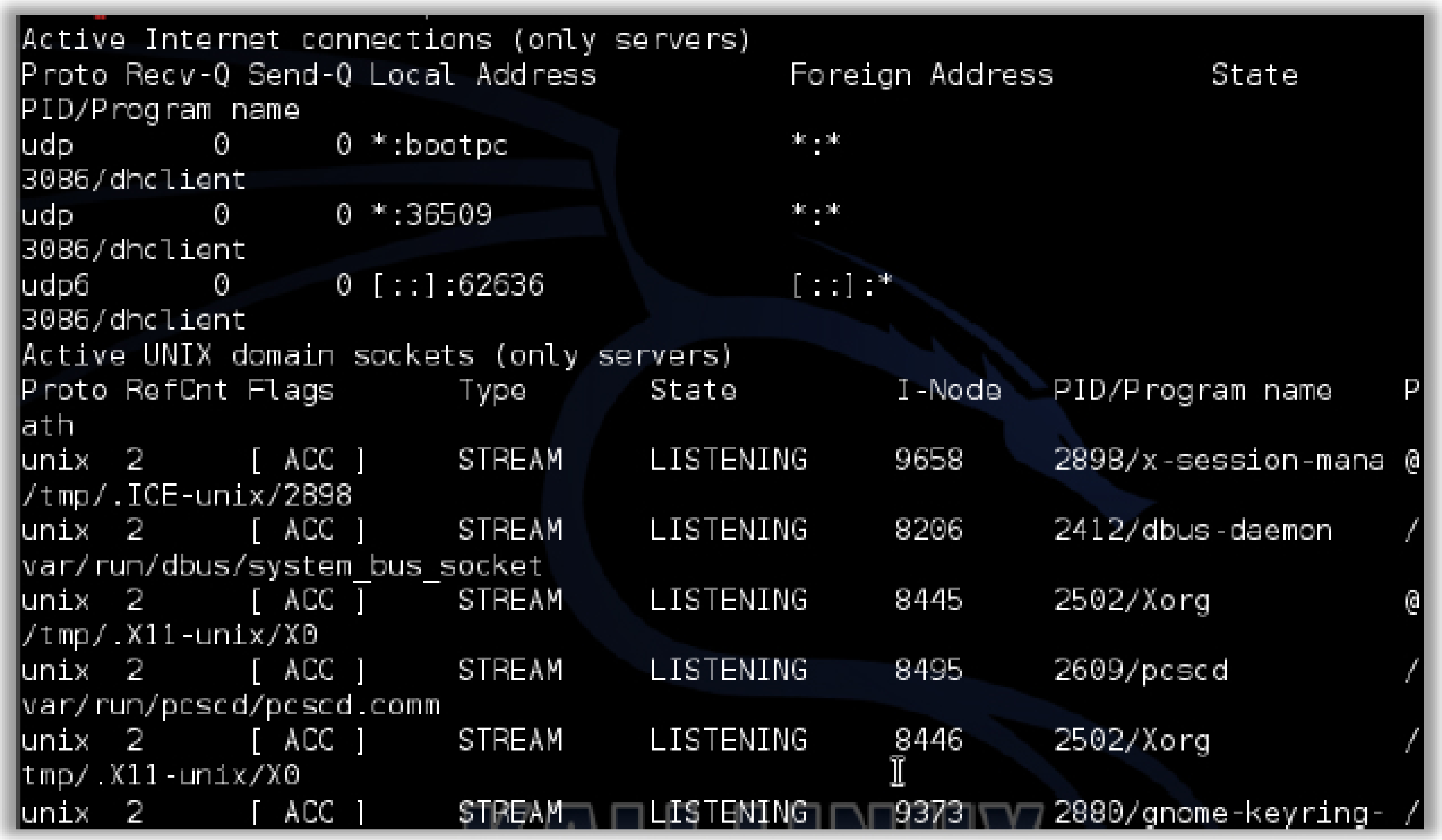
The administrator can use the command # ps ax in order to view all the services running in the particular Linux system. This command lists the active services running in the system along with their product ID (PID). They can then compare the services running on a host with an organization’s policy and disable any unwanted services.



```
root@kali:~# ps ax
  PID TTY      STAT   TIME COMMAND
    1 ?        Ss     0:01 init [2]
    2 ?        S      0:00 [kthreadd]
    3 ?        S      0:01 [ksoftirqd/0]
    5 ?        S<     0:00 [kworker/0:0H]
    6 ?        S      0:00 [kworker/u128:0]
    7 ?        S      0:00 [rcu_sched]
    8 ?        S      0:00 [rcu_bh]
    9 ?        S      0:00 [migration/0]
   10 ?        S      0:00 [watchdog/0]
   11 ?        S<     0:00 [khelper]
   12 ?        S      0:00 [kdevtmpfs]
   13 ?        S<     0:00 [netns]
   14 ?        S<     0:00 [writeback]
   15 ?        SN     0:00 [ksmd]
   16 ?        SN     0:00 [khugepaged]
   17 ?        S<     0:00 [kintegrityd]
   18 ?        S<     0:00 [bioset]
   19 ?        S<     0:00 [kblockd]
   21 ?        S      0:00 [khungtaskd]
   22 ?        S      0:00 [kswapd0]
   23 ?        S      0:00 [fsnotify_mark]
   24 ?        S<     0:00 [crypto]
```

FIGURE 6.27: `ps ax` command

Next, it is possible to find active ports using the netstat command: **`# netstat -lp`**



```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
udp        0      0 *:bootpc                *:*
3086/dhclient
udp        0      0 *:36509                 *:*
3086/dhclient
udp6       0      0 [::]:62636              [::]:*
3086/dhclient
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State         I-Node   PID/Program name    P
ath
unix  2      [ ACC ]     STREAM     LISTENING     9658     2898/x-session-mana @
/tmp/.ICE-unix/2898
unix  2      [ ACC ]     STREAM     LISTENING     8206     2412/dbus-daemon    /
var/run/dbus/system_bus_socket
unix  2      [ ACC ]     STREAM     LISTENING     8445     2502/Xorg           @
/tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     8495     2609/pcscd          /
var/run/pcscd/pcscd.comm
unix  2      [ ACC ]     STREAM     LISTENING     8446     2502/Xorg           /
tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     9373     2880/gnome-keyring- /
```

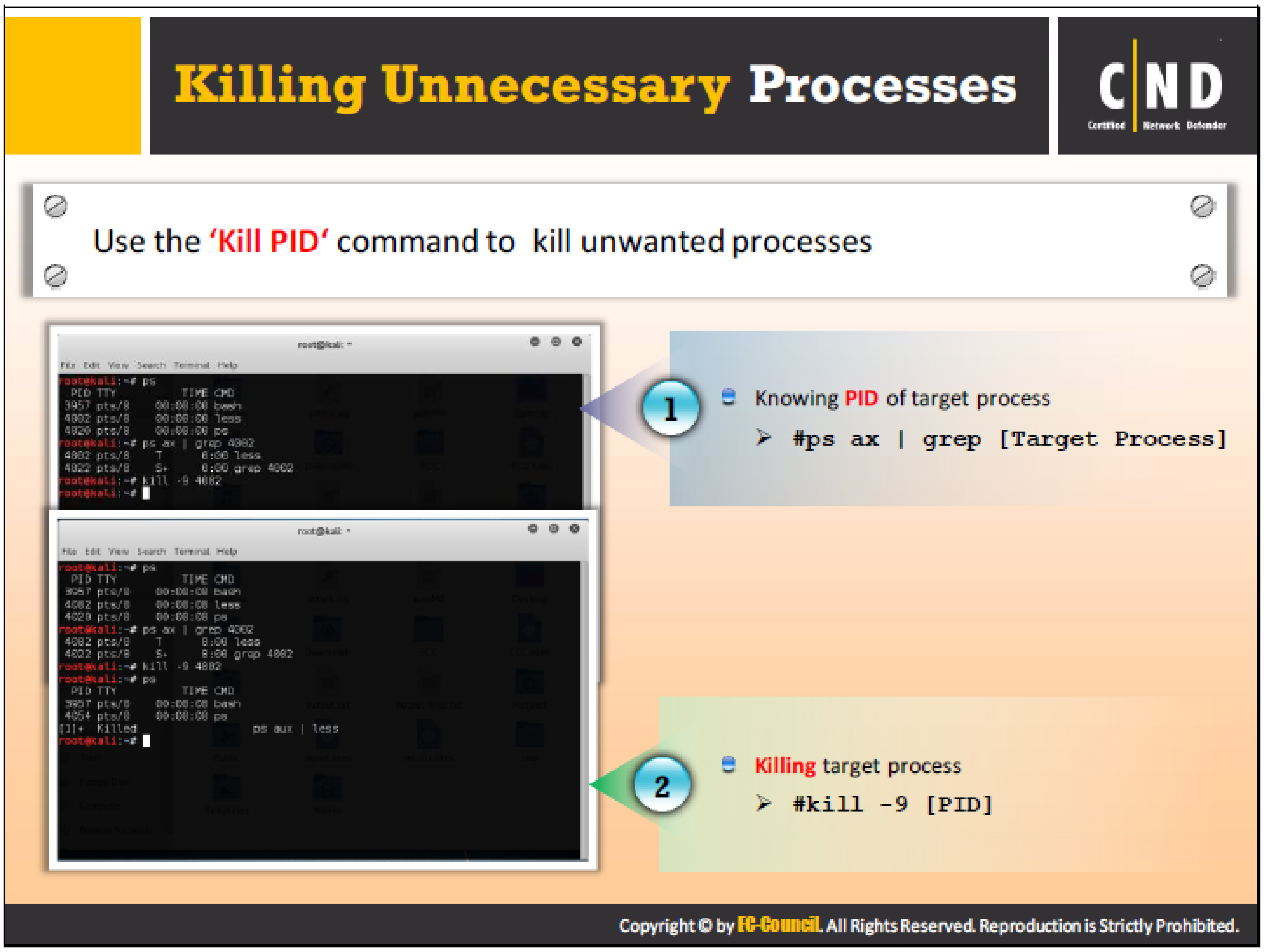
FIGURE 6.28: `netstat` command

The netstat command helps identify the unwanted services running in a system. This makes it easier for the administrator to disable those services. The command chkconfig enables and disables services in Fedora and CentOS. For example, suppose the administrator needs to disable the Apache Web server at the system startup, they can use the following command:

- **`# chkconfig httpd off`**
- **`# chkconfig httpd -del`**

In other operating systems like Ubuntu and LinuxMint the command: **`# update-rc.d -f [service name] remove`** helps to disable a service.

Disabling unwanted services in this way increases the processing speed of the operating system and does not waste system resources for these unwanted services.



Killing Unnecessary Processes

CND
Certified Network Defender

Use the **'Kill PID'** command to kill unwanted processes

root@kali: ~
File Edit View Search Terminal Help

```
root@kali:~# ps
  PID TTY          TIME CMD
 3957 pts/8    00:00:00 bash
 4002 pts/8    00:00:00 less
 4020 pts/8    00:00:00 ps
root@kali:~# ps ax | grep 4002
 4002 pts/8    T      0:00 less
 4022 pts/8    S+     0:00 grep 4002
root@kali:~# kill -9 4002
root@kali:~# 
```

root@kali: ~
File Edit View Search Terminal Help

```
root@kali:~# ps
  PID TTY          TIME CMD
 3957 pts/8    00:00:00 bash
 4002 pts/8    00:00:00 less
 4020 pts/8    00:00:00 ps
root@kali:~# ps ax | grep 4002
 4002 pts/8    T      0:00 less
 4022 pts/8    S+     0:00 grep 4002
root@kali:~# kill -9 4002
root@kali:~# ps
  PID TTY          TIME CMD
 3957 pts/8    00:00:00 bash
 4054 pts/8    00:00:00 ps
[1]+  Killed                  ps aux | less
root@kali:~# 
```

- Knowing **PID** of target process
  - `#ps ax | grep [Target Process]`

- **Killing** target process
  - `#kill -9 [PID]`

The kill command is usually used in order to terminate any services in Linux. This allows the service to run without a reboot after killing a service. There are many ways to execute the Kill command. The kill command is generally represented using:

- `# kill [signal or option] PID (s)`

It is mandatory to know the PID before running the kill command.

Type the command *# ps –A* in order to know the PID's for all the processes running in the system. After knowing the PID for a particular service, type the command for killing a service.

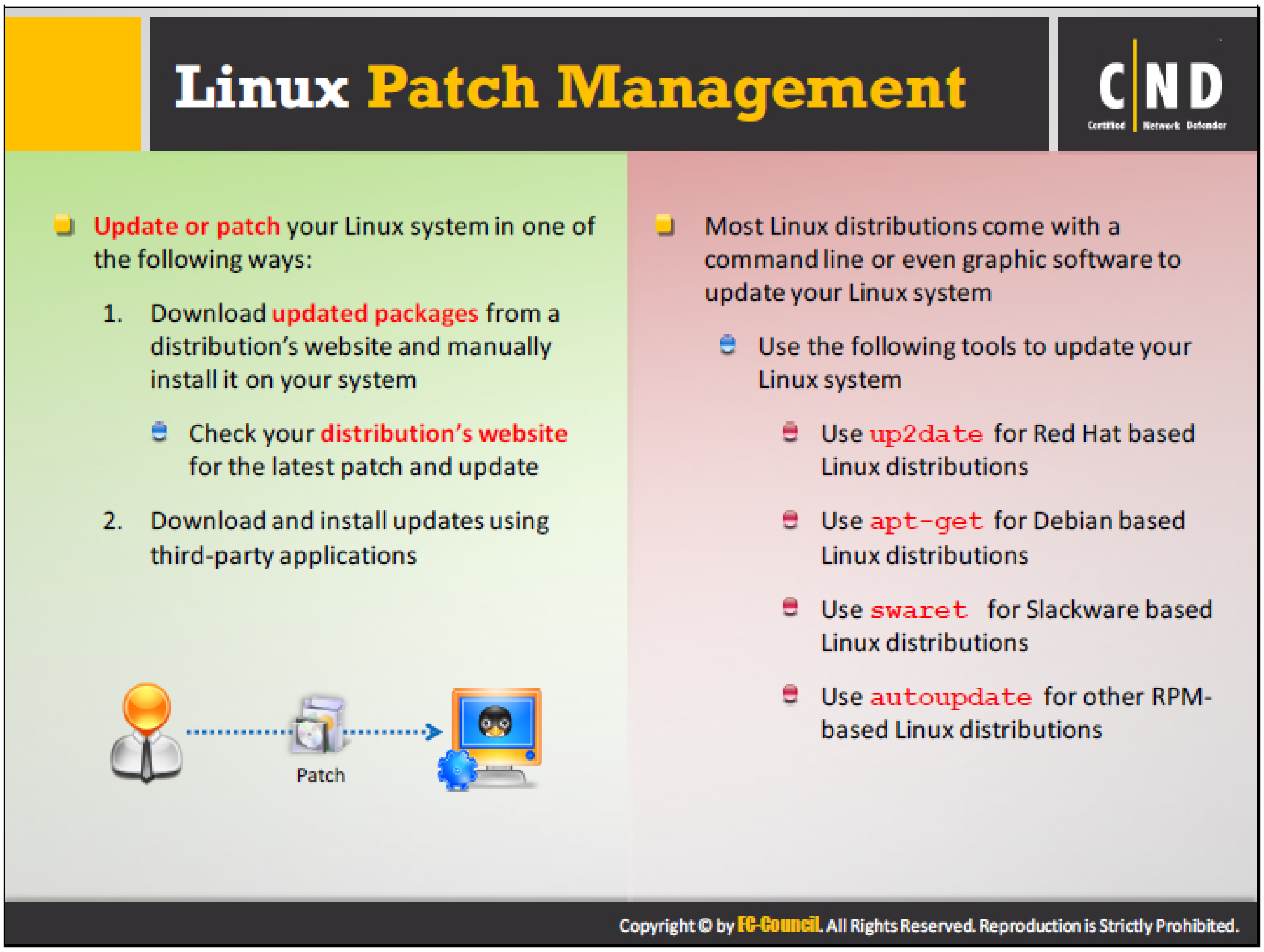
For example, in order to achieve the PID for the service cupsd, type the command:

- `#ps ax | grep cupsd`

This provides the PID for the service cupsd. Now in order to kill this service, type the command:

- `# kill -9 1511`

This will kill the cupsd service running in the system.



Linux Patch Management

- Update or patch your Linux system in one of the following ways:
  1. Download updated packages from a distribution's website and manually install it on your system
     - Check your distribution's website for the latest patch and update
  2. Download and install updates using third-party applications

- Most Linux distributions come with a command line or even graphic software to update your Linux system
  - Use the following tools to update your Linux system
    - Use `up2date` for Red Hat based Linux distributions
    - Use `apt-get` for Debian based Linux distributions
    - Use `swaret` for Slackware based Linux distributions
    - Use `autoupdate` for other RPM-based Linux distributions

In Linux, the patch updates are applied to software components of Linux such as kernel or services. The patches help you remove any existing vulnerabilities, look into security problems and include the latest features. Administrators are required to test the patches before installing on a host machine. Testing the upgraded software helps verify the upgraded software is correct.

Some Linux distributions can be configured to warn you when patches for installed software are available. Security fixes are the most important patches that resolve security issues of the systems. Once the security threat is revealed, Linux distributes its security patches in hours. An administrator should keep themselves up to date while handling security issues of Linux.

An easy way to receive all the updates is to constantly subscribe for updates from the vendors. The updates should be for kernel, inetd and for certain services.

- Linux systems can have a command line or a graphic software tool.
- Most of the updates can be located on the distribution's website.
- The admin can download and install updates using third-party applications.

The Red Hat Linux distribution provides a patch management system solution through two tools:

1. **Red Hat Network (RHN):** To get the benefits of patches available in RHN, organizations are required to purchase its license. The web resource can be configured on host machines. It provides information on the current available patches for Linux.

Users can have custom based or free services from the online resource. For routine awareness of patch releases, administrators are advised to setup a Java based program called RHN Alert Notification Tool. When a new update is released, it notifies the administrator through a change in its icon.

2. **RPM Package Manager:** The functioning of RPM is similar to RHN; however, it does not provide detailed information about every patch available. RPM provides a list of available patches through a user interface. The functioning of RPM is operated by the command rpm. When an important patch is set to necessary, RPM downloads the patch on the system.

Understanding and Checking Linux File Permissions

Type **ls -l** command to list out list of files and their permissions under home directory

Types of permissions

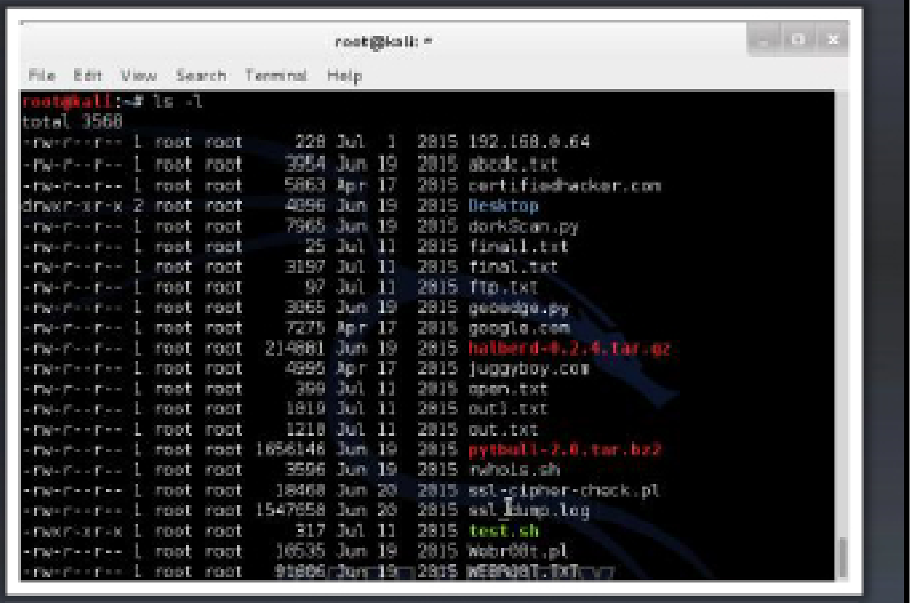
- r →denotes read permission
- w → denotes write permission
- x →denotes execute permission
- - refers to No permission.

Permission details::

- The first character in the directory list denotes file type(d, if directory)
- The next three characters denote user permissions.
- The next three characters denote group permissions.
- The final three characters denote other permissions

Permission Groups: Owner and group

- First name after number is Owner name
- Second name after number id group name



```
root@kali:~# ls -l
total 3568
-rw-r--r-- 1 root root     228 Jul  1  2015 192.168.0.64
-rw-r--r-- 1 root root    3954 Jun 19  2015 abcdc.txt
-rw-r--r-- 1 root root    5863 Apr 17  2015 certifiedhacker.com
drwxr-xr-x 2 root root    4096 Jun 19  2015 Desktop
-rw-r--r-- 1 root root    7965 Jun 19  2015 dorkScan.py
-rw-r--r-- 1 root root      25 Jul 11  2015 final1.txt
-rw-r--r-- 1 root root    3197 Jul 11  2015 final.txt
-rw-r--r-- 1 root root      97 Jul 11  2015 ftp.txt
-rw-r--r-- 1 root root    3065 Jun 19  2015 geoedge.py
-rw-r--r-- 1 root root    7275 Apr 17  2015 google.com
-rw-r--r-- 1 root root  214881 Jun 19  2015 halberd-0.2.4.tar.gz
-rw-r--r-- 1 root root    4995 Apr 17  2015 juggyboy.com
-rw-r--r-- 1 root root     399 Jul 11  2015 open.txt
-rw-r--r-- 1 root root    1819 Jul 11  2015 out1.txt
-rw-r--r-- 1 root root    1218 Jul 11  2015 out.txt
-rw-r--r-- 1 root root 1656146 Jun 19  2015 pybuilt-2.0.tar.bz2
-rw-r--r-- 1 root root    3596 Jun 19  2015 rwhois.sh
-rw-r--r-- 1 root root   18468 Jun 20  2015 ssl-cipher-check.pl
-rw-r--r-- 1 root root 1547658 Jun 20  2015 ssl_dump.log
-rwxr-xr-x 1 root root     317 Jul 11  2015 test.sh
-rw-r--r-- 1 root root   10535 Jun 19  2015 Webr00t.pl
-rw-r--r-- 1 root root   91806 Jun 19  2015 WEBR00T.TXT
```

Access control through file permissions is useful to control unauthorized access to system resources. An individual user, group of users or all who access the system can have access to certain directories and files if they have the permissions to access them.

Each file and directory has three user based permission groups:

- **Owner**: Applies only to the owner of the files or directories.
- **Group**: Applies to the group using the files and directories.
- **All users**: Applies to all the users in the system.

Permission Types

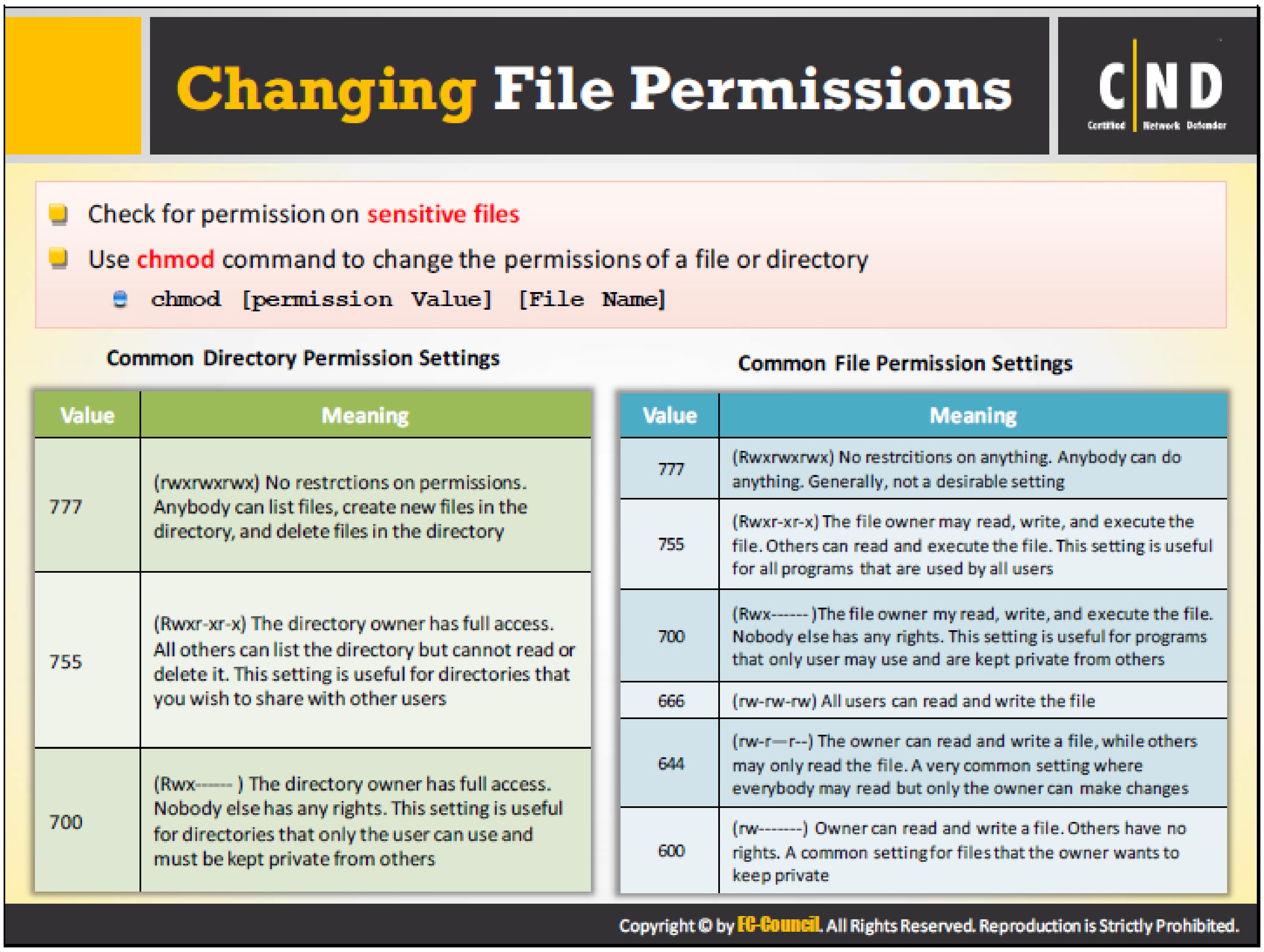
Each file or directory has three types of basic permissions:

- **Read**: Users can only read the contents of the files or directories.
- **Write**: Users can only write or modify the changes of the files or directories.
- **Execute**: Users can execute the files or directories to view its contents. The Execute permission affects a user's capability to execute a file or view the contents of a directory.

User Rights/Permissions

The permission in the command line can be written as: `_rwxrwxrwx 1 owner:group`

1. The first three characters (rwx) are for the owner permissions.
2. The next three characters (rwx) are for the Group permissions.
3. The next three characters (rwx) are for the All Users permissions.
4. The number in the command represents the hard links of the file.
5. The Owner and Group assignment formatted as Owner: Group.



Changing File Permissions

- Check for permission on sensitive files
- Use chmod command to change the permissions of a file or directory
  - `chmod [permission Value] [File Name]`

Common Directory Permission Settings

Value	Meaning
777	(rwxrwxrwx) No restrctions on permissions. Anybody can list files, create new files in the directory, and delete files in the directory
755	(Rwxr-xr-x) The directory owner has full access. All others can list the directory but cannot read or delete it. This setting is useful for directories that you wish to share with other users
700	(Rwx------) The directory owner has full access. Nobody else has any rights. This setting is useful for directories that only the user can use and must be kept private from others

Common File Permission Settings

Value	Meaning
777	(Rwxrwxrwx) No restrcitions on anything. Anybody can do anything. Generally, not a desirable setting
755	(Rwxr-xr-x) The file owner may read, write, and execute the file. Others can read and execute the file. This setting is useful for all programs that are used by all users
700	(Rwx------)The file owner my read, write, and execute the file. Nobody else has any rights. This setting is useful for programs that only user may use and are kept private from others
666	(rw-rw-rw) All users can read and write the file
644	(rw-r—r--) The owner can read and write a file, while others may only read the file. A very common setting where everybody may read but only the owner can make changes
600	(rw-------) Owner can read and write a file. Others have no rights. A common setting for files that the owner wants to keep private

Modifying the Permissions

`chmod` is a Linux command that will allow administrators to change the permissions of the file. Administrators can edit the permissions using `chmod`. Administrators can explicitly assign the permissions or can use the binary number series.

Permissions defined Explicitly

Administrators need to refer the Permission Group and Permission Types. The Permission Groups used are:

- **u**: Owner
- **g**: Group
- **o** or **a**: All Users

The operators used along with the groups are the + (plus) and – (minus). These assignment operators define if the permission has to added or deleted.
Example: A file has its permission set to `_rw_rw_rw`, which means that the owner, group and all users have read and write permission.

- If the permission has to be removed from All Users, the modification will be: **`chmod a-rw file1`**
- If the same group permission has to be added, the command will be:

  `chmod a+rw file1`

Permissions defined through Binary Numbers

A sample permission string would be **chmod 640 file1**, which means that the owner has read and write permissions, the group has read permissions, and all other users have no rights to the file. The first number represents the Owner permission; the second represents the Group permissions; and the last number represents the permissions for all other users. The numbers are a binary representation of the rwx string.

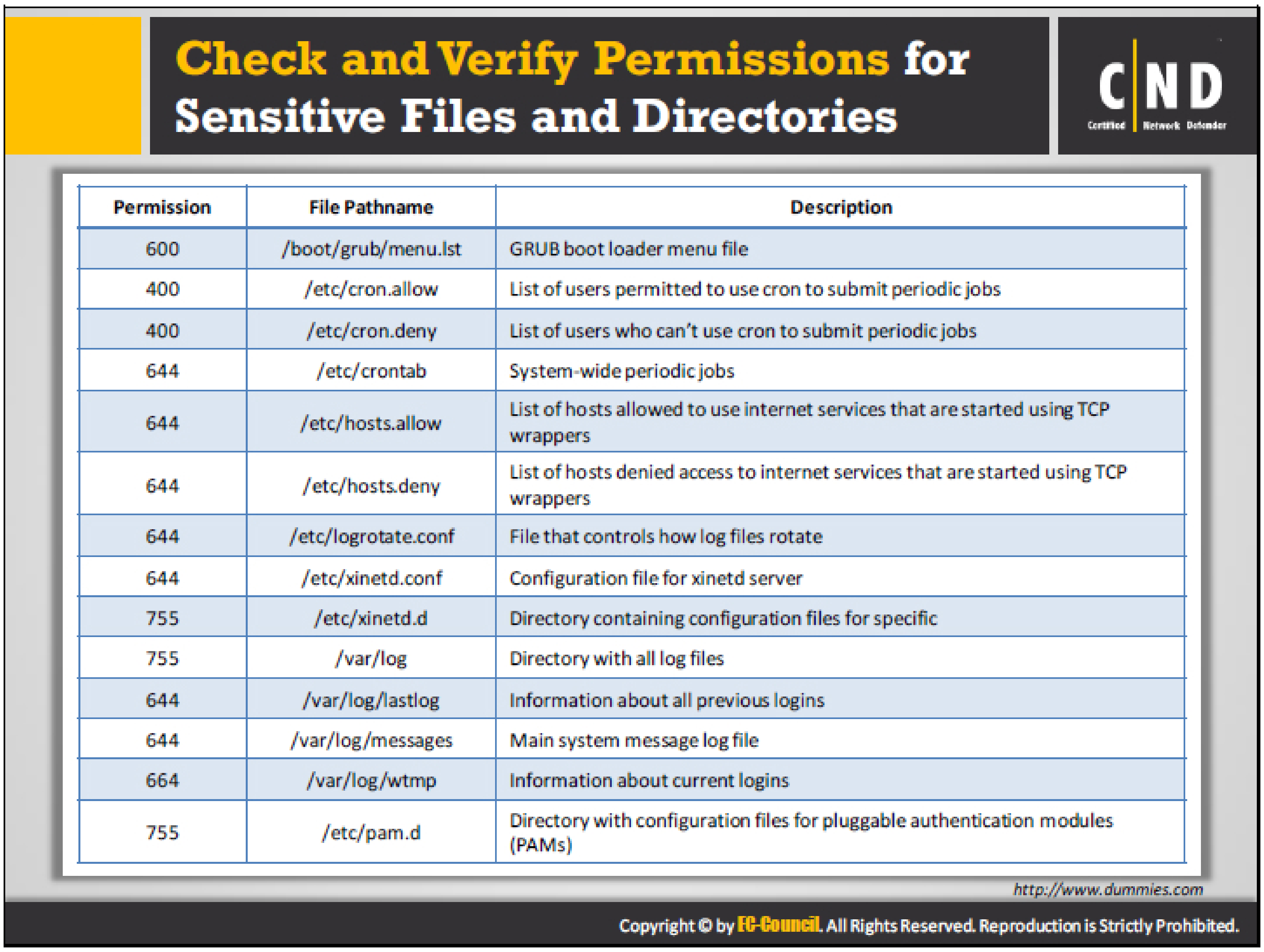
- ***r*** = 4
- ***w*** = 2
- ***x*** = 1

Administrators are required to include the binary permissions for each of the three permission groups.

Advanced Permissions

The special permissions flag can be marked with any of the following:

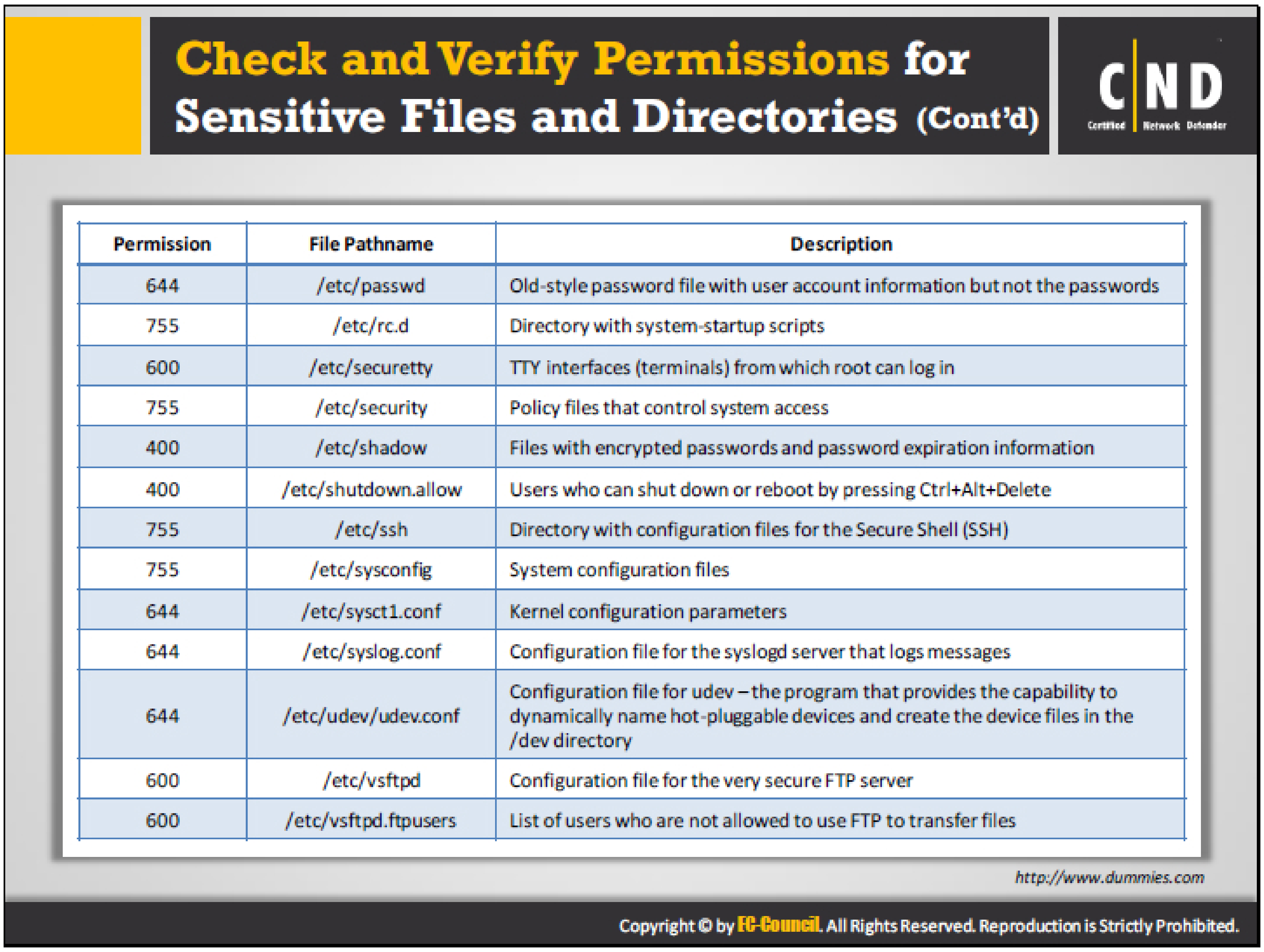
- **_** :no special permissions
- ***d***: directory
- ***l:*** The file or directory is a symbolic link
- ***s***: setuid/setgid permissions.
- ***t***:sticky bit permissions.



Check and Verify Permissions for Sensitive Files and Directories

Permission	File Pathname	Description
600	/boot/grub/menu.lst	GRUB boot loader menu file
400	/etc/cron.allow	List of users permitted to use cron to submit periodic jobs
400	/etc/cron.deny	List of users who can't use cron to submit periodic jobs
644	/etc/crontab	System-wide periodic jobs
644	/etc/hosts.allow	List of hosts allowed to use internet services that are started using TCP wrappers
644	/etc/hosts.deny	List of hosts denied access to internet services that are started using TCP wrappers
644	/etc/logrotate.conf	File that controls how log files rotate
644	/etc/xinetd.conf	Configuration file for xinetd server
755	/etc/xinetd.d	Directory containing configuration files for specific
755	/var/log	Directory with all log files
644	/var/log/lastlog	Information about all previous logins
644	/var/log/messages	Main system message log file
664	/var/log/wtmp	Information about current logins
755	/etc/pam.d	Directory with configuration files for pluggable authentication modules (PAMs)

http://www.dummies.com



Check and Verify Permissions for Sensitive Files and Directories (Cont'd)

Permission	File Pathname	Description
644	/etc/passwd	Old-style password file with user account information but not the passwords
755	/etc/rc.d	Directory with system-startup scripts
600	/etc/securetty	TTY interfaces (terminals) from which root can log in
755	/etc/security	Policy files that control system access
400	/etc/shadow	Files with encrypted passwords and password expiration information
400	/etc/shutdown.allow	Users who can shut down or reboot by pressing Ctrl+Alt+Delete
755	/etc/ssh	Directory with configuration files for the Secure Shell (SSH)
755	/etc/sysconfig	System configuration files
644	/etc/sysct1.conf	Kernel configuration parameters
644	/etc/syslog.conf	Configuration file for the syslogd server that logs messages
644	/etc/udev/udev.conf	Configuration file for udev – the program that provides the capability to dynamically name hot-pluggable devices and create the device files in the /dev directory
600	/etc/vsftpd	Configuration file for the very secure FTP server
600	/etc/vsftpd.ftpusers	List of users who are not allowed to use FTP to transfer files

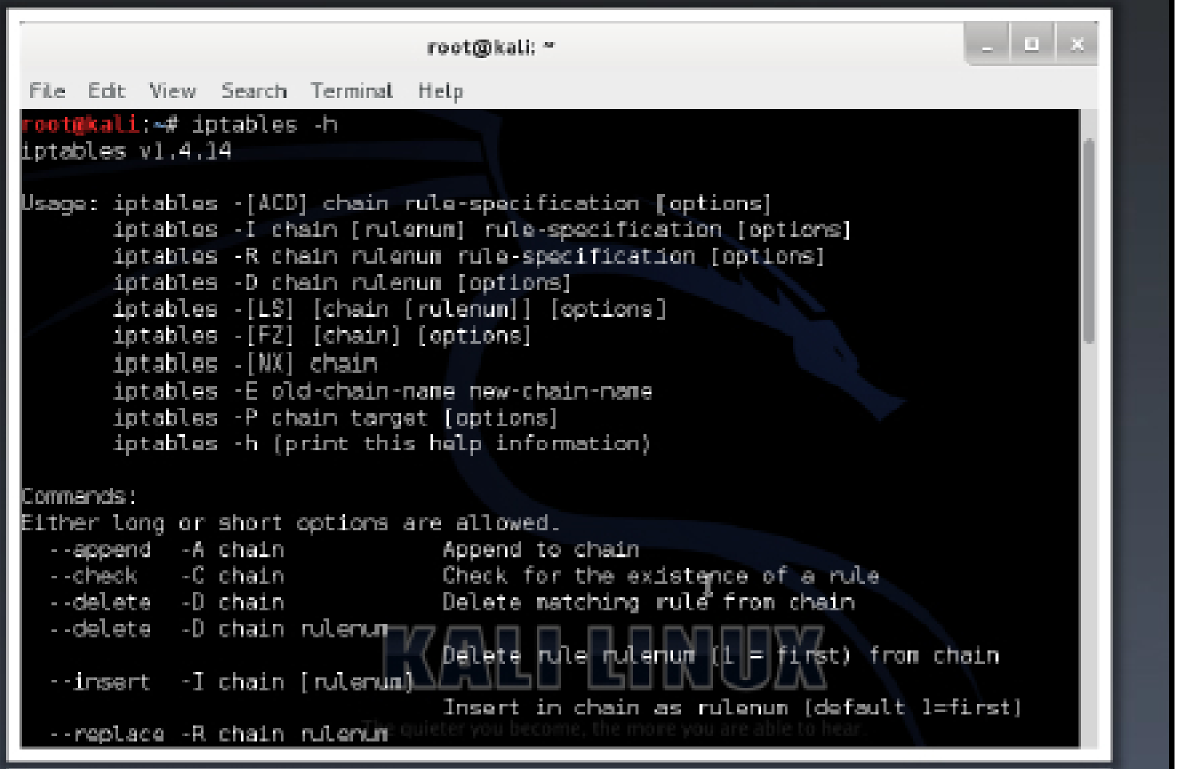
http://www.dummies.com

The table shown includes the typical numeric permission settings for important system files in Linux. This may slightly vary depending on the Linux distribution.

After knowing the numeric permission values for common File and Directory Permission Settings, you will be able to quickly identify the permissions given or changes in the permission values for sensitive files and directories of Linux. Administrators should compare and identify permission value allocations and changes in permission for the Linux hosts on their network.

Host-based Firewall Protection with IPtables

- IPtables is a built-in firewall utility for Linux operating systems.
- IPtables comes pre-installed on any Linux distribution. However, you can update/install it with following command
  - `sudo apt-get install iptables`



```
root@kali:~# iptables -h
iptables v1.4.14

Usage: iptables -[ACD] chain rule-specification [options]
       iptables -I chain [rulenum] rule-specification [options]
       iptables -R chain rulenum rule-specification [options]
       iptables -D chain rulenum [options]
       iptables -[LS] [chain [rulenum]] [options]
       iptables -[FZ] [chain] [options]
       iptables -[NX] chain
       iptables -E old-chain-name new-chain-name
       iptables -P chain target [options]
       iptables -h (print this help information)

Commands:
Either long or short options are allowed.
  --append  -A chain            Append to chain
  --check   -C chain            Check for the existence of a rule
  --delete  -D chain            Delete matching rule from chain
  --delete  -D chain rulenum
                                Delete rule rulenum (1 = first) from chain
  --insert  -I chain [rulenum]
                                Insert in chain as rulenum (default 1=first)
  --replace -R chain rulenum
```

Iptables are command-line firewall utilities that can allow or deny traffic. Iptables are preinstalled in a Linux system. In order to update or install iptables, the user needs to regain the iptable package using the command:

```
sudo apt-get install iptables
```

Every packet traversing through the filter system is assigned to an appropriate table depending on the tasks performed by the packet. The table contains chains that display the details of the destination of the packet. The tables can be used to create rules and the user has the facility to create their own chains and link them from the built-in chains. This facilitates the ability to create complex rules. However, the user needs to be extra alert while using the iptable commands as any small error in the command can lock the system and requires the user to fix the error manually.

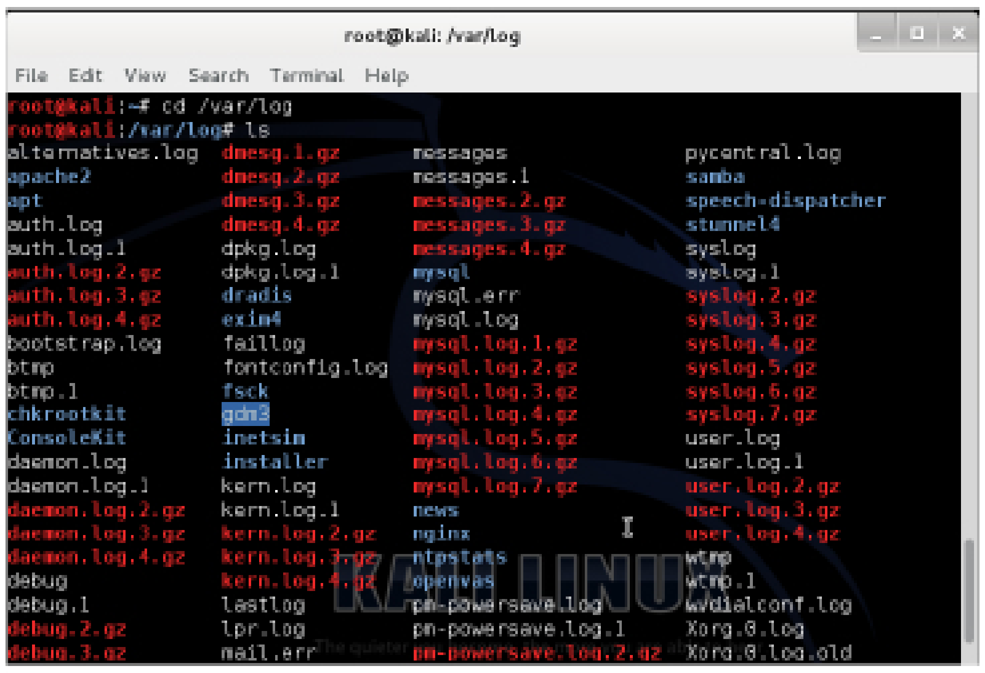
There are three different types of chains:

- **Input**: The input chain verifies the incoming connections and its behavior. The iptable compares the IP address and port of the incoming connection to a rule in the chain.
- **Forward**: The forward chain mainly forwards the incoming connections to its destination. The command: iptables –L –v, verifies whether an incoming connection needs a forward chain.
- **Output**: The output chain is used for output connections, wherein the chain checks for the output chain and decides whether to allow or deny the output request.

Linux Log Review and Audit

Various types of Linux OS and core applications logs are stored under **/var/log directory**

Log Events To Look For	
Successful User Login	"Ac cepted Password", "Accepted Public key", "Session Opened"
Failed User Login	"Authentication Failure", "Failed Password"
User Log off	"Session Closed"
User account change or deletion	"Password changed", "new user", "Delete user"
Sudo actions	"Sudo: ....COMMAND=..."FAILED su"
Service Failure	"Failed" or "Failure"



```
root@kali:~# cd /var/log
root@kali:/var/log# ls
alternatives.log   dmesg.1.gz        messages                  pycentral.log
apache2            dmesg.2.gz        messages.1                samba
apt                dmesg.3.gz        messages.2.gz             speech-dispatcher
auth.log           dmesg.4.gz        messages.3.gz             stunnel4
auth.log.1         dpkg.log          messages.4.gz             syslog
auth.log.2.gz      dpkg.log.1        mysql                     syslog.1
auth.log.3.gz      dradis            mysql.err                 syslog.2.gz
auth.log.4.gz      exim4             mysql.log                 syslog.3.gz
bootstrap.log      faillog           mysql.log.1.gz            syslog.4.gz
btmp               fontconfig.log    mysql.log.2.gz            syslog.5.gz
btmp.1             fsck              mysql.log.3.gz            syslog.6.gz
chkrootkit         gdm3              mysql.log.4.gz            syslog.7.gz
ConsoleKit         inetsim           mysql.log.5.gz            user.log
daemon.log         installer         mysql.log.6.gz            user.log.1
daemon.log.1       kern.log          mysql.log.7.gz            user.log.2.gz
daemon.log.2.gz    kern.log.1        news                      user.log.3.gz
daemon.log.3.gz    kern.log.2.gz     nginx                     user.log.4.gz
daemon.log.4.gz    kern.log.3.gz     ntpstats                  wtmp
debug              kern.log.4.gz     openvas                   wtmp.1
debug.1            lastlog           pm-powersave.log          wvdialconf.log
debug.2.gz         lpr.log           pm-powersave.log.1        Xorg.0.log
debug.3.gz         mail.err          pm-powersave.log.2.gz     Xorg.0.log.old
```

Linux Log Review and Audit (Cont'd)

Common Linux Log Files	
./var/log/messages	General message and system related stuff
./var/log/auth.log	Authentication logs
. /var/log/kern.log	Kernel logs
. /var/log/cron.log	Crond logs (cron job)
. /var/log/maillog	Mail server logs
. /var/log/qmail/	Qmail log directory (more files inside this directory)
. /var/log/httpd/	Apache access and error logs directory
. /var/log/lighttpd/	Lighttpd access and error logs directory
. /var/log/boot.log	System boot log
./var/log/mysqld.log	MySQL database server log file
. /var/log/secure or /var/log/auth.log	Authentication log
. /var/log/utmp or /var/log/wtmp	Login records file
./var/log/yum.log	Yum command log file

Logs provide a shadow of the system events performed on a computer. It lets you know what has happened on the system. Regular monitoring and auditing of the logs help the administrators trace out a user's activities on the system.

Log files are usually text-based files. The logs are stored from the system and various programs/services. All log files are stored in the path /var/log. The log files var/log/wtmp, stores all logins and logouts into the system and /var/log/messages stores logs from all kernel and system programs.

It is advisable to monitor and clean the files in /var/log at regular intervals. The Logrotate utility allows for the automatic rotation, compression, removal and mailing of log files. Logrotate can handle a log file daily, weekly, monthly or when the log file gets to a certain size.

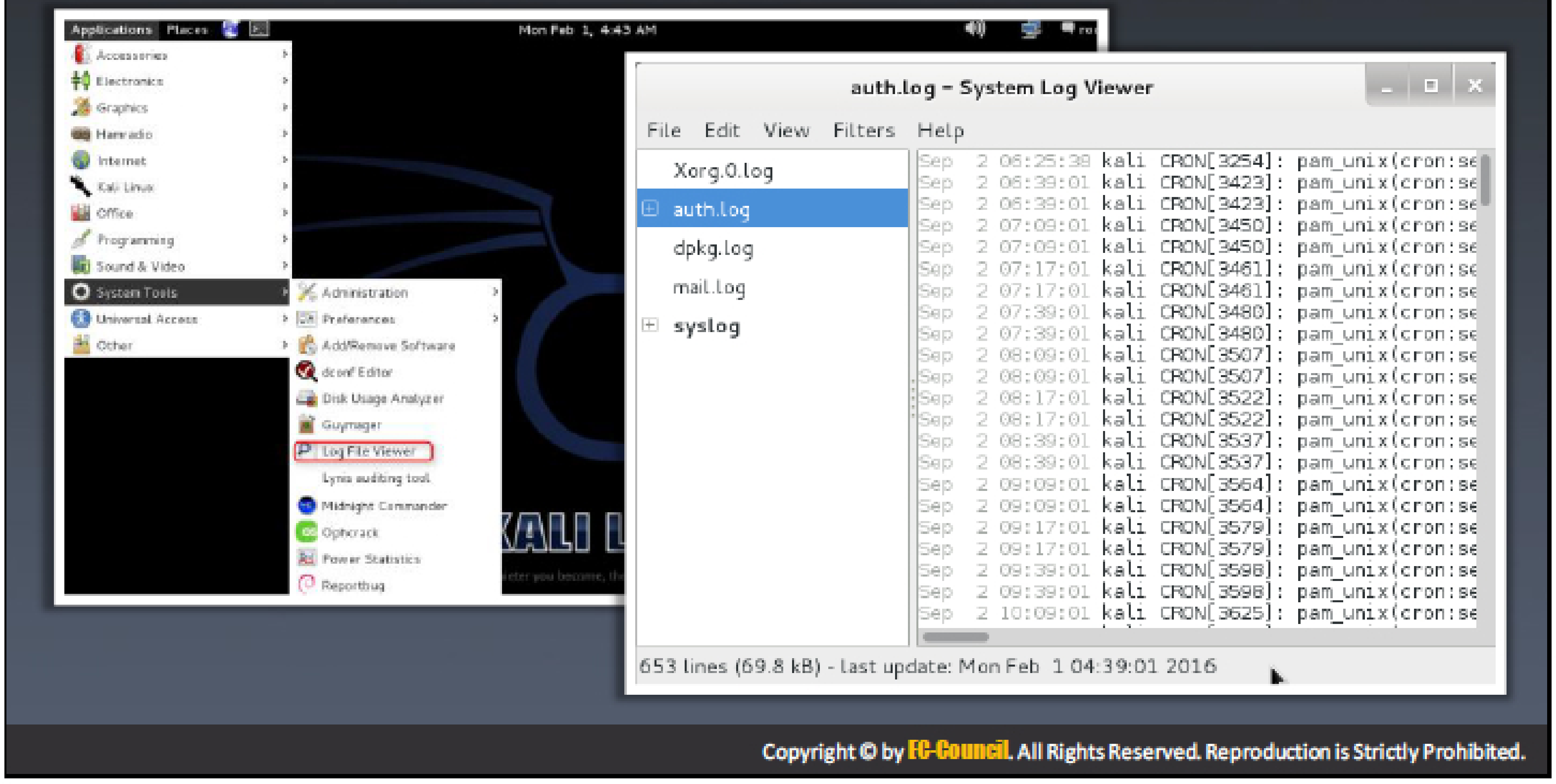
/etc/rsyslog.conf controls what goes inside some of the log files.

Few things to be considered while conducting a log review and audit

- Find the log sources and tools required for performing an audit.
- Keep log records at a single location for easy access.
- Verify whether the user can safely rely on the time stamps due to different time zones.
- Analyze all system changes, updates and errors occurring in the system.
- Check all incidents in a system.
- Comparison of logs provide an overall picture of the status of the system.
- Get all details regarding a log, like the reason for that system event, etc.

System Log Viewer

System Log Viewer enables users to view and monitor system logs



```
Sep  2 06:25:38 kali CRON[3254]: pam_unix(cron:se
Sep  2 06:39:01 kali CRON[3423]: pam_unix(cron:se
Sep  2 06:39:01 kali CRON[3423]: pam_unix(cron:se
Sep  2 07:09:01 kali CRON[3450]: pam_unix(cron:se
Sep  2 07:09:01 kali CRON[3450]: pam_unix(cron:se
Sep  2 07:17:01 kali CRON[3461]: pam_unix(cron:se
Sep  2 07:17:01 kali CRON[3461]: pam_unix(cron:se
Sep  2 07:39:01 kali CRON[3480]: pam_unix(cron:se
Sep  2 07:39:01 kali CRON[3480]: pam_unix(cron:se
Sep  2 08:09:01 kali CRON[3507]: pam_unix(cron:se
Sep  2 08:09:01 kali CRON[3507]: pam_unix(cron:se
Sep  2 08:17:01 kali CRON[3522]: pam_unix(cron:se
Sep  2 08:17:01 kali CRON[3522]: pam_unix(cron:se
Sep  2 08:39:01 kali CRON[3537]: pam_unix(cron:se
Sep  2 08:39:01 kali CRON[3537]: pam_unix(cron:se
Sep  2 09:09:01 kali CRON[3564]: pam_unix(cron:se
Sep  2 09:09:01 kali CRON[3564]: pam_unix(cron:se
Sep  2 09:17:01 kali CRON[3579]: pam_unix(cron:se
Sep  2 09:17:01 kali CRON[3579]: pam_unix(cron:se
Sep  2 09:39:01 kali CRON[3598]: pam_unix(cron:se
Sep  2 09:39:01 kali CRON[3598]: pam_unix(cron:se
Sep  2 10:09:01 kali CRON[3625]: pam_unix(cron:se
```

653 lines (69.8 kB) - last update: Mon Feb 1 04:39:01 2016

Most log files are in plain text format. You can view these log files using any text editor. However, some log files are not readable in a human format when opening with a text editor.

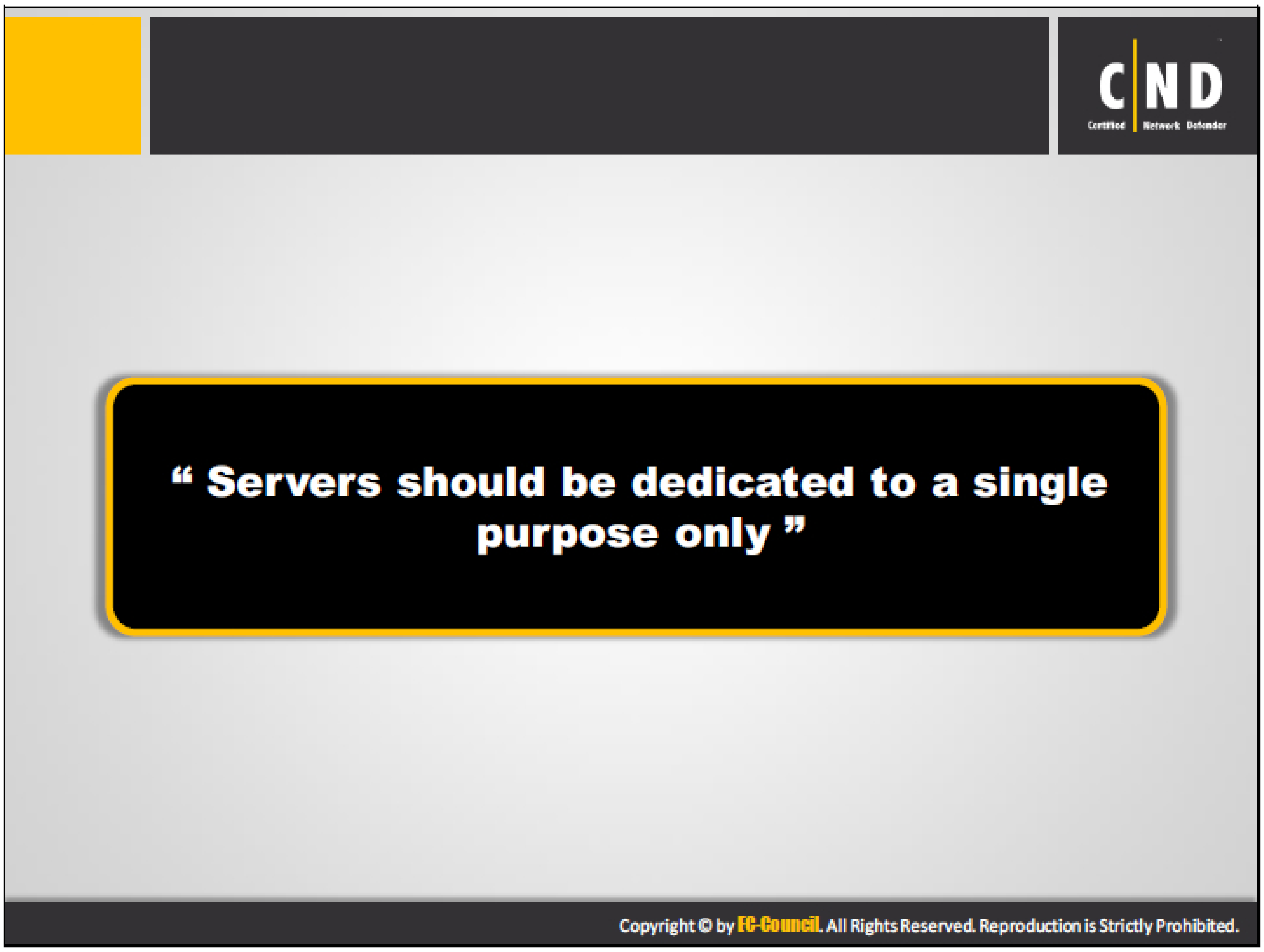
The System Log Viewer is a graphical, menu-driven viewer that facilitates the viewing and monitoring of the system logs. It comes with a few functions that can help you manage your logs, including a log monitor and log statistics display. It allows you to view system log files in an interactive, real-time application.

Log File Viewer is useful if you are new to system administration because it provides an easier, more user-friendly display of your logs than a text display of the log file. It is also useful for more experienced administrators, as it contains a monitor to enable you to continuously monitor crucial logs.

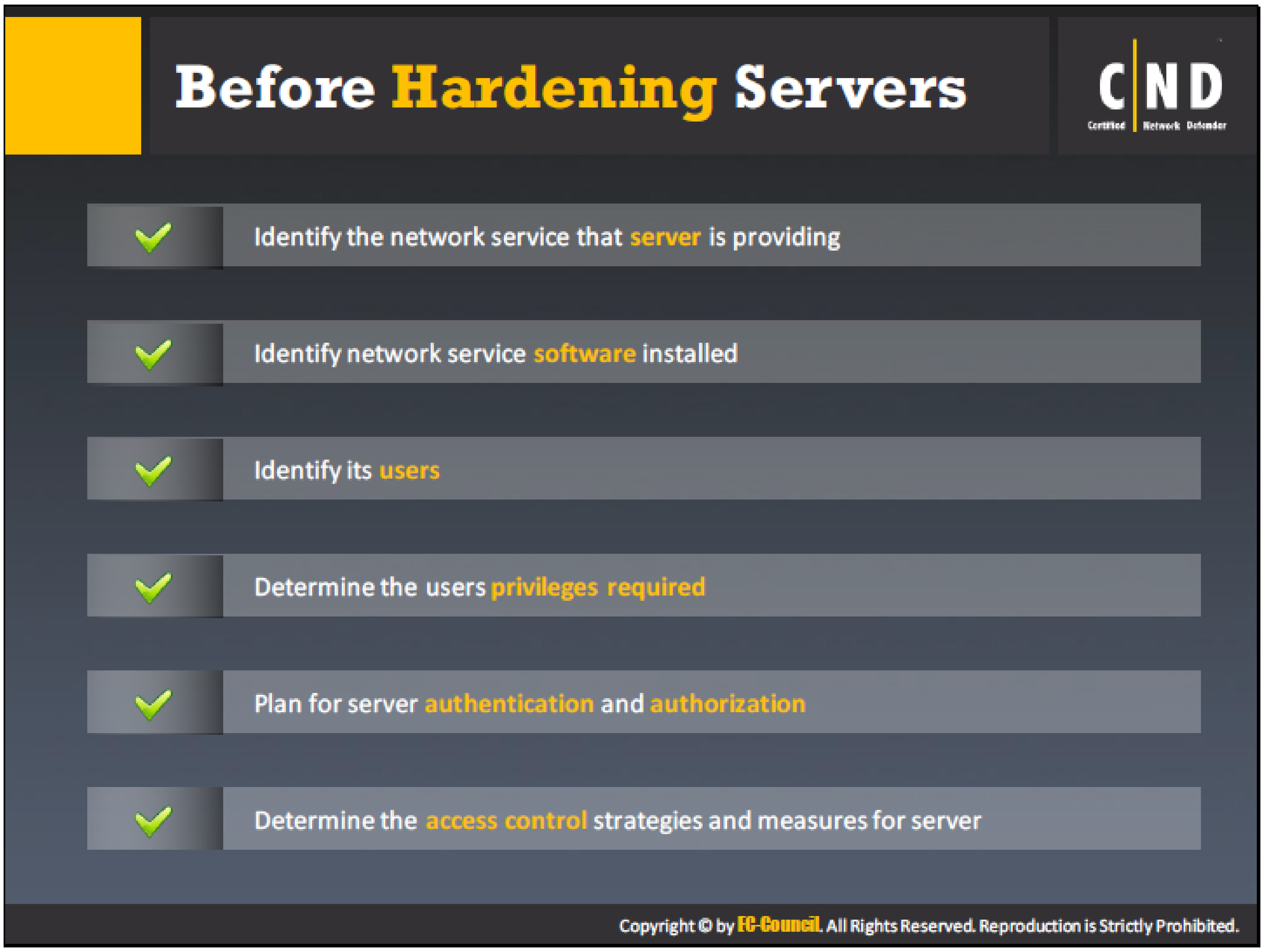
Note: Log File Viewer is useful only to those who have access to the system log files, which generally requires root access.

To View system logs in Kali Linux, go to Applications→System Tools→Log File Viewer

Source: *https://help.gnome.org*



" Servers should be dedicated to a single purpose only "



Before Hardening Servers

- ✓ Identify the network service that server is providing
- ✓ Identify network service software installed
- ✓ Identify its users
- ✓ Determine the users privileges required
- ✓ Plan for server authentication and authorization
- ✓ Determine the access control strategies and measures for server

Server hardening refers to the increased level of security provided in order for the servers to operate in a more secured environment. Hardening a server involves applying all the system security measures with some server specific security measures depending upon the type of service it provides. Administrators should consider the following points before hardening the servers:

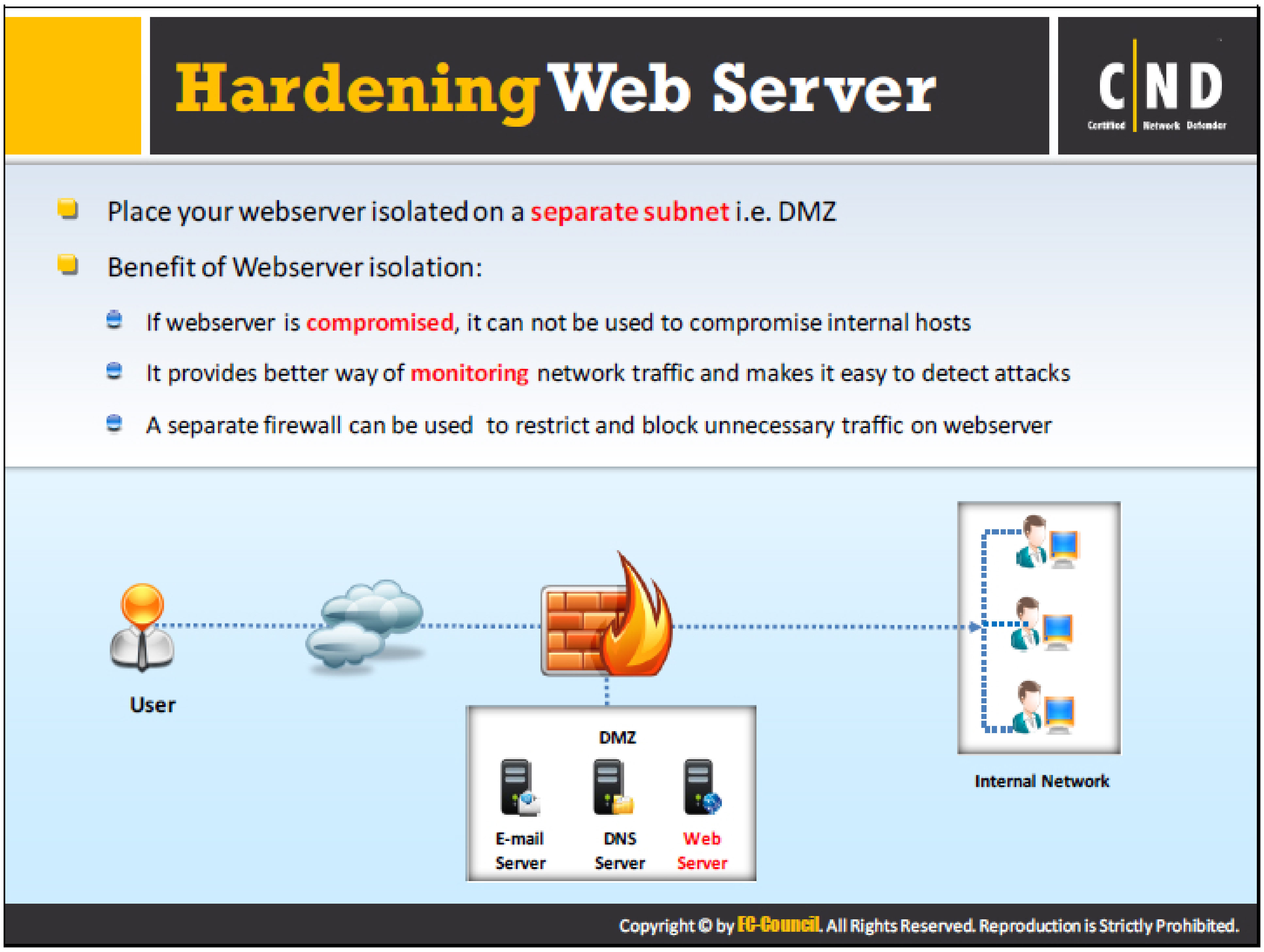
1. Identify the network service that a server is providing.
2. Identify the network service software installed.
3. Identify its users.
4. Determine the user privileges required.
5. Plan for server authentication and authorization.
6. Determine the access control strategies and measures for the server.

Administrators use various methods and tools for hardening the server. Hardening involves securing the key components of the IT architecture to reduce the risks of attack.

The three main components which require hardening are:

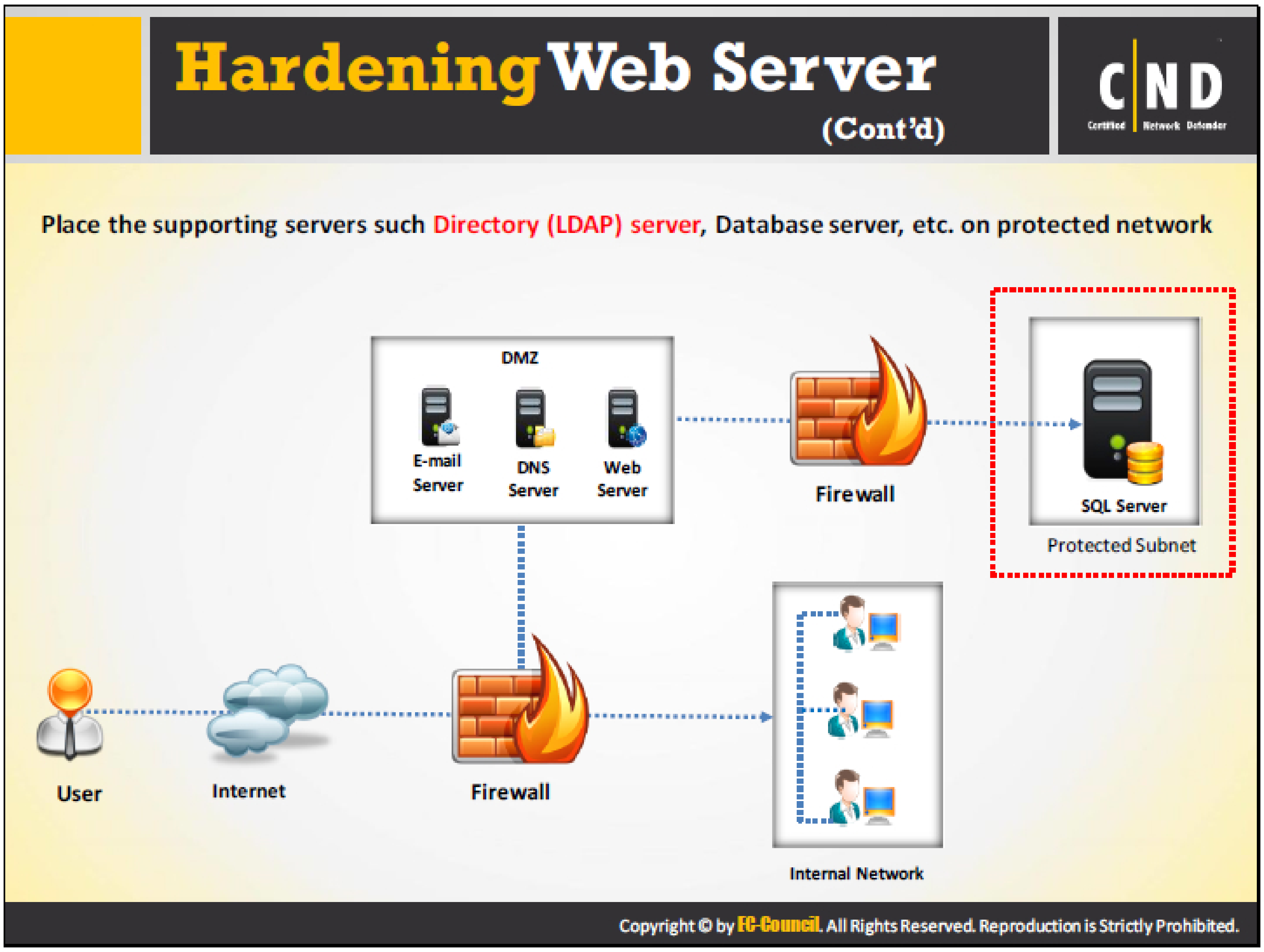
1. **Operating System:** The hardening of an operating system involves securing the system so it is configured to limit the possibilities of internal and/or external attacks. The methods for hardening may vary depending on the operating system used.
2. **Network:** Administrators can perform network hardening activities by using security protocol standards. Administrators can customize and maintain the network policies as per the organization's requirement. Administrators should regularly review the network logs and audit them. Network devices which are not operational should be removed from the network.
3. **Applications:** Every application and service installed on the network should undergo the hardening process. This ensures that any loopholes which are present in the applications and services are protected against attacks. A number of common operating system based services are installed by default and need to be reviewed.

.



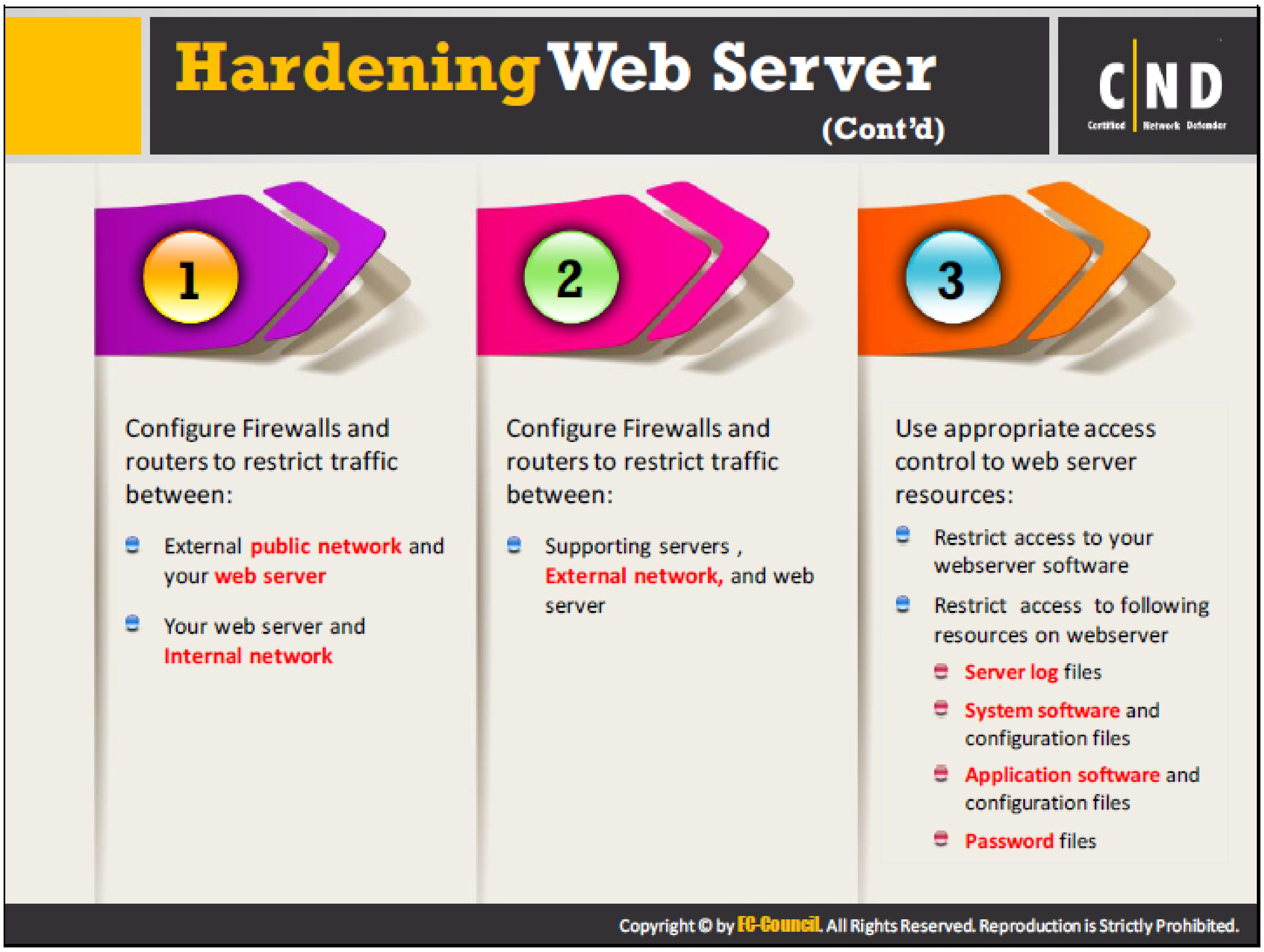
Hardening Web Server

- Place your webserver isolated on a separate subnet i.e. DMZ
- Benefit of Webserver isolation:
  - If webserver is compromised, it can not be used to compromise internal hosts
  - It provides better way of monitoring network traffic and makes it easy to detect attacks
  - A separate firewall can be used to restrict and block unnecessary traffic on webserver



Hardening Web Server (Cont'd)

Place the supporting servers such Directory (LDAP) server, Database server, etc. on protected network



Hardening Web Server (Cont'd)

CND
Certified Network Defender

1

Configure Firewalls and routers to restrict traffic between:

- External public network and your web server
- Your web server and Internal network

2

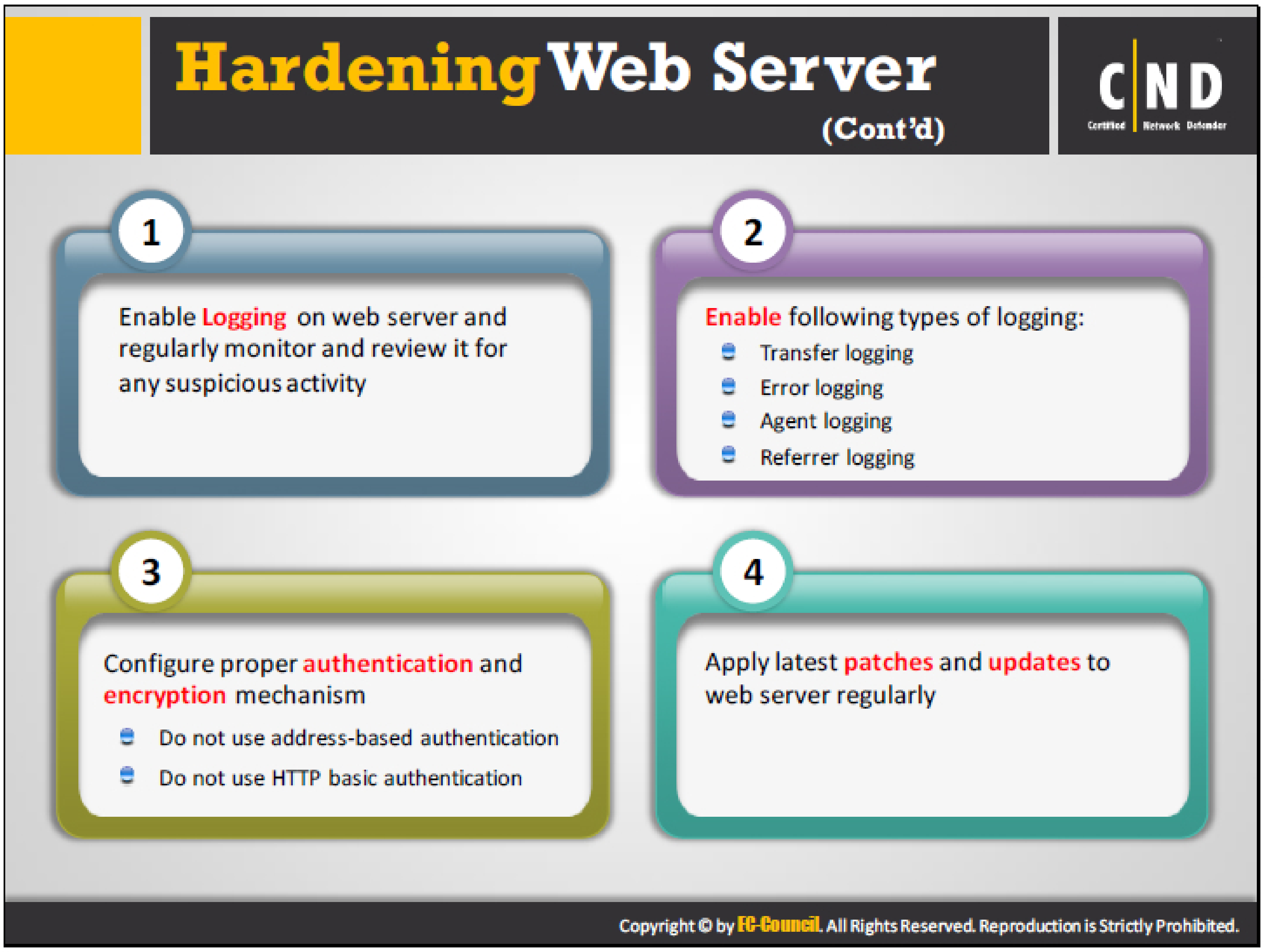
Configure Firewalls and routers to restrict traffic between:

- Supporting servers , External network, and web server

3

Use appropriate access control to web server resources:

- Restrict access to your webserver software
- Restrict access to following resources on webserver
  - Server log files
  - System software and configuration files
  - Application software and configuration files
  - Password files



Hardening Web Server (Cont'd)

CND
Certified Network Defender

1

Enable Logging on web server and regularly monitor and review it for any suspicious activity

2

Enable following types of logging:

- Transfer logging
- Error logging
- Agent logging
- Referrer logging

3

Configure proper authentication and encryption mechanism

- Do not use address-based authentication
- Do not use HTTP basic authentication

4

Apply latest patches and updates to web server regularly

The web server is a client-server architecture that enables service requests through the HTTP protocol. Proper authentication and firewall techniques enhance the security features for sites that do not require public or external access. Secure Sockets Layer ensures security for web based transactions. Proper analysis of the web server logs ensures it is secure and checks for any unusual behavior.

Any attempts to access suspicious webpages have the potential to exploit the security of the web server. Administrators should ensure that web servers are updated with the latest patches.

Hardening of Web Servers can reduce

- Attacks into your own network
- Attacks into some other network

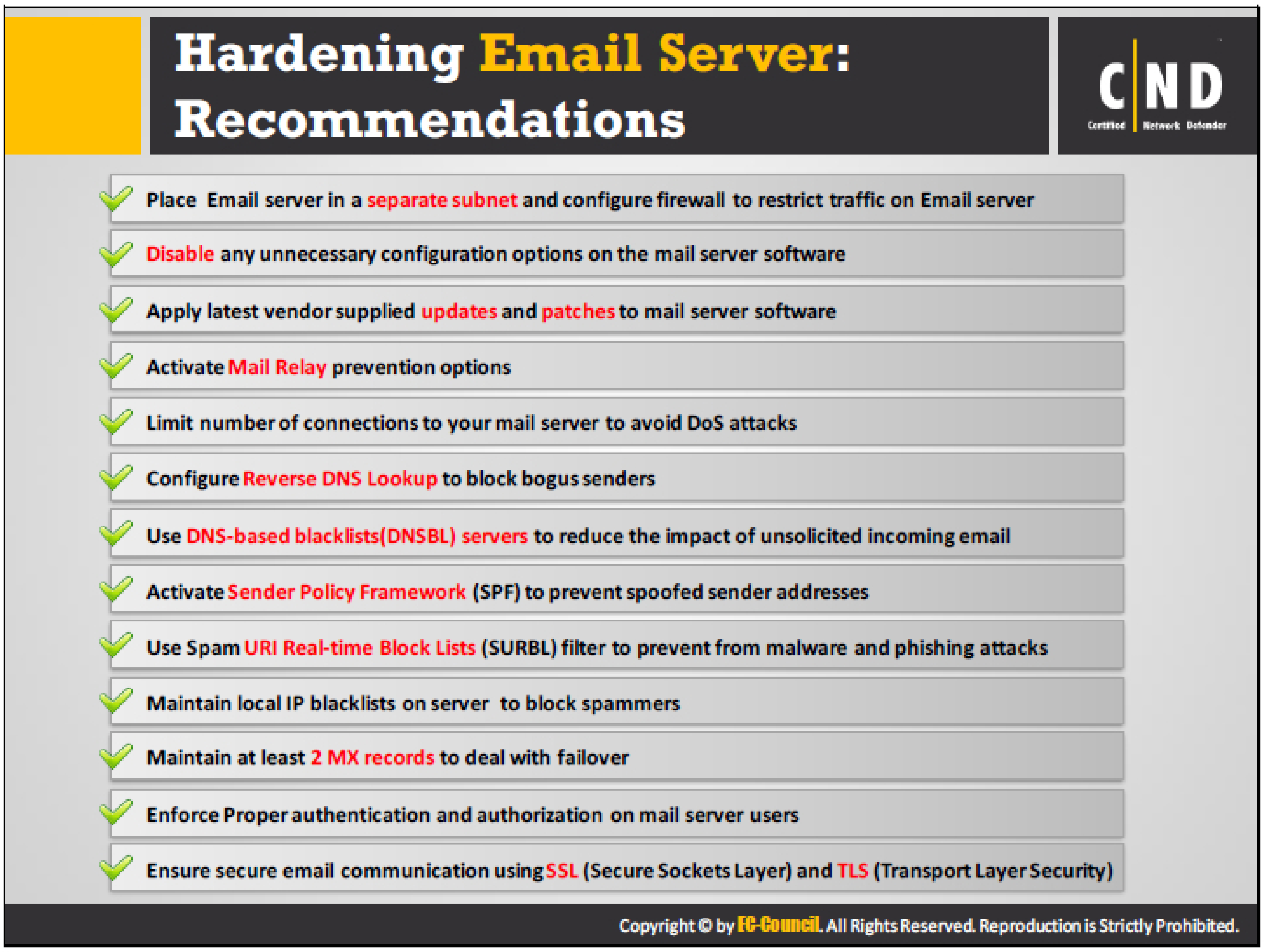
General Guidelines for Web Server Security

- Install servers securely
- Configure appropriate access controls
- Properly organize the web server software and web server host OS
- Secure all web server content
- Uphold the reliability of the web server
- Configure authentication and encryption
- Use file integrity checkers
- Enable logging
- Develop a Backup plan for the webserver
- Establish a secure network for a web server

Web Server Hardening Techniques

- Place the web server at an isolated location: This is because any external access to the web servers could enable them to access internal hosts. Allowing them to capture and monitor the traffic between the internal hosts. Also, it facilitates better management of the servers to prevent attacks.
- Place the supporting servers on other isolated subnets: This allows for the passage of allowed traffic only between the web server and that particular server. For example, only the SQL protocol is permitted between a SQL server and the webserver.
- Disable source routing and IP forwarding on the router: Enabling source routing and IP forwarding can lead to MIM attacks and IP spoofing on a web server.
- Place firewalls with the servers
- Firewall protects the traffic between:
    - The servers

  - The external network and the web server
  - The internal network and the web server
- Use appropriate access control: Controls the access to the web server software.
- Access controls should be applied to:
  - Sever log files
  - System configuration and software files
  - Application software and configuration files
  - Password files
- Recognize the level of protection required: Only authorized administrators can read or write, web server log files. Some temporary files are restricted and are stored in subdirectories. Only those services which created the file has the permission to access those subdirectories and files.
- Enable logging: Proper logging of the web server files helps locate any irregular activities in the server. The following types of logging help monitor web server logs:
  - Transfer logging
  - Error logging
  - Agent logging
  - Referrer logging
- Proper authentication and encryption mechanisms: Find methods to overcome the use of address-based authentication and HTTP basic authentication.
- Keep a copy of the web site content on a secure host: Create strategies for transferring web site content to a secure location as a backup. Also, helps increase the security mechanisms for this content.



Hardening Email Server: Recommendations

- ✓ Place Email server in a separate subnet and configure firewall to restrict traffic on Email server
- ✓ Disable any unnecessary configuration options on the mail server software
- ✓ Apply latest vendor supplied updates and patches to mail server software
- ✓ Activate Mail Relay prevention options
- ✓ Limit number of connections to your mail server to avoid DoS attacks
- ✓ Configure Reverse DNS Lookup to block bogus senders
- ✓ Use DNS-based blacklists(DNSBL) servers to reduce the impact of unsolicited incoming email
- ✓ Activate Sender Policy Framework (SPF) to prevent spoofed sender addresses
- ✓ Use Spam URI Real-time Block Lists (SURBL) filter to prevent from malware and phishing attacks
- ✓ Maintain local IP blacklists on server to block spammers
- ✓ Maintain at least 2 MX records to deal with failover
- ✓ Enforce Proper authentication and authorization on mail server users
- ✓ Ensure secure email communication using SSL (Secure Sockets Layer) and TLS (Transport Layer Security)

An organization requires electronic mail (email) systems (Email Server) for business or simple exchange of information between people. These email servers, if not configured properly, can be compromised and used for a malicious purpose.

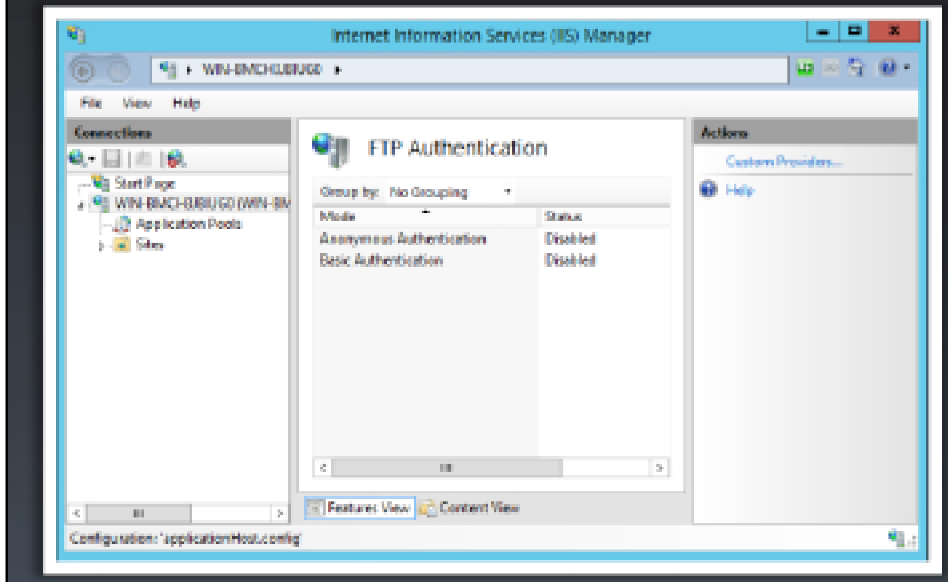
An important thing about the hardening of an e-mail server is to disable the unwanted configuration options in the server software. A perfect method to increase the security of the server is to allow only authorized users access to the e-mail.

Email-sever security guidelines

- Configure the mail relay format properly to prevent attackers from using the mail server as a gateway.
- Configure the SMTP authentication method. This requires users to access the SMTP server and provide username and password credentials before sending an e-mail.
- Restrict the number of users that can access the SMTP server. This minimizes the chances of any DoS attacks on the network.
- Enable DNS lookup to verify the existence of the sender's e-mail domain. This helps restrict any mail from unknown senders.
- Enable the Sender Policy Framework in order to restrict spoofed sender addresses.
- Activate SURBL (Spam URI Real-time Block Lists) in order to identify any unwanted links and messages in an e-mail.

- Keep track of the spammers who always send spam e-mails. This can limit unwanted internet connections on the e-mail system.
- Use POP3 and IMAP for authentication purposes.

Hardening FTP Servers: Recommendations


Internet Information Services (IIS) Manager

FTP Authentication

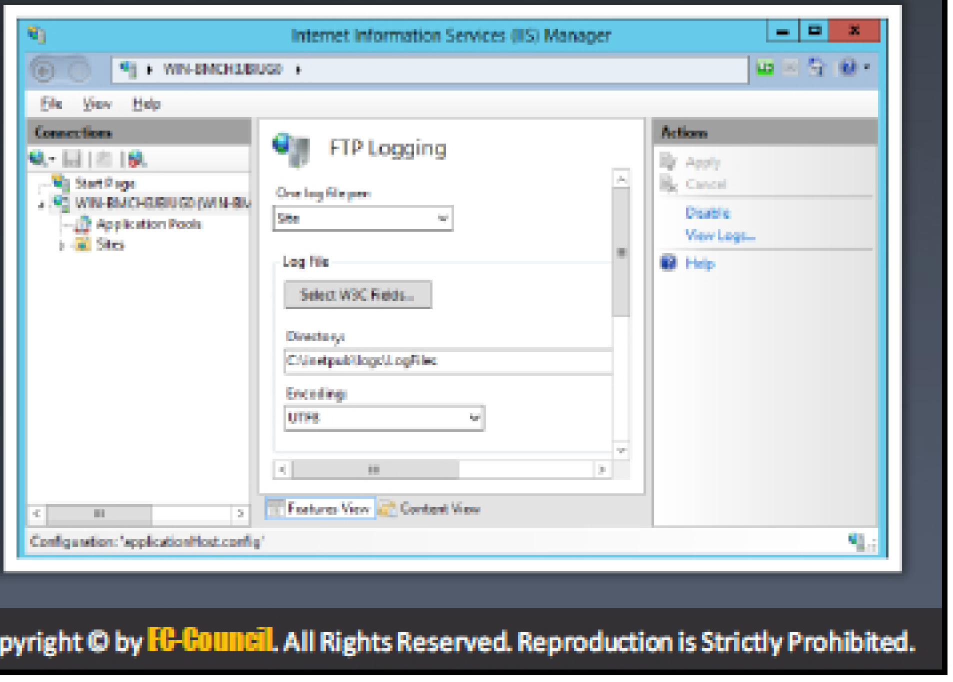
Group by: No Grouping

Mode	Status
Anonymous Authentication	Disabled
Basic Authentication	Disabled

Configuration: 'applicationHost.config'

Disable Anonymous FTP accounts. If not possible, monitor Anonymous FTP accounts regularly

Enable logging for your FTP site


Internet Information Services (IIS) Manager

FTP Logging

One log file per: Site

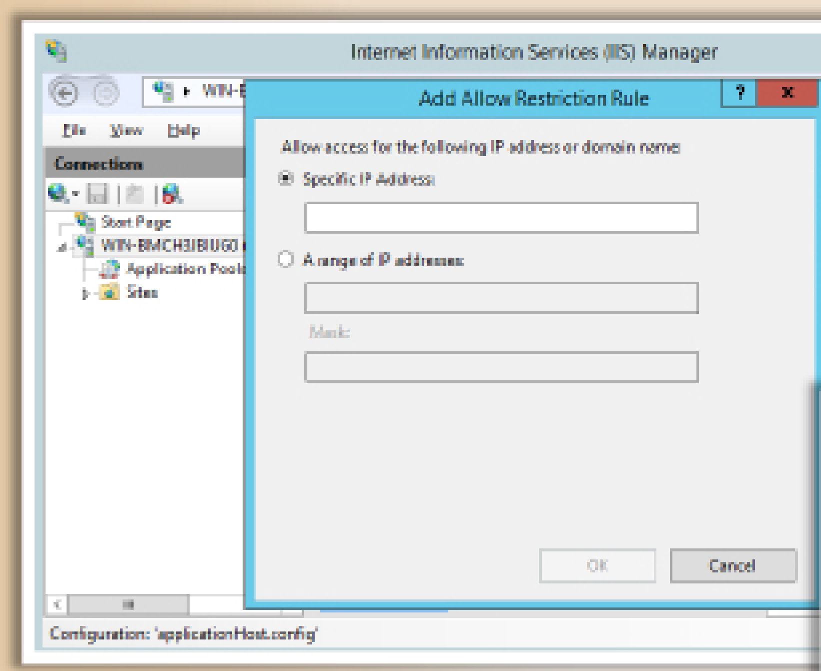
Log File

Directory: C:\inetpub\logs\LogFiles

Encoding: UTF8

Configuration: 'applicationHost.config'

Hardening FTP Servers: Recommendations (Cont'd)


Internet Information Services (IIS) Manager

Add Allow Restriction Rule

Allow access for the following IP address or domain name:

● Specific IP Address:

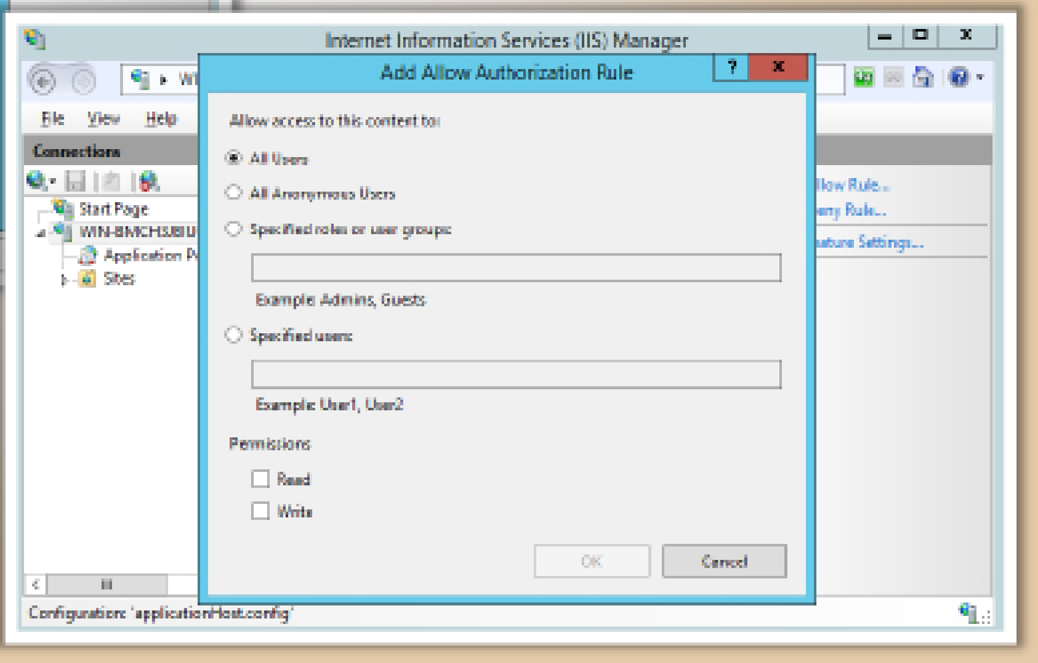
○ A range of IP addresses:

Mask:

Configuration: 'applicationHost.config'

Restrict Access by IP or domain name

Configure Access controls on authenticated FTP accounts with the help of ACLs


Internet Information Services (IIS) Manager

Add Allow Authorization Rule

Allow access to this content to:

● All Users

○ All Anonymous Users

○ Specified roles or user groups:

Example: Admins, Guests

○ Specified users:

Example: User1, User2

Permissions

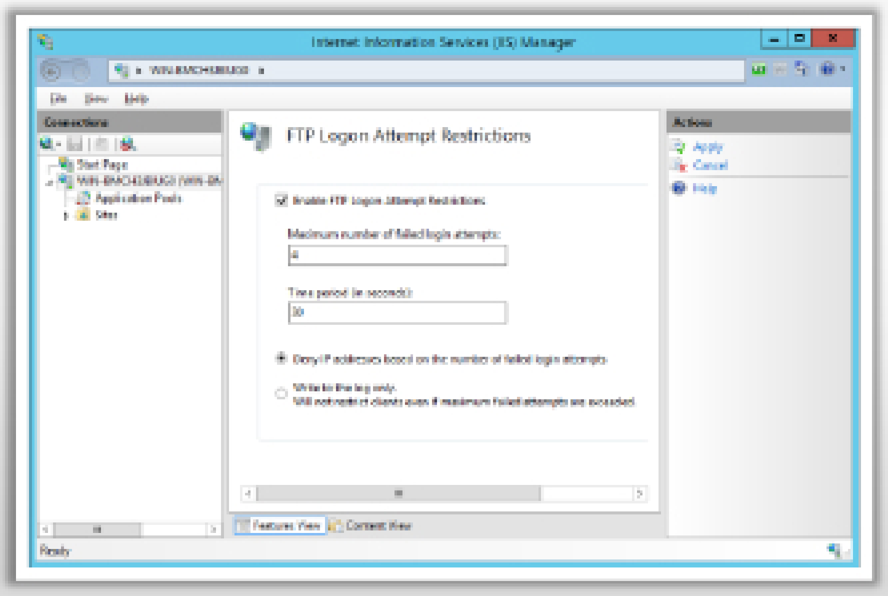
☐ Read

☐ Write

Configuration: 'applicationHost.config'

Hardening FTP Servers: Recommendations (Cont'd)

Restrict **Logon attempts** and time



Internet Information Services (IIS) Manager

FTP Logon Attempt Restrictions

☑ Enable FTP Logon Attempt Restrictions

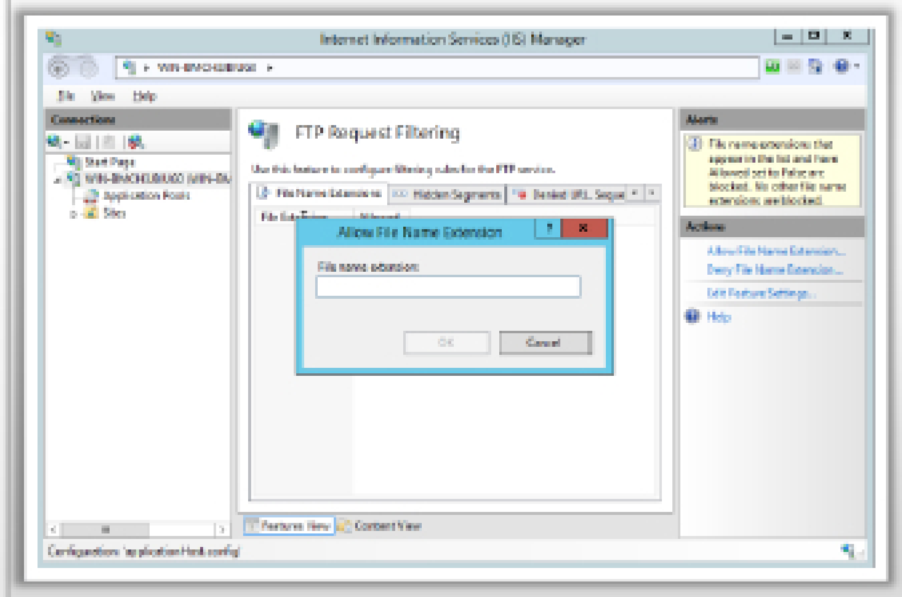
Maximum number of failed login attempts: 4

Time period (in seconds): 30

● Deny IP addresses based on the number of failed login attempts

○ Write to the log only. Will not restrict clients even if maximum failed attempts are exceeded.

Configure **filtering rules** for your FTP service



Internet Information Services (IIS) Manager

FTP Request Filtering

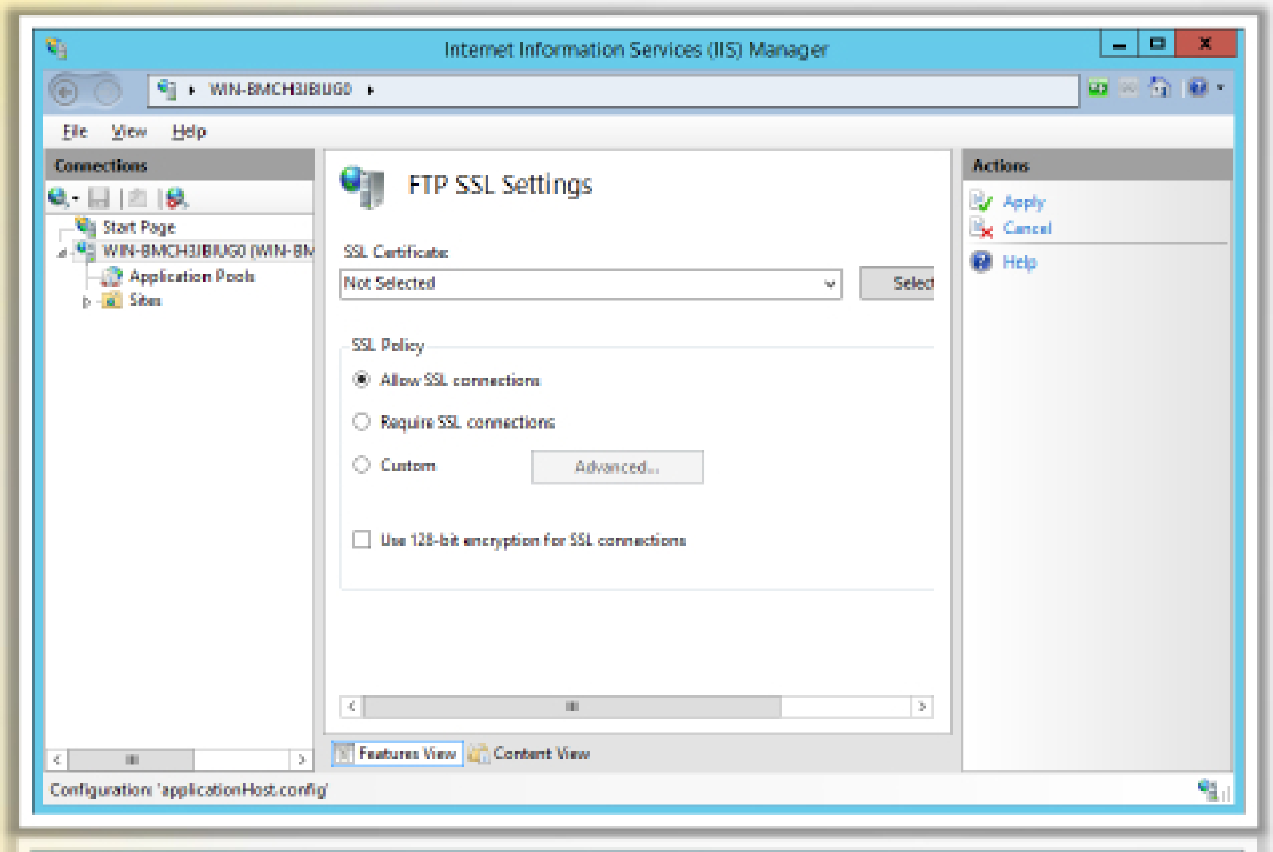
Use this feature to configure filtering rules for the FTP service.

Allow File Name Extension

File name extension:

File name extensions that appear in the list and have Allowed set to False are blocked. No other file name extensions are blocked.

Hardening FTP Servers: Recommendations (Cont'd)



Internet Information Services (IIS) Manager

FTP SSL Settings

SSL Certificate: Not Selected

SSL Policy

● Allow SSL connections

○ Require SSL connections

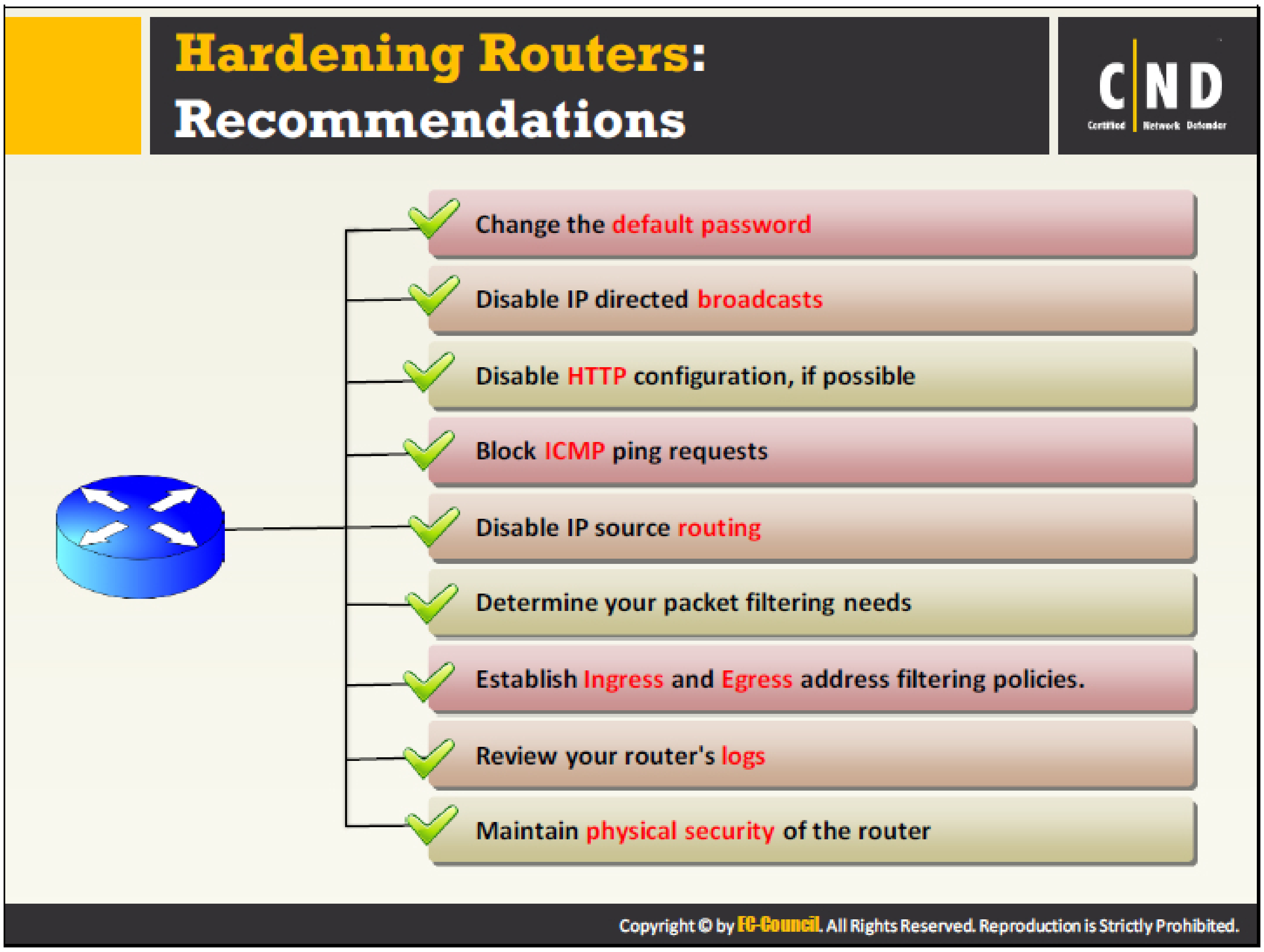
○ Custom

□ Use 128-bit encryption for SSL connections

Use **SSL / FTPS** for authenticated FTP accounts

Administrators should implement the following security measures while configuring the FTP service:

- **Inactivate unidentified FTP accounts:** Installing FTP services automatically enables anonymous access to FTP servers by any user. The users do not need any authentication to use the account. Disabling this anonymous access will minimize unauthorized users accessing the FTP server and placing illegal and dangerous files on your sites. This enables only authorized users to access the FTP server.
- **Enable logging for your FTP site:** Keeping track of the FTP logs can help in identifying the users accessing the site and the IP addresses they use. Logs provide a detailed description on the status of the site and validates if there are any attacks or threats.
- **Configure Access controls on authenticated FTP accounts with the help of ACLs:** Access control lists limit unauthorized access to the FTP directory using NTFS permissions. However, users permitted to the FTP directory should not include everyone in one group as it changes the configuration for those users who are limited to accessing FTP accounts.
- **Restrict access by IP or domain name:** Limiting access to FTP to only a certain number of users reduces attacks from unauthorized users.
- **Restrict logon attempts and time:** Users access the FTP site within a specified logon time. FTP denies permission to any user attempting to access the FTP site after the logon time has expired. With this restriction, only those users who are authorized for a specific time period can access.
- **Configure filtering rules for your FTP service:** The filtering rules check for each FTP request. If it matches the filtering rules, that particular request is allowed or if it doesn't match a filtering rule, it is declined.
- **Use SSL / FTPS for authenticated FTP accounts:** This represents the SSL settings for the FTP service. Increasing the security of the FTP service as only authenticated users achieve access.



Hardening Routers: Recommendations

- Change the default password
- Disable IP directed broadcasts
- Disable HTTP configuration, if possible
- Block ICMP ping requests
- Disable IP source routing
- Determine your packet filtering needs
- Establish Ingress and Egress address filtering policies.
- Review your router's logs
- Maintain physical security of the router

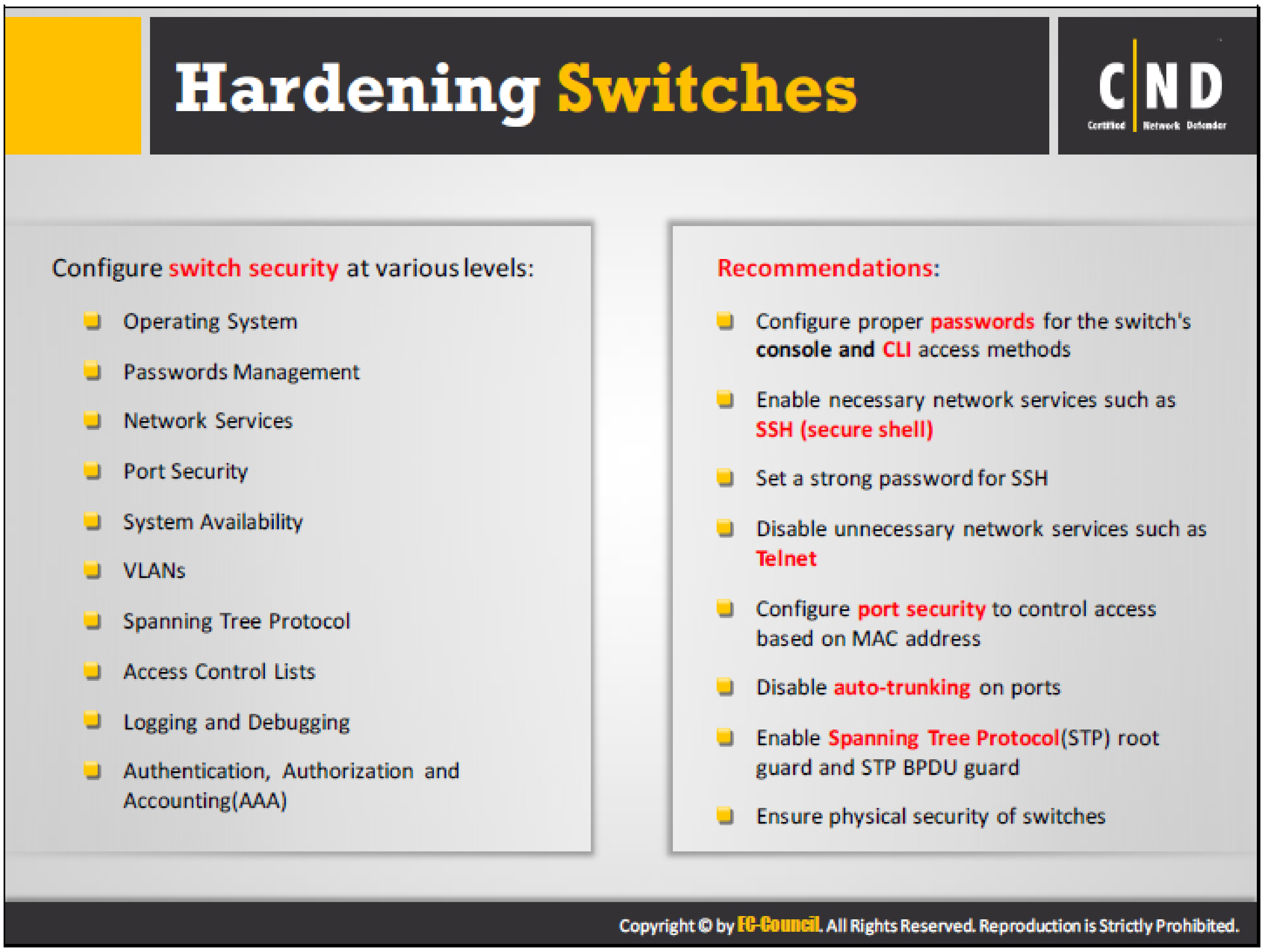
The following are recommended best practices enhancing the security of a router:

- Changing the default password: Most users do not change the default password of the router after installation. This is the same thing as giving a key to attackers so they can easily log in to your router.
- Deactivate IP directed broadcasts: Enabling IP directed broadcasts will allow attackers to send ICMP ECHO requests to another user broadcast address, using a spoofed address. The broadcast network responds to the ECHO request thereby affecting the working of all hosts in the network.
- Deactivate the HTTP configuration: Enabling the HTTP protocol for routers sends clear text traffic.
- Restrict ICMP Ping requests: Accepting PING requests enables attackers to guess the active hosts and thereby scan the network without the original user's knowledge.
- Disable IP source routing: Enabling this routing feature allows attackers to identify the path taken by the packet. This give users the ability to sniff packets from the network.
- Identify the need for packet filtering: Filtering of packets depends on the needs of the organization. The filtering mechanism helps identify whether to permit or block traffic.
- Creating ingress and egress address filtering policies: Creating policies for verifying the inbound and outbound traffic based on an IP address increases the security of the router.

- Physical security of the router: It is mandatory to maintain physical security of the router as inappropriate placement of routers allow attackers to sniff and have direct access to the appliance.
- Review the security logs: Appropriate review of the security logs will provide detailed information regarding what attacks, if any, have been launched against the router. It also provides a detailed description of the router. Reviewing logs of the router provides an overall idea regarding the status of the network too.

In addition to the above recommendations, implement the following best practices to harden your router security:

- Disable unnecessary router interfaces.
- Disable unnecessary services.
- Disable unnecessary management protocols.
- Disable ARP and proxy ARP.



Hardening Switches

Configure switch security at various levels:

- Operating System
- Passwords Management
- Network Services
- Port Security
- System Availability
- VLANs
- Spanning Tree Protocol
- Access Control Lists
- Logging and Debugging
- Authentication, Authorization and Accounting(AAA)

Recommendations:

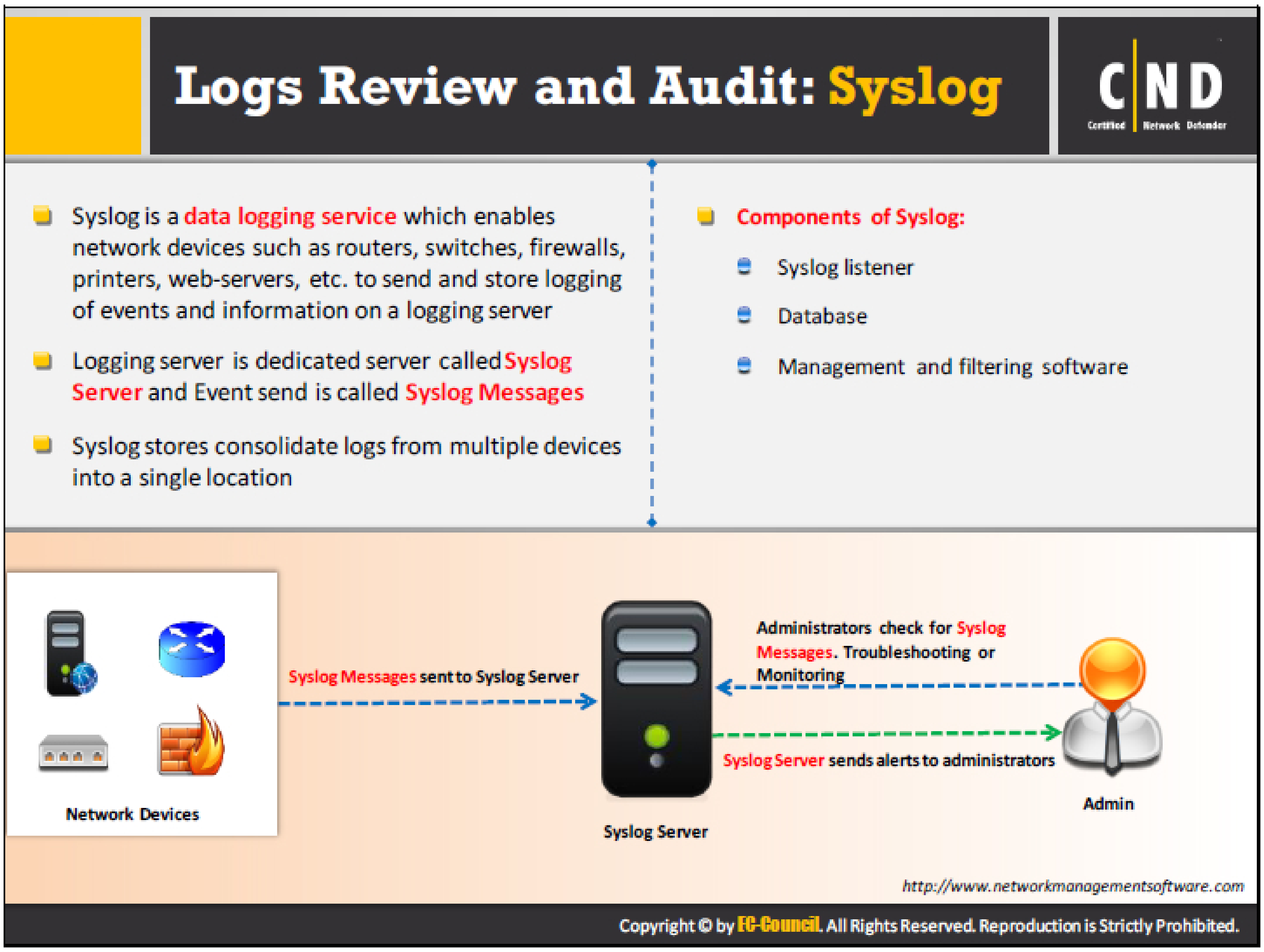
- Configure proper passwords for the switch's **console and** CLI access methods
- Enable necessary network services such as SSH (secure shell)
- Set a strong password for SSH
- Disable unnecessary network services such as Telnet
- Configure port security to control access based on MAC address
- Disable auto-trunking on ports
- Enable Spanning Tree Protocol(STP) root guard and STP BPDU guard
- Ensure physical security of switches

The best way to confirm switch security is by using port level security. Port level security limits the number of MAC addresses connected to a device. The three different methods of connecting MAC addresses to a port are as follows:

- Statically: Allows only a single MAC address to be connected to a port.
- Dynamically: These are present by default in the content – addressable memory.
- Sticky: A MAC address given to a specific port. This MAC address can be lost if not saved during reboot.

Additional switch security best practices:

- Create a strong password.
- Create time-out sessions and user access rights.
- Disable auto - trunking on ports and activate port security for MAC addresses in order to control access.
- Deactivate all ports that are not in use and assign them an unused VLAN number.
- Control the number of VLANs that can pass over a trunk.
- Maximize the use of access control lists.
- Review all security logs of the switch
- Implement AAA for local and remote access to the switch.
- Keep the switch configuration file offline and control access to it.



Logs Review and Audit: Syslog

CND Certified Network Defender

- Syslog is a data logging service which enables network devices such as routers, switches, firewalls, printers, web-servers, etc. to send and store logging of events and information on a logging server
- Logging server is dedicated server called Syslog Server and Event send is called Syslog Messages
- Syslog stores consolidate logs from multiple devices into a single location

- Components of Syslog:
  - Syslog listener
  - Database
  - Management and filtering software

Network Devices

Syslog Messages sent to Syslog Server

Syslog Server

Administrators check for Syslog Messages. Troubleshooting or Monitoring

Syslog Server sends alerts to administrators

Admin

http://www.networkmanagementsoftware.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Syslog enables network devices to record event messages to the logging server or the syslog server. It is possible to log many events and the syslog protocol can handle many different devices. Normally, Windows-based servers do not support syslog. But, there are many third-party tools available that can actually gather the Windows server log information and then forward it to the syslog server.

Syslog is the standard for message logging and uses a facility code that determines the software used for generating the messages and also assigns a severity label to each. The syslog finds its application in system management, security auditing and debugging messages. Many types of devices such as printers, routers, etc. use the syslog standard that enables a centralized method of logging data from different devices.

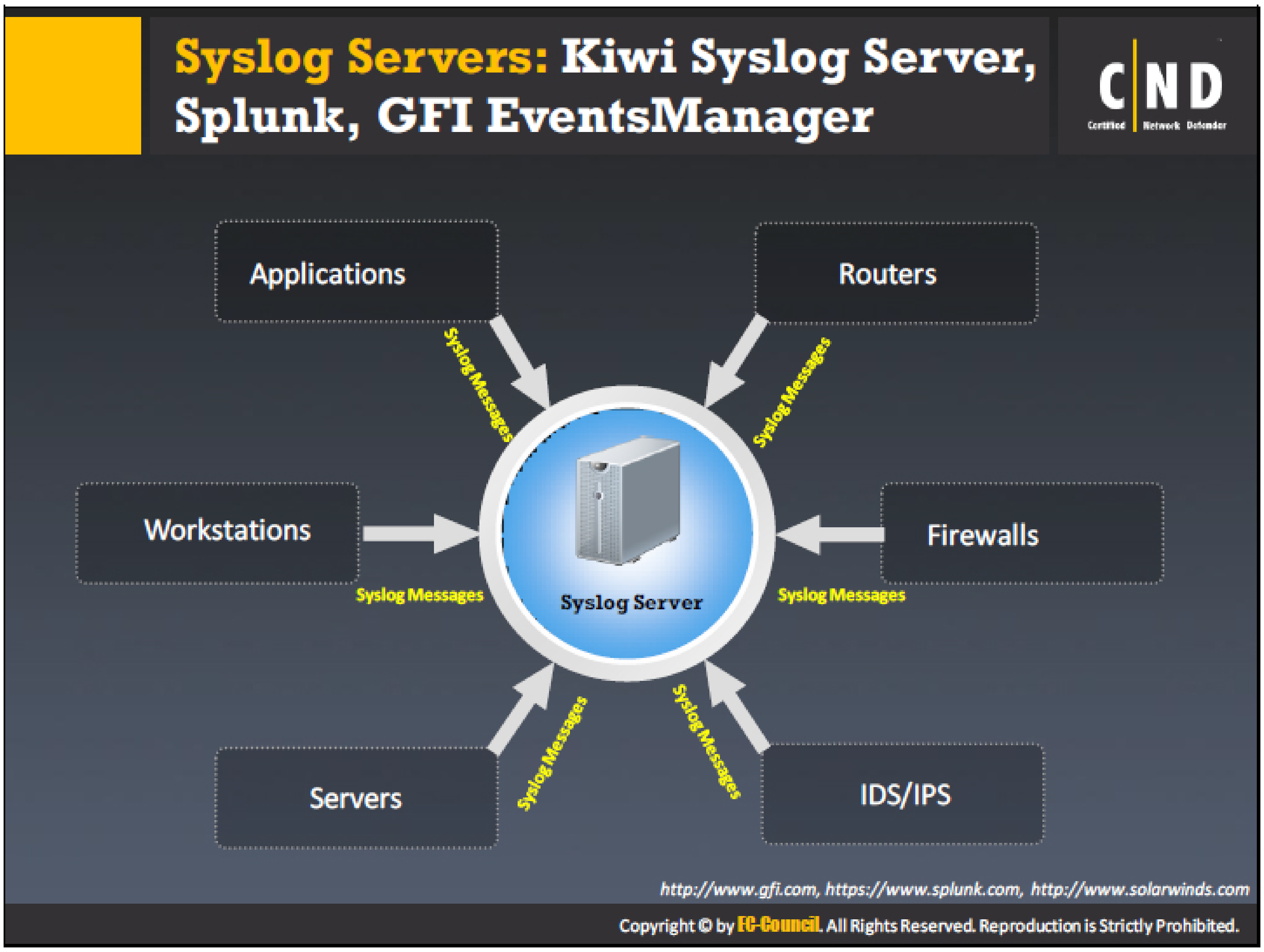
There are many components available for syslog server:

- **Syslog Listener:** The syslog server gathers information sent over the network and a syslog listener acquires all information sent over UDP port 514.
- **Database:** Syslog servers create a database in order to store log data from large networks.
- **Management and Filtering Software:** The management and filtering software helps filter data from the database. At times, network administrators find it difficult to find the log details from the database. The use of this software can actually enable the administrators to filter the required data.

- **Syslog Messages:** Syslog messages include all the information like the IP address, timestamp and the actual log message. The syslog uses a method called facility that identifies the source of message on any machine. The syslog message also has a severity level field that determines the severity level. A severity level of '0' signifies that the message is an emergency. The severity level of '1' signifies that the messages need immediate action and the syslog messages severity can go up in range.

Limitations of Syslog server:

- The syslog protocol actually does not provide any specific method for formatting messages, which causes issues concerning the consistency of the messages.
- Syslog uses UDP as a protocol for the transport of messages. As UDP is connectionless oriented, there are chances for syslog to lose packets.
- No method for authenticating the syslog messages. It can actually provide access to another machine and send fake log events.



Syslog Servers: Kiwi Syslog Server, Splunk, GFI EventsManager

http://www.gfi.com, https://www.splunk.com, http://www.solarwinds.com

GFI EventsManager

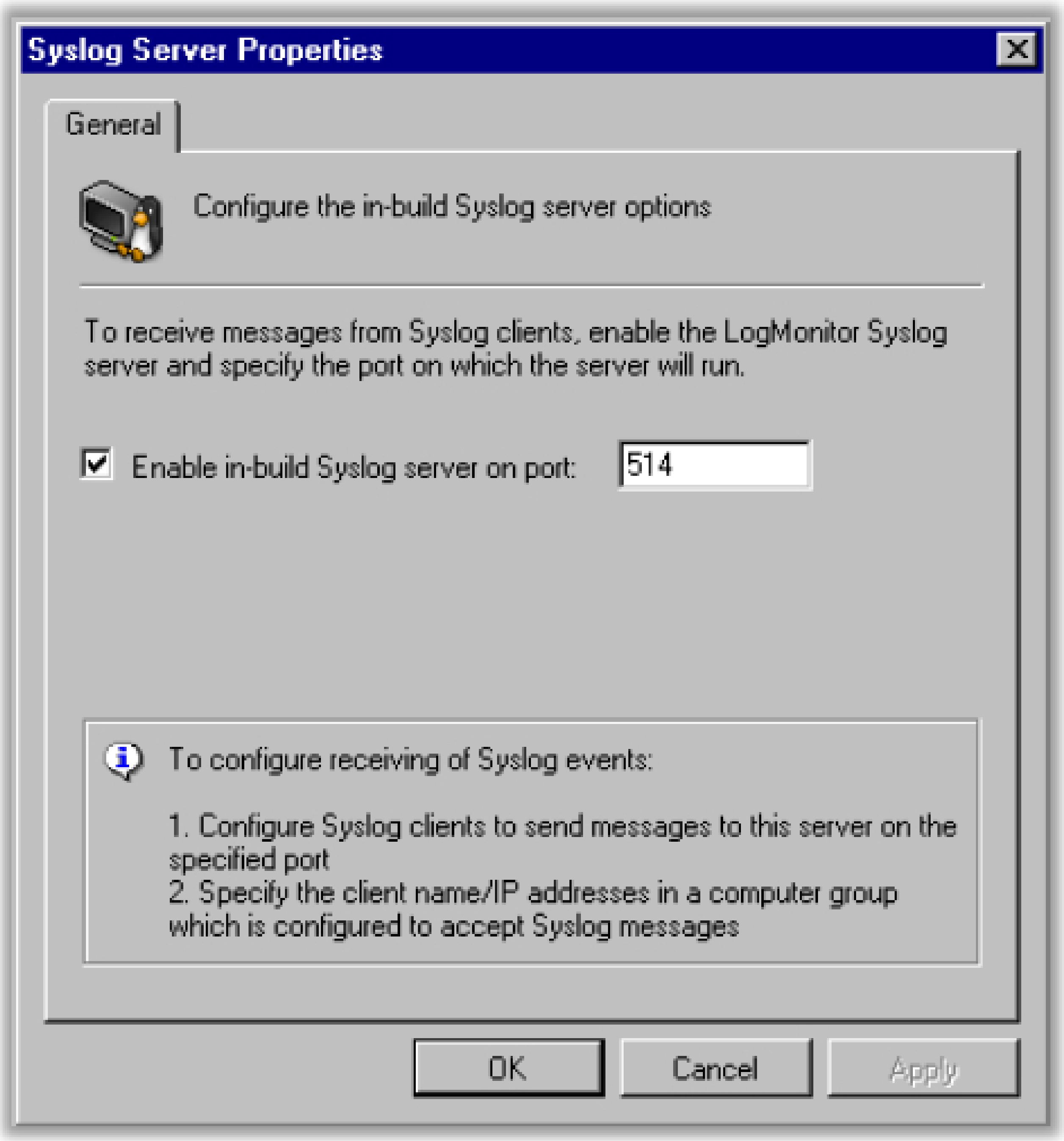
Source: *http://www.gfi.com*

GFI EventsManager performs network wide log monitoring, analysis, management and archiving.

Features:

- Manage event log data for system reliability, security, availability and compliance.
- Log data analysis for SIEM.
- Log data consolidation for compliance.
- Complete IT infrastructure monitoring and management.

GFI EventsManager is designed to act as a Syslog server and receive Syslog events from various devices including Cisco PIX firewall. In order to use GFI EventsManager as a Syslog server, you must configure Cisco PIX firewall and similar devices to send Syslog messages directly to the machine that is running GFI EventsManager.



Syslog Server Properties

Configure the in-build Syslog server options

To receive messages from Syslog clients, enable the LogMonitor Syslog server and specify the port on which the server will run.

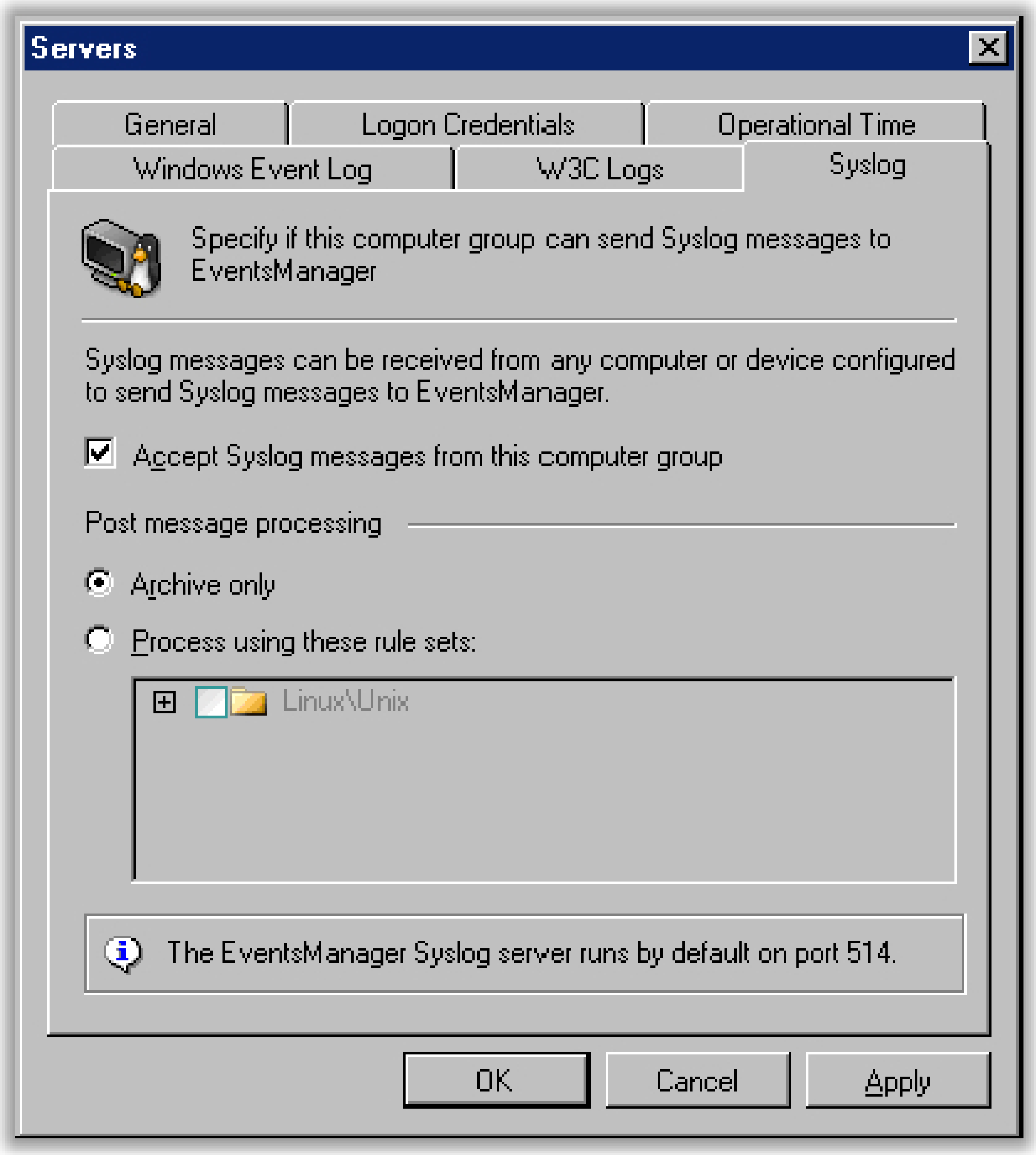
☑ Enable in-build Syslog server on port: 514

To configure receiving of Syslog events:

1. Configure Syslog clients to send messages to this server on the specified port
2. Specify the client name/IP addresses in a computer group which is configured to accept Syslog messages

FIGURE 6.29: Enabling Syslog server port

By default, GFI EventsManager will listen for Syslog messages on port 514, therefore you must make sure that this port is not being used by other applications. The port on which GFI EventsManager listens for Syslog messages is configurable through the management console.



Specify if this computer group can send Syslog messages to EventsManager

Syslog messages can be received from any computer or device configured to send Syslog messages to EventsManager.

☑ Accept Syslog messages from this computer group

Post message processing

● Archive only

○ Process using these rule sets:

⊞ □ Linux\Unix

The EventsManager Syslog server runs by default on port 514.

FIGURE 6.30: Enabling Syslog server to listen messages

To enable GFI EventsManager to collect Syslog events you need to:

1. Bring up the (computer/computer group) properties dialog
2. Click on the Syslog tab
3. To enable the syslog server and listen for messages sent by the computers in a computer group, select the option 'the computers specified in this group will send Syslog events'

Kiwi Syslog Server

Source: http://www.solarwinds.com

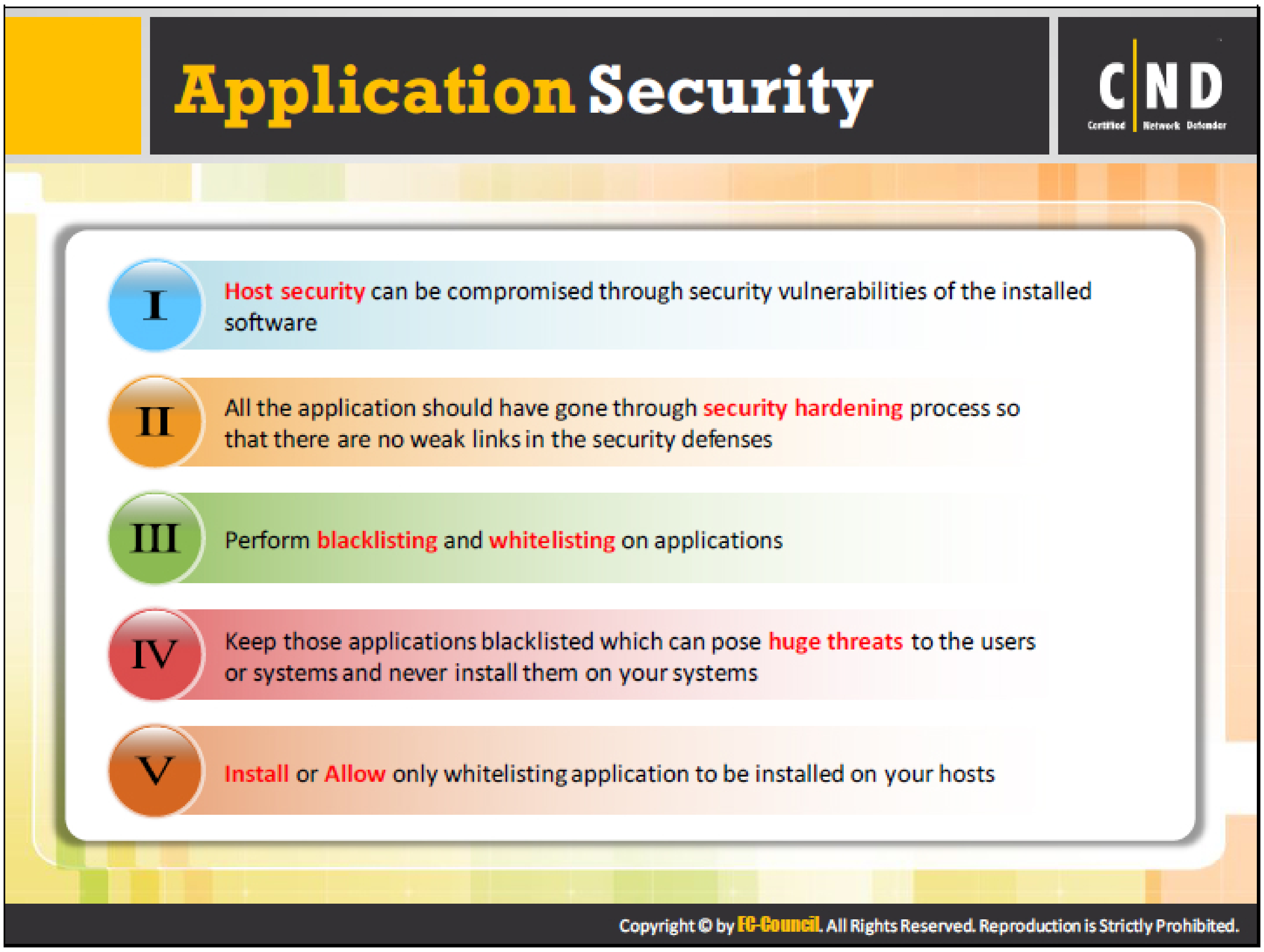
Kiwi Syslog® Server is a syslog server for IT administrators and network teams. Kiwi Syslog Server receives logs, displays, alerts on, and forwards syslog, SNMP trap, and Windows event log messages from routers, switches, firewalls, Linux and UNIX hosts, and Windows machines.

Kiwi Syslog Server also includes log archive management features that allow you to maintain compliance by securing, compressing, moving, and purging logs exactly as specified in your log retention policy.

Splunk Enterprise

Source: http://www.splunk.com

Splunk Enterprise is used to collect, analyze and act upon the untapped value of the big data generated by your technology infrastructure, security systems and business applications—giving you the insights to drive operational performance and business results. It collects and indexes data regardless of format or location logs, clickstreams, sensors, stream network traffic, web servers, custom applications, hypervisors, social media, and cloud services.



Application Security

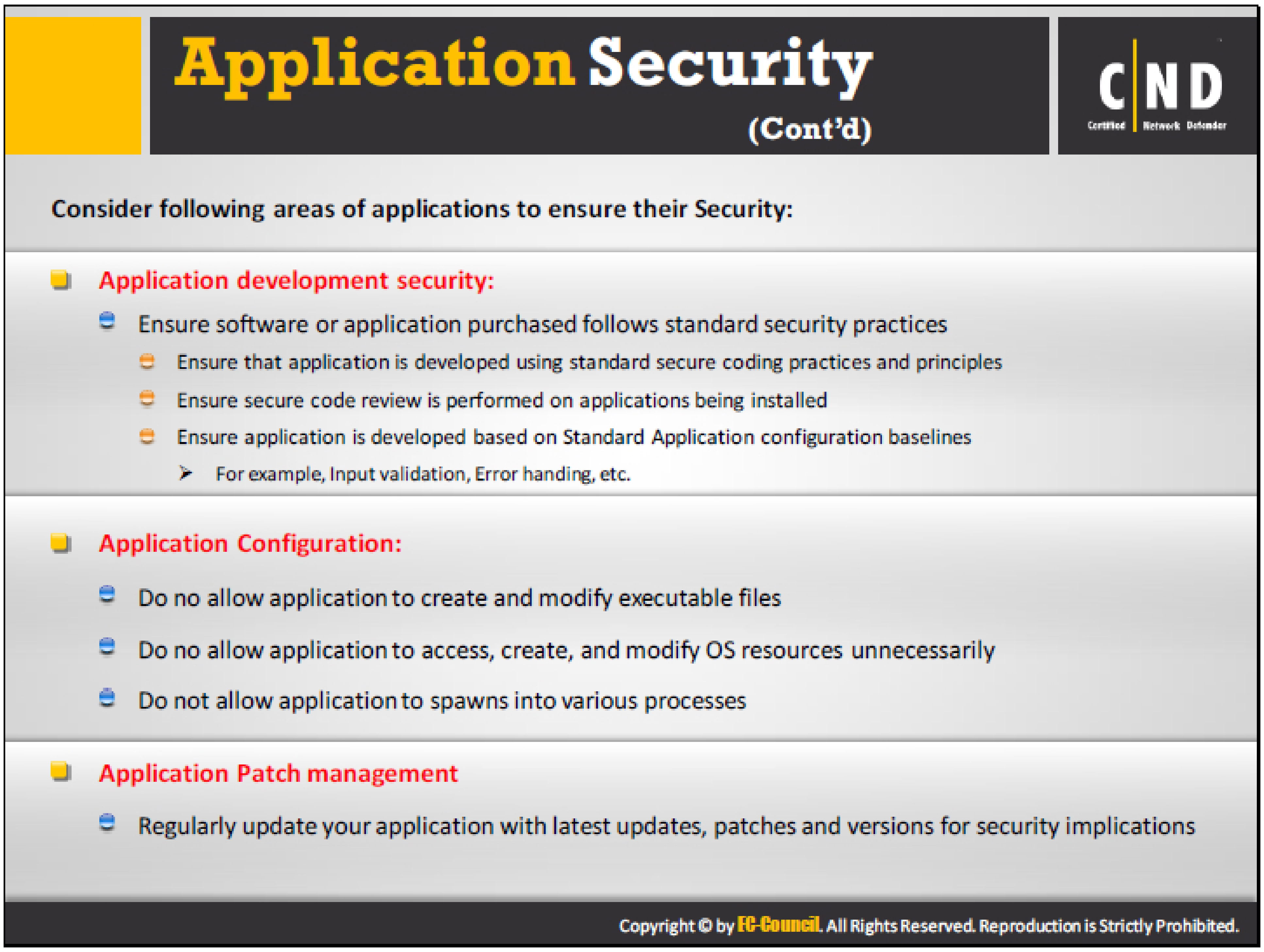
I. **Host security** can be compromised through security vulnerabilities of the installed software

II. All the application should have gone through **security hardening** process so that there are no weak links in the security defenses

III. Perform **blacklisting** and **whitelisting** on applications

IV. Keep those applications blacklisted which can pose **huge threats** to the users or systems and never install them on your systems

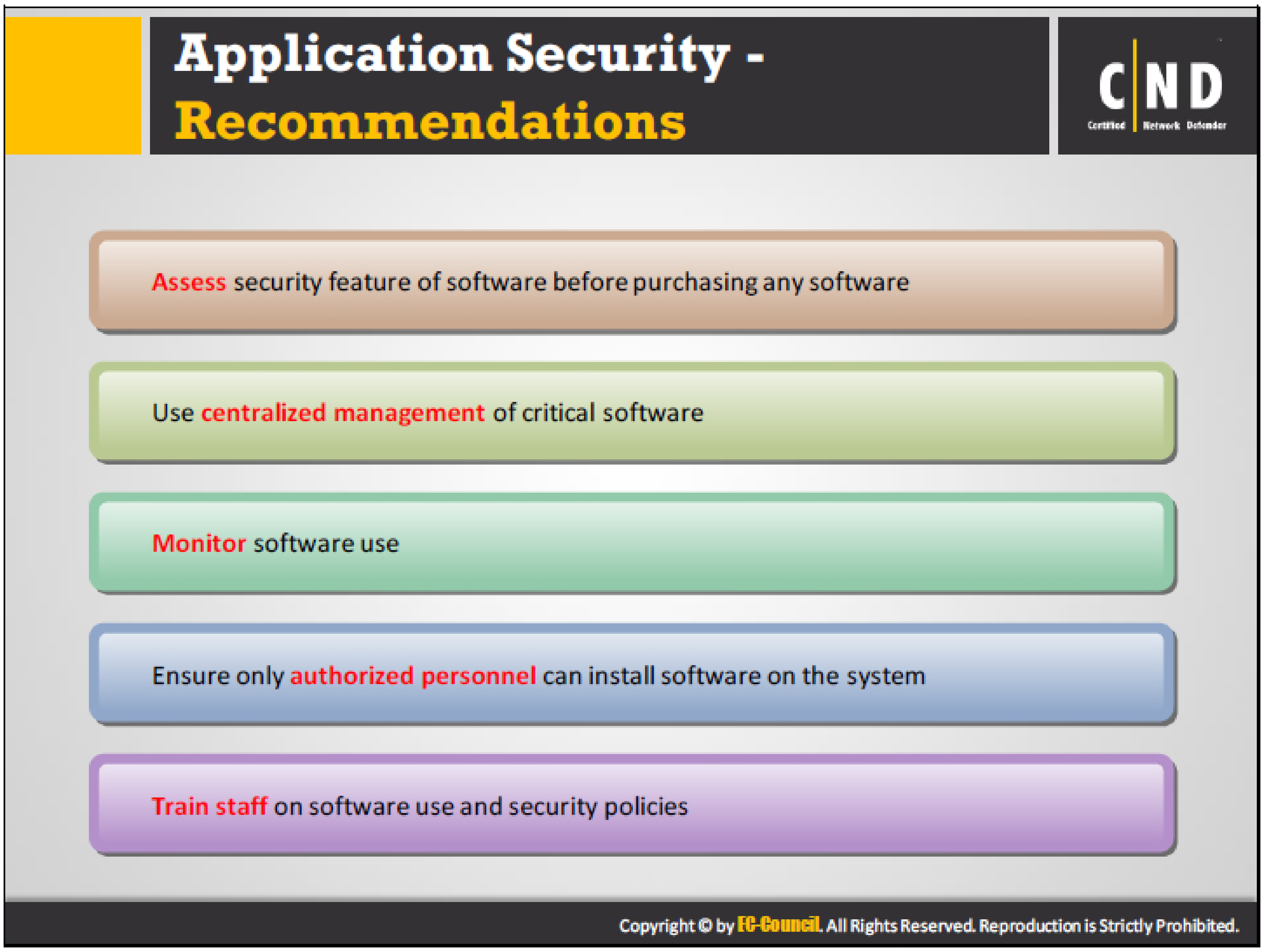
V. **Install** or **Allow** only whitelisting application to be installed on your hosts



Application Security (Cont'd)

Consider following areas of applications to ensure their Security:

- **Application development security:**
  - Ensure software or application purchased follows standard security practices
    - Ensure that application is developed using standard secure coding practices and principles
    - Ensure secure code review is performed on applications being installed
    - Ensure application is developed based on Standard Application configuration baselines
      - For example, Input validation, Error handing, etc.
- **Application Configuration:**
  - Do no allow application to create and modify executable files
  - Do no allow application to access, create, and modify OS resources unnecessarily
  - Do not allow application to spawns into various processes
- **Application Patch management**
  - Regularly update your application with latest updates, patches and versions for security implications



Application Security - Recommendations

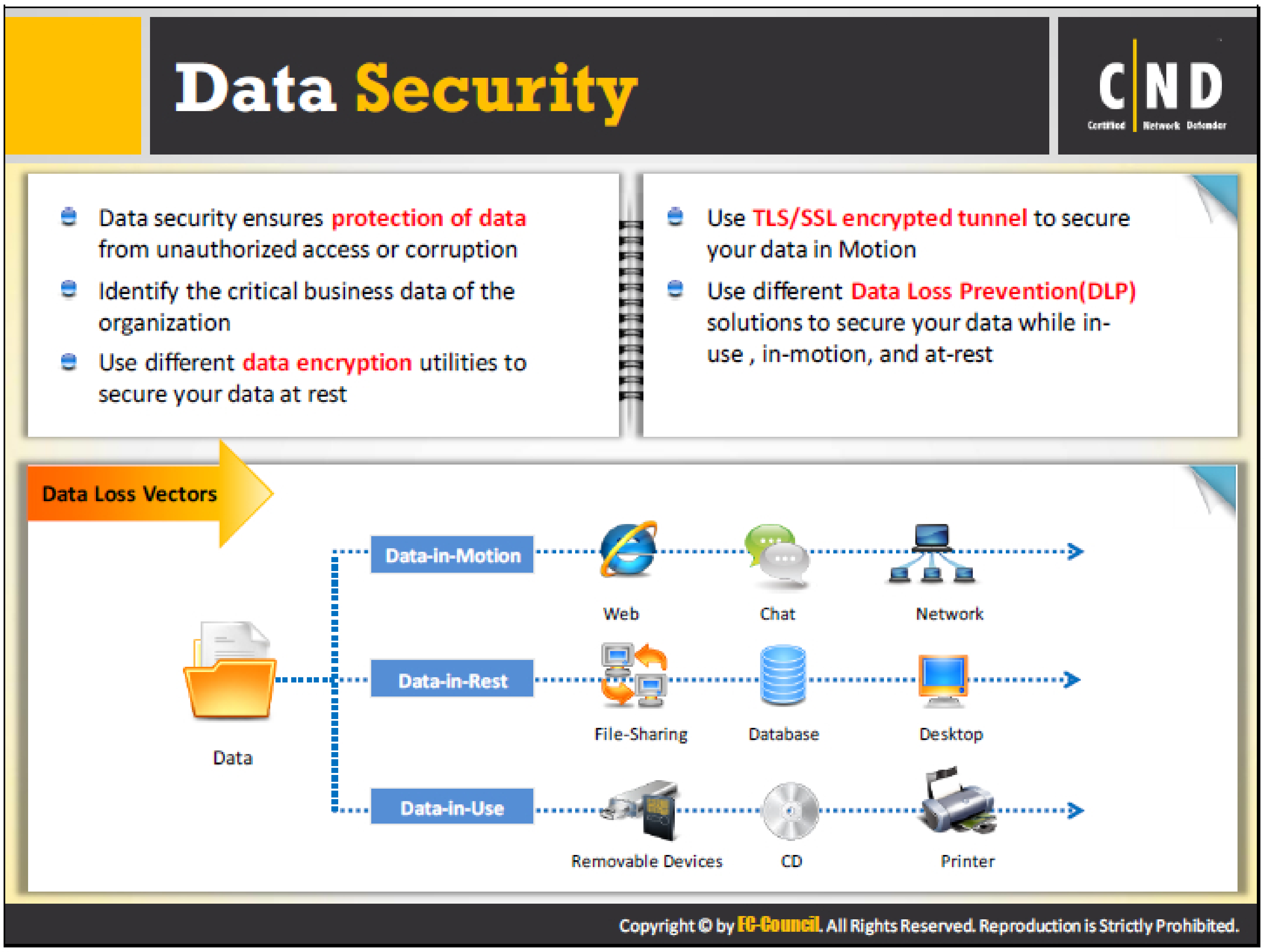
CND
Certified Network Defender

- Assess security feature of software before purchasing any software
- Use centralized management of critical software
- Monitor software use
- Ensure only authorized personnel can install software on the system
- Train staff on software use and security policies

Application security plays an important role in host security. An outdated or insecure application installed on a system, will pose a serious security threat and affect network security as a result. Administrators should ensure the security of an application before installing it on the system. Applications should be installed using the installation guide provided by the vendor. Administrators should change the default password of an application, if it is already set and then change the password at regular intervals. Administrators should not download and install applications from untrusted sources or third-party sites. Installing applications such as these, only adds risk to host security. Untrusted sources may hide malware inside these applications to compromise your system. Administrators should ensure that applications are using strong encryption algorithms when handling an organization's data when at rest and in transit. Monitor vendor sites for new updates and patches for your applications. Organizations need to continuously monitor their applications for vulnerabilities, to reduce the amount of potential risk and to maintain the security of the application. Strategies will differ between organizations, the main concerns are still the same. Secure the applications on the network.

The following points must be considered when securing applications on a system:

- Sensitive organizational information.
- Users accessing applications and access permissions provided to each user.
- Existing application vulnerabilities.
- Application risk factors and the corresponding countermeasures.



Data Security

- Data security ensures protection of data from unauthorized access or corruption
- Identify the critical business data of the organization
- Use different data encryption utilities to secure your data at rest

- Use TLS/SSL encrypted tunnel to secure your data in Motion
- Use different Data Loss Prevention(DLP) solutions to secure your data while in-use , in-motion, and at-rest

Data Loss Vectors

Data security is the main concern for many organizations, irrespective of their size. Data security ensures protective measures are applied to computers, databases and websites. A few examples of data security are hardware/software encryption, data backup and data masking. Organizations should ensure various levels of business data security.

Data Security at Rest

Data at rest refers to inactive data stored in digital form at a physical location. It includes archived or reference data which never changes. Data at rest does not include data moving through the network.

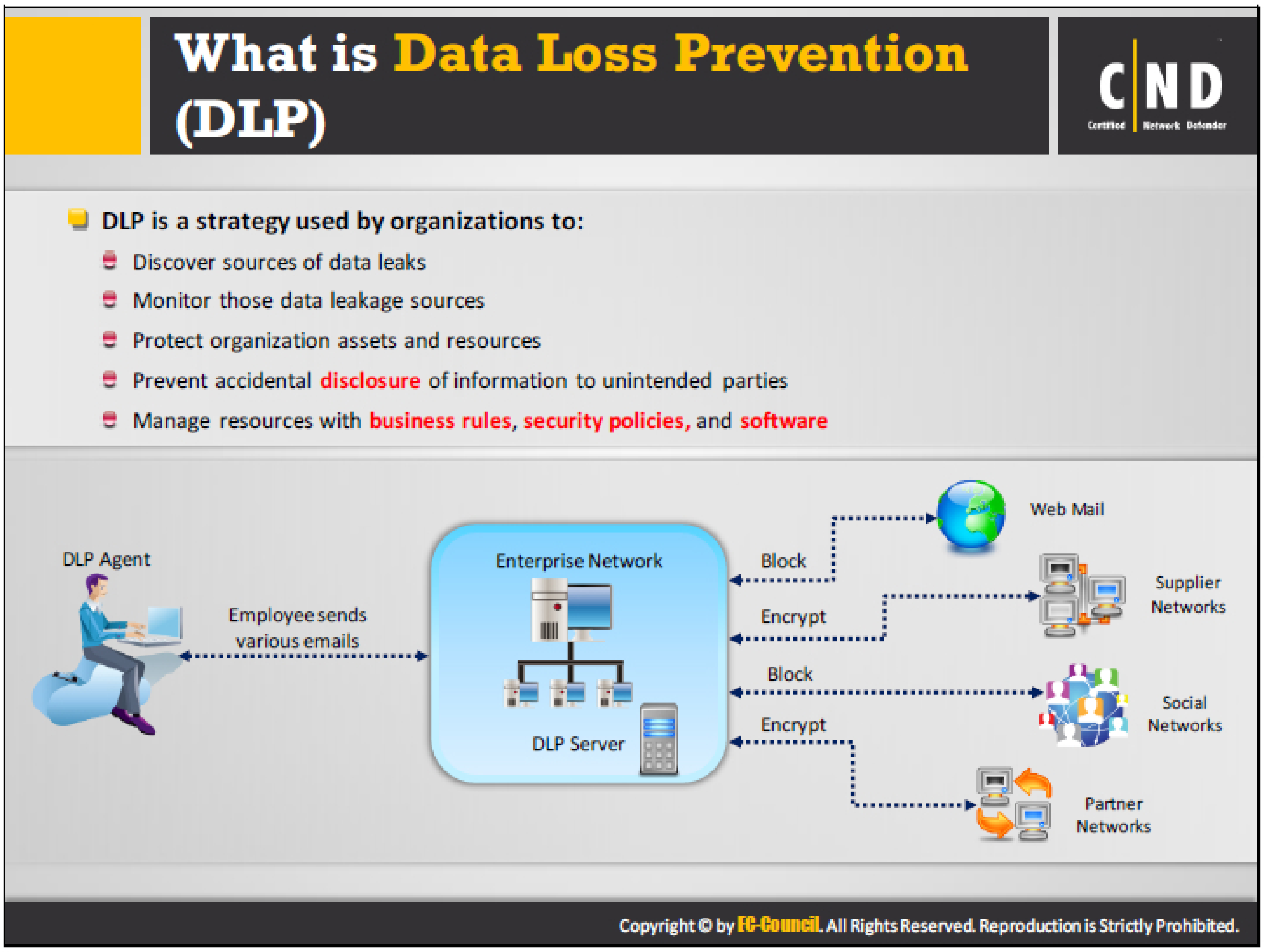
Data at rest encryption, protects the data using encryption. The process of encryption preserves and/or protects the data stored in a particular location. Organizations can completely depend on an encryption process for their data security. The process of encryption applies to both structured and unstructured data. network administrators need to constantly check the encryption mechanisms used for protecting data. The encryption of data at rest includes encryption methods such as AES and RSA. The data needs to be encrypted even in the failure of access controls. Keep the encryption keys at a separate location and make sure the keys are updated constantly. A data federation is another method used for protecting data at rest from unauthorized access.

Data Security in Transit

Data in transit can traverse the network and this gives attackers additional access opportunities to the data. Organizations can protect their confidential data using encryption two types mechanisms: SSL and TLS. SSH replaces TELNET and SFTP replaces FTP. Any protocols using SSL/TLS use certificates to exchange public keys and public keys to exchange private keys. Similarly, a session key uses asymmetric encryption and a certificate for exchange. Symmetric encryption uses the same session key for secure, fast encryption and decryption. Network traffic authentication requires encryption for data in transit. Encryption is not a mandatory mechanism for a public facing website. However, encryption can play a role if the organization wants users to logon before accessing their web pages. This protects the privacy and data of the user.

Data Loss Prevention (DLP)

To confirm users do not send or use sensitive data outside the organization, enable DLP. DLP controls what data users can send through the network. DLP uses different rules to classify what data is critical and sensitive in an organization.



What is Data Loss Prevention (DLP)

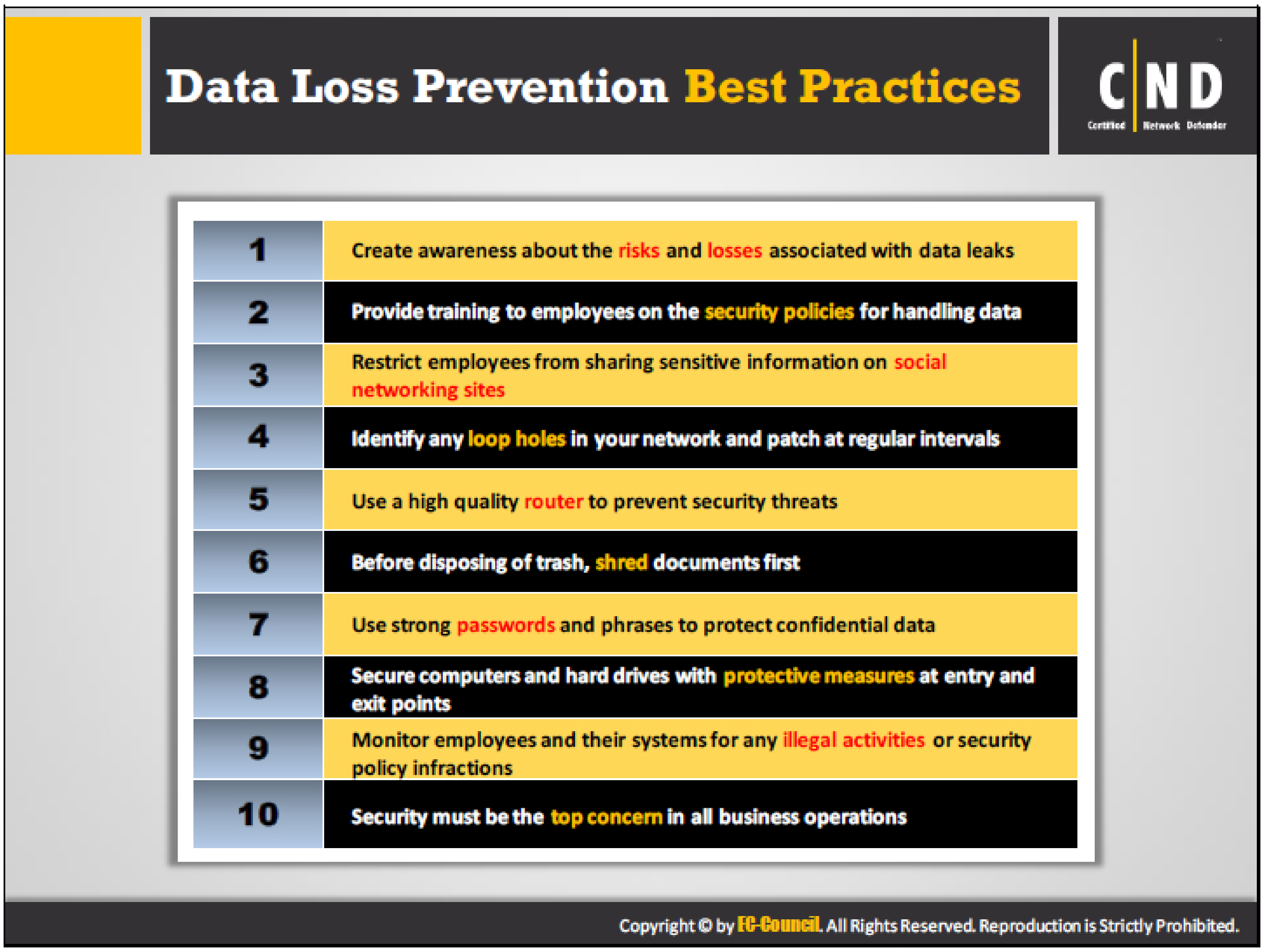
- **DLP is a strategy used by organizations to:**
  - Discover sources of data leaks
  - Monitor those data leakage sources
  - Protect organization assets and resources
  - Prevent accidental **disclosure** of information to unintended parties
  - Manage resources with **business rules**, **security policies**, and **software**

Data loss prevention (DLP) does not allow users to send confidential corporate data outside the organization. The term is used to describe software products that help a network administrator control what data end users can transfer. DLP rules block the transfer of any confidential information across external networks. This controls any unauthorized access to company information and prevents anyone from sending malicious programs to the organization.

Implement DLP software according to the organizational rules set by management. This prevents accidental/malicious data leaks and loss. If an employee tries to forward or even upload company data on cloud storage or even on a blog, the action will be denied by the system.

A DLP policy is adopted by management when internal threats to a company are detected. Data loss prevention is a policy to ensure that none of its employees send sensitive information outside the organization. New emerging DLP tools not only, prevent the loss of data, but also monitor and control irregular activities from occurring on the system.

There are DLP products available that help administrators determine what data users transfer. DLP products are also known as data leak prevention, information loss prevention or extrusion prevention products.

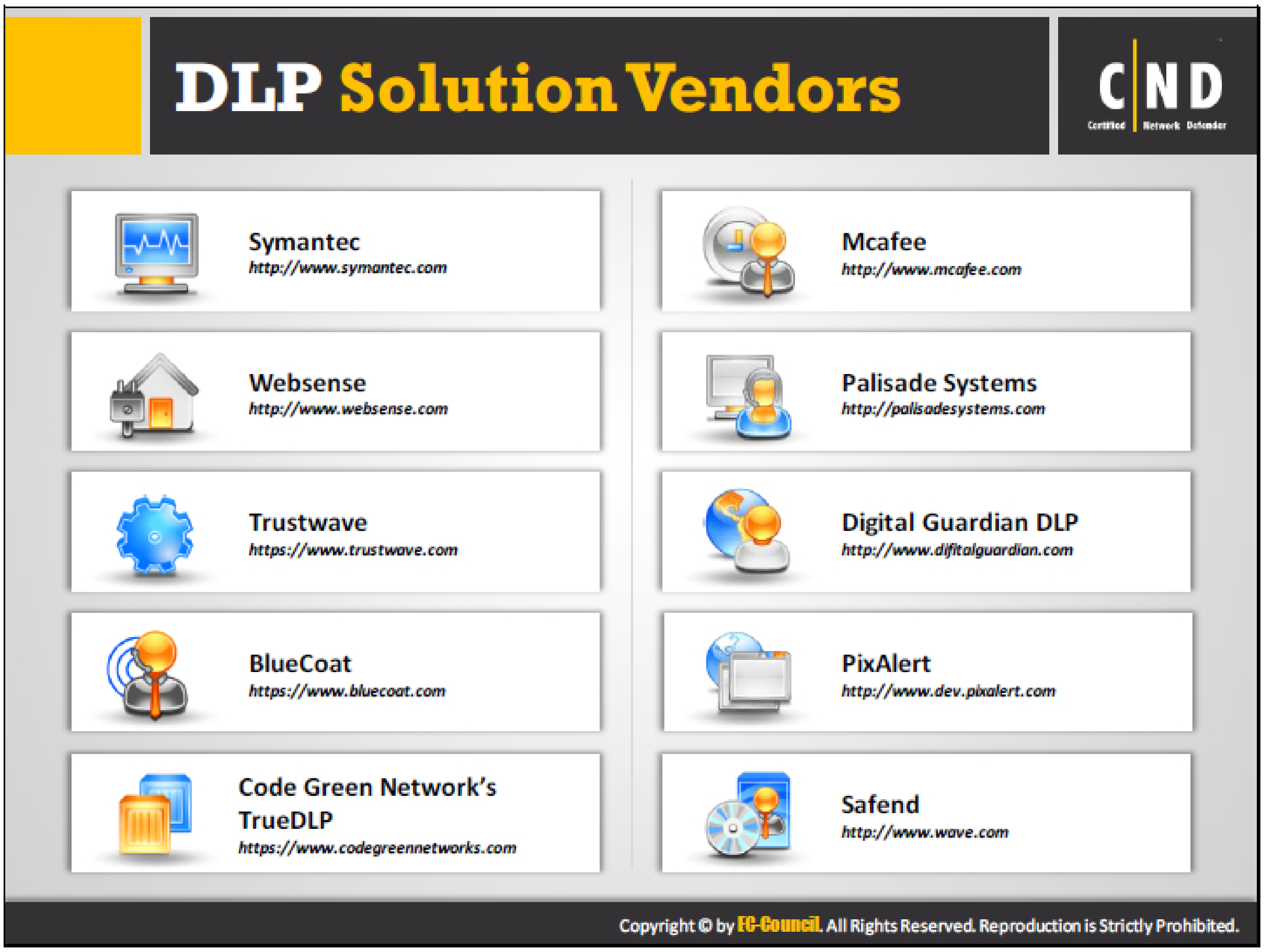


Data Loss Prevention Best Practices

1	Create awareness about the risks and losses associated with data leaks
2	Provide training to employees on the security policies for handling data
3	Restrict employees from sharing sensitive information on social networking sites
4	Identify any loop holes in your network and patch at regular intervals
5	Use a high quality router to prevent security threats
6	Before disposing of trash, shred documents first
7	Use strong passwords and phrases to protect confidential data
8	Secure computers and hard drives with protective measures at entry and exit points
9	Monitor employees and their systems for any illegal activities or security policy infractions
10	Security must be the top concern in all business operations

Data loss prevention best practices are:

- Identify the business need for implementing a DLP solution in an organization.
- Ensure the DLP solution supports various data formats.
- Determine the type of DLP required based on the type of data protection needed.
- Always pay close attention while deploying a DLP, as any small mistake in the implementation will impact data protection.
- DLP should be able to mitigate any false positives.
- Regular risk profile updates and an organization needs to ensure DLP incidents are documented.
- Provide security policy training to employees.
- Restrict employees from sharing sensitive information on social networking sites.



DLP Solution Vendors

Symantec
http://www.symantec.com

Mcafee
http://www.mcafee.com

Websense
http://www.websense.com

Palisade Systems
http://palisadesystems.com

Trustwave
https://www.trustwave.com

Digital Guardian DLP
http://www.difitalguardian.com

BlueCoat
https://www.bluecoat.com

PixAlert
http://www.dev.pixalert.com

Code Green Network's TrueDLP
https://www.codegreennetworks.com

Safend
http://www.wave.com

Symantec

Source: https://www.symantec.com

Symantec DLP keeps track, secures your confidential data and ensures its safety, wherever it lives: in the cloud, on-premises, or on mobile devices. It helps you keep data safe on Windows and Mac endpoints by performing local scanning and real-time monitoring. It monitors confidential data that is being downloaded, copied or transmitted to or from laptops and desktops, through email or cloud storage. It uses a single web-based console to define data loss policies, review and remediate incidents, and perform system administration across all of your endpoints, mobile devices, cloud-based services, and on premise network and storage systems.

Websense

Source: http://www.websense.com

Websense Data Security Suite contains three modules Data Security Gateway, Data Discover, and Data Endpoint. It provides a single intuitive, web-based interface for management and reporting of Websense web, email and data security solutions.

Trustwave

Source: https://www.trustwave.com

Trustwave Data Loss Prevention helps enterprises discover, monitor and secure data at rest, in motion, and in use to prevent exfiltration and ensure regulatory compliance. It analyzes all web-based communication and attachments, including email, instant messenger, P2P file sharing, blogs, social media, FTP and Telnet, for violations of an organization's governance, compliance and acceptable-use policies. Automatically blocks HTTP, HTTPS and FTP traffic violating compliance policies. It can investigate data at rest to find and protect sensitive information residing in the stored data. Discovery of sensitive data allows security teams to focus their initiatives on specific users and systems, and then implement the appropriate measures to meet compliance requirements.

BlueCoat

Source: https://www.bluecoat.com

Blue Coat Data Loss Prevention (DLP) enables you to detect and block potential data leaks quickly and accurately, all while achieving industry and regulatory compliance. With Blue Coat DLP, you can leverage powerful discovery capabilities to prevent sensitive, unsecured data from traveling across the network and winding up in the wrong hands.

Code Green Network's TrueDLP

Source: https://www.codegreennetworks.com

Code Green Networks' TrueDLP™ solution is comprised of Network DLP, Discovery DLP and Cloud DLP, and locates sensitive data resting on databases and network servers, including data in the cloud.

McAfee

Source: http://www.mcafee.com

McAfee Total Protection for Data Loss Prevention (DLP) safeguards intellectual property and ensures compliance by protecting sensitive data wherever it lives on premises, in the cloud, or at the endpoints. McAfee Total Protection for DLP is delivered through physical or virtual low-maintenance appliances and the McAfee ePolicy Orchestrator platform for streamlined deployment, management, updates, and reports.

Palisade Systems

Source: http://palisadesystems.com

Palisade DLP provides a simple, all-in-one, cost-effective approach to data loss prevention (DLP), which enables organizations to:

- **Monitor**: Palisade monitors all traffic and data leaving the network making you aware of what is happening with your most critical data
- **Analyze**: Palisade inspects and analyzes documents for protected/confidential data to discover where sensitive data resides, in use, in motion or at rest.
- **Prevent**: Palisade prevents data loss using DLP enforcement, protocol management and web filtering and enforcing data protection policies to ensure secure treatment of data and proper adherence to company protocols.

Digital Guardian DLP

Source: *https://digitalguardian.com*

Digital Guardian DLP provides visibility and audit reporting of potentially unsecured data.

It uses patent-pending Database Record Matching™ detection to accurately locate and identify sensitive data at rest on endpoints and servers across your networks and cloud storage.

Automatic, configurable scanning of local and network shares using discovery specific inspection policies ensure sensitive content is discovered wherever it is located. Detailed audit logging and reports provide you with the information needed to demonstrate compliance, protect confidential information and reduce data loss risk.

PixAlert

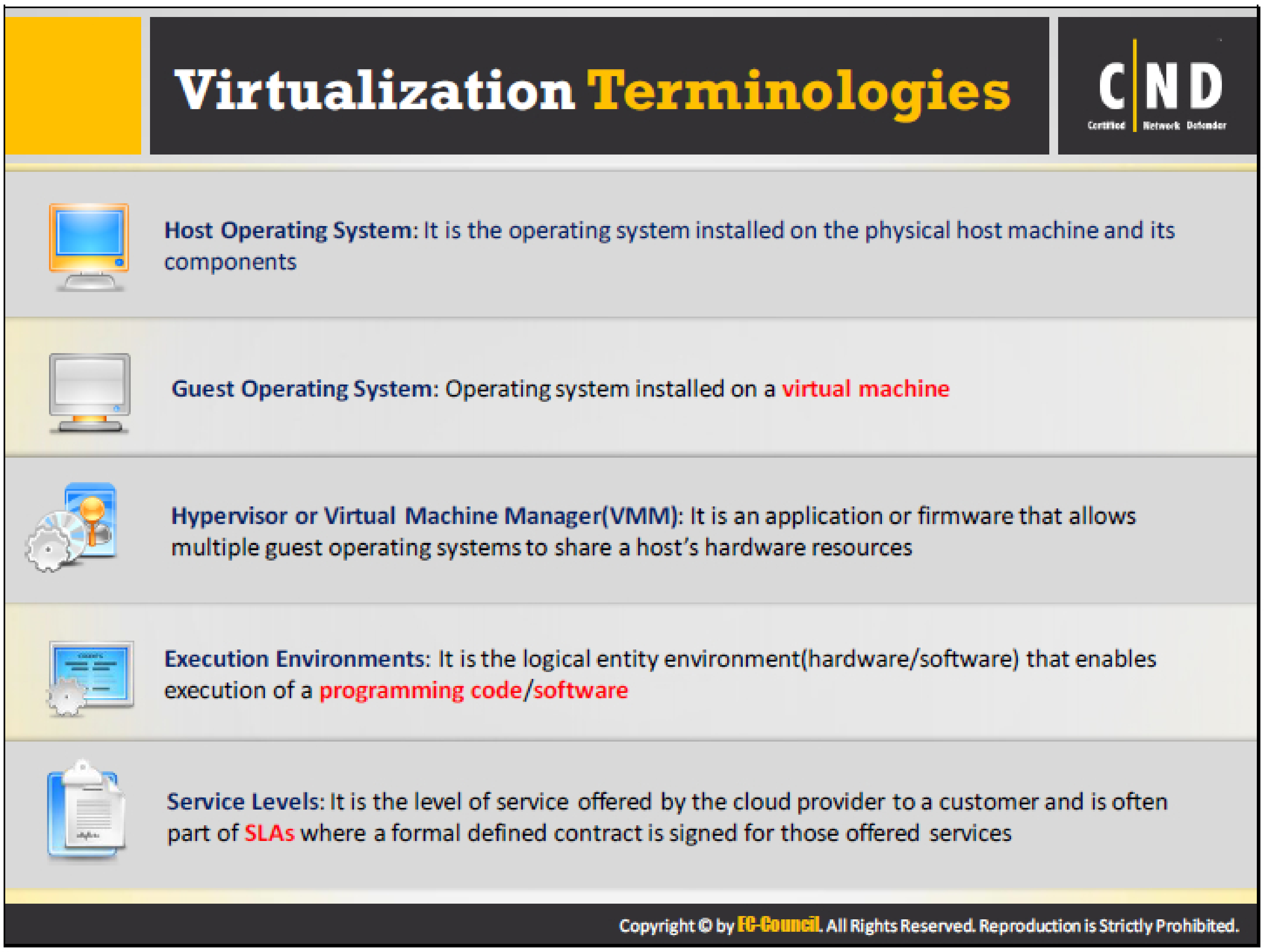
Source: *http://www.dev.pixalert.com*

Data Leakage Prevention (DLP) programs will effectively secure critical and sensitive data by discovering & identifying data at rest that needs to be protected. It helps networks discover and manage where critical data is located, monitoring and protecting networks and employees against dissemination and leakage of unsecure data.

Safend

Source: *https://www.wave.com*

The Wave Data Protection Suite goes wherever your devices go, on or off your network, online or offline. Which means it protects your data from the full range of modern risks: device theft, emails, flash drives, portable hot spots, hardware key loggers, etc.



Virtualization Terminologies

Host Operating System: It is the operating system installed on the physical host machine and its components

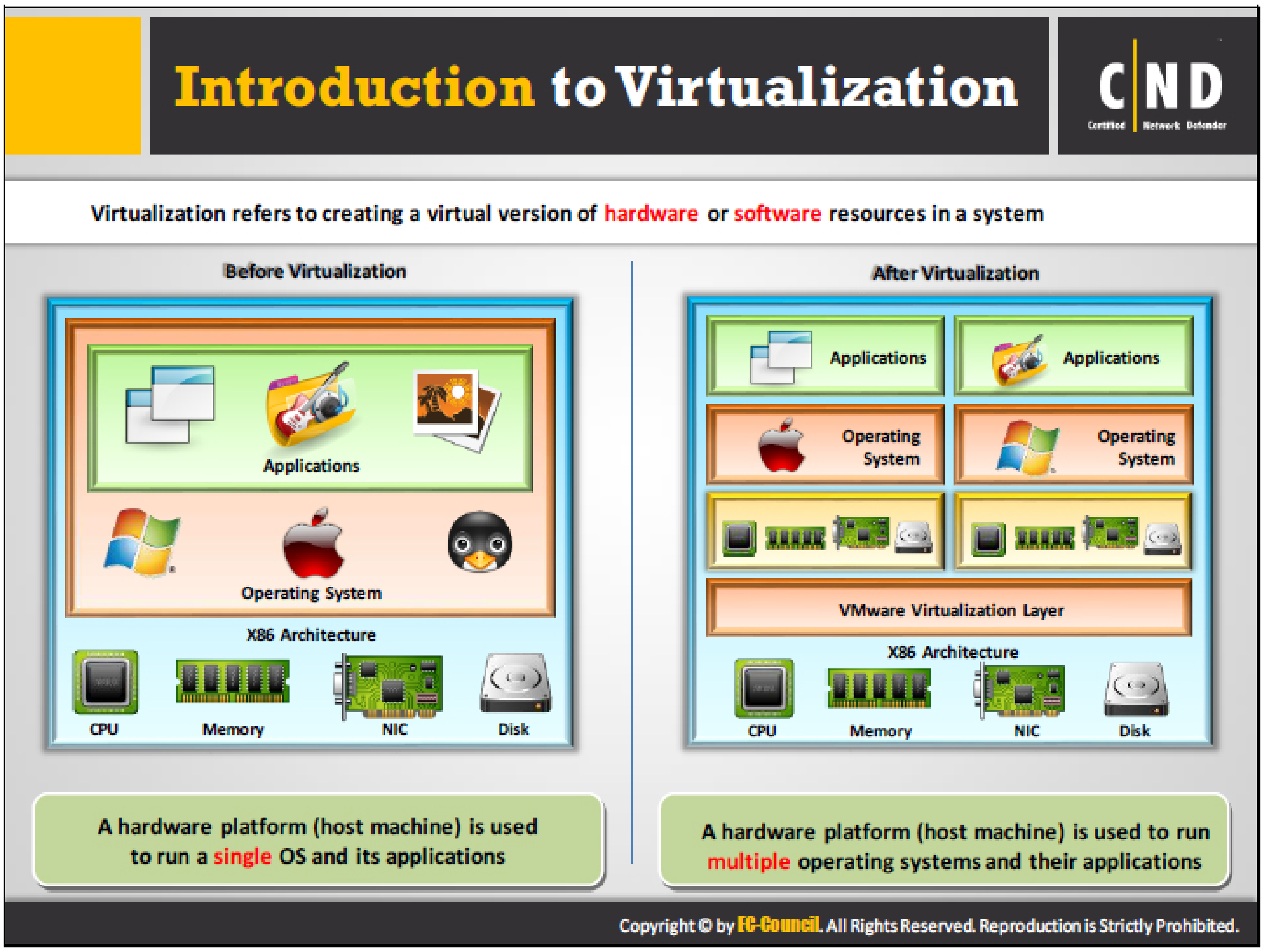
Guest Operating System: Operating system installed on a virtual machine

Hypervisor or Virtual Machine Manager(VMM): It is an application or firmware that allows multiple guest operating systems to share a host's hardware resources

Execution Environments: It is the logical entity environment(hardware/software) that enables execution of a programming code/software

Service Levels: It is the level of service offered by the cloud provider to a customer and is often part of SLAs where a formal defined contract is signed for those offered services

- **Host Operating System:** A Host Operating System is the OS installed physically on the computer hardware which seeks direct access to the hardware resources for computations. Resources it can access include processor, memory, Storage media etc.
- **Guest Operating System:** This is the operating system installed virtually on a host operating system. It is dependent on the host operating system for the computations and resource allocations.
- **Hypervisor or Virtual Machine Manager (VMM):** It is an application or firmware that allows multiple guest operating systems to share a host's hardware resources. It acts as middleware which allows the user to install a virtual operating system called 'Guest OS' on the 'Host OS'.
- **Execution Environments:** It is the logical entity environment (Software/Hardware) that enables execution of programming code/software. JVM (Java Virtual Machine) is the best example which acts as an execution environment for JAVA programs.
- **Service Levels:** A service level is a signed contract between the cloud provider and the cloud customer which lists all the services offered by the cloud provider to the customer. It also includes the terms and conditions between the two parties.



Introduction to Virtualization

Virtualization refers to creating a virtual version of hardware or software resources in a system

A hardware platform (host machine) is used to run a single OS and its applications

A hardware platform (host machine) is used to run multiple operating systems and their applications

Virtualization offers computing, storage and networking hardware. Virtualization refers to the separation of the services or requests from the physical processes. The mechanism of virtualization has enabled IT managers to group resources across the enterprise providing better management of those resources.

1. **Before Virtualization:** The hardware infrastructure (host machine) runs a single operating system with all its applications.

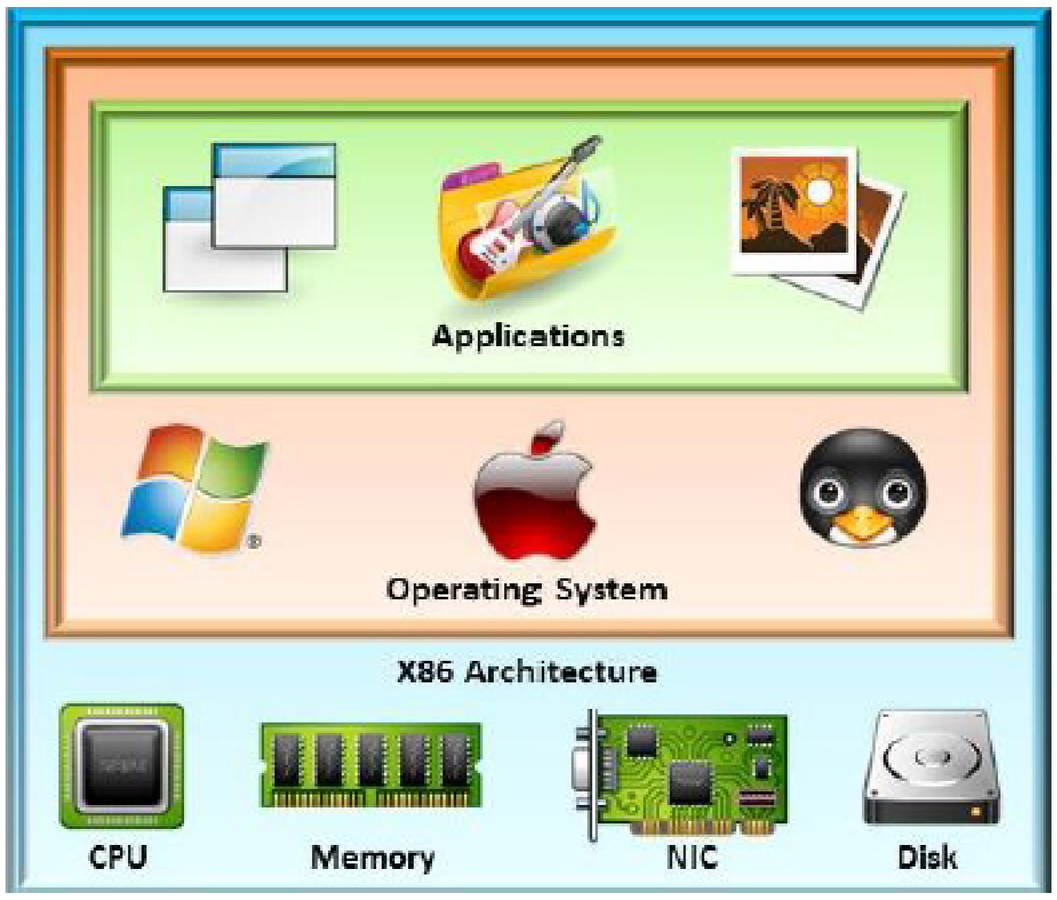


FIGURE 6.29: Before Virtualization

In the figure above, a single instance of an operating system with a set of applications is completely utilizing the given 32-bit hardware infrastructure. 'Host OS' directly interacts with the hardware to request system resources.

2. **After Virtualization:** A hardware platform (host machine) is used to run multiple sets of Virtual operating systems and their applications.

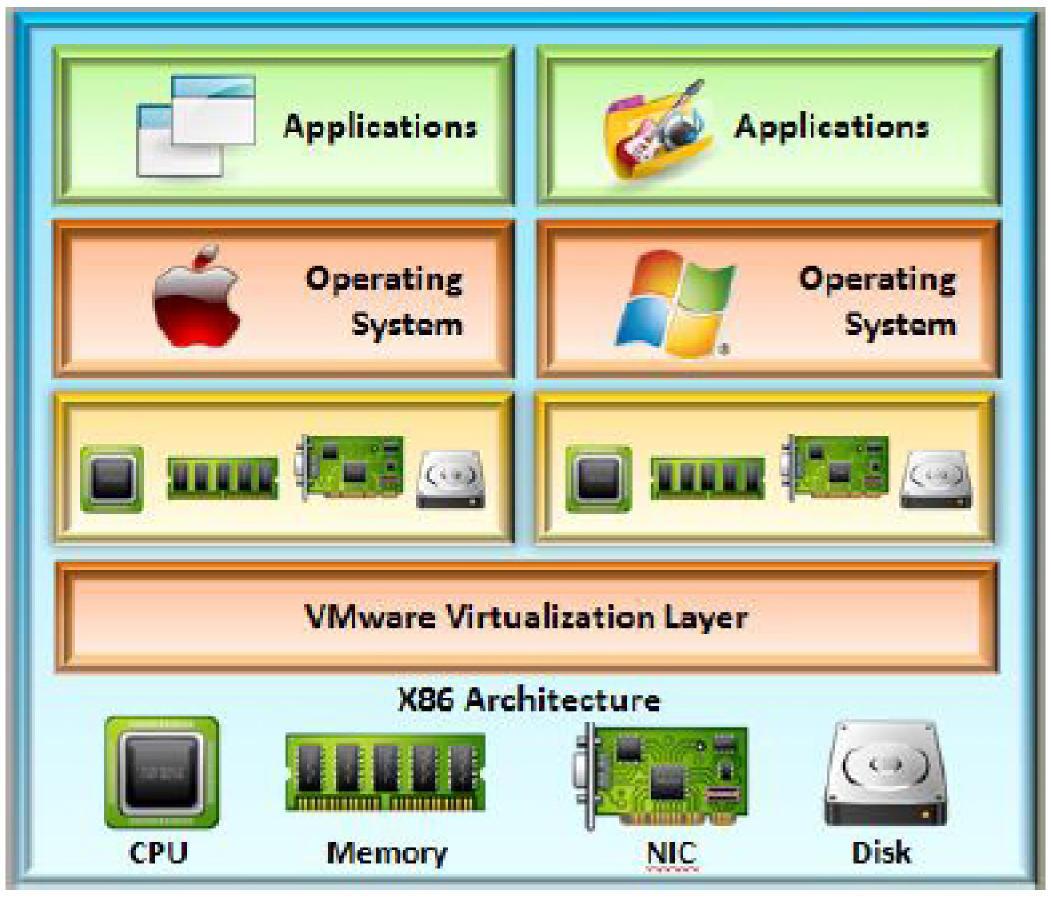


FIGURE 6.30: After Virtualization

In the figure above, the virtualization layer acts as middleware between the operating system installed and the computer hardware. It logically partitions the hardware resources based on the requests received from the host and the guest operating systems. The host OS directly interacts with the computer hardware but the guest OS interacts through the Virtualization Layer. Different types of virtualization techniques are:

1. **Full Virtualization:** The guest OS is not aware that it is running in a virtualized environment. It sends commands to Virtual Machine Manager (VMM) interact with the computer hardware. The VMM then translates the command to binary instructions and forwards it to the host OS. The resources are allocated to the guest OS through the VMM.

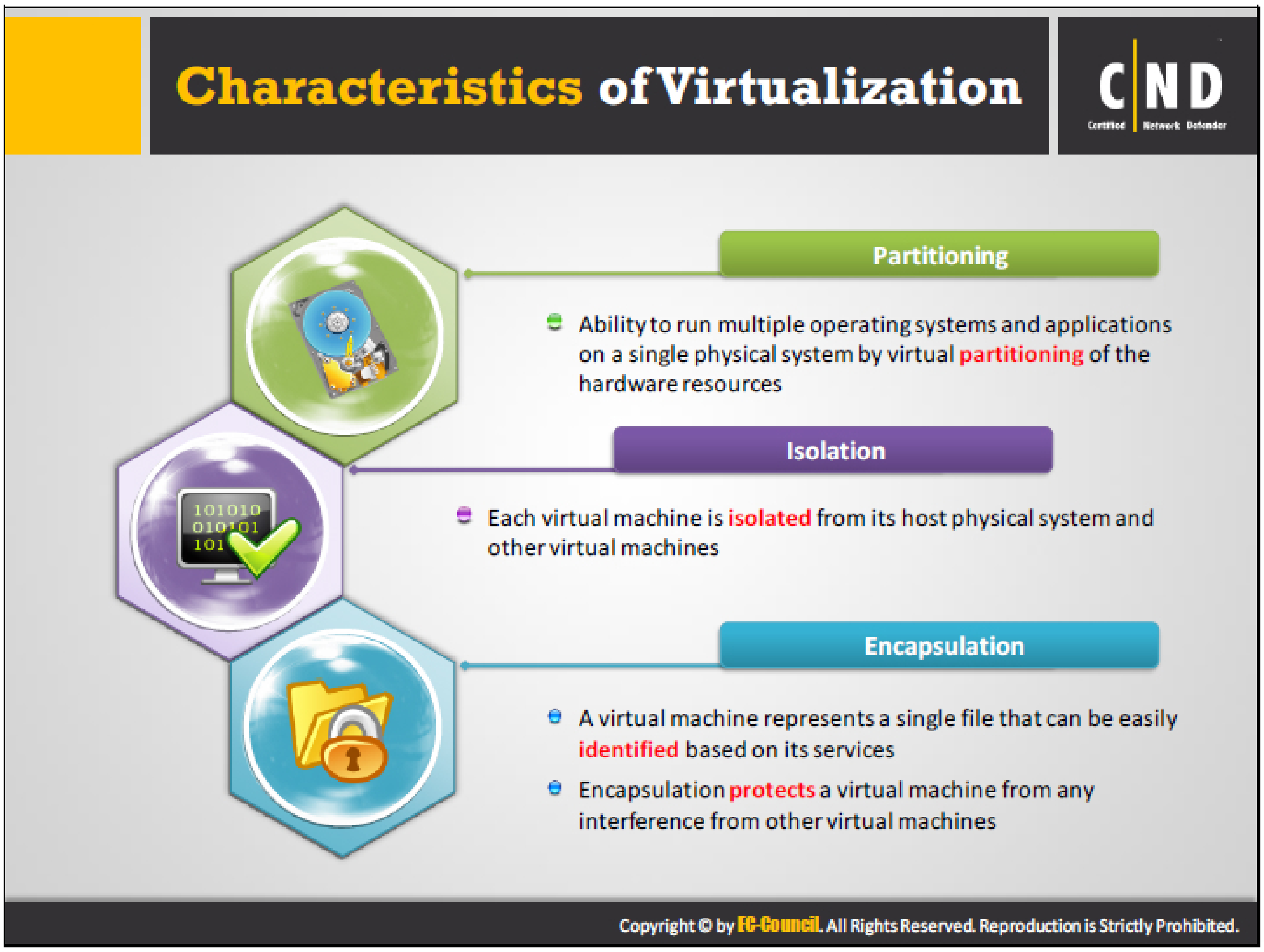
2. **OS assisted Virtualization or Para Virtualization:** In this type of virtualization, the guest OS is aware of the virtual environment in which it is running and communicates with the host machines requesting for the resources. The commands are translated into binary code for the computer hardware. The VMM is not involved in the request and response operations.

3. **Hardware assisted Virtualization:** Modern microprocessor architecture has special instructions to aid the virtualization of hardware. These instructions allow the guest to execute privileged instructions directly on the processer. The operating system makes the system calls behave like a user program.

4. **Hybrid Virtualization:** In this type of virtualization, the guest OS uses the functionality of Para Virtualization and uses the Virtual Machine Manager (VMM) for binary translation to different types of hardware resources.

While designing a virtual environment, the levels involved in the application are:

- **Storage Device Virtualization:** This is the virtualization applied on storage devices such as data striping and data mirroring. RAID is a good example of storage virtualization.
- **File System Virtualization:** This type of virtualization provides complete virtualization to the data for sharing and protection within the software at this level. Virtualized data pools manipulate the files and the data based on user demand.
- **Server Virtualization:** Server level virtualization enables management to partition or virtualize the server's operating system environment. Logical partitioning of the server's hard drive is involved in the server virtualization.
- **Fabric Virtualization:** This level of virtualization makes the virtual devices independent of the physical computer hardware. It creates a massive pool of storage areas for different virtual machines running on the hardware. Virtualization uses Storage Area Network (SAN) technology to perform fabric level virtualization.



Characteristics of Virtualization

Partitioning

- Ability to run multiple operating systems and applications on a single physical system by virtual partitioning of the hardware resources

Isolation

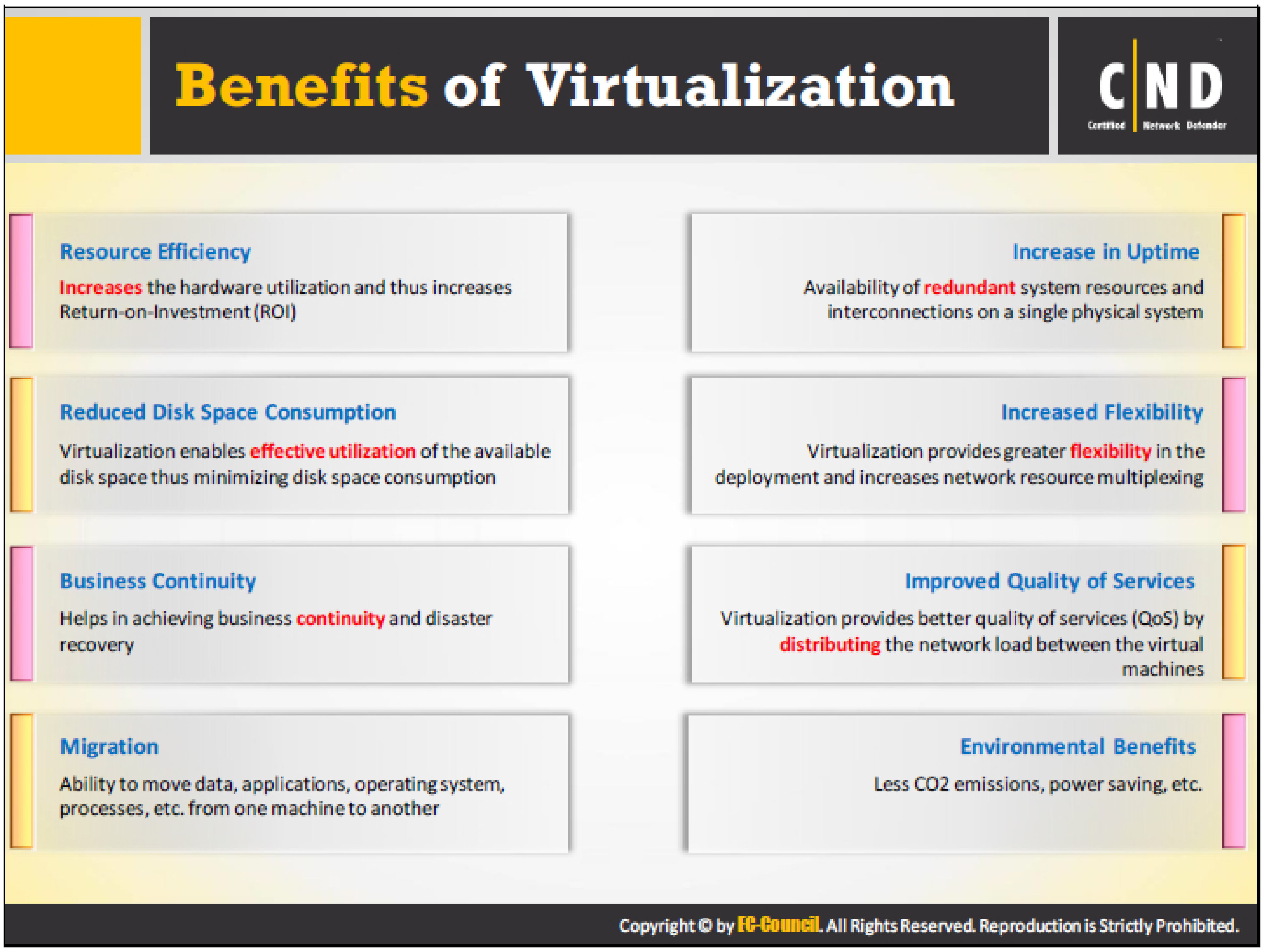
- Each virtual machine is isolated from its host physical system and other virtual machines

Encapsulation

- A virtual machine represents a single file that can be easily identified based on its services
- Encapsulation protects a virtual machine from any interference from other virtual machines

Virtualization has the following characteristics:

- **Partitioning:** It is the ability to run multiple operating system instances with their applications on a single physical system, by virtually partitioning the hardware resources and the resources are allocated to handle host and guest requests.
- **Isolation:** Each virtual machine is isolated from its host physical system and other virtual machines. This characteristic of virtualization prevents the effects of actions performed by one virtual machine from affecting the other machines.
- **Encapsulation:** A virtual machine represents a single file used for identification based on its services. Encapsulation protects a virtual machine from interference from the other virtual machines.



Benefits of Virtualization

CND
Certified Network Defender

Resource Efficiency
Increases the hardware utilization and thus increases Return-on-Investment (ROI)

Increase in Uptime
Availability of redundant system resources and interconnections on a single physical system

Reduced Disk Space Consumption
Virtualization enables effective utilization of the available disk space thus minimizing disk space consumption

Increased Flexibility
Virtualization provides greater flexibility in the deployment and increases network resource multiplexing

Business Continuity
Helps in achieving business continuity and disaster recovery

Improved Quality of Services
Virtualization provides better quality of services (QoS) by distributing the network load between the virtual machines

Migration
Ability to move data, applications, operating system, processes, etc. from one machine to another

Environmental Benefits
Less CO2 emissions, power saving, etc.

Virtualization provides:

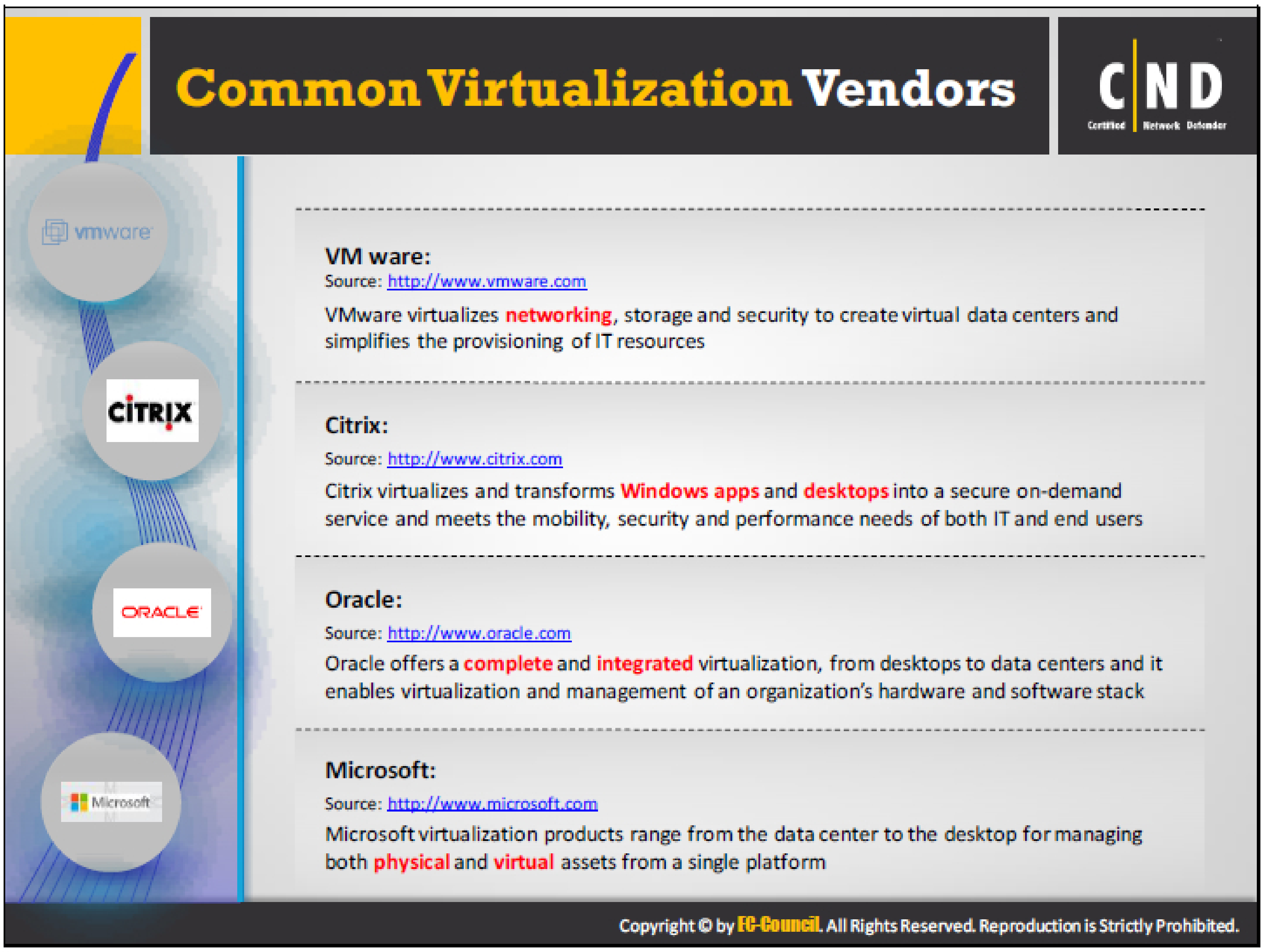
- **A cost-effective solution for the central data hub:** Replacing the physical hardware with virtual machines can actually cut down the cost of purchasing more hardware, increasing the space in the server room. Too many servers can emit a lot of heat leading to a server crash.
- **A time efficient option for the IT infrastructure:** The use of virtual machines can reduce the time it takes for installing computer components in an organization. The concept of virtualization enables the network administrator perform tests on the software without consuming time and resources.
- **Back up the Servers:** Virtualization ensures the complete restoration of the network at a faster rate. The use of virtual machines reduces the time it takes, by the physical hardware, to perform recovery.

The virtualization process enables users in an organization to use different platforms in a single machine according to their needs. It provides continuous transition from one operating system to another in the same machine.

The following are the benefits of virtualization technology:

- Centralized storage in virtual machines prevents the loss of data.
- If the virtual machines are remote, then only one application present in one VM is attacked.

- The VM allows secure sharing of sensitive information.
- An attacked VM can be rolled back to a state prior to the attack.
- Virtualization improves the physical security due to the presence of a few physical devices and a few data centers.
- Provides better event incident handling.
- Provides better methods for effective handling of VM's.



Common Virtualization Vendors

CND
Certified Network Defender
vmware
CITRIX
ORACLE
Microsoft

VM ware:

Source: http://www.vmware.com

VMware virtualizes networking, storage and security to create virtual data centers and simplifies the provisioning of IT resources

Citrix:

Source: http://www.citrix.com

Citrix virtualizes and transforms Windows apps and desktops into a secure on-demand service and meets the mobility, security and performance needs of both IT and end users

Oracle:

Source: http://www.oracle.com

Oracle offers a complete and integrated virtualization, from desktops to data centers and it enables virtualization and management of an organization's hardware and software stack

Microsoft:

Source: http://www.microsoft.com

Microsoft virtualization products range from the data center to the desktop for managing both physical and virtual assets from a single platform

VMware

Source: *http://www.vmware.com*

VMware virtualizes computing, from the data center to the cloud to mobile devices, to help customers be more agile, responsive, and profitable.

It offers services such as:

- VMware vCloud Suite: vCloud Suite is a complete kit used for developing and managing a private cloud infrastructure effectively.
- VMware vSphere: VSphere virtualization enables creation of a cloud infrastructure and virtually collaborates all the server related resources.
- Horizon View: Horizon view is a virtual desktop service which offers remote access to different resources available to the users under a common platform.
- VMware Fusion: Fusion enables Mac users to run Windows based applications without compatibility issues.
- VMware Workstation: Workstation enables the user to run multiple virtual machines from a single desktop.
- VMware VCenter Operations Management Suite : Operations management suite efficiently manages all the services for their user and ensures quality service.

Citrix

Source: *https://www.citrix.com*

Citrix securely delivers Windows, Linux, web and SaaS apps plus full virtual desktops to any device. Citrix solutions for application and desktop virtualization can help your business increase productivity, enhance security and reduce costs.

ORACLE

Source: *http://www.oracle.com*

Oracle offers the virtualization, from desktop to the data center. Oracle virtualization enables you to virtualize and manage your full hardware and software stack.

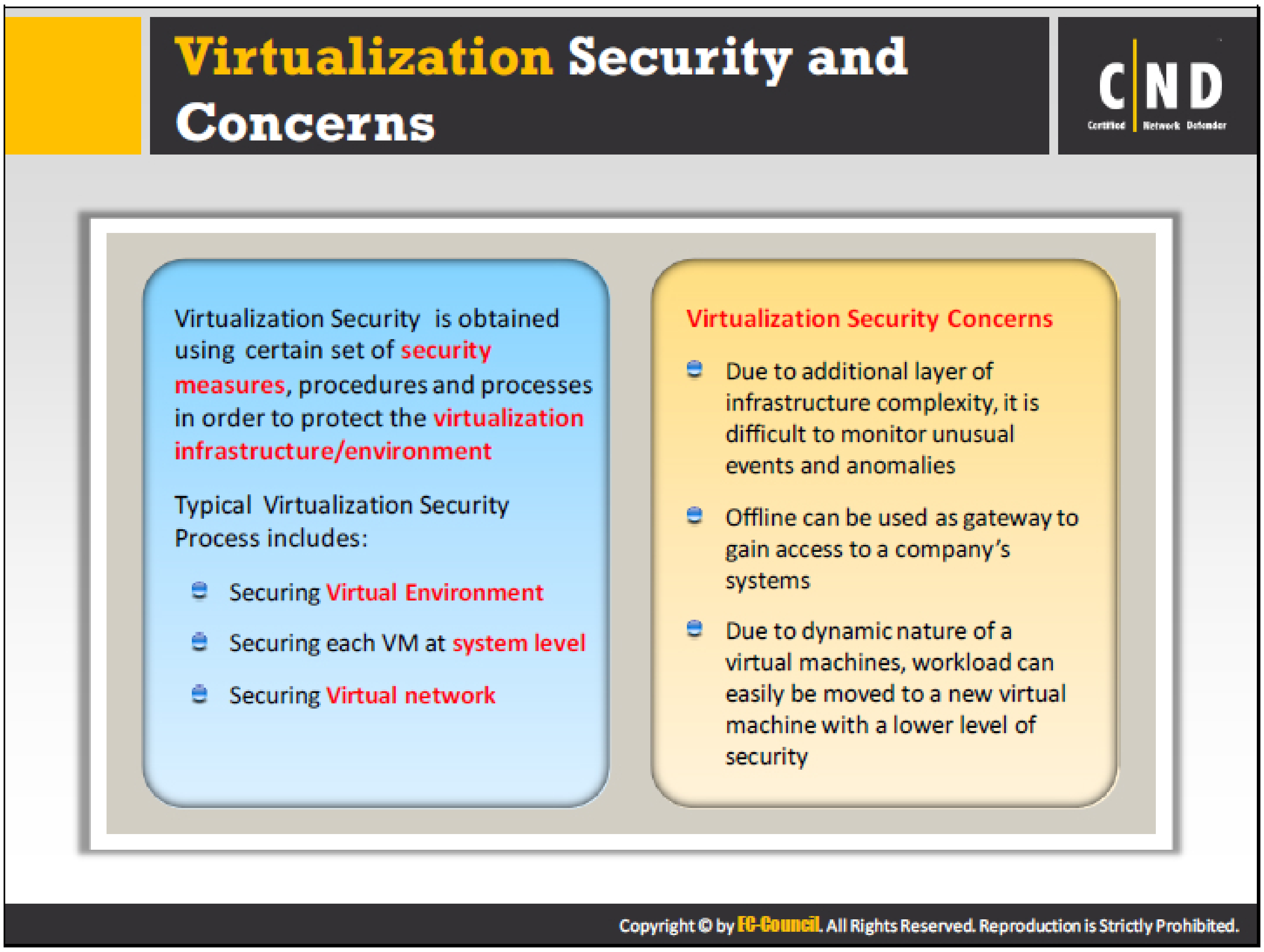
Oracle provides virtualization applications and tools for:

- Server Virtualization: Server Virtualization enables the IT of an enterprise to effectively handle its server infrastructure such as Memory, CPU and storage devices. The server handles multiple client requests simultaneously by logically partitioning and isolating its resources.
- Desktop Virtualization: Desktop virtualization uses Hypervisors which run on a bare-metal server i.e. physical hardware. It provides the flexibility to install several virtual machines and run them along with the host operating system.
- Application Virtualization (App-V): Application virtualization enables the ability to logically distribute the application services to all the users under one specific platform.
- Virtual Desktop Infrastructure (VDI): Virtual Desktop Infrastructure is a way of deploying an operating system on virtual machines to enable remote access for the desktop and applications.

Microsoft

Source: *http://www.microsoft.com*

Microsoft provides built-in virtualization on Hyper-V, which is included in Windows Server. Microsoft virtualization solutions help reduce costs by consolidating more workloads on fewer servers. Increase IT agility and flexibility across on-premises and cloud resources with Microsoft virtualization solutions.



Virtualization Security and Concerns

CND
Certified Network Defender

Virtualization Security is obtained using certain set of security measures, procedures and processes in order to protect the virtualization infrastructure/environment

Typical Virtualization Security Process includes:

- Securing Virtual Environment
- Securing each VM at system level
- Securing Virtual network

Virtualization Security Concerns

- Due to additional layer of infrastructure complexity, it is difficult to monitor unusual events and anomalies
- Offline can be used as gateway to gain access to a company's systems
- Due to dynamic nature of a virtual machines, workload can easily be moved to a new virtual machine with a lower level of security

A virtualized environment facilitates the detection of new attack exposures thereby forcing the user to take protective measures for both hosts and the virtual machines. In a non-virtualized environment, each host is separately held, consisting of separate services and web servers. The services run in their own spaces and they connect directly to the network. In a virtualized environment, several guest hosts are placed in a single host. Here, all the services are grouped together, thereby increasing the chances of vulnerabilities in the system.

Virtualization Security Concerns

There are different issues and challenges while implementing and using virtualization.

Two major challenges are:

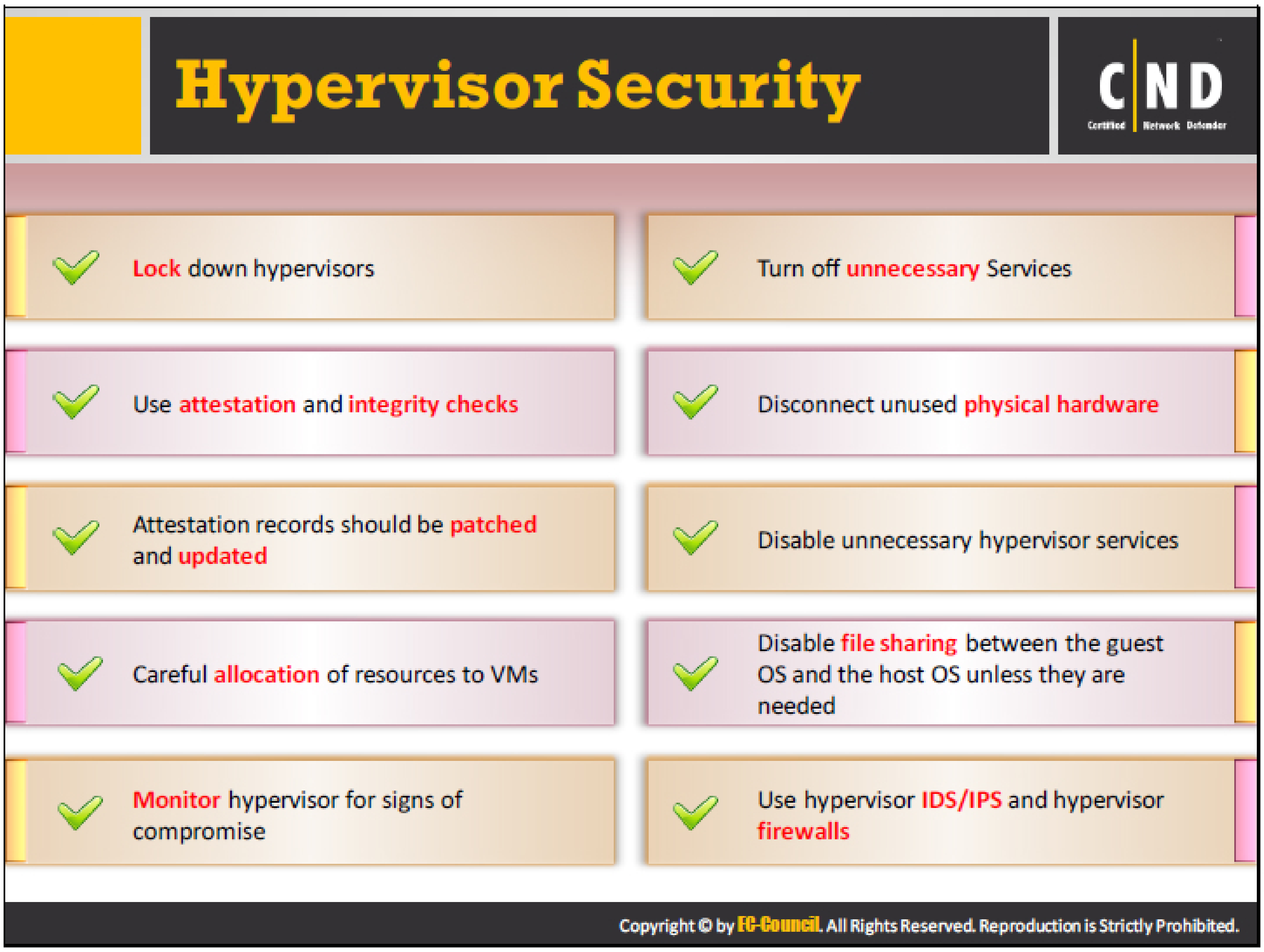
1. Traditional threats
2. New threats

Traditional threats to the virtual environment include:

- Malicious code in virtual machines and appliances.
- Errors while configuring virtual network and firewalls.
- Hypervisor Configuration liabilities.
- Data leakage.

New threats to the Virtual Machine environments are:

- Management console vulnerability allows the attacker to remotely control the virtual machines using the management consoles.
- A vulnerable hypervisor can act as a danger to both the host as well as virtual machines.
- Poor Hypervisor design makes the whole system vulnerable to attacks.
- Lack of updating guest OS and installing security patches to the virtual machines.
- Vulnerabilities in the host system makes it easier for the attacker to dive into the virtual environment without much effort.



Hypervisor Security

- ✓ Lock down hypervisors
- ✓ Turn off unnecessary Services
- ✓ Use attestation and integrity checks
- ✓ Disconnect unused physical hardware
- ✓ Attestation records should be patched and updated
- ✓ Disable unnecessary hypervisor services
- ✓ Careful allocation of resources to VMs
- ✓ Disable file sharing between the guest OS and the host OS unless they are needed
- ✓ Monitor hypervisor for signs of compromise
- ✓ Use hypervisor IDS/IPS and hypervisor firewalls

Securing hypervisor involves securing the hypervisor during its implementation, management and development. Hypervisors can face many threats and risks. Most of the attacks occur within an organization where users try to compromise the virtual machines running in the system. Experts say that the number of attacks on hypervisors has increased dramatically in recent years. This urges the need for securing the hypervisors using patch management and other services.

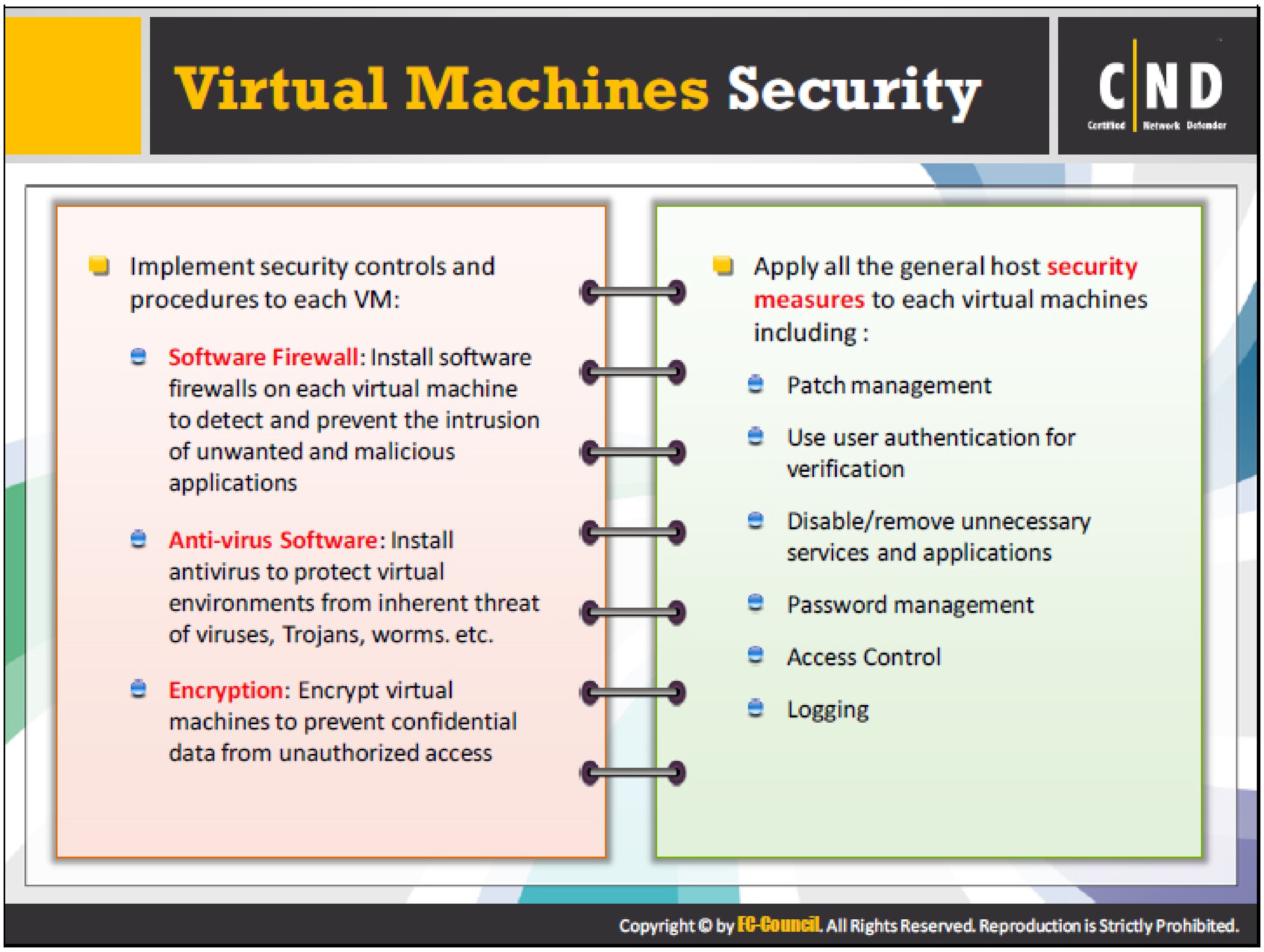
The hypervisor platform enables multiple types of access like SSH, RDP, etc. However, minimizing the remote and console access to the systems actually plays an important role in securing the hypervisor. The hypervisor can be more secure if the hypervisor management is given only access required to run the business environment.

Proper configuration also plays an important role in securing the hypervisor. Configuring only the required settings and services can control the possibilities of threats and risks in the hypervisor. Certain hardening mechanisms like controlling the user and group access on the local system, controlling file permissions, using only required services, etc., can assist in increasing the security of the hypervisor. The administrators need to confirm the security of every platform on the hypervisor.

The hypervisors can decide the amount of resources provided to each guest OS. Resources provided to each guest OS cannot be shared with another guest OS. Providing only limited amount of resources to the guest OS can minimize attacks like denial of service and inserting malicious code into another OS.

The network administrators need to be more careful while handling the access to VLANs. The VLAN assists in keeping the traffic separated between the networks. Allowing the access of VLANs to the virtual network may allow a compromised machine to access all the other VLANs. Administrators need to be more careful while configuring the VLANs and should ensure the presence of only those VLANs that are required for the hypervisor configuration. Securing hypervisors requires the need to secure the direct interface to the system. Securing these with complex and strong passwords allows the administrators to handle the out of band interface (OOB). Implementing a firewall can limit the access of the OOB subnets to only approved IP addresses.

The network administrators can also work on controlling the rights to perform a service using the service account. Controlling the service accounts can actually bring down the risks during the case of service accounts becoming compromised. Usage of long and strong passwords enables the security of the service accounts.



Virtual Machines Security

- Implement security controls and procedures to each VM:
  - **Software Firewall**: Install software firewalls on each virtual machine to detect and prevent the intrusion of unwanted and malicious applications
  - **Anti-virus Software**: Install antivirus to protect virtual environments from inherent threat of viruses, Trojans, worms. etc.
  - **Encryption**: Encrypt virtual machines to prevent confidential data from unauthorized access

- Apply all the general host **security measures** to each virtual machines including :
  - Patch management
  - Use user authentication for verification
  - Disable/remove unnecessary services and applications
  - Password management
  - Access Control
  - Logging

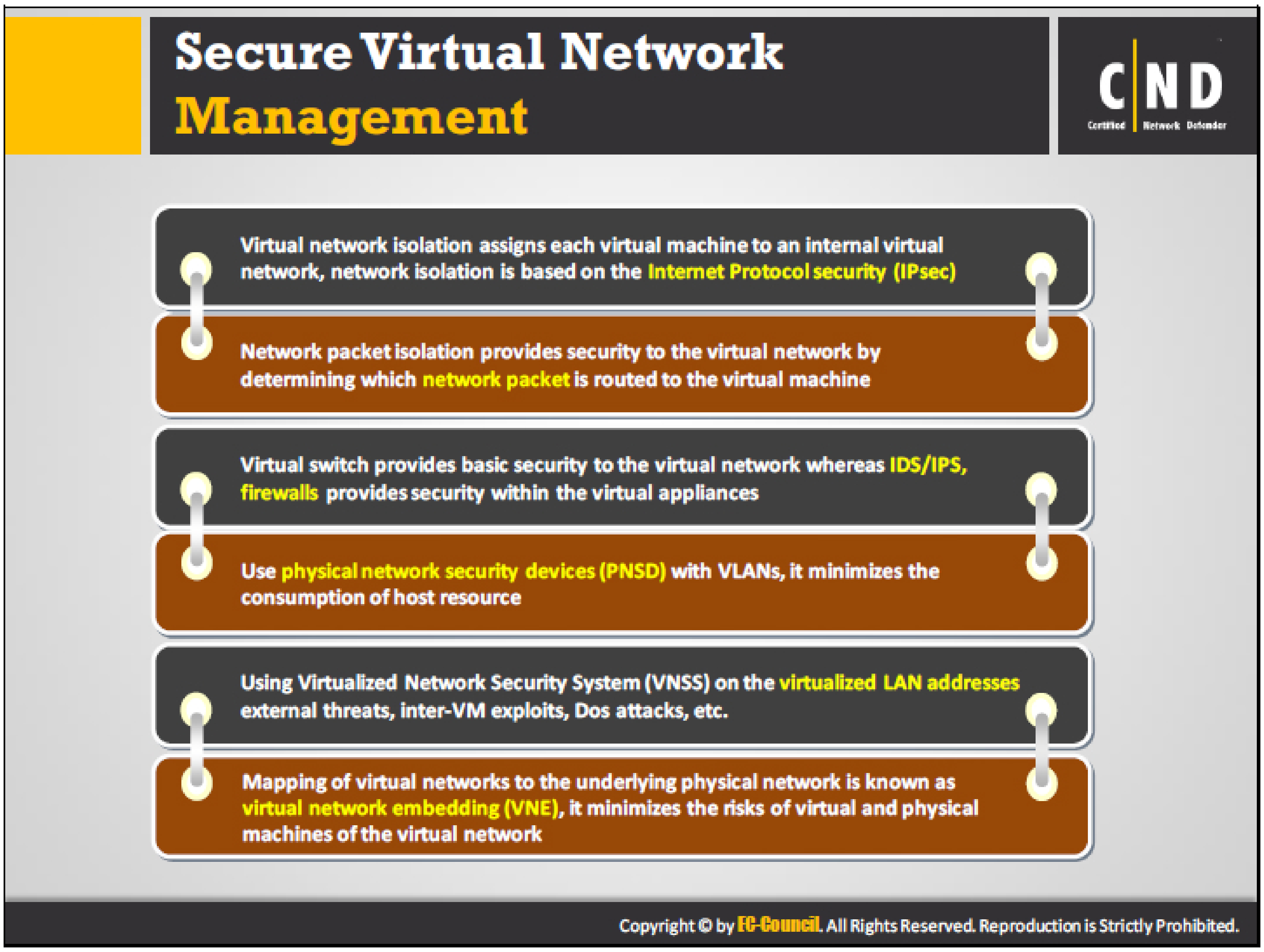
In addition to general security measures for host security, administrators should implement the following security measures to enhance virtual machine security.

- **Implementing Protocols and Procedures:** Designing certain rules and strategies helps secure the virtual machines. Adding the recommendations below will provide more security:
  - Check for operating system updates for the virtual machines on a weekly basis.
  - Check for virtualization software updates on a weekly basis.
  - Update the virtual machines on a weekly basis.
- **Implementing Software Firewall:** It is false that virtual machines are safe as they are always looked at as a sandboxed application. They are prone to external and internal attacks similar to the physical system and always require attention.
  - Software Firewalls monitor the flow of network traffic between different virtual machines.
  - Provides security to each virtual machine and reduces the attack risk.
  - Software firewalls on each virtual machine detects and prevents the intrusion of unwanted and malicious applications.
  - Virtual or software firewalls do not create collision between the firewall implemented on the host operating system.

- There are many software firewalls available like comodo, zone alarm, etc.

- **Deploying Anti-Virus Software**
  - Install anti-virus to protect the virtual environment from the inherent threats of viruses, Trojans, worms, etc.
  - Antivirus deployed on a virtual machine inspects for any unusual activity and scans all files and folders for malicious content.
  - Installation of anti-virus on a host machine does not secure the virtual machine. Install antivirus on a virtual machine in order to secure it properly.
  - Mostly used antiviruses are Kaspersky, McAfee, Microsoft security essential, Symantec endpoint protection, etc.

- **Encrypting the Virtual Machines:** A virtual machine hosts highly confidential data so encryption is required. Encrypting virtual machines protects the virtual machines from unauthorized access. Users must enter a password to encrypt/decrypt virtual machines. Steps to encrypt a virtual machine:
  - **Step 1**: Shut down your virtual machine
  - **Step 2**: Go to configure from the virtual machine menu and a dialogue box appears
  - **Step 3**: Click options and select security
  - **Step 4**: In the security pane, click turn on and provide a password and click ok
  - **Step 5**: The password provided in step 4 will be at the time of encrypting/decrypting the virtual machines



Secure Virtual Network Management

CND
Certified Network Defender

- Virtual network isolation assigns each virtual machine to an internal virtual network, network isolation is based on the Internet Protocol security (IPsec)
- Network packet isolation provides security to the virtual network by determining which network packet is routed to the virtual machine
- Virtual switch provides basic security to the virtual network whereas IDS/IPS, firewalls provides security within the virtual appliances
- Use physical network security devices (PNSD) with VLANs, it minimizes the consumption of host resource
- Using Virtualized Network Security System (VNSS) on the virtualized LAN addresses external threats, inter-VM exploits, Dos attacks, etc.
- Mapping of virtual networks to the underlying physical network is known as virtual network embedding (VNE), it minimizes the risks of virtual and physical machines of the virtual network

Organization approaches for secure virtual network management such as:

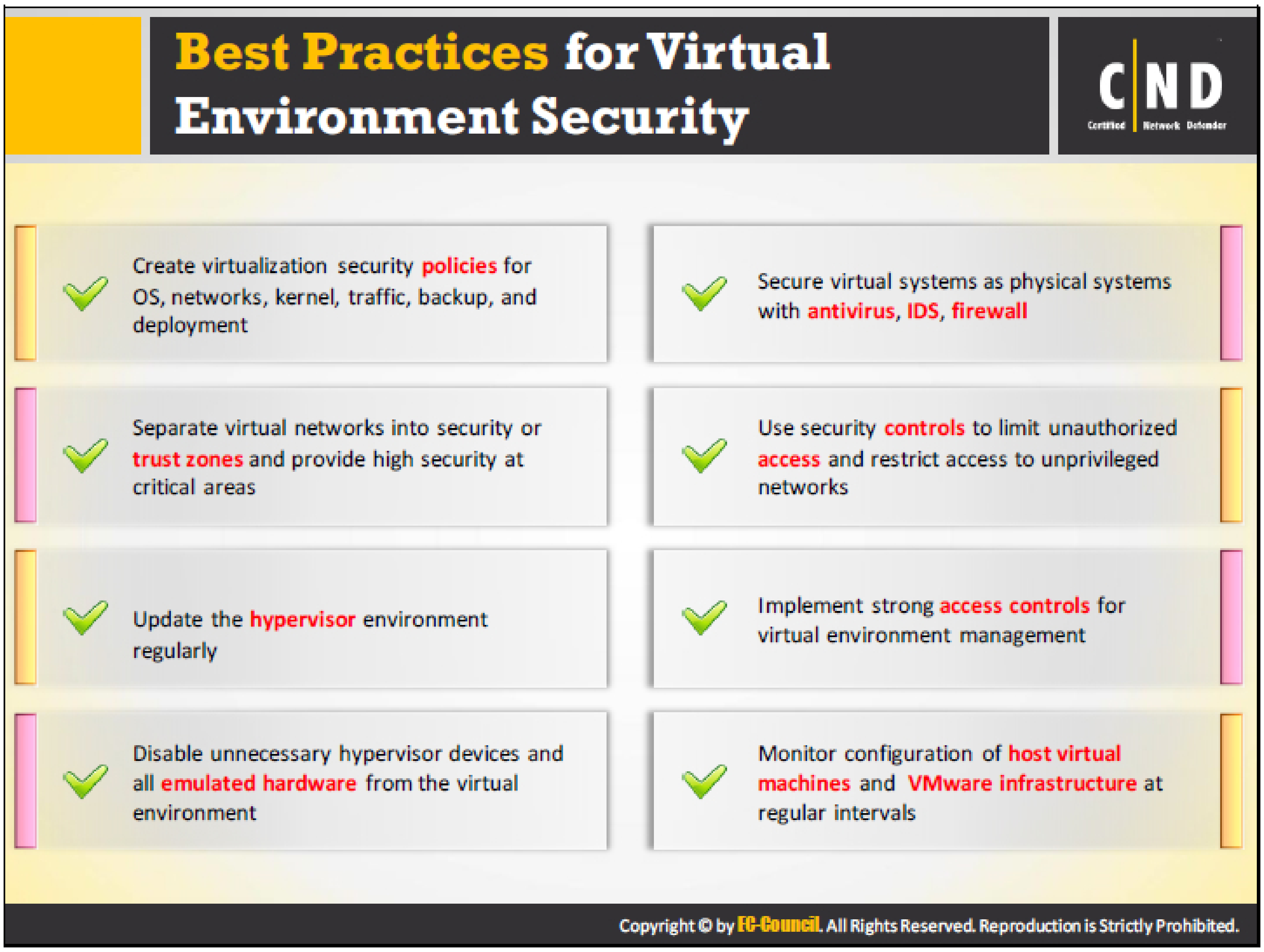
- **Physical Network Security Device (PNSD):** This physical network security device resides outside the host machine and deploying it for every host machine may reduce performance. This approach does not provide security to VMs
- **Physical Network Security Device (PNSD) with VLANs**: Use physical network security devices (PNSD) with VLANs; it reduces the consumption of host resources
- **Host Intrusion Prevention System (HIPS):** It resides inside the virtual server, uses host machine resources and it offers server level protection
- **Virtualized Network Security System (VNSS):** It resides on a virtual LAN and consumes host machine resources. It monitors, partitions the virtual environments and provides security to virtual network segments, VLANs, servers and devices

Methods to secure virtual environments include:

- **Resource Limitation:** Apply resource usage limits to each virtual machine so that it minimizes the risk of using multiple shared hardware resources at one time, which can affect performance of the virtual machine
- **Security Measures:** Install Antivirus, Spyware and intrusion detection systems. Keep everything updated on each virtual machine to reduce security vulnerabilities
- **Native remote management services**: Use native remote management services to reduce the risk of an attacker intrusion to a virtual machine

Guidelines to secure virtual environments are:

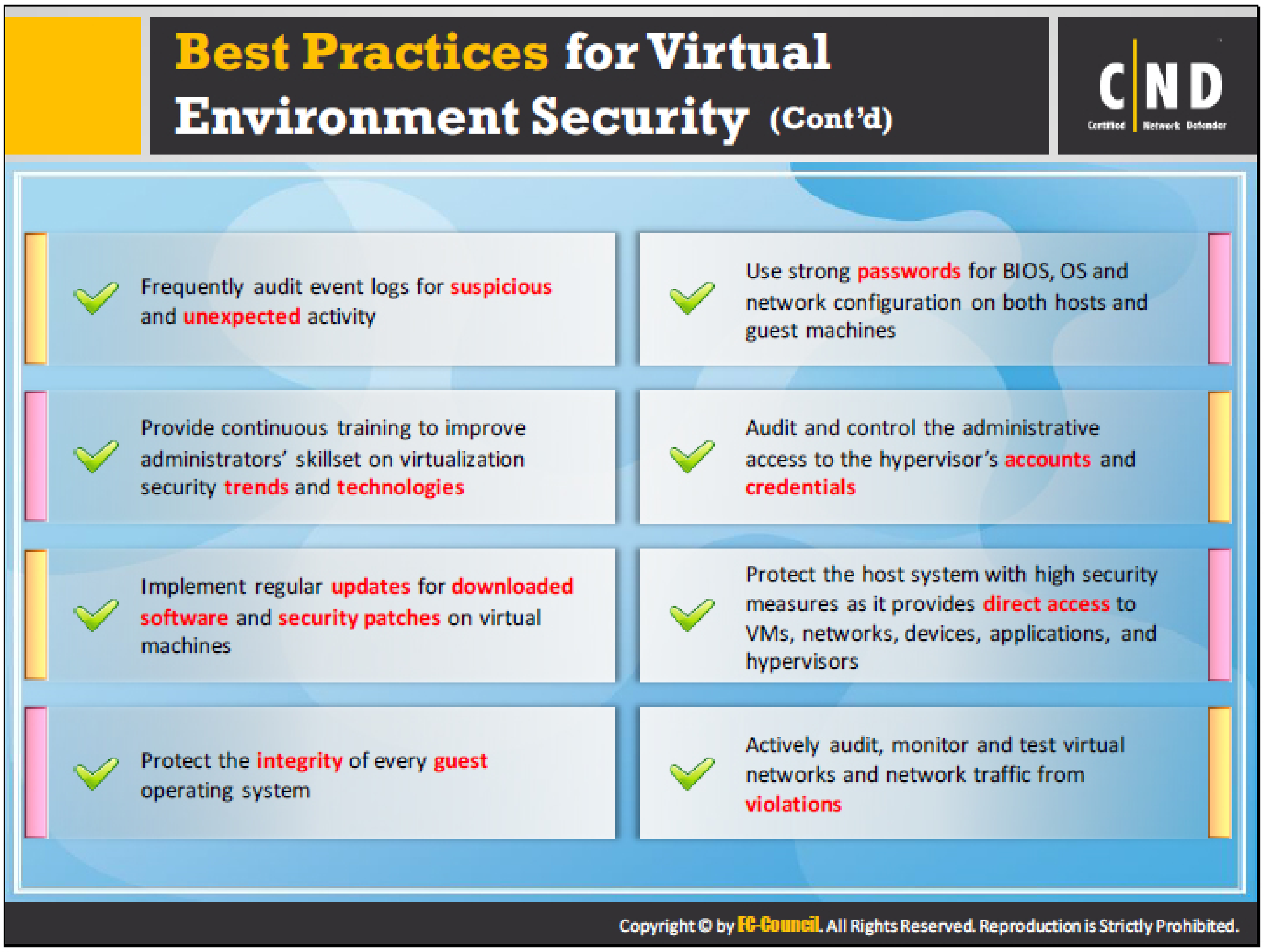
- Authentication to the virtual devices.
- Restricted connectivity to all virtual resources.
- Segmenting the virtual infrastructure.
- Virtual resource reservation and limits.
- Apply standard infrastructure security measures into the virtual infrastructure.
- Use native remote management services (RMS) to communicate with virtual machines .
- Host based IPS (HIPS) protects the virtual environment from security threats.



Best Practices for Virtual Environment Security

C|ND Certified Network Defender

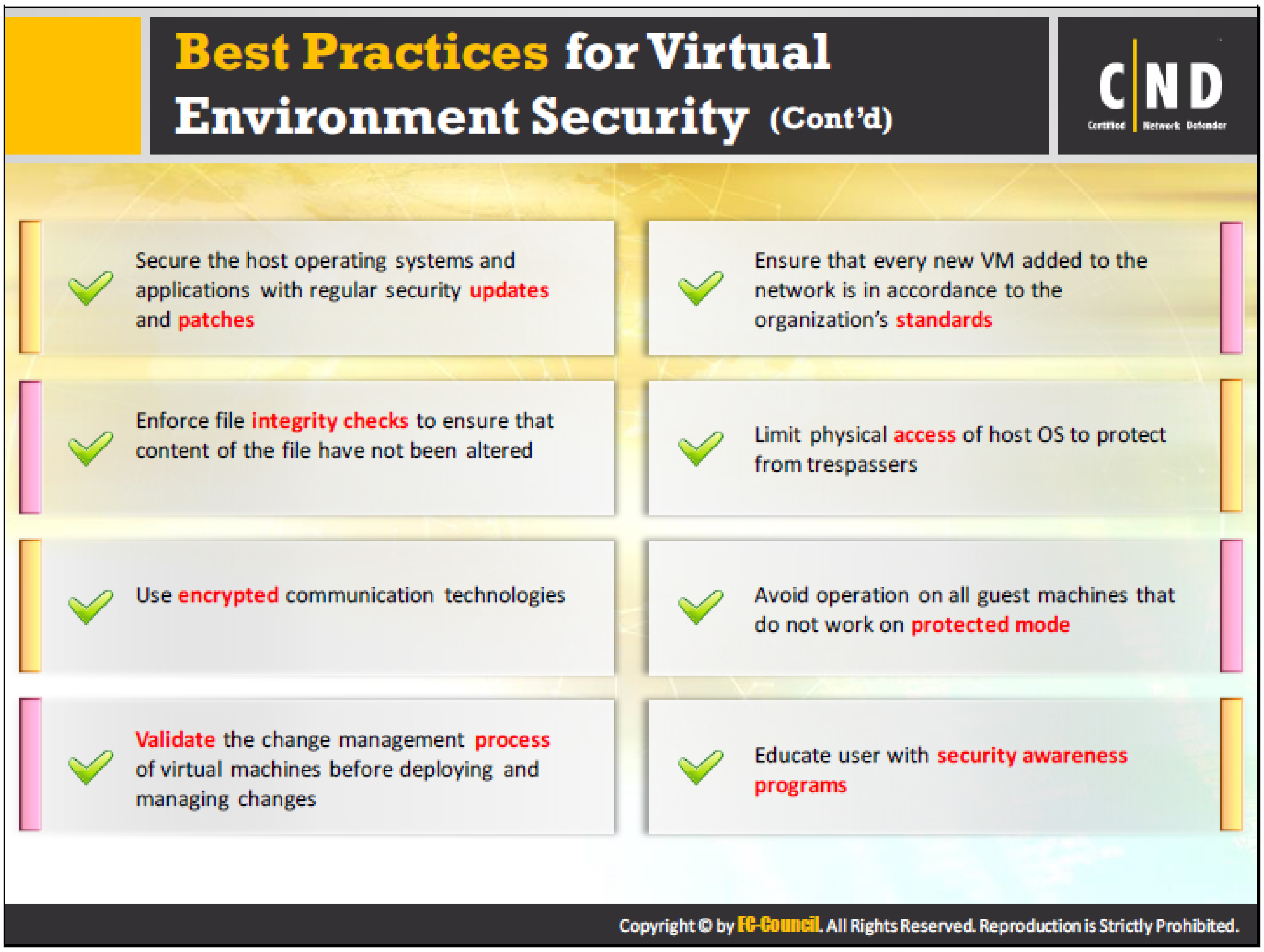
- ✓ Create virtualization security policies for OS, networks, kernel, traffic, backup, and deployment
- ✓ Secure virtual systems as physical systems with antivirus, IDS, firewall
- ✓ Separate virtual networks into security or trust zones and provide high security at critical areas
- ✓ Use security controls to limit unauthorized access and restrict access to unprivileged networks
- ✓ Update the hypervisor environment regularly
- ✓ Implement strong access controls for virtual environment management
- ✓ Disable unnecessary hypervisor devices and all emulated hardware from the virtual environment
- ✓ Monitor configuration of host virtual machines and VMware infrastructure at regular intervals



Best Practices for Virtual Environment Security (Cont'd)

C|ND Certified Network Defender

- ✓ Frequently audit event logs for suspicious and unexpected activity
- ✓ Use strong passwords for BIOS, OS and network configuration on both hosts and guest machines
- ✓ Provide continuous training to improve administrators' skillset on virtualization security trends and technologies
- ✓ Audit and control the administrative access to the hypervisor's accounts and credentials
- ✓ Implement regular updates for downloaded software and security patches on virtual machines
- ✓ Protect the host system with high security measures as it provides direct access to VMs, networks, devices, applications, and hypervisors
- ✓ Protect the integrity of every guest operating system
- ✓ Actively audit, monitor and test virtual networks and network traffic from violations



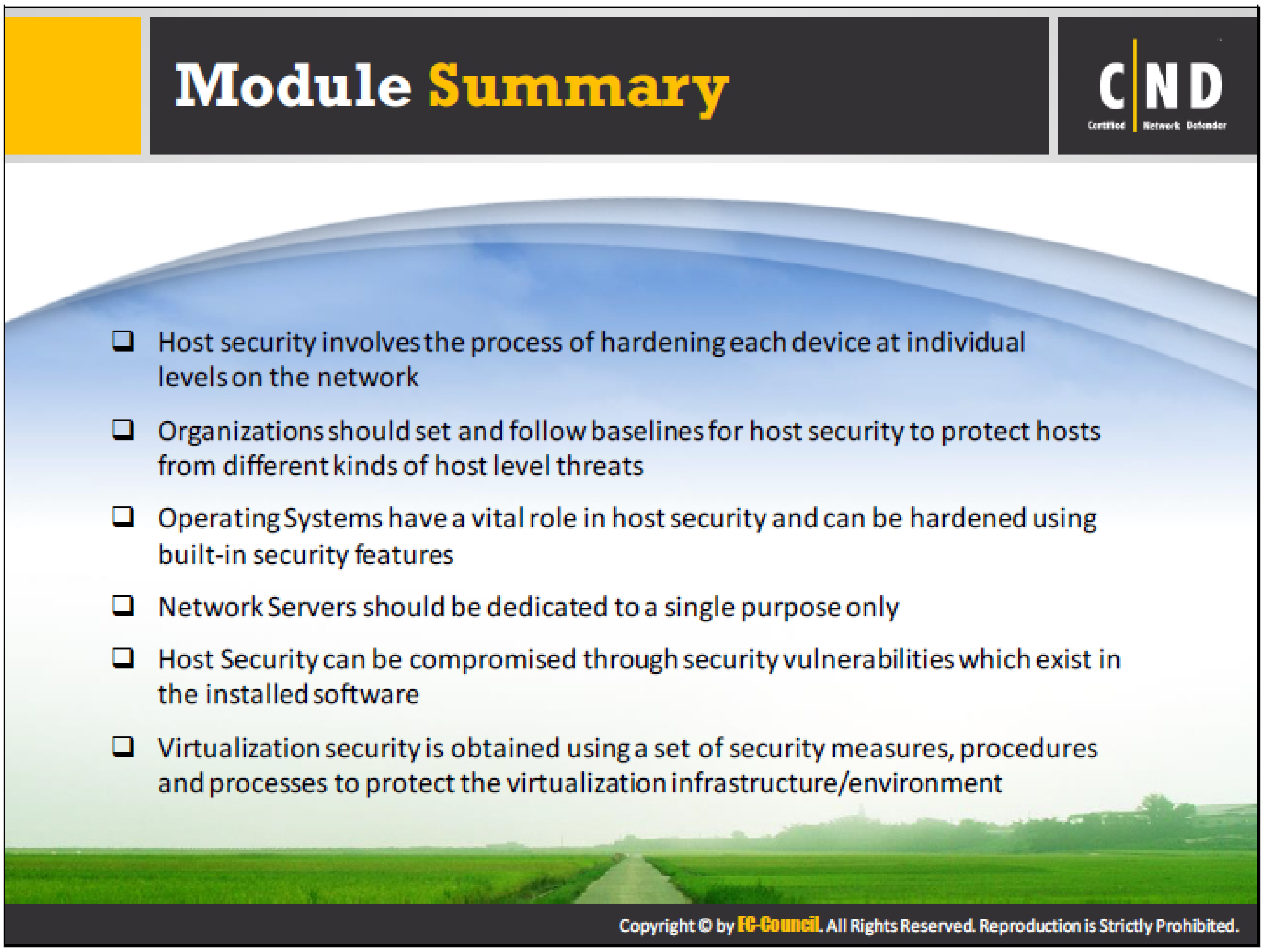
Best Practices for Virtual Environment Security (Cont'd)

CND Certified Network Defender

- ✓ Secure the host operating systems and applications with regular security **updates** and **patches**
- ✓ Ensure that every new VM added to the network is in accordance to the organization's **standards**
- ✓ Enforce file **integrity checks** to ensure that content of the file have not been altered
- ✓ Limit physical **access** of host OS to protect from trespassers
- ✓ Use **encrypted** communication technologies
- ✓ Avoid operation on all guest machines that do not work on **protected mode**
- ✓ **Validate** the change management **process** of virtual machines before deploying and managing changes
- ✓ Educate user with **security awareness programs**

The following are additional best practices for virtualization security:

- **Enforce the least privileges:** It is a core security principle which makes users operate with the least set of privileges that are necessary to finish the task/job.
- **Harden Access Controls:** Deploy controls to the hypervisor and virtual machines in a secure manner to avoid unauthorized access.
- **Monitor the virtual traffic:** There are various tools available and using these tools to identify malicious traffic and defend the virtual machines from intrusions and attackers.
- **Record VM Migrations:** Migration between virtual machines must be recorded to monitor and diagnose machine failures.
- **Monitor VM snapshots and rollback:** Create a work environment to monitor virtual machines. If there any issues, rollback to a stable state using snapshots which are taken at particular intervals by the administrator.
- **Scan and audit virtual machines:** Virtual machines are scanned at regular intervals to discover vulnerabilities and service failures.



Module Summary

CND
Certified Network Defender

- ❑ Host security involves the process of hardening each device at individual levels on the network
- ❑ Organizations should set and follow baselines for host security to protect hosts from different kinds of host level threats
- ❑ Operating Systems have a vital role in host security and can be hardened using built-in security features
- ❑ Network Servers should be dedicated to a single purpose only
- ❑ Host Security can be compromised through security vulnerabilities which exist in the installed software
- ❑ Virtualization security is obtained using a set of security measures, procedures and processes to protect the virtualization infrastructure/environment

In this module, you have learned how important it is to secure an individual host for network security. The module described host security, tools and techniques for securing each individual host on the network. The module helps you prepare security baselines for host security including workstations, router, switches, servers, etc., and provides security measures to prevent them from various host security threats. The module also discussed the virtualization concept and provided security measures for virtual machines in a virtual environment.