Network Traffic Monitoring and Analysis

Module 11

Network Traffic Monitoring and Analysis

Module 11

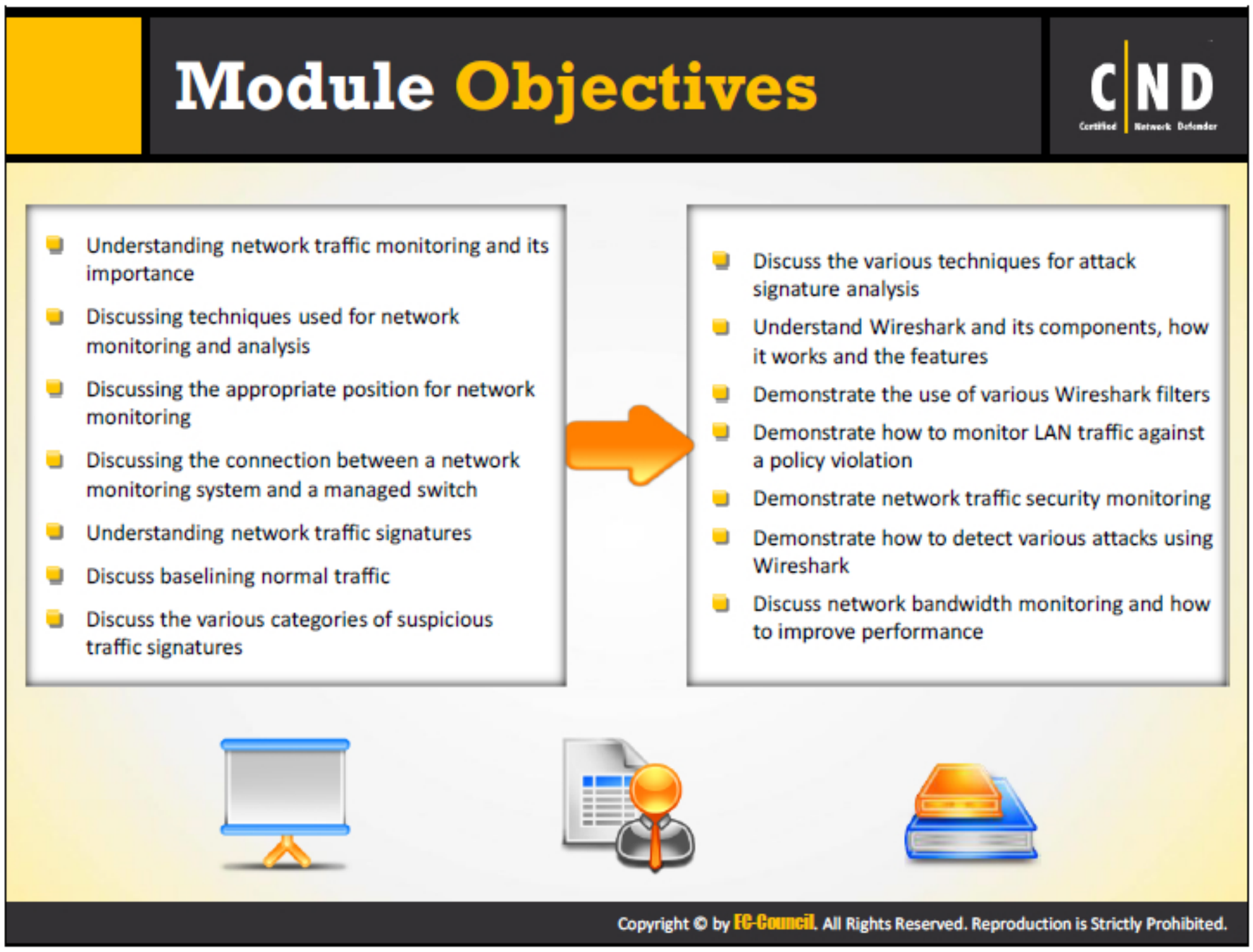
C|ND
Certified Network Defender

Certified Network Defender

Module 11: Network Traffic Monitoring and Analysis

Exam 312-38

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network monitoring and analysis is a very important day to day task for the network administrator. It provides an additional layer of security to the network and involves analyzing network performance and traffic patterns to detect abnormal activities in the network.

This module will teach you various aspects of network monitoring signature analysis. The module starts with an introduction to the network monitoring concept, its importance, and then educates you on how to detect and analyze various types of attacks on your network.

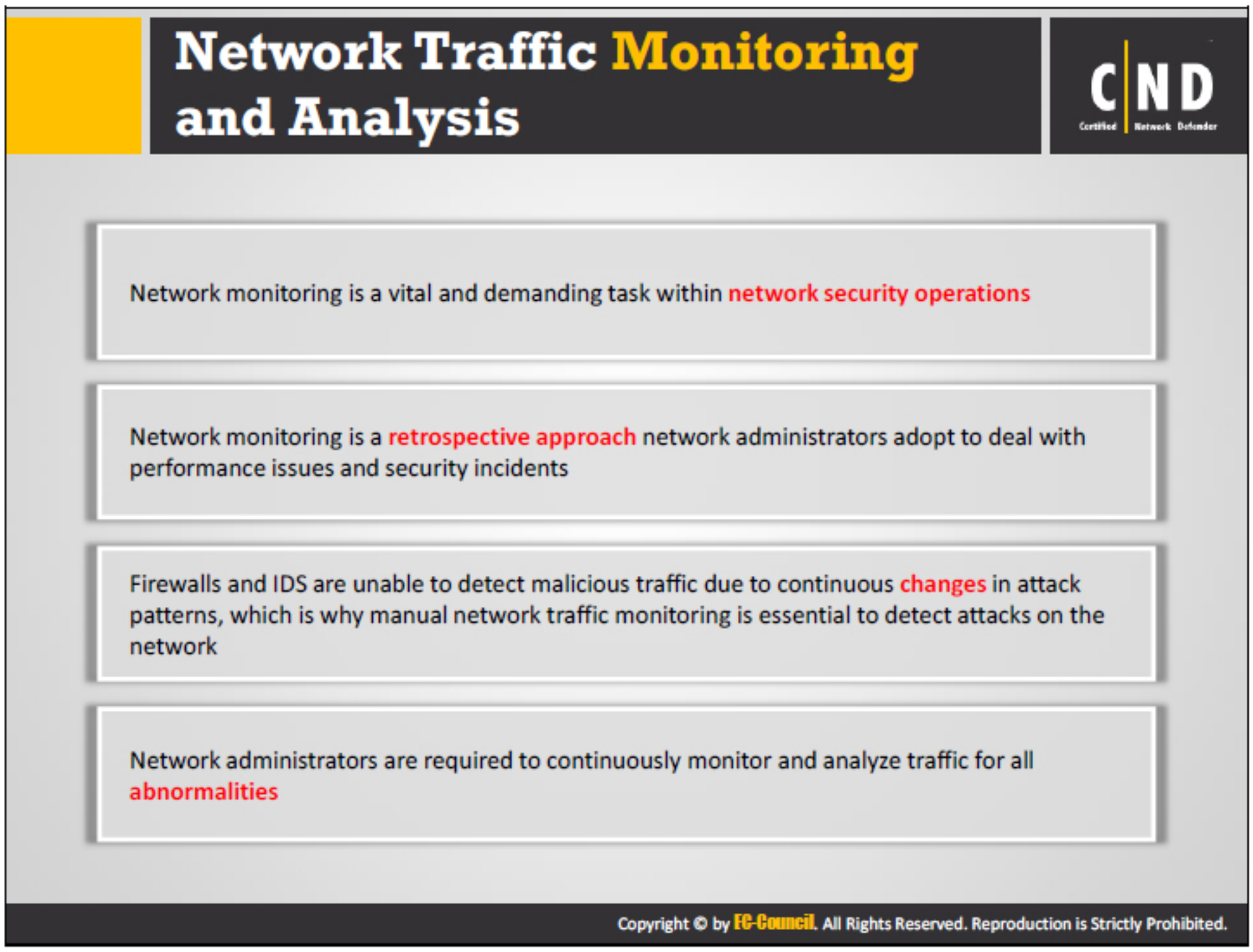
Certified Network Defender Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

C|ND Certified Network Defender

" Network traffic monitoring and analysis is an **integral part** of network security "

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

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

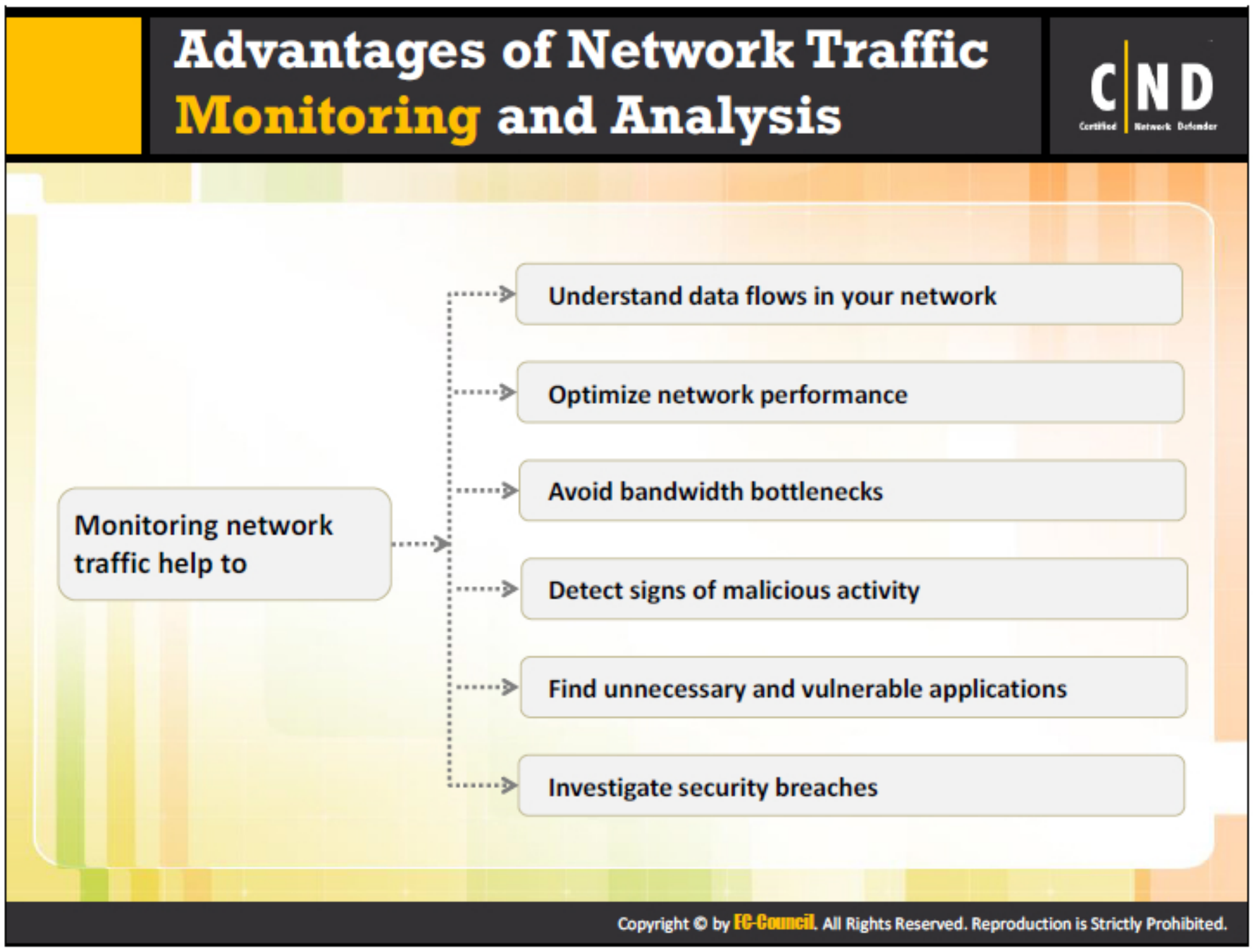


Network traffic monitoring is the process of capturing network traffic and inspecting it closely to determine what is happening on the network. Network Administrators should constantly strive to maintain a smooth network operation. If a network is down even for a small period of time, productivity within a company would decline. In order to be proactive rather than reactive, administrators need to monitor the traffic movement and performance ensuring a security breach doesn't occur within the network.

The network monitoring process involves sniffing the traffic flowing through the network. It requires capturing network packets and conducting a signature analysis to identify any malicious activity. Administrators should continuously monitor and analyze the network traffic to look for the presence of attack signatures.

Network operators use network traffic analysis tools to identify malicious or suspicious packets hiding within the traffic. They monitor download/upload speeds, throughput, content, traffic behaviors, etc. to understand what is going on in the network operations.

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



Network traffic analysis is done to get an in-depth insight into what type of network packets or data is flowing through a network. Typically, it is done through network monitoring or network bandwidth monitoring utilities. The traffic statistics from the network traffic analysis helps:

- Understand and evaluate the network utilization.
- Download/upload speeds.
- Type, size, origin, destination and content/data of packets.

The typical network monitoring advantages are:

- **Proactive:** Network monitoring proactively detects the applications that consume maximum bandwidth and reduce bandwidth. It manages the server bottleneck situation and other systems connected to the network. Network monitoring delivers an efficient quality of service to users. Network monitoring creates a record of all the irregularities occurring in the network that administrators handle later.
- **Utilization:** It is important to analyze the need for network utilization, especially with all the new and evolving technology. Network monitoring provides the complete details on the infrastructure. This provides an idea about the amount of load a network can handle during heavy traffic periods. Leading to the required utilization of the space in the network.
- **Optimization:** Network monitoring techniques gather the network infrastructure information in a timely manner and save it for the administrator. The admin can then take

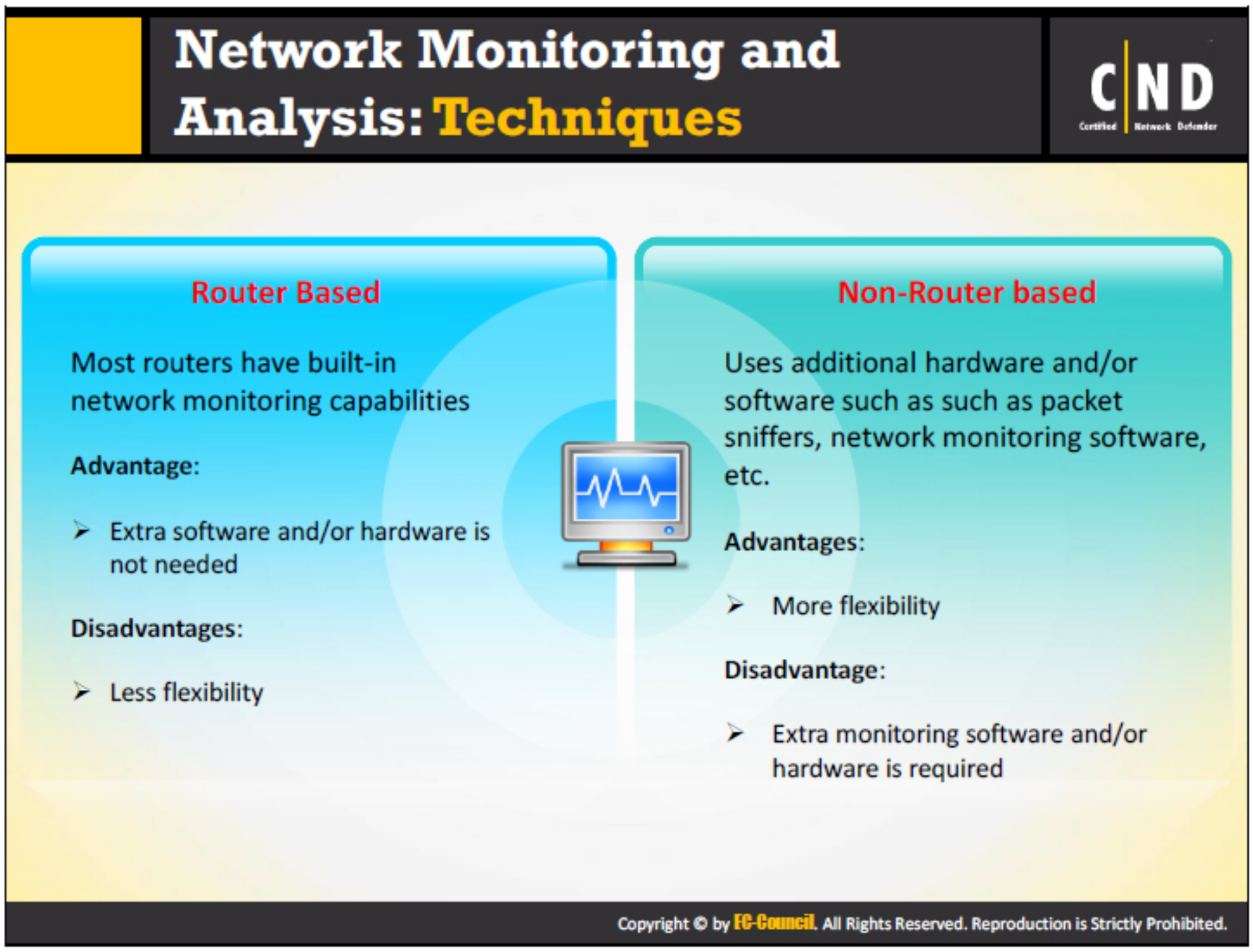
Certified Network Defender Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

the required actions, before the situation worsens. Applications that prove vulnerable to the network are located by this technique.

- **Minimizing Risk:** Network monitoring techniques comprise all the required SLAs and compliance applicable to users or consumers. The complete infrastructure information is required when drafting the SLAs. Real-time monitoring of network topologies and channels helps document these SLAs.

The network monitoring technique is beneficial for administrators. It is very easy to setup and implement considering the complexity of the networks.

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



A network administrator can implement two types of techniques to monitor their network. Each technique has advantages and disadvantages. It is recommended that both a router-based and non-router based techniques be used for the network monitoring task.

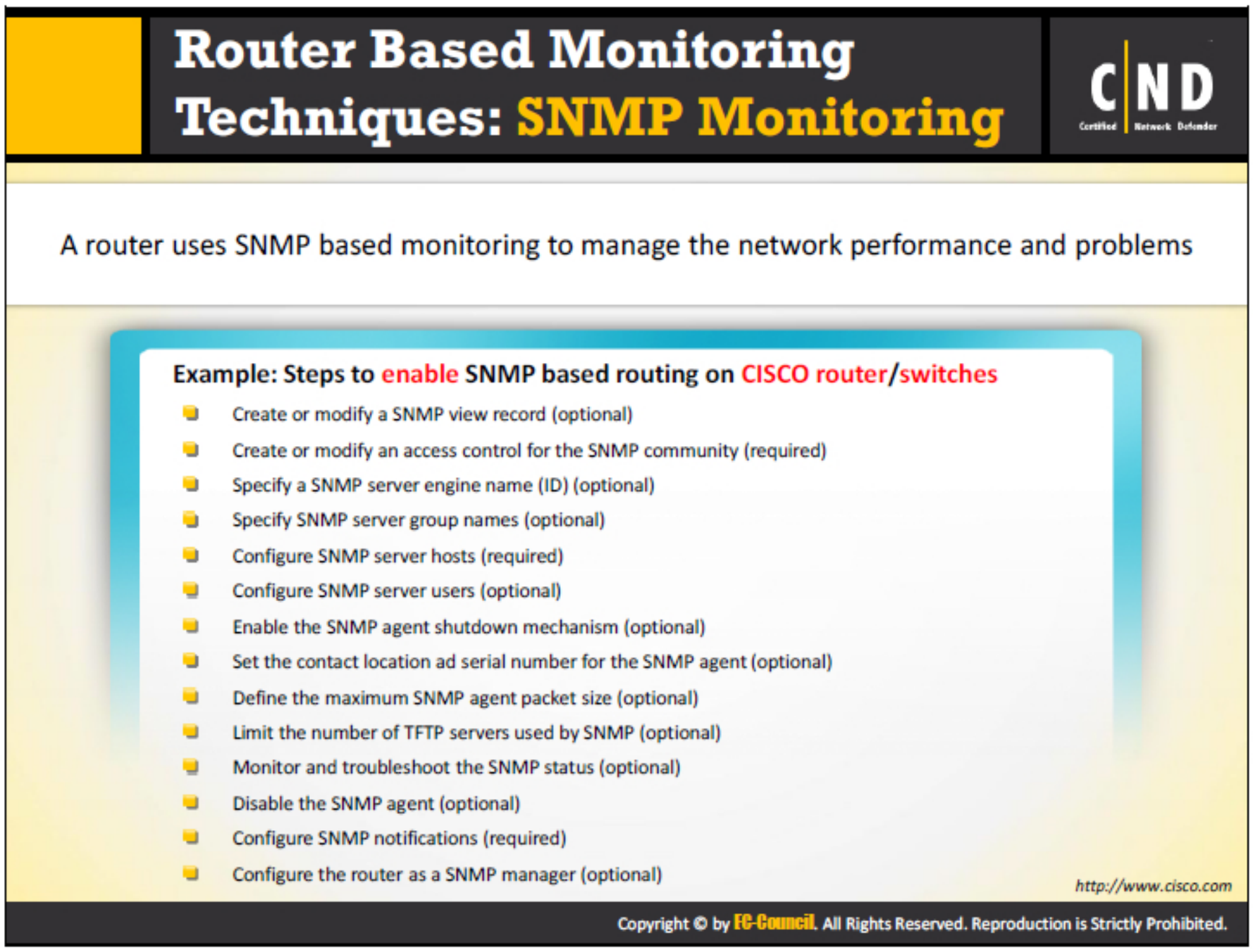
Router based monitoring technique

In router based monitoring, the functionality is hardcoded into the router. To use this functionality it must first be enabled and configured using the router interface. With its built-in feature, it is less expensive, but offers less flexibility. This inbuilt feature uses SNMP monitoring, Netflow monitoring and remote monitoring techniques to monitor the network.

Non-Router based monitoring technique

In non-router based monitoring, a dedicated external hardware device or additional software is required to monitor your network. Because of this, it is more expensive than using a router based technique. However, it offers more flexibility in monitoring than a router based technique.

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



Simple Networking Monitoring Protocol (SNMP) is a part of the TCP/IP suite and functions on the application layer. SNMP helps administrators manage network performance by resolving network issues it encounters. The passive sensors implemented from a router to a host gather traffic statistics.

Elements of SNMP-based Monitoring

SNMP consists of a SNMP manager, SNMP agent, managed devices and a management information base (MIB).

- **SNMP Manager:** SNMP manager is a system that maintains the proper network function. The communication between the SNMP manager and agents uses a message format. The SNMP manager controls and monitors the activities of the host. The main role of a SNMP manager is:
  - Querying the SNMP agents.
  - Receiving a response from the SNMP agent.
  - Implementing changes to the agents.
  - Monitors asynchronous events from the agent.
- **SNMP Agent:** SNMP agent maintains and saves the data for network devices. This data is passed on to the managing systems of the network. An SNMP agent can only work when a

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

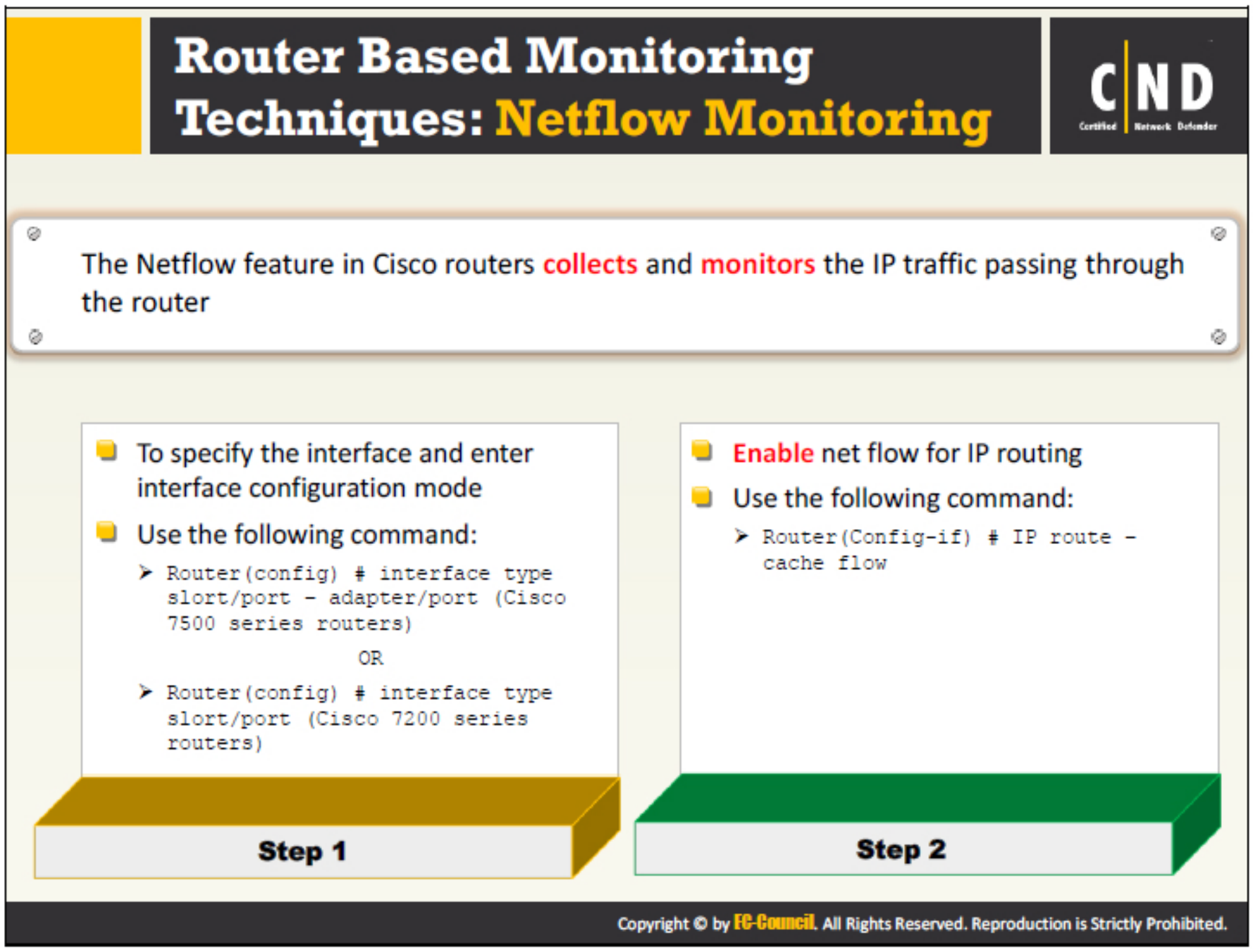
relationship is defined between a SNMP manager and a SNMP agent. The main role of SNMP agents is:

- Gathering management information.
- Storing and retrieving management information.
- Notify the SNMP manager an event has occurred.

- **Managed Devices:** Network based devices such as routers, switches and servers require some form of monitoring and management.
- **Management Information base (MIB):** The SNMP manager uses the device records saved by the SNMP agent. The sharing of this database is known as the Management Information Base. The MIB allows the SNMP manager to query SNMP agents about the devices.
- **SNMP Commands:** The SNMP commands make the implementation of SNMP less complex for administrators. Here are the SNMP commands:
  - **GET:** It retrieves the information from the managed device. It is used by SNMP managers.
  - **GET NEXT:** Works similar to GET and also retrieves the object identifiers from the MIB.
  - **GET BULK:** Retrieves large amounts of data from the MIB.
  - **SET:** SNMP managers use this command to modify or assign the value of the managed device.
  - **TRAPS:** SNMP agents use this command to notify SNMP managers about an event occurring in the network.
  - **INFORM:** Similar to TRAPS, but it includes the SNMP manager's acknowledgement to receive the notification.
  - **RESPONSE:** The SNMP manager uses this command to carry the actions back to the agents.

Information collected by SNMP helps to control the network by resolving the issues in real time before affecting the productivity of the organization.

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

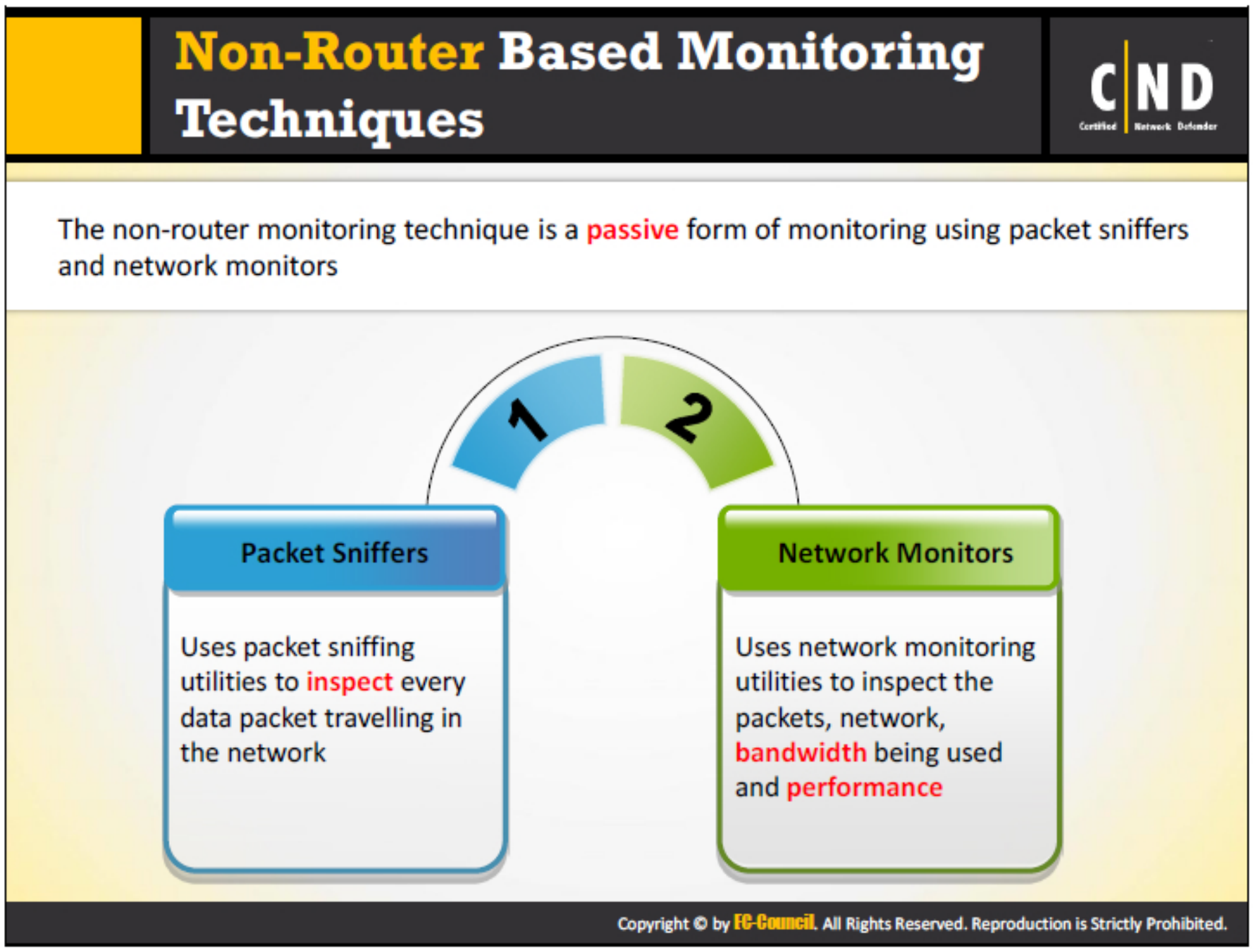


The Netflow monitoring technique has the ability to collect the IP network traffic while entering or exiting the interface. This helps administrators determine the source and destination of the traffic, class of service and reason for traffic congestion, whenever it occurs. Netflow monitoring allows a network a wide view of the traffic enhancing the performance monitoring and security of the network. Cisco devices support Netflow based network monitoring.

Elements of Netflow-based Monitoring

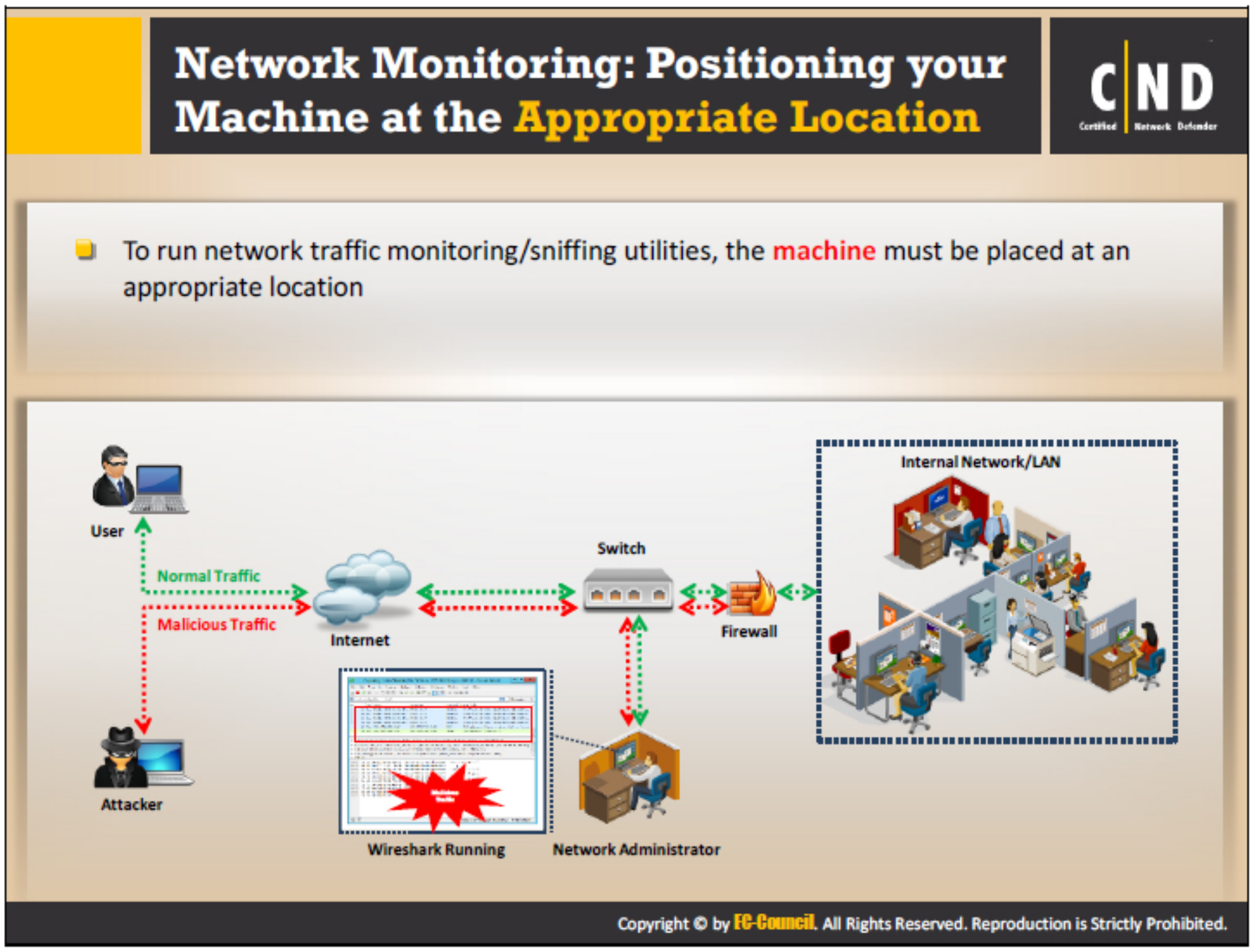
- **Netflow Exporter:** The Netflow exporter collects all the packets and transfers the data towards the collector.
- **Netflow Collector:** The Netflow collector involves pre-processing flow of data received from the Netflow exporter.
- **Analysis Console:** Administrators are responsible for the analysis console that analyzes the intrusion detection or traffic profiling.

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



Non-router based monitoring techniques use active or passive monitoring or a combination of these to monitor the network. The administrator uses a variety of tools to help them monitor their network performance and analyze traffic patterns. Typically, these tools involve packet sniffing, network monitoring and bandwidth monitoring. Network and bandwidth monitoring tools use SNMP to monitor devices, bandwidth, performance, availability for all devices and services. Packet sniffing tools are used to analyze the traffic pattern and identify anomalies in the network traffic.

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



Administrators should place and connect their system so they can view all the inbound and outbound traffic flowing through their network. Network administrators should ensure that each packet is inspected against policy violations. The machine must be placed as described in the figure below. It should connect to the switch in front of the firewall and is installed with the required packet sniffing and network monitoring tools.

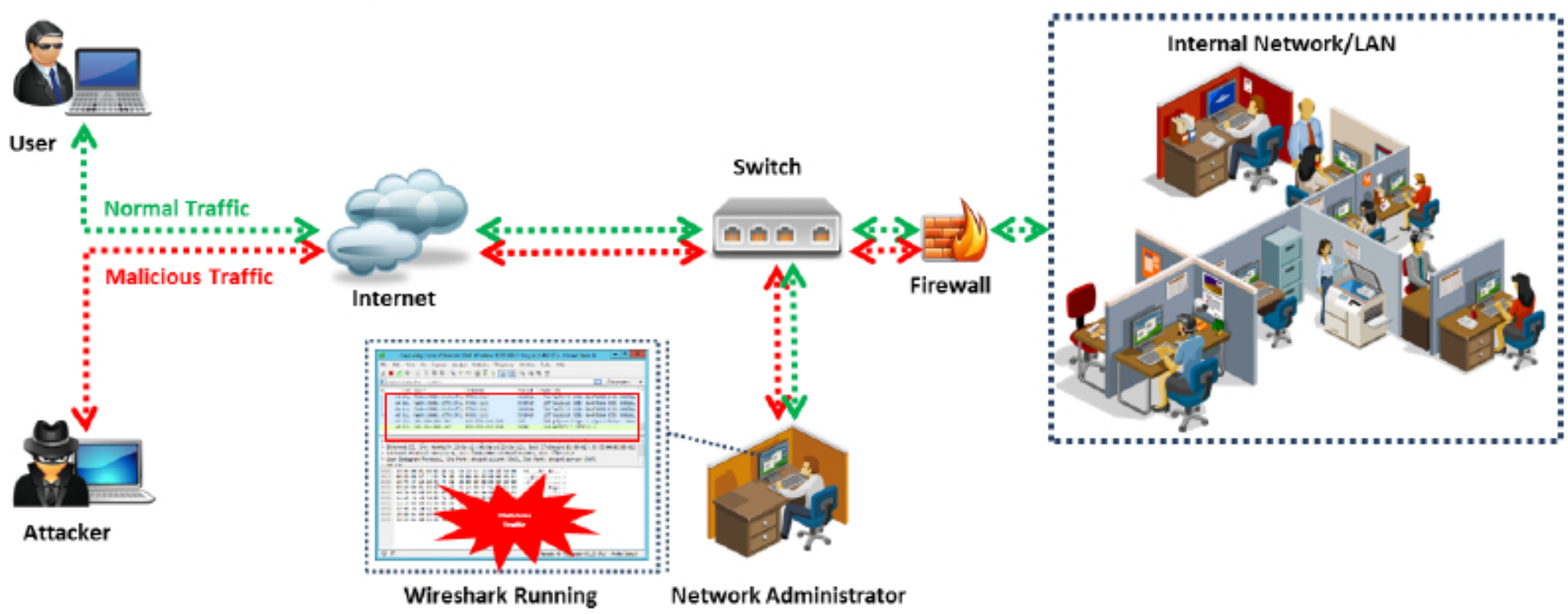
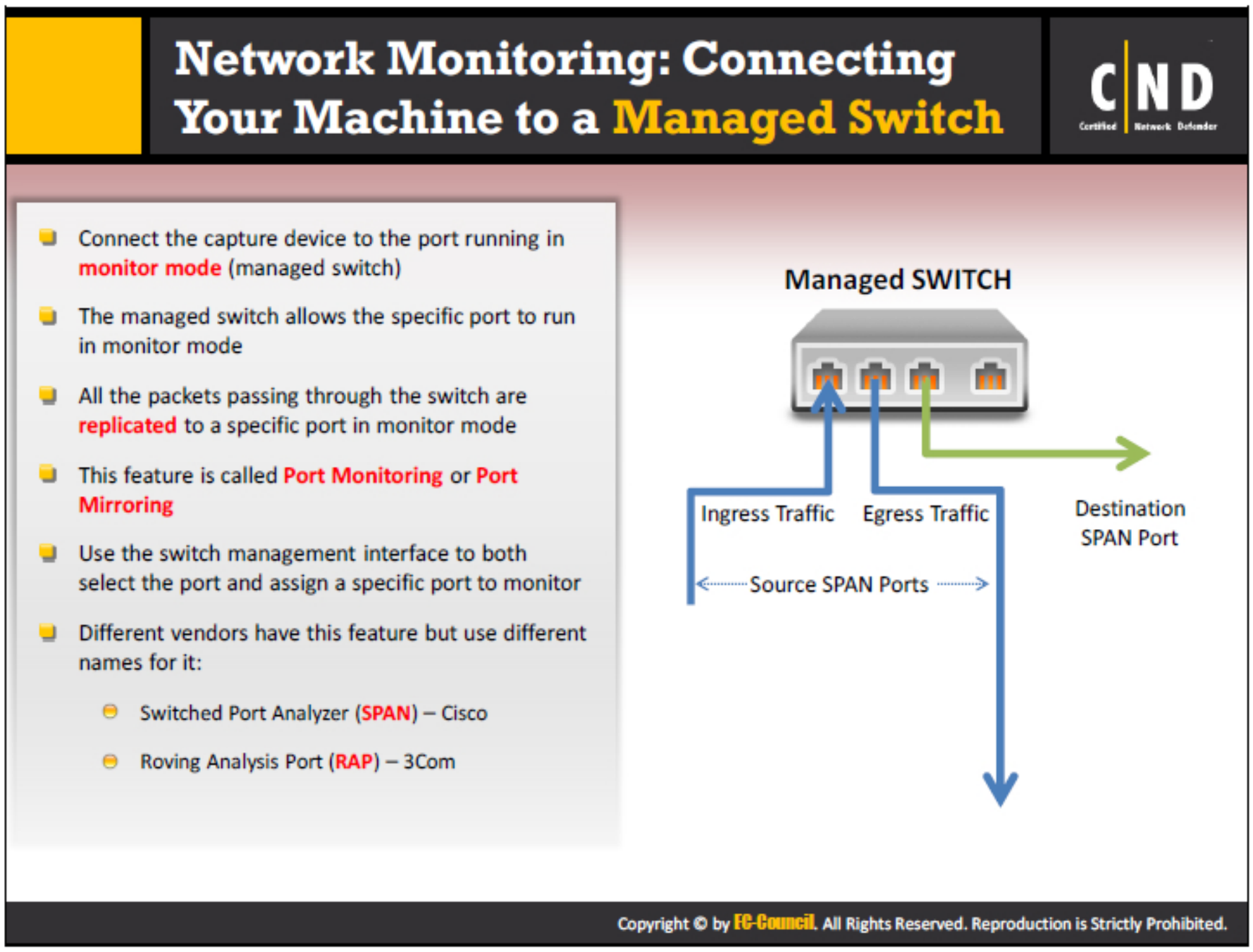


FIGURE 11.1: Deployment of machines at appropriate location

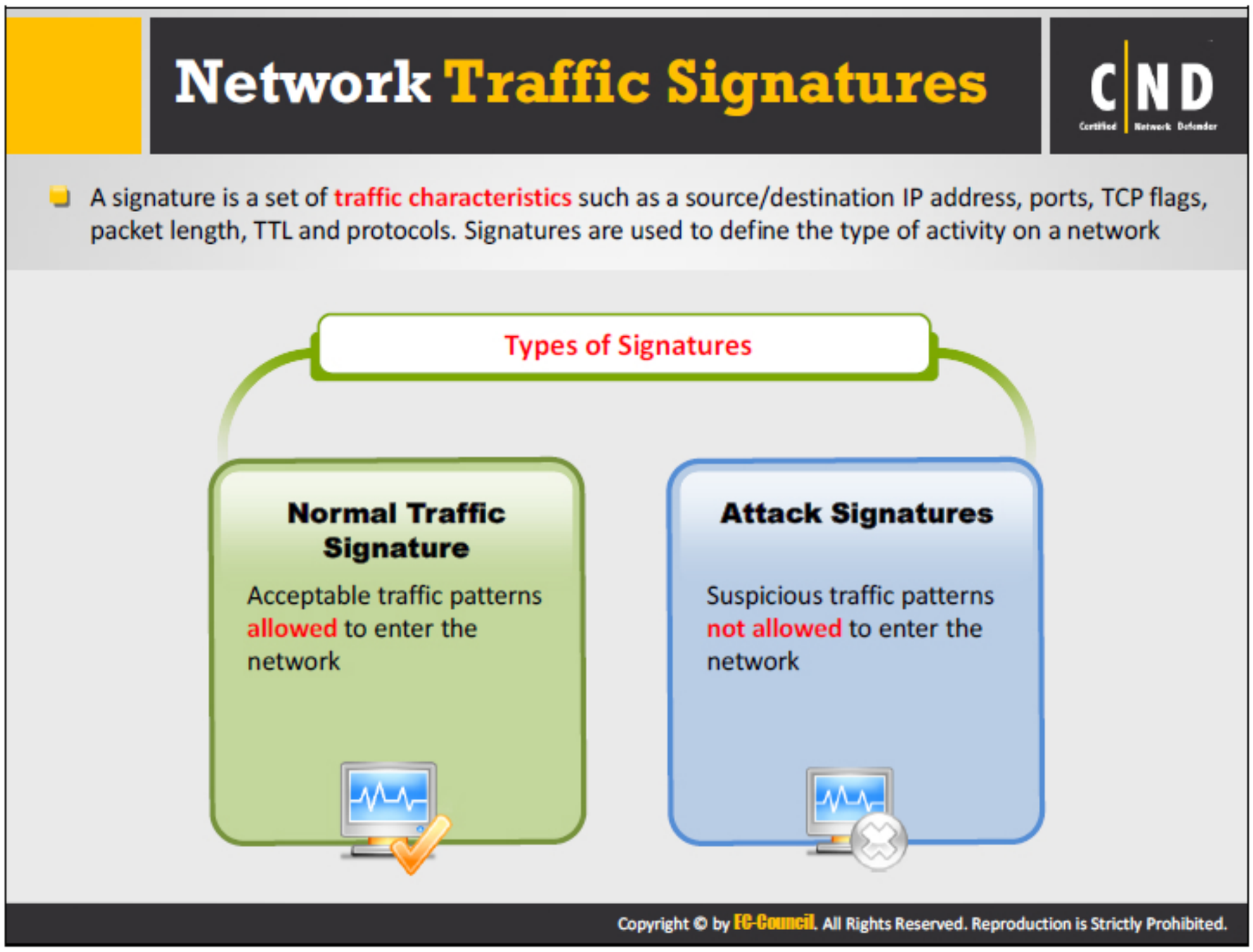
Certified Network Defender Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Administrators should ensure the switch is connected and configured as a managed switch. A managed switch can only view the network traffic flowing through the network. Configure the switch as a managed switch by enabling the port monitoring or port mirroring feature on a specific port in the switch. Different vendors have different names for this feature. For example, the port mirroring feature on a CISCO switch is known as a Switched Port Analyzer (SPAN) port. The port mirroring process includes copying the switch network traffic and sending it to another port in the switch so the monitoring tool can analyze it.

The managed switch can configure, manage, and monitor the LAN. It allows the administrator to have greater control over the flow of data traversing the network. With accessibility to manage the data flow, the chances of an intrusion are much lower. Though a managed switch may cost more than an unmanaged switch, it assures better security and filtered data transmissions among the system.

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



A signature is a set of characters that define network activity, including IP addresses, TCP flags, and port numbers. It includes a set of rules used to detect malicious traffic entering a network. Signatures are used to:

- Alert for unusual traffic on the network.
- Identify suspicious header characteristics in a packet.
- Configure an intrusion detection system to identify attacks or probes.
- Knowledge about a specific attack that happened or a vulnerability to be exploited.
- Match patterns in a packet analysis.

Type of Signatures

Signatures are classified into two main categories depending on their behavior:

- **Normal Traffic Signatures**: They include the normal network traffic regularly flowing to and from the network. These signatures are defined based on a normal traffic baseline for the organization. These signatures do not contain any malicious signature patterns and can be allowed to enter the network.
- **Attack Signatures**: The traffic patterns that look suspicious are generally treated as attack signatures. These signatures should not be allowed to enter the network. If allowed, they often are the reason for a network security breach. These signatures deviate from the normal signature behavior and should be analyzed.

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

Baselining Normal Traffic Signatures

- A network baseline is the accepted behavior for normal network traffic. It is a benchmark to differentiate between normal and suspicious traffic
- Network traffic baselines differ between organizations and change over time according to the operating environment and prevailing threat scenario

Some considerations to create a baseline for normal traffic:

- TCP/IP communication is a three-way handshake for normal traffic
- SYN flag appears at the beginning and the FIN flag is at the end of a connection
- All conversations originating inside the DMZ are trusted traffic items
- Any traffic violating the network policies indicates malicious traffic. For example, if there is FTP traffic where this type is restricted, indicates a potential issue
- Any DHCP traffic from unknown DHCP servers indicates a rogue DHCP server
- Mail traffic originating in the network but not sent to a mail server is suspect
- Any DNS traffic not sent to the DNS server is suspect
- Any outgoing traffic with internal addresses not matching the organization's address space may be malicious

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

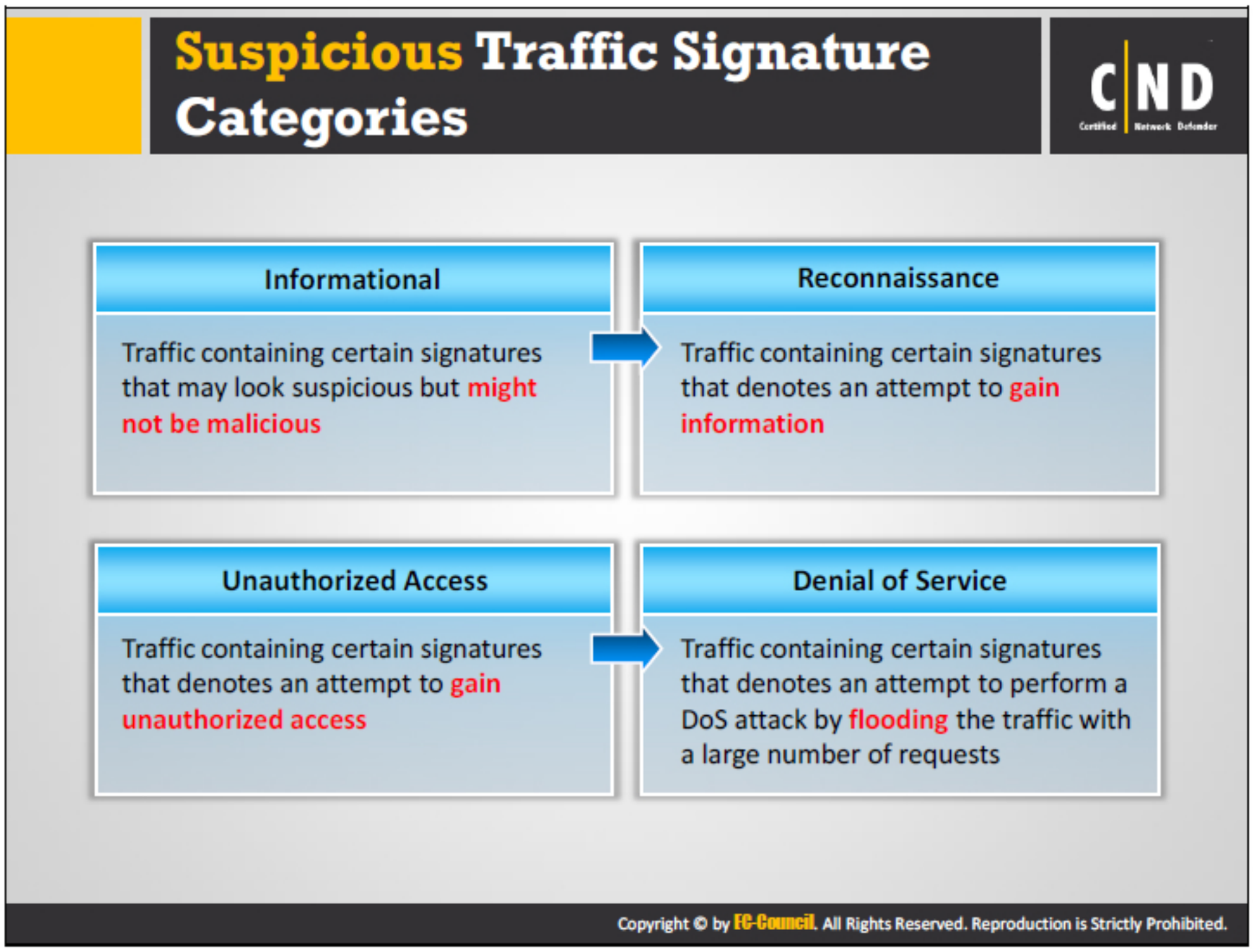
The network traffic baseline helps understand the behavioral patterns of the network. Baselining allows a set of metrics to monitor network performance. These metrics define the normal working condition of an enterprise's network traffic. The network traffic is compared with metrics to detect any changes in the traffic, which could be an alert to the security of the network. A network traffic baseline establishes the accepted packets, which are safe for the organization. Baselining the traffic makes it easier to detect suspicious activities on the network. Any deviation from the normal traffic baseline can be considered suspicious traffic signatures. The administrator should define a network baseline for their organization and validate the traffic against it. Baselining is more effective if it works in parallel with the organization's policy. With the help of normal traffic baselining administrators can judge the requirements needed to secure the network.

Although, there is no industry standard to measure network traffic performance baselines, there are network monitoring tools which provide estimates on what type of traffic is normal. A network traffic baseline should be defined for all incoming, outgoing, internet traffic and WAN links. The network traffic baseline should also contain the traffic for critical business data and backup systems.

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

- According to a network traffic baseline, normal traffic signatures for TCP packets should have the following characteristics:
  - To establish a three-way handshake TCP uses SYN, SYN ACK and ACK bits in every session.
  - The ACK bit should be set in every packet, except for the initial packet in which the SYN bit is set.
  - FIN ACK and ACK are used in a terminating the connection. PSH FIN and ACK may also be used initially in the same process.
  - RST and RST ACK are used to quickly end an on-going connection.
  - During the conversation (after a handshake and before termination) packets only contain an ACK bit by default. Sometimes they may also have a PSH or URG bit set.
- A suspicious TCP packet, has one or more of the following characteristics:
  - If both SYN and FIN bits are set, it is an illegal TCP packet.
  - SYN FIN PSH, SYN FIN RST, SIN FIN PSH RST are all variants of SIN FIN. An attacker sets these additional bits to avoid being detected.
  - A packet which has only a FIN flag is illegal as FIN can be used in network mapping, port scanning and other stealth activities.
  - Some packets have all six flags unset known as a NULL flag. These are illegal packets.
  - Source or destination port is zero.
  - If the ACK flag is set, then the acknowledgement number should not be zero.
  - If a packet only has the SYN bit set (which is at the beginning, to establish a connection), and any other data is present then it's an illegal packet.
  - If the destination address is a broadcast address (ending with 0 or 255) it's an illegal packet.
  - Every TCP packet has two bits reserved for future use. If any of them or both of them are set it's an illegal packet.

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



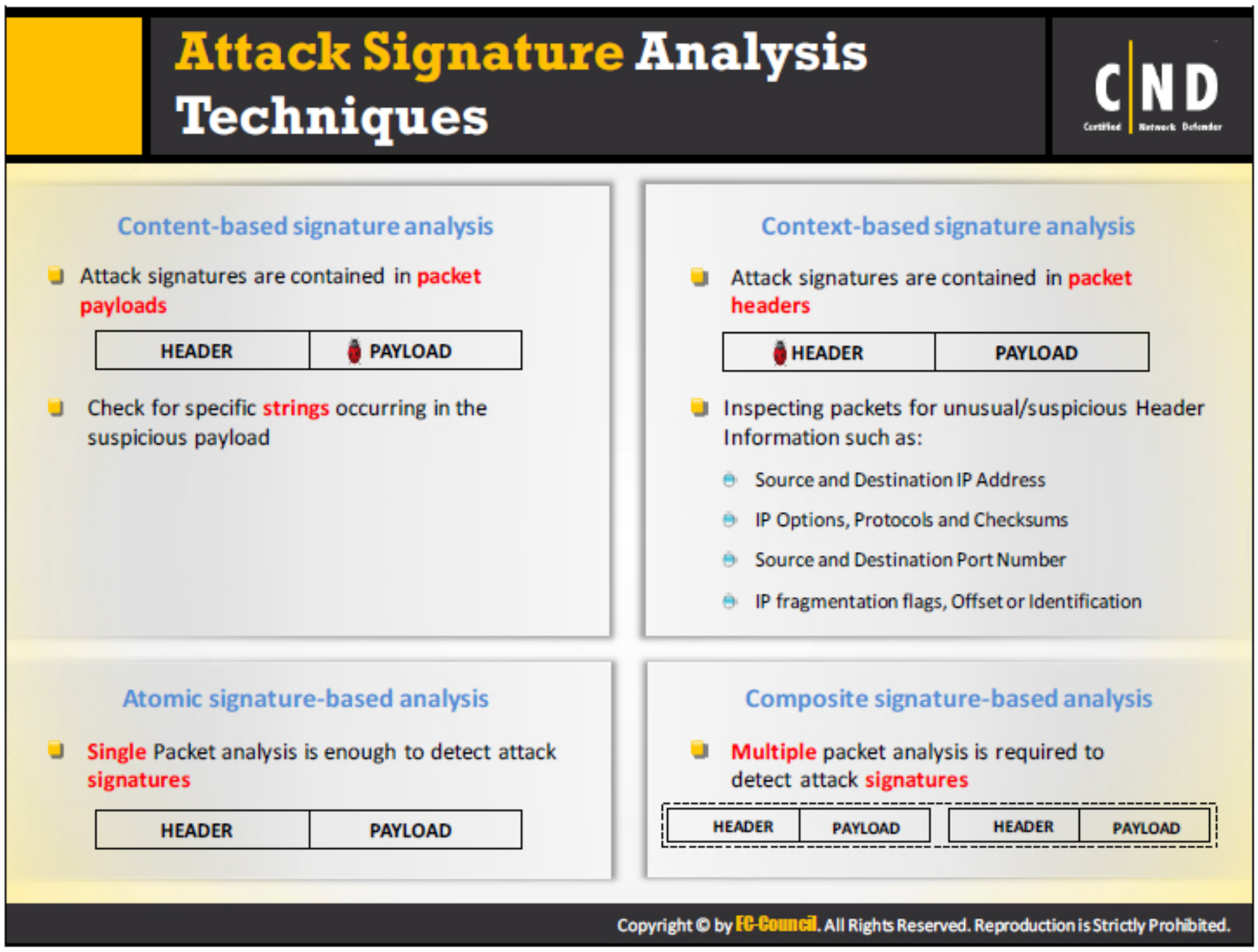
Network traffic deviating from its normal behavior, is categorized as a suspicious traffic signature. It is classified into four categories:

- **Informational:** The informational traffic signature detects normal network activity. Although this may not look suspicious, the data gathered through the information signature can be used for suspicious activities. For example, the informational traffic signatures may include:
  - ICMP echo requests
  - TCP connection requests
  - UDP connections
- **Reconnaissance**: The reconnaissance traffic consists of signatures which indicate an attempt to gain network access. Reconnaissance is an unauthorized discovery of vulnerabilities, mapping of systems and services. Reconnaissance is also known as information gathering and in most of these cases it normally precedes a network attack. For example, the reconnaissance traffic signatures may include:
  - Ping sweep attempts
  - Port scan attempts
  - DNS query attempts

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

- **Unauthorized Access:** Traffic may contain signs of someone attempting to gain unauthorized access, unauthorized data retrieval, system access or privileged escalation, etc. An attacker who does not have privileges to access an organization's network, usually generates this type of traffic with the intention of capturing sensitive data. For example, the unauthorized access traffic signatures may include:
  - Password cracking attempts
  - Sniffing attempts
- **Denial of Service:** Traffic may contain a large number of requests from a single or multiple sources as an attempt to perform a Denial of Service attack. This type of attempt is made to disrupt the service of the target organization. For example, the DoS traffic signatures may include:
  - Ping of Death attempts
  - SYN Flood attempts

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



Attack signature analysis techniques are classified into four different categories including:

- **Content-based Signature:** Content-based signatures are detected by analyzing the data in the payload and matching a text string to a specific set of characters. If undetected, these signatures can open backdoors in a system, providing administrative controls to an outsider.
- **Context-based Signature:** Packets are usually altered using the header information. Suspicious signatures in the header can include malicious data that can affect:
  - Source and destination IP addresses
  - Source and destination port numbers
  - IP options
  - IP protocols
  - IP, TCP and UDP checksums
- **Atomic Signature:** To detect an atomic signature, administrators need to analyze a single packet to determine if the signature includes malicious patterns. To detect these signature patterns, administrators do not require any knowledge of past or future activities.
- **Composite Signature:** In contrast to atomic signatures, administrators need to analyze a series of packets over a long period of time to detect attack signatures. Detecting these

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

attack patterns is very difficult. ICMP flooding is an example of the attacks performed using composite signatures. In this attack, multiple ICMP packets are sent to a single host so the server is busy responding to the requests.

Attacker signatures may be located in either the header or payload of the packet.

Unusual/Suspicious information in Header

The attacker can alter the packet header information to bypass the filter and get into the network. To detect packets with malicious header formats, administrators should have an understanding on the header fields they can modify. Header fields include suspicious signatures such as:

- Source and destination IP address
- Source and destination port number
- IP options, protocol, and checksums
- IP fragmentation flags, offset, or identification

Administrators should also have an understanding of the various attack signatures that may come through the header information. This helps them take remediation actions against suspicious packets.

Although an illegal header value is certainly a fundamental component of these signatures, administrators should also understand valid headers can also have suspicious header values. For example, suspicious connections to port numbers may provide a quick method to identify possible Trojan activity. Unfortunately, normal traffic may also use these odd port numbers. A detailed signature includes other characteristics of the traffic and is needed to determine the true nature of this traffic. Suspicious but legal values such as a port number are best used in combination with other values.

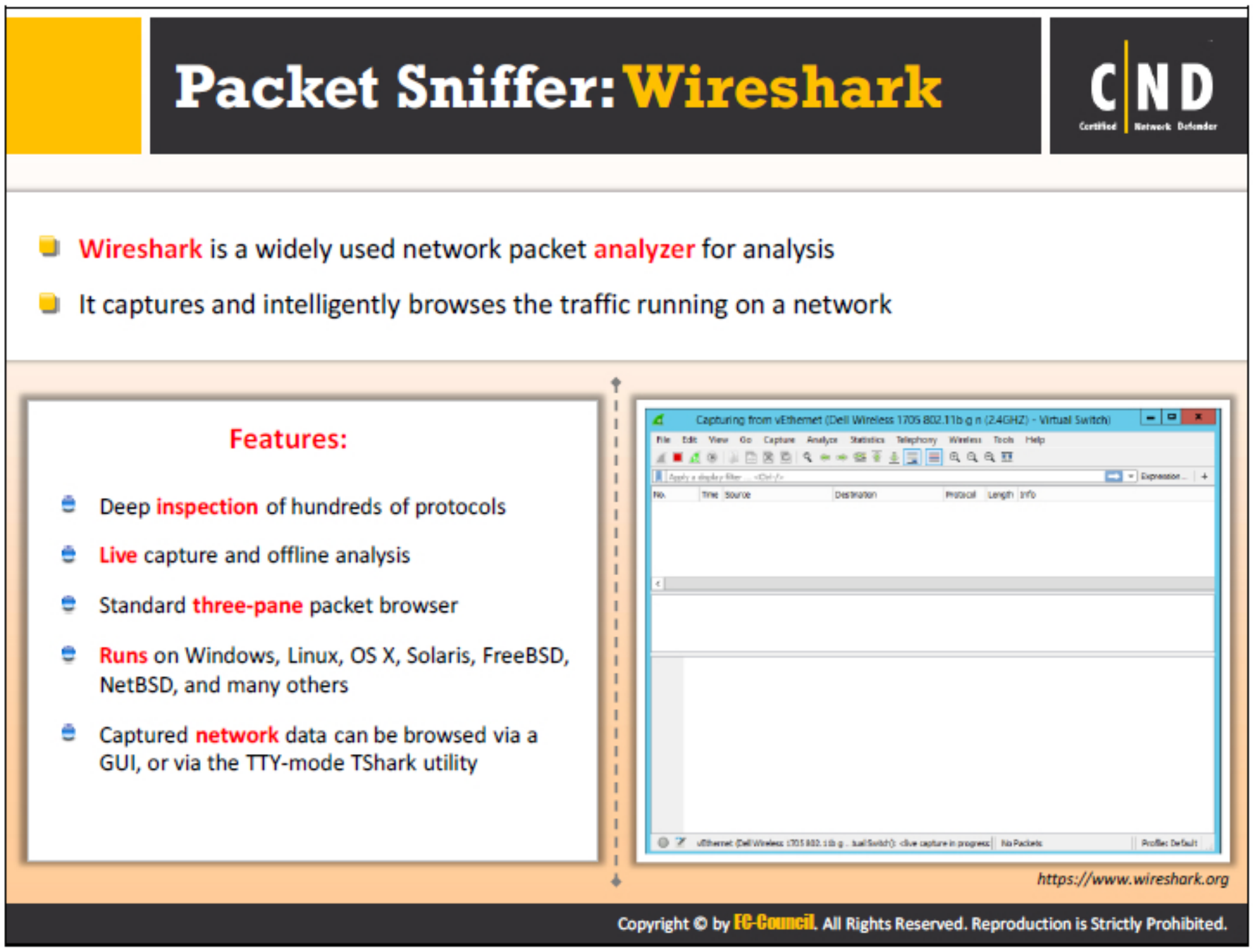
Suspicious Data in the Payload

Administrators should also have an understanding of the possible attack signatures that may come through data in the payload. They should check for specific strings occurring in the payload of each packet before allowing it through the network.

Administrators need to examine the packet payloads within TCP and UDP to identify suspicious payload values. They should understand that a protocol such as DNS is contained within TCP or UDP. Decoding a packet's IP header information, gives a clear indication of whether its payload contains TCP, UDP or another protocol. If the payload is TCP, administrators need to process some of the TCP header information within the IP payload before accessing the TCP payload. DNS data is contained within UDP and TCP payloads.

An example for this is a DNS buffer overflow attempt contained in the payload of a query. By parsing the DNS fields and checking the length of each, administrators can identify an attempt to perform a buffer overflow using a DNS field. Another method is to look for exploiting shellcode sequences in the payload.

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



A packet analyzer or packet sniffer is a tool that can intercept and log traffic passing through the network. The sniffer is used in network management because of its monitoring and analyzing features, which help to detect intrusions, supervise network contents, troubleshoot network and control traffic. Network administrators use them to analyze the behavior of an application or device causing network issues.

The information running through a network is a valuable source of evidence to counter intrusions or anomalous connections. The need to capture this information has led to the development of packet sniffers.

Wireshark

Wireshark is an open source cross-platform packet capture and analysis tool. It is available for Windows and Linux operating systems. The GUI window gives a detailed breakdown of the network protocol stack for each packet. Wireshark can also save packet data to a file for offline analysis as well as export and import packet captures to and from other tools. Statistics can also be generated for packet capture files.

Wireshark can be used for network troubleshooting, to investigate security issues and to analyze and understand network protocols. The packet sniffer can exploit information passed in plain text.

- **Features:**

  Wireshark has a rich feature set which includes the following:

  - Identify poor network performance due to high path latency

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

- Locate internetwork devices that drop packets
- Validate optimal configuration of network hosts
- Analyze application functionality and dependencies
- Optimize application behavior for best performance
- Analyze network capacity before application launch
- Verify application security during launch, log in and data transfer
- Identify unusual network traffic indicating potentially compromised hosts

Network Packet Capture Prerequisites

Setting up Wireshark to capture packets for the first time can be tricky. Here are a few common problems that are encountered while capturing packets with Wireshark for the first time:

- Administrators require special privileges to start a live capture.
- You need to choose the right network interface to capture packet data from.
- You need to capture at the correct location in the network to view the traffic you want to see.

Wireshark Network Analysis Activities

Capturing live network data is one of the major features of Wireshark. The Wireshark capture engine enables administrators to:

- Capture from different types of network hardware such as Ethernet or 802.11.
- Stop the capture based on different triggers such as the amount of captured data, elapsed time or the number of packets.
- Simultaneously show decoded packets while the capturing is in progress.
- Filter packets, reducing the amount of data to be captured.
- Save packets in multiple files during a long capture.
- Simultaneously capture from multiple network interfaces.

First Network Packet Capture using Wireshark

To capture packets using Wireshark, first install and launch the tool on your network. Select the appropriate network interface to capture traffic from. Different methods used to start capturing packets with Wireshark:

1. Double-click on an interface in the main window.
2. You can get an overview of the available interfaces using the Capture Interface dialog box.
3. Start a capture from this dialog box using the Start button.
4. You can immediately start a capture using your current settings by selecting **Capture → Start** or by clicking the first toolbar button.
5. If you already know the name of the capture interface, you can start Wireshark from the command line: `$ wireshark -i eth0 -k`

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

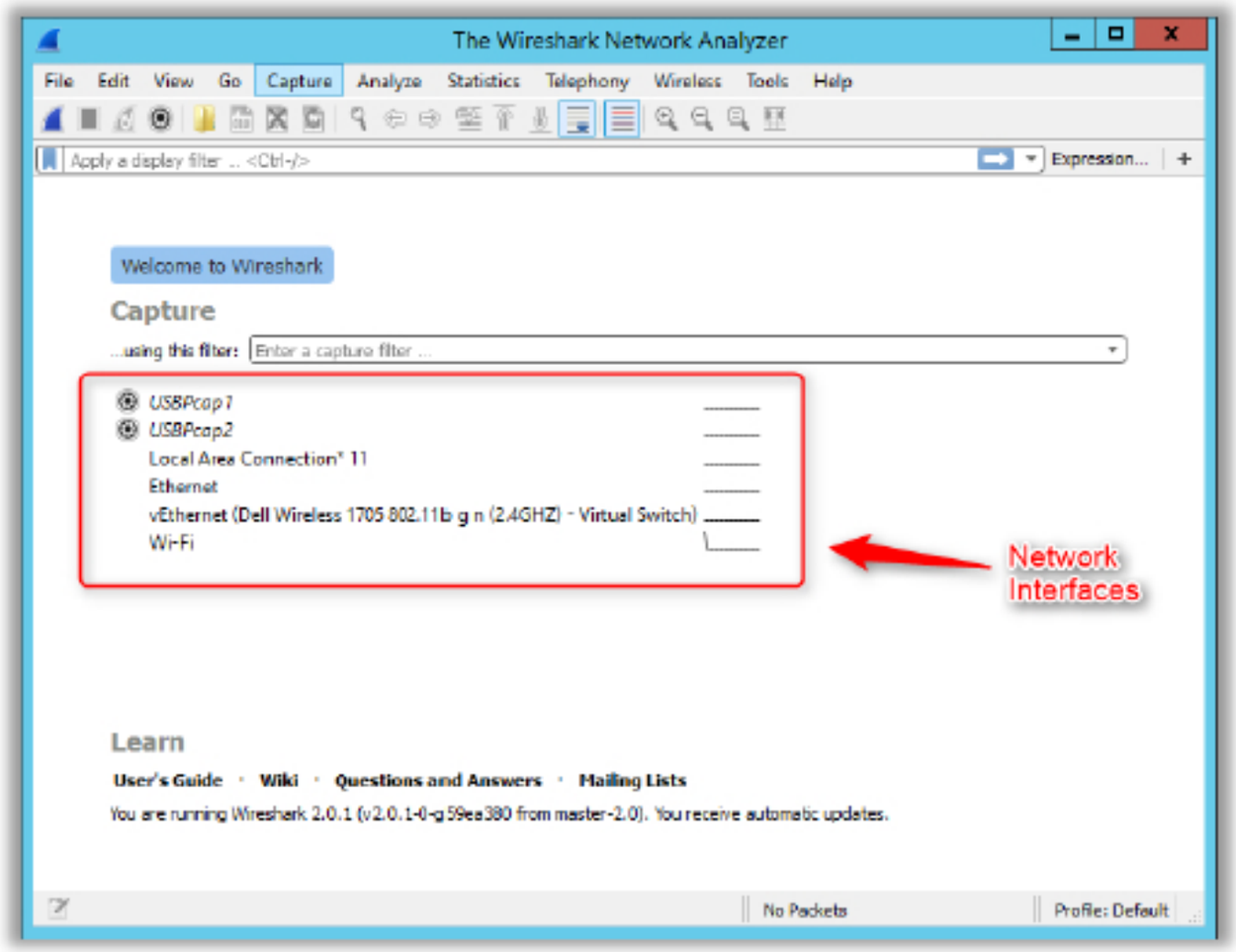


FIGURE 11.2: Wireshark network analyzer

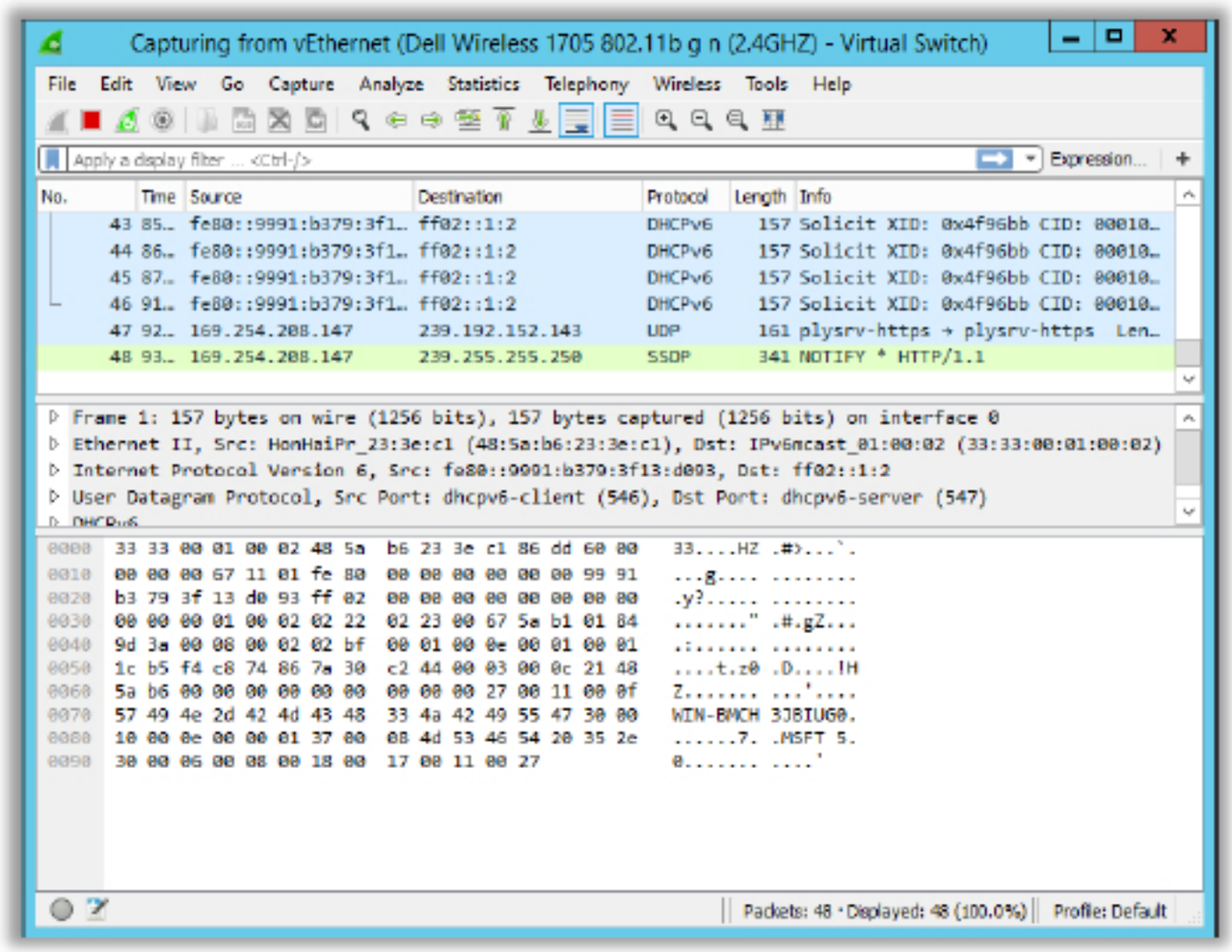
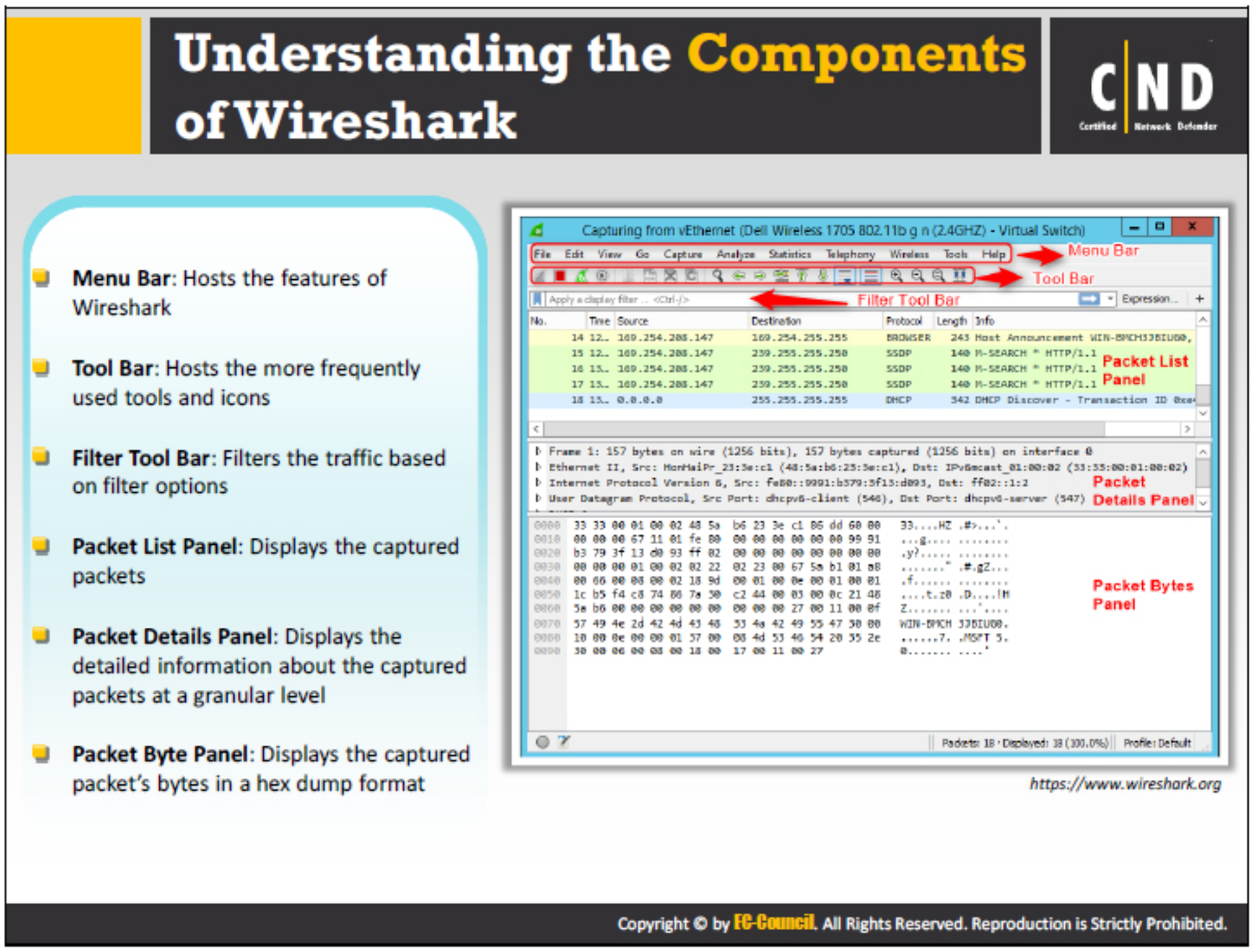


FIGURE 11.3: Capturing network interfaces

Source: *https://www.wireshark.org*

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



The main menu of the Wireshark tool contains the following items:

- **File:** This menu contains items to open and merge, capture files, save, print, import and export capture files in whole or in part, and to quit the Wireshark application.
- **Edit:** This menu contains items to find a packet, time reference or mark one or more packets. It handles the configuration profiles and sets your preferences.
- **View:** This menu controls the display of the captured data, including colorization of packets, font zoom, showing a packet in a separate window, expanding and collapsing the packet tree details.
- **Colorize Packet List:** This option allows administrators to control whether or not Wireshark should colorize the packet list. Enabling colorization will slow down the display of new packets while capturing and loading capture files.
- **Coloring Rules:** This option allows administrators to color packets in the packet list pane according to the filter expressions of their choice. It can be very useful for spotting certain types of packets.
- **Colorize Conversation:** This menu item brings up a submenu that allows the color of the packets to be changed in the packet list pane based on the addresses of the currently selected packet. This makes it easy to distinguish packets belonging to different conversations.

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

- **Go:** This menu contains options to navigate to a specific packet including a previous packet, next packet, corresponding packet, first packet and last packet.
- **Capture:** This menu allows the capture to start, stop and restart and edit capture filters.
  - **Capture Filters:** This option allows administrators to create and edit capture filters. Filters can be named and saved for future use.
- **Analyze:** This menu contains items to manipulate, display and apply filters, enable or disable the dissection of protocols, configure user specified decodes and follow a different stream including TCP, UDP and SSL.
  - **Follow TCP Stream:** This option displays all the TCP segments captured that are on the same TCP connection as a selected packet.
  - **Follow UDP Stream:** This option displays all the UDP segments captured that are on the same UDP connection as a selected packet.
  - **Follow SSL Stream:** This option displays all the SSL segments captured that are on the same SSL connection as a selected packet.
- **Statistics:** This menu contains options to display various statistic windows, including a summary of the packets that have been captured, display protocol hierarchy statistics, IO graphs, flow graphs and more.
- **Telephony:** This menu contains options to display various telephony related statistic windows, including a media analysis, flow diagrams, display protocol hierarchy statistics and more.
- **Wireless:** This menu shows Bluetooth and IEEE 802.11 wireless statistics.
- **Tools:** This menu contains various tools available in Wireshark, including creating firewall ACL rules and using the Lua interpreter.
  - **Firewall ACL Rules:** This allows you to create command-line ACL rules for many different firewall products, including Cisco IOS, Linux Netfilter, OpenBSD and Windows Firewall. Rules for MAC addresses, IPv4 addresses, TCP and UDP ports, and IPv4+port combinations are supported. It is assumed that the rules will be applied to an outside interface.
  - **Lua:** It includes options that allow administrators to work with the Lua interpreter, which is built-in to Wireshark. Wireshark uses Lua to write protocol dissectors.
- **Help:** This menu contains items to help the user, including access to basic help manual pages for the various command line tools, online access to some of the webpages and the About Wireshark dialog.
- **The Main Toolbar:** The main toolbar provides quick access to frequently used items from the menu. This toolbar cannot be customized by the user. If the space on the screen is needed to show more packet data, then hide the toolbar using the View menu. As in the menu, only the items useful in the current program state will be available. The others will be greyed out.

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

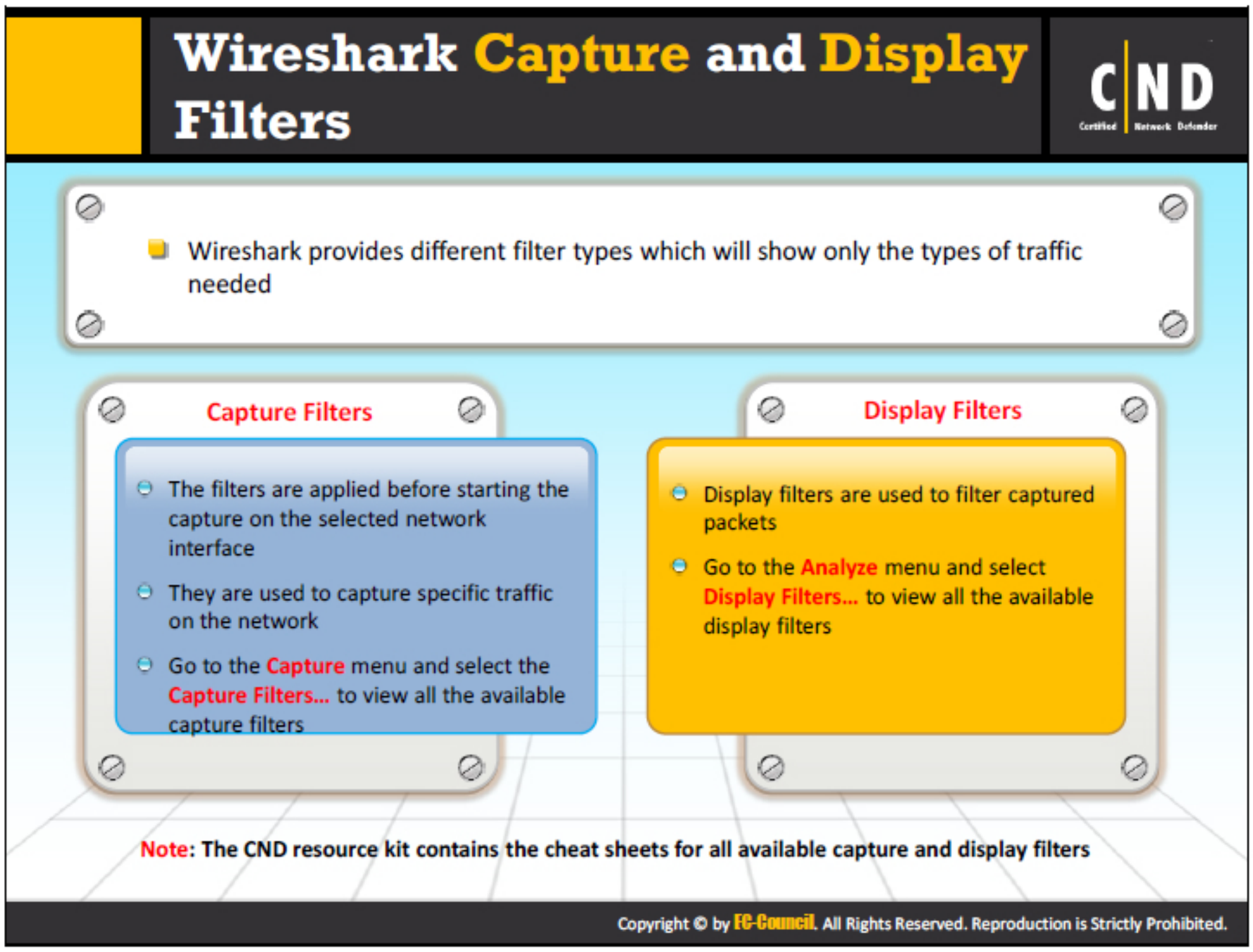
- **The Filter Toolbar:** The filter toolbar allows administrators to quickly edit and apply display filters.
- **Packet List Panel:** This is a list of packets in the current capture file. It colors the packets based on the protocol. Each line in the packet list corresponds to one packet in the capture file. If you select a line in this pane, more details will be displayed in the Packet Details and Packet Bytes panes.

  The default columns will show:

  - **No:** The number of the packets in the capture file. This number won't change, even if a display filter is used.
  - **Time**: The timestamp of the packet. The presentation format of this timestamp can be changed.
  - **Source:** The address where this packet is coming from.
  - **Destination**: The address where this packet is going to.
  - **Protocol**: The protocol name in a short version.
  - **Info**: Additional information about the packet content.
- **Packet Details Panel:** This views the details of the selected packet. It includes the different protocols making up the layers of data for this packet. The protocols and fields of the packet are displayed using a tree, which can be expanded and collapsed. Layers include Frame, Ethernet, IP, TCP, UDP, ICMP and application protocols such as HTTP.
- **Packet Bytes Panel:** This panel views the packet bytes in a hex dump and ASCII encodings. For a hex dump, the left side shows the offset in the packet data and the middle of the packet data is shown in a hexadecimal representation. On the right the corresponding ASCII characters are displayed.
- **The Status Bar:** The status bar displays informational messages. In general, the left side will show context related information, the middle part will show the current number of packets and the right side will show the selected configuration profile. Administrators can drag the handles between the text areas to change the size.

Source: *https://www.wireshark.org*

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



Wireshark provides the opportunity to use different types of filters to sort out the network traffic. The tool helps confine the search and shows only the desired traffic. By default, Wireshark provides Capture Filters and Display Filters to filter the traffic.

Administrators can define filters and give them labels for later use. This saves time in recreating and retyping the more complex filters used often.

Display Filters

Display filters are used on captured packets. These are useful when the need to apply filters before starting packet captures is not required. Capture all the packets that traverse on the network and then sort the captured items using display filters.

Display filters are used while displaying packets. They allow administrators to concentrate on the packets they are most interested in, while at the same time hiding the uninteresting ones. They allow administrators to select packets by:

- Protocol
- The presence of a field
- The value of a field
- A comparison between fields

To define a new filter or edit an existing one, select **Capture → Capture Filters or Analyze → Display Filters**. A dialog box will open with options to define new and edit existing filters.

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

The mechanism for defining and saving capture filters and display filters is almost identical. Administrators can use the "+" (plus) button to add new filters and the "-" (minus) button to remove any unwanted filters. The copy button is used to copy a selected filter. Administrators can edit existing filters by double-clicking on the filter. After creating a new filter or editing an existing filter, click OK to save the changes.

Capture Filters

Capture Filters are applied before starting a capture of the traffic on the selected network interface. You cannot apply capture filters directly on captured traffic. A capture filter should only be applied when the administrator knows what they are looking for. Administrators should be aware of all capture filters available, to quickly find network anomalies.

Wireshark uses the libpcap filter language for capture filters. A capture filter takes the form of a series of primitive expressions connected by conjunctions (and/or) and optionally preceded by 'not'. The syntax of a capture filters is: **`[not] primitive [and|or [not] primitive ...]`**

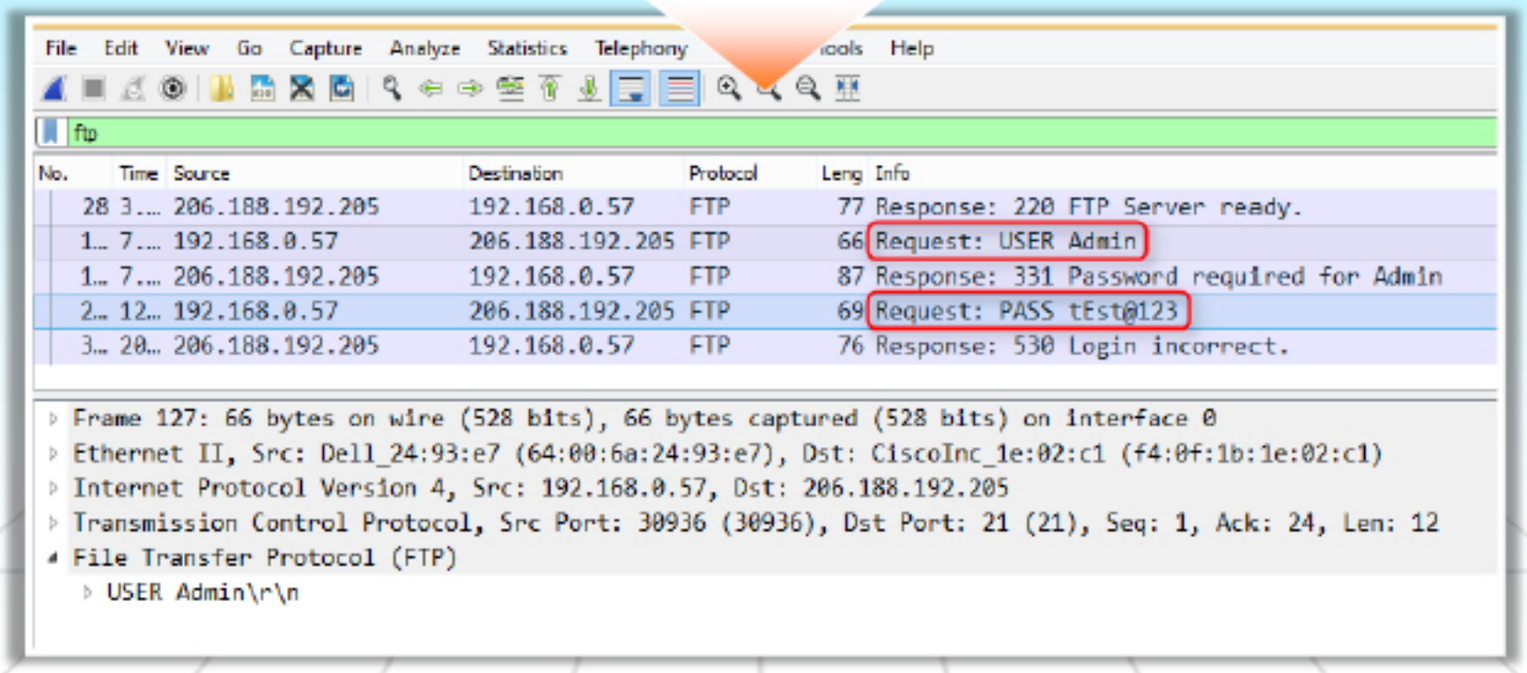
For example, a capture filter for Telnet that captures traffic to and from a particular host is: **`tcp port 23 and host 10.0.0.5`**

Source: *https://www.wireshark.org/*

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

Monitoring and Analyzing FTP Traffic

- The FTP protocol is used to transfer files over TCP and its default port is 21
- FTP causes security concerns especially where it is used in an organization
- FTP sends data in a clear text format and it is susceptible to sniffing
- Use the ftp filter to check whether any unauthorized FTP sessions have been established in the network



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

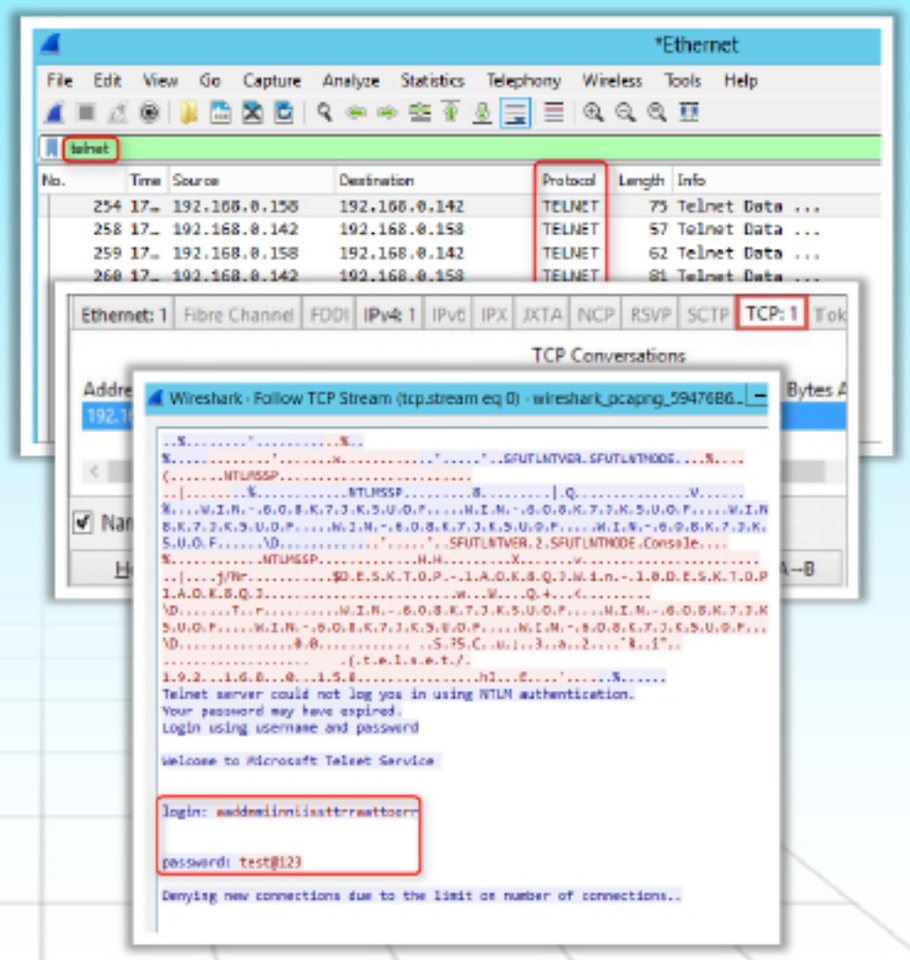
FTP doesn't offer a secure network environment nor does it offer secure user authentication. Individuals do not need authentication to access the FTP server in the network. This provides an easy method for attackers to get on the network and access resources. FTP does not provide encryption in the data transfer process. The data transfer between the sender and the receiver is in plain text. The critical information such as usernames and passwords is exposed to attackers. Implementation of FTP in an organization's network leaves the data accessible to external sources. Deploying FTP in a network can lead to types of attacks such as, FTP bounce, FTP brute force and packet sniffing.

Administrators should monitor the FTP traffic using Wireshark. It provides the administrator with complete information about the FTP traffic on the network. Applying a FTP filter helps detect unauthorized sessions running on the server. Apart from monitoring the traffic on the FTP server, administrators should also monitor the existing file content and the file size stored in the server.

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

Monitoring and Analyzing TELNET Traffic

- Telnet can provide access to a remote host, including most network equipment and operating systems
- Telnet is **not encrypted**, the password and all other data is transmitted as clear text
- Ideally it should be disabled, enabling it poses huge **security risks** to the network
- It becomes essential to check whether any telnet session is established within the network
- To check for established telnet sessions:
  - Go to the **Statistics** Menu and click on **Conversations**
  - Go to the **TCP tab** and select the appropriate Telnet communication indicated by port 23 and Click **Follow Stream...**
  - The Telnet traffic and the credentials in clear text will be viewable



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

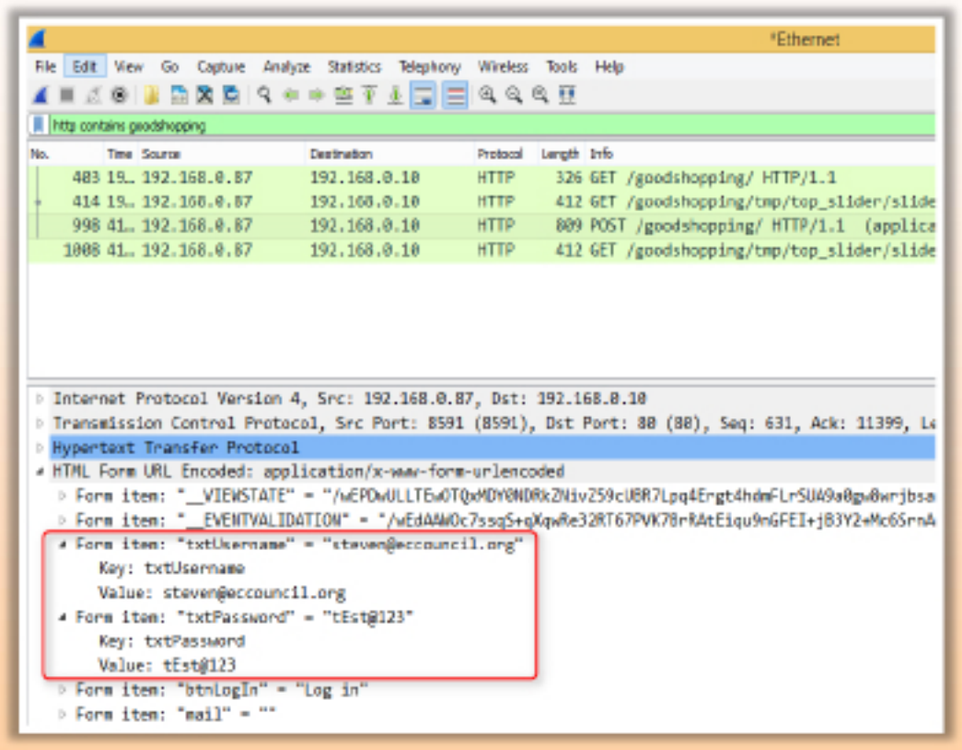
The Telnet protocol works on a client server model. It provides access to remote network equipment and operating systems. The data transferred through Telnet is not encrypted, making it easy for intruders to eavesdrop. If a person has access to a network device with Telnet configured, they can gain access to the network and user account information. Generally, Telnet should be disabled in the organization.

Telnet is a session oriented protocol, which means the connection has to be open during the entire session. Attackers can use Telnet open sessions to carry out a network security breach. Administrators should monitor Telnet sessions (if any) running on their network. Timely monitoring of Telnet sessions through Wireshark can greatly minimize the risk for a network intrusion.

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

Monitoring and Analyzing HTTP Traffic

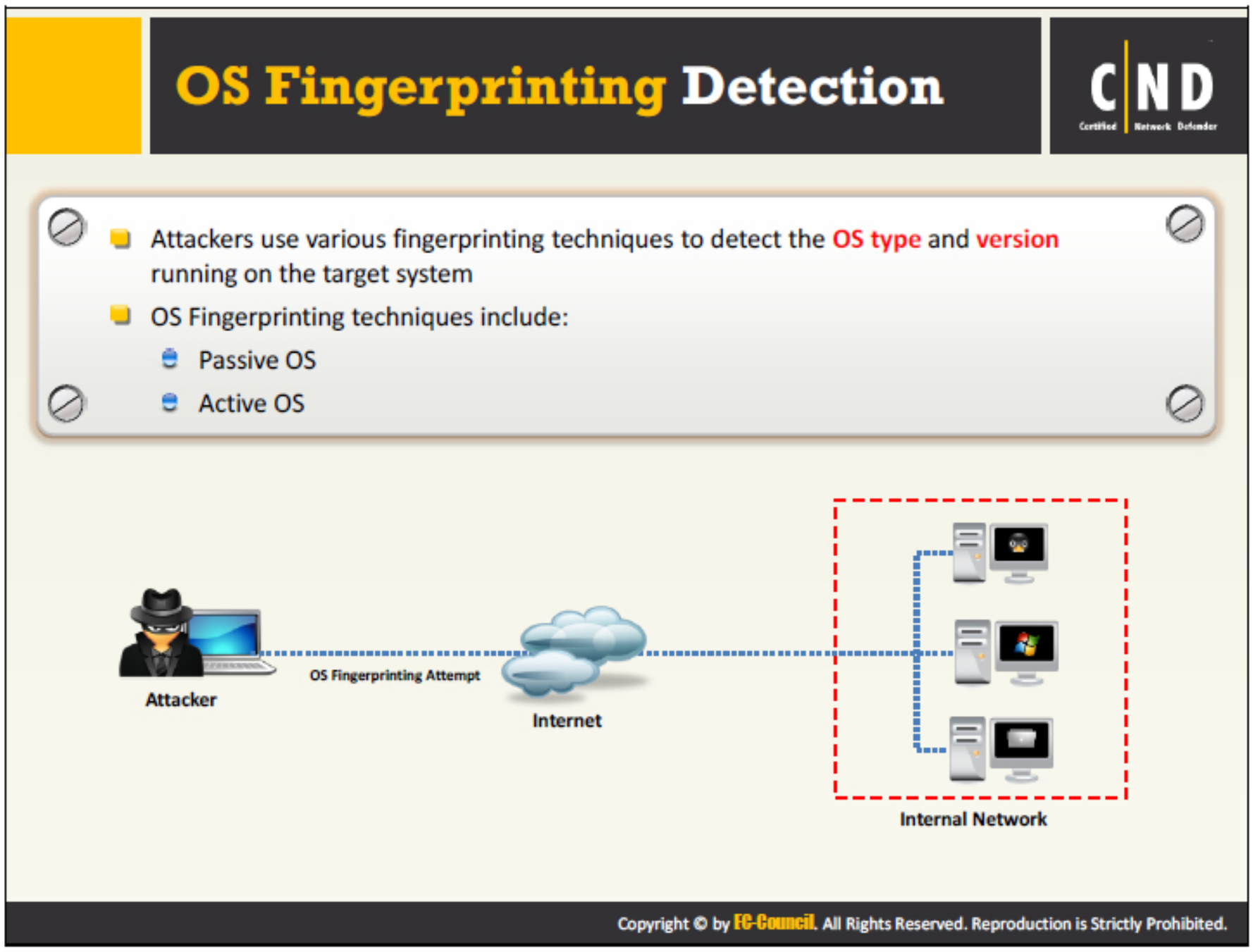
- HTTP sends information in plain text format
- Monitor and analyze HTTP traffic to:
  - Check if there is any sensitive information using HTTP
  - Detect malicious traffic
  - Check the traffic against a policy violation
  - Detect applications using unnecessary/restricted services
- Use the http filter to check the specific HTTP traffic



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

Applications implementing HTTP send data in clear text format. Implementing HTTP can pose security risks to the organization as sensitive information such as username and passwords are sent over as HTTP requests. The attacker can easily sniff the traffic and steal sensitive information for malicious use. Administrators have to ensure that their HTTP traffic is sent over an encrypted protocol such as HTTPS. At the same time, they should monitor and ensure their applications do not send data over HTTP. Monitoring the HTTP traffic also helps detect the volume of HTTP traffic flowing through the network.

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



OS fingerprinting is a process of gaining information about the target host's OS. Attackers use this method during their reconnaissance phase. Once the target OS is identified, the attacker can then find out what possible vulnerabilities exist in the OS or a specific version of the OS. An attacker can get into the network with the vulnerabilities existing in the OS. The attacker can attempt both active and passive OS Fingerprinting to detect the target OS.

Passive OS Fingerprinting

In this technique, the attacker does not send any packets to the target instead, they sniff the TCP/IP ports and analyze the default value for the various IP packet fields.

Active OS Fingerprinting

In this technique, the attacker sends packets to the target. If the target responds to the packets, the attacker analyzes the responses and identifies the underlying OS.

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

Detecting Passive OS Fingerprinting Attempts

- Check for certain fingerprinting values in Wireshark to detect passive OS fingerprinting attempts
- The table shows the common passive OS fingerprinting values

Protocol Header	Field	Default Value	Operating System
IP	Initial Time to Live	64	Nmap, BSD, Mac OS 10, Linux
		128	Novell, Windows
		255	CISCO IOS, Palm OS, Solaris
IP	Don't Fragment Flag	Set	BSD, Mac OS 10, Linux, Novell, Windows, Palm OS, Solaris
		Not set	Nmap, CISCO IOS
TCP	Maximum Segment Size	0	Nmap
		1440	Windows, Novell
		1460	BSD, Mac OS 10, Linux, Solaris
TCP	Window Size	1024-4096	Nmap
		65535	BSD, Mac OS 10
		2920-5840	Linux
		16384	Novell
		4128	Cisco IOS
		24820	Solaris
		Variable	Windows
TCP	Sack OK	Set	Linux, Windows. Open BSD
		Not set	Nmap, FreeBSD, MacOS 10, Novell,Cisco IOS, Solaris

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

In passive OS fingerprinting the attacker does not send any packets in the traffic rather, they sniff the TCP/IP ports. The detection of the target OS is done based on verifying the various IP header fields. The IP header consists of a field such as initial TTL, do not fragment flag, maximum segment size, window size, sack OK. The default values of these fields can help administrators to detect the fingerprinting attempt. Administrators should inspect these fields to detect OS fingerprinting attempts on their network. However, the default values for these fields may vary when the packet traverses between one router and another. It is very difficult to detect a passive fingerprinting attempt. Firewalls or other security devices cannot detect passive OS fingerprinting either. It has become essential for administrators to detect these attempts manually with the help of packet sniffing tools.

The following table shows the possible default values of the IP header fields for different types of OSes. This will help administrators compare and identify OS fingerprinting attempts.

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

Protocol Header	Field	Default Value	Operating System
IP	Initial Time to Live	64	Nmap, BSD, Mac OS 10, Linux
		128	Novell, Windows
		255	CISCO IOS, Palm OS, Solaris
IP	Don't Fragment Flag	Set	BSD, Mac OS 10, Linux, Novell, Windows, Palm OS, Solaris
		Not set	Nmap, CISCO IOS
TCP	Maximum Segment Size	0	Nmap
		1440	Windows, Novell
		1460	BSD, Mac OS 10, Linux, Solaris
TCP	Window Size	1024-4096	Nmap
		65535	BSD, Mac OS 10
		2920-5840	Linux
		16384	Novell
		4128	Cisco IOS
		24820	Solaris
		Variable	Windows
TCP	Sack OK	Set	Linux, Windows. Open BSD
		Not set	Nmap, FreeBSD, MacOS 10, Novell,Cisco IOS, Solaris

TABLE 11.1: Default values of IP header for different operating systems

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

Detecting Active OS Fingerprinting Attempts

- Wireshark can detect active OS fingerprinting attempts based on the probes sent by attackers
- An attacker may send ICMP probes and TCP probes to look for a response from the potential target OS
- Attackers make different types of active OS fingerprinting attempts on a target such as:
  - ICMP-Based
  - TCP-Based

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

In active OS fingerprinting, an attacker sends packets to the target and waits for the reply. They will then analyze the reply received from the target to determine the OS. An attacker performs active OS fingerprinting in two ways. They can either use ICMP probes or TCP probes to detect the target OS. The attacker then analyzes the reply from the target and makes an educated guess based on the reply obtained from the target.

Administrators can detect active OS fingerprinting attempts much easier compared to passive OS fingerprinting attempts. Administrators use specific Wireshark filters to filter out the OS fingerprinting traffic.

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

Detecting ICMP Based OS Fingerprinting

- Attackers send unique ICMP probes to the target and look for the response
- Use the following filter to locate unusual ICMP requests
  - `(icmp.type==8 && (!(icmp.code==8))`
  - `(icmp.type==13) || (icmp.type==15||(icmp.type==17)`
- Discover the unique ICMP probes, unusual ICMP code, ICMP timestamp requests(13), ICMP information requests(15) and ICMP address mask requests (917) from the traffic to make an educated guess to detect OS fingerprinting

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

An attacker can use various tools to perform ICMP based fingerprinting. These tools send a specific ICMP probe to the target. It depends upon how it manipulates the ICMP probe to detect the target OS.

- Some tools use unique ICMP probes.
- Some tools use ICMP echo requests with an unusual ICMP code.
- Some tools use ICMP Timestamp requests (13), ICMP Information requests (15), ICMP Address Mask requests (17), etc.

The administrator can use various traffic filters on ICMP and check for these types of ICMP requests being received from the outside.

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

Detecting TCP Based OS Fingerprinting

Attackers send TCP probes using specific field values in the header to look for the response and reveal details about the OS

The fields to look for when trying to find OS fingerprinting attempts are Initial Sequence Numbers, timestamp, IP ID sequence and TCP options

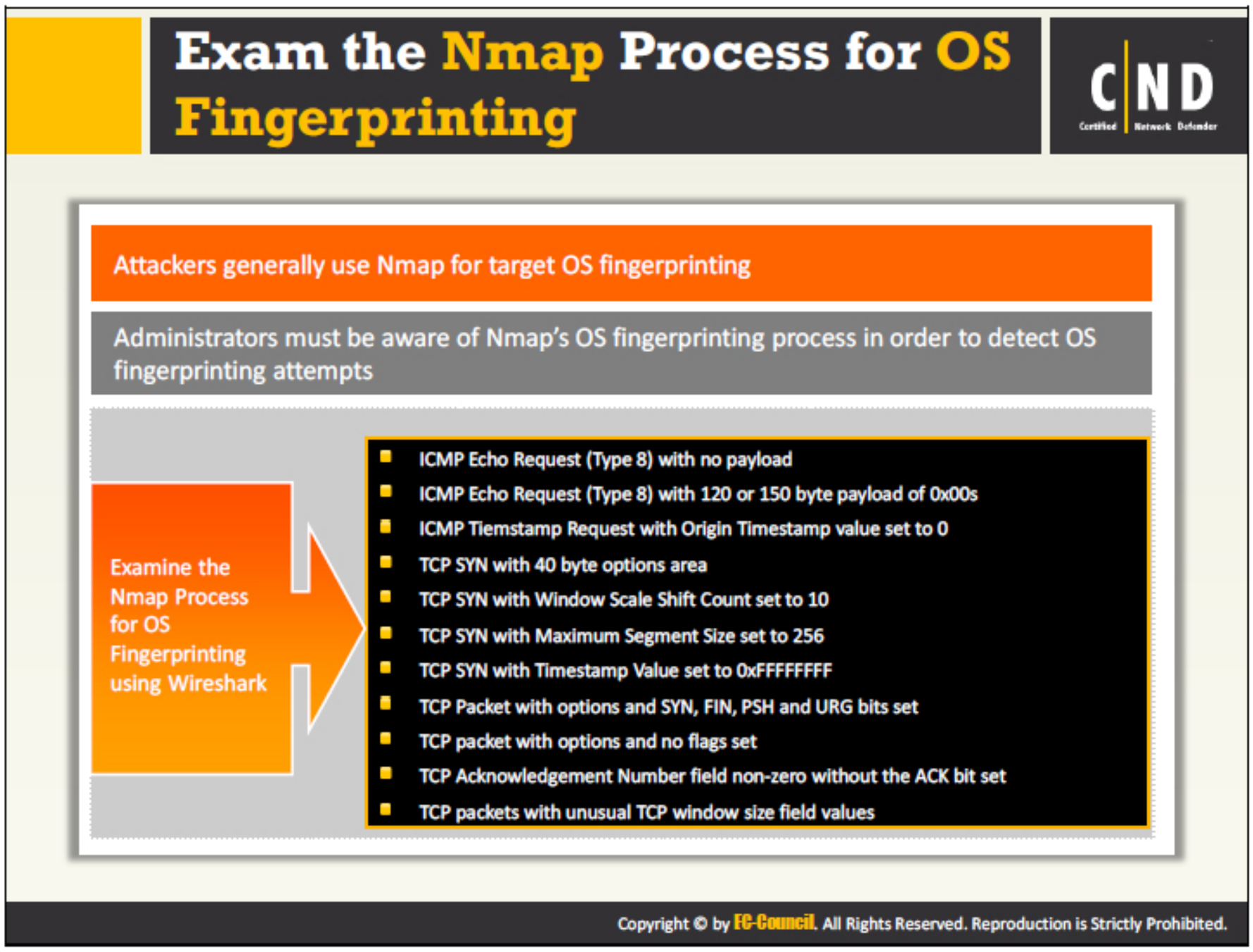
- Use the following filter to find OS fingerprinting attempts
  - `(tcp.flags==0x02) && (tcp.window_size <1025)`
  - `tcp.flags==0x2b`
  - `tcp.flags==0x00`
  - `tcp.options.wscale_val==10`
  - `tcp.options.mss_val<1460`

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

In TCP based OS fingerprinting, an attacker sends TCP probe packets to the target and then waits for the response. Based on the response received from the target, the attacker then makes a valid guess to determine the OS. An attacker may use a variety of tools to perform TCP-based fingerprinting such as Nmap and Queso. The attacker sends different types of TCP probes and based on the response received can detect the OS running on the target.

- **FIN Probe**: Sending a FIN without an ACK or SYN flag to an open port. Many broken OS implementations such as MS Windows, BSDI, CISCO, HP/UX, MVS, and IRIX replies back to a FIN probe with RESET.
- **BOGUS Flag Probe**: Sending a SYN Packet with an undefined TCP "flag" in the TCP header. The Linux OS version prior to 2.0.35 responds to this packet with the flag set.
- **TCP Initial Window**: Checking the size of the window field in the response.
- **TCP ISN Sampling**: Sending the connection request and then finding specific patterns in the initial sequence numbers in the response.
- **IPID Sampling**: Checking the IPID value for each packet in the response. Most operating systems increment a system-wide IPID value.
- **TCP Timestamp**: Checking the TCP timestamp option values in the response. It may be at frequencies of 2Hz, 100Hz, or 1000Hz, and still others return 0.
- **Don't Fragment bit:** Some OS set a “Don't Fragment" bit in the response.
- **ACK Value:** Checking the ACK field in the response.

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



In most cases, attackers generally use Nmap to perform target OS fingerprinting. It is necessary to understand how Nmap is used to perform OS fingerprinting. Knowing the Nmap process for OS fingerprinting will help to detect OS detection attempts made using Nmap.

The Nmap Process for OS Fingerprinting

Nmap sends a series of TCP and UDP packets to remote hosts and examines every bit in the response. Nmap compares the results for all the fields tested with its database **`nmap-os-db`**. If the database finds a match for the tested fields it gives the OS information. The database consists of a complete description for the OS, including the vendor name, OS generation, OS type and device type. OS fingerprinting is one of the main features of Nmap. The Nmap process depends on the response from the devices. The responses received will vary every time. If a Windows OS receives the response as a TCP ACK frame, the response of Linux for the same frame will be different. With these minor responses, Nmap builds detailed fingerprints for different operating systems.

Nmap investigates the TCP/IP stack of the systems by sending them eight different packets. Once the target machines receive the packets they either:

- Respond with a different TCP/IP stack respectively.
- Respond with a consistent TCP/IP stack.

This test allows Nmap to determine the accurate information for the operating system running on the machine and its version. The tests sent by the machine running Nmap are:

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

- **Tseq:** The machine sends a series of SYN packets to the targets to analyze their TCP sequence numbers.
- **T1:** A SYN packet with the options (WNMTE) is sent to an open TCP port.
- **T2:** A NULL packet with the options (WNMTE) is sent to an open TCP port.
- **T3:** A SYN, FIN, PSH, URG packet with the options (WNMTE) is sent to an open TCP port.
- **T4:** An ACK packet with the options (WNMTE) is sent to an open TCP port.
- **T5:** A SYN packet with the options (WNMTE) is sent to a closed TCP port.
- **T6:** An ACK packet with the options (WNMTE) is sent to a closed TCP port.
- **T7:** A FIN, PSH, URG packet with the options (WNMTE) is sent to a closed TCP port.
- **PU:** A packet to a closed UDP port.

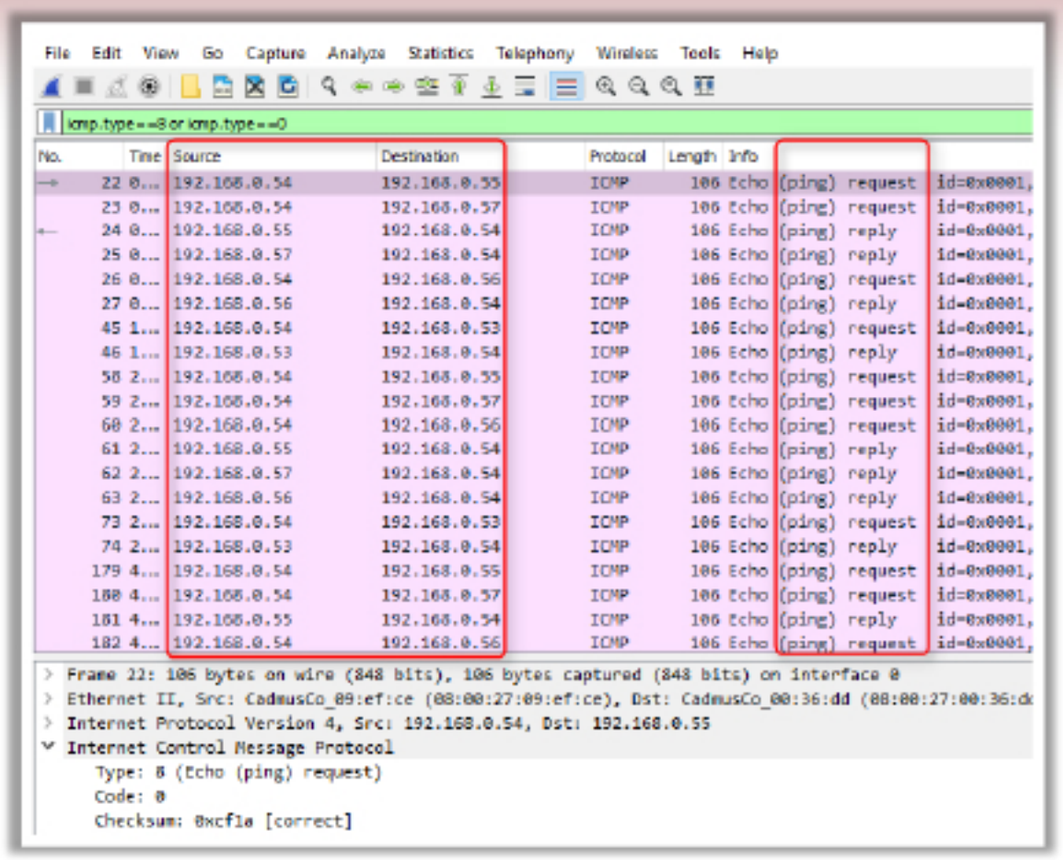
An attacker will use several methods to determine the target OS, few of them are:

- Did the target host respond?
- Did the target host have the "Don't Fragment" bit set?
- Window size of the target host.
- Status of the ACK number for the TCP packet sent to Nmap.
- Flags set in the TCP packet.

These methods can be applied to any operating system or the version of the operating system. All of the matched OS fingerprints are saved in a text file in Nmap called nmap-os-fingerprints.

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

Detecting a PING Sweep Attempt



- Attackers use a ping sweep to determine the live hosts within a specified IP range
- It is accomplished using ICMP, TCP or UDP
- Attackers send a series of ICMP, TCP or UDP echo requests to the specified IP range
- Use the filter `icmp.type==8 or icmp.type==0` to detect an ICMP ping sweep attempt
- Use the filter `tcp.dstport==7` to detect a TCP ping sweep attempt
- Use the filter `udp.dstport==7` to detect an UDP ping sweep attempt

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

A ping sweep scan helps attackers discover the active systems in the network. It involves sending multiple ICMP, TCP or UDP ECHO requests to target ports and then analyzing the ECHO reply obtained from the port.

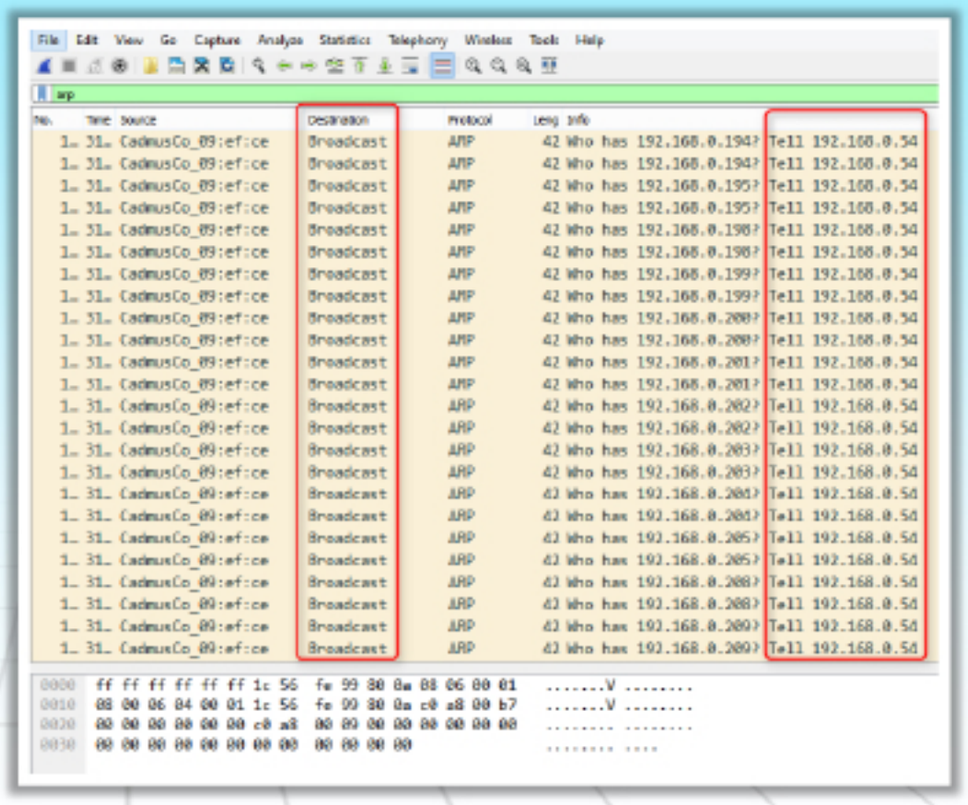
In an ICMP ping sweep, the attacker sends an ICMP type 8 ECHO request followed by an ICMP type 0 and analyzes the ECHO reply. To detect the ICMP ping sweep, find the ICMP type 8 and ICMP type 0 ECHO requests in the network traffic. It is recommended that a filter is used to accomplish this task. Use the filter **`icmp.type==8`** or **`icmp.type==0`** to detect an ICMP ping sweep attempt.

In a TCP/UDP ping sweep, an attacker sends an ECHO request packet to the TCP/UDP port 7. To detect the TCP/UDP ping sweep attempt, find the TCP ECHO request packets going to port 7 and the UDP ECHO request packets going to port 7 in the network traffic. Use the filter **`tcp.dstport==7`** to detect the TCP ping sweep and the filter **`udp.dstport==7`** to detect the UDP ping sweep attempts. If the target port doesn't support an ECHO reply, then this technique will not work.

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

Detecting an ARP Sweep/ ARP Scan Attempt

- An attacker's **ICMP ping sweep** will not work if a firewall is implemented in the network
- Attackers will then try an ARP sweep technique to scan hidden hosts behind the network firewall
- In the ARP sweep technique, an attacker sends an ARP broadcast request to every IP in the network. If they get an ARP response, then they know the host is live
- Use the **arp** filter to detect ARP sweep and ARP scan attempts on the network

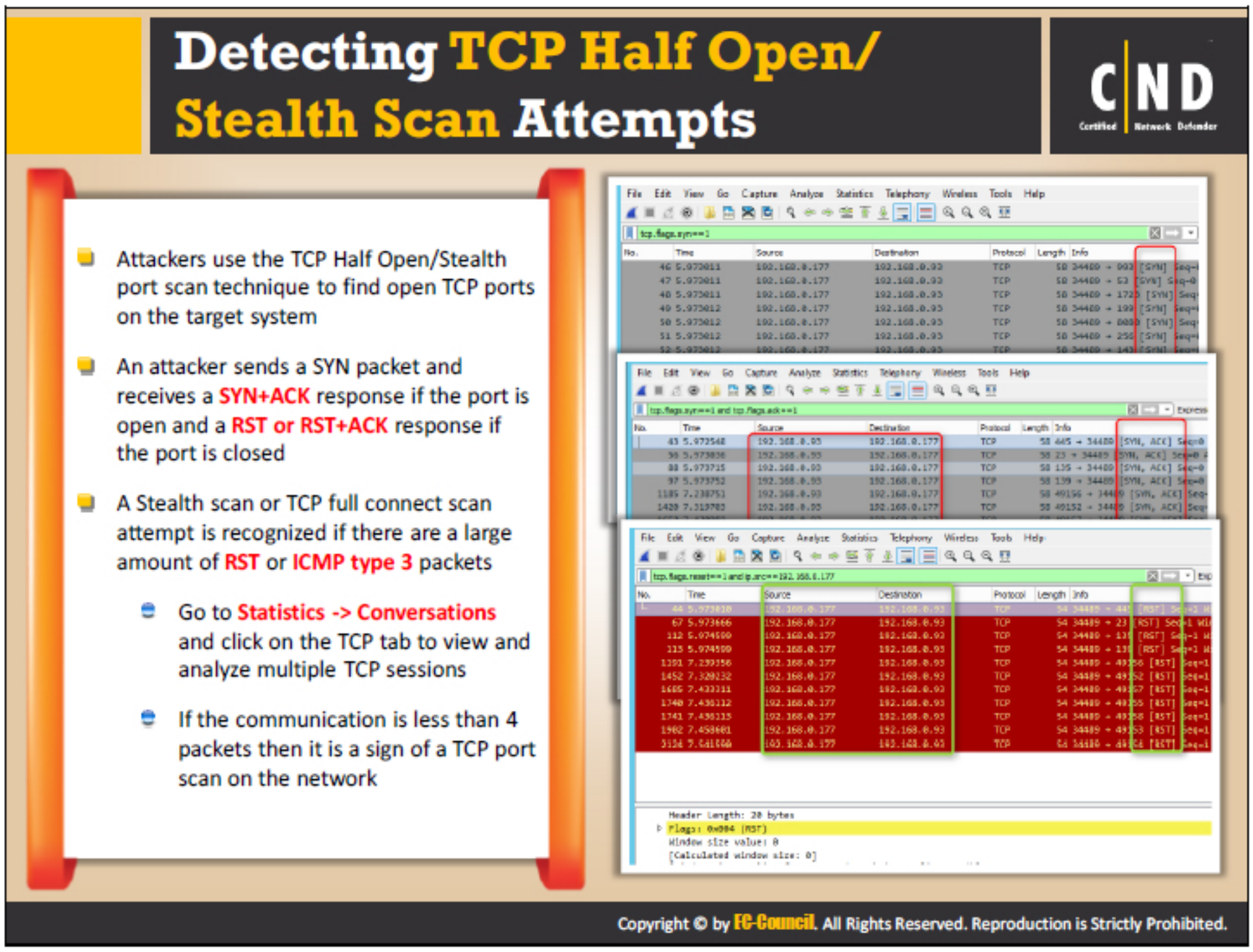


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Similar to a ping sweep scan, an attacker also uses an ARP Sweep/ARP Scan to locate active IPs in the network. Attackers use this method especially when a firewall is implemented in between them and the target network. If a firewall is implemented in the network the ping sweep method will not work. In an ARP sweep, an attacker broadcasts ARP packets to all the hosts in the selected subnet and waits for a response. If they get an ARP response from a specific host, this indicates the host is live.

ARP communications cannot be disabled to restrict an ARP sweep attempt on the network as all TCP/IP communication is based on it. If ARP communication is disabled, it will also break the TCP communication. However, administrators can easily monitor and detect this type of attempt using an ARP filter in Wireshark. If they detect an unexpected number of broadcast ARP requests, then they also know it indicates an ARP sweep attempt on the network.

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



The attacker uses a TCP Half Open/Stealth scan to detect open or closed TCP ports on the target system. It involves sending a SYN packet to the target port exactly like normal TCP communication and waits for the response. If they receive a SYN+ACK packet in the response, then it indicates the target port is open. If they receive a RST or RST+ACK packet in the response, then it indicates the port is closed. If the target port is behind a firewall, then they will receive an ICMP type 3 packet with a code 1, 2, 3, 9, 10 or 13 in the response.

The TCP half connection can act as an open gate for attackers to get in to the network. It is necessary for administrators to detect the TCP Half Open connection. If there are too many RST packets or ICMP type 3 response packets in Wireshark, then it can be a sign of a TCP Half Open/Stealth scan attempt on the network.

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

Detecting a TCP Full Connect Scan Attempt

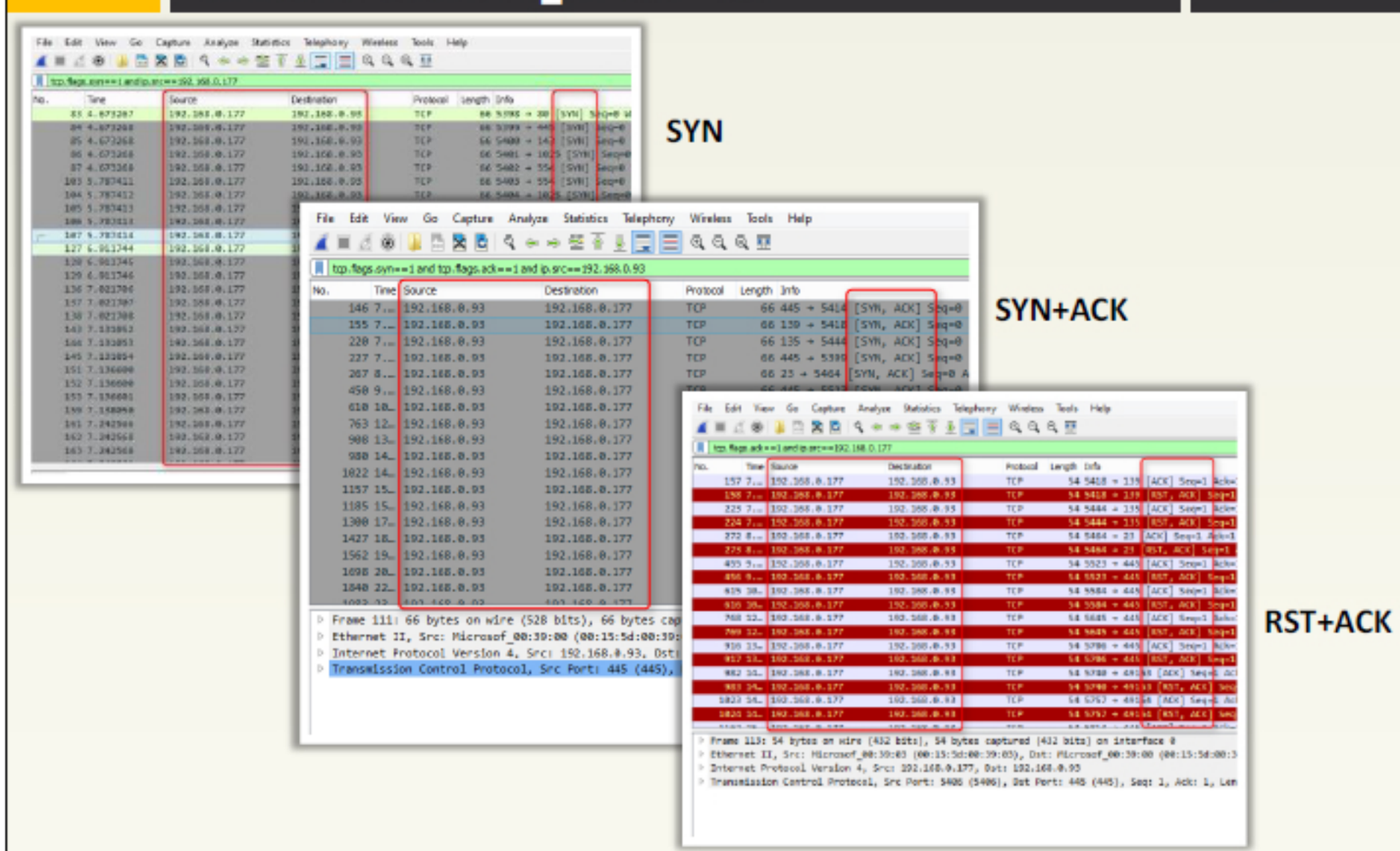
- In a TCP full connect scan, the attacker performs a complete three-way handshake to find open ports on the target system
- A TCP full connect scan is recognized using the same methods to detect a stealth scan or a TCP full connect scan attempt
- Check for **SYN+ACK**, **RST** & **RST+ACK** packets or **ICMP type 3** packets
- Use the following filters to quickly detect both TCP half open and TCP full connect scanning attempts on the network

- To check **SYN+ACK**, **RST** & **RST+ACK** packets in communication
  - `tcp.flags==0x002 or tcp.flags==0x012 or tcp. flags==0x004 or tcp.flags==0x014`
- To check **ICMP type 3** packets with a code 1,2,3,9,10, or 13 Packet
  - `icmp.type==3 and (icmp.code==1 or icmp.code==2 or icmp.code==3 or icmp.code==9 or icmp.code==10 or icmp.code==13)`

- To check **SYN+ACK**, **RST** & **RST+ACK** packets along with ICMP type 3 packets
  - `tcp.flags==0x002 or tcp.flags==0x012 or tcp. flags==0x004 or tcp.flags==0x014 or (icmp.type==3 and (icmp.code==1 or icmp.code==2 or icmp. code==3 or icmp.code==9 or icmp.code==10 or icmp.code==13))`

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

Detecting a TCP Full Connect Scan Attempt (Cont'd)



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

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

A TCP full connect scan or a TCP connect scan is the default scan that establishes a complete three-way handshake connection. A successful three-way handshake means that the port is open. To establish a TCP full connect scan, the attacker sends a SYN probe packet to the target port. If the port is open the attacker will receive a SYN/ACK packet in the response. It indicates the target port is open. The attacker will complete the communication by sending an ACK flag and will send a RST flag to terminate the session. If the port is closed, the attacker will receive the response as a RST/ACK. If the target port is behind a firewall, they will receive an ICMP type 3 packet with a code 1, 2, 3, 9, 10 or 13 in the response.

As a full TCP connection is established in the network, it is easy for an administrator to detect a TCP full connect scan attempt with the help of Wireshark. The following filters are used to detect a TCP Full Connect scan attempt:

Apply the filter for SYN, SYN+ACK and RST+ACK packets:

```
tcp.flags==0x002  or  tcp.flags==0x012  or  tcp.flags==0x004  or
tcp.flags==0x014
```

Apply the filter for ICMP type 3 packets:

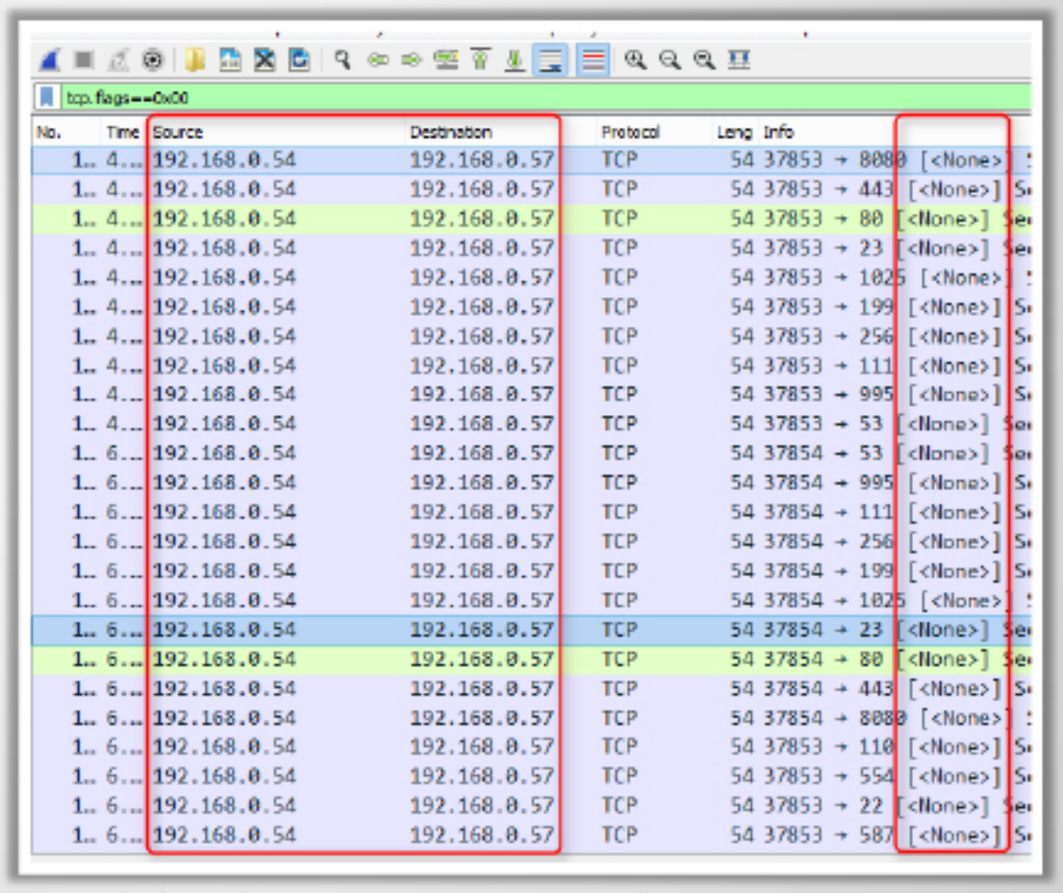
```
icmp.type==3  and  (icmp.code==1  or  icmp.code==2  or  icmp.code==3
or icmp.code==9 or icmp.code==10 or icmp.code==13)
```


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

Detecting a TCP Null Scan Attempt

- In a Null port scan an attacker sends a TCP packet without setting a flag on it
- If they receive a RST packet in response, then the port is closed. If there is no response, then the port is open or filtered
- Use the following filter to view the packets moving without a flag set

  `TCP.flags==0x000`

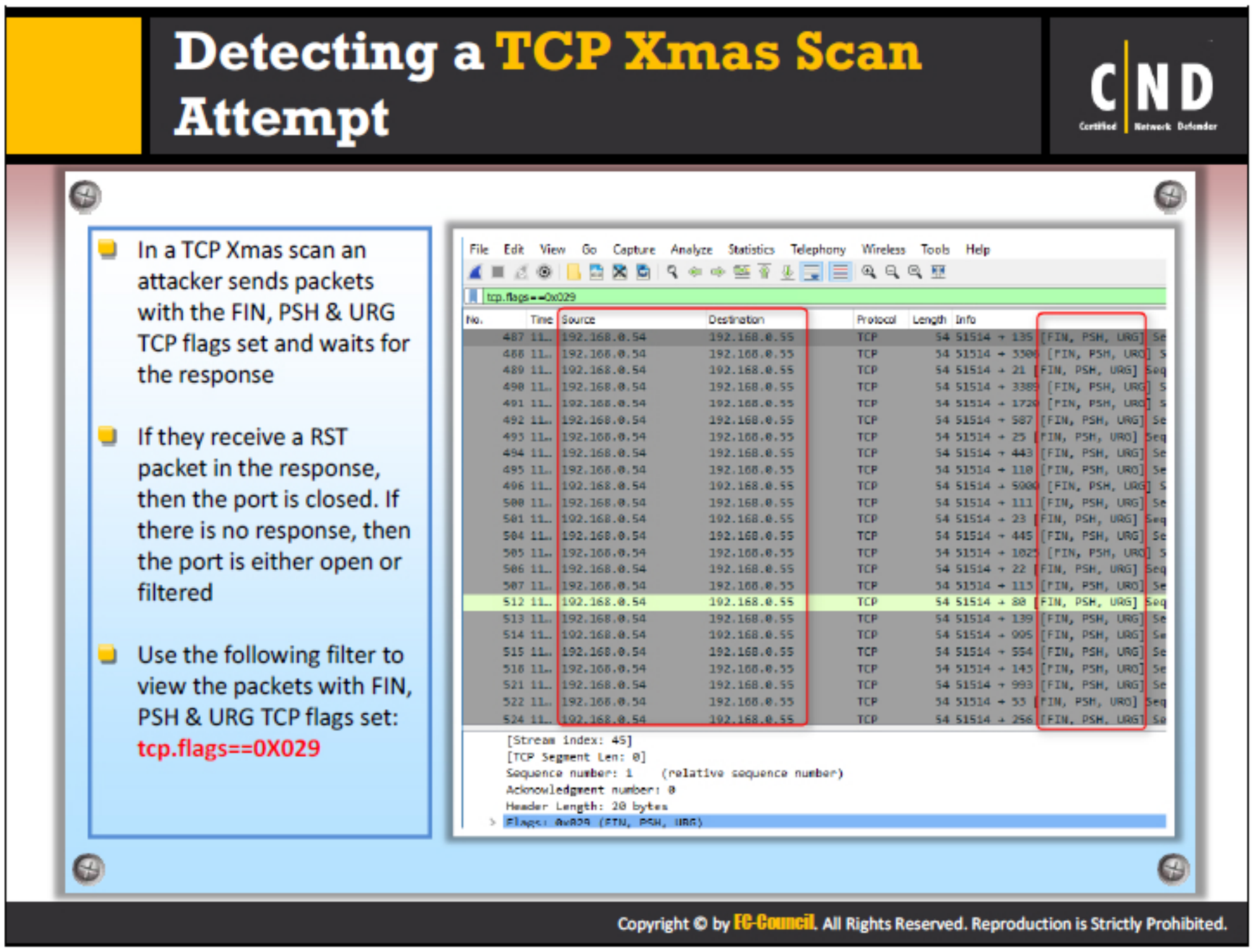


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

A TCP Null scan helps attackers identify the listening ports in the network. A TCP Null scan is a series of TCP scan packets containing a sequence number of 0 and no set flag. Since the null scan does not contain any set flags, it can penetrate through a router and a firewall that filter incoming packets with particular flags set.

In the TCP Null scan, the attacker sends a TCP packet to the target port. If the port is closed, it will receive a RST flag. If the port is open, the port will not respond because there are no flags sent with the packet. A TCP Null scan sets all the TCP headers (ACK, FIN, RST, SYN, URG, and PSH) to NULL. By applying the filter **`tcp.flags==0x000`** in Wireshark administrators can detect a TCP Null scan on UNIX servers. A TCP Null scan does not support Windows.

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



In the TCP Xmas scan, attackers scan the entire network and look for the machines that are up and running. It also scans for the services running on those machines.

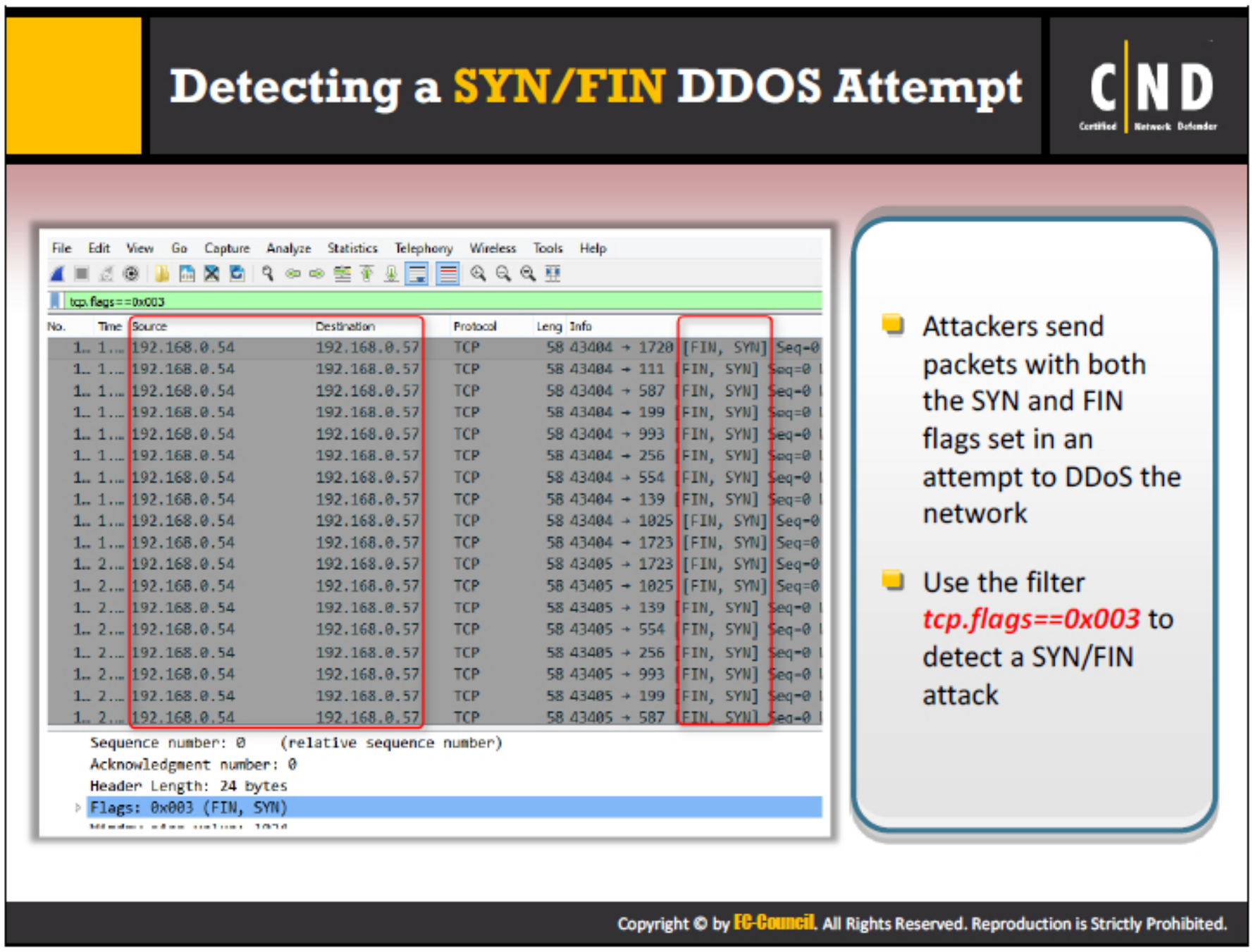
The Xmas scan involves sending packets set with URG, PSH, ACK and FIN flags. If the port is closed, it will receive a RST flag. If the port is open, the port will not respond as there are no flags sent with the packet.

The TCP Xmas can scan through the firewall and ACL filters. An ACL filter blocks the ports with the help of SYN packets. However, the FIN and ACK packets bypass this security.

FIN scans do not work on many operating systems. Operating Systems like Microsoft Windows send a RST flag to any malformed TCP segment. This makes it difficult for the attacker to distinguish between the open and closed ports.

Apply the filter **`tcp.flags==0X029`** in Wireshark to detect a TCP Xmas scan attempt.

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



In a SYN attack, the attacker sends a succession of SYN requests to a target's system in order to make the system unavailable for legitimate users. It exploits a known weakness in the TCP connection.

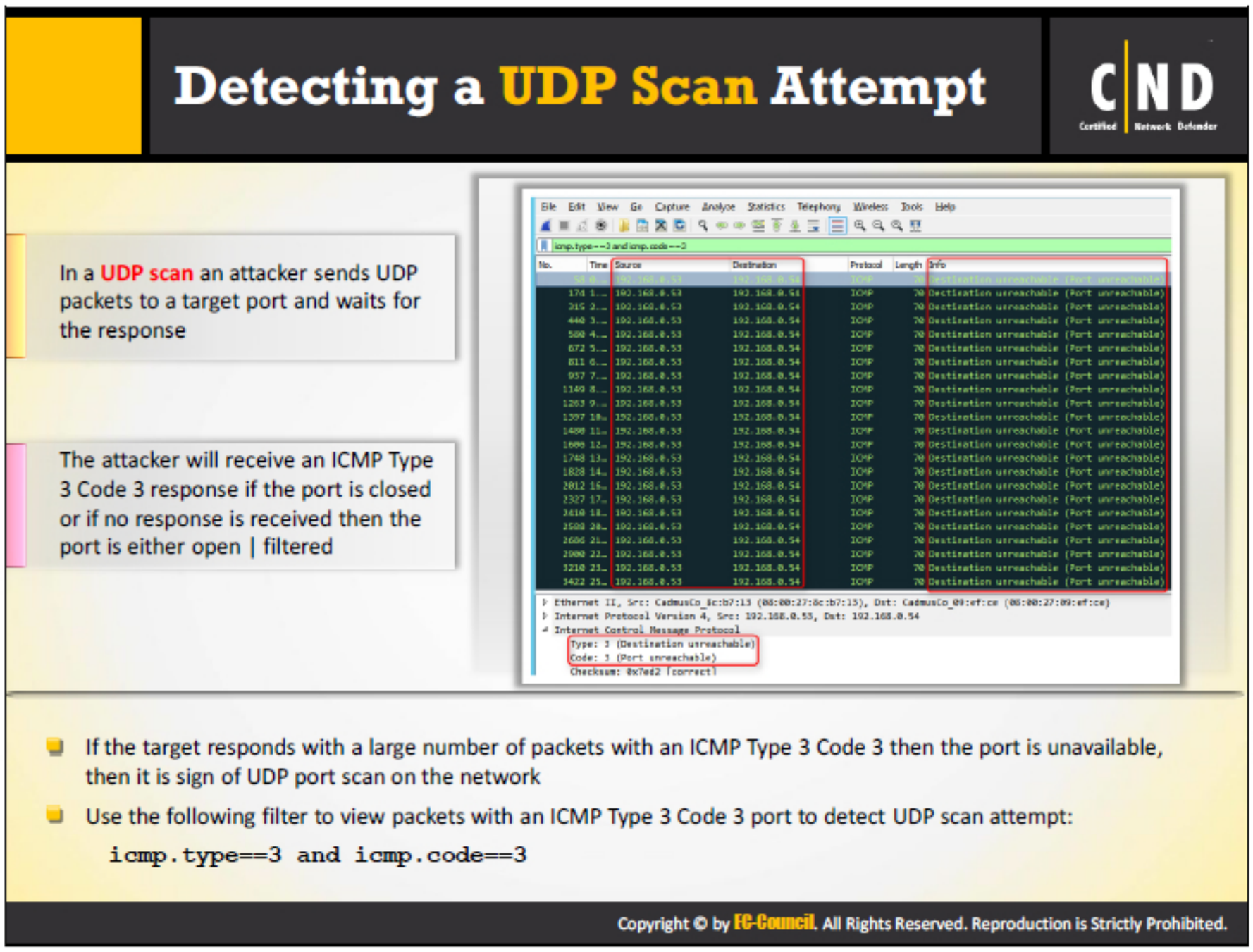
Typical TCP communication (TCP three-way handshake) works as follows:

1. Client sends the SYN packet to request a connection
2. Server responds back with SYN-ACK
3. Client then responds with an ACK to establish the connection

The SYN flood attack is initiated by not responding to the server with an expected ACK in the last step of the TCP communication. The server will wait for the acknowledgement, causing network congestion problems.

The SYN flag establishes a connection and the FIN flag terminates the connection. In a SYN/FIN DDoS attempt, the attacker floods the network by setting both the SYN and FIN flags. In a typical TCP communication, both the SYN and FIN are not set simultaneously. If an administrator detects traffic with both a SYN and FIN flags set, then it is a sign of a SYN/FIN DDoS attempt. The SYN/FIN DDoS attempt can exhaust the firewall on the server by sending the packets regularly. To detect such suspicious attacks, you should use the filter **`tcp.flags==0X003`** to find out if these traffic entries are in the same packet.

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

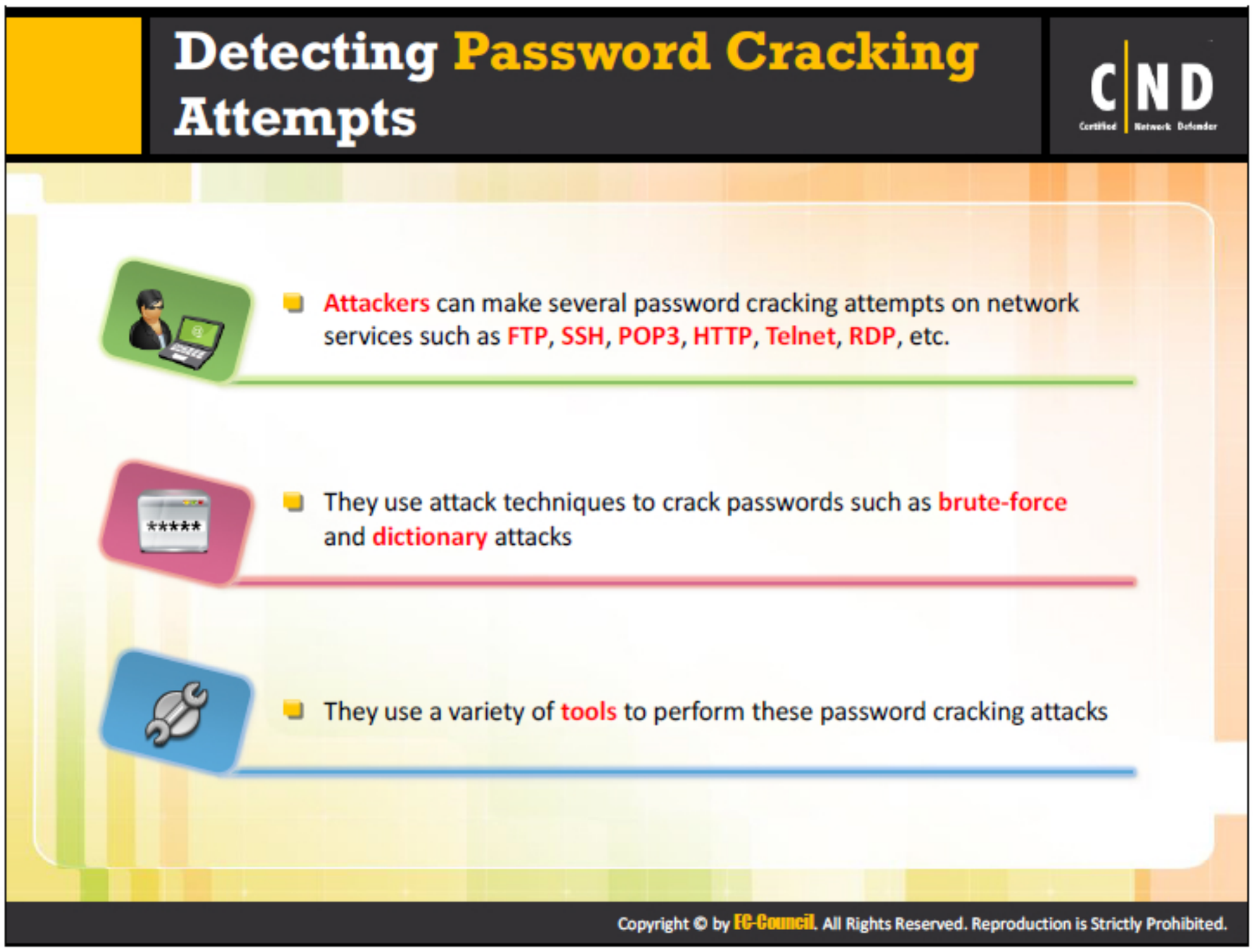


The UDP service can receive packets without establishing a connection. When an attacker sends a UDP packet to the target, either of the following can occur:

- If the UDP port is open, the target accepts the packet and does not send any response.
- If the UDP port is closed, the ICMP packet is sent in response.

UDP scanning is more difficult to probe than TCP as it does not depend on the acknowledgements received. A UDP scan gathers all the ICMP errors received from closed ports. Administrators should take proper measure to handle open UDP ports to avoid any intrusion in the network. While monitoring if any machine is replying with bulk ICMP type 3 responses, it is a sign of a UDP scan attempt on the network. To identify the UDP scan attempt, run the filter **`icmp.type==3`** and **`icmp.code==3`** in Wireshark.

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



Password cracking is a process of gaining or recovering passwords either through trial and error or running a password guessing attempt using an available file. These contain the most commonly used passwords. These techniques are called a brute force attack and a dictionary attack respectively.

Brute-Force Attack

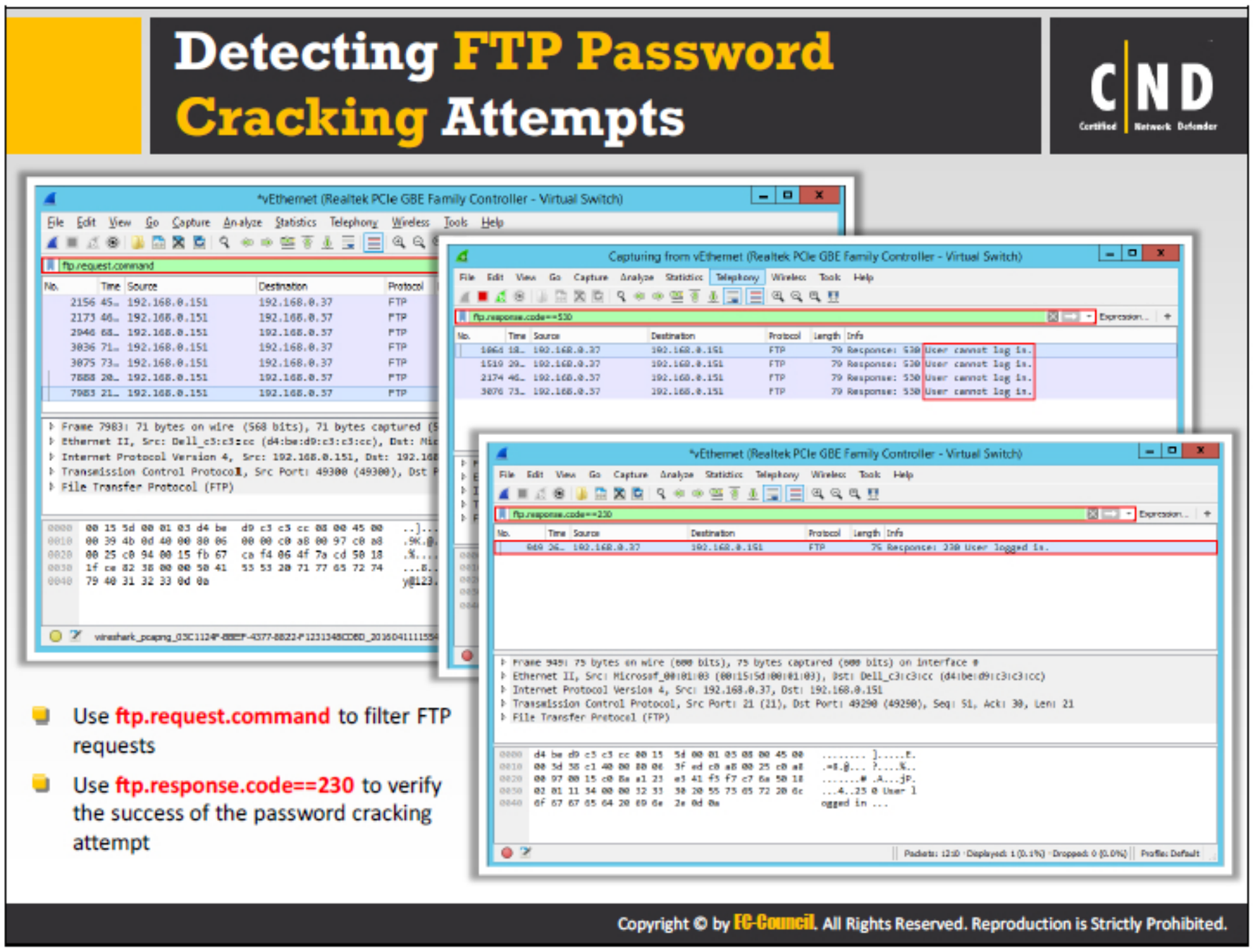
Though brute-force attacks can be a lengthy process, attackers use various tools to implement on the network.

Dictionary Attack

The attacker uses a limited set of words to perform a dictionary attack. With SSH services running in the network, it is easier for attackers to perform a dictionary attack. SSH dictionary attacks rely on the log files or on the network traffic. The dictionary attack can be accomplished easily on an account that has a weak password. This type of attack is performed on a single target machine or on the network.

An administrator can detect this type of attack by monitoring the number of log in attempts made from the same IP address or username.

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



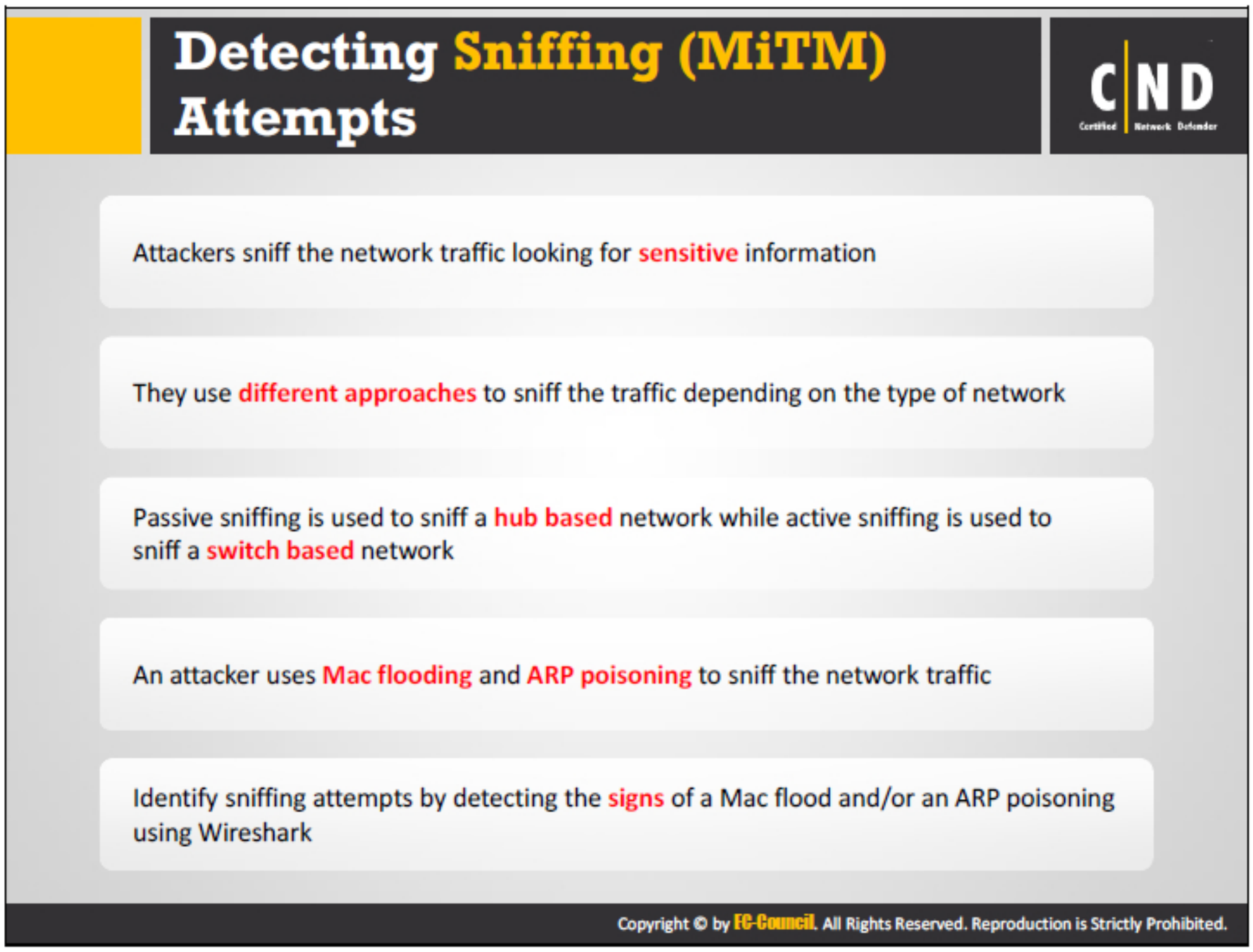
The file transfer protocol (FTP) is a standard protocol to transmit files between systems over the Internet using the TCP/IP suite. FTP is a client server protocol relying on two communication channels between a client and a server. One manages the conversations and the other is responsible for the actual content transmission. A client initiates a session with a download request, which the server responds with the particular file requested.

An FTP session requires the user to login to the FTP server with their username and password. In an FTP password attack, the attacker tries to gain user's password.

Use the filter **`ftp.request.command`** in Wireshark to detect a FTP password cracking attempt in the network. The filter **`ftp.request.command`** provides all the FTP requests made in the network. It also displays the number of attempts made by the attacker to gain access to the FTP server.

- To check the successful attempt of FTP password cracking, apply the filter **`ftp.response.code = = 230`**
- To check the unsuccessful attempt of FTP password cracking, apply the filter **`ftp.response.code = = 530`**

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



Sniffing or Man in The Middle attacks are a form of eavesdropping where an attacker captures packets by placing themselves between a client and a server. Sniffing is attempted using either an active form or a passive form.

Active Sniffing

Sniffing performed over a switched network is called active sniffing. The attacker injects packets into the network traffic to gain information from the switch, which maintains its own ARP cache known as content addressable memory (CAM).

Passive Sniffing

Sniffing performed on the hub is called passive sniffing. Since a hub broadcasts all packets, an attacker only has to initiate the session and wait for someone else to send packets on the same collision domain.

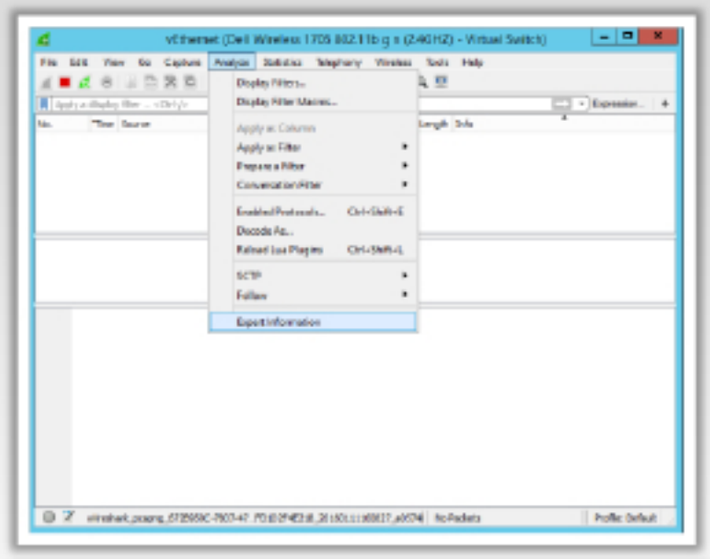
The methods used in sniffing are:

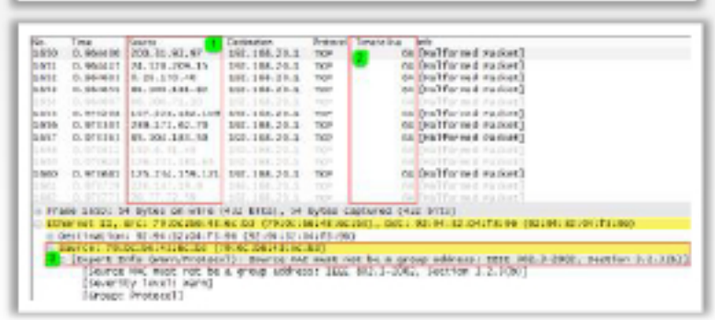
- MAC flooding
- ARP poisoning

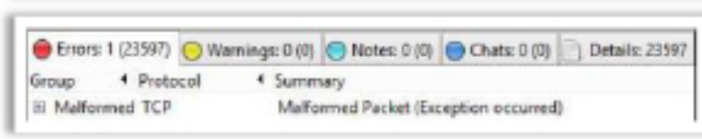
Certified Network Defender Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting a Mac Flooding Attempt

- Wireshark detects MAC Flooded packets using the Expert Information window
- Wireshark considers these as malformed packets
- To view these malformed packets, go to the Analyze menu and select Expert Information
- The signs of a MAC flooding are detected by analyzing the source IP, destination IP and the TTL values
- Check if the traffic is originating from various IP addresses going to the same destination IP addresses with the same TTL values
- This is an indication of a MAC flooding attempt on the network







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

MAC flooding is an active sniffing method in which the attacker connects to a port on the switch. They send a flurry of Ethernet frames with various fake MAC addresses. The switch maintains a CAM (content addressable memory) table, which the attacker is trying to gain access to. This attack is also known as CAM flooding attack.

A MAC flooding attempt is detected in Wireshark by carefully analyzing the packet's source and destination addresses along with its Time to live (TTL).

After capturing the packets go to the 'Analyze' tab and click on 'Expert Information' from the drop down context menu.

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

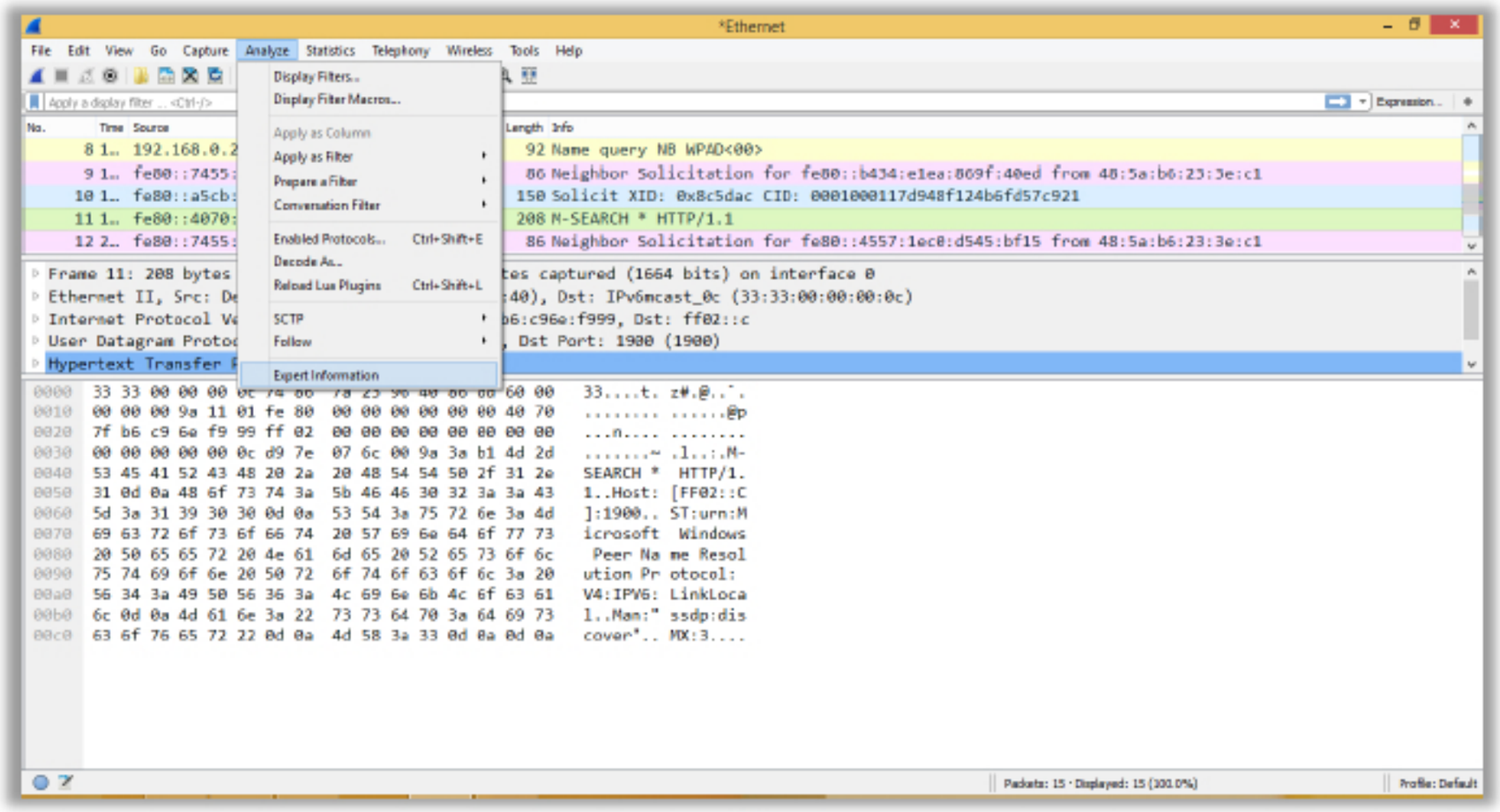


FIGURE 11.4: Selecting Expert Information from Analyze tab in Wireshark

Look for malformed packets in the Expert Information tab.

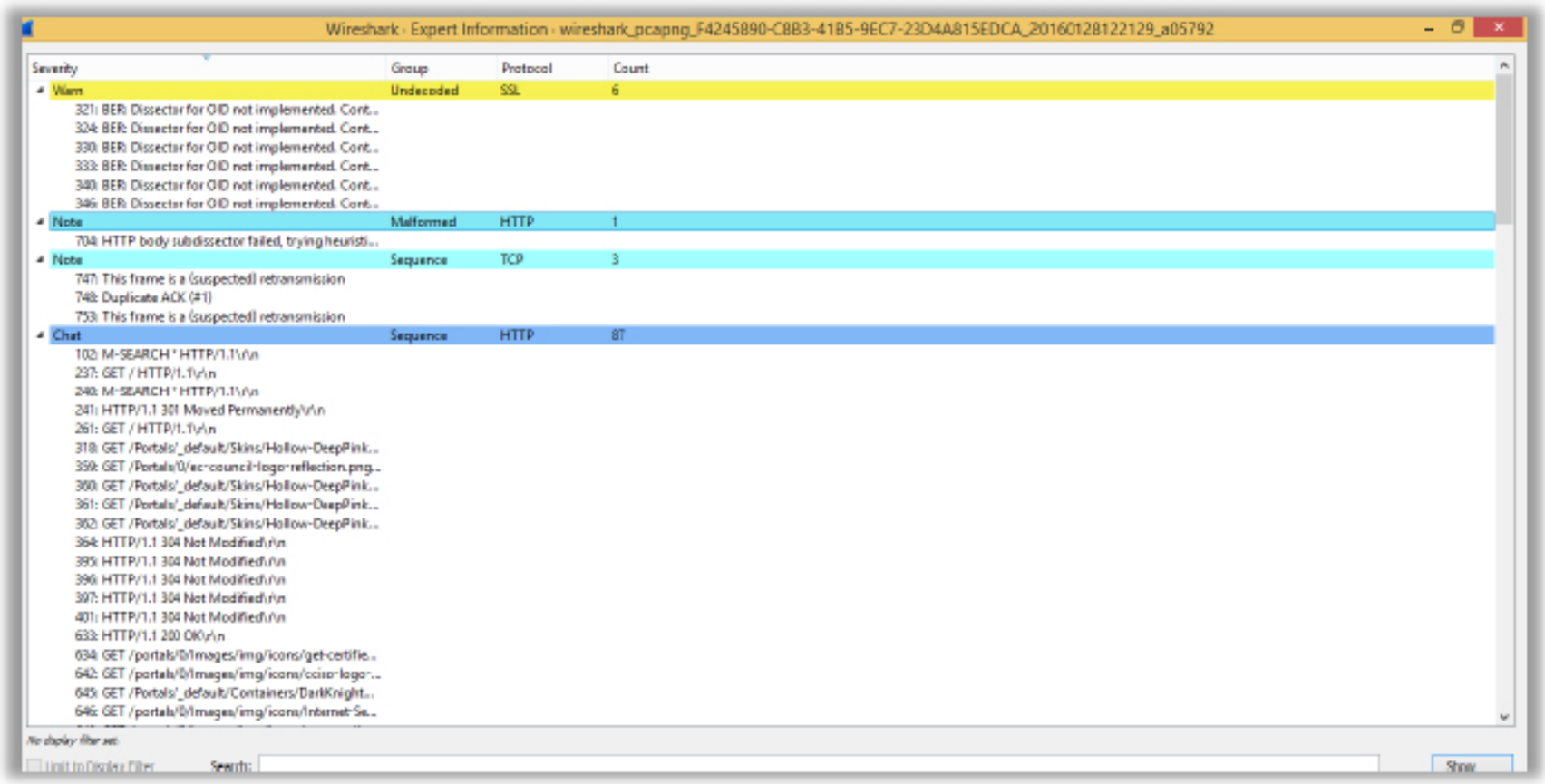


FIGURE 11.5: Malformed packets in Expert Information tab in Wireshark

Malformed packets result for various reasons and they may not be an attempt to MAC flood. To accurately detect a MAC flooding attempt check if several packets are destined towards the same machine but originated from different sources.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

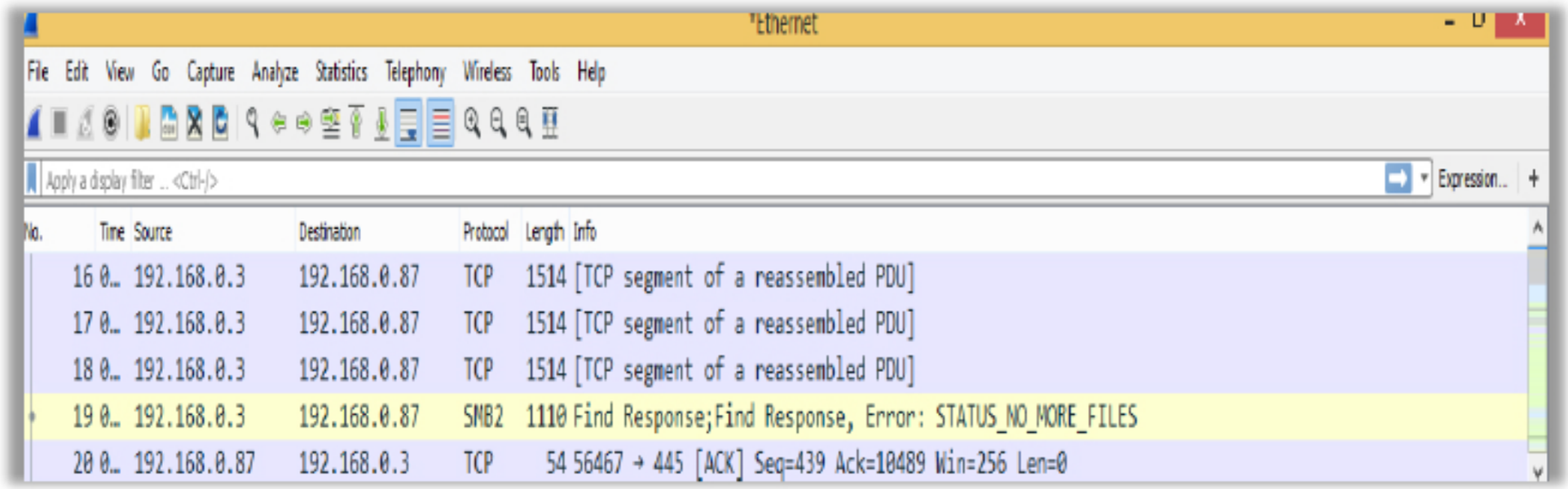


FIGURE 11.6: MAC flood attempt

Although in the above screenshot, the destination address is the same it should be noted the source address is the same, which implies the packets were sent from a legitimate source. Administrators can also verify the TTL values for each packet. If every source has the same TTL values and all the packets are directed towards the same machine, it is an indication of a MAC flood attempt on the network.

Preventing MAC Flooding:

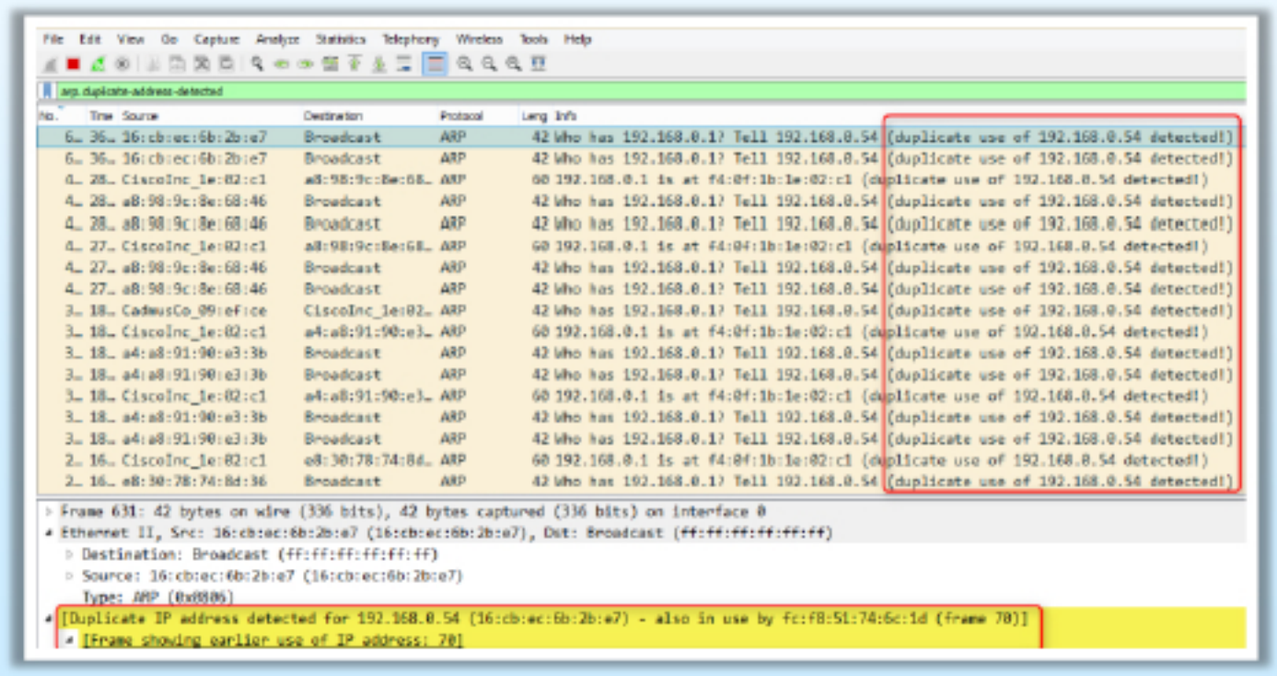
- MAC flooding can be avoided by using Port security that is a built-in feature with Cisco switches. Port security limits the number of MAC addresses. It creates a small MAC address table as compared to the traditional larger ones.
- Implementing authentication, authorization and accounting (AAA) by vendors, minimizes the MAC flooding risk.
- Implementing IEEE suites allows packet filtering rules to be installed by an AAA server.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting an ARP Poisoning Attempt

- In an ARP poisoning attack, the attacker's MAC address is associated with the IP address of the target host or a number of hosts in the target network
- Check for '**duplicate IP address configured**' messages in the Warnings tab in Wireshark
- To locate duplicate IP address traffic use the filter:

  `arp.duplicate-address-detected`



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

The address resolution protocol (ARP) maps the MAC address to an IP address. In an ARP poisoning attack, an attacker changes the MAC address of the target system to his MAC address. All packets destined to the target system are now going to the attacker's machine. An attacker can monitor the data flow in the network, forge more than one device on the network and have all their packets directed towards them instead. An ARP poisoning attack can be detected in Wireshark by looking for a warning message which reads 'duplicate IP address configured'. An administrator can use the filter **arp.duplicate-address-detected,** after capturing the packets. The packets with these messages are shown in figure below. It is an indication of an ARP poisoning attempt on the network.

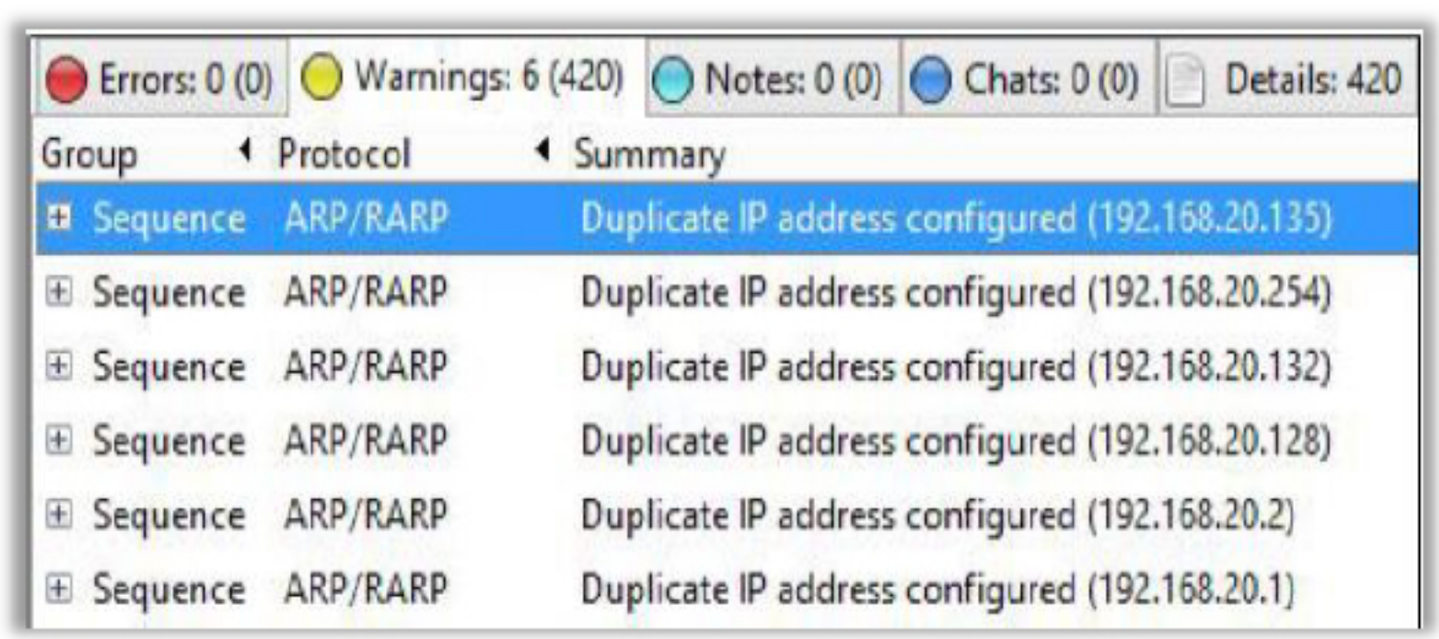


FIGURE 11.7: ARP poisoning attempt

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

Network Sniffer

Source: http://www.colasoft.com

Network Sniffer can help you locate network problems by allowing you to capture and view the packet level data on your network. It consists of a well-integrated set of functions that can resolve network problems. It can list all the network packets in real-time from multi-network cards (Include Modem, ISDN, ADSL) and can also support capturing packets based on applications (SOCKET, TDI etc.).

VisualSniffer

Source: http://www.biovisualtech.com

VisualSniffer is a packet capture tool and protocol analyzer (IP sniffer or packet sniffer) for a Windows system. VisualSniffer can be used by LAN administrators and security professionals for network monitoring, intrusion detection and network traffic logging. It can also be used by network programmers, for checking what the developing program has sent and received or others to get a full picture of the network traffic.

SniffPass Password Sniffer

Source: http://www.nirsoft.net

SniffPass captures the passwords that pass through the network adapter. SniffPass can capture the passwords of the following Protocols: POP3, IMAP4, SMTP, FTP, and HTTP (basic authentication passwords).

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

Capsa Packet Sniffer

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

Capsa Packet Sniffer is a network analyzer for Ethernet monitoring, troubleshooting and analysis. It monitors network activities, pinpoints network problems and enhances network security.

ColaSoft Packet Builder

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

Colasoft Packet Builder creates custom network packets. It helps check the network protection against attacks and intruders. It also supports saving packets to packet files and sending packets to the network.

dsniff

Source: *https://www.monkey.org*

dsniff includes a collection of tools for network auditing and penetration testing. These tools help passively monitor a network for interesting data (passwords, e-mail, files, etc.). Some of the tools in the tool suite facilitate the interception of network traffic normally unavailable to an attacker.

PacketMon

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

PacketMon captures the packets transmitted through the network in order to monitor and administer the network properly.

SmartSniff

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

SmartSniff is a network monitoring utility allowing the capture of TCP/IP packets that pass through the network adapter and view the captured data as a sequence of conversations between clients and servers.

Tcpdump

Source: *http://www.tcpdump.org*

Tcpdump is a command line network analyzer tool or more technically a packet sniffer. Administrators can use this utility for network analysis.

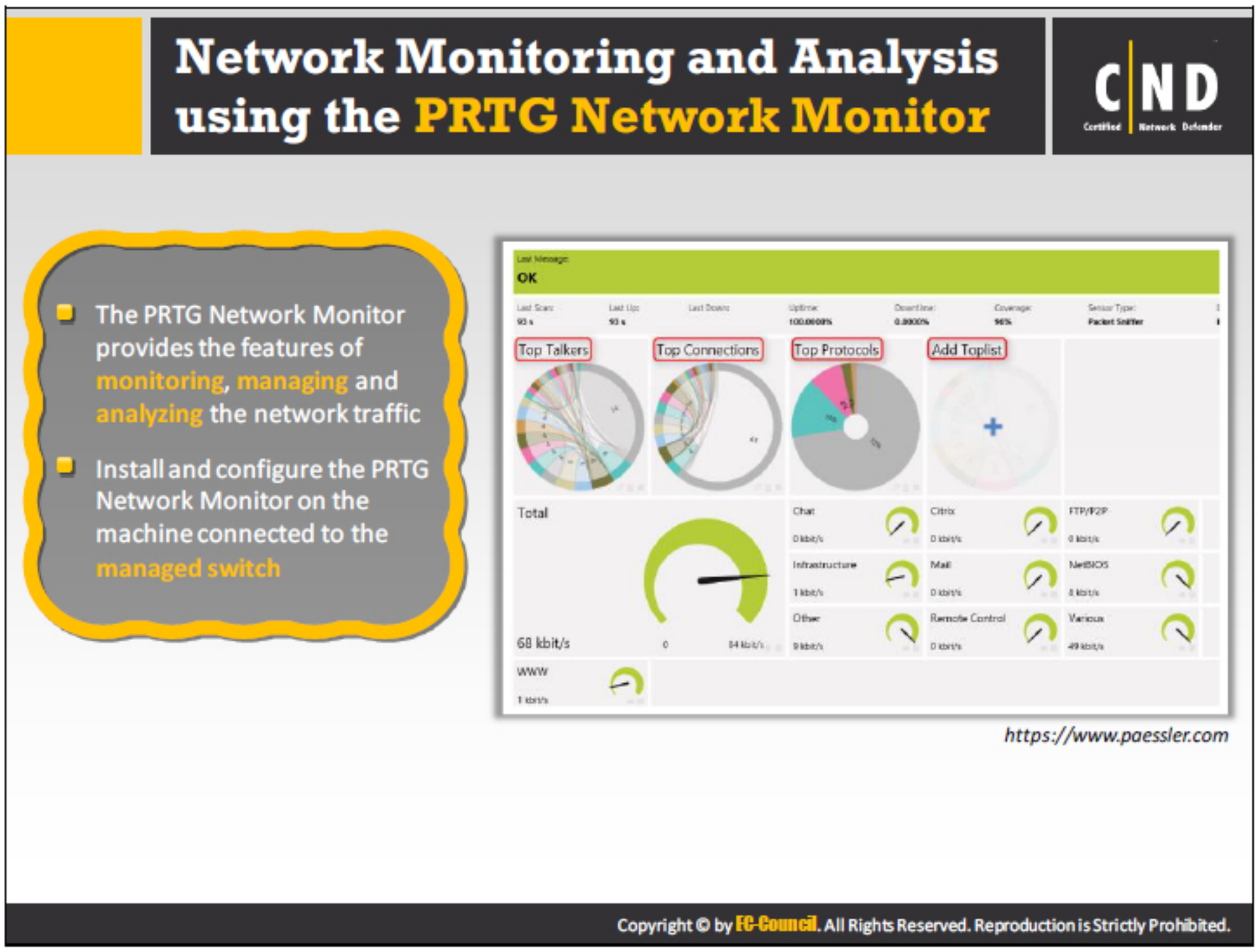
Snort

Source: *https://www.snort.org*

Snort is capable of real-time traffic analysis and packet logging. Snort can be configured to run in three modes:

- Sniffer mode, which simply reads the packets off the network and displays them in a continuous stream on the console (screen).
- Packet Logger mode, which logs the packets to the disk.
- Network Intrusion Detection System (NIDS) mode, which performs detection and analysis on the network traffic. This is the most complex and configurable mode.

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



PRTG Network Monitor is a network monitoring software which supports remote management using any web browser or smart phone, various notification methods and multiple location monitoring. Administrators can use this utility for availability, usage and activity monitoring, covering the entire range from website monitoring to database performance monitoring.

It helps:

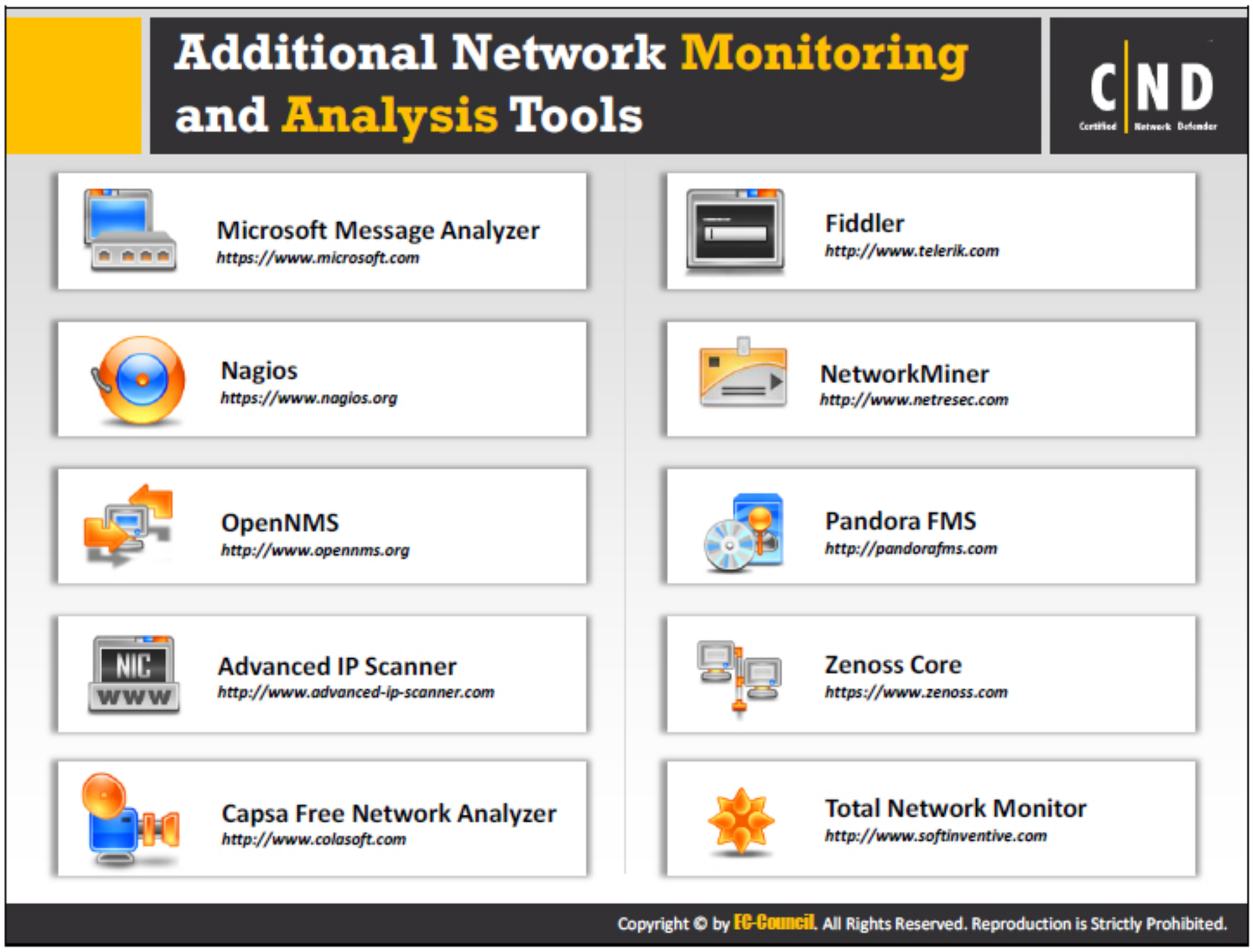
- Avoid bandwidth and performance bottlenecks.
- Identify applications or servers using up the available bandwidth.
- Instantly identify sudden spikes caused by malicious code.
- Reduce the costs of purchasing additional hardware and bandwidth.

PRTG can collect data for almost anything of interest on the network. It supports multiple protocols for collecting this data:

- SNMP and WMI.
- Packet Sniffing.
- NetFlow, IPFIX, jFlow, and sFlow.

Source: https://www.paessler.com

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



Microsoft Message Analyzer

Source: https://www.microsoft.com

Message Analyzer enables an administrator to capture, display and analyze protocol messaging traffic and other system messages. Message Analyzer also can import, aggregate and analyze data from log and trace files.

Nagios

Source: https://www.nagios.org

Nagios monitors the entire IT infrastructure to ensure systems, applications, services, and business processes are functioning properly.

OpenNMS

Source: http://www.opennms.org

The application comes with a large number of service monitors that perform synthetic transactions ranging from a simple ICMP request (ping) or port check, up through complex website monitoring and round trip e-mail testing.

Advanced IP Scanner

Source: http://www.advanced-ip-scanner.com

Advanced IP Scanner analyzes the traffic in the LAN. The program shows all network devices, provides access to shared folders and FTP servers. It provides remote control of computers and can even switch computers off remotely.

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

Capsa Free Network Analyzer

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

Capsa Free Network Analyzer is a network analyzer that allows monitoring network traffic, troubleshooting network issues and analyzing packets. It allows an administrator to monitor network activities, pinpoint network problems and enhance network security and so on. It automatically diagnoses network problems and suggests solutions. It lists all hosts in the network with details (traffic, IP, MAC, etc.)

Fiddler

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

Fiddler enables an administrator to inspect incoming and outgoing data to monitor, modify requests and responses before the browser receives them.

NetworkMiner

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

NetworkMiner can be used as a passive network sniffer/packet capturing tool in order to detect operating systems, sessions, hostnames, open ports etc. without putting any traffic on the network. NetworkMiner can extract files and certificates transferred over the network by parsing a PCAP file or by sniffing traffic directly from the network.

Pandora FMS

Source: *http://pandorafms.com*

Pandora FMS monitors a client's network, with no external access. It uses industry standard SNMP v1, v2c and v3 processing alongside powerful SNMP trap management for network monitoring. It uses a native IPAM integration to manage IP addresses (IPv4/IPv6 compatible).

Zenoss Core

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

Zenoss automatically builds and maintains a topology model of the entire network, including devices, routers, interfaces and routes. It keeps up with rapidly changing network usage patterns.

Total Network Monitor

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

Total Network Monitor is a network monitoring software program that is designed to continuously monitor the local network, individual computers and services that require careful attention and thorough control. It monitors and keeps track of a particular aspect of service operation, server health or a file system. The monitor log shows the full history of the executed actions and readings from all the monitors.

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

Bandwidth Monitoring

- Bandwidth is the amount of information that can be transmitted over a network in a given amount of time
- Network bandwidth selection plays a vital role in the design, maintenance and performance of an organization's network
- Poor bandwidth management leads to network congestion and poor performance of the network

- Bandwidth monitoring involves measuring and controlling the traffic on a network link to avoid overfilling of link
- Factors for measuring bandwidth are:
  - Determine the amount of available network bandwidth
  - Determine the average utilization required by a specific application

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

Bandwidth Monitoring (Cont'd)

- Understand the bandwidth and resource consumption for better network management
- Use bandwidth monitoring tools to measure the bandwidth of the network link

- Focus on the following considerations to lower down the bandwidth requirements:
  - Server-side computing
  - Data caching
  - Data compression
  - Latency mitigation
  - Loss mitigation

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

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

Bandwidth is the amount data that can be transferred from one point to another. Bandwidth is one of the criteria defining network performance. An effective bandwidth is the one that provides the highest transmission rate. The bandwidth monitoring test will identify the maximum throughput of a system. Bandwidth monitoring tools provide output of the real-time network traffic for any device. The tools provide bandwidth information at the interface level and the device level. If the bandwidth detected is low, it degrades the functioning of the network.

An organization works on two types of bandwidth speed: upload and download. The speed at which the data is sent to the destination is called the upload speed. The speed at which the destination receives the data is called the download speed. With growing networks and huge volumes of data, organizations have started to maximize their upload and download speeds.

It is also important to consider the bandwidth capacity in the network. Bandwidth capacity involves the maximum data rate a link can transfer. With hundreds of users in the network, it is important to know the bandwidth usage required per day. Although it can be a tedious job for administrators to determine the usage per day capacity of the bandwidth, a blue print of the usage can help draft a proper bandwidth monitoring plan.

Bandwidth monitoring includes monitoring various bandwidth utilizations that are implemented in the organization. Many software tools allow you to monitor bandwidth in real time. Bandwidth monitoring benefits are:

- Bandwidth monitoring helps determine the network utilization for the system. Systems using high bandwidth amounts should be monitored closely as they can be suspicious activities or have become a victim of suspicious activity.
- High amounts of network traffic lead to network congestion and affect the function of the organization. Deploying a network limit, will provide an alarm when the network is about to reach the maximum bandwidth.
- If the network congestion is high depending on the size of the organization, additional links can be added to the network. An additional link in the network will boost the network performance resulting in reduced network congestion.

Improve Bandwidth Usage

Organizations should follow certain rules to increase bandwidth usage in their environment. The rules below differ per the size and requirement of the organization:

- **Limited Use of Media Sites:** Organizations can limit their employees using media access, like online gaming, movies, music, etc. This will enhance the upload as well as the download speed of the overall network.
- **Proxy Cache:** When a user visits a website for the first time, the content of the site is saved (cached) on the proxy server. If the user visits the same website again the content does not have to be downloaded again.
- **QoS:** Quality of Service (QoS) is a bandwidth reservation mechanism. Certain applications require additional bandwidth, administrators can configure the QoS for these

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

applications. In the future if a user accesses these applications, the QoS bandwidth will be utilized. Utilizing QoS bandwidth will not affect the bandwidth usage for other users in the network.

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

Bandwidth Monitoring - Best Practices

Best practices for administrators considering current and future bandwidth needs:

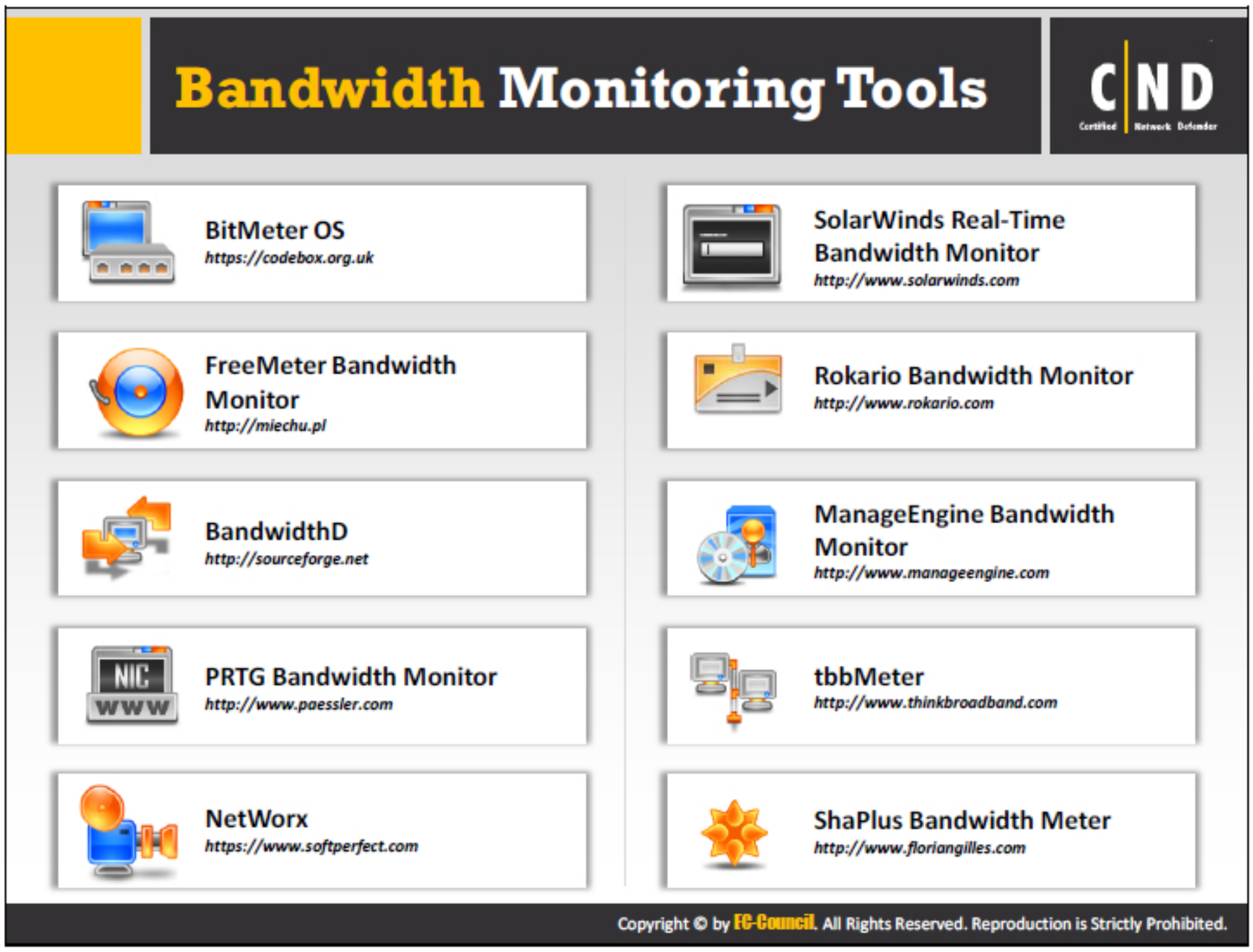
- It is recommended to use only a **single bandwidth monitoring tool** to assess the current utilization of bandwidth for the organization
- Define and categorize the **bandwidth need** based on the application, user, user groups, time period, etc.
- Calculate the **total number of nodes** that contribute to the overall bandwidth requirement including workstations, shared printers, and servers
- Calculate the **average** bandwidth required per node
- Always consider **peak bandwidth requirements** for the organization
- Determine, assess and list the **type of application** that should be used within a specific time period and how much bandwidth it will consume
- Check with the **Internet service provider (ISP)** as to whether they allow provisions for growth in the bandwidth requirements

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

The following best practices can also be helpful in effective bandwidth monitoring:

- Timely educating or training the employees about excessive bandwidth consumption can create awareness among them concerning bandwidth usage.
- Monitor the traffic consumed by the network components in the organization.
- Implement of QoS policy to prioritize bandwidth usage as per the application requirement.
- Optimize the WAN capacity to increase the bandwidth of the network.
- Backup the devices that are configured on the network. During a power failure or network failure, these backups act as a good configuration and keep the bandwidth stable.

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



BitMeter OS

Source: *https://codebox.org.uk*

BitMeter OS keeps track of how much of the internet/network connection is used and allows an administrator to view this information either via a web browser or by using the command line tools.

FreeMeter Bandwidth Monitor

Source: *http://miechu.pl*

FreeMeter Bandwidth Monitor is used to monitor the network bandwidth and any or all network interfaces. It also provides supporting utilities, including Ping, Trace, UPnP utilities, etc.

BandwidthD

Source: *https://sourceforge.net*

BandwidthD monitors the amount of traffic being received/transmitted by specific machines and or subnets. It tracks the usage of TCP/IP network subnets and builds HTML files with graphs to display utilization.

PRTG Bandwidth Monitor

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

PRTG Bandwidth Monitor analyzes the traffic in the network and provides detailed results - tables and graphs. It monitors network devices, bandwidth, servers, applications, virtual environments, remote systems, IoT and many more.

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

NetWorx

Source: https://www.softperfect.com

NetWorx monitors all the network connections or just a specific network connection, such as Wireless or Mobile Broadband. The incoming and outgoing traffic is represented on a line chart and logged into a file, so the statistics can always be viewed about the daily, weekly and monthly bandwidth usage and dial-up duration. The reports can be exported to a variety of formats, such as HTML, MS Word and Excel for further analysis.

SolarWinds Real-Time Bandwidth Monitor

Source: http://www.solarwinds.com

With the Real-Time Bandwidth Monitor, critical and warning thresholds can be set to instantly see when usage is out of bounds.

Rokario Bandwidth Monitor

Source: http://www.rokario.com

Rokario Bandwidth Monitor enables an administrator to keep a close eye on the amount of bandwidth accumulated over the current hour, day, week, month or even year. Advanced logging tools make it easy to view the bandwidth usage and make alterations to bandwidth logs.

ManageEngine Bandwidth Monitor

Source: https://www.manageengine.com

The Bandwidth Monitor tool provides real-time network traffic of any SNMP device. It provides the bandwidth usage details both on an interface - level and at the device-level. It uses SNMP to fetch the bandwidth utilization details of a network interface. The bandwidth utilization of the device displays a comparison of the individual traffic and its interfaces.

tbbMeter

Source: http://www.thinkbroadband.com

tbbMeter is a bandwidth meter that monitors Internet usage. It shows how much the computer is sending to and receiving from the Internet in real time. It also shows how the Internet usage varies at different times of the day.

ShaPlus Bandwidth Meter

Source: http://www.shaplus.com

ShaPlus Bandwidth Meter is a bandwidth monitoring software used to track Internet bandwidth usage. It displays the bandwidth usage in the current session, day and month.

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

Module Summary

- Network traffic monitoring and signature analysis involves capturing network packets and analyzing them to identify any signs of malicious activity
- Signatures are patterns created using a set of rules which identify typical intrusive activity on the network
- Signature analysis helps differentiate legitimate traffic from suspicious traffic
- Wireshark is a widely used network packet analyzer for network analysis
- A network baseline is a description of the accepted behavior for the network traffic
- Administrators should monitor the network traffic for different types of attack attempts

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

This module covered the importance of manual network traffic monitoring, types of network signatures, network traffic baselining, network monitoring tools and detection techniques for various types of attacks. The skills acquired include the ability to monitor and detect various types of network traffic abnormalities in the network. The information learned in this module provided the skills to manage and monitor the network devices in the infrastructure. Then also the skills to monitor the network bandwidth.

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