# Host Security

## Module 06

Lab

1

# Disabling Unnecessary Services Running on User Systems

*Unnecessary services can open doors for attackers.*

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

## Lab Scenario

Unnecessary services running on the system can allow attackers to exploit vulnerabilities on and gain access to the system or network. As a network administrator, you should be aware of which services are unnecessary based on the organizational policy. Disabling these unnecessary/unused services on a system is one of the important activities that should be performed for security reasons.

## Lab Objectives

The objective of this lab is to identify the unnecessary/unused services on a particular system and disable them.

## Lab Environment

To perform the lab, you need:

- A virtual machine running **Windows 10**
- A virtual machine running **Ubuntu**
- A web browser with an **Internet** connection

## Lab Duration

Time: 10 Minutes

## Overview for Disabling Unnecessary Services

Operating systems enable a set of services to function properly. Apart from the default services launched by an OS, users may enable certain services or install applications that enable other dependent services. After the desired task is complete these services may still be left enabled. Attackers can exploit these services to launch various attacks on the system.

# Lab Tasks

TASK 1

**Disabling unnecessary services on Windows computer**

1. The required services that should be running on a computer is stated in the organization's security policy. This set of required services is generally known as a baseline. Based on this, you can identify the unnecessary services running on a specific computer.

2. Launch the **Windows 10** virtual machine and login as the Administrator.

3. Type **services.msc** in the **Search the web and Windows** and press **Enter**.

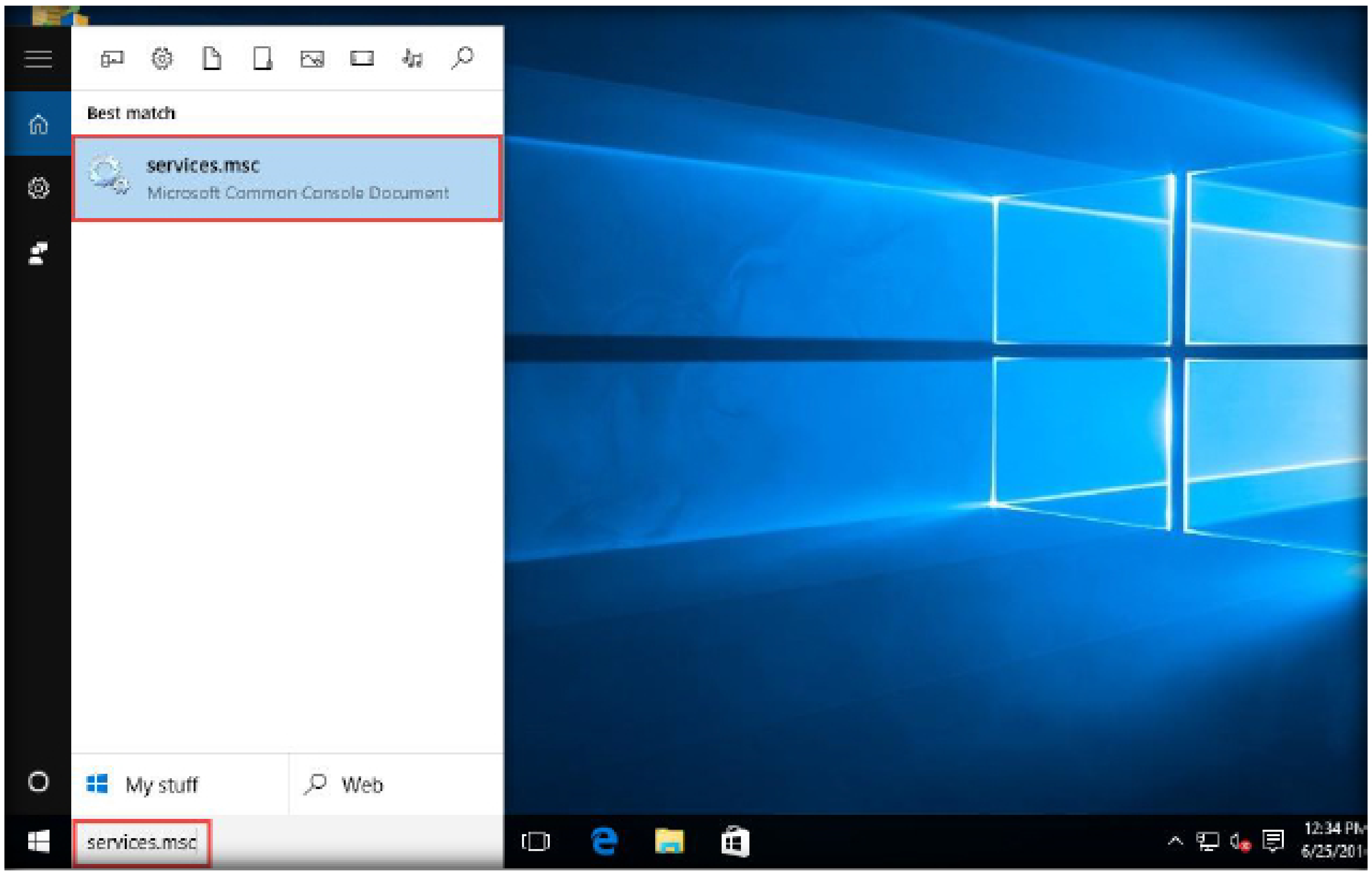
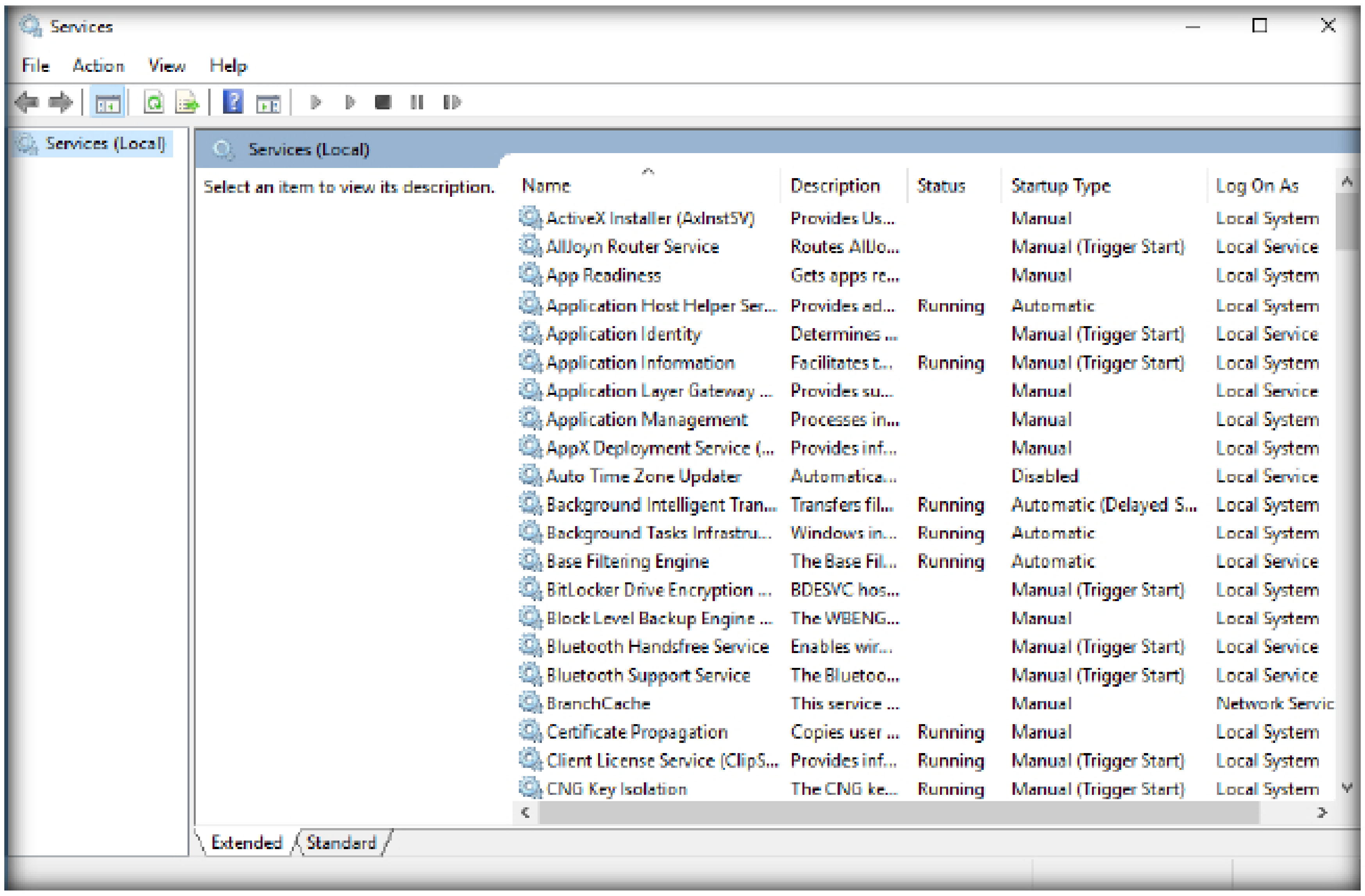


FIGURE 1.1: Windows 10 Machine Launching Services

Microsoft Windows services, formerly known as NT services, enable you to create long-running executable applications that run in their own Windows sessions.

4. The **Services** window will open as shown in following screenshot. This window will show all the services running on the system with a **Running** status.



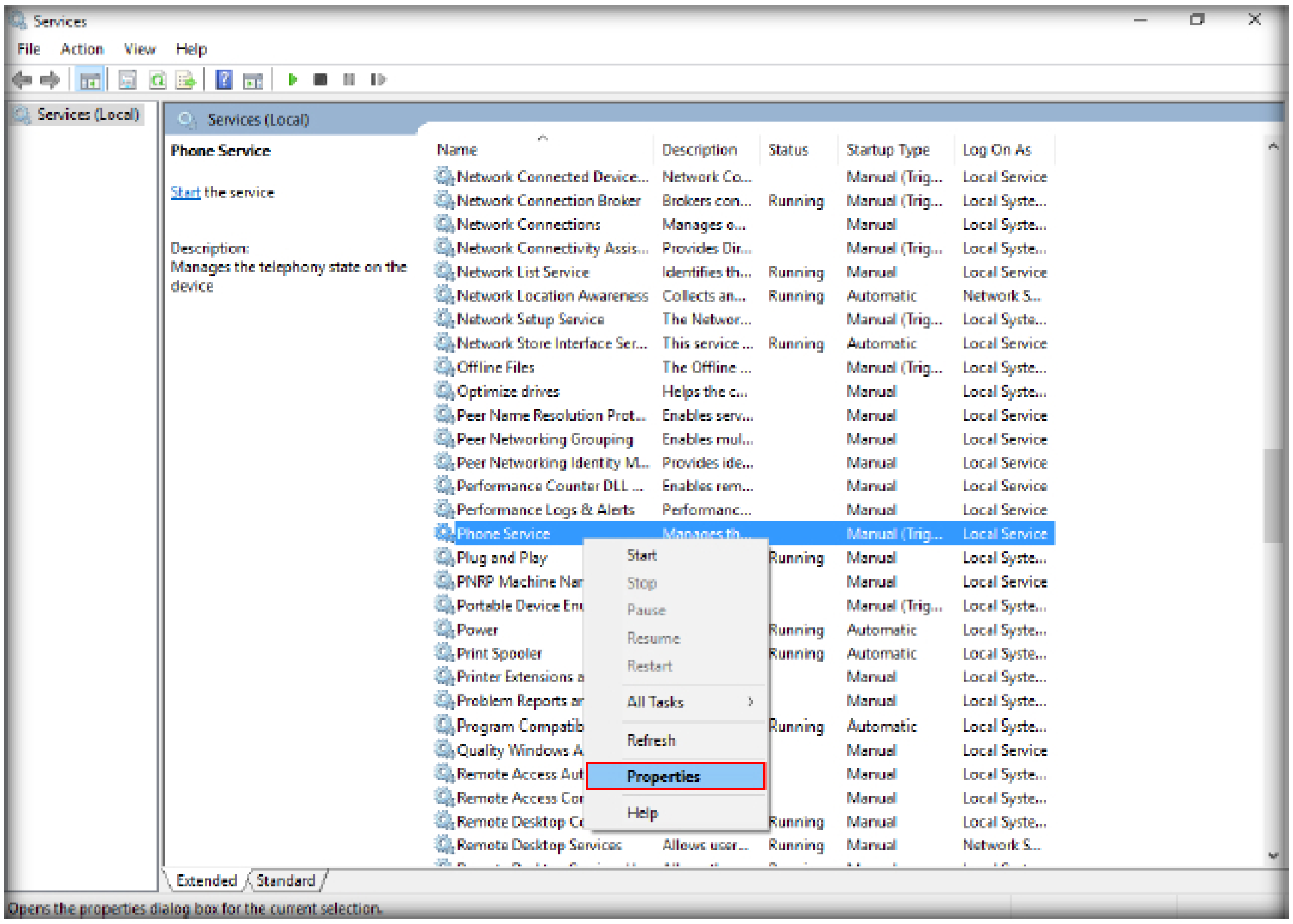
Select an item to view its description.

| Name | Description | Status | Startup Type | Log On As |
|---|---|---|---|---|
| ActiveX Installer (AxInstSV) | Provides Us... | | Manual | Local System |
| AllJoyn Router Service | Routes AllJo... | | Manual (Trigger Start) | Local Service |
| App Readiness | Gets apps re... | | Manual | Local System |
| Application Host Helper Ser... | Provides ad... | Running | Automatic | Local System |
| Application Identity | Determines ... | | Manual (Trigger Start) | Local Service |
| Application Information | Facilitates t... | Running | Manual (Trigger Start) | Local System |
| Application Layer Gateway ... | Provides su... | | Manual | Local Service |
| Application Management | Processes in... | | Manual | Local System |
| AppX Deployment Service (... | Provides inf... | | Manual | Local System |
| Auto Time Zone Updater | Automatica... | | Disabled | Local Service |
| Background Intelligent Tran... | Transfers fil... | Running | Automatic (Delayed S... | Local System |
| Background Tasks Infrastru... | Windows in... | Running | Automatic | Local System |
| Base Filtering Engine | The Base Fil... | Running | Automatic | Local Service |
| BitLocker Drive Encryption ... | BDESVC hos... | | Manual (Trigger Start) | Local System |
| Block Level Backup Engine ... | The WBENG... | | Manual | Local System |
| Bluetooth Handsfree Service | Enables wir... | | Manual (Trigger Start) | Local Service |
| Bluetooth Support Service | The Bluetoo... | | Manual (Trigger Start) | Local Service |
| BranchCache | This service ... | | Manual | Network Servic |
| Certificate Propagation | Copies user ... | Running | Manual | Local System |
| Client License Service (ClipS... | Provides inf... | Running | Manual (Trigger Start) | Local System |
| CNG Key Isolation | The CNG ke... | Running | Manual (Trigger Start) | Local System |

FIGURE 1.2: Services Window

These services can be automatically started when the computer boots, can be paused and restarted, and do not show any user interface. These features make services ideal for use on a server or whenever you need long-running functionality that does not interfere with other users who are working on the same computer.

5. Now find out the unnecessary services running on the system and disable them. To disable a service, right-click on the service and click **Properties** from the context menu.



Phone Service

Start the service

Description:
Manages the telephony state on the device

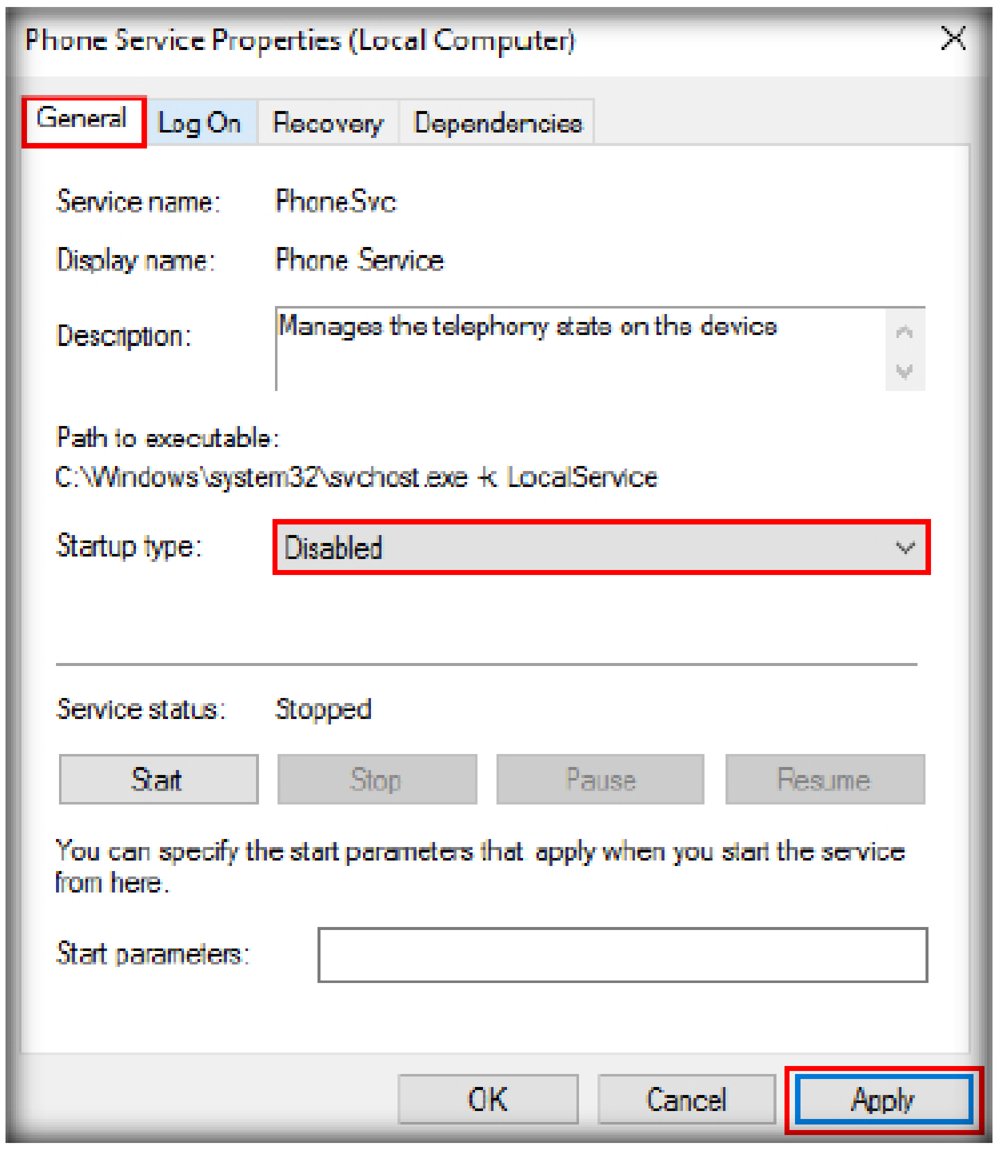
| Name | Description | Status | Startup Type | Log On As |
|---|---|---|---|---|
| Network Connected Device... | Network Co... | | Manual (Trig... | Local Service |
| Network Connection Broker | Brokers con... | Running | Manual (Trig... | Local Syste... |
| Network Connections | Manages o... | | Manual | Local Syste... |
| Network Connectivity Assis... | Provides Dir... | | Manual (Trig... | Local Syste... |
| Network List Service | Identifies th... | Running | Manual | Local Service |
| Network Location Awareness | Collects an... | Running | Automatic | Network S... |
| Network Setup Service | The Networ... | | Manual (Trig... | Local Syste... |
| Network Store Interface Ser... | This service ... | Running | Automatic | Local Service |
| Offline Files | The Offline ... | | Manual (Trig... | Local Syste... |
| Optimize drives | Helps the c... | | Manual | Local Syste... |
| Peer Name Resolution Prot... | Enables serv... | | Manual | Local Service |
| Peer Networking Grouping | Enables mul... | | Manual | Local Service |
| Peer Networking Identity M... | Provides ide... | | Manual | Local Service |
| Performance Counter DLL ... | Enables rem... | | Manual | Local Service |
| Performance Logs & Alerts | Performanc... | | Manual | Local Service |
| Phone Service | Manages th... | | Manual (Trig... | Local Service |
| Plug and Play | | Running | Manual | Local Syste... |
| PNRP Machine Nar | | | Manual | Local Service |
| Portable Device Enu | | | Manual (Trig... | Local Syste... |
| Power | | Running | Automatic | Local Syste... |
| Print Spooler | | Running | Automatic | Local Syste... |
| Printer Extensions a | | | Manual | Local Syste... |
| Problem Reports ar | | | Manual | Local Syste... |
| Program Compatib | | Running | Automatic | Local Syste... |
| Quality Windows A | | | Manual | Local Service |
| Remote Access Aut | | | Manual | Local Syste... |
| Remote Access Cor | | | Manual | Local Syste... |
| Remote Desktop Co | | Running | Manual | Local Syste... |
| Remote Desktop Services | Allows user... | Running | Manual | Network S... |

Opens the properties dialog box for the current selection.

FIGURE 1.3: Stopping Unnecessary Service

You can also run services in the security context of a specific user account that is different from the logged-on user or the default computer account. For more information about services and Windows sessions, see the Windows SDK documentation in the MSDN Library.

6. The selected service **Properties** window appears, choose **Disabled** in the Startup type section and click **Apply** to disable the service.



Service name: PhoneSvc

Display name: Phone Service

Description: Manages the telephony state on the device

Path to executable:
C:\Windows\system32\svchost.exe -k LocalService

Startup type: Disabled

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

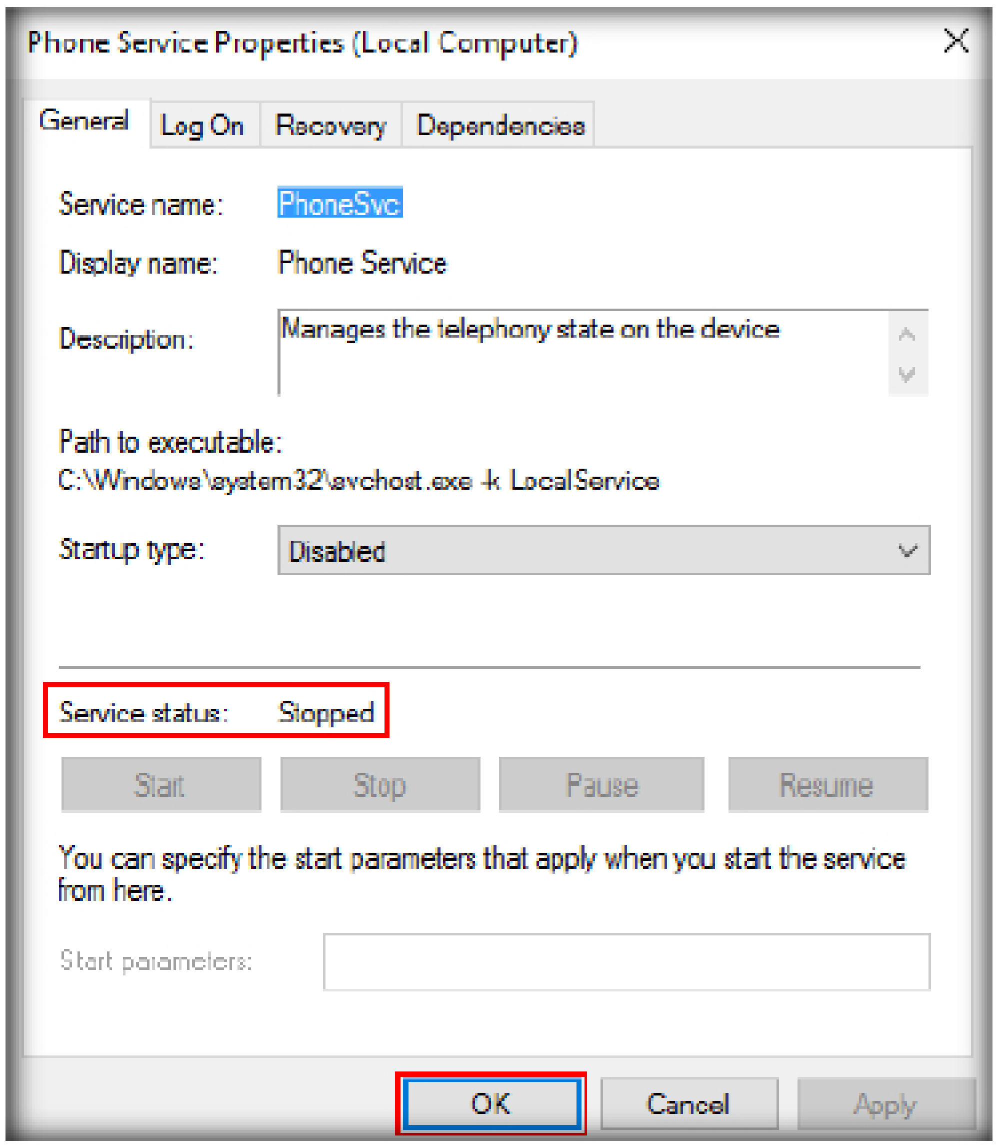
Start parameters:

FIGURE 1.4: Disabling Service

7. Once the service is **Stopped** click **OK** as shown in the screenshot. You can check the service status in the properties window.

8. The service has been disabled permanently in the Windows machine, unless the network administrator enables it again when required.

You can easily create services by creating an application that is installed as a service. For example, suppose you want to monitor performance counter data and react to threshold values. You could write a Windows Service application that listens to the performance counter data, deploy the application, and begin collecting and analyzing data.



Service name: PhoneSvc

Display name: Phone Service

Description: Manages the telephony state on the device

Path to executable:
C:\Windows\system32\svchost.exe -k LocalService

Startup type: Disabled

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

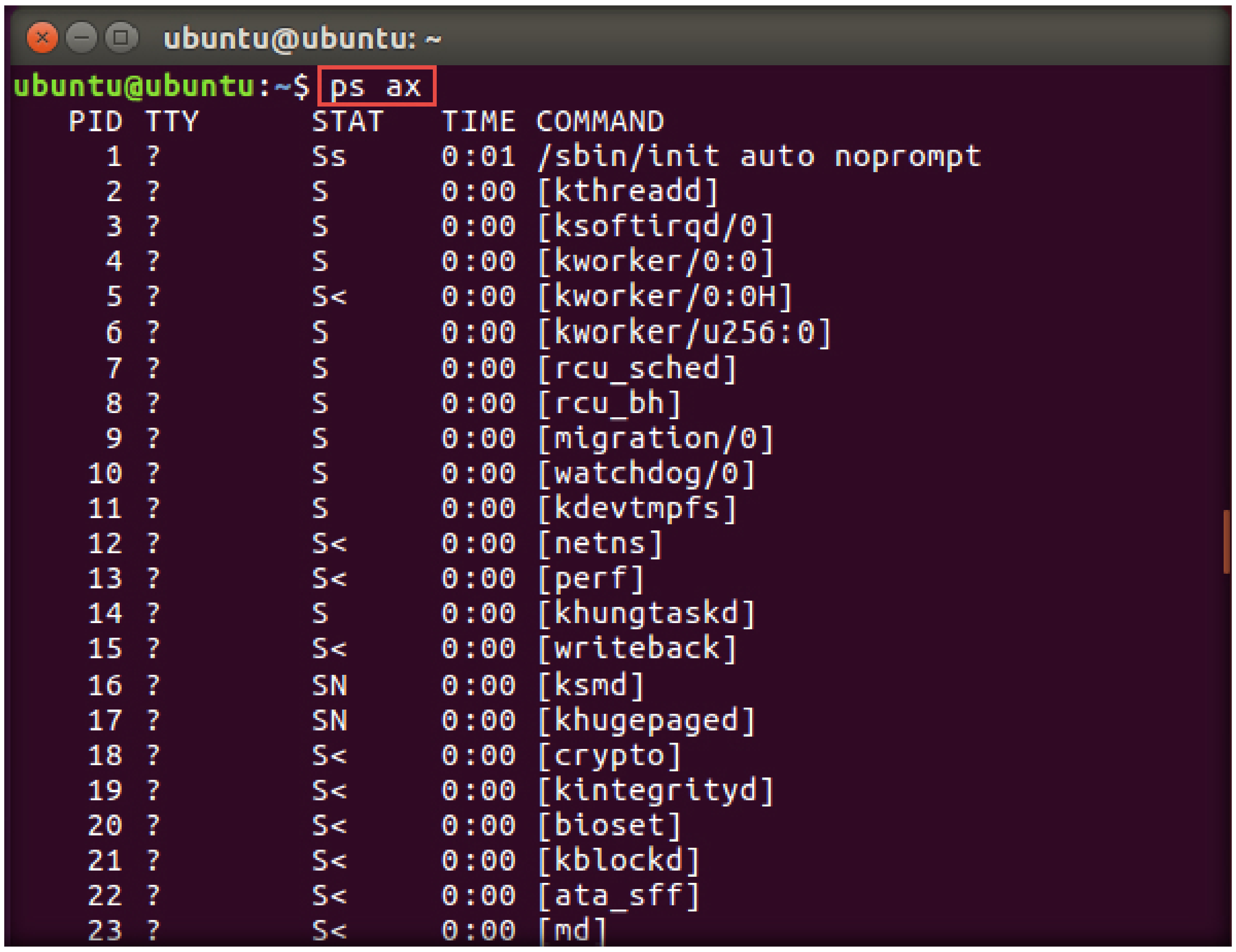
FIGURE 1.5: Service is Stopped

**TASK 2**

**Disabling unnecessary services on Linux computer**

9. Launch the Ubuntu virtual machine and open a command line terminal.

10. Type the **ps ax** command and press **Enter** to know the kind of services running on the system.



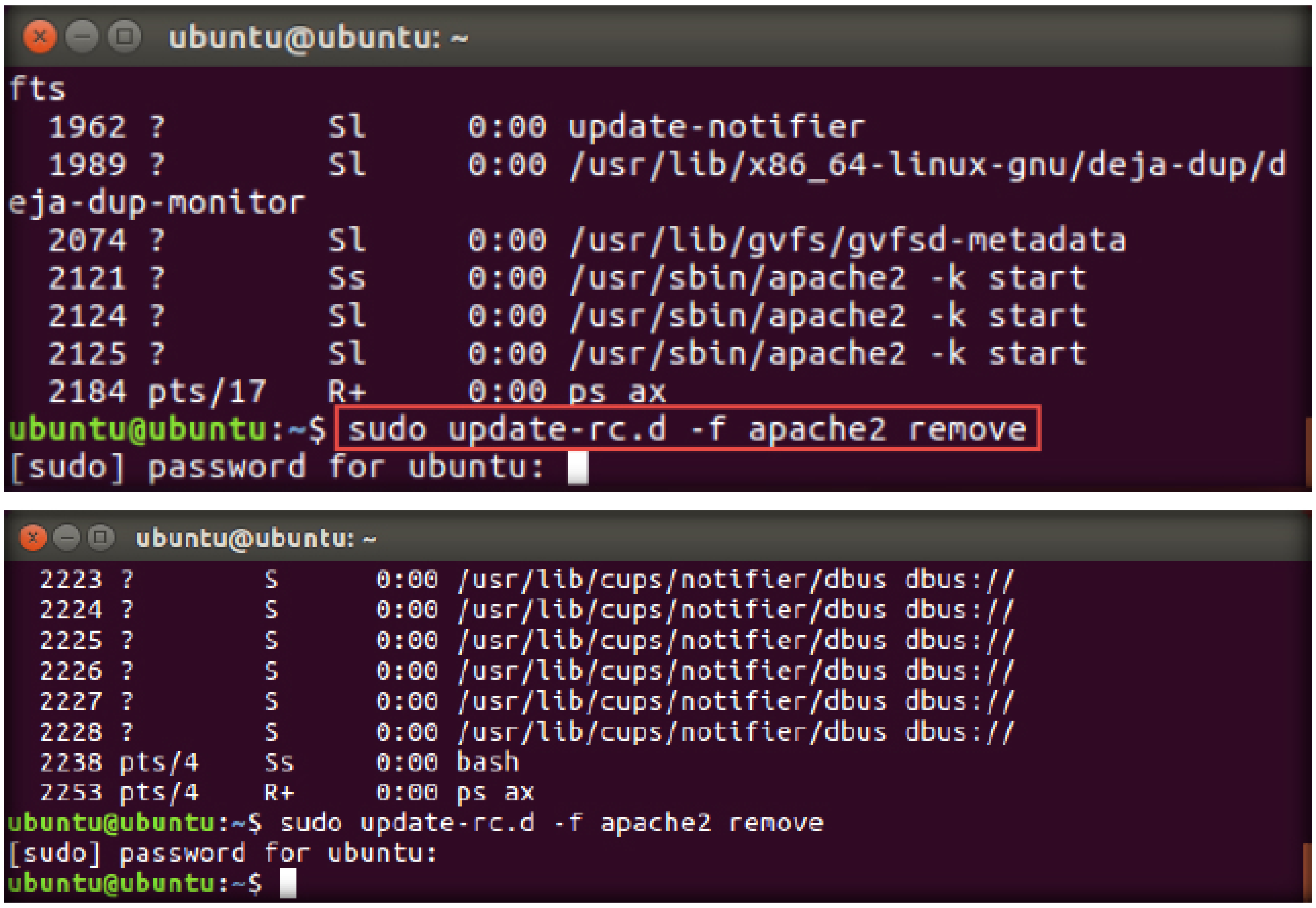
```
ubuntu@ubuntu: ~
ubuntu@ubuntu:~$ ps ax
  PID TTY      STAT   TIME COMMAND
    1 ?        Ss     0:01 /sbin/init auto noprompt
    2 ?        S      0:00 [kthreadd]
    3 ?        S      0:00 [ksoftirqd/0]
    4 ?        S      0:00 [kworker/0:0]
    5 ?        S<     0:00 [kworker/0:0H]
    6 ?        S      0:00 [kworker/u256:0]
    7 ?        S      0:00 [rcu_sched]
    8 ?        S      0:00 [rcu_bh]
    9 ?        S      0:00 [migration/0]
   10 ?        S      0:00 [watchdog/0]
   11 ?        S      0:00 [kdevtmpfs]
   12 ?        S<     0:00 [netns]
   13 ?        S<     0:00 [perf]
   14 ?        S      0:00 [khungtaskd]
   15 ?        S<     0:00 [writeback]
   16 ?        SN     0:00 [ksmd]
   17 ?        SN     0:00 [khugepaged]
   18 ?        S<     0:00 [crypto]
   19 ?        S<     0:00 [kintegrityd]
   20 ?        S<     0:00 [bioset]
   21 ?        S<     0:00 [kblockd]
   22 ?        S<     0:00 [ata_sff]
   23 ?        S<     0:00 [md]
```

FIGURE 1.6: Checking Running process in Ubuntu

11. You require the Root (Administrator) privilege to disable unnecessary services in the computer.

12. To disable a specific service, type the command **sudo update-rc.d –f [service name] remove** and press **Enter**. It will ask for the root password, enter **toor** as the password and press **Enter**. (Here in this lab, we are disabling the **apache2** service)

The service command references a service using its init script, stored in the /etc/init.d directory. Check that directory if you aren't sure what name the system uses for a service.



```
ubuntu@ubuntu: ~
fts
  1962 ?        Sl     0:00 update-notifier
  1989 ?        Sl     0:00 /usr/lib/x86_64-linux-gnu/deja-dup/d
eja-dup-monitor
  2074 ?        Sl     0:00 /usr/lib/gvfs/gvfsd-metadata
  2121 ?        Ss     0:00 /usr/sbin/apache2 -k start
  2124 ?        Sl     0:00 /usr/sbin/apache2 -k start
  2125 ?        Sl     0:00 /usr/sbin/apache2 -k start
  2184 pts/17   R+     0:00 ps ax
ubuntu@ubuntu:~$ sudo update-rc.d -f apache2 remove
[sudo] password for ubuntu: 
```

```
ubuntu@ubuntu: ~
  2223 ?        S      0:00 /usr/lib/cups/notifier/dbus dbus://
  2224 ?        S      0:00 /usr/lib/cups/notifier/dbus dbus://
  2225 ?        S      0:00 /usr/lib/cups/notifier/dbus dbus://
  2226 ?        S      0:00 /usr/lib/cups/notifier/dbus dbus://
  2227 ?        S      0:00 /usr/lib/cups/notifier/dbus dbus://
  2228 ?        S      0:00 /usr/lib/cups/notifier/dbus dbus://
  2238 pts/4    Ss     0:00 bash
  2253 pts/4    R+     0:00 ps ax
ubuntu@ubuntu:~$ sudo update-rc.d -f apache2 remove
[sudo] password for ubuntu:
ubuntu@ubuntu:~$ 
```

FIGURE 1.7: Stopping Unnecessary Services in Ubuntu

13. Type **reboot** and press **Enter** to restart the machine.

## Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

| Internet Connection Required | |
|---|---|
| ☐ Yes | ☑ No |
| Platform Supported | |
| ☑ Classroom | ☑ iLabs |

Lab

2

# Detecting Missing Security Patches using MBSA on Windows

*MBSA is used to identify missing security updates and common security misconfigurations.*

## Lab Scenario

In real-life scenarios, it is not possible or an ideal practice to manually check the missing security patches, updates, misconfigurations on a Windows machine. As a network administrator, you should find a way to automate the process. The administrator can use MBSA to automate the process for checking if there are missing security patches on a Windows platform.

**ICON KEY**

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

## Lab Objectives

This lab will demonstrate how to use the MBSA tool to check for missing security patches on a Windows system.

## Lab Environment

To carry out the lab, you need:

- A virtual machine running Windows Server 2012
- A virtual machine running Windows Server 2008
- MBSA, located at **Z:\CND-Tools\CND Module 06 Host Security\Patch Management Tools\MBSA**
- A Web browser with an Internet connection
- **Administrative** privileges to run the tools

## Lab Duration

Time: 20 Minutes

## Overview of MBSA

The Microsoft Baseline Security Analyzer (MBSA) helps small and medium-sized businesses determine their security state in accordance with Microsoft security recommendations and offers specific remediation guidance.

## Lab Tasks

**TASK 1**

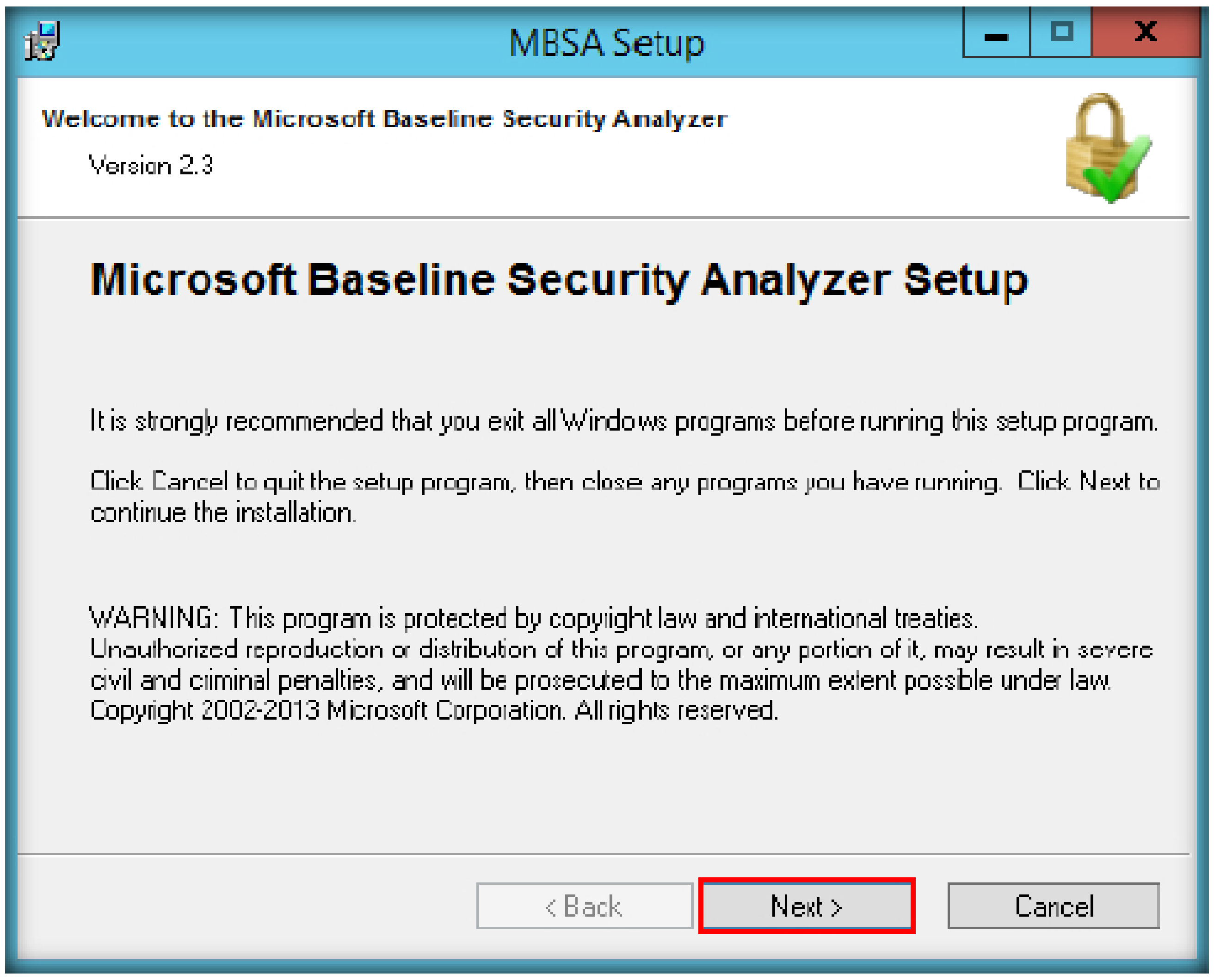
**Install MBSA in Administrator Machine (Windows Server 2012)**

1. Launch the **Windows Server 2012** machine and login as Admin, the credentials are Username: **Administrator**, and Password: **Pa$$w0rd**.

   **Note**: By default, the Administrator user profile is selected, just type the provided password in the password field and press **Enter**.

2. Navigate to **Z:\CND-Tools\CND Module 06 Host Security\Patch Management Tools\MBSA** and double-click **MBSASetup-x64-EN.msi**

3. The **MBSA Setup** window appears. Click **Next**.



MBSA Setup

Welcome to the Microsoft Baseline Security Analyzer

Version 2.3

**Microsoft Baseline Security Analyzer Setup**

It is strongly recommended that you exit all Windows programs before running this setup program.

Click Cancel to quit the setup program, then close any programs you have running. Click Next to continue the installation.

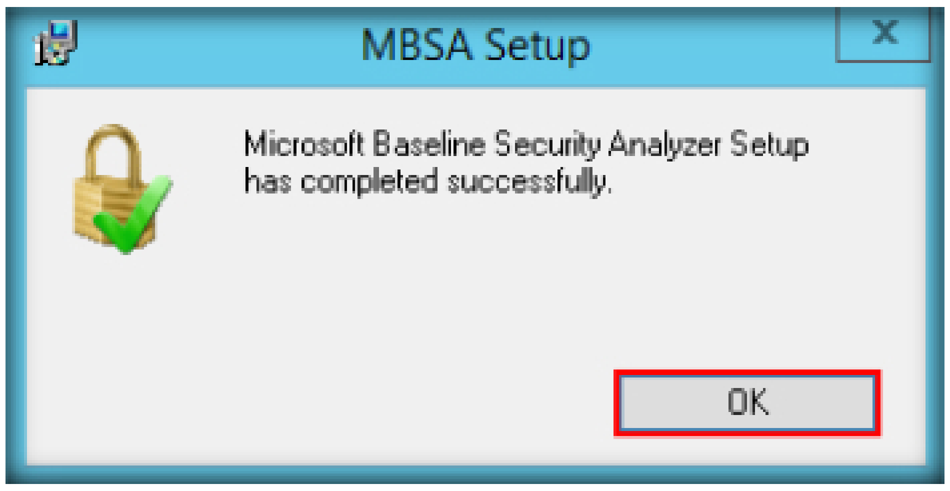
WARNING: This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.
Copyright 2002-2013 Microsoft Corporation. All rights reserved.

FIGURE 2.1: MBSA setup page

The MBSA provides built-in checks to determine if Windows administrative vulnerabilities are present, if weak passwords are being used on Windows accounts, the presence of known IIS and SQL administrative vulnerabilities, and which security updates are required for each individual system. The MBSA provides a dynamic assessment of missing security updates.

4. Follow the wizard driven instructions and complete the installation.

5. A MBSA Setup pop-up appears after completion of the installation, click **OK**.



MBSA Setup

Microsoft Baseline Security Analyzer Setup has completed successfully.

FIGURE 2.2: MBSA Installation complete

**TASK 2**

**Launch MBSA**

6. Navigate to the **desktop** and double-click the **Microsoft Baseline Security Analyzer 2.3** short-cut icon in order to launch.

   **Note**: Alternatively, you can also launch the **Microsoft Baseline Security Analyzer 2.3** from the installed start menu apps.

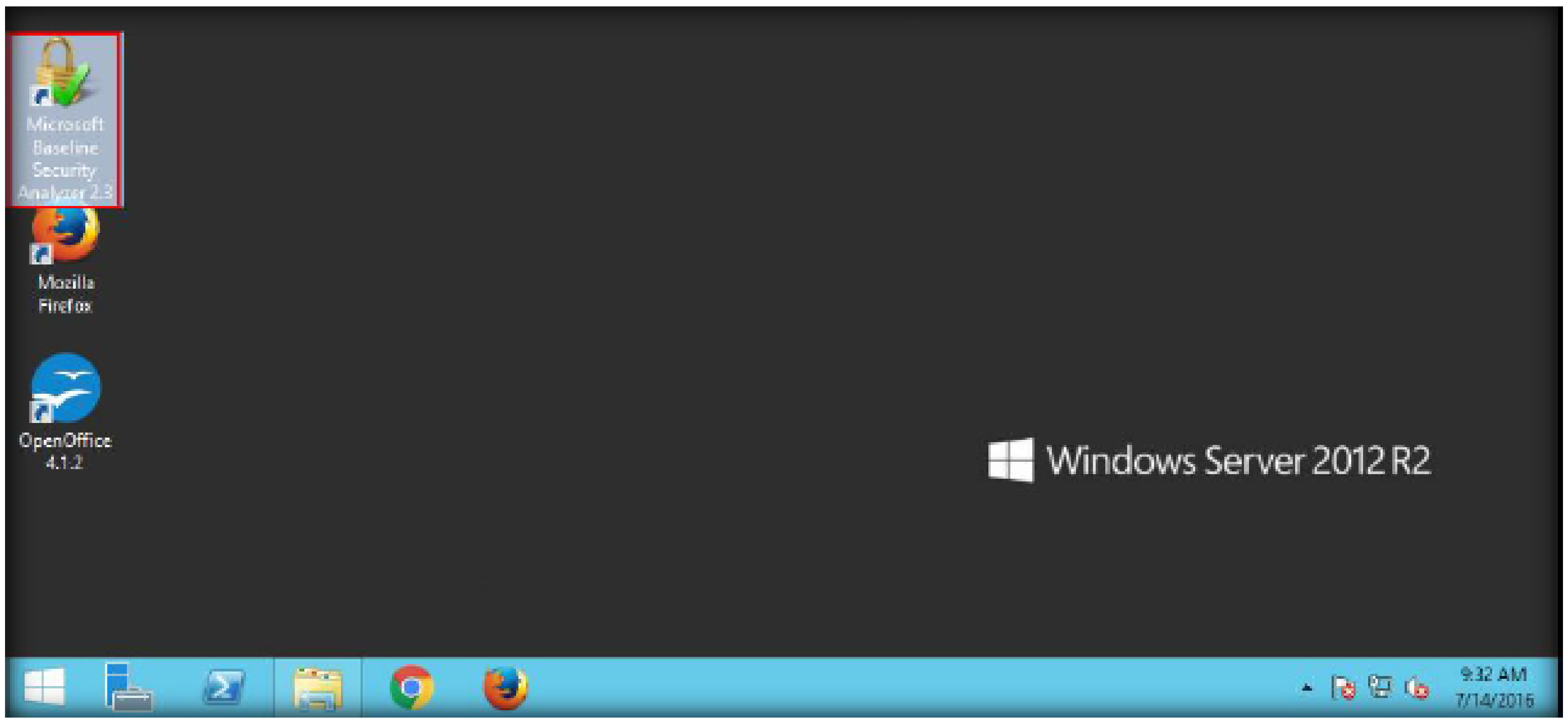
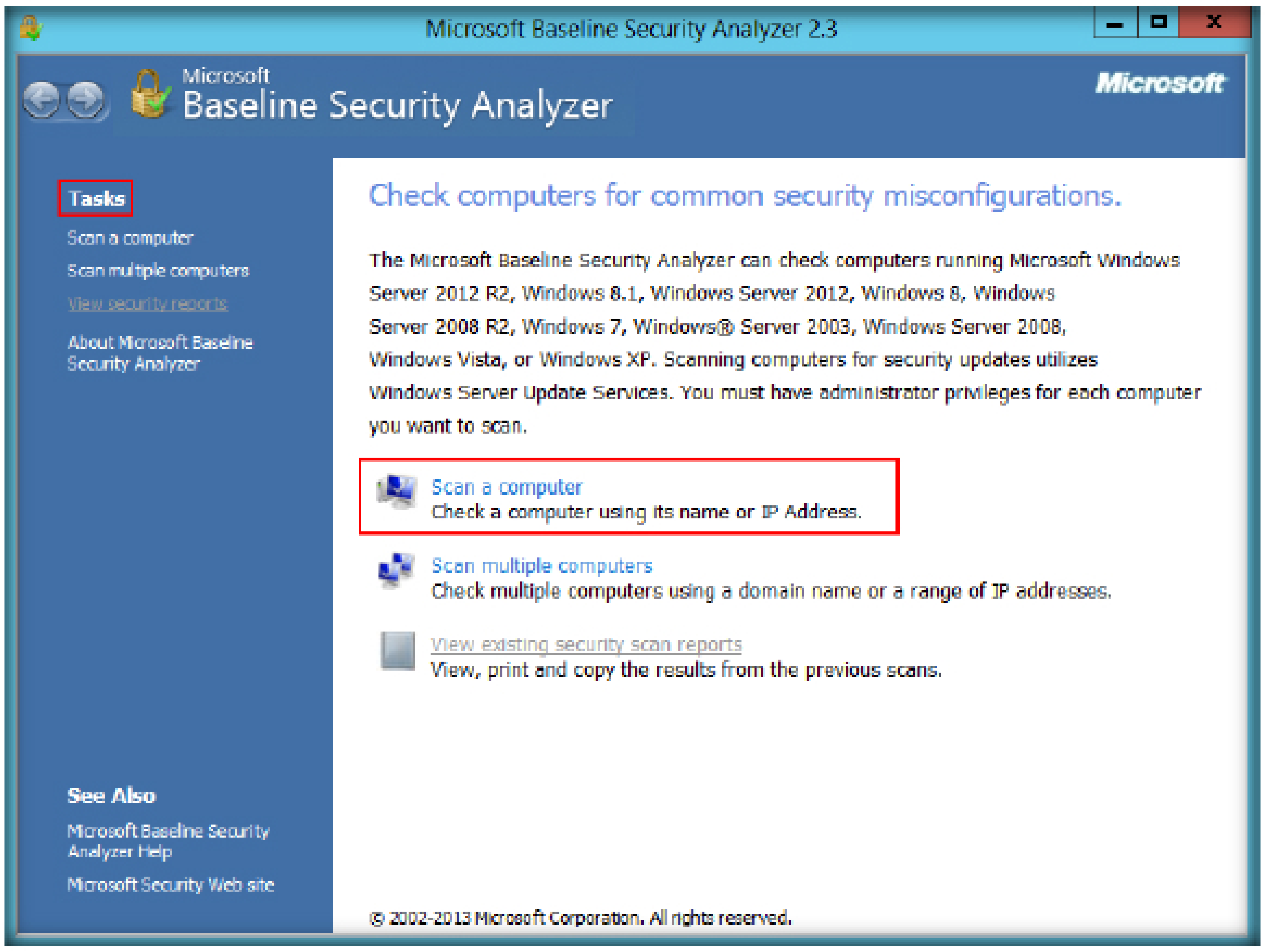


FIGURE 2.3: Launching MBSA from Desktop

7. The **Microsoft Baseline Security Analyzer 2.3** main window appears as shown in the screenshot, by default the **Tasks** option is selected in the left pane of the window. Click **Scan a computer**.

The MBSA can scan one or more computers by domain, IP address range or other grouping. Once complete, the MBSA provides a detailed report and instructions on how to help turn your system into a more secure working environment.


Microsoft Baseline Security Analyzer 2.3
Microsoft
Baseline Security Analyzer
Microsoft
Tasks
Scan a computer
Scan multiple computers
View security reports
About Microsoft Baseline Security Analyzer
See Also
Microsoft Baseline Security Analyzer Help
Microsoft Security Web site

Check computers for common security misconfigurations.

The Microsoft Baseline Security Analyzer can check computers running Microsoft Windows Server 2012 R2, Windows 8.1, Windows Server 2012, Windows 8, Windows Server 2008 R2, Windows 7, Windows® Server 2003, Windows Server 2008, Windows Vista, or Windows XP. Scanning computers for security updates utilizes Windows Server Update Services. You must have administrator privileges for each computer you want to scan.

Scan a computer
Check a computer using its name or IP Address.

Scan multiple computers
Check multiple computers using a domain name or a range of IP addresses.

View existing security scan reports
View, print and copy the results from the previous scans.

© 2002-2013 Microsoft Corporation. All rights reserved.

FIGURE 2.4: Scanning a Computer

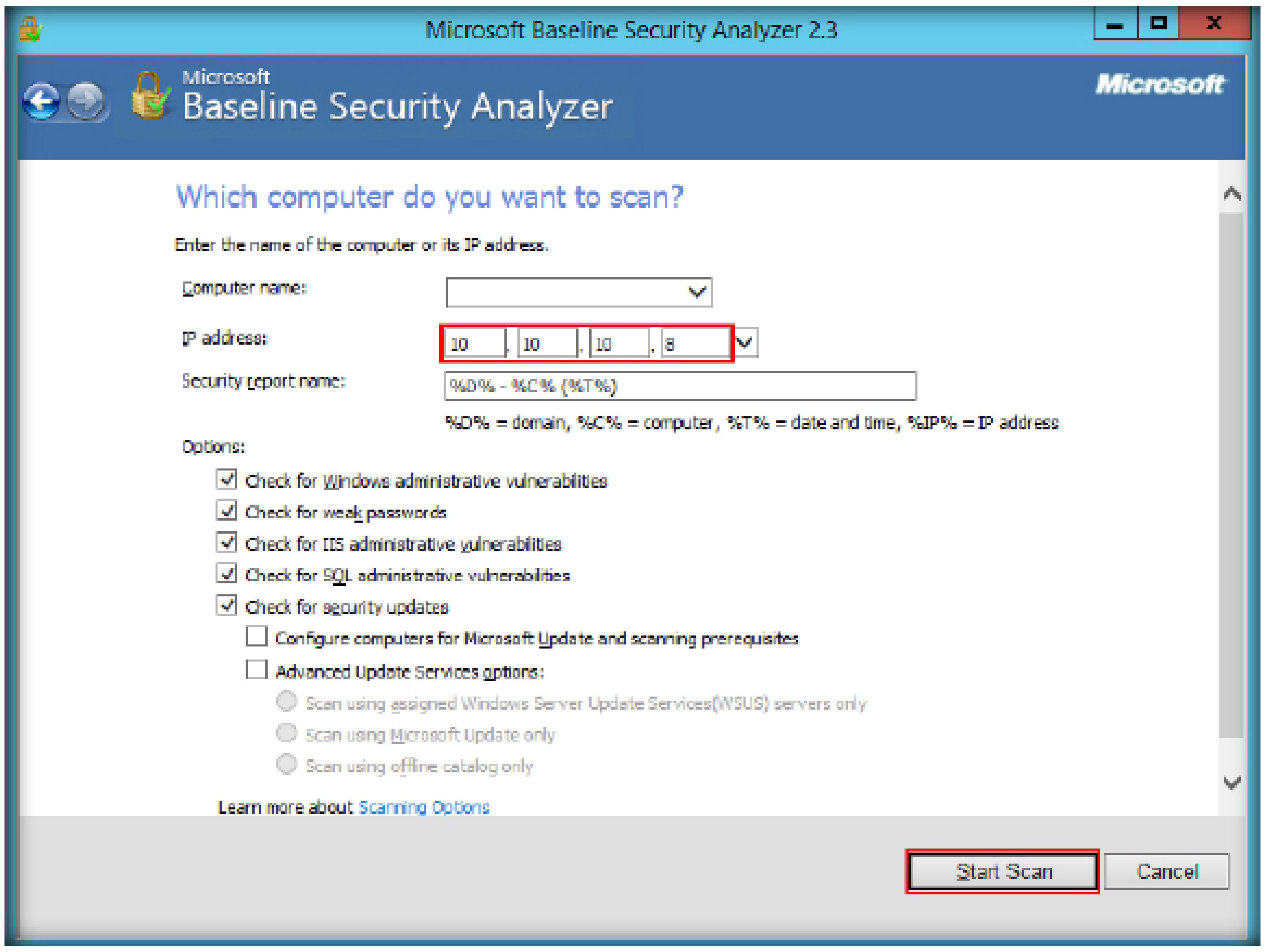
8. Which computer do you want to scan? A wizard appears, you can enter the **Computer name** or **IP address** in the respected fields, leave the other settings as default and click **Start Scan**.

9. In this lab we are going to scan the Windows Server 2008 (CND domain) machine and its IP address of **10.10.10.8**.

**TASK 3**

**Perform Scan**

**Note**: The IP address may vary if you have set different IP addresses in your lab environment.


Microsoft Baseline Security Analyzer 2.3
Microsoft
Baseline Security Analyzer
Microsoft

Which computer do you want to scan?

Enter the name of the computer or its IP address.

Computer name:

IP address: 10 . 10 . 10 . 8

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

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

Options:

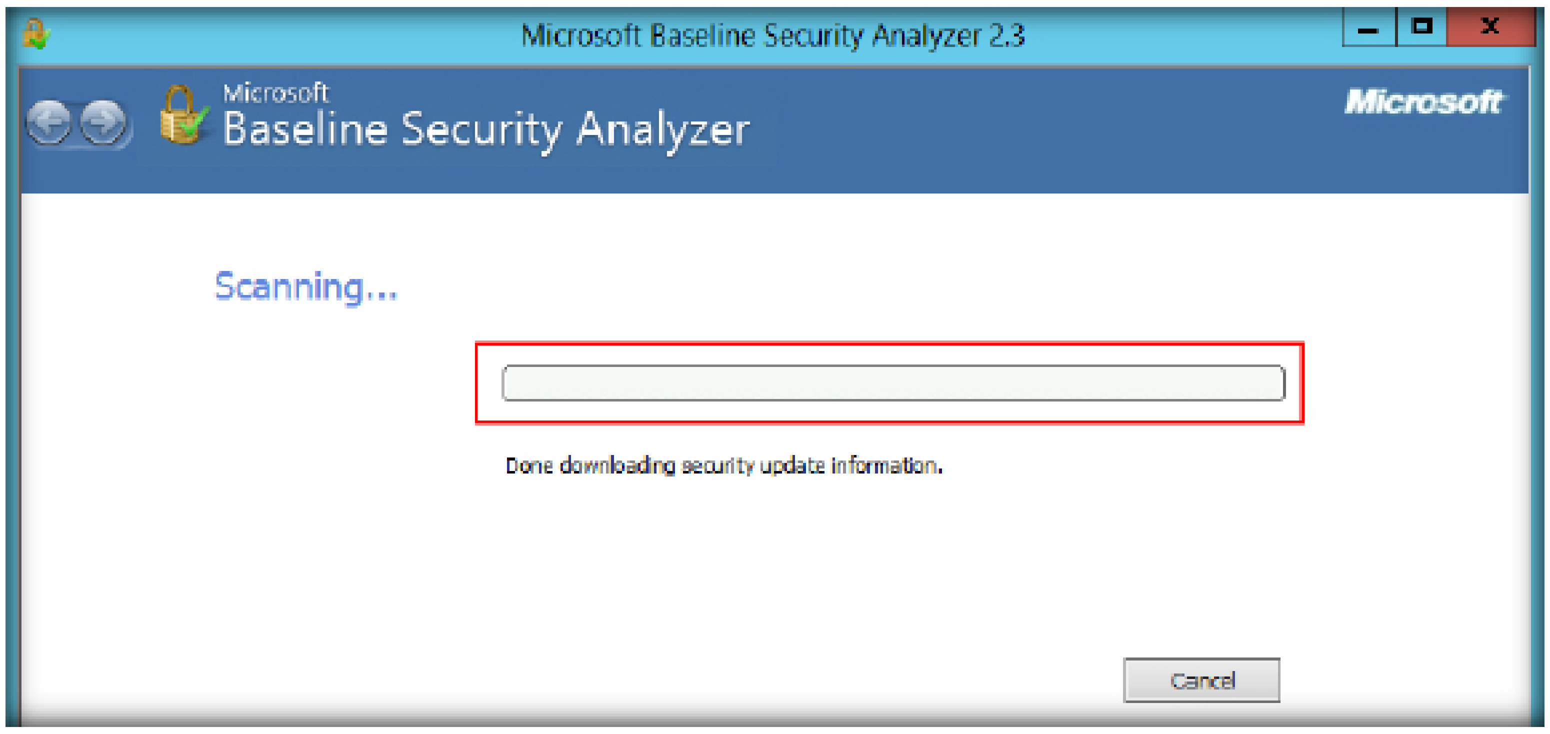
☑ Check for Windows administrative vulnerabilities
☑ Check for weak passwords
☑ Check for IIS administrative vulnerabilities
☑ Check for SQL administrative vulnerabilities
☑ Check for security updates
□ Configure computers for Microsoft Update and scanning prerequisites
□ Advanced Update Services options: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

Learn more about Scanning Options

FIGURE 2.5: MBSA initiates Scan

10. Wait until the scanning process is completed; it will take a few seconds to complete the scan.

The MBSA will create and store individual XML security reports for each computer scanned and will display the reports in the graphical user interface in HTML.


Microsoft Baseline Security Analyzer 2.3
Microsoft
Baseline Security Analyzer
Microsoft

Scanning...

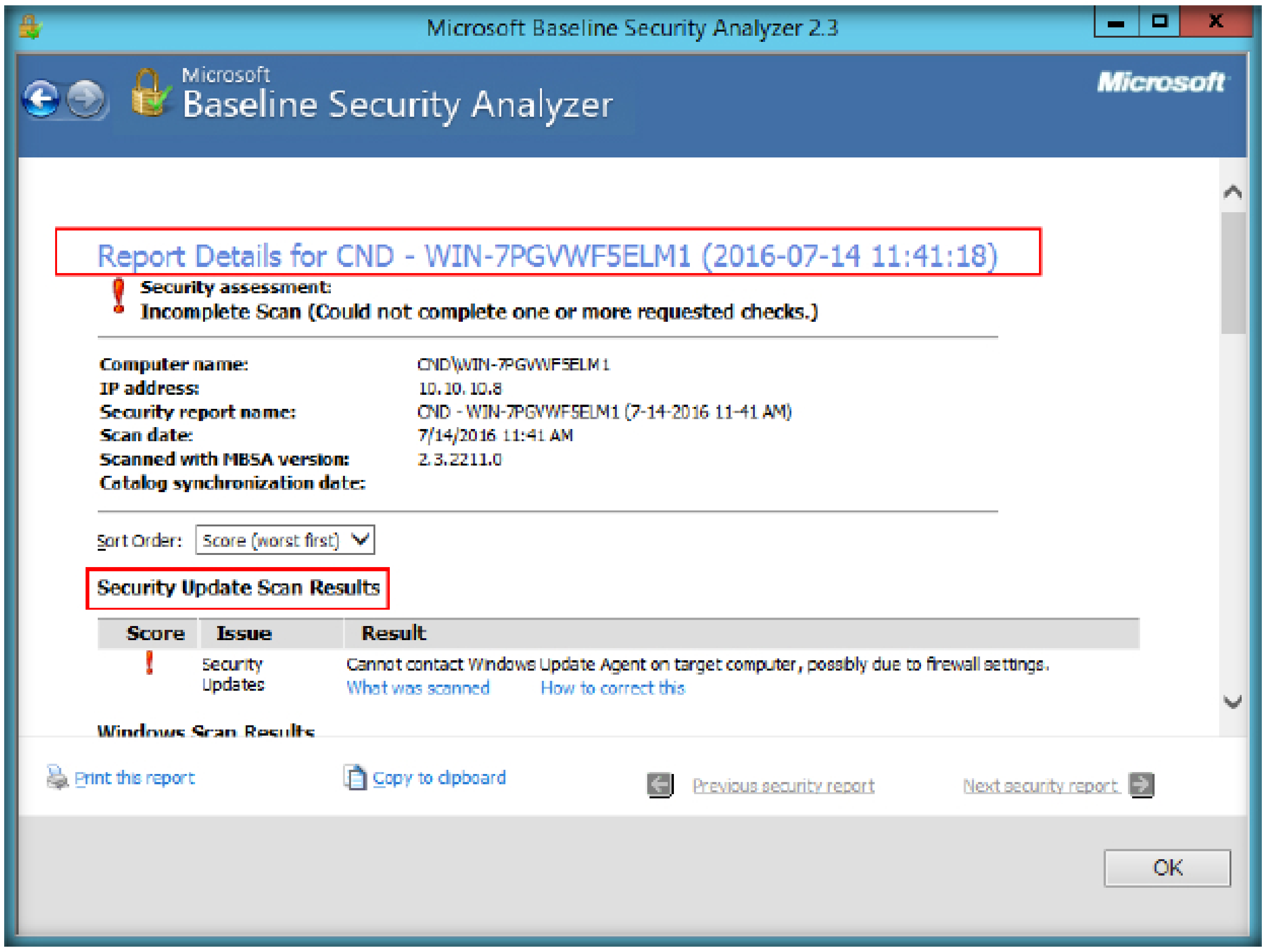
Done downloading security update information.

FIGURE 2.6: MBSA Scanning in Progress

11. Once the scan is completed scroll down and view the results in the **Security Update Scan Results** section. It will be showing missing security patches, security misconfigurations, etc.

    **Note**: The computer name may vary in your lab environment.

To use the MBSA tool, users will need either Windows Server 2008 R2, Windows 7, Server 2003, Server 2008, Vista, XP or Windows 2000 and will need administrator privileges sufficient to scan the target computers.



Report Details for CND - WIN-7PGVWF5ELM1 (2016-07-14 11:41:18)

**Security assessment:**
**Incomplete Scan (Could not complete one or more requested checks.)**

| | |
|---|---|
| **Computer name:** | CND\WIN-7PGVWF5ELM1 |
| **IP address:** | 10.10.10.8 |
| **Security report name:** | CND - WIN-7PGVWF5ELM1 (7-14-2016 11-41 AM) |
| **Scan date:** | 7/14/2016 11:41 AM |
| **Scanned with MBSA version:** | 2.3.2211.0 |
| **Catalog synchronization date:** | |

Sort Order: Score (worst first)

**Security Update Scan Results**

| Score | Issue | Result |
|---|---|---|
| ! | Security Updates | Cannot contact Windows Update Agent on target computer, possibly due to firewall settings.<br>What was scanned How to correct this |

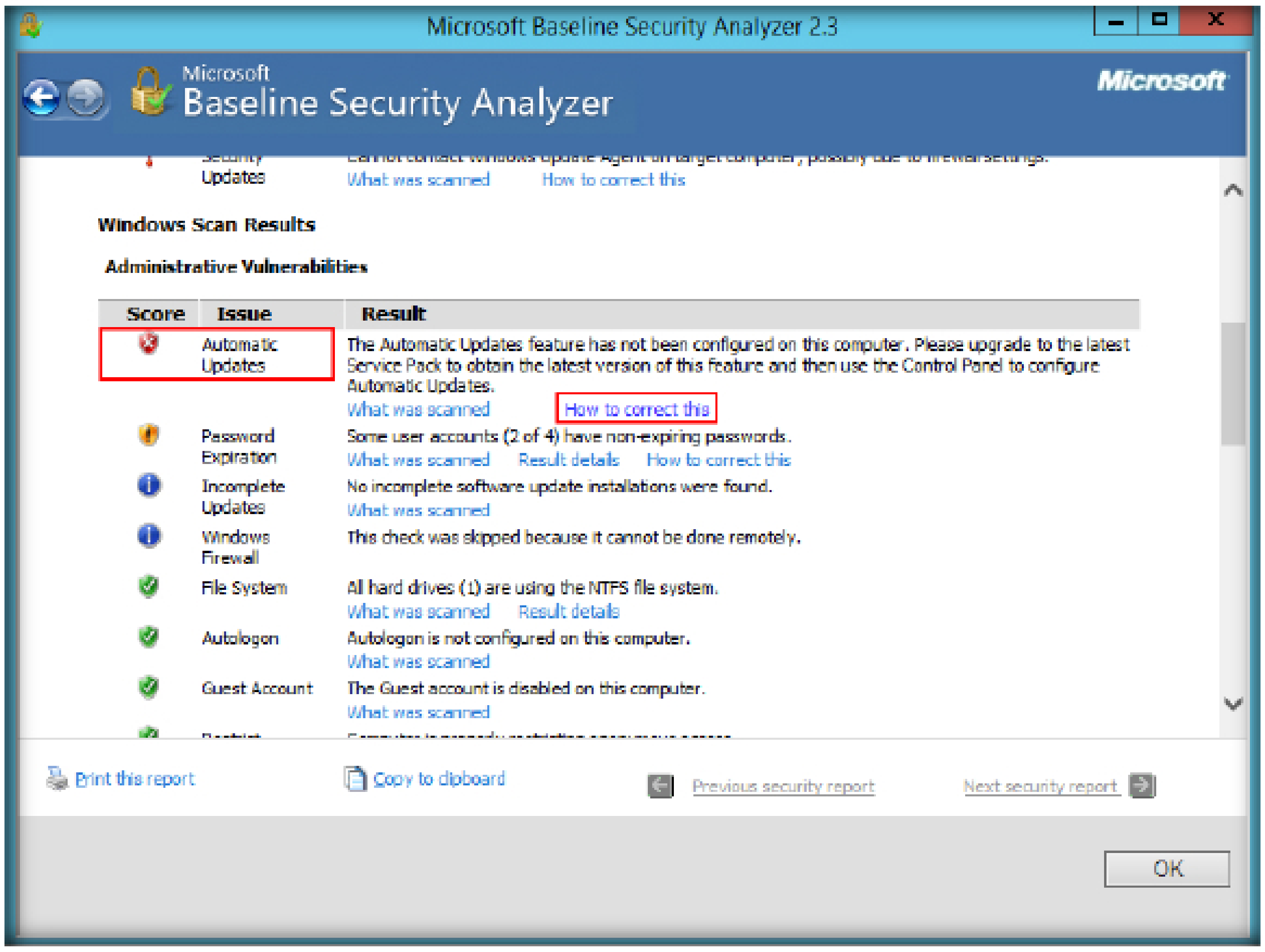
**Windows Scan Results**

FIGURE 2.7: MBSA Scan Results

12. Scroll down to view the Windows Scan Results, it will display the complete Administrative Vulnerabilities found in the targeted machine as shown in the screenshot.
13. MBSA shows the severity level of the vulnerability under Score, Name of the vulnerability in Issue, and information about the reported vulnerability and how to fix the issue in Result.

14. In this lab we are going to check the **Automatic Updates** vulnerability and how to fix this issue. To fix this issue, click the **How to correct this** link under the reported vulnerability.

After installing MBSA and running the tool, users can scan a computer using its name or IP address, scan multiple computers within a domain name or a range of IP addresses, or view existing security scan reports.


Microsoft Baseline Security Analyzer 2.3
Microsoft
Baseline Security Analyzer
Microsoft

Updates  What was scanned  How to correct this

**Windows Scan Results**

**Administrative Vulnerabilities**

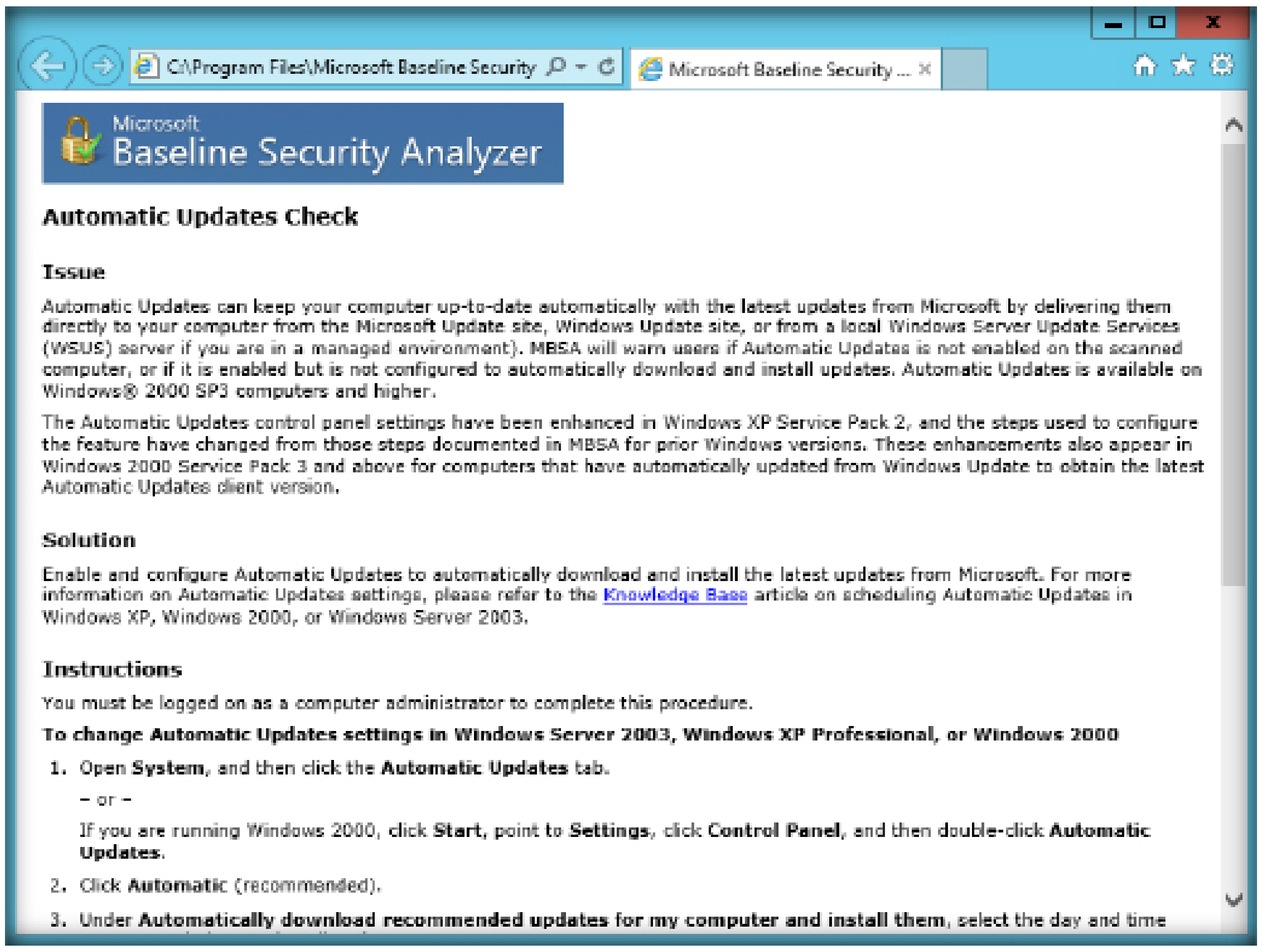
| Score | Issue | Result |
|---|---|---|
| ✗ | Automatic Updates | The Automatic Updates feature has not been configured on this computer. Please upgrade to the latest Service Pack to obtain the latest version of this feature and then use the Control Panel to configure Automatic Updates.<br>What was scanned  How to correct this |
| ! | Password Expiration | Some user accounts (2 of 4) have non-expiring passwords.<br>What was scanned  Result details  How to correct this |
| i | Incomplete Updates | No incomplete software update installations were found.<br>What was scanned |
| i | Windows Firewall | This check was skipped because it cannot be done remotely. |
| ✓ | File System | All hard drives (1) are using the NTFS file system.<br>What was scanned  Result details |
| ✓ | Autologon | Autologon is not configured on this computer.<br>What was scanned |
| ✓ | Guest Account | The Guest account is disabled on this computer.<br>What was scanned |

FIGURE 2.8: Windows Scan Results

15. Once you click on the How to correct this link, a browser window will appear with the solution to fix the respective issue as shown in the screenshot. Scroll down to view the complete information to fix the issue.

16. To resolve this issue, login to the target machine, follow the step by step instructions that are provided by the MBSA tool.

There are even more options available through the command-line interface to support scripting and fine-tuned control over MBSA's scanning and reporting features.


C:\Program Files\Microsoft Baseline Security
Microsoft Baseline Security ...
Microsoft
Baseline Security Analyzer

**Automatic Updates Check**

**Issue**

Automatic Updates can keep your computer up-to-date automatically with the latest updates from Microsoft by delivering them directly to your computer from the Microsoft Update site, Windows Update site, or from a local Windows Server Update Services (WSUS) server if you are in a managed environment). MBSA will warn users if Automatic Updates is not enabled on the scanned computer, or if it is enabled but is not configured to automatically download and install updates. Automatic Updates is available on Windows® 2000 SP3 computers and higher.

The Automatic Updates control panel settings have been enhanced in Windows XP Service Pack 2, and the steps used to configure the feature have changed from those steps documented in MBSA for prior Windows versions. These enhancements also appear in Windows 2000 Service Pack 3 and above for computers that have automatically updated from Windows Update to obtain the latest Automatic Updates client version.

**Solution**

Enable and configure Automatic Updates to automatically download and install the latest updates from Microsoft. For more information on Automatic Updates settings, please refer to the Knowledge Base article on scheduling Automatic Updates in Windows XP, Windows 2000, or Windows Server 2003.

**Instructions**

You must be logged on as a computer administrator to complete this procedure.

**To change Automatic Updates settings in Windows Server 2003, Windows XP Professional, or Windows 2000**

1. Open **System**, and then click the **Automatic Updates** tab.

   – or –

   If you are running Windows 2000, click **Start**, point to **Settings**, click **Control Panel**, and then double-click **Automatic Updates**.
2. Click **Automatic** (recommended).
3. Under **Automatically download recommended updates for my computer and install them**, select the day and time

FIGURE 2.9: How to fix the vulnerabilities Solution

17. Let us now fix the issue. To do this, click the **Windows Server 2008** machine and login.
18. Credentials to login:
    - Username: **CND\Administrator**
    - Password: **Pa$$w0rd**

**TASK 4**

**Fixing the Vulnerability**

19. Go to **Start** → **Control Panel** and double-click the **Windows Updates** icon.

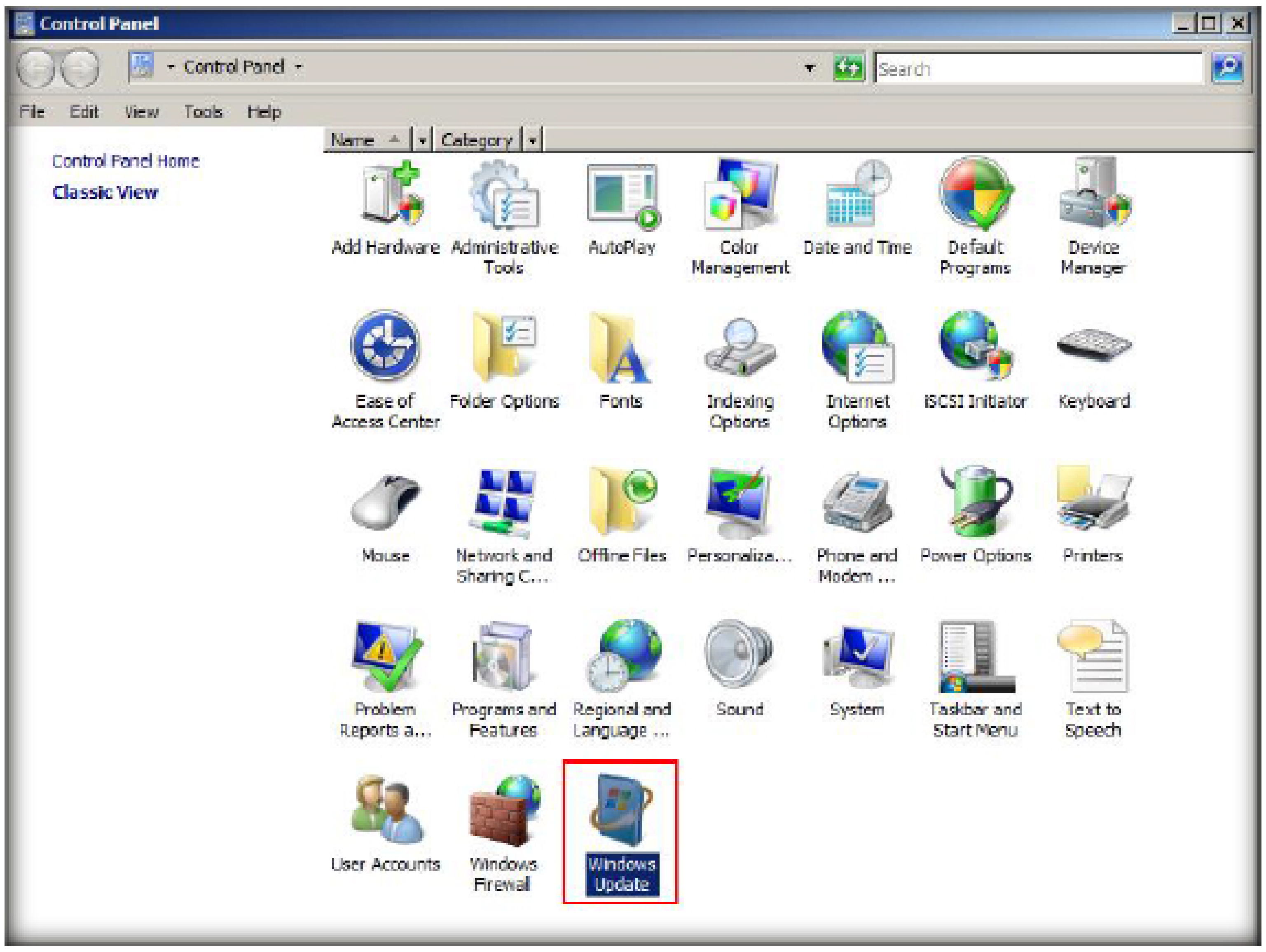
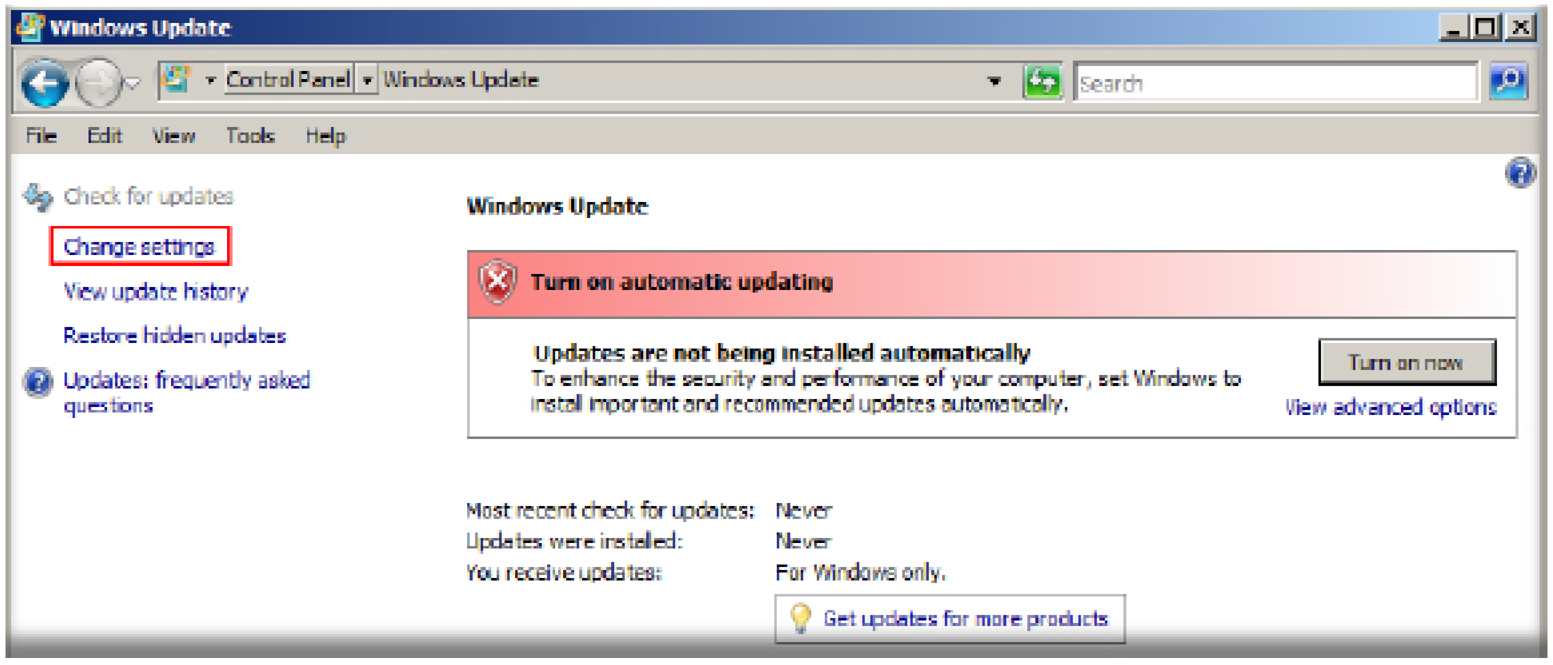


FIGURE 2.10: Windows Server 2008 Control Panel

The MBSA also provides an expanded list of options beyond what is available via the graphical interface via the command-line interface. These options can be accessed by opening a command-prompt in the MBSA installation directory and running MBSACLI.exe /?

20. A Windows Update window appears, click the **Change settings** link in the left hand side of the window.



Turn on automatic updating

Updates are not being installed automatically

To enhance the security and performance of your computer, set Windows to install important and recommended updates automatically.

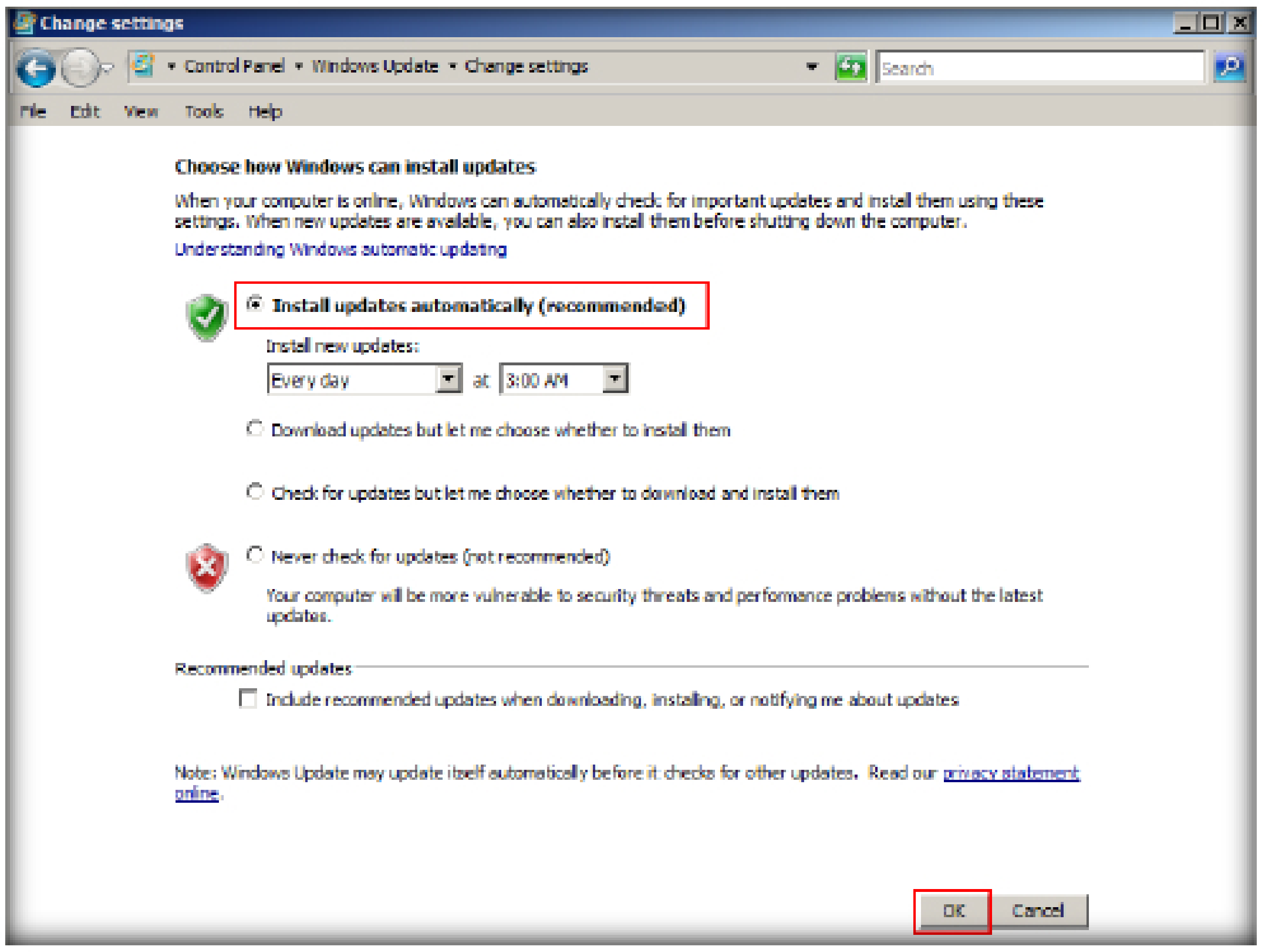
Most recent check for updates: Never
Updates were installed: Never
You receive updates: For Windows only.

FIGURE 2.11: Windows Server 2008 Windows Update

21. In the Change settings window, choose the **Install updates automatically (recommended)** radio button and schedule the time to **Install new updates** or leave the settings as default and then click **OK**.

After you select the appropriate options and computers, you then trigger the scan, which typically takes several minutes to run. By default, the MBSA will automatically attempt to reach Microsoft Update for the latest catalog. The MBSA will augment the scan using any updates approved by the WSUS admin in managed environments.

22. As soon as you click the **OK** button, it will start checking for new updates and it will prompt you to install the updates. Install the required updates on the machine.


Change settings

Control Panel ▸ Windows Update ▸ Change settings

Choose how Windows can install updates

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

Understanding Windows automatic updating

● Install updates automatically (recommended)

Install new updates: Every day at 3:00 AM

○ Download updates but let me choose whether to install them

○ Check for updates but let me choose whether to download and install them

○ Never check for updates (not recommended)

Your computer will be more vulnerable to security threats and performance problems without the latest updates.

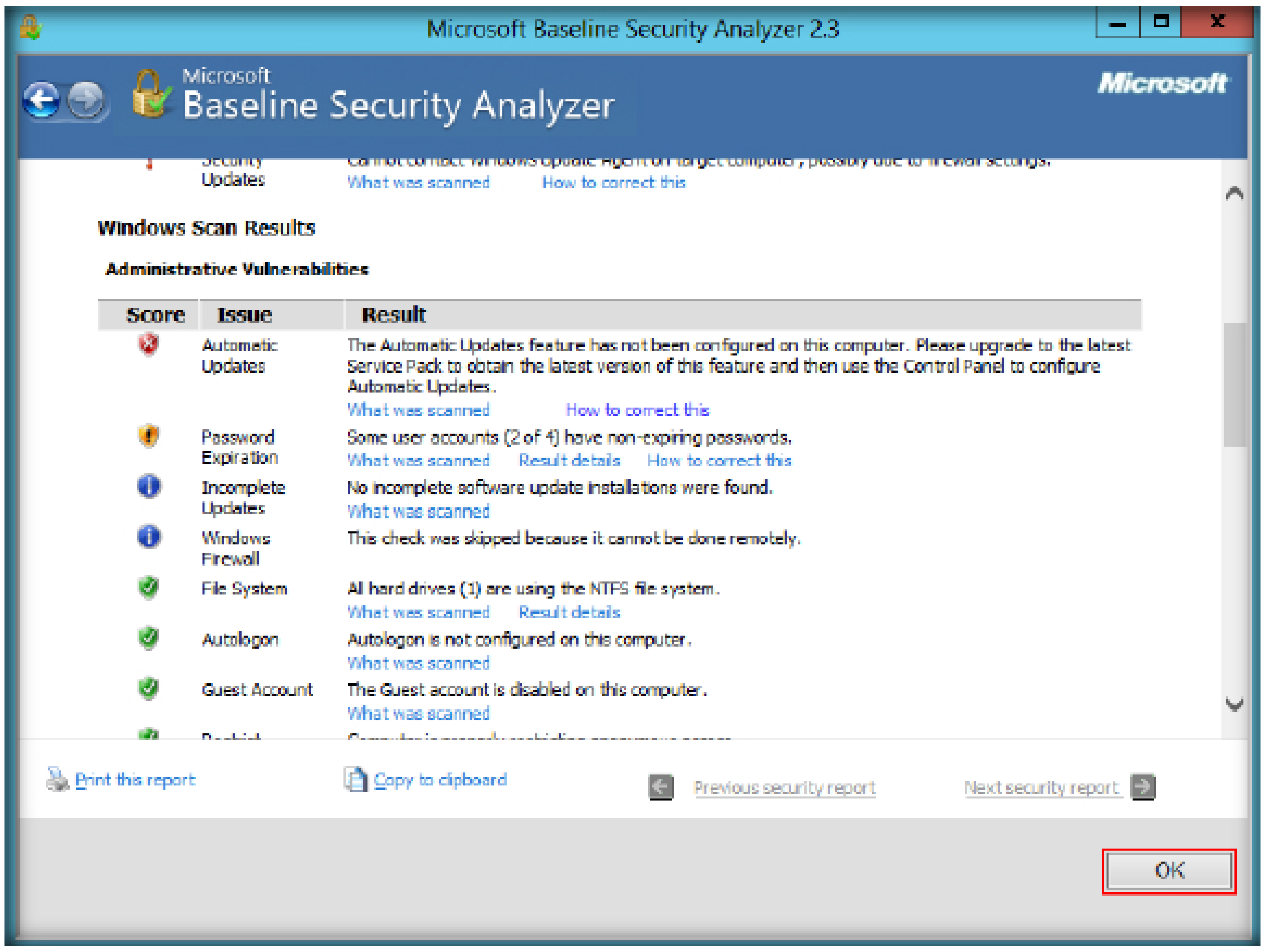
Recommended updates

□ Include recommended updates when downloading, installing, or notifying me about updates

Note: Windows Update may update itself automatically before it checks for other updates. Read our privacy statement online.

FIGURE 2.12: Choosing how Windows can Install Updates

23. Now switch back to the Windows Server 2012 machine and click **OK** to go back to the main screen of MBSA.


Microsoft Baseline Security Analyzer 2.3

Microsoft Baseline Security Analyzer

Security Updates — Cannot contact Windows Update Agent on target computer, possibly due to firewall settings. What was scanned How to correct this

Windows Scan Results

Administrative Vulnerabilities

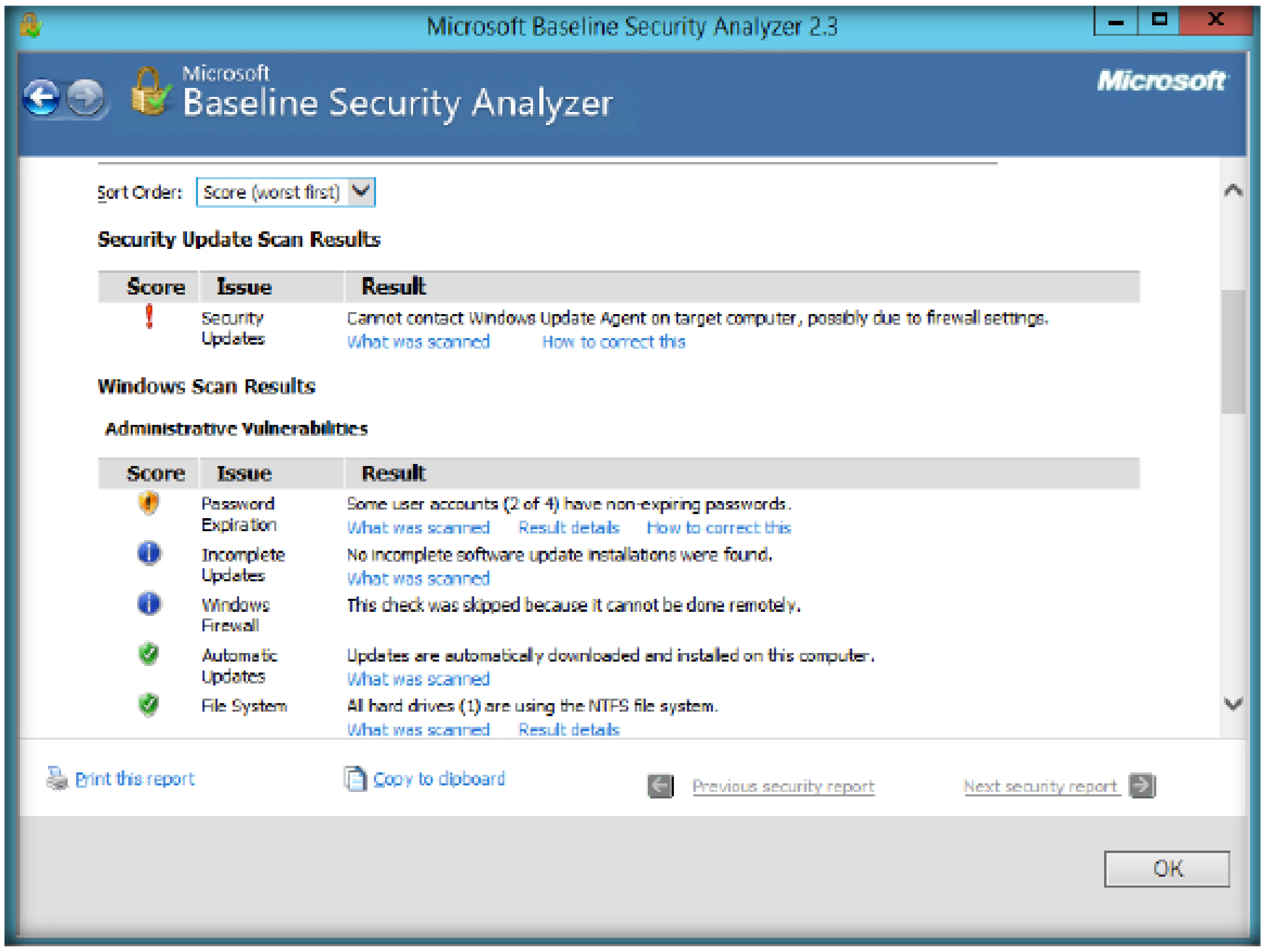
| Score | Issue | Result |
|---|---|---|
| ✗ | Automatic Updates | The Automatic Updates feature has not been configured on this computer. Please upgrade to the latest Service Pack to obtain the latest version of this feature and then use the Control Panel to configure Automatic Updates.<br>What was scanned How to correct this |
| ! | Password Expiration | Some user accounts (2 of 4) have non-expiring passwords.<br>What was scanned Result details How to correct this |
| i | Incomplete Updates | No incomplete software update installations were found.<br>What was scanned |
| i | Windows Firewall | This check was skipped because it cannot be done remotely. |
| ✓ | File System | All hard drives (1) are using the NTFS file system.<br>What was scanned Result details |
| ✓ | Autologon | Autologon is not configured on this computer.<br>What was scanned |
| ✓ | Guest Account | The Guest account is disabled on this computer.<br>What was scanned |

FIGURE 2.13: MBSA Windows Scan Results

24. Follow steps **7** to **14** to rescan the Windows Server 2008 machine and check if the issue is fixed.

25. Now the Automatic Updates issue is fixed as shown in the screenshot. Similarly, you can fix all the Administrative Vulnerabilities using the respective scan results.

MBSA Scan Results after fixing the found vulnerabilities in the Targeted machine.


Microsoft Baseline Security Analyzer 2.3
Microsoft
Baseline Security Analyzer
Microsoft

Sort Order: Score (worst first)

**Security Update Scan Results**

| Score | Issue | Result |
|---|---|---|
| ! | Security Updates | Cannot contact Windows Update Agent on target computer, possibly due to firewall settings.<br>What was scanned How to correct this |

**Windows Scan Results**

**Administrative Vulnerabilities**

| Score | Issue | Result |
|---|---|---|
| ⚠ | Password Expiration | Some user accounts (2 of 4) have non-expiring passwords.<br>What was scanned Result details How to correct this |
| ⓘ | Incomplete Updates | No incomplete software update installations were found.<br>What was scanned |
| ⓘ | Windows Firewall | This check was skipped because it cannot be done remotely. |
| ✓ | Automatic Updates | Updates are automatically downloaded and installed on this computer.<br>What was scanned |
| ✓ | File System | All hard drives (1) are using the NTFS file system.<br>What was scanned Result details |

FIGURE 2.14: MBSA Fixed the Issue

## Lab Analysis

Analyze and document the results of the lab exercise. Give your opinion on your target's security posture and exposure through free public information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

| Internet Connection Required | |
|---|---|
| □ Yes | ☑ No |
| Platform Supported | |
| ☑ Classroom | ☑ iLabs |

Lab

3

# Conducting Security Checks using buck-security On Linux

*buck-security is a collection of security checks for Linux*

## Lab Scenario

As a network administrator, you should be able to conduct security checks against a Linux system in order to know the security status of the system.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

## Lab Objectives

This lab will demonstrate how to conduct a security check on an Ubuntu Linux system.

## Lab Environment

To carry out the lab, you need:

- A virtual machine running Ubuntu Linux
- A Web browser with an Internet connection
- **Administrative** privileges to run the tools

## Lab Duration

Time: 10 Minutes

## Overview of buck-security

The aim of buck-security is to allow you to get a quick overview of the security status for your system. It is useful to get an overview of the security status of the system immediately. It runs important tests and returns the results to you after a couple of minutes.

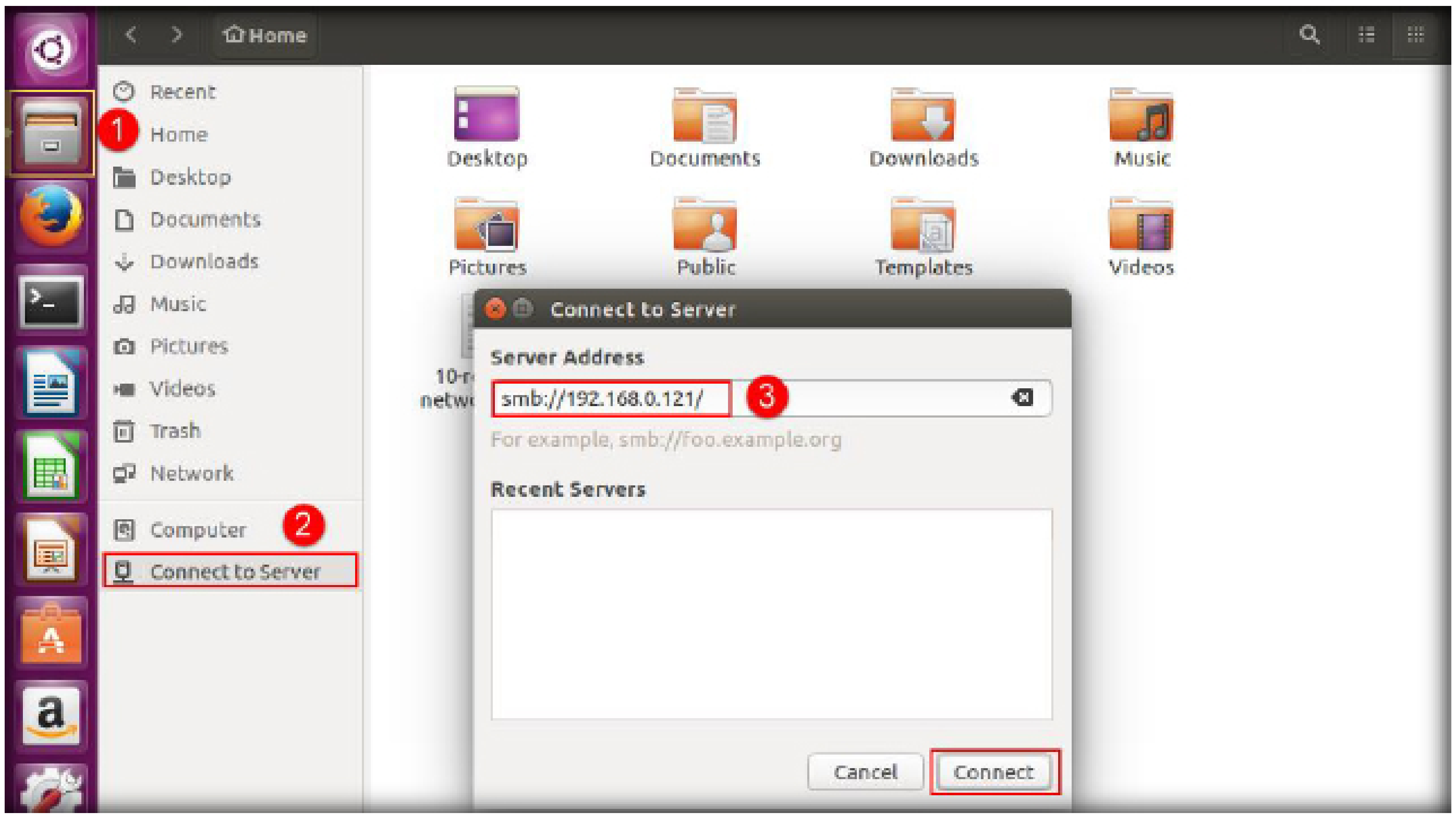
## Lab Tasks

1. Turn on and log in to the **Ubuntu** VM

The aim of buck-security is to allow you to get a quick overview of the security status of your system. As a Linux system administrator - but also as a normal Linux user - you often wonder if your system is secure.

2. Navigate to task bar and click the Files icon. Next, click Connect to Server and when the connect to Server window appears, type the following: **smb://IP Address of the CND-Tools shared folder machine** and click **Connect**.

   **Note**: The IP address may vary in your lab environment.



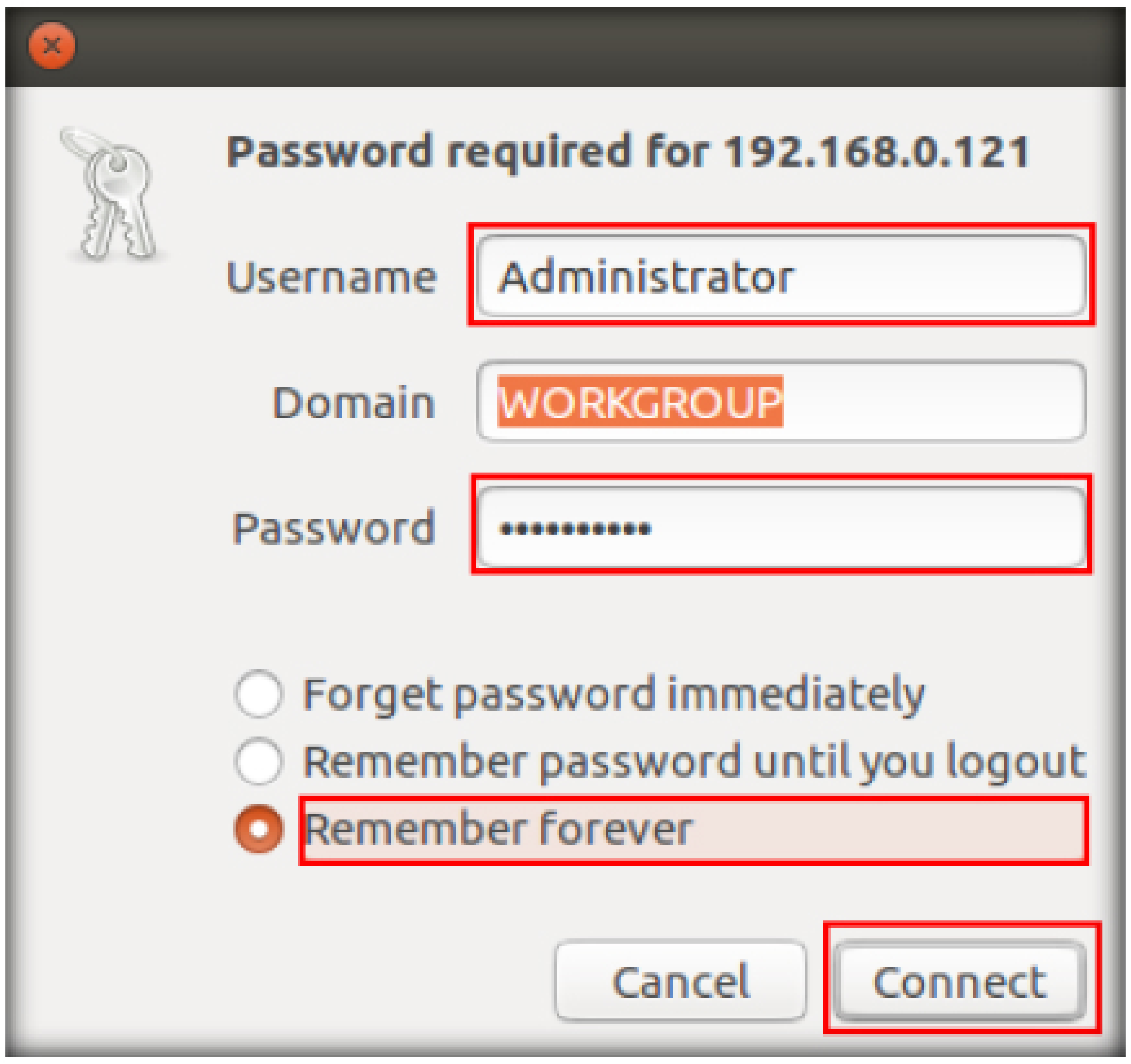
Server Address: smb://192.168.0.121/

For example, smb://foo.example.org

FIGURE 3.1: Entering super user mode

3. Password required for pop-up appears, type the credentials of your local host machine where the shared folder is located and check **Remember forever** radio button and click **Connect**.

In this situation, it is useful to get an overview of the security status of the system immediately. Buck-security was designed exactly for this. It runs important tests and returns the results to you after a couple of minutes.



Password required for 192.168.0.121

Username: Administrator

Domain: WORKGROUP

Password: •••••••••••

○ Forget password immediately
○ Remember password until you logout
● Remember forever

FIGURE 3.2: Entering super user mode

Buck Security should be just a small tool in your holistic security concept. Server security is a complex PROCESS which can't be guaranteed by a simple tool.

4. Navigate to CND-tools on IP address of the machine (where CND-Tools are shared) → CND Module 06 Host Security → Linux Security and copy **buck-security-master** folder and paste it on the **Desktop**.

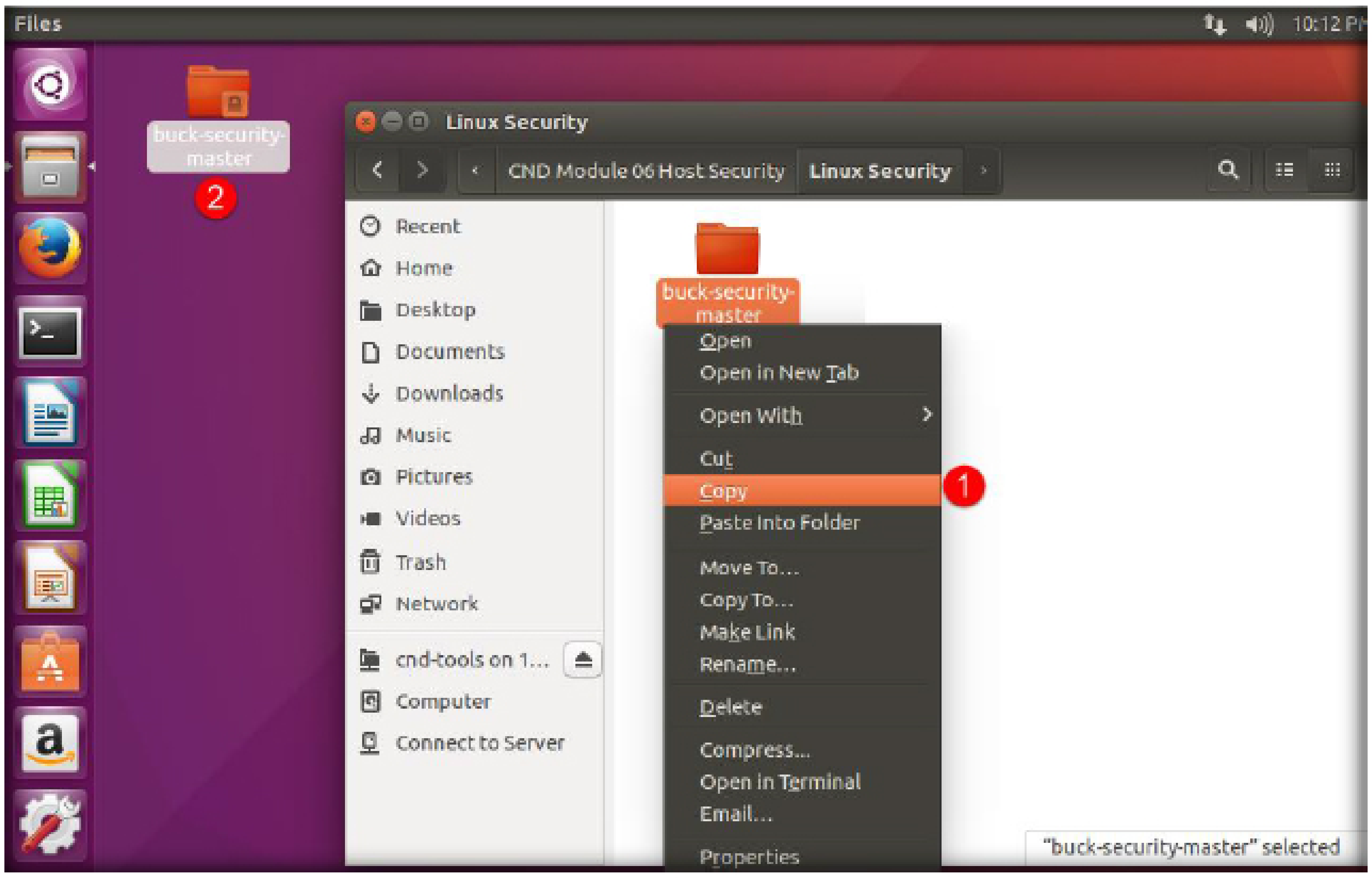


FIGURE 3.3: Entering super user mode

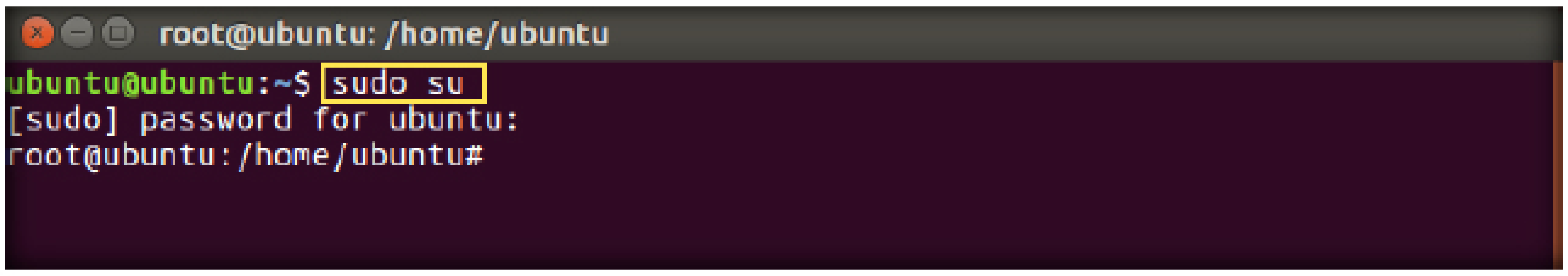
5. Launch a **Terminal**, and type **sudo su** and press **Enter**

6. It will prompt you for **sudo** (Administrator) password, type **toor** and press **Enter**.

**Note**: The password is not visible while you are typing in the terminal window. The password may vary a different password was chosen at the time of installation.

**TASK 1**

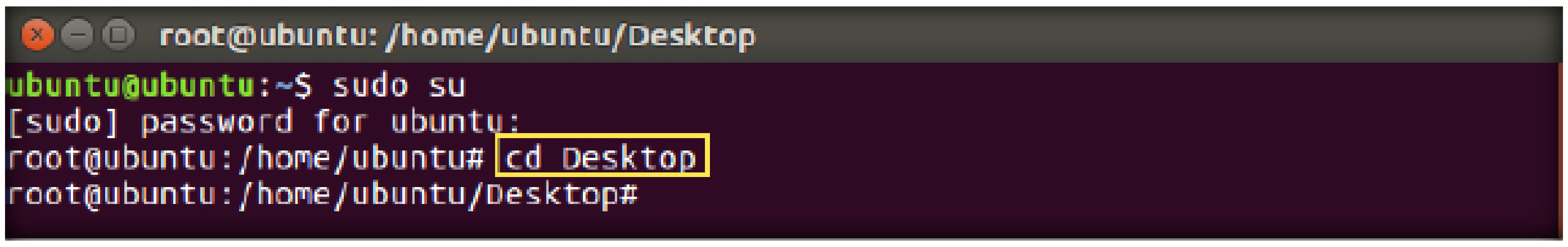
**Launching buck-security in Ubuntu Linux terminal**



```
root@ubuntu: /home/ubuntu
ubuntu@ubuntu:~$ sudo su
[sudo] password for ubuntu:
root@ubuntu:/home/ubuntu#
```

FIGURE 3.4: Entering super user mode

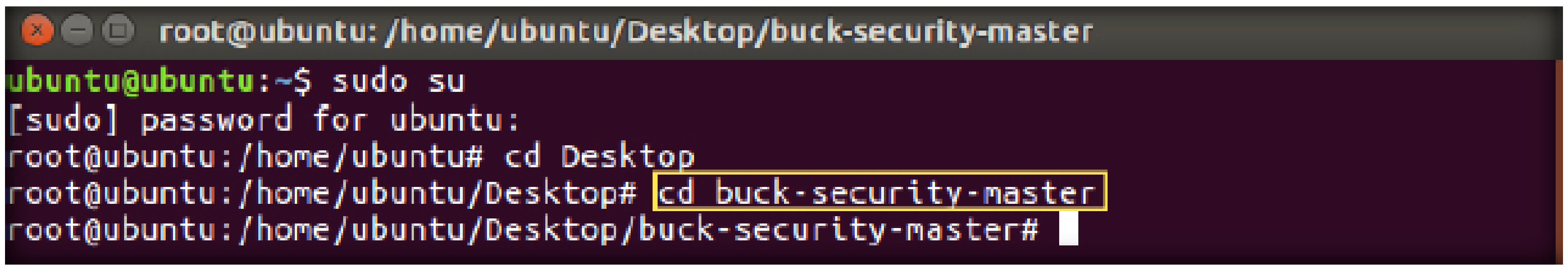
7. Type **cd Desktop** and press **Enter** to navigate to the **Desktop** folder.



```
root@ubuntu: /home/ubuntu/Desktop
ubuntu@ubuntu:~$ sudo su
[sudo] password for ubuntu:
root@ubuntu:/home/ubuntu# cd Desktop
root@ubuntu:/home/ubuntu/Desktop#
```

FIGURE 3.5: Entering Downloads folder

8. Type **cd buck-security-master** and press **Enter** to access the buck-security directory.



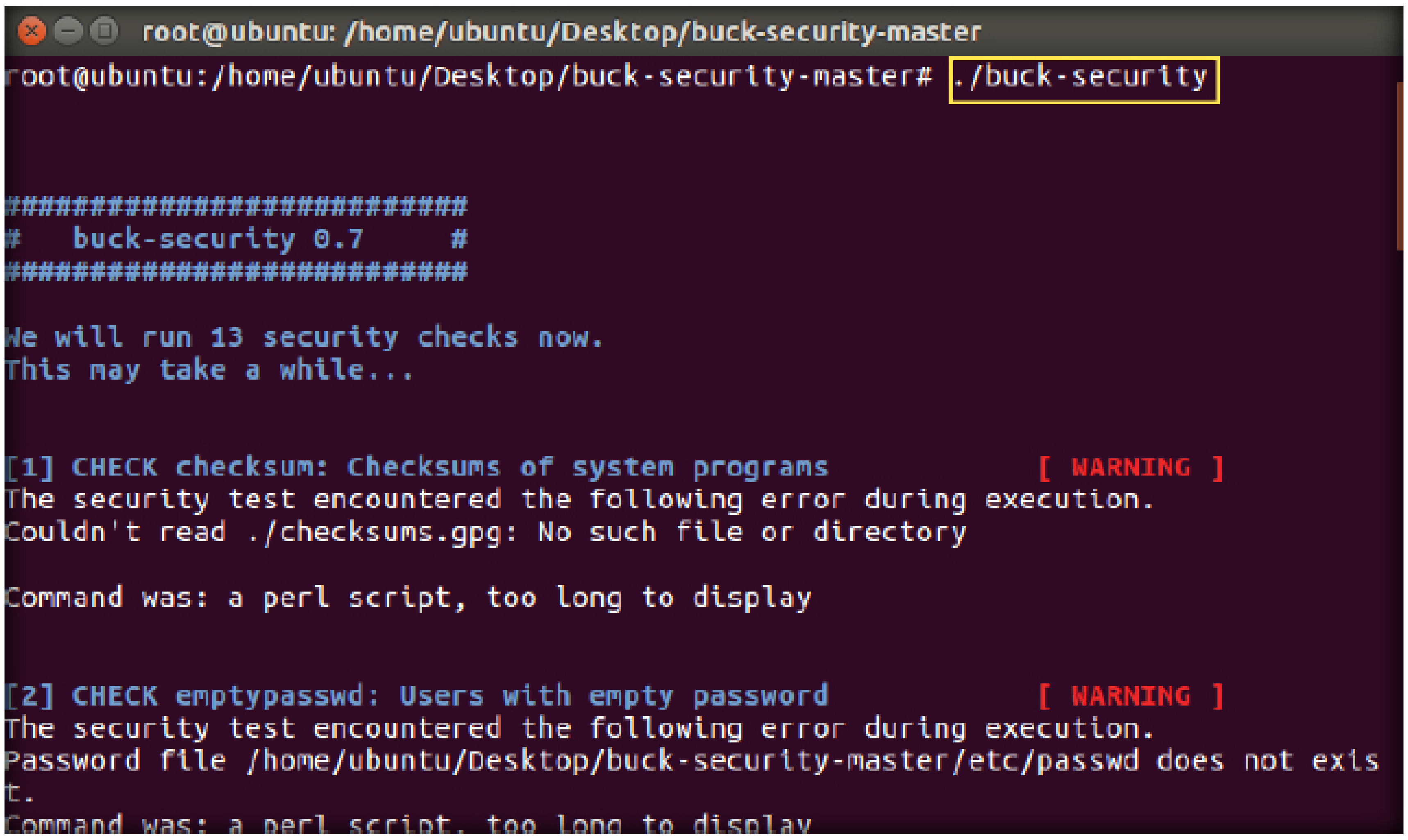
```
ubuntu@ubuntu:~$ sudo su
[sudo] password for ubuntu:
root@ubuntu:/home/ubuntu# cd Desktop
root@ubuntu:/home/ubuntu/Desktop# cd buck-security-master
root@ubuntu:/home/ubuntu/Desktop/buck-security-master#
```

FIGURE 3.6: Entering Buck-security folder

**TASK 2**

**Running Security Check**

9. Type **./buck-security** and press **Enter**. This command will run the security scan on the Linux machine and check for vulnerabilities in that machine.



```
root@ubuntu:/home/ubuntu/Desktop/buck-security-master# ./buck-security


###########################
#   buck-security 0.7     #
###########################

We will run 13 security checks now.
This may take a while...


[1] CHECK checksum: Checksums of system programs            [ WARNING ]
The security test encountered the following error during execution.
Couldn't read ./checksums.gpg: No such file or directory

Command was: a perl script, too long to display


[2] CHECK emptypasswd: Users with empty password            [ WARNING ]
The security test encountered the following error during execution.
Password file /home/ubuntu/Desktop/buck-security-master/etc/passwd does not exis
t.
Command was: a perl script, too long to display
```

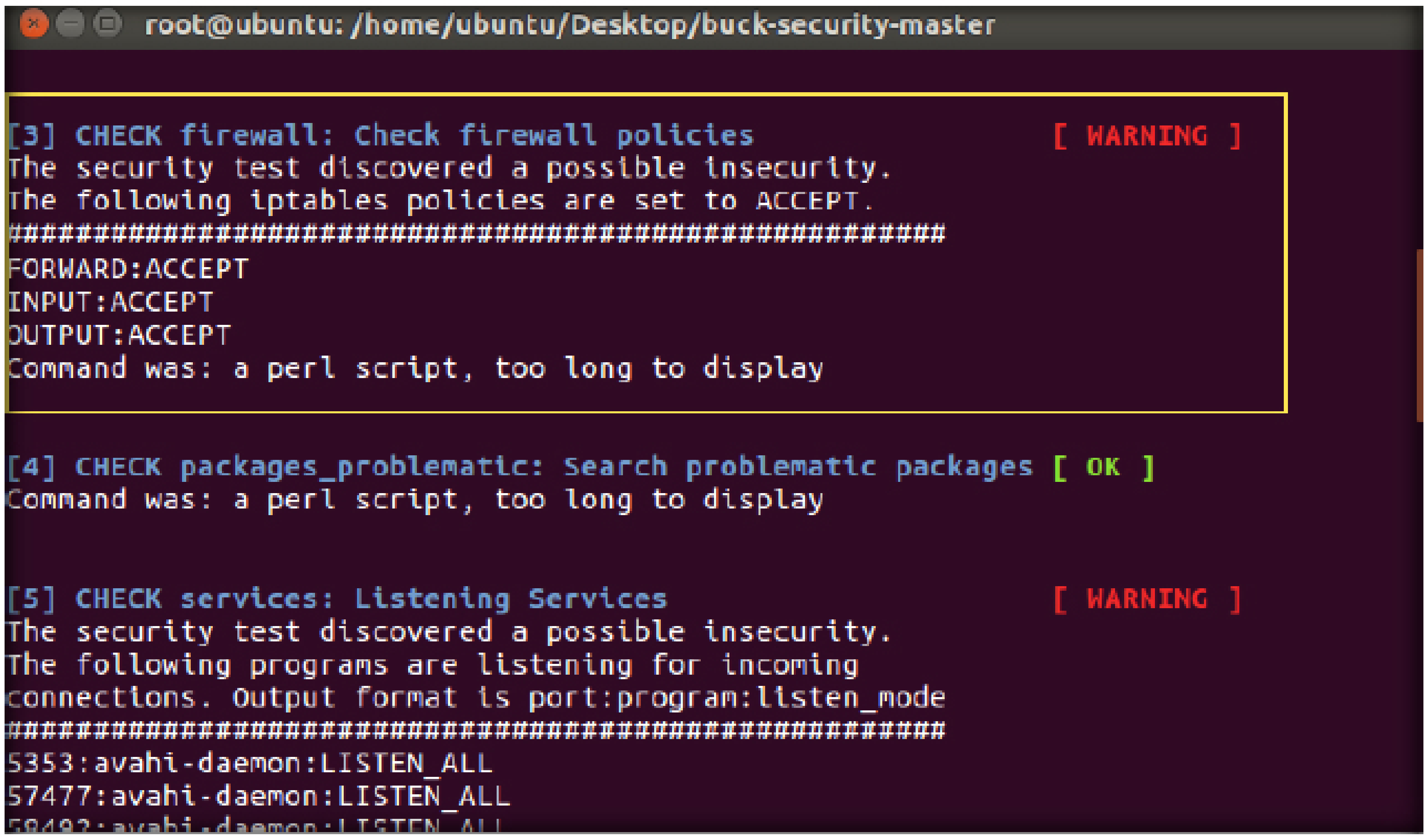
FIGURE 3.7: Buck security output first part

The different security-checks are the core of Buck Security. In every security book for Linux you'll find a couple of small tricks to check the security status of your system. Buck Security aims to unite all these small but important and useful checks in one easy-to-use program.

10. Scroll down to view the security Warning messages that were discovered by buck-security.

11. Buck-security will display a warning message, if any issues are found in the security measures as shown in the screenshot.

12. In this lab scroll down to the **[3] CHECK firewall: Check firewall policies** section. This section shows you the complete settings of the Firewall in the Linux machine.



```
root@ubuntu: /home/ubuntu/Desktop/buck-security-master

[3] CHECK firewall: Check firewall policies              [ WARNING ]
The security test discovered a possible insecurity.
The following iptables policies are set to ACCEPT.
######################################################
FORWARD:ACCEPT
INPUT:ACCEPT
OUTPUT:ACCEPT
Command was: a perl script, too long to display

[4] CHECK packages_problematic: Search problematic packages [ OK ]
Command was: a perl script, too long to display

[5] CHECK services: Listening Services                   [ WARNING ]
The security test discovered a possible insecurity.
The following programs are listening for incoming
connections. Output format is port:program:listen_mode
######################################################
5353:avahi-daemon:LISTEN_ALL
57477:avahi-daemon:LISTEN_ALL
58492:avahi-daemon:LISTEN_ALL
```

FIGURE 3.8: Entering super user mode

The most common use of the sticky bit today is on directories, where, when set, items inside the directory can be renamed or deleted only by the item's owner, the directory's owner, or the superuser; without the sticky bit set, any user with write and execute permissions for the directory can rename or delete contained files, regardless of the owner. Typically, this is set on the /tmp directory to prevent

13. You can run the security scan using buck-security against an Ubuntu machine, to find the issues and vulnerabilities within the machine and fix those vulnerabilities.

## Lab Analysis

Analyze and document the results of the lab exercise. Give your opinion on your target's security posture and exposure through free public information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

| | |
|---|---|
| **Internet Connection Required** | |
| □ Yes | ☑ No |
| Platform Supported | |
| ☑ Classroom | ☑ iLabs |

Lab

4

# Remote Patch Management using BatchPatch

*BatchPatch is a software patch management tool. It can remotely initiate Windows Update, WSUS, software deployments, and reboots on many computers.*

## Lab Scenario

An administrator is required to apply security patches or updates to a system in order to ensure they are not vulnerable to attack. Patch management is one of the important tasks administrators should perform periodically to ensure all systems in the network are patched and updated. The Administrator should have knowledge of various patch management tools that perform remote patch management.

**ICON KEY**

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

## Lab Objectives

This lab will demonstrate how to perform remote patch management on Windows using the BatchPatch tool.

## Lab Environment

To carry out the lab, you need:

- A virtual machine running Windows Server 2012
- A virtual machine running Windows 10
- A Web browser with an Internet connection
- BatchPatch, located at **Z:\CND-Tools\CND Module 06 Host Security\Patch Management Tools\BatchPatch**
- **Administrative** privileges to run the tools

## Lab Duration

Time: 25 Minutes

## Overview of BatchPatch

With the BatchPatch management tool, you can initiate the download and/or the installation of Windows updates on MANY remote computers simultaneously from a single console. Computers can be standalone, in a Workgroup or members of a domain.

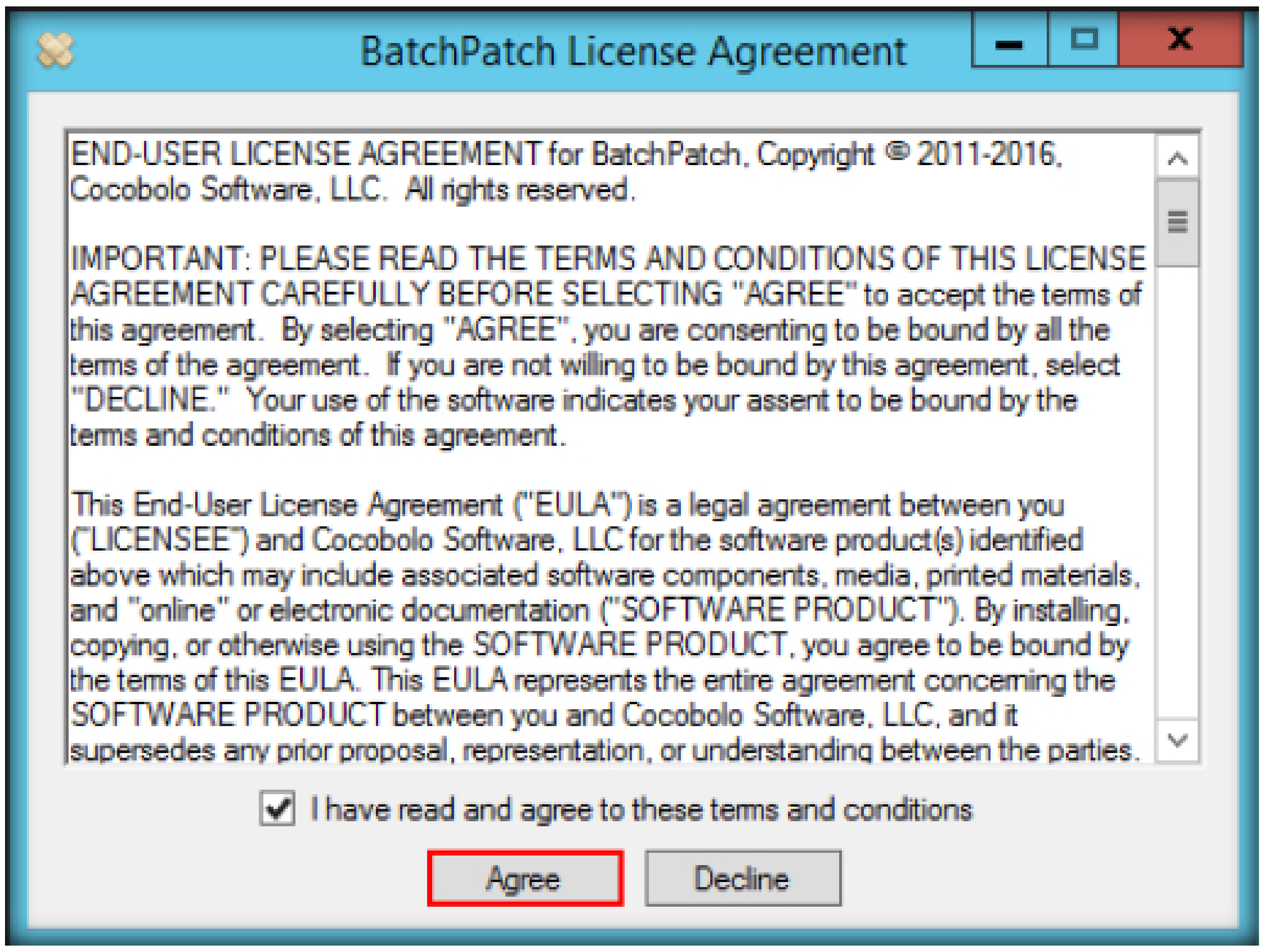
## Lab Tasks

1. Launch the **Windows Server 2012 virtual machine** and login

**TASK 1**

**Install and Launch**

2. Navigate to **Z:\CND-Tools\CND Module 06 Host Security\Patch Management Tools\BatchPatch** and double-click **batchpatch.exe** to start the installation
3. If an **Open File – Security Warning** window appears. Click **Run** to continue.
4. The **BatchPatch License Agreement** window appears. Ensure that the checkbox is ticked and click **Agree**.



END-USER LICENSE AGREEMENT for BatchPatch, Copyright © 2011-2016, Cocobolo Software, LLC. All rights reserved.

IMPORTANT: PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE SELECTING "AGREE" to accept the terms of this agreement. By selecting "AGREE", you are consenting to be bound by all the terms of the agreement. If you are not willing to be bound by this agreement, select "DECLINE." Your use of the software indicates your assent to be bound by the terms and conditions of this agreement.

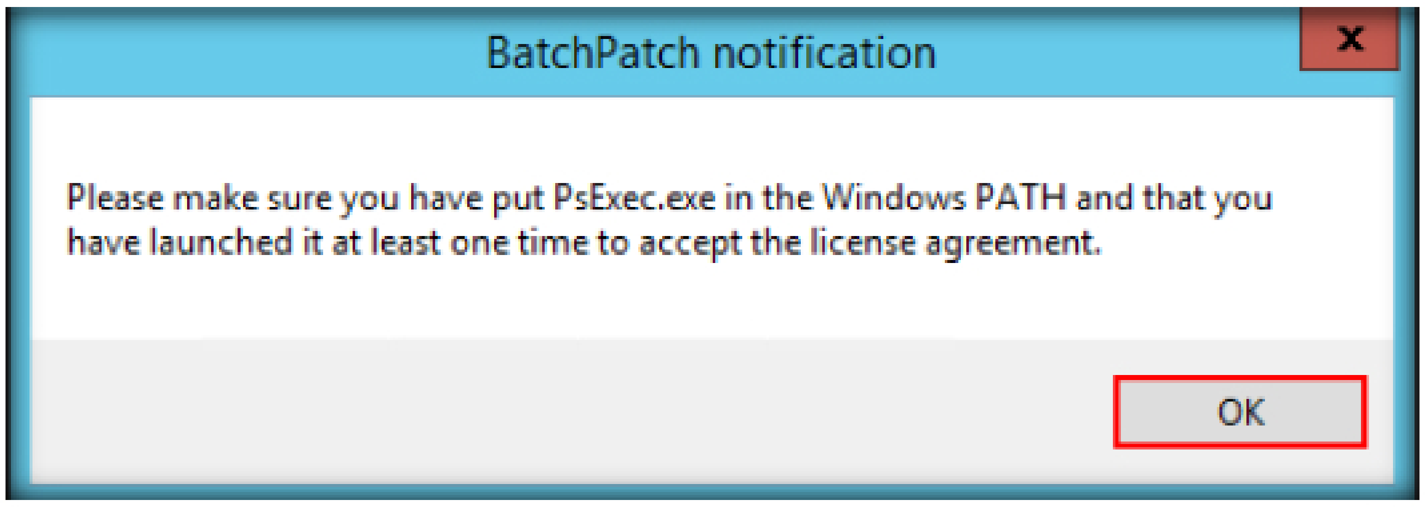
This End-User License Agreement ("EULA") is a legal agreement between you ("LICENSEE") and Cocobolo Software, LLC for the software product(s) identified above which may include associated software components, media, printed materials, and "online" or electronic documentation ("SOFTWARE PRODUCT"). By installing, copying, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. This EULA represents the entire agreement concerning the SOFTWARE PRODUCT between you and Cocobolo Software, LLC, and it supersedes any prior proposal, representation, or understanding between the parties.

☑ I have read and agree to these terms and conditions

FIGURE 4.1: Agreeing the license

Initiate the download and/or installation of Windows updates on MANY remote computers simultaneously from a single console. Computers can be standalone, in a Workgroup, or members of a domain.

5. The **BatchPatch notification** window pops up. Click **OK**.

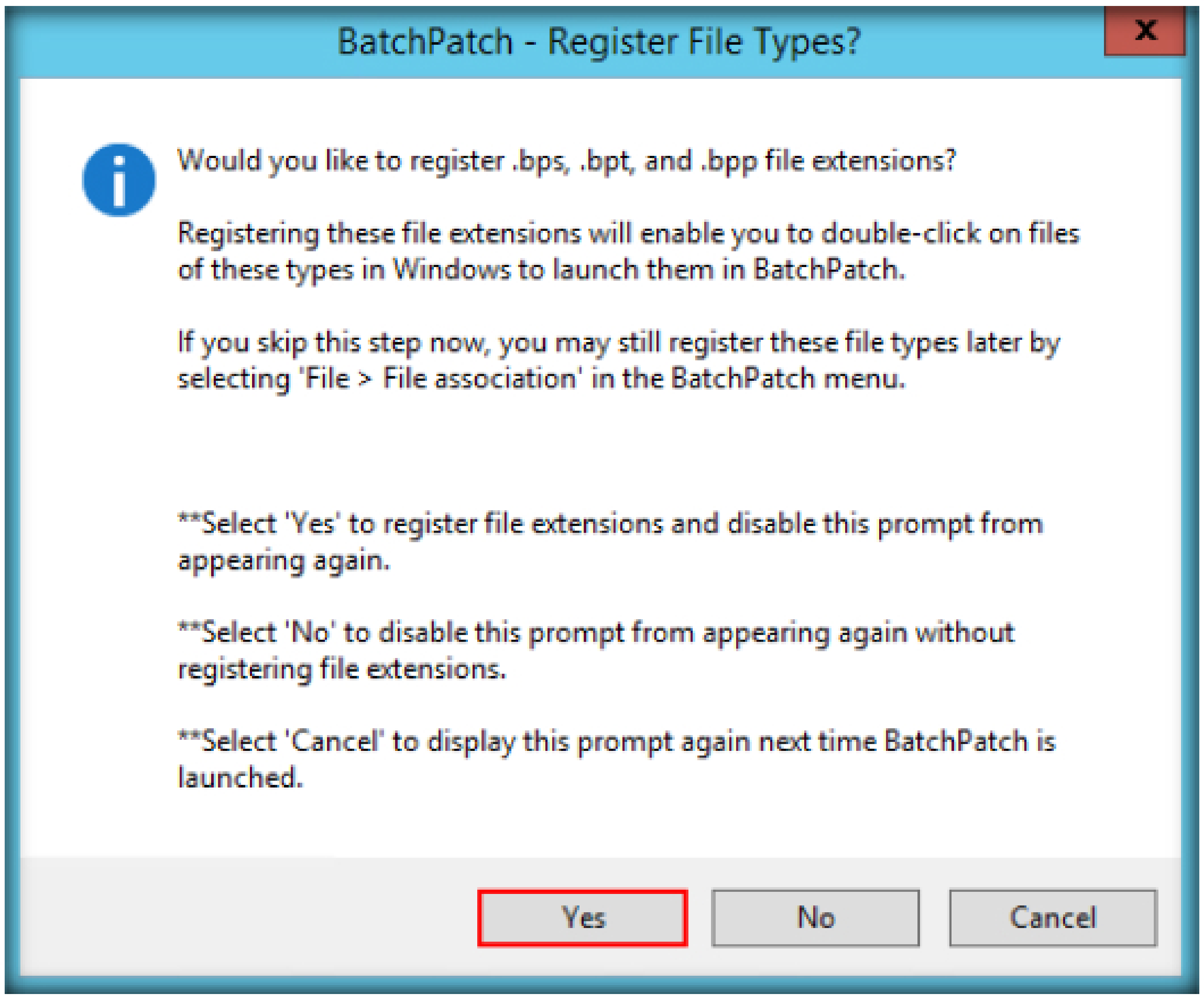


Please make sure you have put PsExec.exe in the Windows PATH and that you have launched it at least one time to accept the license agreement.

FIGURE 4.2: BatchPatch notification

Choose to install all available updates or just install specific updates, by name. Additional filters are also available, allowing you to select updates by their classification groupings: Critical Updates, Security Updates, Definition Updates, Updates, Update Rollups, Service Packs, Feature Packs, Drivers, and Tools. Or mimic Microsoft Windows Update and choose to install only Important and/or recommended updates.

6. The **BatchPatch - Register File Types?** window appears. Click **Yes**.



BatchPatch - Register File Types?

Would you like to register .bps, .bpt, and .bpp file extensions?

Registering these file extensions will enable you to double-click on files of these types in Windows to launch them in BatchPatch.

If you skip this step now, you may still register these file types later by selecting 'File > File association' in the BatchPatch menu.

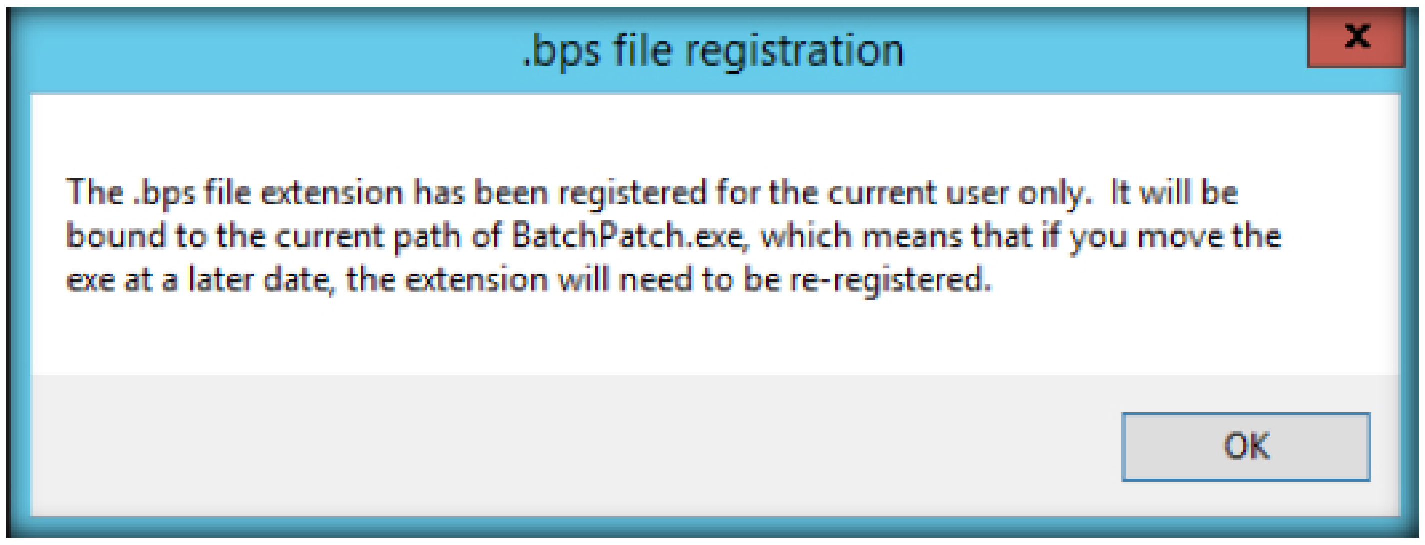
**Select 'Yes' to register file extensions and disable this prompt from appearing again.

**Select 'No' to disable this prompt from appearing again without registering file extensions.

**Select 'Cancel' to display this prompt again next time BatchPatch is launched.

FIGURE 4.3: BatchPatch registration

7. The **.bps file registration** window appears. Click **OK**.



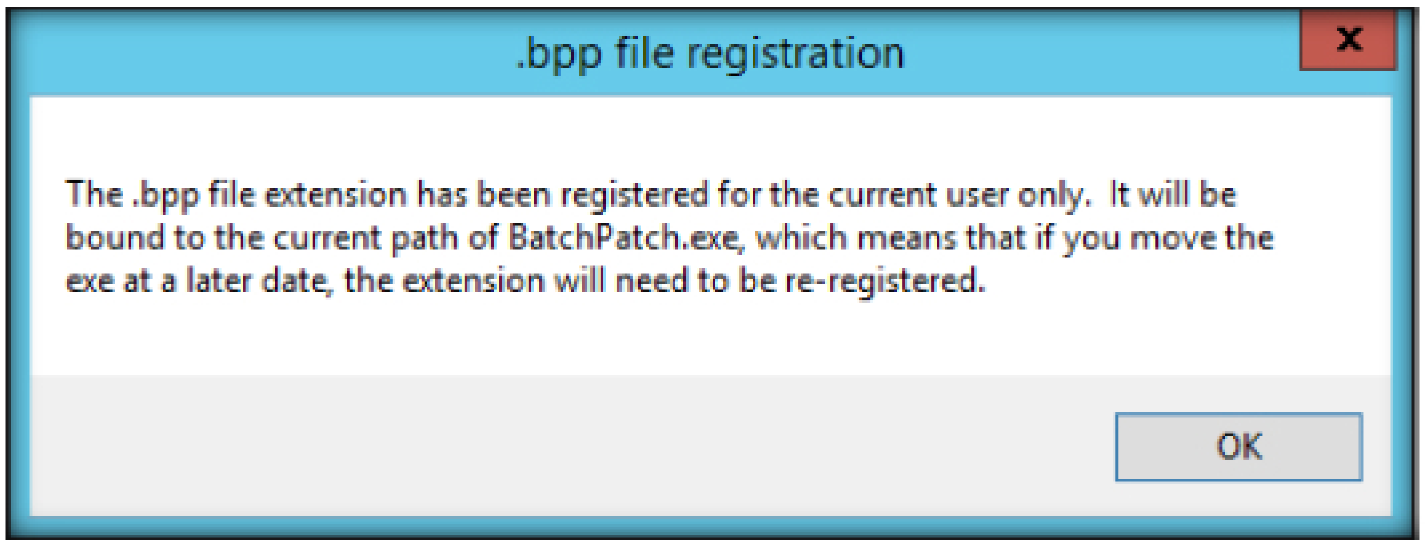
.bps file registration

The .bps file extension has been registered for the current user only. It will be bound to the current path of BatchPatch.exe, which means that if you move the exe at a later date, the extension will need to be re-registered.

FIGURE 4.4: .bps window

Use your own managed WSUS server, or use BatchPatch in conjunction with Windows Update or Microsoft Update as an effective WSUS alternative.

8. The **.bpp file registration** window appears. Click **OK**.



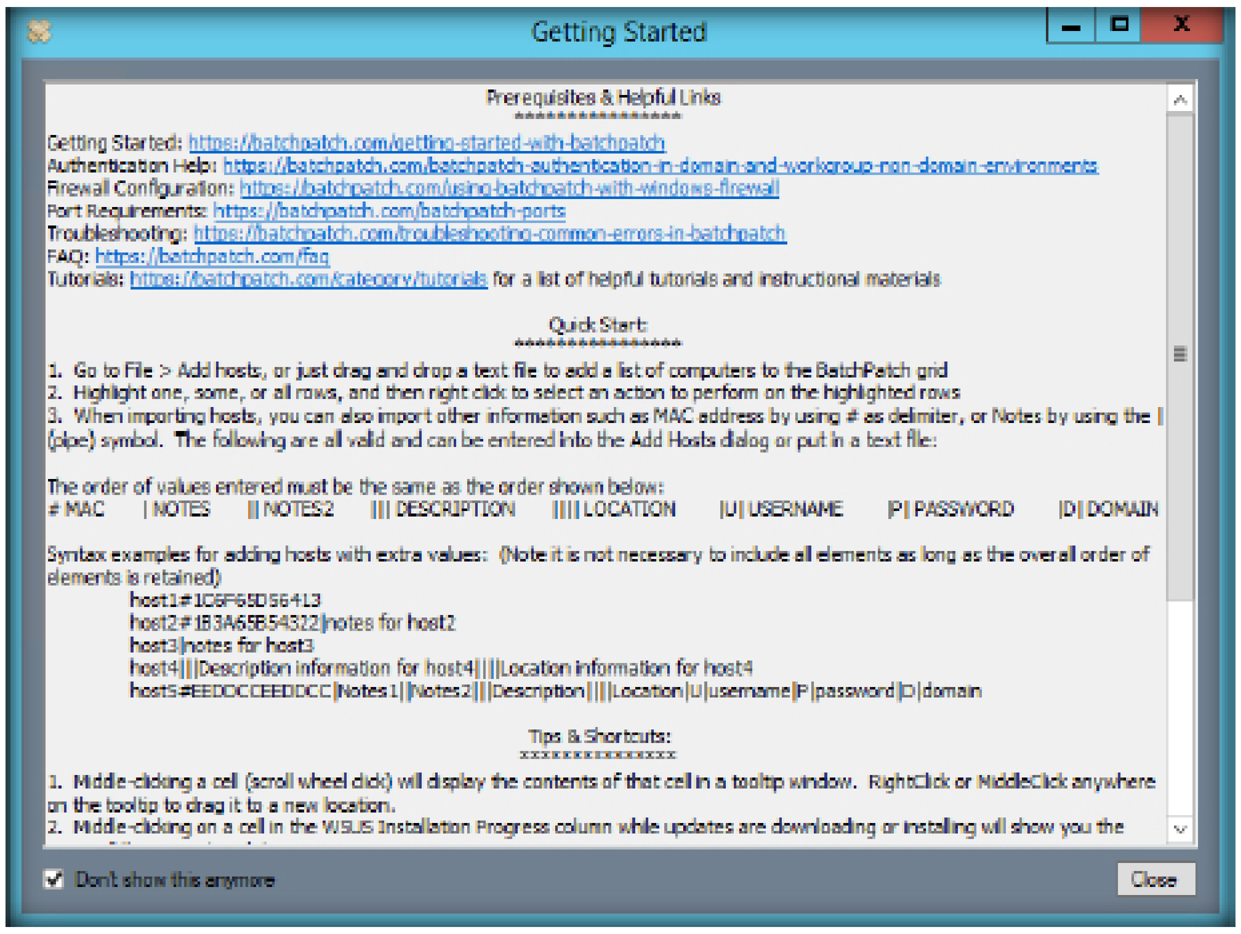
.bpp file registration

The .bpp file extension has been registered for the current user only. It will be bound to the current path of BatchPatch.exe, which means that if you move the exe at a later date, the extension will need to be re-registered.

FIGURE 4.5: .bpp file registration

Turn BatchPatch into a central distribution point for Windows Updates using the optional 'Cached Mode.'

9. The **Getting Started** window appears. Tick **Don't show this anymore** checkbox and click **Close**.



Getting Started

Prerequisites & Helpful Links
******************

Getting Started: https://batchpatch.com/getting-started-with-batchpatch
Authentication Help: https://batchpatch.com/batchpatch-authentication-in-domain-and-workgroup-non-domain-environments
Firewall Configuration: https://batchpatch.com/using-batchpatch-with-windows-firewall
Port Requirements: https://batchpatch.com/batchpatch-ports
Troubleshooting: https://batchpatch.com/troubleshooting-common-errors-in-batchpatch
FAQ: https://batchpatch.com/faq
Tutorials: https://batchpatch.com/category/tutorials for a list of helpful tutorials and instructional materials

Quick Start:
******************

1. Go to File > Add hosts, or just drag and drop a text file to add a list of computers to the BatchPatch grid
2. Highlight one, some, or all rows, and then right click to select an action to perform on the highlighted rows
3. When importing hosts, you can also import other information such as MAC address by using # as delimiter, or Notes by using the | (pipe) symbol. The following are all valid and can be entered into the Add Hosts dialog or put in a text file:

The order of values entered must be the same as the order shown below:

```
# MAC      | NOTES     || NOTES2     ||| DESCRIPTION     |||| LOCATION     |U| USERNAME     |P| PASSWORD     |D| DOMAIN
```

Syntax examples for adding hosts with extra values: (Note it is not necessary to include all elements as long as the overall order of elements is retained)

```
        host1#1C6F65D56413
        host2#1B3A65B54322|notes for host2
        host3|notes for host3
        host4|||Description information for host4||||Location information for host4
        host5#EEDDCCEEDDCC|Notes1||Notes2|||Description||||Location|U|username|P|password|D|domain
```

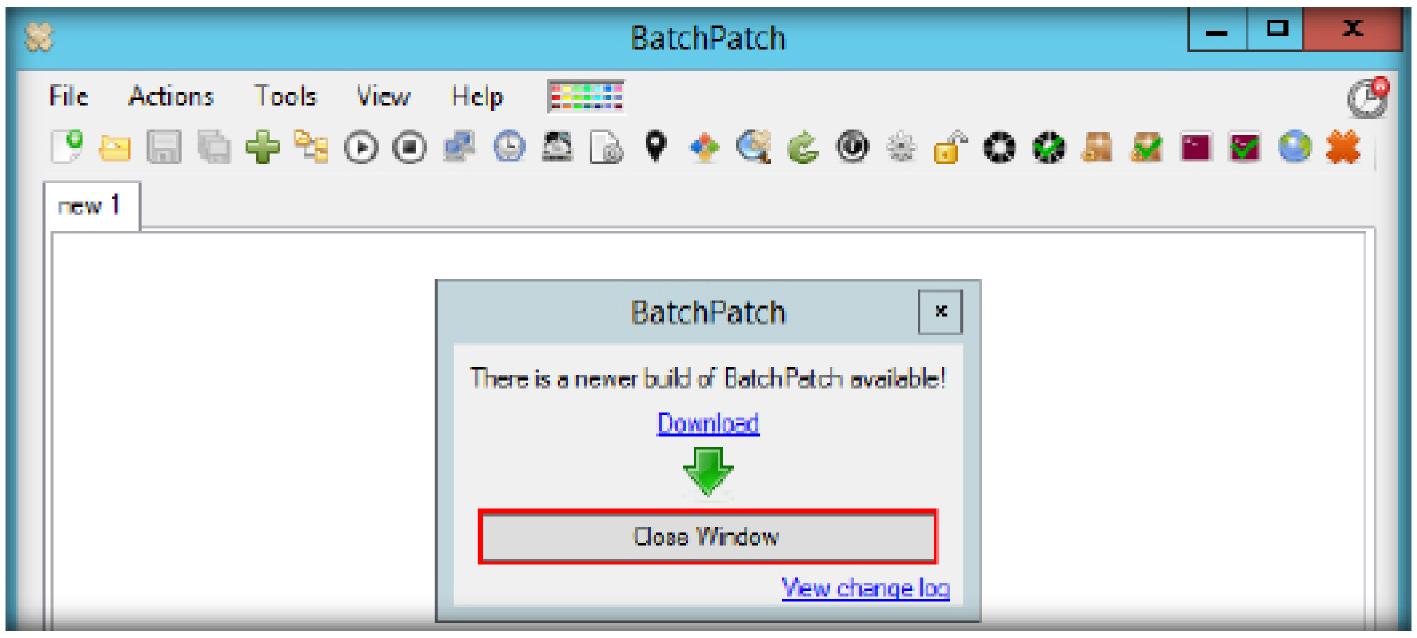
Tips & Shortcuts:
xxxxxxxxxxxxxxxx

1. Middle-clicking a cell (scroll wheel click) will display the contents of that cell in a tooltip window. RightClick or MiddleClick anywhere on the tooltip to drag it to a new location.
2. Middle-clicking on a cell in the WSUS Installation Progress column while updates are downloading or installing will show you the

☑ Don't show this anymore

FIGURE 4.6: Introduction window

10. The **BatchPatch** main window appears along with the BatchPatch pop-up as shown in the screenshot, click the **Close Window**.



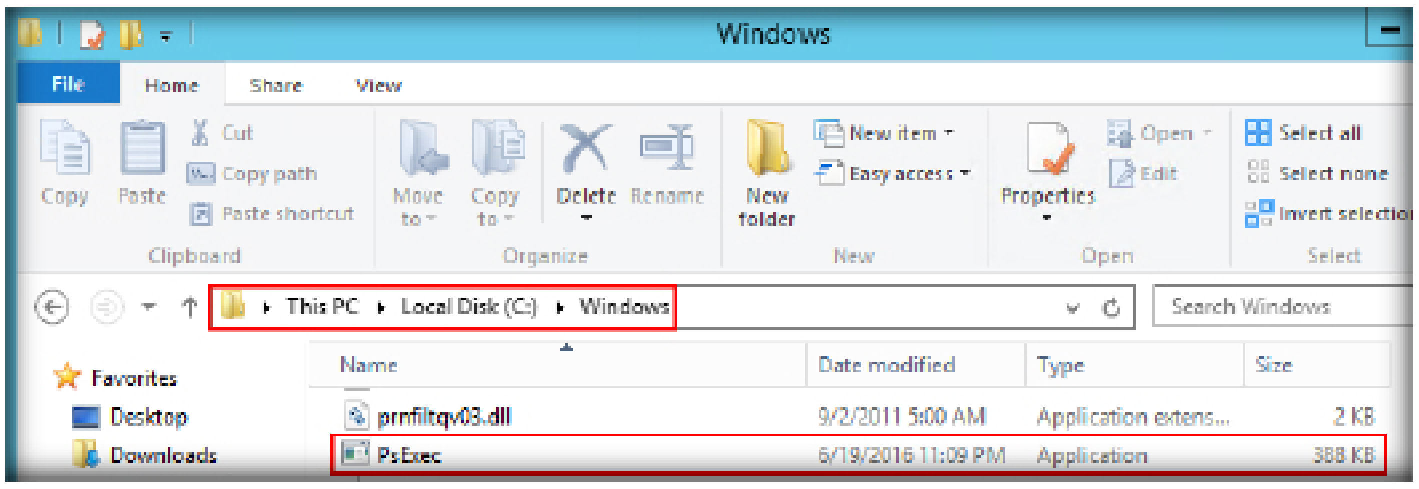
BatchPatch

There is a newer build of BatchPatch available!

FIGURE 4.7: BatchPatch window

**Copy PsExec Tool**

11. Navigate to **Z:\CND-Tools\CND Module 06 Host Security\Patch Management Tools\PSTools** and copy **PsExec.exe** file and paste in **C:\Windows.**



| Name | Date modified | Type | Size |
|---|---|---|---|
| prnfiltqv03.dll | 9/2/2011 5:00 AM | Application extens... | 2 KB |
| PsExec | 6/19/2016 11:09 PM | Application | 388 KB |

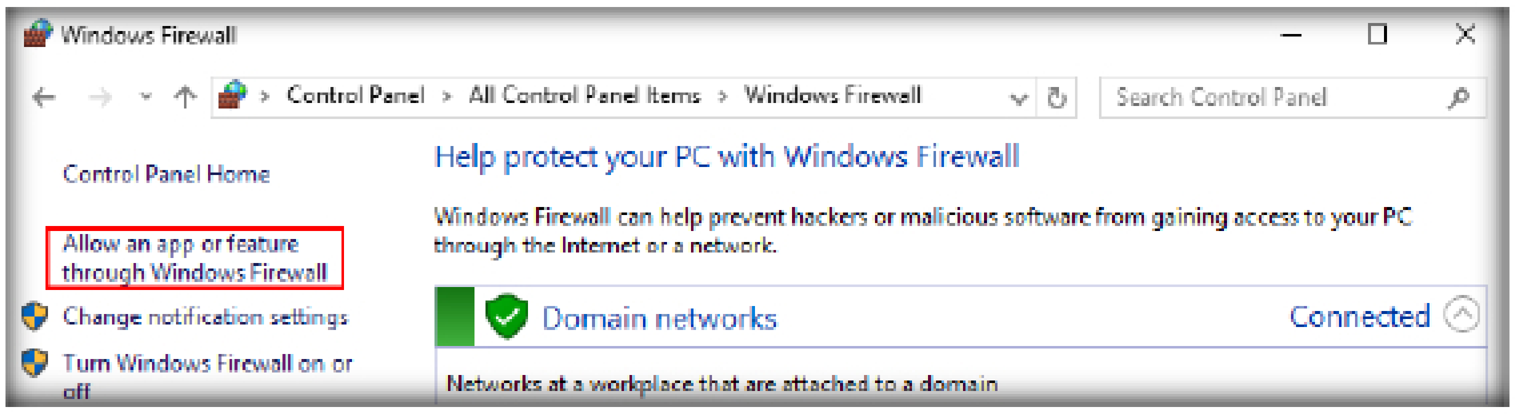
FIGURE 4.8: PsExec file moved

12. Now, Launch the **Windows 10** virtual machine and login as the Local Administrator.

Apply Windows Updates to computers that do NOT have internet access (offline Windows Update) using 'Offline Mode.'

13. Go to the **Control Panel** and click the **Windows Firewall** in All Control Panel items.

14. In the **Windows Firewall** settings, click the **Allow an app or feature through Windows Firewall** from the left pane of the window as shown in the screenshot.



Windows Firewall

Control Panel > All Control Panel Items > Windows Firewall

Search Control Panel

Control Panel Home

Allow an app or feature through Windows Firewall

Change notification settings

Turn Windows Firewall on or off

Help protect your PC with Windows Firewall

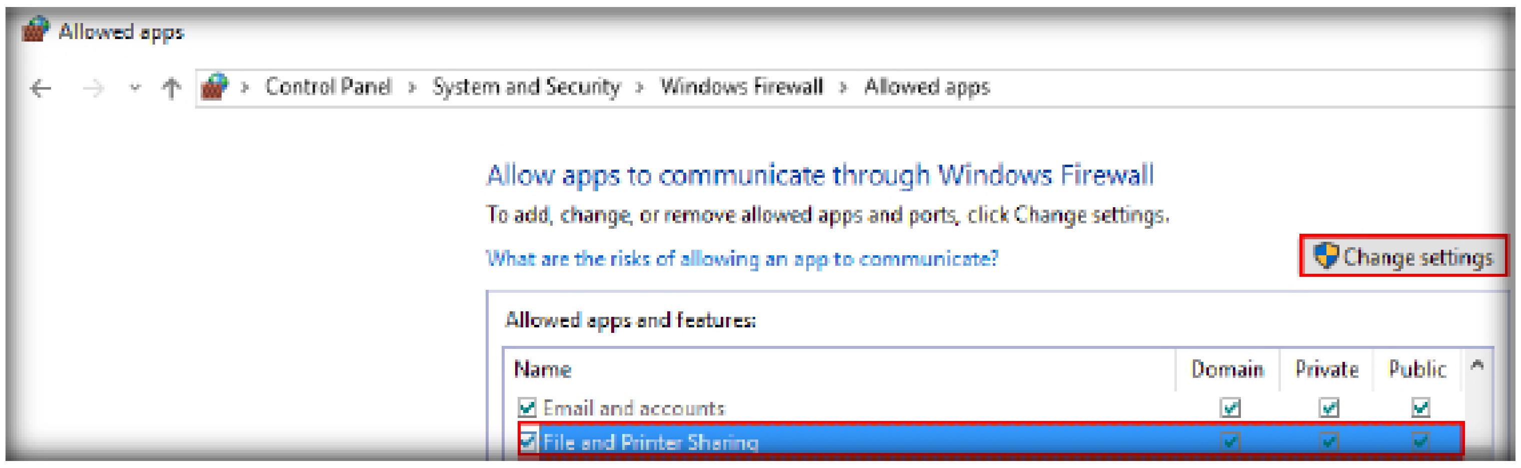
Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Domain networks — Connected

Networks at a workplace that are attached to a domain

FIGURE 4.9: Changing Firewall settings

15. The **Allowed apps** window appears. Click **Change settings.** Check the boxes for **Domain**, **Private** and **Public** for **File and Printer sharing**.



Allowed apps

Control Panel > System and Security > Windows Firewall > Allowed apps

Allow apps to communicate through Windows Firewall

To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

Change settings

Allowed apps and features:

| Name | Domain | Private | Public |
|---|---|---|---|
| ☑ Email and accounts | ☑ | ☑ | ☑ |
| ☑ File and Printer Sharing | ☑ | ☑ | ☑ |

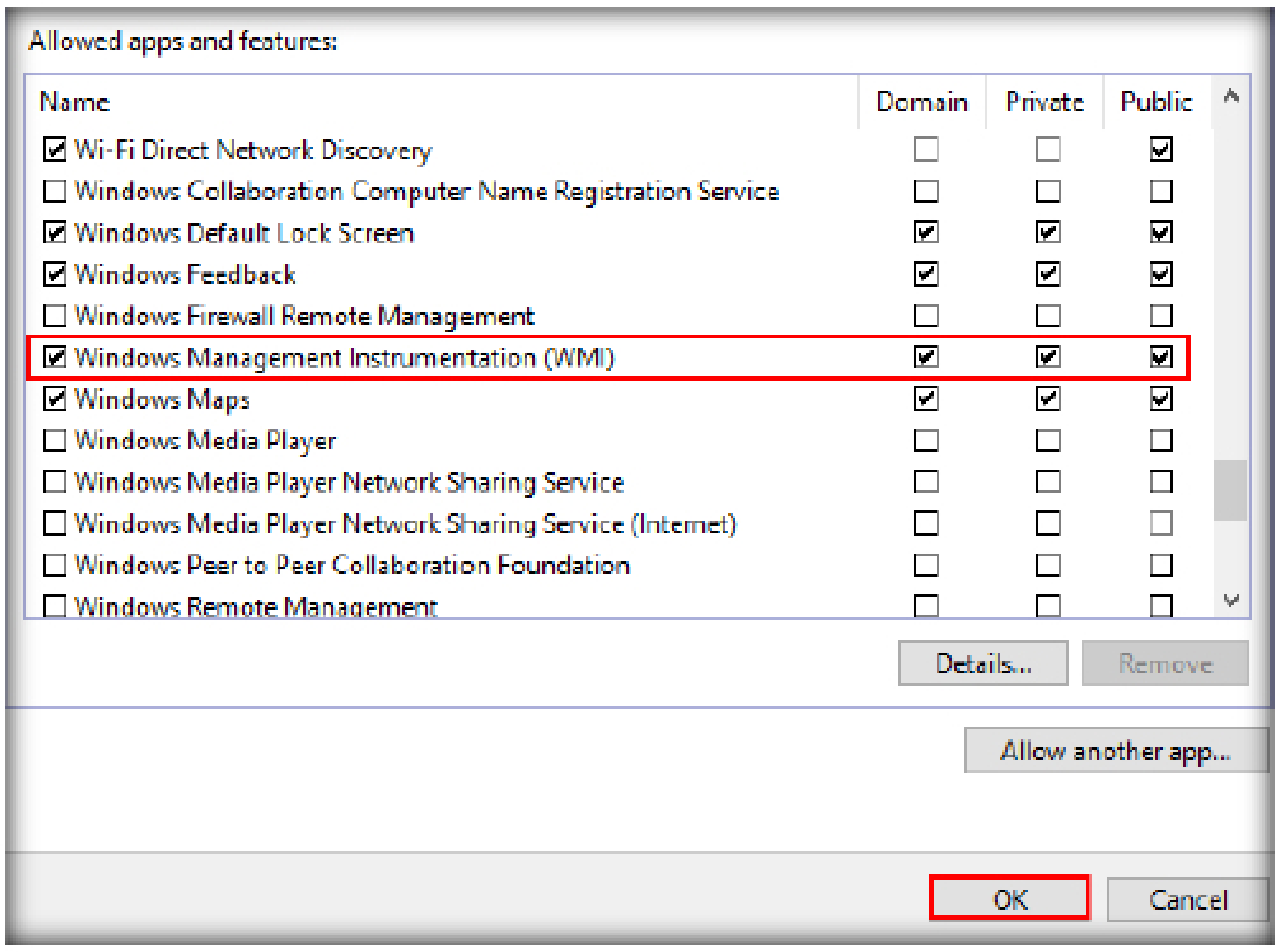
FIGURE 4.10: Enabling File and Printer sharing

Retrieve Windows Update history information from all of your computers into a consolidated report.

16. Scroll down and check the boxes for **Domain, Private** and **Public** for **Windows Management Instrumentation (WMI)** and click **OK**.

17. Close all the windows that were open in the Windows 10 Machine and log off the machine.

Deploy software remotely to an entire network of computers with just a few of clicks.



Allowed apps and features:

| Name | Domain | Private | Public |
|---|---|---|---|
| ☑ Wi-Fi Direct Network Discovery | ☐ | ☐ | ☑ |
| ☐ Windows Collaboration Computer Name Registration Service | ☐ | ☐ | ☐ |
| ☑ Windows Default Lock Screen | ☑ | ☑ | ☑ |
| ☑ Windows Feedback | ☑ | ☑ | ☑ |
| ☐ Windows Firewall Remote Management | ☐ | ☐ | ☐ |
| ☑ Windows Management Instrumentation (WMI) | ☑ | ☑ | ☑ |
| ☑ Windows Maps | ☑ | ☑ | ☑ |
| ☐ Windows Media Player | ☐ | ☐ | ☐ |
| ☐ Windows Media Player Network Sharing Service | ☐ | ☐ | ☐ |
| ☐ Windows Media Player Network Sharing Service (Internet) | ☐ | ☐ | ☐ |
| ☐ Windows Peer to Peer Collaboration Foundation | ☐ | ☐ | ☐ |
| ☐ Windows Remote Management | ☐ | ☐ | ☐ |

FIGURE 4.11: Finalizing the Firewall settings

18. Switch back to the **Windows Server 2012** machine and go to the **BatchPatch** main window

19. Click **Files** and select **Add hosts...**.

Deploy standalone Microsoft or third-party patches such as Adobe or Java updates, as well as registry keys, scripts, and just about anything else to remote hosts. Push install MSIs remotely to multiple computers (.msi .msp .msu .exe .reg .vbs .cmd and more). Take a look at the software deployment page for more information, tutorials, and videos.

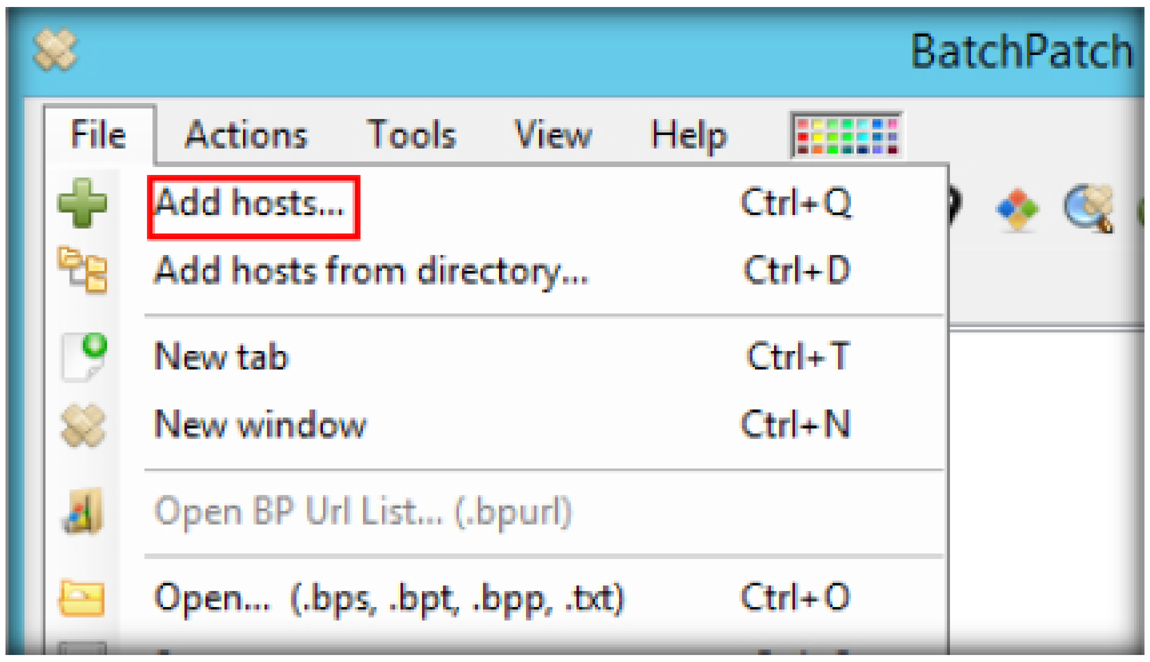
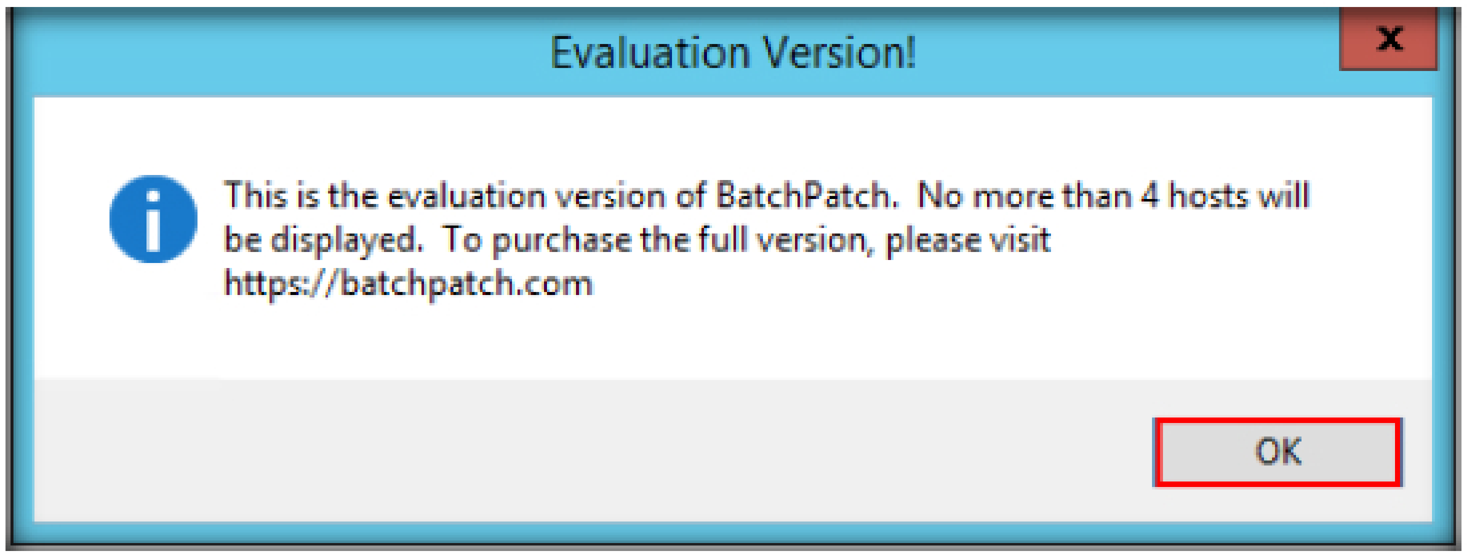

BatchPatch
File
Actions
Tools
View
Help
Add hosts... Ctrl+Q
Add hosts from directory... Ctrl+D
New tab Ctrl+T
New window Ctrl+N
Open BP Url List... (.bpurl)
Open... (.bps, .bpt, .bpp, .txt) Ctrl+O

FIGURE 4.12: Adding Host

20. The **Evaluation version** window appears. Click **OK**.



This is the evaluation version of BatchPatch. No more than 4 hosts will be displayed. To purchase the full version, please visit https://batchpatch.com

FIGURE 4.13: Host limitation message

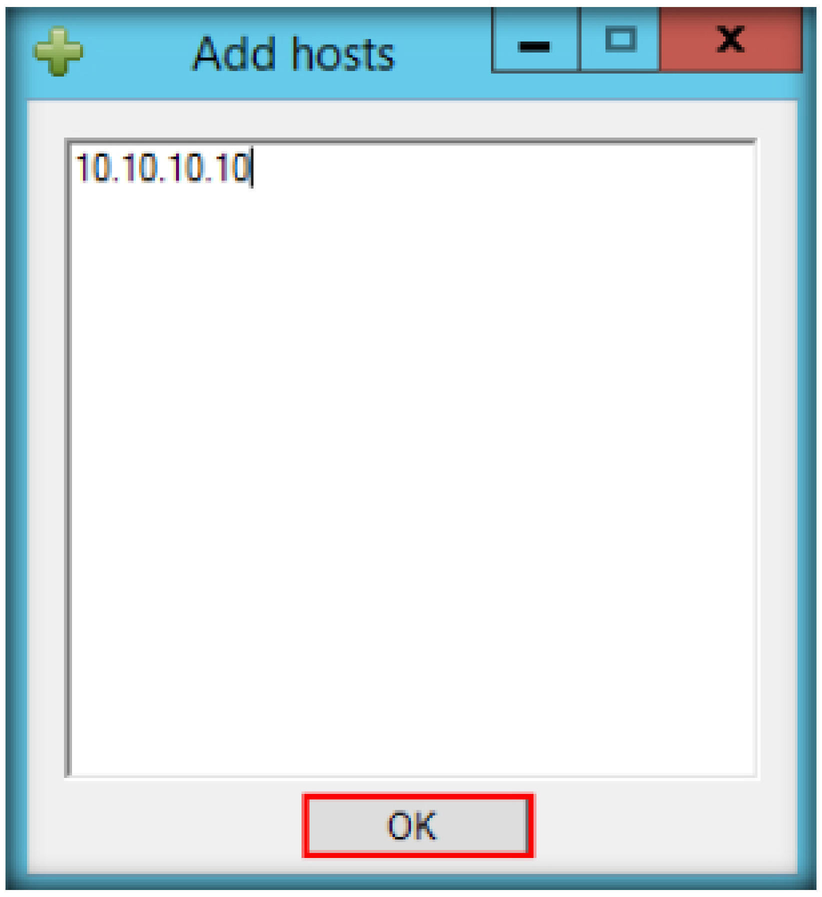
**TASK 3**

**Add Host**

21. The **Add Hosts** window appears. Enter the IP address of the Windows 10 machine (10.10.10.10) and click **OK**.

**Note**: The IP addresses may vary in your lab environment.

Reboot or shutdown remote hosts and monitor status in real-time with integrated pinging.



10.10.10.10

FIGURE 4.14: Adding a host

22. The Windows 10 machine will be added in the BatchPatch main window. Right click the added host and select **Specify alternate logon credentials**.

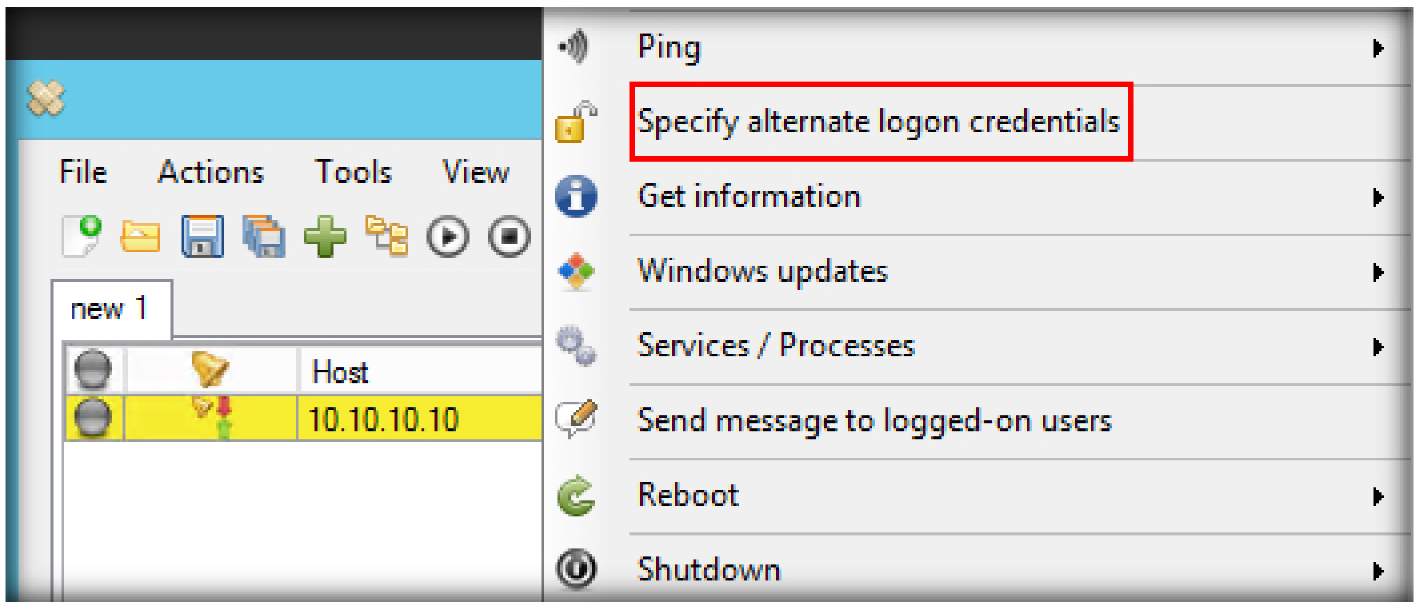
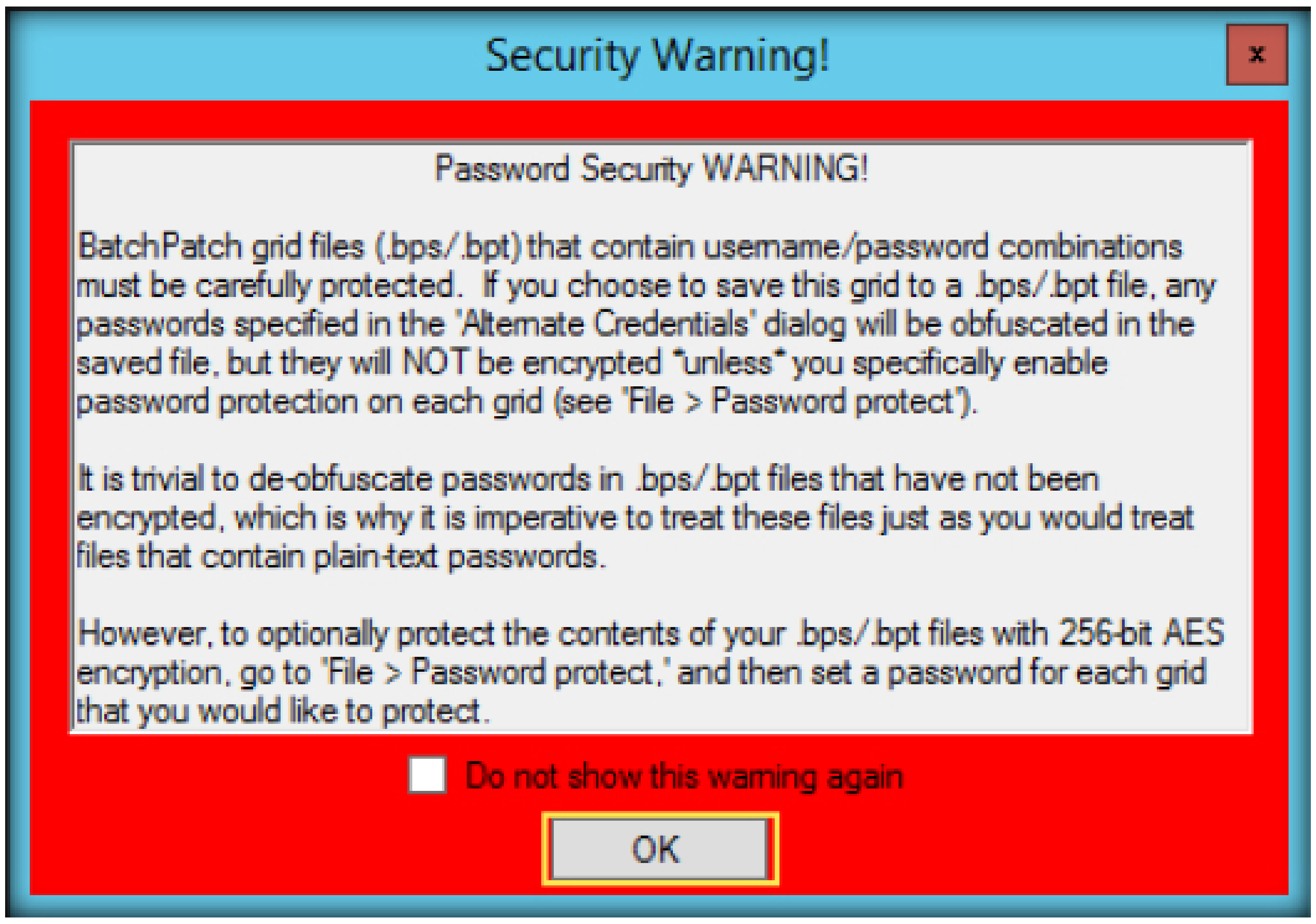


FIGURE 4.15: Changing logon credentials

BatchPatch offers a very convenient method for remote script execution, enabling you to easily and quickly retrieve information from your target computers, push configuration changes, apply custom settings, and do just about anything else you can think of.

23. The **Security Warning** window appears. Click **OK**.



Password Security WARNING!

BatchPatch grid files (.bps/.bpt) that contain username/password combinations must be carefully protected. If you choose to save this grid to a .bps/.bpt file, any passwords specified in the 'Alternate Credentials' dialog will be obfuscated in the saved file, but they will NOT be encrypted *unless* you specifically enable password protection on each grid (see 'File > Password protect').

It is trivial to de-obfuscate passwords in .bps/.bpt files that have not been encrypted, which is why it is imperative to treat these files just as you would treat files that contain plain-text passwords.

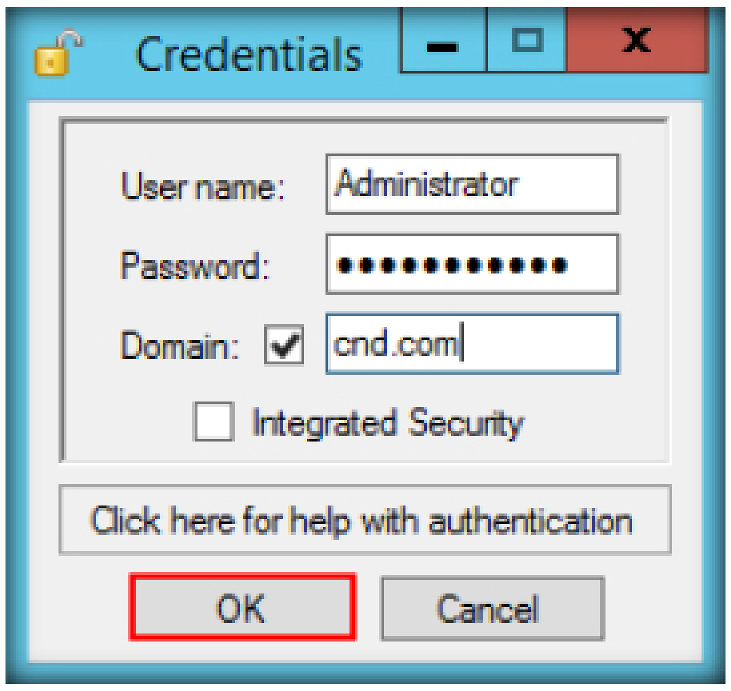
However, to optionally protect the contents of your .bps/.bpt files with 256-bit AES encryption, go to 'File > Password protect,' and then set a password for each grid that you would like to protect.

□ Do not show this warning again

FIGURE 4.16: Warning message

Integrated job queues: You can create a set of actions to execute sequentially on remote hosts, which allows you to run scripts before and/or after a reboot, or string together multiple patch and reboot cycles etc.

24. The **Credentials** window appears. Enter the **Windows Server 2008** machine credentials and domain name then click **OK**.



User name: Administrator

Password: ●●●●●●●●●●●

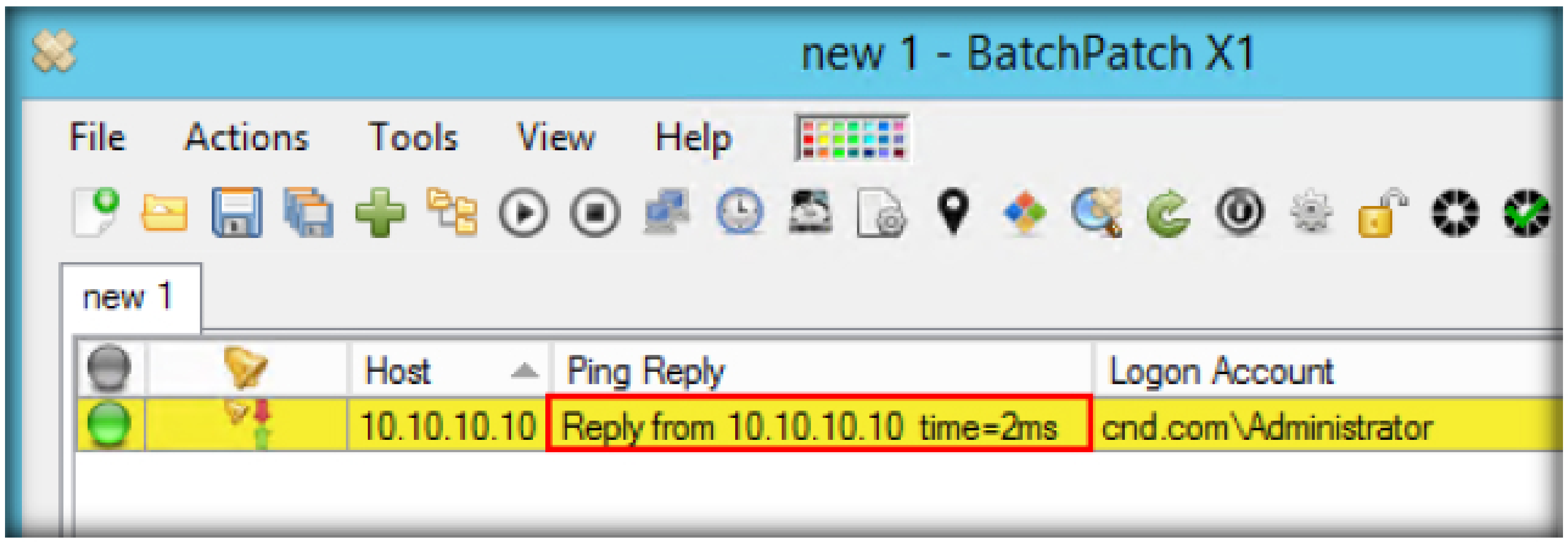
Domain: ☑ cnd.com

□ Integrated Security

FIGURE 4.17: Entering Domain system credentials

Advanced multi-host custom sequencing options to handle complex update and reboot tasks involving numerous computers with online/offline dependencies, all of which can be configured for single-click execution.

25. Click **10.10.10.10** and type the letter **P** from the keyboard to start pinging the **Windows 10** machine then press **ctrl+P** to stop the ping.



| Host | Ping Reply | Logon Account |
|---|---|---|
| 10.10.10.10 | Reply from 10.10.10.10 time=2ms | cnd.com\Administrator |

FIGURE 4.18: Ping successful

Retrieve the last boot time from remote hosts (very handy when rebooting computers).

26. Right click on **10.10.10.10** and select **Windows updates → Check for available updates** from the context menu as shown in the screenshot.

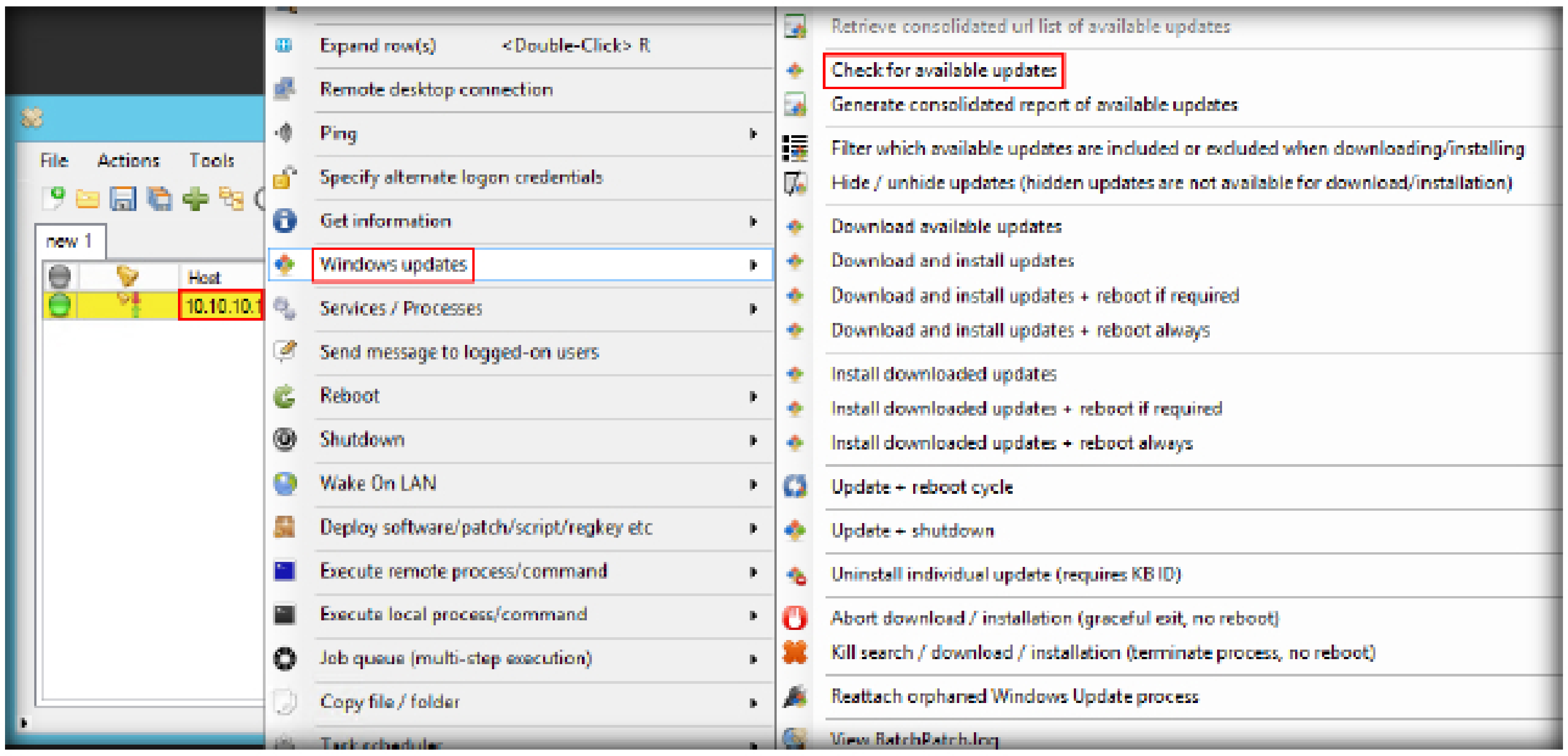
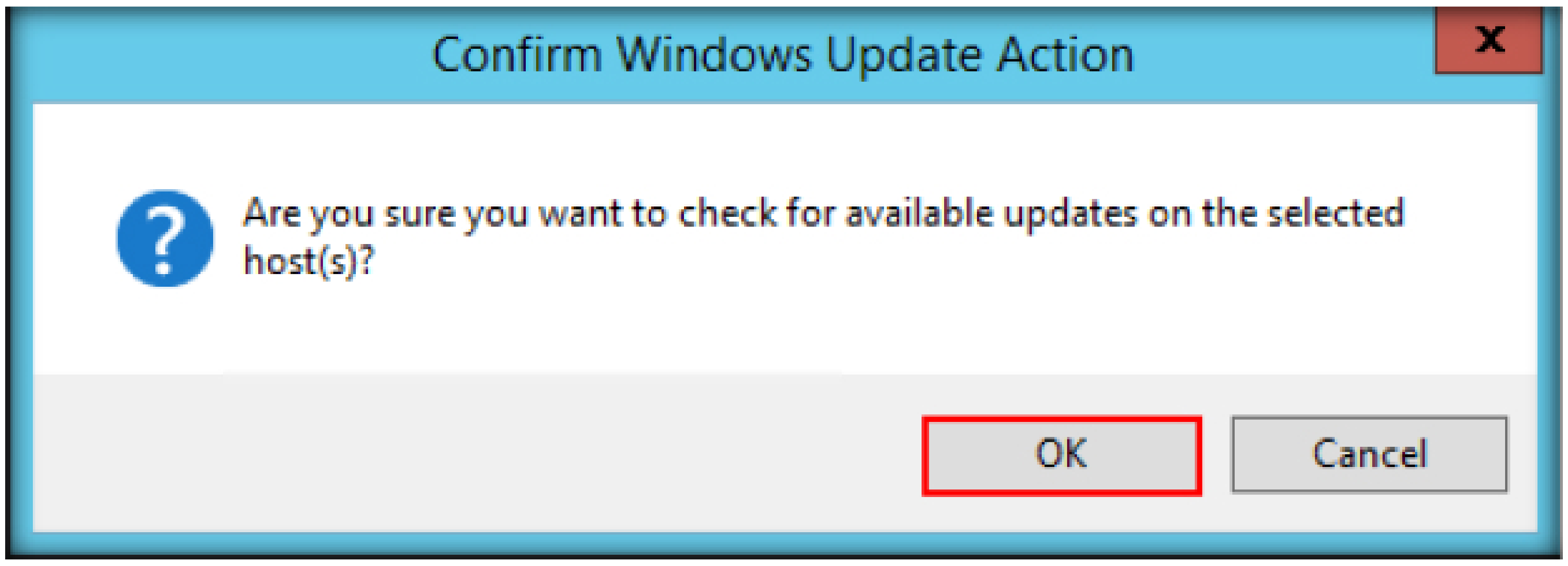

File
Actions
Tools
new 1
Host
10.10.10.1
Expand row(s) <Double-Click> R
Remote desktop connection
Ping
Specify alternate logon credentials
Get information
Windows updates
Services / Processes
Send message to logged-on users
Reboot
Shutdown
Wake On LAN
Deploy software/patch/script/regkey etc
Execute remote process/command
Execute local process/command
Job queue (multi-step execution)
Copy file / folder
Task scheduler
Retrieve consolidated url list of available updates
Check for available updates
Generate consolidated report of available updates
Filter which available updates are included or excluded when downloading/installing
Hide / unhide updates (hidden updates are not available for download/installation)
Download available updates
Download and install updates
Download and install updates + reboot if required
Download and install updates + reboot always
Install downloaded updates
Install downloaded updates + reboot if required
Install downloaded updates + reboot always
Update + reboot cycle
Update + shutdown
Uninstall individual update (requires KB ID)
Abort download / installation (graceful exit, no reboot)
Kill search / download / installation (terminate process, no reboot)
Reattach orphaned Windows Update process
View BatchPatch.log

FIGURE 4.19: Checking for patch updates

27. The **Confirm Windows Update Action** window appears. Click **OK**.

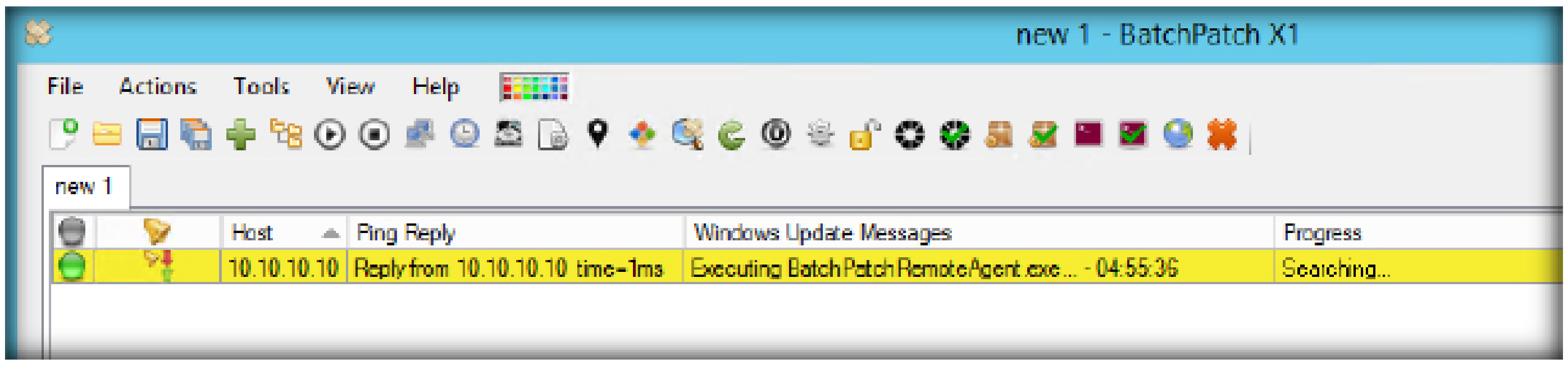


Are you sure you want to check for available updates on the selected host(s)?

FIGURE 4.20: Confirming the update check

28. If an **Open File – Security Warning** window pops up. Click **Run**.

29. BatchPatch will take some time depending on the updates available; wait for the process to be completed.

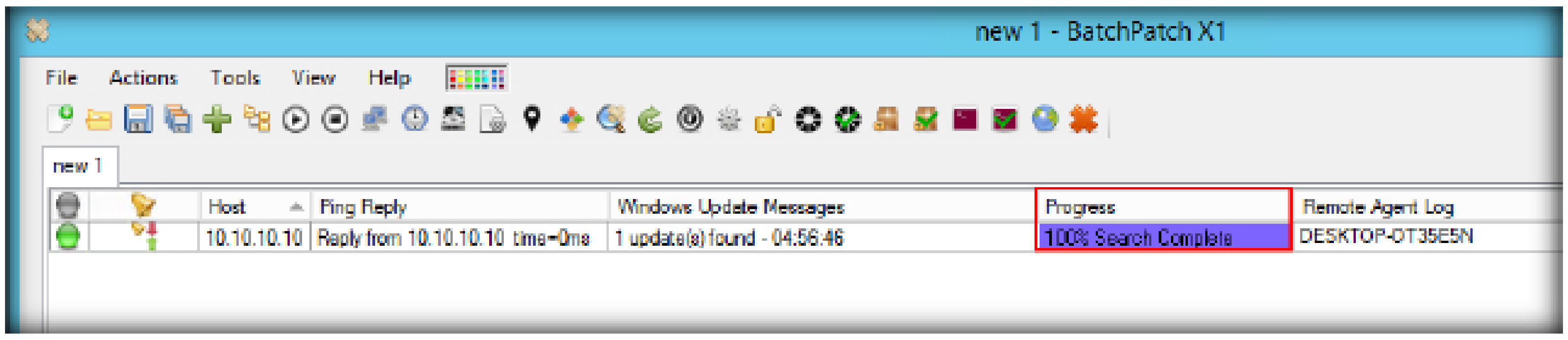


| Host | Ping Reply | Windows Update Messages | Progress |
|---|---|---|---|
| 10.10.10.10 | Reply from 10.10.10.10 time=1ms | Executing BatchPatchRemoteAgent.exe... - 04:55:36 | Searching... |

FIGURE 4.21: Windows update search in progress

BatchPatch was designed to be simple and intuitive. Special attention was paid to keeping the app as slim as possible. No installation necessary– just launch the EXE and you're ready to go! You start by loading a list of computer names, IP addresses or MAC addresses (MACs are required for Wake on LAN). Then highlight one, some, or all rows in the grid to perform actions on just the selected hosts. Either right click on the currently selected rows or use the Actions menu to select an action to perform. It doesn't get much easier than that!

30. Once all the updates are found, the **Progress** field changes to **100% Search Complete**.



| Host | Ping Reply | Windows Update Messages | Progress | Remote Agent Log |
|---|---|---|---|---|
| 10.10.10.10 | Reply from 10.10.10.10 time=0ms | 1 update(s) found - 04:56:46 | 100% Search Complete | DESKTOP-OT35E5N |

FIGURE 4.22: Found Windows updates

31. Right click on **10.10.10.10** and select **Windows updates** -> **Download and install updates + reboot if required**.

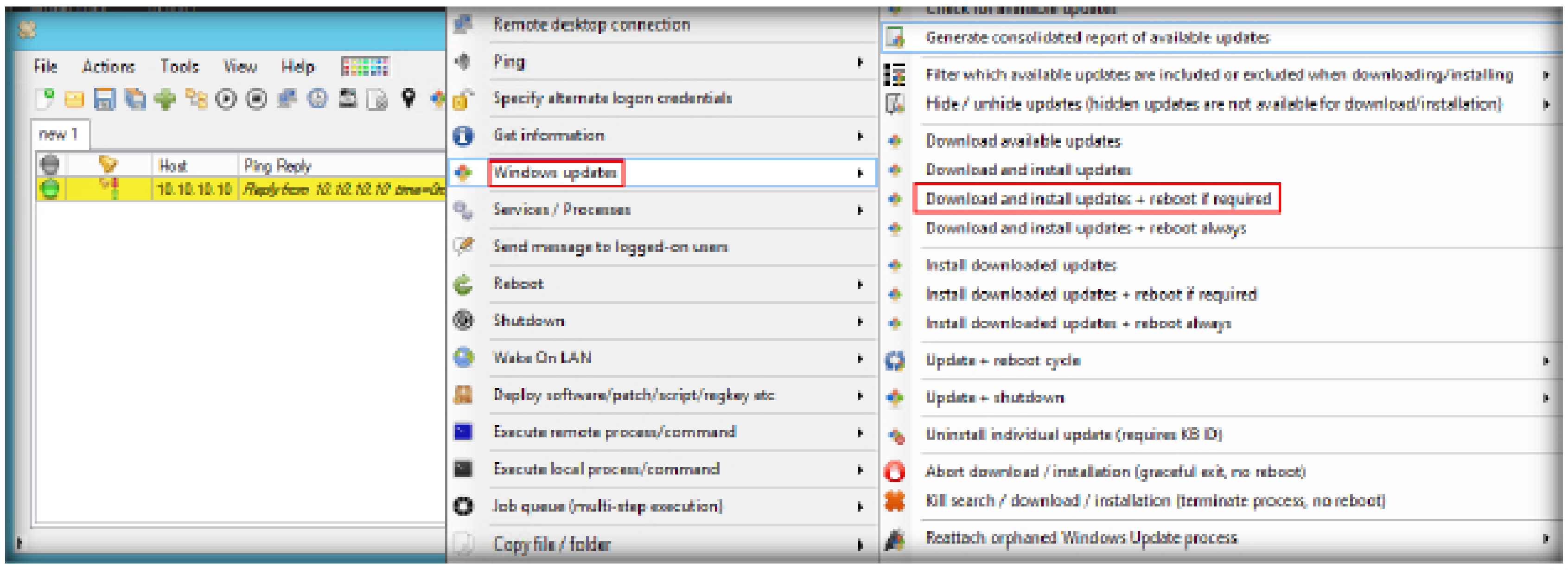
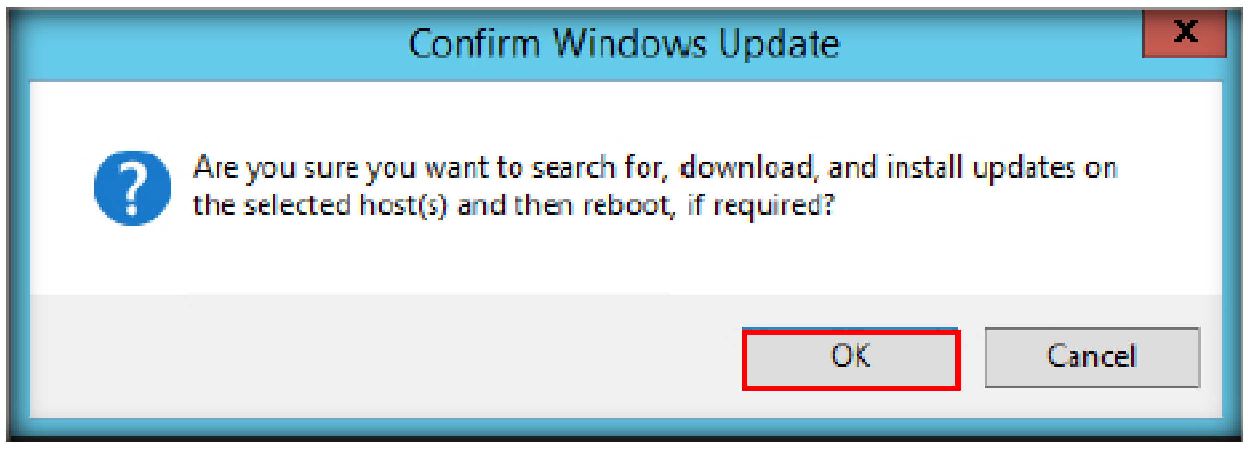

File Actions Tools View Help
new 1
Host
Ping Reply
10.10.10.10
Reply from 10.10.10.10 time=0
Remote desktop connection
Ping
Specify alternate logon credentials
Get information
Windows updates
Services / Processes
Send message to logged-on users
Reboot
Shutdown
Wake On LAN
Deploy software/patch/script/regkey etc
Execute remote process/command
Execute local process/command
Job queue (multi-step execution)
Copy file / folder
Check for available updates
Generate consolidated report of available updates
Filter which available updates are included or excluded when downloading/installing
Hide / unhide updates (hidden updates are not available for download/installation)
Download available updates
Download and install updates
Download and install updates + reboot if required
Download and install updates + reboot always
Install downloaded updates
Install downloaded updates + reboot if required
Install downloaded updates + reboot always
Update + reboot cycle
Update + shutdown
Uninstall individual update (requires KB ID)
Abort download / installation (graceful exit, no reboot)
Kill search / download / installation (terminate process, no reboot)
Reattach orphaned Windows Update process

FIGURE 4.23: Downloading and installing updates

32. The **Confirm Windows Update** window appears. Click OK.



Are you sure you want to search for, download, and install updates on the selected host(s) and then reboot, if required?

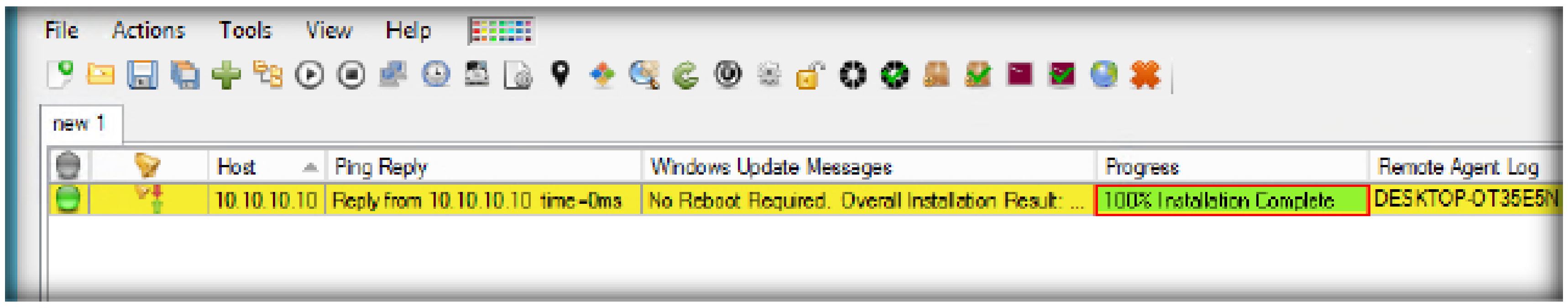
FIGURE 4.24: Confirming Download and install of updates

Retrieve the list of services that are set to "Automatic" but not currently running on the remote hosts (diagnose boot up issues).

33. If an **Open File – Security Warning** window appears. Click **Run**.

34. Once the download and installation is complete, view the Progress field value. It will show **100% Installation Complete**.

**Note**: If the installed updates require a reboot, the target machine will be rebooted automatically once the installation is completed. In this lab the updates that were installed didn't required a reboot as shown in the screenshot.



| | | Host | Ping Reply | Windows Update Messages | Progress | Remote Agent Log |
|---|---|---|---|---|---|---|
| ● | | 10.10.10.10 | Reply from 10.10.10.10 time=0ms | No Reboot Required. Overall Installation Result: ... | 100% Installation Complete | DESKTOP-OT35E5N |

FIGURE 4.25: Successfully downloaded and installed updates

## Lab Analysis

Analyze and document the results of the lab exercise. Give your opinion on your target's security posture and exposure through free public information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

| Internet Connection Required | |
|---|---|
| □ Yes | ☑ No |
| **Platform Supported** | |
| ☑ Classroom | ☑ iLabs |

Lab

5

# Configuring a Syslog Server for Log Review and Audit

*Syslog is a data logging service which enables network devices such as routers, switches, firewalls, printers, web-servers, etc. to send, store events and information on a logging server.*

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

## Lab Scenario

Conducting a log review and audit for all the network devices in a network is an important task. Administrators must detect and analyze any unauthorized activity on the network. They have to conduct log reviews and audits periodically as a part of their normal network security activity. The Administrator should know how to configure a syslog server so that they can conduct a log review for all their network devices using a single console.

## Lab Objectives

This lab will demonstrate how to configure a syslog server and conduct a log review for remote network devices.

## Lab Environment

To carry out the lab, you need:

- A virtual machine running Windows Server 2012
- A Web browser with an Internet connection
- Kiwi Syslog Server, located at **Z:\CND-Tools\CND Module 06 Host Security\Log Monitoring Tools\Kiwi Syslog Server**
- **Administrative** privileges to run the tools

## Lab Duration

Time: 25 Minutes

# Overview of Kiwi Syslog Server

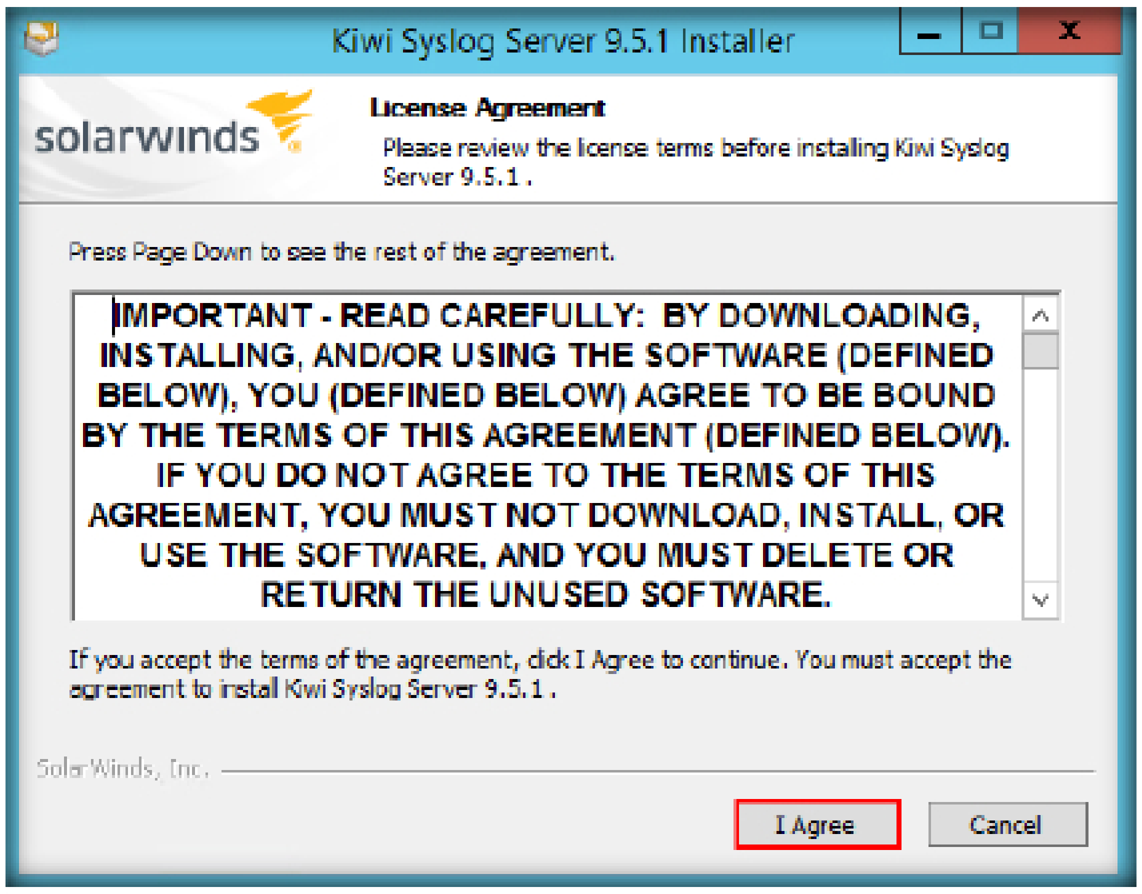
With Kiwi Syslog Server you can collect, view, and archive up to 5 sources; including routers, computers or other devices.

# Lab Tasks

**TASK 1**

**Installing Kiwi Syslog Server Console**

1. Launch the **Windows Server 2012** virtual machine and login as the Administrator.
2. Navigate to **Z:\CND-Tools\CND Module 06 Host Security\Log Monitoring Tools\Kiwi Syslog Server** and double-click the **Kiwi_Syslog_Server_9.5.1.Eval.setup.exe** to start the installation.
3. The **License Agreement** window appears. Click **I Agree**.



Kiwi Syslog Server 9.5.1 Installer

**License Agreement**

Please review the license terms before installing Kiwi Syslog Server 9.5.1 .

Press Page Down to see the rest of the agreement.

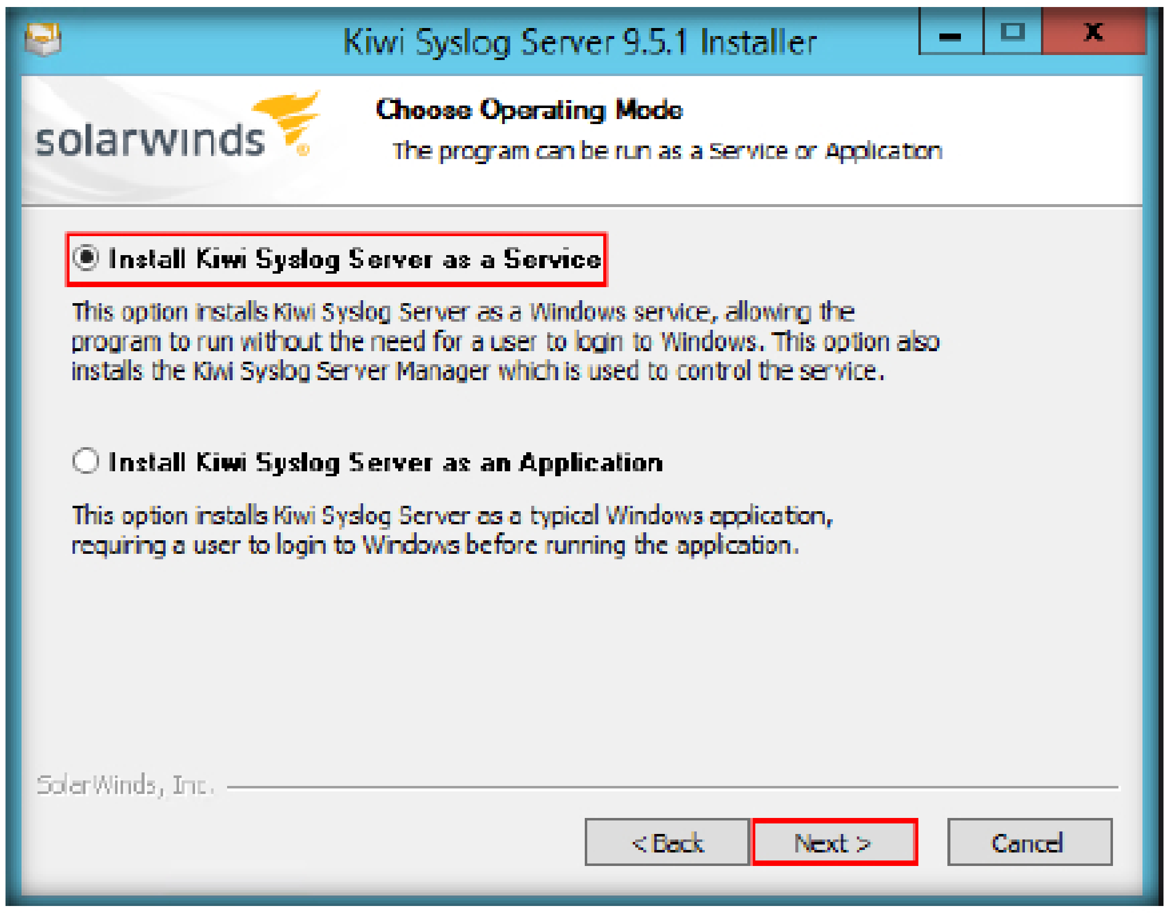
IMPORTANT - READ CAREFULLY: BY DOWNLOADING, INSTALLING, AND/OR USING THE SOFTWARE (DEFINED BELOW), YOU (DEFINED BELOW) AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT (DEFINED BELOW). IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE.

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Kiwi Syslog Server 9.5.1 .

FIGURE 5.1: Agreeing to the license agreement

Centralized Management of Syslog Messages & SNMP traps – Receive and consolidate syslog messages and SNMP traps from network devices and Linux and UNIX hosts.

4. The **Choose Operating Mode** window appears. Ensure the **Install Kiwi Syslog Server as a Service** radio button is enabled. Click **Next**.



Kiwi Syslog Server 9.5.1 Installer

**Choose Operating Mode**

The program can be run as a Service or Application

● Install Kiwi Syslog Server as a Service

This option installs Kiwi Syslog Server as a Windows service, allowing the program to run without the need for a user to login to Windows. This option also installs the Kiwi Syslog Server Manager which is used to control the service.

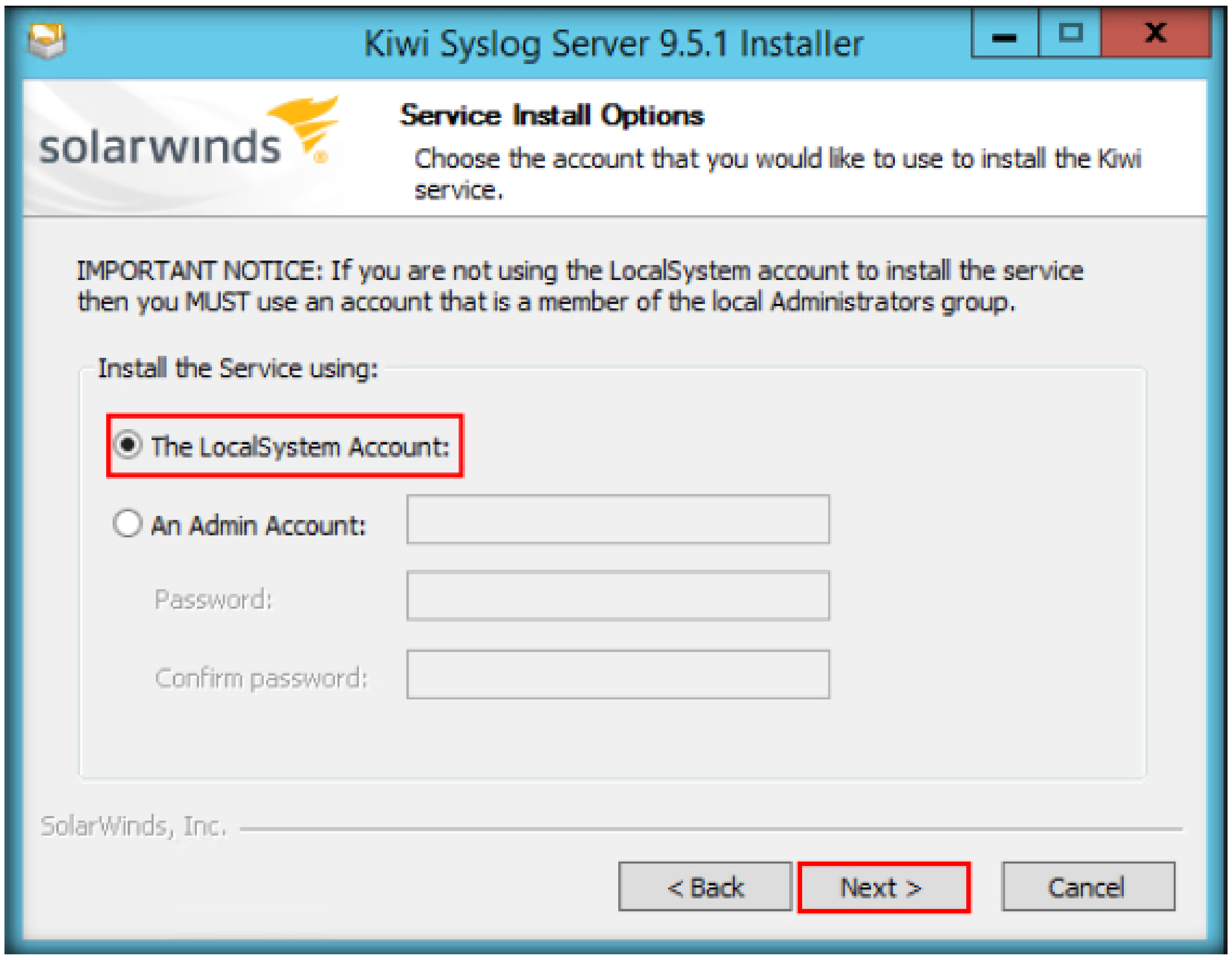
○ Install Kiwi Syslog Server as an Application

This option installs Kiwi Syslog Server as a typical Windows application, requiring a user to login to Windows before running the application.

FIGURE 5.2: Choosing the Operating mode

Real-Time Syslog Alerting & Notification – receive real-time alerts based on collected syslog and SNMP trap data (message text, host name/IP, date/time of message, syslog facility, level, etc.).

5. The **Service Install Options** window appears. Ensure the **LocalSystem Account:** radio button is enabled and click **Next**.



Kiwi Syslog Server 9.5.1 Installer

**Service Install Options**

Choose the account that you would like to use to install the Kiwi service.

IMPORTANT NOTICE: If you are not using the LocalSystem account to install the service then you MUST use an account that is a member of the local Administrators group.

Install the Service using:

● The LocalSystem Account:

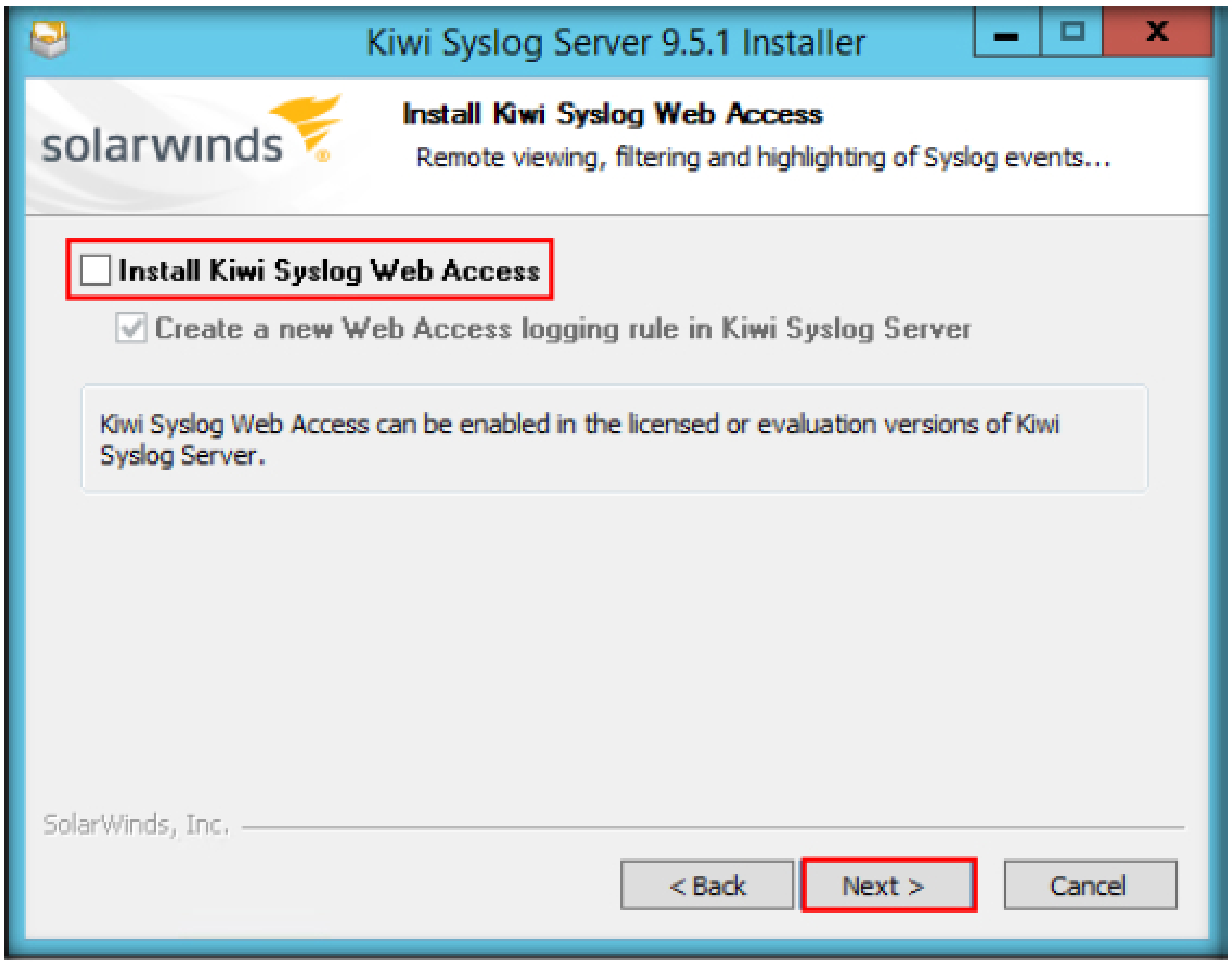
○ An Admin Account:

Password:

Confirm password:

FIGURE 5.3: Choosing the Service install type

6. The **Install Kiwi Syslog Web Access** window appears. Uncheck the **Install Kiwi Syslog Web Access** checkbox and click **Next**.



Kiwi Syslog Server 9.5.1 Installer

**Install Kiwi Syslog Web Access**

Remote viewing, filtering and highlighting of Syslog events...

□ Install Kiwi Syslog Web Access

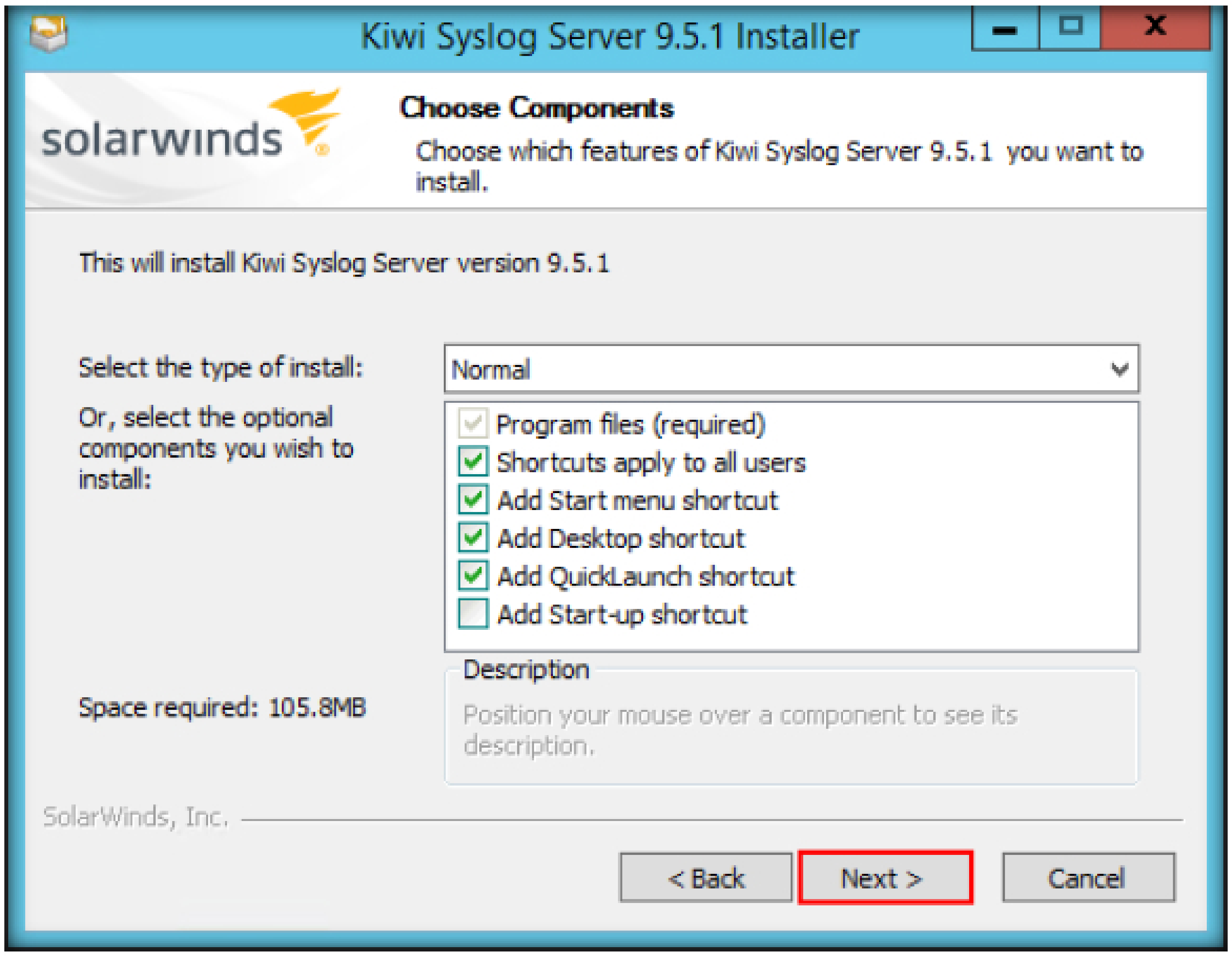
☑ Create a new Web Access logging rule in Kiwi Syslog Server

Kiwi Syslog Web Access can be enabled in the licensed or evaluation versions of Kiwi Syslog Server.

FIGURE 5.4: Not opting to install Kiwi web access

Automatically Respond to Log Messages – Execute automated actions upon receiving log messages: send email, forward to another host, run script, log to file/database/Windows® event log, etc.

7. The **Choose Components** window appears. Do not make any changes. Click **Next**.



Kiwi Syslog Server 9.5.1 Installer

**Choose Components**

Choose which features of Kiwi Syslog Server 9.5.1 you want to install.

This will install Kiwi Syslog Server version 9.5.1

Select the type of install: Normal

Or, select the optional components you wish to install:

- ☑ Program files (required)
- ☑ Shortcuts apply to all users
- ☑ Add Start menu shortcut
- ☑ Add Desktop shortcut
- ☑ Add QuickLaunch shortcut
- ☐ Add Start-up shortcut

Description

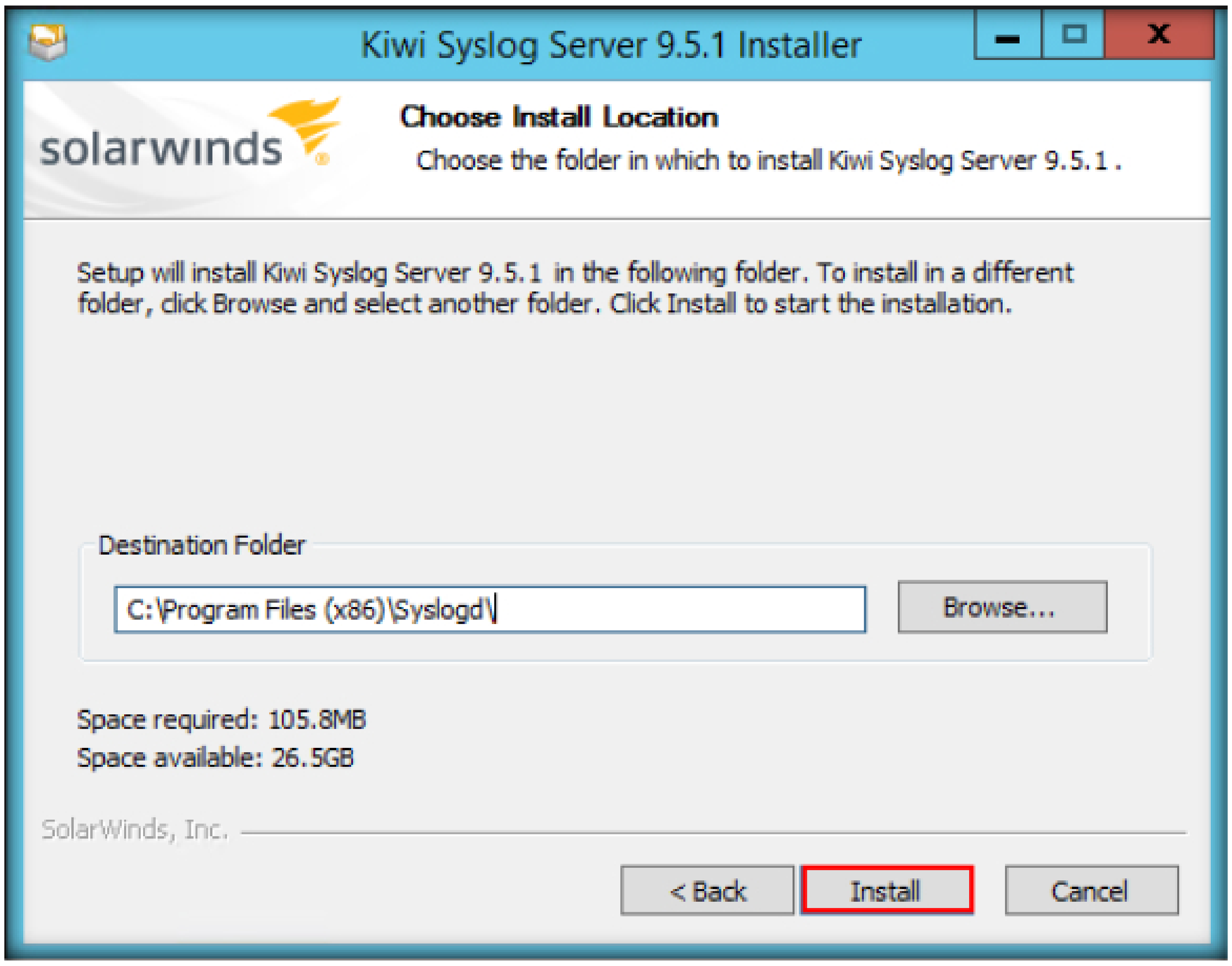
Position your mouse over a component to see its description.

Space required: 105.8MB

FIGURE 5.5: Selecting Kiwi components to install

Monitor & Manage Logs from Web Console – Use the out-of-the-box Web access utility to monitor and manage syslog messages and SNMP traps from any Web browser.

8. The **Choose Install Location** window appears. Leave it as default and click **Install**.



Kiwi Syslog Server 9.5.1 Installer

**Choose Install Location**

Choose the folder in which to install Kiwi Syslog Server 9.5.1 .

Setup will install Kiwi Syslog Server 9.5.1 in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

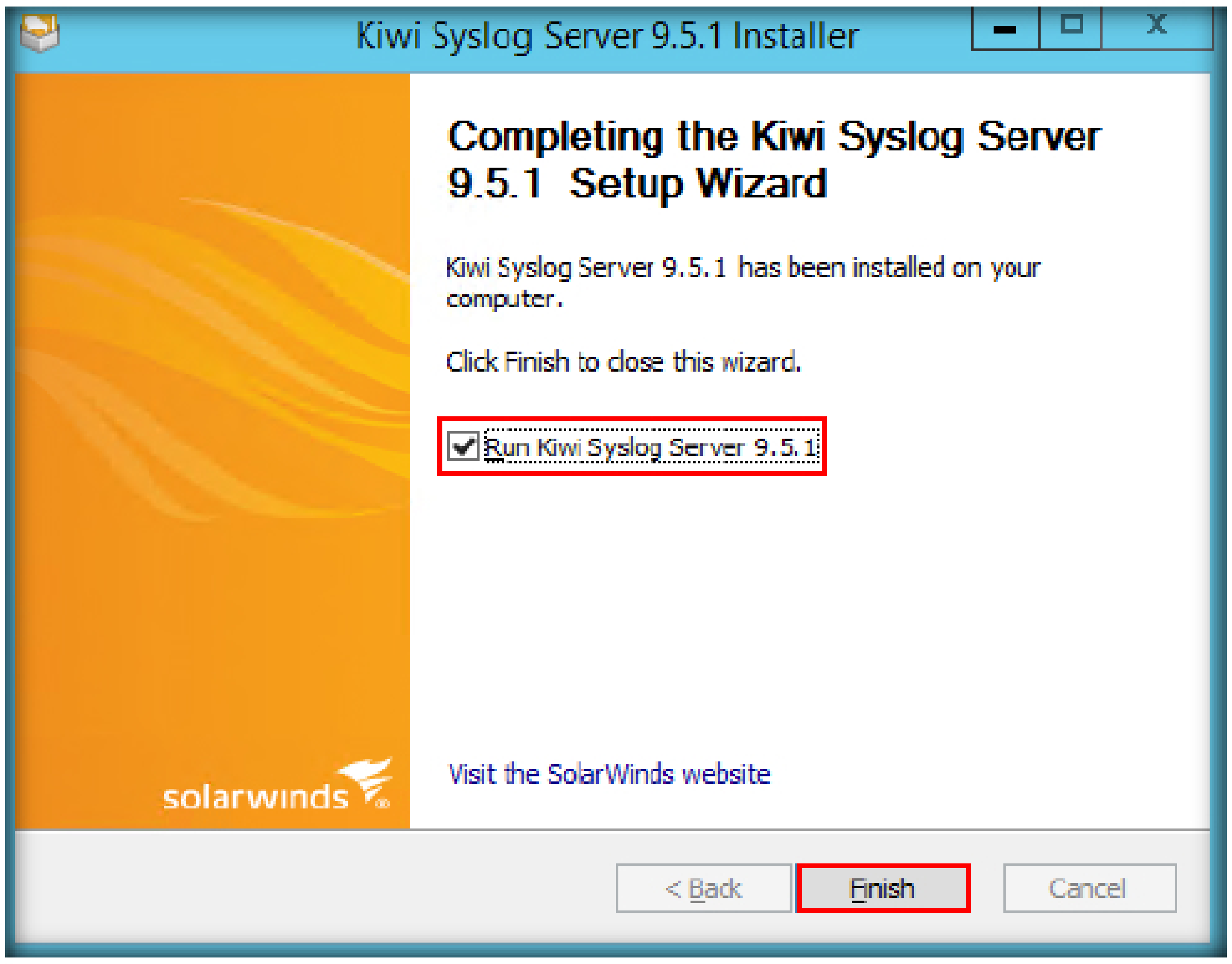
Destination Folder: C:\Program Files (x86)\Syslogd\

Space required: 105.8MB

Space available: 26.5GB

FIGURE 5.6: Selecting the location to install Kiwi Syslog server

9. After the installation is completed, you will see the following window with the successful installation message. Ensure the **Run Kiwi Syslog Server 9.5.1** checkbox is checked and click **Finish**.



Kiwi Syslog Server 9.5.1 Installer

**Completing the Kiwi Syslog Server 9.5.1 Setup Wizard**

Kiwi Syslog Server 9.5.1 has been installed on your computer.

Click Finish to close this wizard.

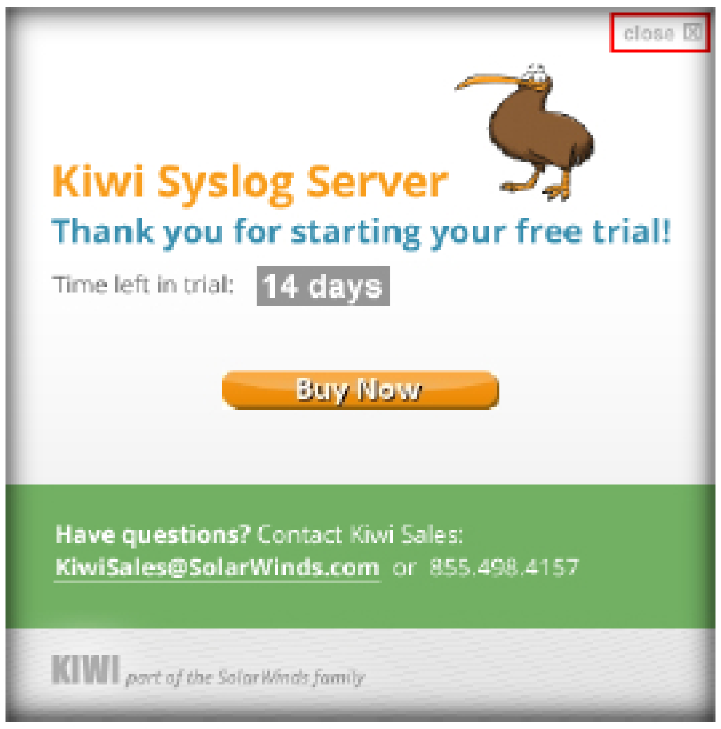
☑ Run Kiwi Syslog Server 9.5.1

FIGURE 5.7: Launching Kiwi Syslog Server

**TASK 2**

**Configuring Kiwi Syslog Server to listen various types of messages**

10. Thank you for starting your free trial! Pop-up appears then click **Close**.



Kiwi Syslog Server

Thank you for starting your free trial!

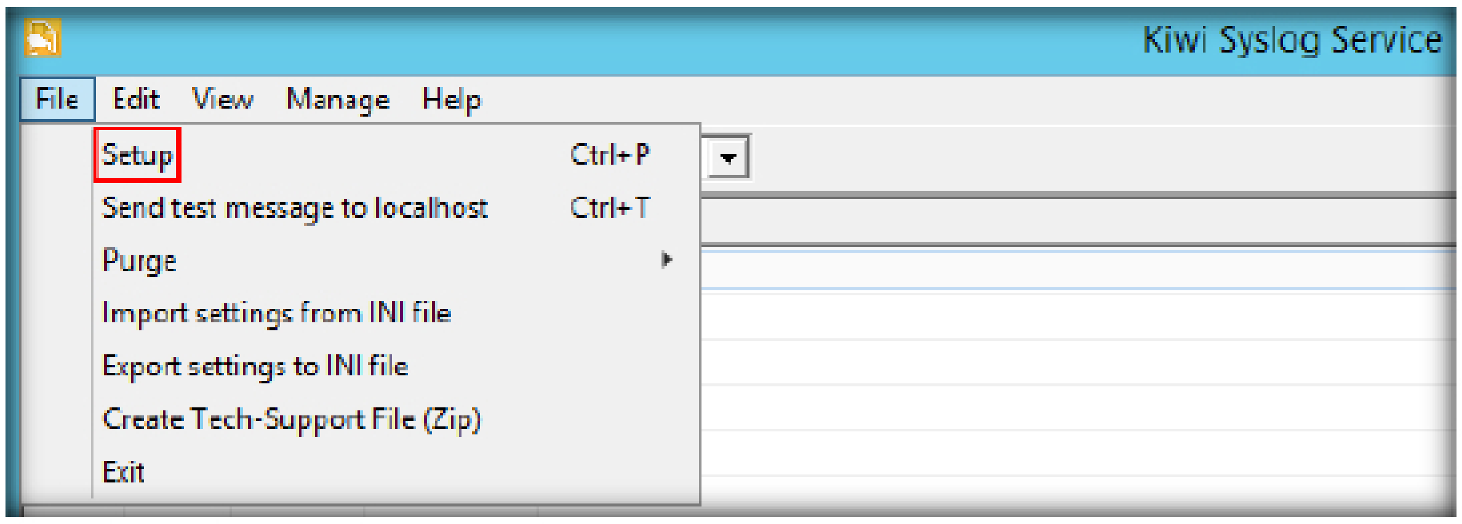
Time left in trial: 14 days

Have questions? Contact Kiwi Sales: KiwiSales@SolarWinds.com or 855.498.4157

FIGURE 5.8: Installation Completed

11. The Kiwi Syslog Server main window appears. Click the **File** menu and select **Setup**.

Store & Archive Logs for Regulatory Compliance – Automate log archival and cleanup schedules to comply with your log retention policy and regulatory requirements.



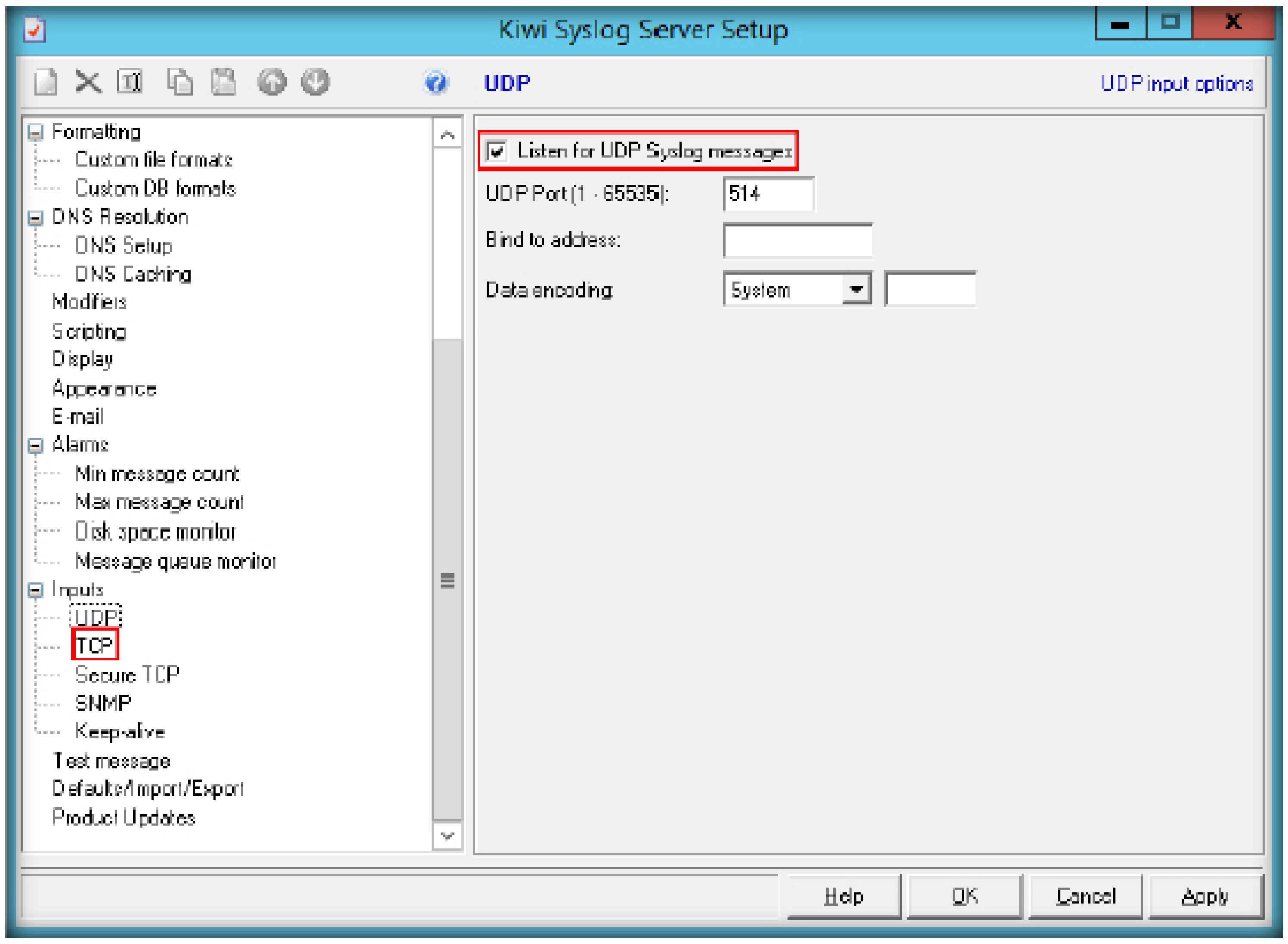
Kiwi Syslog Service
File
Edit
View
Manage
Help
Setup Ctrl+P
Send test message to localhost Ctrl+T
Purge
Import settings from INI file
Export settings to INI file
Create Tech-Support File (Zip)
Exit

FIGURE 5.9: Navigating to Setup

12. The **Kiwi Syslog Server Setup** window appears. In the left pane, scroll down and expand the **Inputs** section and click **UDP**.

13. By default, **Listen for UDP Syslog messages** is checked. If the option is not checked enable the option.

14. Click **TCP** under **Inputs** in the left pane.



Kiwi Syslog Server Setup

UDP

☑ Listen for UDP Syslog messages

UDP Port (1 - 65535): 514

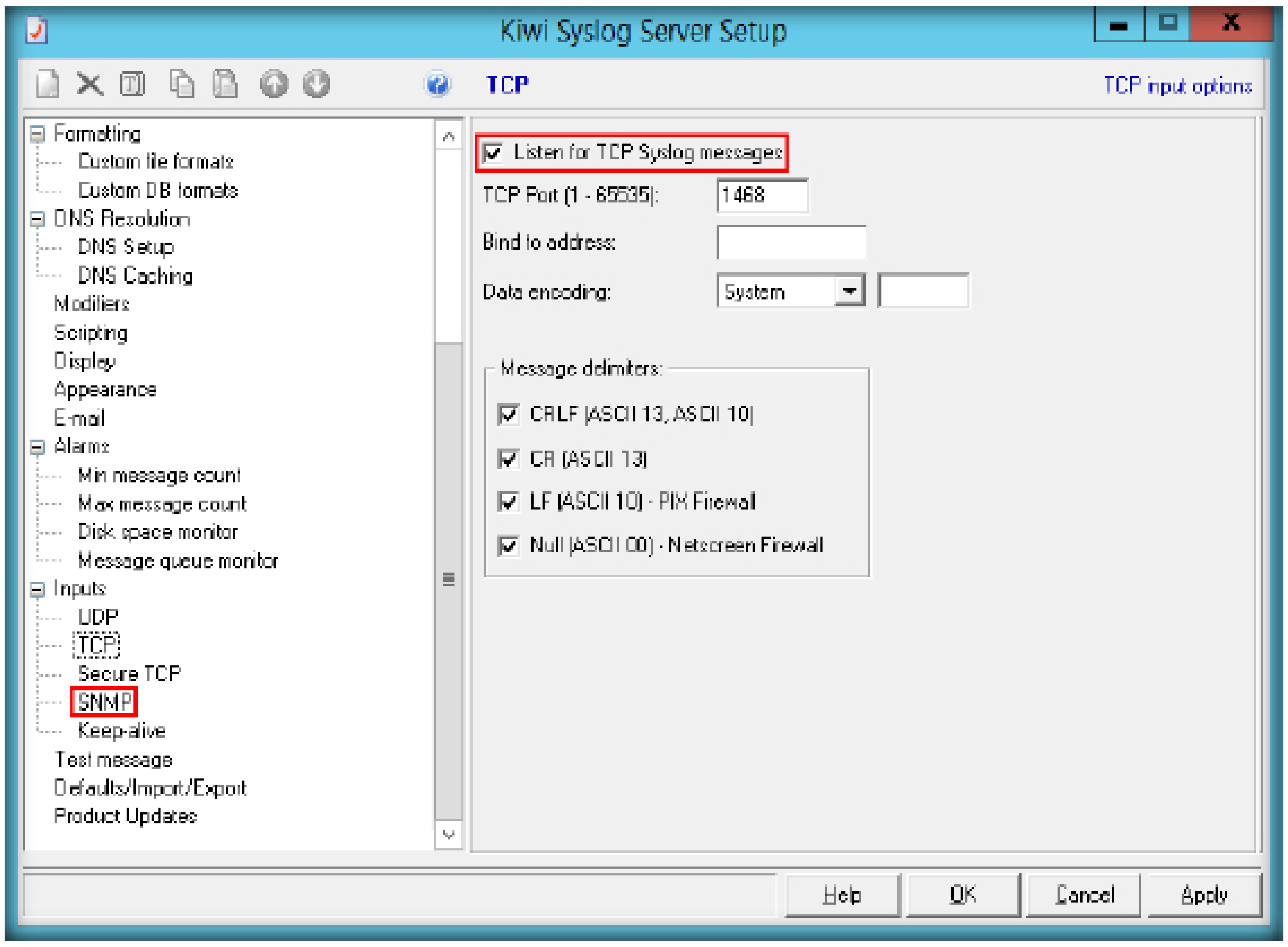
Bind to address:

Data encoding: System

FIGURE 5.10: Enabling UDP syslog messages

15. Click the **Listen for TCP Syslog messages** checkbox and leave the settings as default then click **SNMP** under **Inputs** in the left pane.

Generate Syslog Reports on Specific Devices, Events, & Actions – Generate HTML and plain text reports and deliver via email or send to disk. View syslog statistics and trends on graphical charts on the management console.



Kiwi Syslog Server Setup

TCP

☑ Listen for TCP Syslog messages

TCP Port (1 - 65535): 1468

Bind to address:

Data encoding: System

Message delimiters:

☑ CRLF (ASCII 13, ASCII 10)

☑ CR (ASCII 13)

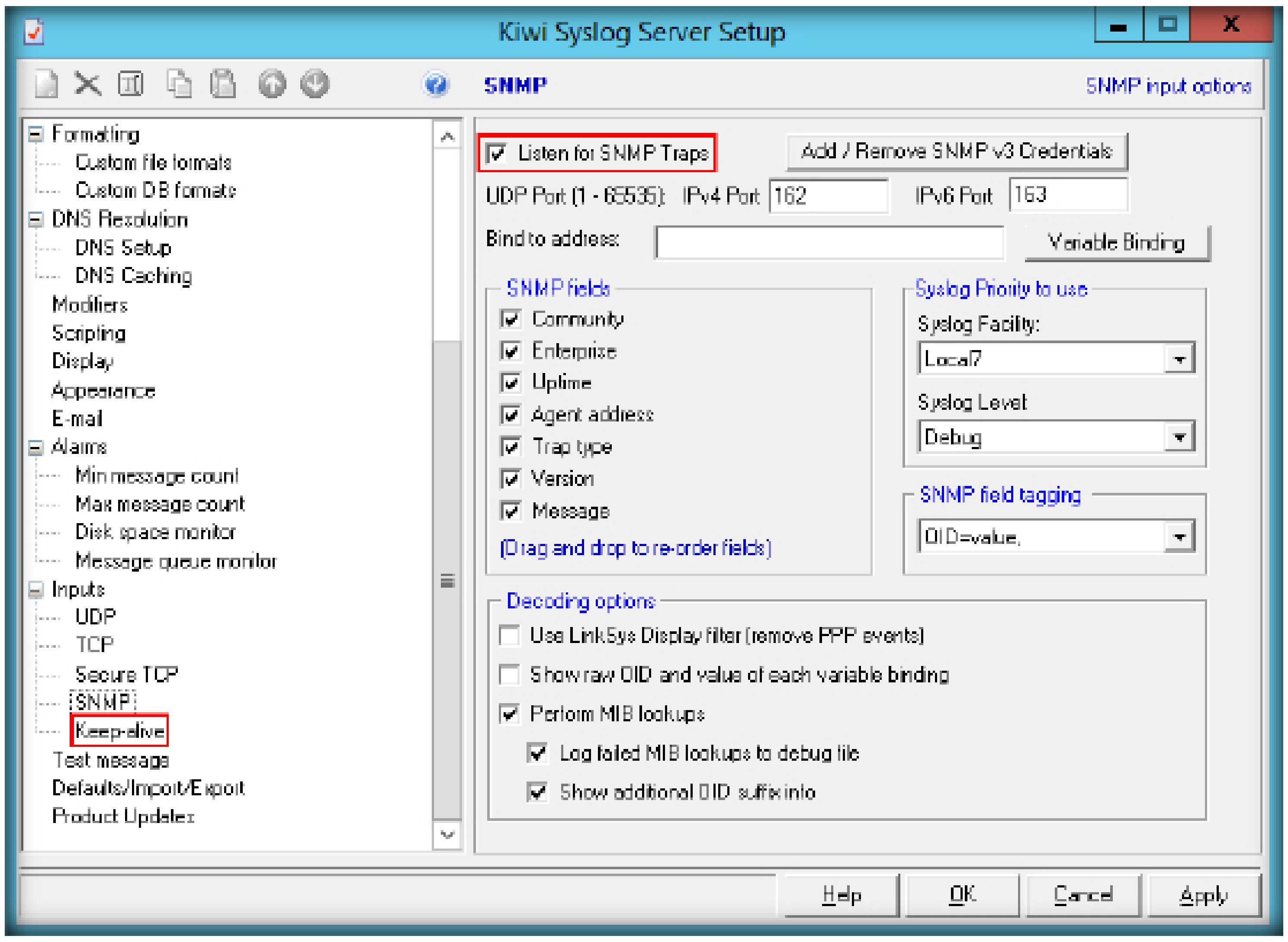
☑ LF (ASCII 10) - PIX Firewall

☑ Null (ASCII 00) - Netscreen Firewall

FIGURE 5.11: Enabling TCP syslog messages

16. Click the **Listen for SNMP Traps** check box and leave the settings to default.

17. Click **Keep-alive** under **Inputs** in the left pane.



Kiwi Syslog Server Setup

SNMP — SNMP input options

☑ Listen for SNMP Traps

UDP Port (1 - 65535): IPv4 Port 162 IPv6 Port 163

Bind to address:

SNMP fields: ☑ Community ☑ Enterprise ☑ Uptime ☑ Agent address ☑ Trap type ☑ Version ☑ Message (Drag and drop to re-order fields)

Syslog Priority to use: Syslog Facility: Local7; Syslog Level: Debug

SNMP field tagging: OID=value,

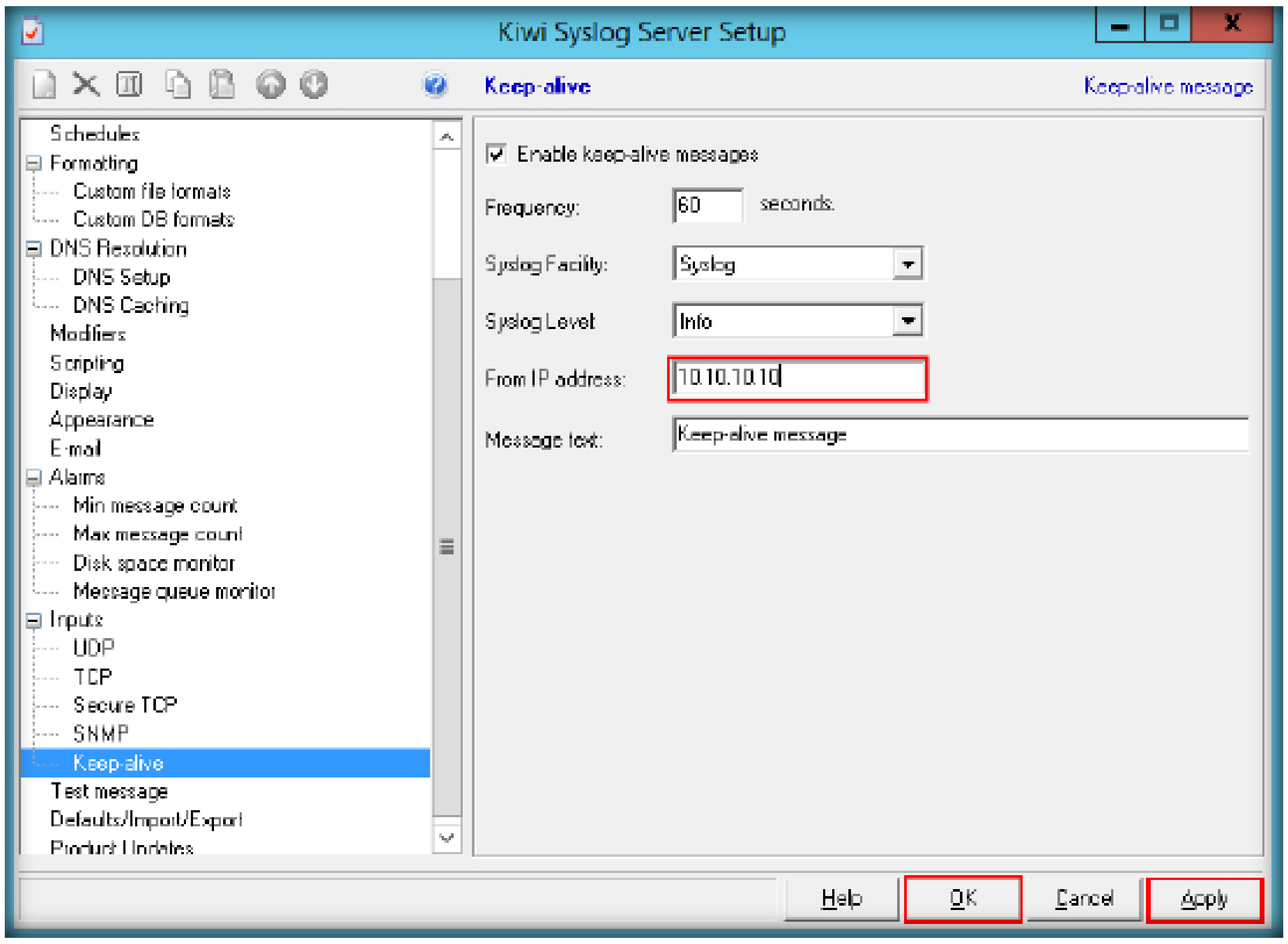
Decoding options:
□ Use LinkSys Display filter (remove PPP events)
□ Show raw OID and value of each variable binding
☑ Perform MIB lookups
☑ Log failed MIB lookups to debug file
☑ Show additional OID suffix info

FIGURE 5.12: Enabling SNMP traps

Deploy quickly: Installs in minutes. Start collecting syslog messages, SNMP traps, and Windows event log data from your IT infrastructure.

18. Tick **Enable Keep-alive messages** checkbox. Enter **10.10.10.10** in the **From IP address:** column (to record the logs of the user machine). Click **Apply** and then click **OK**.

Note: 10.10.10.10 is the IP address of the Windows 10 machine. The IP address may vary for your lab environment.



Kiwi Syslog Server Setup

Keep-alive — Keep-alive message

☑ Enable keep-alive messages

Frequency: 60 seconds

Syslog Facility: Syslog

Syslog Level: Info

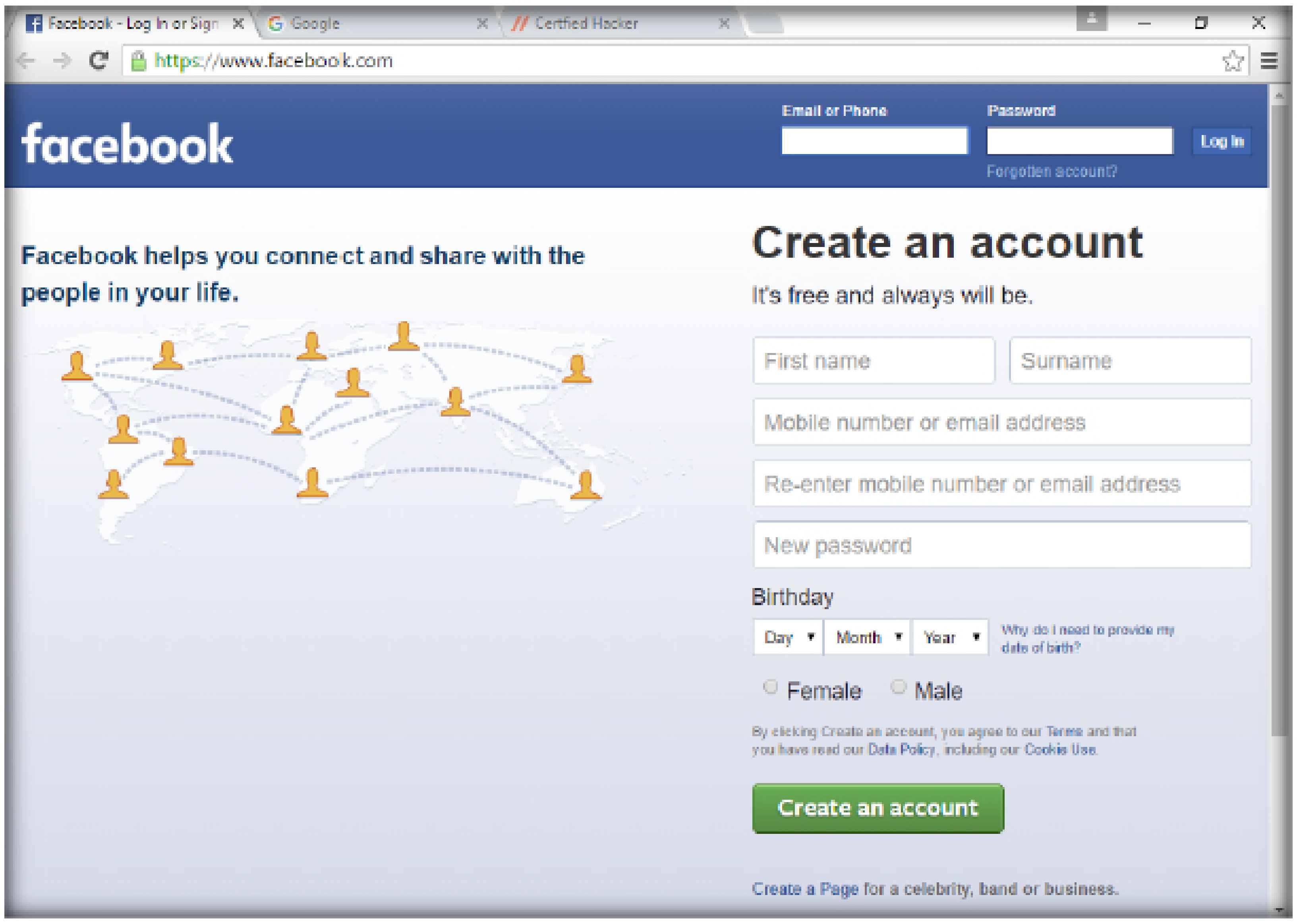
From IP address: 10.10.10.10

Message text: Keep-alive message

FIGURE 5.13: Enabling keep-alive messages

19. The Syslog server is configured to record the logs of the configured users machine.

20. Next, login to the Windows 10 machine as a domain user and browse webpages. Domain credentials are Username: **CND\Martin** and Password: **qwerty@123** as shown in the screenshot.



Facebook helps you connect and share with the people in your life.

Create an account

It's free and always will be.

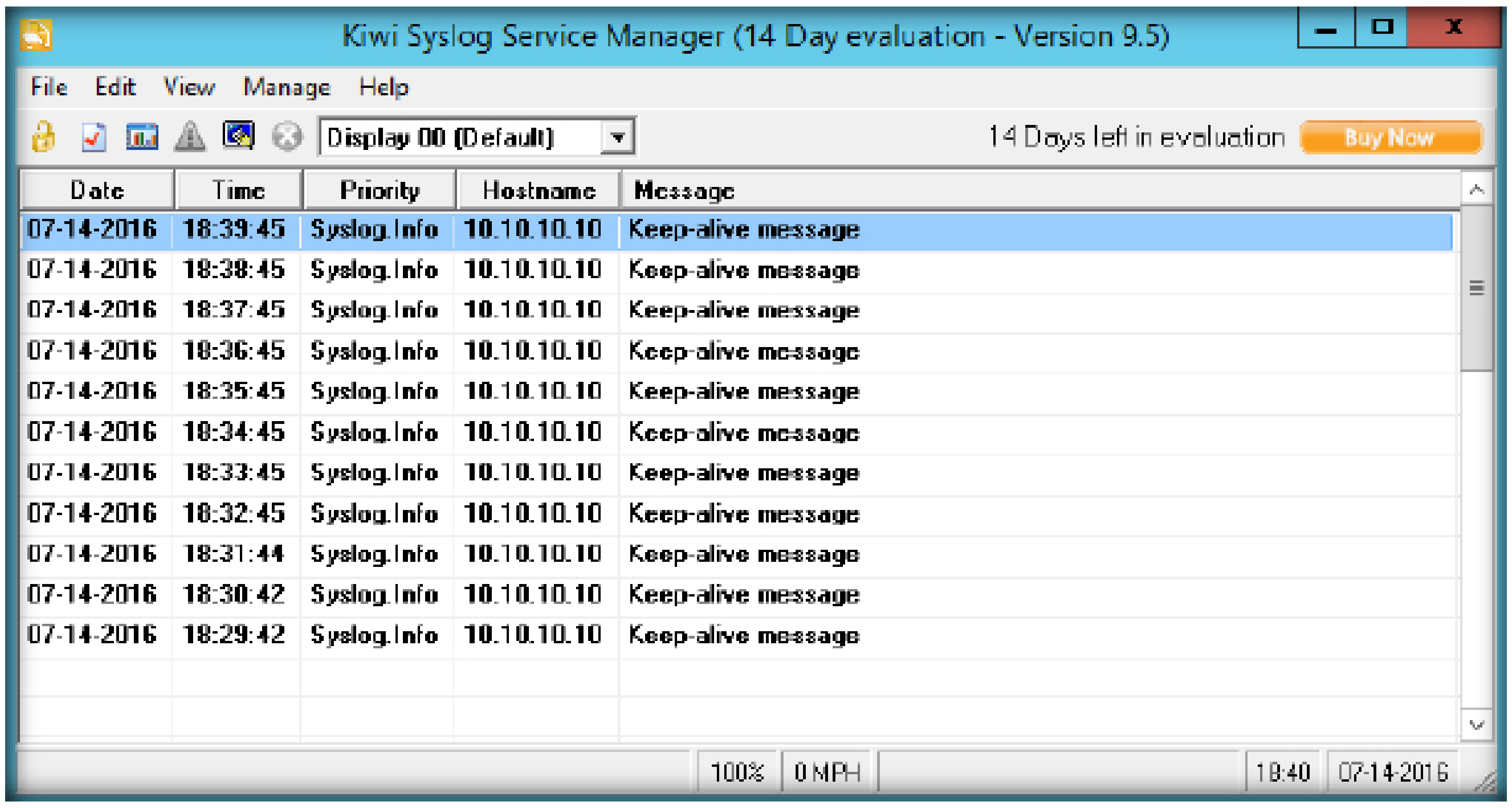
Why do I need to provide my date of birth?

By clicking Create an account, you agree to our Terms and that you have read our Data Policy, including our Cookie Use.

Create a Page for a celebrity, band or business.

FIGURE 5.14: Activities in Windows 10 Machine

21. Switch back to the Windows Server 2012 machine where the Kiwi Syslog server is running. You can see the Syslog server has recorded a few logs encountered through the Windows 10 machine as shown in the screenshot.


Kiwi Syslog Service Manager (14 Day evaluation - Version 9.5)
File
Edit
View
Manage
Help
Display 00 (Default)
14 Days left in evaluation
Buy Now
100%
0 MPH
18:40
07-14-2016

```
Date        Time      Priority     Hostname     Message
07-14-2016  18:39:45  Syslog.Info  10.10.10.10  Keep-alive message
07-14-2016  18:38:45  Syslog.Info  10.10.10.10  Keep-alive message
07-14-2016  18:37:45  Syslog.Info  10.10.10.10  Keep-alive message
07-14-2016  18:36:45  Syslog.Info  10.10.10.10  Keep-alive message
07-14-2016  18:35:45  Syslog.Info  10.10.10.10  Keep-alive message
07-14-2016  18:34:45  Syslog.Info  10.10.10.10  Keep-alive message
07-14-2016  18:33:45  Syslog.Info  10.10.10.10  Keep-alive message
07-14-2016  18:32:45  Syslog.Info  10.10.10.10  Keep-alive message
07-14-2016  18:31:44  Syslog.Info  10.10.10.10  Keep-alive message
07-14-2016  18:30:42  Syslog.Info  10.10.10.10  Keep-alive message
07-14-2016  18:29:42  Syslog.Info  10.10.10.10  Keep-alive message
```

Figure 5.15: Syslog received in Kiwi Server

**Note**: If you have minimized the Kiwi Syslog server, the Kiwi syslog server icon will be shown in the notification area on the desktop.

## Lab Analysis

Analyze and document the results of the lab exercise. Give your opinion on your target's security posture and exposure through free public information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

| Internet Connection Required | |
|---|---|
| □ Yes | ☑ No |
| Platform Supported | |
| ☑ Classroom | ☑ iLabs |

Lab

6

# Remote Log Capture Using Splunk Universal Forwarder

Splunk is a tool for collecting, monitoring, and analyzing log files from servers, applications, or other sources.

## Lab Scenario

Maintaining the health and security of the remote systems in a network is the primary task of a network administrator. Setting up a remote log server will ensure that the logs remain uncompromised in the event of an intruder attack. You need to install a log forwarder in all machines in the network. This will store all the logs in the main log management server.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

## Lab Objectives

This lab will demonstrate how to install and configure a log forwarder to capture remote system logs.

## Lab Environment

To carry out the lab, you need:

- A virtual machine running Windows server 2012 with Splunk installed on it
- A virtual machine running Windows 10
- SplunkForwarder located at **Z:\CND-Tools\CND Module 06 Host Security\Log Monitoring Tools\Splunk**
- Administrative privileges to run the tools
- A web browser with Internet access
- If you wish to install the latest version of tools; screenshots and steps might differ from the ones shown in the lab environment.

## Lab Duration

Time: 30 Minutes

## Overview of Universal Forwarder

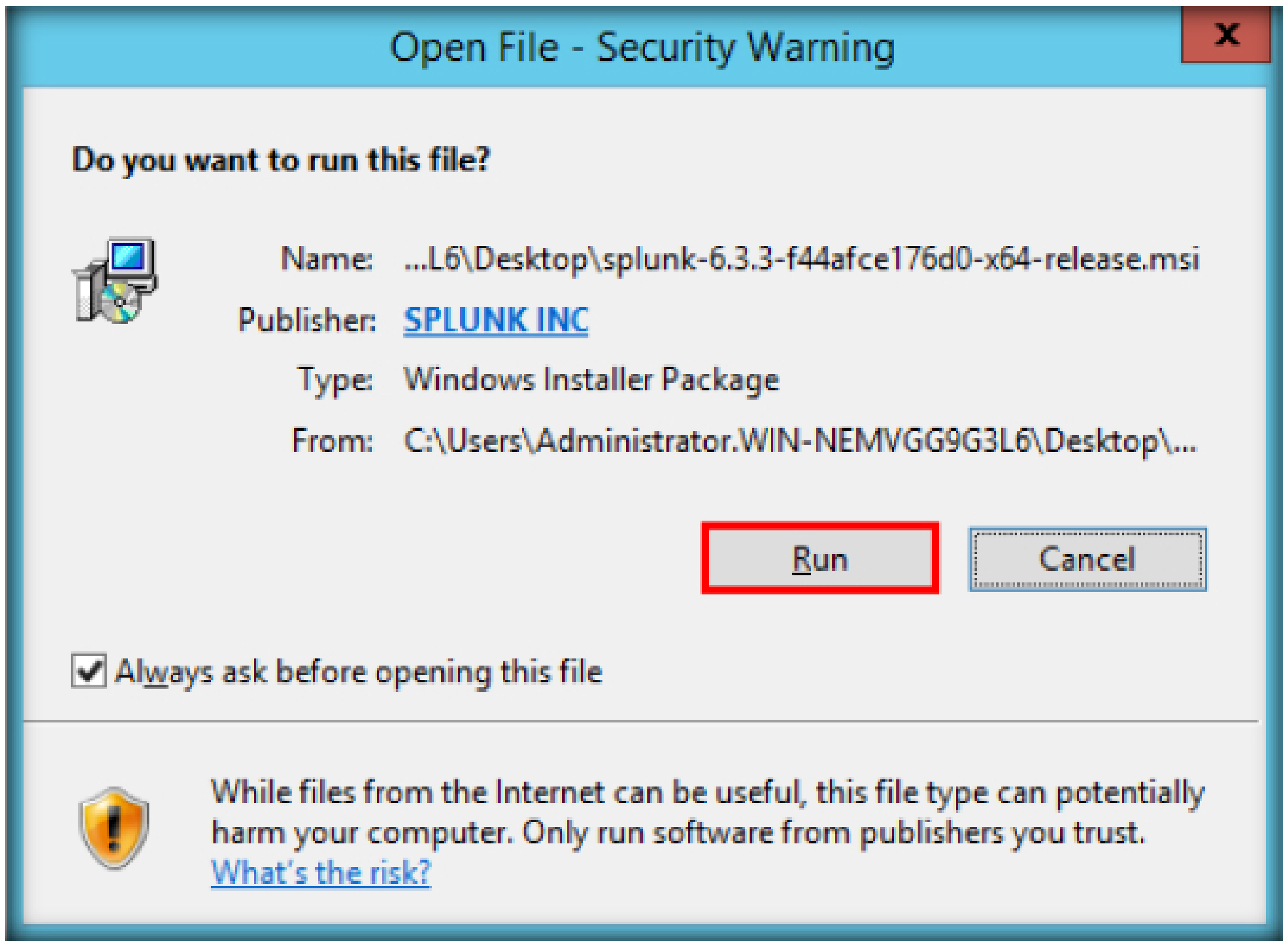
The universal forwarder is a Splunk Enterprise instance that contains only the essential components needed to forward data. The application provides reliable, secure data collection from remote sources and forwards that data into Splunk (Enterprise, Light, Cloud or Hunk) for indexing and consolidation.

## Lab Tasks

**TASK 1**

**Installing Splunk console**

1. Launch **Windows Server 2012** and navigate to **Z:\CND-Tools\CND Module 06 Host Security\Log Monitoring Tools\Splunk**
2. Double click **splunk-6.3.3-f44afce176d0-x64-release.msi** to start the installation. If the **Open File - Security Warning** window pops up, click **Run**.



Open File - Security Warning

Do you want to run this file?

Name: ...L6\Desktop\splunk-6.3.3-f44afce176d0-x64-release.msi

Publisher: SPLUNK INC

Type: Windows Installer Package

From: C:\Users\Administrator.WIN-NEMVGG9G3L6\Desktop\...

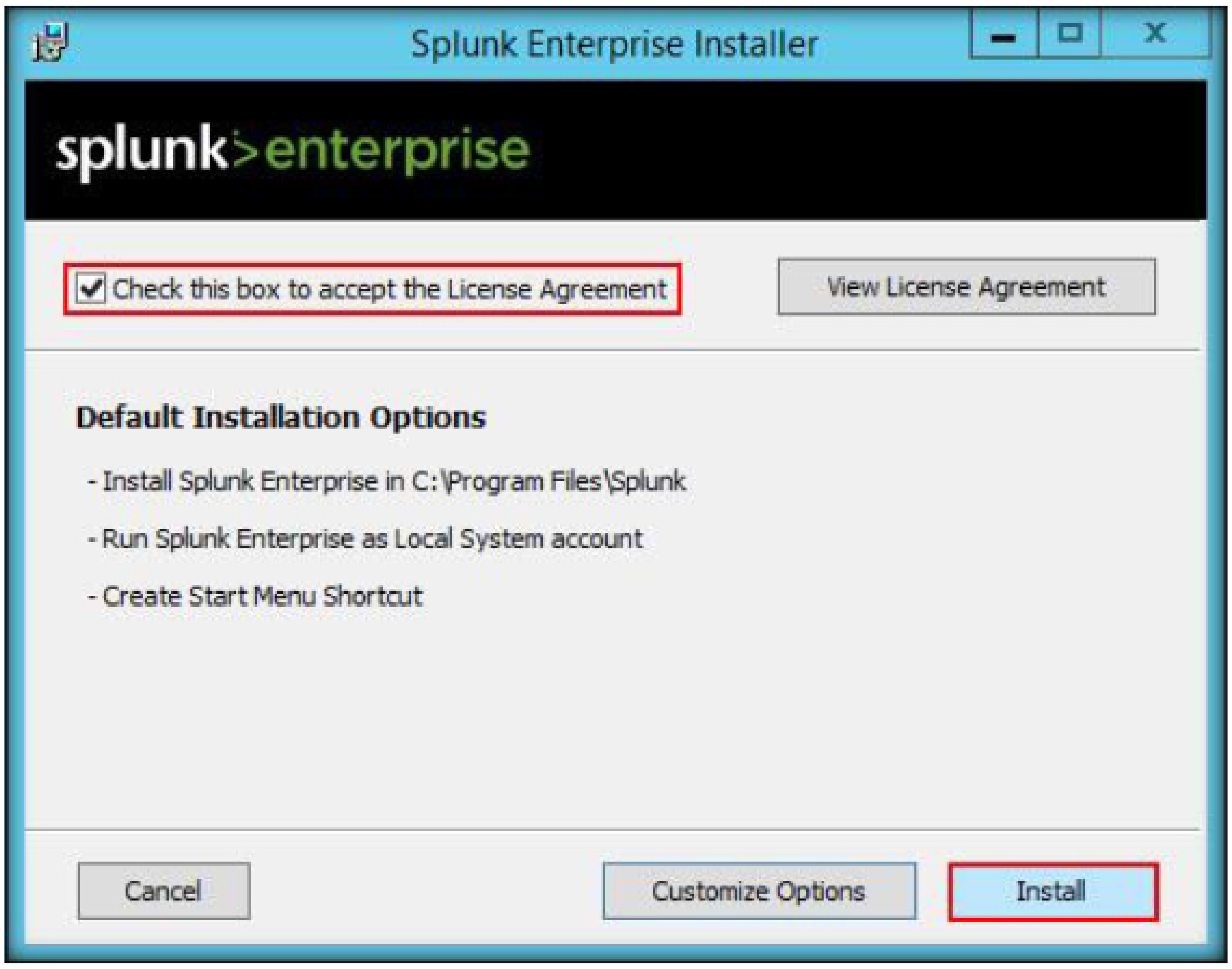
☑ Always ask before opening this file

While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

FIGURE 6.1: Open File – Security Warning

**Note**: If a notification appears stating the "SmartScreen has prevented the app from running", click More info, and then click Run anyway.

3. The **Splunk Enterprise Installer** window appears. Accept the license agreement and click **Install**.



Splunk Enterprise Installer

splunk>enterprise

☑ Check this box to accept the License Agreement

**Default Installation Options**

- Install Splunk Enterprise in C:\Program Files\Splunk

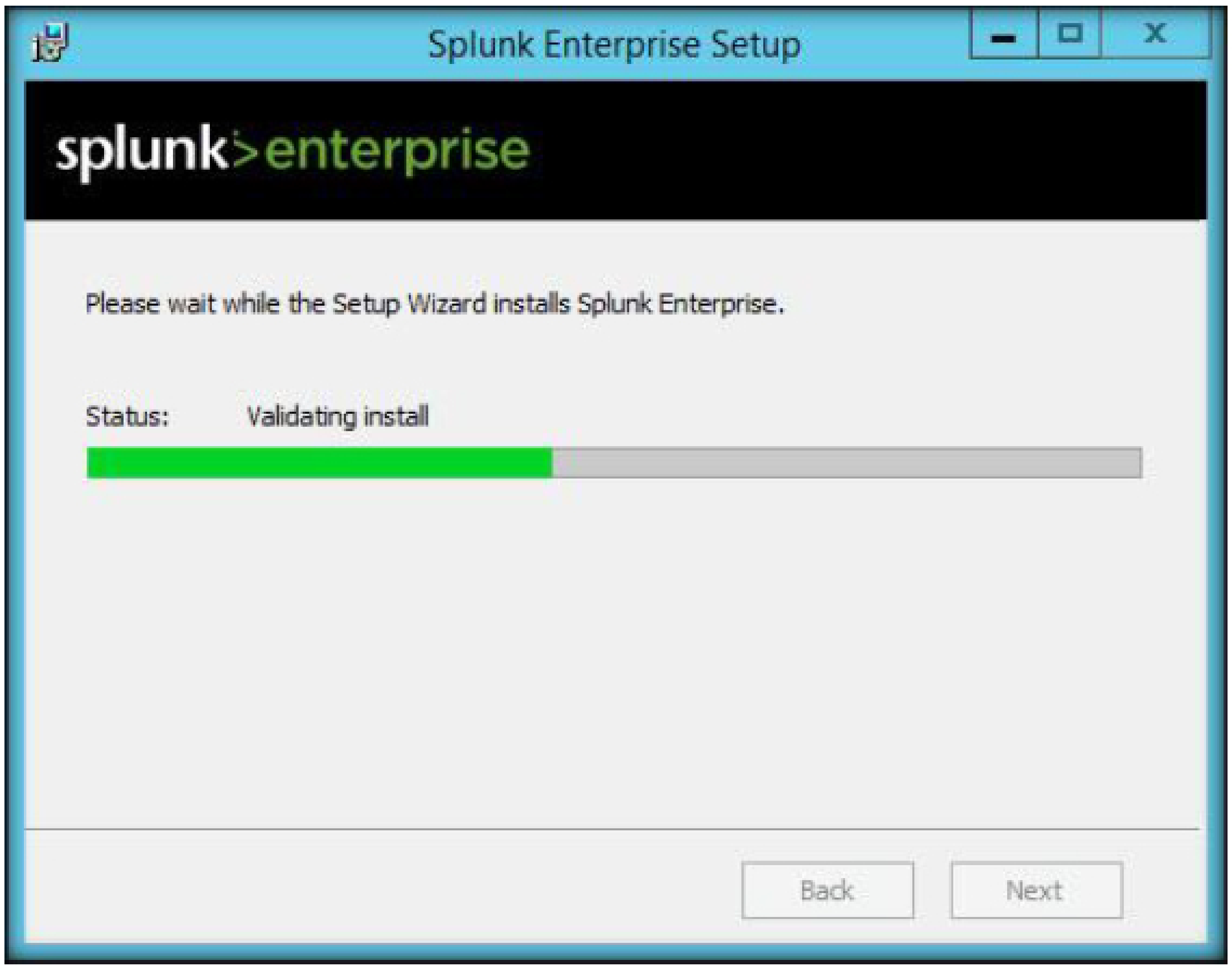
- Run Splunk Enterprise as Local System account

- Create Start Menu Shortcut

FIGURE 6.2: Splunk license agreement

Using no predefined schema, Splunk Universal Forwarders and collection methods such as syslog, HTTP direct API, scripted inputs, and the mobile SDK can index unstructured data from sources such as applications, sensors, endpoint devices,

4. Wait for the installation to complete.



Splunk Enterprise Setup

splunk>enterprise

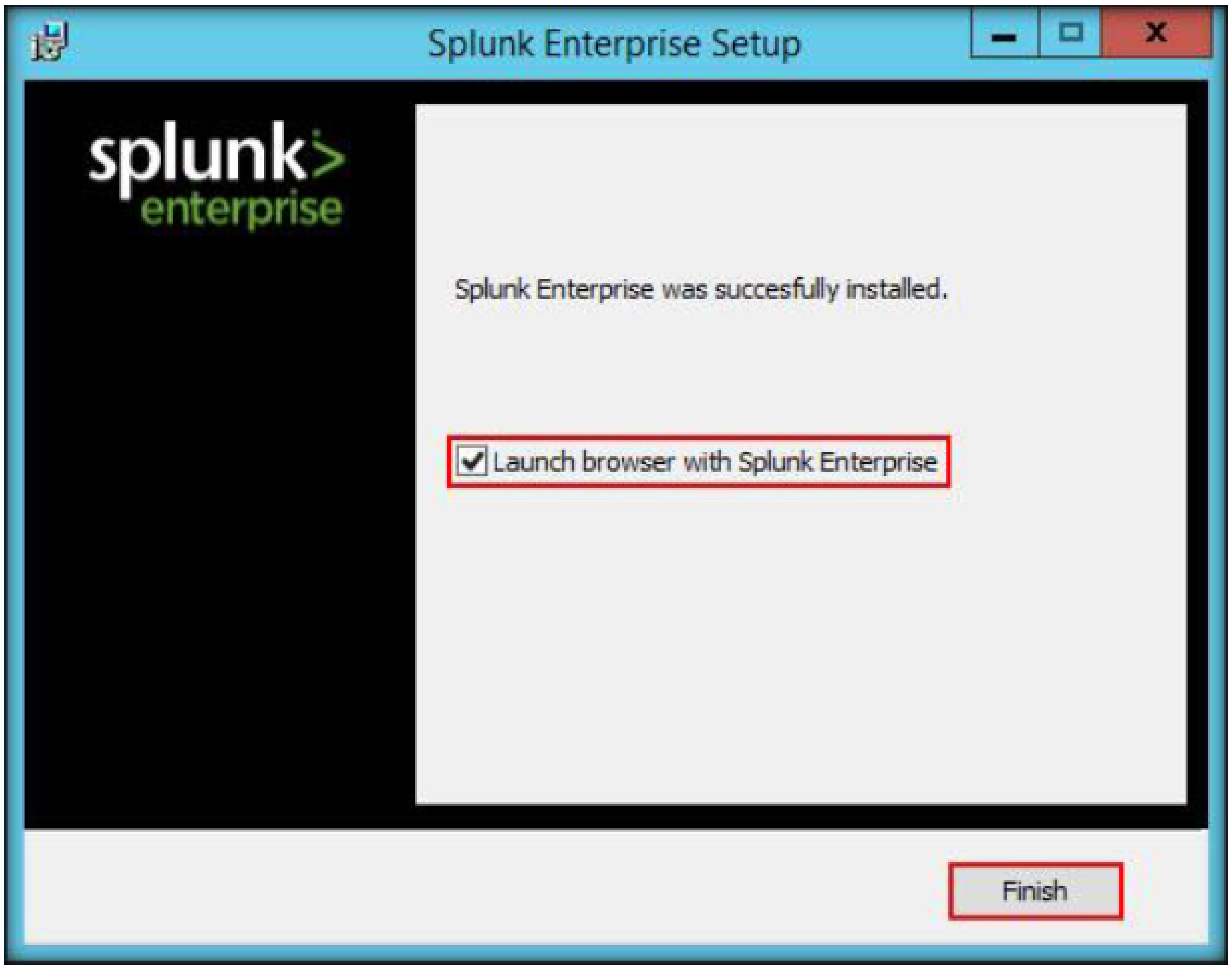
Please wait while the Setup Wizard installs Splunk Enterprise.

Status: Validating install

FIGURE 6.3: Splunk installation progress

5. After the installation is complete, ensure the **Launch browser with Splunk Enterprise** box is checked then click **Finish**.

By monitoring and analyzing everything from customer click streams and transactions to security events and network activity, Splunk Enterprise helps you gain valuable Operational Intelligence from your machine-generated data. And with a full range of powerful search, visualization and pre-packaged content for use-cases, any user can quickly discover and share insights. Just point your raw data at Splunk Enterprise and start analyzing your world.



Splunk Enterprise was succesfully installed.

☑ Launch browser with Splunk Enterprise

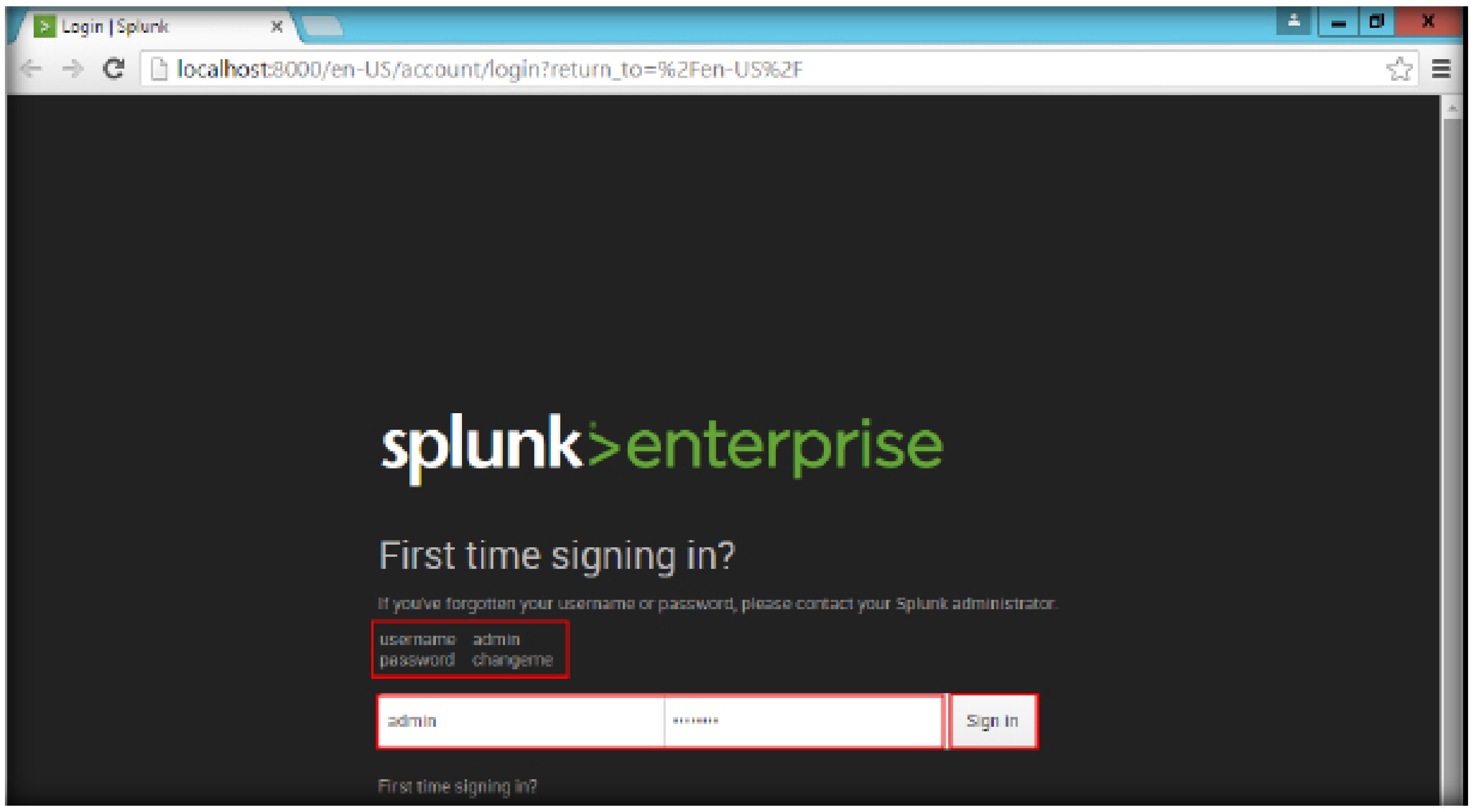
FIGURE 6.4: Splunk installed successfully

## TASK 2

**Login to Splunk**

6. Splunk Enterprise launches in your default browser. The **First time signing in?** page appears. Enter the default **username** and **password** (provided by Splunk) in their respective fields and click **Sign in**.

7. The default credentials for the first login display on the screen as shown in the screenshot.



localhost:8000/en-US/account/login?return_to=%2Fen-US%2F

First time signing in?

If you've forgotten your username or password, please contact your Splunk administrator.

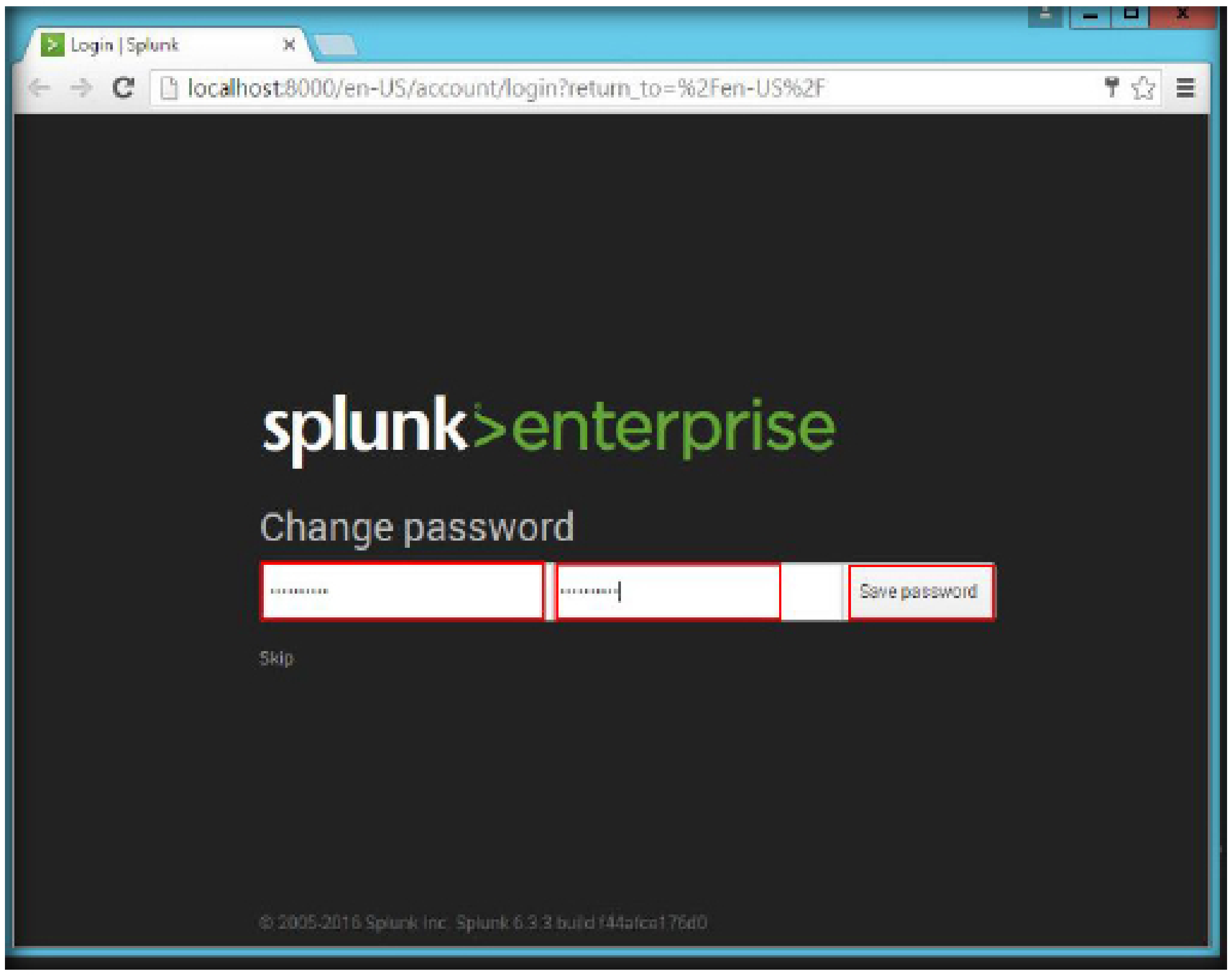
username admin
password changeme

admin ········

First time signing in?

FIGURE 6.5: Splunk installed successfully

8. The **Change password** page appears. Create a strong password and click **Save password**.



Login | Splunk

localhost:8000/en-US/account/login?return_to=%2Fen-US%2F

splunk>enterprise

Change password

© 2005-2016 Splunk Inc. Splunk 6.3.3 build f44afce176d0

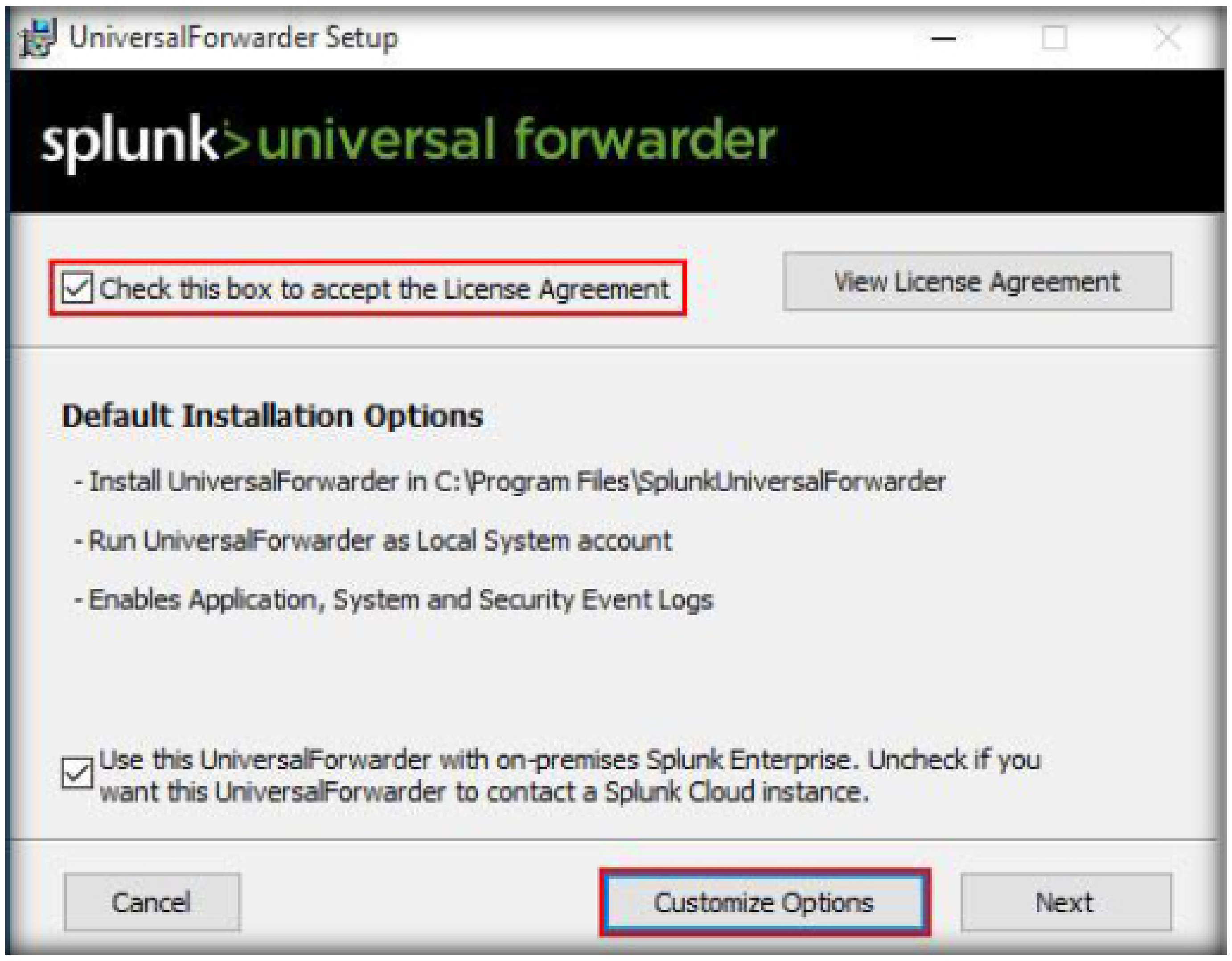
FIGURE 6.6: Splunk installed successfully

9. In order to monitor logs in a Windows 10 virtual machine, you need to install the Universal log forwarder in it.

10. Login as a local administrator and navigate to **Z:\CND-Tools\CND Module 06 Host Security\Log Monitoring Tools\Splunk**, and double-click **splunkforwarder-6.4.0-f2c836328108-x64-release.msi**.

Using no predefined schema, Splunk Universal Forwarders and collection methods such as syslog, HTTP direct API, scripted inputs, and the mobile SDK can index unstructured data from sources such as applications, sensors, endpoint devices, mainframes, industrial systems and network packet streams.

11. The UniversalForwarder Setup window appears, accept the license agreement and click **Customize Options**.



UniversalForwarder Setup

splunk>universal forwarder

☑ Check this box to accept the License Agreement

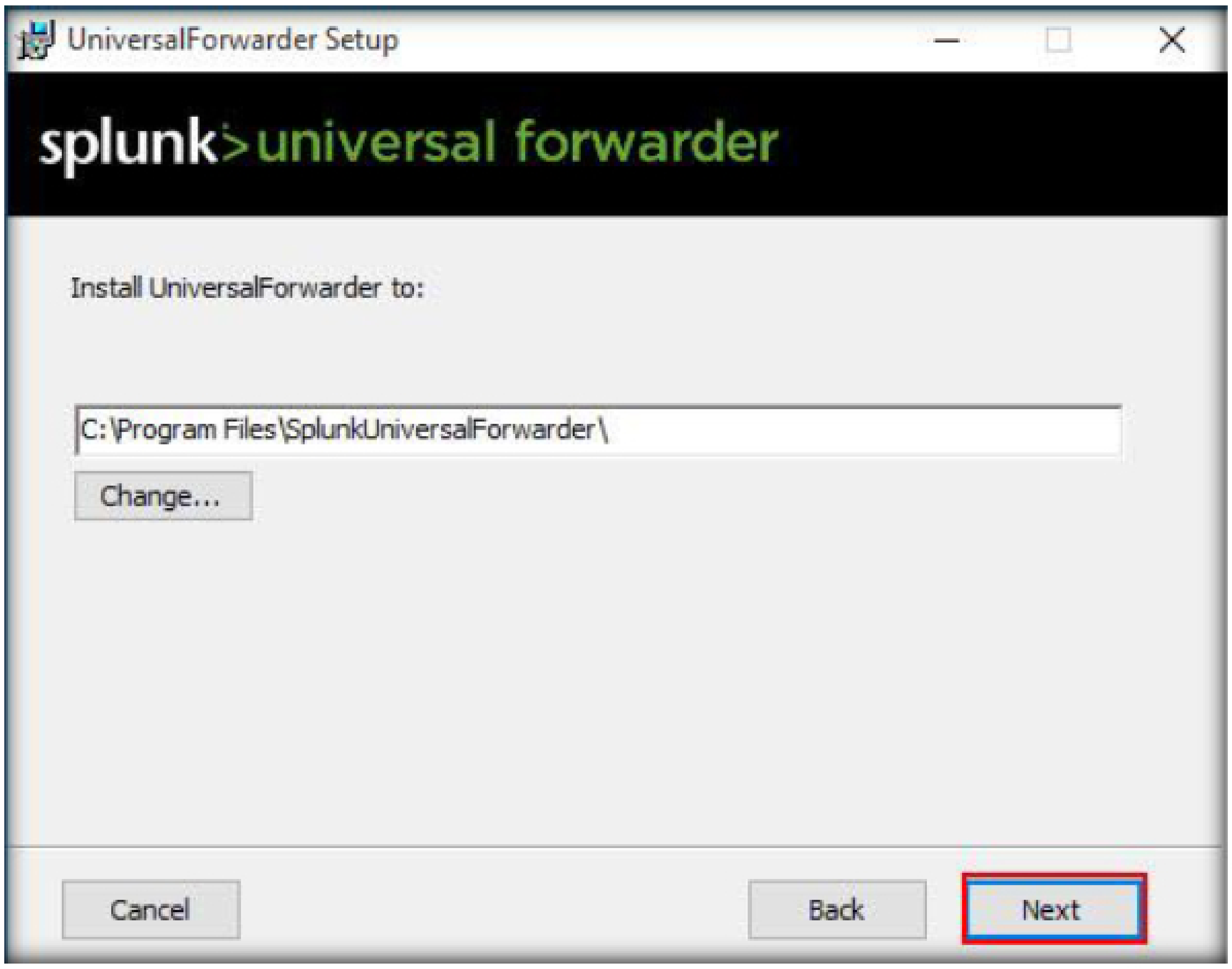
**Default Installation Options**

- Install UniversalForwarder in C:\Program Files\SplunkUniversalForwarder
- Run UniversalForwarder as Local System account
- Enables Application, System and Security Event Logs

☑ Use this UniversalForwarder with on-premises Splunk Enterprise. Uncheck if you want this UniversalForwarder to contact a Splunk Cloud instance.

FIGURE 6.7: Installing Splunk forwarder

12. Leave the installation path set to the default location, click **Next**.

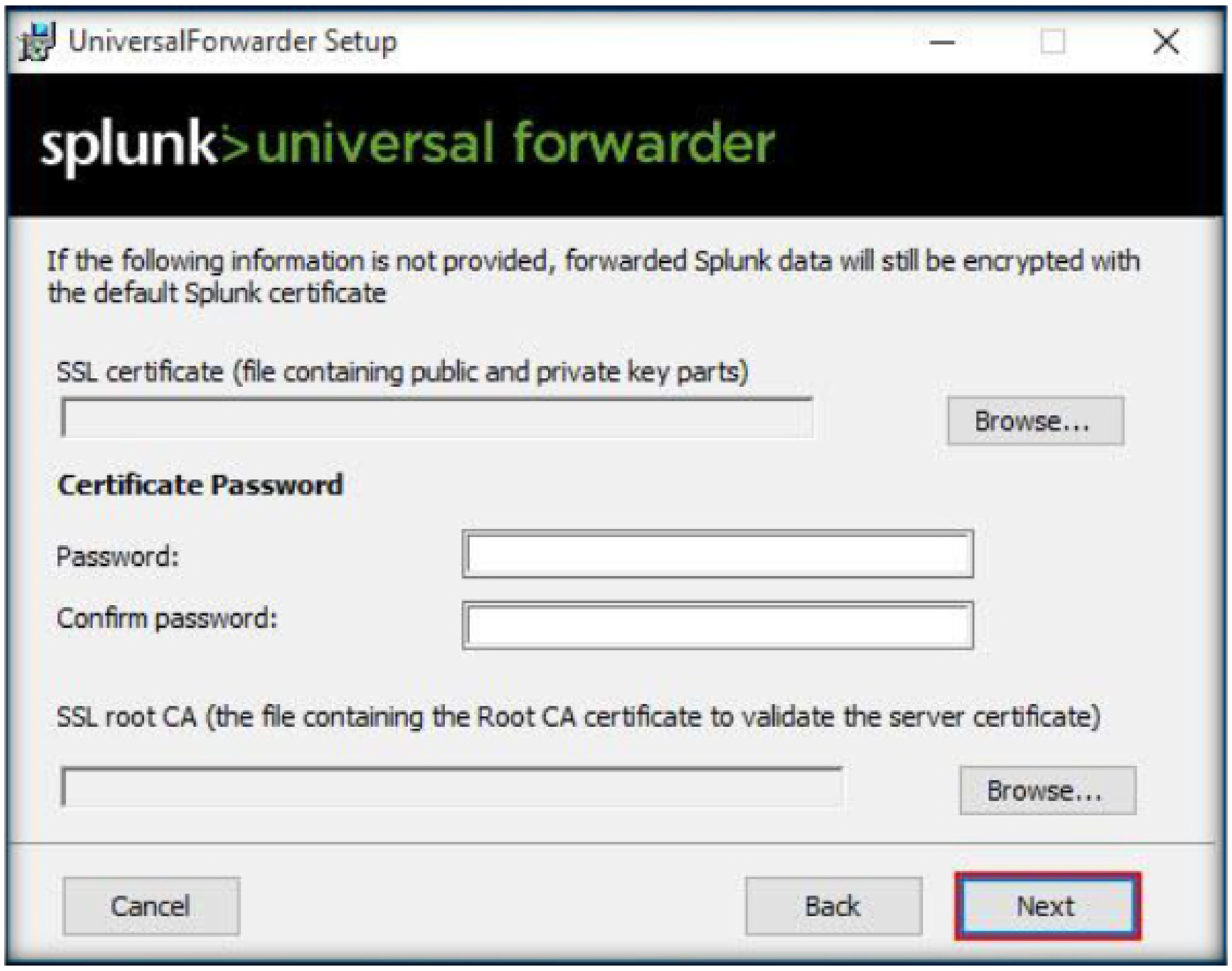


Install UniversalForwarder to:

C:\Program Files\SplunkUniversalForwarder\

FIGURE 6.8: Choosing location to install Splunk forwarder

13. Click **Next** in the Splunk Certificate section.



If the following information is not provided, forwarded Splunk data will still be encrypted with the default Splunk certificate

SSL certificate (file containing public and private key parts)

**Certificate Password**

Password:

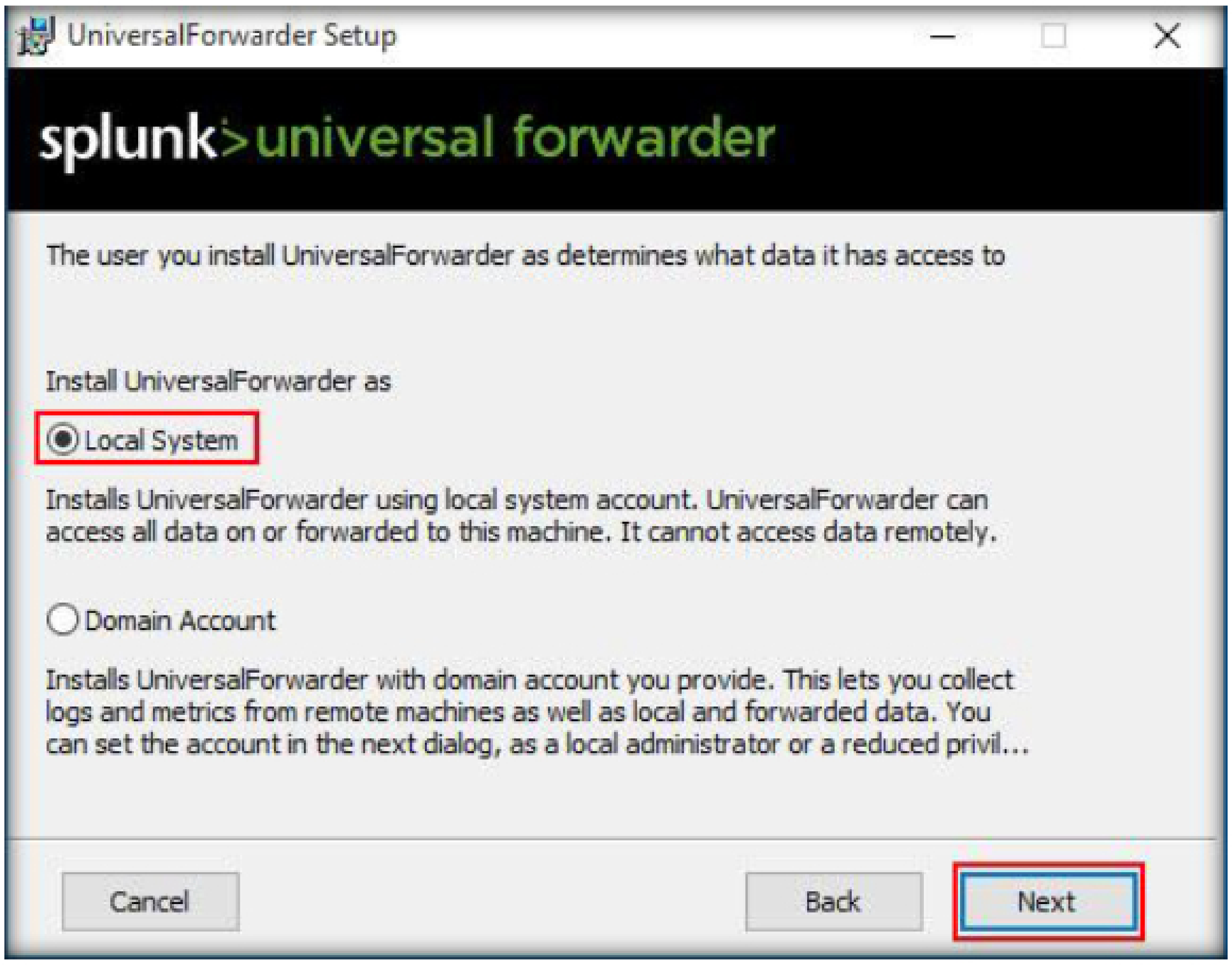
Confirm password:

SSL root CA (the file containing the Root CA certificate to validate the server certificate)

FIGURE 6.9: Installing Splunk Forwarder

Timeline shows start/stop/duration of processes on a timeline and is commonly used by IT to investigate processes that run for a longer time period and to monitor batch processes. It can also be used for business analytics to quickly portray order processing.

14. In the next step, select the **Local System** radio button, in order to install Universal Forwarder as a Local System and click **Next**.



UniversalForwarder Setup

splunk>universal forwarder

The user you install UniversalForwarder as determines what data it has access to

Install UniversalForwarder as

● Local System

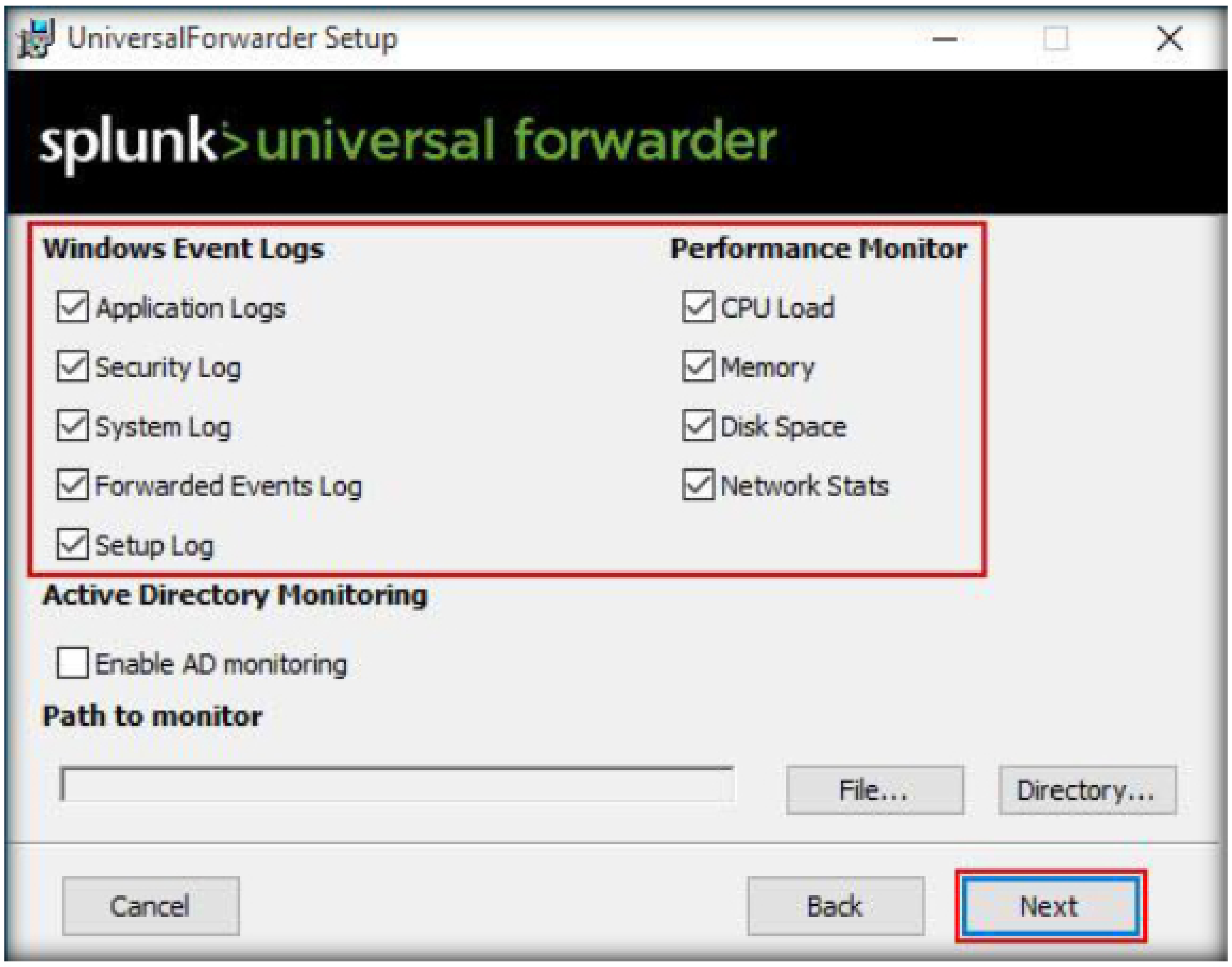
Installs UniversalForwarder using local system account. UniversalForwarder can access all data on or forwarded to this machine. It cannot access data remotely.

○ Domain Account

Installs UniversalForwarder with domain account you provide. This lets you collect logs and metrics from remote machines as well as local and forwarded data. You can set the account in the next dialog, as a local administrator or a reduced privil...

FIGURE 6.10: Installing Splunk Forwarder as a Local System

15. Next , check all the entities under **Windows Event Logs** and **Performance Monitor** and click **Next**.



UniversalForwarder Setup

splunk>universal forwarder

**Windows Event Logs**

☑ Application Logs
☑ Security Log
☑ System Log
☑ Forwarded Events Log
☑ Setup Log

**Performance Monitor**

☑ CPU Load
☑ Memory
☑ Disk Space
☑ Network Stats

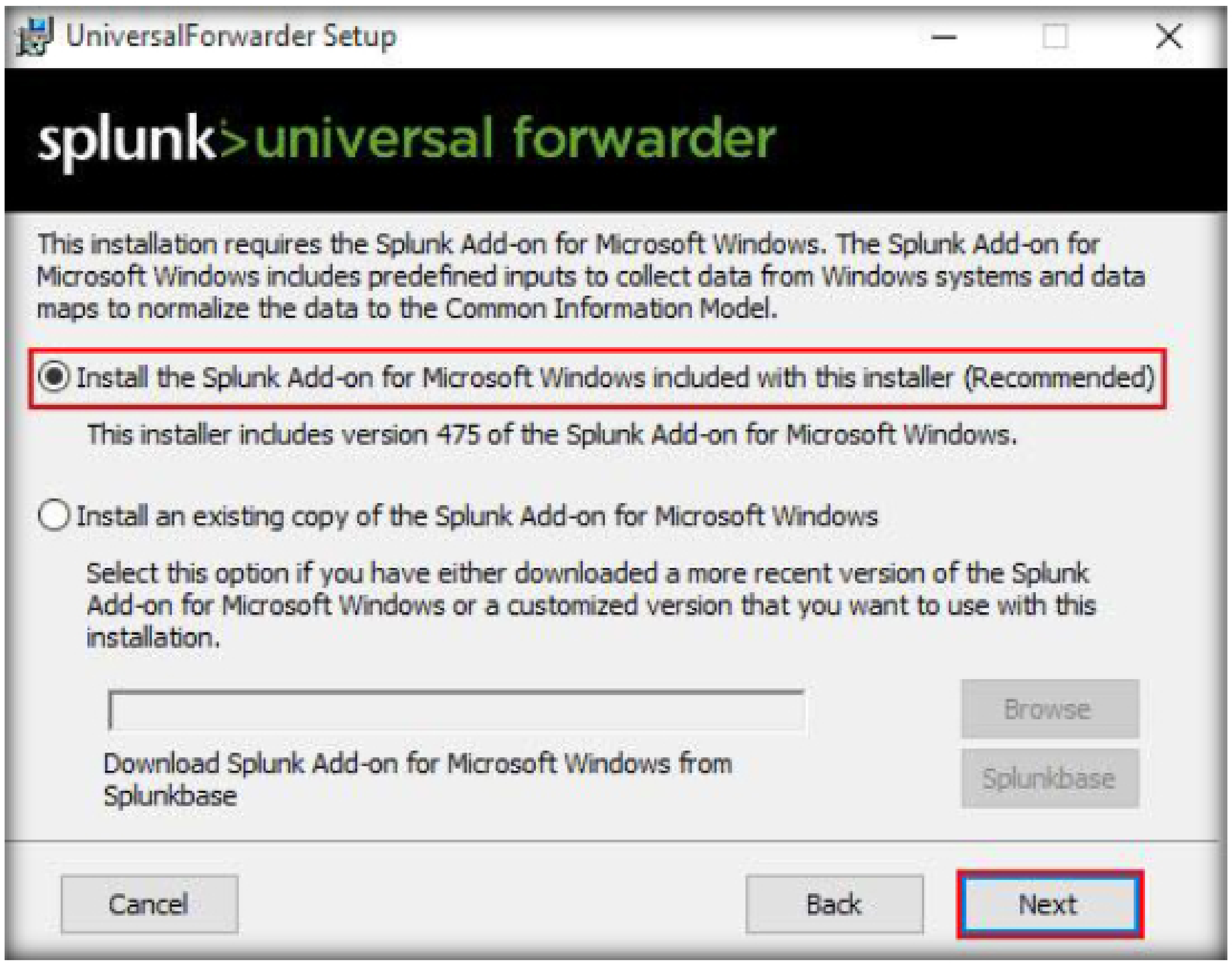
**Active Directory Monitoring**

□ Enable AD monitoring

**Path to monitor**

FIGURE 6.11: Selecting the events to forward

16. Select the **Install the Splunk Add-on for Microsoft Windows included with the installer (Recommended)** radio button and click **Next**. This installs the Splunk Add-on for Microsoft Windows along with the installer.



This installation requires the Splunk Add-on for Microsoft Windows. The Splunk Add-on for Microsoft Windows indudes predefined inputs to collect data from Windows systems and data maps to normalize the data to the Common Information Model.

● Install the Splunk Add-on for Microsoft Windows induded with this installer (Recommended)

This installer indudes version 475 of the Splunk Add-on for Microsoft Windows.

○ Install an existing copy of the Splunk Add-on for Microsoft Windows

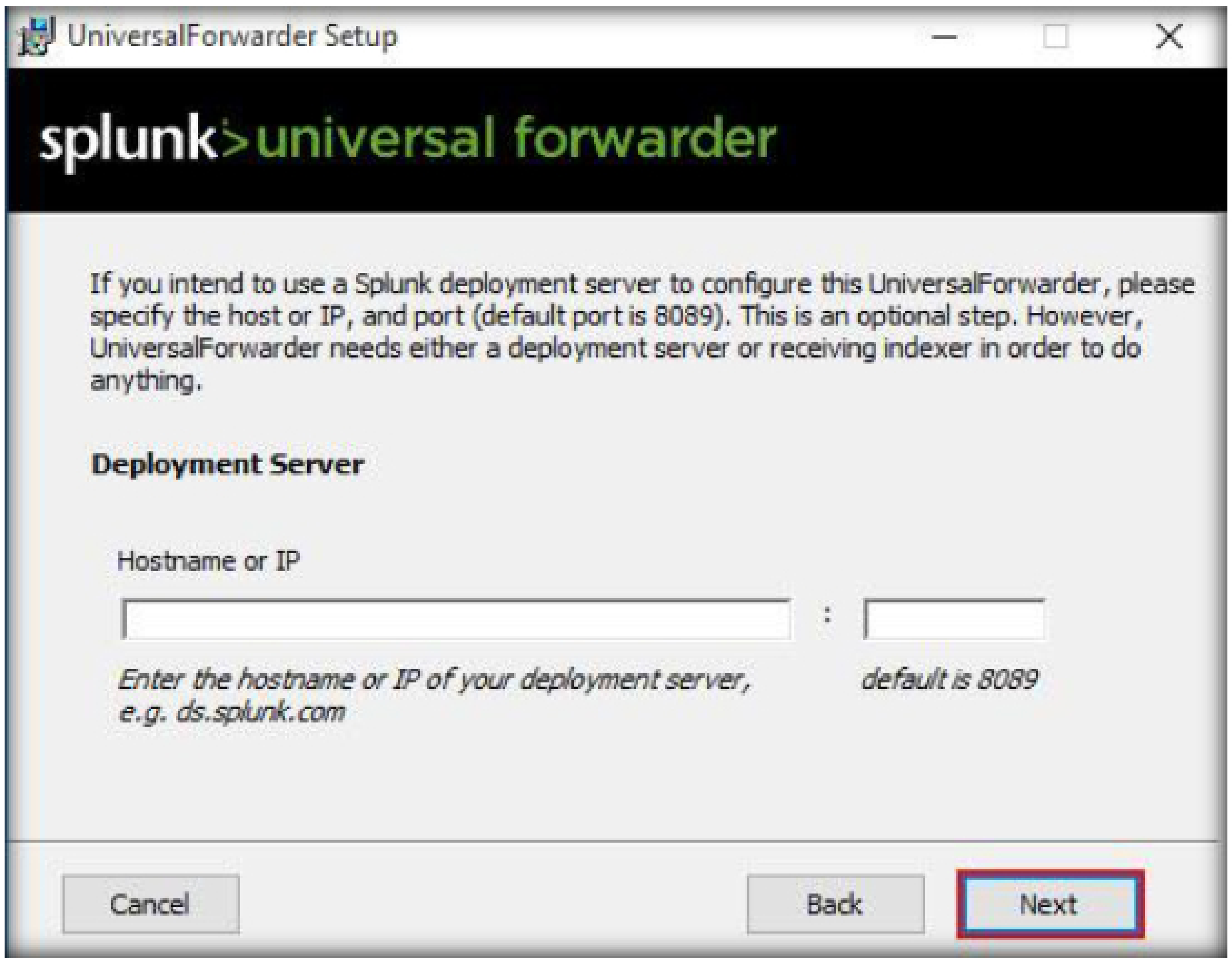
Select this option if you have either downloaded a more recent version of the Splunk Add-on for Microsoft Windows or a customized version that you want to use with this installation.

Download Splunk Add-on for Microsoft Windows from Splunkbase

FIGURE 6.12: Installing Microsoft Add on with Splunk forwarder

17. Leave the **Deployment Server** section without issuing the Deployment IP and port number details and click **Next**.

Visualizations make it easier to analyze and interact with data during investigations or within dashboards and reports. The right visual goes a long way to understanding the results of the analysis of your most complex data. With rich visualization you can easily find the right diagram to make your results known across your organization—in the boardroom or in the war room. Splunk base contains a wide array of Splunk-built visuals, and a development framework that makes it simple for customers and partners to create new visuals and make them



If you intend to use a Splunk deployment server to configure this UniversalForwarder, please specify the host or IP, and port (default port is 8089). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.

**Deployment Server**

Hostname or IP :

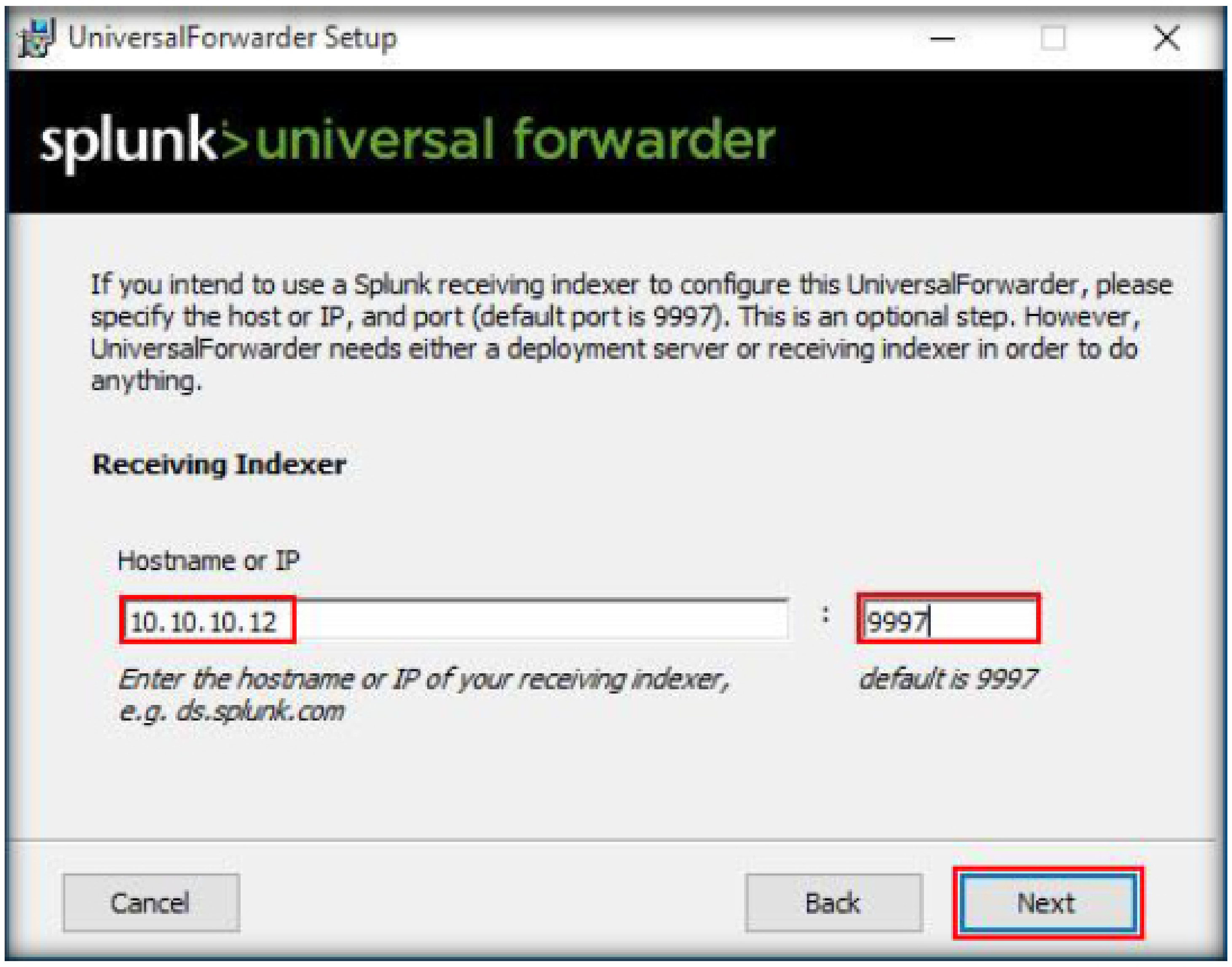
*Enter the hostname or IP of your deployment server, e.g. ds.splunk.com*

*default is 8089*

FIGURE 6.13: Splunk forwarder Deployment server

18. In the **Receiving Indexer** section, enter the IP address for Windows Server 2012 i.e., **10.10.10.12** in the **Hostname or IP** field, enter Port **9997** in the **port** field and click **Next**.

    **Note**: The IP address may vary if you used a different IP address at the time of lab setup.



If you intend to use a Splunk receiving indexer to configure this UniversalForwarder, please specify the host or IP, and port (default port is 9997). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.

**Receiving Indexer**

Hostname or IP: 10.10.10.12 : 9997

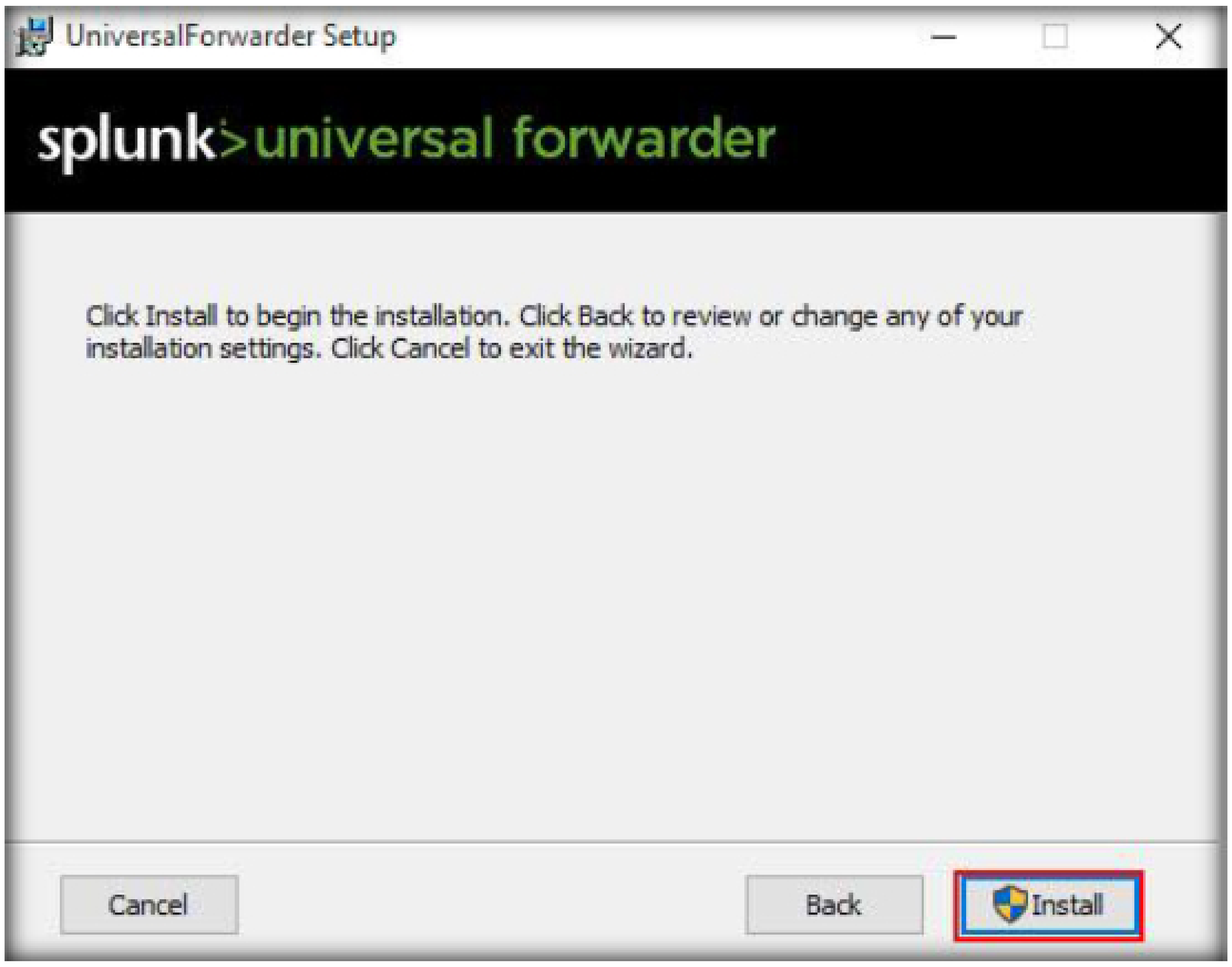
*Enter the hostname or IP of your receiving indexer, e.g. ds.splunk.com*

*default is 9997*

FIGURE 6.14: Setting values in Receiver

19. Once you are through with the configuration, click **Install**, while installing if a User Account Control pop-up appears, click **Yes**.

Expanded system monitoring, single sign-on options and role-based management increase operational efficiency, security and flexibility.



Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

FIGURE 6.15: Starting the installation of Splunk forwarder

20. Click the **Finish** button after the installation completes.

21. You have successfully configured the universal forwarder to forward all logs to the Splunk enterprise console deployed in the Windows Server 2012 machine through port 9997.

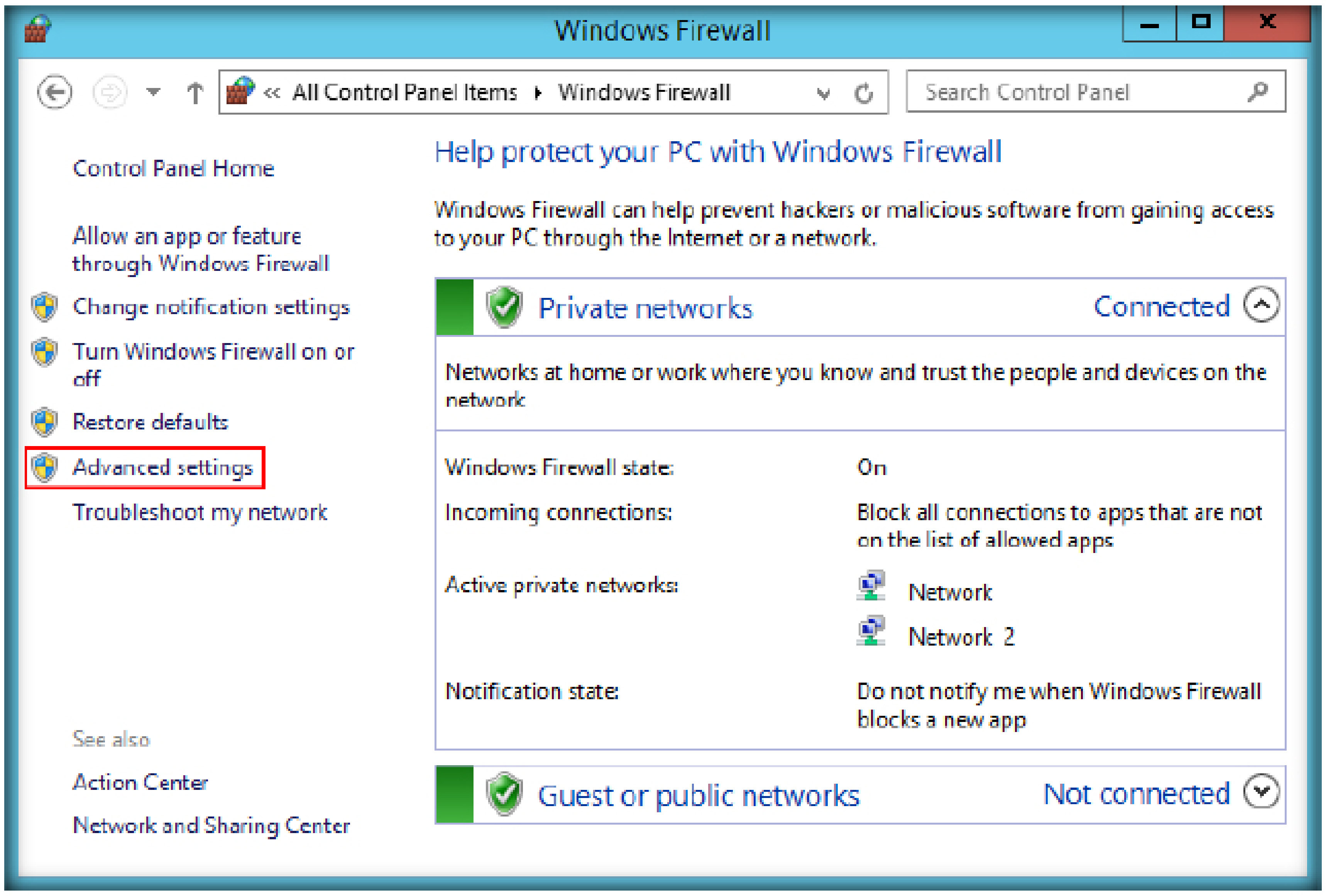
22. Windows Server 2012 has a firewall enabled, it blocks the traffic that is trying to enter the machine through port 9997.

23. To allow the traffic to enter the machine, you need to add a Windows Firewall Rule for port **9997**.

24. Switch back to the Windows Server 2012 virtual machine and close all the windows that are open and then launch the **Windows Firewall**.

25. In Windows Firewall window, click the **Advanced settings** link on the left-hand side of the window.

Windows Firewall with Advanced Security settings to create a new rule for Inbound traffic.


Windows Firewall
« All Control Panel Items ▸ Windows Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center

Help protect your PC with Windows Firewall

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

Private networks — Connected

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

Windows Firewall state: On

Incoming connections: Block all connections to apps that are not on the list of allowed apps

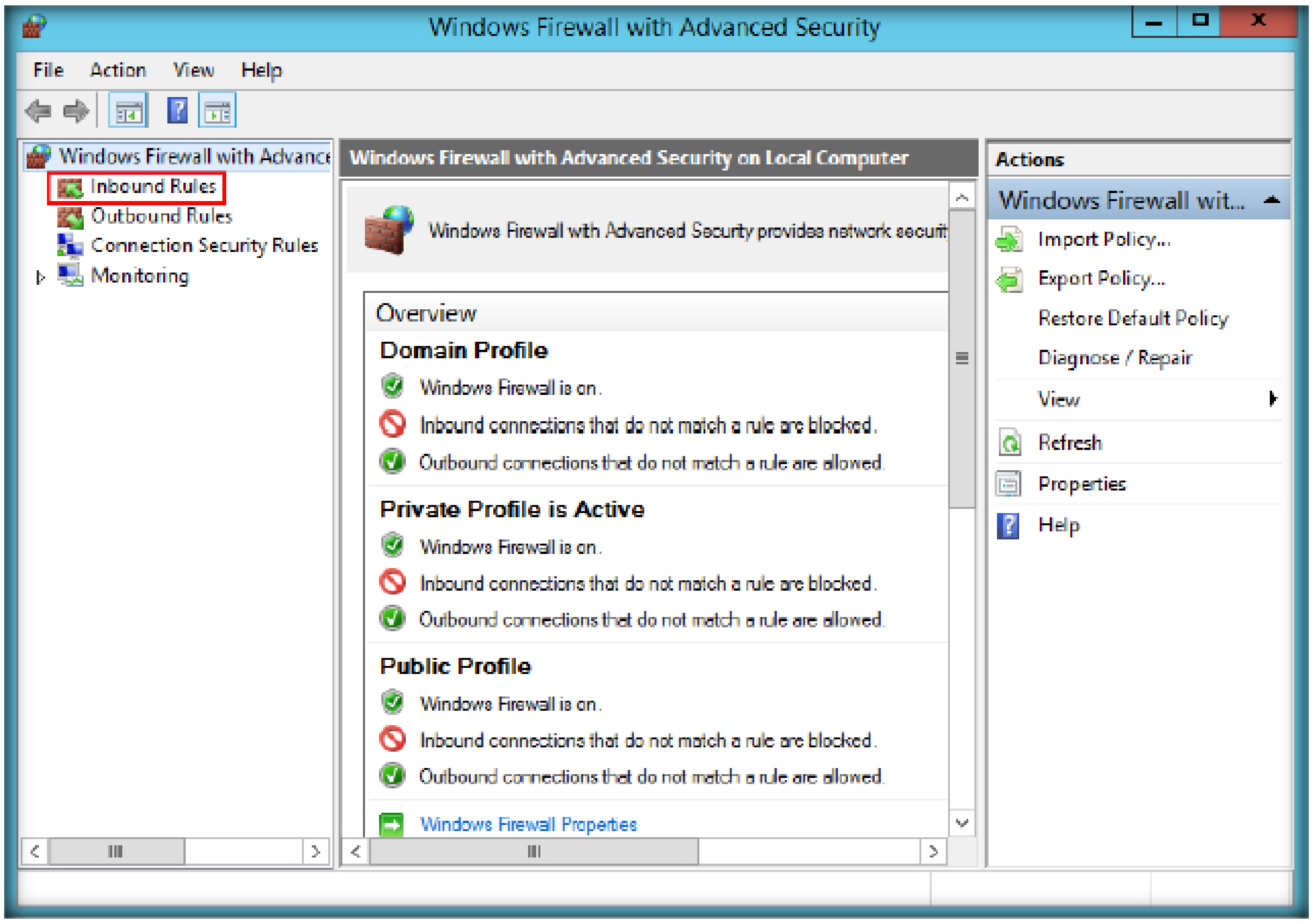
Active private networks: Network<br>Network 2

Notification state: Do not notify me when Windows Firewall blocks a new app

Guest or public networks — Not connected

FIGURE 6.16: Navigating to Windows Firewall Advanced settings

26. The **Windows Firewall with Advanced Security** control panel appears, select **Inbound Rules** from the left pane.



Windows Firewall with Advanced Security provides network securit

Overview

**Domain Profile**

- Windows Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

**Private Profile is Active**

- Windows Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

**Public Profile**

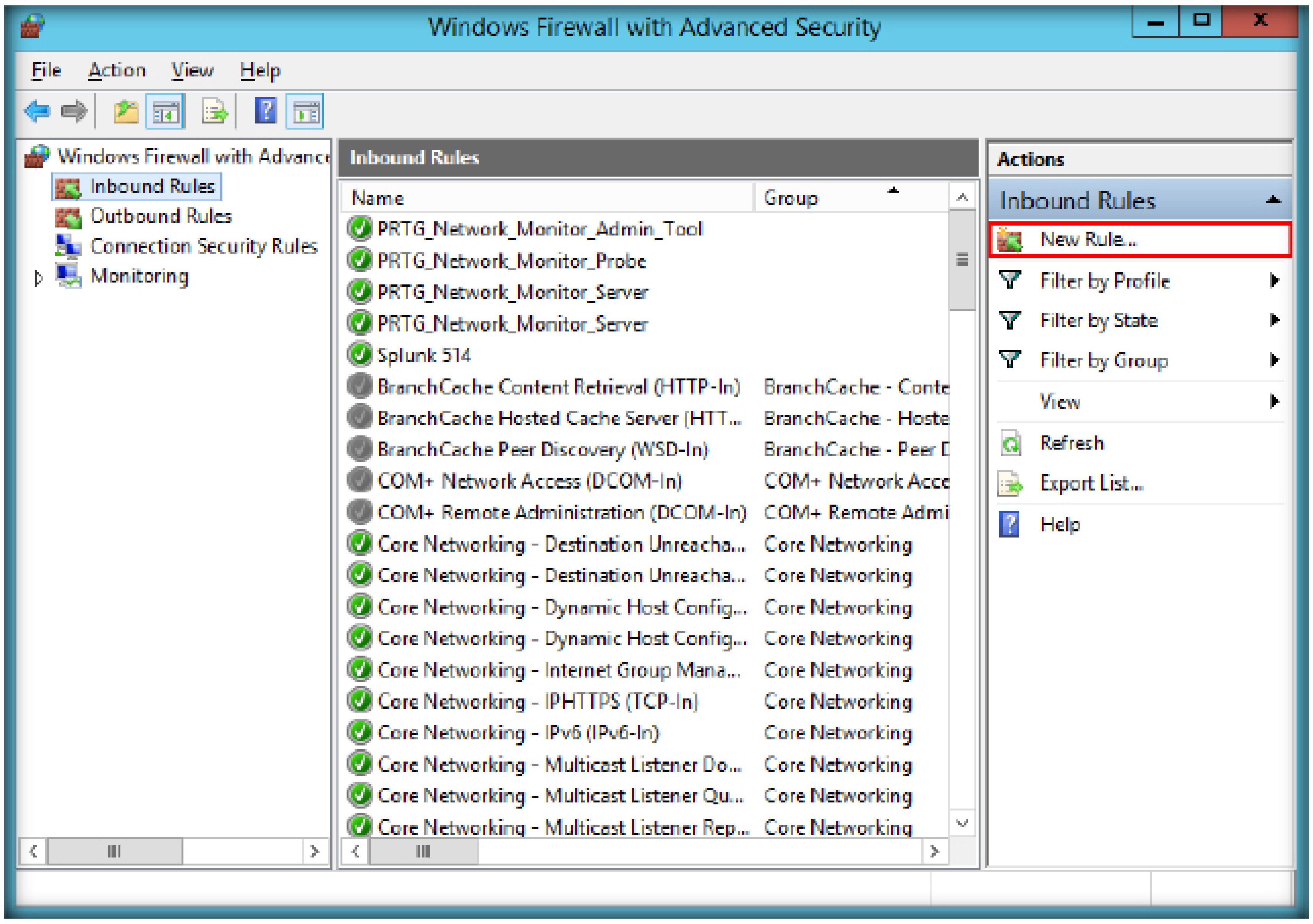
- Windows Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Windows Firewall Properties

FIGURE 6.17: Windows Firewall Advanced settings

Creating a New Rule for Inbound Traffic

27. Click **New Rule...** in the right pane to add a new inbound rule.

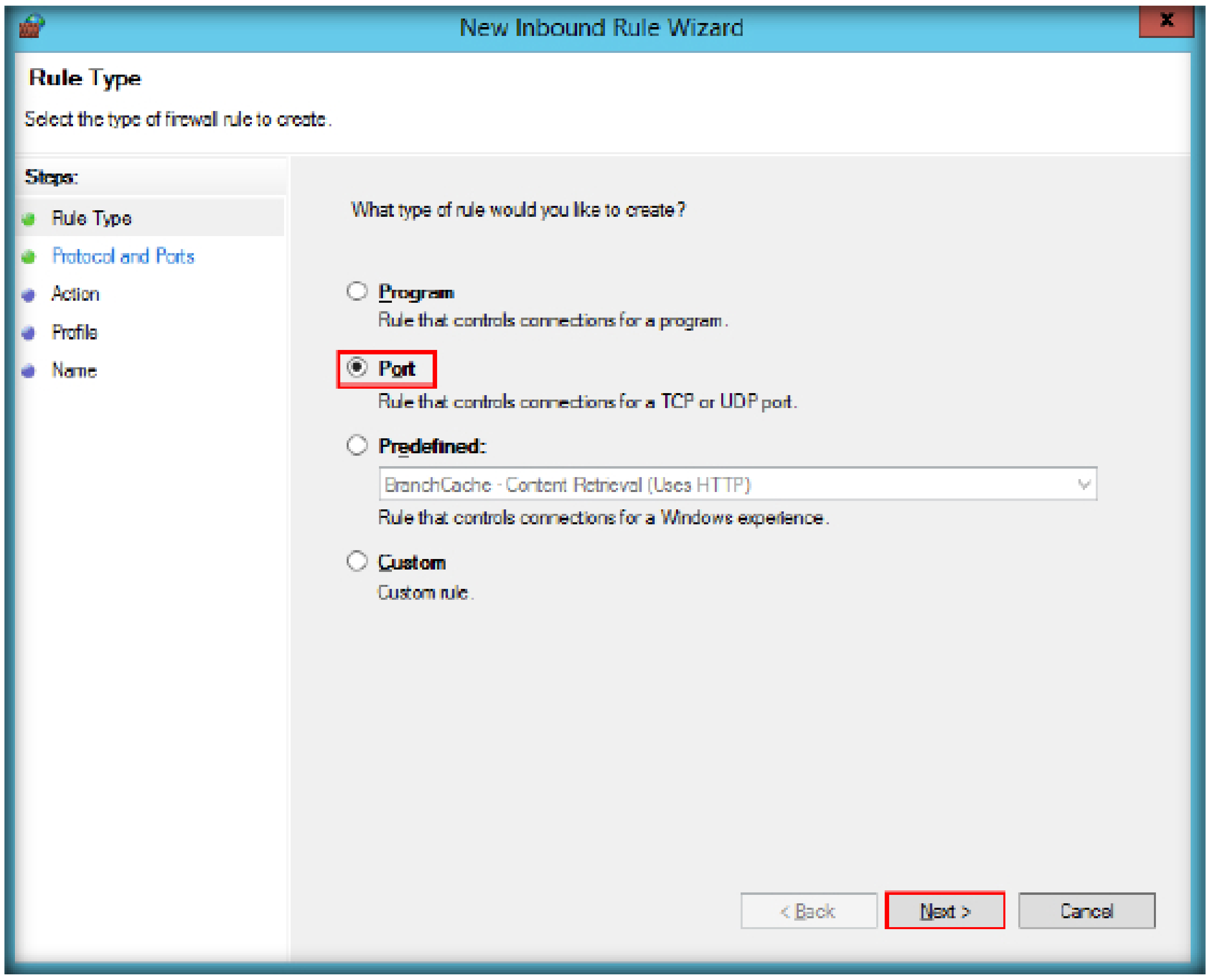


| Name | Group |
|---|---|
| PRTG_Network_Monitor_Admin_Tool | |
| PRTG_Network_Monitor_Probe | |
| PRTG_Network_Monitor_Server | |
| PRTG_Network_Monitor_Server | |
| Splunk 514 | |
| BranchCache Content Retrieval (HTTP-In) | BranchCache - Conte |
| BranchCache Hosted Cache Server (HTT... | BranchCache - Hoste |
| BranchCache Peer Discovery (WSD-In) | BranchCache - Peer D |
| COM+ Network Access (DCOM-In) | COM+ Network Acce |
| COM+ Remote Administration (DCOM-In) | COM+ Remote Admi |
| Core Networking - Destination Unreacha... | Core Networking |
| Core Networking - Destination Unreacha... | Core Networking |
| Core Networking - Dynamic Host Config... | Core Networking |
| Core Networking - Dynamic Host Config... | Core Networking |
| Core Networking - Internet Group Mana... | Core Networking |
| Core Networking - IPHTTPS (TCP-In) | Core Networking |
| Core Networking - IPv6 (IPv6-In) | Core Networking |
| Core Networking - Multicast Listener Do... | Core Networking |
| Core Networking - Multicast Listener Qu... | Core Networking |
| Core Networking - Multicast Listener Rep... | Core Networking |

FIGURE 6.18: Adding Inbound rule in Windows Firewall Advanced settings

Creating a Rule for a port in the Windows Firewall with Advanced Settings.

28. The **New Inbound Rule Wizard** appears, select the **Port** radio button in the **Rule Type** section and click **Next**.



New Inbound Rule Wizard

**Rule Type**

Select the type of firewall rule to create.

What type of rule would you like to create?

○ Program
Rule that controls connections for a program.

● Port
Rule that controls connections for a TCP or UDP port.

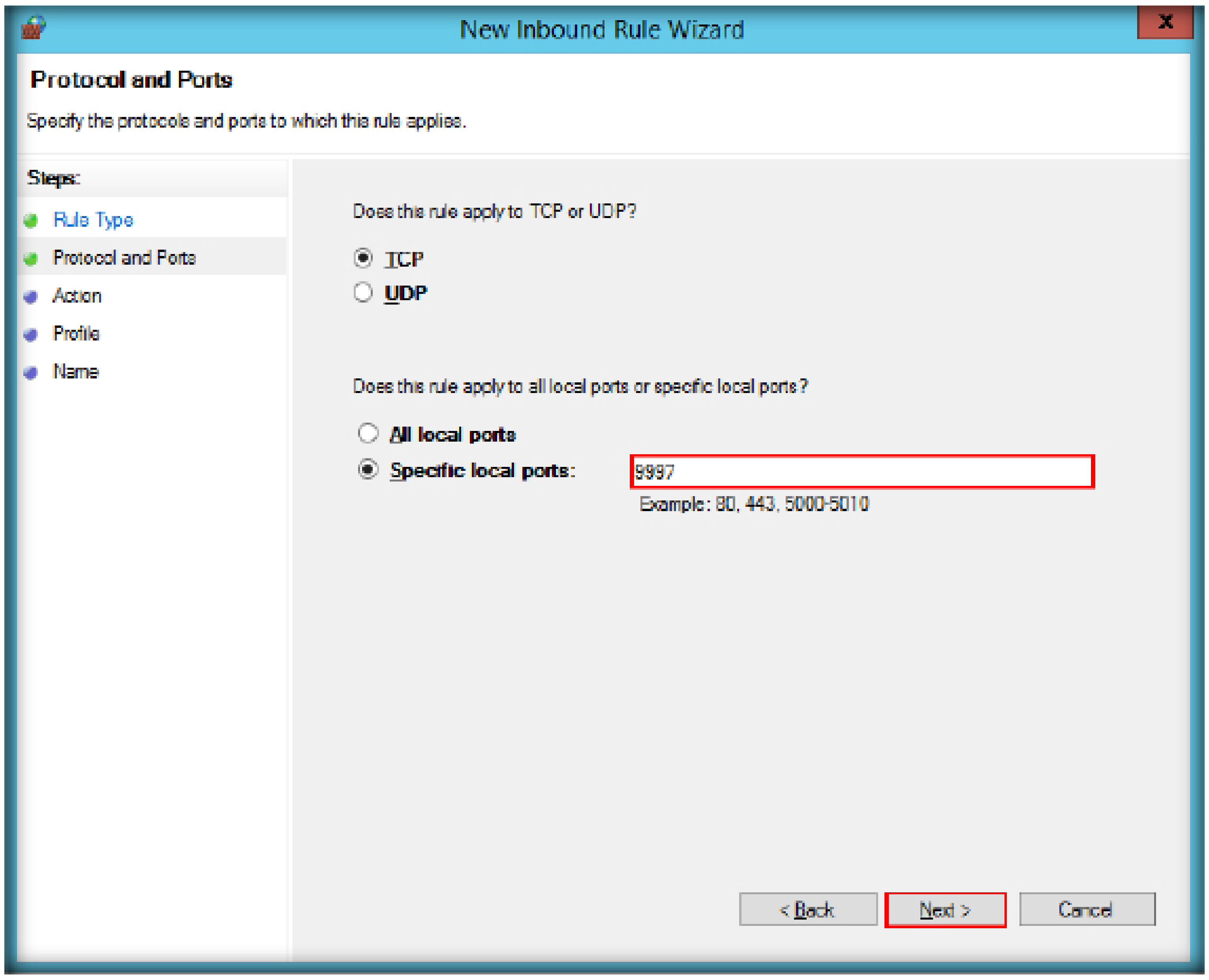
○ Predefined:
BranchCache - Content Retrieval (Uses HTTP)
Rule that controls connections for a Windows experience.

○ Custom
Custom rule.

FIGURE 6.19: Selecting a port

Assigning a Specific port in the Rule

29. The **Protocol and Ports** section appears, Specify port **9997** in the **Specific local port** field and click **Next**.



New Inbound Rule Wizard

**Protocol and Ports**

Specify the protocols and ports to which this rule applies.

Does this rule apply to TCP or UDP?

● TCP
○ UDP

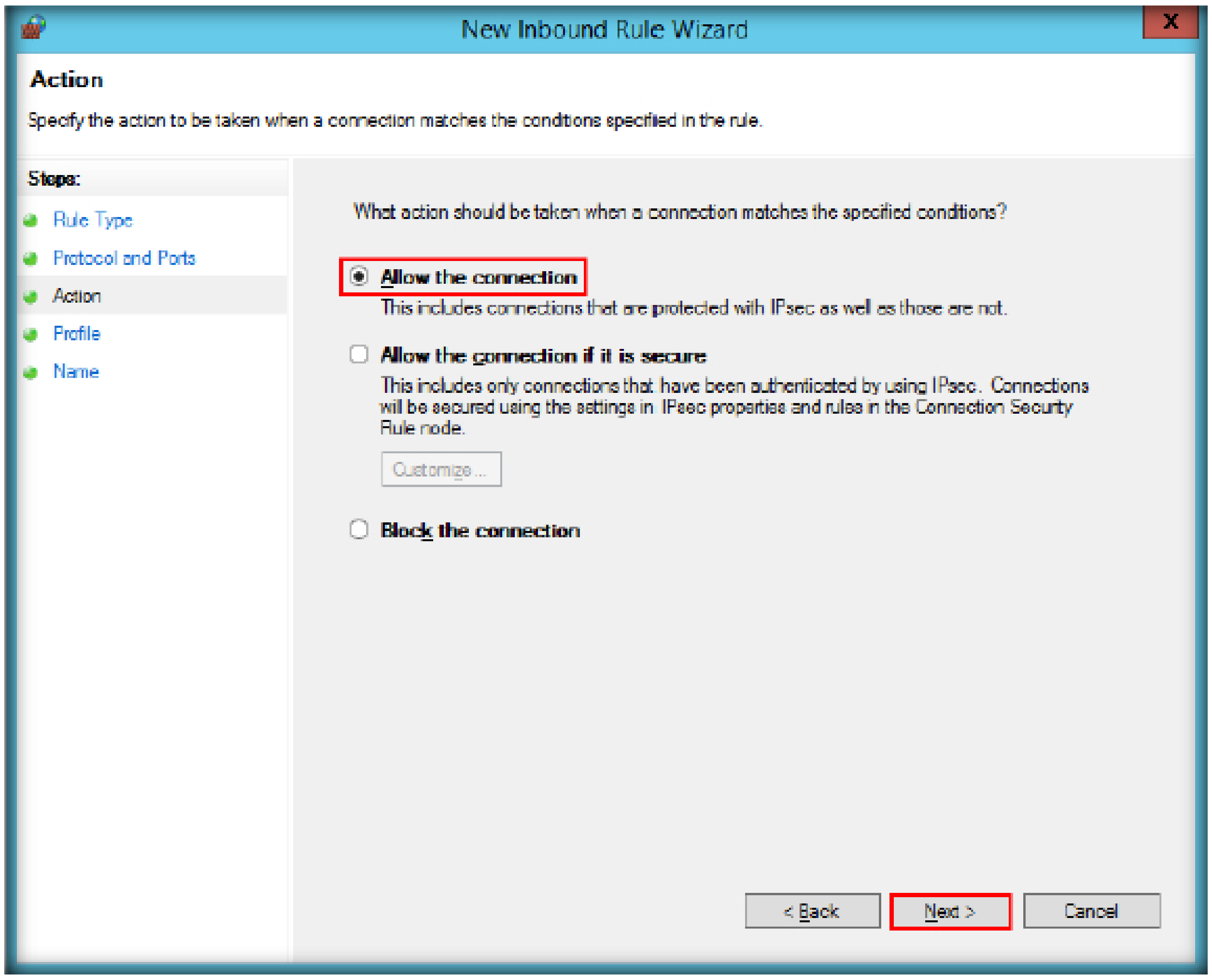
Does this rule apply to all local ports or specific local ports?

○ All local ports
● Specific local ports: 9997
Example: 80, 443, 5000-5010

FIGURE 6.20: Specifying the port number

30. The **Action** section of the wizard appears, select the **Allow the connection** radio button and click **Next**.

Assigning an Action for the newly created rule in the Windows Firewall with Advanced Settings wizard.



New Inbound Rule Wizard

**Action**

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

● **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

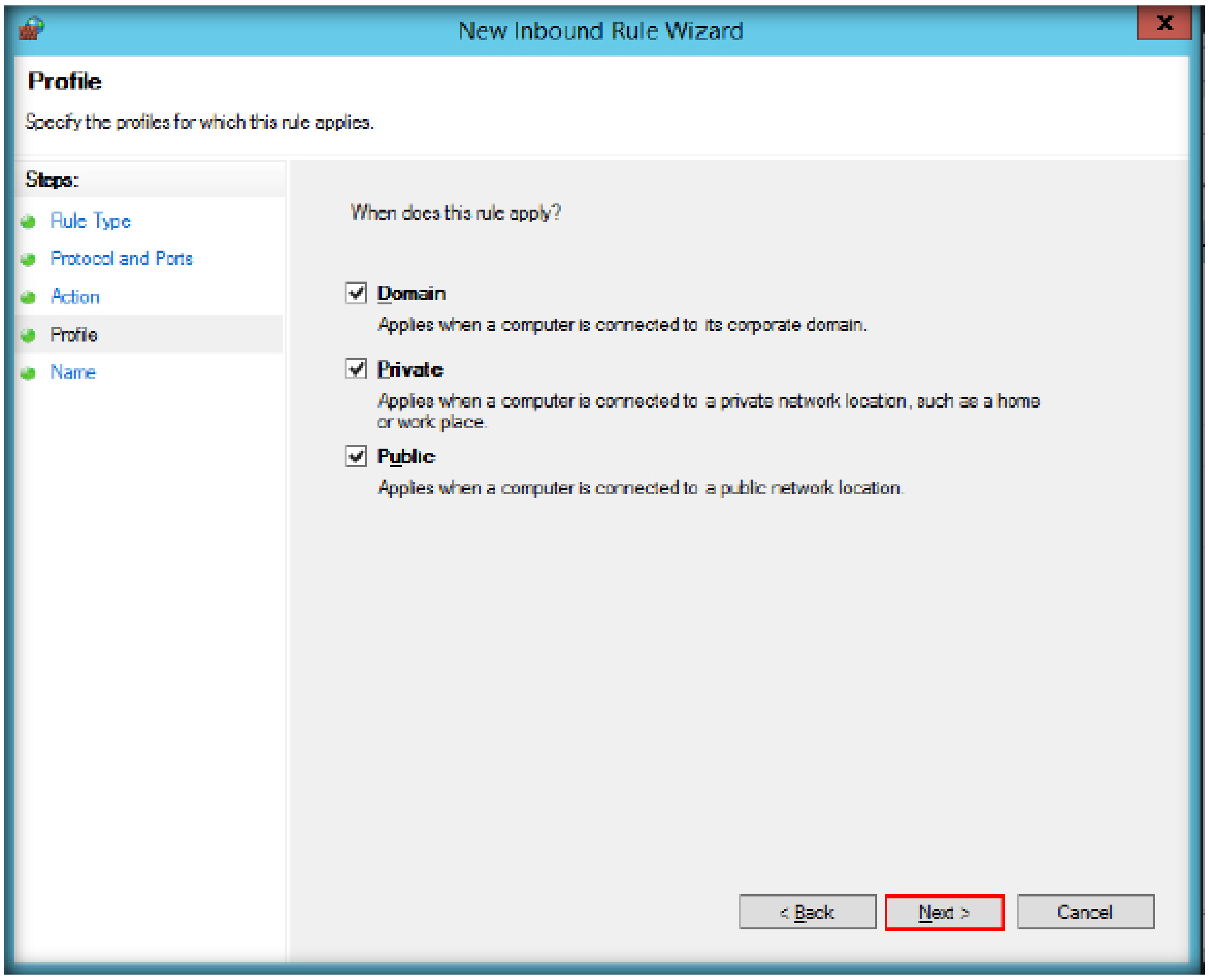
○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ **Block the connection**

FIGURE 6.21: Allowing the connection for the specified port

31. In the **Profile** section, leave the configuration set as default and click **Next**.

Applying a rule to the Profile for a machine



New Inbound Rule Wizard

**Profile**

Specify the profiles for which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

When does this rule apply?

☑ **Domain**
Applies when a computer is connected to its corporate domain.

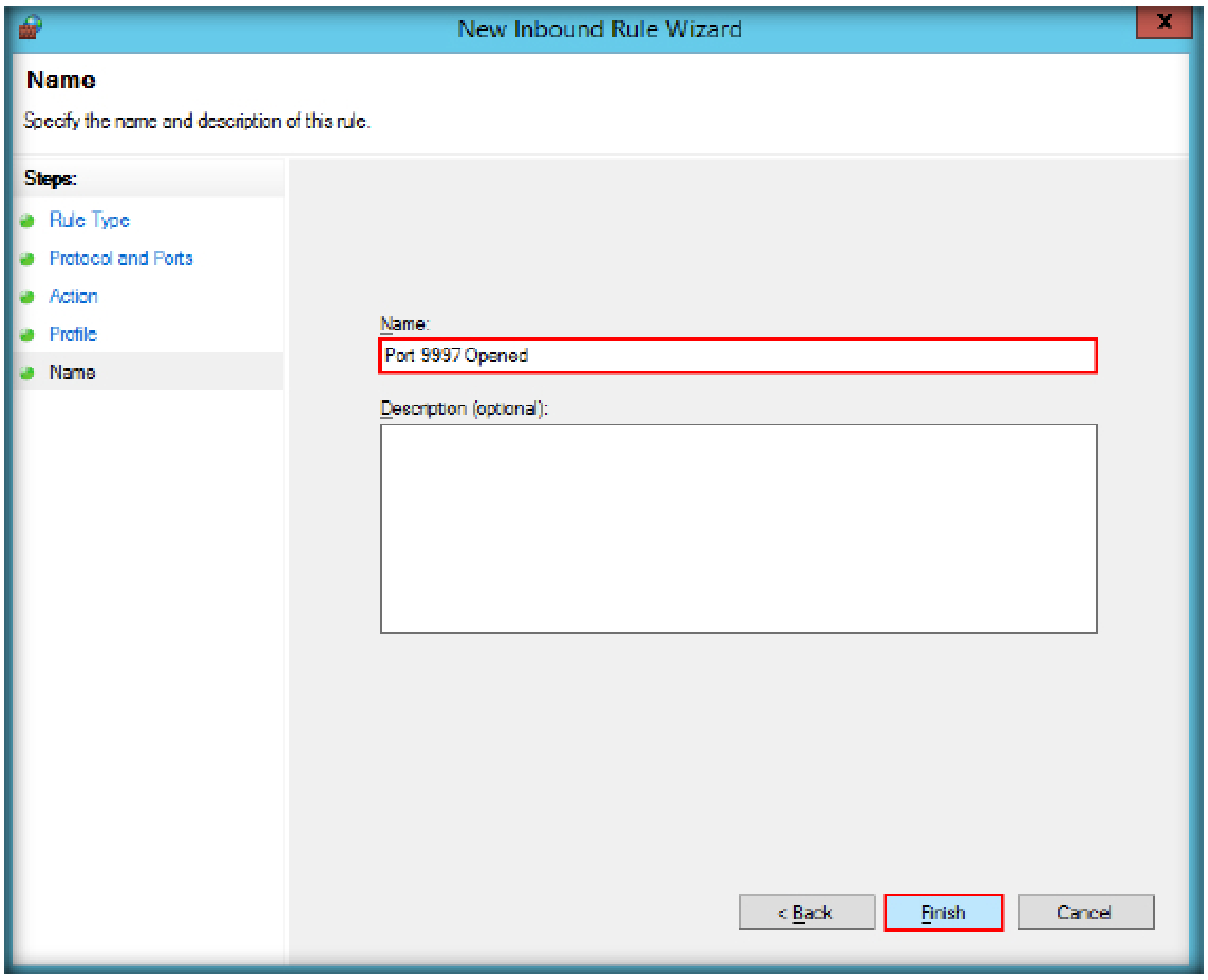
☑ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

☑ **Public**
Applies when a computer is connected to a public network location.

FIGURE 6.22: Selecting the profiles for the rule

32. The **Name** section of the wizard appears, type the **Rule** name as **Port 9997 Opened** in the **Name** field and click **Finish**.

Naming a Rule in Windows Firewall with Advanced Settings



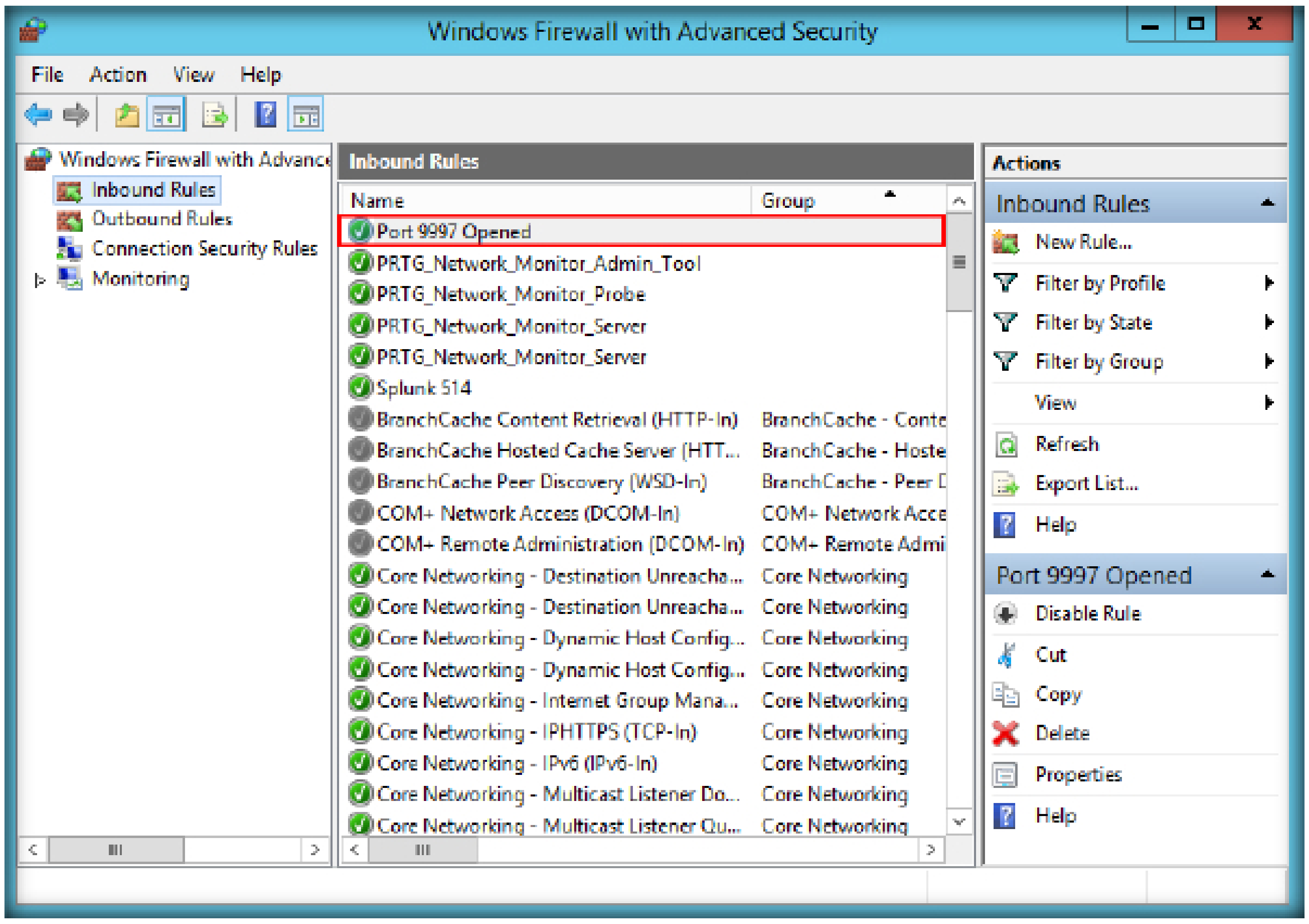
Name: Port 9997 Opened

FIGURE 6.23: Naming the rule

33. The new rule is now added to the firewall rules as shown in the following screenshot.

34. Next, **close** all the firewall windows after configuration completes.

Multi-site clustering and automatic load balancing scale to support hundreds of terabytes of data per day, optimize response times and provide continuous availability. Search Head Clustering provides support for a virtually unlimited number of concurrent users and searches. The High Performance Analytics Store and other acceleration technologies enable you to generate reports on big data at lightning fast speeds.



Inbound Rules

| Name | Group |
|---|---|
| Port 9997 Opened | |
| PRTG_Network_Monitor_Admin_Tool | |
| PRTG_Network_Monitor_Probe | |
| PRTG_Network_Monitor_Server | |
| PRTG_Network_Monitor_Server | |
| Splunk 514 | |
| BranchCache Content Retrieval (HTTP-In) | BranchCache - Conte |
| BranchCache Hosted Cache Server (HTT... | BranchCache - Hoste |
| BranchCache Peer Discovery (WSD-In) | BranchCache - Peer D |
| COM+ Network Access (DCOM-In) | COM+ Network Acce |
| COM+ Remote Administration (DCOM-In) | COM+ Remote Admi |
| Core Networking - Destination Unreacha... | Core Networking |
| Core Networking - Destination Unreacha... | Core Networking |
| Core Networking - Dynamic Host Config... | Core Networking |
| Core Networking - Dynamic Host Config... | Core Networking |
| Core Networking - Internet Group Mana... | Core Networking |
| Core Networking - IPHTTPS (TCP-In) | Core Networking |
| Core Networking - IPv6 (IPv6-In) | Core Networking |
| Core Networking - Multicast Listener Do... | Core Networking |
| Core Networking - Multicast Listener Qu... | Core Networking |

FIGURE 6.24: New rule created successfully

35. Now that a new firewall rule in Windows Server 2012 is configured and the Universal Forwarder in Windows 10 is set up, the next thing to do is configure Splunk enterprise in Windows Server 2012 to receive the traffic coming from the Windows 10 machine.

36. Open a web browser and type http://localhost:8000 in the address bar and press **Enter** then login with the Splunk credentials as shown in the screenshot.

    **Note**: In this lab we are using a Chrome browser. If you are using a different browser the screenshots may differ.

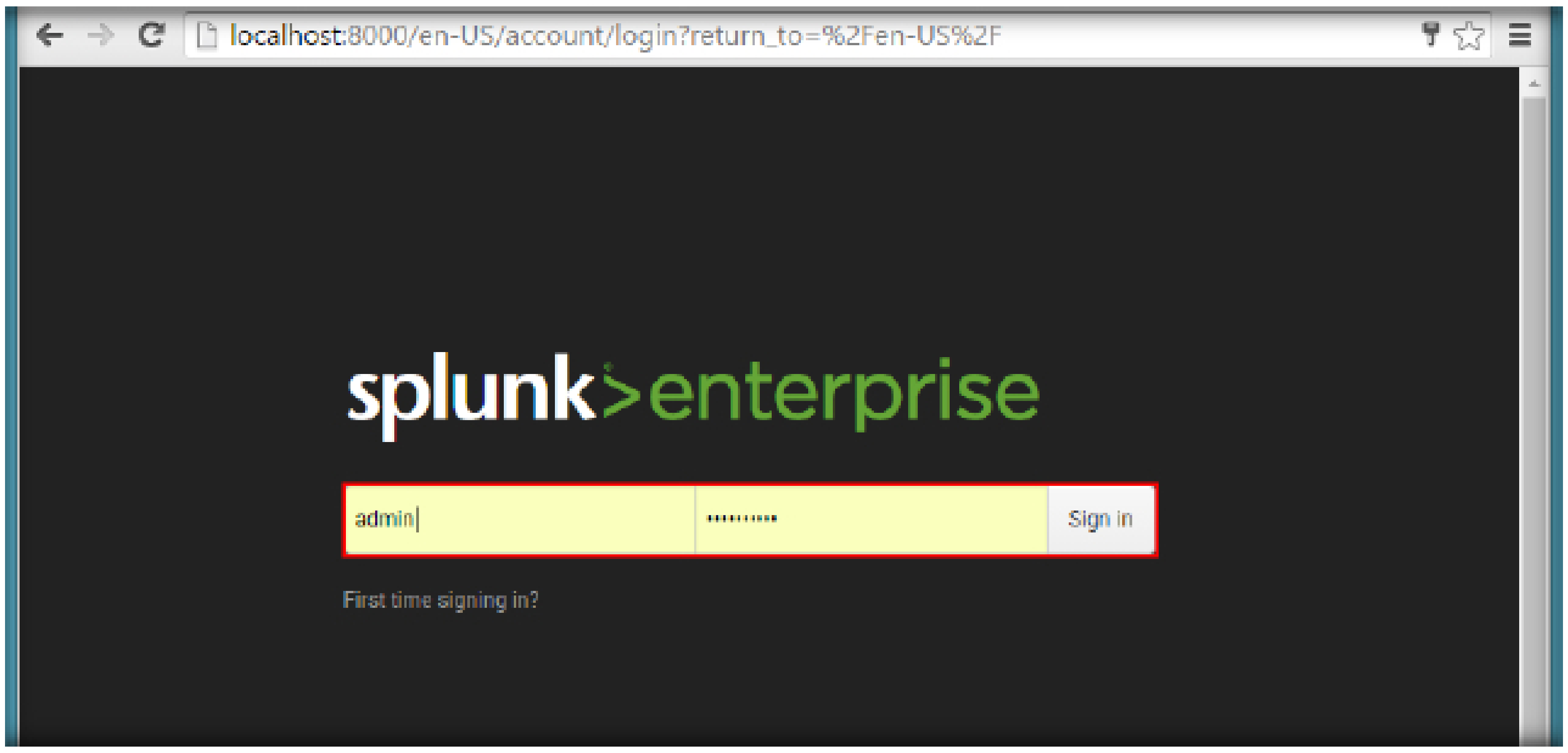


FIGURE 6.25: Logging in to Splunk

37. Splunk web console appears, click the **Forwarding and receiving** link under the **DATA** section in the **Settings** drop-down menu.

Apps deliver a user experience designed to make Splunk immediately useful and relevant for typical tasks and roles. Apps simplify and optimize user tasks, yet allow access to the data and functions of the full platform.

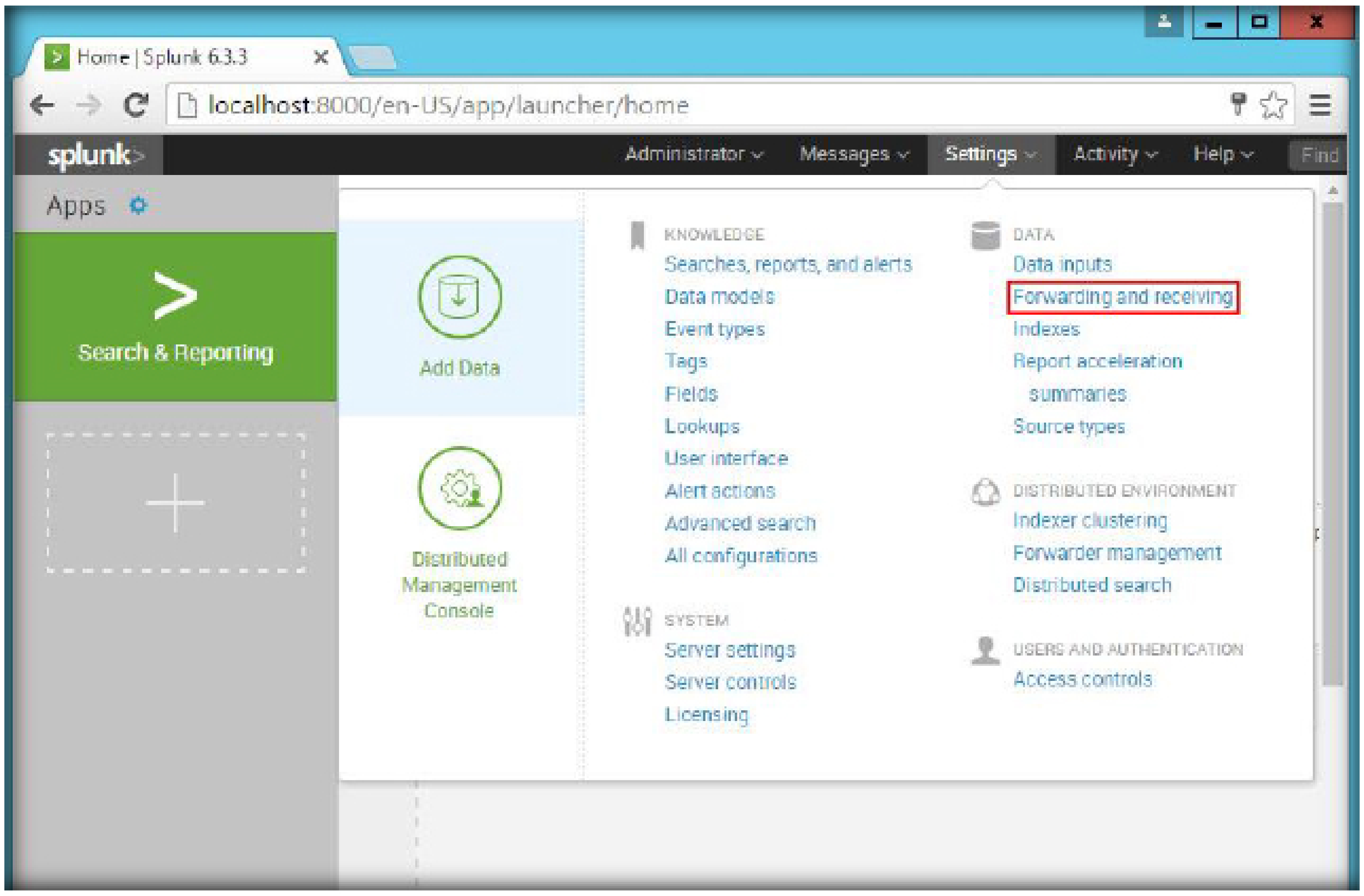
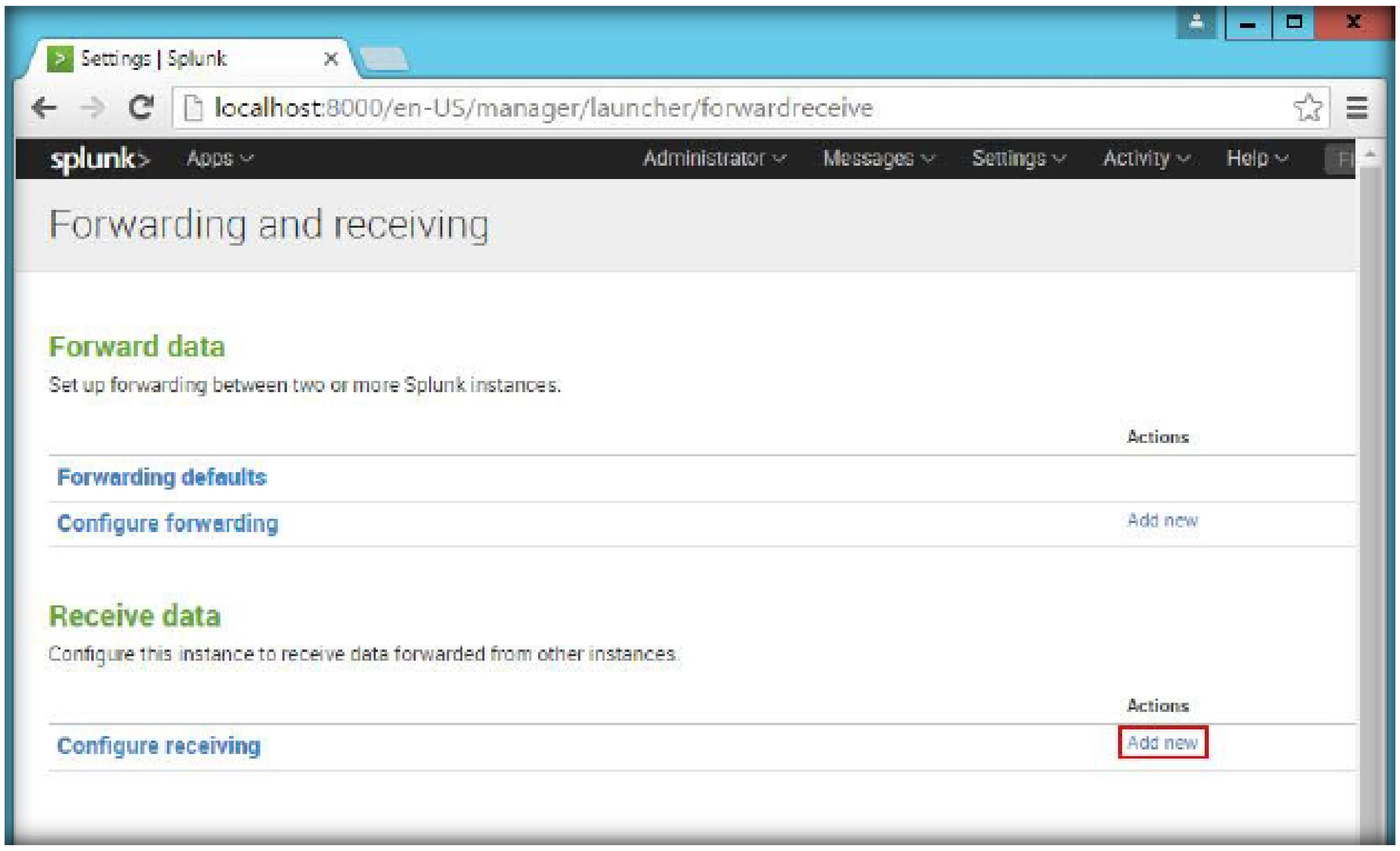


FIGURE 6.26: Navigating to Forwarding and receiving

38. The forwarding and receiving console appears. This is where a new instance will be added to receive the data forwarded from Universal Forwarder. Click **Add new** link for the **Configure receiving** field.

Whatever your need, these apps help you get powerful results right out of the box. Browse Splunk base to take advantage of the hundreds of apps and add-ons that you can immediately use with Splunk.



Forwarding and receiving

Forward data

Set up forwarding between two or more Splunk instances.

| | Actions |
|---|---|
| Forwarding defaults | |
| Configure forwarding | Add new |

Receive data

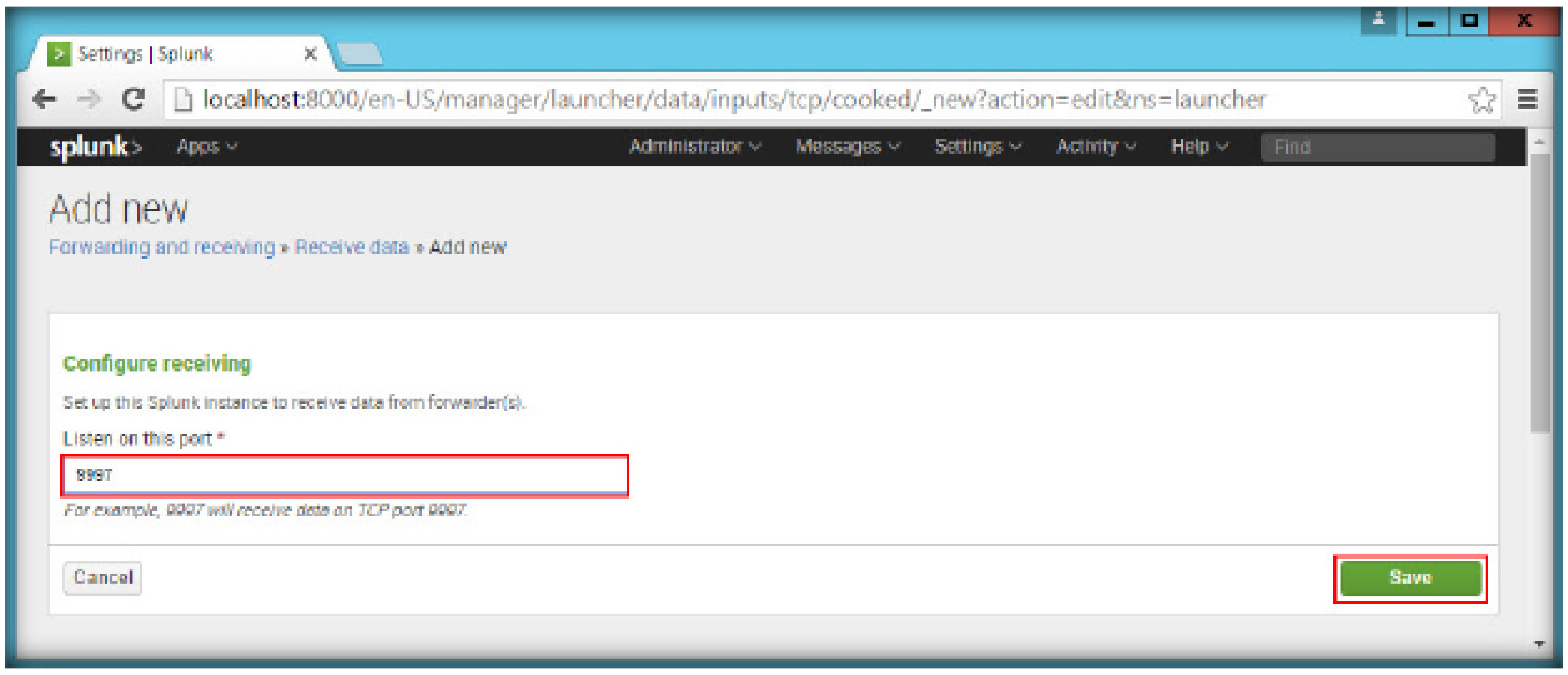
Configure this instance to receive data forwarded from other instances.

| | Actions |
|---|---|
| Configure receiving | Add new |

FIGURE 6.27: Configuring receiving settings

39. The Add new console appears, enter port **9997** in the Listen on this port field and click **Save**.

The Splunk platform imports and indexes virtually any machine data and provides powerful search and analysis features that deliver immediate value to your business. We also offer hundreds of apps and add-ons that can enhance and extend the Splunk platform with ready-to-use functions ranging from optimized data collection to monitor security, IT management and more.


Settings | Splunk
localhost:8000/en-US/manager/launcher/data/inputs/tcp/cooked/_new?action=edit&ns=launcher
splunk>
Apps
Administrator
Messages
Settings
Activity
Help
Find
Cancel
Save

Add new

Forwarding and receiving » Receive data » Add new

Configure receiving

Set up this Splunk instance to receive data from forwarder(s).

Listen on this port *

9997

*For example, 9997 will receive data on TCP port 9997.*

FIGURE 6.28: Specifying receiver port number

40. Once the port is added, go to **Apps** and select **Manage Apps**.

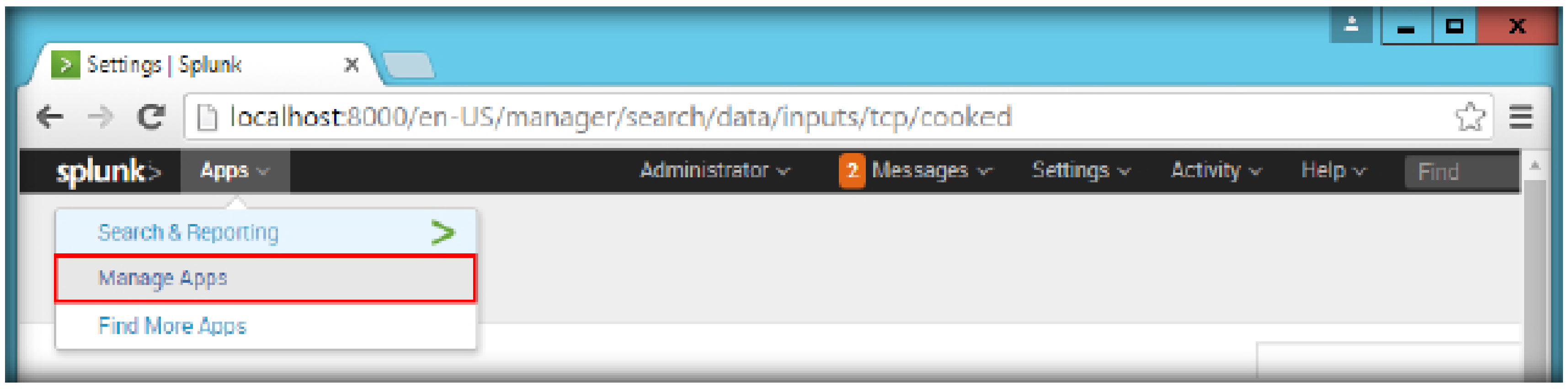
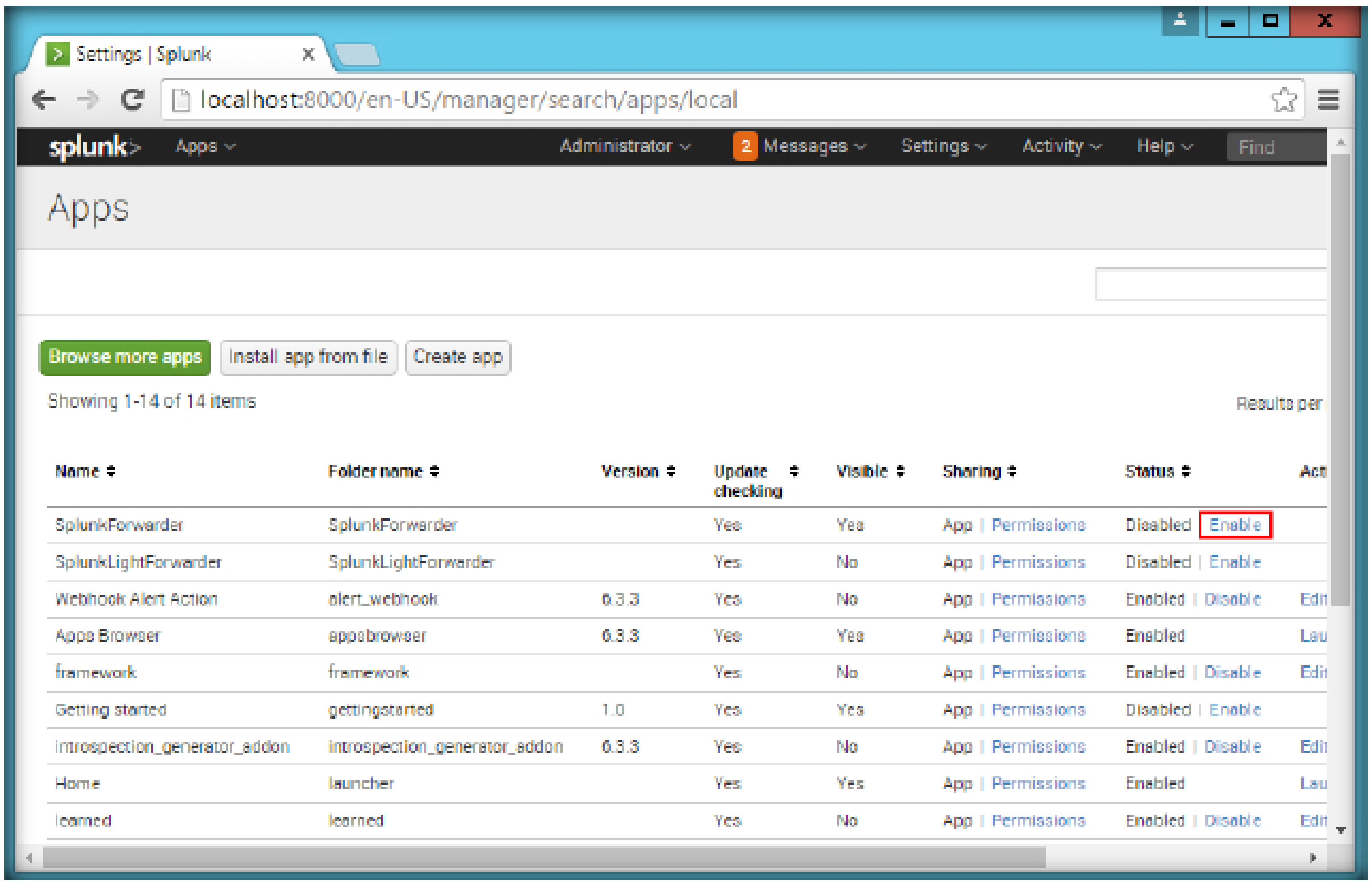


FIGURE 6.29: Navigating to apps

41. The Apps console appears, click the **Enable** link associated with the **SplunkForwarder** application.

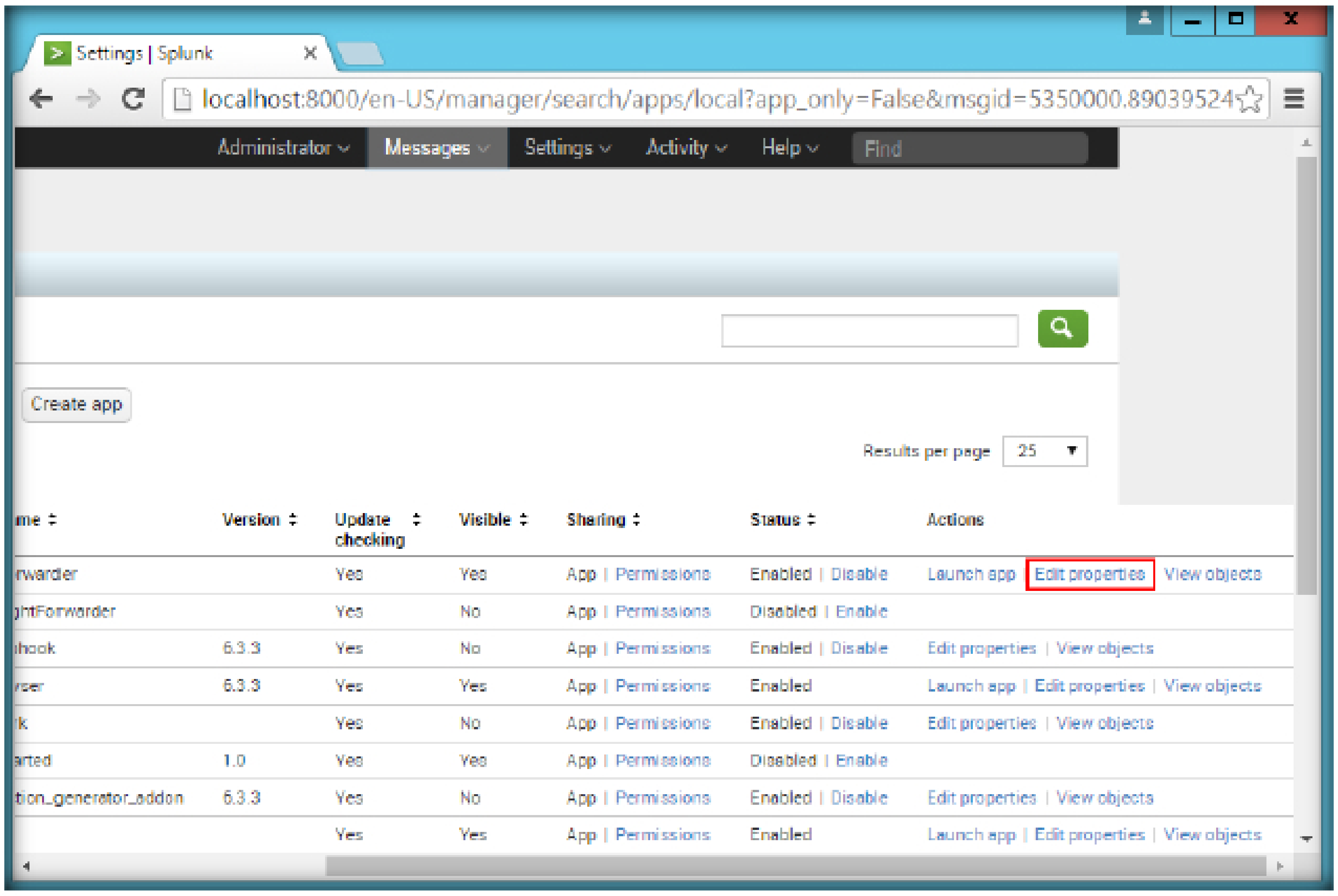


Showing 1-14 of 14 items

| Name | Folder name | Version | Update checking | Visible | Sharing | Status | Act |
|---|---|---|---|---|---|---|---|
| SplunkForwarder | SplunkForwarder | | Yes | Yes | App \| Permissions | Disabled Enable | |
| SplunkLightForwarder | SplunkLightForwarder | | Yes | No | App \| Permissions | Disabled \| Enable | |
| Webhook Alert Action | alert_webhook | 6.3.3 | Yes | No | App \| Permissions | Enabled \| Disable | Edit |
| Apps Browser | appsbrowser | 6.3.3 | Yes | Yes | App \| Permissions | Enabled | Lau |
| framework | framework | | Yes | No | App \| Permissions | Enabled \| Disable | Edit |
| Getting started | gettingstarted | 1.0 | Yes | Yes | App \| Permissions | Disabled \| Enable | |
| introspection_generator_addon | introspection_generator_addon | 6.3.3 | Yes | No | App \| Permissions | Enabled \| Disable | Edit |
| Home | launcher | | Yes | Yes | App \| Permissions | Enabled | Lau |
| learned | learned | | Yes | No | App \| Permissions | Enabled \| Disable | Edit |

FIGURE 6.30: Enabling the forwarder app

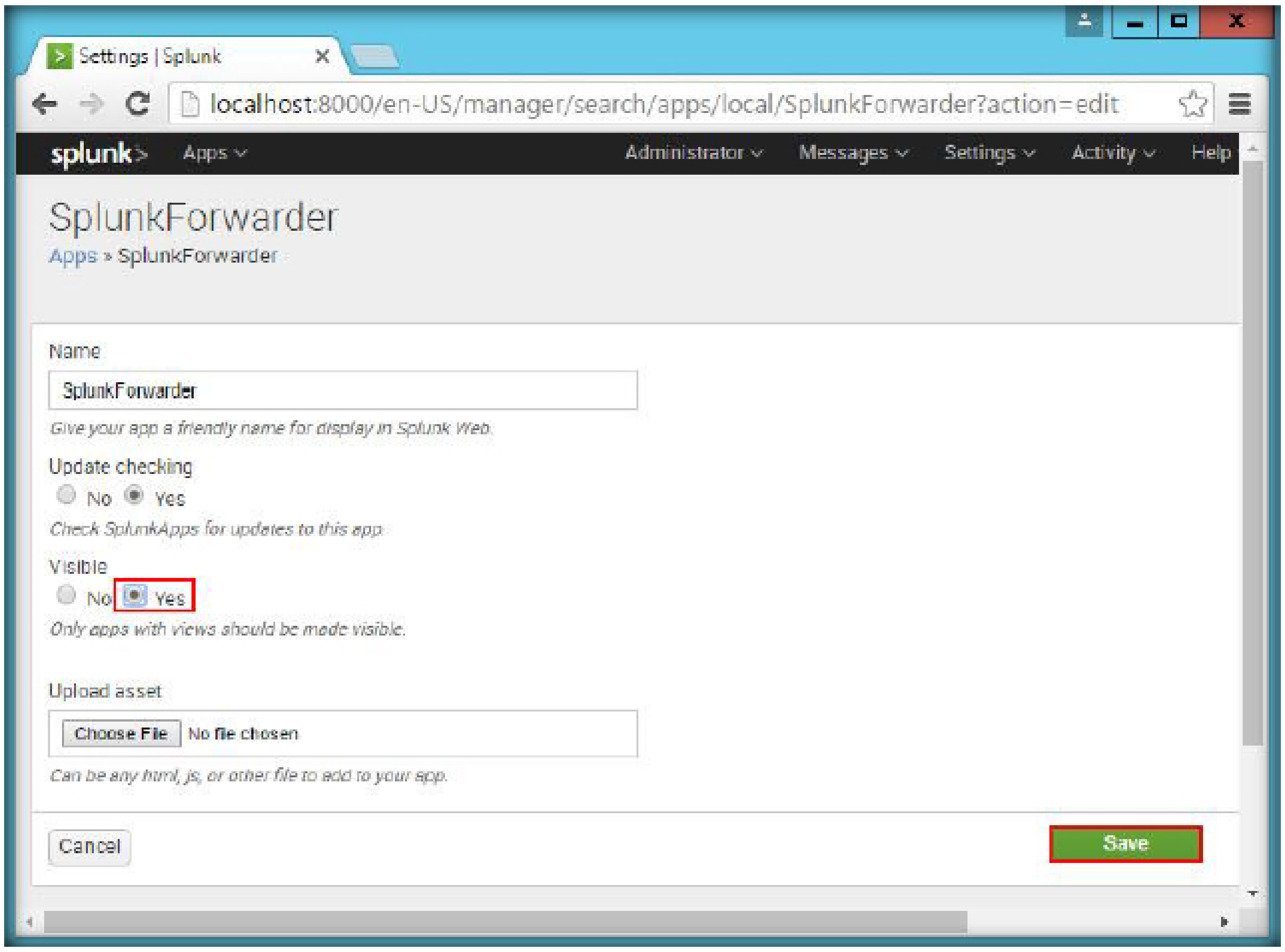
42. When the application is enabled, click the **Edit Properties** link.



| me | Version | Update checking | Visible | Sharing | Status | Actions |
|---|---|---|---|---|---|---|
| rwarder | | Yes | Yes | App \| Permissions | Enabled \| Disable | Launch app \| Edit properties View objects |
| ghtForwarder | | Yes | No | App \| Permissions | Disabled \| Enable | |
| hook | 6.3.3 | Yes | No | App \| Permissions | Enabled \| Disable | Edit properties \| View objects |
| vser | 6.3.3 | Yes | Yes | App \| Permissions | Enabled | Launch app \| Edit properties \| View objects |
| k | | Yes | No | App \| Permissions | Enabled \| Disable | Edit properties \| View objects |
| arted | 1.0 | Yes | Yes | App \| Permissions | Disabled \| Enable | |
| tion_generator_addon | 6.3.3 | Yes | No | App \| Permissions | Enabled \| Disable | Edit properties \| View objects |
| | | Yes | Yes | App \| Permissions | Enabled | Launch app \| Edit properties \| View objects |

FIGURE 6.31: Editing Forwarder app properties

43. The **SplunkForwarder** console appears, click **Yes** under the **Visible** section then click **Save**.



localhost:8000/en-US/manager/search/apps/local/SplunkForwarder?action=edit

SplunkForwarder

Apps » SplunkForwarder

Name

SplunkForwarder

*Give your app a friendly name for display in Splunk Web.*

Update checking

○ No ● Yes

*Check SplunkApps for updates to this app.*

Visible

○ No ● Yes

*Only apps with views should be made visible.*

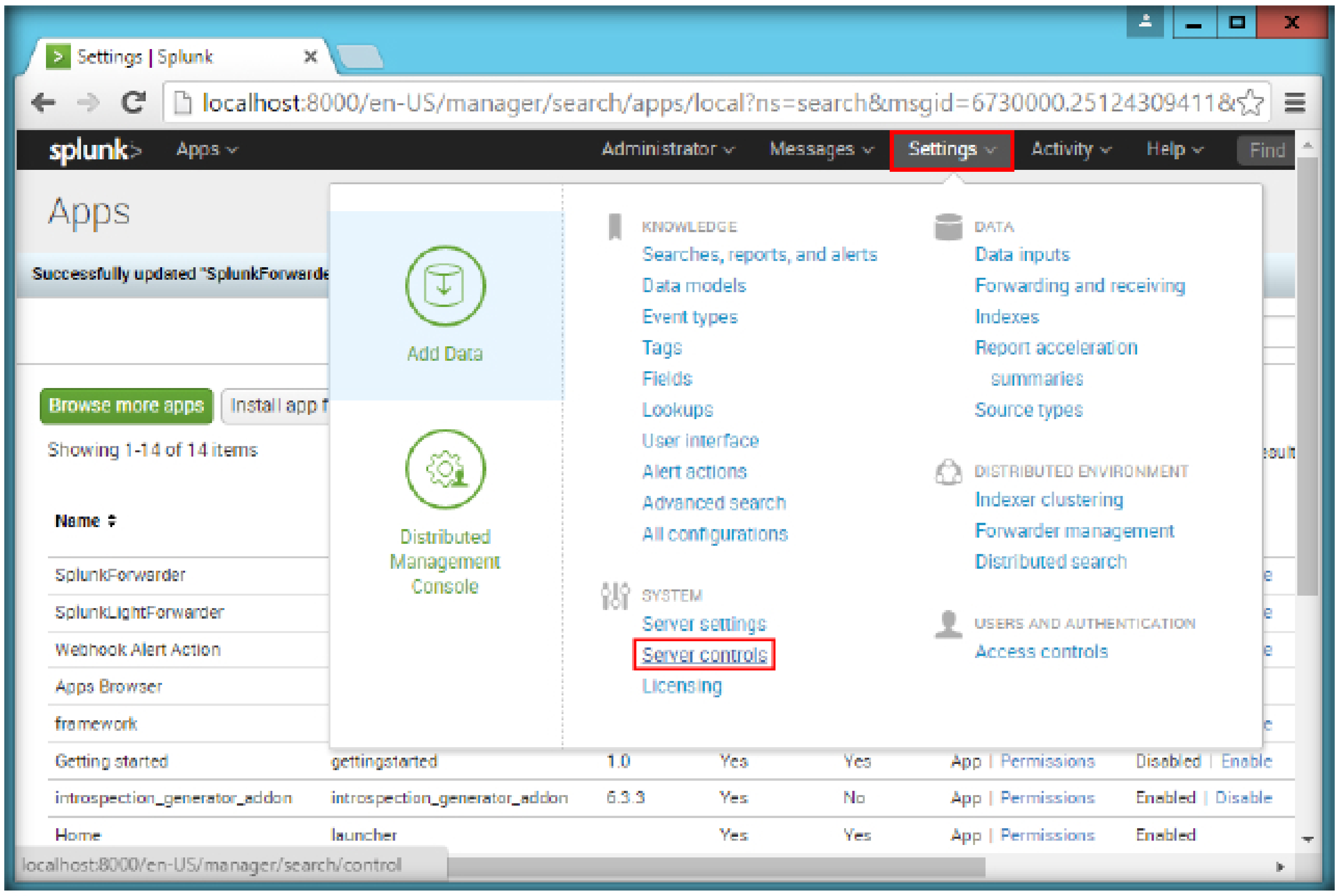
Upload asset

Choose File No file chosen

*Can be any html, js, or other file to add to your app.*

FIGURE 6.32: Making forwarder app visible

44. Go to **Settings** and select **Server controls** under the **SYSTEM** section.



localhost:8000/en-US/manager/search/apps/local?ns=search&msgid=6730000.25124309411&

Successfully updated "SplunkForwarde

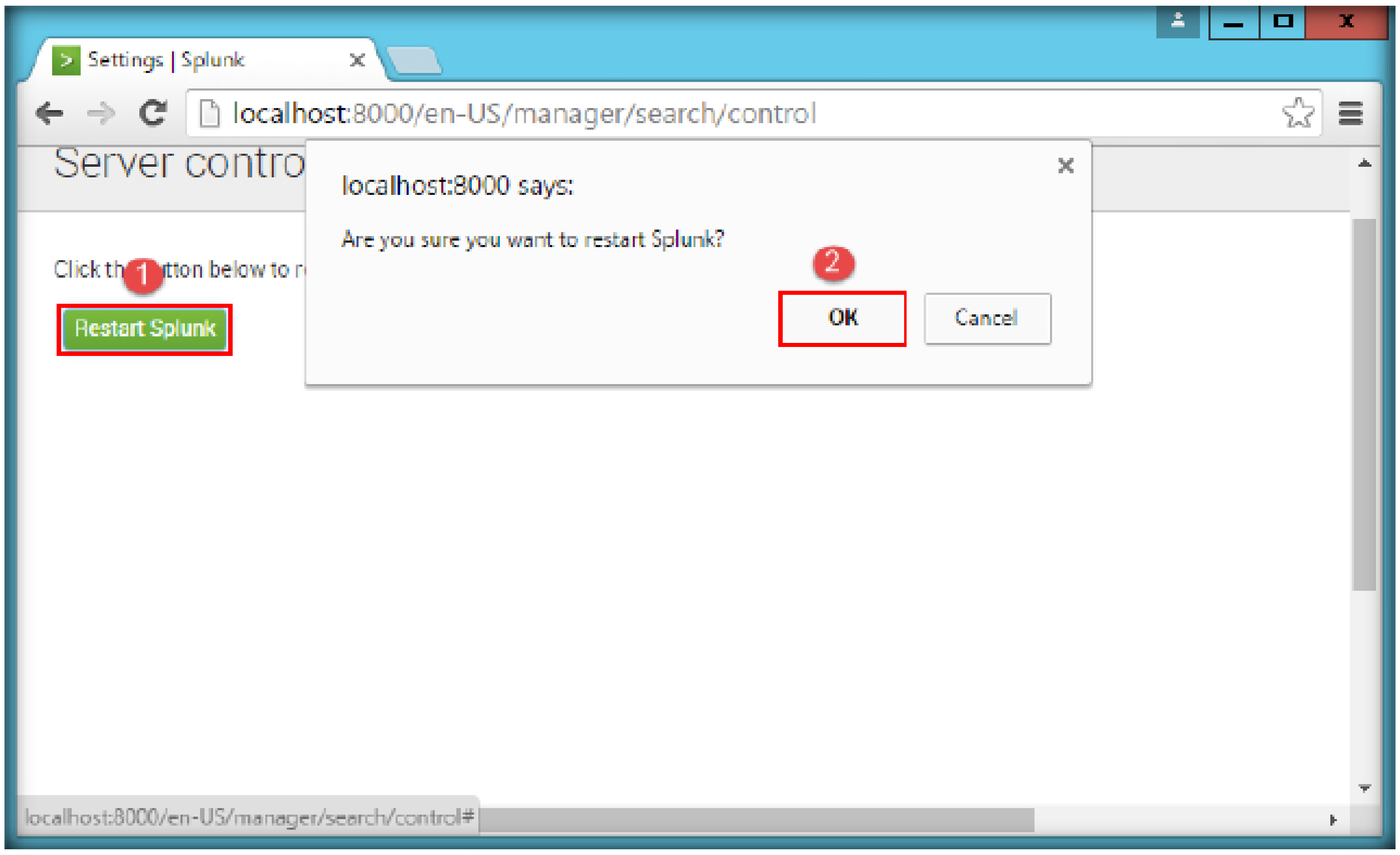
Showing 1-14 of 14 items

| Name ⇕ | | | | | | |
|---|---|---|---|---|---|---|
| SplunkForwarder | | | | | | |
| SplunkLightForwarder | | | | | | |
| Webhook Alert Action | | | | | | |
| Apps Browser | | | | | | |
| framework | | | | | | |
| Getting started | gettingstarted | 1.0 | Yes | Yes | App \| Permissions | Disabled \| Enable |
| introspection_generator_addon | introspection_generator_addon | 6.3.3 | Yes | No | App \| Permissions | Enabled \| Disable |
| Home | launcher | | Yes | Yes | App \| Permissions | Enabled |

localhost:8000/en-US/manager/search/control

FIGURE 6.33: Navigating to Server controls

45. The Server controls console appears, click **Restart Splunk**. A confirmation pop-up appears, click **OK**.


Settings | Splunk
localhost:8000/en-US/manager/search/control
Server contro
Click th  tton below to r
1
Restart Splunk
2
OK
Cancel
localhost:8000/en-US/manager/search/control#

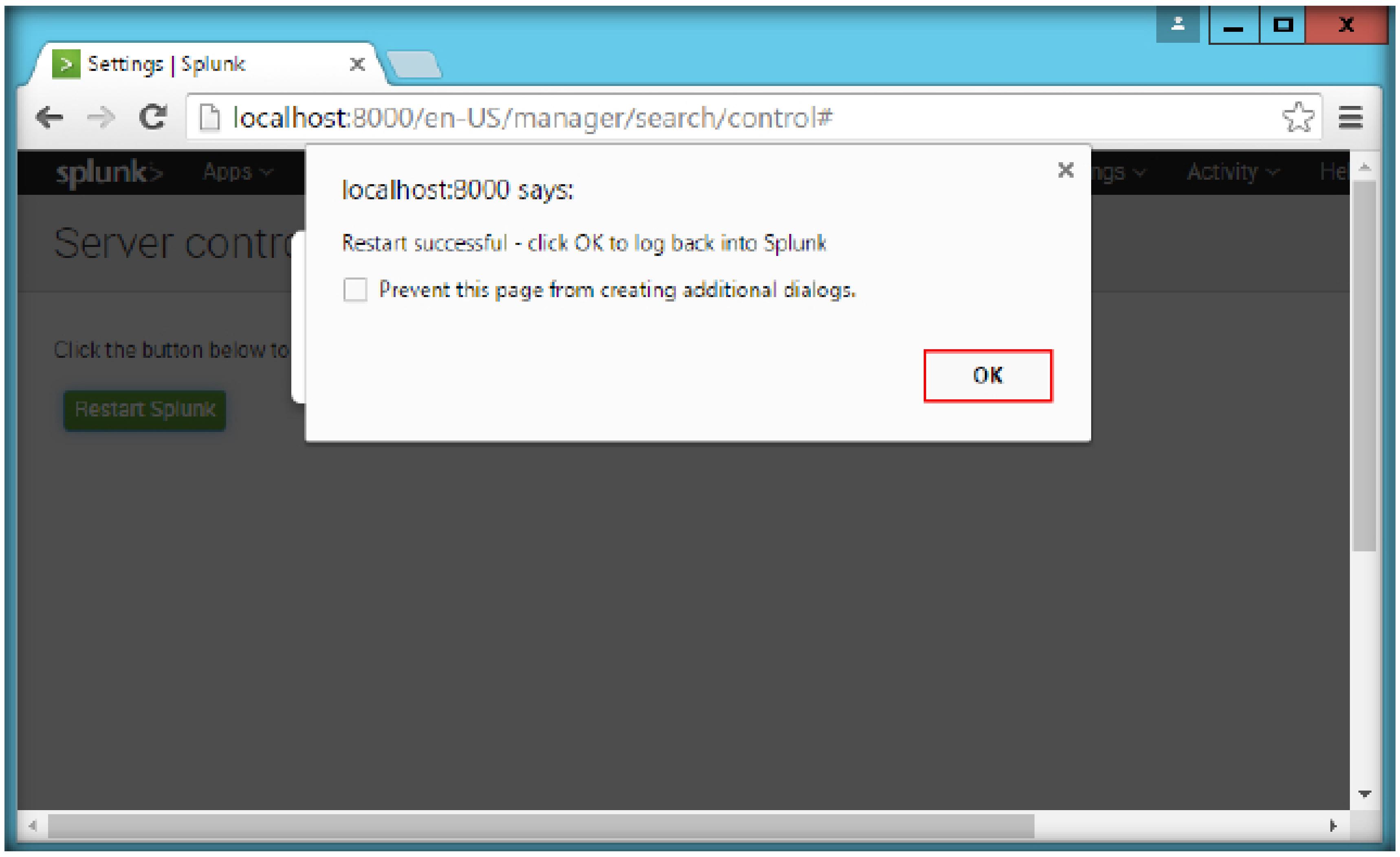
localhost:8000 says:

Are you sure you want to restart Splunk?

FIGURE 6.34: Restarting Splunk

The distributed management console provides enterprise-wide administration and maintains a complete, signed audit trail of administrative actions and

46. On a successful restart, a pop-up appears, click **OK**.


Settings | Splunk
localhost:8000/en-US/manager/search/control#
splunk>
Apps
ngs
Activity
He
Server contr
Click the button below to
Restart Splunk
OK

localhost:8000 says:

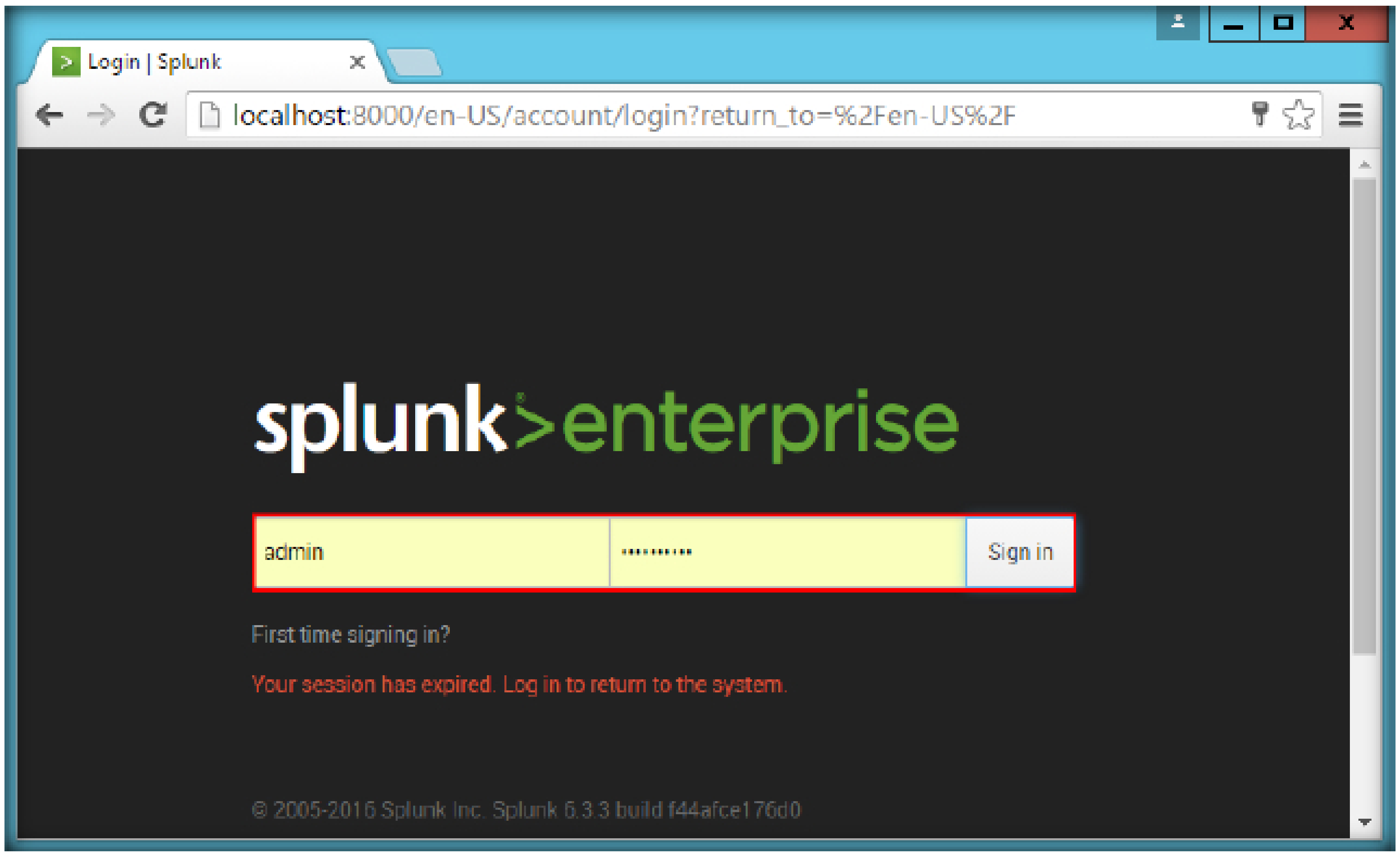
Restart successful - click OK to log back into Splunk

□ Prevent this page from creating additional dialogs.

FIGURE 6.35: Splunk restarted successfully

47. You will be redirected to the login page. Enter the user credentials and click **Sign in**.

The Splunk platform makes it easy to customize Splunk Enterprise to meet the needs of any project.


Login | Splunk
localhost:8000/en-US/account/login?return_to=%2Fen-US%2F
splunk>enterprise
admin
••••••••••
Sign in
First time signing in?
© 2005-2016 Splunk Inc. Splunk 6.3.3 build f44afce176d0

Your session has expired. Log in to return to the system.

FIGURE 6.36: Logging in to Splunk

48. When logged in, click **SplunkForwarder** in the left pane.

A robust security model provides secure data transfer, granular role-based access controls, LDAP integration and single sign-on, auditability and data integrity.

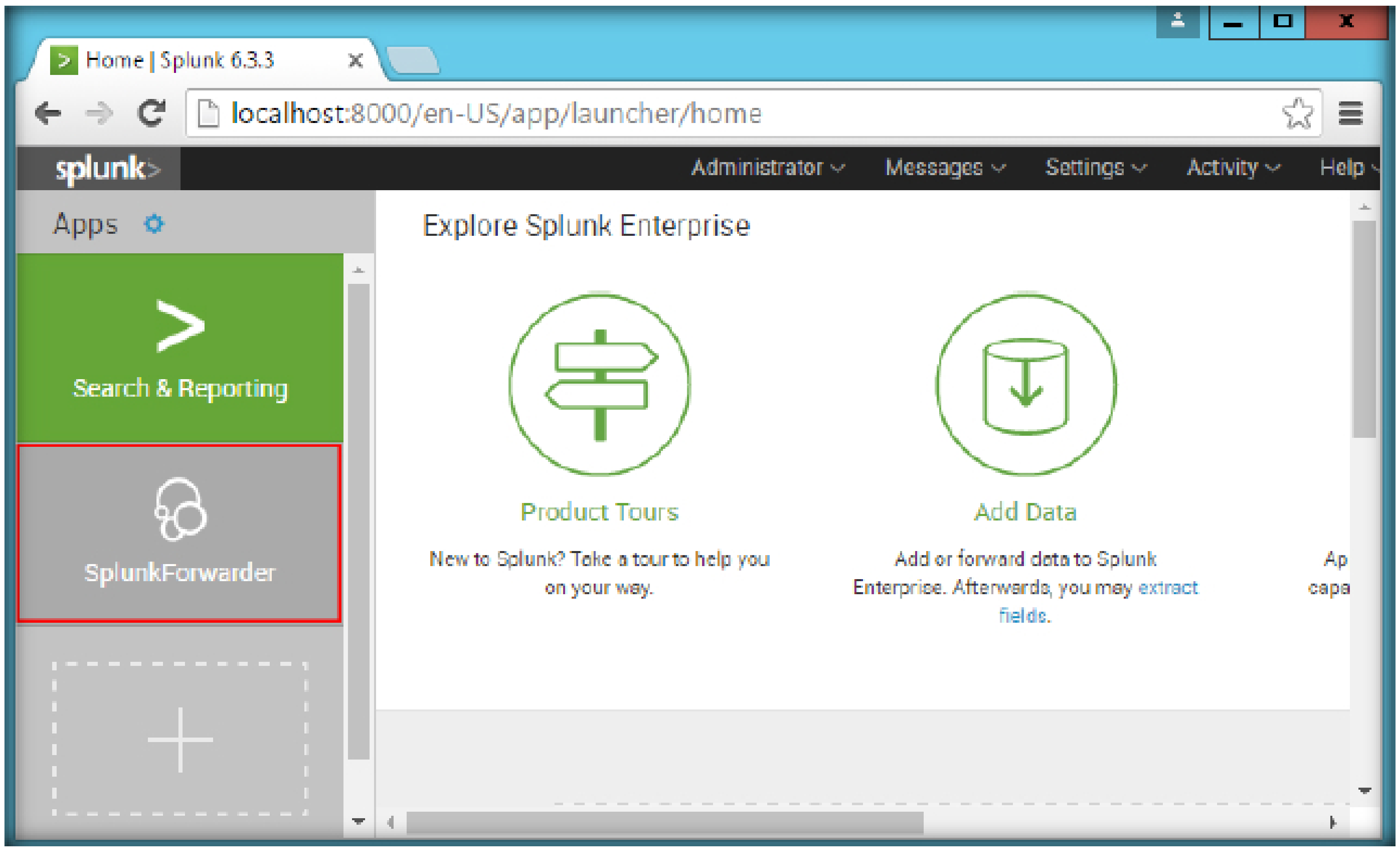
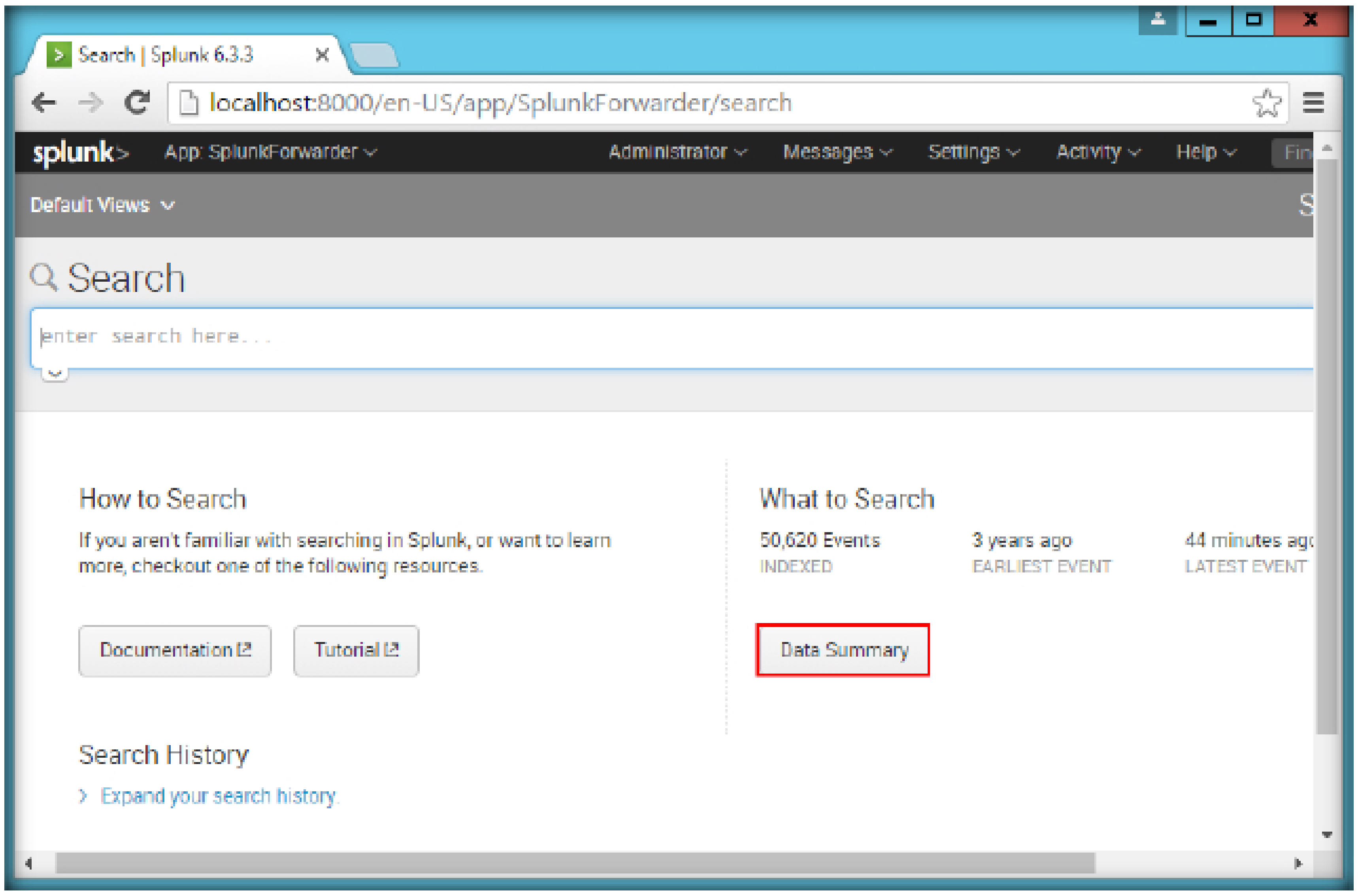

Home | Splunk 6.3.3
localhost:8000/en-US/app/launcher/home
splunk>
Administrator
Messages
Settings
Activity
Help
Apps
Search & Reporting
SplunkForwarder
Explore Splunk Enterprise
Product Tours
New to Splunk? Take a tour to help you on your way.
Add Data
Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.
Ap
capa

FIGURE 6.37: Launching the SplunkForwarder app

49. The **Search** console appears, click **Data Summary** under the **What to Search** section.



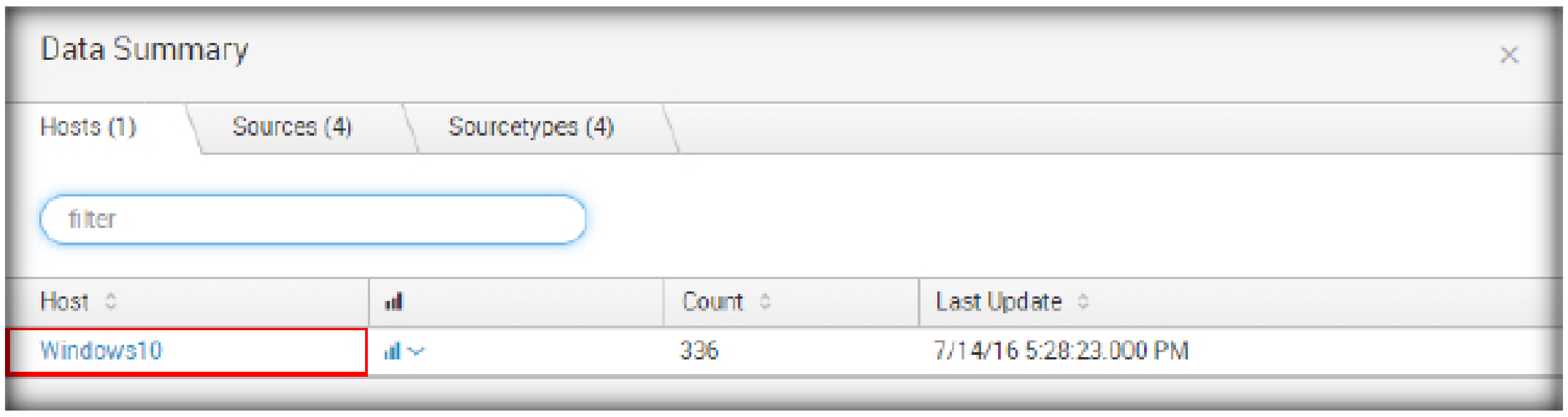
If you aren't familiar with searching in Splunk, or want to learn more, checkout one of the following resources.

| 50,620 Events | 3 years ago | 44 minutes ago |
|---|---|---|
| INDEXED | EARLIEST EVENT | LATEST EVENT |

FIGURE 6.38: Viewing user system data

Every transaction is authenticated, whether through the web and mobile interfaces, command line interface or the Splunk Enterprise API.

50. A host list appears, select the host machine name for Windows 10 (here, **Windows10**), the computer name may differ in your lab.

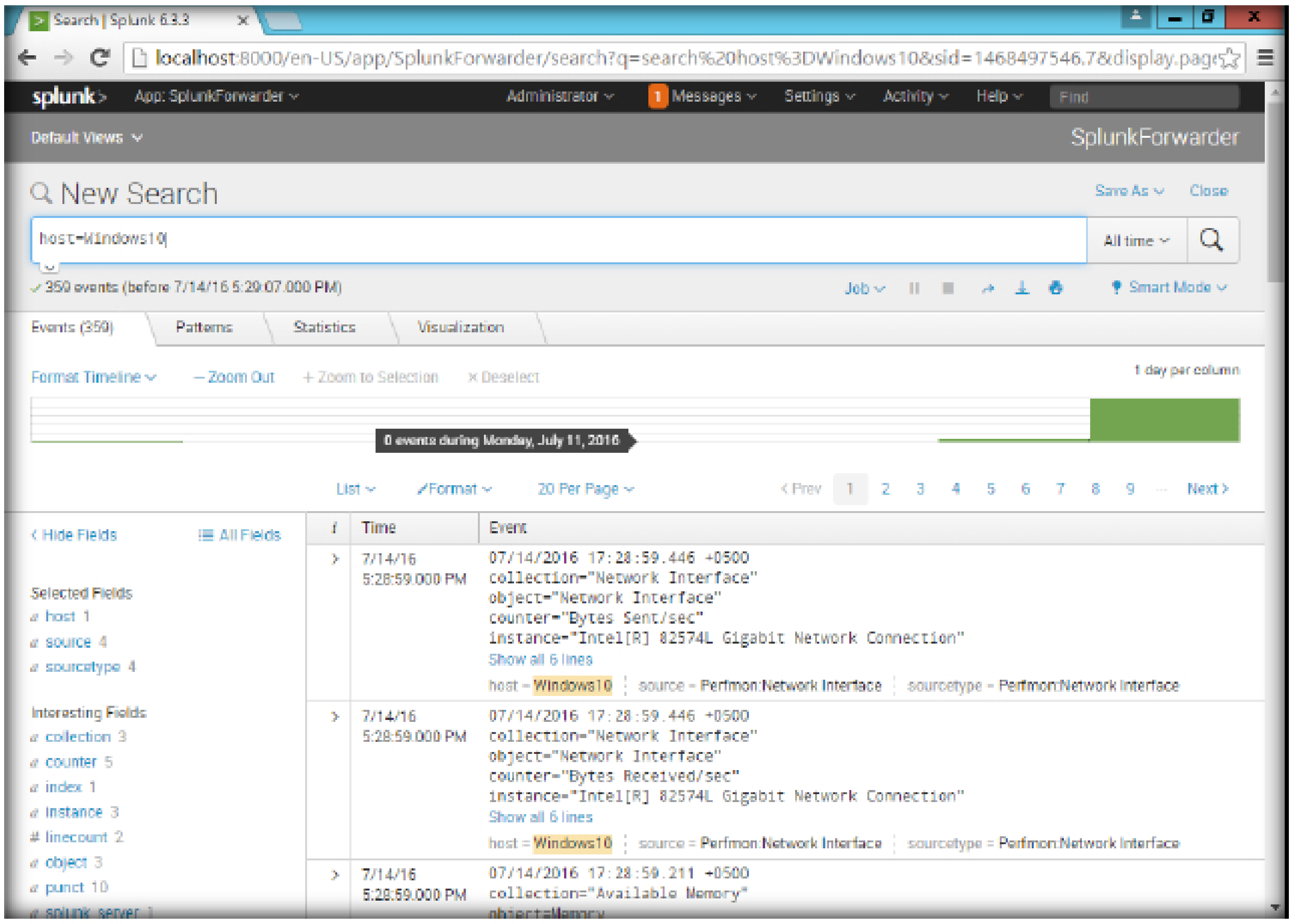


| Host | | Count | Last Update |
|---|---|---|---|
| Windows10 | | 336 | 7/14/16 5:28:23.000 PM |

FIGURE 6.39: Selecting Windows 10 machine

Splunk can also combine your machine data with data in your relational databases, data warehouses, and Hadoop and NoSQL data stores.

51. All the logs pertaining to Windows 10 are recorded in Splunk as shown in the following screenshot.



Search: `host=Windows10`

✓ 359 events (before 7/14/16 5:29:07.000 PM)

```
i   Time                      Event
>   7/14/16                   07/14/2016 17:28:59.446 +0500
    5:28:59.000 PM            collection="Network Interface"
                              object="Network Interface"
                              counter="Bytes Sent/sec"
                              instance="Intel[R] 82574L Gigabit Network Connection"
                              Show all 6 lines
                              host = Windows10 | source = Perfmon:Network Interface | sourcetype = Perfmon:Network Interface
>   7/14/16                   07/14/2016 17:28:59.446 +0500
    5:28:59.000 PM            collection="Network Interface"
                              object="Network Interface"
                              counter="Bytes Received/sec"
                              instance="Intel[R] 82574L Gigabit Network Connection"
                              Show all 6 lines
                              host = Windows10 | source = Perfmon:Network Interface | sourcetype = Perfmon:Network Interface
>   7/14/16                   07/14/2016 17:28:59.211 +0500
    5:28:59.000 PM            collection="Available Memory"
                              object=Memory
```

FIGURE 6.40: Results of Windows 10 machine

52. From these logs, you can analyze the performance entities and windows events for the remote machine (Windows 10).

## Lab Analysis

Analyze and document the results of the lab exercise. Give your opinion on your target's security posture and exposure through free public information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

| Internet Connection Required | |
|---|---|
| □ Yes | ☑ No |
| **Platform Supported** | |
| ☑ Classroom | ☑ iLabs |

Lab

7

# Monitoring Activities on a Remote System using Spytech SpyAgent

*Spytech SpyAgent is a powerful computer spy software that allows you to monitor everything users do on a computer—in complete stealth. SpyAgent provides a large array of essential computer monitoring features, as well as a website, application, and chat-client blocking, lockdown scheduling, and remote delivery of logs via email or FTP.*

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

## Lab Scenario

Today, employees are given access to a wide array of electronic communication equipment. Email, instant messaging, global positioning systems, telephone systems, and video cameras have given employers new ways to monitor the conduct and performance of their employees. Many employees are provided with a laptop computer and mobile phone they can take home and use for business outside the workplace. Whether an employee can reasonably expect privacy when using such company-supplied equipment depends, in large part, on the security policy the employer has put in place and made known to employees. As a network administrator, you should know how to track and monitor activities of remote users in the organization.

In this lab, we explain the process of monitoring employee activities using Spytech SpyAgent.

## Lab Objectives

The objective of this lab is to demonstrate how to monitor user activities remotely using Spytech SpyAgent.

## Lab Environment

To perform this lab, you need:

- A virtual machine running Windows Server 2012
- A virtual machine running Windows 10
- Administrative privileges to install and run the tools

## Lab Duration

Time: 25 Minutes

## Overview of the Lab

SpyAgent provides a large array of essential computer monitoring features, as well as a website, an application, and chat client blocking, logging scheduling, and remote delivery of logs via email or FTP.

## Lab Tasks

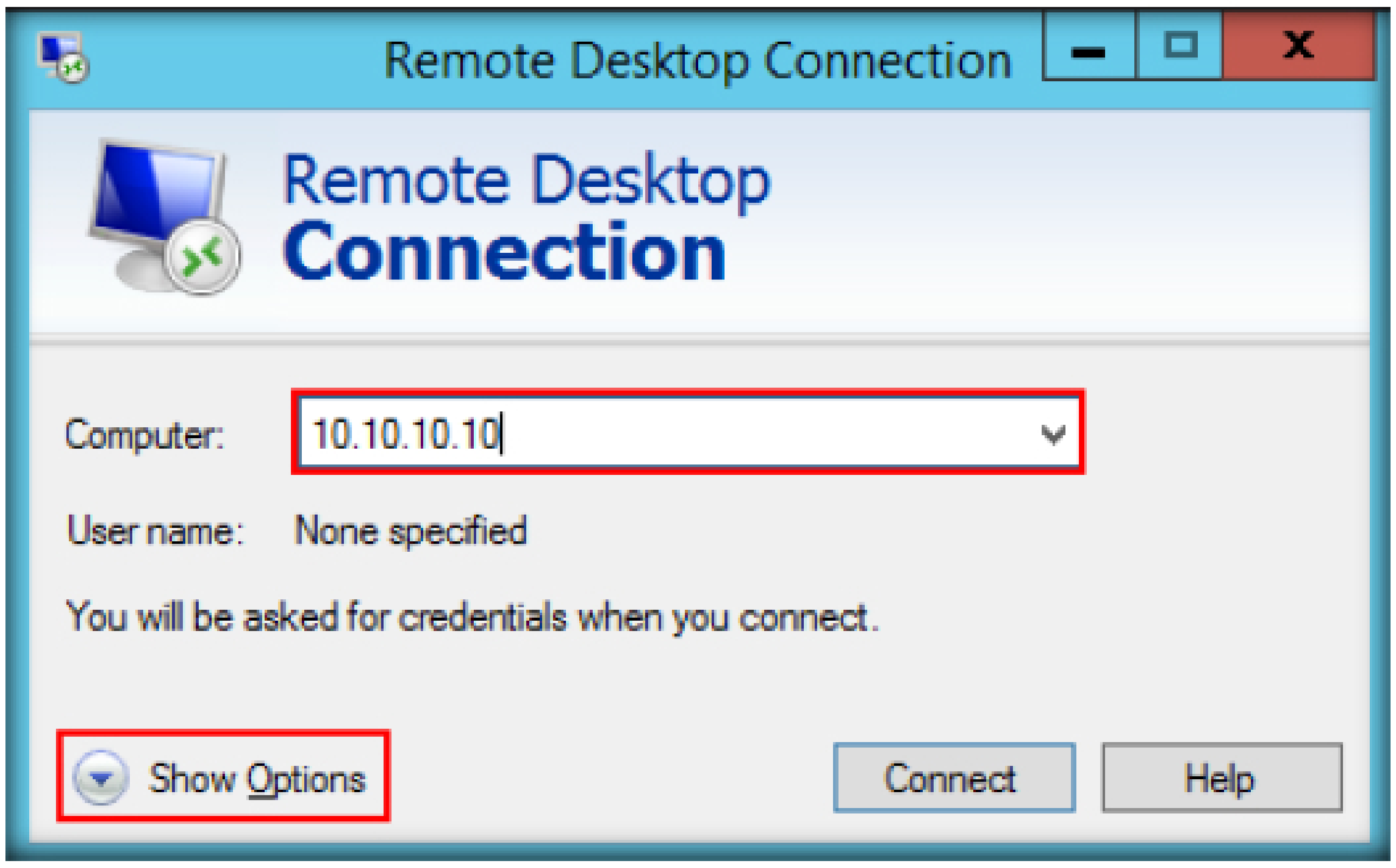
TASK 1

**Accessing Windows 10 Remotely**

**Note:** Before starting this Lab, make sure the Windows 10 machine is turned on and no user is logged in.

1. Launch the **Windows Server 2012** machine and right-click the **Start** icon at the lower left corner of the desktop then click **Search**.
2. In the right pane of the window, search for a **Remote Desktop Connection**.
3. The Remote Desktop Connection window appears; enter the IP address for **Windows 10** (10.10.10.10) in the Computer field and click the **Show Options** button.

   **Note**: The IP address may vary if you have assigned different IPs in your lab environment.



Computer: 10.10.10.10

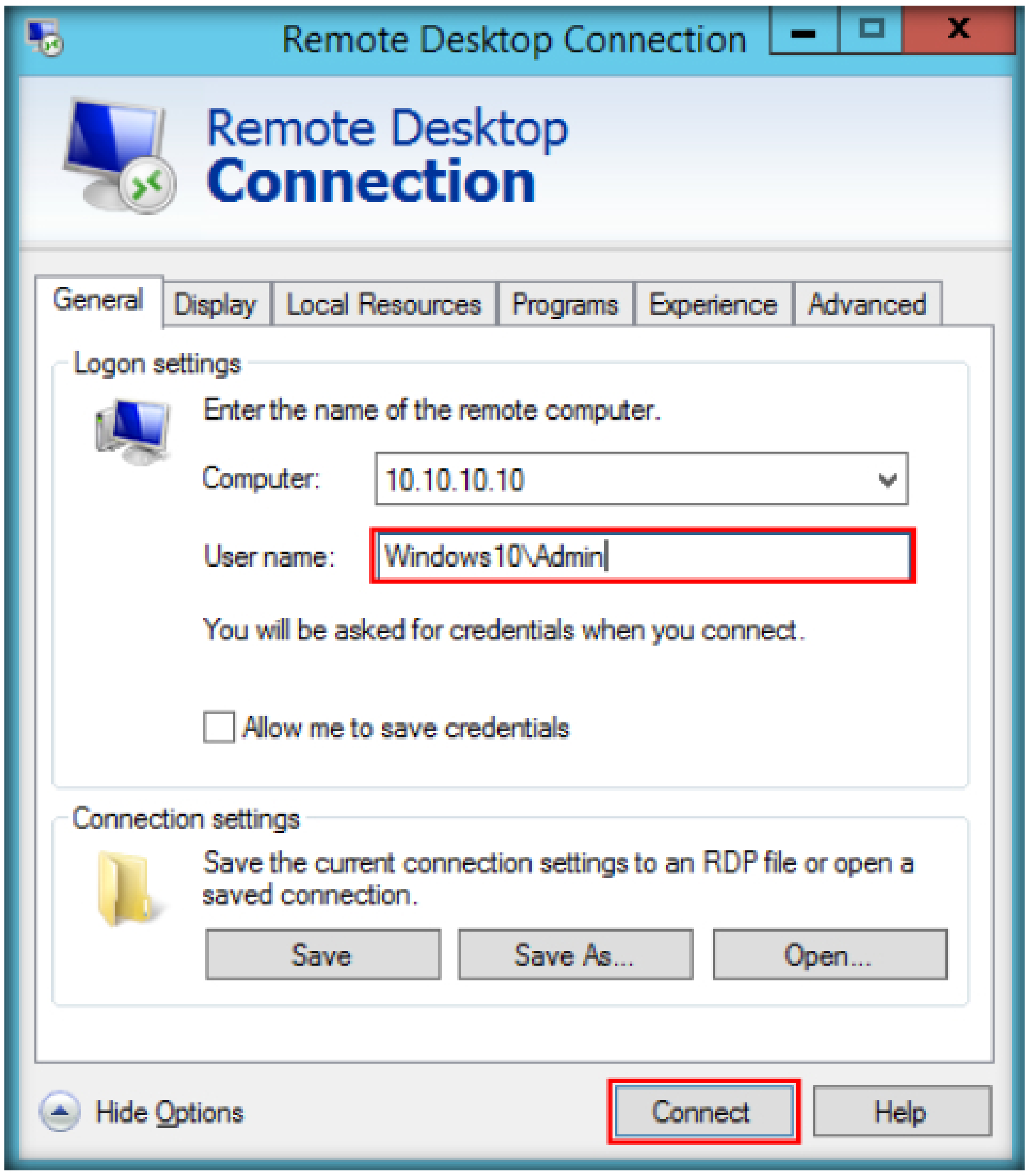
User name: None specified

You will be asked for credentials when you connect.

FIGURE 7.1: Remote Desktop Connection

4. In the User name: field type **Windows10\Admin** (login as a local admin account), and click **Connect**.

Establishing a Remote Connection



Logon settings

Enter the name of the remote computer.

Computer: 10.10.10.10

User name: Windows10\Admin

You will be asked for credentials when you connect.

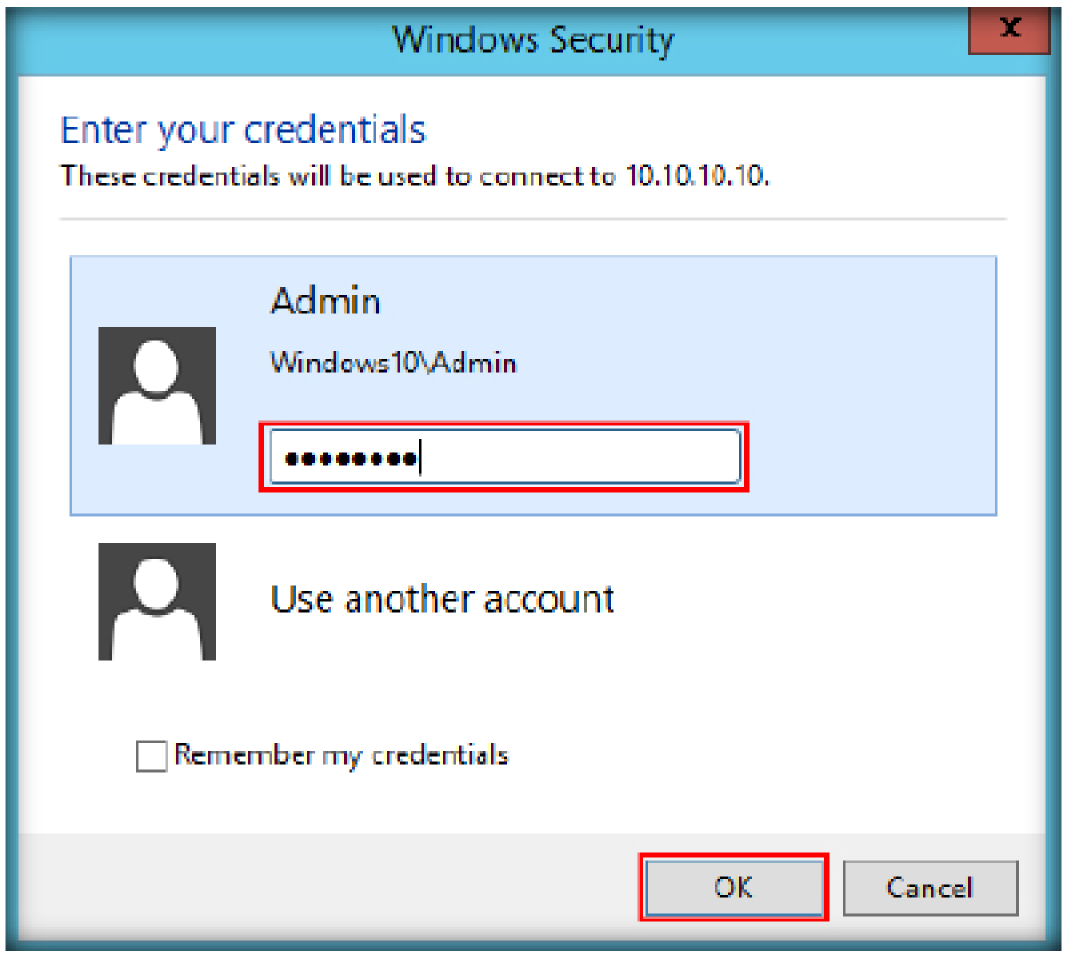
□ Allow me to save credentials

Connection settings

Save the current connection settings to an RDP file or open a saved connection.

FIGURE 7.2: Accessing Windows 10 Remotely

5. The Windows Security pop-up appears, type **Pa$$w0rd** to login as a local administrator for the Windows 10 machine and click **OK**.



Enter your credentials

These credentials will be used to connect to 10.10.10.10.

Admin

Windows10\Admin

••••••••

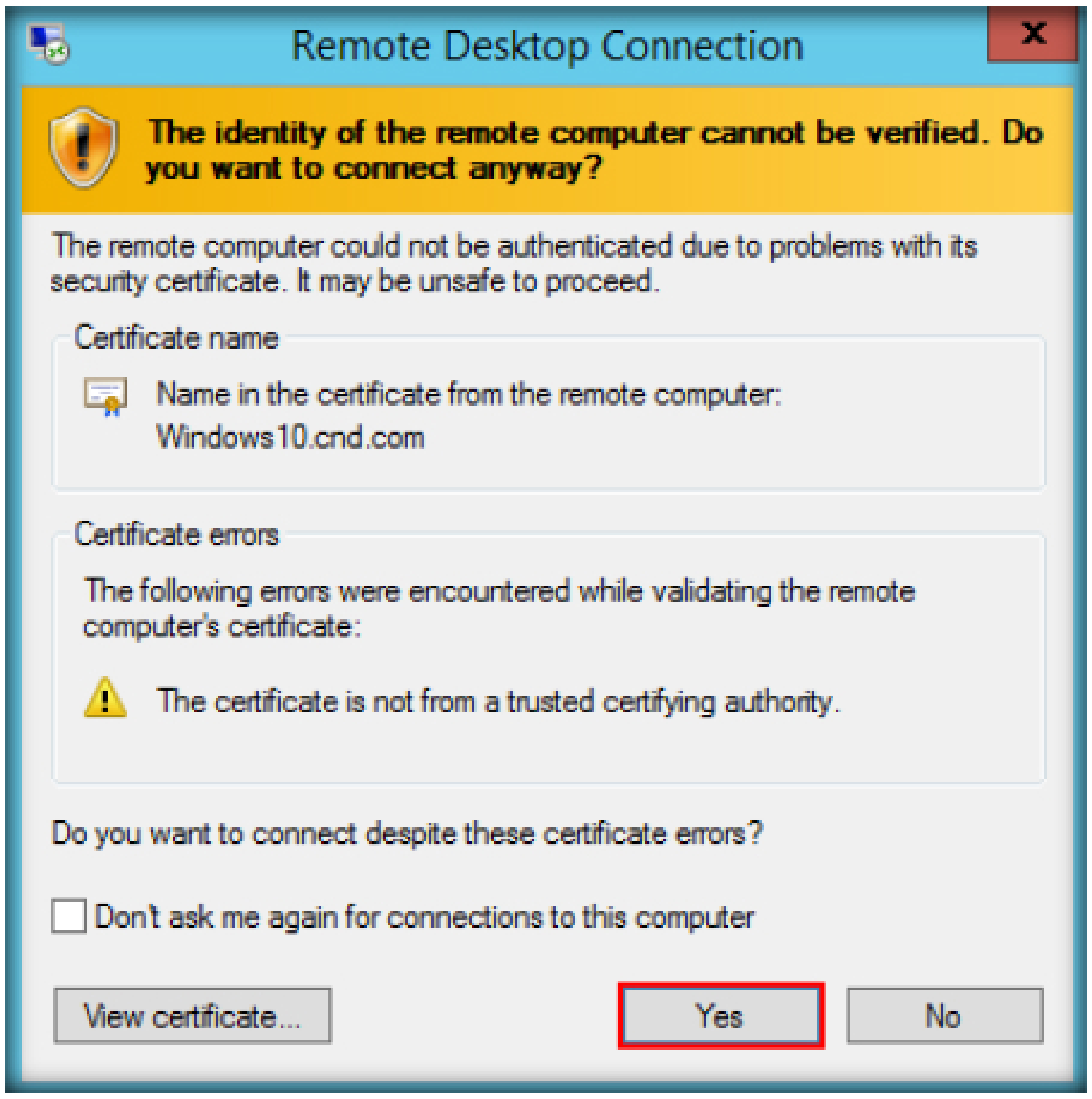
Use another account

□ Remember my credentials

You can download the Spytech SpyAgent from *http://www.spytech-web.com*

FIGURE 7.3: Windows Local Admin

6. A **Remote Desktop Connection** prompt appears. Click **Yes**.



Remote Desktop Connection

**The identity of the remote computer cannot be verified. Do you want to connect anyway?**

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
Windows10.cnd.com

Certificate errors

The following errors were encountered while validating the remote computer's certificate:

⚠ The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

□ Don't ask me again for connections to this computer

FIGURE 7.4: Remote Desktop Connection Certificate

Active Mode: this option allows SpyAgent to be started in monitoring mode when it is opened - no need for manually starting its monitoring

7. Remote connection is established for the **Windows 10** machine, and local administrator log in.

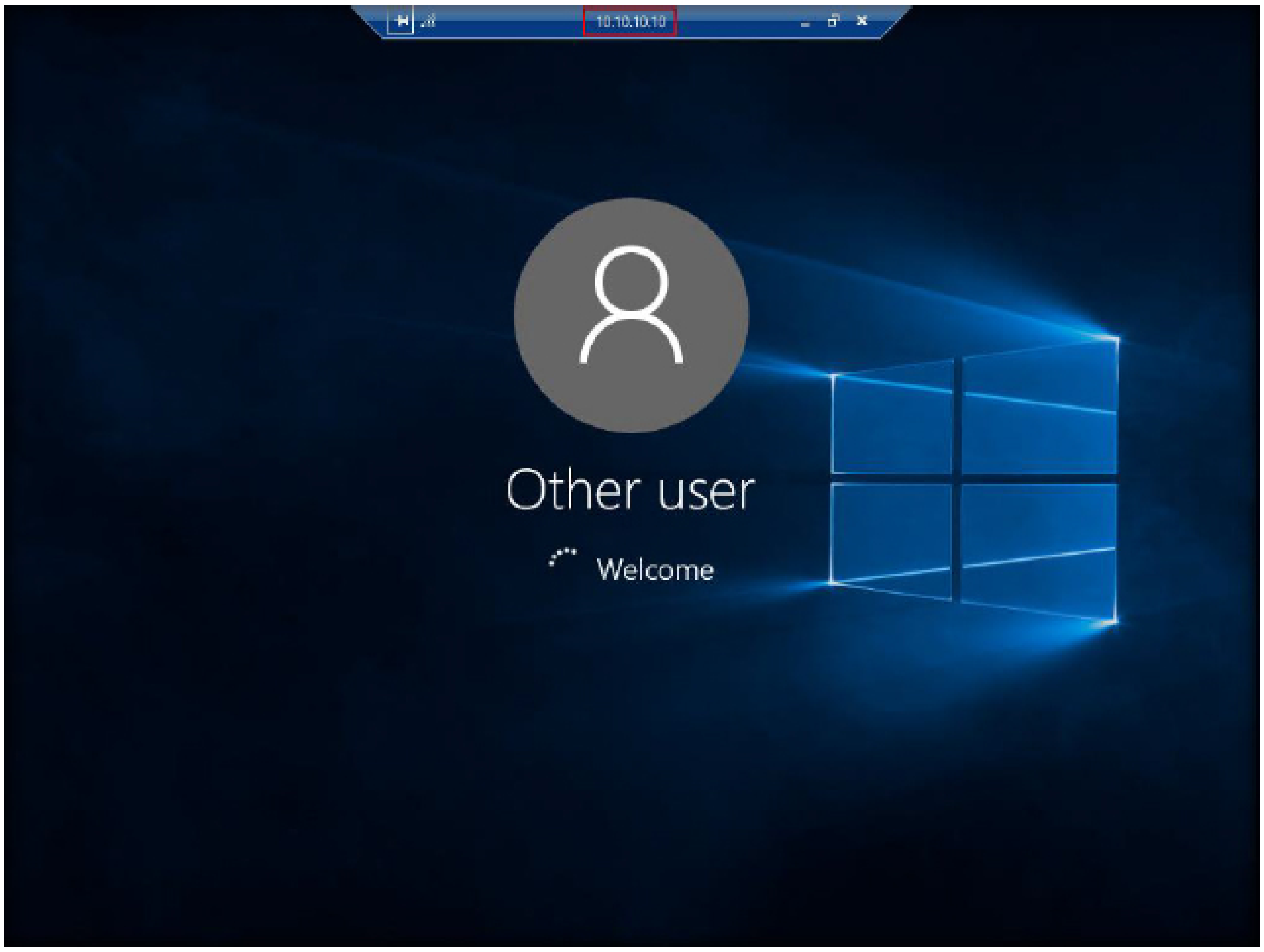


FIGURE 7.5: Windows 10 Machine Remote

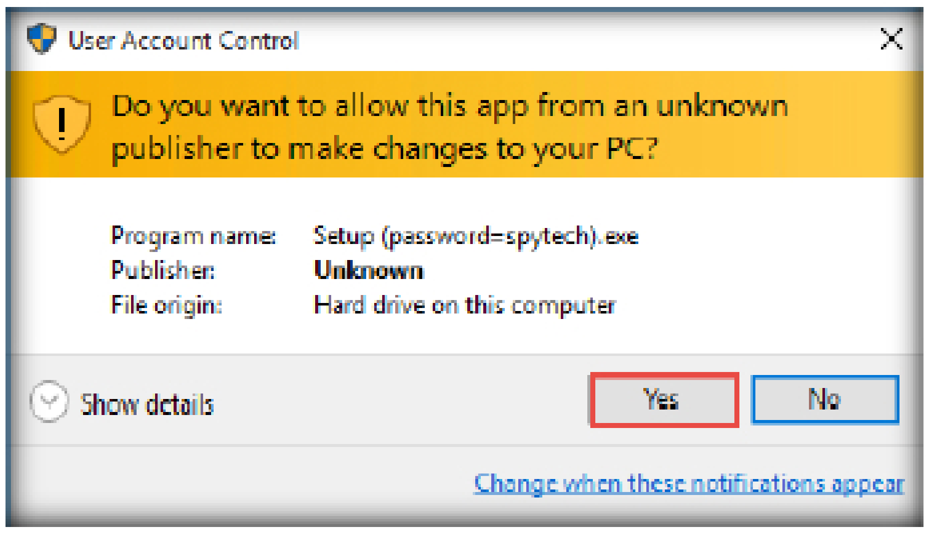
Stealth Mode: this option allows SpyAgent to run in total stealth. Combined with 'Active Mode' the software will load and run in monitoring mode without being detected.

8. Navigate to **Z:\CND-Tools\CND Module 06 Host Security\Employee Monitoring Tools\Spyagent** and double-click **Setup (password=spytech).exe** to start the installation.

TASK 2

**Install Spytech SpyAgent**

9. The **User Account Control** window appears. Click **Yes**.



User Account Control

Do you want to allow this app from an unknown publisher to make changes to your PC?

Program name: Setup (password=spytech).exe
Publisher: **Unknown**
File origin: Hard drive on this computer

FIGURE 7.6: User Account Control

10. The **Spytech SpyAgent Setup** window appears. Click **Next**.

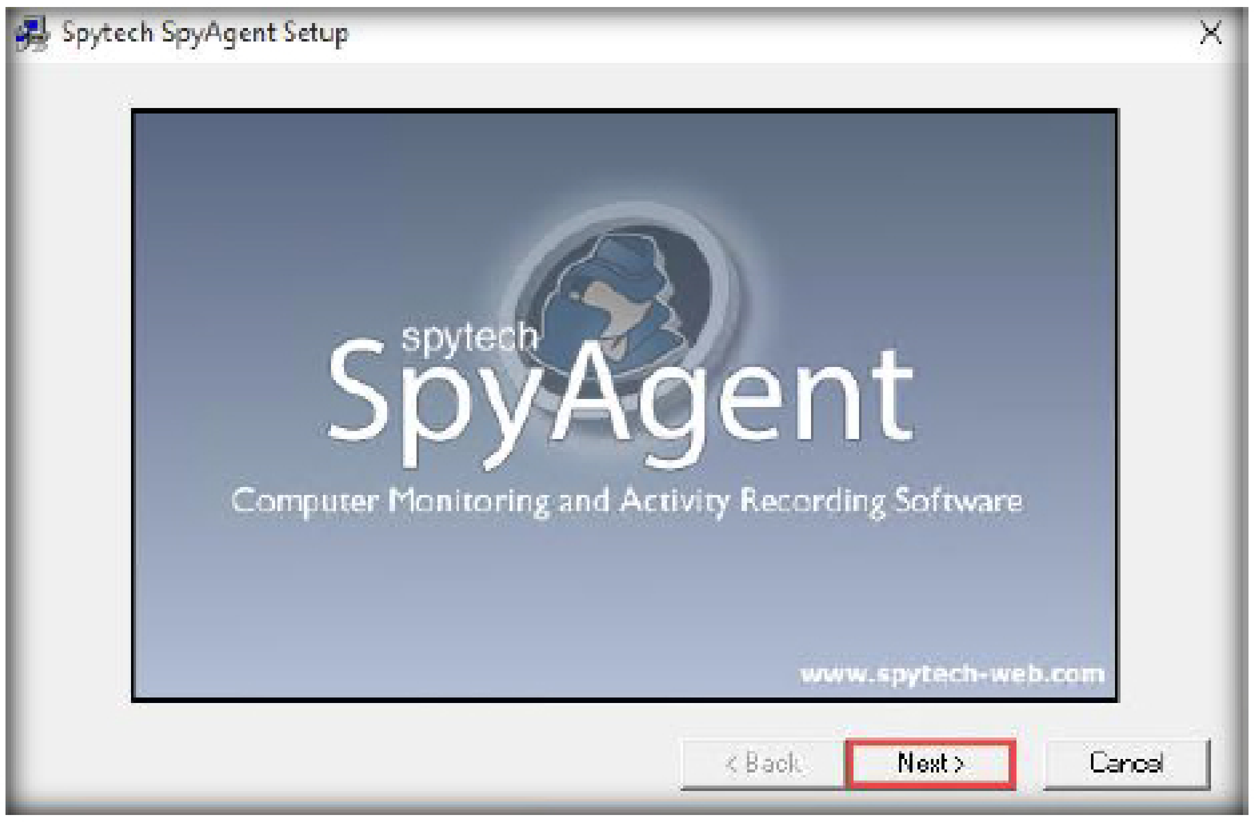
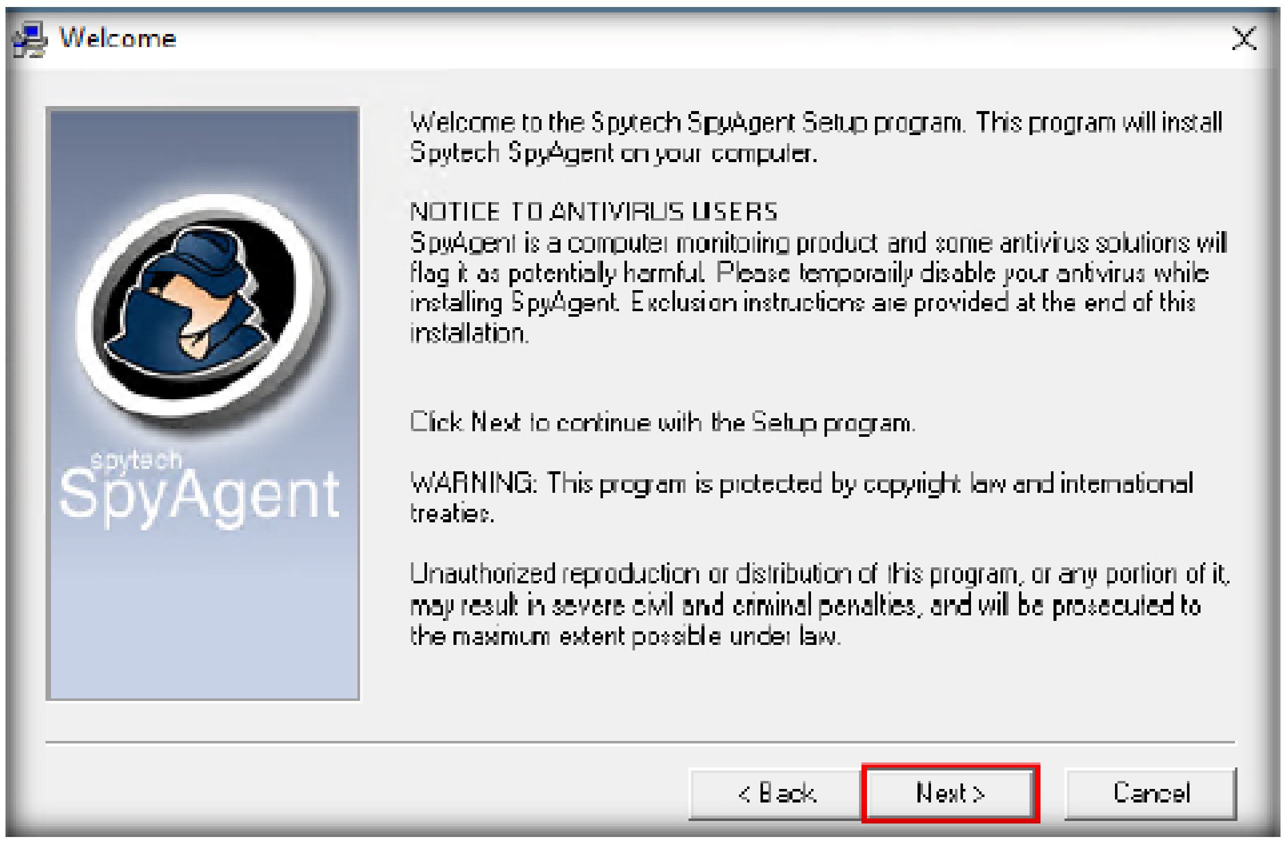


FIGURE 7.7: Spytech SpyAgent Setup

Splash Warning: This option allows you to display a message to the user when SpyAgent is started. This message can be configured in the Advanced Settings→ Splash Screen window

11. The Notice to Antivirus Users wizard appears, click Next to continue with the installation.



Welcome

Welcome to the Spytech SpyAgent Setup program. This program will install Spytech SpyAgent on your computer.

NOTICE TO ANTIVIRUS USERS
SpyAgent is a computer monitoring product and some antivirus solutions will flag it as potentially harmful. Please temporarily disable your antivirus while installing SpyAgent. Exclusion instructions are provided at the end of this installation.

Click Next to continue with the Setup program.

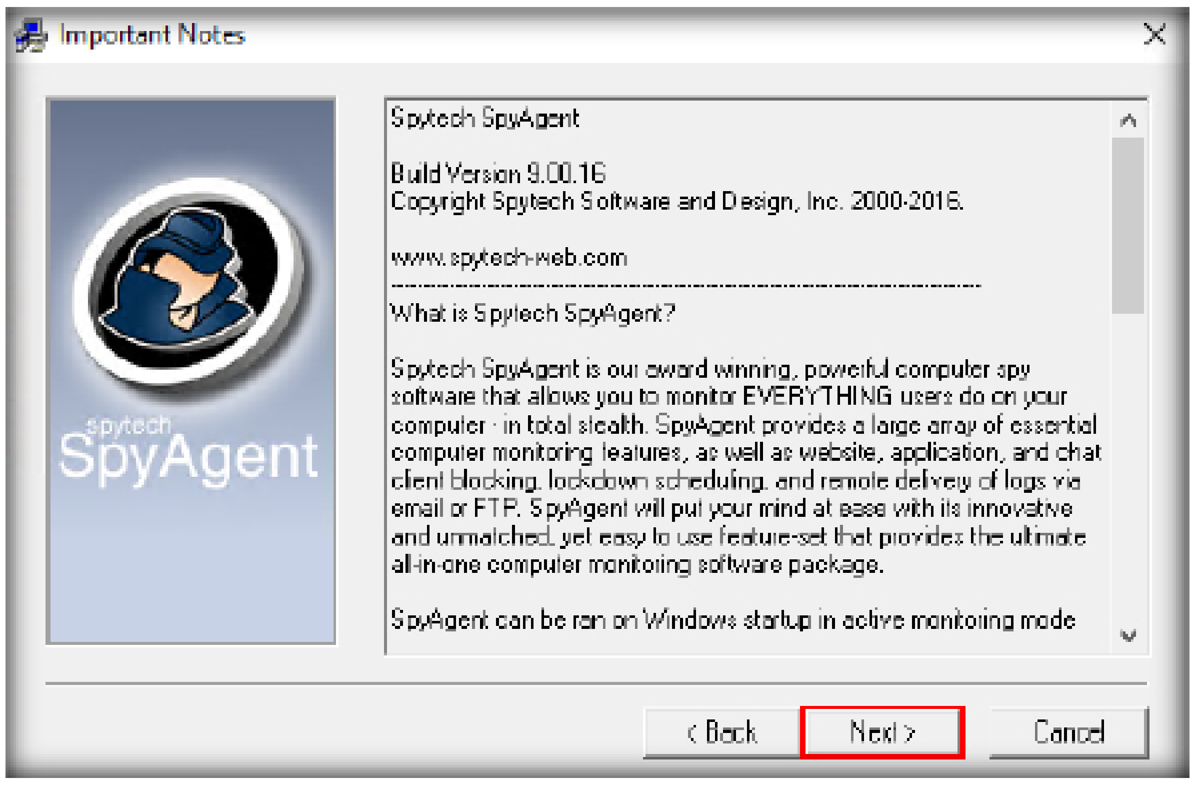
WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

FIGURE 7.8: Spytech SpyAgent Welcome

**Log Location**: this allows you to specify where you want SpyAgent to store its activity logs. For Windows NT/2000/XP systems, monitoring ALL users is recommended the log location be set to x:\documents and settings\all users

12. The Important Notes wizard appears, click Next.



Spytech SpyAgent

Build Version 9.00.16
Copyright Spytech Software and Design, Inc. 2000-2016.

www.spytech-web.com
-----------------------------------------------------------------------------------------
What is Spytech SpyAgent?

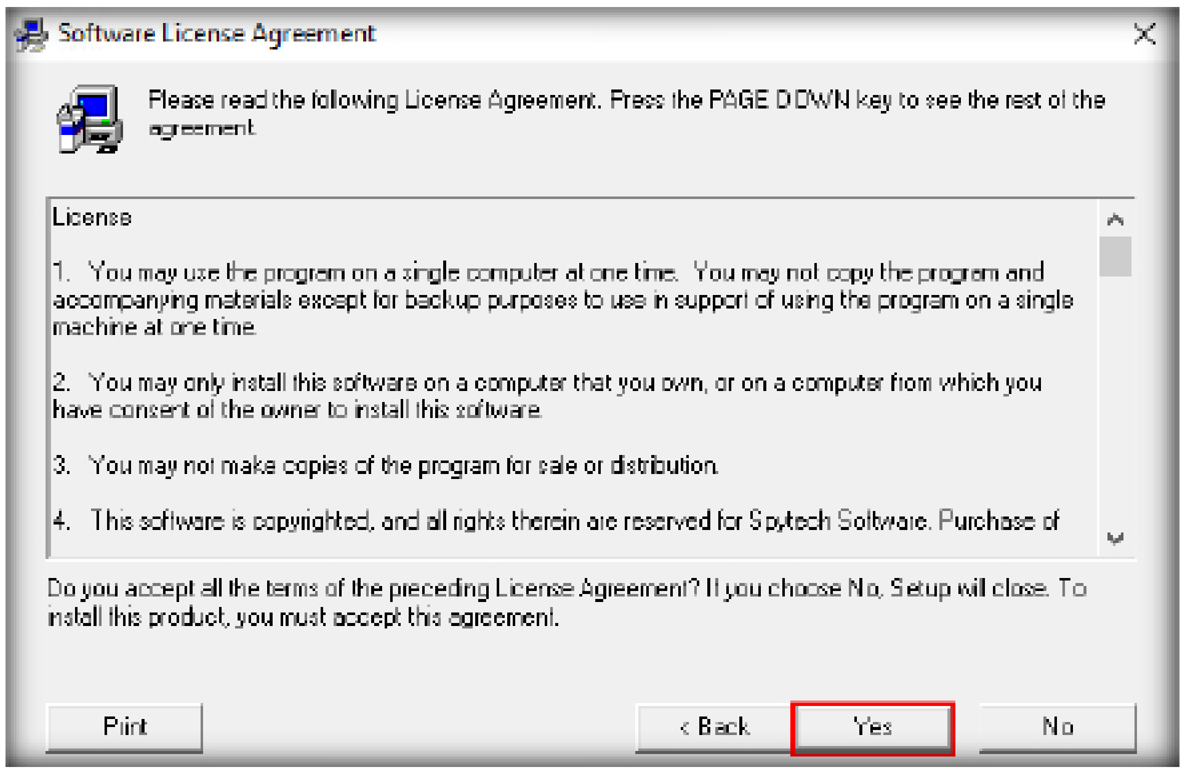
Spytech SpyAgent is our award winning, powerful computer spy software that allows you to monitor EVERYTHING users do on your computer - in total stealth. SpyAgent provides a large array of essential computer monitoring features, as well as website, application, and chat client blocking, lockdown scheduling, and remote delivery of logs via email or FTP. SpyAgent will put your mind at ease with its innovative and unmatched, yet easy to use feature-set that provides the ultimate all-in-one computer monitoring software package.

SpyAgent can be ran on Windows startup in active monitoring mode

FIGURE 7.9: Spytech SpyAgent Important Notes

13. The Software License Agreement wizard appears, click **Yes** to accept the terms and conditions.

SpyAgent can deliver its activity logs in secret to your own personal email or FTP account



Please read the following License Agreement. Press the PAGE DOWN key to see the rest of the agreement.

License

1. You may use the program on a single computer at one time. You may not copy the program and accompanying materials except for backup purposes to use in support of using the program on a single machine at one time.

2. You may only install this software on a computer that you own, or on a computer from which you have consent of the owner to install this software.

3. You may not make copies of the program for sale or distribution.

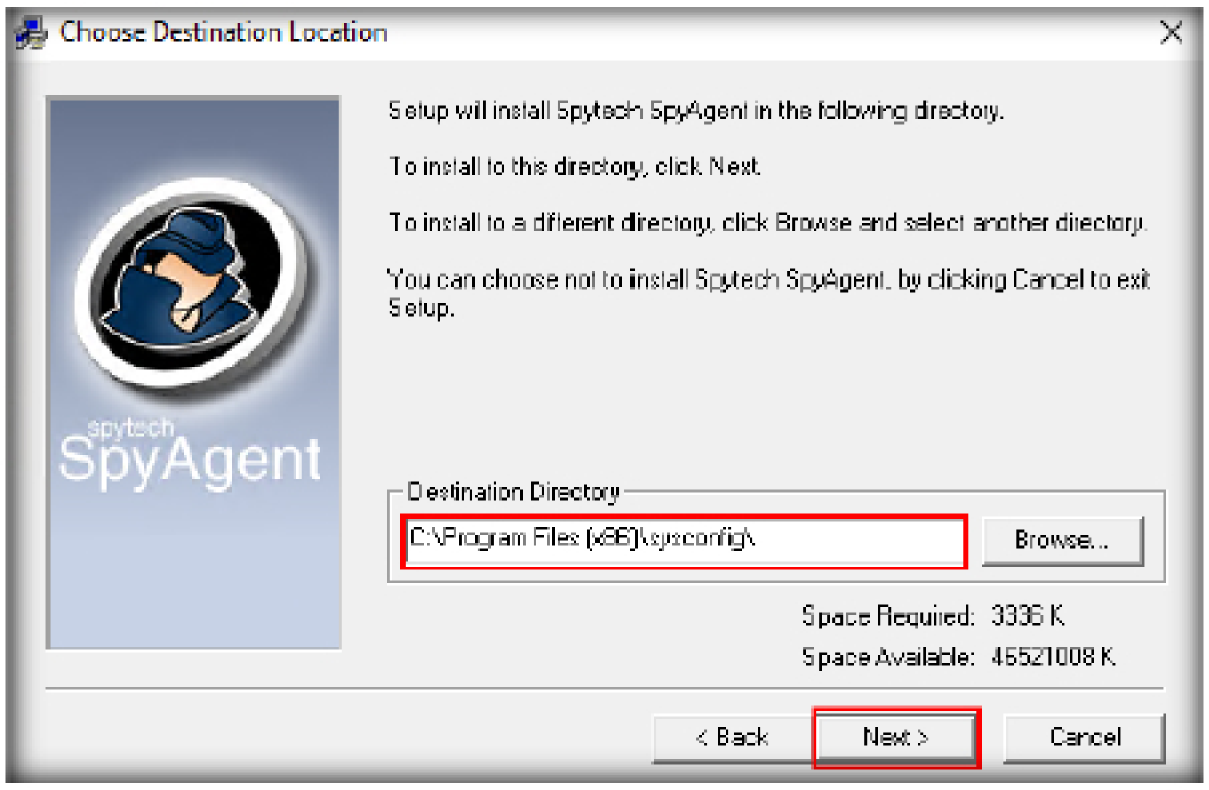
4. This software is copyrighted, and all rights therein are reserved for Spytech Software. Purchase of

Do you accept all the terms of the preceding License Agreement? If you choose No, Setup will close. To install this product, you must accept this agreement.

FIGURE 7.10: Spytech SpyAgent License Agreement

14. The Choose Destination Location wizard appears, leave the Destination Directory to default and click **Next**.

**Internet Traffic Data**: This logs ALL incoming and outgoing internet data transmitted and received by users. All email passwords, FTP passwords, website transmissions, etc. will be logged by this feature



Setup will install Spytech SpyAgent in the following directory.

To install to this directory, click Next.

To install to a different directory, click Browse and select another directory.

You can choose not to install Spytech SpyAgent, by clicking Cancel to exit Setup.

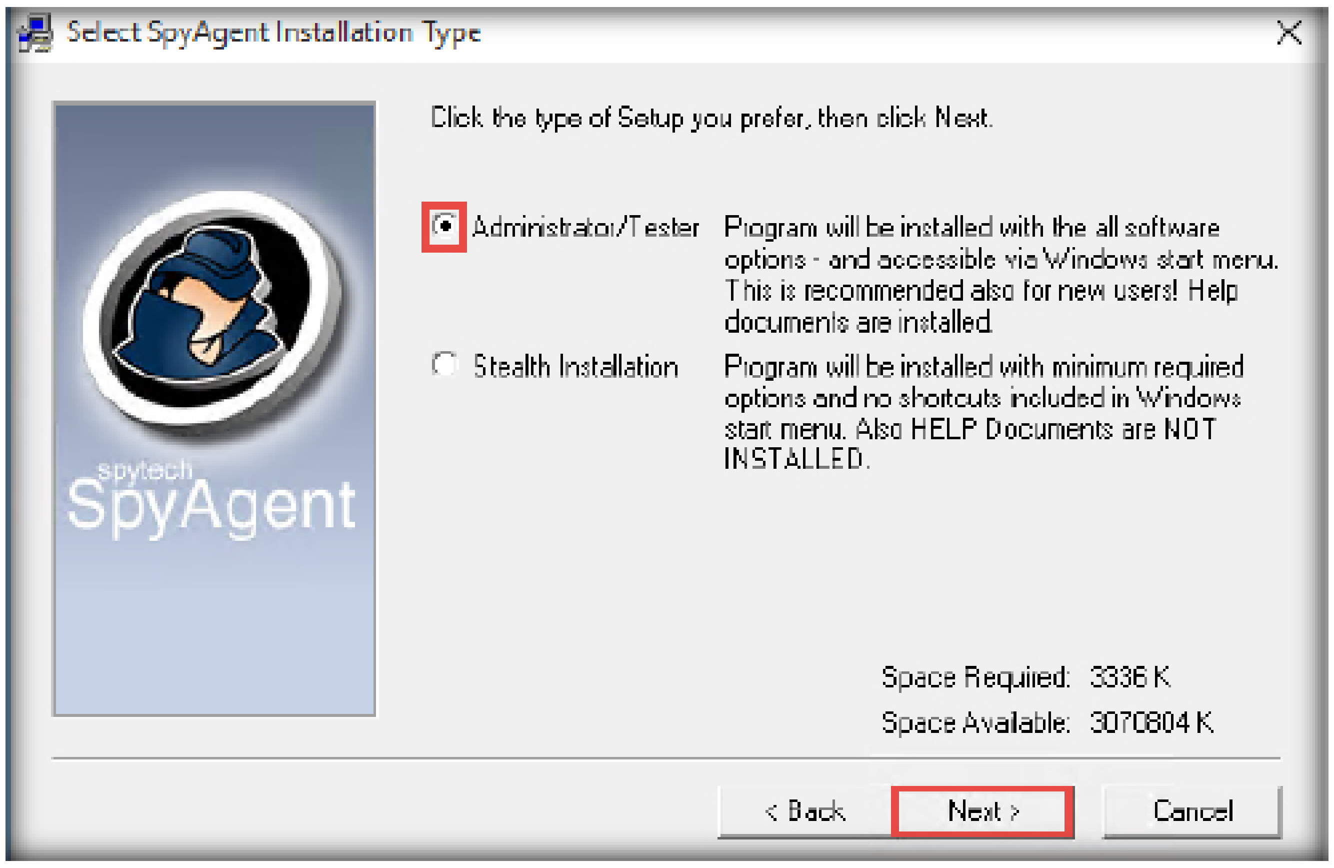
Destination Directory
C:\Program Files (x86)\spyconfig\

Space Required: 3336 K
Space Available: 45521008 K

FIGURE 7.11: Spytech SpyAgent Destination Location selection

SpyAgent has the unique ability to allow you to have its activity logs delivered to your personal e-mail address or FTP account.

15. The Select SpyAgent Installation Type wizard appears, click the **Administrator /Tester** radio (default) and click **Next**.



Select SpyAgent Installation Type

Click the type of Setup you prefer, then click Next.

● Administrator/Tester — Program will be installed with the all software options - and accessible via Windows start menu. This is recommended also for new users! Help documents are installed.

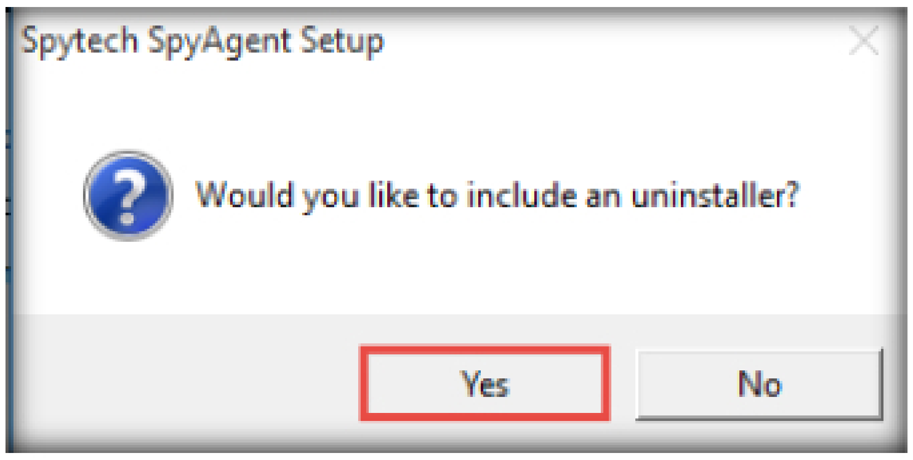
○ Stealth Installation — Program will be installed with minimum required options and no shortcuts included in Windows start menu. Also HELP Documents are NOT INSTALLED.

Space Required: 3336 K
Space Available: 3070804 K

FIGURE 7.12: Spytech SpyAgent Installation Type

16. Continue with the installation until you reach the **Spytech SpyAgent setup** window. Click **Yes**.

SpyAgent has a built in scheduling feature that allows you to configure SpyAgent to log user activities during specific hours of the day, or to lock down your computer at certain times.



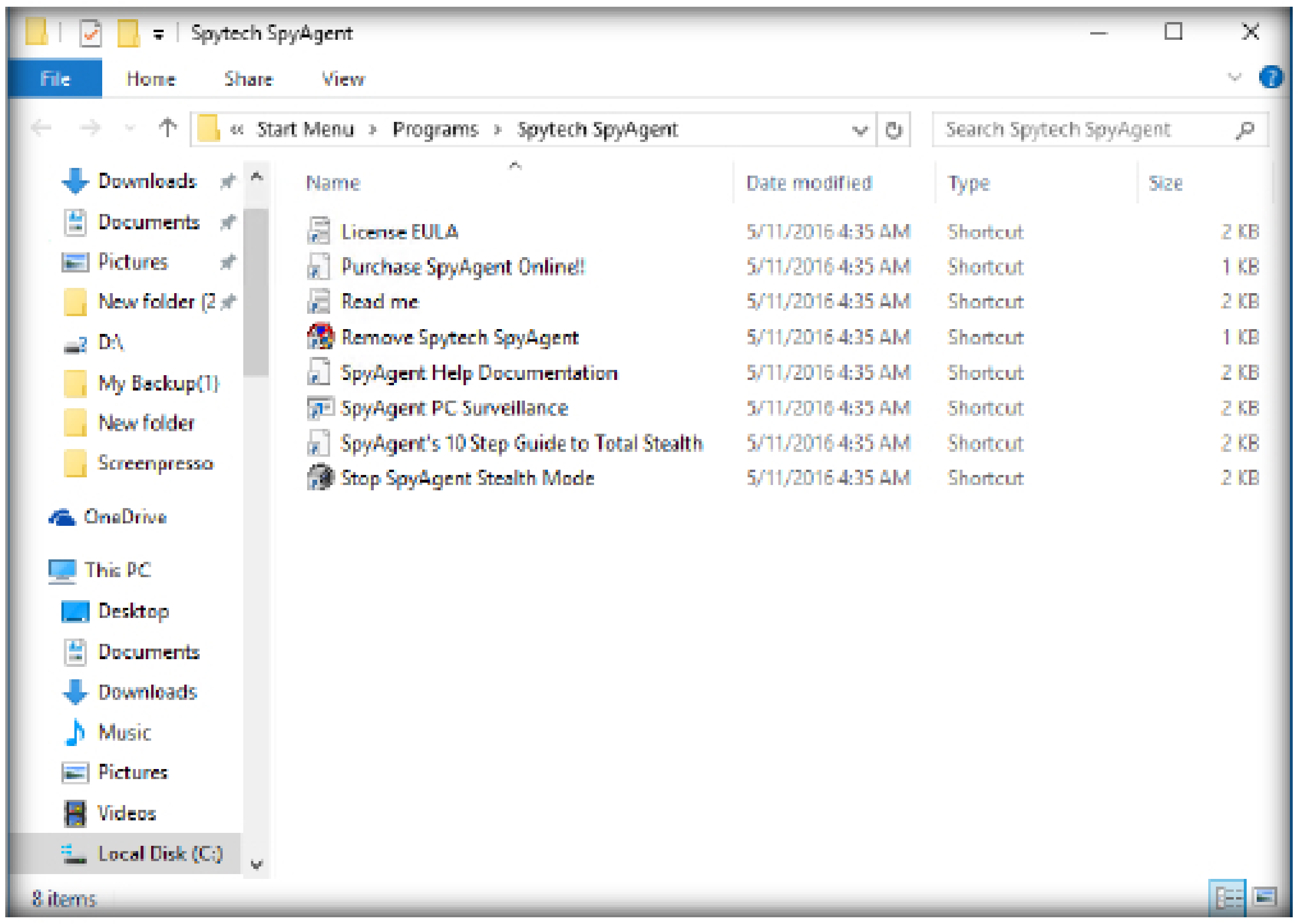
Spytech SpyAgent Setup

Would you like to include an uninstaller?

FIGURE 7.13: Spytech SpyAgent Setup pop-up

17. The **Spytech SpyAgent** window appears after installation completes, minimize or close the window.

SpyAgent has a feature called SmartLogging that lets you trigger monitoring when certain events arise, instead of running constantly logging everything that users do. SmartLogging ties into the keystrokes, websites visited, applications ran, and windows used logging functions.



Spytech SpyAgent

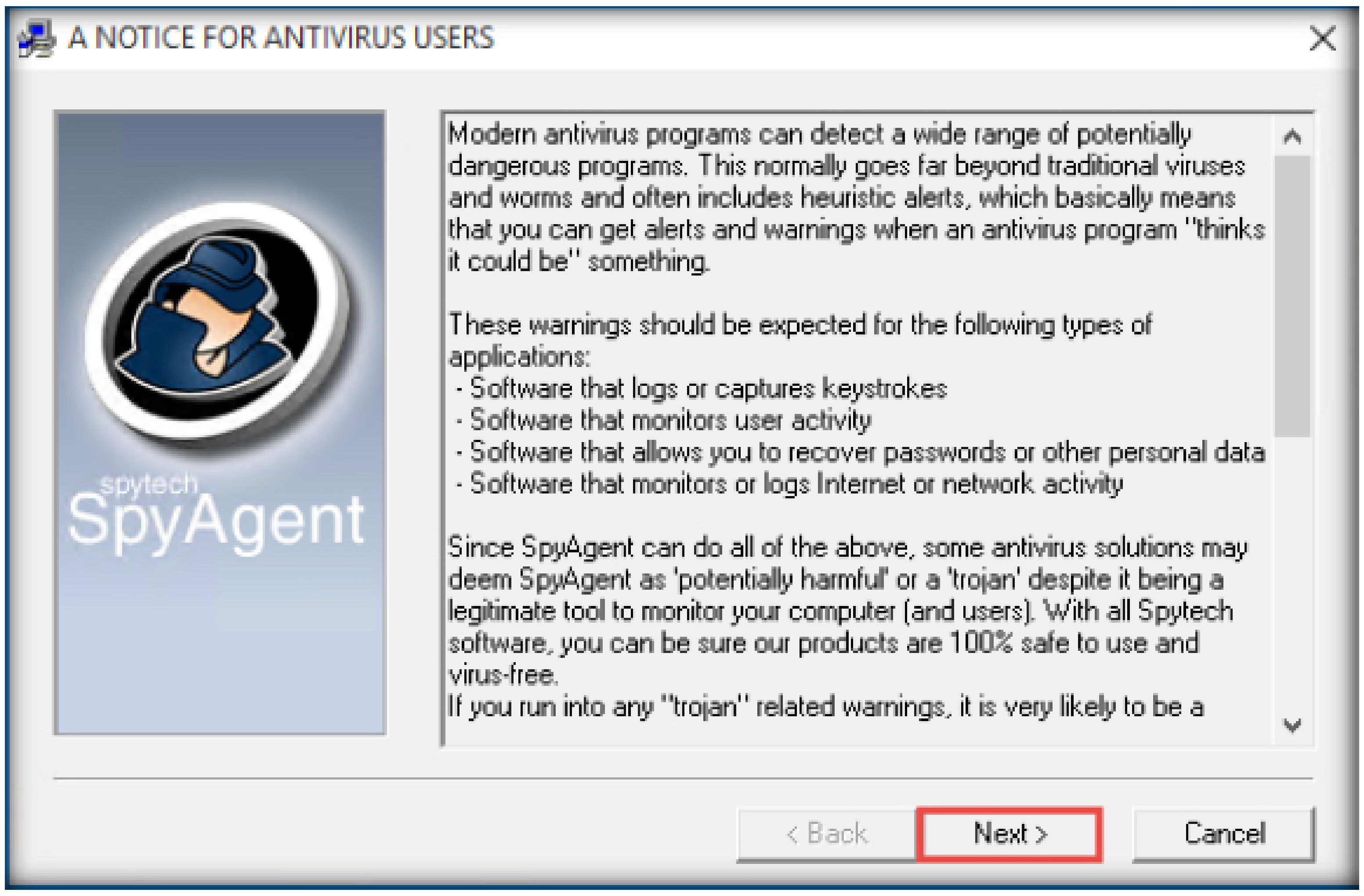
« Start Menu › Programs › Spytech SpyAgent

| Name | Date modified | Type | Size |
|---|---|---|---|
| License EULA | 5/11/2016 4:35 AM | Shortcut | 2 KB |
| Purchase SpyAgent Online! | 5/11/2016 4:35 AM | Shortcut | 1 KB |
| Read me | 5/11/2016 4:35 AM | Shortcut | 2 KB |
| Remove Spytech SpyAgent | 5/11/2016 4:35 AM | Shortcut | 1 KB |
| SpyAgent Help Documentation | 5/11/2016 4:35 AM | Shortcut | 2 KB |
| SpyAgent PC Surveillance | 5/11/2016 4:35 AM | Shortcut | 2 KB |
| SpyAgent's 10 Step Guide to Total Stealth | 5/11/2016 4:35 AM | Shortcut | 2 KB |
| Stop SpyAgent Stealth Mode | 5/11/2016 4:35 AM | Shortcut | 2 KB |

8 items

FIGURE 7.14: Spytech SpyAgent Installation Folder

18. The **A NOTICE FOR ANTIVIRUS USERS** window appears; read the notice and click **Next**.



A NOTICE FOR ANTIVIRUS USERS

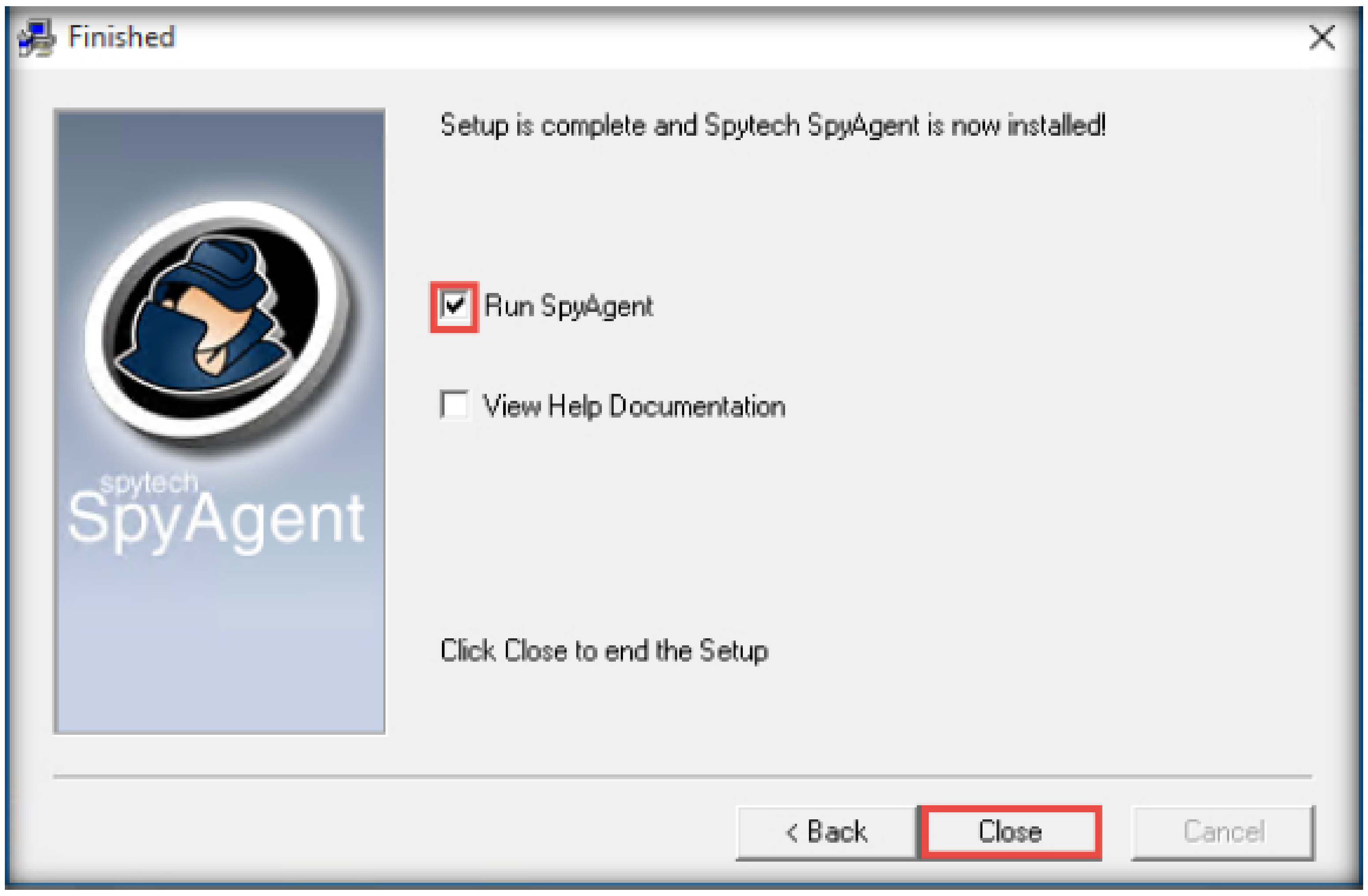
Modern antivirus programs can detect a wide range of potentially dangerous programs. This normally goes far beyond traditional viruses and worms and often includes heuristic alerts, which basically means that you can get alerts and warnings when an antivirus program "thinks it could be" something.

These warnings should be expected for the following types of applications:
- Software that logs or captures keystrokes
- Software that monitors user activity
- Software that allows you to recover passwords or other personal data
- Software that monitors or logs Internet or network activity

Since SpyAgent can do all of the above, some antivirus solutions may deem SpyAgent as 'potentially harmful' or a 'trojan' despite it being a legitimate tool to monitor your computer (and users). With all Spytech software, you can be sure our products are 100% safe to use and virus-free.
If you run into any "trojan" related warnings, it is very likely to be a

FIGURE 7.15: Spytech SpyAgent Notice for Antivirus

19. The **Finished** window appears. Ensure **Run SpyAgent** is checked and click **Close**.



Finished

Setup is complete and Spytech SpyAgent is now installed!

☑ Run SpyAgent

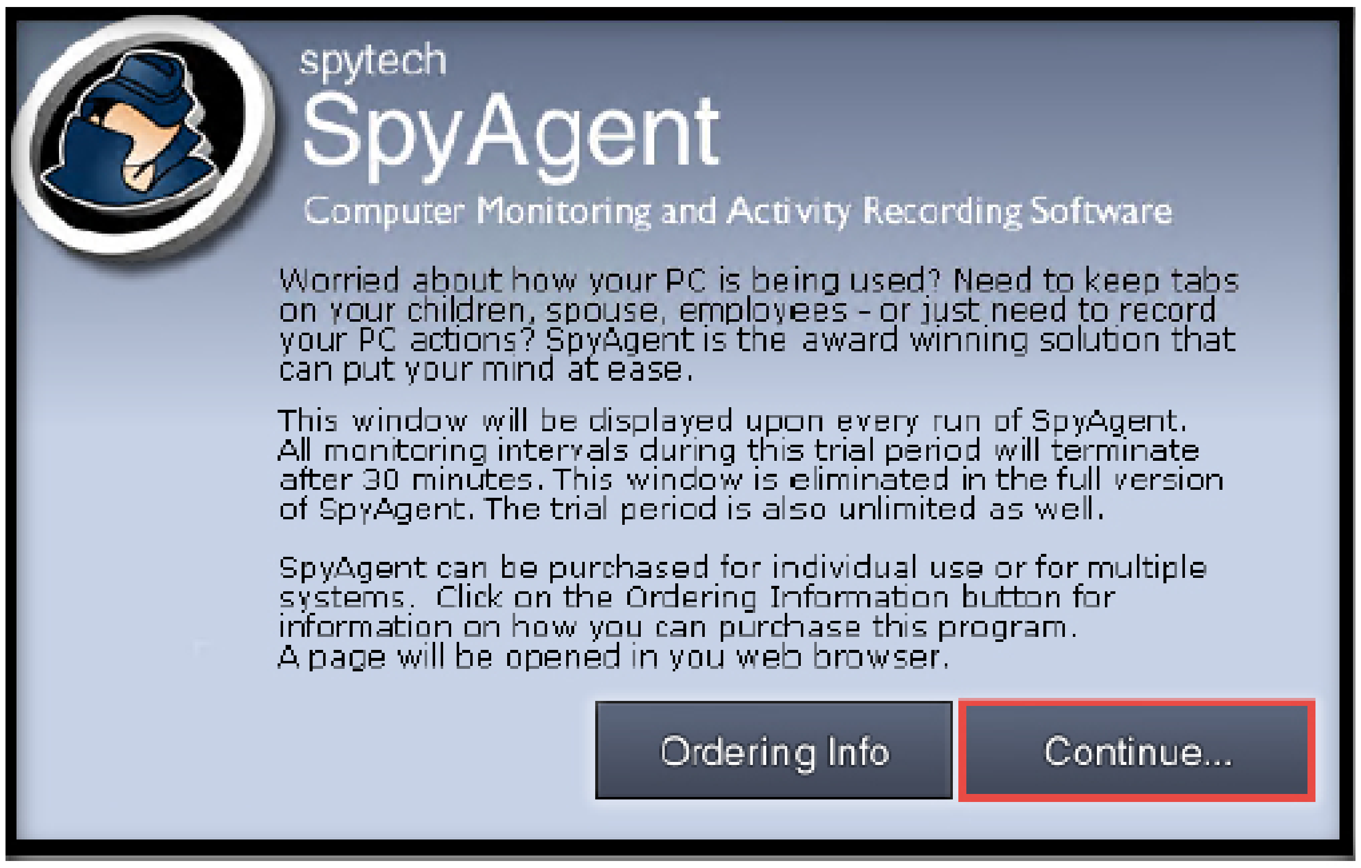
□ View Help Documentation

Click Close to end the Setup

FIGURE 7.16: Spytech SpyAgent Installation Finished

SpyAgent allows you to save all of SpyAgent's keystrokes, websites, windows, applications, connections, clipboard, activity, print jobs, file usage, and documents logs to a specified directory at once - for easier viewing later on - or so you can clear your logs without losing data.

20. The **Spytech SpyAgent** dialog box appears; click **Continue...**.



spytech

SpyAgent

Computer Monitoring and Activity Recording Software

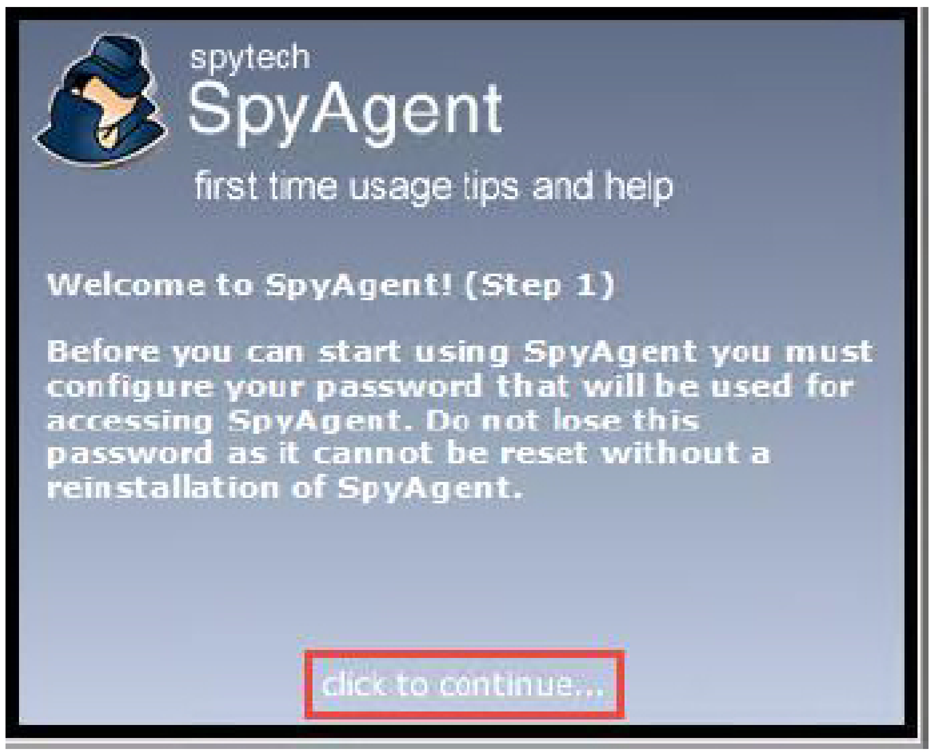
Worried about how your PC is being used? Need to keep tabs on your children, spouse, employees - or just need to record your PC actions? SpyAgent is the award winning solution that can put your mind at ease.

This window will be displayed upon every run of SpyAgent. All monitoring intervals during this trial period will terminate after 30 minutes. This window is eliminated in the full version of SpyAgent. The trial period is also unlimited as well.

SpyAgent can be purchased for individual use or for multiple systems. Click on the Ordering Information button for information on how you can purchase this program. A page will be opened in you web browser.

FIGURE 7.17: Spytech SpyAgent Configuration

21. The **Step 1** of the setup wizard appears; select **click to continue...**.



spytech

SpyAgent

first time usage tips and help

Welcome to SpyAgent! (Step 1)

Before you can start using SpyAgent you must configure your password that will be used for accessing SpyAgent. Do not lose this password as it cannot be reset without a reinstallation of SpyAgent.

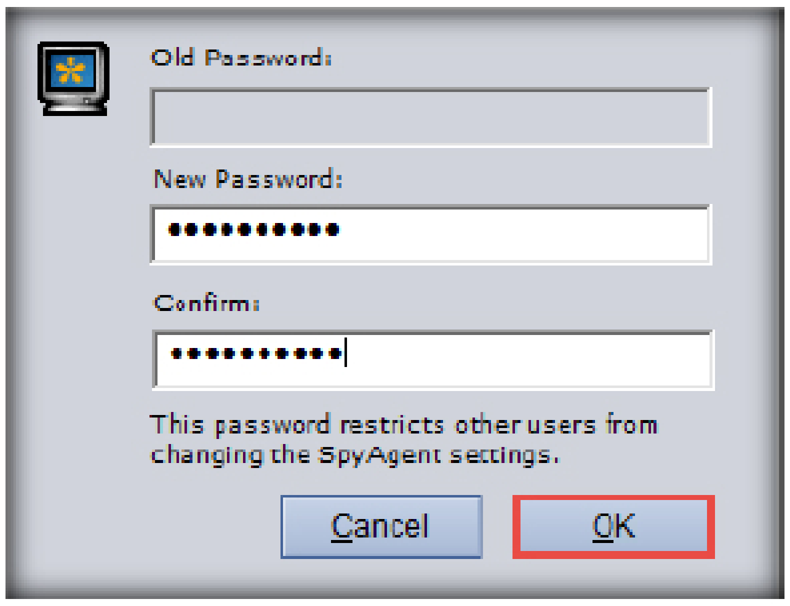
FIGURE 7.18: Spytech SpyAgent Step 1

SpyAgent features a large set of reporting tools that allow you to save and prepare log data for later viewing, documentation, and printing. All reports are formatted in HTML format for viewing with your web-browser.

22. Enter a password in the **New Password** field, then retype the same password in the **Confirm** field.

**Note:** The password entered is **qwerty@123**

23. Click **OK**.



Old Password:

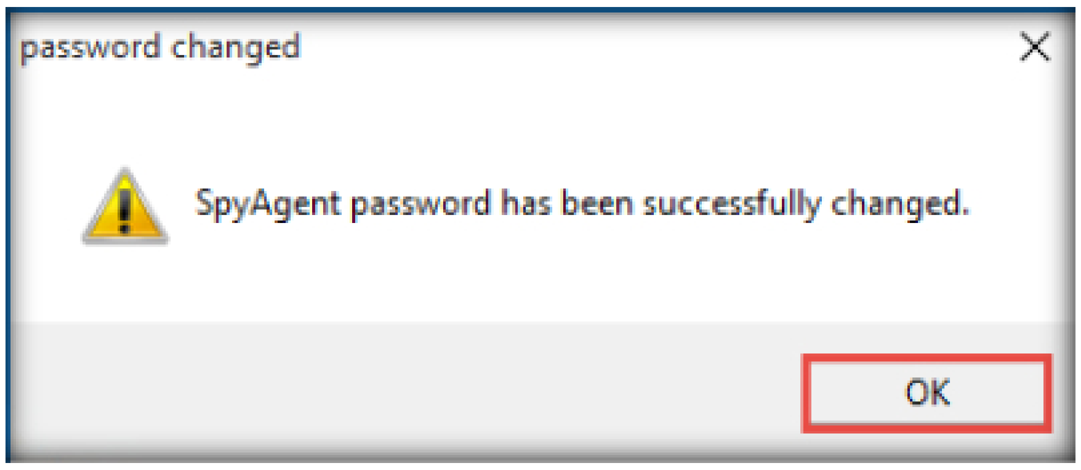
New Password: ••••••••••

Confirm: ••••••••••

This password restricts other users from changing the SpyAgent settings.

FIGURE 7.19: Spytech SpyAgent Assigning Password

24. The **password changed** pop-up appears; click **OK**.



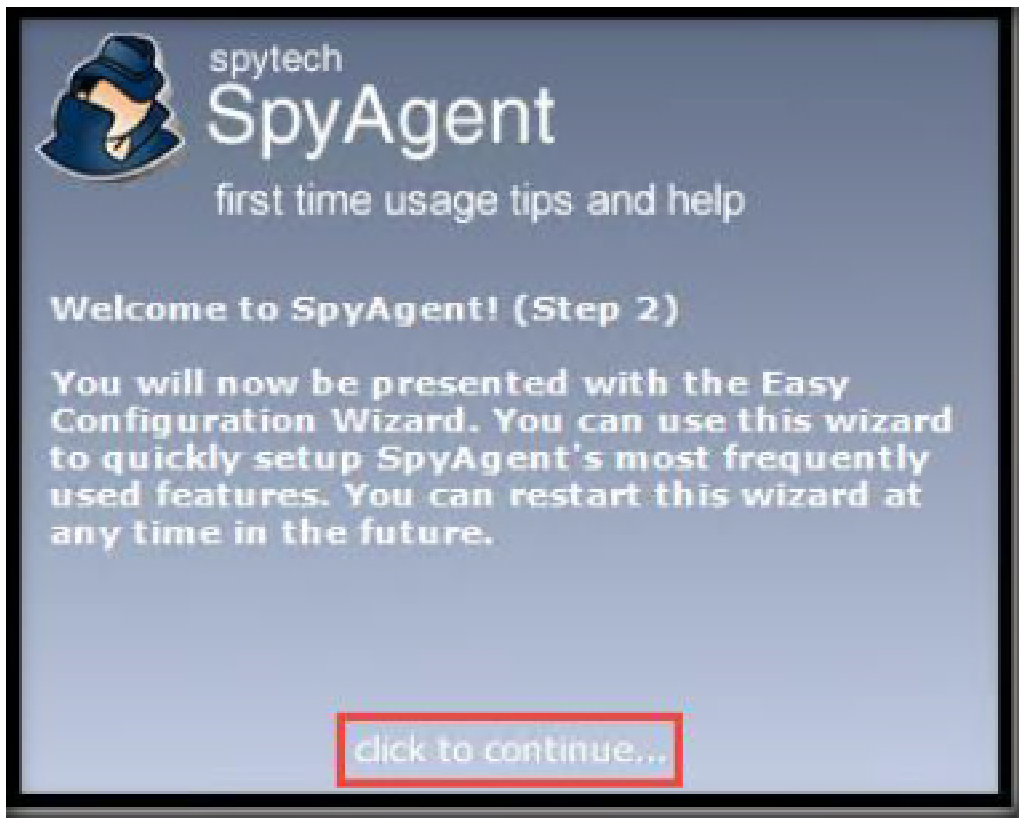
password changed

SpyAgent password has been successfully changed.

FIGURE 7.20: Spytech SpyAgent Password changed

Keystroke Logging Monitor and log all keystrokes along with the window they are typed in and timestamp. Click the "Format" button to remove and apply text formatting to make the log more readable. Passwords captured are flagged for easy viewing. If screenshot capturing is enabled, SpyAgent will display related screenshots alongside the keystroke log entries.

25. The **Step 2** of the Welcome wizard appears, select **click to continue…**

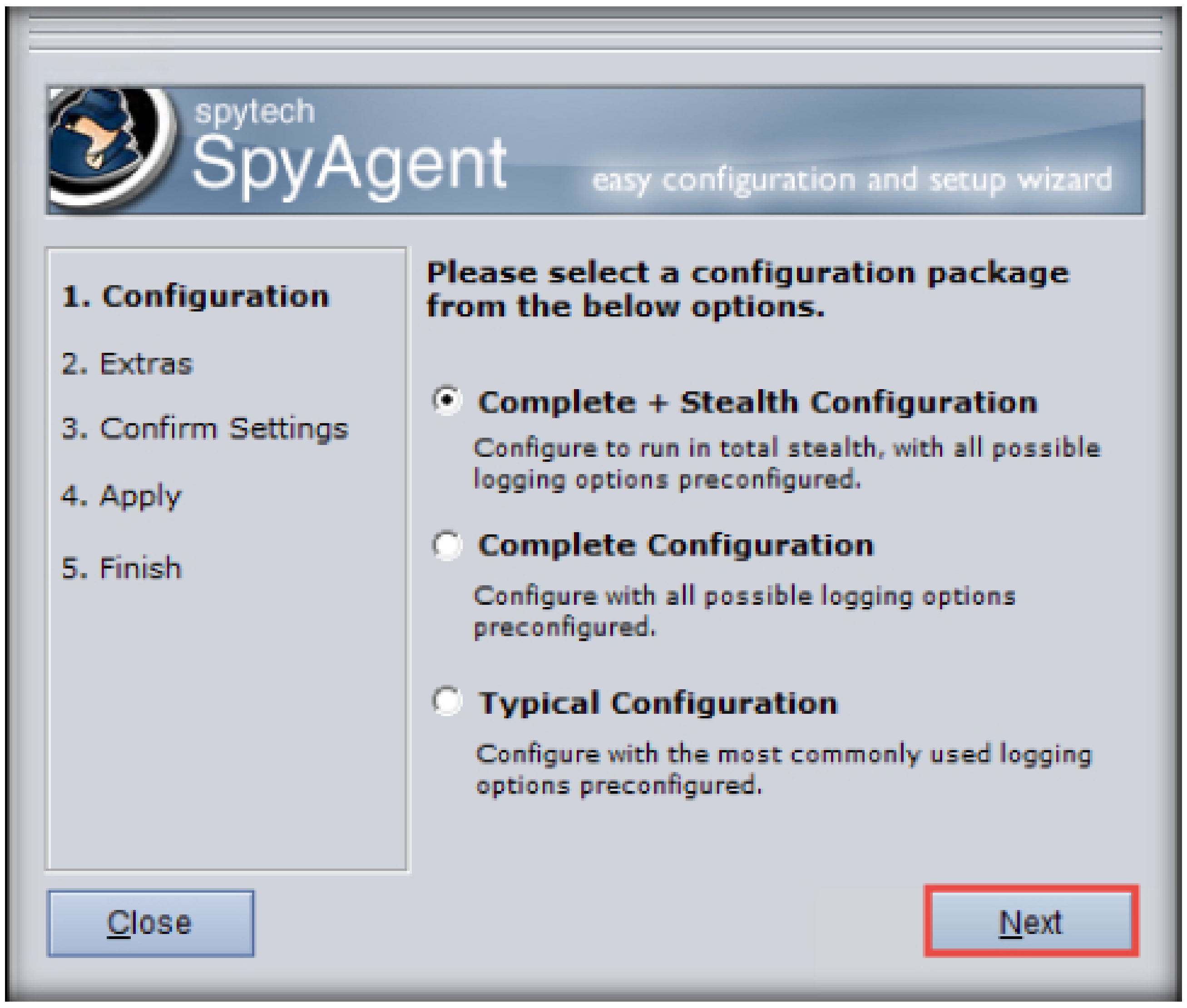


Welcome to SpyAgent! (Step 2)

You will now be presented with the Easy Configuration Wizard. You can use this wizard to quickly setup SpyAgent's most frequently used features. You can restart this wizard at any time in the future.

FIGURE 7.21: Spytech SpyAgent Step 2

26. The **Configuration** section of the setup wizard appears; click the **Complete + Stealth Configuration** radio button, and click **Next**.



Please select a configuration package from the below options.

● Complete + Stealth Configuration
Configure to run in total stealth, with all possible logging options preconfigured.

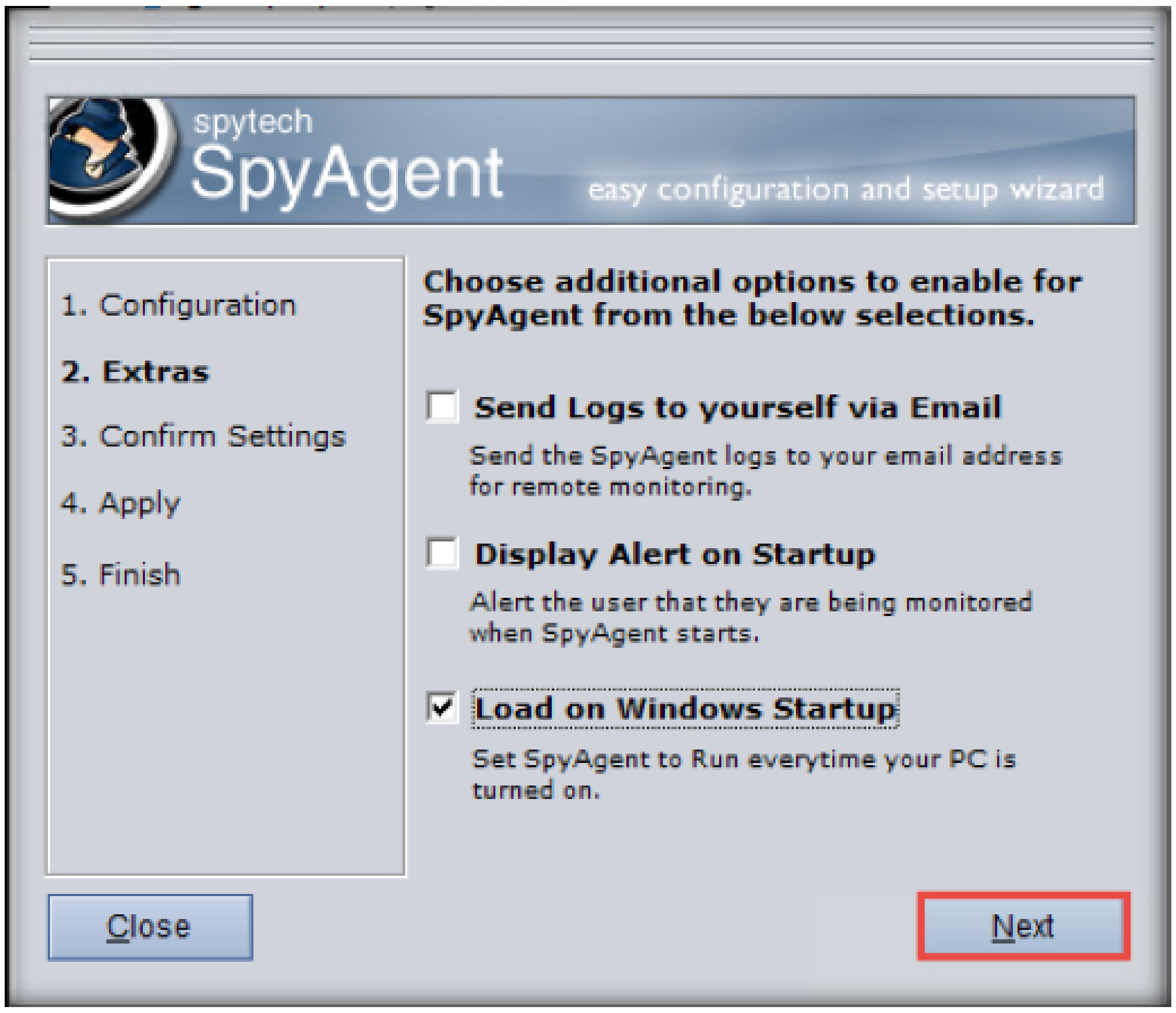
○ Complete Configuration
Configure with all possible logging options preconfigured.

○ Typical Configuration
Configure with the most commonly used logging options preconfigured.

FIGURE 7.22: Spytech SpyAgent Configuration

Emails Sent and ReceivedMonitor and log all emails sent and received by users of your computer! All SMTP and POP3 messages are recorded for later viewing. Attachments are logged as well.

27. The **Extras** section of the setup wizard appears; check the **Load on Windows Startup** option, and click **Next**.



Choose additional options to enable for SpyAgent from the below selections.

□ Send Logs to yourself via Email
Send the SpyAgent logs to your email address for remote monitoring.

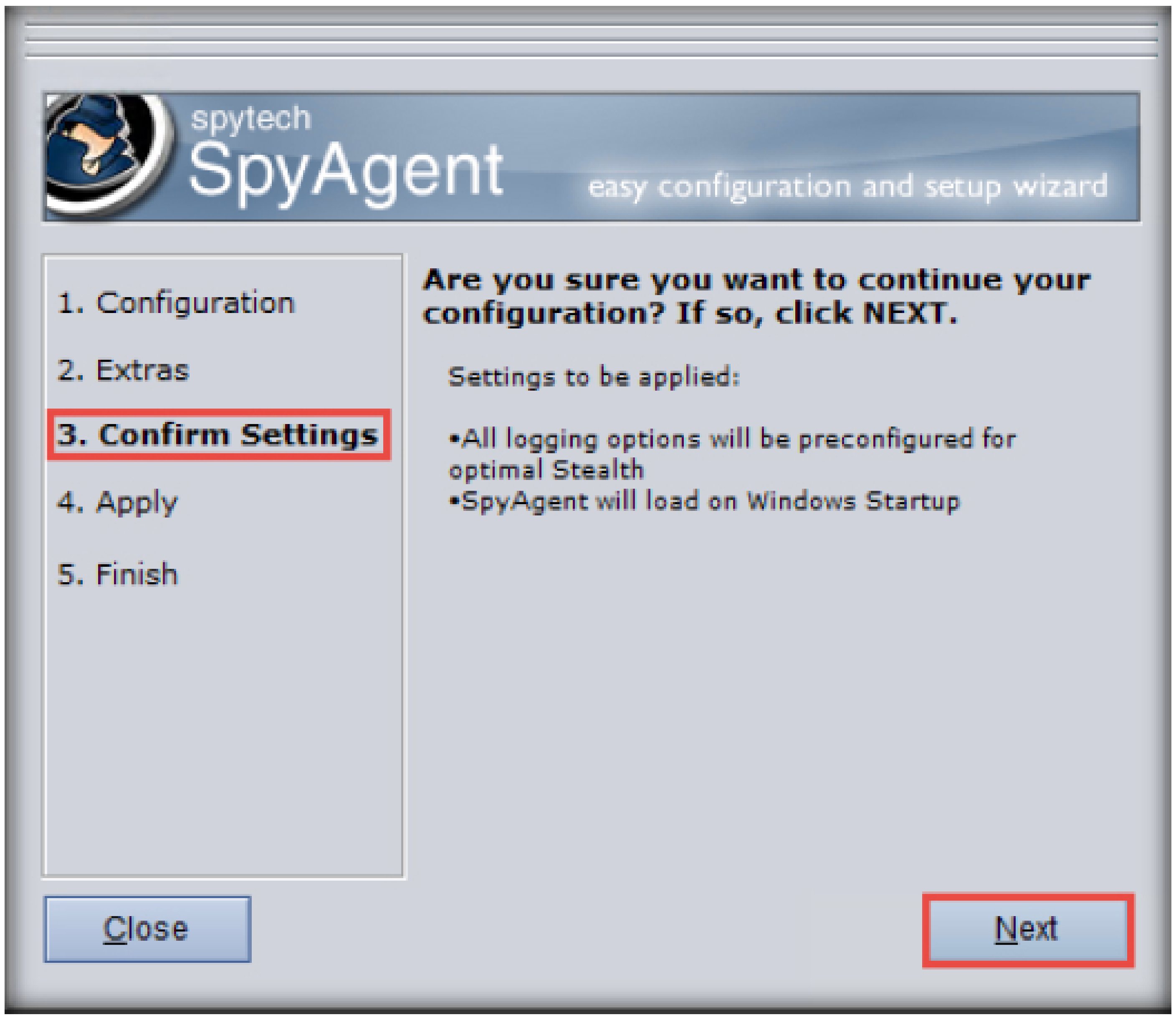
□ Display Alert on Startup
Alert the user that they are being monitored when SpyAgent starts.

☑ Load on Windows Startup
Set SpyAgent to Run everytime your PC is turned on.

FIGURE 7.23: Spytech SpyAgent Extras

Events Timeline: Logging Log all events users performed and view them in an organized chronically ordered listing. The Events Timeline lets you view what the events the user performed, in the order they did them. Events logged include Program Starts/Stops, Keystrokes Typed, Email and Chat Messages, Website Visits, Document Viewings and Printings, how long users were active and idle each session, and more.

28. The **Confirm Settings** section of the setup wizard appears; click **Next** to continue.



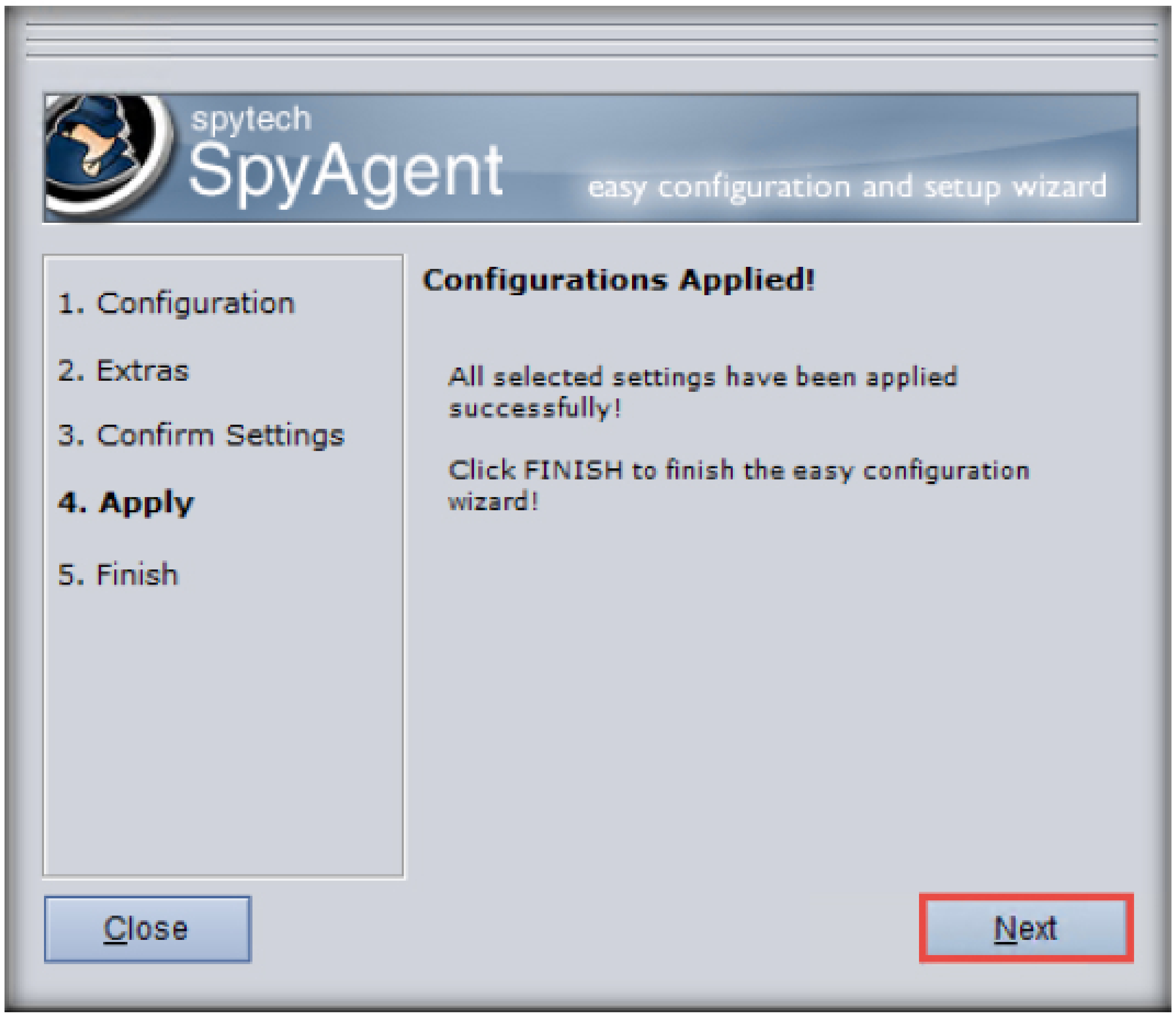
Are you sure you want to continue your configuration? If so, click NEXT.

Settings to be applied:

•All logging options will be preconfigured for optimal Stealth
•SpyAgent will load on Windows Startup

FIGURE 7.24: Spytech SpyAgent Confirm Settings

29. The **Apply** section of the setup wizard appears; click **Next**.



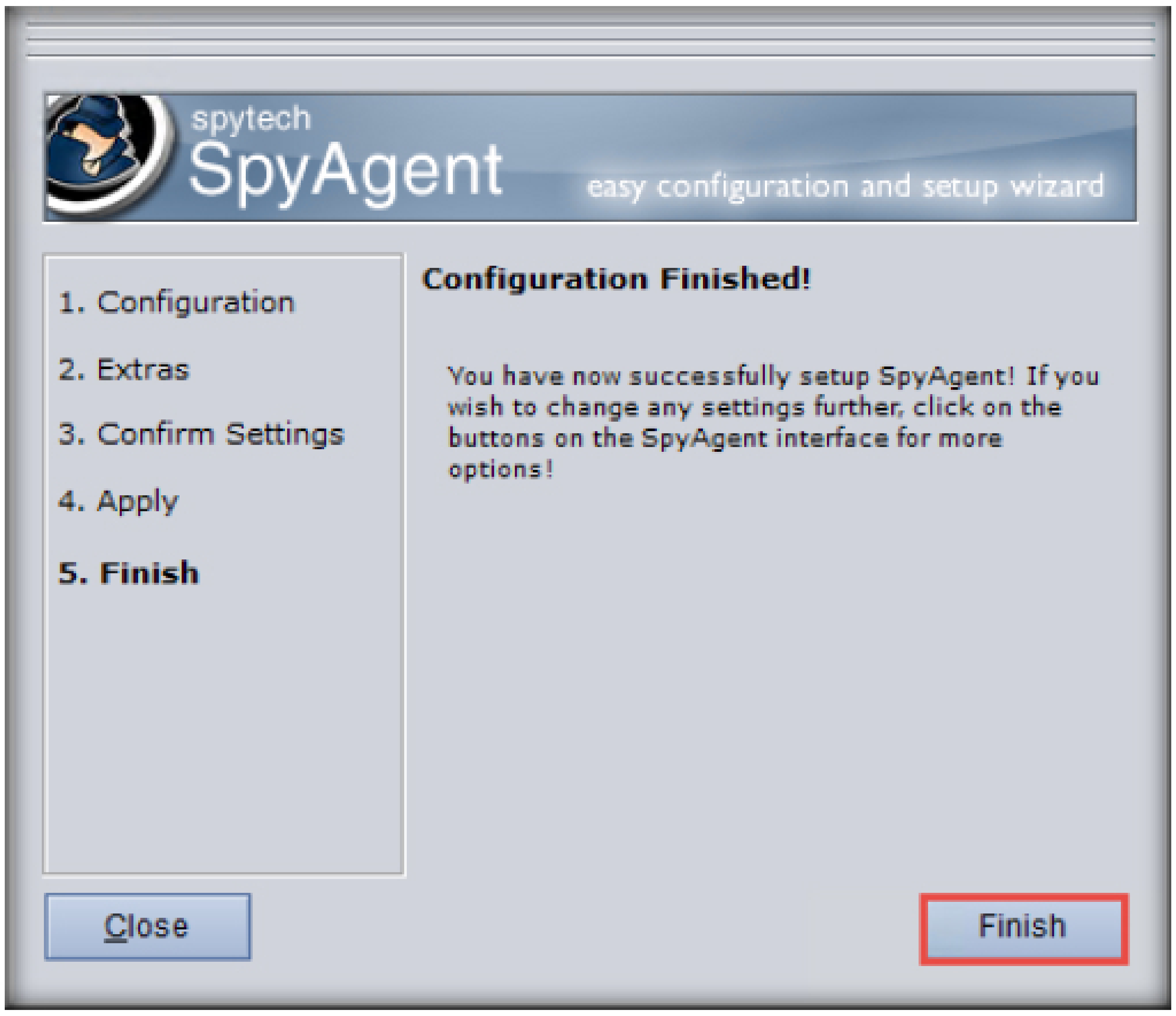
**Configurations Applied!**

All selected settings have been applied successfully!

Click FINISH to finish the easy configuration wizard!

FIGURE 7.25: Spytech SpyAgent Applying Configuration

30. The **Configuration Finished** window appears, click **Finish** to successfully setup SpyAgent.



**Configuration Finished!**

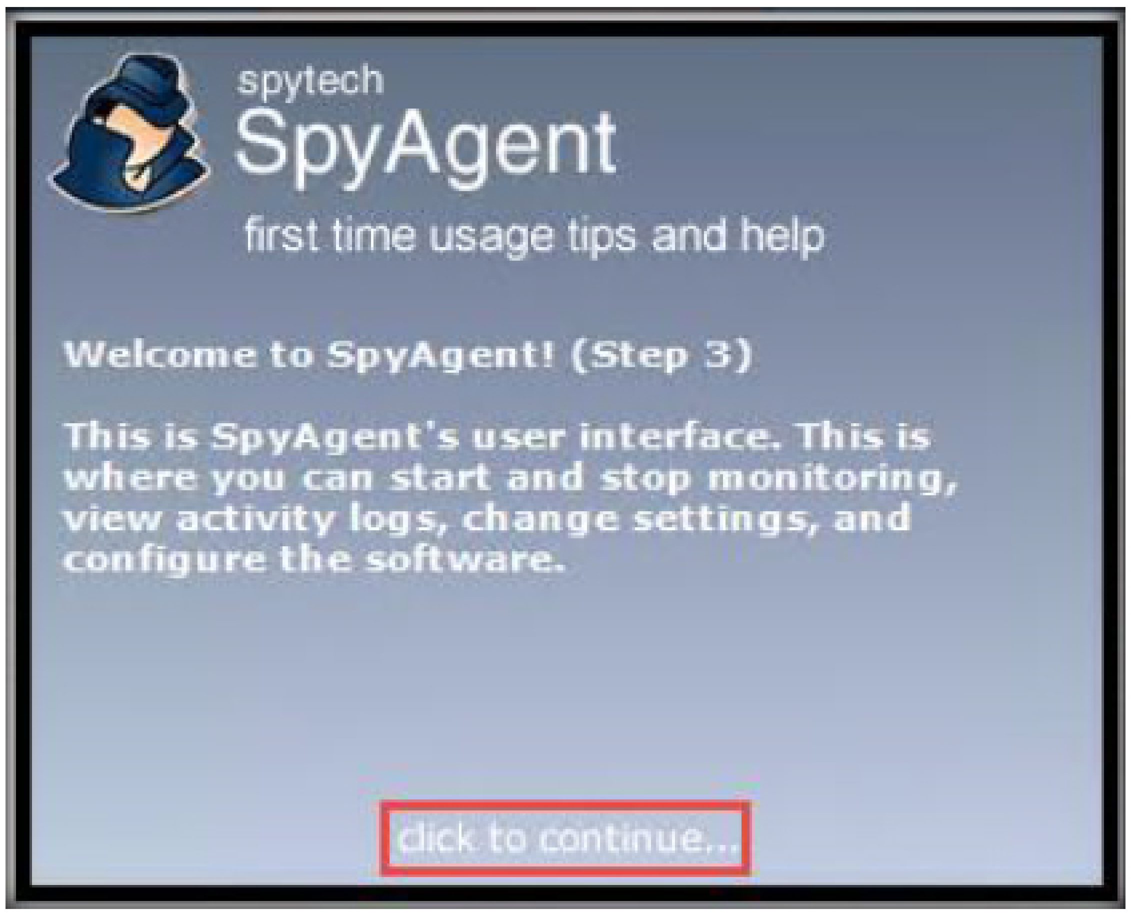
You have now successfully setup SpyAgent! If you wish to change any settings further, click on the buttons on the SpyAgent interface for more options!

FIGURE 7.26: Spytech SpyAgent Configuration Finish

Internet Chat:: Conversations Monitor and log both sides of all chat conversations made on chat clients. Supported clients include the latest versions of: AOL (including 9.0 and Optimized), AOL Instant Messenger, AIM, Yahoo Messenger, Excite Messenger, GoogleTalk, Skype, XFire, and ICQ.

31. The main **SpyAgent** window appears, along with **Step 3** of the setup wizard.

32. Select **click to continue....**



spytech SpyAgent

first time usage tips and help

Welcome to SpyAgent! (Step 3)

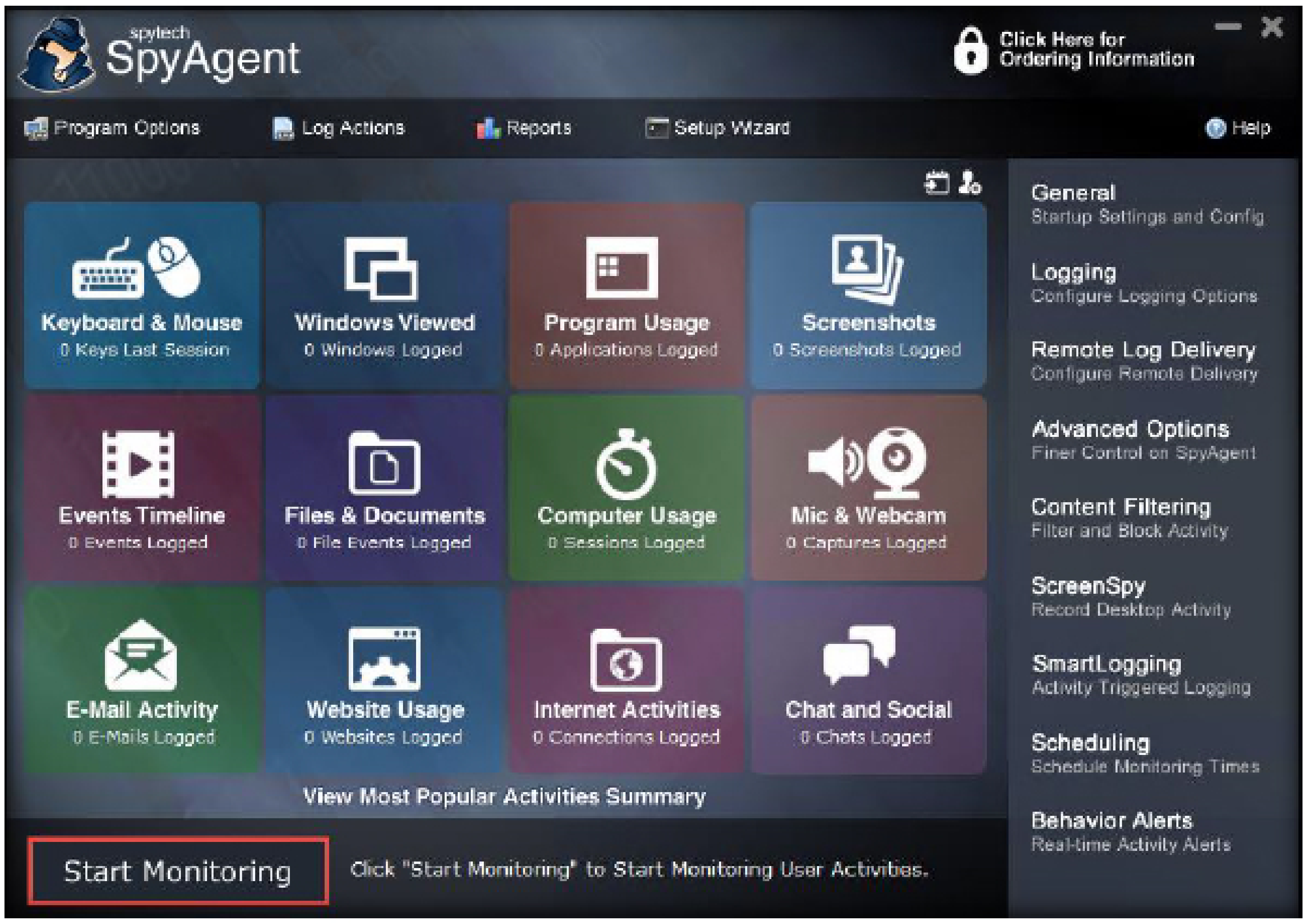
This is SpyAgent's user interface. This is where you can start and stop monitoring, view activity logs, change settings, and configure the software.

click to continue...

FIGURE 7.27: Spytech SpyAgent Step 3

33. If a **Getting Started** dialog-box appears, click **No**.

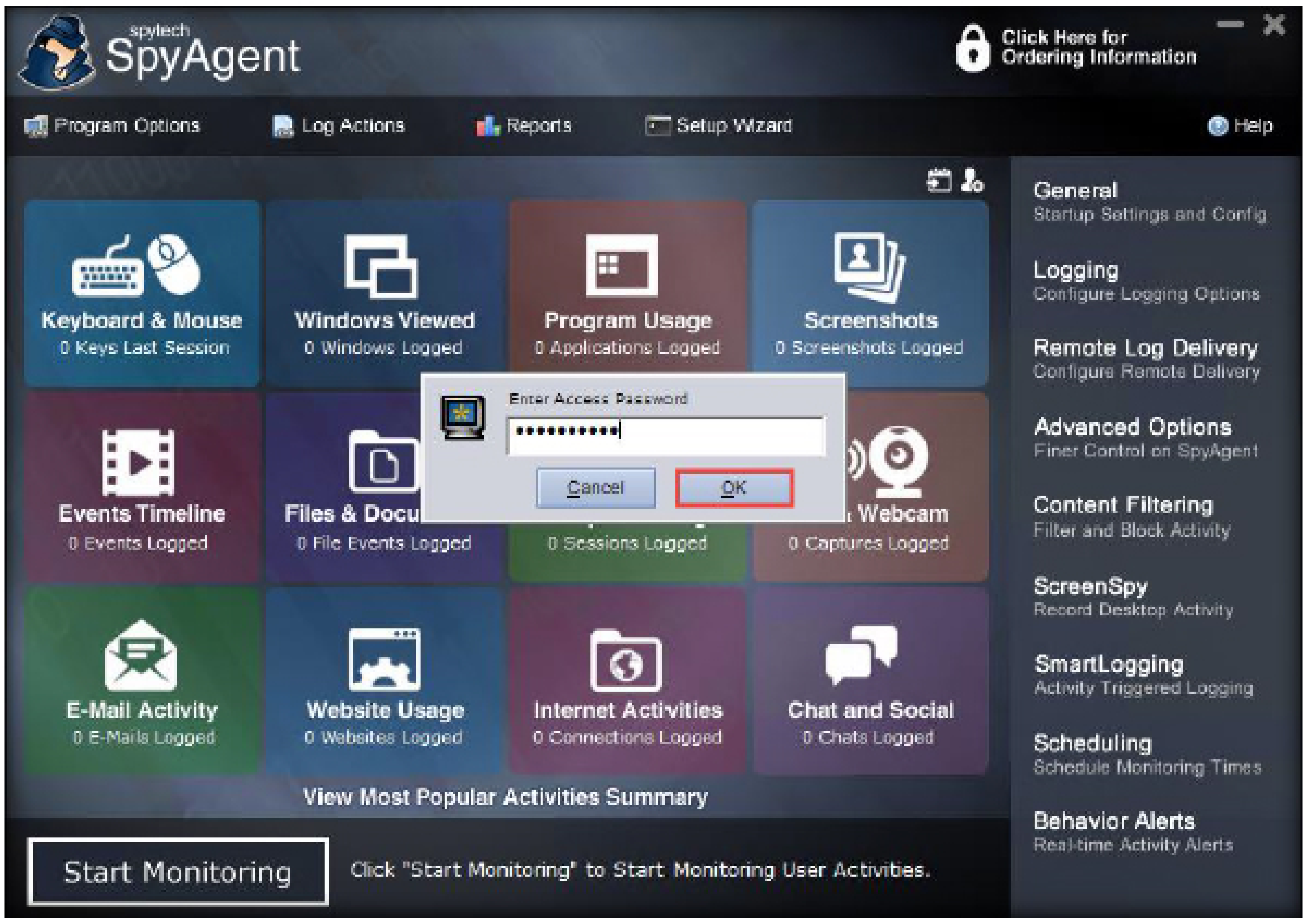
34. To track the general user activities, click **Start Monitoring**.



Click "Start Monitoring" to Start Monitoring User Activities.

FIGURE 7.28: Spytech SpyAgent Start Monitoring

35. The **Enter Access Password** window appears, enter the **password** specified in **step 23** (in this lab, **qwerty@123**), then click **OK**.



Enter Access Password

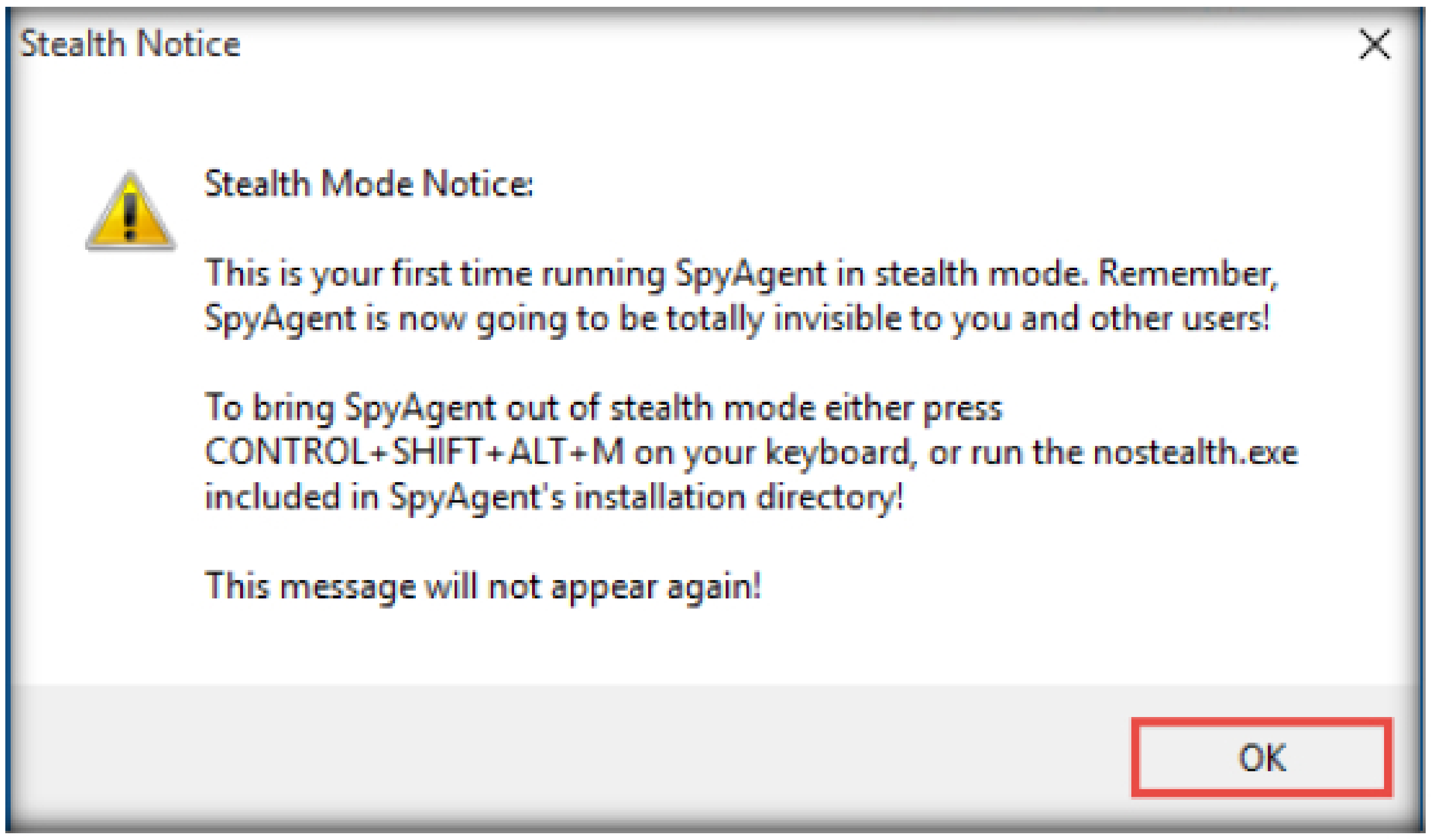
••••••••••

FIGURE 7.29: Spytech SpyAgent Enter Access Password

Website Activity: Log all website visits and online searches performed by the popular browsers used today. All website visits are logged by website address, username, and time of the site visit. SpyAgent also logs how long users visit each website so you can easily see what websites are visited the longest. SpyAgent supports the latest versions of the following browsers: Internet Explorer, Opera, Mozilla, Firefox, Flock, Google Chrome, and America Online.

36. The **Stealth Notice** window appears. Read the instructions then click **OK**.

**Note**: To bring SpyAgent out of stealth mode, press **Ctrl+Shift+Alt+M**



Stealth Notice

Stealth Mode Notice:

This is your first time running SpyAgent in stealth mode. Remember, SpyAgent is now going to be totally invisible to you and other users!

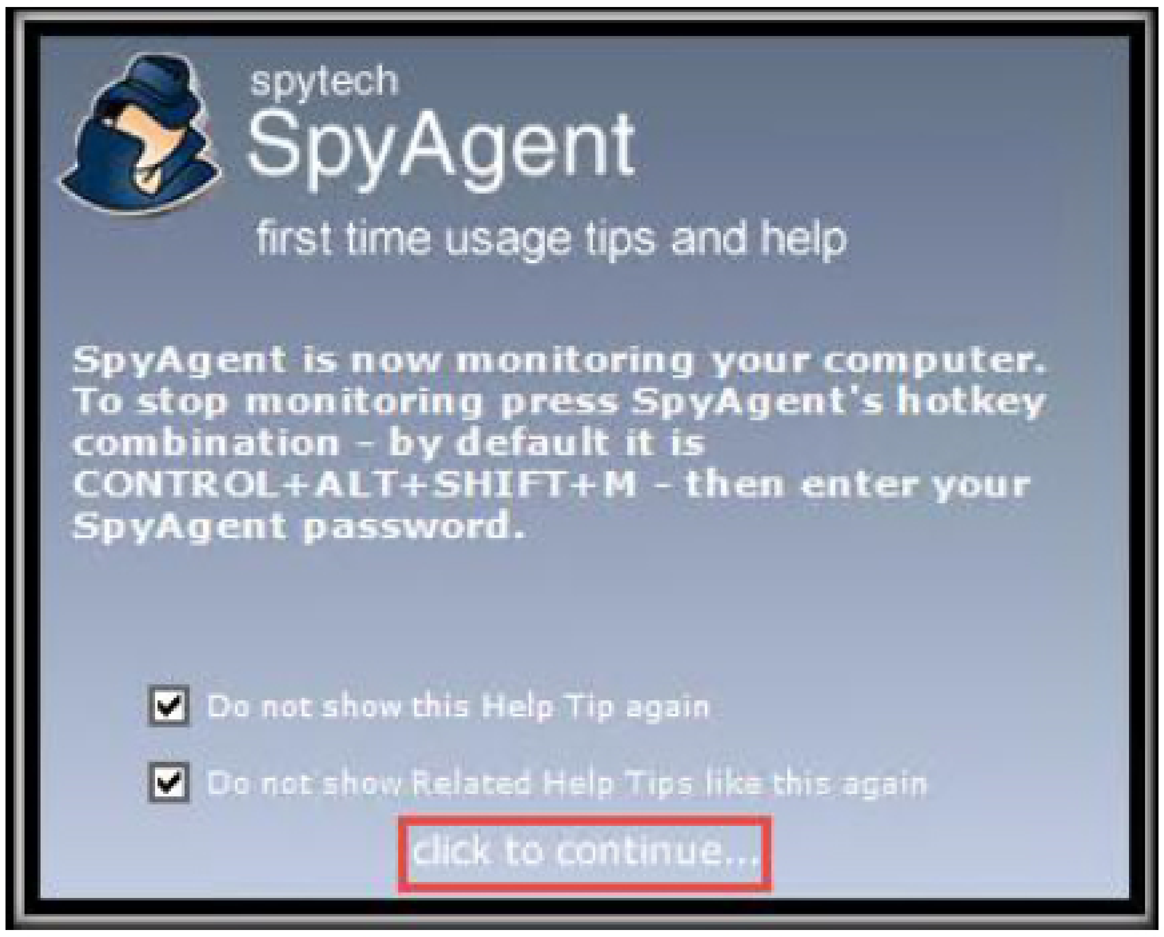
To bring SpyAgent out of stealth mode either press CONTROL+SHIFT+ALT+M on your keyboard, or run the nostealth.exe included in SpyAgent's installation directory!

This message will not appear again!

FIGURE 7.30: Spytech SpyAgent Stealth Mode Notice

37. A SpyAgent pop-up appears. Check the **Do not show this Help Tip again** and the **Do not show Related Help Tips like this again**, then select **click to continue....**

Application Usage: Monitor and log all applications ran by users - SpyAgent logs when the application was started, stopped, and how long it was actually used. Users cannot fool SpyAgent by simply opening a program and leaving it running in the background - SpyAgent will know how long the program was actually used.



SpyAgent is now monitoring your computer. To stop monitoring press SpyAgent's hotkey combination - by default it is CONTROL+ALT+SHIFT+M - then enter your SpyAgent password.

☑ Do not show this Help Tip again

☑ Do not show Related Help Tips like this again

click to continue...

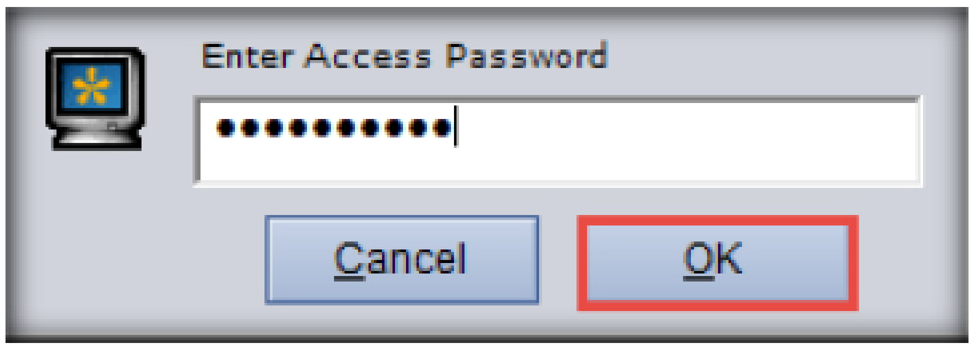
FIGURE 7.31: Spytech SpyAgent Tips

38. Next, close the remote connection and login to the **Windows 10** machine as a domain user (Username: **CND\Martin** and Password: **qwerty@123**). Perform random activities such as browsing webpages, etc...

39. Switch back to the **Windows Server 2012** machine and establish a new Remote Desktop Connection (RDC) to connect to the **Windows 10** machine (follow steps from **1** to **7 in** this lab exercise).

40. To bring SpyAgent out of stealth mode, press **CTRL+Shift+Alt+M** on the keyboard.

41. SpyAgent will ask for the Access Password (**qwerty@123**), enter the password and click **OK**.



Enter Access Password

••••••••••

FIGURE 7.32: Spytech SpyAgent Accessing from stealth mode

Webmail and Website Content:: Log webmail messages from most major webmail providers - such as Gmail, Yahoo Mail, and MySpace webmail. SpyAgent logs incoming messages read by the user, as well as messages they send out through webmail. All website content visited can be logged as well.

42. To check user keystrokes from the keyboard, click **Keyboard & Mouse** on the **SpyAgent** GUI.

43. Select the **View Keystrokes Log**.

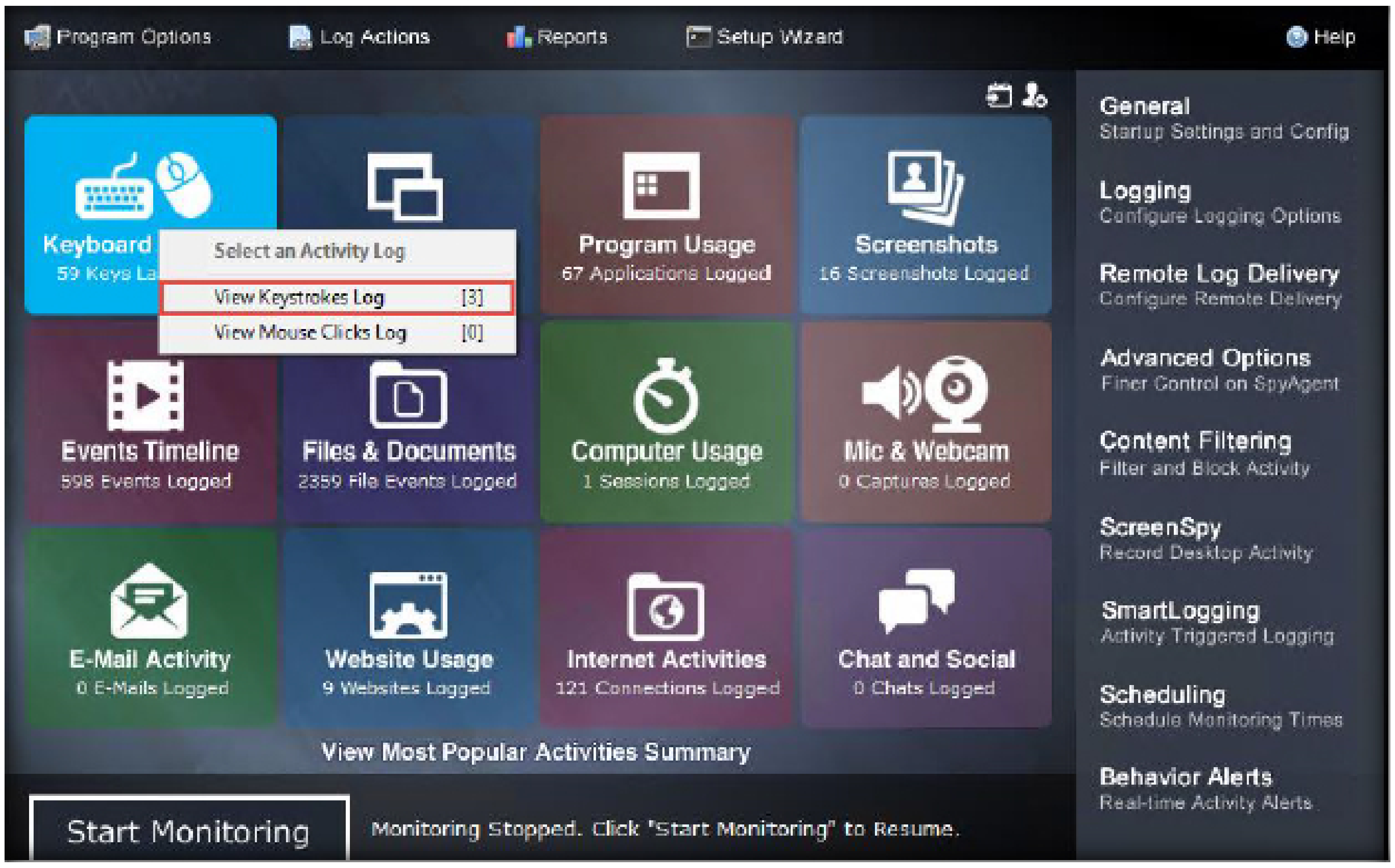
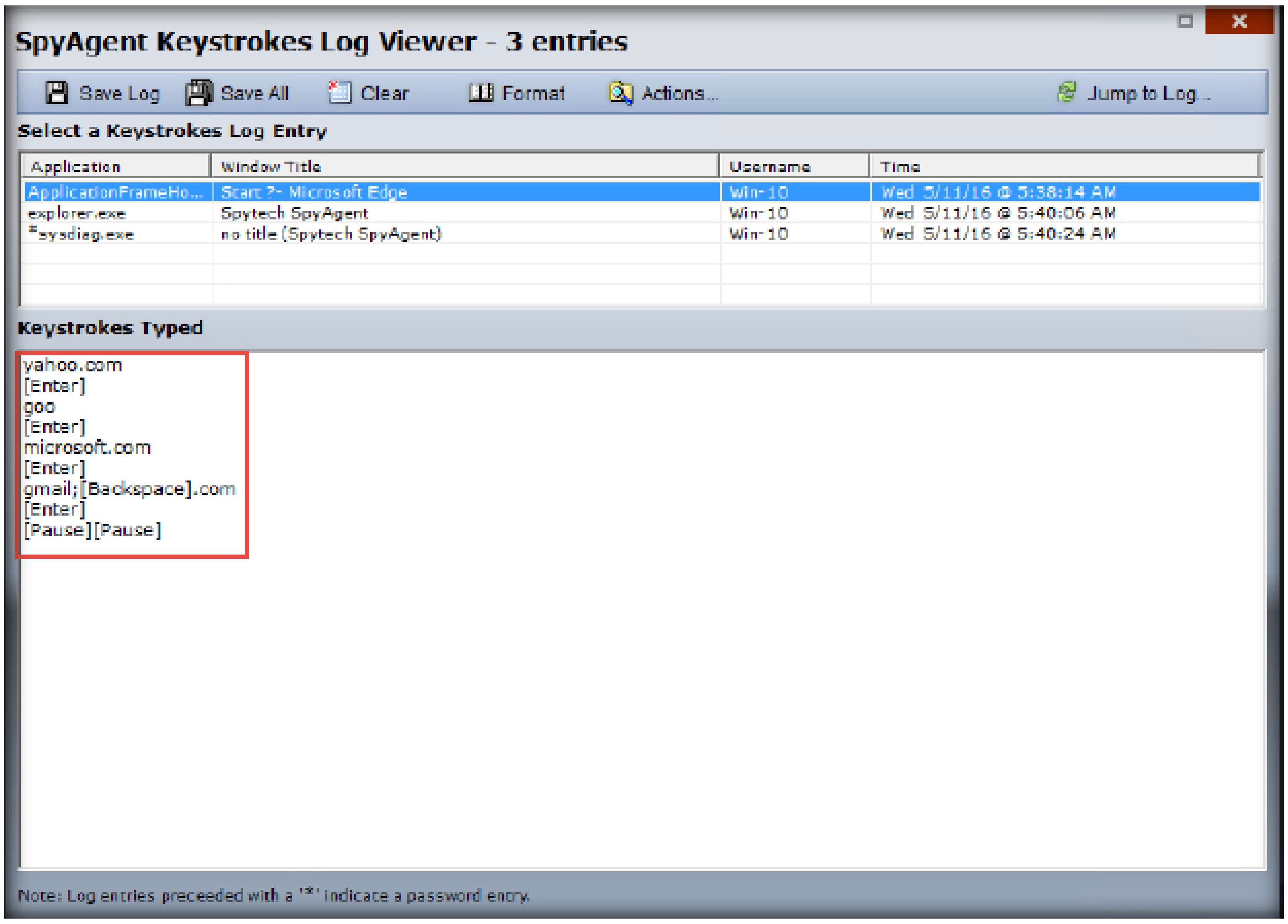


FIGURE 7.33: Spytech SpyAgent Viewing recorded keystrokes

44. The keystroke logs pressed by the user can be reviewed by simply selecting them.

Intelligent Screenshot Capturing: SpyAgent can take snapshots of your desktop at set intervals of time, whenever the mouse is clicked, or whenever websites are visited, allowing you to visually see what is happening at all times. The screenshot capture manager has a built-in video-like slideshow playback for easy viewing, and screenshots are categorized by content - social networking, webmail, website usage, and more. The screenshot capturing can be configured to increase its capture frequency when window captions containing specific keywords are interacted with so vital information is not missed.



SpyAgent Keystrokes Log Viewer - 3 entries

Select a Keystrokes Log Entry

| Application | Window Title | Username | Time |
|---|---|---|---|
| ApplicationFrameHo... | Start ?- Microsoft Edge | Win-10 | Wed 5/11/16 @ 5:38:14 AM |
| explorer.exe | Spytech SpyAgent | Win-10 | Wed 5/11/16 @ 5:40:06 AM |
| *sysdiag.exe | no title (Spytech SpyAgent) | Win-10 | Wed 5/11/16 @ 5:40:24 AM |

Keystrokes Typed

```
yahoo.com
[Enter]
goo
[Enter]
microsoft.com
[Enter]
gmail;[Backspace].com
[Enter]
[Pause][Pause]
```

Note: Log entries preceeded with a '*' indicate a password entry.

FIGURE 7.34: Spytech SpyAgent Keystrokes Recorded

45. In this way you can view screenshots, program usage, chat & messages, and many other user activities on the user's computer.

## Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion regarding your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

| Internet Connection Required | |
|---|---|
| ☐ Yes | ☑ No |
| **Platform Supported** | |
| ☑ Classroom | ☑ iLabs |

Lab

8

# Auditing System Information using MSINFO32

*MSINFO32allows you to view details about the hardware and software configuration on your machine.*

## Lab Scenario

Sometimes, an administrator needs to know the software and hardware configuration to diagnose issues in the network. Windows OS provides System Information or the MSInfo Utility or msinfo32.exe to gather information about the computer, to diagnose issues or to access other tools. An Administrator can use the MSInfo Utility to perform system auditing to know the current software and hardware configuration on a specific Windows system.

**ICON KEY**

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

## Lab Objectives

This lab will demonstrate the use of the MSInfo Utility to view the software and hardware configuration on a specific Windows system.

## Lab Environment

To carry out the lab, you need:

- A virtual machine running Windows 10.

## Lab Duration

Time: 25 Minutes

## Overview of MSInfo

With the MSInfo Utility, you can view the information about a Windows system. It provides information such as:

- OEM System Information (manufacturer, model, and type)
- The type of central processing unit (CPU)
- The amount of memory and system resources

- BIOS version
- Locale
- Time zone
- User name in the format of DOMAINNAME\USERNAME (only present if the computer is configured for a domain)
- Boot device (if multiple devices are present on the computer)
- The path to the Page file
- Hardware Resources category

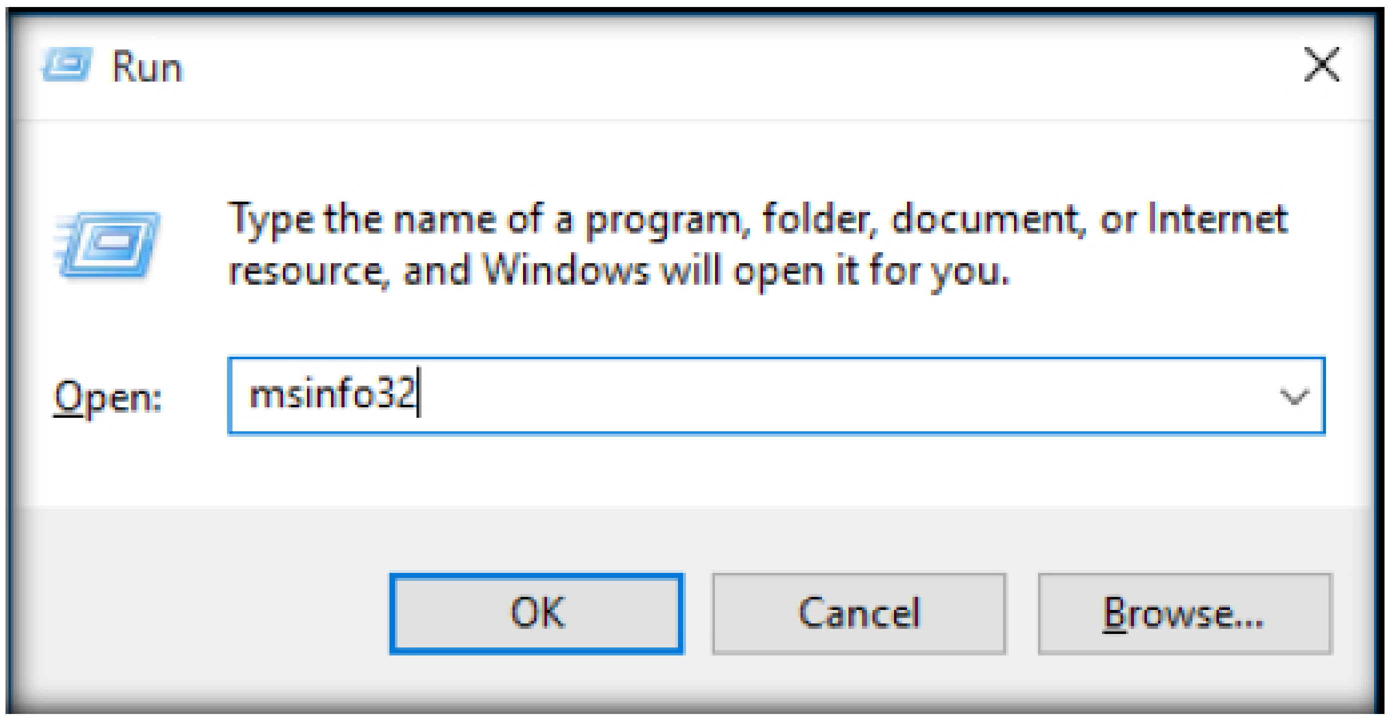
## Lab Tasks

**TASK 1**

**Launching System Information window**

Note: To locate the problem areas, you can compare the current configuration of the machine with a known good configuration.

1. Launch the **Windows 10** machine as a Local Administrator.
2. Press the **Windows and R keys**. The **Run** window pops up. Enter **msinfo32** in the **Open** section and click **Enter**.



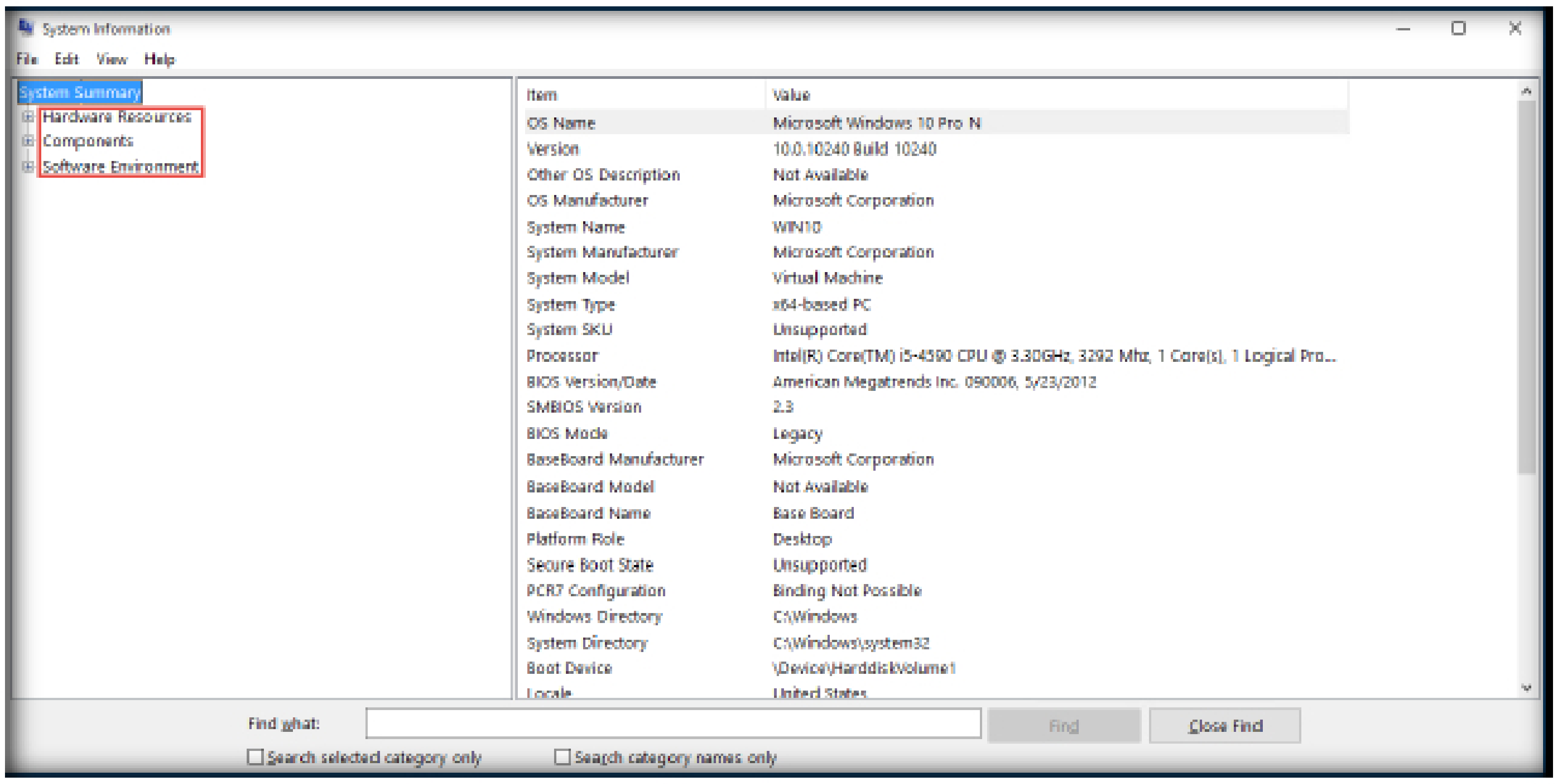
Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: msinfo32

FIGURE 8.1: RUN pop-up

3. The **System Information** window pops up. You can view the system summary where you can see the Hardware Resources, Components and Software Environment configured on the system.



| Item | Value |
|---|---|
| OS Name | Microsoft Windows 10 Pro N |
| Version | 10.0.10240 Build 10240 |
| Other OS Description | Not Available |
| OS Manufacturer | Microsoft Corporation |
| System Name | WIN10 |
| System Manufacturer | Microsoft Corporation |
| System Model | Virtual Machine |
| System Type | x64-based PC |
| System SKU | Unsupported |
| Processor | Intel(R) Core(TM) i5-4590 CPU @ 3.30GHz, 3292 Mhz, 1 Core(s), 1 Logical Pro... |
| BIOS Version/Date | American Megatrends Inc. 090006, 5/23/2012 |
| SMBIOS Version | 2.3 |
| BIOS Mode | Legacy |
| BaseBoard Manufacturer | Microsoft Corporation |
| BaseBoard Model | Not Available |
| BaseBoard Name | Base Board |
| Platform Role | Desktop |
| Secure Boot State | Unsupported |
| PCR7 Configuration | Binding Not Possible |
| Windows Directory | C:\Windows |
| System Directory | C:\Windows\system32 |
| Boot Device | \Device\HarddiskVolume1 |
| Locale | United States |

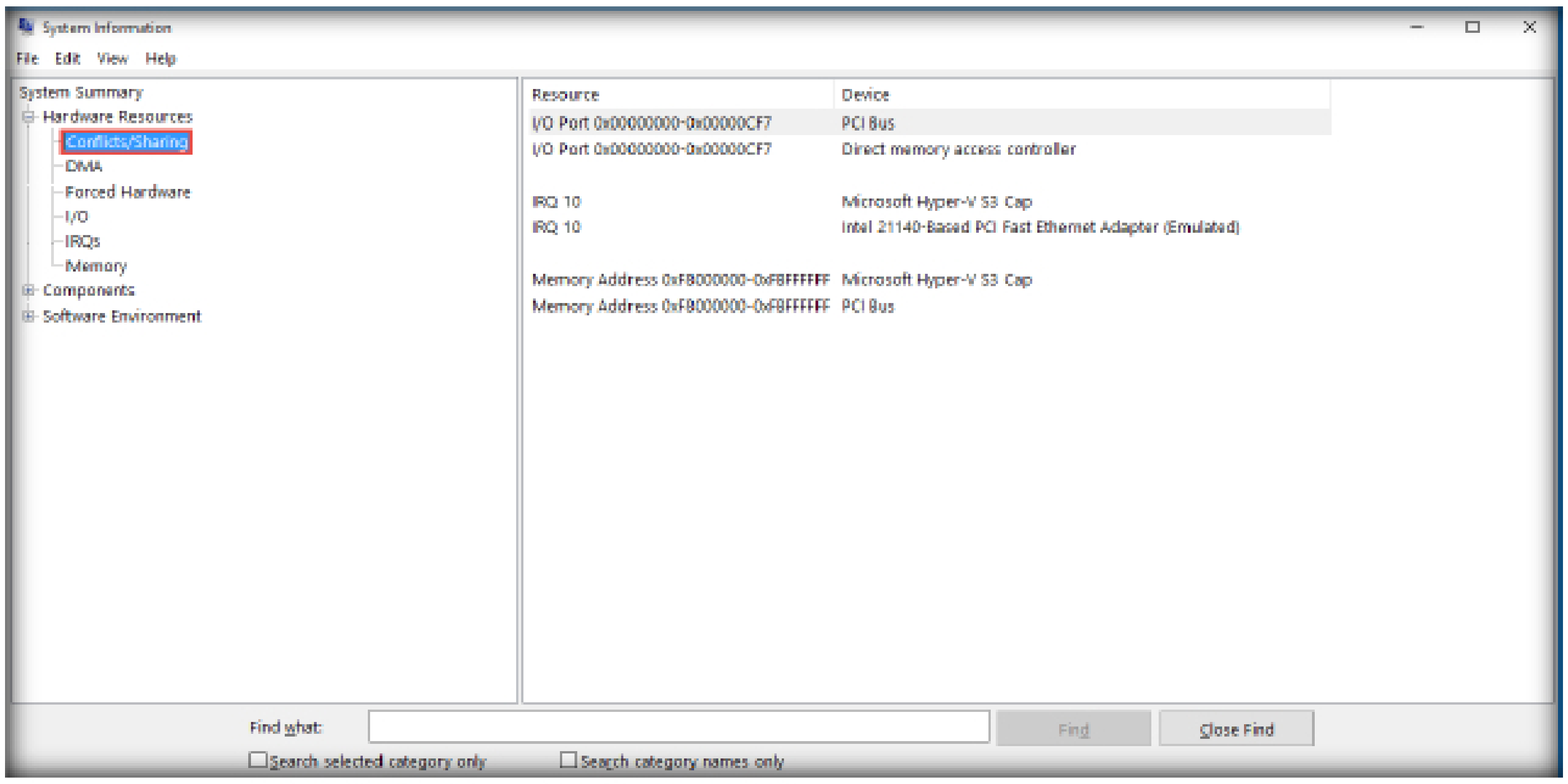
FIGURE 8.2: System Information (MSINFO) Window

**TASK 2**

**Knowing the Hardware resources used by the system**

4. Expand **Hardware Resources**

5. The first subsection of **Hardware Resources** is **Conflicts/Sharing**. Click it to view its results in the right pane.



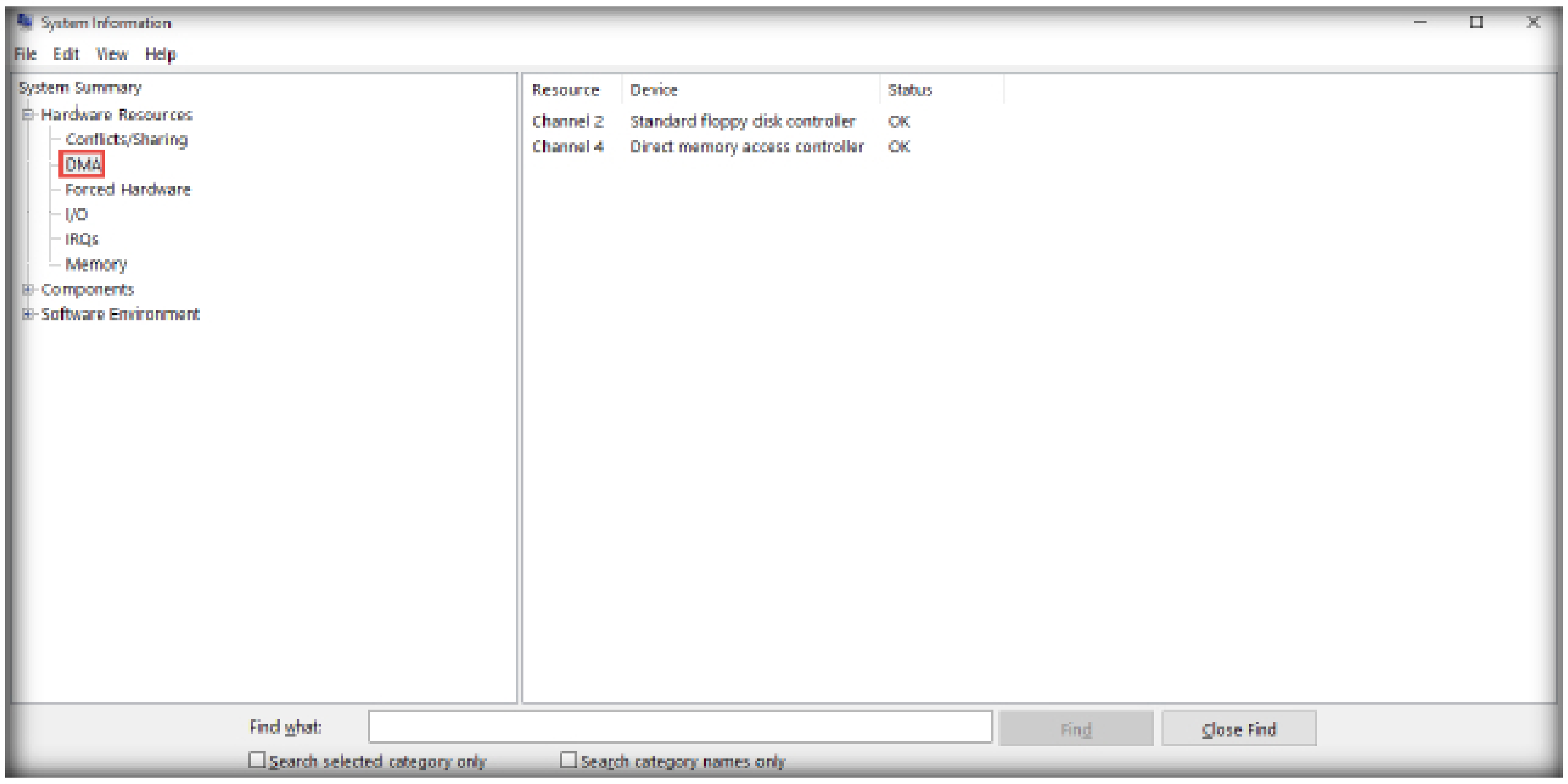
| Resource | Device |
|---|---|
| I/O Port 0x00000000-0x00000CF7 | PCI Bus |
| I/O Port 0x00000000-0x00000CF7 | Direct memory access controller |
| | |
| IRQ 10 | Microsoft Hyper-V S3 Cap |
| IRQ 10 | Intel 21140-Based PCI Fast Ethernet Adapter (Emulated) |
| | |
| Memory Address 0xF8000000-0xFBFFFFFF | Microsoft Hyper-V S3 Cap |
| Memory Address 0xF8000000-0xFBFFFFFF | PCI Bus |

FIGURE 8.3: System Information Hardware Resources

6. You can view the devices which share the same resources. If any device has an issue and is listed in shared devices, it might be due to a resource usage conflict.

7. Next, is the subsection **Direct memory access (DMA)**. In DMA, data is transferred directly from the memory to the hardware without involving the CPU.

8. You can view a device which has **DMA access** by clicking on DMA.

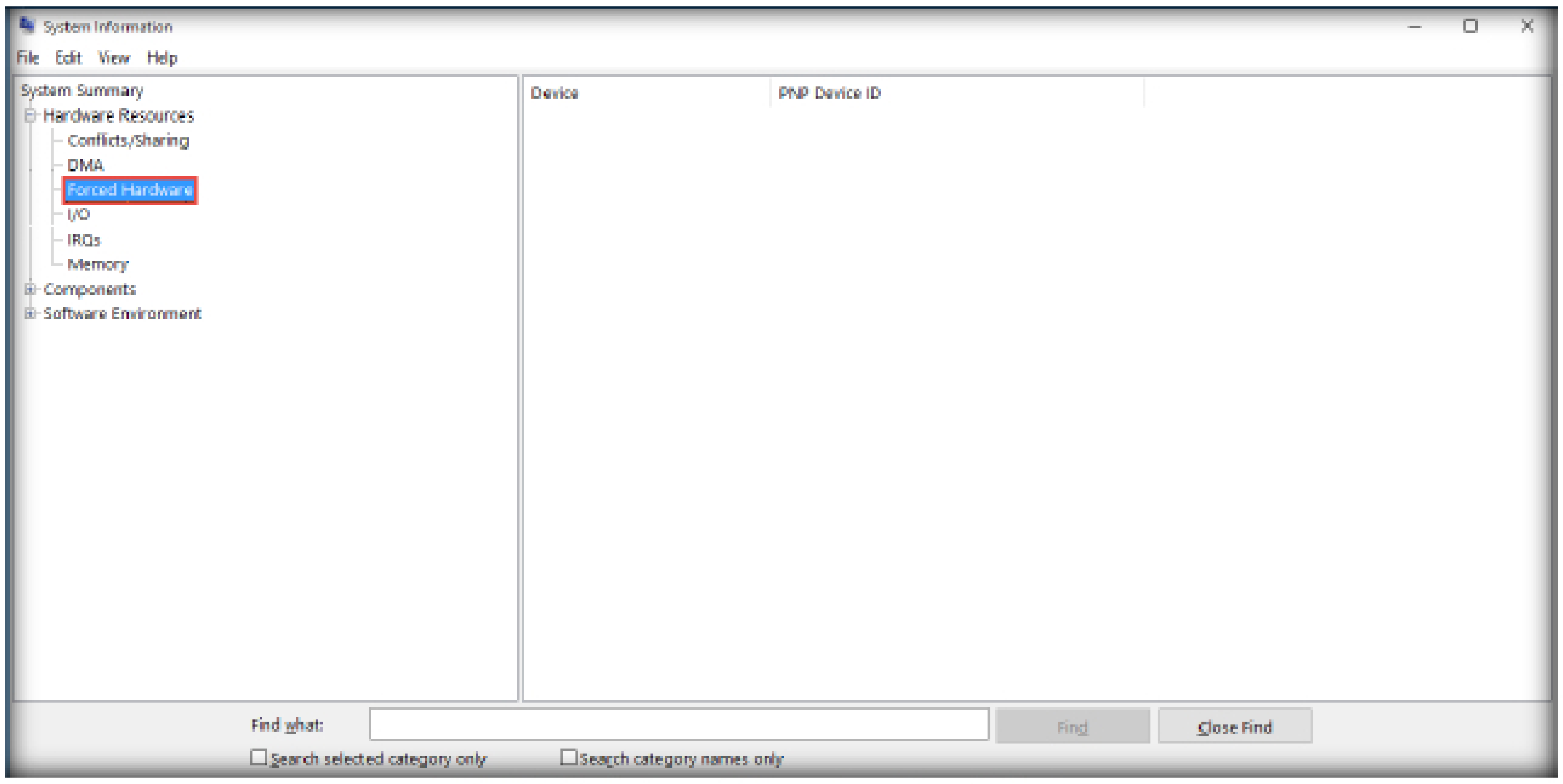


| Resource | Device | Status |
|---|---|---|
| Channel 2 | Standard floppy disk controller | OK |
| Channel 4 | Direct memory access controller | OK |

FIGURE 8.4: System Information DMA

9. If the status is showing up in an error state, you should update the drivers or contact the manufacturer.

10. The next subsection is **Forced Hardware**. It lists any devices which are configured manually by the user. It normally lists the plug and play (PnP) devices.



| Device | PNP Device ID |
|---|---|

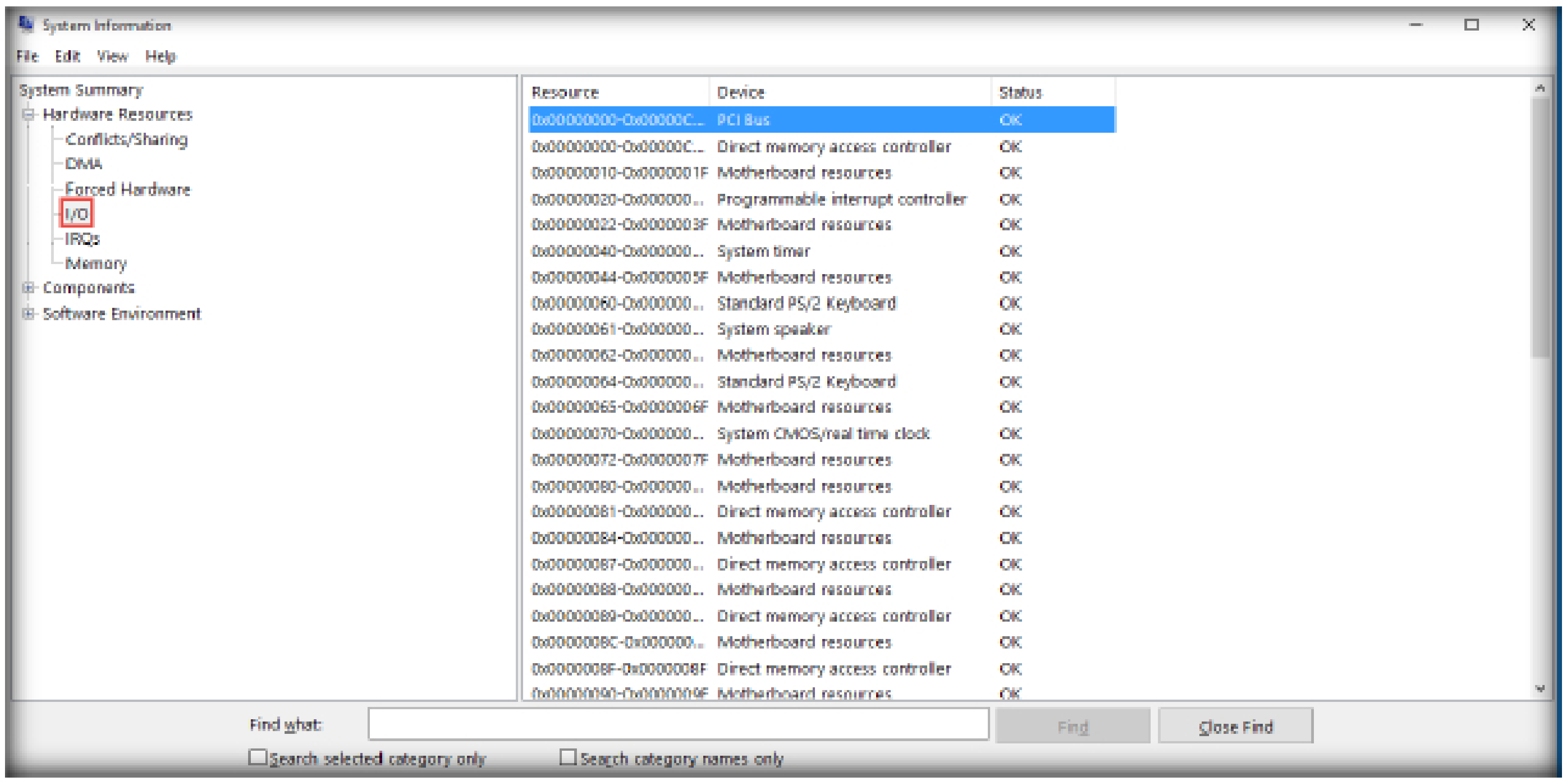
FIGURE 8.5: System Information Forced Hardware

11. **Forced hardware** uses user specific resources and not system specific resources like regular hardware devices.

12. The next subsection deals with system resources. Let's look at the first resource which is Input/Output (**I/O**).

The resource column indicates which resource has been allocated to which device. The corresponding device shows up in the Device column

13. I/O transfers data from a **computer to device** and **vice versa**.

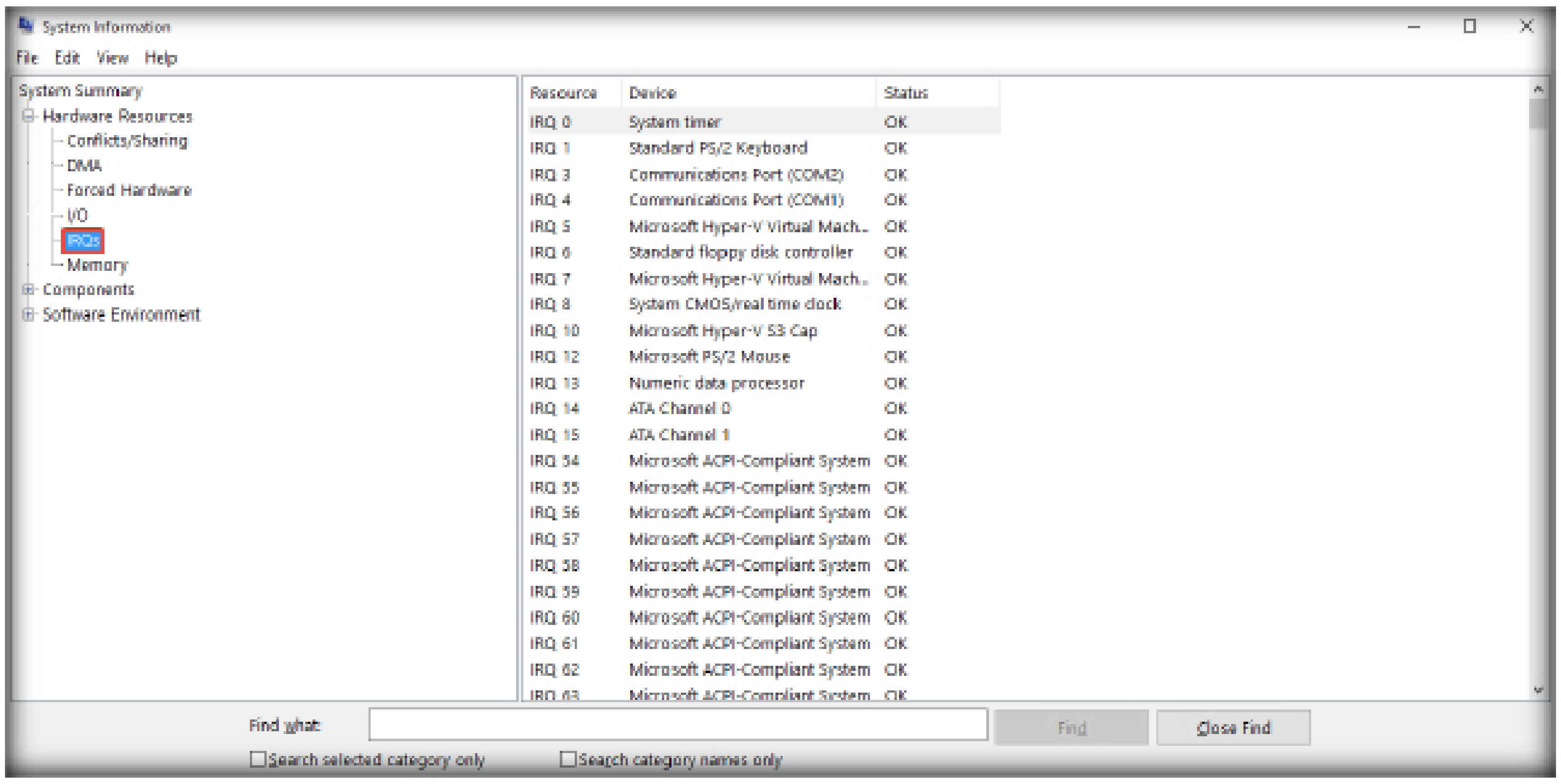


| Resource | Device | Status |
|---|---|---|
| 0x00000000-0x00000C... | PCI Bus | OK |
| 0x00000000-0x00000C... | Direct memory access controller | OK |
| 0x00000010-0x0000001F | Motherboard resources | OK |
| 0x00000020-0x000000... | Programmable interrupt controller | OK |
| 0x00000022-0x0000003F | Motherboard resources | OK |
| 0x00000040-0x000000... | System timer | OK |
| 0x00000044-0x0000005F | Motherboard resources | OK |
| 0x00000060-0x000000... | Standard PS/2 Keyboard | OK |
| 0x00000061-0x000000... | System speaker | OK |
| 0x00000062-0x000000... | Motherboard resources | OK |
| 0x00000064-0x000000... | Standard PS/2 Keyboard | OK |
| 0x00000065-0x0000006F | Motherboard resources | OK |
| 0x00000070-0x000000... | System CMOS/real time clock | OK |
| 0x00000072-0x0000007F | Motherboard resources | OK |
| 0x00000080-0x000000... | Motherboard resources | OK |
| 0x00000081-0x000000... | Direct memory access controller | OK |
| 0x00000084-0x000000... | Motherboard resources | OK |
| 0x00000087-0x000000... | Direct memory access controller | OK |
| 0x00000088-0x000000... | Motherboard resources | OK |
| 0x00000089-0x000000... | Direct memory access controller | OK |
| 0x0000008C-0x000000... | Motherboard resources | OK |
| 0x0000008F-0x0000008F | Direct memory access controller | OK |
| 0x00000090-0x0000009F | Motherboard resources | OK |

FIGURE 8.6: System Information Input and Output Device

The status column of the I/O shows whether the device running status is OK or has an error.

14. Next is the **(Interrupt request) IRQ**. IRQ is the hardware path through which devices send interrupt signals to the microprocessor.

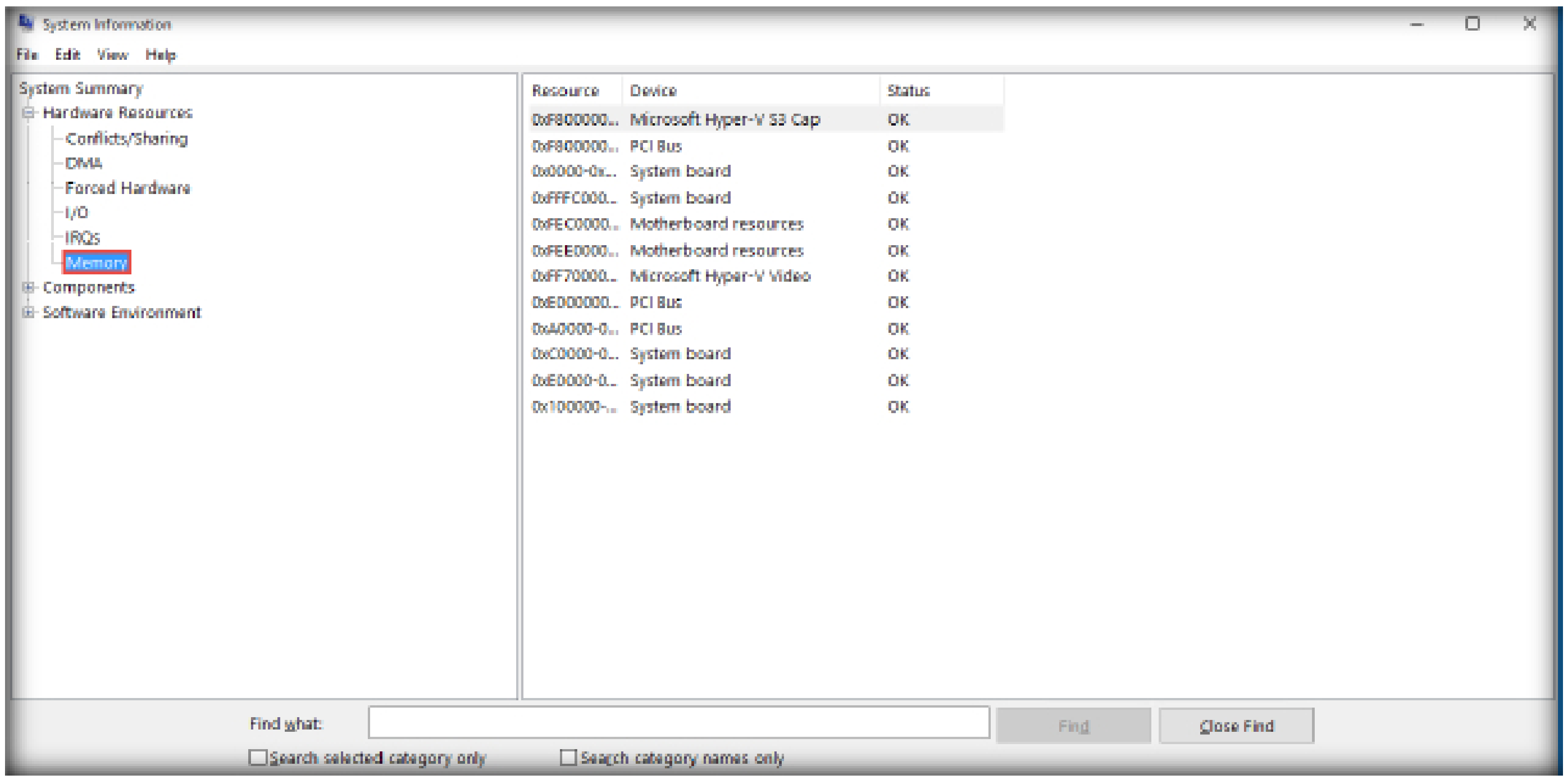


| Resource | Device | Status |
|---|---|---|
| IRQ 0 | System timer | OK |
| IRQ 1 | Standard PS/2 Keyboard | OK |
| IRQ 3 | Communications Port (COM2) | OK |
| IRQ 4 | Communications Port (COM1) | OK |
| IRQ 5 | Microsoft Hyper-V Virtual Mach... | OK |
| IRQ 6 | Standard floppy disk controller | OK |
| IRQ 7 | Microsoft Hyper-V Virtual Mach... | OK |
| IRQ 8 | System CMOS/real time clock | OK |
| IRQ 10 | Microsoft Hyper-V S3 Cap | OK |
| IRQ 12 | Microsoft PS/2 Mouse | OK |
| IRQ 13 | Numeric data processor | OK |
| IRQ 14 | ATA Channel 0 | OK |
| IRQ 15 | ATA Channel 1 | OK |
| IRQ 54 | Microsoft ACPI-Compliant System | OK |
| IRQ 55 | Microsoft ACPI-Compliant System | OK |
| IRQ 56 | Microsoft ACPI-Compliant System | OK |
| IRQ 57 | Microsoft ACPI-Compliant System | OK |
| IRQ 58 | Microsoft ACPI-Compliant System | OK |
| IRQ 59 | Microsoft ACPI-Compliant System | OK |
| IRQ 60 | Microsoft ACPI-Compliant System | OK |
| IRQ 61 | Microsoft ACPI-Compliant System | OK |
| IRQ 62 | Microsoft ACPI-Compliant System | OK |
| IRQ 63 | Microsoft ACPI-Compliant System | OK |

FIGURE 8.7: IRQ's Information

Devices and Operating systems use memory address ranges for communication. The status indicates an OK or error state

15. The final subsection is **Memory**. It explores the memory devices used by the system.



| Resource | Device | Status |
|---|---|---|
| 0xF800000... | Microsoft Hyper-V S3 Cap | OK |
| 0xF800000... | PCI Bus | OK |
| 0x0000-0x... | System board | OK |
| 0xFFFC000... | System board | OK |
| 0xFEC0000... | Motherboard resources | OK |
| 0xFEE0000... | Motherboard resources | OK |
| 0xFF70000... | Microsoft Hyper-V Video | OK |
| 0xE000000... | PCI Bus | OK |
| 0xA0000-0... | PCI Bus | OK |
| 0xC0000-0... | System board | OK |
| 0xE0000-0... | System board | OK |
| 0x100000-... | System board | OK |

FIGURE 8.8: Memory Information

## TASK 3

## Knowing the Components used by the system

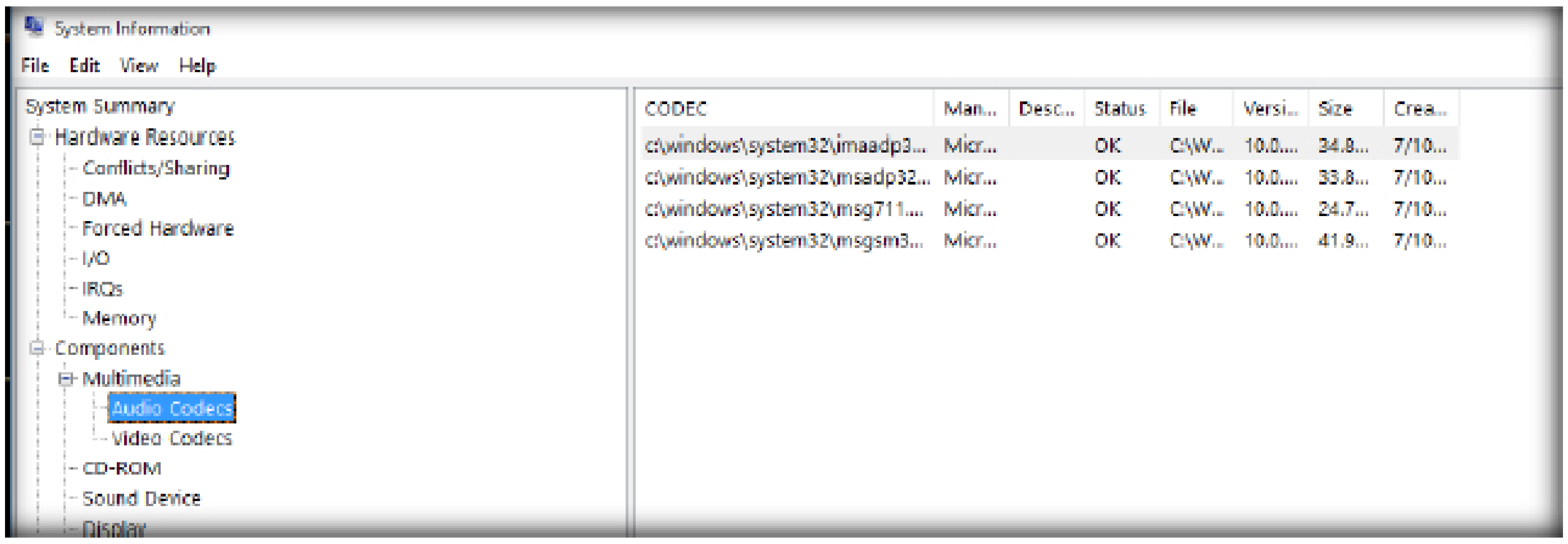
A codec (code-decode), could be either a device or a program which codes ore decodes signals or digital data streams.

In MS info under audio and video codec you can find, the installation location of the codec under the CODEC field.
The manufacturer name is present under the manufacturer column. Some codecs have a description present under description field.

The status shows if a codec is working well or not and the file points to the location and version displays the current codec version.

The size and creation date show the size of a codec on the disk and the date on which it was created.

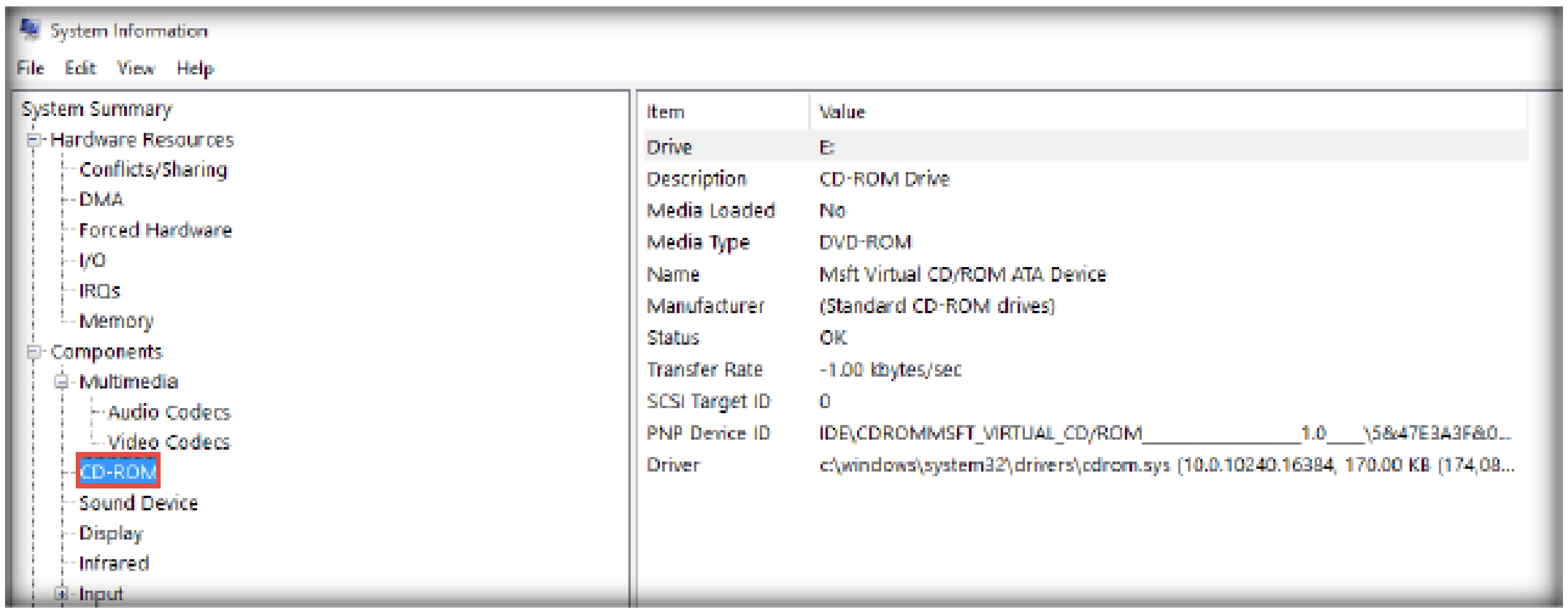
16. The next section is the **Components** section. The first subsection is Multimedia which is a combination of **Audio and Video Codecs**.



| CODEC | Man... | Desc... | Status | File | Versi... | Size | Crea... |
|---|---|---|---|---|---|---|---|
| c:\windows\system32\imaadp3... | Micr... | | OK | C:\W... | 10.0.... | 34.8... | 7/10... |
| c:\windows\system32\msadp32... | Micr... | | OK | C:\W... | 10.0.... | 33.8... | 7/10... |
| c:\windows\system32\msg711.... | Micr... | | OK | C:\W... | 10.0.... | 24.7... | 7/10... |
| c:\windows\system32\msgsm3... | Micr... | | OK | C:\W... | 10.0.... | 41.9... | 7/10... |

FIGURE 8.9: Multimedia Information

17. The next subsection after Multimedia is **Compact Disc (CD-ROM)**.



| Item | Value |
|---|---|
| Drive | E: |
| Description | CD-ROM Drive |
| Media Loaded | No |
| Media Type | DVD-ROM |
| Name | Msft Virtual CD/ROM ATA Device |
| Manufacturer | (Standard CD-ROM drives) |
| Status | OK |
| Transfer Rate | -1.00 kbytes/sec |
| SCSI Target ID | 0 |
| PNP Device ID | IDE\CDROMMSFT_VIRTUAL_CD/ROM_________________1.0____\5&47E3A3F&0... |
| Driver | c:\windows\system32\drivers\cdrom.sys (10.0.10240.16384, 170.00 KB (174,08... |

FIGURE 8.10: CD-ROM Information

18. After CD-ROM is **Sound device**, which displays audio devices on the computer. Although it is empty here, on a regular host machine it displays the device name, manufacturer name, status, PnP Id and installation location.

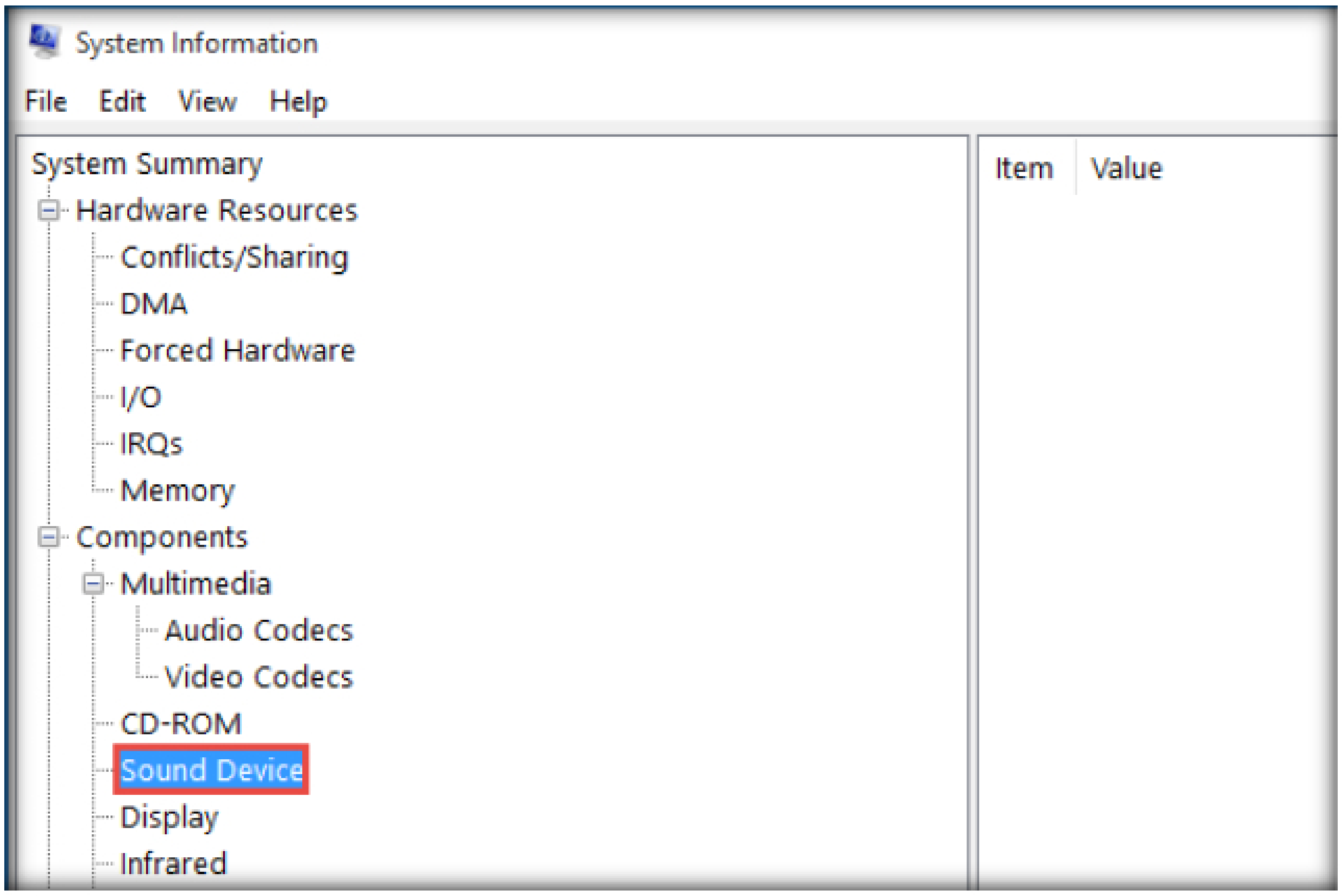


FIGURE 8.11: Sound Device Information

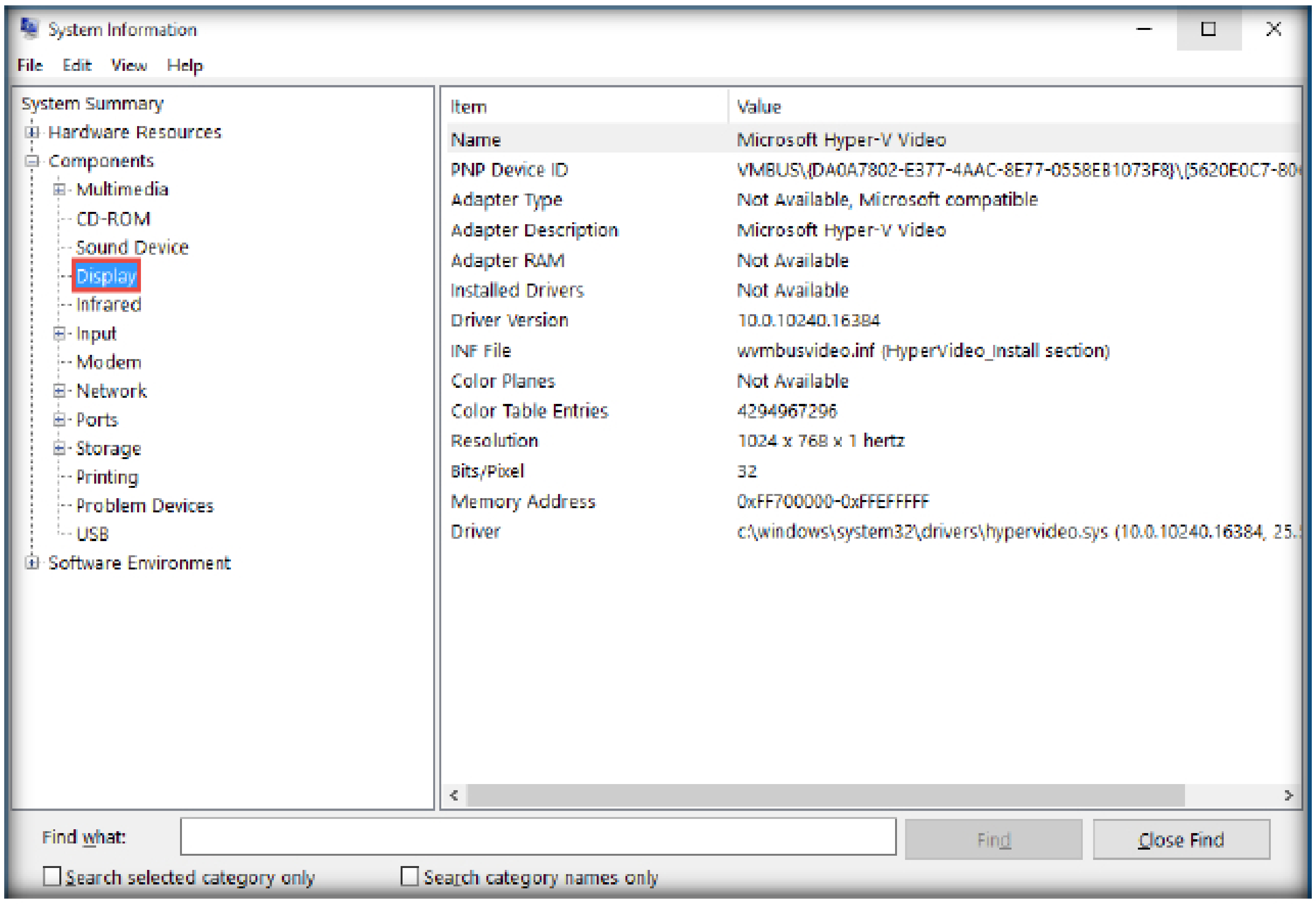
CD-ROM lists the drive assigned followed by a short description. Media loaded shows if there is any disc currently in the CD-ROM or not.

Media type shows the functionalities of the drive. The next three sections, name, manufacturer and status show the drive name, its manufacturer name and current status.

Transfer rate shows the speeds at which the CD-ROM can transfer data, SCSI target ID shows the priority of the CD ROM which can range from 0-7 for simple SCSI.

PNP shows the Plug and play ID of the CD-ROM and finally driver shows the location the device driver is installed.

19. The next subsection is **Display**. It shows the name and Device ID, the type of adapter, an adapter description and RAM allocated to adapter.

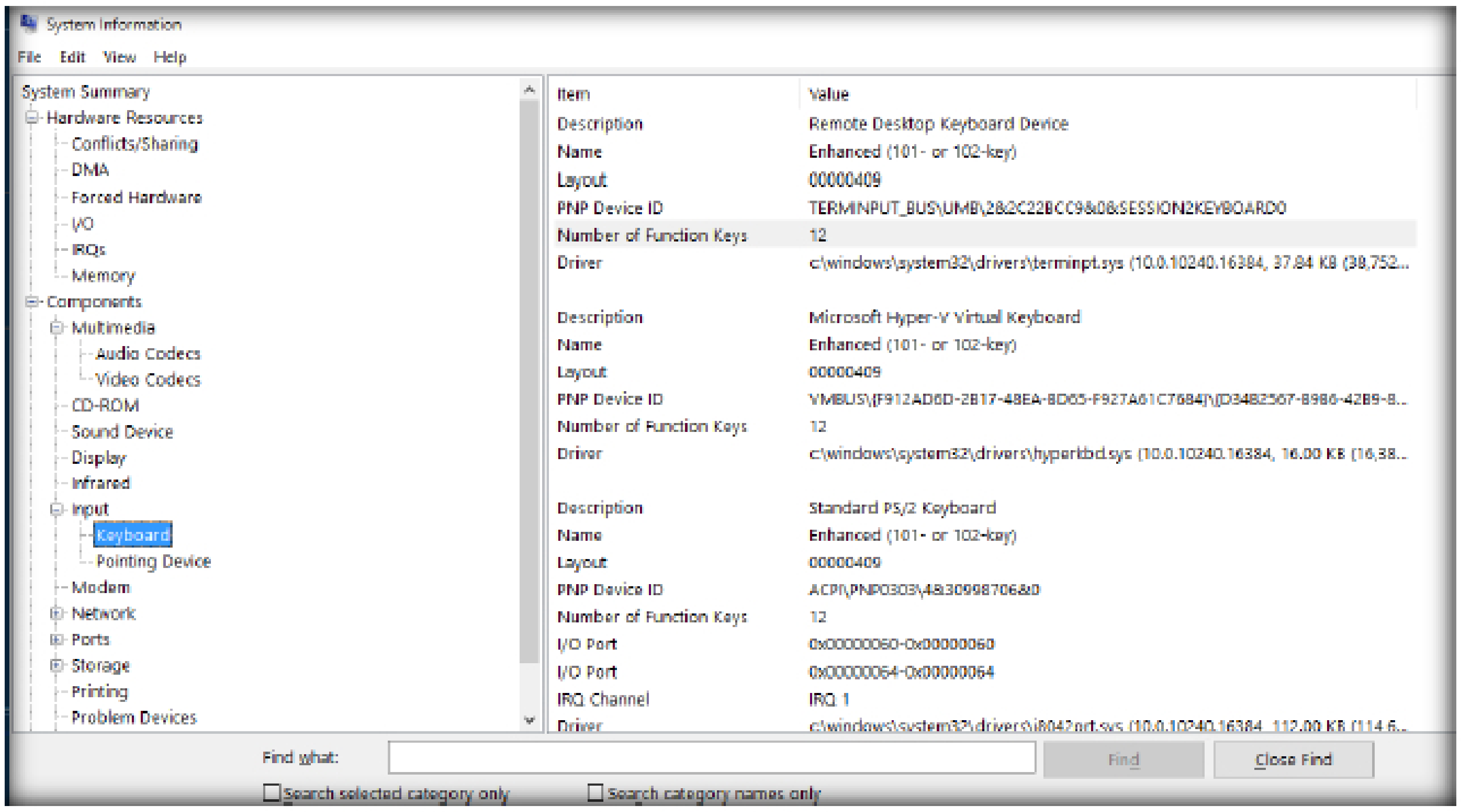


| Item | Value |
|---|---|
| Name | Microsoft Hyper-V Video |
| PNP Device ID | VMBUS\{DA0A7802-E377-4AAC-8E77-0558EB1073F8}\{5620E0C7-80 |
| Adapter Type | Not Available, Microsoft compatible |
| Adapter Description | Microsoft Hyper-V Video |
| Adapter RAM | Not Available |
| Installed Drivers | Not Available |
| Driver Version | 10.0.10240.16384 |
| INF File | wvmbusvideo.inf (HyperVideo_Install section) |
| Color Planes | Not Available |
| Color Table Entries | 4294967296 |
| Resolution | 1024 x 768 x 1 hertz |
| Bits/Pixel | 32 |
| Memory Address | 0xFF700000-0xFFEFFFFF |
| Driver | c:\windows\system32\drivers\hypervideo.sys (10.0.10240.16384, 25. |

FIGURE 8.12: Display Settings Information

20. Next is **Infrared**, since this is not supported it is left without any details.

21. The **Input** subsection is next. It is made up of two parts. **Keyboard** and **Pointing Devices.** The **Keyboard** subsection is provided below:

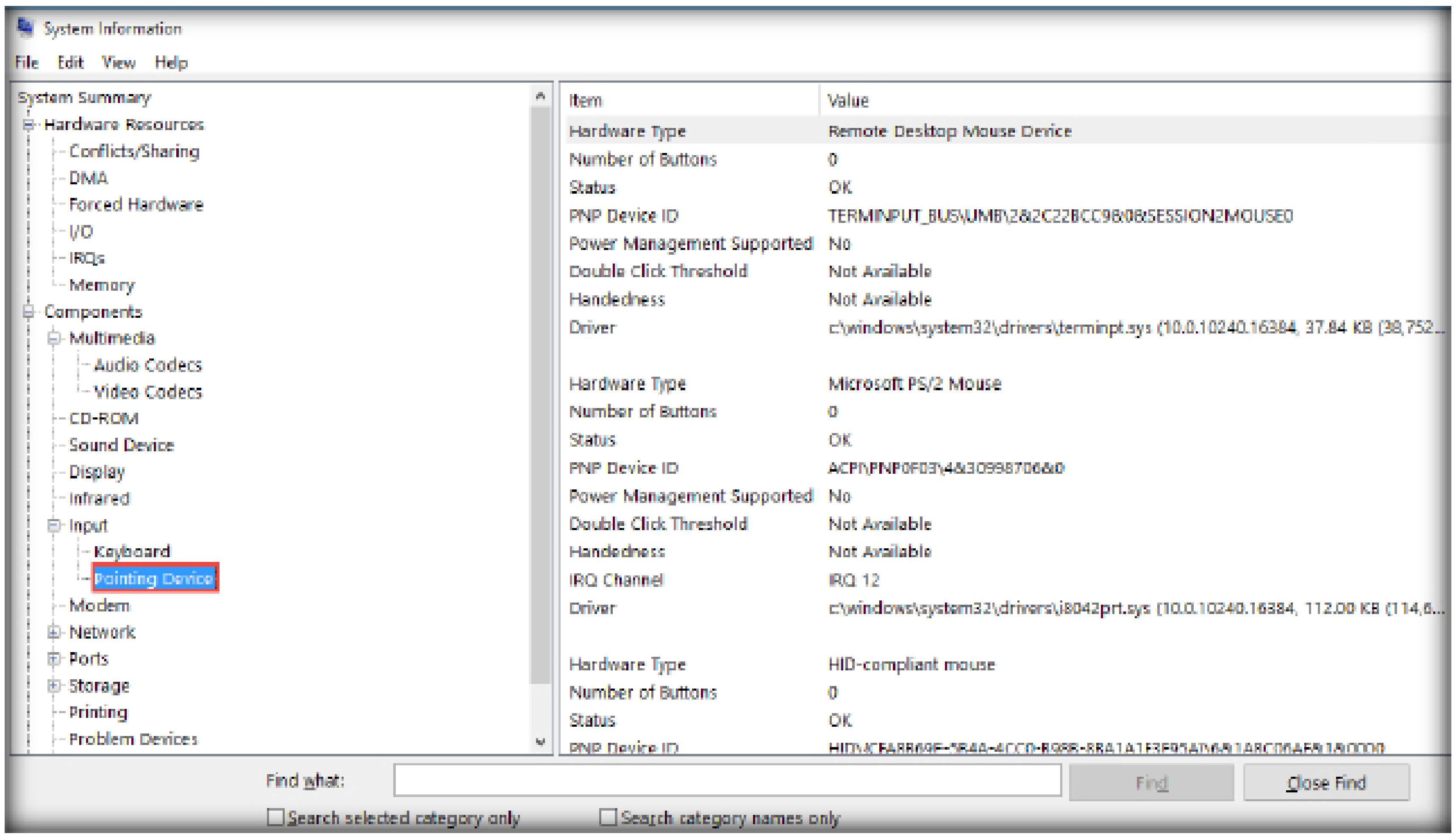


| Item | Value |
|---|---|
| Description | Remote Desktop Keyboard Device |
| Name | Enhanced (101- or 102-key) |
| Layout | 00000409 |
| PNP Device ID | TERMINPUT_BUS\UMB\2&2C22BCC9&0&SESSION2KEYBOARD0 |
| Number of Function Keys | 12 |
| Driver | c:\windows\system32\drivers\terminpt.sys (10.0.10240.16384, 37.84 KB (38,752... |
| | |
| Description | Microsoft Hyper-V Virtual Keyboard |
| Name | Enhanced (101- or 102-key) |
| Layout | 00000409 |
| PNP Device ID | VMBUS\{F912AD6D-2B17-48EA-BD65-F927A61C7684}\{D3482567-8986-42B9-8... |
| Number of Function Keys | 12 |
| Driver | c:\windows\system32\drivers\hyperkbd.sys (10.0.10240.16384, 16.00 KB (16,38... |
| | |
| Description | Standard PS/2 Keyboard |
| Name | Enhanced (101- or 102-key) |
| Layout | 00000409 |
| PNP Device ID | ACPI\PNP0303\4&30998706&0 |
| Number of Function Keys | 12 |
| I/O Port | 0x00000060-0x00000060 |
| I/O Port | 0x00000064-0x00000064 |
| IRQ Channel | IRQ 1 |
| Driver | c:\windows\system32\drivers\i8042prt.sys (10.0.10240.16384, 112.00 KB (114,6... |

FIGURE 8.13: Keyboard Settings Information

22. The **Pointing Device** (mouse) shows the Hardware type (USB) used to connect the device to the PC. The next section shows the name and layout of the pointing device.

The keyboard shows various information viz the description which is the mode of connection USB port, name and layout of the keyboard, PnP ID and no. of functional keys and finally the drivers location



| Item | Value |
|---|---|
| Hardware Type | Remote Desktop Mouse Device |
| Number of Buttons | 0 |
| Status | OK |
| PNP Device ID | TERMINPUT_BUS\UMB\2&2C22BCC9&0&SESSION2MOUSE0 |
| Power Management Supported | No |
| Double Click Threshold | Not Available |
| Handedness | Not Available |
| Driver | c:\windows\system32\drivers\terminpt.sys (10.0.10240.16384, 37.84 KB (38,752... |
| | |
| Hardware Type | Microsoft PS/2 Mouse |
| Number of Buttons | 0 |
| Status | OK |
| PNP Device ID | ACPI\PNP0F03\4&30998706&0 |
| Power Management Supported | No |
| Double Click Threshold | Not Available |
| Handedness | Not Available |
| IRQ Channel | IRQ 12 |
| Driver | c:\windows\system32\drivers\i8042prt.sys (10.0.10240.16384, 112.00 KB (114,6... |
| | |
| Hardware Type | HID-compliant mouse |
| Number of Buttons | 0 |
| Status | OK |
| PNP Device ID | HID\{CFA8B69E-5B4A-4CC0-B98B-8BA1A1F3F95A}\6&1A8C06AE&1&0000 |

FIGURE 8.14: Pointing Device Information

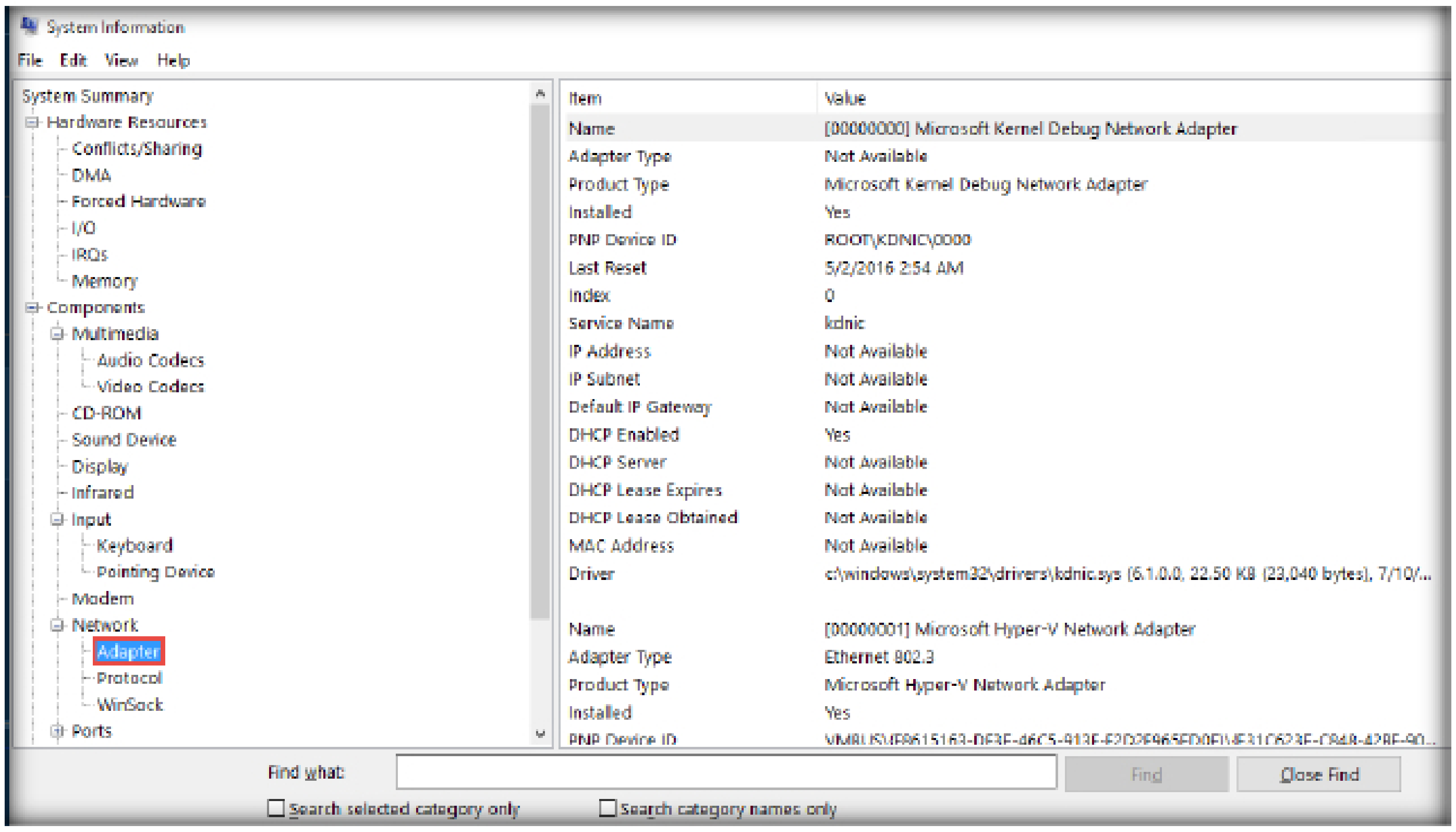
23. The **Modem** subsection is empty since no Modem is currently used on the device.

24. The Network subsection is made of three parts. First is the **Network Adapter**.

It shows information like Name and type of adapter, if its installed or not and the PnP ID.

The last reset, shows the date and the time it was last reset. Indexed values are shown in the next section. Next is service name.

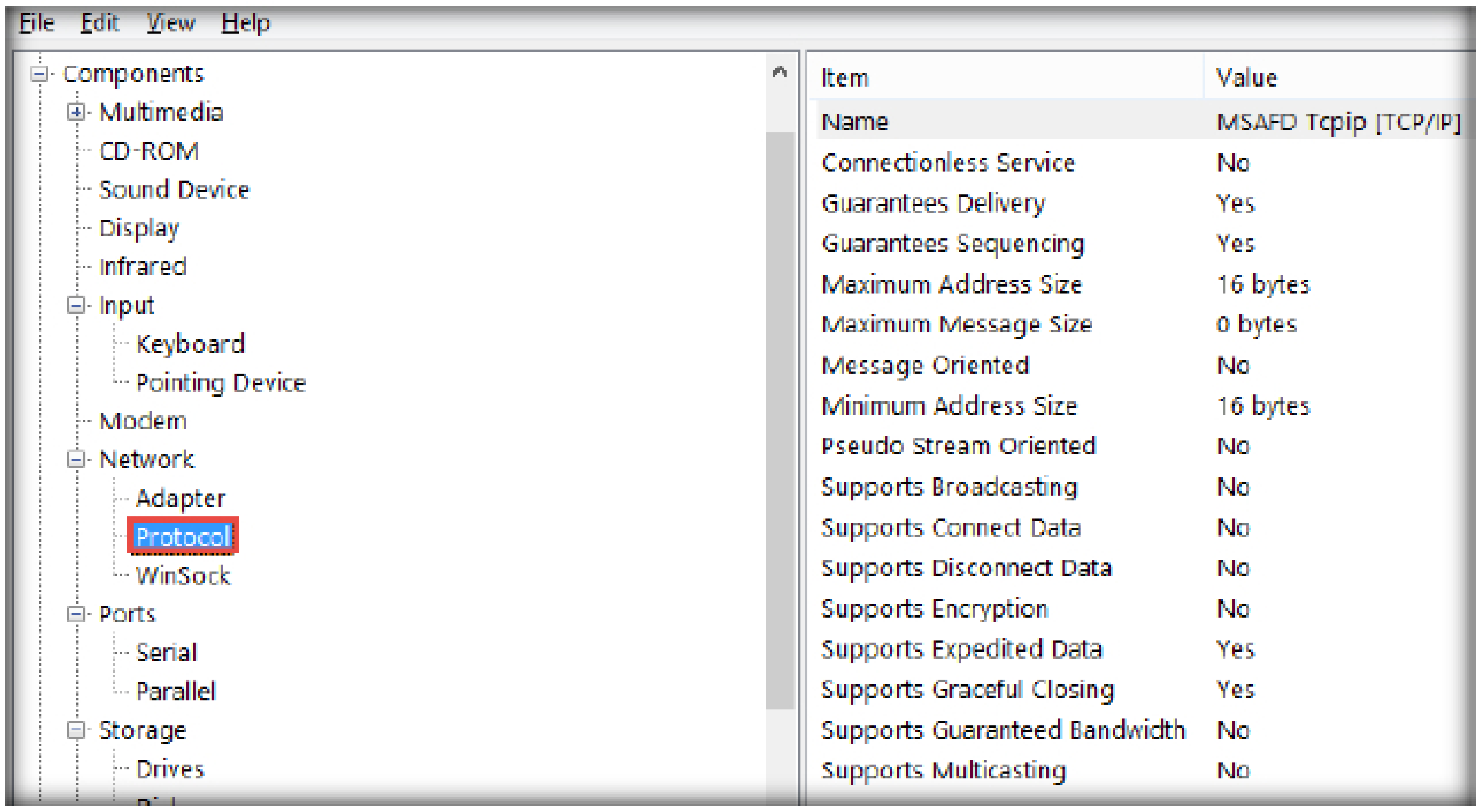
Network adapter's IP address, subnet mask and default gateway are showcased in next section. It is followed by the DHCP details and MAC address of the adapter.



| Item | Value |
|---|---|
| Name | [00000000] Microsoft Kernel Debug Network Adapter |
| Adapter Type | Not Available |
| Product Type | Microsoft Kernel Debug Network Adapter |
| Installed | Yes |
| PNP Device ID | ROOT\KDNIC\0000 |
| Last Reset | 5/2/2016 2:54 AM |
| Index | 0 |
| Service Name | kdnic |
| IP Address | Not Available |
| IP Subnet | Not Available |
| Default IP Gateway | Not Available |
| DHCP Enabled | Yes |
| DHCP Server | Not Available |
| DHCP Lease Expires | Not Available |
| DHCP Lease Obtained | Not Available |
| MAC Address | Not Available |
| Driver | c:\windows\system32\drivers\kdnic.sys (6.1.0.0, 22.50 KB (23,040 bytes), 7/10/... |
| | |
| Name | [00000001] Microsoft Hyper-V Network Adapter |
| Adapter Type | Ethernet 802.3 |
| Product Type | Microsoft Hyper-V Network Adapter |
| Installed | Yes |
| PNP Device ID | VMBUS\{F8615163-DF3E-46C5-913F-F2D2F965ED0E}\{E31C623F-C848-428E-90... |

FIGURE 8.15: Adapter Information

25. The next network subsection is **Protocol**. It shows the name of the protocol. It also shows if the protocol is connectionless or not, and it guarantees the delivery and sequencing of the message.

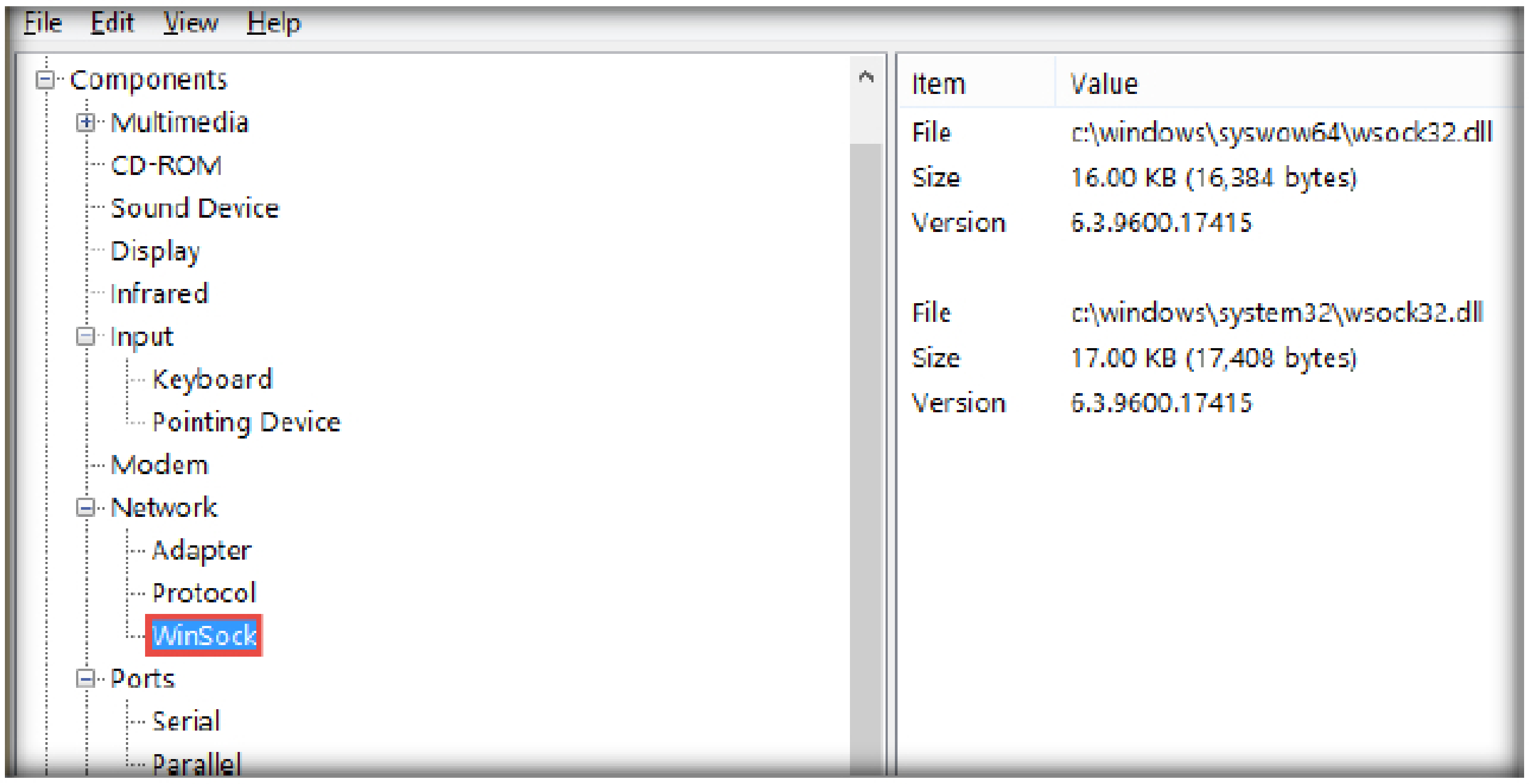


| Item | Value |
|---|---|
| Name | MSAFD Tcpip [TCP/IP] |
| Connectionless Service | No |
| Guarantees Delivery | Yes |
| Guarantees Sequencing | Yes |
| Maximum Address Size | 16 bytes |
| Maximum Message Size | 0 bytes |
| Message Oriented | No |
| Minimum Address Size | 16 bytes |
| Pseudo Stream Oriented | No |
| Supports Broadcasting | No |
| Supports Connect Data | No |
| Supports Disconnect Data | No |
| Supports Encryption | No |
| Supports Expedited Data | Yes |
| Supports Graceful Closing | Yes |
| Supports Guaranteed Bandwidth | No |
| Supports Multicasting | No |

FIGURE 8.16: Protocol Information

26. The third subsection is **Winsock**, which is a programming support interface to handle input/output requests.

27. In **Winsock** the fields described are file location, size of program, and version of the program.

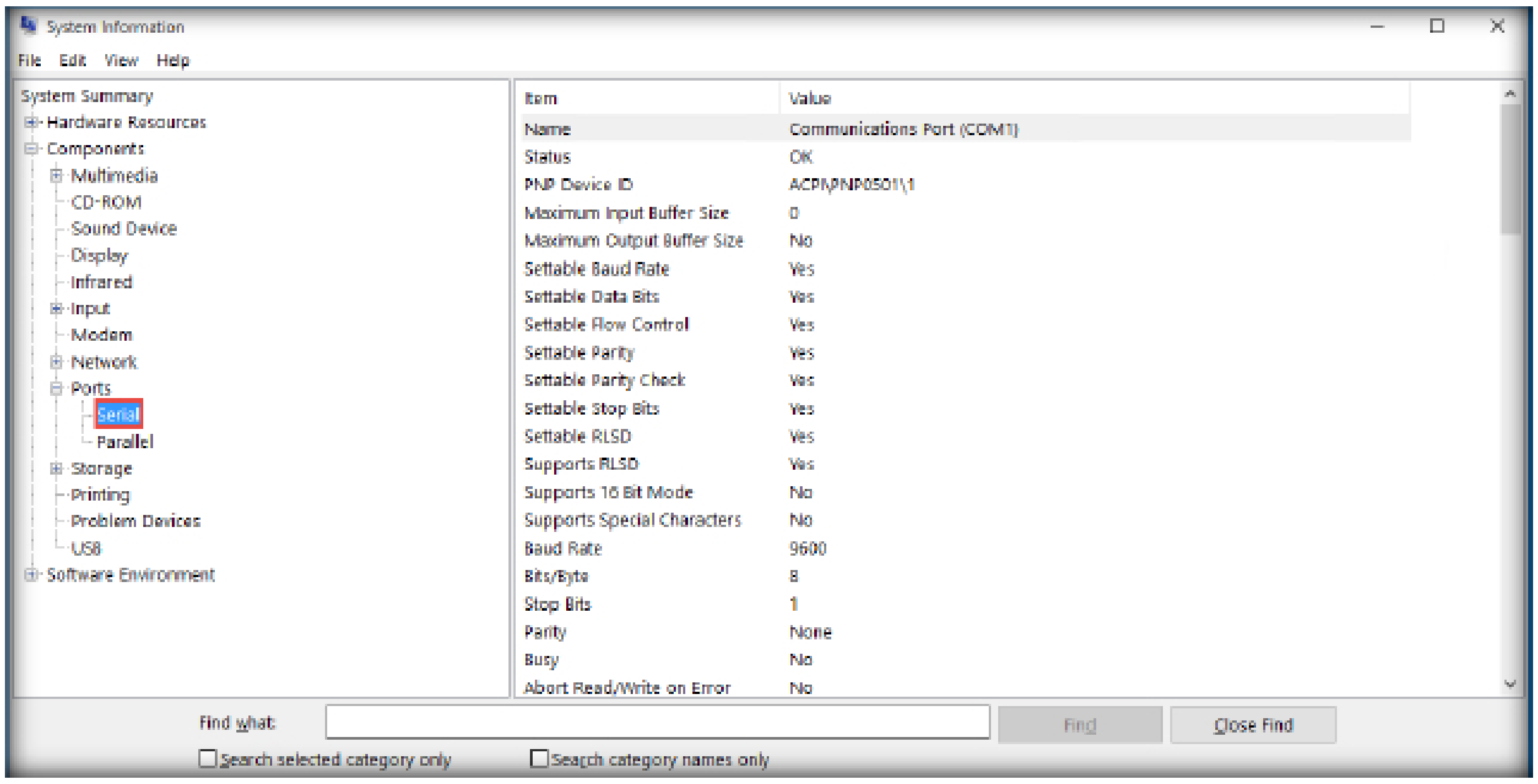


| Item | Value |
|---|---|
| File | c:\windows\syswow64\wsock32.dll |
| Size | 16.00 KB (16,384 bytes) |
| Version | 6.3.9600.17415 |
| | |
| File | c:\windows\system32\wsock32.dll |
| Size | 17.00 KB (17,408 bytes) |
| Version | 6.3.9600.17415 |

FIGURE 8.17: WinSock Information

28. The **Ports** subsection describes the **Serial** and **Parallel** ports present on the system.

29. The **Serial** ports display the **Name** of the attached device, **Status**, **PNP ID**, and other information.



| Item | Value |
|---|---|
| Name | Communications Port (COM1) |
| Status | OK |
| PNP Device ID | ACPI\PNP0501\1 |
| Maximum Input Buffer Size | 0 |
| Maximum Output Buffer Size | No |
| Settable Baud Rate | Yes |
| Settable Data Bits | Yes |
| Settable Flow Control | Yes |
| Settable Parity | Yes |
| Settable Parity Check | Yes |
| Settable Stop Bits | Yes |
| Settable RLSD | Yes |
| Supports RLSD | Yes |
| Supports 16 Bit Mode | No |
| Supports Special Characters | No |
| Baud Rate | 9600 |
| Bits/Byte | 8 |
| Stop Bits | 1 |
| Parity | None |
| Busy | No |
| Abort Read/Write on Error | No |

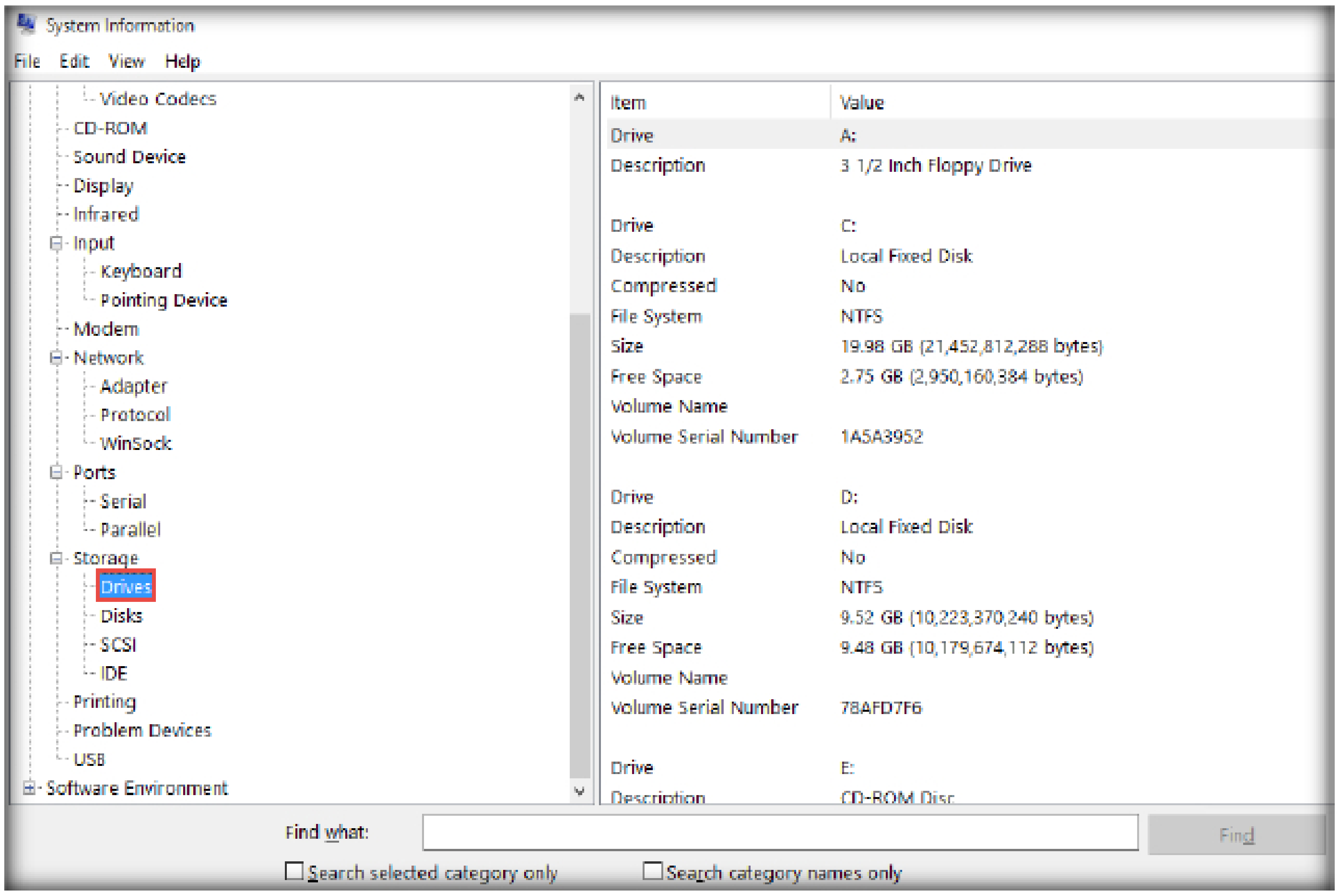
FIGURE 8.18: Serial Ports Information

SCSI provides details like name, manufacturer and current status of the device.

Furthermore, it provides details like PnP device ID and location where the Drivers are loaded.

30. The next subsection is **Storage**, which is further divided into four parts.

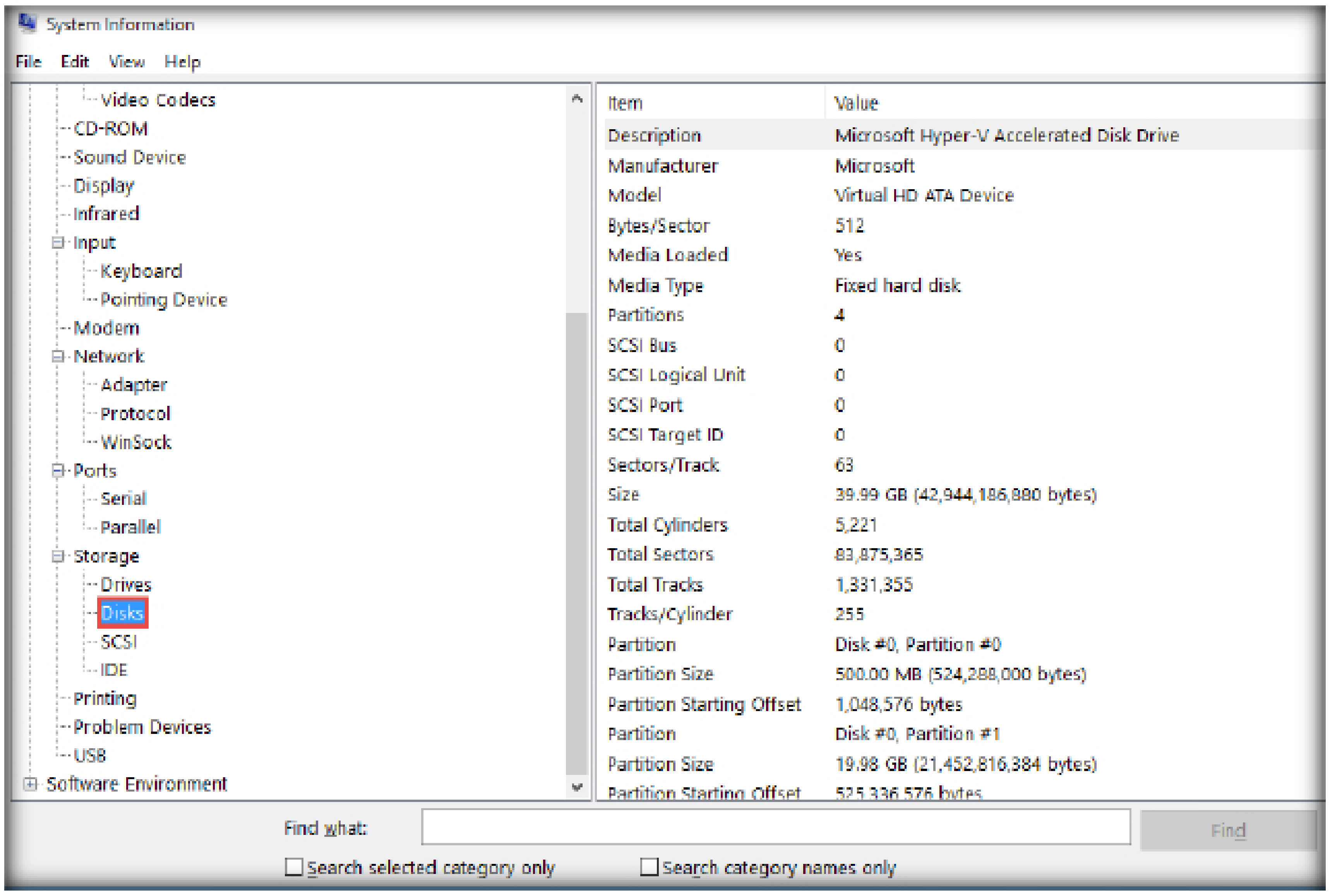
31. The first section in storage is **Drives**. The drives provide the name and a short description of the drive.



| Item | Value |
|---|---|
| Drive | A: |
| Description | 3 1/2 Inch Floppy Drive |
| | |
| Drive | C: |
| Description | Local Fixed Disk |
| Compressed | No |
| File System | NTFS |
| Size | 19.98 GB (21,452,812,288 bytes) |
| Free Space | 2.75 GB (2,950,160,384 bytes) |
| Volume Name | |
| Volume Serial Number | 1A5A3952 |
| | |
| Drive | D: |
| Description | Local Fixed Disk |
| Compressed | No |
| File System | NTFS |
| Size | 9.52 GB (10,223,370,240 bytes) |
| Free Space | 9.48 GB (10,179,674,112 bytes) |
| Volume Name | |
| Volume Serial Number | 78AFD7F6 |
| | |
| Drive | E: |
| Description | CD-ROM Disc |

FIGURE 8.19: Available Drives Information

32. The second subsection under storage is **Disks**. It consists of description, manufacturer name and model number for the disks.



| Item | Value |
|---|---|
| Description | Microsoft Hyper-V Accelerated Disk Drive |
| Manufacturer | Microsoft |
| Model | Virtual HD ATA Device |
| Bytes/Sector | 512 |
| Media Loaded | Yes |
| Media Type | Fixed hard disk |
| Partitions | 4 |
| SCSI Bus | 0 |
| SCSI Logical Unit | 0 |
| SCSI Port | 0 |
| SCSI Target ID | 0 |
| Sectors/Track | 63 |
| Size | 39.99 GB (42,944,186,880 bytes) |
| Total Cylinders | 5,221 |
| Total Sectors | 83,875,365 |
| Total Tracks | 1,331,355 |
| Tracks/Cylinder | 255 |
| Partition | Disk #0, Partition #0 |
| Partition Size | 500.00 MB (524,288,000 bytes) |
| Partition Starting Offset | 1,048,576 bytes |
| Partition | Disk #0, Partition #1 |
| Partition Size | 19.98 GB (21,452,816,384 bytes) |
| Partition Starting Offset | 525,336,576 bytes |

FIGURE 8.20: Available Disks Information

Disks describe the bytes/ sector stored on the disk and if the disk is currently loaded in the system or not. The media type describes if the disk is permanent or not.

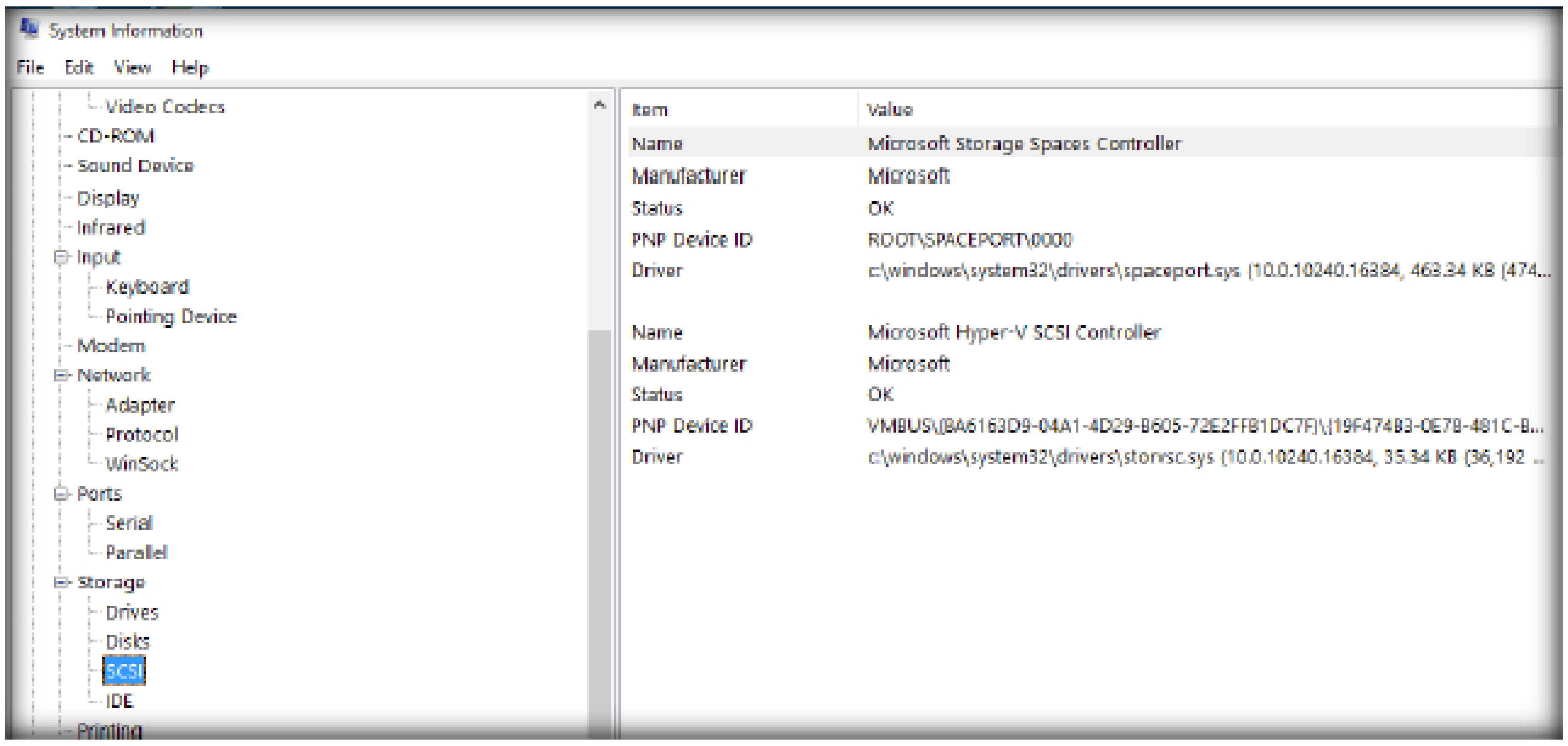
The partitions show the number of partitions on the disk and SCSI shows the SCSI's bus, logical unit, port and target ID.

Sectors per track describes the number of sectors present per track on the disk.

The total cylinders, sectors and tracks are shown in the next sector, followed by the number of tracks per cylinder present.

The final sub section describes every partition size and the offset at which it starts.

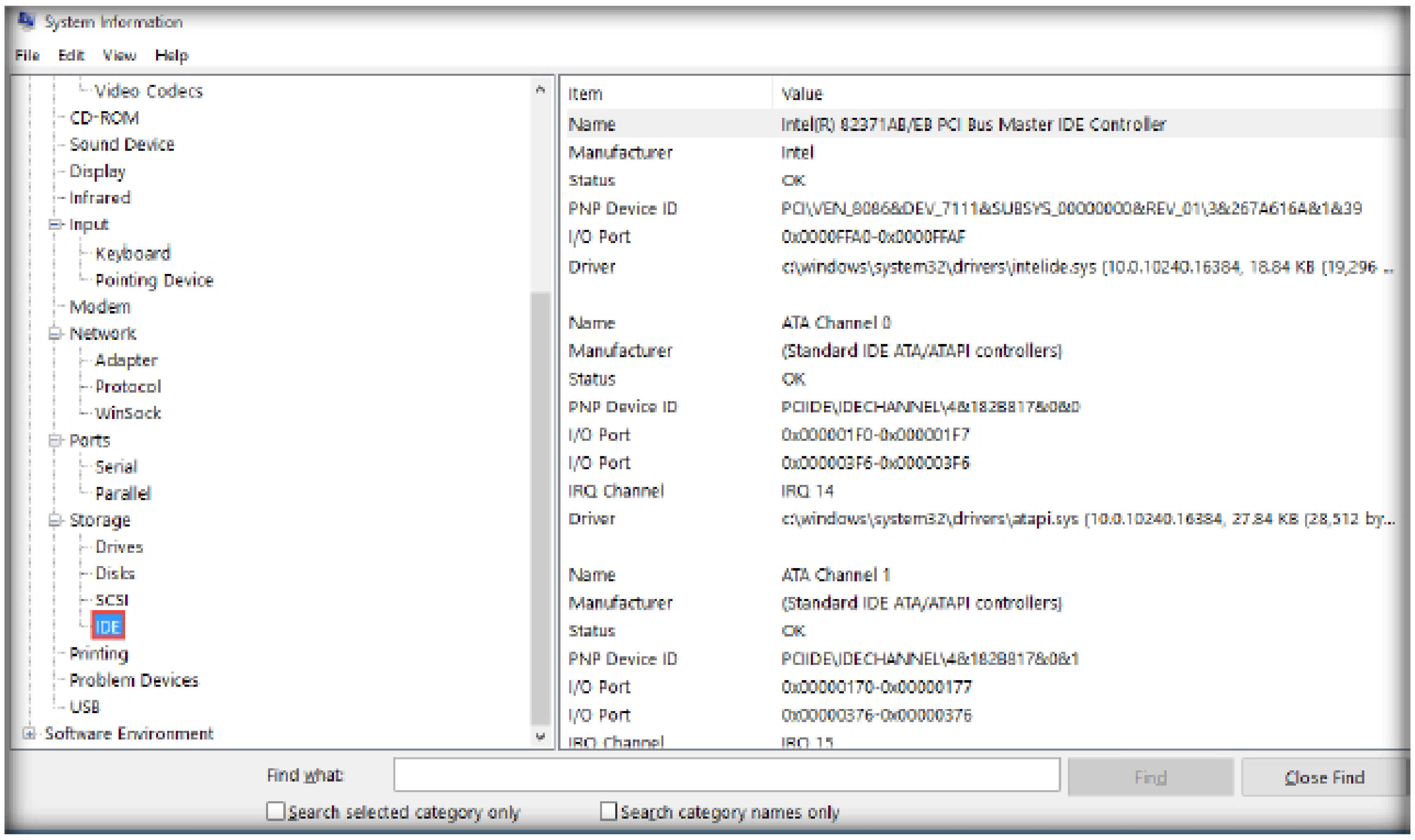
33. **SCSI** is the next subsection under storage. It is a standard parallel interface which enables the attachment of printers, disk drives, and other peripheral standards.



| Item | Value |
|---|---|
| Name | Microsoft Storage Spaces Controller |
| Manufacturer | Microsoft |
| Status | OK |
| PNP Device ID | ROOT\SPACEPORT\0000 |
| Driver | c:\windows\system32\drivers\spaceport.sys (10.0.10240.16384, 463.34 KB (474... |
| | |
| Name | Microsoft Hyper-V SCSI Controller |
| Manufacturer | Microsoft |
| Status | OK |
| PNP Device ID | VMBUS\{BA6163D9-04A1-4D29-B605-72E2FFB1DC7F}\{19F474B3-0E78-481C-B... |
| Driver | c:\windows\system32\drivers\storvsc.sys (10.0.10240.16384, 35.34 KB (36,192 ... |

FIGURE 8.21: SCSI Storage Information

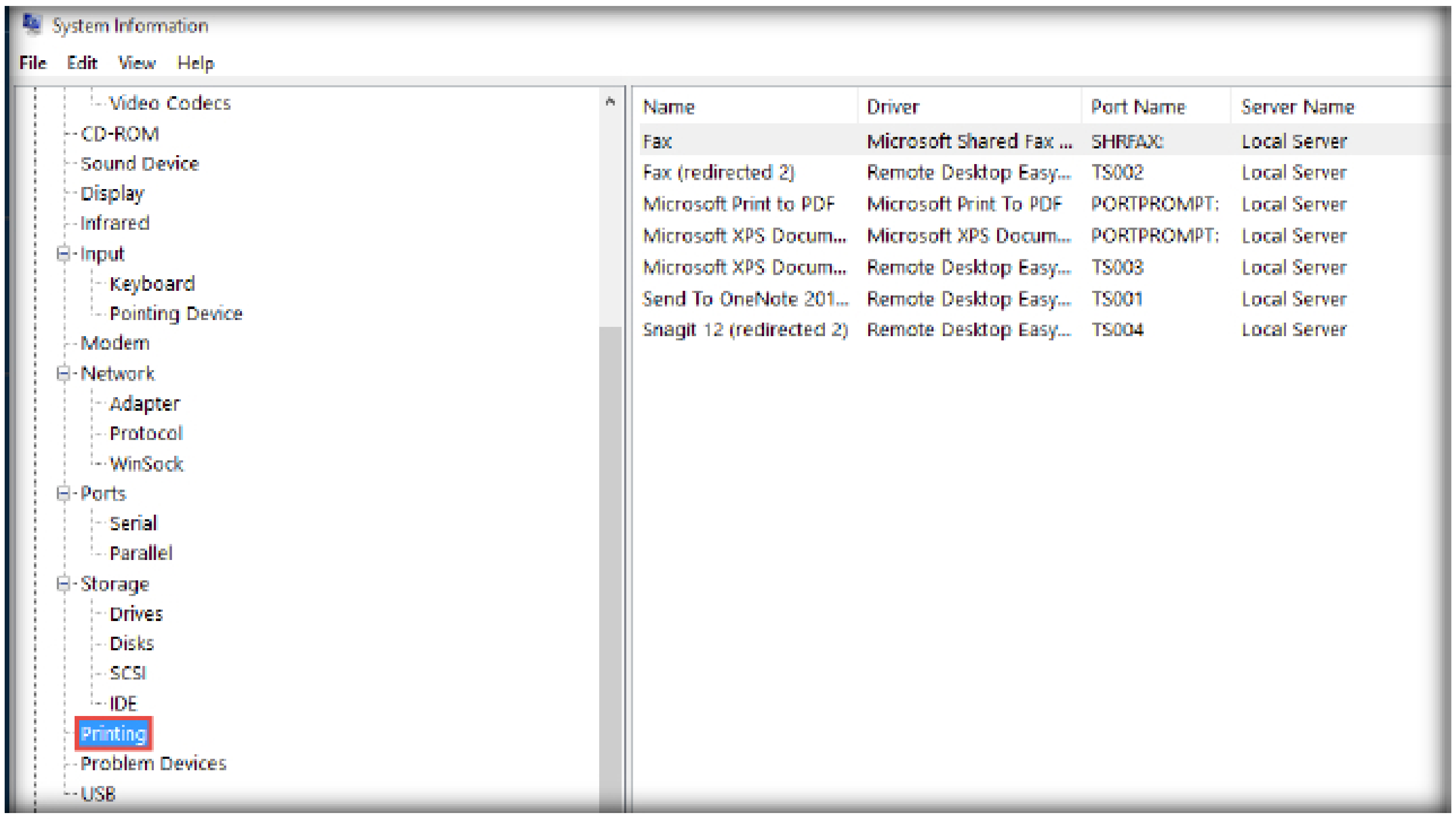
34. **IDE** (Integrated Development Environment) is the fourth subsection and it provides a set of comprehensive facilities to programmers which assist them in software development.



| Item | Value |
|---|---|
| Name | Intel(R) 82371AB/EB PCI Bus Master IDE Controller |
| Manufacturer | Intel |
| Status | OK |
| PNP Device ID | PCI\VEN_8086&DEV_7111&SUBSYS_00000000&REV_01\3&267A616A&1&39 |
| I/O Port | 0x0000FFA0-0x0000FFAF |
| Driver | c:\windows\system32\drivers\intelide.sys (10.0.10240.16384, 18.84 KB (19,296 ... |
| | |
| Name | ATA Channel 0 |
| Manufacturer | (Standard IDE ATA/ATAPI controllers) |
| Status | OK |
| PNP Device ID | PCIIDE\IDECHANNEL\4&1828817&0&0 |
| I/O Port | 0x000001F0-0x000001F7 |
| I/O Port | 0x000003F6-0x000003F6 |
| IRQ Channel | IRQ 14 |
| Driver | c:\windows\system32\drivers\atapi.sys (10.0.10240.16384, 27.84 KB (28,512 by... |
| | |
| Name | ATA Channel 1 |
| Manufacturer | (Standard IDE ATA/ATAPI controllers) |
| Status | OK |
| PNP Device ID | PCIIDE\IDECHANNEL\4&1828817&0&1 |
| I/O Port | 0x00000170-0x00000177 |
| I/O Port | 0x00000376-0x00000376 |
| IRQ Channel | IRQ 15 |

FIGURE 8.22: IDE Information

35. Next is the **Printing** subsection. It describes the printing devices **Name**, **Driver**, **Port Name,** and **Server Name**.



| Name | Driver | Port Name | Server Name |
|---|---|---|---|
| Fax | Microsoft Shared Fax ... | SHRFAX: | Local Server |
| Fax (redirected 2) | Remote Desktop Easy... | TS002 | Local Server |
| Microsoft Print to PDF | Microsoft Print To PDF | PORTPROMPT: | Local Server |
| Microsoft XPS Docum... | Microsoft XPS Docum... | PORTPROMPT: | Local Server |
| Microsoft XPS Docum... | Remote Desktop Easy... | TS003 | Local Server |
| Send To OneNote 201... | Remote Desktop Easy... | TS001 | Local Server |
| Snagit 12 (redirected 2) | Remote Desktop Easy... | TS004 | Local Server |

FIGURE 8.23: Printing Information

36. The **Problem Devices** appear when the hardware devices are facing issues. We can see the issue (error code) with the device.

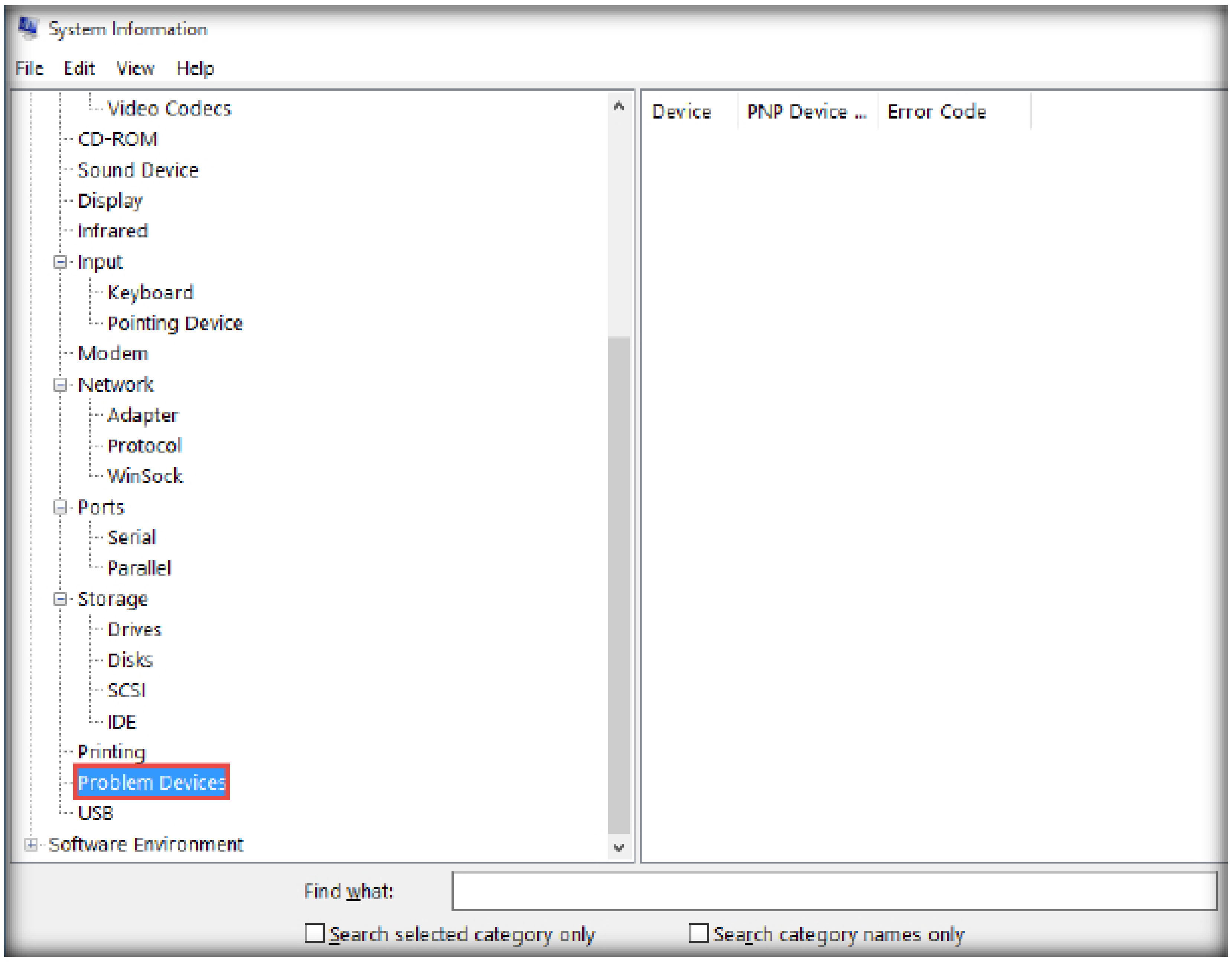


FIGURE 8.24: Problem Devices Information

37. The **USB** subsection which is currently empty, usually shows the USB port names and PNP ID's.

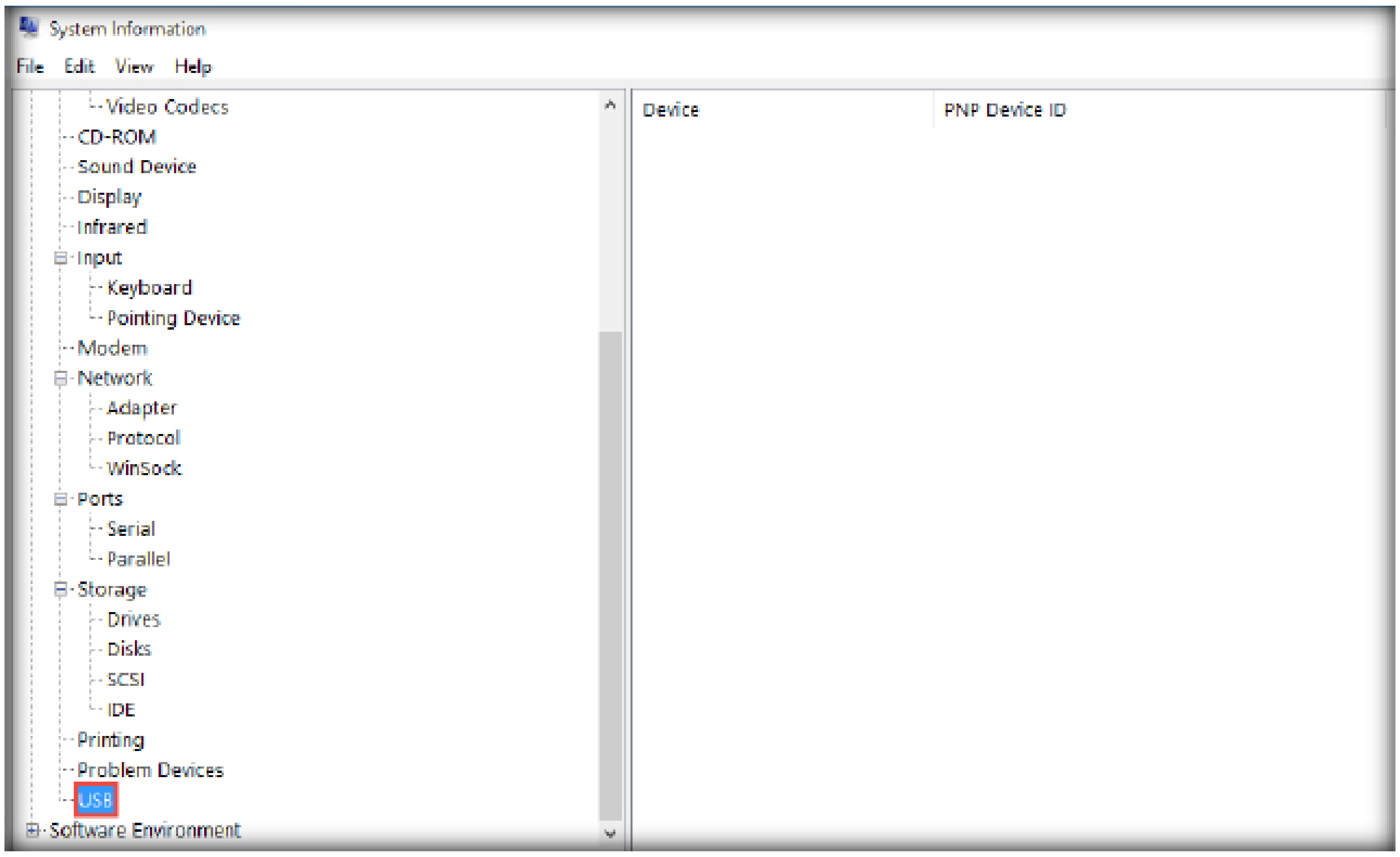
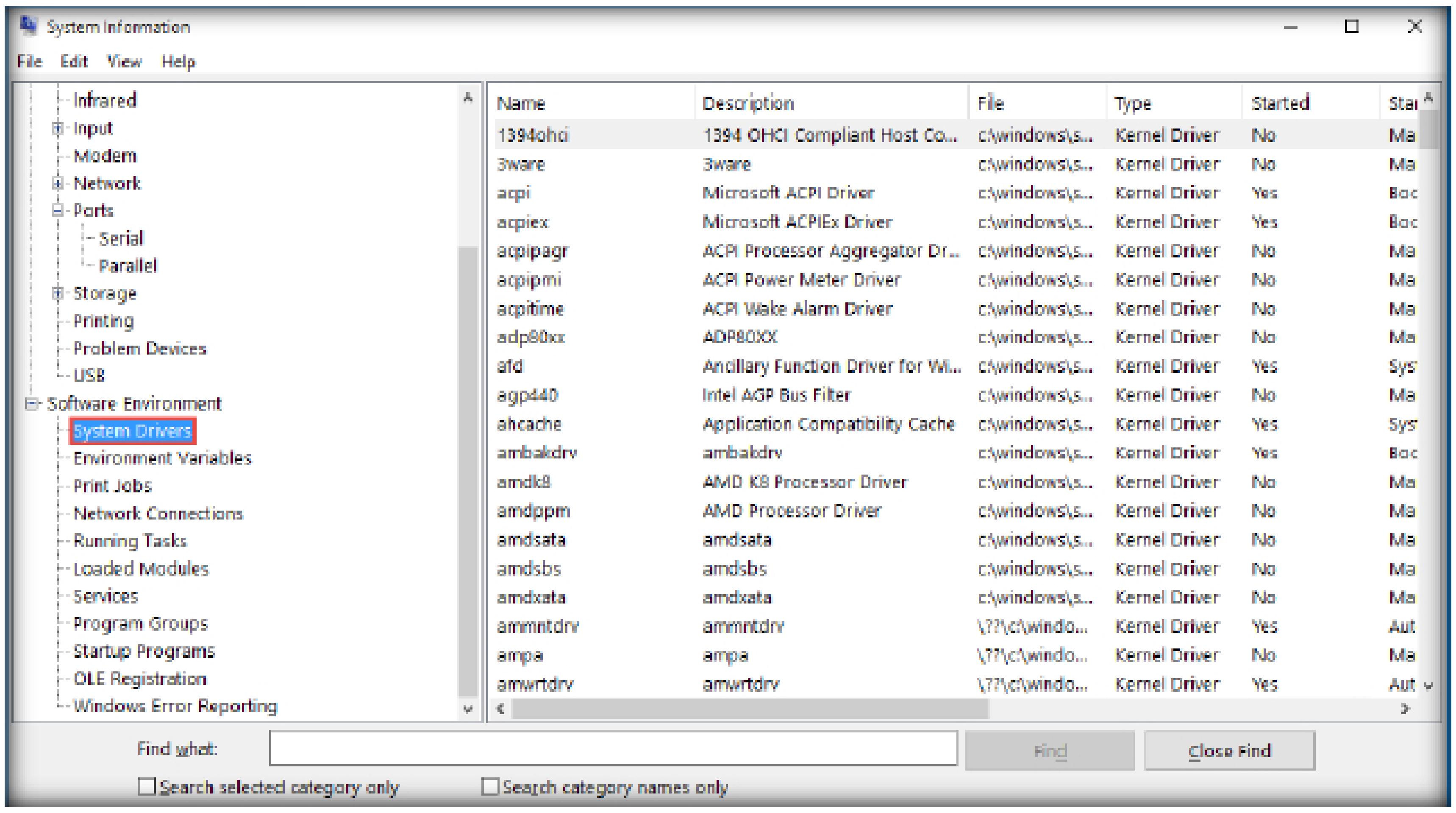


FIGURE 8.25: Available USB Ports Information

TASK 4

**Knowing the software configuration on the system**

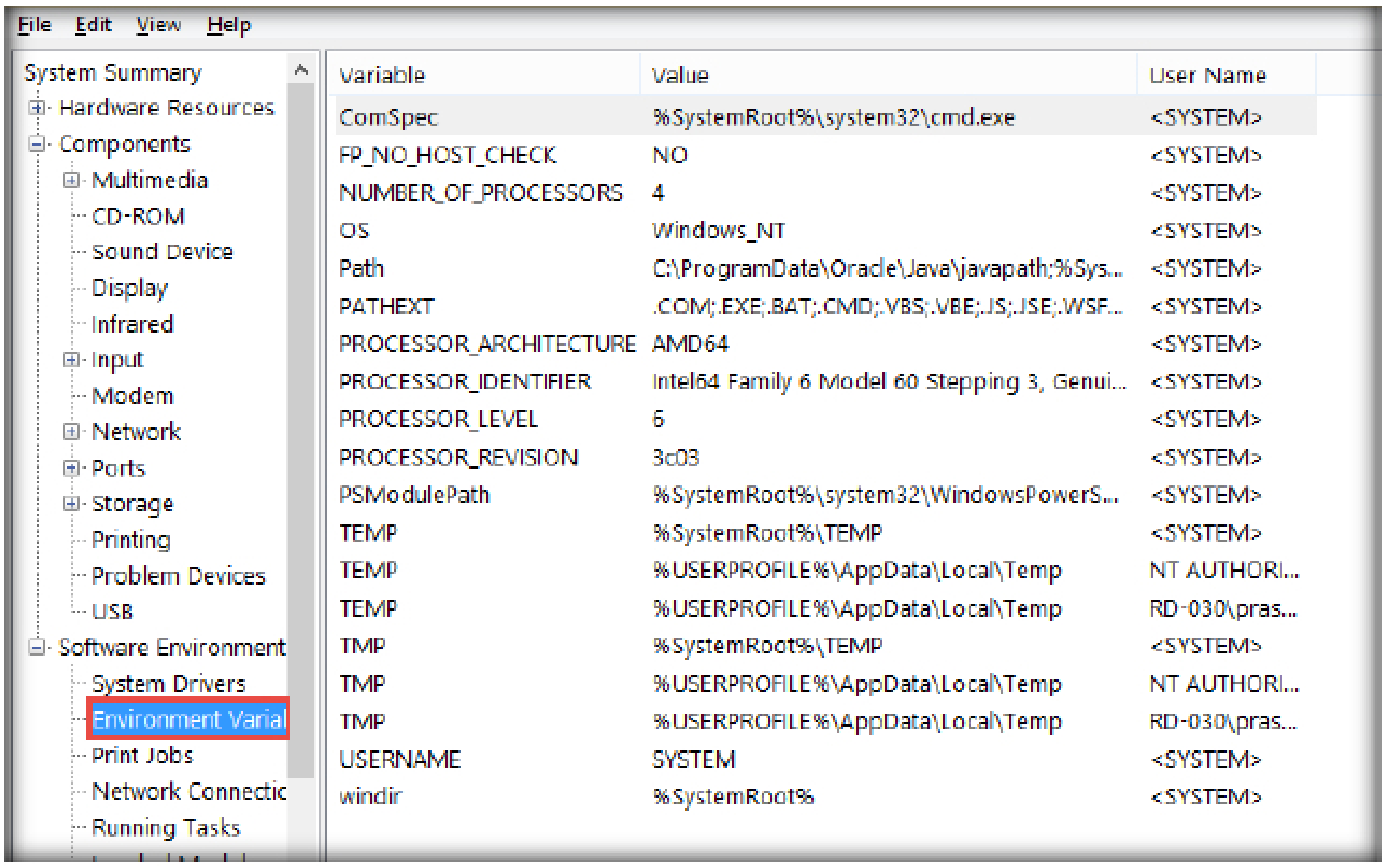
38. The next section is the **Software Environment** section. The first subsection is **System Drivers**.



| Name | Description | File | Type | Started | Star |
|---|---|---|---|---|---|
| 1394ohci | 1394 OHCI Compliant Host Co... | c:\windows\s... | Kernel Driver | No | Ma |
| 3ware | 3ware | c:\windows\s... | Kernel Driver | No | Ma |
| acpi | Microsoft ACPI Driver | c:\windows\s... | Kernel Driver | Yes | Boc |
| acpiex | Microsoft ACPIEx Driver | c:\windows\s... | Kernel Driver | Yes | Boc |
| acpipagr | ACPI Processor Aggregator Dr... | c:\windows\s... | Kernel Driver | No | Ma |
| acpipmi | ACPI Power Meter Driver | c:\windows\s... | Kernel Driver | No | Ma |
| acpitime | ACPI Wake Alarm Driver | c:\windows\s... | Kernel Driver | No | Ma |
| adp80xx | ADP80XX | c:\windows\s... | Kernel Driver | No | Ma |
| afd | Ancillary Function Driver for Wi... | c:\windows\s... | Kernel Driver | Yes | Sys |
| agp440 | Intel AGP Bus Filter | c:\windows\s... | Kernel Driver | No | Ma |
| ahcache | Application Compatibility Cache | c:\windows\s... | Kernel Driver | Yes | Sys |
| ambakdrv | ambakdrv | c:\windows\s... | Kernel Driver | Yes | Boc |
| amdk8 | AMD K8 Processor Driver | c:\windows\s... | Kernel Driver | No | Ma |
| amdppm | AMD Processor Driver | c:\windows\s... | Kernel Driver | No | Ma |
| amdsata | amdsata | c:\windows\s... | Kernel Driver | No | Ma |
| amdsbs | amdsbs | c:\windows\s... | Kernel Driver | No | Ma |
| amdxata | amdxata | c:\windows\s... | Kernel Driver | No | Ma |
| ammntdrv | ammntdrv | \??\c:\windo... | Kernel Driver | Yes | Aut |
| ampa | ampa | \??\c:\windo... | Kernel Driver | No | Ma |
| amwrtdrv | amwrtdrv | \??\c:\windo... | Kernel Driver | Yes | Aut |

FIGURE 8.26: System Drivers Information

39. The next subsection is **Environment Variables**. These variables have an immense effect on how a process behaves on a computer. An environment variable can be user defined or system defined.



| Variable | Value | User Name |
|---|---|---|
| ComSpec | %SystemRoot%\system32\cmd.exe | <SYSTEM> |
| FP_NO_HOST_CHECK | NO | <SYSTEM> |
| NUMBER_OF_PROCESSORS | 4 | <SYSTEM> |
| OS | Windows_NT | <SYSTEM> |
| Path | C:\ProgramData\Oracle\Java\javapath;%Sys... | <SYSTEM> |
| PATHEXT | .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF... | <SYSTEM> |
| PROCESSOR_ARCHITECTURE | AMD64 | <SYSTEM> |
| PROCESSOR_IDENTIFIER | Intel64 Family 6 Model 60 Stepping 3, Genui... | <SYSTEM> |
| PROCESSOR_LEVEL | 6 | <SYSTEM> |
| PROCESSOR_REVISION | 3c03 | <SYSTEM> |
| PSModulePath | %SystemRoot%\system32\WindowsPowerS... | <SYSTEM> |
| TEMP | %SystemRoot%\TEMP | <SYSTEM> |
| TEMP | %USERPROFILE%\AppData\Local\Temp | NT AUTHORI... |
| TEMP | %USERPROFILE%\AppData\Local\Temp | RD-030\pras... |
| TMP | %SystemRoot%\TEMP | <SYSTEM> |
| TMP | %USERPROFILE%\AppData\Local\Temp | NT AUTHORI... |
| TMP | %USERPROFILE%\AppData\Local\Temp | RD-030\pras... |
| USERNAME | SYSTEM | <SYSTEM> |
| windir | %SystemRoot% | <SYSTEM> |

FIGURE 8.27: Environment Variables Information

40. The next subsection is Print Jobs. It describes the document name, size, its owner, whom to be notified, and current status.

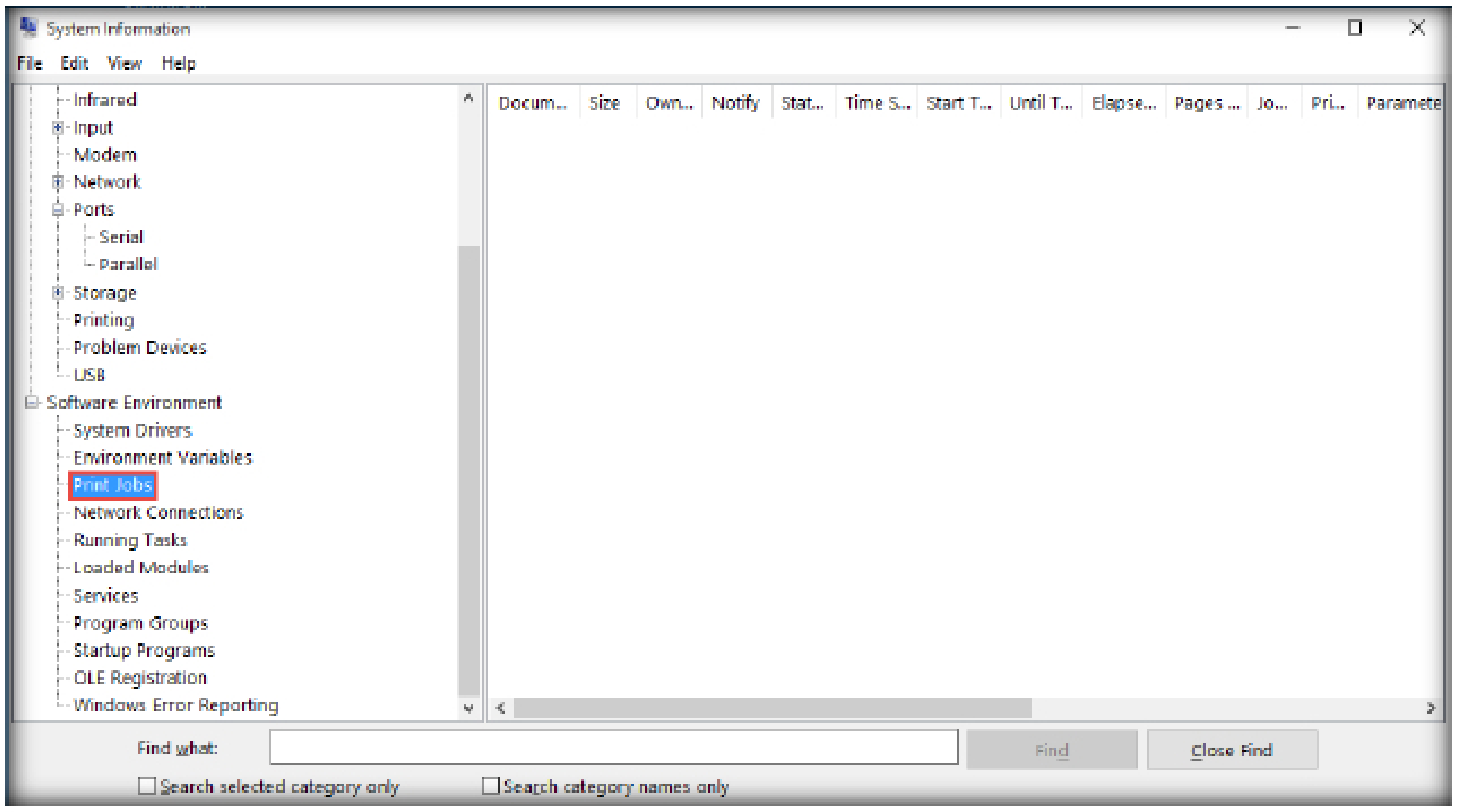


FIGURE 8.28: Print Jobs Information

41. Following Print Jobs is the **Network Connections** subsection. It generally shows NAS devices attached to the network.

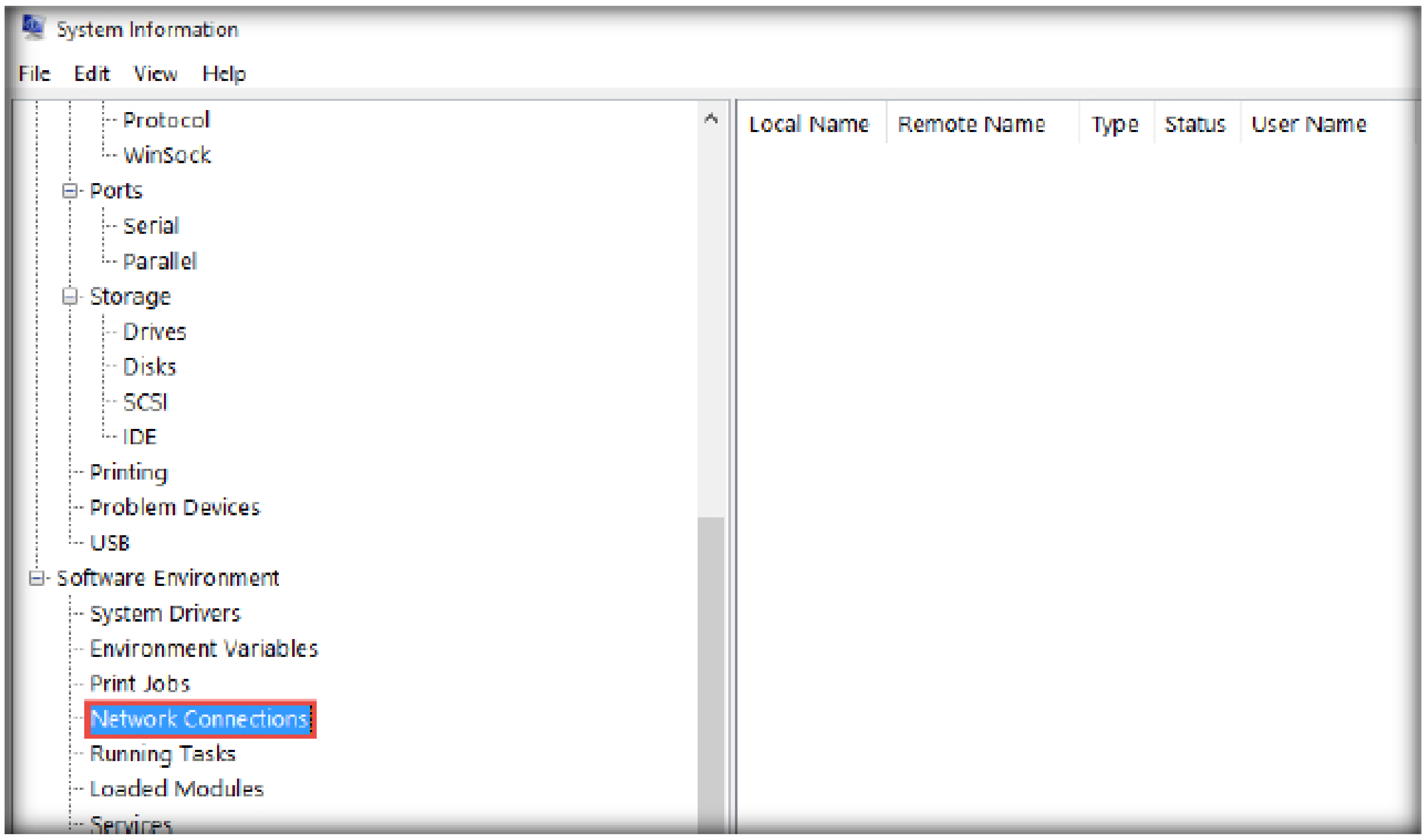
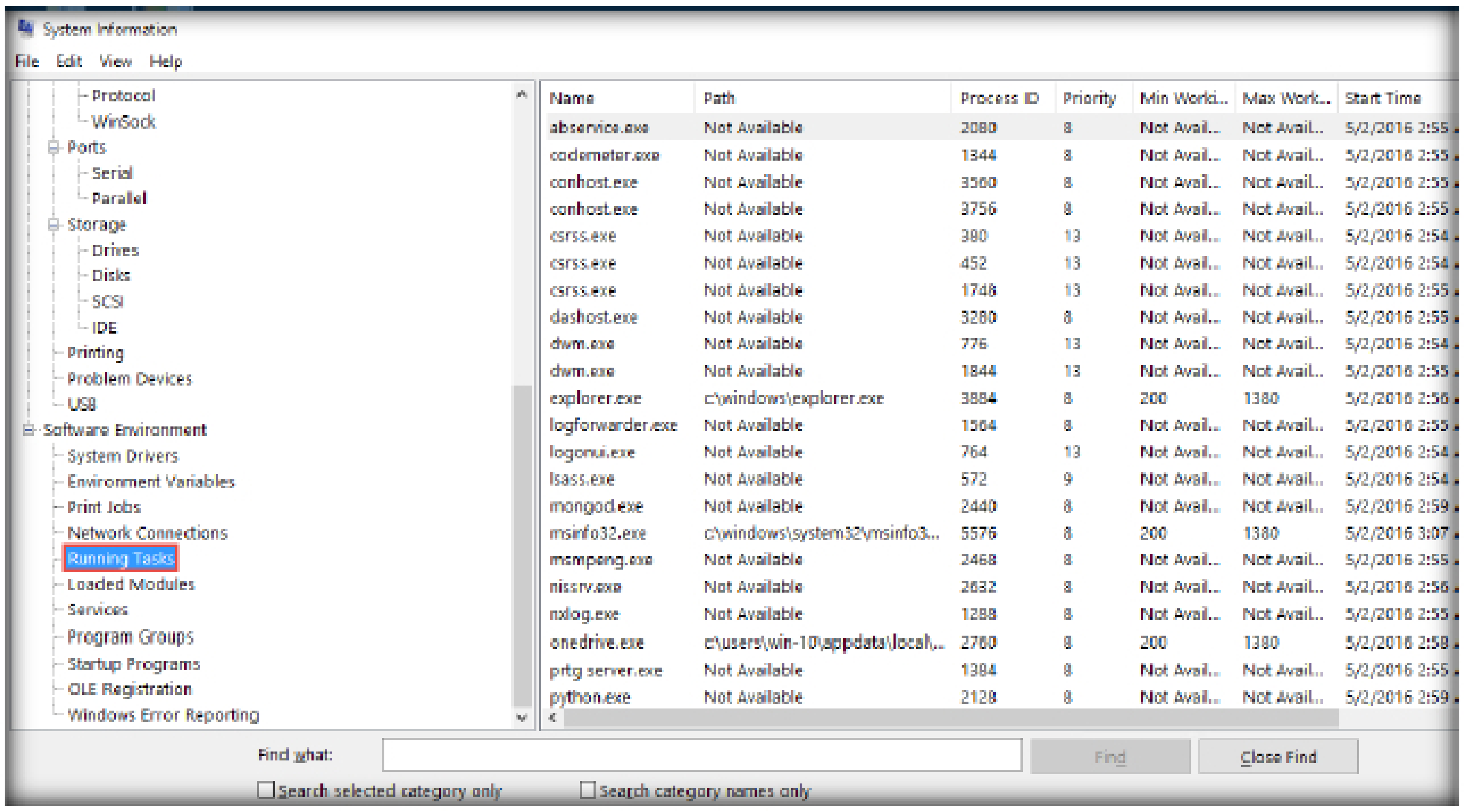


FIGURE 8.29: Network Connection Information

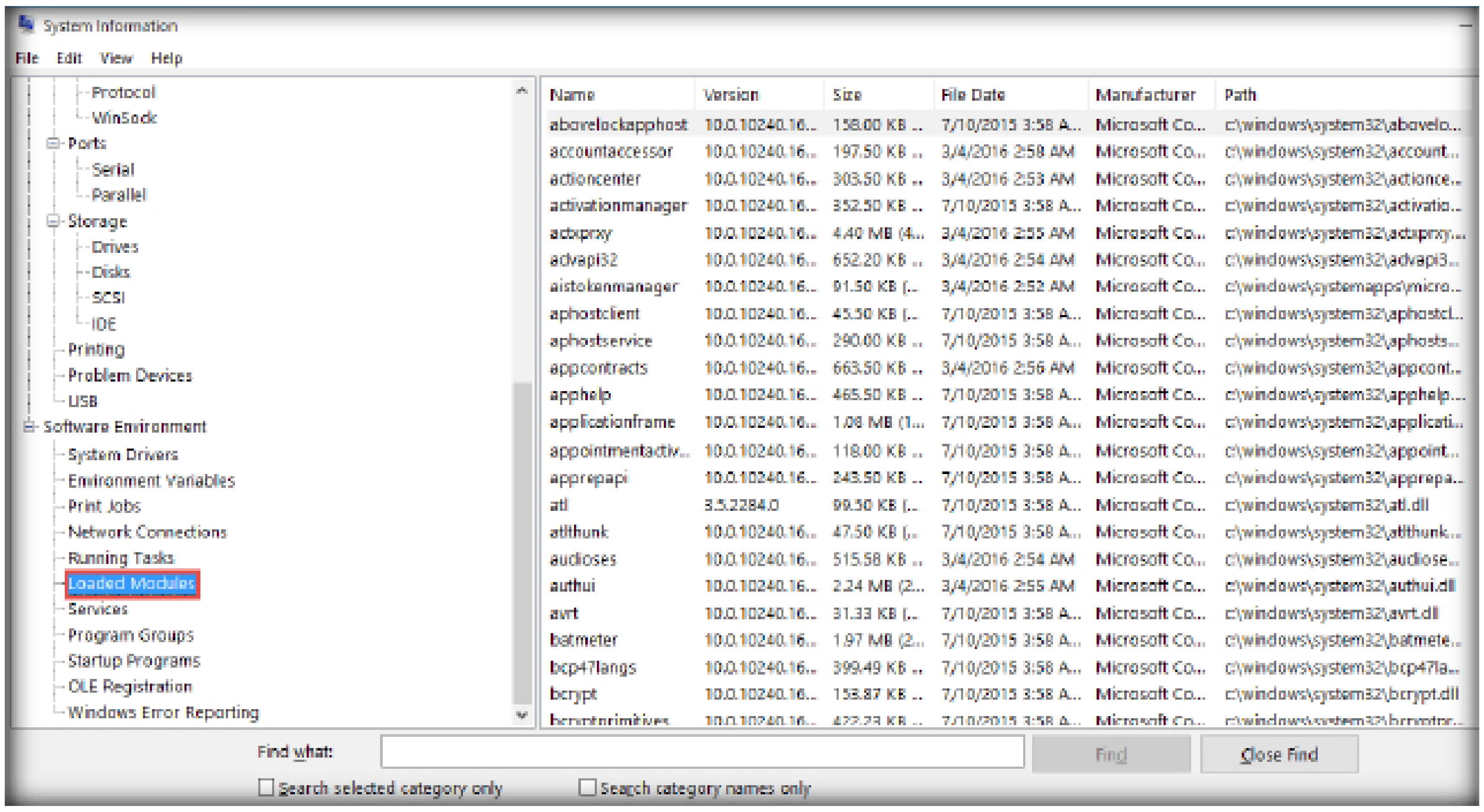
42. The next section shows the **Running Tasks** on the system.



| Name | Path | Process ID | Priority | Min Worki... | Max Work... | Start Time |
|---|---|---|---|---|---|---|
| abservice.exe | Not Available | 2080 | 8 | Not Avail... | Not Avail... | 5/2/2016 2:55 |
| codemeter.exe | Not Available | 1344 | 8 | Not Avail... | Not Avail... | 5/2/2016 2:55 |
| conhost.exe | Not Available | 3560 | 8 | Not Avail... | Not Avail... | 5/2/2016 2:55 |
| conhost.exe | Not Available | 3756 | 8 | Not Avail... | Not Avail... | 5/2/2016 2:55 |
| csrss.exe | Not Available | 380 | 13 | Not Avail... | Not Avail... | 5/2/2016 2:54 |
| csrss.exe | Not Available | 452 | 13 | Not Avail... | Not Avail... | 5/2/2016 2:54 |
| csrss.exe | Not Available | 1748 | 13 | Not Avail... | Not Avail... | 5/2/2016 2:55 |
| dashost.exe | Not Available | 3280 | 8 | Not Avail... | Not Avail... | 5/2/2016 2:55 |
| dwm.exe | Not Available | 776 | 13 | Not Avail... | Not Avail... | 5/2/2016 2:54 |
| dwm.exe | Not Available | 1844 | 13 | Not Avail... | Not Avail... | 5/2/2016 2:55 |
| explorer.exe | c:\windows\explorer.exe | 3884 | 8 | 200 | 1380 | 5/2/2016 2:56 |
| logforwarder.exe | Not Available | 1564 | 8 | Not Avail... | Not Avail... | 5/2/2016 2:55 |
| logonui.exe | Not Available | 764 | 13 | Not Avail... | Not Avail... | 5/2/2016 2:54 |
| lsass.exe | Not Available | 572 | 9 | Not Avail... | Not Avail... | 5/2/2016 2:54 |
| mongod.exe | Not Available | 2440 | 8 | Not Avail... | Not Avail... | 5/2/2016 2:59 |
| msinfo32.exe | c:\windows\system32\msinfo3... | 5576 | 8 | 200 | 1380 | 5/2/2016 3:07 |
| msmpeng.exe | Not Available | 2468 | 8 | Not Avail... | Not Avail... | 5/2/2016 2:55 |
| nissrv.exe | Not Available | 2632 | 8 | Not Avail... | Not Avail... | 5/2/2016 2:56 |
| nxlog.exe | Not Available | 1288 | 8 | Not Avail... | Not Avail... | 5/2/2016 2:55 |
| onedrive.exe | c:\users\win-10\appdata\local\... | 2760 | 8 | 200 | 1380 | 5/2/2016 2:58 |
| prtg server.exe | Not Available | 1384 | 8 | Not Avail... | Not Avail... | 5/2/2016 2:55 |
| python.exe | Not Available | 2128 | 8 | Not Avail... | Not Avail... | 5/2/2016 2:59 |

FIGURE 8.30: Running Tasks Information

43. After that is **Loaded Modules**. It shows the name, version, and size of the module.

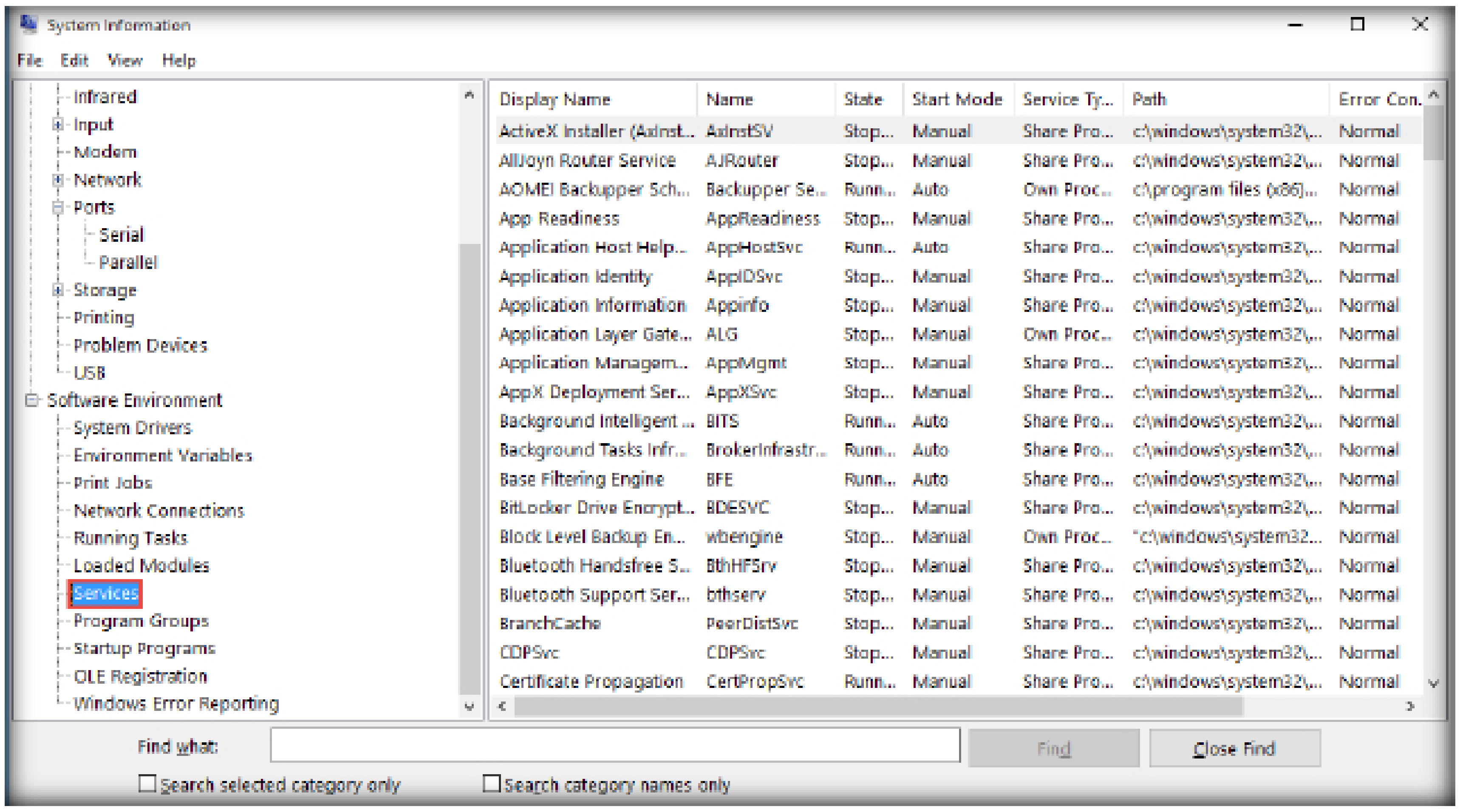


| Name | Version | Size | File Date | Manufacturer | Path |
|---|---|---|---|---|---|
| aborelockapphost | 10.0.10240.16... | 158.00 KB ... | 7/10/2015 3:58 A... | Microsoft Co... | c:\windows\system32\abovelo... |
| accountaccessor | 10.0.10240.16... | 197.50 KB ... | 3/4/2016 2:58 AM | Microsoft Co... | c:\windows\system32\account... |
| actioncenter | 10.0.10240.16... | 303.50 KB ... | 3/4/2016 2:53 AM | Microsoft Co... | c:\windows\system32\actionce... |
| activationmanager | 10.0.10240.16... | 352.50 KB ... | 7/10/2015 3:58 A... | Microsoft Co... | c:\windows\system32\activatio... |
| actxprxy | 10.0.10240.16... | 4.40 MB (4... | 3/4/2016 2:55 AM | Microsoft Co... | c:\windows\system32\actxprxy... |
| advapi32 | 10.0.10240.16... | 652.20 KB ... | 3/4/2016 2:54 AM | Microsoft Co... | c:\windows\system32\advapi3... |
| aistokenmanager | 10.0.10240.16... | 91.50 KB (... | 3/4/2016 2:52 AM | Microsoft Co... | c:\windows\systemapps\micro... |
| aphostclient | 10.0.10240.16... | 45.50 KB (... | 7/10/2015 3:58 A... | Microsoft Co... | c:\windows\system32\aphostcl... |
| aphostservice | 10.0.10240.16... | 290.00 KB ... | 7/10/2015 3:58 A... | Microsoft Co... | c:\windows\system32\aphosts... |
| appcontracts | 10.0.10240.16... | 663.50 KB ... | 3/4/2016 2:56 AM | Microsoft Co... | c:\windows\system32\appcont... |
| apphelp | 10.0.10240.16... | 465.50 KB ... | 7/10/2015 3:58 A... | Microsoft Co... | c:\windows\system32\apphelp... |
| applicationframe | 10.0.10240.16... | 1.08 MB (1... | 7/10/2015 3:58 A... | Microsoft Co... | c:\windows\system32\applicati... |
| appointmentactiv... | 10.0.10240.16... | 118.00 KB ... | 7/10/2015 3:58 A... | Microsoft Co... | c:\windows\system32\appoint... |
| apprepapi | 10.0.10240.16... | 243.50 KB ... | 7/10/2015 3:58 A... | Microsoft Co... | c:\windows\system32\apprepa... |
| atl | 3.5.2284.0 | 99.50 KB (... | 7/10/2015 3:58 A... | Microsoft Co... | c:\windows\system32\atl.dll |
| atlthunk | 10.0.10240.16... | 47.50 KB (... | 7/10/2015 3:58 A... | Microsoft Co... | c:\windows\system32\atlthunk... |
| audioses | 10.0.10240.16... | 515.58 KB ... | 3/4/2016 2:54 AM | Microsoft Co... | c:\windows\system32\audiose... |
| authui | 10.0.10240.16... | 2.24 MB (2... | 3/4/2016 2:55 AM | Microsoft Co... | c:\windows\system32\authui.dll |
| avrt | 10.0.10240.16... | 31.33 KB (... | 7/10/2015 3:58 A... | Microsoft Co... | c:\windows\system32\avrt.dll |
| batmeter | 10.0.10240.16... | 1.97 MB (2... | 7/10/2015 3:58 A... | Microsoft Co... | c:\windows\system32\batmete... |
| bcp47langs | 10.0.10240.16... | 399.49 KB ... | 7/10/2015 3:58 A... | Microsoft Co... | c:\windows\system32\bcp47la... |
| bcrypt | 10.0.10240.16... | 153.87 KB ... | 7/10/2015 3:58 A... | Microsoft Co... | c:\windows\system32\bcrypt.dll |
| bcryptprimitives | 10.0.10240.16... | 422.23 KB ... | 7/10/2015 3:58 A... | Microsoft Co... | c:\windows\system32\bcryptpr... |

□ Search selected category only □ Search category names only

FIGURE 8.31: Loaded Modules Information

44. Next up is the **Services** running on the computer. It shows the name and display name of the service, its current state, and start mode.

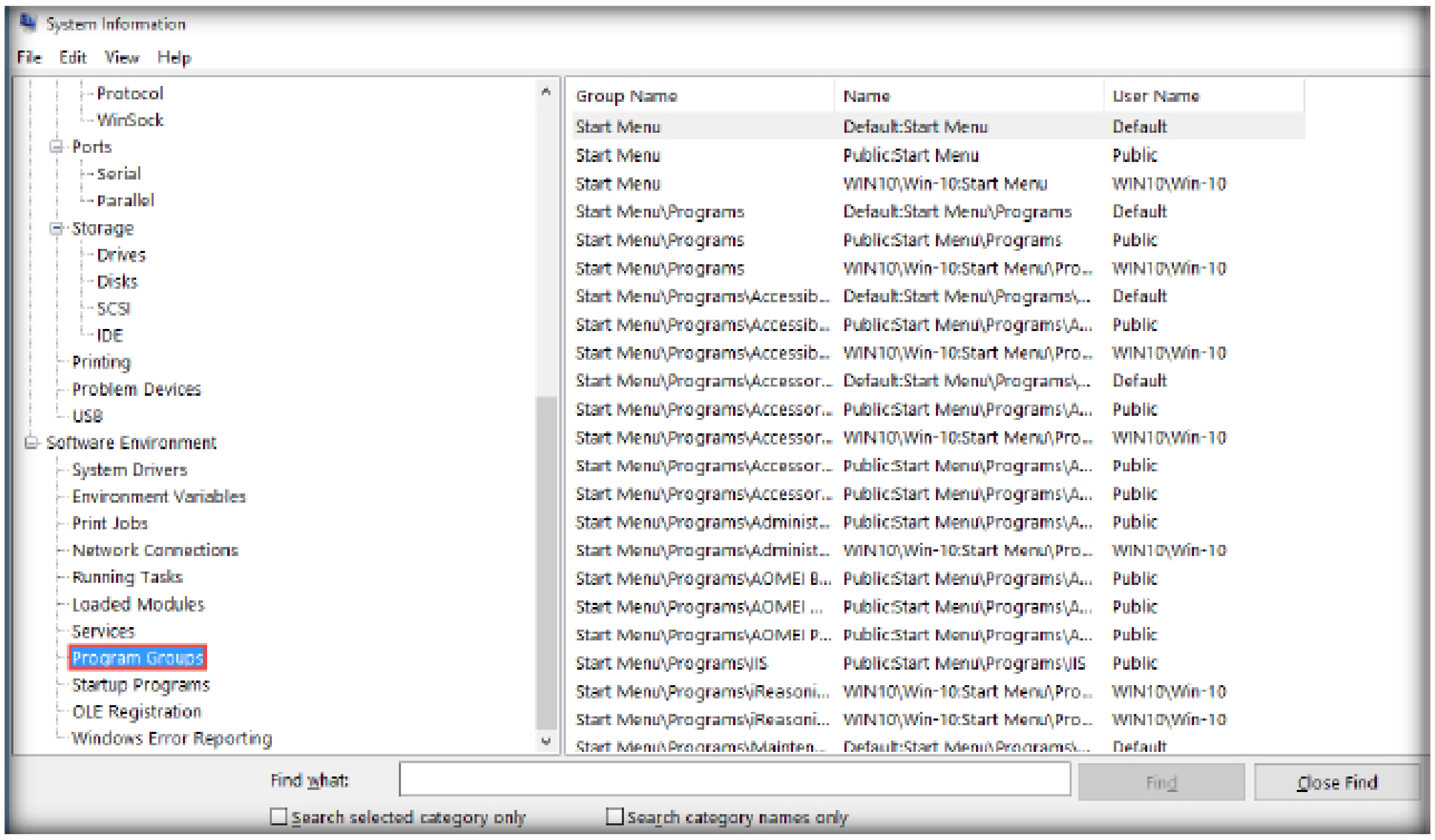


| Display Name | Name | State | Start Mode | Service Ty... | Path | Error Con. |
|---|---|---|---|---|---|---|
| ActiveX Installer (AxInst... | AxInstSV | Stop... | Manual | Share Pro... | c:\windows\system32\... | Normal |
| AllJoyn Router Service | AJRouter | Stop... | Manual | Share Pro... | c:\windows\system32\... | Normal |
| AOMEI Backupper Sch... | Backupper Se... | Runn... | Auto | Own Proc... | c:\program files (x86)\... | Normal |
| App Readiness | AppReadiness | Stop... | Manual | Share Pro... | c:\windows\system32\... | Normal |
| Application Host Help... | AppHostSvc | Runn... | Auto | Share Pro... | c:\windows\system32\... | Normal |
| Application Identity | AppIDSvc | Stop... | Manual | Share Pro... | c:\windows\system32\... | Normal |
| Application Information | Appinfo | Stop... | Manual | Share Pro... | c:\windows\system32\... | Normal |
| Application Layer Gate... | ALG | Stop... | Manual | Own Proc... | c:\windows\system32\... | Normal |
| Application Managem... | AppMgmt | Stop... | Manual | Share Pro... | c:\windows\system32\... | Normal |
| AppX Deployment Ser... | AppXSvc | Stop... | Manual | Share Pro... | c:\windows\system32\... | Normal |
| Background Intelligent ... | BITS | Runn... | Auto | Share Pro... | c:\windows\system32\... | Normal |
| Background Tasks Infr... | BrokerInfrastr... | Runn... | Auto | Share Pro... | c:\windows\system32\... | Normal |
| Base Filtering Engine | BFE | Runn... | Auto | Share Pro... | c:\windows\system32\... | Normal |
| BitLocker Drive Encrypt... | BDESVC | Stop... | Manual | Share Pro... | c:\windows\system32\... | Normal |
| Block Level Backup En... | wbengine | Stop... | Manual | Own Proc... | "c:\windows\system32... | Normal |
| Bluetooth Handsfree S... | BthHFSrv | Stop... | Manual | Share Pro... | c:\windows\system32\... | Normal |
| Bluetooth Support Ser... | bthserv | Stop... | Manual | Share Pro... | c:\windows\system32\... | Normal |
| BranchCache | PeerDistSvc | Stop... | Manual | Share Pro... | c:\windows\system32\... | Normal |
| CDPSvc | CDPSvc | Stop... | Manual | Share Pro... | c:\windows\system32\... | Normal |
| Certificate Propagation | CertPropSvc | Runn... | Manual | Share Pro... | c:\windows\system32\... | Normal |

□ Search selected category only □ Search category names only

FIGURE 8.32: Available Services Information

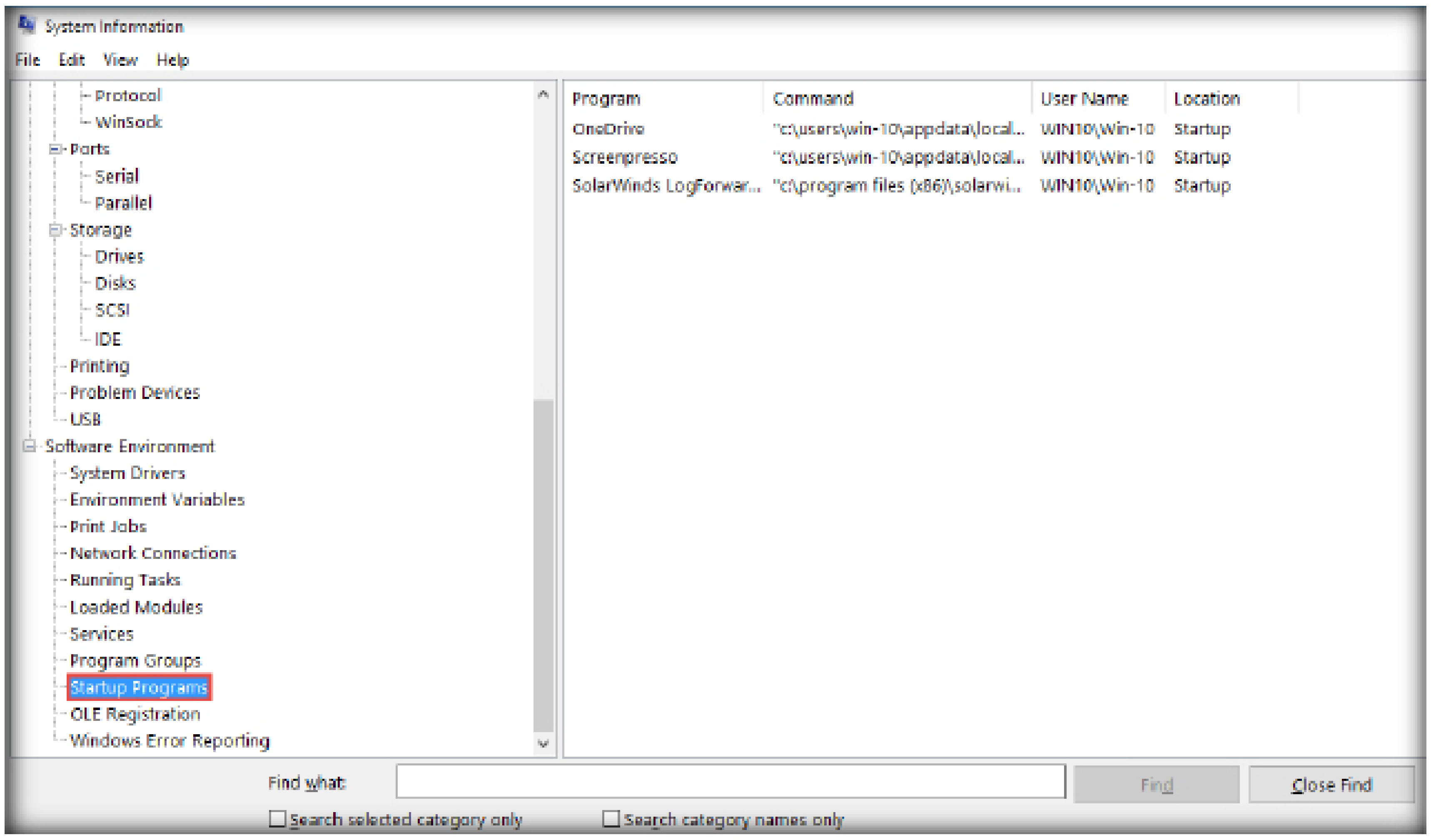
45. **Program Groups** is the next subsection. It has various start menu items grouped under programs. It shows the group name, name of the program and user name.



| Group Name | Name | User Name |
|---|---|---|
| Start Menu | Default:Start Menu | Default |
| Start Menu | Public:Start Menu | Public |
| Start Menu | WIN10\Win-10:Start Menu | WIN10\Win-10 |
| Start Menu\Programs | Default:Start Menu\Programs | Default |
| Start Menu\Programs | Public:Start Menu\Programs | Public |
| Start Menu\Programs | WIN10\Win-10:Start Menu\Pro... | WIN10\Win-10 |
| Start Menu\Programs\Accessib... | Default:Start Menu\Programs\... | Default |
| Start Menu\Programs\Accessib... | Public:Start Menu\Programs\A... | Public |
| Start Menu\Programs\Accessib... | WIN10\Win-10:Start Menu\Pro... | WIN10\Win-10 |
| Start Menu\Programs\Accessor... | Default:Start Menu\Programs\... | Default |
| Start Menu\Programs\Accessor... | Public:Start Menu\Programs\A... | Public |
| Start Menu\Programs\Accessor... | WIN10\Win-10:Start Menu\Pro... | WIN10\Win-10 |
| Start Menu\Programs\Accessor... | Public:Start Menu\Programs\A... | Public |
| Start Menu\Programs\Accessor... | Public:Start Menu\Programs\A... | Public |
| Start Menu\Programs\Administ... | Public:Start Menu\Programs\A... | Public |
| Start Menu\Programs\Administ... | WIN10\Win-10:Start Menu\Pro... | WIN10\Win-10 |
| Start Menu\Programs\AOMEI B... | Public:Start Menu\Programs\A... | Public |
| Start Menu\Programs\AOMEI ... | Public:Start Menu\Programs\A... | Public |
| Start Menu\Programs\AOMEI P... | Public:Start Menu\Programs\A... | Public |
| Start Menu\Programs\IIS | Public:Start Menu\Programs\IIS | Public |
| Start Menu\Programs\jReasoni... | WIN10\Win-10:Start Menu\Pro... | WIN10\Win-10 |
| Start Menu\Programs\jReasoni... | WIN10\Win-10:Start Menu\Pro... | WIN10\Win-10 |
| Start Menu\Programs\Mainten... | Default:Start Menu\Programs\... | Default |

FIGURE 8.33: Program Groups Information

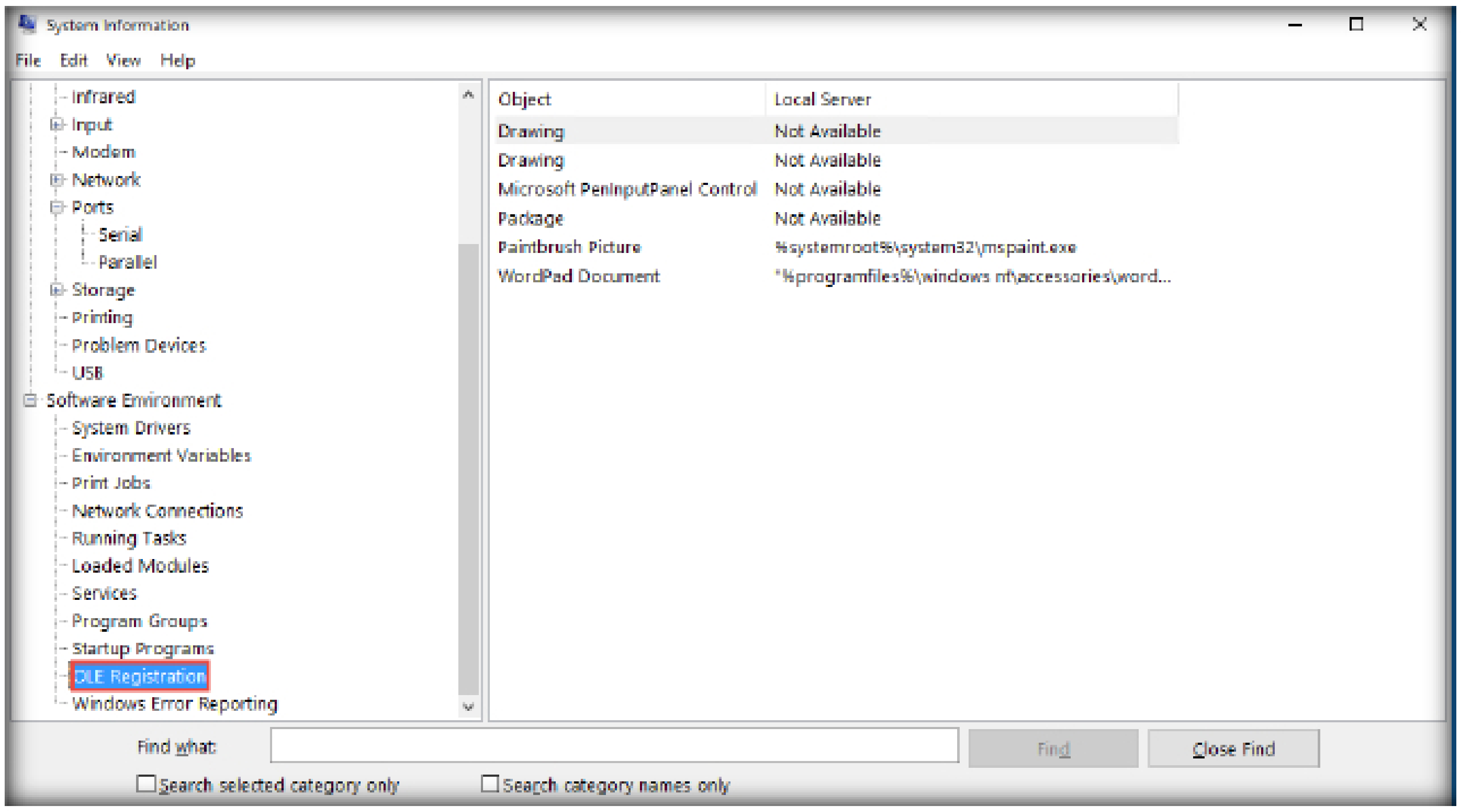
46. The **Startup Programs** shows a list of programs that auto start when the system starts.



| Program | Command | User Name | Location |
|---|---|---|---|
| OneDrive | "c:\users\win-10\appdata\local... | WIN10\Win-10 | Startup |
| Screenpresso | "c:\users\win-10\appdata\local... | WIN10\Win-10 | Startup |
| SolarWinds LogForwar... | "c:\program files (x86)\solarwi... | WIN10\Win-10 | Startup |

FIGURE 8.34: Startup Programs List Information

47. The next subsection is **OLE** (object linking and embedding) registration. It has information about components and their servers, which are registered as OLE programs.



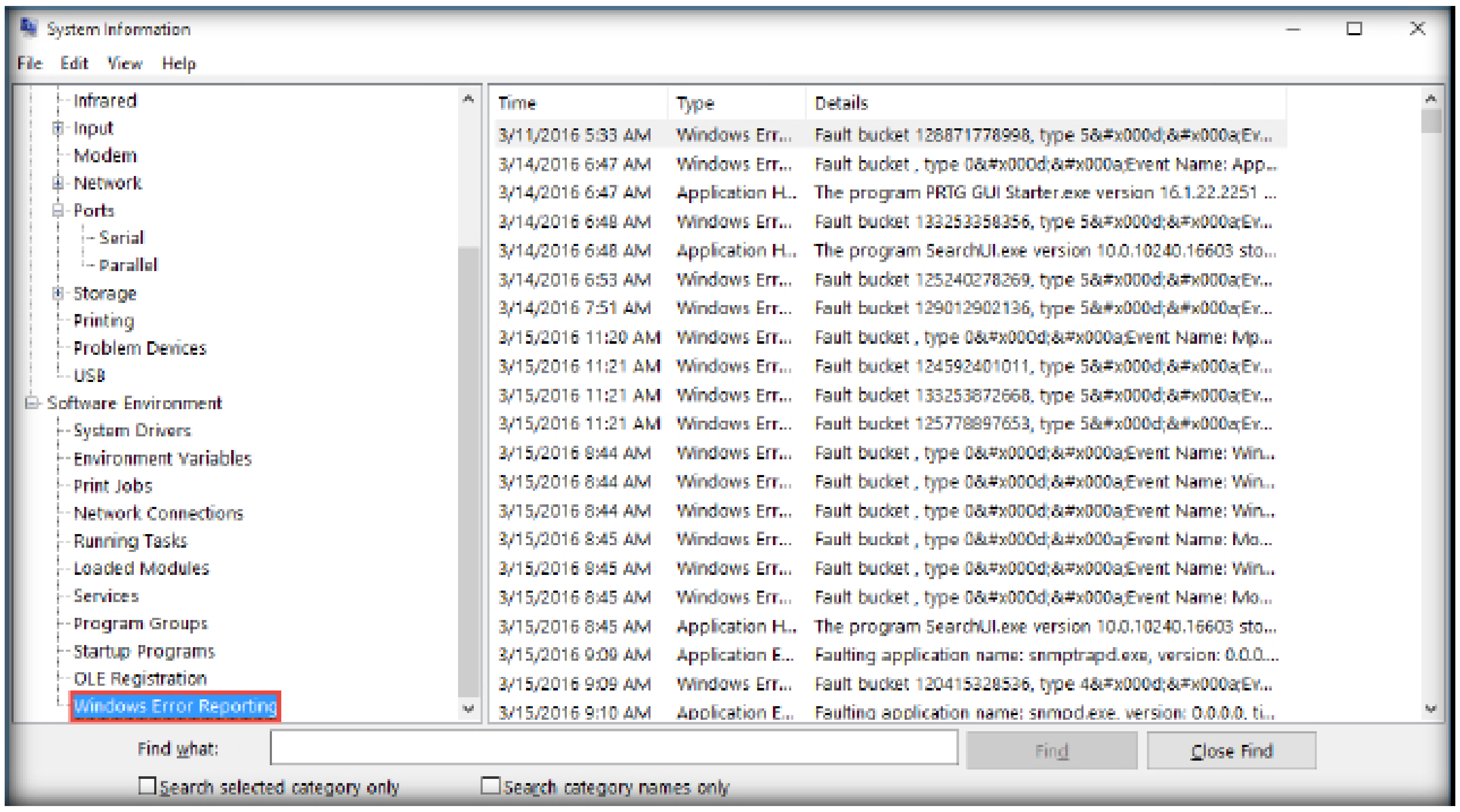
| Object | Local Server |
|---|---|
| Drawing | Not Available |
| Drawing | Not Available |
| Microsoft PenInputPanel Control | Not Available |
| Package | Not Available |
| Paintbrush Picture | %systemroot%\system32\mspaint.exe |
| WordPad Document | "%programfiles%\windows nt\accessories\word... |

Find what:

☐ Search selected category only ☐ Search category names only

FIGURE 8.35: OLE Registration Information

48. The final subsection is **Windows Error Reporting**. It shows the date and the time an error occurs, type of error and the details of the error.



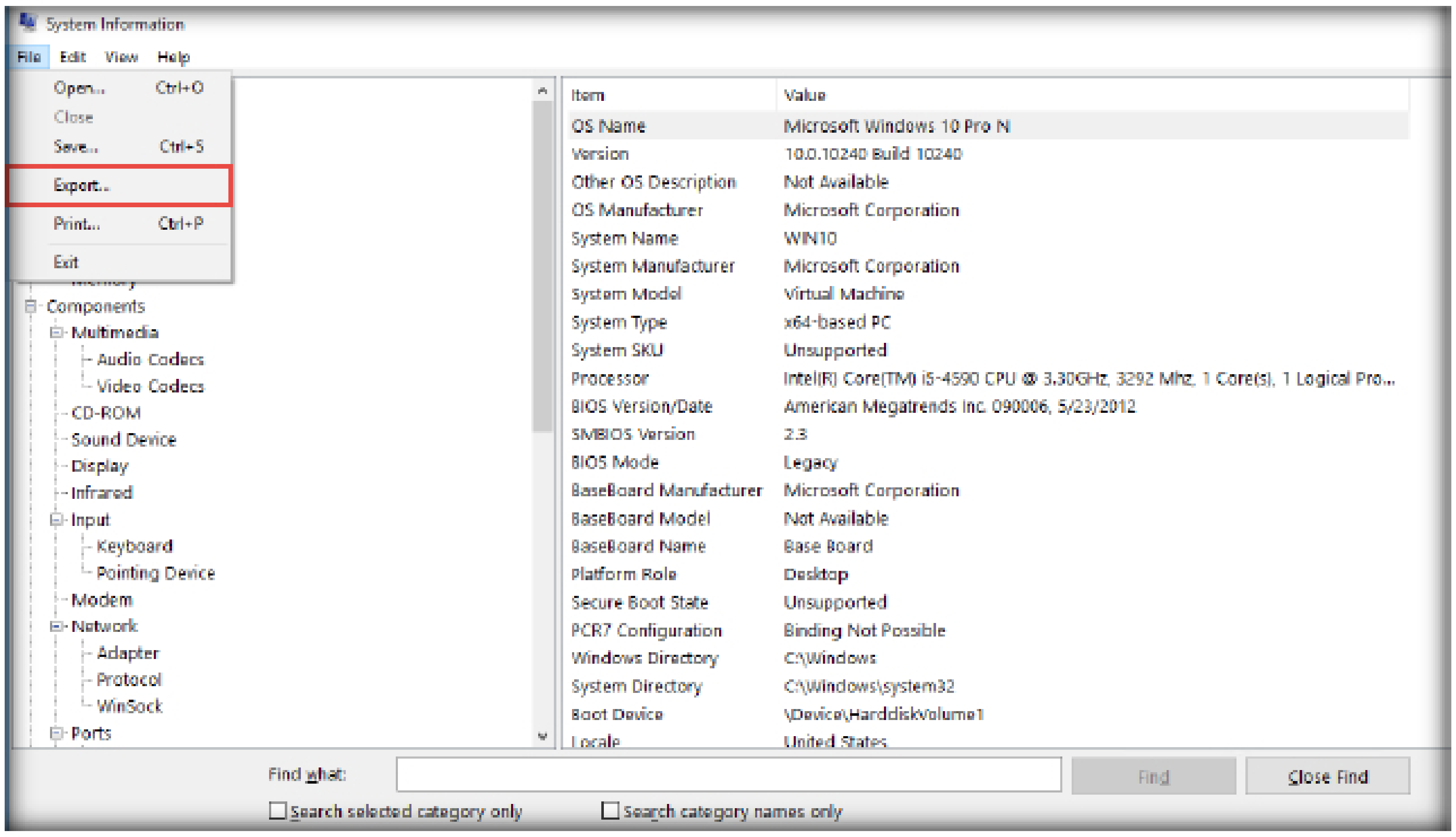
| Time | Type | Details |
|---|---|---|
| 3/11/2016 5:33 AM | Windows Err... | Fault bucket 128871778998, type 5&#x000d;&#x000a;Ev... |
| 3/14/2016 6:47 AM | Windows Err... | Fault bucket , type 0&#x000d;&#x000a;Event Name: App... |
| 3/14/2016 6:47 AM | Application H... | The program PRTG GUI Starter.exe version 16.1.22.2251 ... |
| 3/14/2016 6:48 AM | Windows Err... | Fault bucket 133253358356, type 5&#x000d;&#x000a;Ev... |
| 3/14/2016 6:48 AM | Application H... | The program SearchUI.exe version 10.0.10240.16603 sto... |
| 3/14/2016 6:53 AM | Windows Err... | Fault bucket 125240278269, type 5&#x000d;&#x000a;Ev... |
| 3/14/2016 7:51 AM | Windows Err... | Fault bucket 129012902136, type 5&#x000d;&#x000a;Ev... |
| 3/15/2016 11:20 AM | Windows Err... | Fault bucket , type 0&#x000d;&#x000a;Event Name: Mp... |
| 3/15/2016 11:21 AM | Windows Err... | Fault bucket 124592401011, type 5&#x000d;&#x000a;Ev... |
| 3/15/2016 11:21 AM | Windows Err... | Fault bucket 133253872668, type 5&#x000d;&#x000a;Ev... |
| 3/15/2016 11:21 AM | Windows Err... | Fault bucket 125778897653, type 5&#x000d;&#x000a;Ev... |
| 3/15/2016 8:44 AM | Windows Err... | Fault bucket , type 0&#x000d;&#x000a;Event Name: Win... |
| 3/15/2016 8:44 AM | Windows Err... | Fault bucket , type 0&#x000d;&#x000a;Event Name: Win... |
| 3/15/2016 8:44 AM | Windows Err... | Fault bucket , type 0&#x000d;&#x000a;Event Name: Win... |
| 3/15/2016 8:45 AM | Windows Err... | Fault bucket , type 0&#x000d;&#x000a;Event Name: Mo... |
| 3/15/2016 8:45 AM | Windows Err... | Fault bucket , type 0&#x000d;&#x000a;Event Name: Win... |
| 3/15/2016 8:45 AM | Windows Err... | Fault bucket , type 0&#x000d;&#x000a;Event Name: Mo... |
| 3/15/2016 8:45 AM | Application H... | The program SearchUI.exe version 10.0.10240.16603 sto... |
| 3/15/2016 9:09 AM | Application E... | Faulting application name: snmptrapd.exe, version: 0.0.0.... |
| 3/15/2016 9:09 AM | Windows Err... | Fault bucket 120415328536, type 4&#x000d;&#x000a;Ev... |
| 3/15/2016 9:10 AM | Application E... | Faulting application name: snmpd.exe, version: 0.0.0.0, ti... |

Find what:

☐ Search selected category only ☐ Search category names only

FIGURE 8.36: Windows Error Reporting Information

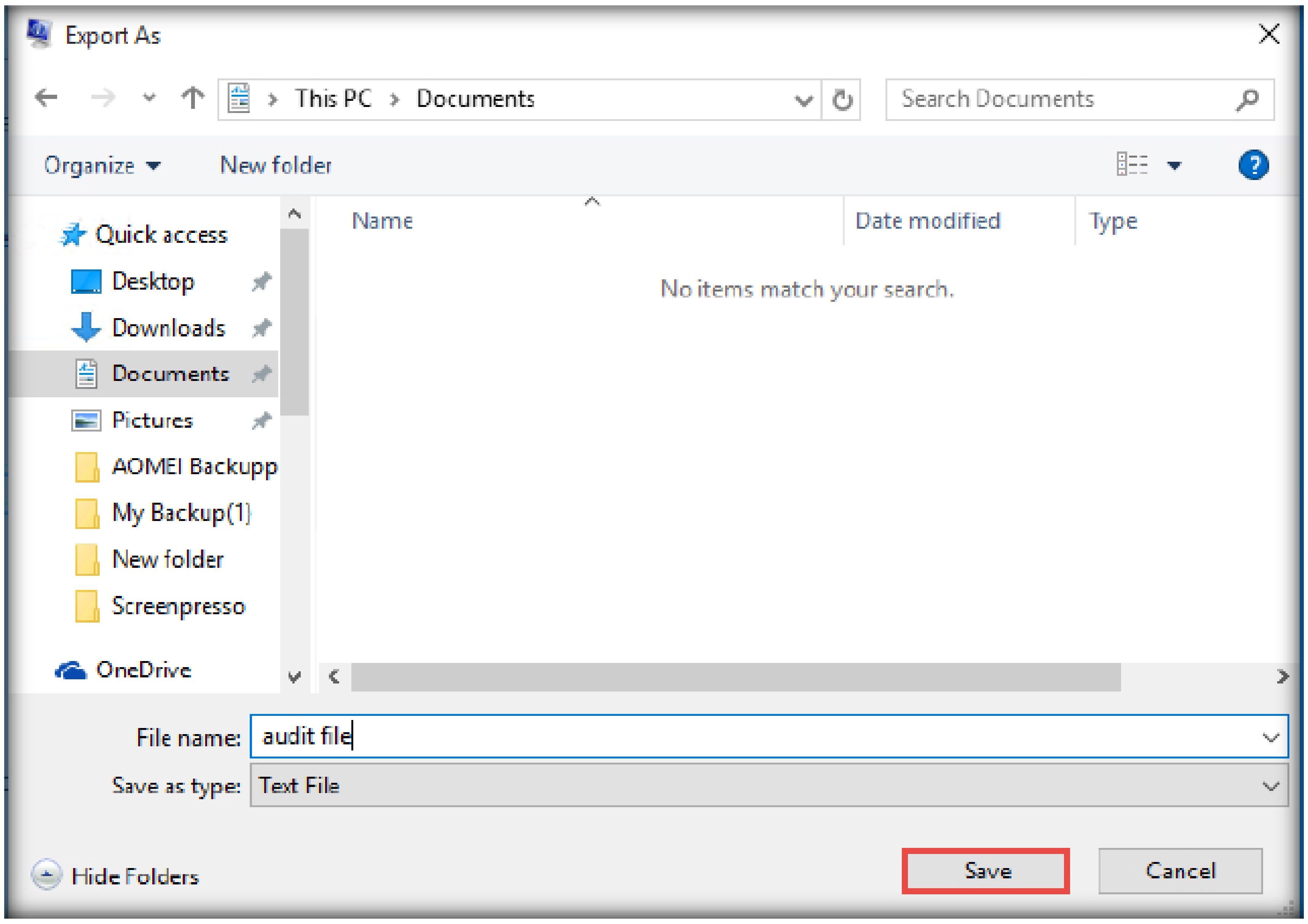
49. If you want to store the current status of msinfo32 for future audits, you can go to **File ->Export** and provide a name and save as a text file.



| Item | Value |
|---|---|
| OS Name | Microsoft Windows 10 Pro N |
| Version | 10.0.10240 Build 10240 |
| Other OS Description | Not Available |
| OS Manufacturer | Microsoft Corporation |
| System Name | WIN10 |
| System Manufacturer | Microsoft Corporation |
| System Model | Virtual Machine |
| System Type | x64-based PC |
| System SKU | Unsupported |
| Processor | Intel(R) Core(TM) i5-4590 CPU @ 3.30GHz, 3292 Mhz, 1 Core(s), 1 Logical Pro... |
| BIOS Version/Date | American Megatrends Inc. 090006, 5/23/2012 |
| SMBIOS Version | 2.3 |
| BIOS Mode | Legacy |
| BaseBoard Manufacturer | Microsoft Corporation |
| BaseBoard Model | Not Available |
| BaseBoard Name | Base Board |
| Platform Role | Desktop |
| Secure Boot State | Unsupported |
| PCR7 Configuration | Binding Not Possible |
| Windows Directory | C:\Windows |
| System Directory | C:\Windows\system32 |
| Boot Device | \Device\HarddiskVolume1 |
| Locale | United States |

FIGURE 8.37: Exporting System Information

50. The **Export As** window appears. Select a location, provide a name in **File name** section and click **Save**.



No items match your search.

File name: audit file

Save as type: Text File

FIGURE 8.38: Saving Exported Audit File

## Lab Analysis

Analyze and document the results of the lab exercise. Give your opinion on your target's security posture and exposure through free public information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

| Internet Connection Required | |
|---|---|
| ☐ Yes | ☑ No |
| Platform Supported | |
| ☑ Classroom | ☑ iLabs |

Lab

9

# Implementing Host-based Firewall Protection with iptables

*iptables are a command-line firewall utility that uses policy chains to allow or block traffic.*

## Lab Scenario

As an administrator, you should know how to configure an iptables host based firewall to allow or block traffic to or from a Linux system. iptables allow administrators to enter rules for the firewall into the existing tables using the command line.

**ICON KEY**

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

## Lab Objectives

This lab will demonstrate how to configure an iptables host-based firewall in an Ubuntu machine.

## Lab Environment

To carry out the lab, you need:

- A virtual machine running Windows Server 2012
- WinPcap installed in the Windows Server 2012 virtual machine
- A virtual machine running Ubuntu
- **Administrative** privileges to run the tools

## Lab Duration

Time: 25 Minutes

## Overview of iptables

iptables is a standard firewall included in most Linux distributions. With the default chain policies configured, you can start adding rules to iptables so it knows what to do when it encounters a connection from or to a particular IP address or port.

## Lab Tasks

1. Launch the **Ubuntu** machine and login.
2. Launch **Windows Server 2012** and login as an Administrator.

**TASK 1**

**Install and Launch Nmap**

3. Install Nmap, to install Nmap navigate to **Z:\CND-Tools\CND Module 06 Host Security\Port Scanning Tools\Nmap** and double-click nmap-6-25-setup.exe.
4. While installation is in progress, Nmap will prompt you to install WinPcap, if it is already installed skip the installation of WinPcap, and proceed to the installation of Nmap.
5. Select the Desktop icon check box, at the Create Shortcuts wizard of the Nmap installation and follow the wizard driven installation steps.
6. To launch Nmap – Zenmap GUI, navigate to the Desktop and double-click the Nmap – Zenmap GUI icon in order to launch the application. Alternatively, you can also launch from the installed start menu apps.

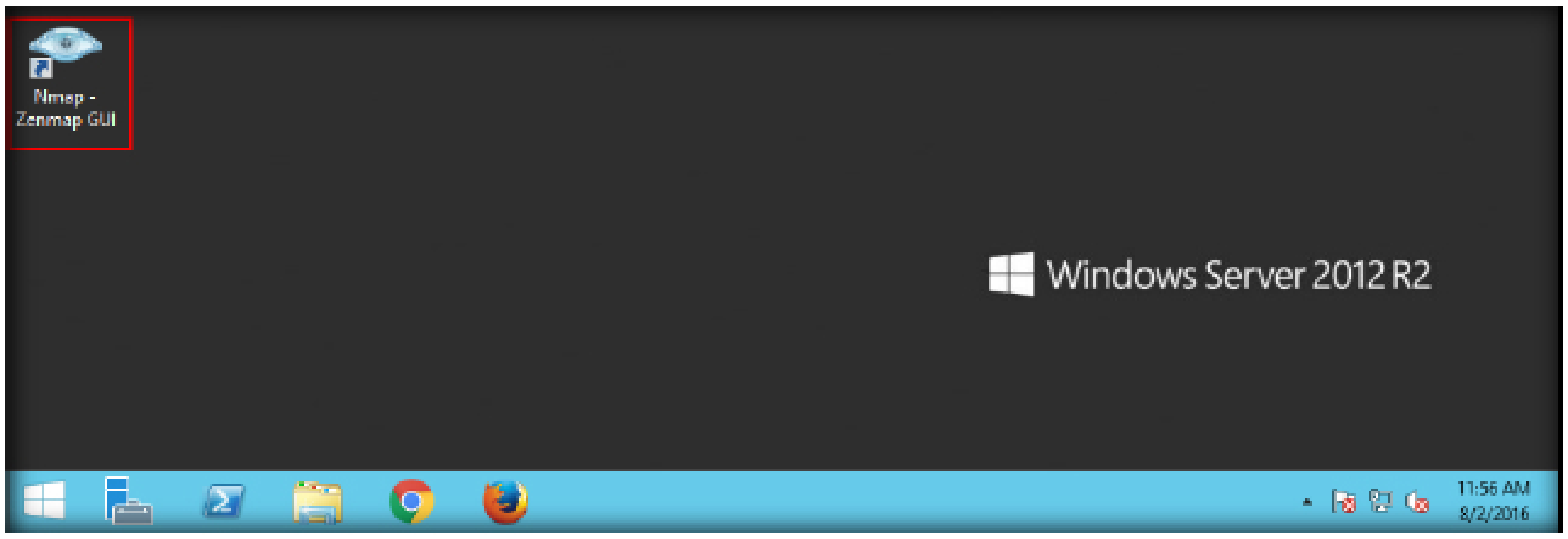
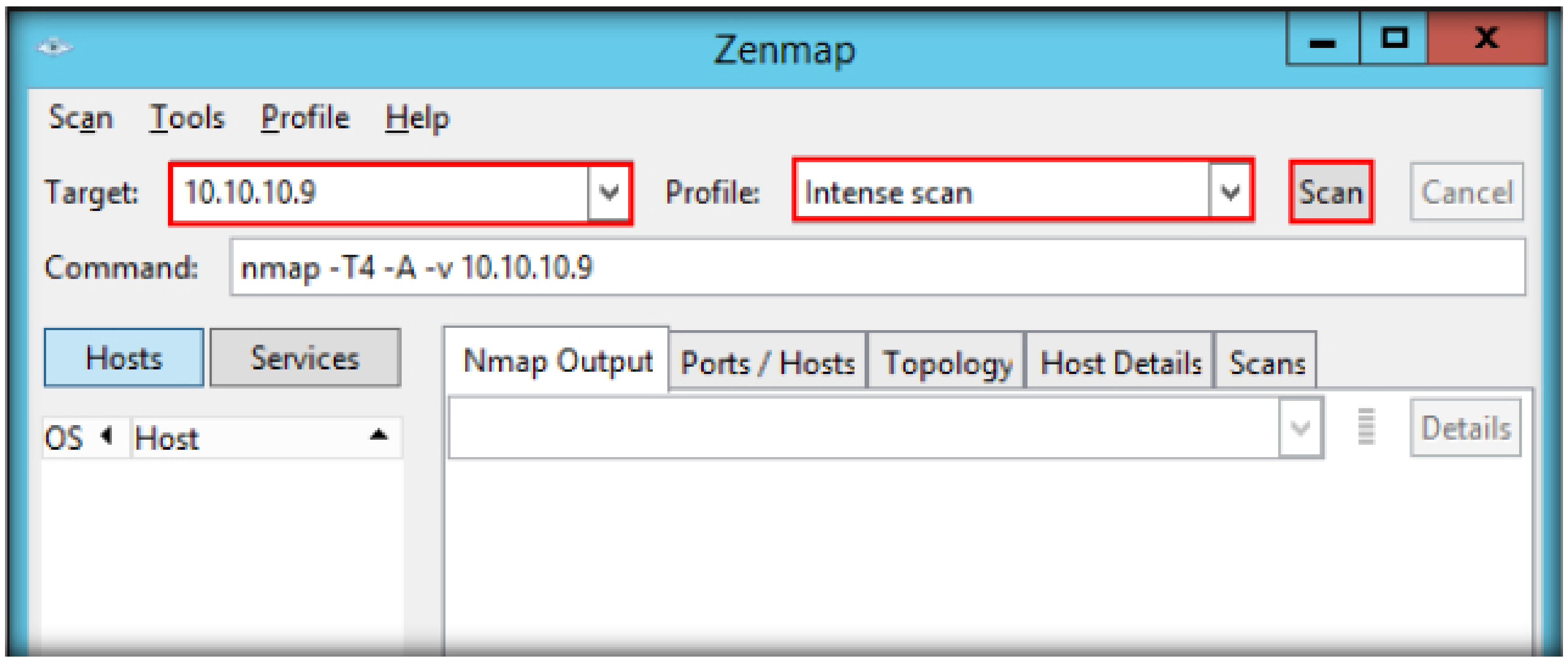


FIGURE 9.1: Launching NMAP

**Tools Demonstrated in this lab are located at Z:\CND-Tools\CND Module 06 Host Security\Port Scanning Tools\Nmap**

7. The Zenmap main window appears as shown in the screenshot. Type **10.10.10.9** in the **Target:** field, select **Intense scan** in the **Profile:** field and click **Scan**.

Note: 10.10.10.9 is the IP Address of the Ubuntu Machine. IP addresses may differ in your lab environment.



Target: 10.10.10.9

Profile: Intense scan

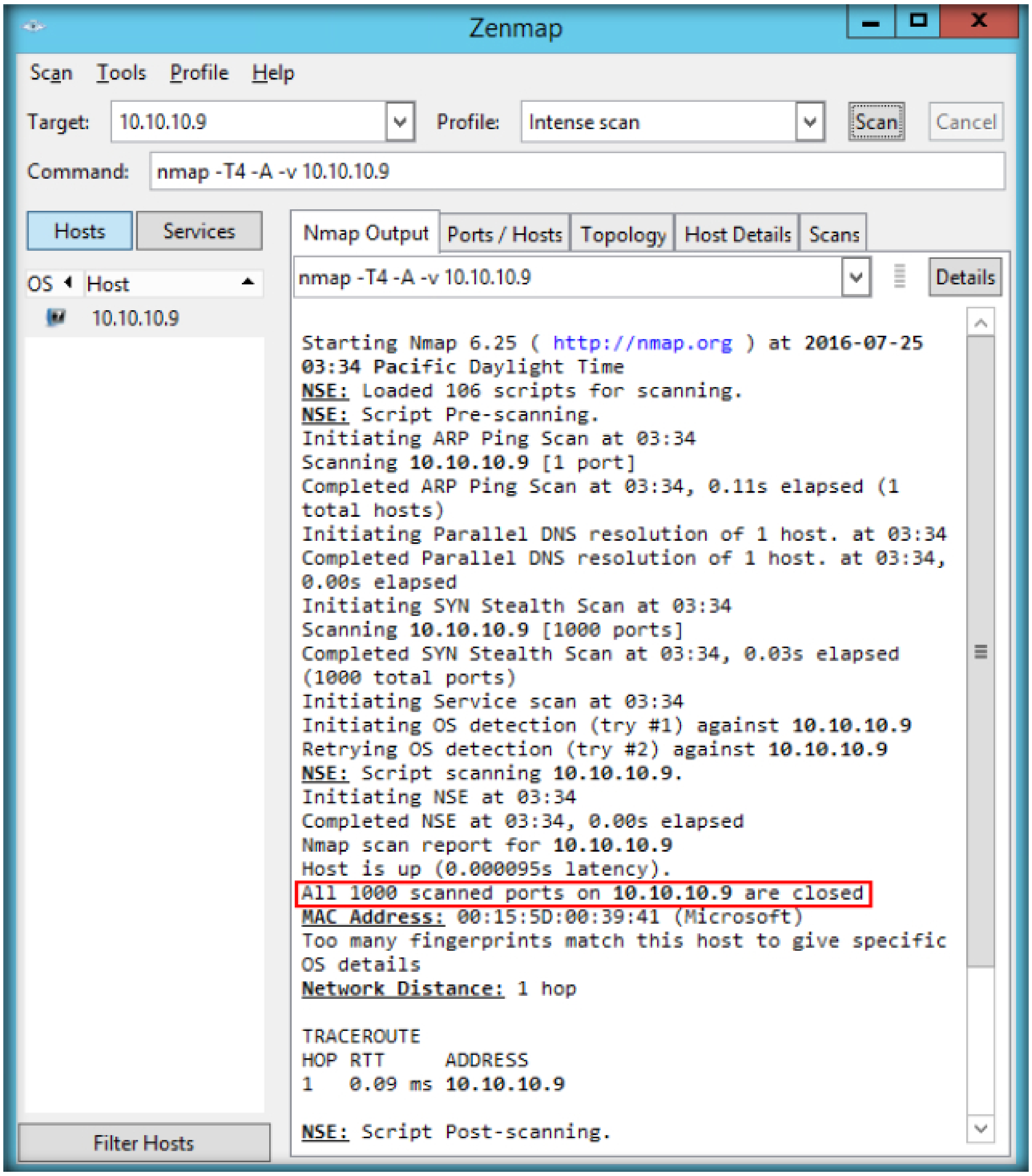
Command: nmap -T4 -A -v 10.10.10.9

FIGURE 9.2: Selecting the Scan Profile

8. Zenmap will show you the scan results of the Ubuntu machine as shown in the screenshot.

The "Intense scan" is just one of several scan profiles that come with Zenmap. Choose a profile by selecting it from the "Profile" combo box. Profiles exist for several common scans.

An intense, comprehensive scan. The -A option enables OS detection (-O), version detection (-sV), script scanning (-sC), and traceroute (--traceroute). Without root privileges only version detection and script scanning are run. This is considered an intrusive scan.



Target: 10.10.10.9

Profile: Intense scan

Command: nmap -T4 -A -v 10.10.10.9

10.10.10.9

nmap -T4 -A -v 10.10.10.9

```
Starting Nmap 6.25 ( http://nmap.org ) at 2016-07-25
03:34 Pacific Daylight Time
NSE: Loaded 106 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 03:34
Scanning 10.10.10.9 [1 port]
Completed ARP Ping Scan at 03:34, 0.11s elapsed (1
total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:34
Completed Parallel DNS resolution of 1 host. at 03:34,
0.00s elapsed
Initiating SYN Stealth Scan at 03:34
Scanning 10.10.10.9 [1000 ports]
Completed SYN Stealth Scan at 03:34, 0.03s elapsed
(1000 total ports)
Initiating Service scan at 03:34
Initiating OS detection (try #1) against 10.10.10.9
Retrying OS detection (try #2) against 10.10.10.9
NSE: Script scanning 10.10.10.9.
Initiating NSE at 03:34
Completed NSE at 03:34, 0.00s elapsed
Nmap scan report for 10.10.10.9
Host is up (0.000095s latency).
All 1000 scanned ports on 10.10.10.9 are closed
MAC Address: 00:15:5D:00:39:41 (Microsoft)
Too many fingerprints match this host to give specific
OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.09 ms 10.10.10.9

NSE: Script Post-scanning.
```

FIGURE 9.3: Scan Results

## TASK 2

**Ping Test**

9. Right click the Start icon in the lower left corner of the desktop and click **Command Prompt** from the context menu.

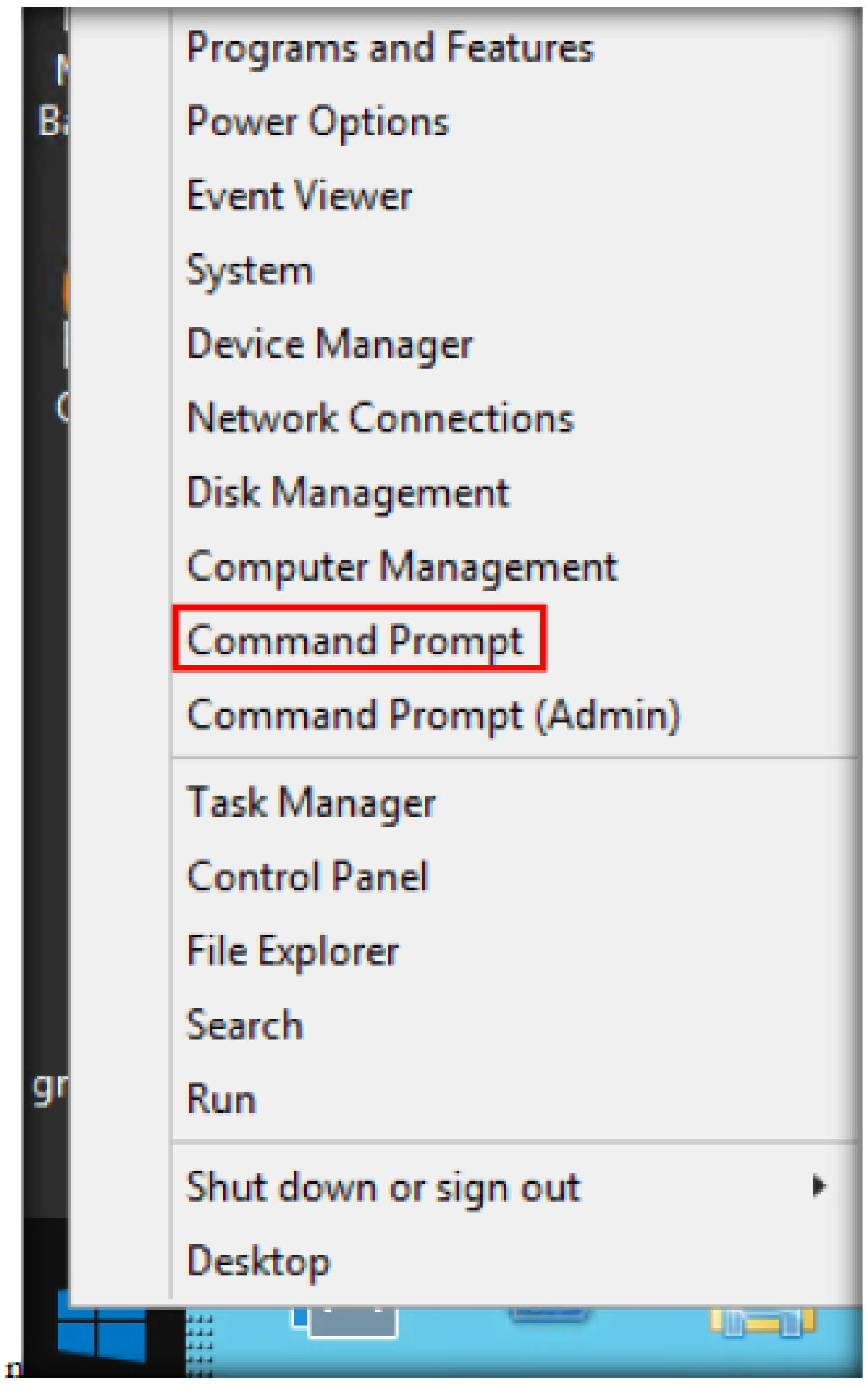
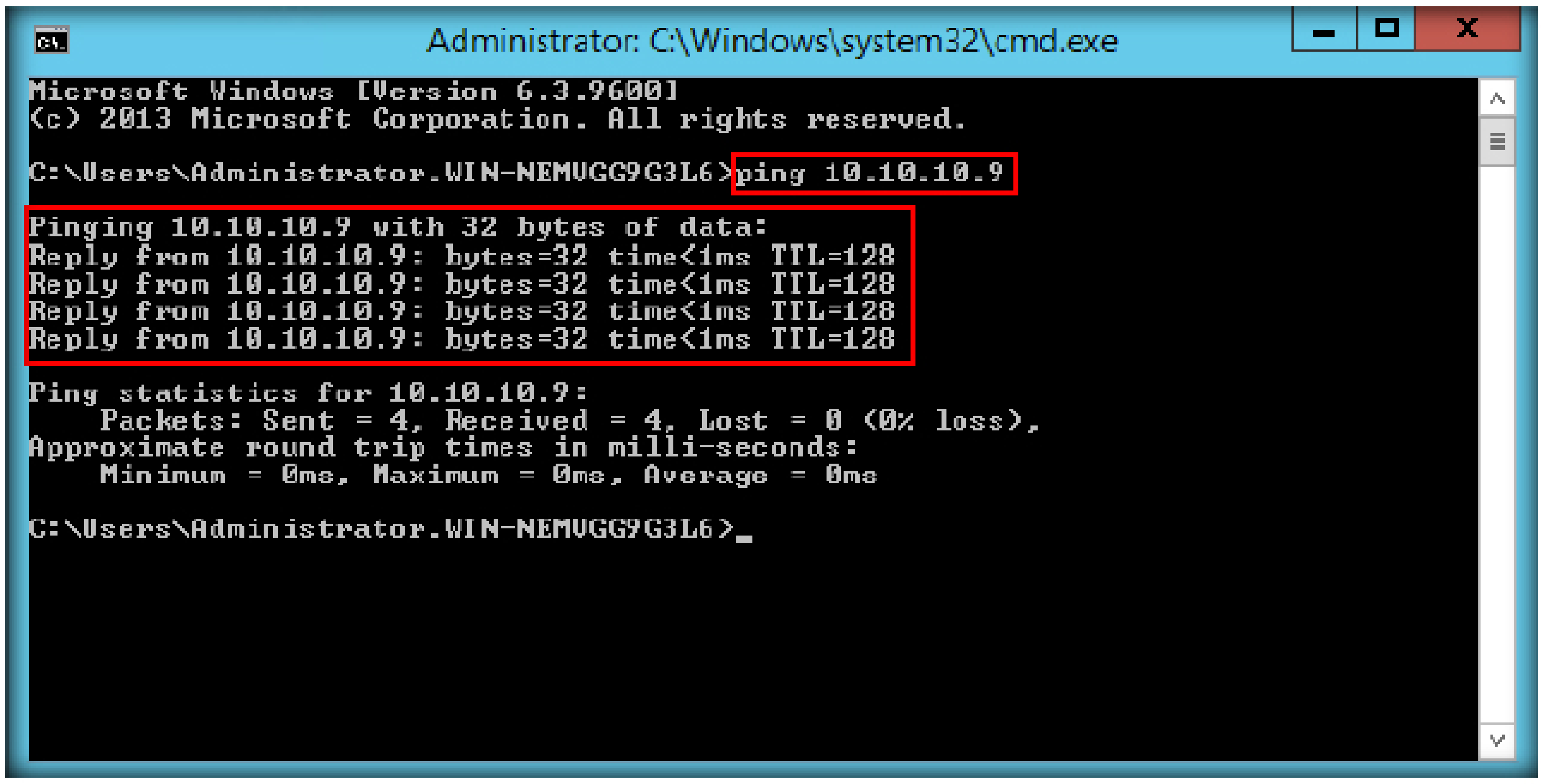


FIGURE 9.4: Launching Command Prompt

The PING command sends a test packet of data to a designated IP address.

10. In the command prompt window type **ping 10.10.10.9** and press **Enter**.

11. You can see that the Ubuntu device is accepting connections from any machine.



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.WIN-NEMUGG9G3L6>ping 10.10.10.9

Pinging 10.10.10.9 with 32 bytes of data:
Reply from 10.10.10.9: bytes=32 time<1ms TTL=128
Reply from 10.10.10.9: bytes=32 time<1ms TTL=128
Reply from 10.10.10.9: bytes=32 time<1ms TTL=128
Reply from 10.10.10.9: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.10.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator.WIN-NEMUGG9G3L6>_
```

FIGURE 9.5: Ping Successful

12. Switch to the **Ubuntu** machine and right click on the Desktop and select **Open Terminal**. Alternatively, you can click the Terminal icon from the taskbar.

iptables is a user-space application program that allows a system administrator to configure the tables provided by the Linux kernel firewall (implemented as different Netfilter modules) and the chains and rules it stores.

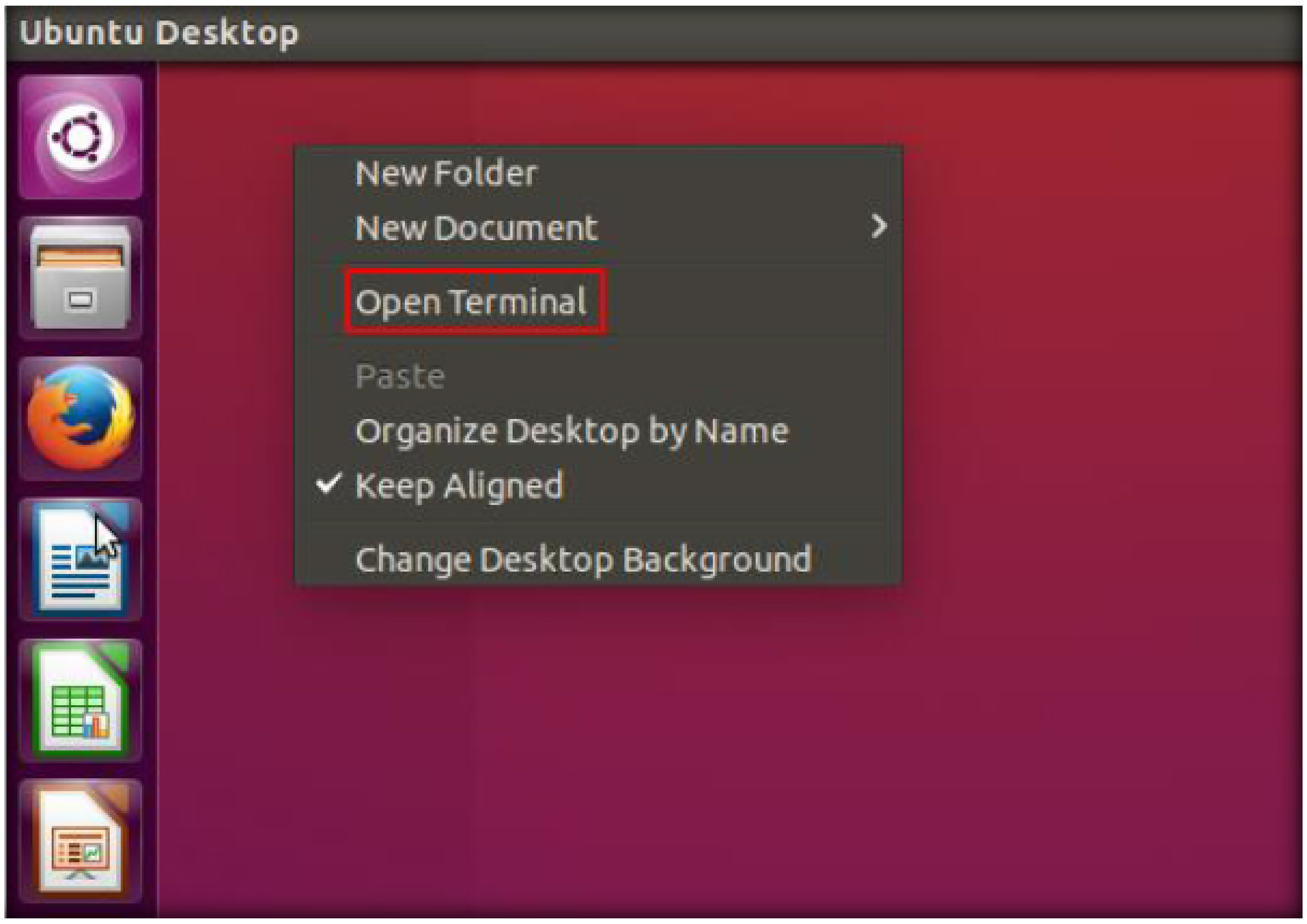
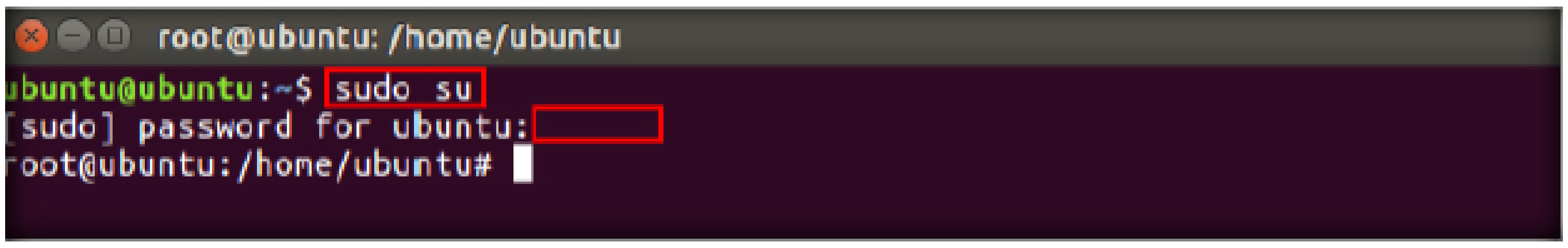


FIGURE 9.6: Launching a Terminal in Ubuntu

13. Switch to super user mode by using the command **sudo su**. Enter the root password as **toor**.

Note: The password that you enter will not be visible.



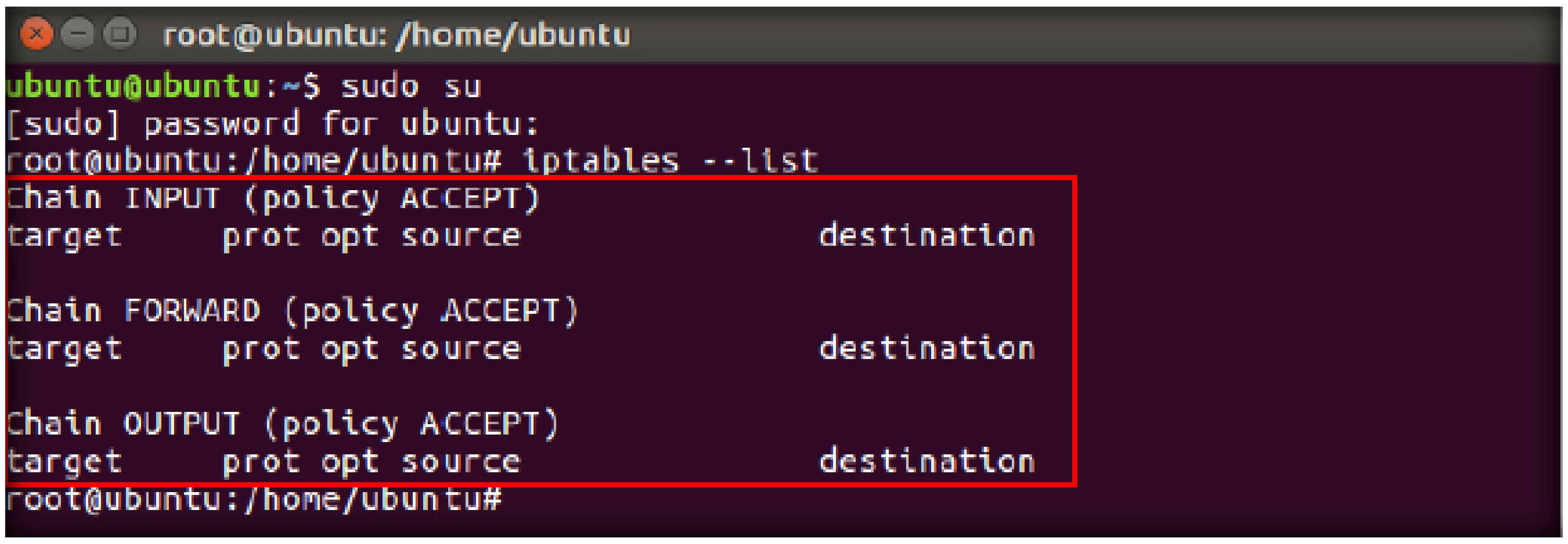
```
root@ubuntu: /home/ubuntu
buntu@ubuntu:~$ sudo su
sudo] password for ubuntu:
oot@ubuntu:/home/ubuntu# 
```

FIGURE 9.7: Gaining an Access as Super User

14. Type **iptables --list** and press **Enter**. This command will list the existing iptables rules as shown in the screenshot.

15. You can see that all three chains accept all kinds of information. Now, we need to change these rule settings to make Ubuntu secure.

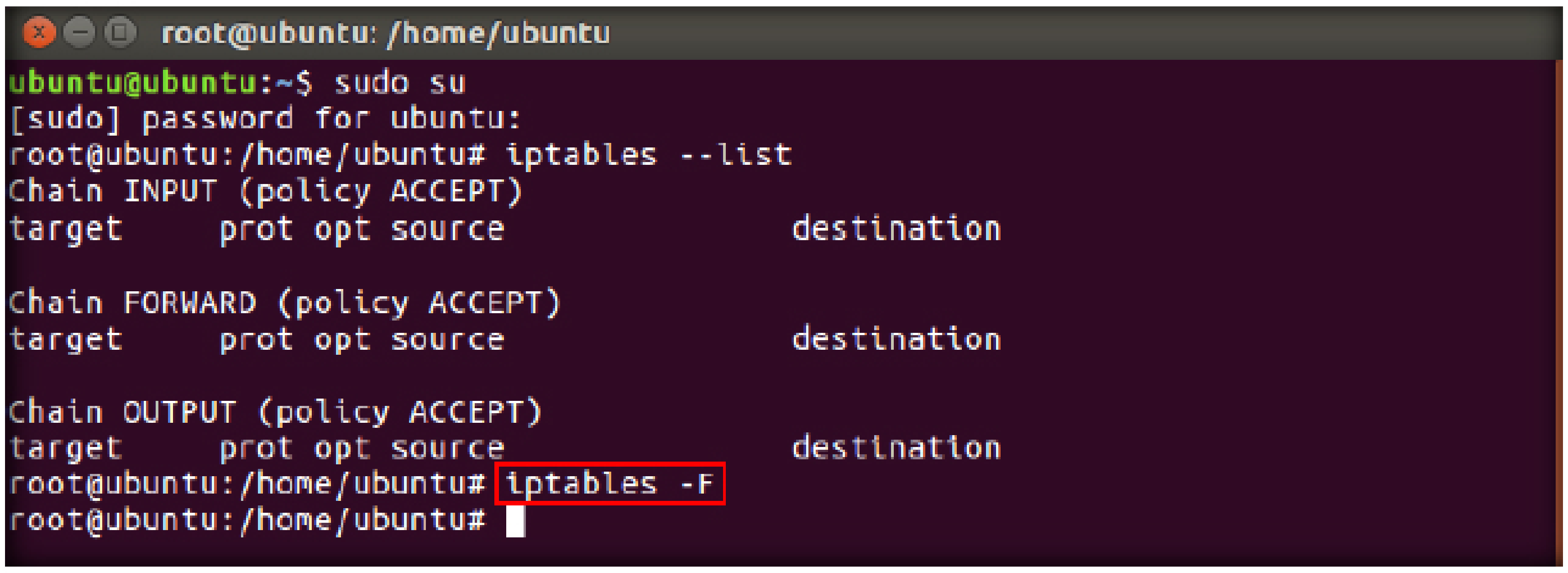
IP tables have three kind of rule chains. INPUT defines what connection can enter the device. OUTPUT defines what connection can leave the device and FORWARD defines whether the system can forward packets like a Router



```
root@ubuntu: /home/ubuntu
ubuntu@ubuntu:~$ sudo su
[sudo] password for ubuntu:
root@ubuntu:/home/ubuntu# iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@ubuntu:/home/ubuntu#
```

FIGURE 9.8: Verifying iptables Rules

16. Type iptables –F, this command will flush all the rules and temporarily disables the firewall.

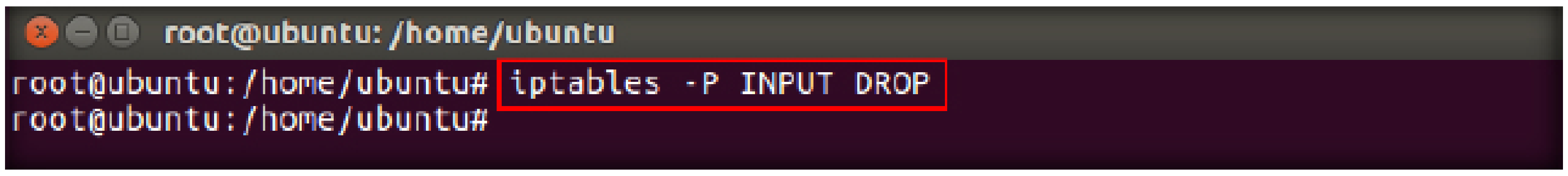


```
ubuntu@ubuntu:~$ sudo su
[sudo] password for ubuntu:
root@ubuntu:/home/ubuntu# iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@ubuntu:/home/ubuntu# iptables -F
root@ubuntu:/home/ubuntu#
```

FIGURE 9.9: Flushing the Rules

iptables requires elevated privileges to operate and must be executed by user root, otherwise it fails to function. On most Linux systems, iptables is installed as /usr/sbin/iptables and documented in its man pages, which can be opened using man iptables when installed.

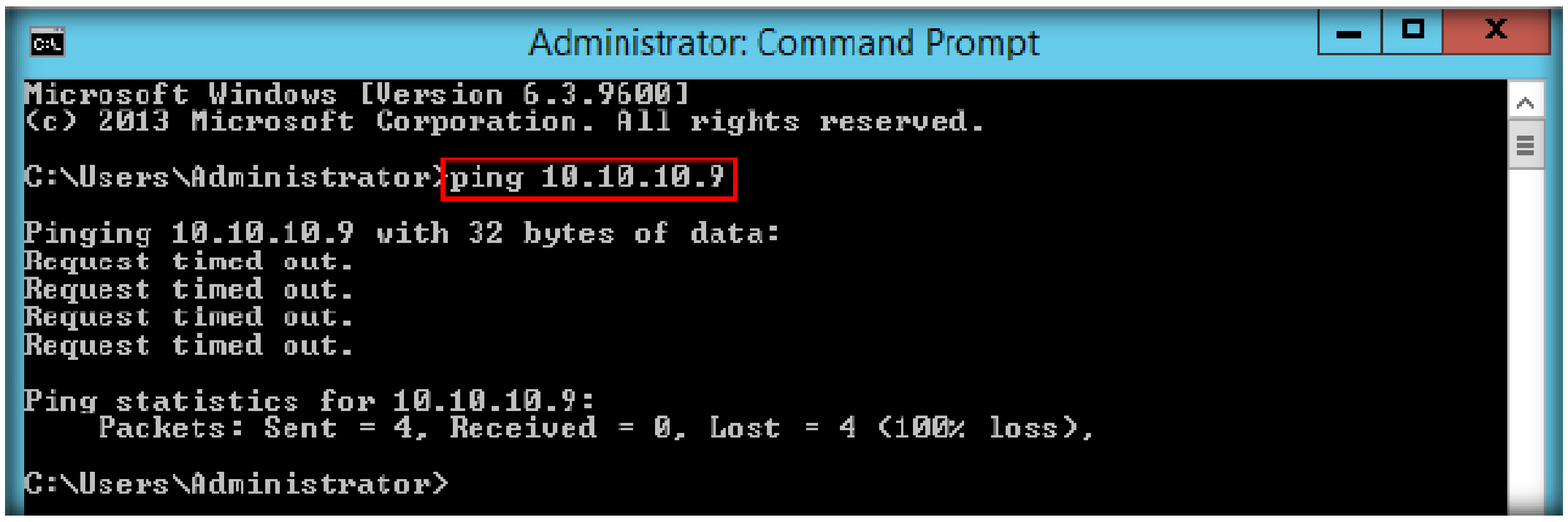
17. Type **iptables –P INPUT DROP** and press **Enter**. In this command –P switch is used to set the default policy on the specific chain. This command will make the firewall block all incoming communication for the Ubuntu machine.



```
root@ubuntu:/home/ubuntu# iptables -P INPUT DROP
root@ubuntu:/home/ubuntu#
```

FIGURE 9.10: Dropping all Input Packets

18. Switch back to Windows Server 2012 and open a command prompt and type **ping 10.10.10.9** and press **Enter**. As you have blocked the incoming communication for the Ubuntu machine, you will not get any response; as shown in the screenshot below.

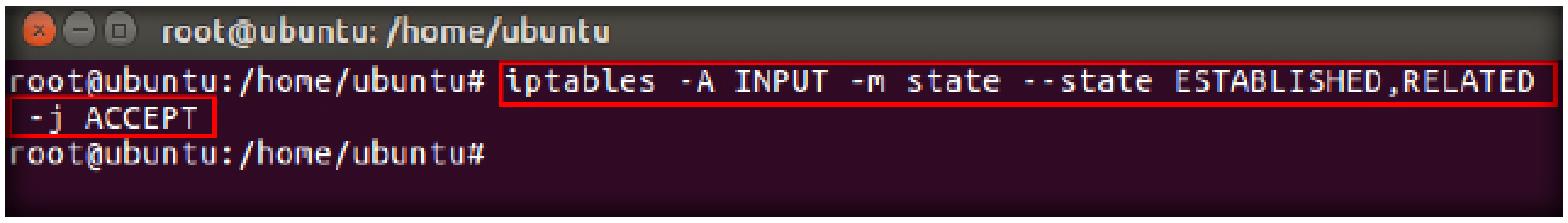


```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 10.10.10.9

Pinging 10.10.10.9 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.10.9:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Administrator>
```

FIGURE 9.11: Verifying Changed Rules

It may also be found in /sbin/iptables, but since iptables is more like a service rather than an "essential binary", the preferred location remains /usr/sbin.

19. Switch back to the Ubuntu machine and type **iptables –A INPUT –m state --state ESTABLISHED,RELATED –j ACCEPT** and press **Enter**. This command makes your device accept only those incoming connections which are initiated by you.

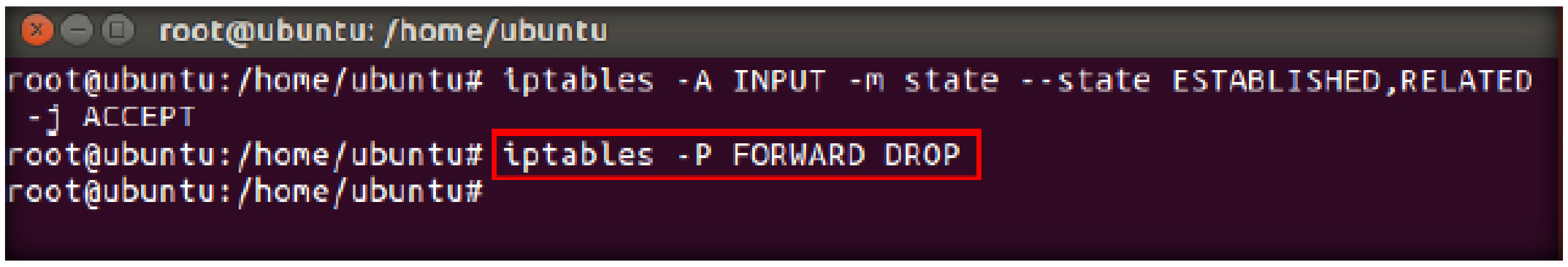


```
root@ubuntu:/home/ubuntu# iptables -A INPUT -m state --state ESTABLISHED,RELATED
 -j ACCEPT
root@ubuntu:/home/ubuntu#
```

FIGURE 9.12: Dropping Packets Not Initiated by User

20. To block forwarding, type **iptables -P FORWARD DROP** and press Enter

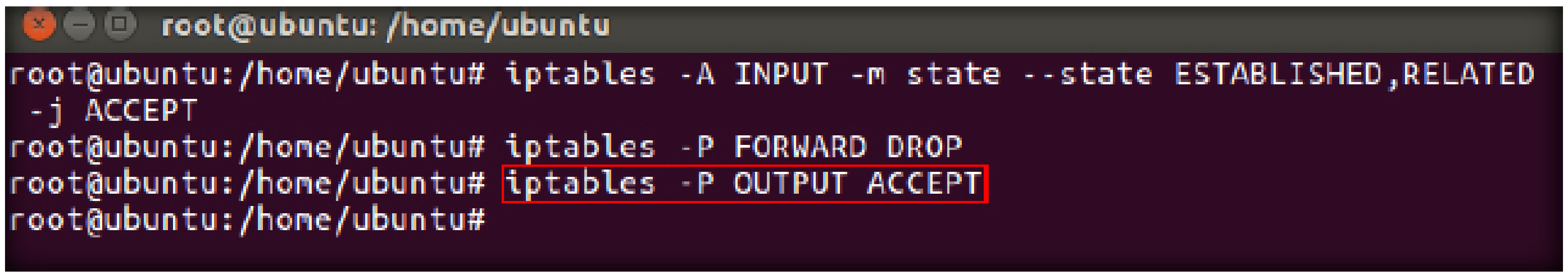
🗁 Different kernel modules and programs are currently used for different protocols; iptables applies to IPv4, ip6tables to IPv6, arptables to ARP, and ebtables to Ethernet frames.



```
root@ubuntu:/home/ubuntu# iptables -A INPUT -m state --state ESTABLISHED,RELATED
 -j ACCEPT
root@ubuntu:/home/ubuntu# iptables -P FORWARD DROP
root@ubuntu:/home/ubuntu#
```

FIGURE 9.13: Disabling Forwarding of Packets

21. To allow accepting of packets for outgoing connections, type **iptables –P OUTPUT ACCEPT** and press Enter



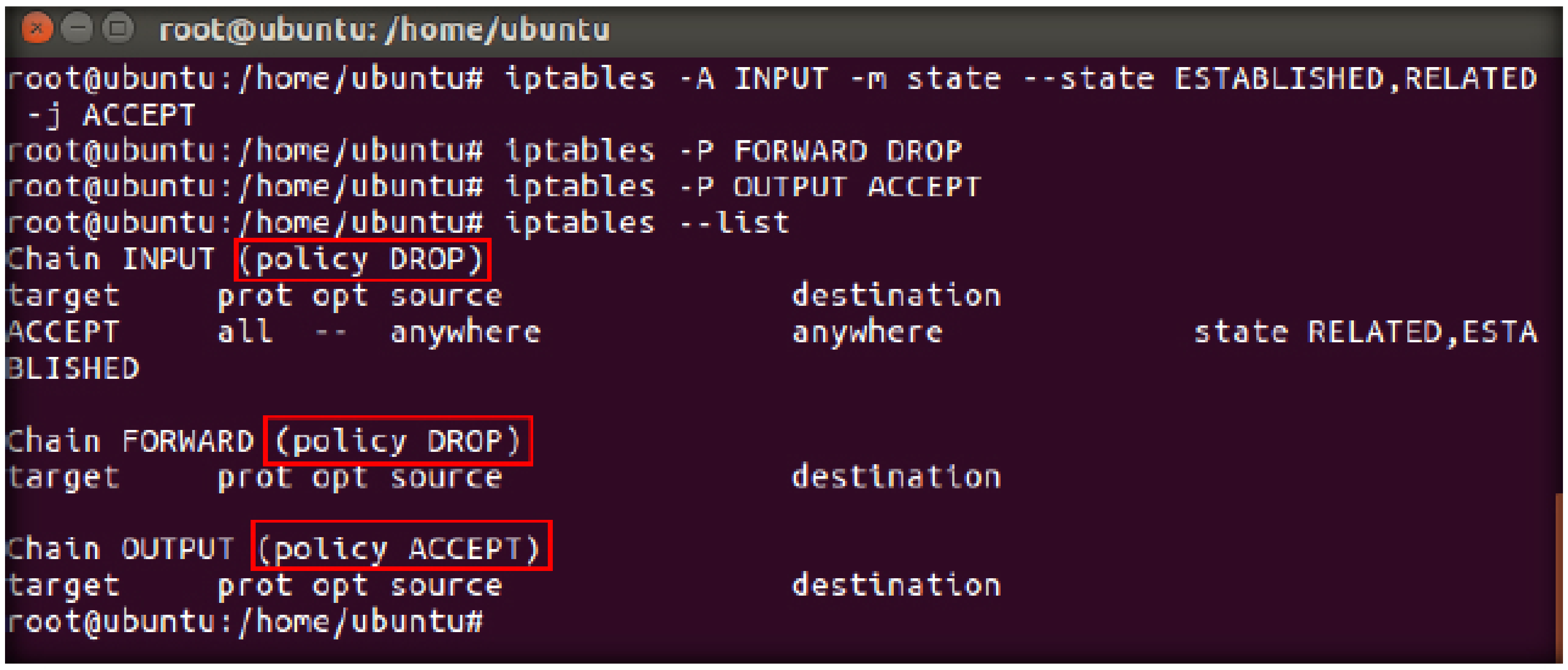
```
root@ubuntu:/home/ubuntu# iptables -A INPUT -m state --state ESTABLISHED,RELATED
 -j ACCEPT
root@ubuntu:/home/ubuntu# iptables -P FORWARD DROP
root@ubuntu:/home/ubuntu# iptables -P OUTPUT ACCEPT
root@ubuntu:/home/ubuntu#
```

FIGURE 9.14: Disabling Forwarding

22. We have configured all three chains. Type **iptables --list** and press Enter, to recheck the firewall configuration we have set for the Ubuntu machine.

23. At the beginning of this lab we saw that all the firewall rules were listed as accept at step 15. Now we have configured the firewall with the new set of rules as shown in the screenshot.

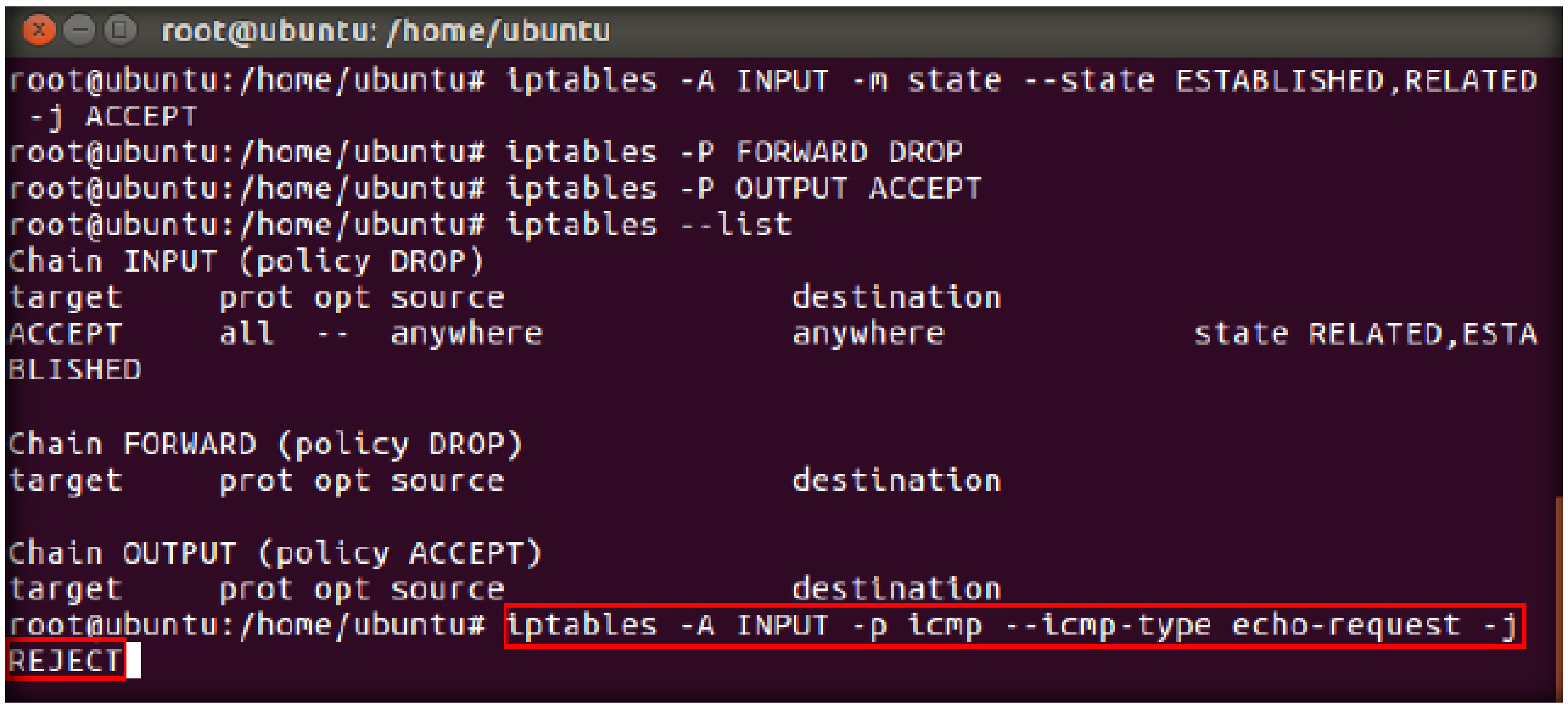
🗁 The term iptables is also commonly used to inclusively refer to the kernel-level components. x_tables is the name of the kernel module carrying the shared code portion used by all four modules that also provides the API used for extensions; subsequently, Xtables is more or less used to refer to the entire firewall (v4, v6, arp, and eb) architecture.



```
root@ubuntu:/home/ubuntu# iptables -A INPUT -m state --state ESTABLISHED,RELATED
 -j ACCEPT
root@ubuntu:/home/ubuntu# iptables -P FORWARD DROP
root@ubuntu:/home/ubuntu# iptables -P OUTPUT ACCEPT
root@ubuntu:/home/ubuntu# iptables --list
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTA
BLISHED

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@ubuntu:/home/ubuntu#
```

FIGURE 9.15: iptables Checking the Configuration

24. To block a Ping request, type **iptables –A INPUT –p icmp –icmp-type echo-request –j REJECT** and press Enter.

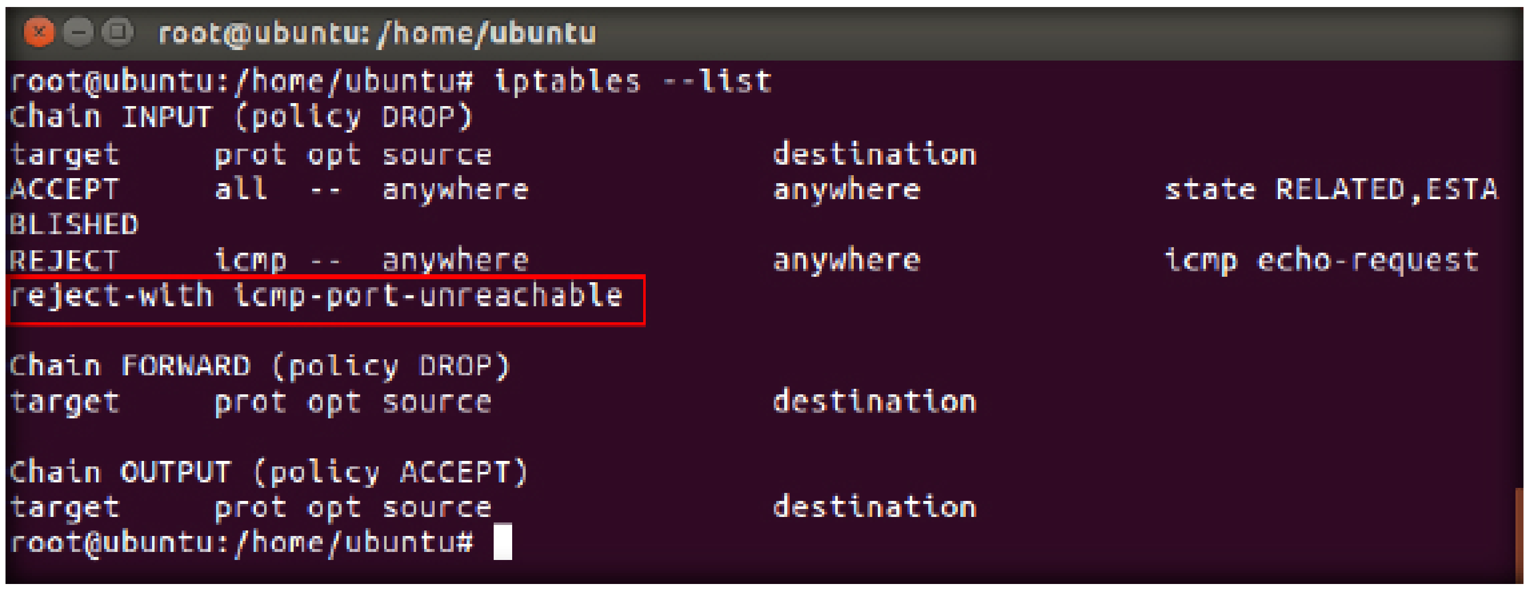


```
root@ubuntu:/home/ubuntu# iptables -A INPUT -m state --state ESTABLISHED,RELATED
 -j ACCEPT
root@ubuntu:/home/ubuntu# iptables -P FORWARD DROP
root@ubuntu:/home/ubuntu# iptables -P OUTPUT ACCEPT
root@ubuntu:/home/ubuntu# iptables --list
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTA
BLISHED

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@ubuntu:/home/ubuntu# iptables -A INPUT -p icmp --icmp-type echo-request -j
REJECT
```

FIGURE 9.16: Ping Blocking

Xtables allows the system administrator to define tables containing chains of rules for the treatment of packets. Each table is associated with a different kind of packet processing. Packets are processed by sequentially traversing the rules in chains. A rule in a chain can cause it to go or jump to another chain, and this can be repeated to whatever level of nesting is desired. (A jump is like a “call”, i.e. the point that was jumped from is remembered.) Every network packet arriving at or leaving from the computer traverses at least one chain.

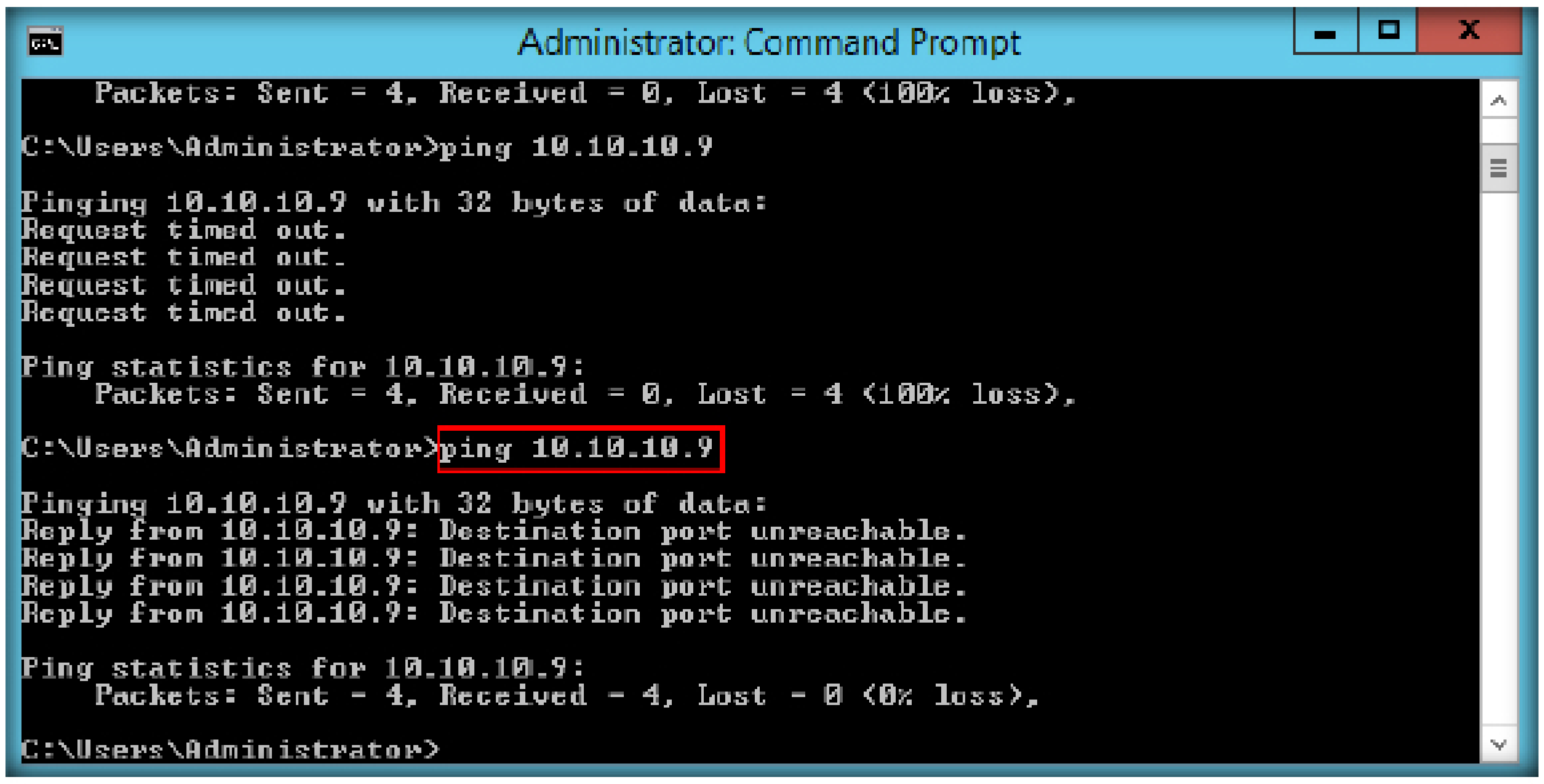
25. Type **iptables --list** and press Enter, to verify the new rules are created.



```
root@ubuntu:/home/ubuntu# iptables --list
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTA
BLISHED
REJECT     icmp --  anywhere             anywhere             icmp echo-request
reject-with icmp-port-unreachable

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@ubuntu:/home/ubuntu#
```

FIGURE 9.17: Blocking Ping Requests

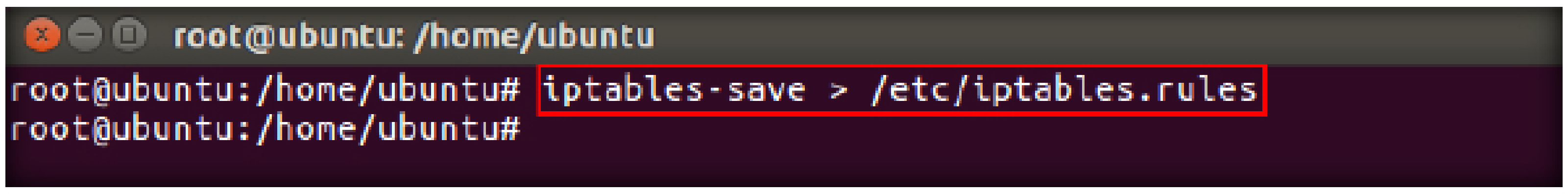
26. Switch to the Windows Server 2012 machine and open the command prompt window and type **ping 10.10.10.9** and press **Enter**. Now, you should see the message as **Destination port Unreachable** as shown in the screenshot. This is because we have blocked ping requests in the previous step.



```
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Administrator>ping 10.10.10.9

Pinging 10.10.10.9 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.10.9:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Administrator>ping 10.10.10.9

Pinging 10.10.10.9 with 32 bytes of data:
Reply from 10.10.10.9: Destination port unreachable.
Reply from 10.10.10.9: Destination port unreachable.
Reply from 10.10.10.9: Destination port unreachable.
Reply from 10.10.10.9: Destination port unreachable.

Ping statistics for 10.10.10.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\Administrator>
```

FIGURE 9.18: Verifying Ping Rule

27. Switch back to the Ubuntu machine, to restore the iptable configuration at boot time, type **iptables-save > /etc/iptables.rules** and press Enter

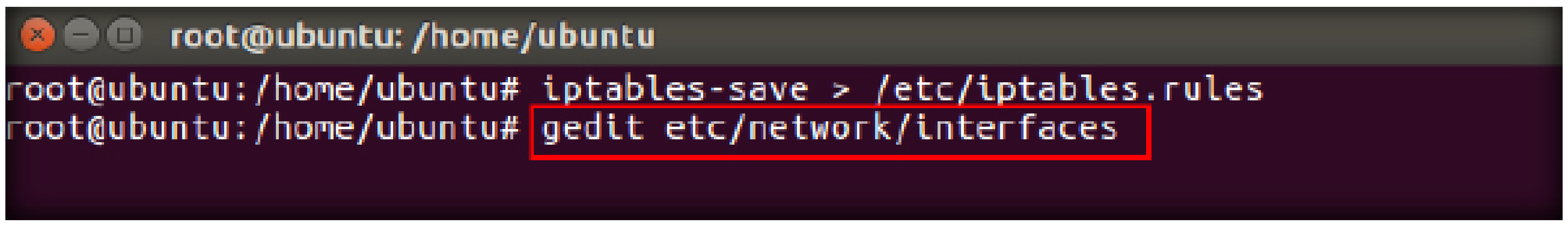


```
root@ubuntu:/home/ubuntu# iptables-save > /etc/iptables.rules
root@ubuntu:/home/ubuntu#
```

FIGURE 9.19: Restoring the Settings at Boot Time

iptables -P INPUT ACCEPT If connecting remotely we must first temporarily set the default policy on the INPUT chain to ACCEPT otherwise once we flush the current rules we will be locked out of our server.

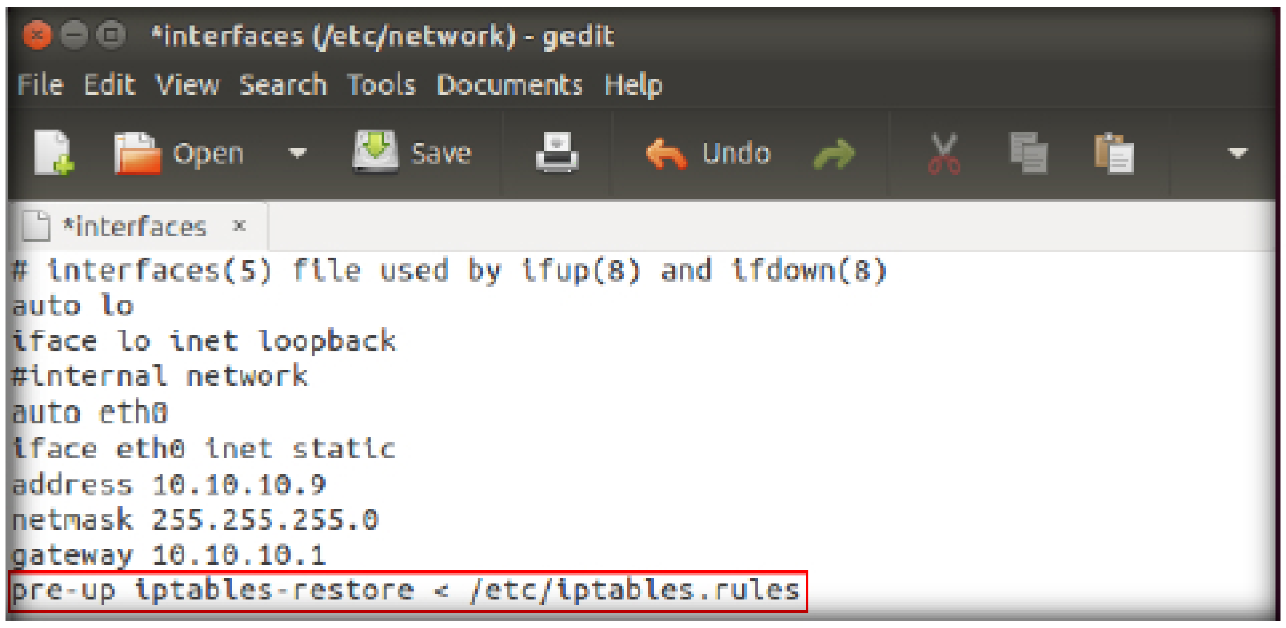
28. To save the settings permanently, type **gedit etc/network/interfaces** type and press Enter, to access the interfaces file to edit.



```
root@ubuntu:/home/ubuntu# iptables-save > /etc/iptables.rules
root@ubuntu:/home/ubuntu# gedit etc/network/interfaces
```

FIGURE 9.20: Accessing Interfaces File

29. The Interfaces file opens in editor mode as shown in the screenshot. Add the following line at the bottom **pre-up iptables-restore < /etc/iptables.rules**.



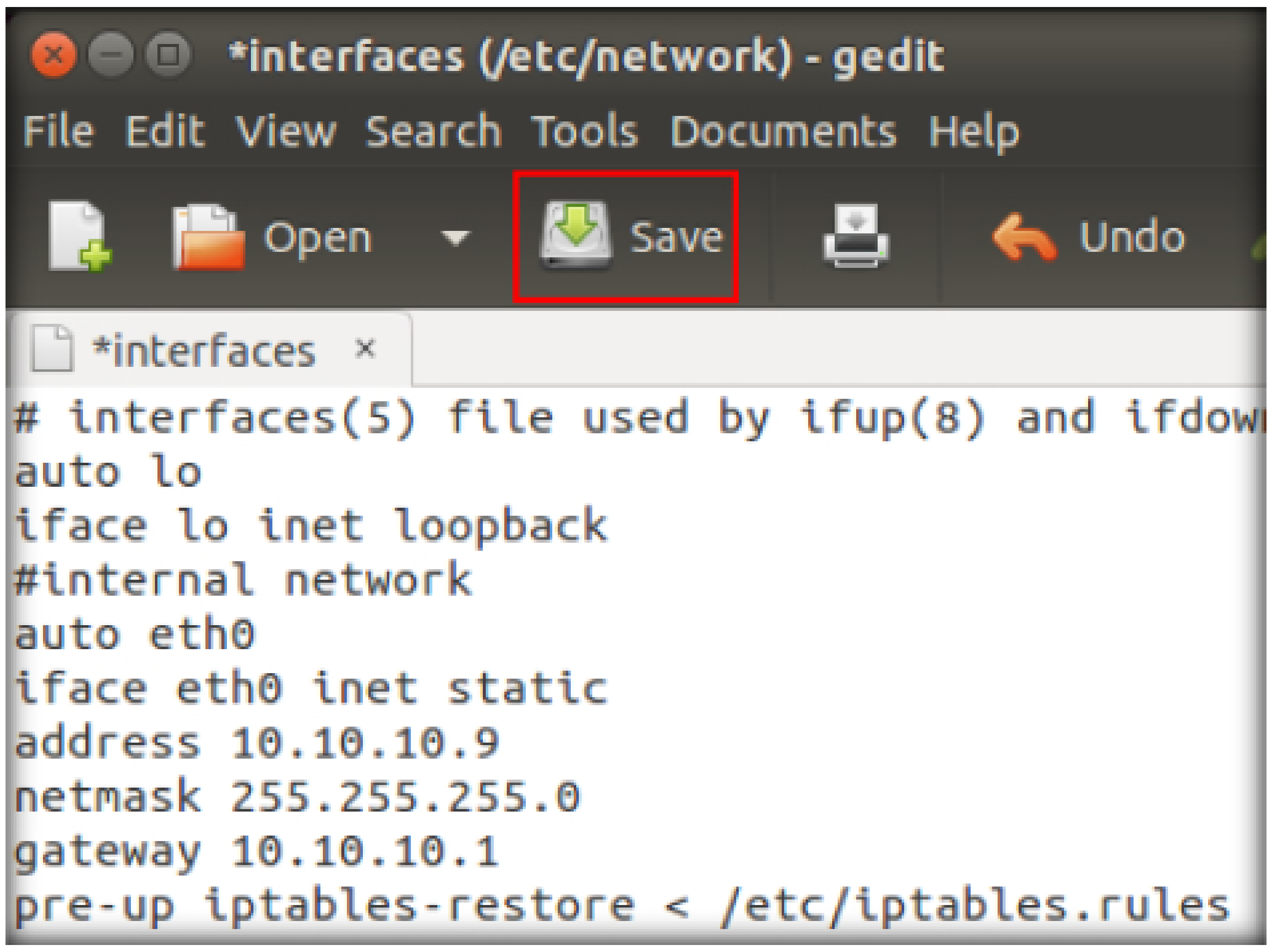
*interfaces (/etc/network) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
*interfaces

```
# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback
#internal network
auto eth0
iface eth0 inet static
address 10.10.10.9
netmask 255.255.255.0
gateway 10.10.10.1
pre-up iptables-restore < /etc/iptables.rules
```

FIGURE 9.21: Adding a Rule in Interfaces File

30. Click **Save** and close the interfaces window.

iptables -F We used the -F switch to flush all existing rules so we start with a clean state from which to add new rules.



*interfaces (/etc/network) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
*interfaces

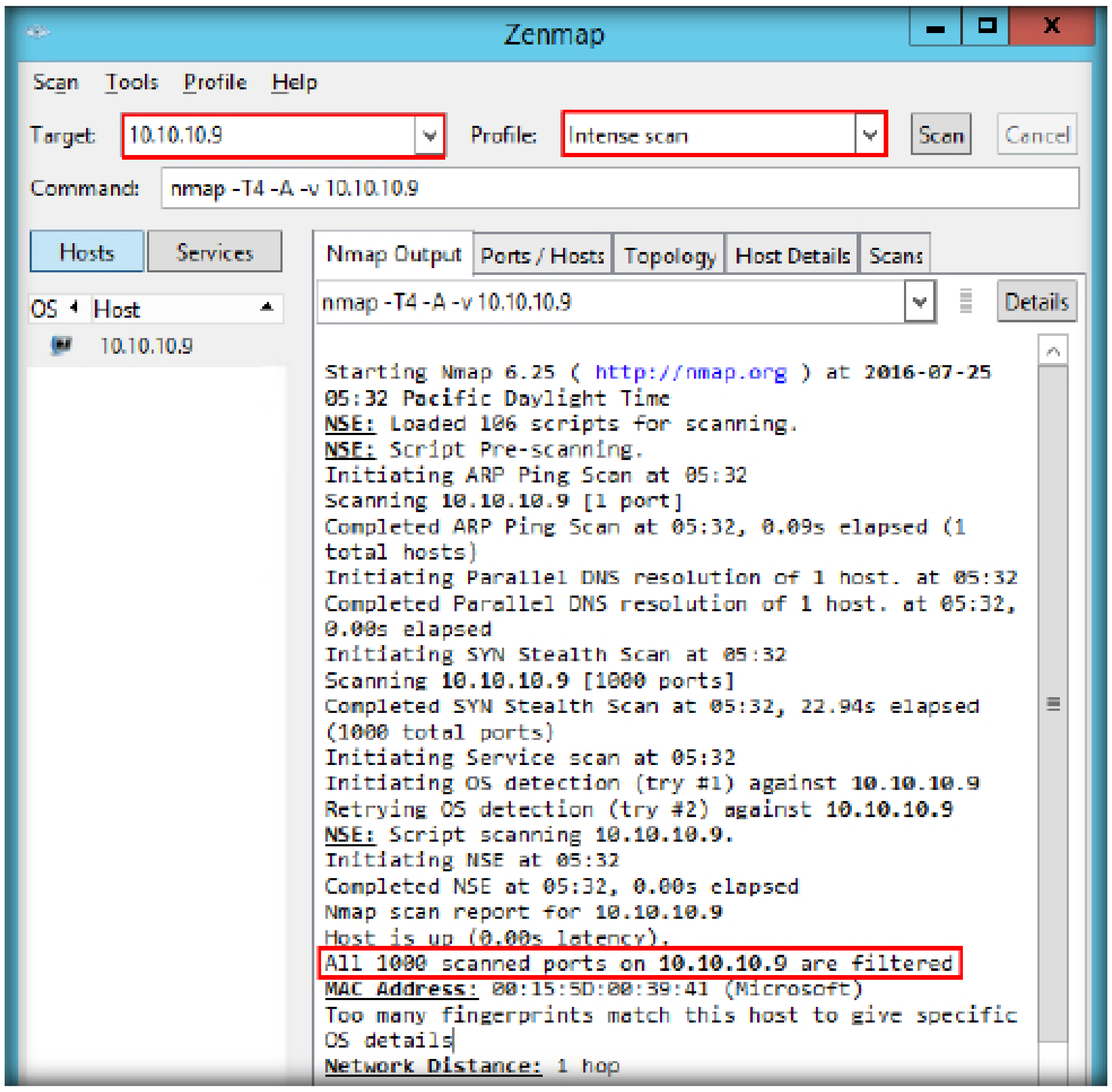
```
# interfaces(5) file used by ifup(8) and ifdow
auto lo
iface lo inet loopback
#internal network
auto eth0
iface eth0 inet static
address 10.10.10.9
netmask 255.255.255.0
gateway 10.10.10.1
pre-up iptables-restore < /etc/iptables.rules
```

FIGURE 9.22: Saving the interfaces

31. Switch back to **Windows Server 2012** and run an **intense scan** on **10.10.10.9** from Zenmap.

32. As you can see all the ports are filtered which indicates that they are present behind a firewall. If a port is closed and you send a SYN packet, it replies with a RST packet, but filtered ports never reply to SYN packets from unknown hosts. They only initiate a connection from a user.

iptables -A INPUT -i lo -j ACCEPT Now it's time to start adding some rules. We use the -A switch to append (or add) a rule to a specific chain, the INPUT chain in this instance. Then we use the -i switch (for interface) to specify packets matching or destined for the lo (localhost, 127.0.0.1) interface and finally -j (jump) to the target action for packets matching the rule - in this case ACCEPT. So this rule will allow all incoming packets destined for the localhost interface to be accepted. This is generally required as many software applications expect to be able to communicate with the localhost adaptor.



Target: 10.10.10.9

Profile: Intense scan

Command: nmap -T4 -A -v 10.10.10.9

10.10.10.9

nmap -T4 -A -v 10.10.10.9

```
Starting Nmap 6.25 ( http://nmap.org ) at 2016-07-25
05:32 Pacific Daylight Time
NSE: Loaded 106 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 05:32
Scanning 10.10.10.9 [1 port]
Completed ARP Ping Scan at 05:32, 0.09s elapsed (1
total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:32
Completed Parallel DNS resolution of 1 host. at 05:32,
0.00s elapsed
Initiating SYN Stealth Scan at 05:32
Scanning 10.10.10.9 [1000 ports]
Completed SYN Stealth Scan at 05:32, 22.94s elapsed
(1000 total ports)
Initiating Service scan at 05:32
Initiating OS detection (try #1) against 10.10.10.9
Retrying OS detection (try #2) against 10.10.10.9
NSE: Script scanning 10.10.10.9.
Initiating NSE at 05:32
Completed NSE at 05:32, 0.00s elapsed
Nmap scan report for 10.10.10.9
Host is up (0.00s latency).
All 1000 scanned ports on 10.10.10.9 are filtered
MAC Address: 00:15:5D:00:39:41 (Microsoft)
Too many fingerprints match this host to give specific
OS details
Network Distance: 1 hop
```

FIGURE 9.23: All Ports Filtered after New iptables Rules

# Lab Analysis

Analyze and document the results of the lab exercise. Give your opinion on your target's security posture and exposure through free public information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

| Internet Connection Required | |
|---|---|
| ☐ Yes | ☑ No |
| **Platform Supported** | |
| ☑ Classroom | ☑ iLabs |

Lab

10

# Managing Network Hosts Using an OSSEC Agent in OSSIM

*OSSEC is an open-source host-based intrusion detection system (HIDS).*

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

## Lab Scenario

Network administrators are required to monitor servers in their organization's network. For this, they need a Host-based Intrusion Detection System (HIDS) to perform log analysis, integrity checking, Windows registry monitoring, rootkit detection, time-based alerting, and active response. As an administrator, you should know how to deploy OSSEC agents in OSSIM.

## Lab Objectives

This lab will demonstrate how to deploy an OSSEC Agent in OSSIM.

## Lab Environment

To carry out the lab, you need:

- A virtual machine running Windows Server 2012
- OSSIM virtual machine
- A virtual machine running Windows Server 2008
- A virtual machine running Windows 10
- A Web browser with an Internet connection
- **Administrative** privileges to run the tools

## Lab Duration

Time: 10 Minutes

## Overview of OSSIM

OSSIM (Open Source Security Information Management) is an open source security information and event management system. It has a selection of tools integrated into it designed to aid network administrators with computer security, intrusion detection, and prevention.

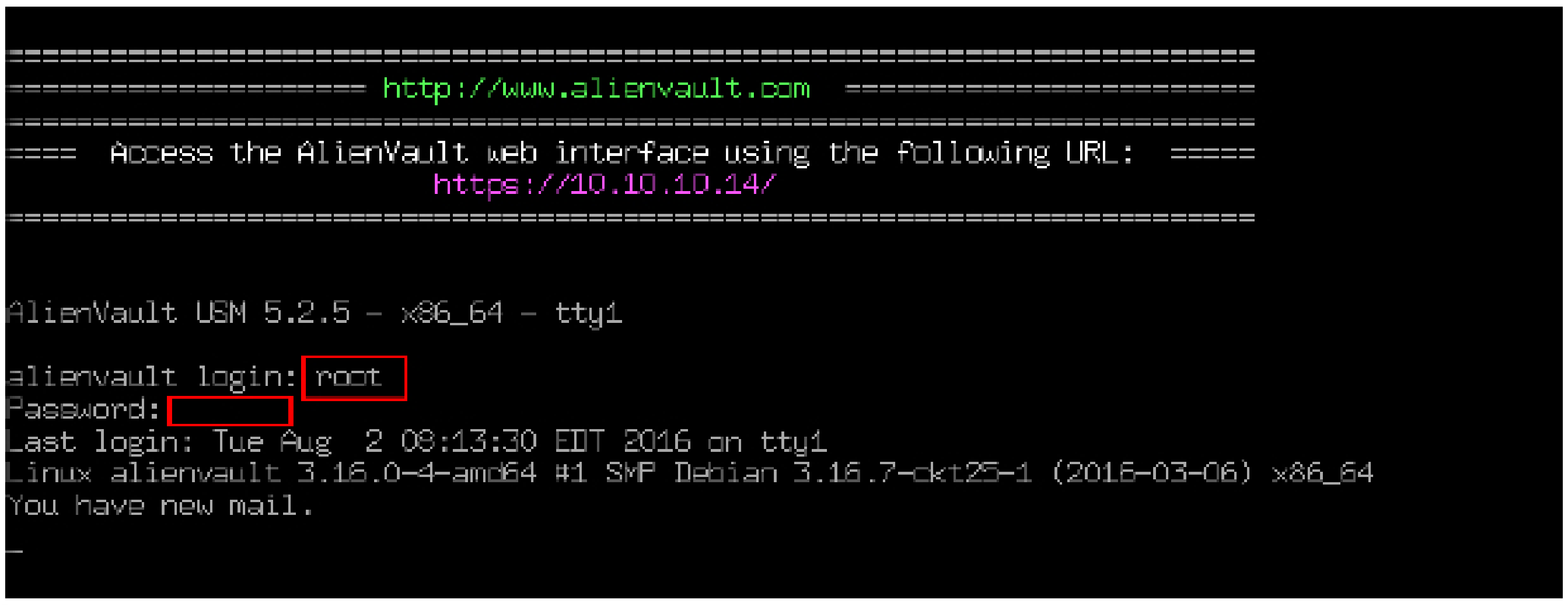
## Lab Tasks

**TASK 1**

**Login to OSSIM**

1. Before starting this lab, make sure the Windows 10 and Windows Server 2008 machines are turned on.
2. Power on the OSSIM virtual machine from the VMware workstation, and wait until the log in screen appears.
3. In the log in screen type **root** in the alienvault login field and press **Enter**. In the password field type **toor** as the password and press **Enter**.

   Note: Password is not visible.



```
=========================================================================
==================== http://www.alienvault.com  =========================
=========================================================================
====  Access the AlienVault web interface using the following URL:  =====
                        https://10.10.10.14/
=========================================================================


AlienVault USM 5.2.5 - x86_64 - tty1

alienvault login: root
Password:
Last login: Tue Aug  2 08:13:30 EDT 2016 on tty1
Linux alienvault 3.16.0-4-amd64 #1 SMP Debian 3.16.7-ckt25-1 (2016-03-06) x86_64
You have new mail.
_
```

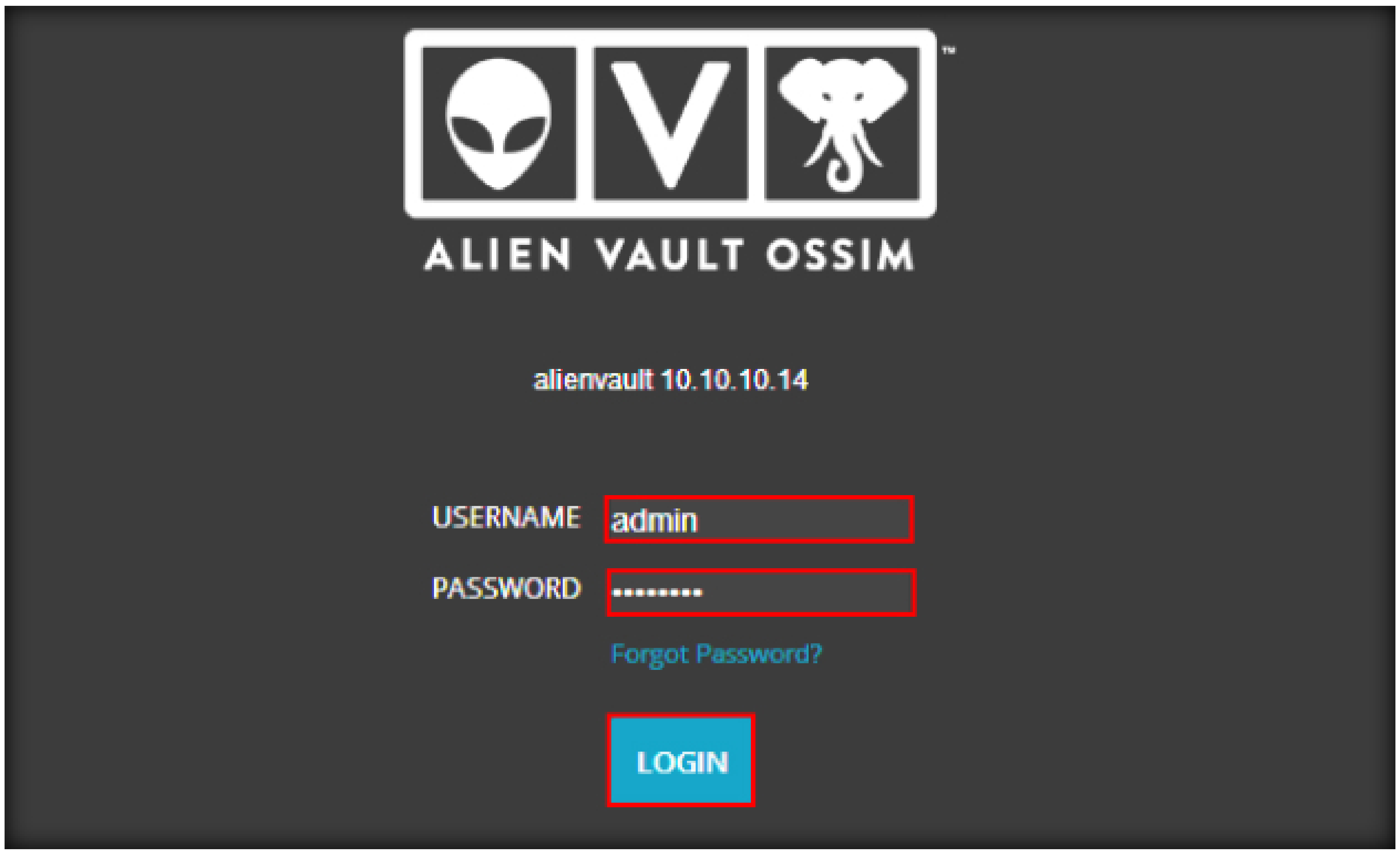
FIGURE 10.1: OSSIM Login Window

4. Launch the Windows Server 2012 machine and log in. Now close the Server Manager window and open a web browser. In this lab we are using a Chrome browser.

   Note: If you are using a different browser the screenshots may differ in your lab environment.

5. Type https://10.10.10.14 and press Enter in the address bar of the browser.

6. The OSSIM Login page appears. Enter **admin** in USERNAME field, **qwerty@123** in PASSWORD field and click LOGIN.



USERNAME: admin

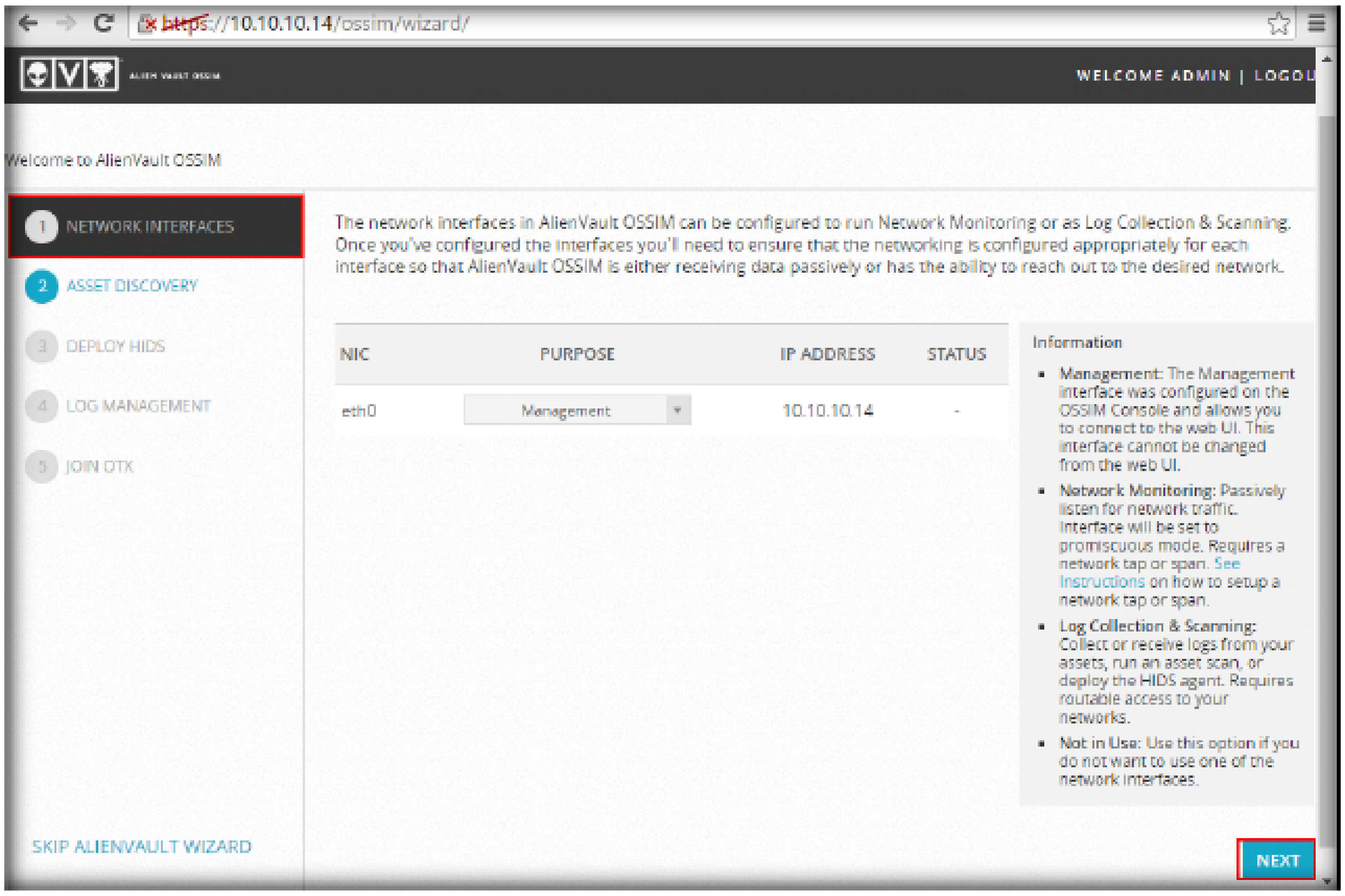
PASSWORD: ••••••••

FIGURE 10.2: Logging in to alien vault

**TASK 2**

**Deploy OSSEC Agent**

7. The **NETWORK INTERFACES** page appears. Click **Next**.



Welcome to AlienVault OSSIM

The network interfaces in AlienVault OSSIM can be configured to run Network Monitoring or as Log Collection & Scanning. Once you've configured the interfaces you'll need to ensure that the networking is configured appropriately for each interface so that AlienVault OSSIM is either receiving data passively or has the ability to reach out to the desired network.

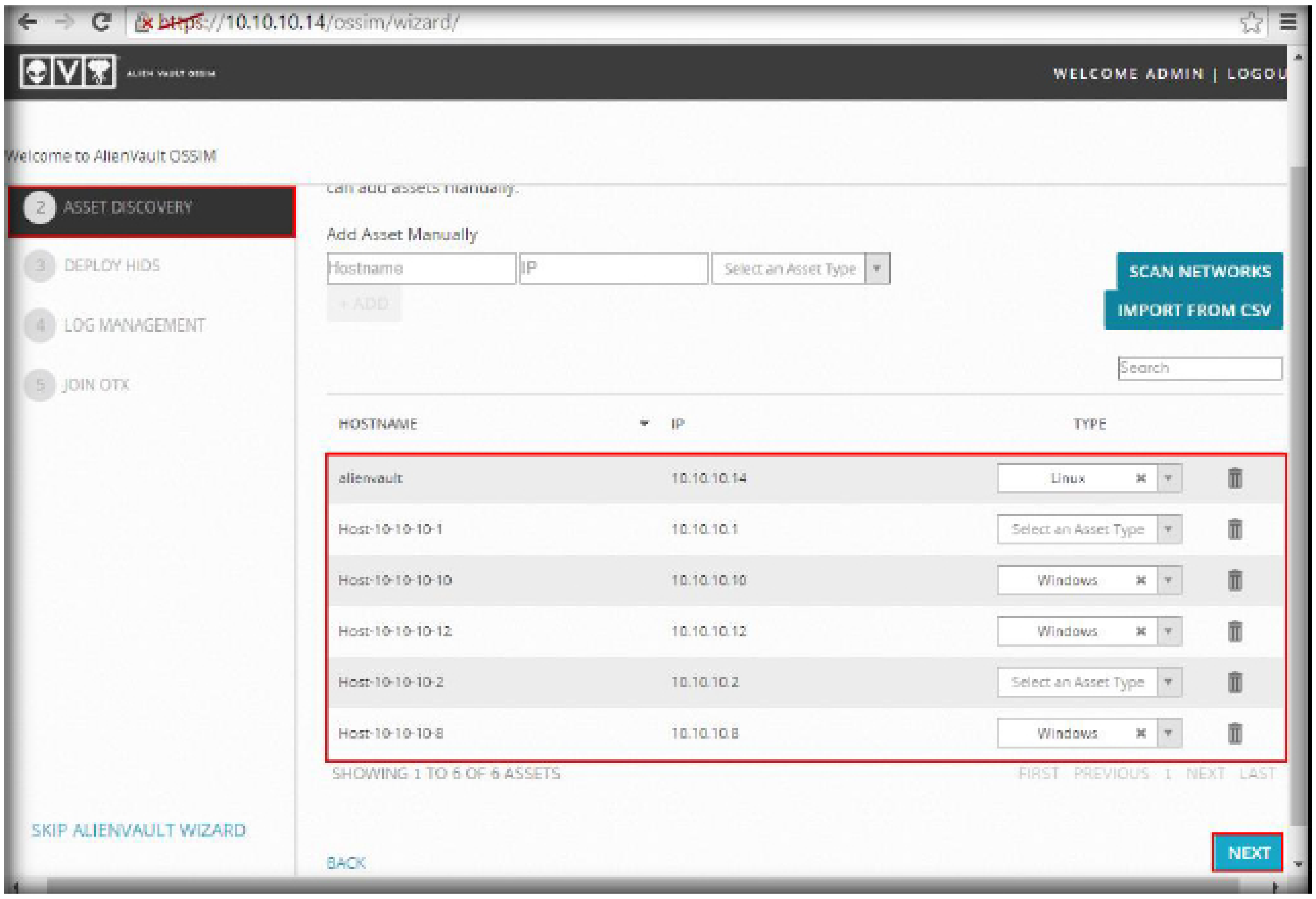
| NIC | PURPOSE | IP ADDRESS | STATUS |
|---|---|---|---|
| eth0 | Management | 10.10.10.14 | - |

Information

- Management: The Management interface was configured on the OSSIM Console and allows you to connect to the web UI. This interface cannot be changed from the web UI.
- Network Monitoring: Passively listen for network traffic. Interface will be set to promiscuous mode. Requires a network tap or span. See Instructions on how to setup a network tap or span.
- Log Collection & Scanning: Collect or receive logs from your assets, run an asset scan, or deploy the HIDS agent. Requires routable access to your networks.
- Not in Use: Use this option if you do not want to use one of the network interfaces.

FIGURE 10.3: Network interfaces

8. The **ASSET DISCOVERY** page appears. You can see the detected live hosts in the network, scroll down and click **Next**.

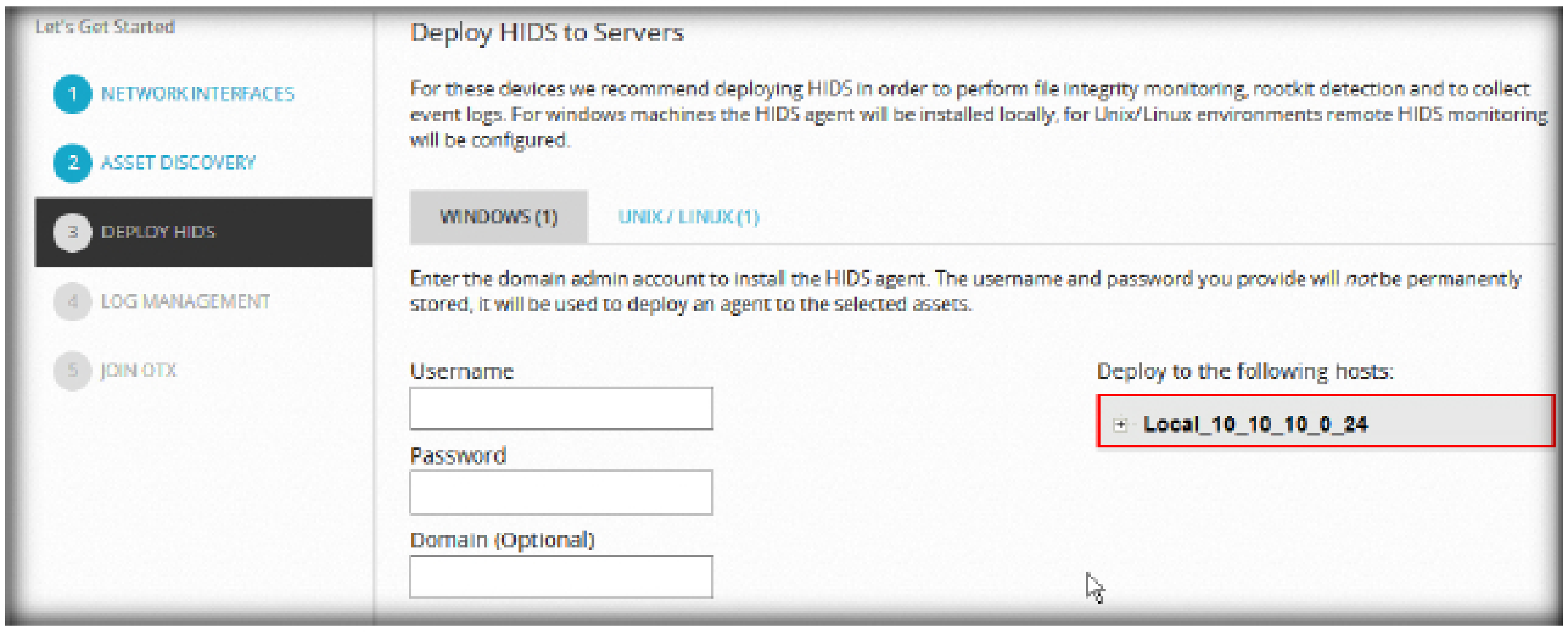


| HOSTNAME | IP | TYPE |
|---|---|---|
| alienvault | 10.10.10.14 | Linux |
| Host-10-10-10-1 | 10.10.10.1 | Select an Asset Type |
| Host-10-10-10-10 | 10.10.10.10 | Windows |
| Host-10-10-10-12 | 10.10.10.12 | Windows |
| Host-10-10-10-2 | 10.10.10.2 | Select an Asset Type |
| Host-10-10-10-8 | 10.10.10.8 | Windows |

SHOWING 1 TO 6 OF 6 ASSETS

FIGURE 10.4: Live assets discovered

9. The **Deploy HIDS to Servers** window appears. Expand **Local_10_10_10_0_24**.



Deploy HIDS to Servers

For these devices we recommend deploying HIDS in order to perform file integrity monitoring, rootkit detection and to collect event logs. For windows machines the HIDS agent will be installed locally, for Unix/Linux environments remote HIDS monitoring will be configured.

Enter the domain admin account to install the HIDS agent. The username and password you provide will *not* be permanently stored, it will be used to deploy an agent to the selected assets.

Username

Password

Domain (Optional)

Deploy to the following hosts:

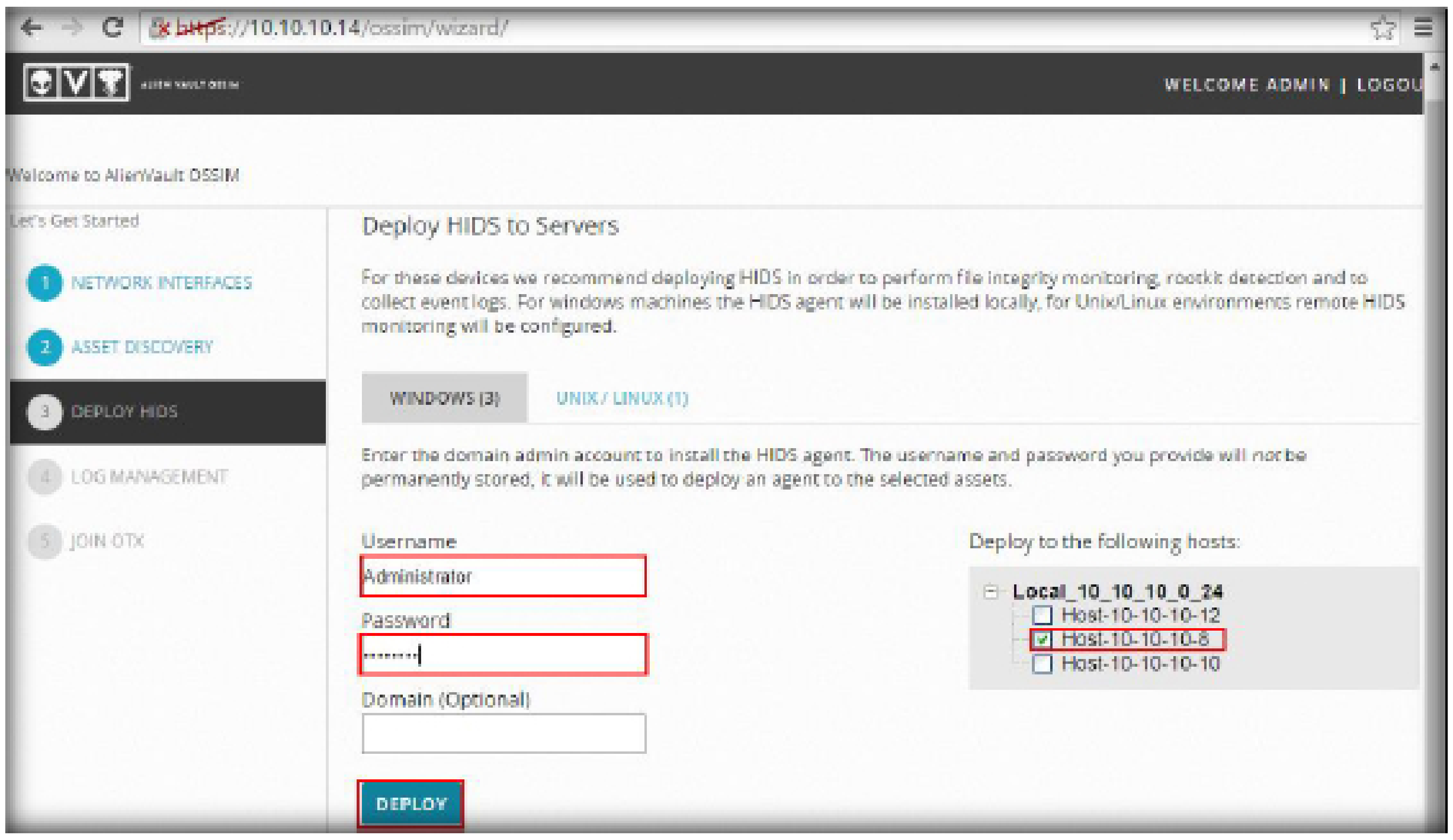
⊞ Local_10_10_10_0_24

FIGURE 10.5: Deploying HIDS

10. Select the **Host-10-10-10-8** checkbox. Enter the login credentials for the Windows Server 2008 and click **Deploy**.

    a. Username: **Administrator**

    b. Password: **Pa$$w0rd**



Welcome to AlienVault OSSIM

Deploy HIDS to Servers

For these devices we recommend deploying HIDS in order to perform file integrity monitoring, rootkit detection and to collect event logs. For windows machines the HIDS agent will be installed locally, for Unix/Linux environments remote HIDS monitoring will be configured.

Enter the domain admin account to install the HIDS agent. The username and password you provide will *not* be permanently stored, it will be used to deploy an agent to the selected assets.

Username: Administrator

Password: ••••••••

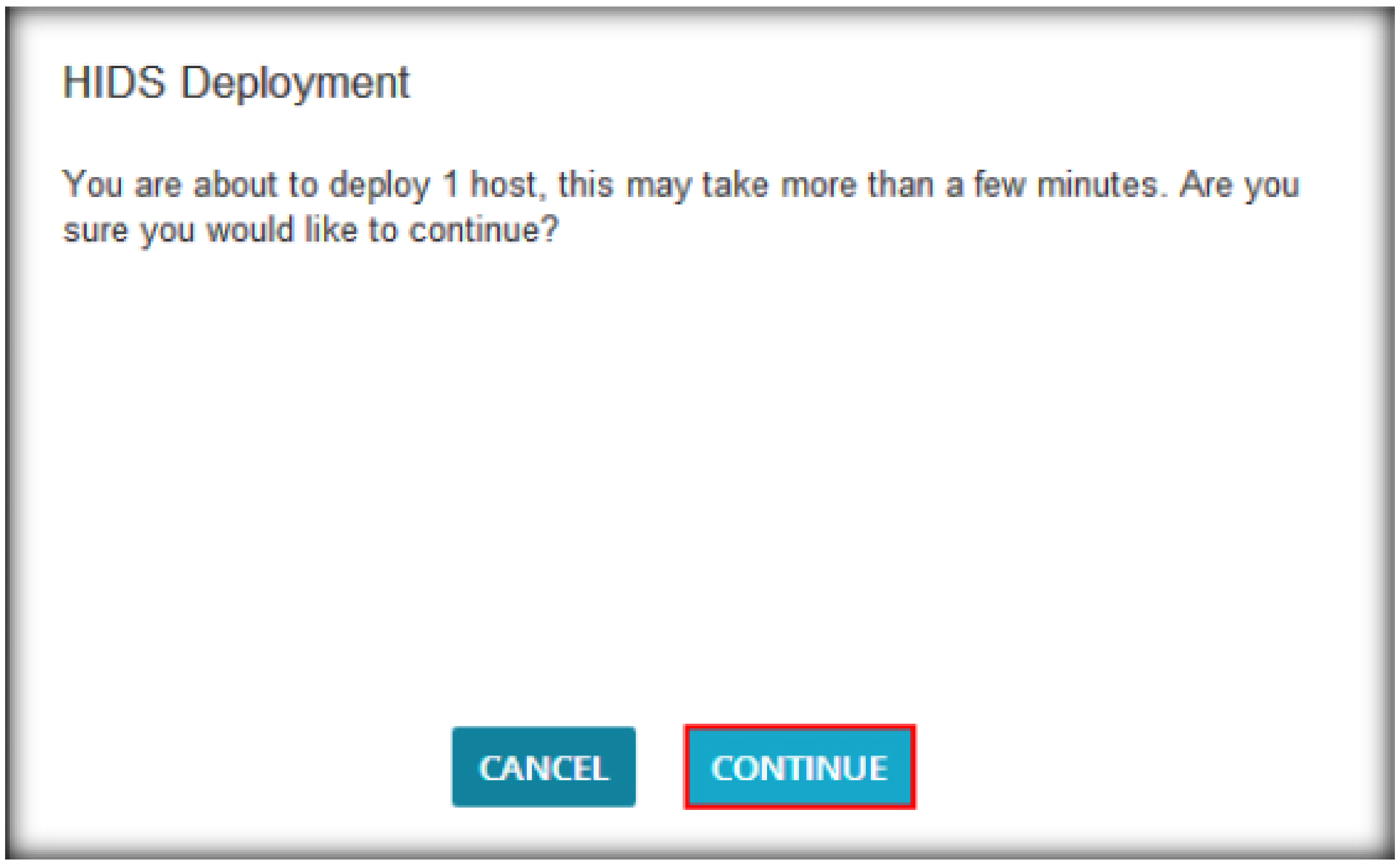
Domain (Optional):

Deploy to the following hosts:

- Local_10_10_10_0_24
  - □ Host-10-10-10-12
  - ☑ Host-10-10-10-8
  - □ Host-10-10-10-10

FIGURE 10.6: Entering credentials

11. The **HIDS Deployment** pop-up appears. Click **Continue**.

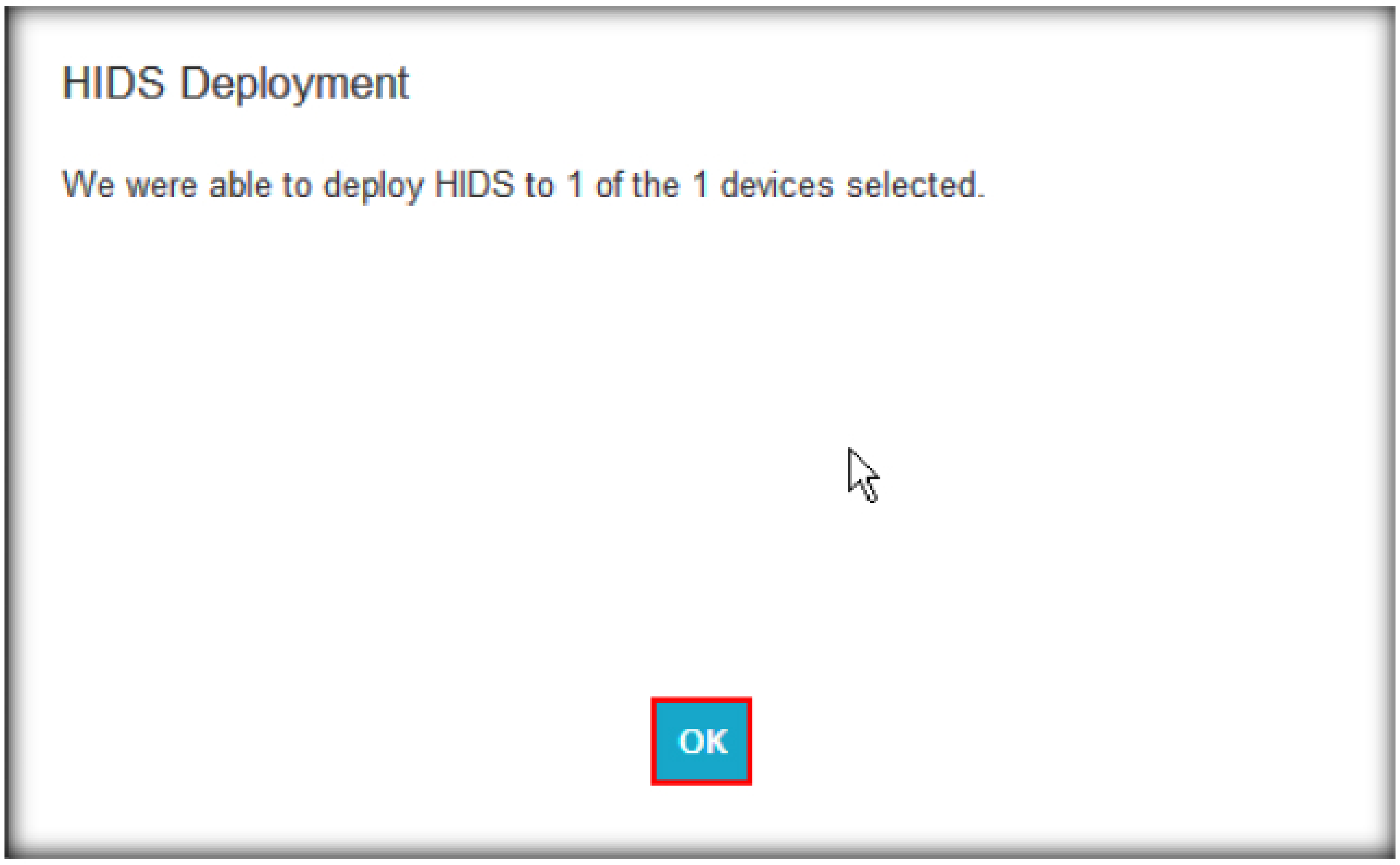


HIDS Deployment

You are about to deploy 1 host, this may take more than a few minutes. Are you sure you would like to continue?

FIGURE 10.7: Confirming the deployment

12. You will get the deployment successful message. Click **OK**.

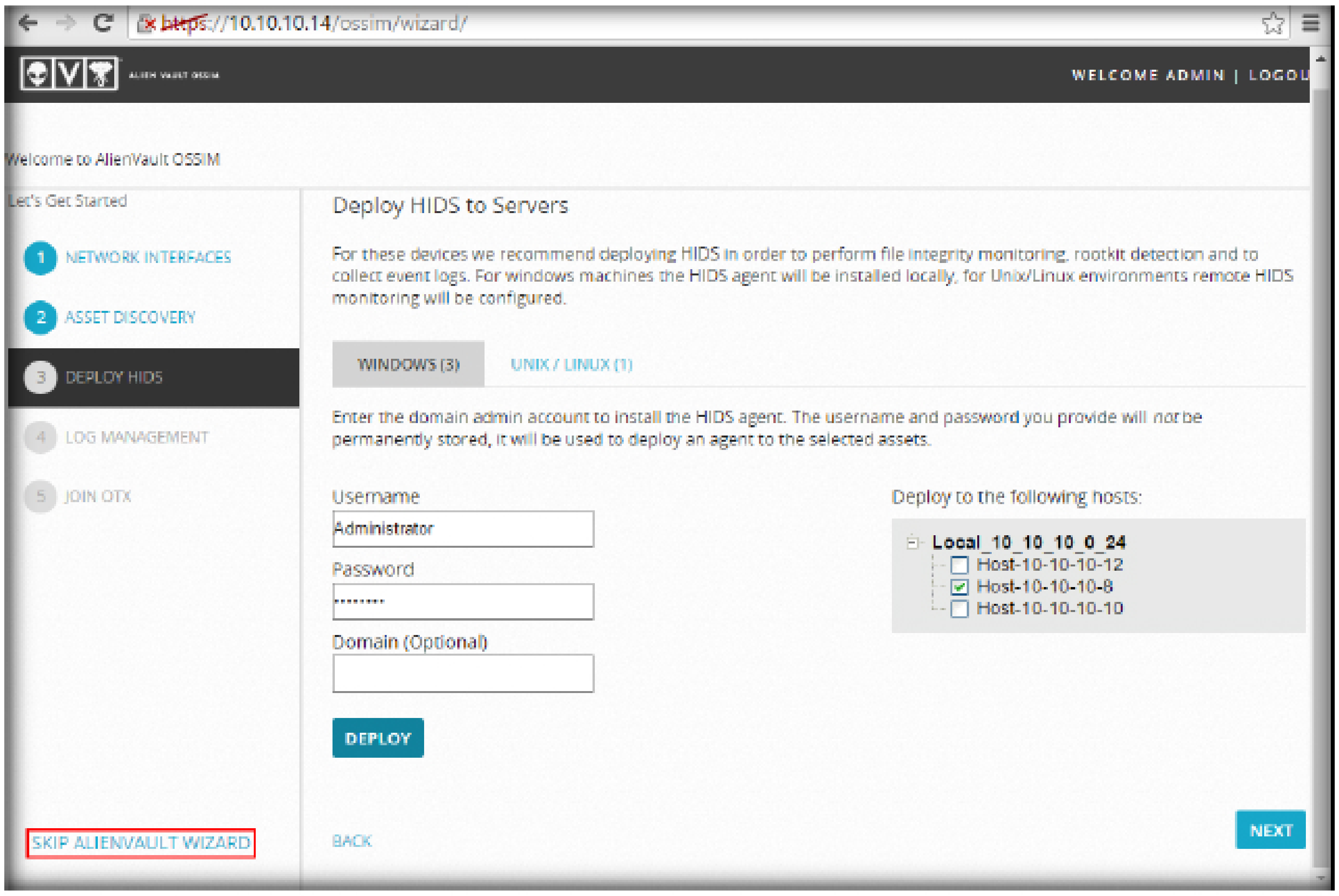


HIDS Deployment

We were able to deploy HIDS to 1 of the 1 devices selected.

FIGURE 10.8: Successfully deployed HIDS

13. Click **SKIP ALIENVAULT WIZARD**.



Welcome to AlienVault OSSIM

Let's Get Started

Deploy HIDS to Servers

For these devices we recommend deploying HIDS in order to perform file integrity monitoring, rootkit detection and to collect event logs. For windows machines the HIDS agent will be installed locally, for Unix/Linux environments remote HIDS monitoring will be configured.

Enter the domain admin account to install the HIDS agent. The username and password you provide will *not* be permanently stored, it will be used to deploy an agent to the selected assets.

Username: Administrator

Password: ••••••••

Domain (Optional):

Deploy to the following hosts:

Local_10_10_10_0_24
- □ Host-10-10-10-12
- ☑ Host-10-10-10-8
- □ Host-10-10-10-10

FIGURE 10.9: Moving to next step

14. Hover the mouse cursor on **ENVIRONMENT** and select **DETECTION**.

    Note: If HELP US IMPROVE ALIENVALUT OSSIM pop-up appears, click Cancel.

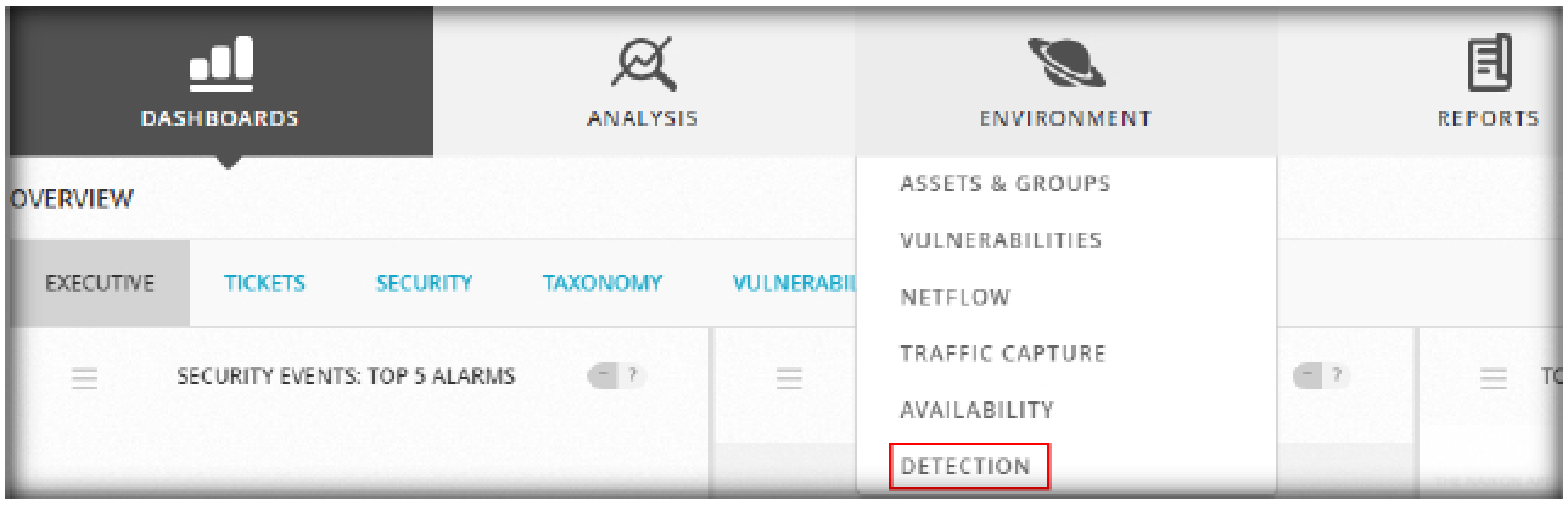
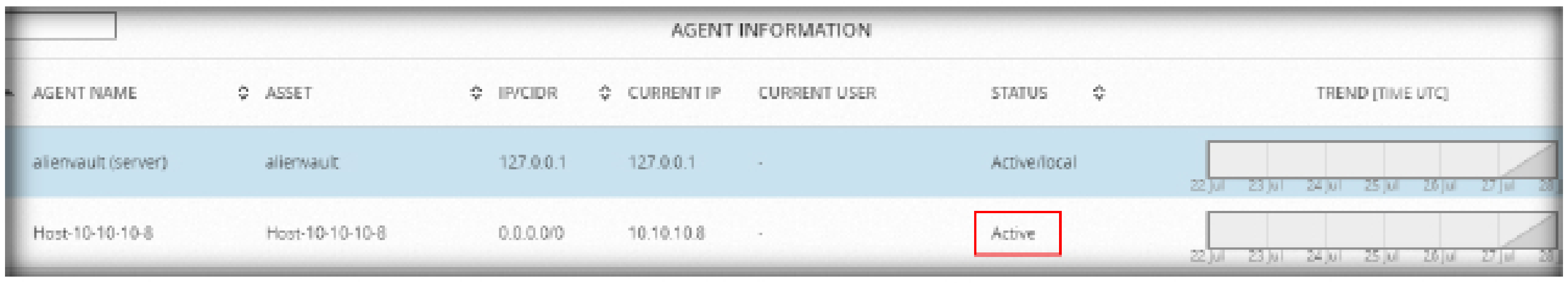


FIGURE 10.10: Navigating to detection

15. You can see the agent for host 10.10.10.8 (Windows Server 2008) is **Active**.

16. We have successfully deployed an OSSEC agent in the Windows Server 2008 to monitor.



AGENT INFORMATION

| AGENT NAME | ASSET | IP/CIDR | CURRENT IP | CURRENT USER | STATUS | TREND [TIME UTC] |
|---|---|---|---|---|---|---|
| alienvault (server) | alienvault | 127.0.0.1 | 127.0.0.1 | - | Active/local | |
| Host-10-10-10-8 | Host-10-10-10-8 | 0.0.0.0/0 | 10.10.10.8 | - | Active | |

FIGURE 10.11: Agent is active

## Lab Analysis

Analyze and document the results of the lab exercise. Give your opinion on your target's security posture and exposure through free public information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

| Internet Connection Required | |
|---|---|
| □ Yes | ☑ No |
| **Platform Supported** | |
| ☑ Classroom | ☑ iLabs |

Lab

11

# Viewing SIEM Events with OSSIM

*OSSIM (Open Source Security Information Management) is an open source security information and event management system.*

## Lab Scenario

It is necessary to collect all events and logs pertaining to an organization's infrastructure and examine them to check if things are in order. As a chief network defender, you need to deploy SIEM on the organization's network and view the events and logs stored in the SIEMs.

**ICON KEY**

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

## Lab Objectives

This lab will demonstrate how to view SIEM events with OSSIM.

## Lab Environment

To carry out the lab, you need:

- OSSIM virtual machine
- A virtual machine running Windows Server 2012
- A Web browser with an Internet connection
- **Administrative** privileges to run the tools

## Lab Duration

Time: 15 Minutes

## Overview of SIEM

A SIEM collects event data from various security logs within the organization, such as those for enterprise security controls, operating systems and applications. The SIEM converts the event data into a format it understands, analyzes it, generates alerts for any suspicious events and creates reports on the events.

## Lab Tasks

TASK 1

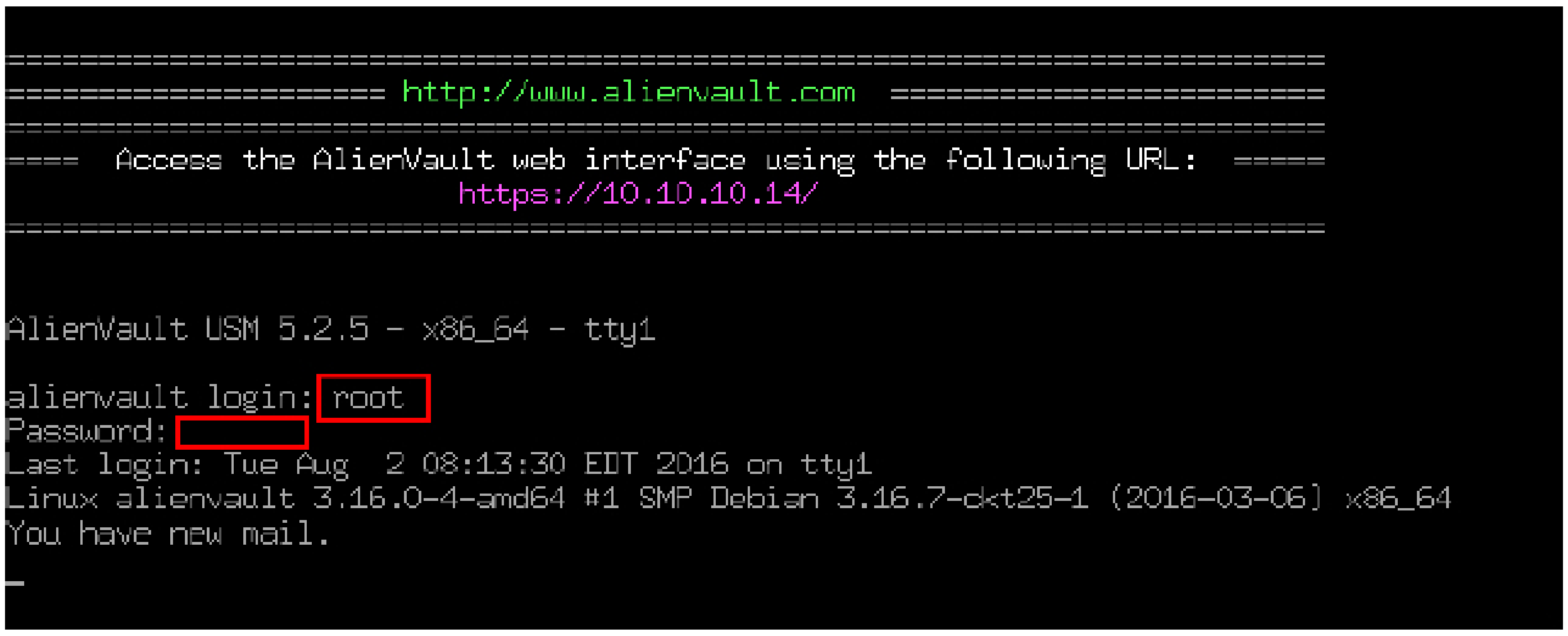
**Log on to OSSIM**

1. Before starting this lab, make sure the Windows 10 and Windows Server 2008 machine is turned on.

2. Power on the OSSIM virtual machine from the VMware workstation, and wait until the log in screen appears.

3. In the log in screen type **root** in the Alienvault login field and press **Enter**. In the password field type **toor** as the password and press **Enter**.

   Note: Password is not visible.



```
========================================================================
==================== http://www.alienvault.com  =======================
========================================================================
====  Access the AlienVault web interface using the following URL:  =====
                         https://10.10.10.14/
========================================================================


AlienVault USM 5.2.5 - x86_64 - tty1

alienvault login: root
Password:
Last login: Tue Aug  2 08:13:30 EDT 2016 on tty1
Linux alienvault 3.16.0-4-amd64 #1 SMP Debian 3.16.7-ckt25-1 (2016-03-06) x86_64
You have new mail.
_
```

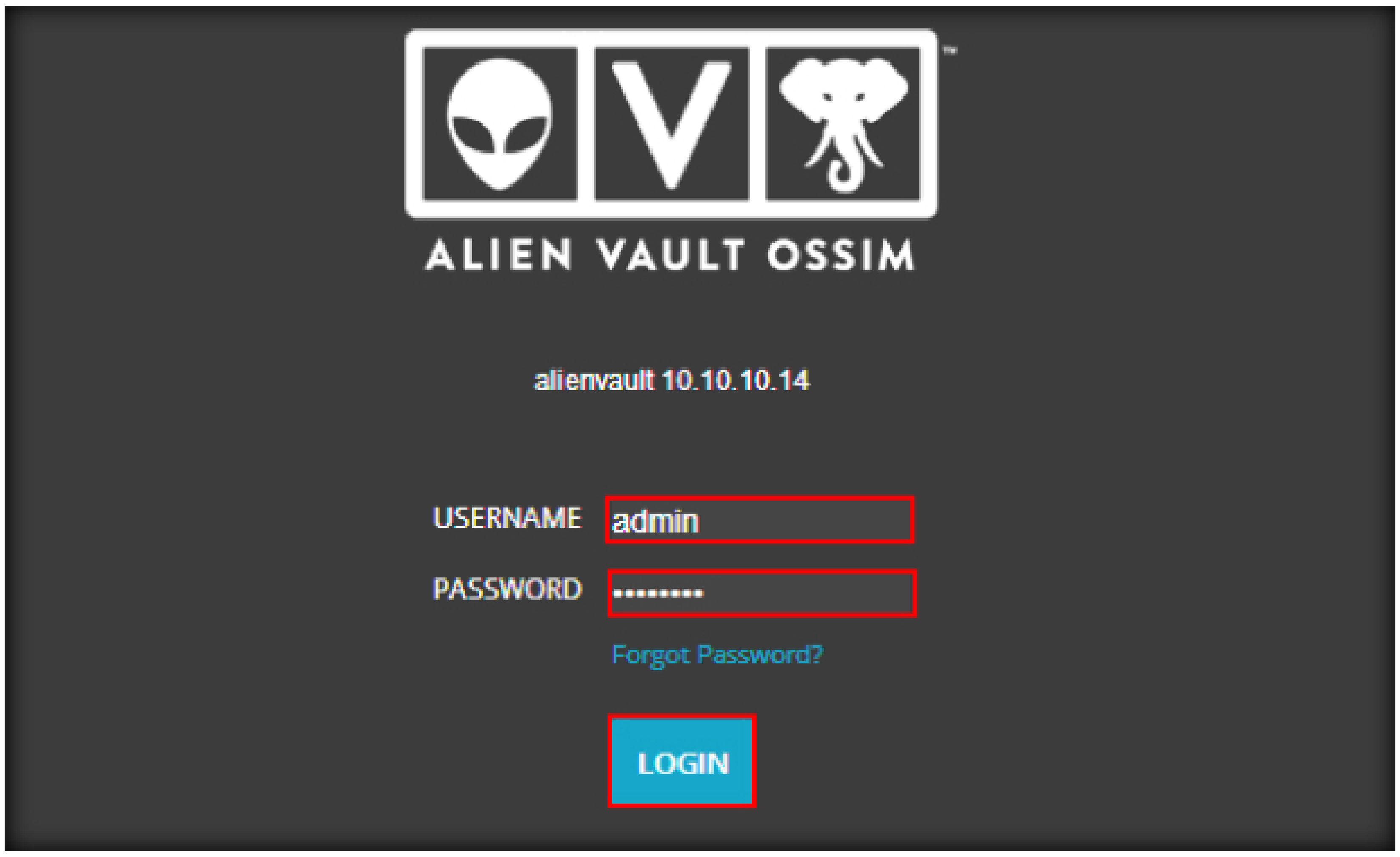
FIGURE 11.1: OSSIM Login Window

4. Launch the Windows Server 2012 machine and log in. Now close the Server Manager window and open a web browser. In this lab we are using a Chrome browser.

   Note: If you are using a different browser the screenshots may differ in your lab environment.

5. Type https://10.10.10.14 and press **Enter** in the address bar of the browser.

6. The OSSIM Login page appears. Enter **admin** in the USERNAME field, **qwerty@123** in the PASSWORD field and click LOGIN.



USERNAME admin

PASSWORD ••••••••

FIGURE 11.2: Logging in to Alien Vault

**TASK 2**

**View Security Events**

7. To view SIEM events, hover the mouse cursor on **ANALYSIS** and click **SECURITY EVENTS (SIEM)**.

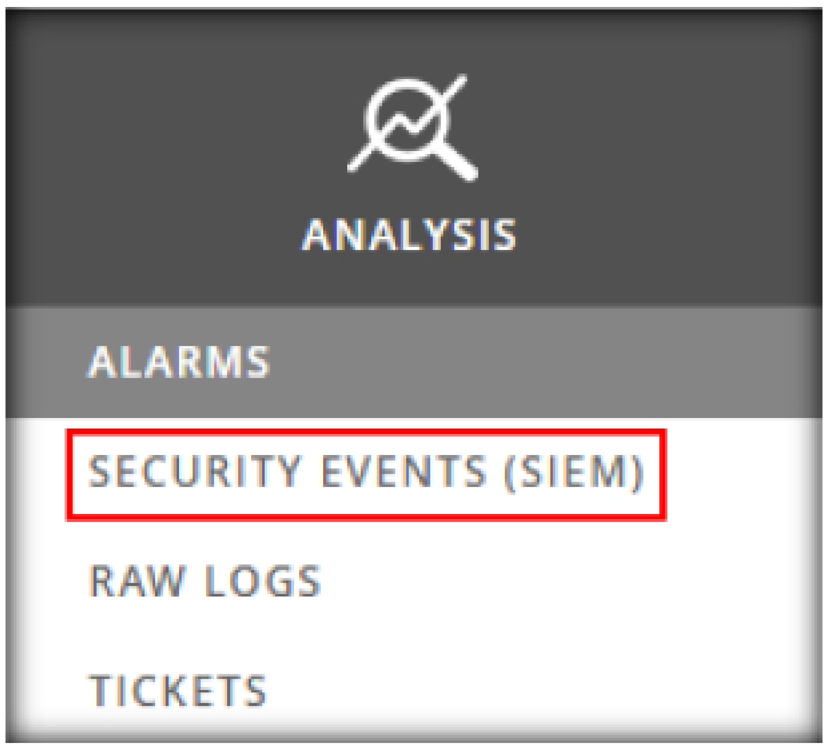
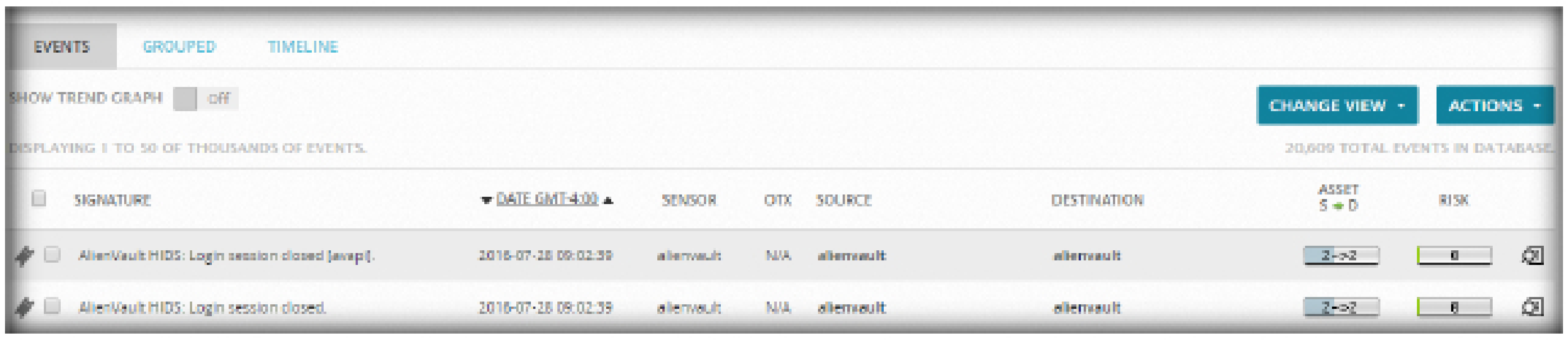


FIGURE 11.3: Navigating to Security Events

8. Scroll down and view the various types of events.



DISPLAYING 1 TO 50 OF THOUSANDS OF EVENTS. 20,609 TOTAL EVENTS IN DATABASE.

| | SIGNATURE | DATE GMT-4:00 | SENSOR | OTX | SOURCE | DESTINATION | ASSET S → D | RISK |
|---|---|---|---|---|---|---|---|---|
| □ | AlienVault HIDS: Login session closed [avapi]. | 2016-07-28 09:02:39 | alienvault | N/A | alienvault | alienvault | 2->2 | 0 |
| □ | AlienVault HIDS: Login session closed. | 2016-07-28 09:02:39 | alienvault | N/A | alienvault | alienvault | 2->2 | 0 |

FIGURE 11.4: Navigating to Taxonomy View

9. To view SIEM logs which are related to the 10.10.10.8 host, click **ADVANCED SEARCH**.

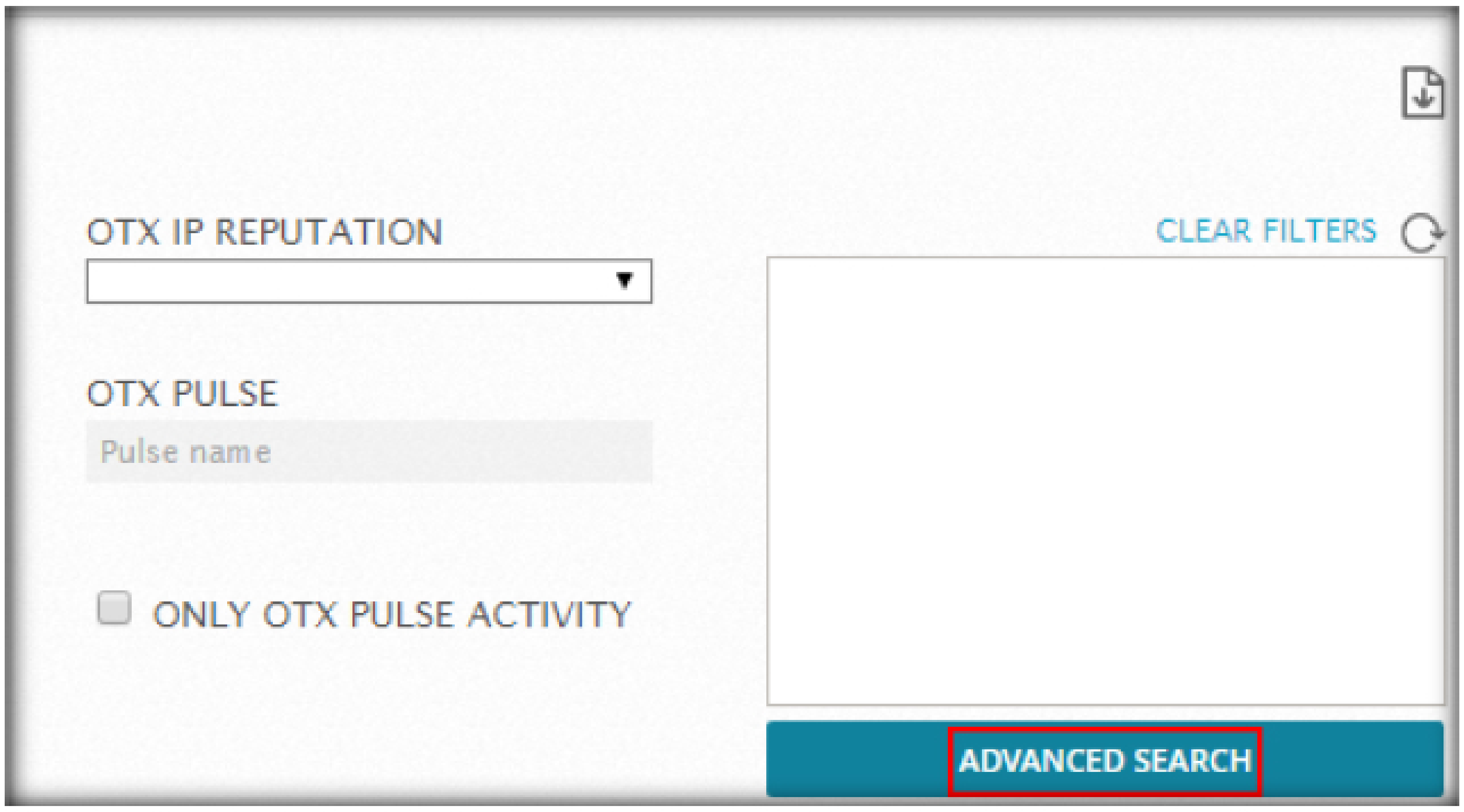
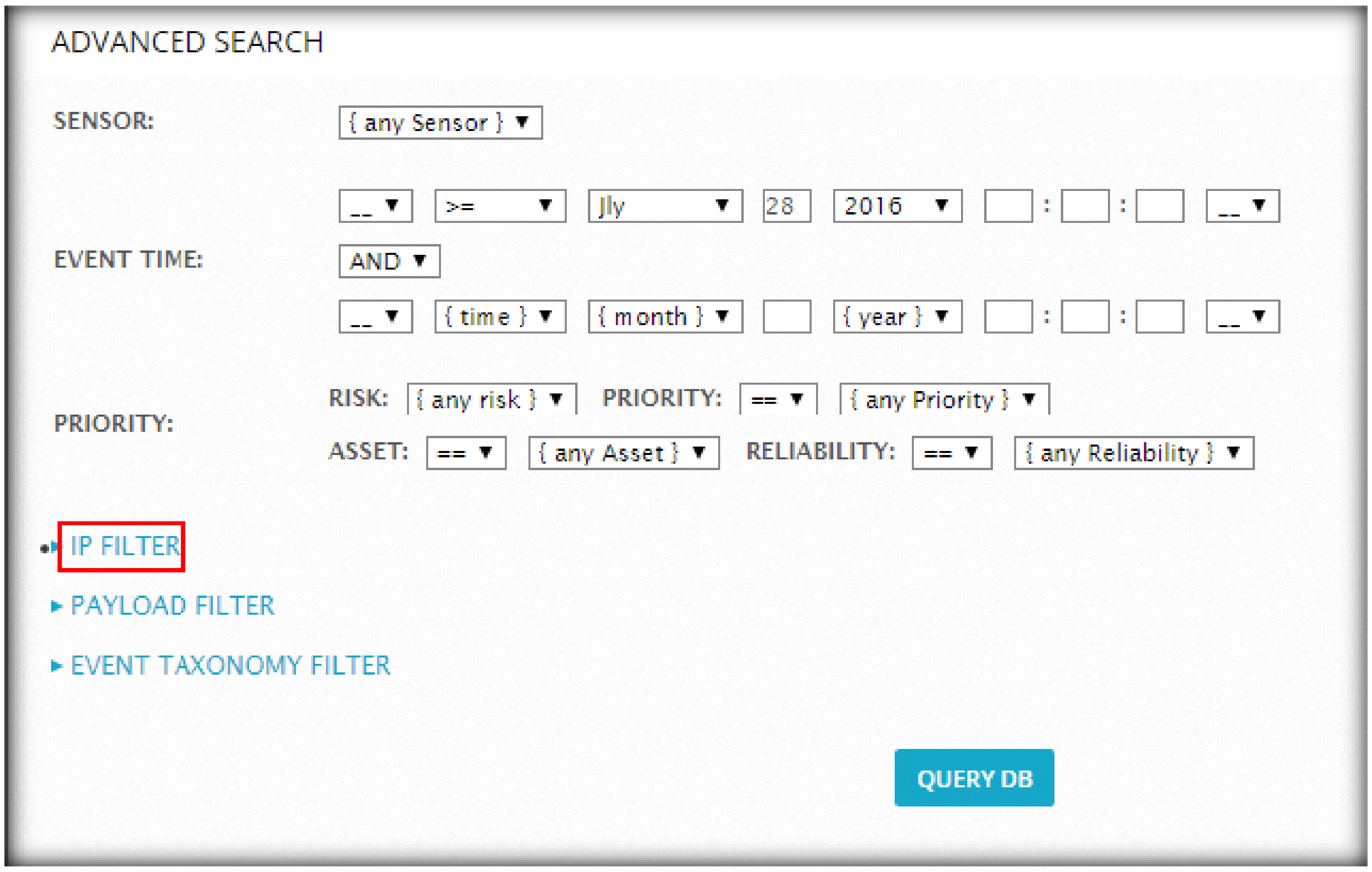


FIGURE 11.5: Navigating to Advanced Search

10. The **ADVANCED SEARCH** appears. Expand IP FILTER.


ADVANCED SEARCH

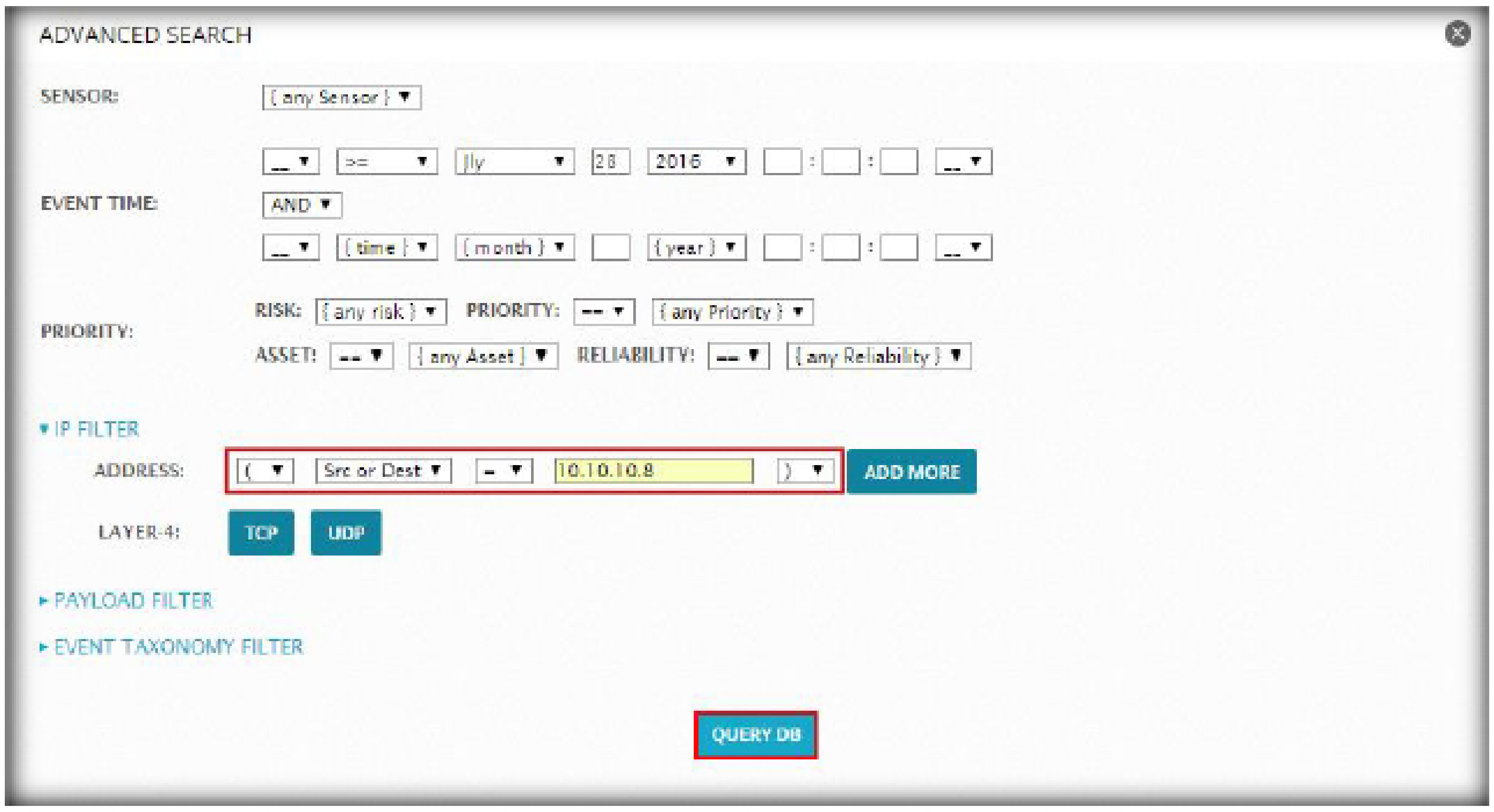
SENSOR: { any Sensor }

EVENT TIME: -- >= Jly 28 2016 : : --
AND
-- { time } { month } { year } : : --

PRIORITY: RISK: { any risk } PRIORITY: == { any Priority }
ASSET: == { any Asset } RELIABILITY: == { any Reliability }

FIGURE 11.6: Expanding IP Filter

11. Select the values in the **ADDRESS** field as shown in the screenshot, click **QUERY DB**.



ADVANCED SEARCH

SENSOR: { any Sensor }

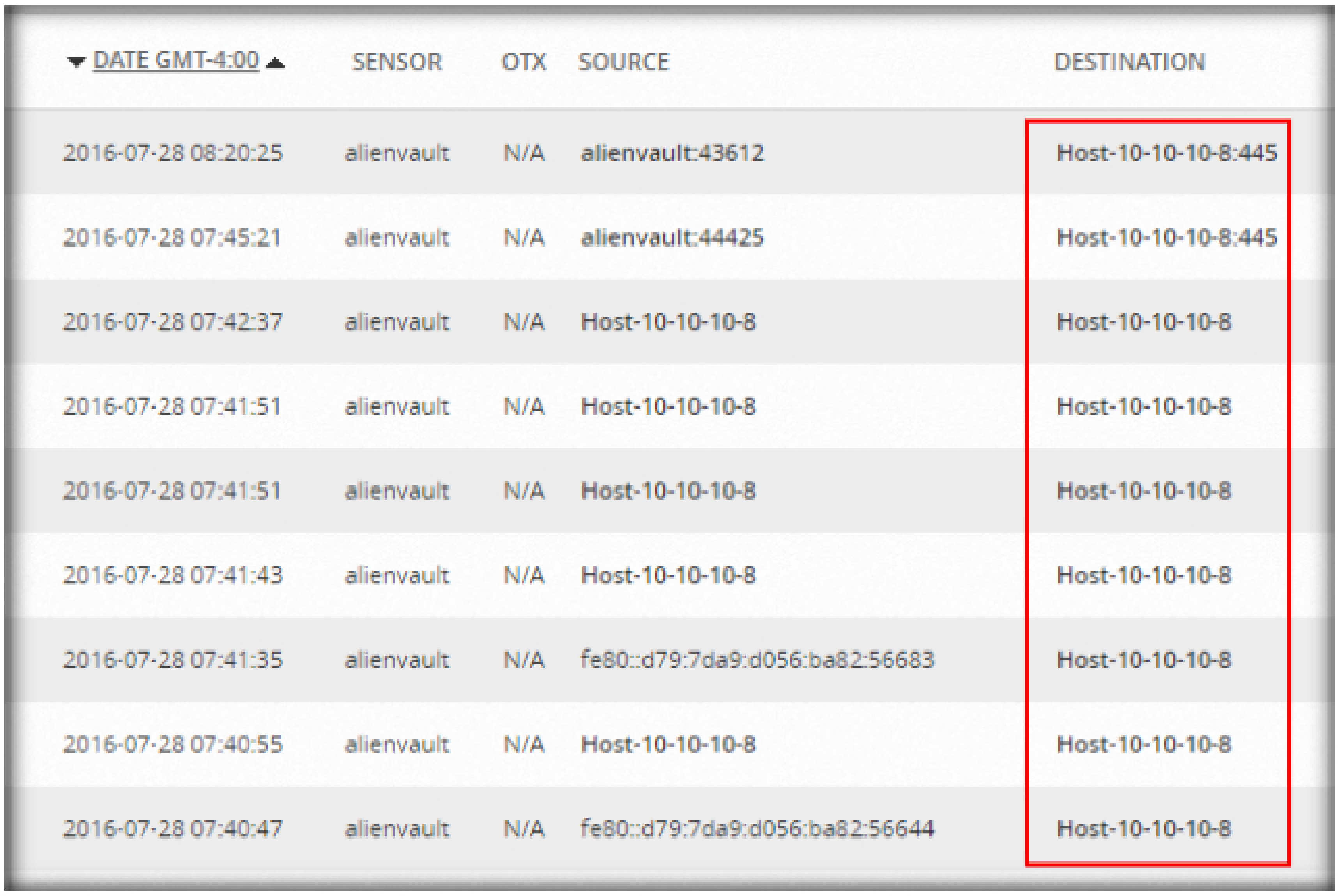
EVENT TIME: __ >= Jly 28 2016 : : __
AND
__ { time } { month } { year } : : __

PRIORITY:
RISK: { any risk } PRIORITY: -- { any Priority }
ASSET: -- { any Asset } RELIABILITY: -- { any Reliability }

IP FILTER
ADDRESS: ( Src or Dest = 10.10.10.8 )

FIGURE 11.7: Adding Filter Details

12. You can view all events for the **10.10.10.8** host, irrespective of whether the address is in the source or destination field.



| DATE GMT-4:00 | SENSOR | OTX | SOURCE | DESTINATION |
|---|---|---|---|---|
| 2016-07-28 08:20:25 | alienvault | N/A | alienvault:43612 | Host-10-10-10-8:445 |
| 2016-07-28 07:45:21 | alienvault | N/A | alienvault:44425 | Host-10-10-10-8:445 |
| 2016-07-28 07:42:37 | alienvault | N/A | Host-10-10-10-8 | Host-10-10-10-8 |
| 2016-07-28 07:41:51 | alienvault | N/A | Host-10-10-10-8 | Host-10-10-10-8 |
| 2016-07-28 07:41:51 | alienvault | N/A | Host-10-10-10-8 | Host-10-10-10-8 |
| 2016-07-28 07:41:43 | alienvault | N/A | Host-10-10-10-8 | Host-10-10-10-8 |
| 2016-07-28 07:41:35 | alienvault | N/A | fe80::d79:7da9:d056:ba82:56683 | Host-10-10-10-8 |
| 2016-07-28 07:40:55 | alienvault | N/A | Host-10-10-10-8 | Host-10-10-10-8 |
| 2016-07-28 07:40:47 | alienvault | N/A | fe80::d79:7da9:d056:ba82:56644 | Host-10-10-10-8 |

FIGURE 11.8: SIEM Logs Filtered

## Lab Analysis

Analyze and document the results of the lab exercise. Give your opinion on your target's security posture and exposure through free public information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

| Internet Connection Required | |
|---|---|
| □ Yes | ☑ No |
| Platform Supported | |
| ☑ Classroom | ☑ iLabs |