# Network Traffic Monitoring and Analysis

## Module 11

Lab 1

# Capturing Network Traffic using Wireshark

*Wireshark is a network packet analyzer, which is used to capture network packets and display packet data in detail.*

## Lab Scenario

Traffic flowing through a network contains various kinds of data. Understanding the packets of data flowing through the network using command line applications is a tedious task, and it is difficult to sort out the required traffic from the live traffic that is flowing through the network. Hence, it is necessary to have an application with a graphical user interface that can capture the entire traffic in a network, and help you in filtering the traffic. Being a network administrator, you need to have Wireshark installed to monitor and capture network traffic.

ICON KEY

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

## Lab Objectives

The objective of this lab is to demonstrate the installation of Wireshark and capturing network traffic

## Lab Environment

To carry out the lab, you need:

- Wireshark, located at **Z:\CND-Tools\CND Module 11 Network Traffic Monitoring and Analysis\Packet Sniffing Tools\Wireshark**
- You can also download the latest version of Wireshark from the link https://www.wireshark.org/download.html
- If you decide to download the latest version, then screenshots shown in the lab may differ
- A virtual machine running Windows Server 2012
- A Web browser with Internet connection
- **Administrative** privileges to run tools

You can download Wireshark from http://www.wireshark.org.



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

# Lab Duration

Time: 10 Minutes

# Overview of Packet Capture

Packet capture means intercepting data packets traversing over a network using packet capture tools like Wireshark. These captured packets are analyzed in order to determine whether proper network security policies are being followed.

# Lab Tasks

1. Log on to **Windows Server 2012** virtual machine in Hyper-V Manager
2. Before beginning this lab, ensure that WinPcap is installed.
3. Navigate to **Z:\CND-Tools\CND Module 11 Network Traffic Monitoring and Analysis\Packet Sniffing Tools\Wireshark** and double-click **Wireshark-win64-2.0.2.exe**
4. If **Open File - Security Warning** pop-up appears, click **Run**.
5. Follow the wizard-driven installation steps to install Wireshark

**TASK 1**

**Installing and Launching Wireshark**

Wireshark is an open source packet analyzer used for network troubleshooting, analysis, software and communications protocol development, and education.

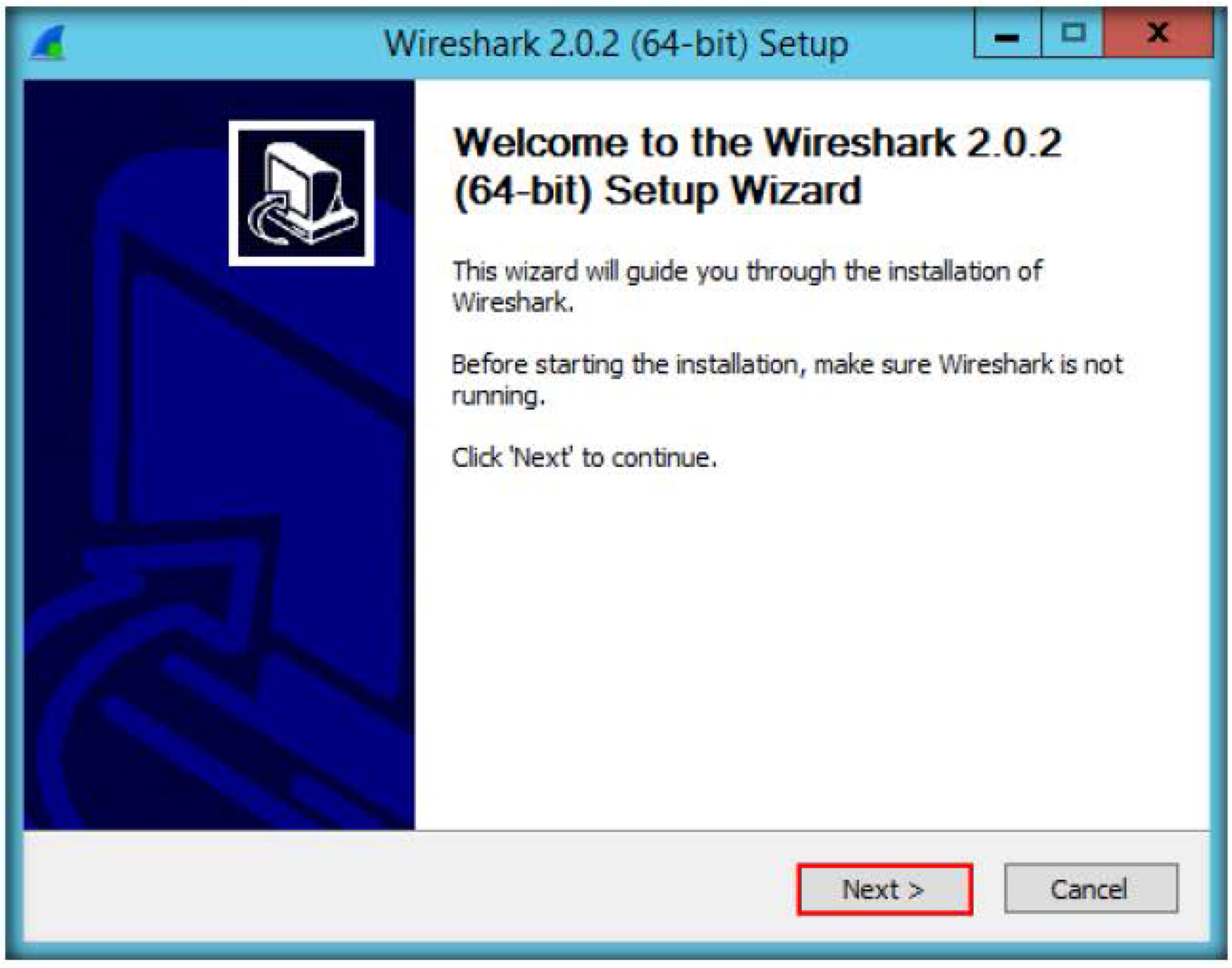



FIGURE 1.1: Wireshark installation wizard


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

6. During installation, a window appears asking you to install WinPcap. If you have already installed the application, click **Cancel**; else, click **Next** if you have not installed WinPcap.

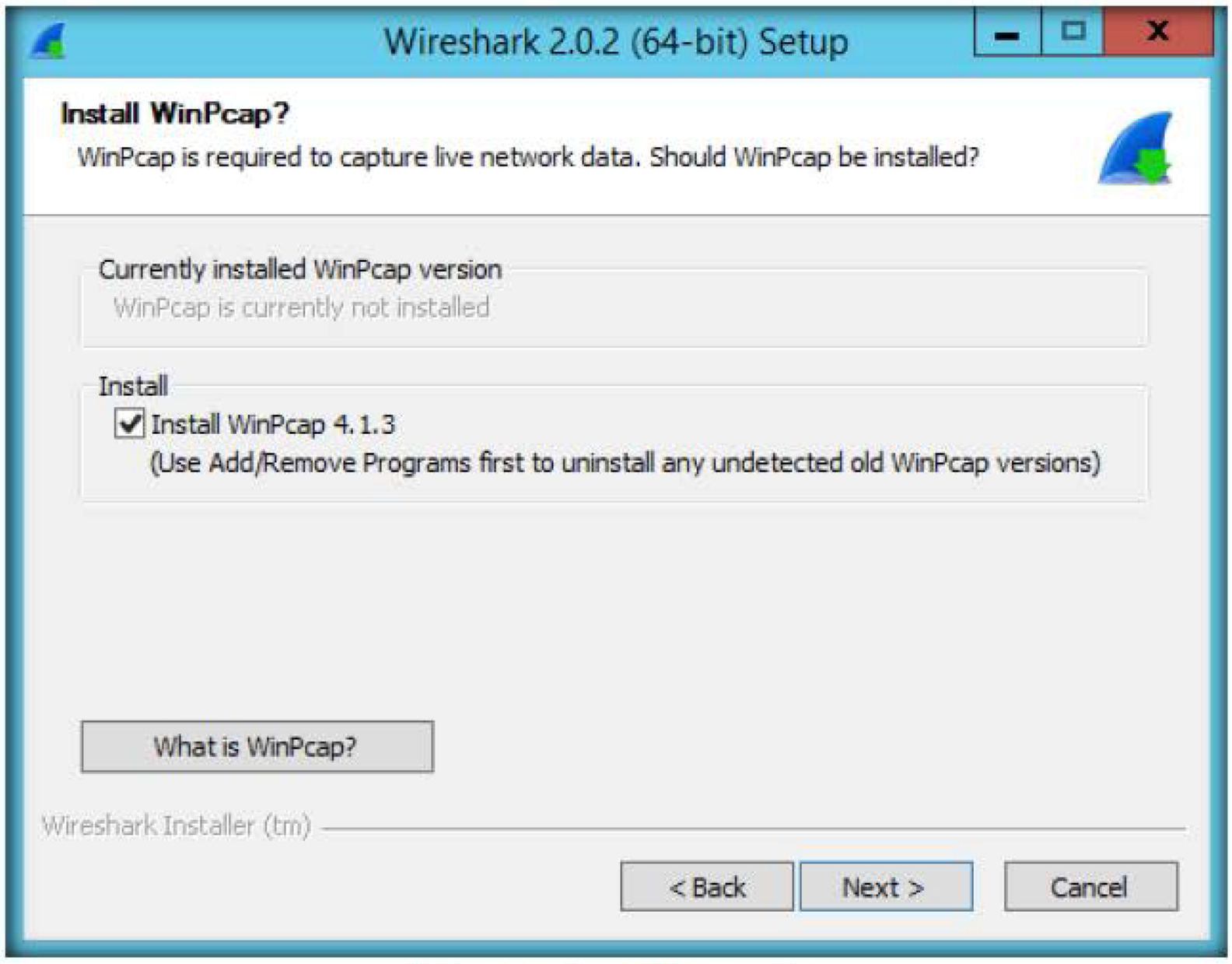



Figure 1.2: WinPcap installation wizard

Wireshark is a tool that allows packet traces to be sniffed, captured and analyzed. Before Wireshark (or in general, any packet capture tool) is used, careful consideration should be given to where in the network packets are to be captured.

7. On completing the installation, launch **Wireshark** from the **Apps** screen

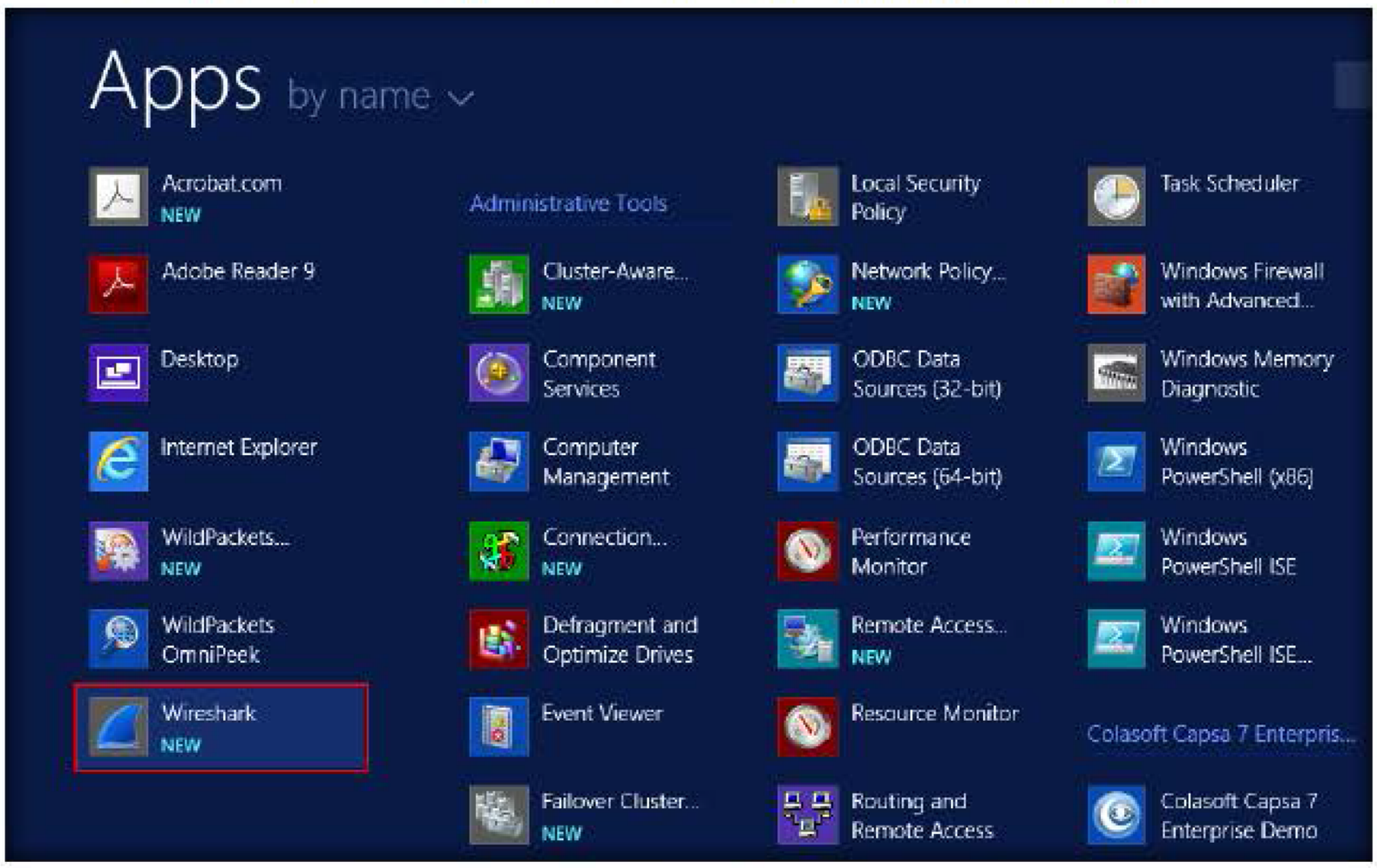



FIGURE 1.3: Windows Server 2012 Apps Screen



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

8. The main window of Wireshark appears as shown in following screenshot:

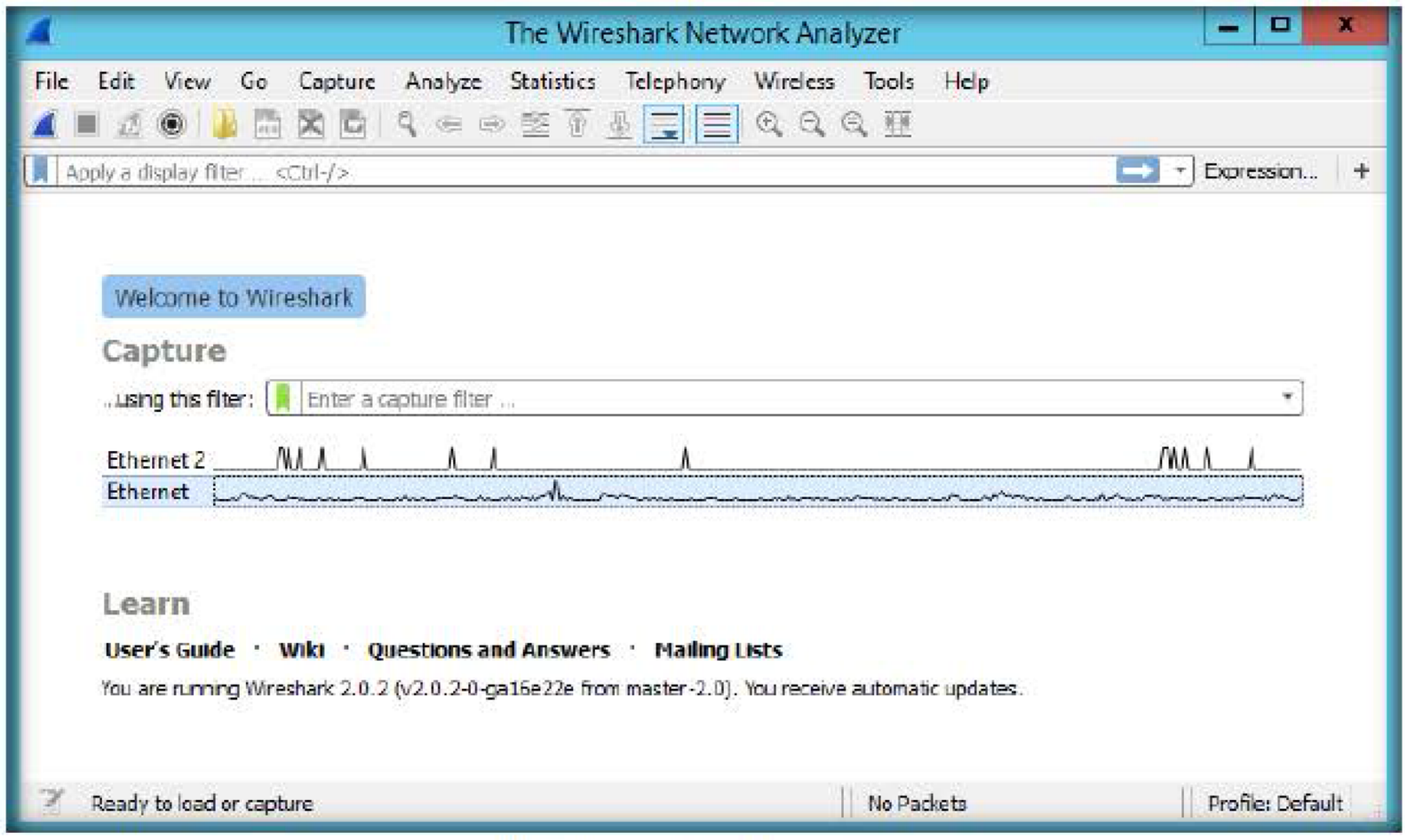



FIGURE 1.4: Wireshark Window

**TASK 2**

**Capturing Network Traffic Using Wireshark**

9. Now, you need to select an interface on which you want Wireshark to capture traffic. To begin packet capture, select an interface of your choice, and click **Capture** (shark fin) icon.

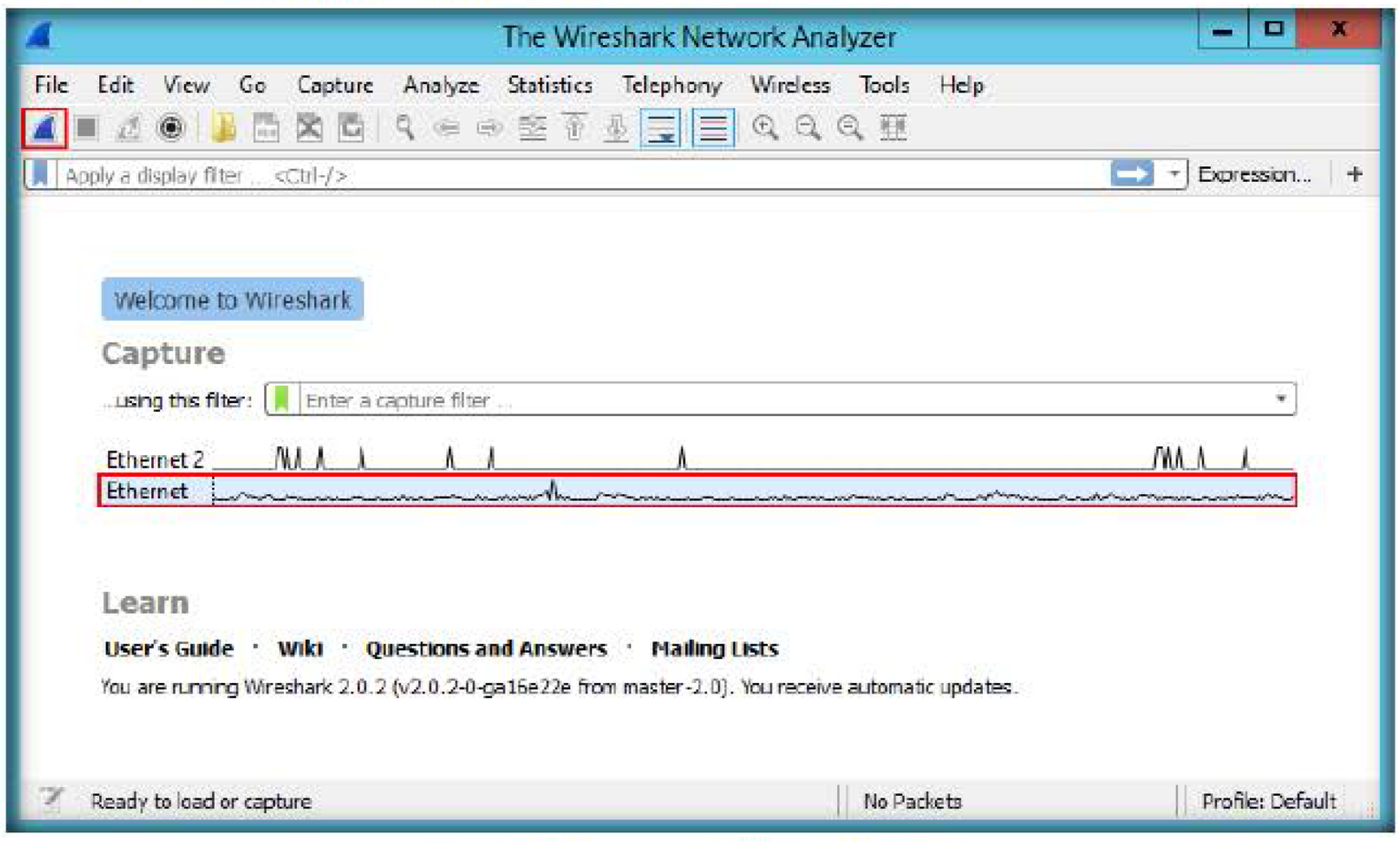



FIGURE 1.5: Capturing traffic in Wireshark



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

10. Wireshark begins to capture traffic of the selected interface as shown in the following screenshot:

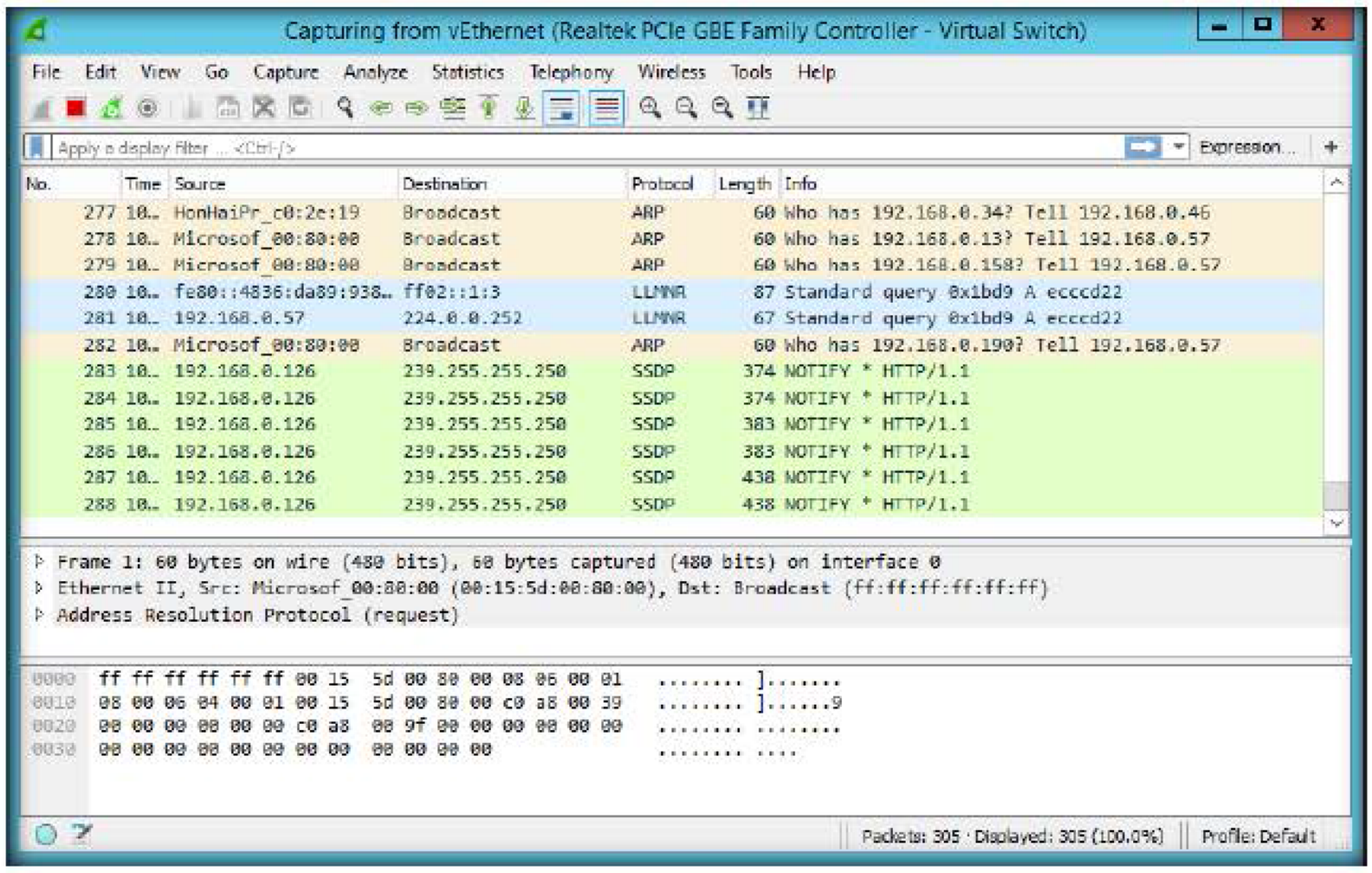



FIGURE 1.6: Traffic Captured on Wireshark

Wireshark uses colors to help you identify the types of traffic at a glance. By default, green is TCP traffic, dark blue is DNS traffic, light blue is UDP traffic, and black identifies TCP packets with problems

11. This way, you can configure Wireshark to capture network traffic

## 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 |


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

Lab 2

# Applying Various Filters in Wireshark

*Wireshark provides numerous filters that can be applied to get only the required packets*

ICON KEY

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

## Lab Scenario

Wireshark filters traffic flowing through the entire network. This traffic contains various kinds of data packets associated with various protocols, flowing between the source and destination. So, searching for a specific packet, port or an IP address manually is extremely difficult. In such cases, applying Wireshark filters helps network administrators to track down the huge amount of traffic and discover the intended packets. As a network administrator, it is essential to have a good knowledge of various Wireshark filters that help you in narrowing down the traffic and obtaining the desired result.

## Lab Objectives

The objective of this lab is to help you become familiar with various Wireshark filters

## Lab Environment

To carry out this lab, you need:

- Wireshark, located at **Z:\CND-Tools\CND Module 11 Network Traffic Monitoring and Analysis\Packet Sniffing Tools\Wireshark**
- You can also download the latest version of Wireshark from the link https://www.wireshark.org/download.html
- If you decide to download the latest version, then screenshots shown in the lab might differ
- A virtual machine running Windows Server 2012
- A virtual machine running Windows Server 2008
- A Web browser with Internet connection


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

- **Administrative** privileges to run tools

## Lab Duration

Time: 25 Minutes

## Overview of Wireshark

You can download Wireshark from http://www.wireshark.org.

There are various filters in Wireshark that help you filter packets containing:

- Source IP address
- Destination IP address
- ICMP traffic and so on

## Lab Tasks

1. Before beginning this lab, ensure that you are logged on to the Windows Server 2012 and Windows Server 2008 virtual machines
2. Launch Wireshark and start capturing traffic on your network
3. In order to capture traffic in Wireshark, browse the websites http://www.in.com and http://10.10.10.8/cnd
4. The **Filter** field at the top of the Wireshark main window allows you to apply various filters which help with narrowing down the traffic

A capture filter takes the form of a series of primitive expressions connected by conjunctions (and/or) and optionally preceded by not

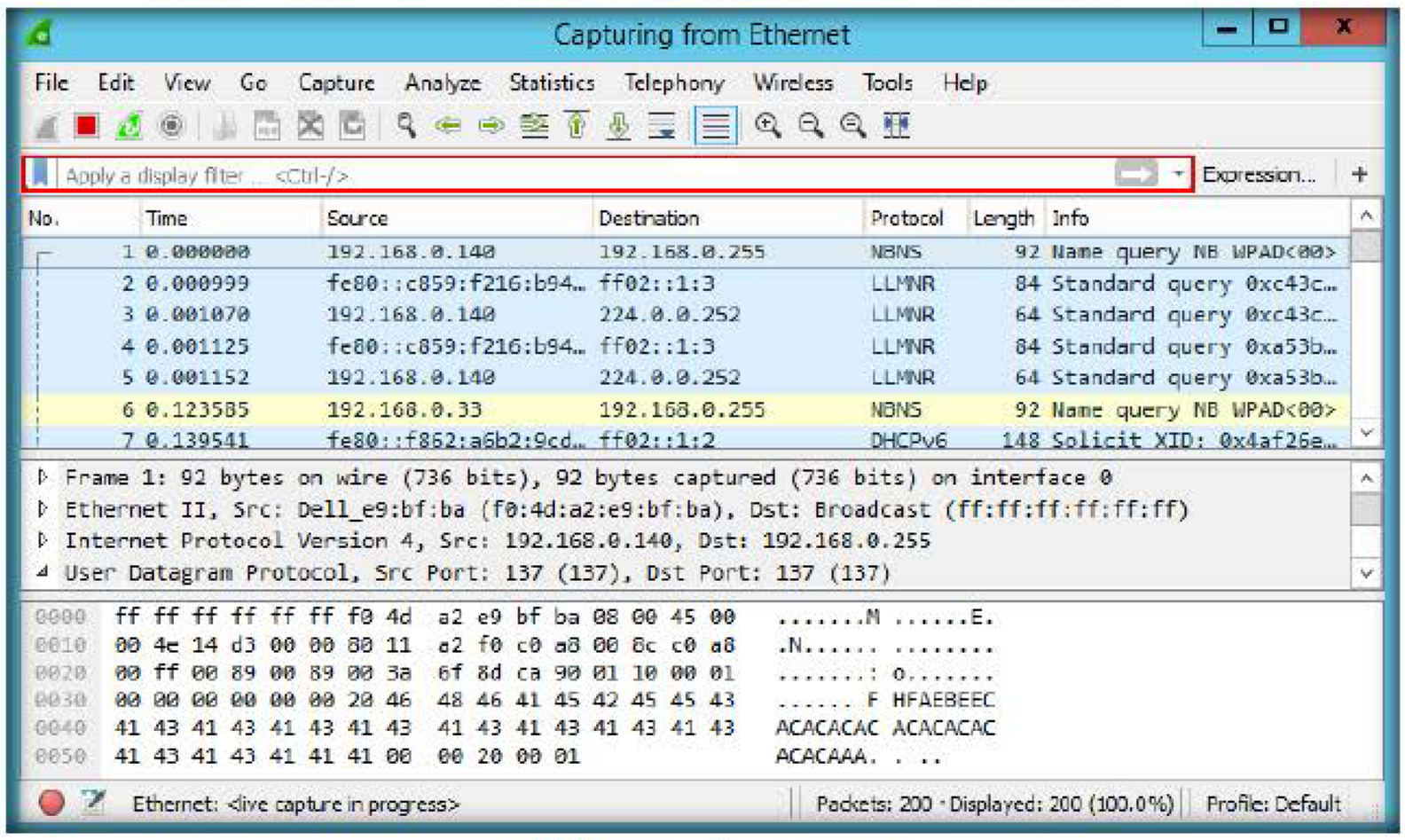



FIGURE 2.1: Wireshark Filter Field



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

**TASK 1**

**Filtering traffic by Protocol**

5. To view the HTTP specific traffic flowing in your network, type **http** in the **filter** field and press **Enter**. By applying this filter, Wireshark filters HTTP traffic flowing through the network and displays it as shown in the following screenshot:

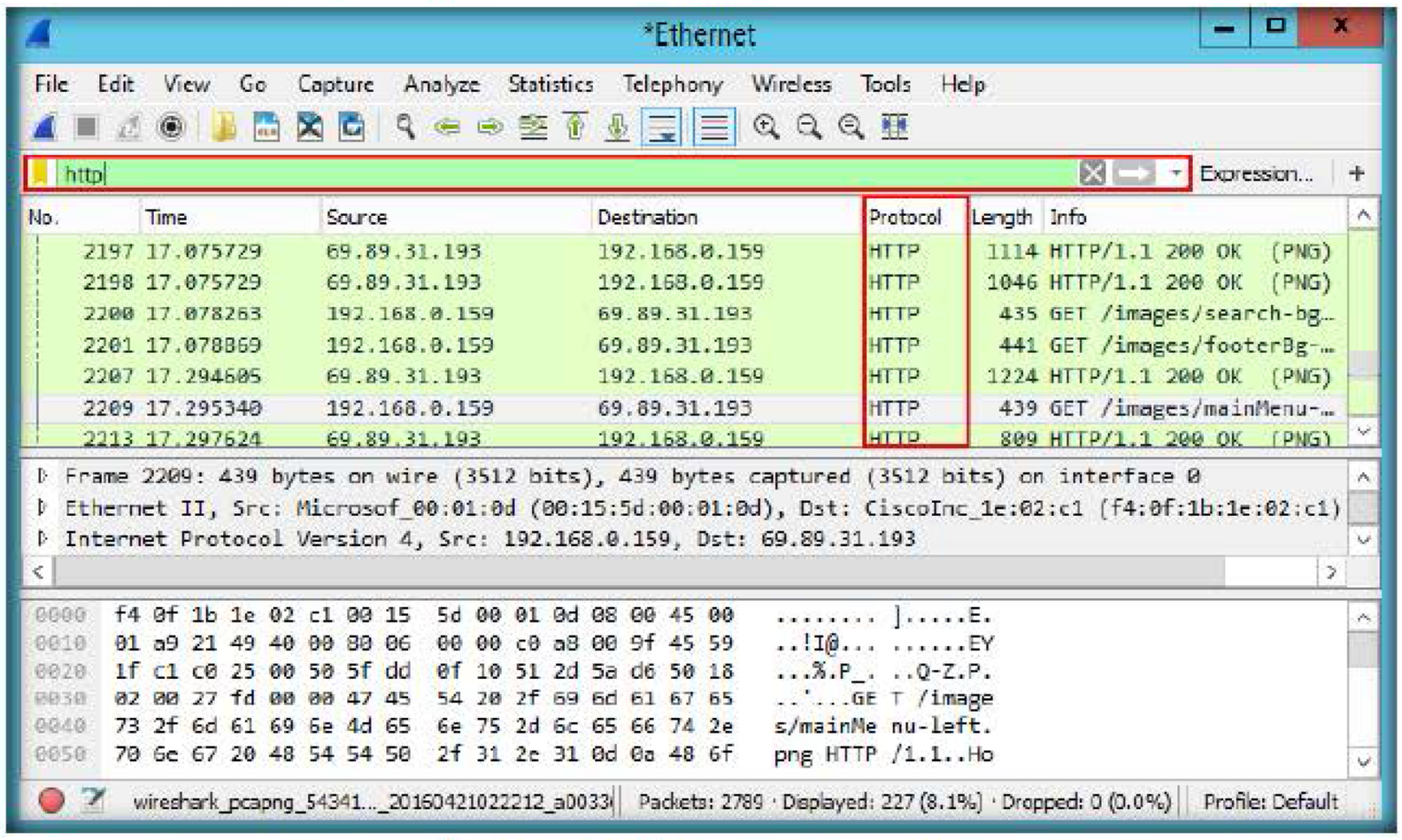



FIGURE 2.2 Packet Filtering with HTTP Packets

6. To view the TCP specific traffic flowing in your network, type **tcp** in the **filter field** and press **Enter**. By applying this filter, Wireshark filters TCP traffic flowing through the network and displays it as shown in the following screenshot:

The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems. HTTP functions as a request–response protocol in the client–server computing model.

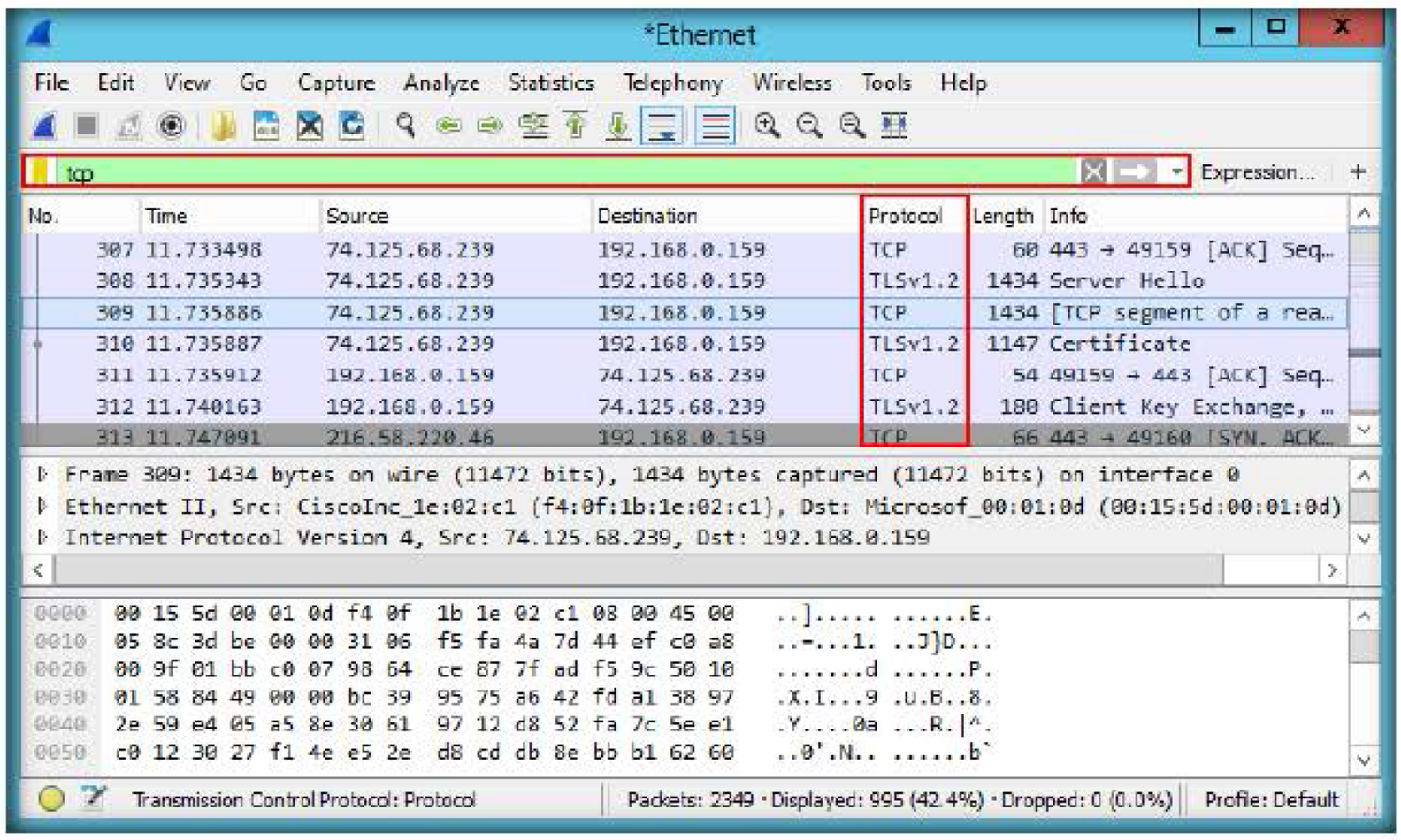



FIGURE 2.3: Packet Filtering with TCP Packets



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

7. To view the ARP specific traffic flowing in your network, type **arp** in the **filter field** and press **Enter**. By applying this filter, Wireshark filters ARP traffic flowing through the network and displays it as shown in the following screenshot:

The Address Resolution Protocol (ARP) is a telecommunication protocol used for resolution of Internet layer addresses into link layer addresses, a critical function in multiple-access networks.

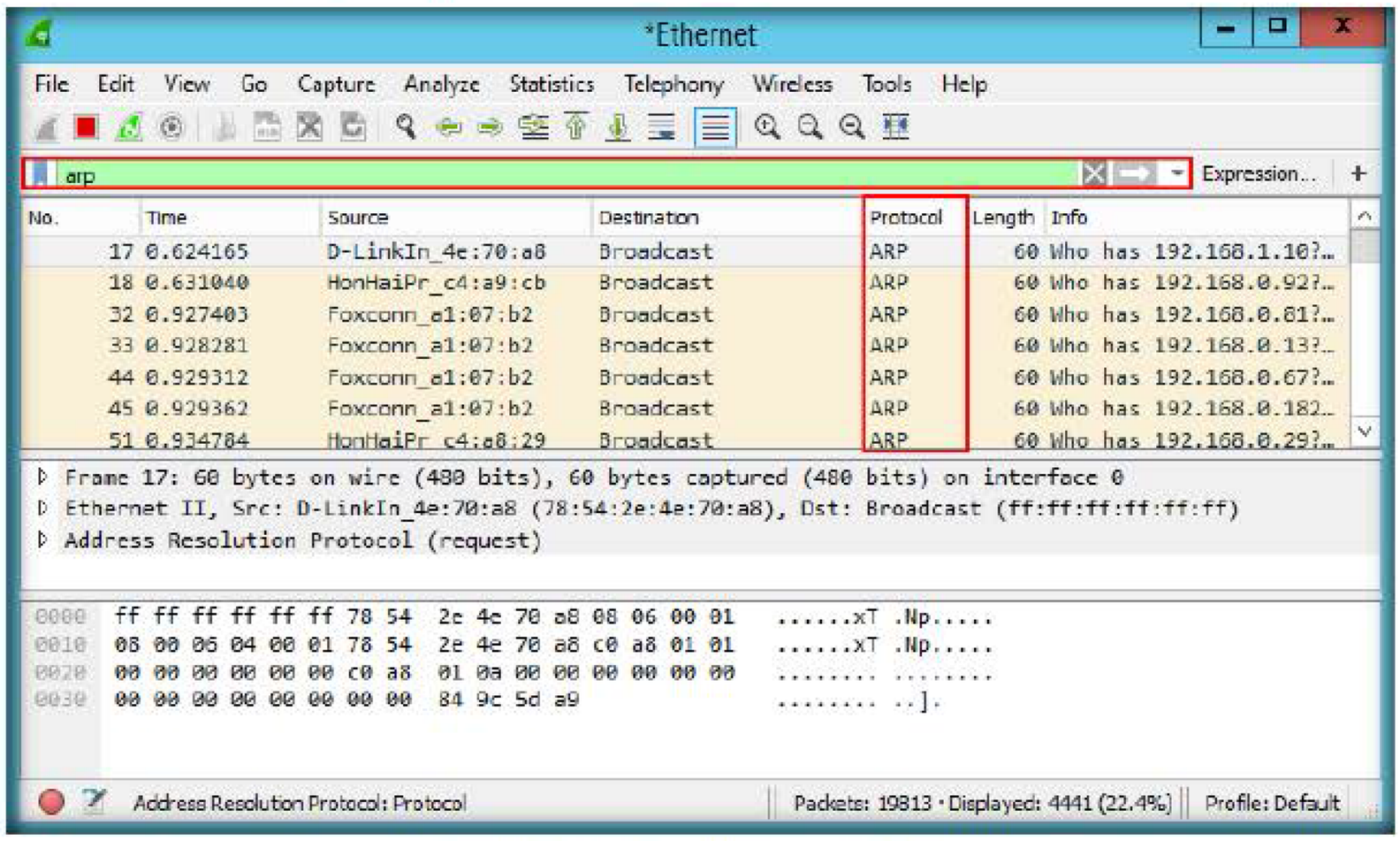



FIGURE 2.4: Packet Filtering with ARP Packets

8. In the same way, you may use various other filters to filter the required traffic

**TASK 2**

**Filtering Traffic by IP addresses**

9. You can also filter traffic based on the source and destination IP addresses. To view traffic originating or destined to a specific IP address, apply filter **[ip.addr==IP Address]** (The IP addresses shown here may differ in your environment)

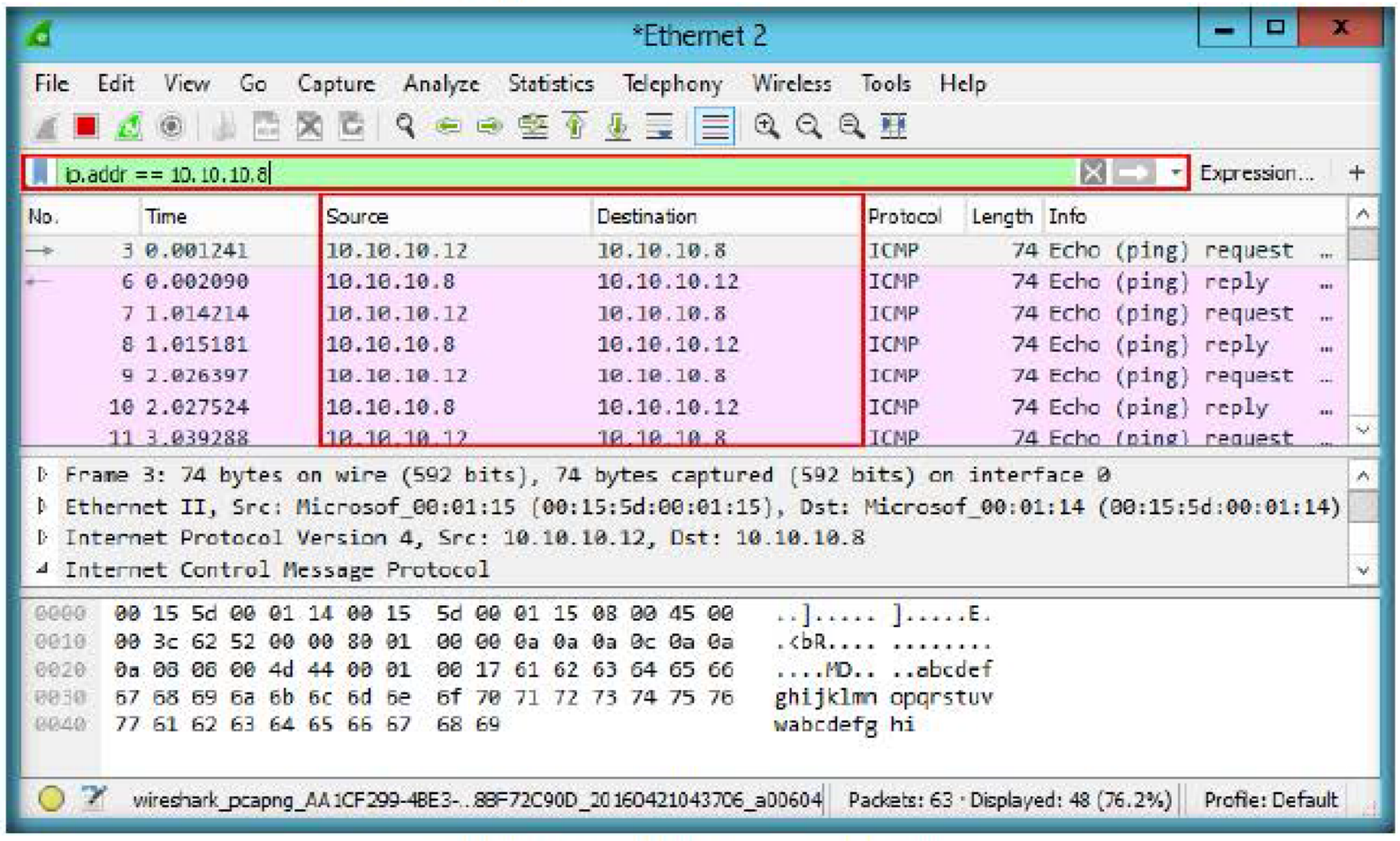



FIGURE 2.5: Packet Filtering with IP Address



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

10. To view traffic originating from specific IP addresses, apply the filter **[ip.src==IP Address]**

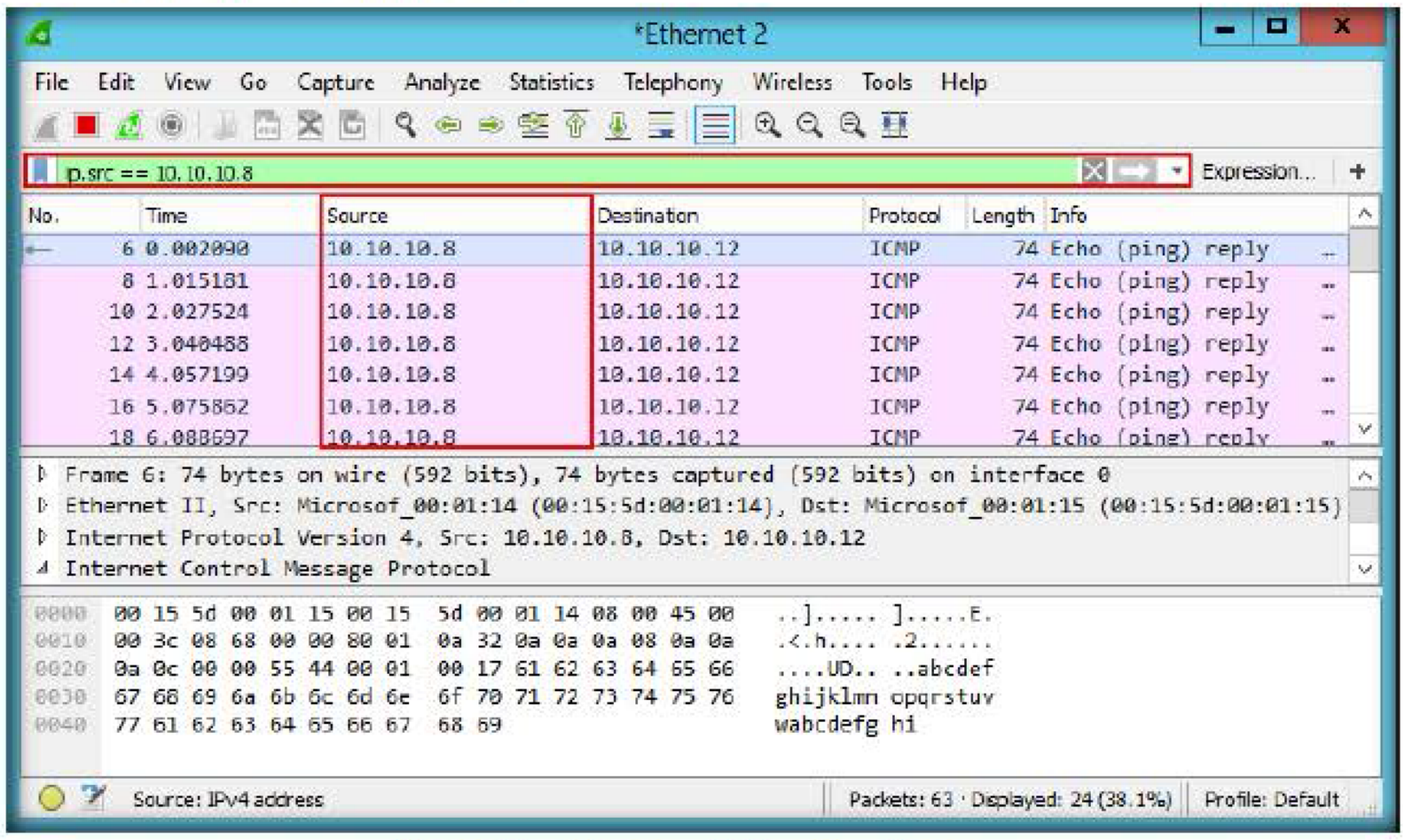



FIGURE 2.6: Packet filtering with source IP Address

Each machine connected to the Internet has an address known as an Internet Protocol address (IP address). The IP address takes the form of four numbers separated by dots, for example: 123.45.67.890. In simple terms, it is the numeric address of a computer connected to the Internet; also called Internet address.

11. To view the traffic destined to a specific IP address, apply the filter **[ip.dst==IP Address]**

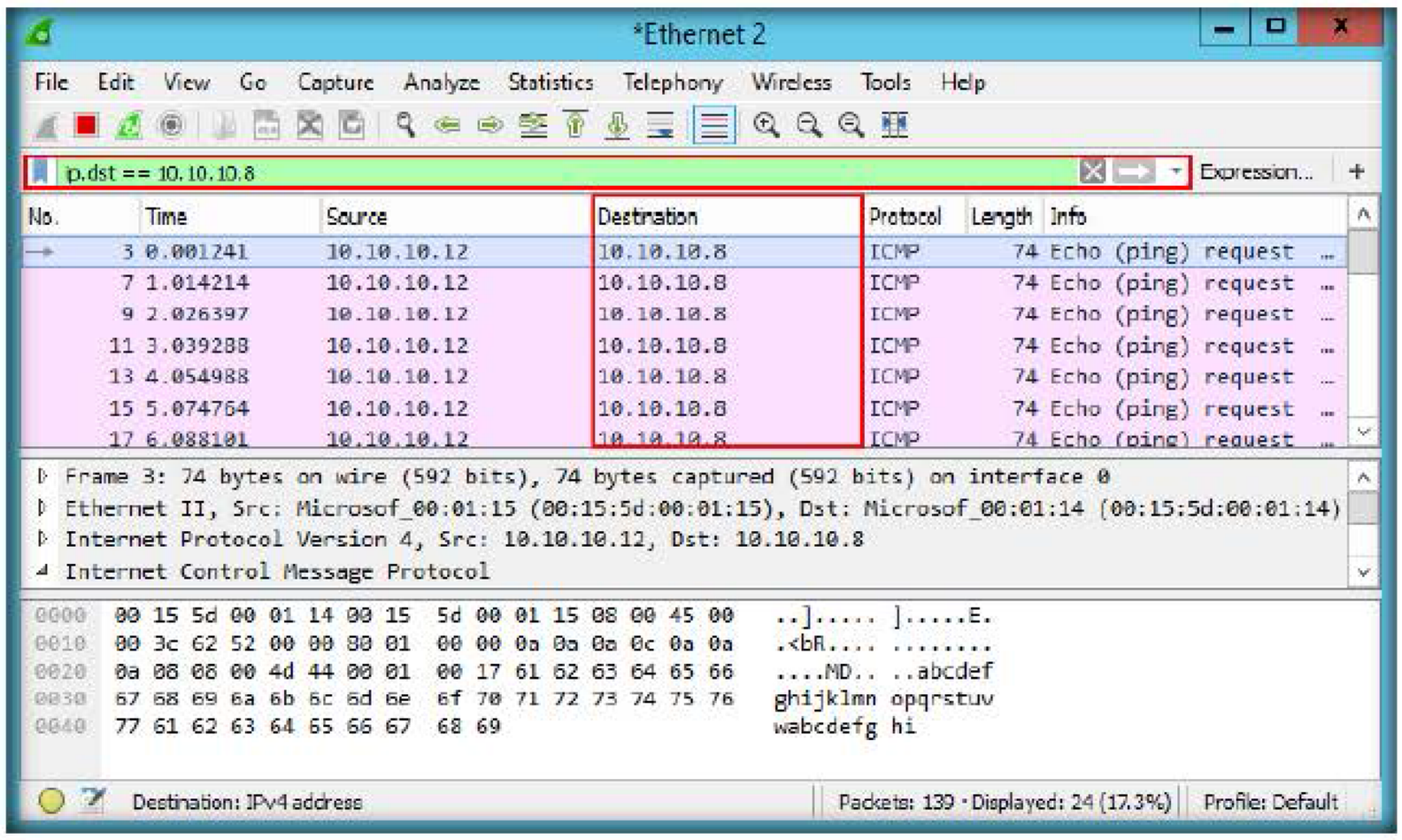



FIGURE 2.7: Packet filtering with Destination IP Address

IP addresses are used to deliver packets of data across a network and have what is termed end-to-end significance. This means that the source and destination IP address remains constant as the packet traverses a network. In simple terms the, Destination IP address is the receiver of information.



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

12. You can also use various conditional operators on IP address filtering to filter traffic of your interest

| Symbol | Meaning |
|---|---|
| == | Is equal to |
| != | Not equal to |
| > | Is greater than |
| < | Is lesser than |
| >= | Greater than or equal to |
| <= | Less than or equal to |

TABLE 2.1: List of Comparison of Operators Used in Filtering

13. To view traffic higher than a specific IP address, use **>** conditional operator in conjunction with IP address filtering. Apply the filter **ip.dst > [IP Address]** to find the destination IP Addresses greater than the specified IP Address.

The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems

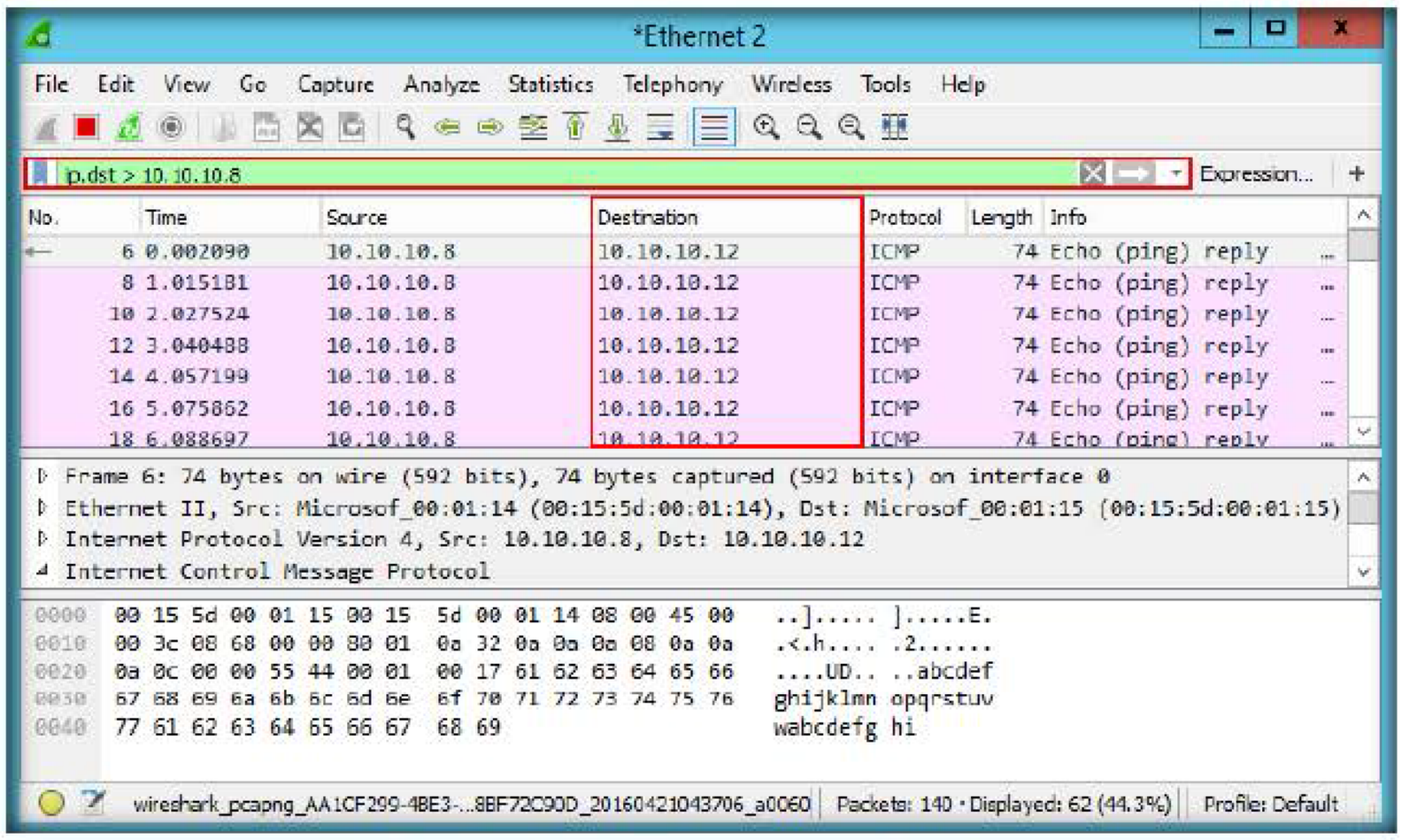
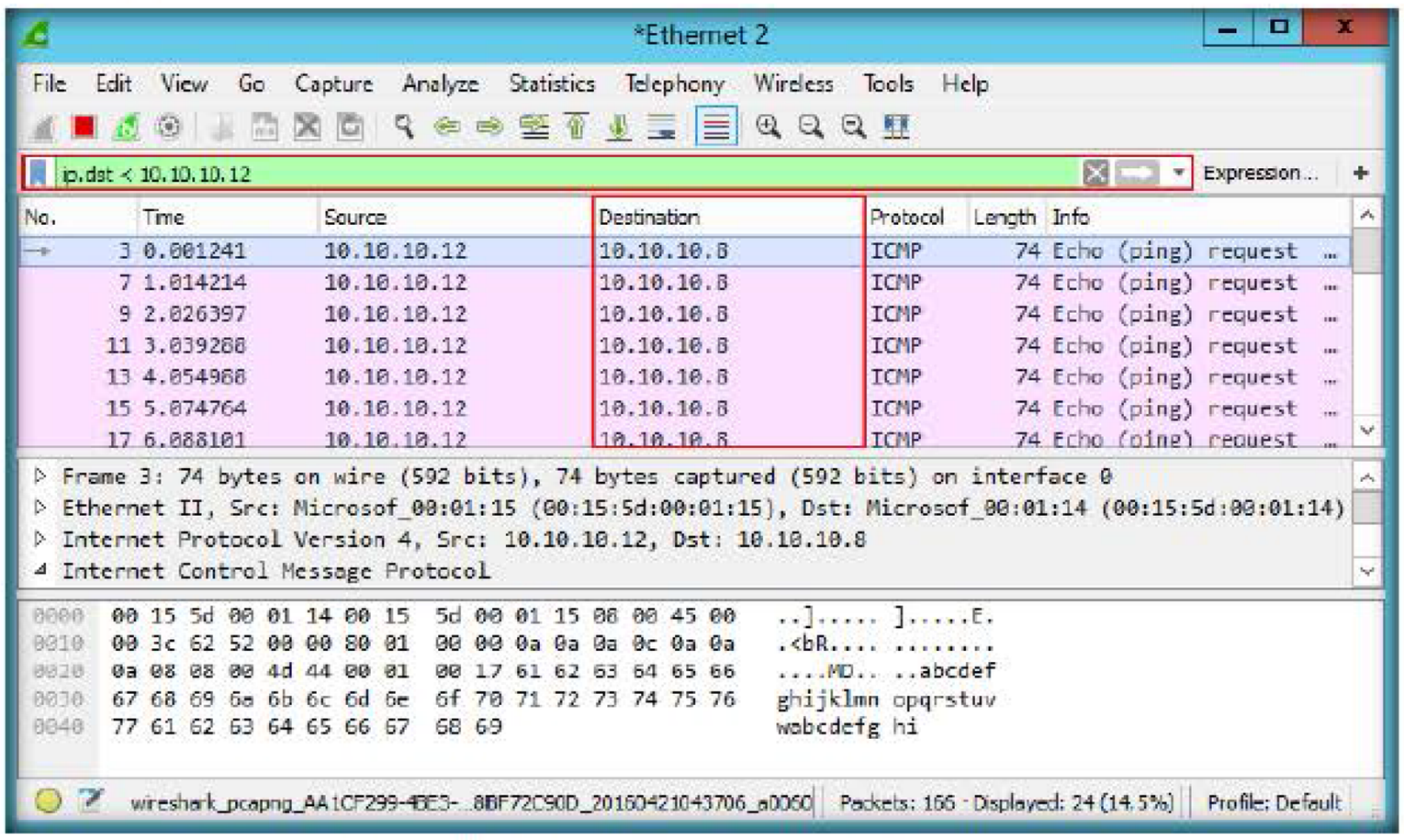



FIGURE: 2.8: Packet Filtering Using Greater Than Operator


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

14. To view traffic less than a specific IP address. Use the **<** conditional operator in conjunction with IP address filtering. Apply the filter **ip.dst < [IP Address]** to find the destination IP Addresses less than the specified IP Address.




PACKET 2.9: Packet Filtering using Less Than Operator

15. You can also filter traffic based on the source and destination port. To view traffic originating or destined to the TCP port, apply the filter **tcp.port==80**

The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type "dns" and you'll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.

**TASK 5**

**Filtering Traffic by Port Number**

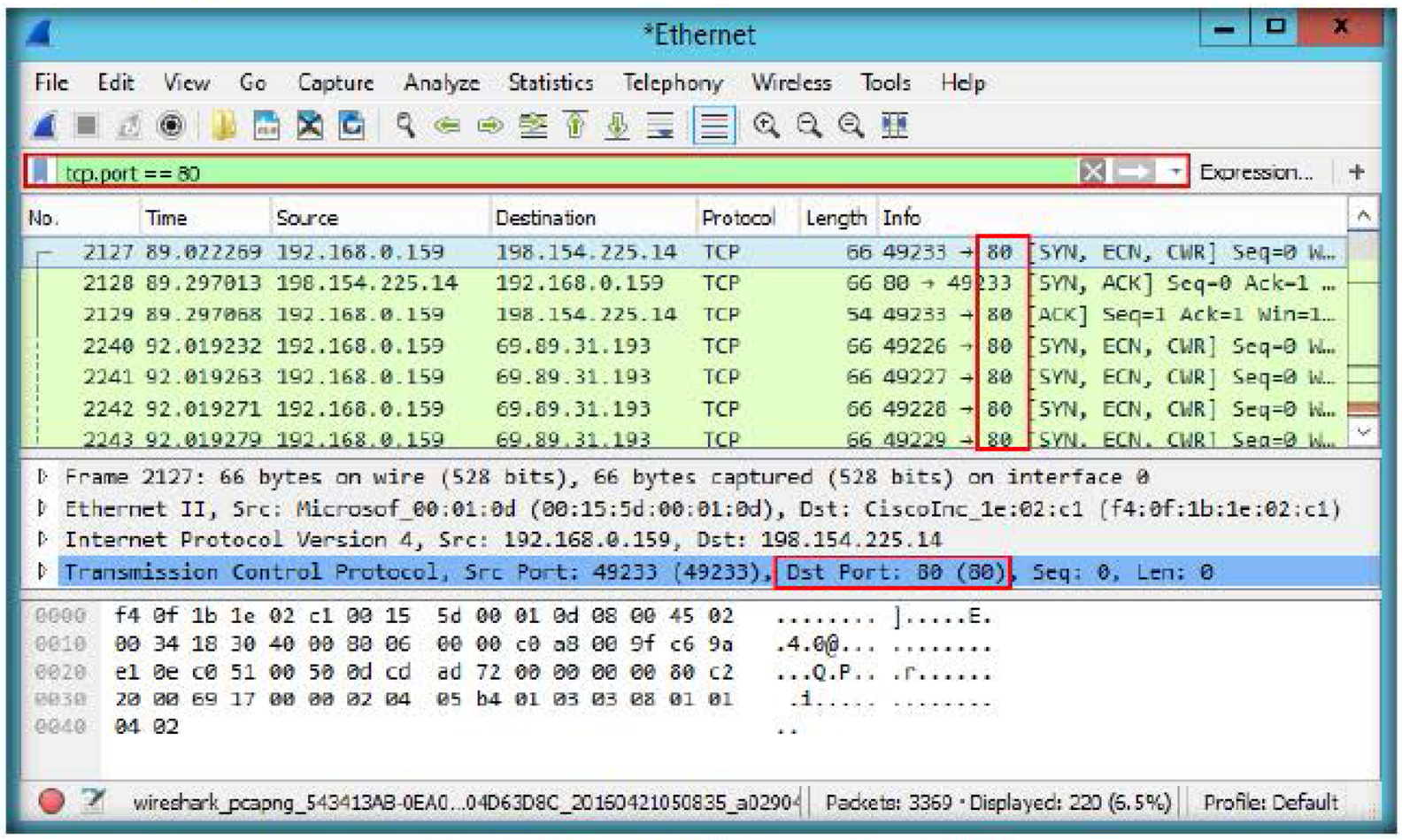



FIGURE: 2.10: Packet Filtering Based on Port Number


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

16. To view traffic originating from a specific port, apply the filter **tcp.srcport==port number**

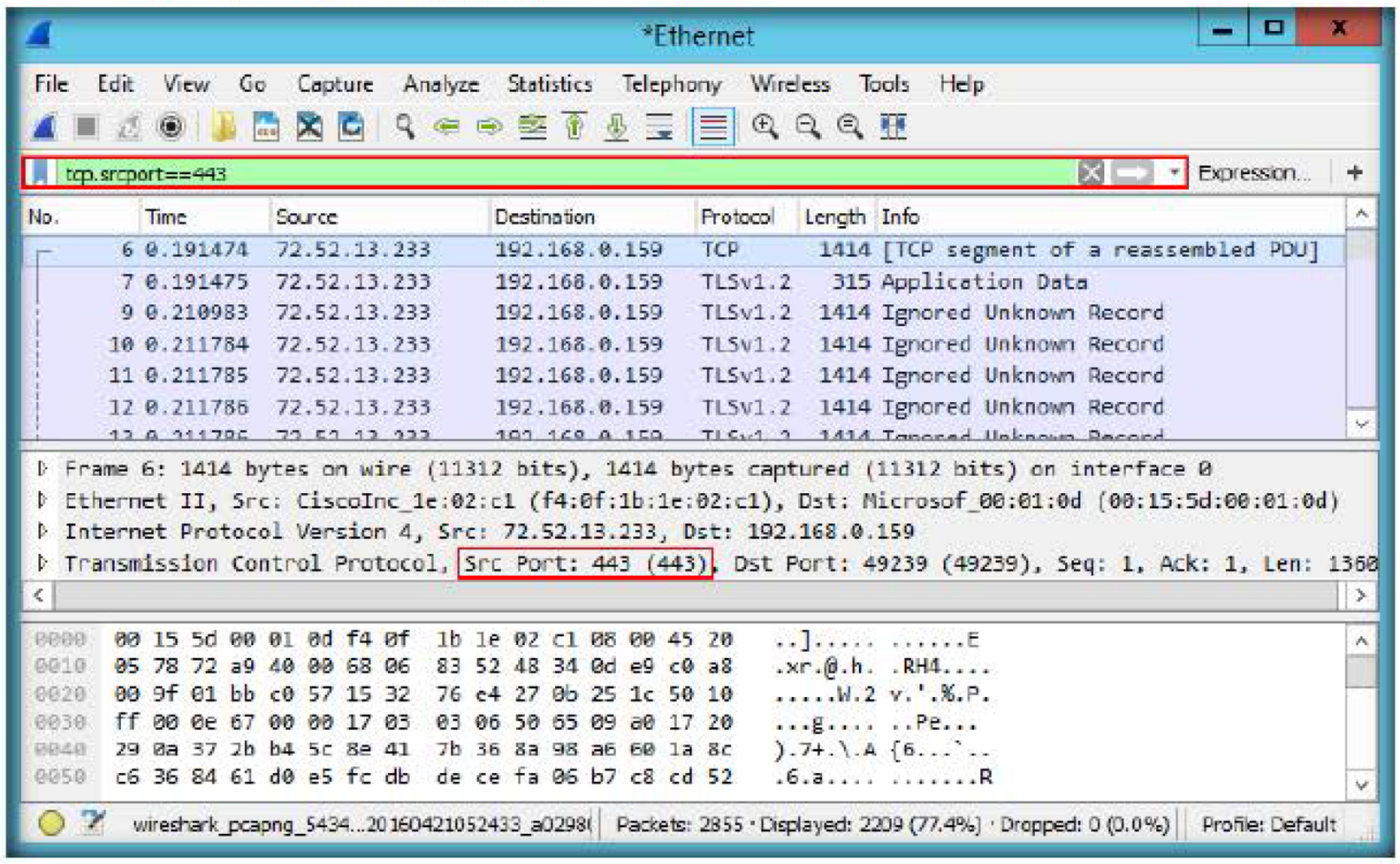



FIGURE 2.11: Packet Filtering Based on Source Port Number

17. To view traffic destined to a specific port, apply the filter **tcp.dstport==port number**

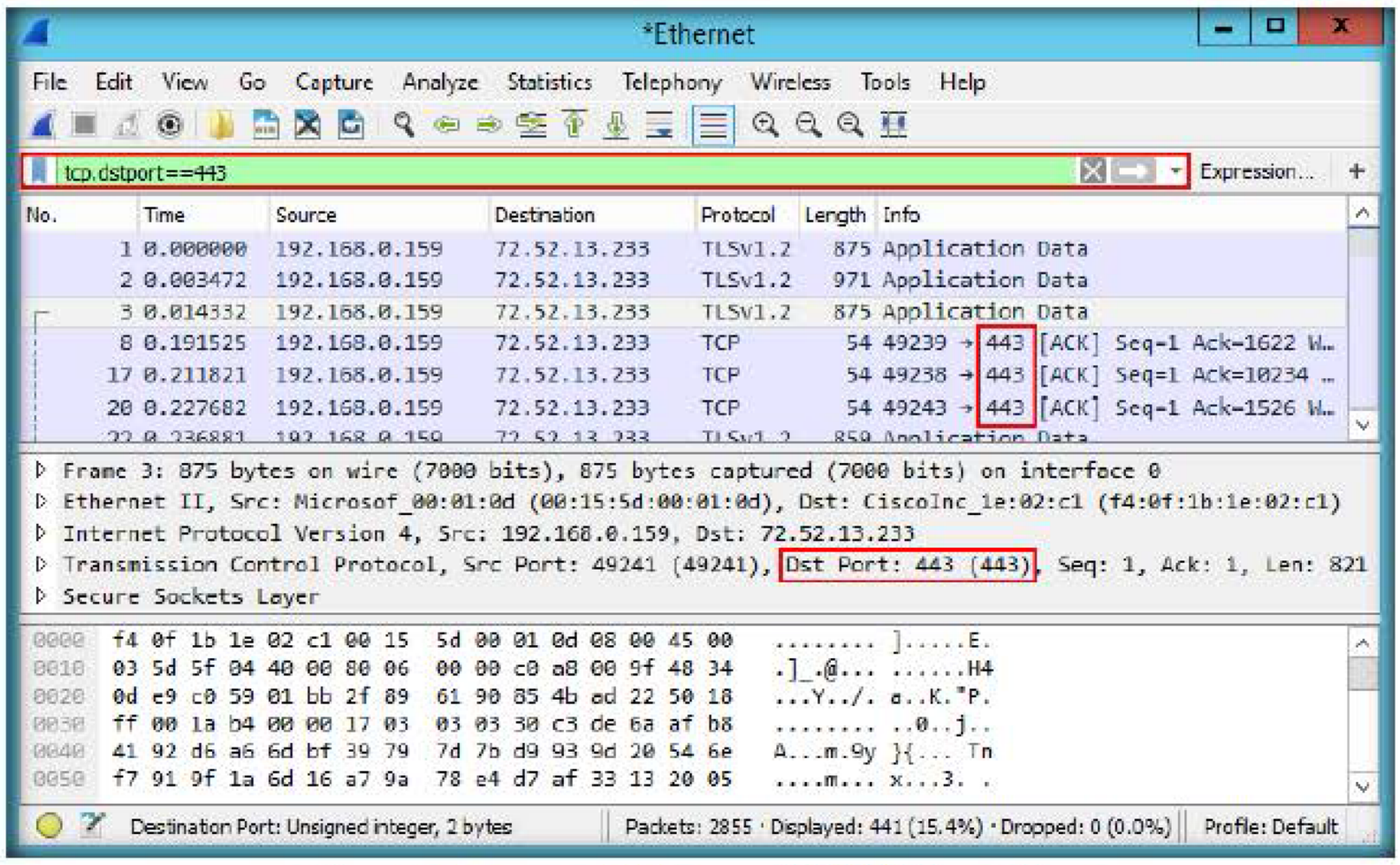



FIGURE 2.12: Packet Filtering Based on Destination Port Number


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

18. You can also use various conditional operators with the port filtering technique to filter out traffic of your interest. Apply the filter **!(tcp.port==port number)** to find the packets that are not traversing on the specified port.

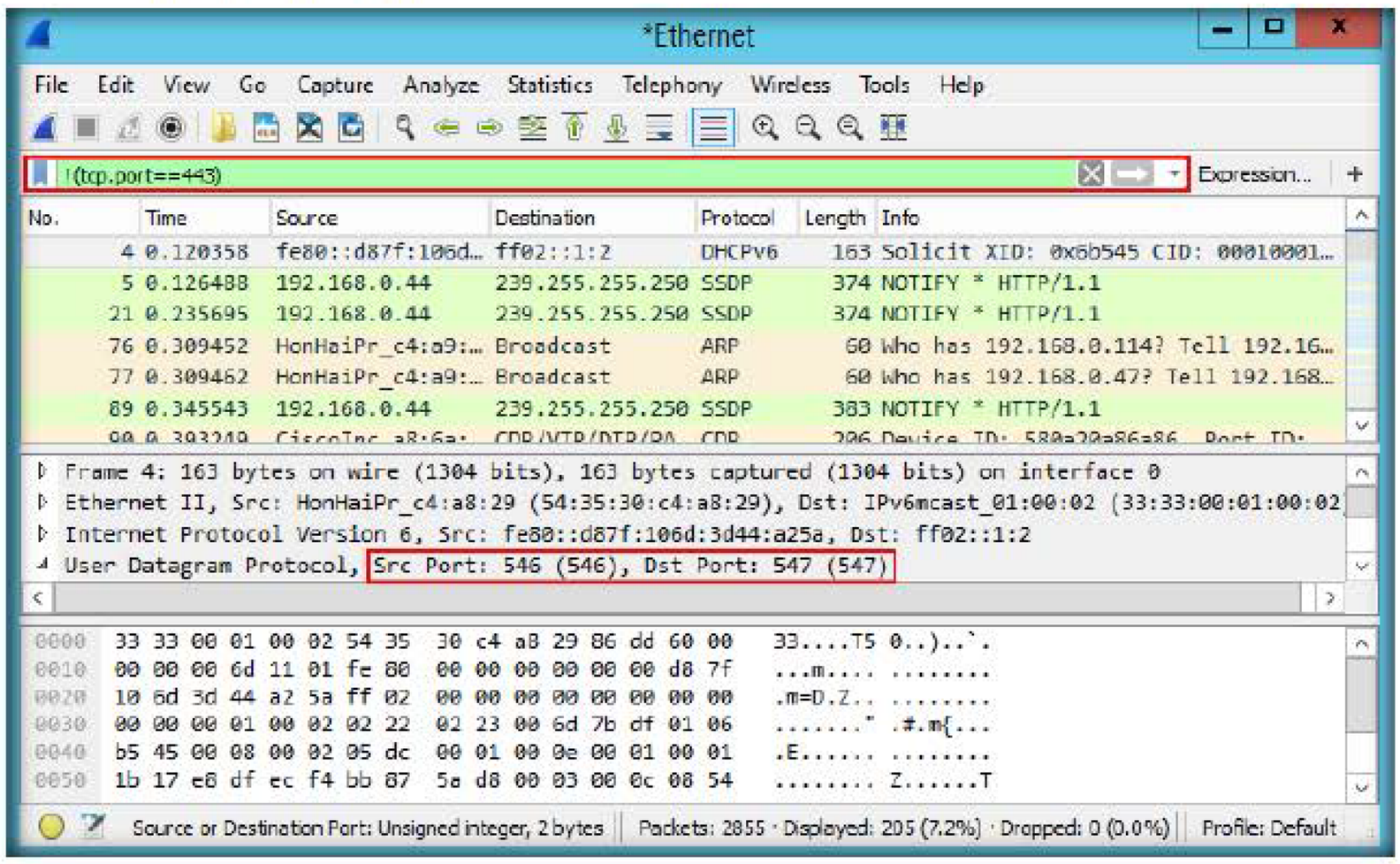



FIGURE 2.13: Packet Filtering Using the Negation Operator

19. To view traffic originating or destined to a port **greater than or equal to** a specific port, apply the filter **tcp.port>=port number**

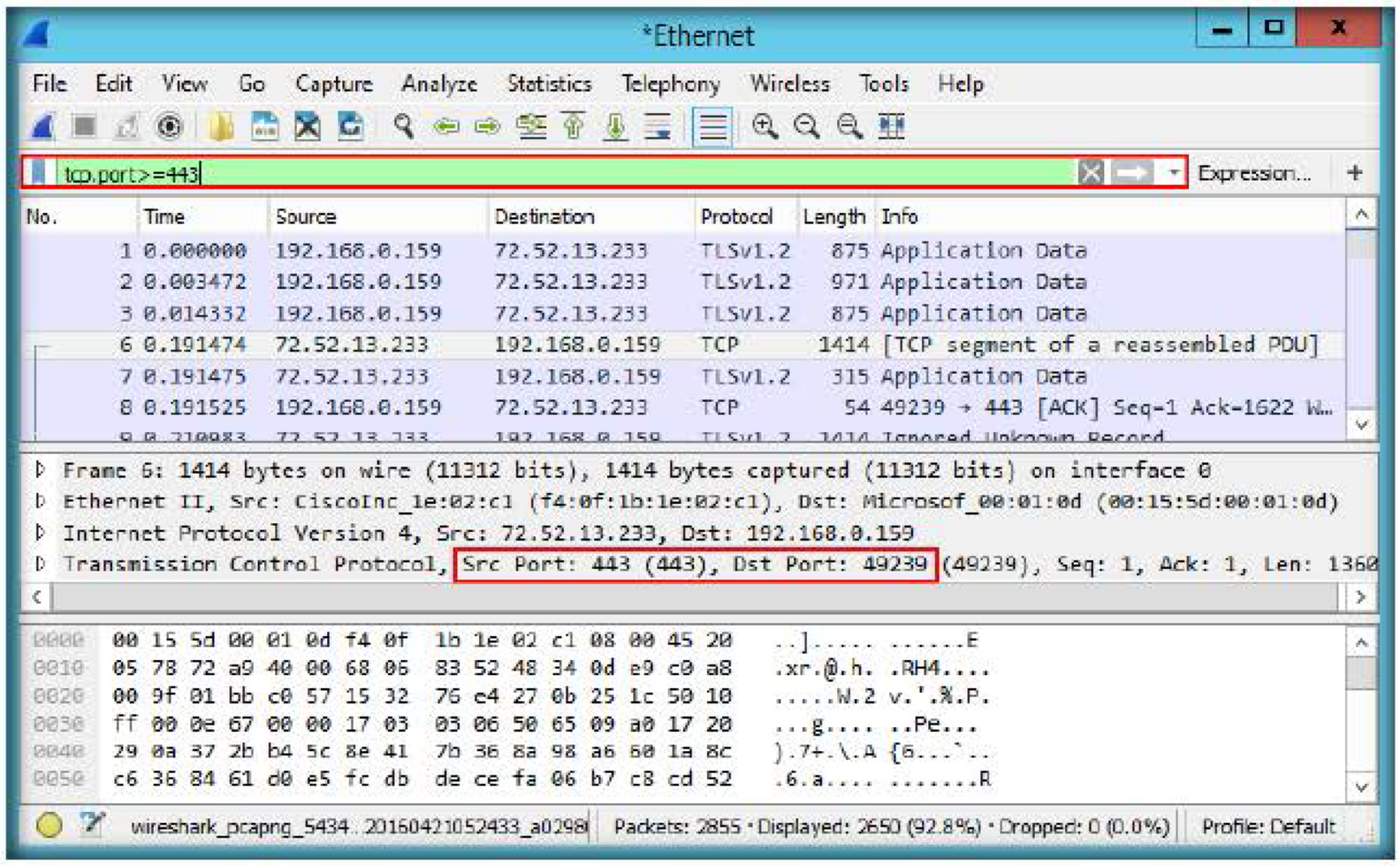



FIGURE 2.14: Filtering Using the Greater Than or Equal to Operator


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

20. To view traffic originating or destined to a port **less than or equal to** a specific port, apply the filter **tcp.port<=port number**

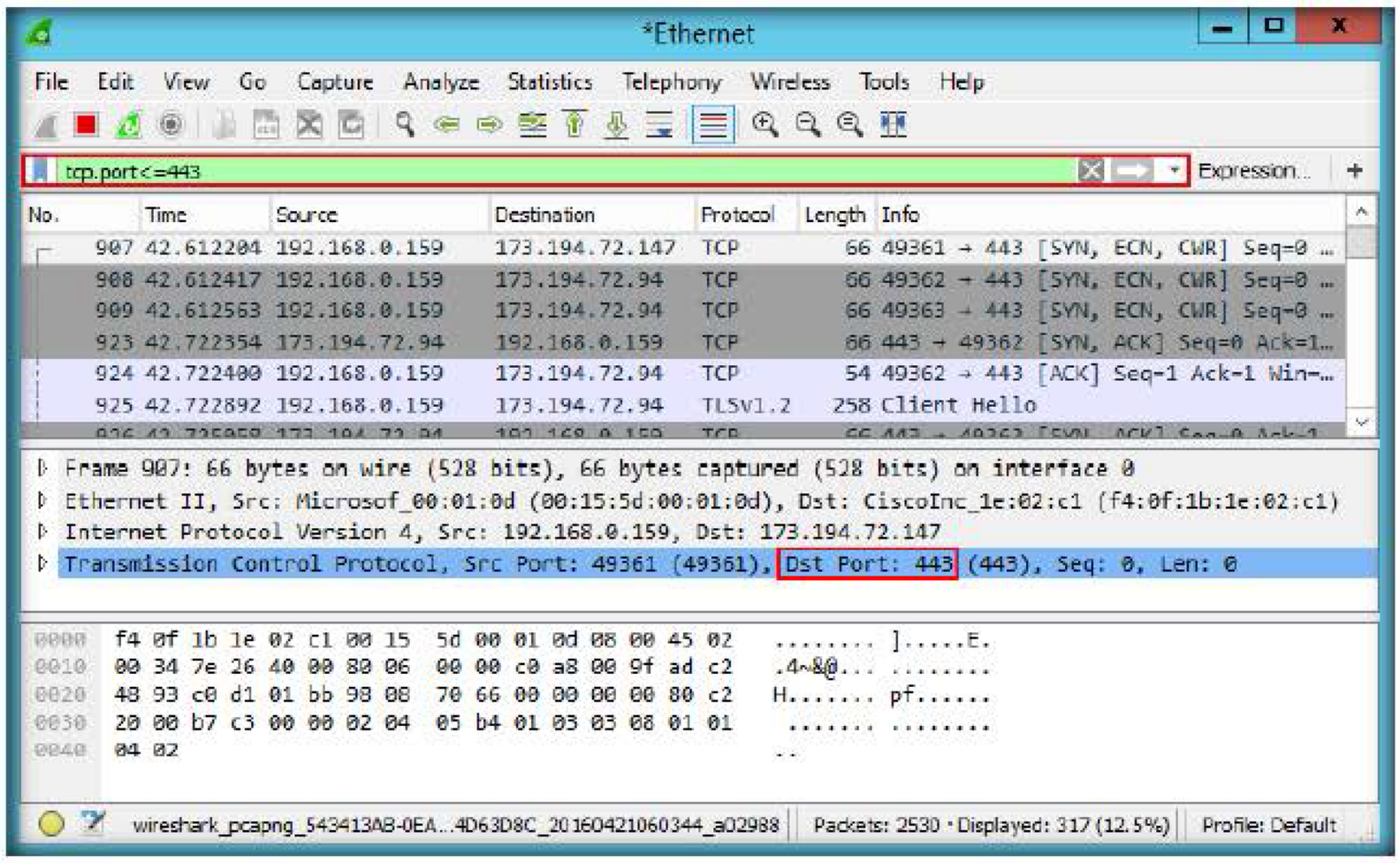



FIGURE 2.15: Filtering Packets Using less Than or Equal to Operator

**Note:** You can use various conditional operators on the port filtering technique to filter out traffic of your interest

**TASK 6**

**Filtering Traffic Using 'Contains' Keyword**

21. You can also filter traffic based on a specific string contained in the traffic. Apply the filter **http contains [string]** to filter out the traffic which contains the mentioned string.

**Note:** This can only be applied to characters and not numerical. It searches for a sequence of characters provided in the filter.

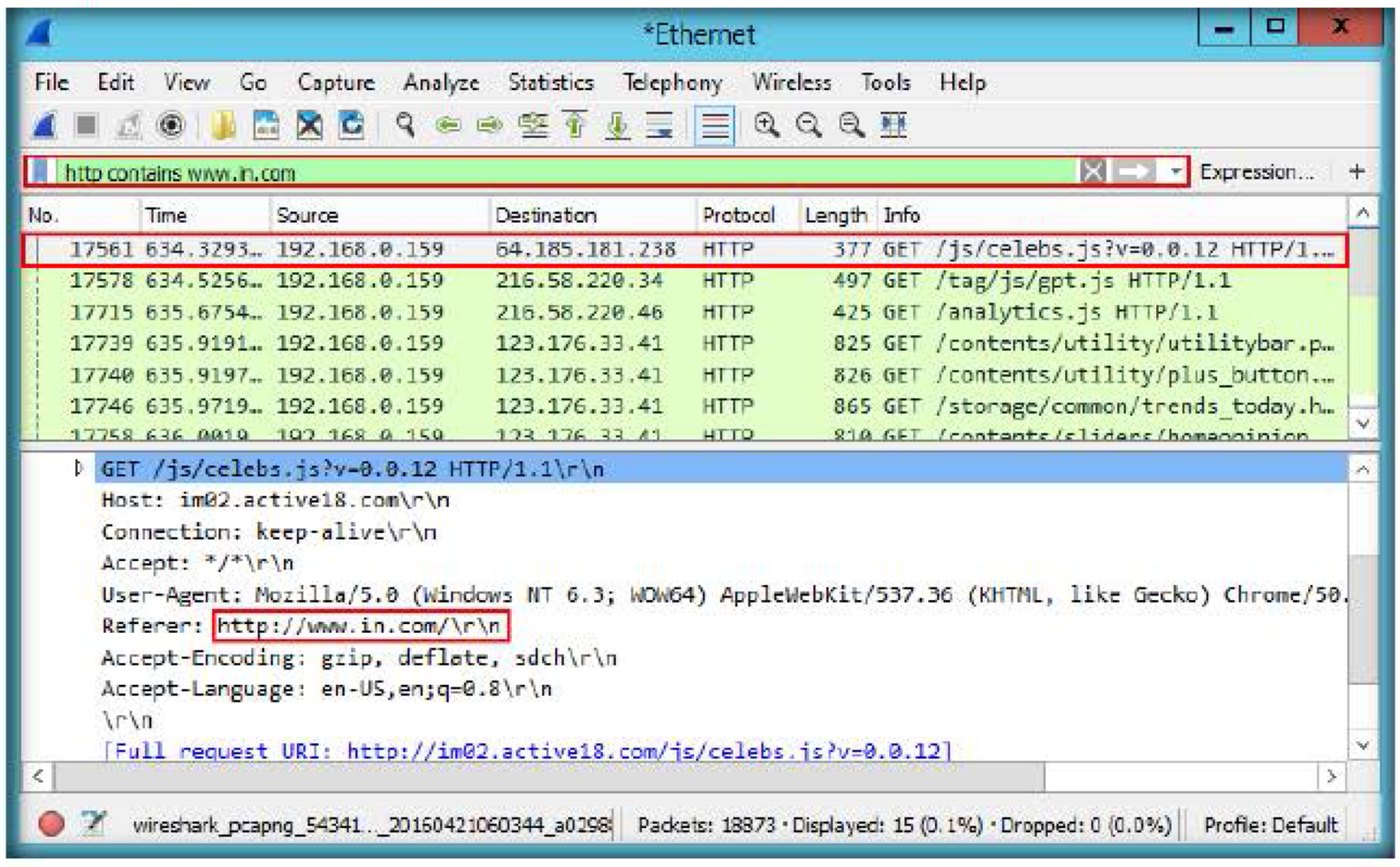



FIGURE 2.16: Filtering Packets Using the Contains Keyword



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

22. To view the HTTP traffic whose request header fields (**referrer or host**) contain a specific string, apply **http.referer contains [string]** or **http.host contains [string]** filter

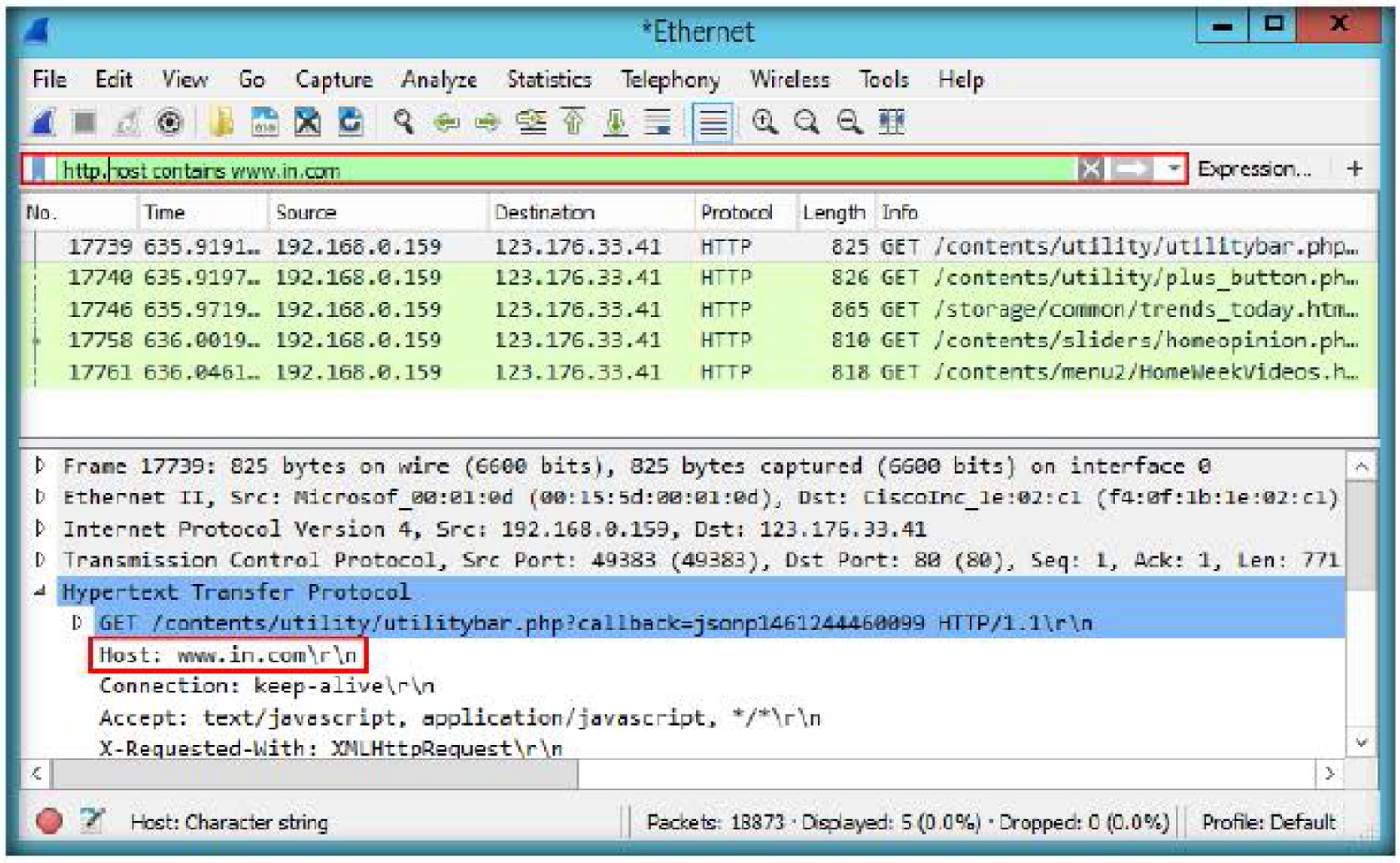



FIGURE 2.17: Filtering Packets Using Host Field and Contains Keyword

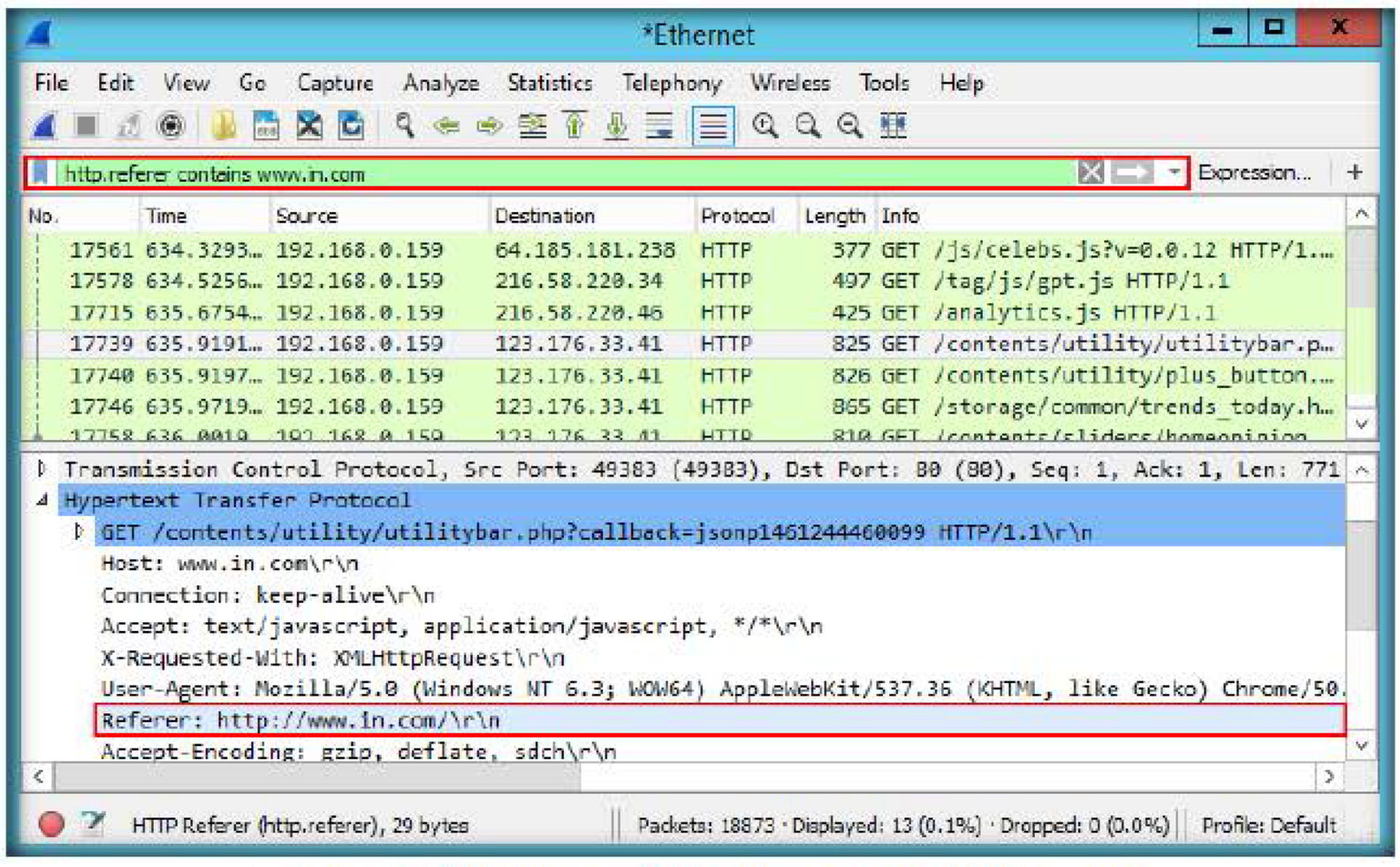



FIGURE 2.18: Filtering Packets Using Referer Field and Contains Keyword



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

**TASK 8**

**Filtering Traffic Using 'matches' Keyword**

23. You can also filter traffic based on a specific pattern contained in the traffic. Apply the filter **http.accept matches [pattern]** to filter out the traffic which contains an exact pattern. It matches the sequence of exact characters in a pattern with the traffic.

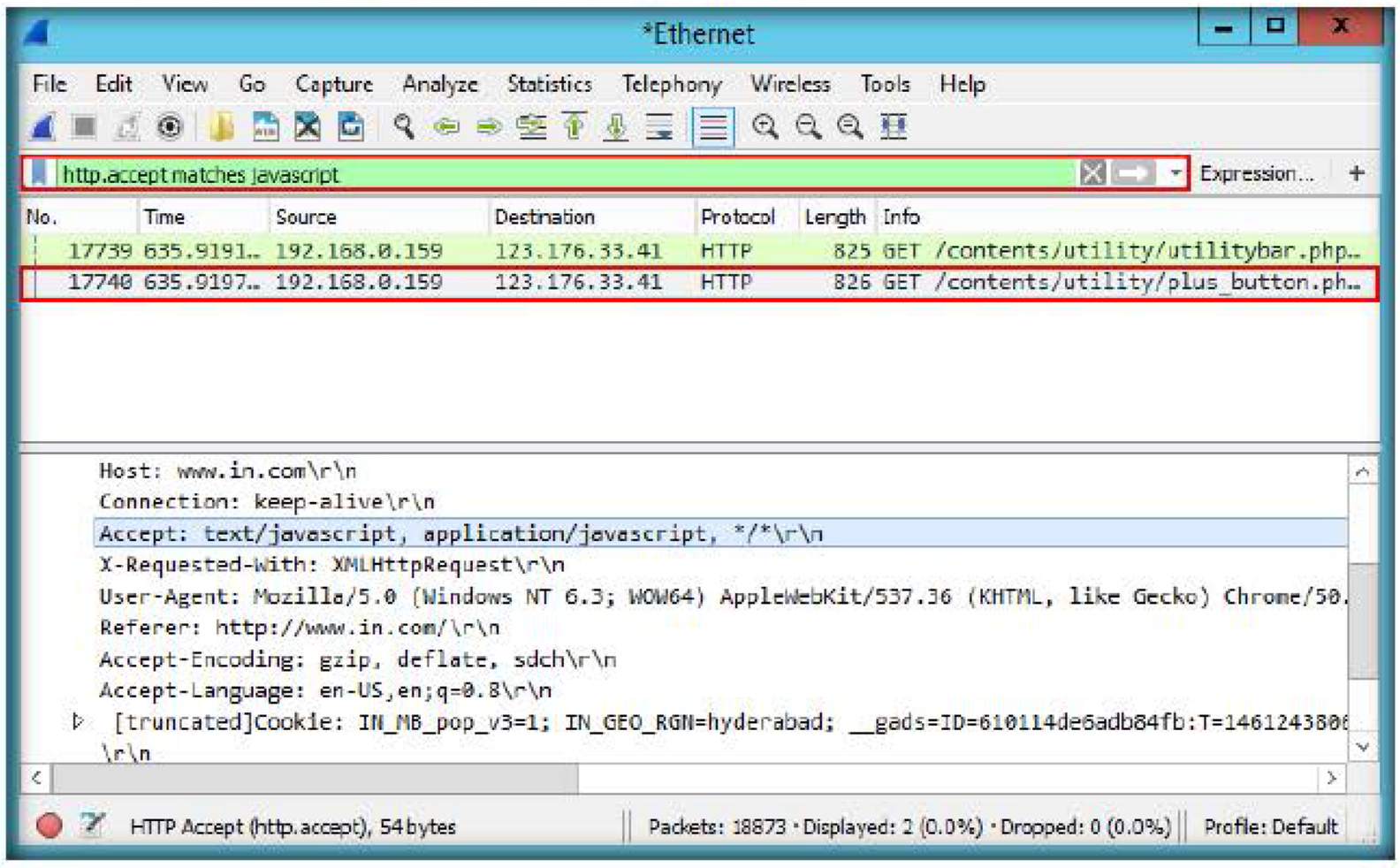



FIGURE 2.19: Filtering Using the Matches Keyword

**TASK 9**

**Filtering Traffic Using Membership Operator**

24. To view traffic originating from a specific set of IP addresses, apply the membership operator **ip.src in {[IP Address 1] [IP Address 2] [...]}** to filter traffic of your interest. It allows you to compare IP address fields with a set of values.

**TASK 10**

**Filtering traffic based on TCP flag**

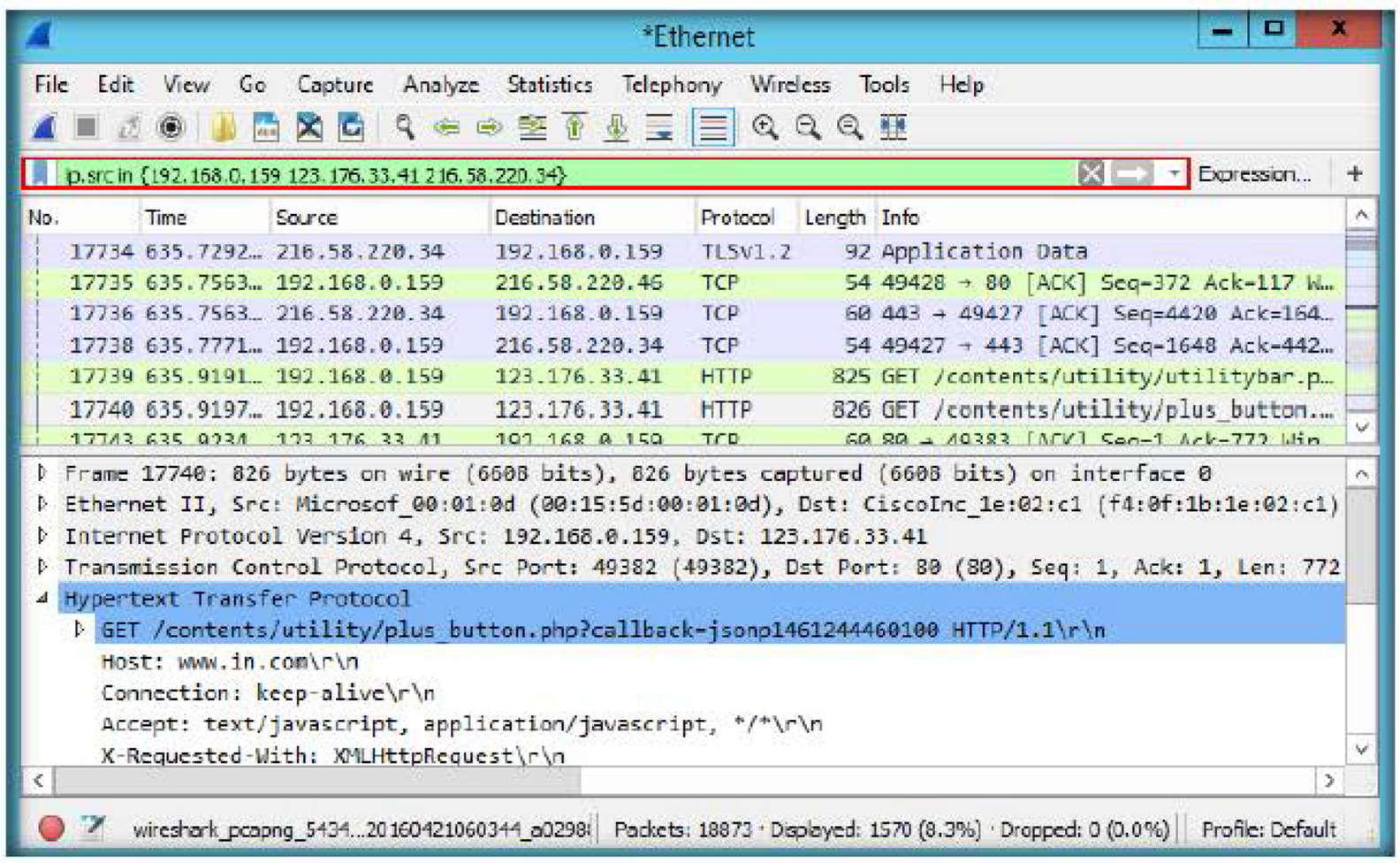



FIGURE 2.20: Filtering Packets using Membership Operator



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

25. To view the TCP traffic with a specific TCP flag set, apply the filter **tcp.flags & [flag code]**. (Here flag code 0x012 denotes packets with the SYN and ACK bits set, or SYN or ACK bits set)

**Note**: Similarly, you may use the flag code 0x002 to check packets with a SYN flag set and flag code 0x010 to check packets with an ACK flag set. Use the appropriate code for any respective flag packets.

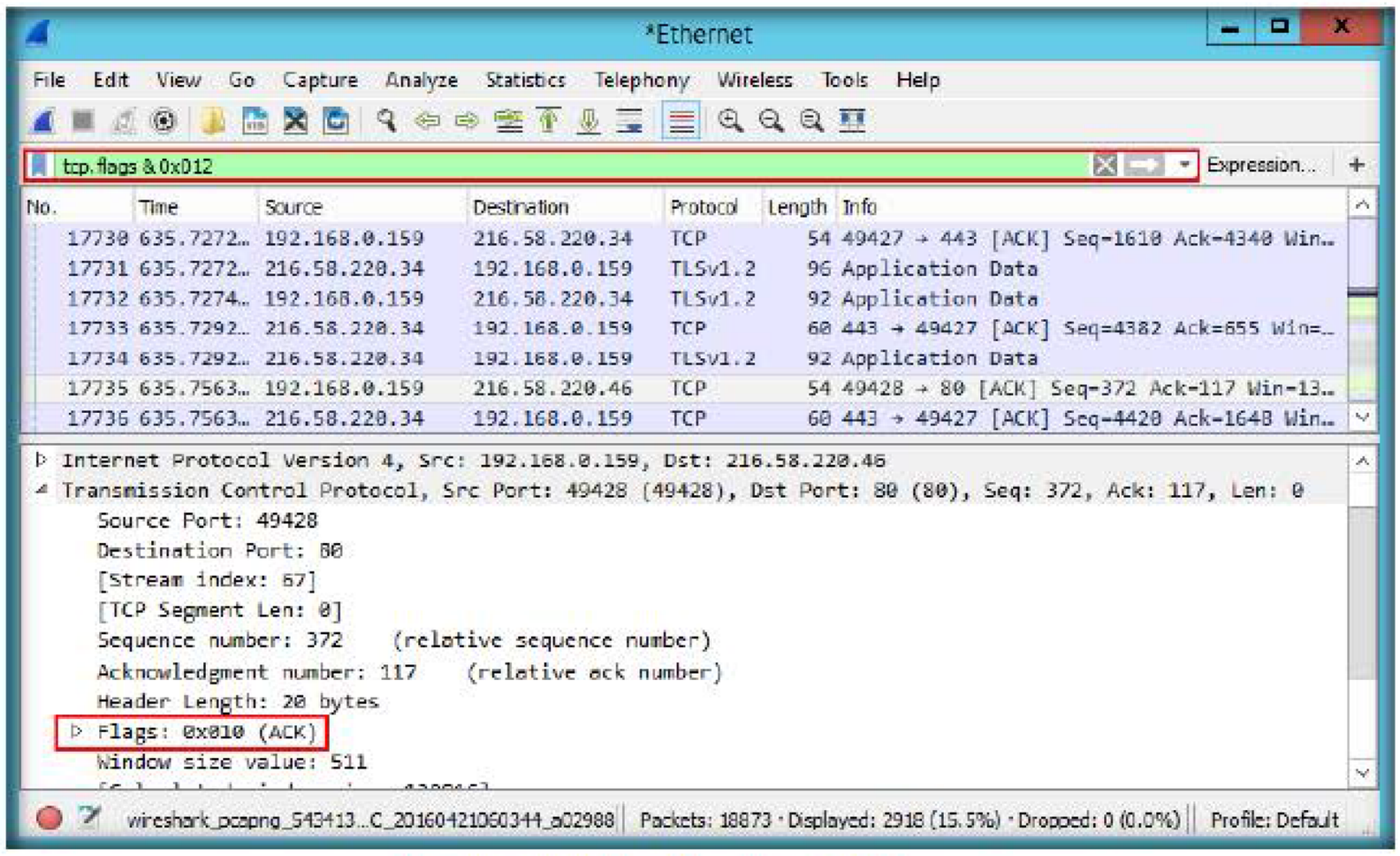



FIGURE 2.21: Filtering Using the Bit Field Operator

26. You can also view the Wireshark filters in conjunction using one or more logical operators to view traffic of interest.

**TASK 11**

**Filtering Traffic Using Logical Operators**

27. For instance, to view the TCP traffic with a sequence number of 2841 and length 1107, apply the **tcp.seq==1 && tcp.len==1380** filter

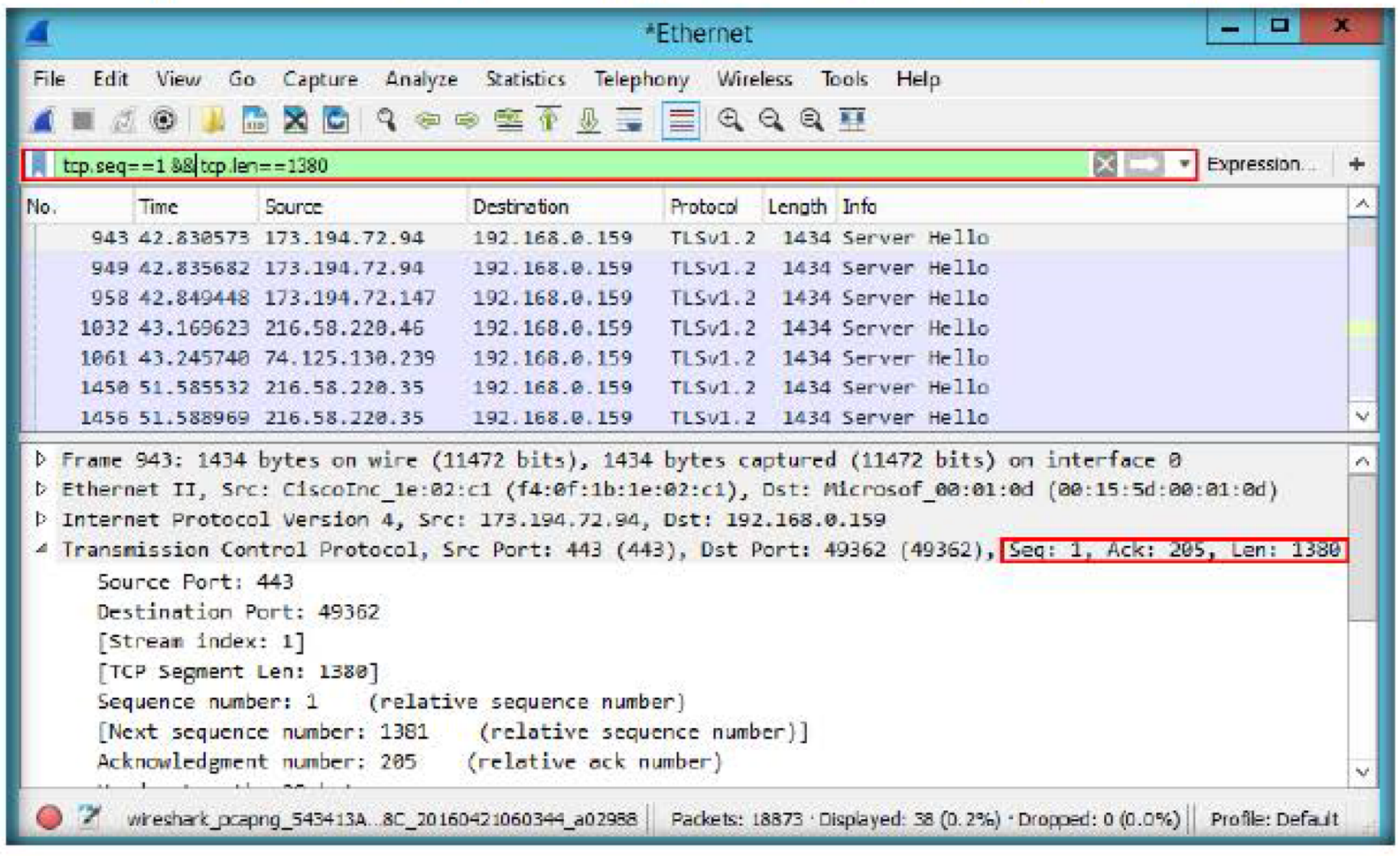



FIGURE 2.22: Filtering Using Logical AND Operator



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

28. You can specify one or more conditional and logical operators to find the traffic of your interest.

    For example, you can apply an ICMP based filter to filter traffic originating and destined to a specific IP address with a request type of 8 and checksum value 0x4d53. Apply the following **icmp.type==8 && icmp.checksum==0x4d53 && ip.src==[source IP address] && ip.dst==[Destination IP address]** filter to view only those ICMP packets.

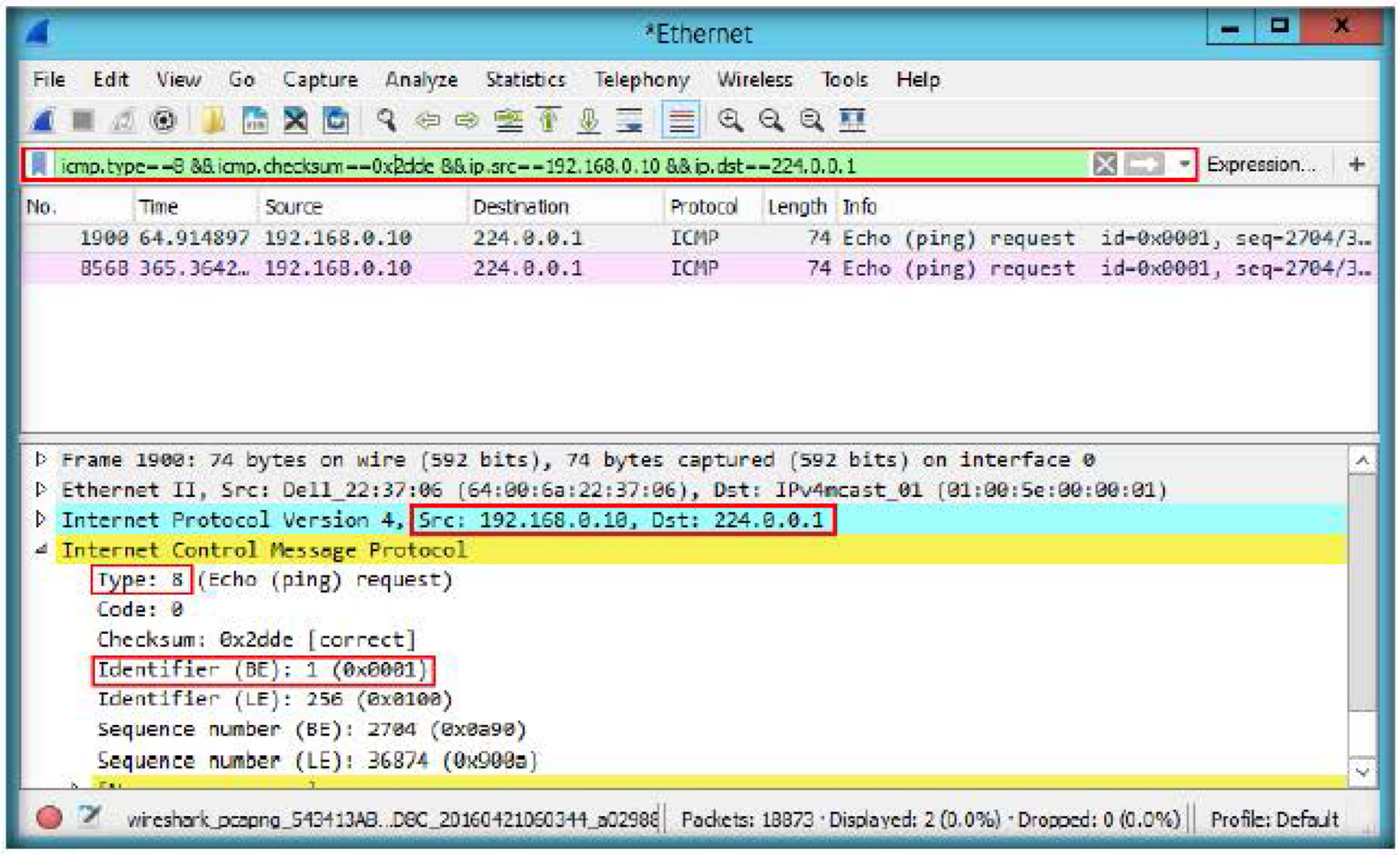



FIGURE 2.23: Using Logical AND With More Than two Operators

29. Similarly, you can use a **Logical OR operator**. To check the number of packets which are **referencing a particular URL** or are **referred by a particular URL**, browse a website of your choice, here **http://www.in.com**, and apply **http.user_agent==[URL] or http.host==[URL]**

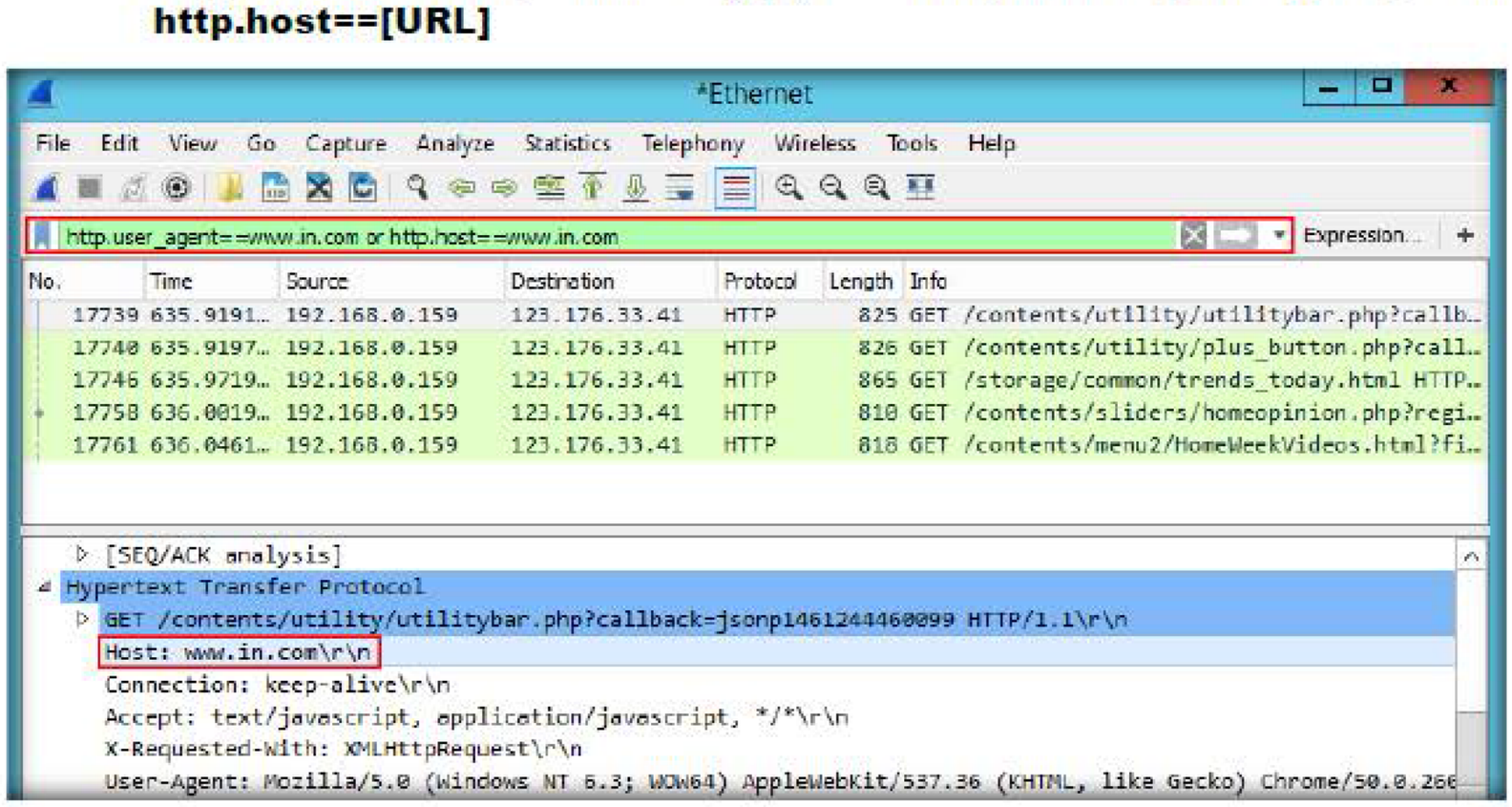



FIGURE 2.24: Packet Filtering Using OR Operator



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

30. Thus, Wireshark allows you to use a wide range of filters to filter traffic per your interest

## 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 |


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

Lab 3

# Detecting Clear-Text Traffic using Wireshark

*Wireshark is a network packet analyzer, which is used to capture network packets and display packet data in detail.*

ICON KEY

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

## Lab Scenario

Some of the applications allow their users to communicate through protocols like HTTP, FTP, Telnet, etc. These protocols transfer data over TCP in clear text format, which can be easily understood by someone eavesdropping on the network. As a network defense architect, you need to know how to determine if there is any sensitive information (such as user credentials) flowing through the network.

## Lab Objectives

The objective of this lab is to help students learn how to:

- Detect sensitive data flowing through the network in clear text format

## Lab Environment

To perform the lab, you need:

- Cain & Abel located at **Z:\CND-Tools\CND Module 11 Network Traffic Monitoring and Analysis\ARP Poisoning Tools\Cain&Abel**
- You can also download the latest version of Cain & Abel from the link http://www.oxid.it/cain.html
- Wireshark, located at **Z:\CND-Tools\CND Module 11 Network Traffic Monitoring and Analysis\Packet Sniffing Tools\Wireshark**
- You can also download the latest version of Wireshark from the link https://www.wireshark.org/download.html
- If you decide to download the latest version, then screenshots shown in the lab might differ
- A virtual machine running Windows Server 2012



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

- A virtual machine running Windows Server 2008
- A virtual machine running Windows 10
- A Web browser with Internet connection
- **Administrative** privileges to run tools

## Lab Duration

Time: 25 Minutes

## Overview of Lab

Packet capture means intercepting data packets traversing over a network using packet capture tools such as Wireshark. These captured packets are analyzed in order to determine whether proper network security policies are being followed.

## Lab Tasks

**TASK 1**

**Clear-text HTTP Traffic**

1. Since this is a test environment, there is no SPAN port to enable Wireshark to capture traffic flowing throughout the network. So, we shall perform ARP Poisoning using the Cain & Abel application, to enable Wireshark to capture traffic between the required machines.
2. Log on to Windows Server 2012 virtual machine.
3. Navigate to **Z:\CND-Tools\CND Module 11 Network Traffic Monitoring and Analysis\ARP Poisoning Tools\Cain&Abel** and double-click **ca_setup.exe**.
4. If the **Open File - Security Warning** pop-up appears, click **Run**.


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

5. Follow the wizard-driven installation steps to install Cain & Abel.

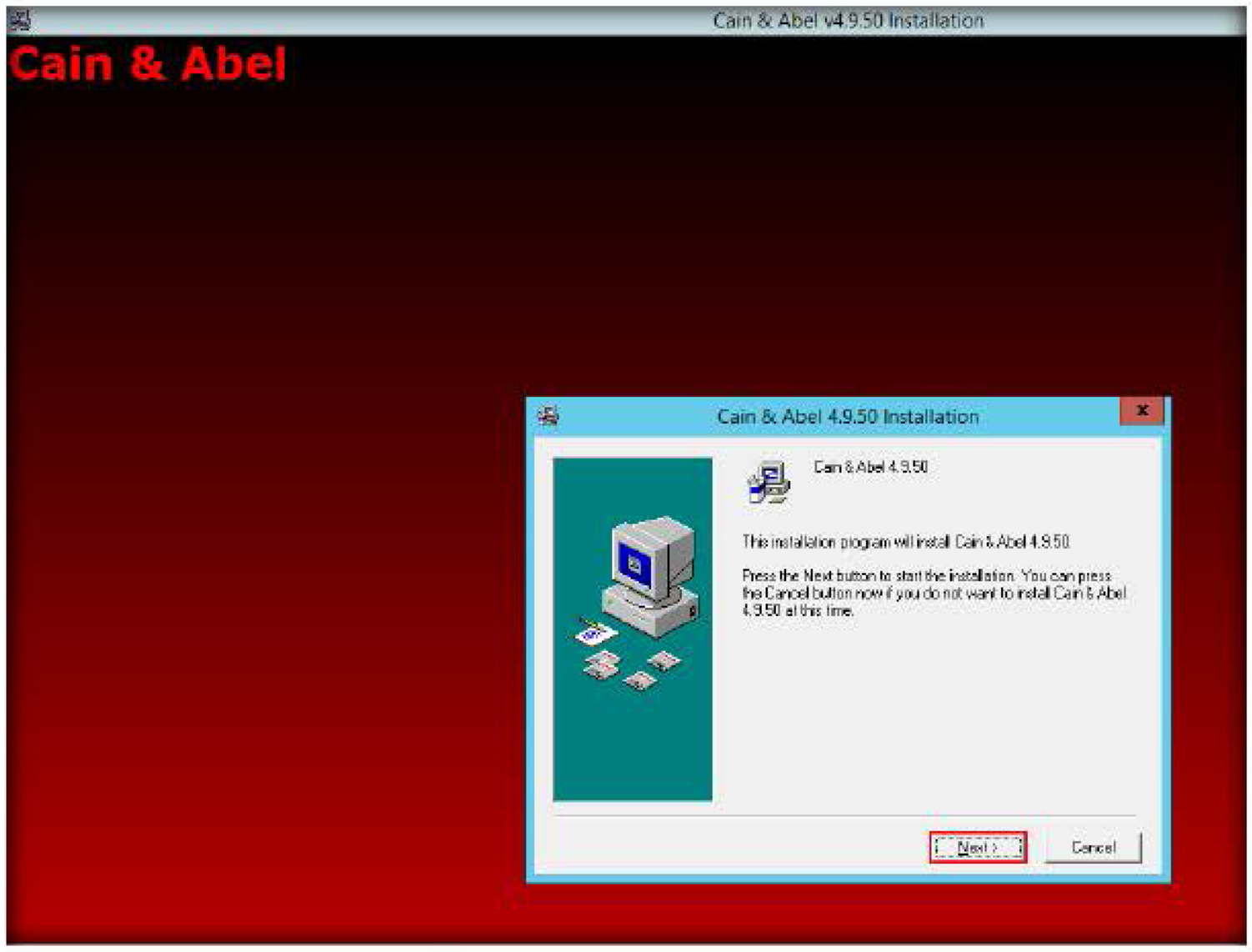



FIGURE 3.1: Cain & Abel installation

6. The **WinPcap Installation** pop-up appears; click **Don't install,** as you have already installed it during the lab setup.

Man in the Middle attack has the potential to eavesdrop on a switched LAN to sniff for clear-text data (McClure, Scambray). It can also be used for substitution attacks that can actively manipulate data.




FIGURE 3.2: WinPcap Installation pop-up

7. Launch the **Windows Server 2008** and **Windows 10** virtual machines.


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

8. Switch back to the Windows Server 2012 virtual machine, and launch **Cain & Abel** from the **Apps** screen.

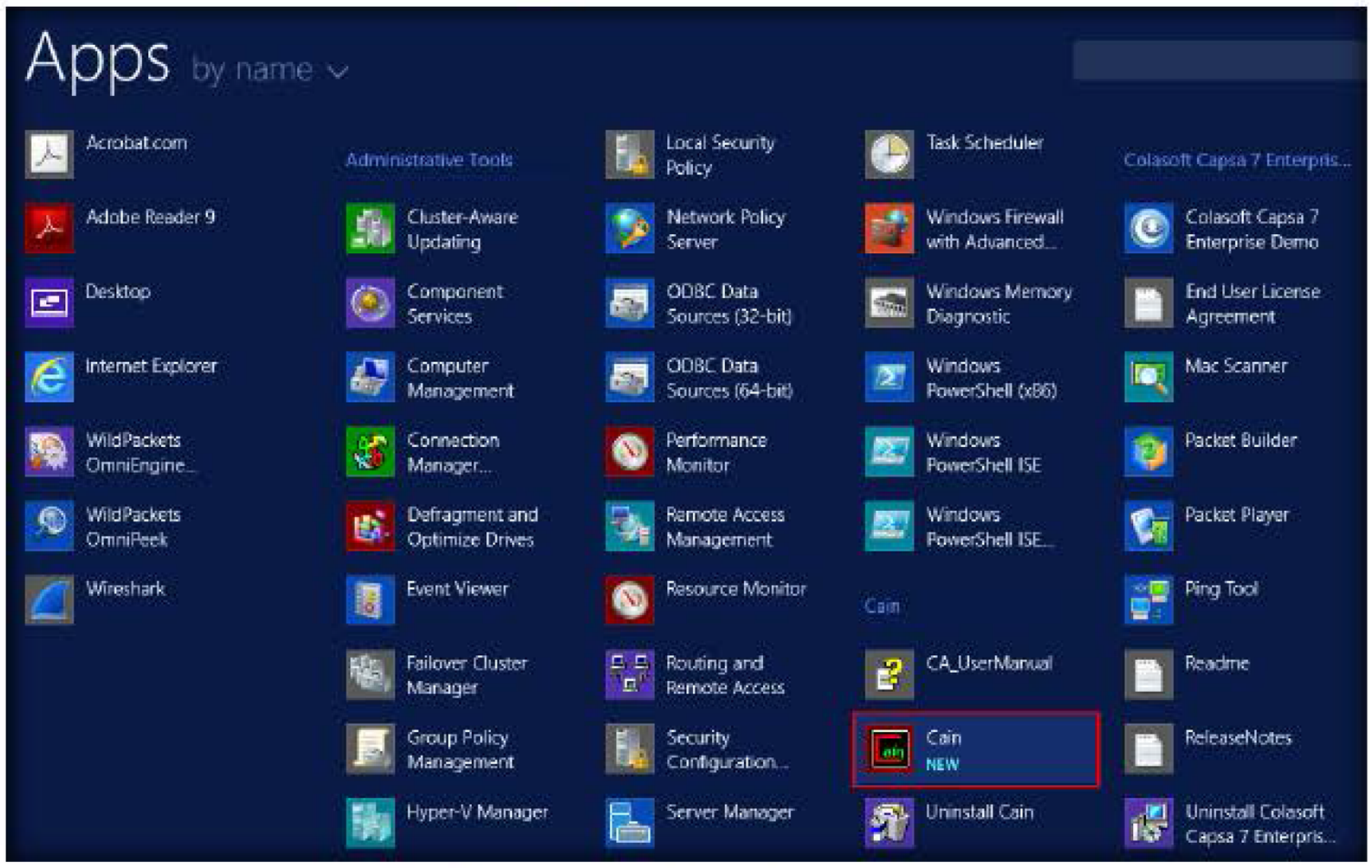



FIGURE 3.3: Launching Cain & Abel from Apps screen

9. If a **Cain** pop-up appears, click **OK**.

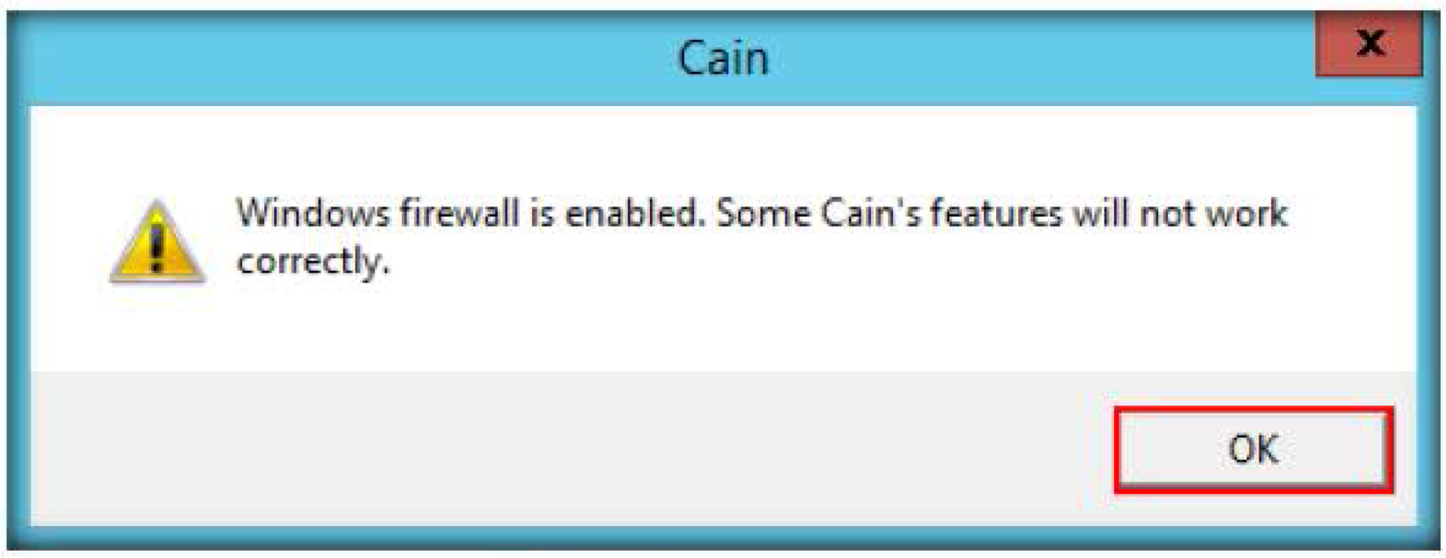



FIGURE 3.4: Cain pop up window


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

10. The main window of Cain & Abel appears as shown in the screenshot:

Cain & Abel covers some security aspects/weakness intrinsic of protocol's standards, authentication methods and caching mechanisms.

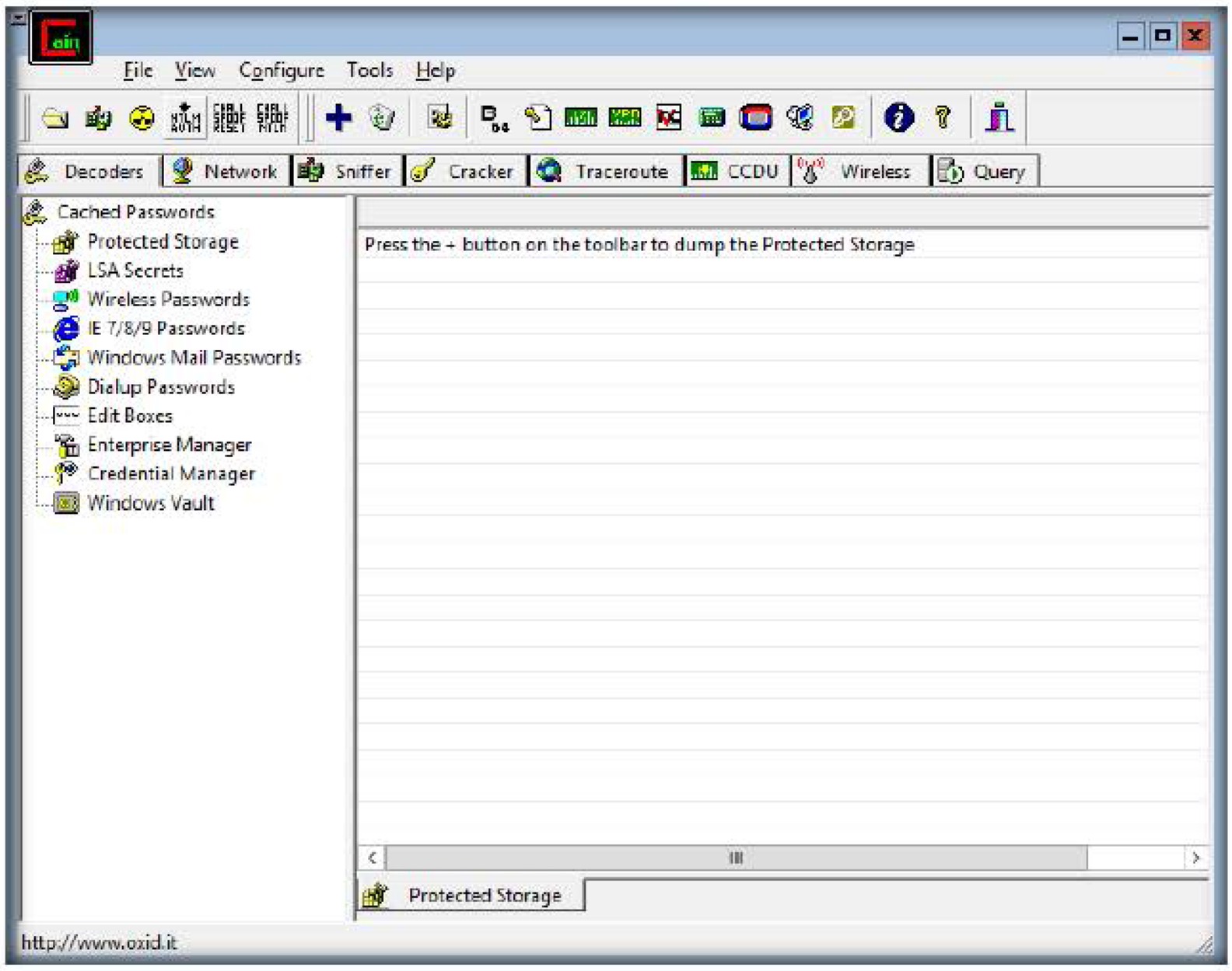



FIGURE 3.5: Cain & Abel Main Window

11. To configure the **Ethernet card**, click **Configure** from the menu bar.

APR-SSH1 can capture and decrypt SSH version 1 session that are then saved to a text file. APR-HTTPS can intercept and forge digital certificates on the fly but because the trusted authority does not sign these certificates a warning message will be displayed to the end user.

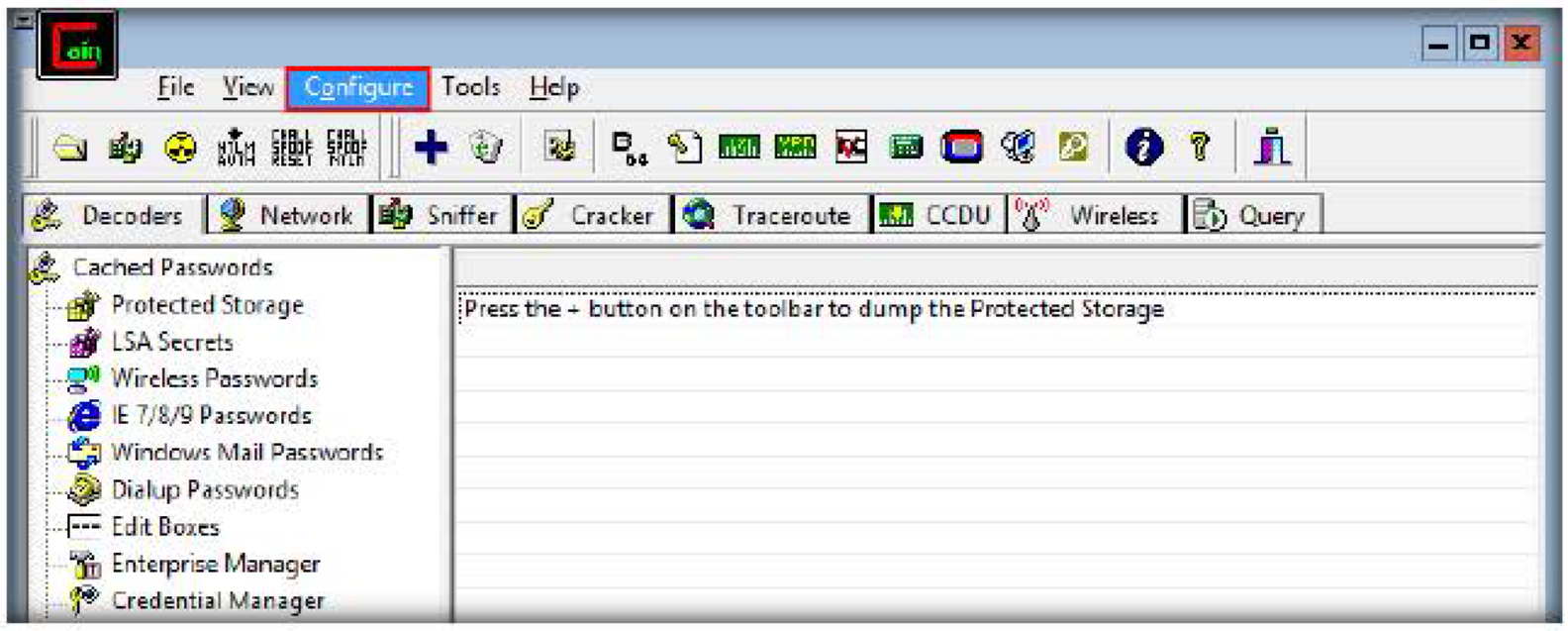



FIGURE 3.6: Cain & Abel Configuration Option


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

12. The **Configuration Dialog** window appears.
13. The window consists of several tabs. Click the **Sniffer** tab to select the sniffing adapter.
14. Select the **Adapter** associated with the IP address 10.10.10.* subnet, click **Apply**, and then click **OK**.

Replay attacks can also be used to resend a sniffed password hash to authenticate an unauthorized user.

For IP and MAC spoofing you have to choose addresses that are not already present on the network. By default Cain uses the spoofed MAC "001122334455" for two reasons: first that address can be easily identified for troubleshooting and second it is not supposed to exist in your network.

**Note**: You cannot have two or more Cain machines on the same Layer-2 using APR's MAC spoofing and the same Spoofed MAC address.

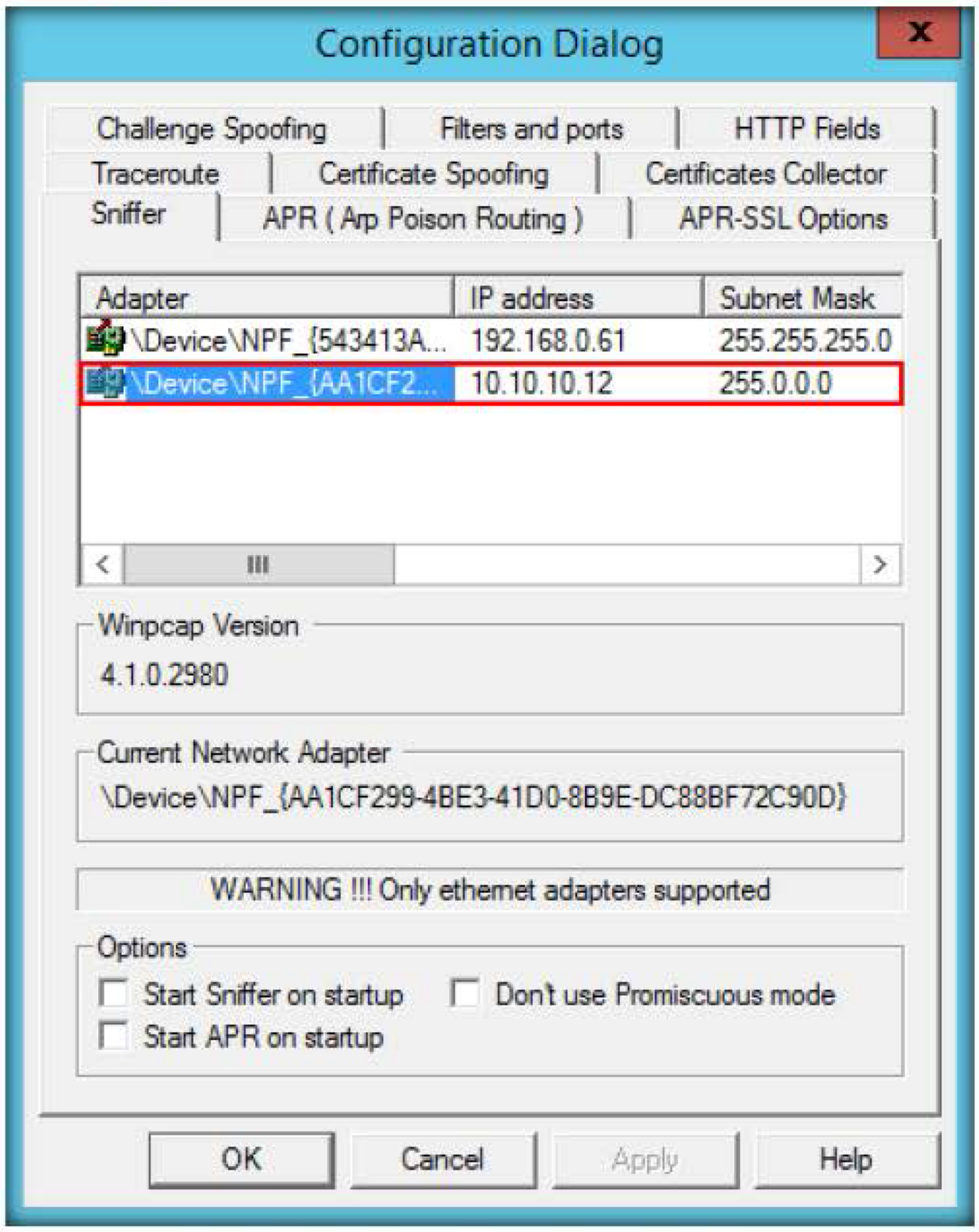



FIGURE 3.7: Cain & Abel Configuration Dialog Window

15. Click **Start/Stop Sniffer** on the toolbar to begin sniffing.

The most crucial item in that list is the radioactive hazard APR. It is in this window that we select our victim(s).

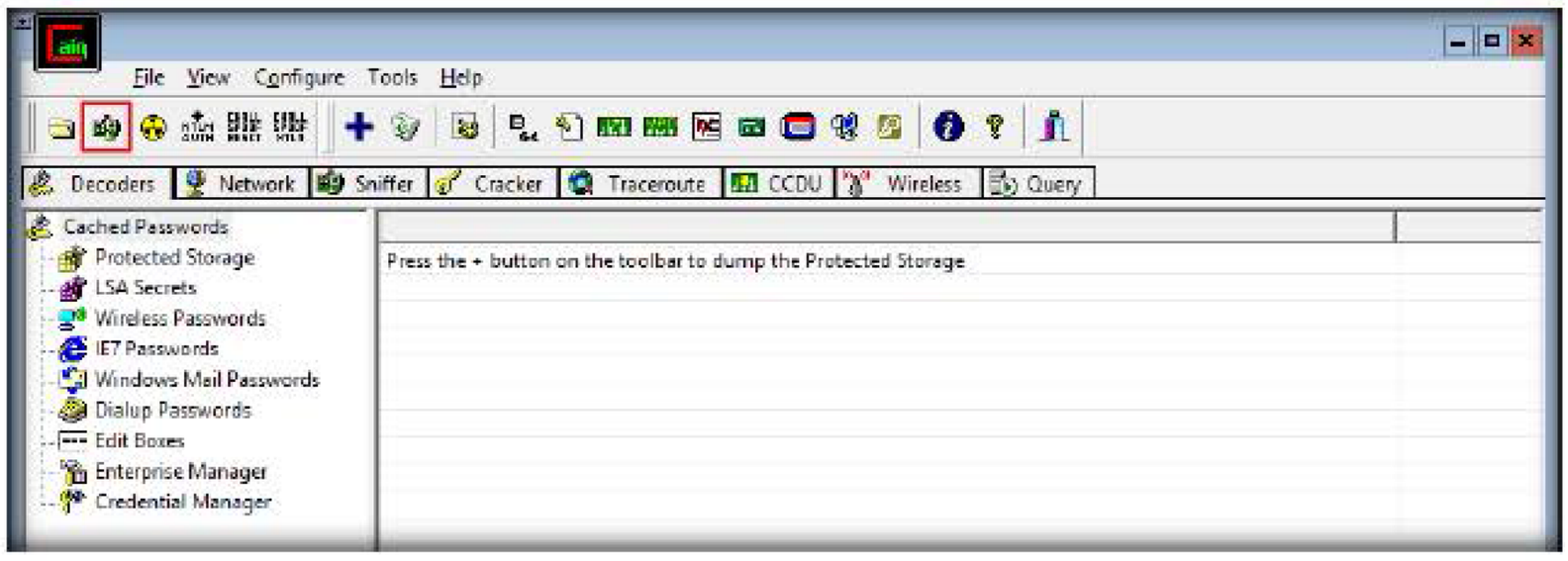



FIGURE 3.8: Starting a sniffer


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

Note: If the **Cain** Warning pop-up opens, click **OK**.

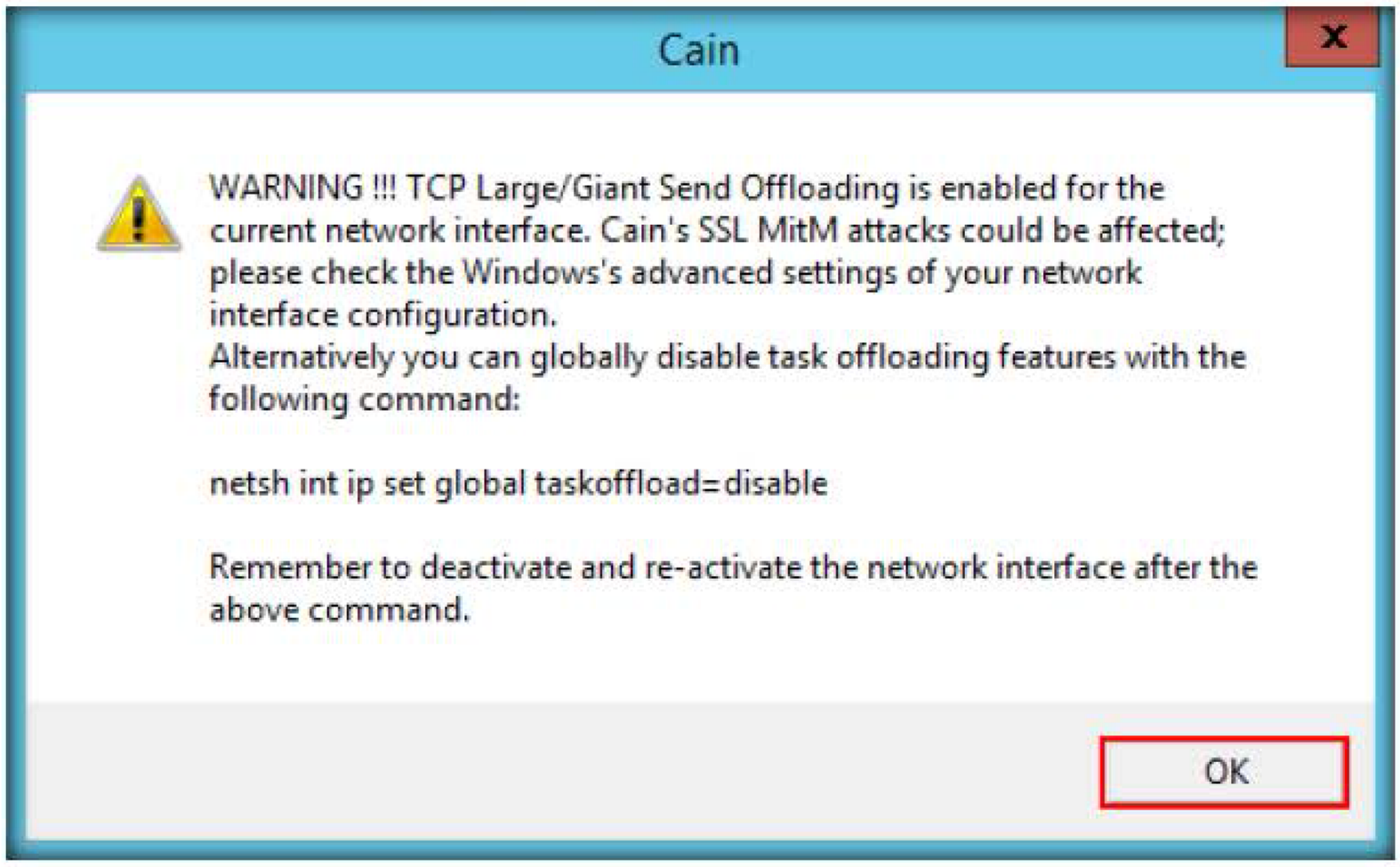



FIGURE 3.9: Cain Warning pop-up

Be warned that there is the possibility that you will cause damage and/or loss of data using this software and that in no way shall the author be liable for such damages or loss of data.

16. Now click the **Sniffer** tab.

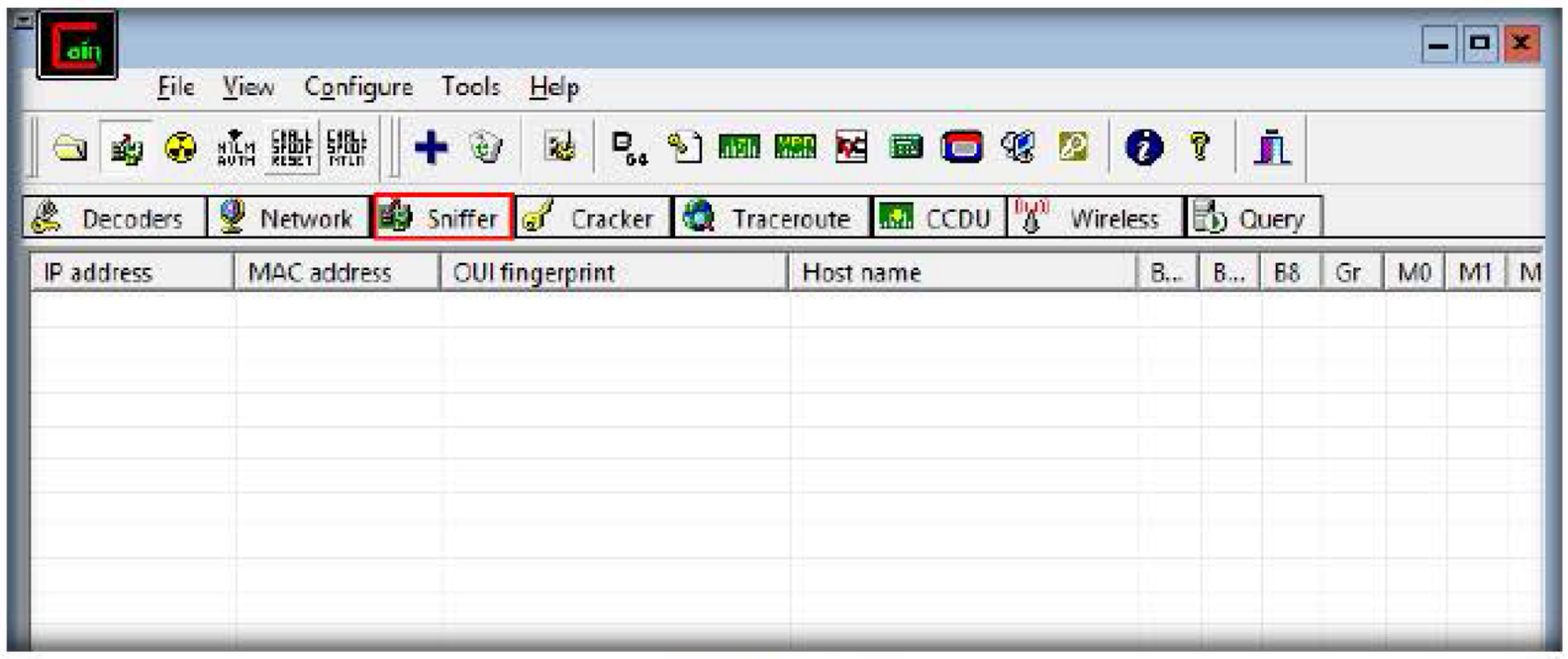



FIGURE 3.10: Sniffer tab

17. Click the plus (**+**) icon, or right click in the window, and select **Scan MAC Addresses** to scan the network for hosts.


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

18. The **MAC Address Scanner** window appears, select the **Range** radio button, enter the scan range **10.10.10.1-10.10.10.254**. Check **All Tests**, then click **OK.**

APR-RDP can capture and decrypt Microsoft's Remote Desktop Protocol as well.

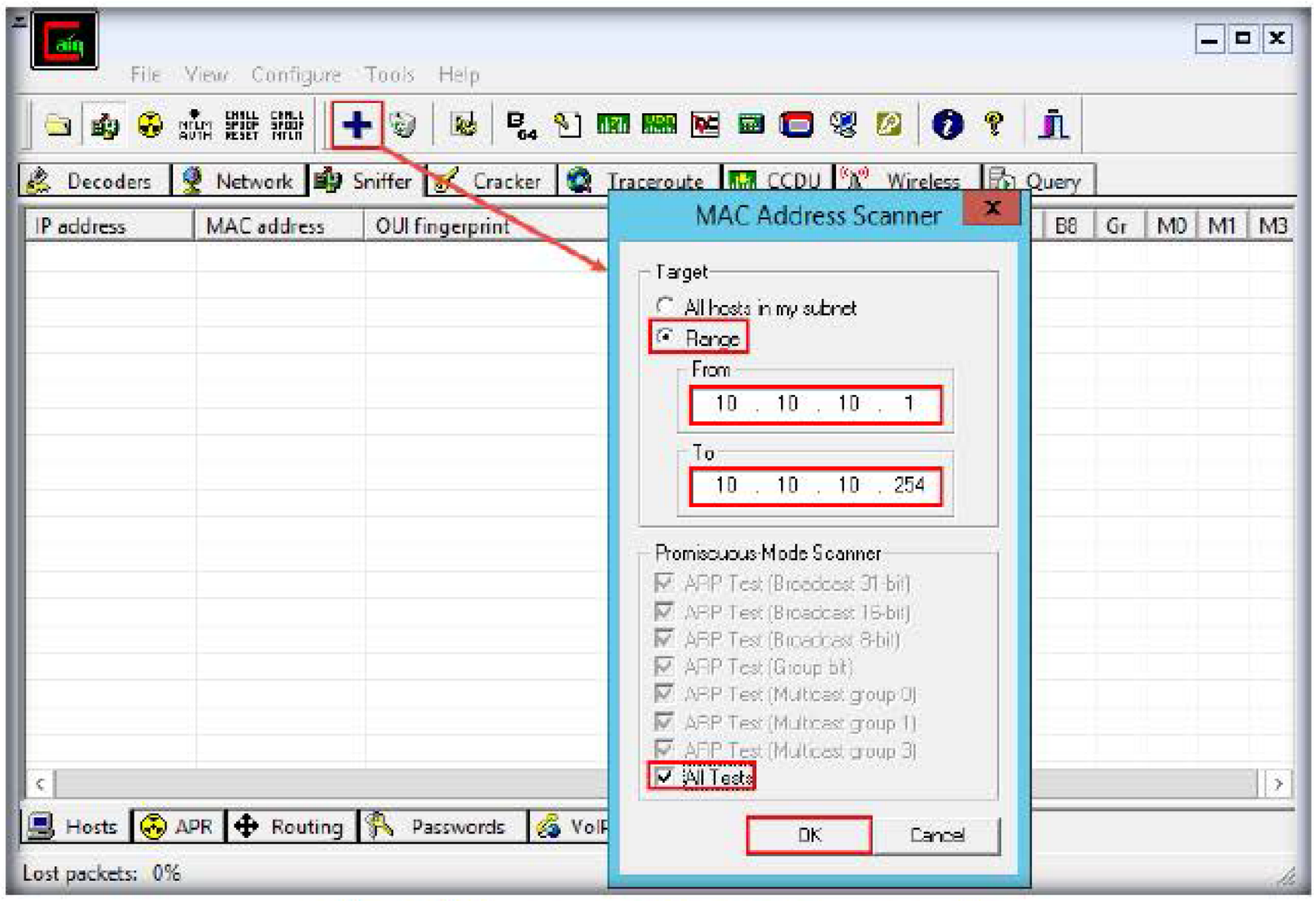



FIGURE 3.11: Cain & Abel - MAC Address Scanner Window

19. Cain & Abel starts **scanning** for MAC addresses and **lists** all those found.

Speeding up capture speed by wireless packet injection.

20. After the scan is **completed**, a list of detected **MAC addresses** is displayed as shown in the screenshot:

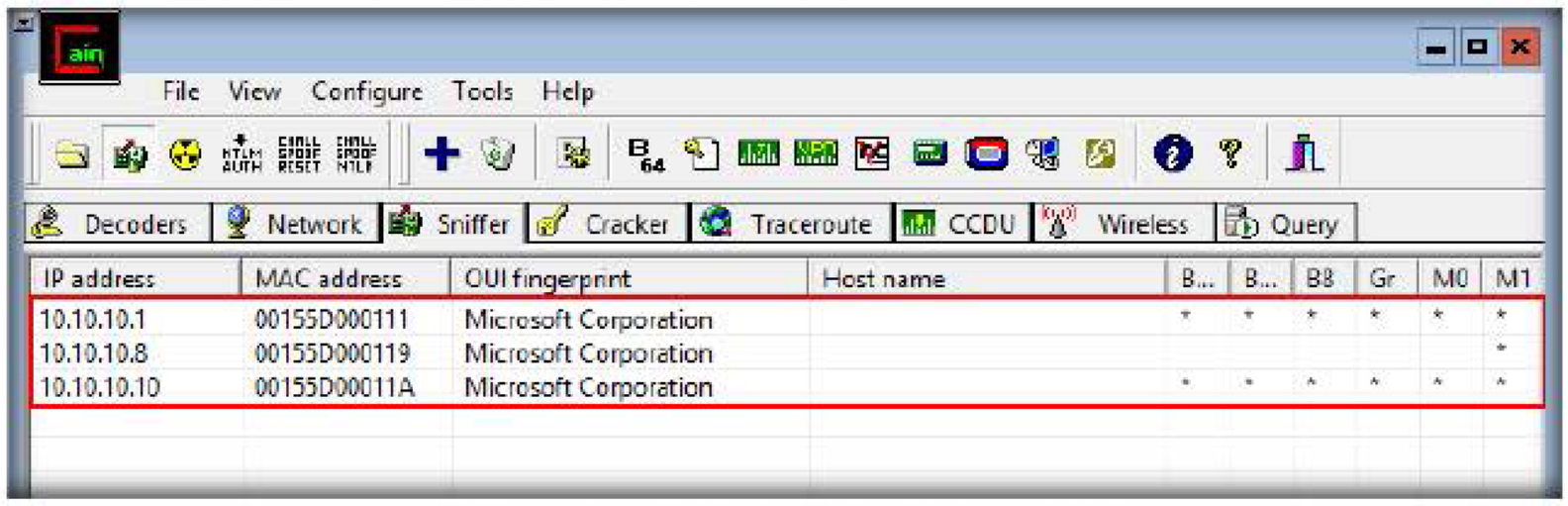



FIGURE 3.12: Cain & Abel - MAC Address Scanned


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

21. Click the **APR** tab at the lower end of the window.

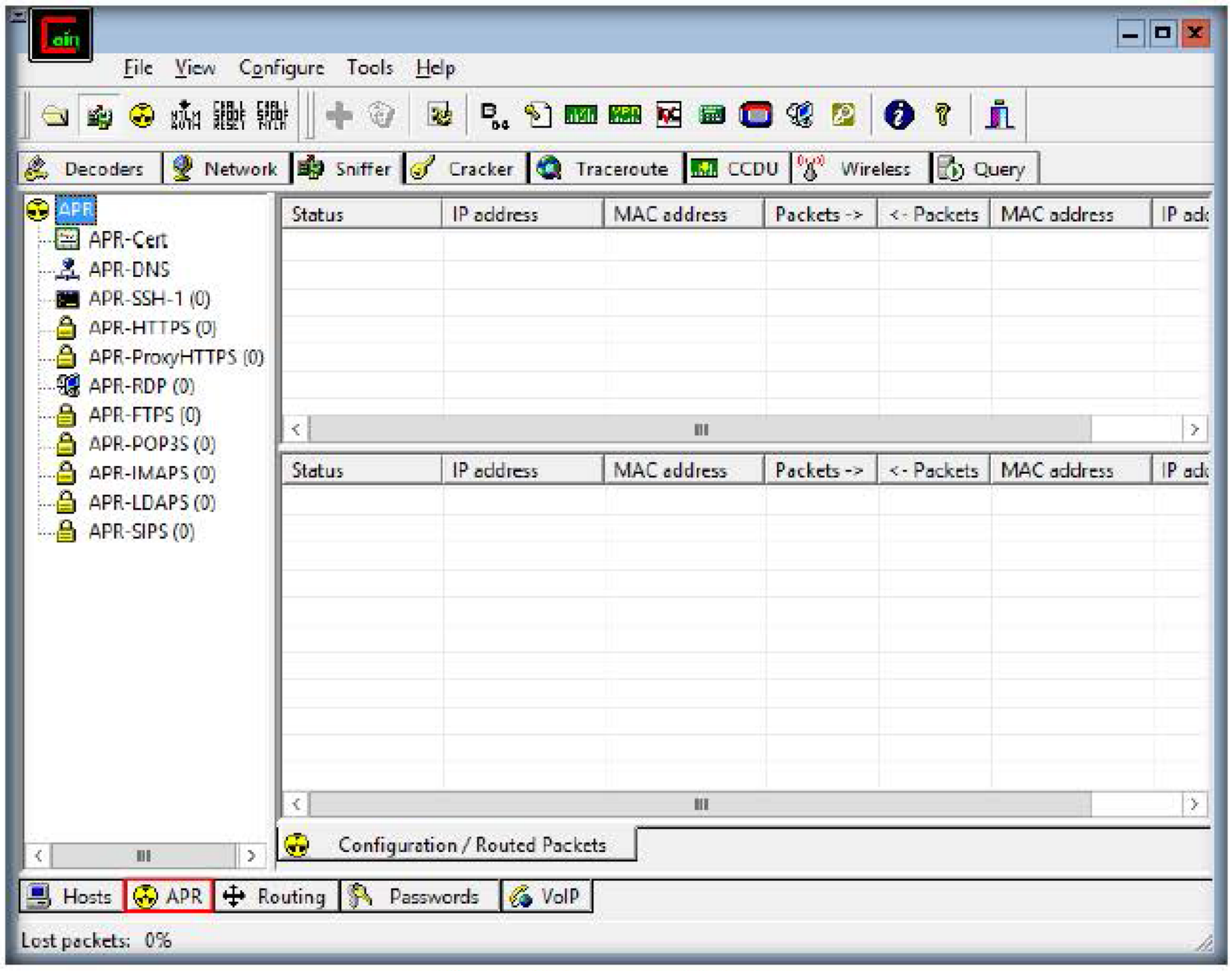



FIGURE 3.13: Cain & Abel ARP Tab

APR state Half-Routing means that APR is routing the traffic correctly but only in one direction (ex: Client->Server or Server->Client). This can happen if one of the two hosts cannot be poisoned or if asymmetric routing is used on the LAN. In this state the sniffer loses all the packets for an entire direction so it cannot grab authentications that use a challenge-response mechanism.

Note that the Cain & Abel program does not exploit any software vulnerabilities or bugs that could not be fixed with little effort.

22. Click anywhere in the right pane on the top most section to activate the **+** icon.

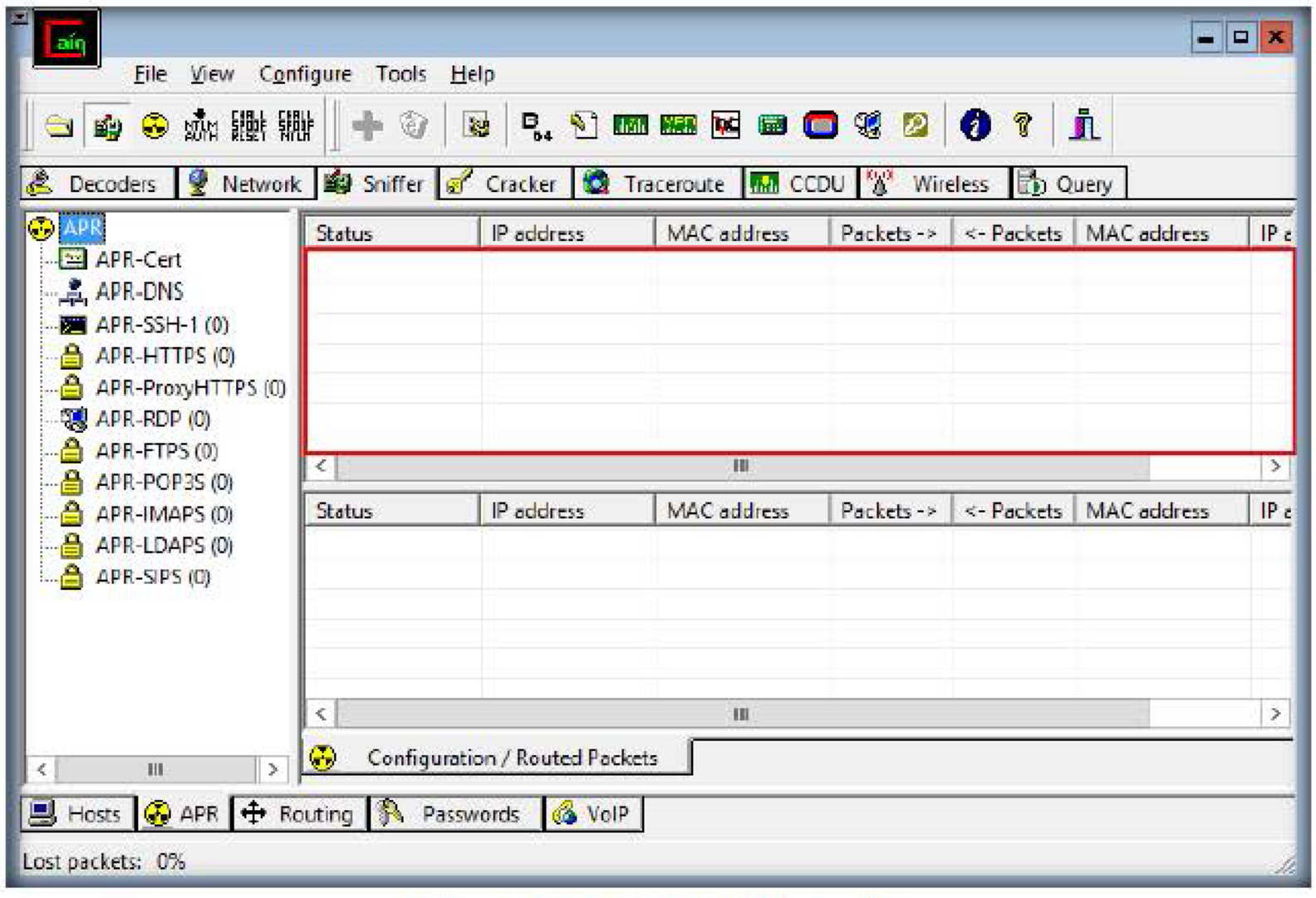



FIGURE 3.14: Cain & Abel Sniffer Section

APR state Full-Routing means that the IP traffic between two hosts has been completely hijacked and APR is working in FULL-DUPLEX. (ex: Server<->Client). The sniffer will grab authentication information accordingly to the sniffer filters set.



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

23. Click the Plus (+) icon; the **New ARP Poison Routing** window opens, from which we can add IPs to listen to traffic.

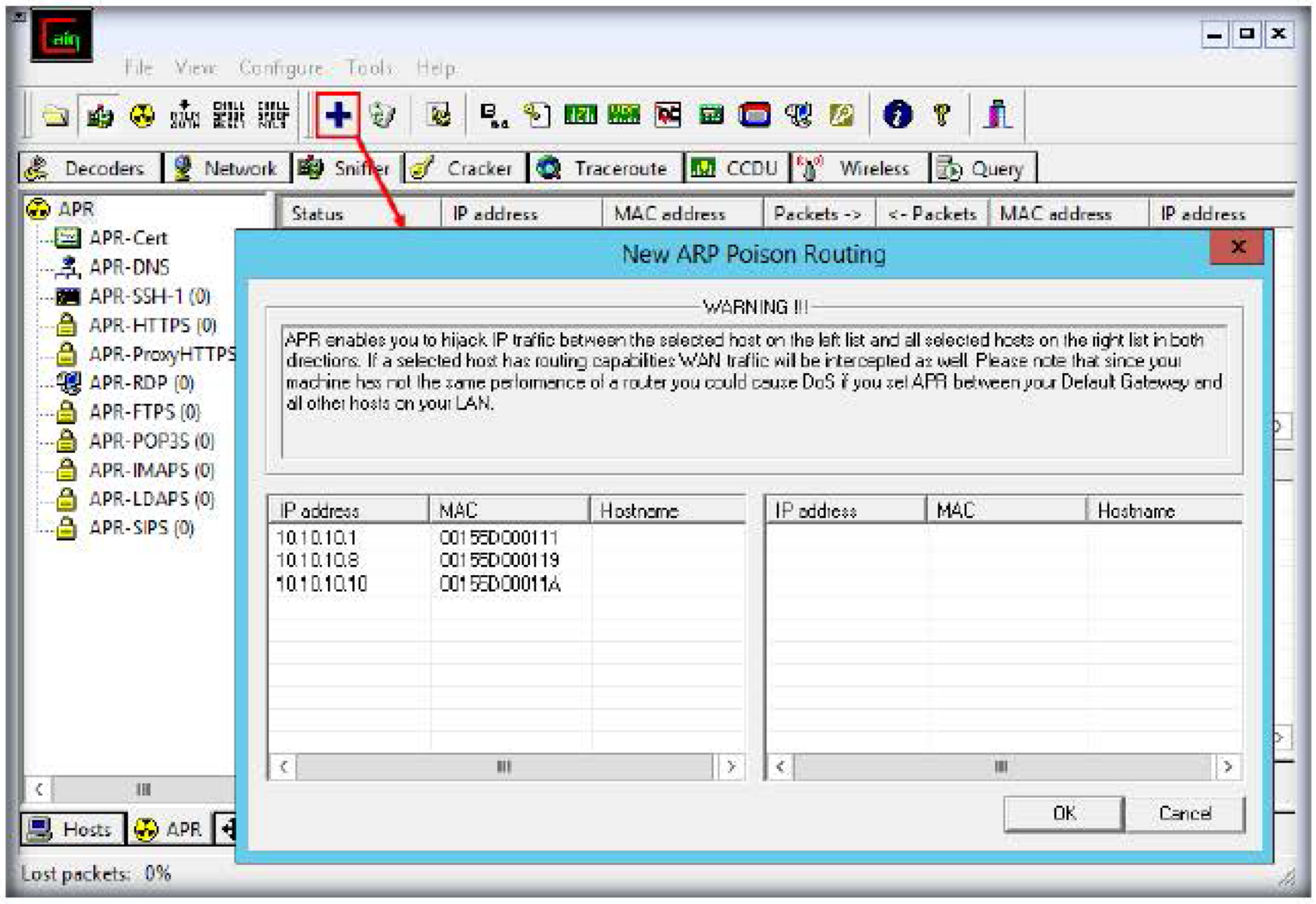



FIGURE 3.15: New ARP Poison Routing window

24. To monitor the traffic between two computers, select **10.10.10.10** (**Windows 10**) and **10.10.10.8** (**Windows Server 2008**). Click **OK**

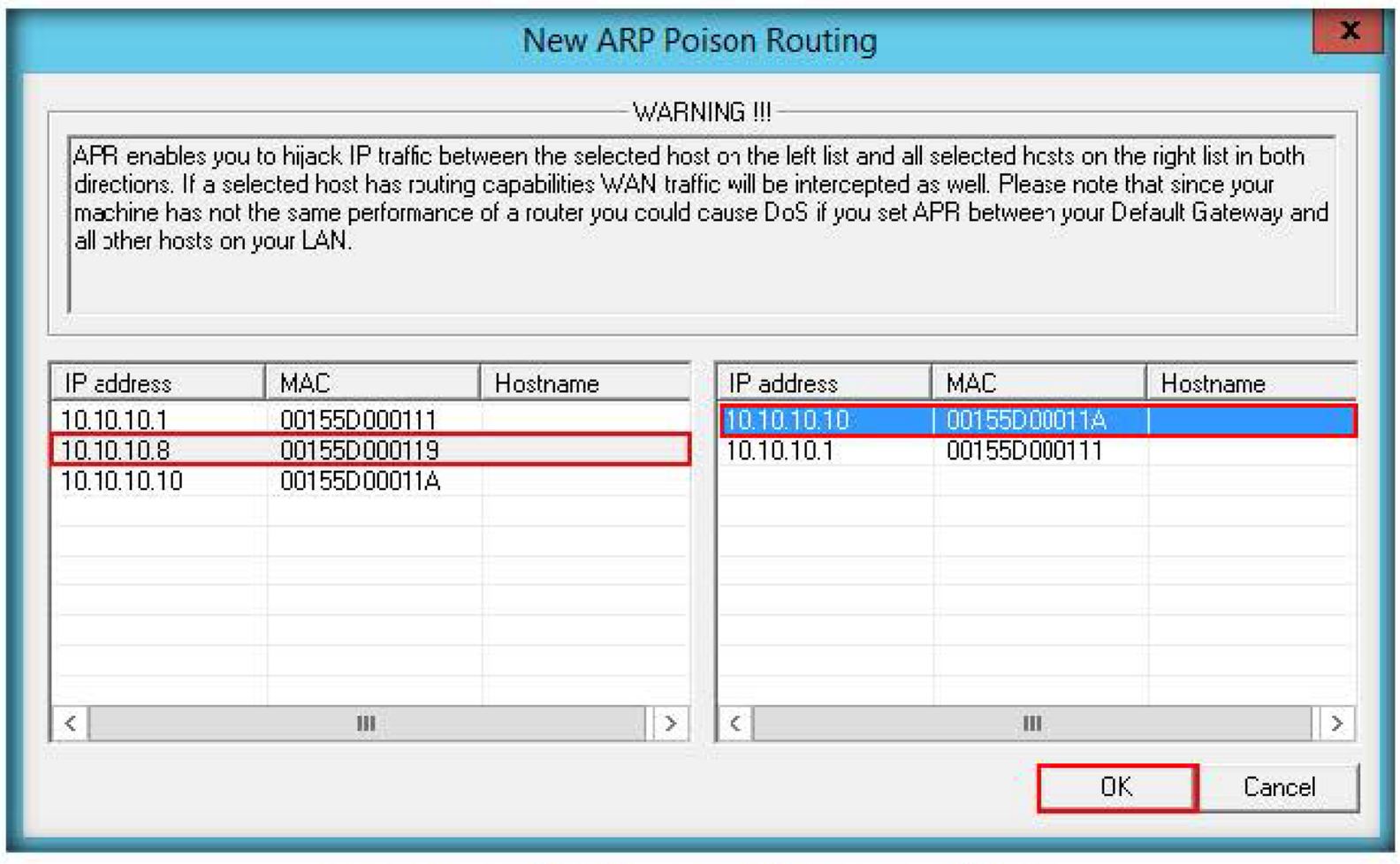



FIGURE 3.16: Monitoring the traffic between two computers

The Protected Store is a storage facility provided as part of Microsoft CryptoAPI. It's primary use is to securely store private keys that have been issued to a user.

All of the information in the Protected Store is encrypted, using a key that is derived from the user's logon password. Access to the information is tightly regulated so that only the owner of the material can access it


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

25. Select the added IP address in the **Configuration/Routed** packets, and click **Start/Stop APR**.

📖 Many Windows applications use this feature; Internet Explorer, Outlook and Outlook Express for example store user names and passwords using this service.

Note: If a **Couldn't bind HTTPS acceptor socket** pop-up appears, click **OK**.

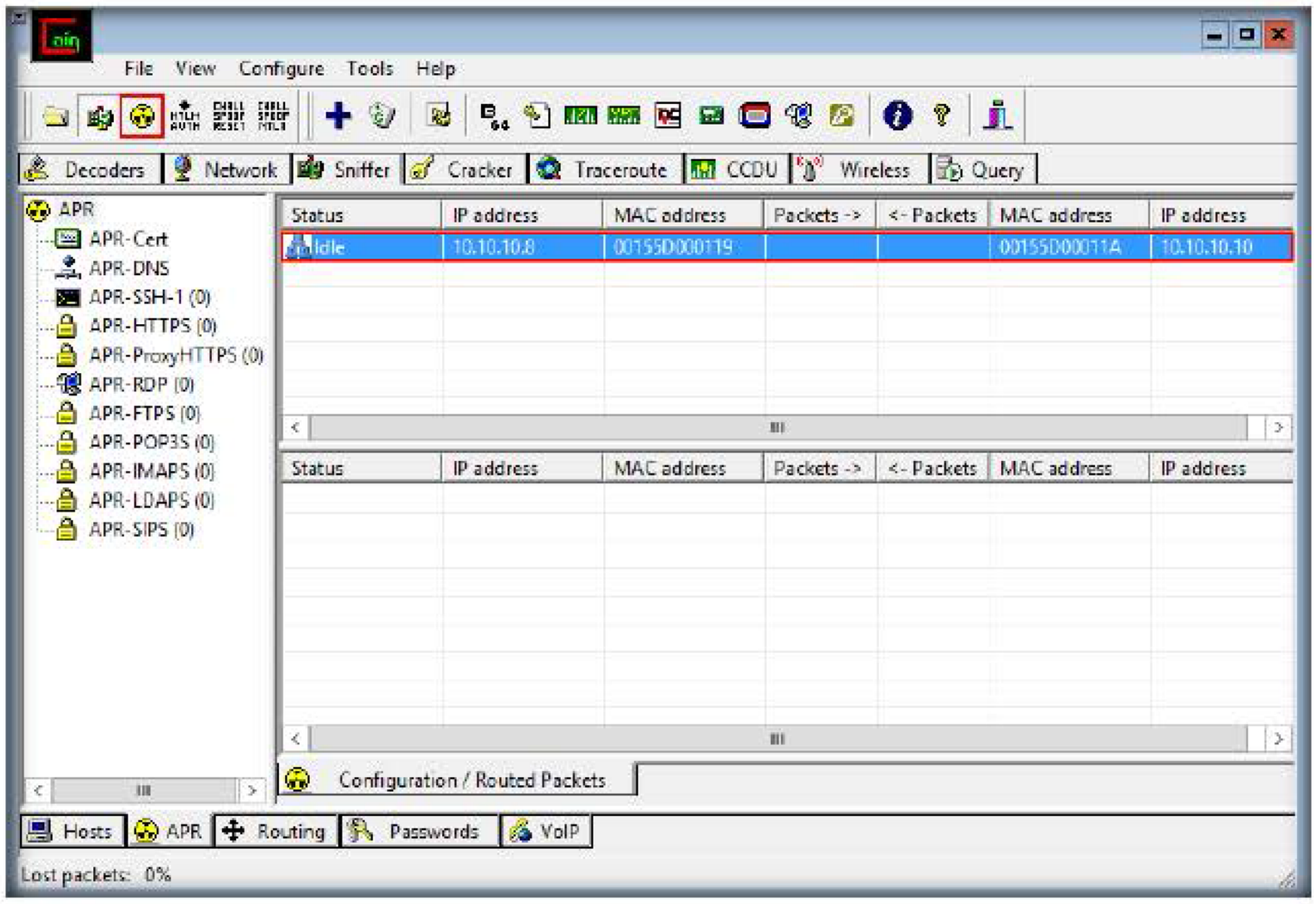



FIGURE 3.17: Cain & Abel ARP Poisoning

26. Now, launch Wireshark and begin the traffic capture on the Windows Server 2012 machine
27. Browse the **cnd** Website installed on the Windows Server 2008 machine (Here the IP address of the machine is **10.10.10.8**. It may vary in your environment)
28. Now, log on to the Windows 10 virtual machine
29. Launch a web browser, type the URL http://10.10.10.8/cnd/wp-login.php in the address bar and press **Enter**.


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

30. The WordPress login page appears, login to the **cnd** website using the credentials **admin/qwerty@123**

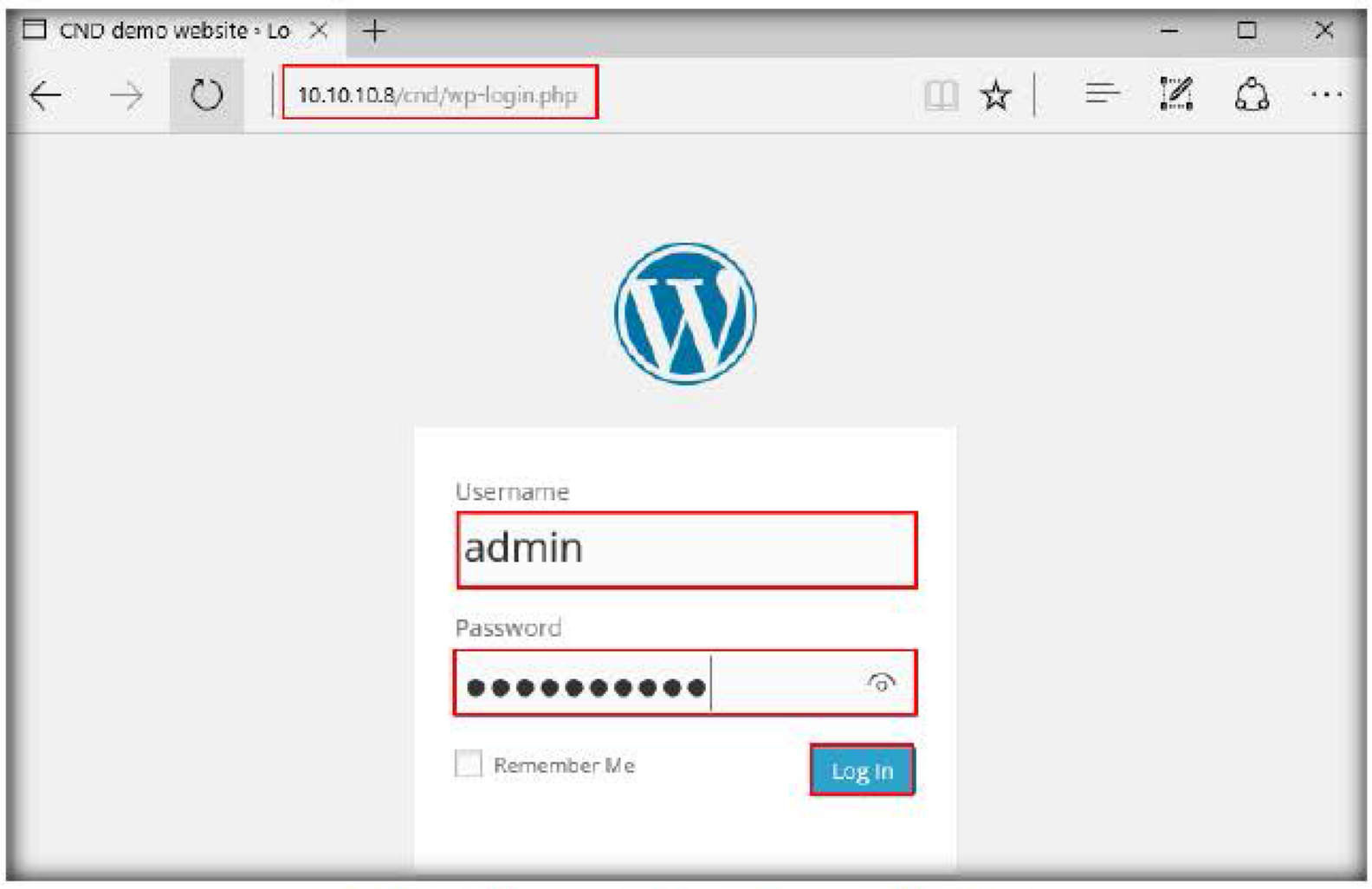
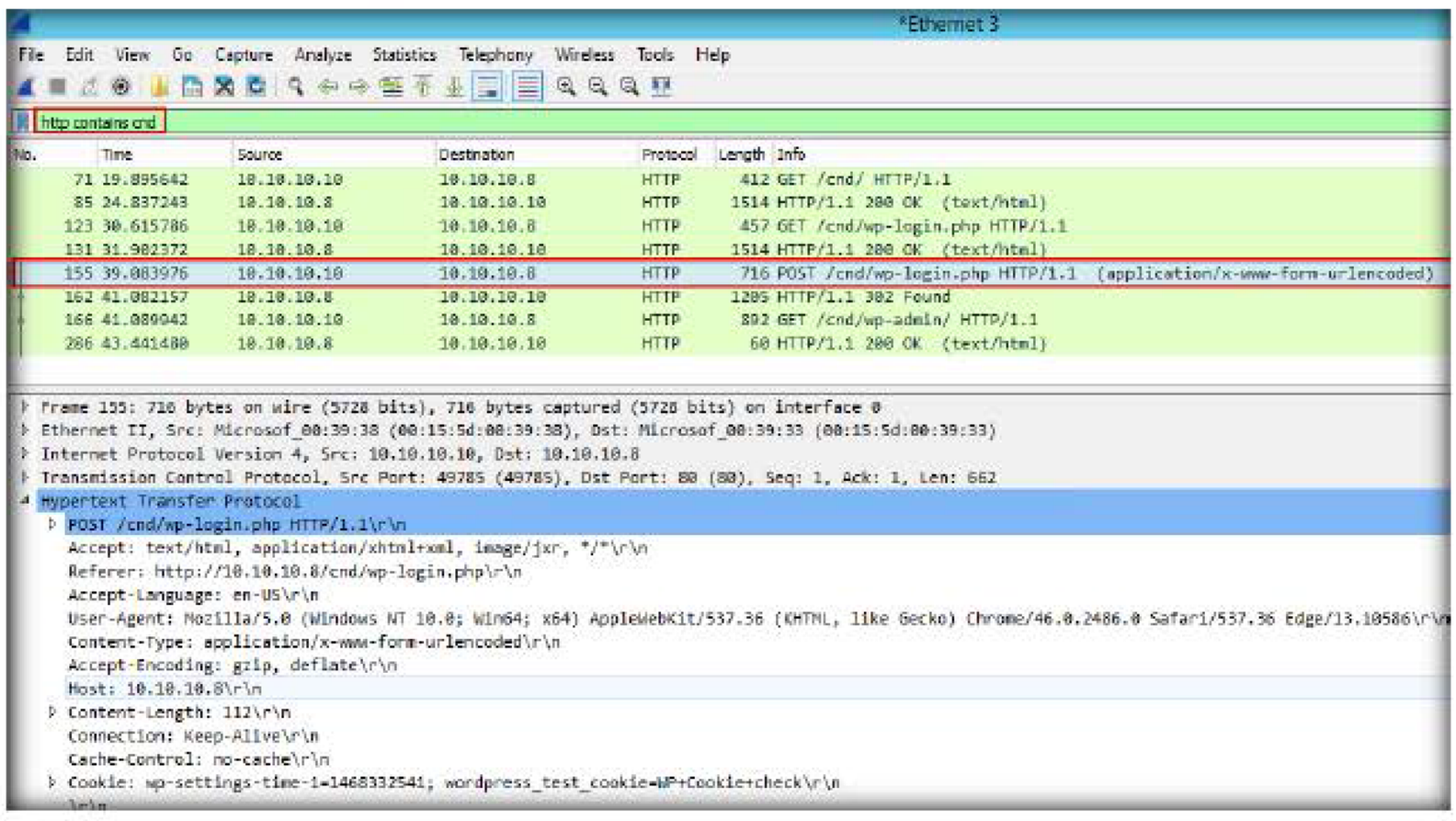



FIGURE 3.18: Login credentials entered in a non HTTPS page

31. Now go to Wireshark and stop capturing. Filter for the packet with the code **http contains [forms]** (here, **cnd**) since our web URL had forms in it. Choose the HTTP post packet from the filtered list and right-click on its HTML form encoded and click **Follow→TCP Stream** from context menu.






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

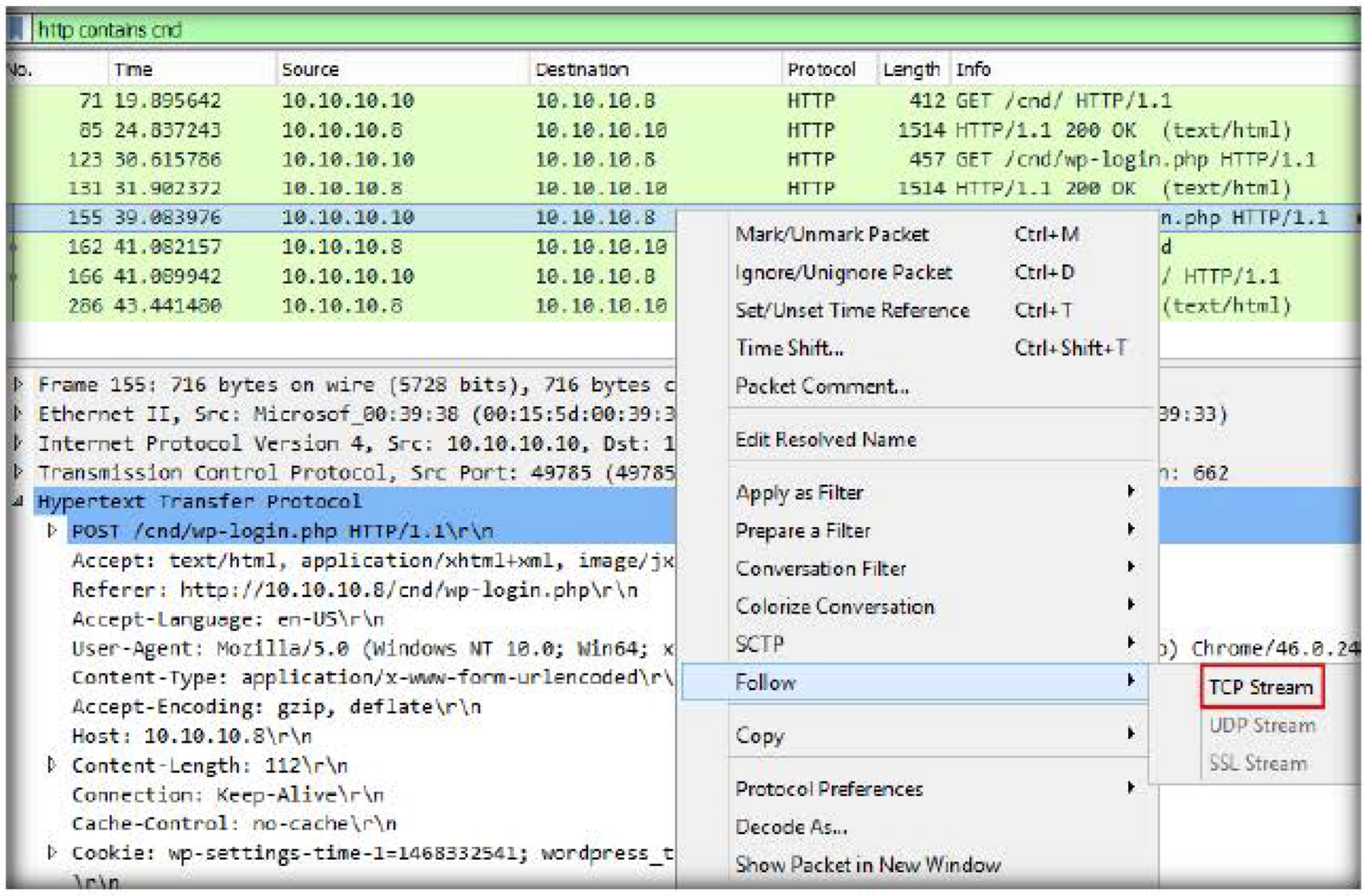






FIGURE 3.19: Plain text password transmitted by Non HTTPS packet


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

**TASK 1**

**Clear-text FTP Traffic**

32. This demonstrates **clear text traffic** flowing in a **FTP** network
33. Begin a new packet capture in the Windows Server 2012 virtual machine
34. Switch to the Windows 10 virtual machine, launch a command prompt. Type ftp 10.10.10.8 (10.10.10.8 is the IP Address of Windows Server 2008) and press **Enter**. You will be prompted to enter the FTP credentials of the server. Enter any username and password of your choice. In this lab, the username and password are **Admin** and **test@123**.

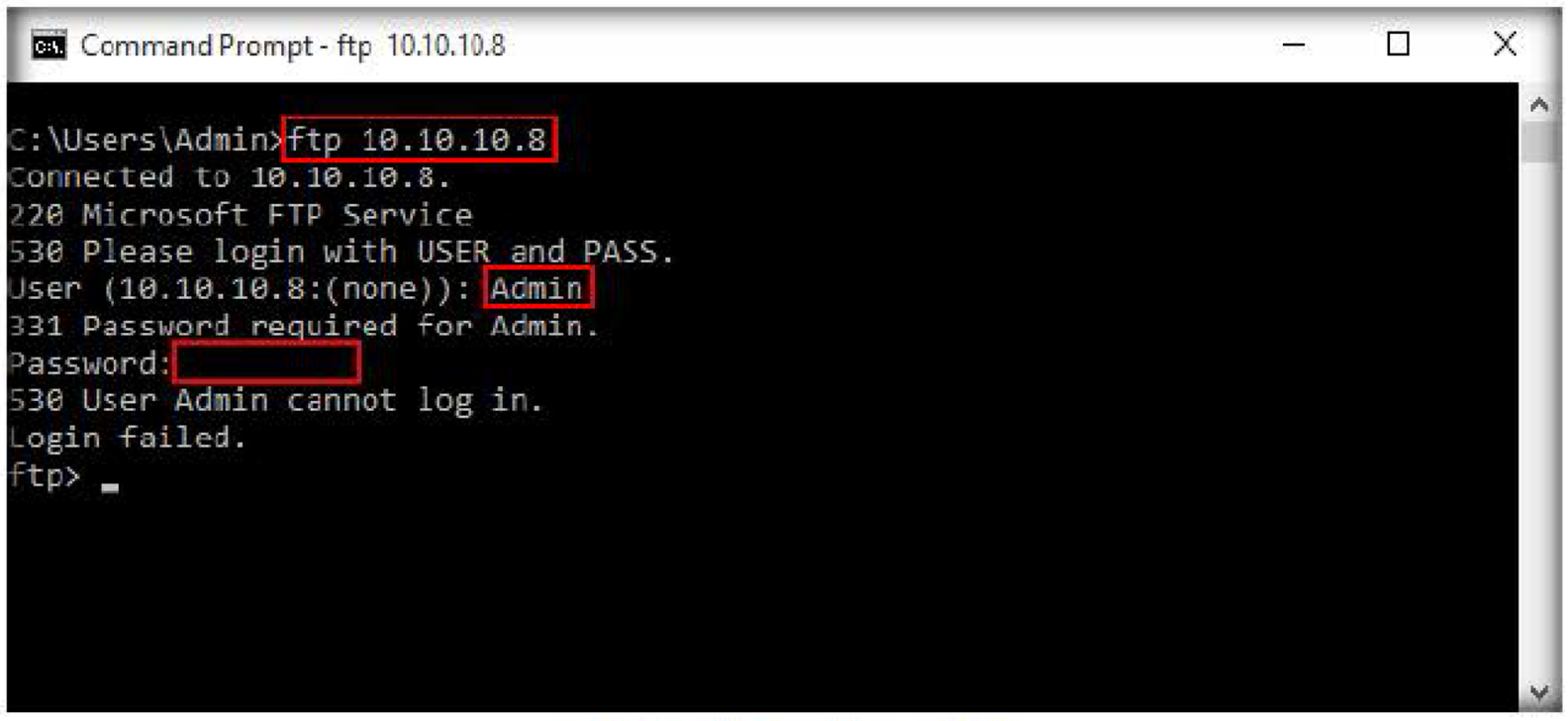



FIGURE 3.20: Logging in to FTP

35. Switch to the Windows Server 2012 virtual machine.
36. **Stop the capture** process in Wireshark and look for the FTP traffic in the scanned results

FTP transmits data unencrypted

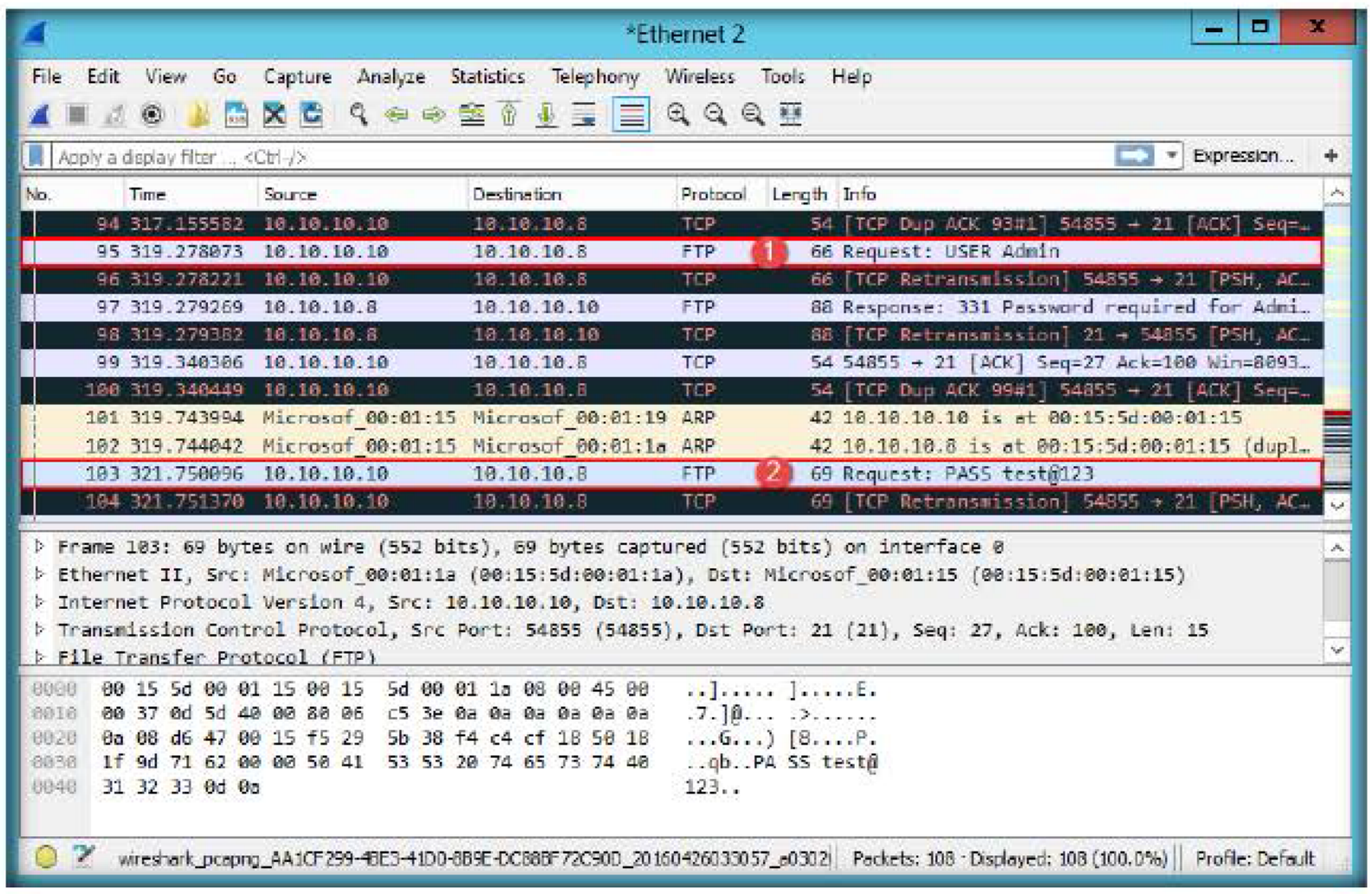



FIGURE 3.21: FTP clear text traffic detected in wireshark

37. In the above screenshot we can clearly see that the **Username** is found to be **Admin** and **password** is found to be **test@123** in the FTP traffic



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

**TASK 2**

**Clear-text Telnet Traffic**

38. Now we shall use Wireshark to view **clear text traffic** flowing through the **TELNET** protocol
39. Before beginning this task, ensure that the **Telnet Client** is installed in the **Windows 10** virtual machine and the **Telnet Server** is installed and running on the **Windows Server 2008**.
40. Begin a Wireshark packet capture in the Windows Server 2012 virtual machine
41. Switch to the Windows 10 virtual machine, launch a command prompt, type **telnet 10.10.10.8** (10.10.10.8 is the IP Address of the Windows Server 2008) and press **Enter**.

Telnet is an application layer protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection.

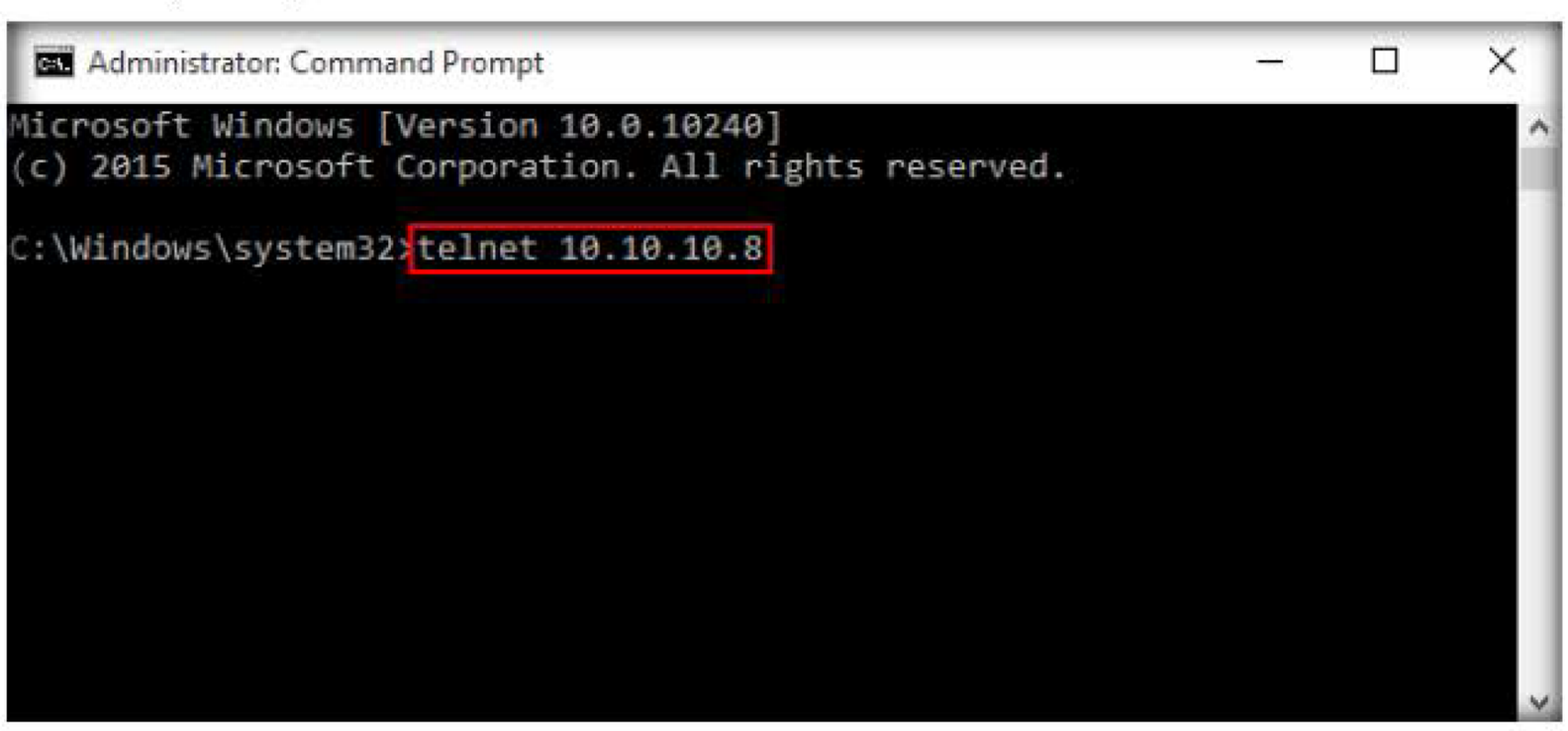



FIGURE 3.22: Establishing Telnet connection

42. A **Welcome** screen appears, type **y** and press **Enter** in order to send the password information in the Internet zone.

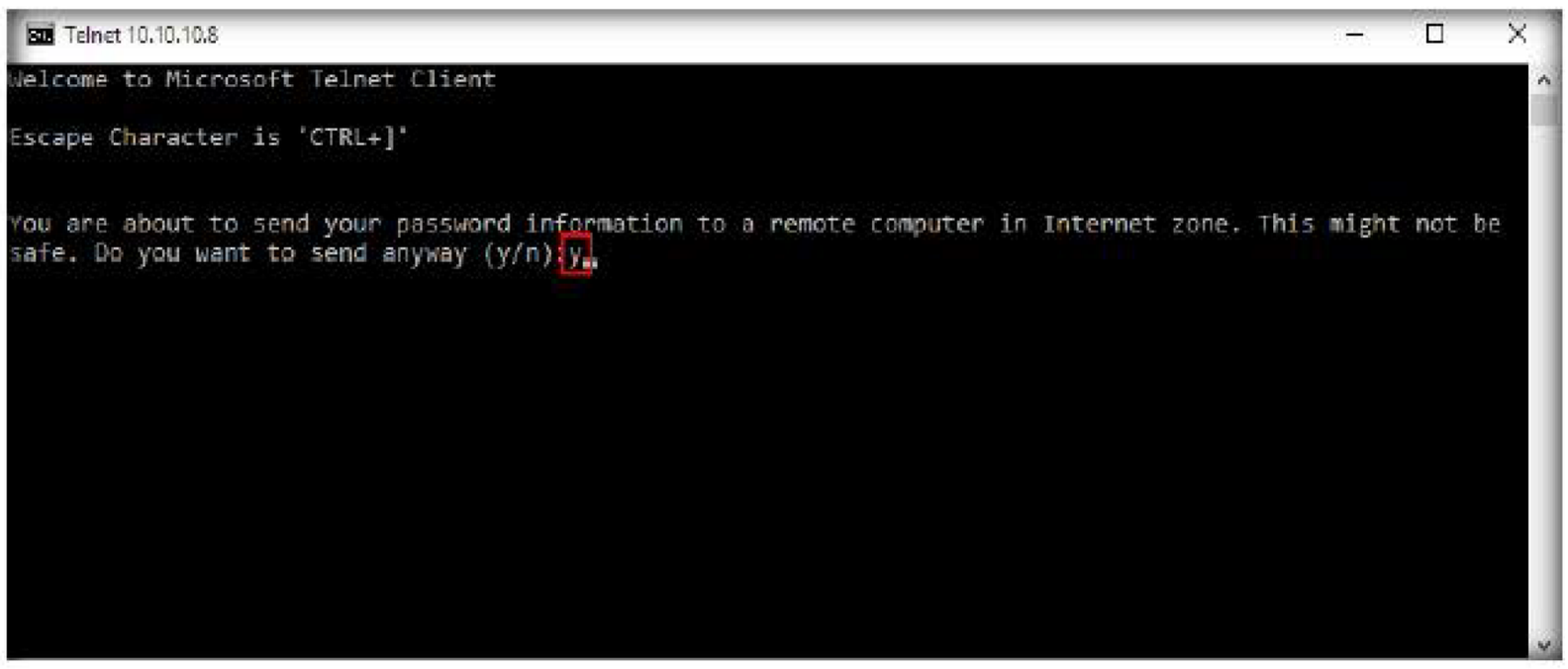



FIGURE 3.23: Confirming the connection


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

43. Capture packets in Wireshark while transmitting data using the Telnet protocol

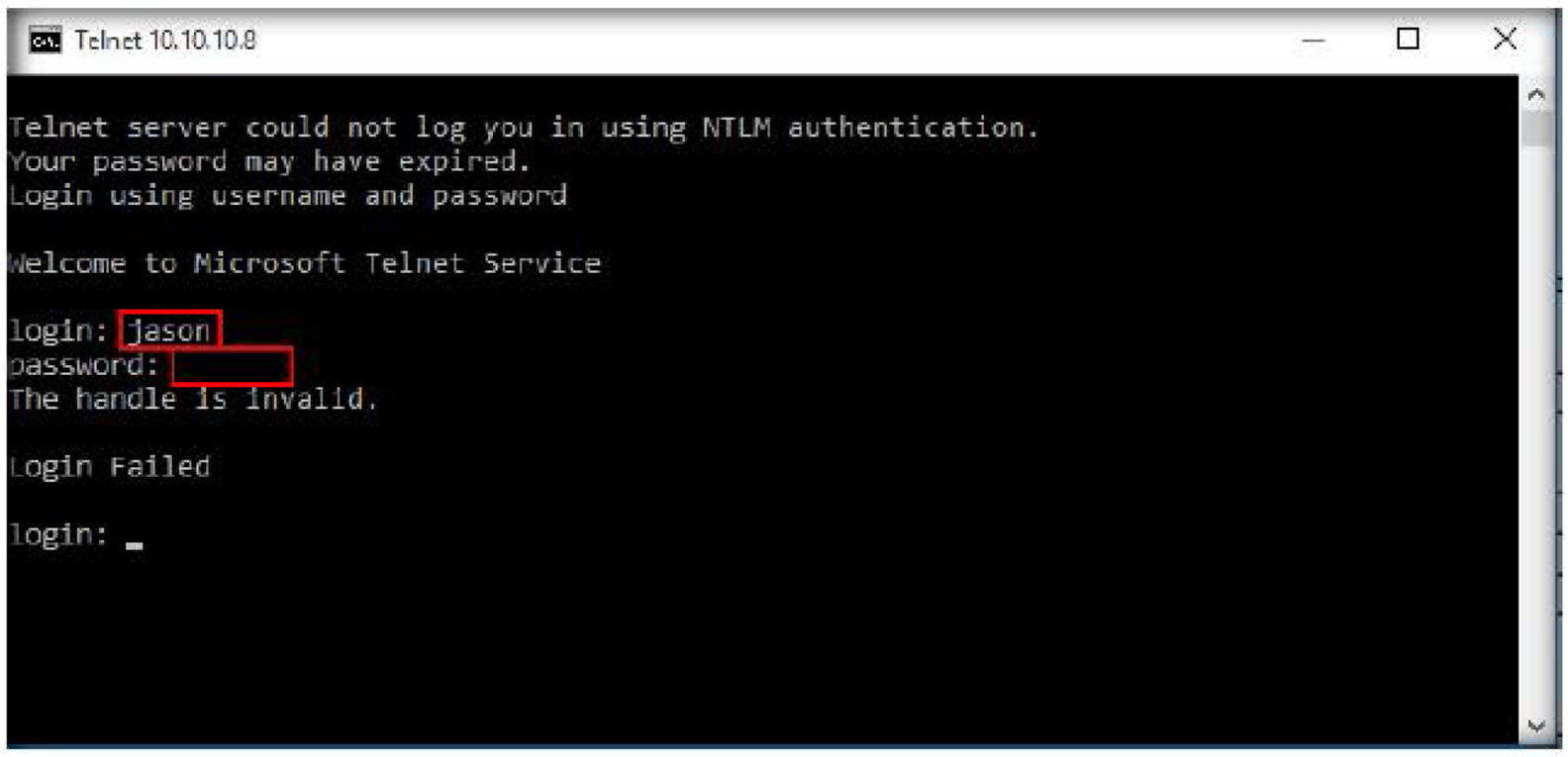



FIGURE 3.24 Logging in to TELNET

44. Switch back to the Windows Server 2012 virtual machine. Now stop the capture and filter all the traffic pertaining to the **telnet** protocol.

You cannot directly filter Telnet protocols while capturing. However, if you know the TCP port used (see above), you can filter on that one.

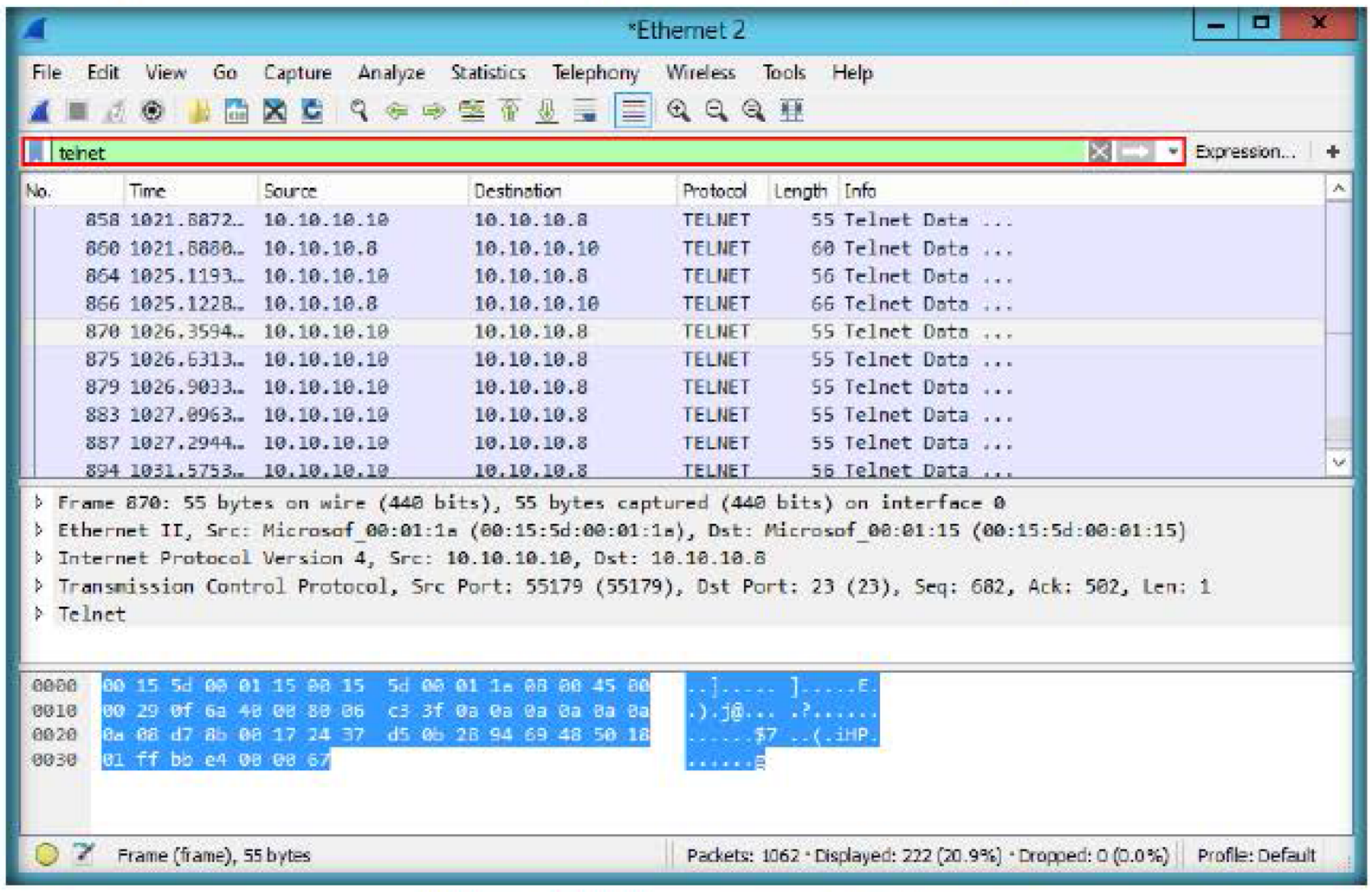



FIGURE 3.25 Filtering wireshark with telnet



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

45. Since TELNET transmits data alphabet letter by alphabet letter, you cannot understand anything if you observe an individual packet. Go to **Analyze** in the Wireshark toolbar, select **Follow** and click **TCP stream**.

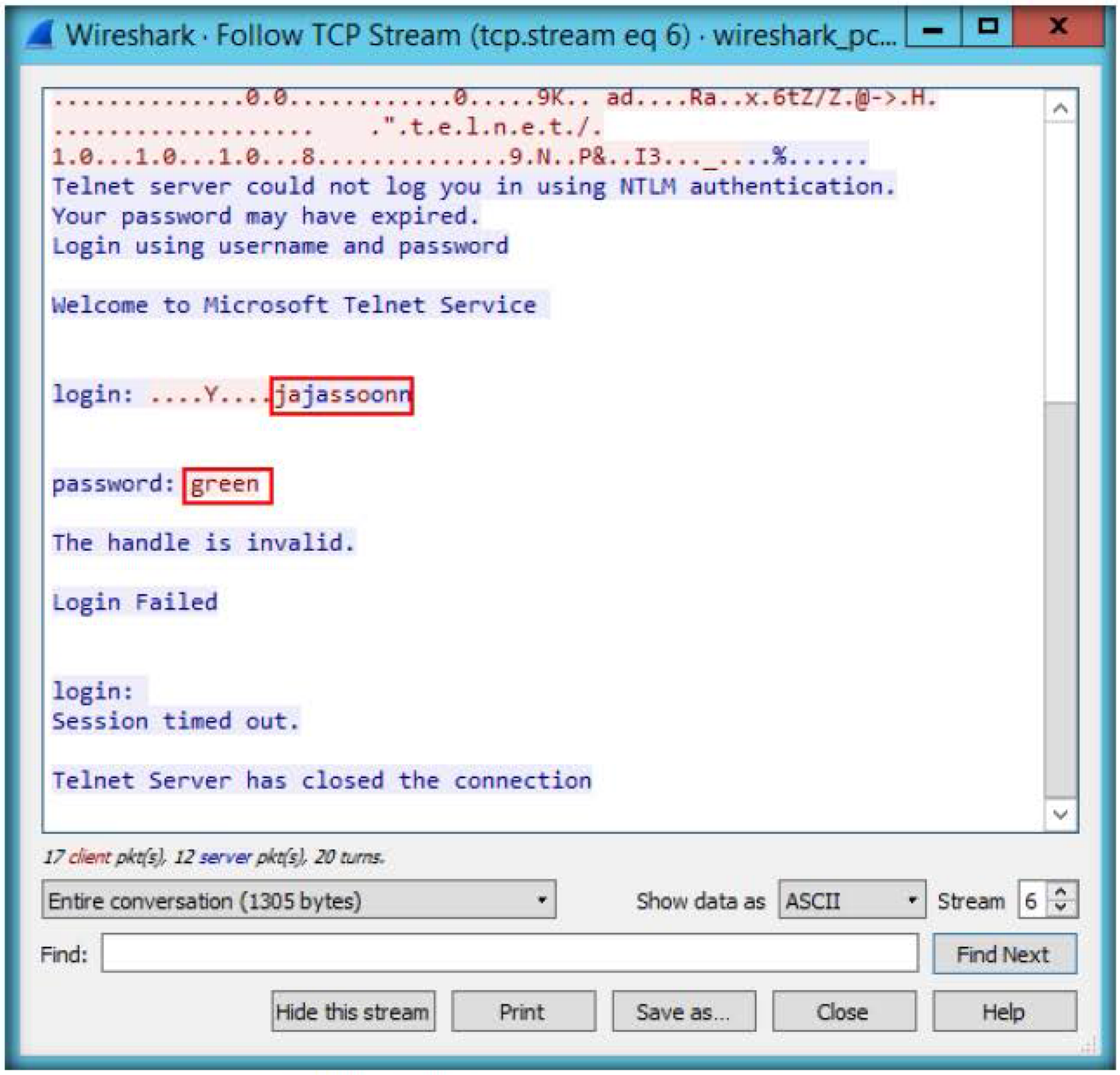



FIGURE 3.26: Telnet clear text traffic captured in Wireshark

If you are working with TCP based protocols it can be very helpful to see the data from a TCP stream in the way that the application layer sees it. Perhaps you are looking for passwords in a Telnet stream, or you are trying to make sense of a data stream. The stream content is displayed in the same sequence as it appeared on the network. Traffic from A to B is marked in red, while traffic from B to A is marked in blue. If you like, you can change these colors in the "Colors" page of the "Preferences" dialog.

## 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 |



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

Lab 4

# Monitoring and Detecting Network Reconnaissance, Access and DoS/DDoS Attempts

*Wireshark is a network packet analyzer, which is used to capture network packets and display packet data in detail.*

ICON KEY

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

## Lab Scenario

Network reconnaissance is the initial phase of an attack where attackers collect as much information about a network as possible, including the IP Address range, OS version, services running on the OS, etc. The attackers then use this information to identify the vulnerabilities in the network and proceed to the next phase of the attack. Attackers mainly look at gaining access to a system, or to enforce a denial of service attack, and make the system stop responding to the requests coming from its clients. As a network administrator, you need to know how to analyze the packets captured by Wireshark, and detect the reconnaissance activities occurring on the network; network access related attempts as well as denial of service attempts performed on a machine or a network.

## Lab Objectives

The objective of this lab is to teach you how to understand the process to detect various types of scans and attacks occurring on a network.

## Lab Environment

To perform the lab, you need:

- Cain & Abel located at **Z:\CND-Tools\CND Module 11 Network Traffic Monitoring and Analysis\ARP Poisoning Tools\Cain&Abel**
- You can also download the latest version of Cain & Abel from the link http://www.oxid.it/cain.html
- Wireshark, located at **Z:\CND-Tools\CND Module 11 Network Traffic Monitoring and Analysis\Packet Sniffing Tools\Wireshark**


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

- Nmap, located at **Z:\CND-Tools\CND Module 11 Network Traffic Monitoring and Analysis\Port Scanning Tools\Nmap**
- You can also download the latest version of Wireshark from the link https://www.wireshark.org/download.html
- If you decide to download the latest version, then screenshots shown in the lab might differ
- A virtual machine running Windows Server 2012
- A virtual machine running Windows Server 2008
- A virtual machine running Windows 10
- A virtual machine running Ubuntu Linux
- A Web browser with Internet connection
- **Administrative** privileges to run tools

## Lab Duration

Time: 120 Minutes

## Overview of Packet Analysis

In a network, there is always a diversified amount of traffic flowing between two end points, and this can be intercepted by Wireshark. Proper analysis/examination of each of the packets can help identify malicious activities occurring in the network.

## Lab Tasks

1. Before beginning this lab, launch Cain&Abel in Windows Server 2012 and follow steps 9-25 of the previous lab to perform ARP poisoning between the Windows 10 and the Windows Server 2008.
2. Also, install Nmap located at **Z:\CND-Tools\CND Module 11 Network Traffic Monitoring and Analysis\Port Scanning Tools\Nmap** in Windows 10 machine
3. Now we shall look at how to detect various TCP flag based attacks. By using Nmap in the Windows 10 machine to perform a TCP half scan/SYN Scan. Install Wireshark in the Windows 10 virtual machine.

**TASK 1**

**Detecting TCP Half Scan attempt**

**Note**: TCP half scan is a reconnaissance attack in which the attacker attempts to gain information as to which ports are open on the victim's system. The attacker sends a SYN packet to show that he is interested in establishing a connection. If a port is open it replies with a (SYN+ACK) packet else, it sends a RST packet. If the attacker gets a SYN+ACK packet to complete the connection the attacker should send an ACK packet but he is not interested in establishing any connection. His intention was to know if the port is open or not which was established after he got SYN+ACK packet. Now he either sends a RST packet to close the connection or doesn't send any more packets at all.


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

4. Make sure that you are running Wireshark in the **Windows Server 2012** virtual machine.
5. In this scenario, the target machine's IP Address is **10.10.10.8** (Windows Server 2008) and the attacker machine's IP address is **10.10.10.10** (Windows 10).
6. To perform a SYN scan on the target machine, switch to the Windows 10 machine, launch Nmap, and type the command **nmap -sS -T4 10.10.10.8** in the **Command** field then click **Scan**.

TCP SYN scan s often referred to as half-open scanning, because you don't open a full TCP connection. You send a SYN packet, as if you are going to open a real connection and then wait for a response. A SYN/ACK indicates the port is listening (open), while a RST (reset) is indicative of a non-listener.

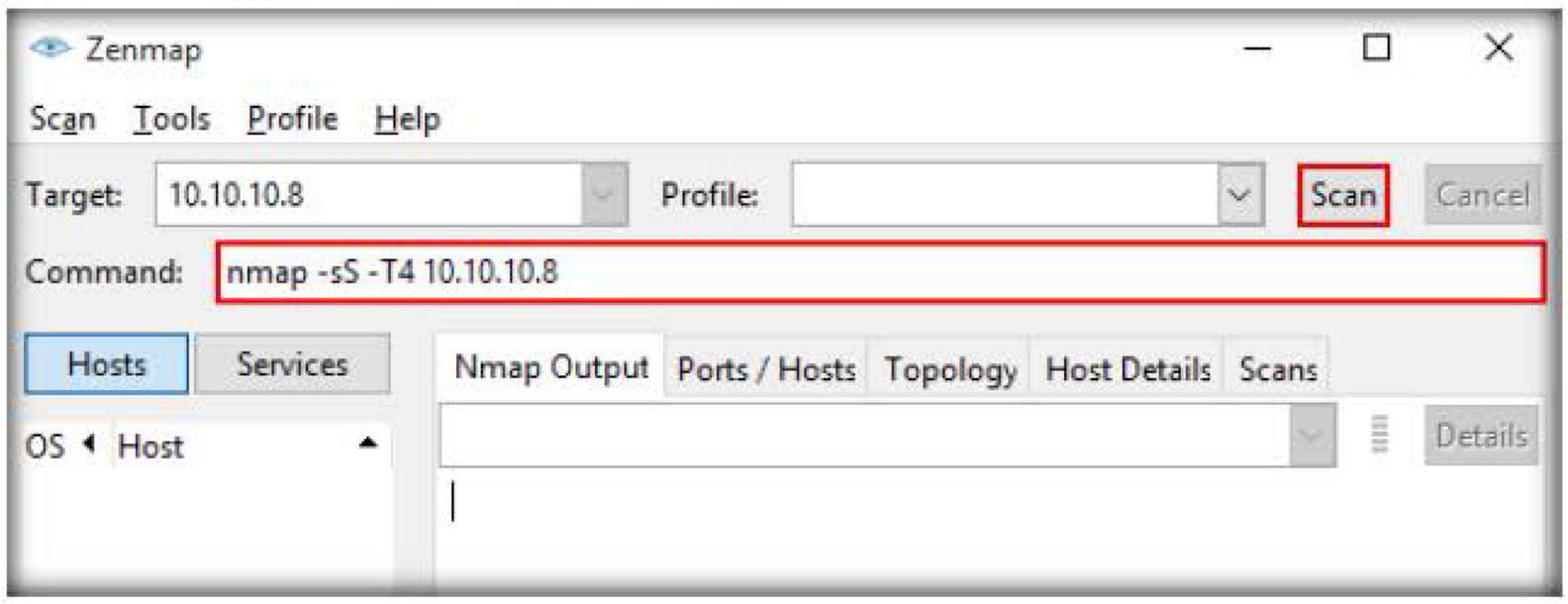



FIGURE 4.1: Performing SYN Scan Using NMAP

7. When the scan completes, switch back to the Windows Server 2012 virtual machine, stop the packet capture and issue the syntax **tcp.flags.syn==1** in the **Filter** field. This displays all the packets containing the SYN request and the SYN, ACK response between **Windows 10** and **Windows Server 2008** as shown in the following screenshot:

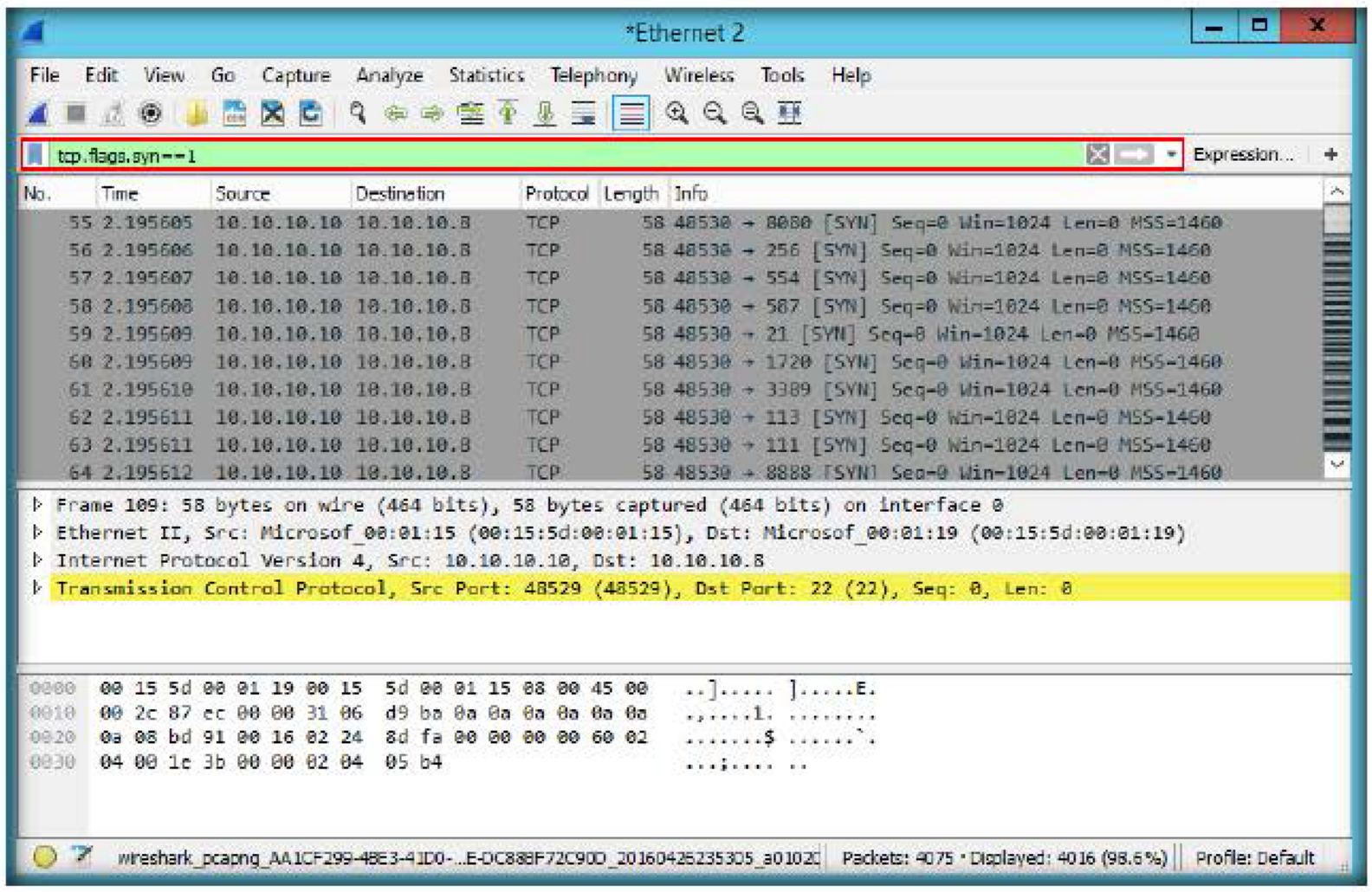



FIGURE 4.2: TCP SYN packets from attacker to victim


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

8. Since a huge number of SYN requests are sent to the target machine, the target's ports which are open reply with **SYN+ACK**. Issue the syntax **tcp.flags.syn==1 and tcp.flags.ack==1** to view the traffic containing the SYN, ACK response packets.

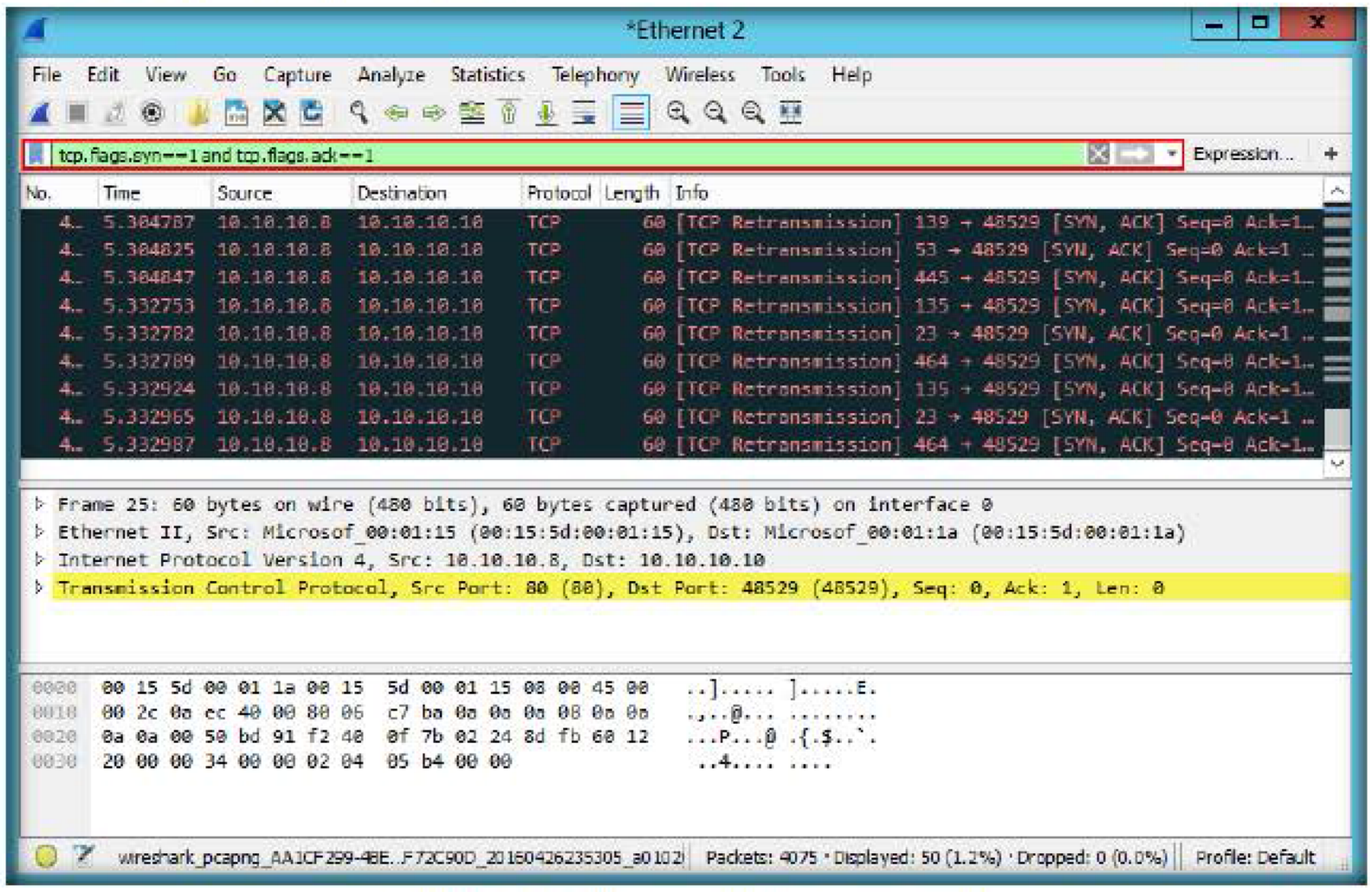



FIGURE 4.3: TCP ACK+SYN flags retransmitted

9. From this, it is evident that an **attempt** was made to **scan open ports** by an attacker using the **TCP half scan** method

**TASK 2**

**Detecting TCP Connect Scan Attempt**

10. Now we shall perform the **TCP full connect scan**. In the half scan attack, an attacker replies with a RST to close the connection after getting to know the open ports. But in a **full connect scan the attacker establishes a full 3 way TCP** handshake and after connection is established **immediately terminates it** with a RST packet or does not reply at all.
11. The attacker is **10.10.10.10** and the target is **10.10.10.8**. He implements a full scan attempt using Nmap.
12. Launch Wireshark in the Windows Server 2012 machine, and begin a packet capture.


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

13. Switch to the Windows 10 machine, launch Nmap, type the command **nmap -sT -T4 10.10.10.8** in the **Command** field then click **Scan**.

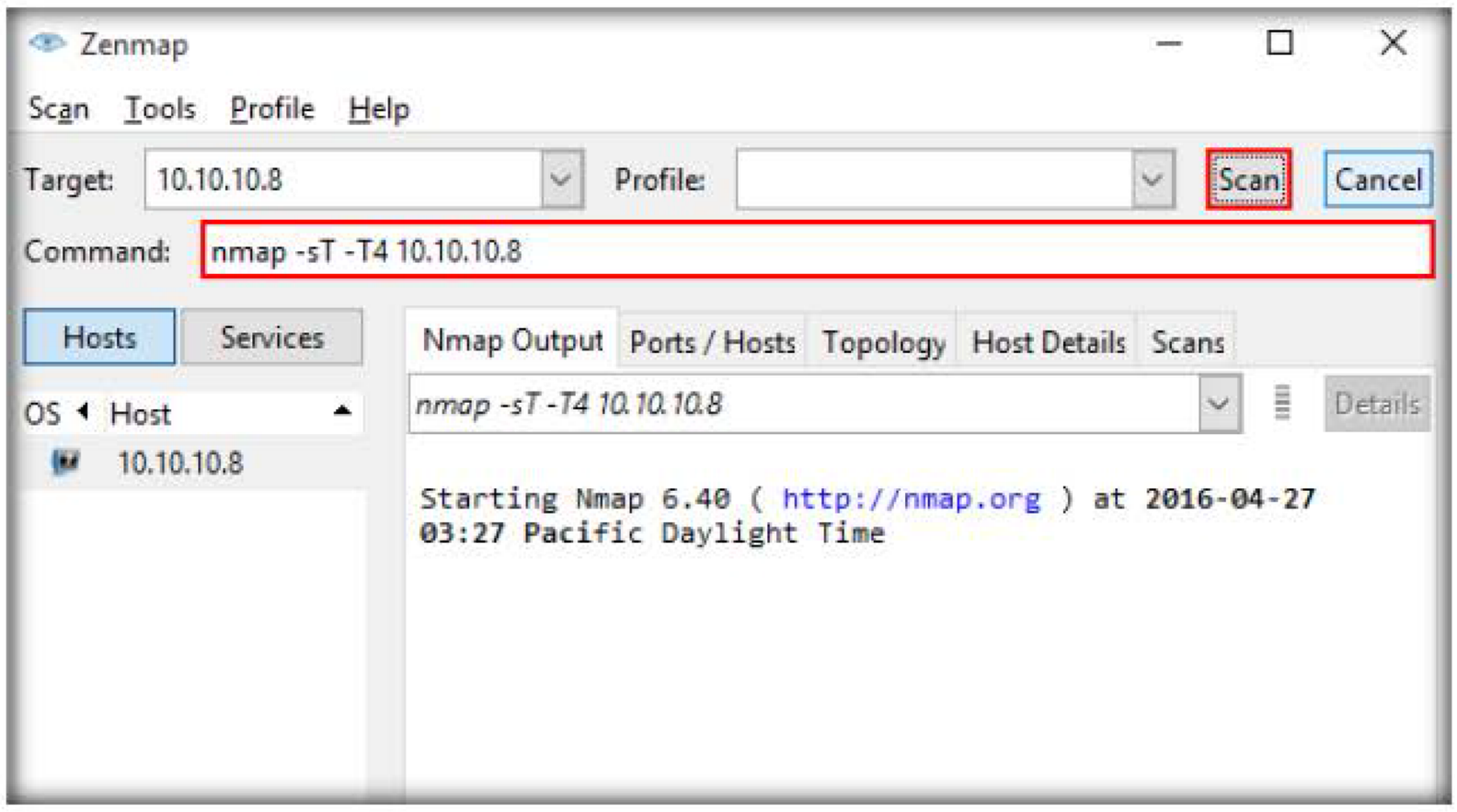



FIGURE 4.4: Implementing TCP full scan attack

TCP connect scan is the default TCP scan type when SYN scan is not an option. When a SYN scan is available, it is usually a better choice. Nmap has less control over the high level connect call than with raw packets, making it less efficient. The system call completes connections to open target ports rather than performing the half-open reset that a SYN scan does.

14. When the scan completes, switch back to the Windows Server 2012 virtual machine, stop the packet capture and issue the syntax **tcp.flags.syn==1 and ip.src==10.10.10.8** in the **Filter** field. This displays all the packets containing the SYN request and the SYN, ACK response between **Windows 10** and **Windows Server 2008** as shown in the following screenshot:

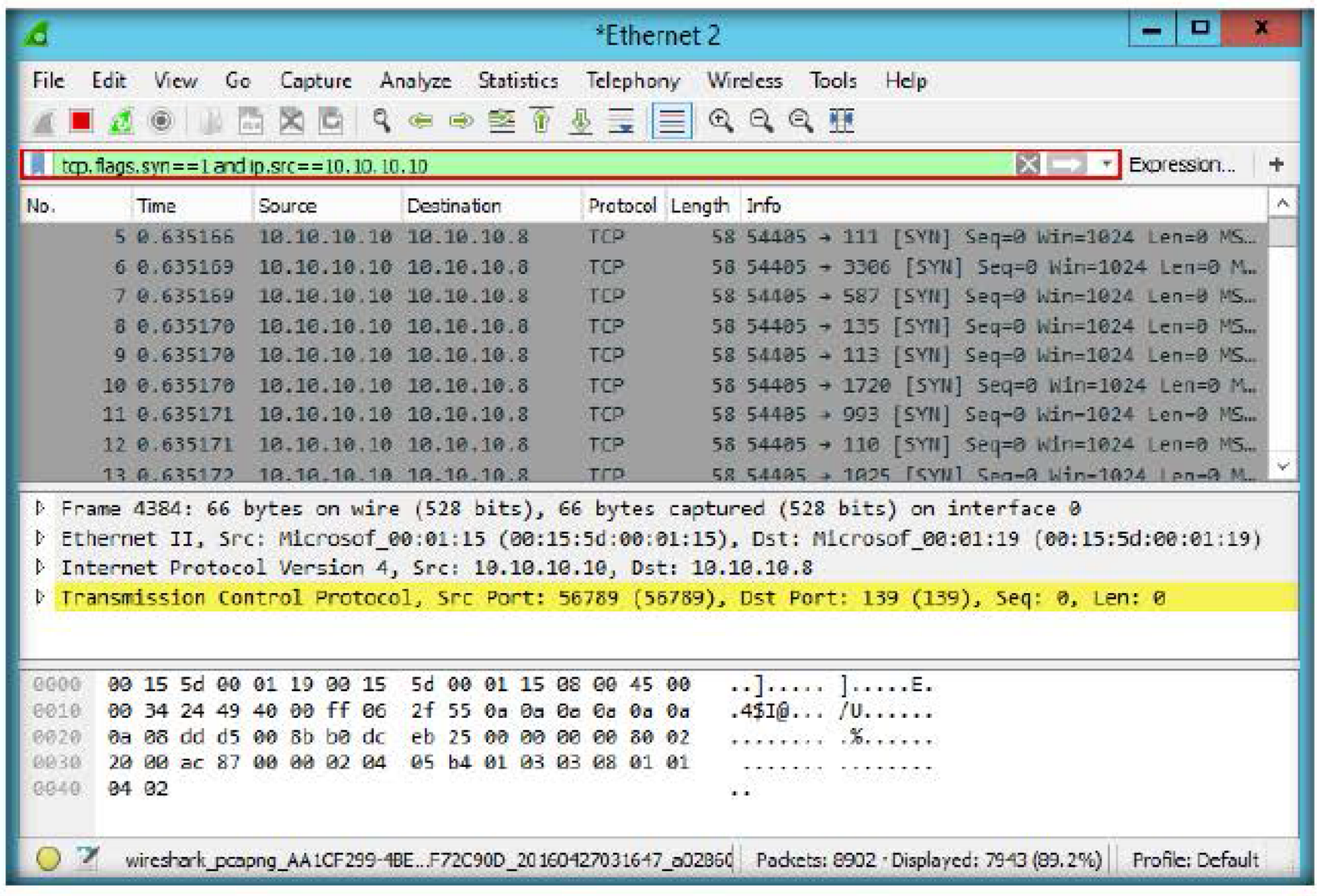



FIGURE 4.5 TCP SYN packets from attacker to victim



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

15. Now, the **victim is filled up with SYN packets** and it starts **replying to the attacker with SYN, ACK** packets from the open ports. You can observe particular ports of a victim which are open and which are replying to the attacker. Use code **tcp.flags.syn==1 and tcp.flags.ack==1 and ip.src==10.10.10.8**

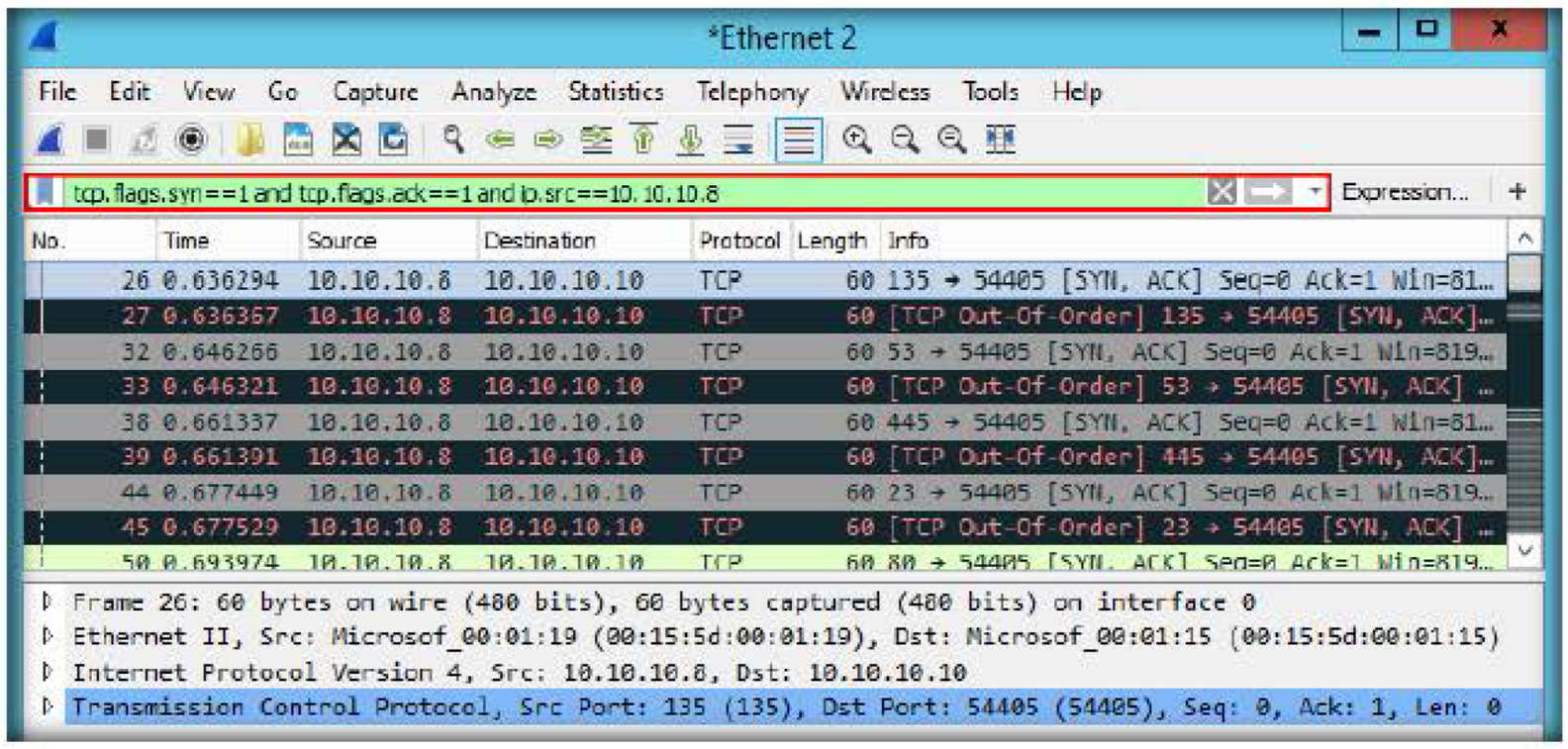



FIGURE 4.6: Victim replies to the attacker with SYN/ACK packets

**Note:** We can see that ports **23, 445, 49153, 49154, 49152, 49156, 139 and 135** are some of the ports which are **open** and have replied to the attacker.

16. Now moving on, the **attacker goes on and sends ACK packets** to open ports. (We filter with open ports only). After an attacker sends the ACK packets, the **TCP 3-way connection is established**. But instead of sending data he immediately **terminates the connection** by sending an **RST packet**, immediately after the ACK packet.

17. To view this, switch to the Windows Server 2012 machine, and issue the command **tcp.flags.ack==1 && ip.src==10.10.10.10** in the **Filter** field.

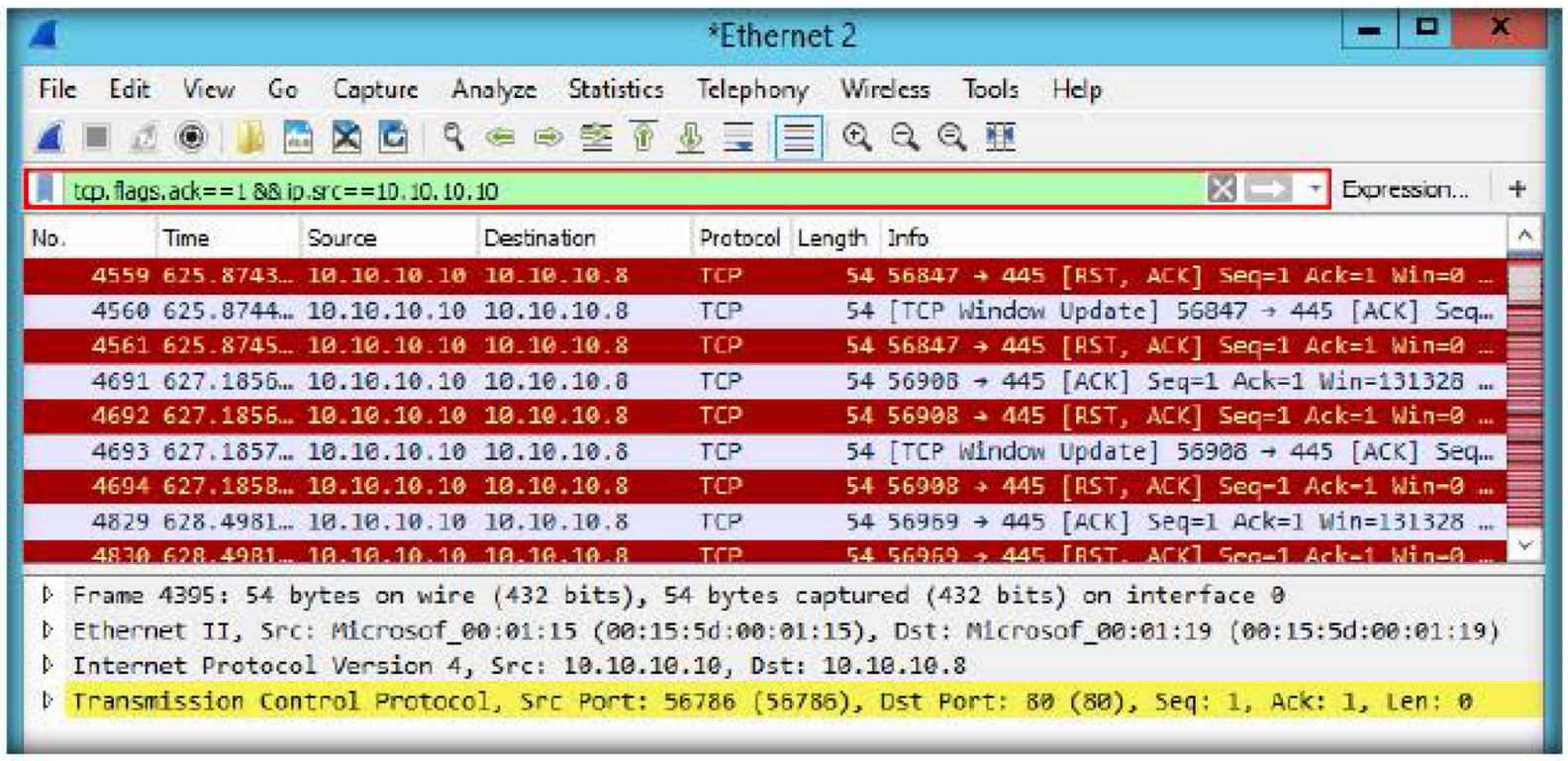



FIGURE 4.7: Attacker replies to victim with ACK packets



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

**TASK 3**

**Detecting TCP null scan attempt**

18. To demonstrate a **TCP Null scan attack**. In this type of attack, the attacker sends TCP packets with **no flag set**. It is only done **to check open ports**. An **open port does not reply to a Null packet** and a **closed port replies with the RST flag set.**
19. In this case, our attacker's machine is **10.10.10.10** and the victim's machine is **10.10.10.8**.
20. Begin a new Wireshark packet capture in the Windows Server 2012 virtual machine.
21. Switch to the Windows 10 virtual machine, launch Nmap, type the command **nmap -sN -T4 -A -v 10.10.10.8** in the **Command** field then click **Scan**.

The Null Scan exploits a subtle loophole in the TCP RFC to differentiate between open and closed ports. The Null scan does not set any bits (TCP flag header is 0)

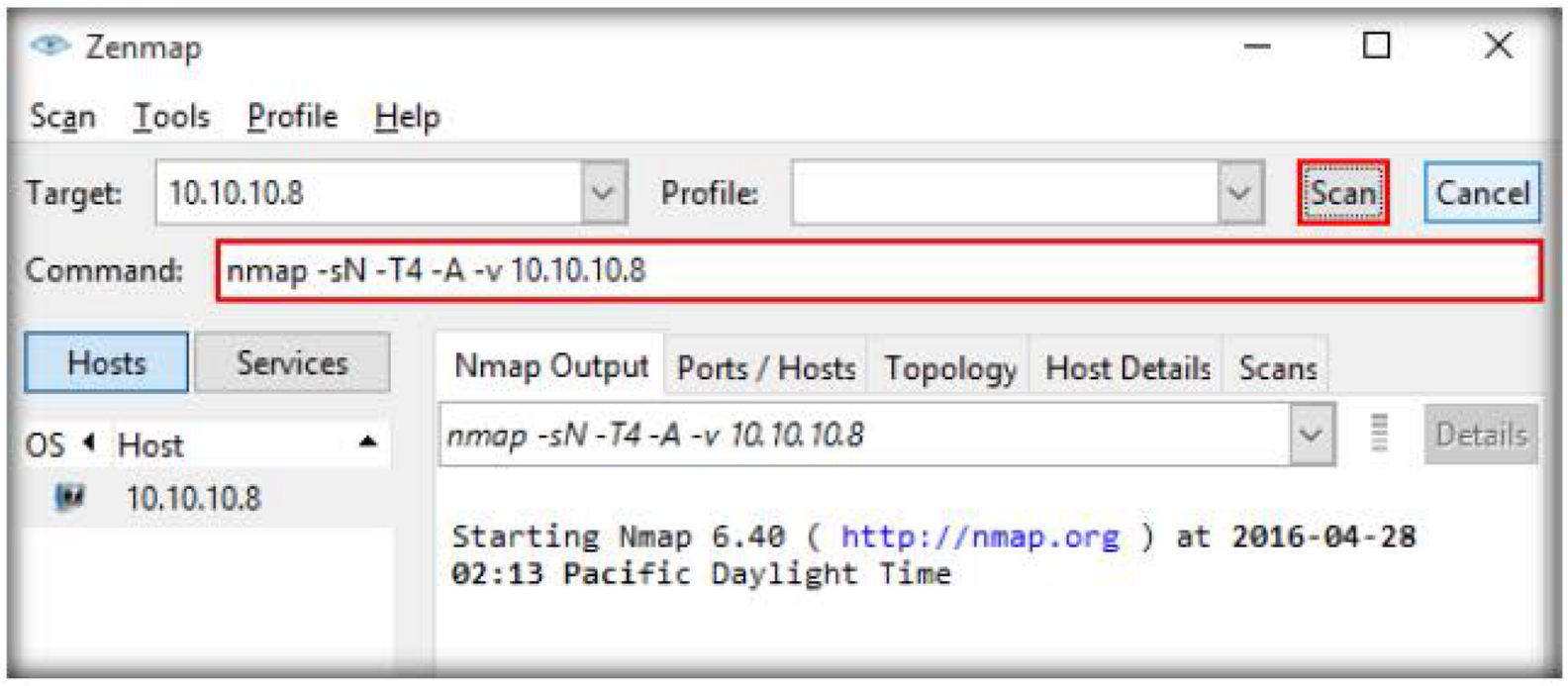



FIGURE 4.8: TCP NULL scan attack using NMAP

22. When the scan completes, switch back to the Windows Server 2012 virtual machine, stop the packet capture and issue the syntax **tcp.flags==0x00** in the **Filter** field. This displays all the packets containing the NULL request and the SYN, ACK response between **Windows 10** and **Windows Server 2008** as shown in the following screenshot:

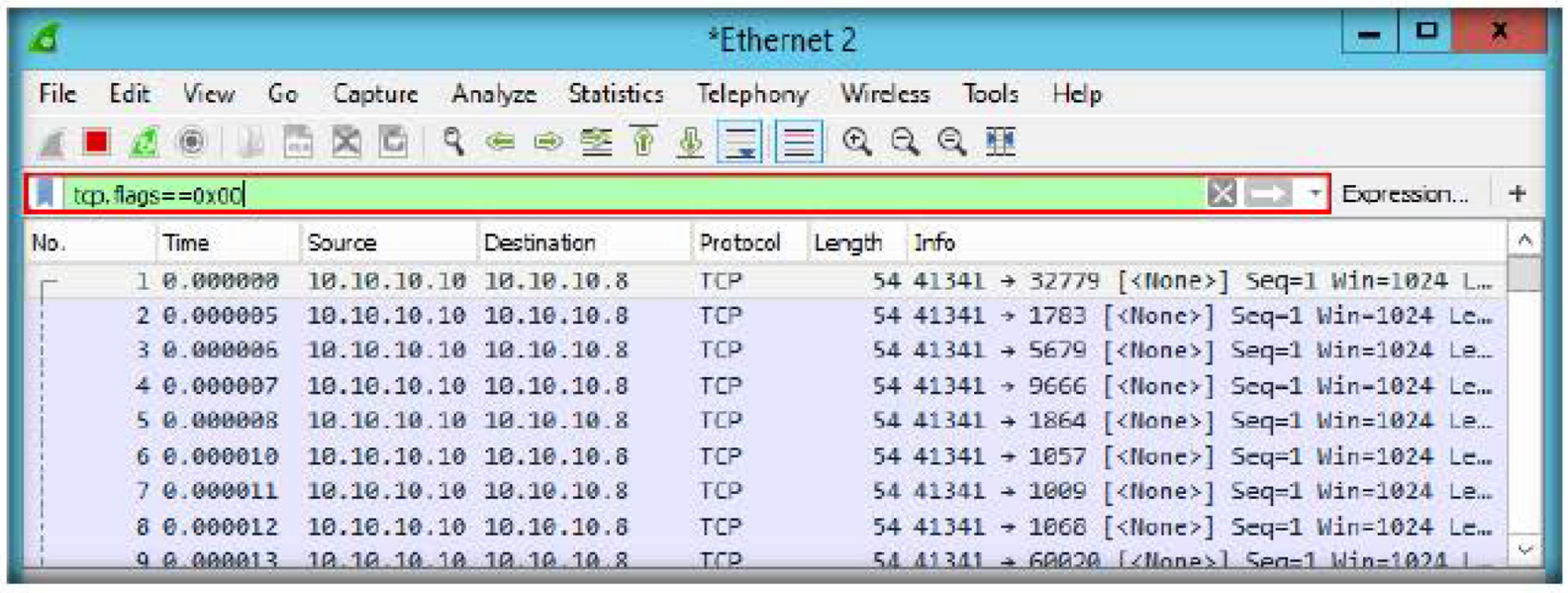



FIGURE 4.9: TCP NULL scan detected in Wireshark

Note: In the above screenshot a lot of packets **have no flag set** in them. They are sent from **10.10.10.10 (attacker) to 10.10.10.8 (target)**. It clearly shows a **TCP null scan attack**.


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

**TASK 4**

**Detecting TCP Xmas scan attempt**

23. Now a demonstration of a **TCP Xmas attack**. In this type of attack, the attacker sends TCP packets with **FIN, PSH and URG** bits set. Just like its NULL counterpart, the **victim's open ports do not reply** and **closed ones reply with an RST packet.** The attacker is **10.10.10.10** and the target is **10.10.10.8**.

Note: Since **URG is used to enhance the priority of a packet** and **PSH is used to push the data**; now with these two flags set, if **FIN (finish) is also set** it means that the **connection should be closed**. Now, two flags indicate data to be pushed and in fact pushed urgently and at the same time another flag asks to terminate the connection. So this packet is meaningless. It is only sent to check open ports.

24. Begin a new Wireshark packet capture in the Windows Server 2012 virtual machine.
25. Switch to the Windows 10 virtual machine, launch Nmap, type the command **nmap -sX -T4 -A -v 10.10.10.8** in the **Command** field then click **Scan**.

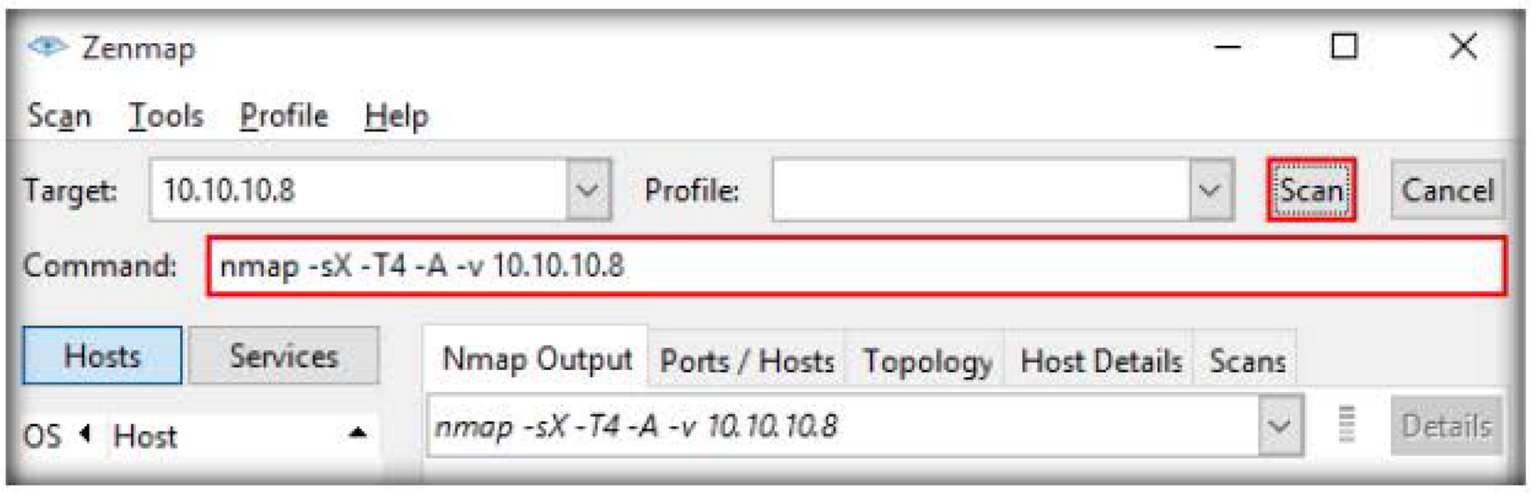



FIGURE 4.10: TCP Xmas attack in Wireshark

The Xmas Scan exploits a subtle loophole in the TCP RFC to differentiate between open and closed ports. This scan sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.

26. Switch to the **Windows Server 2012** virtual machine, stop the Wireshark packet capture, and issue the syntax **tcp.flags==0x029** in the filter field to detect a Xmas scan.

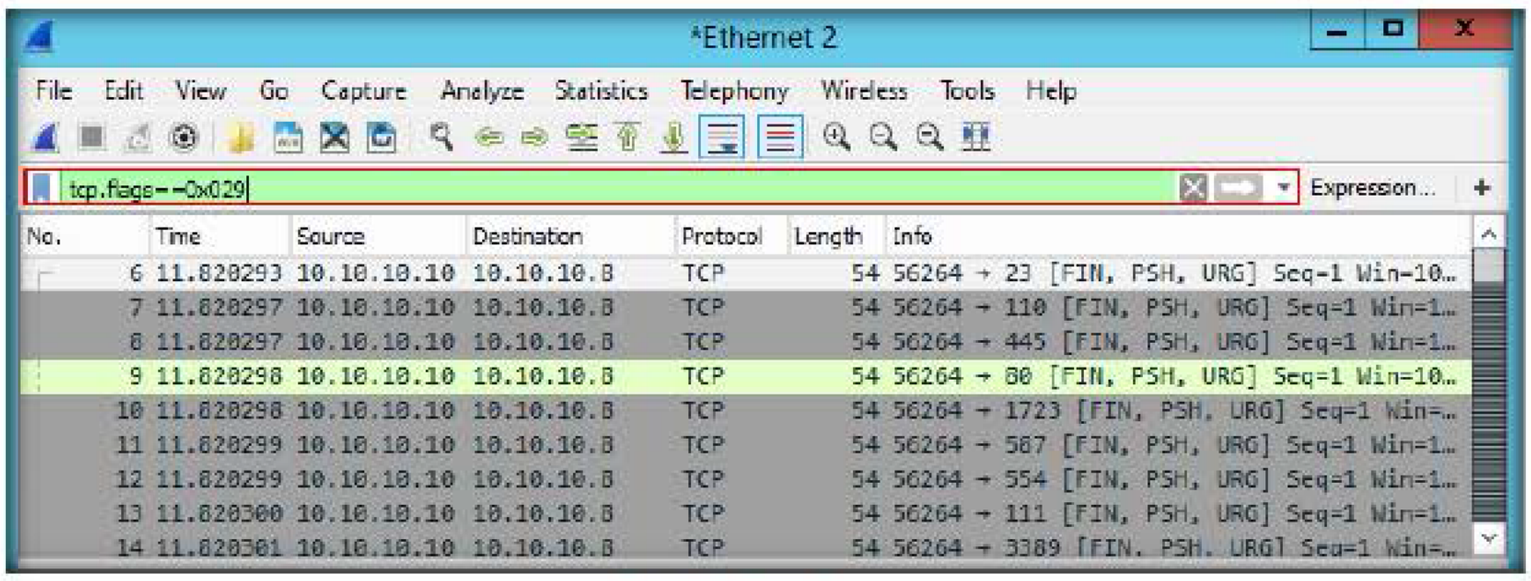



FIGURE 4.11: TCP Xmas attack

27. In the above scenario we can clearly see that the target machine is flooded with packets in which **FIN, PSH and URG bits are set**. So it can be concluded that a TCP **X-mas** scan was performed.


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

**TASK 5**

**Detecting SYN/FIN Attack**

28. The next attach to take a look at is the **DDOS attack** which is also called a **SYN/FIN attack**. In this type of attack, the attacker floods the victim with packets in which both the **SYN** and **FIN** flags are set.
29. The attacker machine's IP Address is **10.10.10.10** (Windows 10) and the target machine's IP Address is **10.10.10.8** (Windows Server 2008).
30. Begin a new Wireshark packet capture in the Windows Server 2012.
31. Switch to the **Windows 10** virtual machine, launch Nmap, type the command **nmap --scanflags synfin 10.10.10.8** in the **Command** field then click **Scan**.

A SYN scan is the default and most popular scan option for good reasons. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by restrictive firewalls.

A Fin Scan exploits a subtle loophole in the TCP RFC to differentiate between open and closed ports. It sets just the TCP FIN bit.

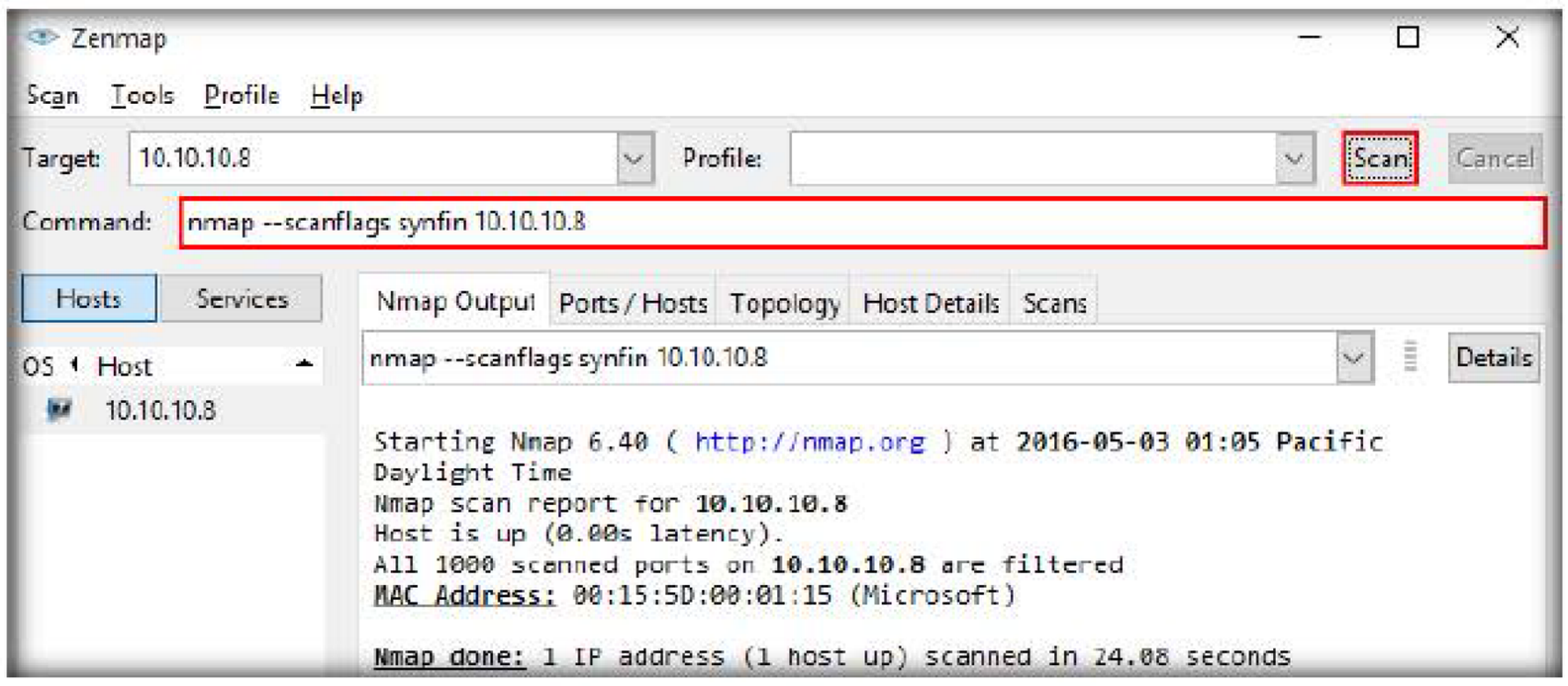



FIGURE 4.12: Attacker Implementing syn/fin Attack

32. When the scan completes, switch to the Windows Server 2012 virtual machine, stop the Wireshark packet capture, and issue the syntax **tcp.flags==0x003** in the Filter flag. You will observe packets containing the **SYN** and **FIN** flags as seen in the list view pane of Wireshark and as shown in the following screenshot:

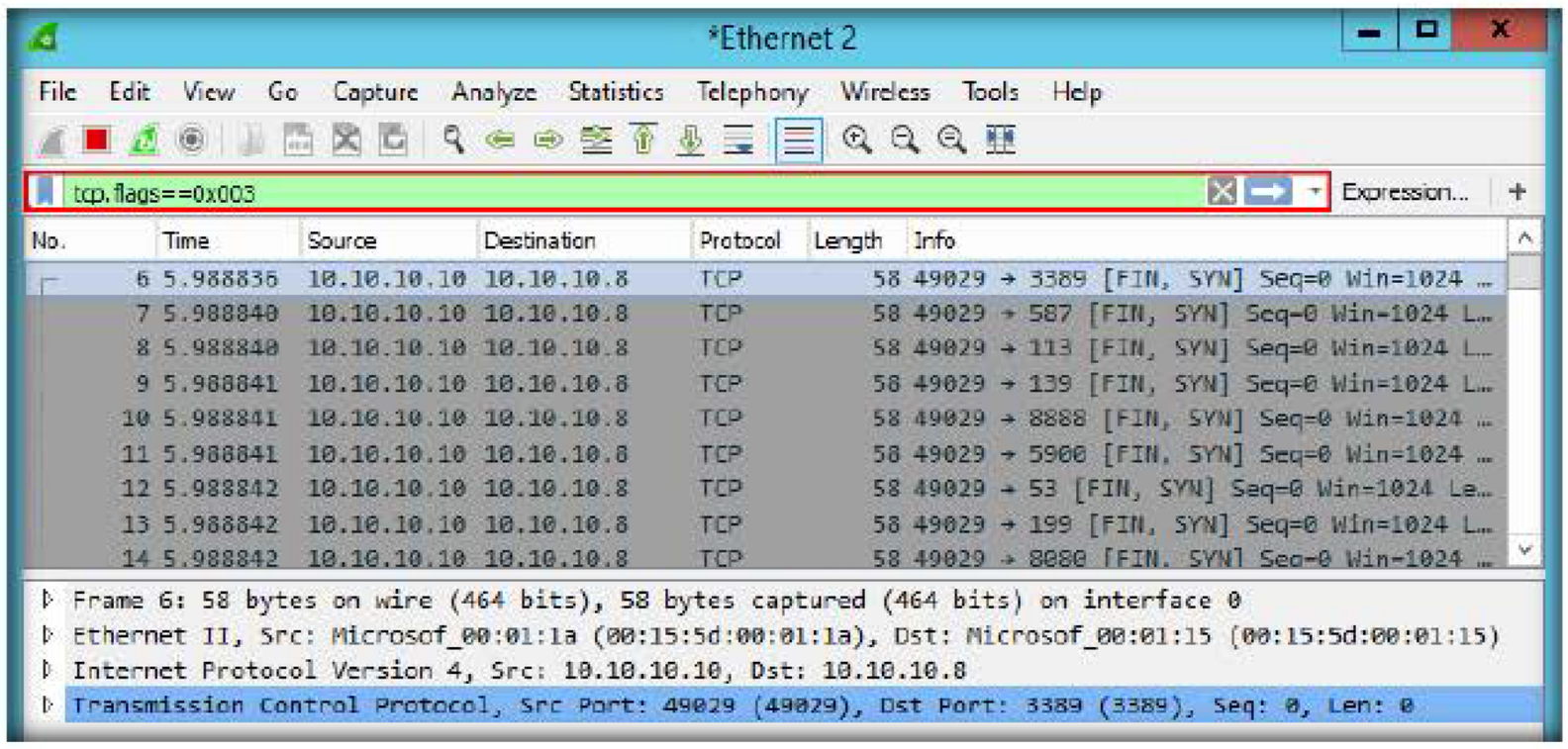



FIGURE 4.13: SYN/FIN Attack Detected in Wireshark



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

**TASK 6**

**Detecting ARP sweep attempt**

33. Now, we shall perform an ARP sweep scan which is used to detect live hosts on a network. In this type of scan, the **attacker broadcasts numerous ARP packets** requesting the **MAC addresses of all the machines**.
34. The attacker's IP address is **10.10.10.10** (Windows 10) and he sends out ARP broadcast packets in the entire network of 10.10.10.*. The Nmap command to scan the entire subnet is **nmap -sn 10.10.10.0/24**.
35. Launch Nmap in the Windows 10 machine, type the command **nmap -sn 10.10.10.0/24** in the Command field then click **Scan**.

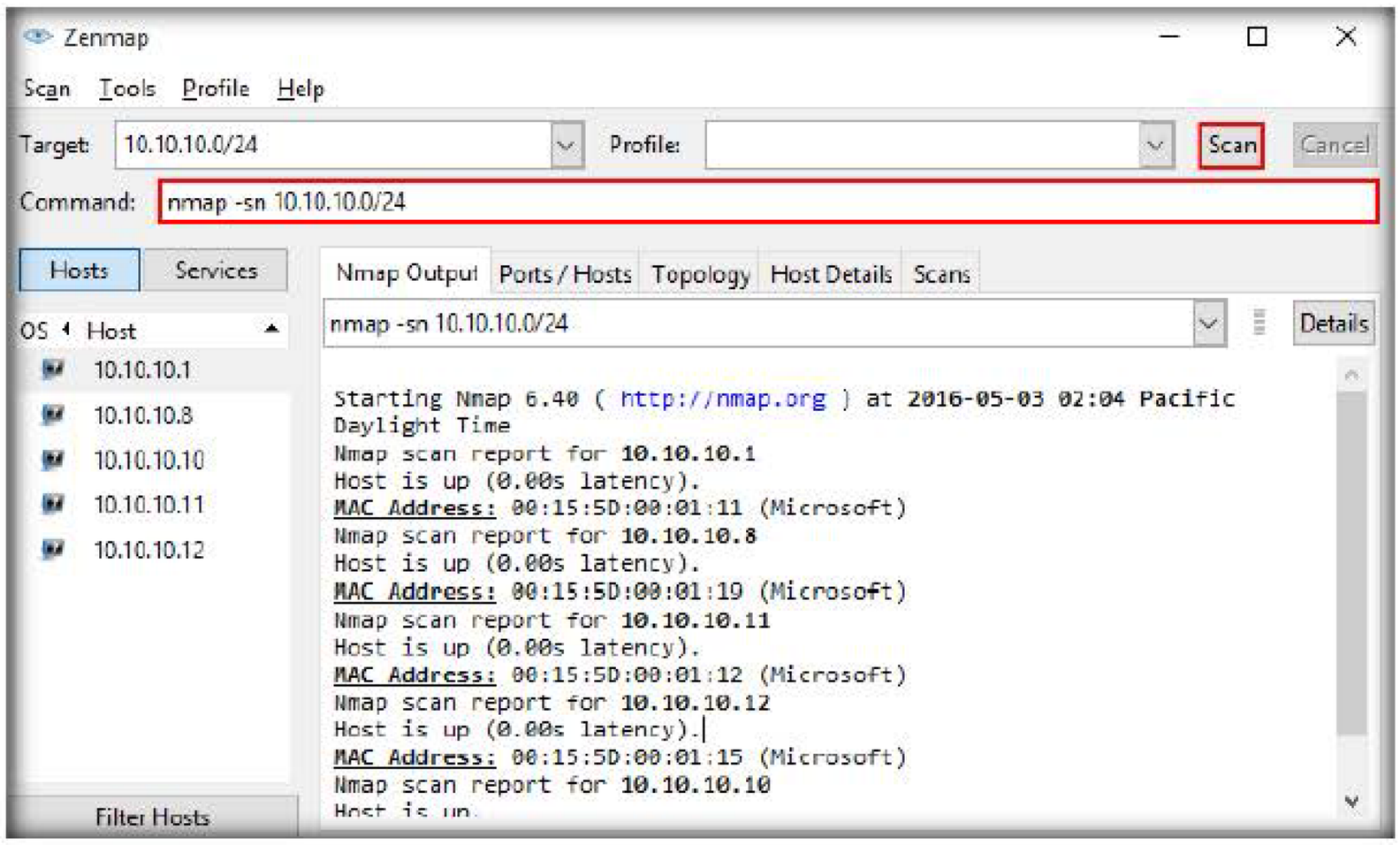



FIGURE 4.14: Attacker scanning for live hosts in the network

This option tells Nmap not to do a port scan after host discovery, and only print out the available hosts that responded to the host discovery probes. When a privileged user tries to scan targets on a local Ethernet network, ARP requests are used unless --send-ip was specified. The -sn option can be combined with any of the discovery probe types (the -P* options, excluding -Pn) for greater flexibility.

36. Switch to the Windows Server 2012 virtual machine, stop the Wireshark packet capture, and issue the syntax **arp** in the **Filter** field.
37. Wireshark displays all the ARP packets that have been broadcasted in the network, proving that an **ARP sweep attack** has been performed on the network, as shown in the following screenshot:

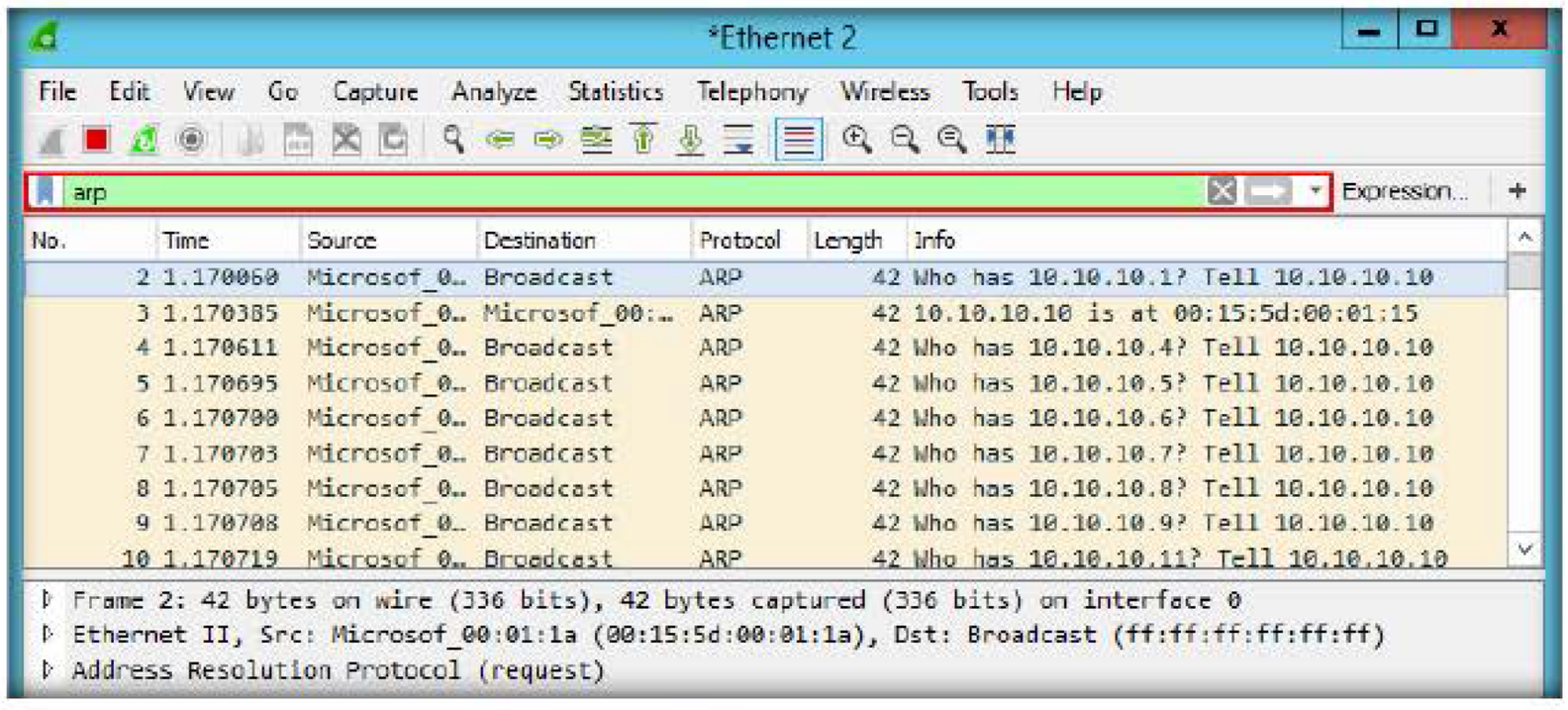



FIGURE 4.15: ARP scan detected in wireshark



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

**TASK 7**

**Detecting Ping Sweep attempt**

31. In this lab, we shall perform a **Ping sweep scan**, which is also **done to test live hosts in a network**. In this scan, an attacker pings a single host, multiple hosts, or even the entire network, in an attempt to discover the live hosts in the network.
32. We will ping the Windows Server 2012 (**10.10.10.12**), Ubuntu (**10.10.10.9**) and Windows Server 2008 (**10.10.10.8**) machines.
33. Before beginning the lab, ensure that you are logged on to the above mentioned machines.
34. Begin a new packet capture in the Windows Server 2012 virtual machine.
35. Switch to the Windows 10 virtual machine, navigate to **Z:\CND-Tools\CND Module 11 Network Traffic Monitoring and Analysis\Packet Sniffing Tools\Wireshark\Cping**, double-click **cping_1.2.1.218.exe**, and follow the wizard driven installation steps to install the Colasoft Ping Tool.

**Note:** Once you double-click the executable, if a **User Account Control** pop-up appears, click **Yes**.

Colasoft Ping is used to ping machines in a network. It supports pinging multiple IP addresses simultaneously and list the comparative responding times in a graphic chart.

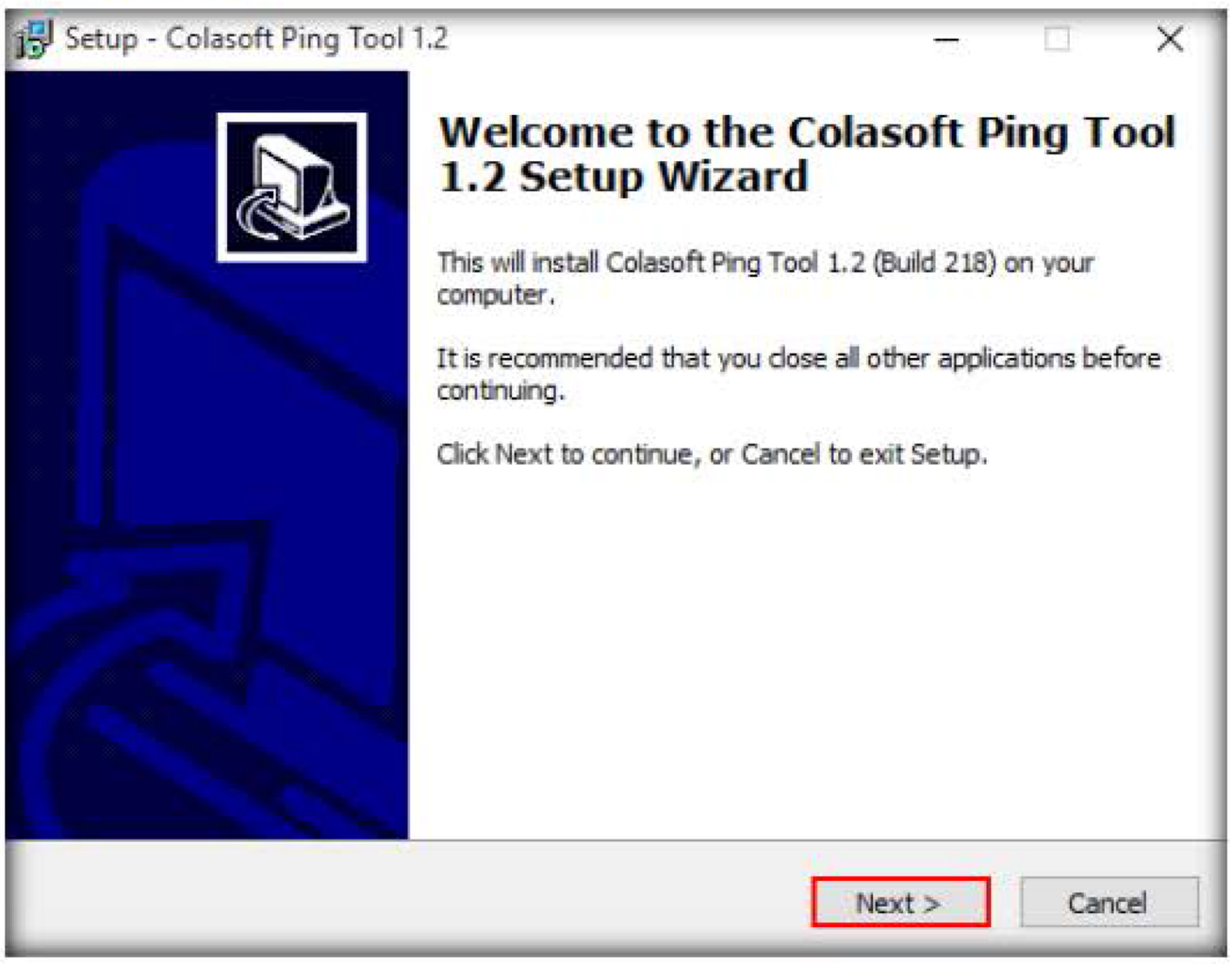



FIGURE 4.16: Installing Colasoft Ping Tool

36. When the installation completes, double-click the **Colasoft Ping Tool** icon on the **Desktop** to launch the application.


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

37. Enter the target IP addresses **10.10.10.8**, **10.10.10.9** and **10.10.10.12** in the **Target** field then click the **Start Ping** button.

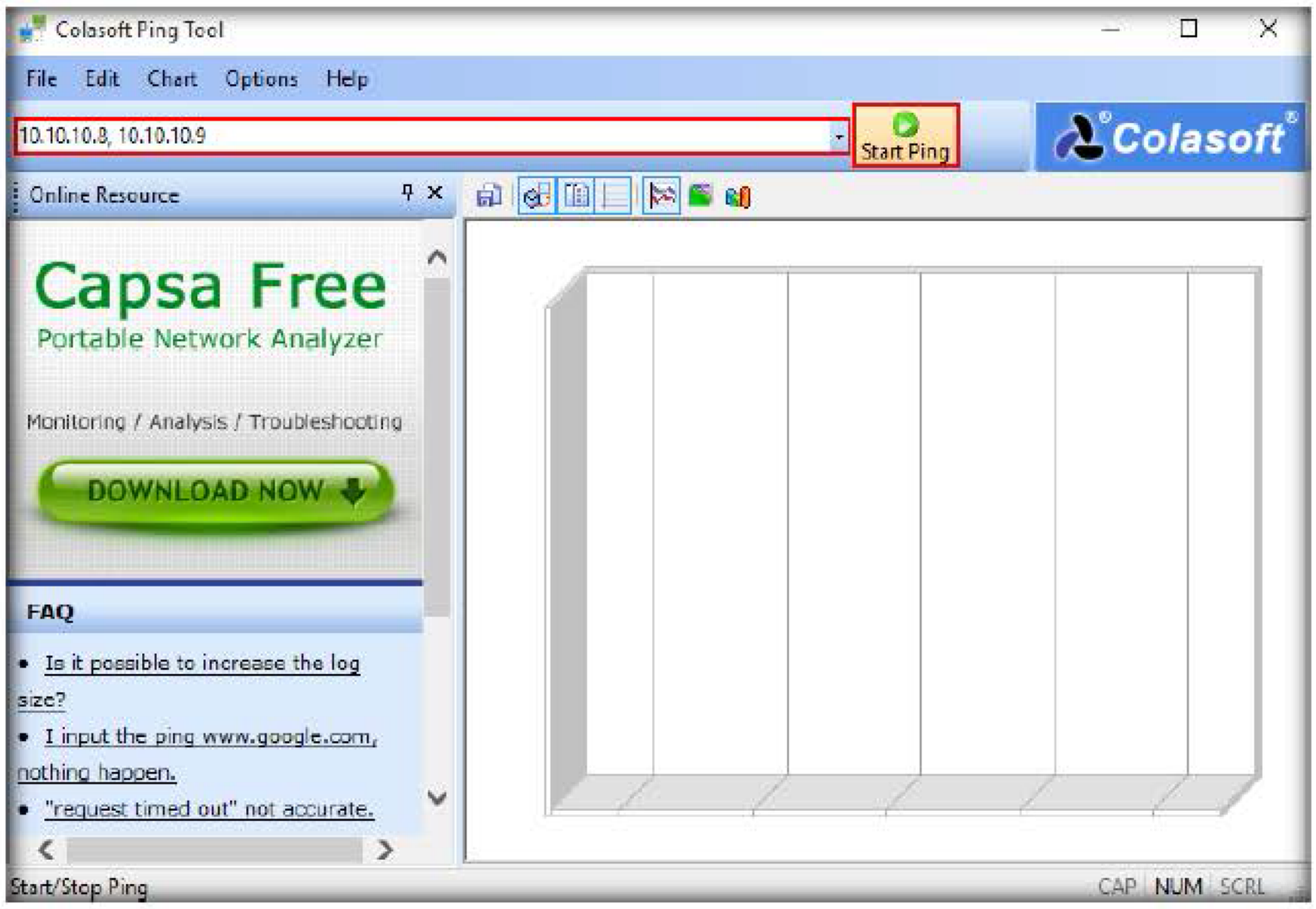



FIGURE 4.17: Cola soft ping tool used to implement ping sweep attack

32. The application begins to ping the machines, and records the response time for those machines which respond to the ping request, as shown in the following screenshot:

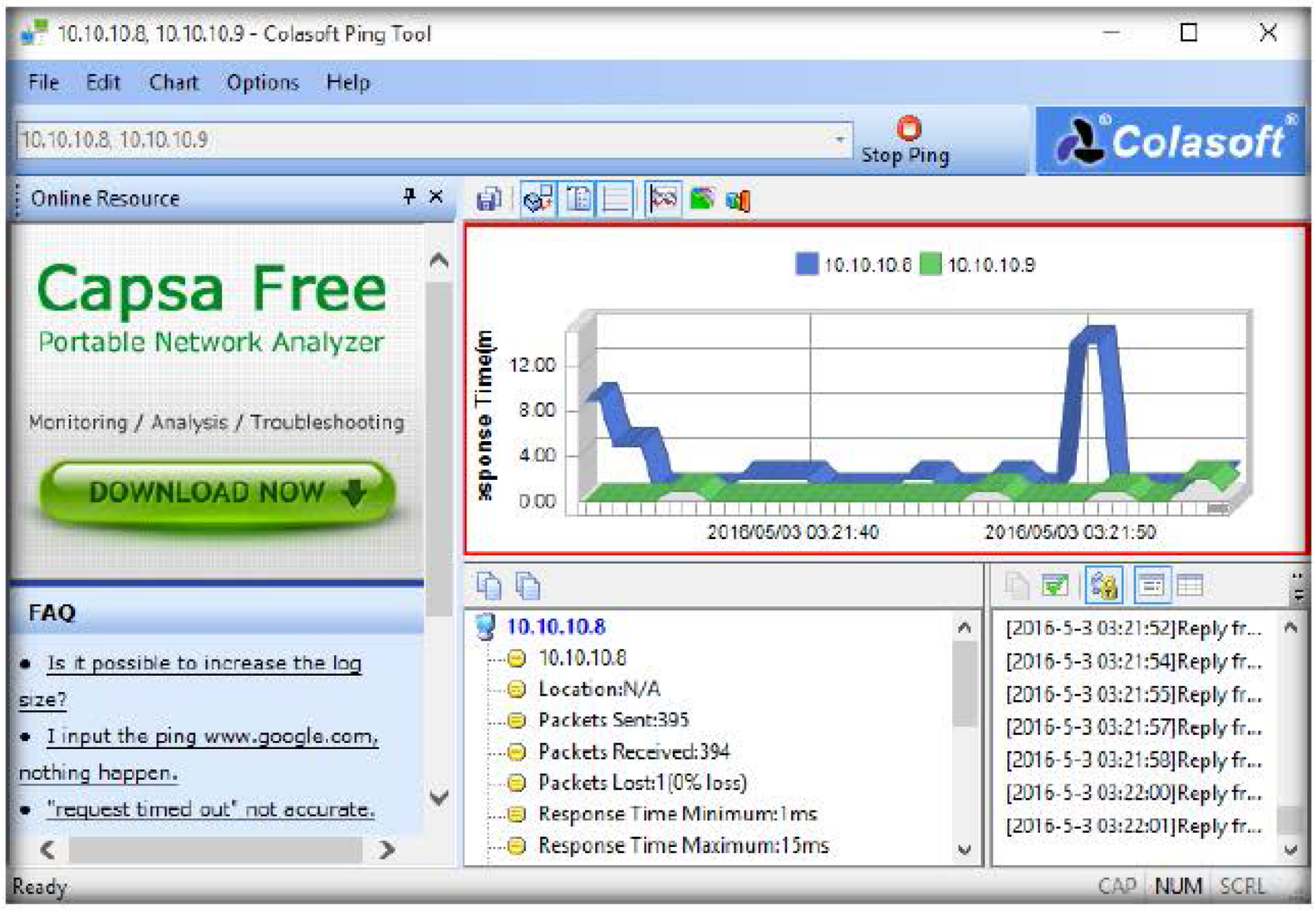



FIGURE 4.18: Results of Colasoft Ping Tool


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

33. Switch to the **Windows Server 2012** virtual machine and stop the Wireshark packet capture.

34. In Wireshark, look out for ICMP packets which are in a sequence of requests and replies. Issue the syntax **icmp.type==8 or icmp.type==0** in the **Filter** field, to detect a ping sweep attack.

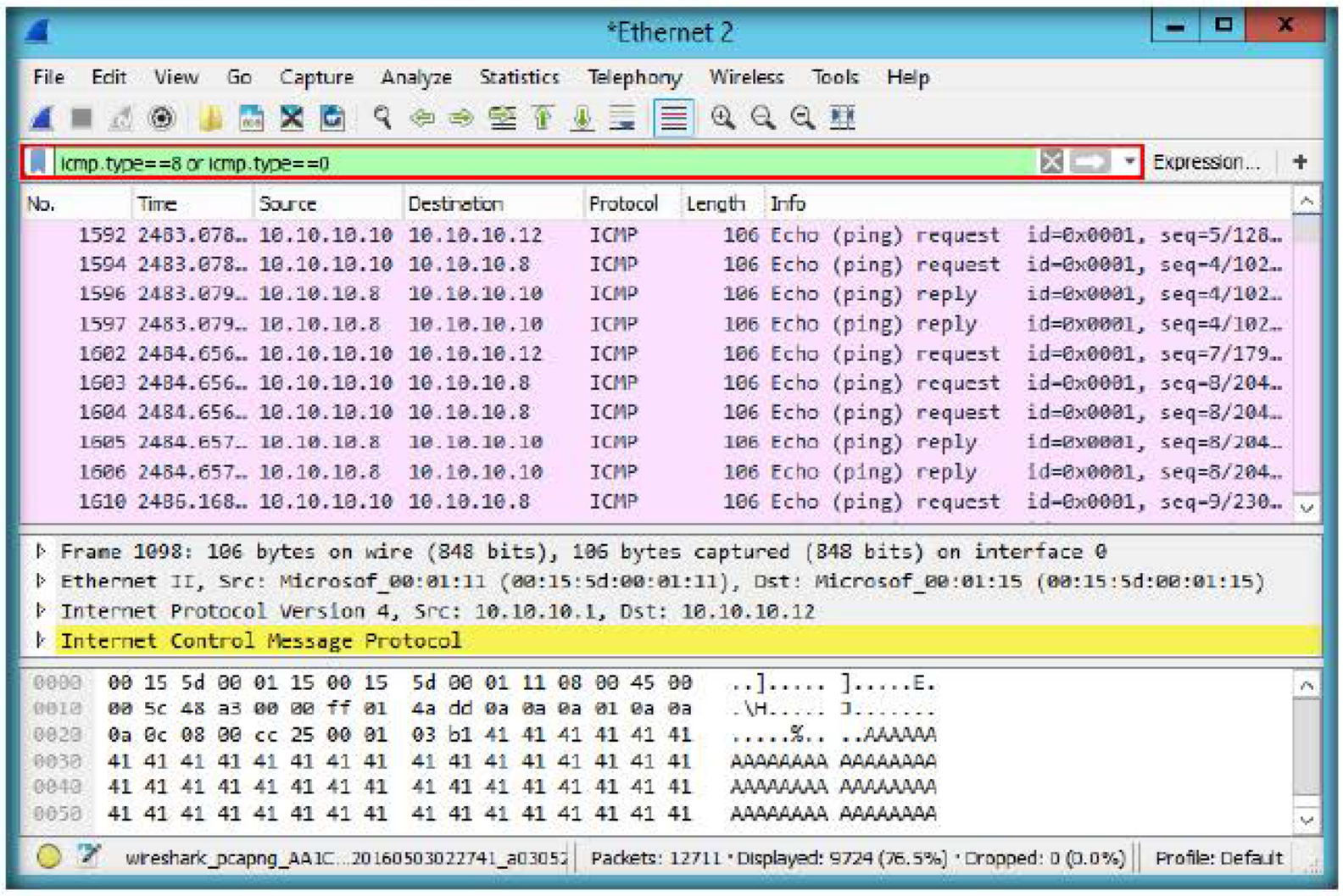



FIGURE 4.19: Ping sweep attack detected in Wireshark

35. Next, we are demonstrating an ARP poisoning attack.

36. Before beginning this lab, start a Wireshark packet capture in the Windows Server 2012 machine.

37. Log on to the **Windows 10** virtual machine, and launch Nmap. Type the command **nmap -Pn --spoof-mac 0 10.10.10.1** (gateway of the network) in the **Command** field then click **Scan**.

Issuing this syntax asks Nmap to use the given MAC address for all of the raw Ethernet frames it sends. This option implies --send-eth to ensure that Nmap actually sends Ethernet-level packets.

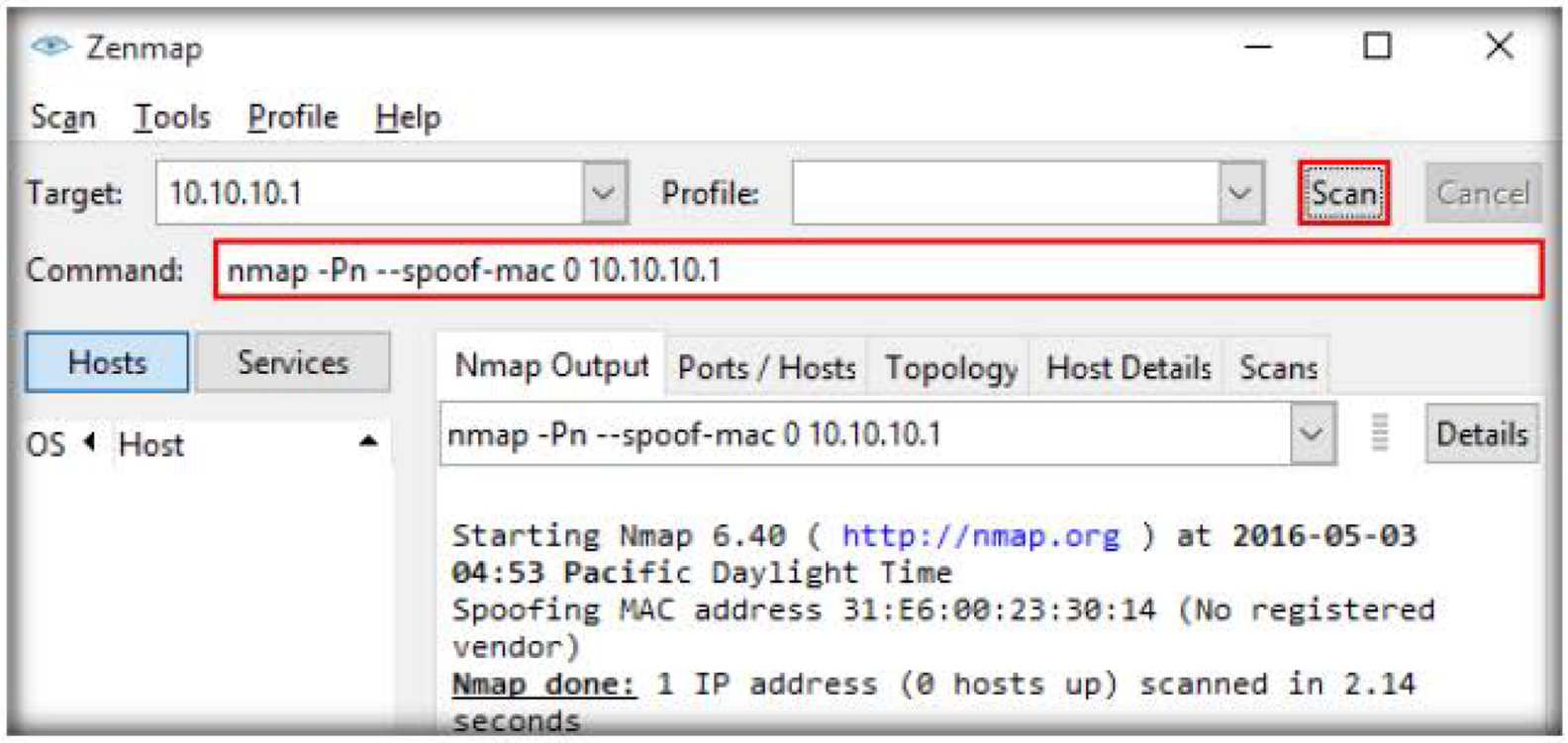



FIGURE 4.20: Implementing ARP poisoning in NMAP


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

38. When the scan completes, switch to the Windows Server 2012 virtual machine and stop the packet capture.
39. Issue the syntax **arp.duplicate-address-detected** in the Filter field to find the packets containing any duplicate IP Addresses.

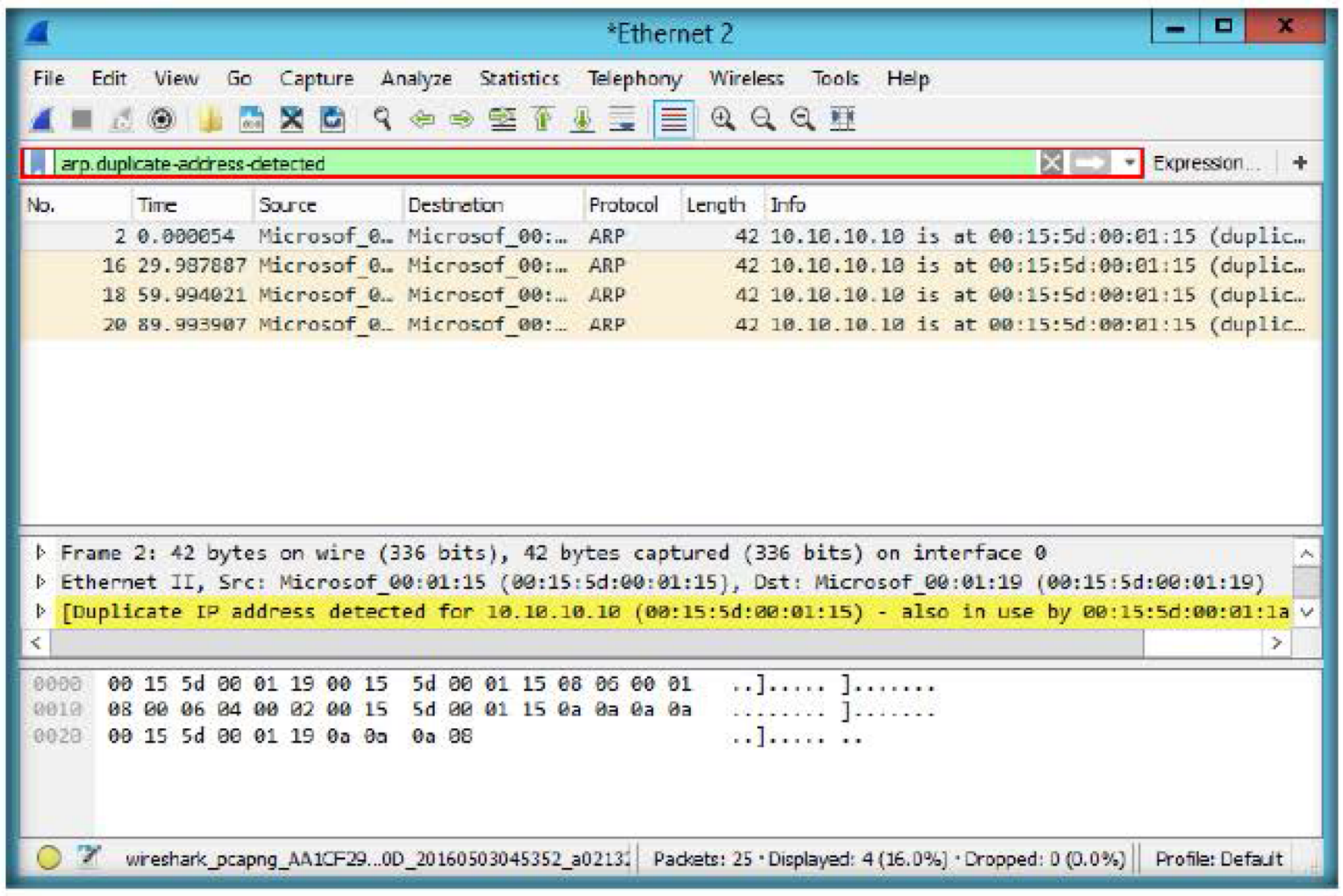



FIGURE 4.21: ARP poisoning attack detected in Wireshark

**TASK 8**

**Detecting FIN scan attempt**

40. Before beginning this lab, start a new Wireshark packet capture in the Windows Server 2012.
41. Switch to the Windows 10 machine, launch Nmap, and type the command **nmap -sF -T4 10.10.10.8** (Windows Server 2008) in the **Command** field then click **Scan**.

The Fin Scan exploits a subtle loophole in the TCP RFC to differentiate between open and closed ports. It Sets just the TCP FIN bit.

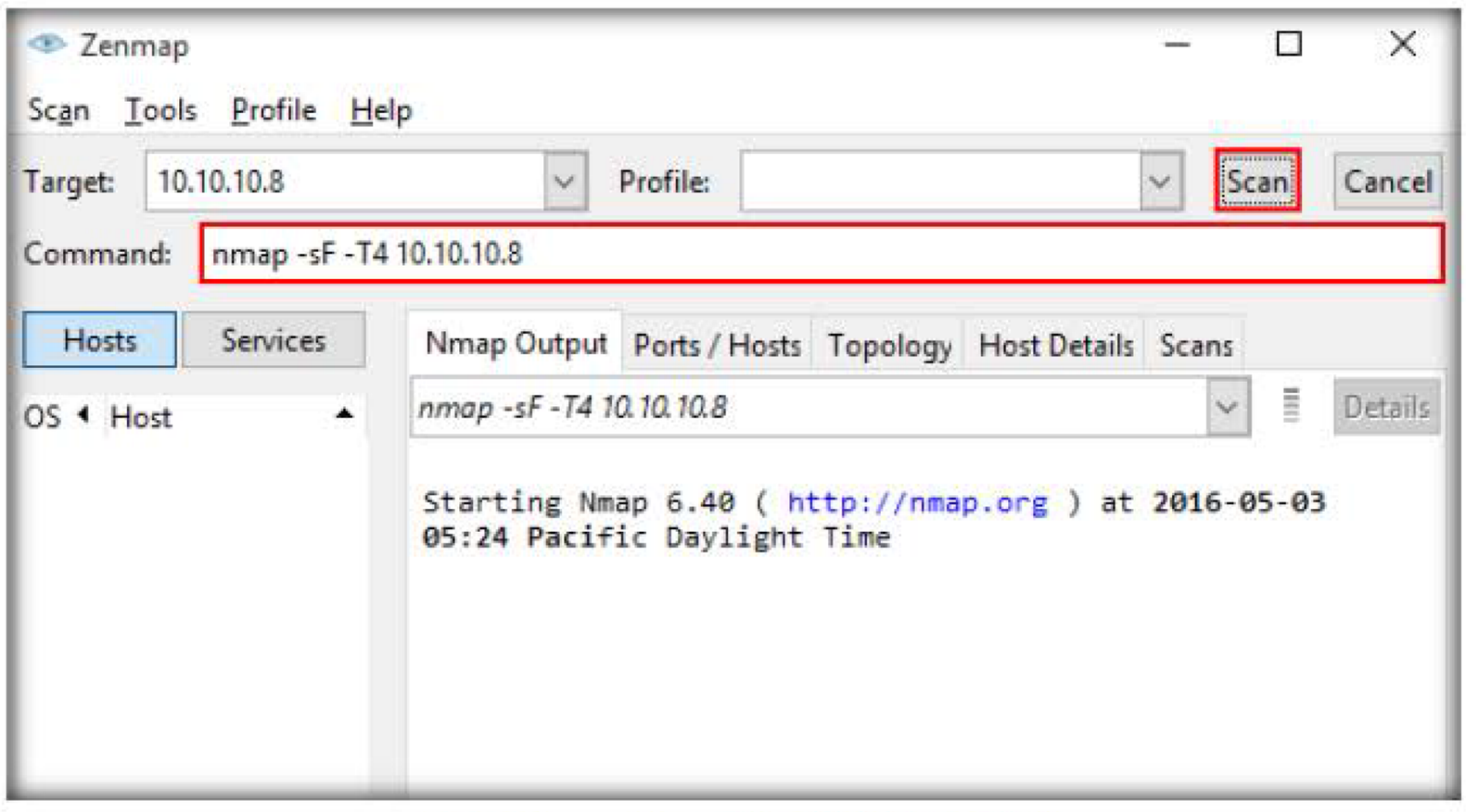



FIGURE 4.22: FIN scan attack performed in Nmap


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

42. Switch back to the Windows Server 2012, stop the Wireshark packet capture and issue the filter **tcp.flags.fin==1** in the **Filter** field.

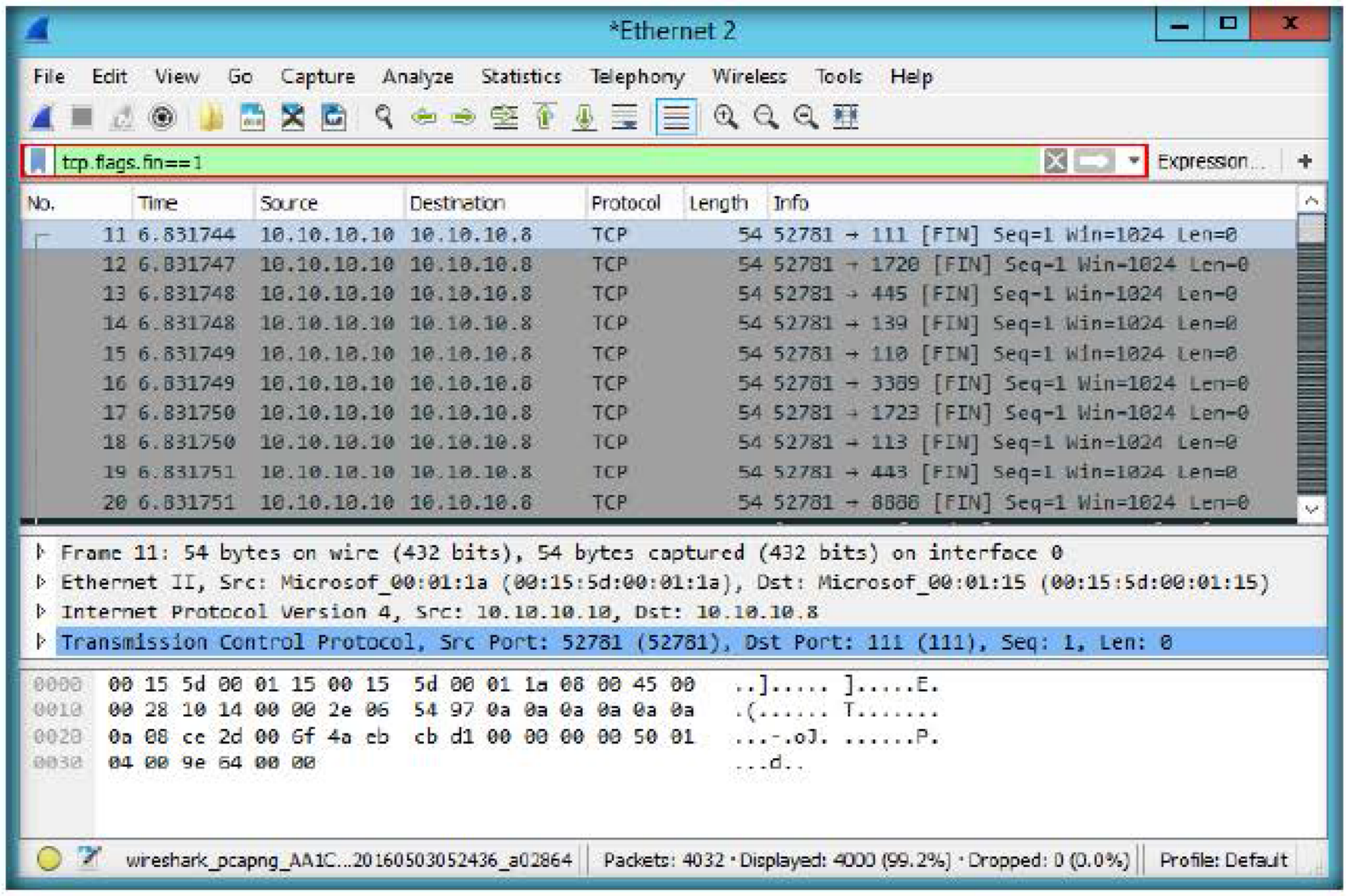



FIGURE 4.23: FIN scan detected in Wireshark

Note: Note the presence of a **FIN packet** which is used to **terminate a connection**, indicating there **has to be a SYN packet** which **started the connection**. Now filter the traffic captured by Wireshark to view the packets containing a **SYN** flag.

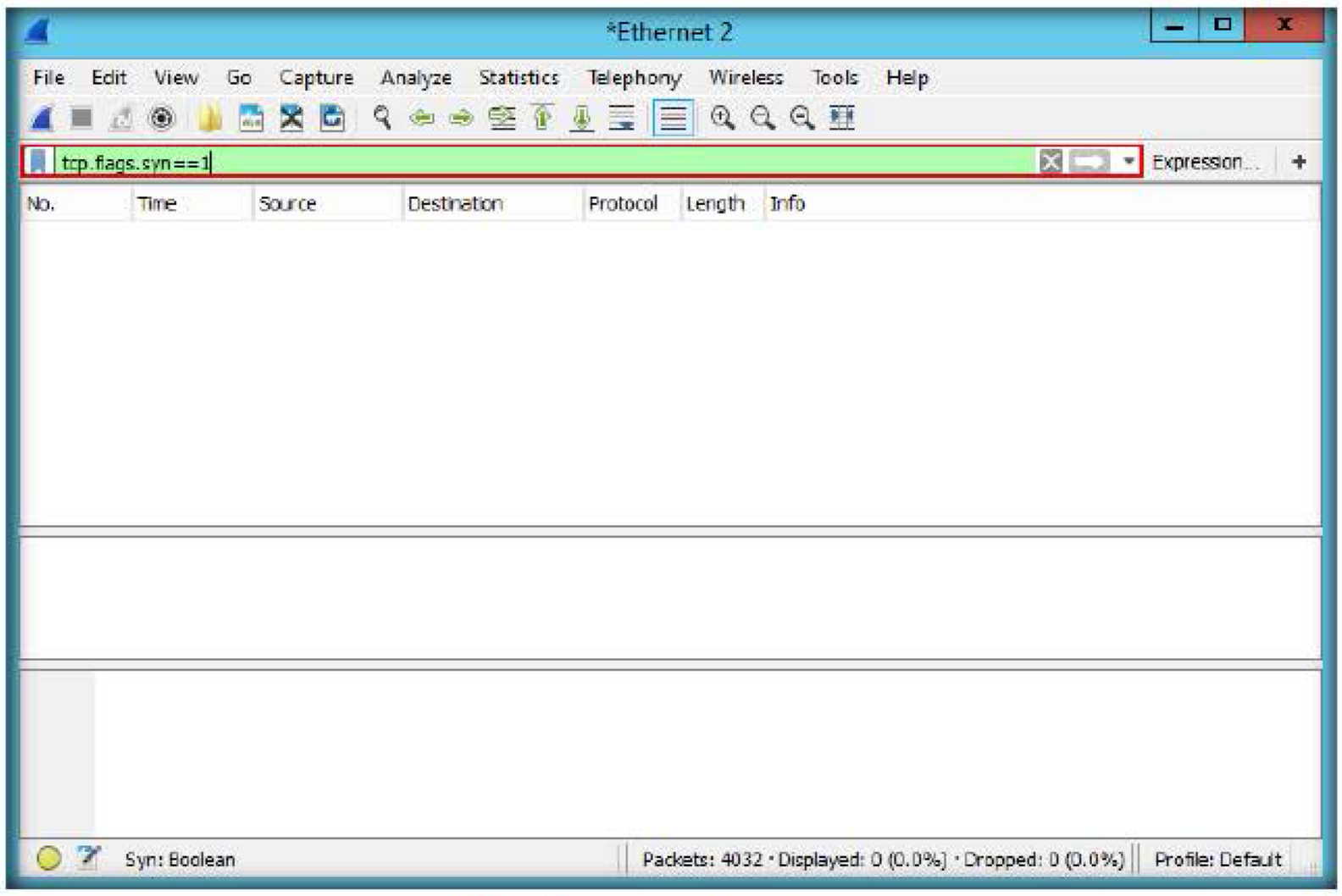



FIGURE 4.24: Absence of SYN packets


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

**Note:** The presence of a huge number of FIN packets which do not have a corresponding SYN packet indicates that a FIN scan has been performed.

**TASK 9**

**Detecting IP Protocol scan attempt**

43. Next is an **IP protocol scan**. This scan is performed in order to know the **IP protocols supported by the target** machine.
44. Before beginning this lab task, start the Wireshark packet capture in the Windows Server 2012 virtual machine.
45. Switch to the Windows 10 machine, launch Nmap, and type the command **nmap -sO -T4 10.10.10.8** (Windows Server 2008) in the **Command** field then click **Scan**.

The attacker sends IP packets without proper headers to the victim (for TCP, UDP, ICMP, SCTP, and IGMP proper headers are sent out). If he gets an ICMP error message on a protocol unreachable (type-3 and code-2), it indicates that the protocol is not in use. If an ICMP message with ICMP port unreachable message (type-3 and code-3) is received, it means that the particular protocol is in use; and some other ICMP message like type-3 and code-0,1,3,9,10 and 13 means that the protocol is filtered. However, in case of TCP, UDP, ICMP, SCTP, and IGMP protocols, if any reply is received on these protocols they are considered to be open. Even if after repeated transmission, a protocol does not respond in any way, it is categorized as open or filtered.

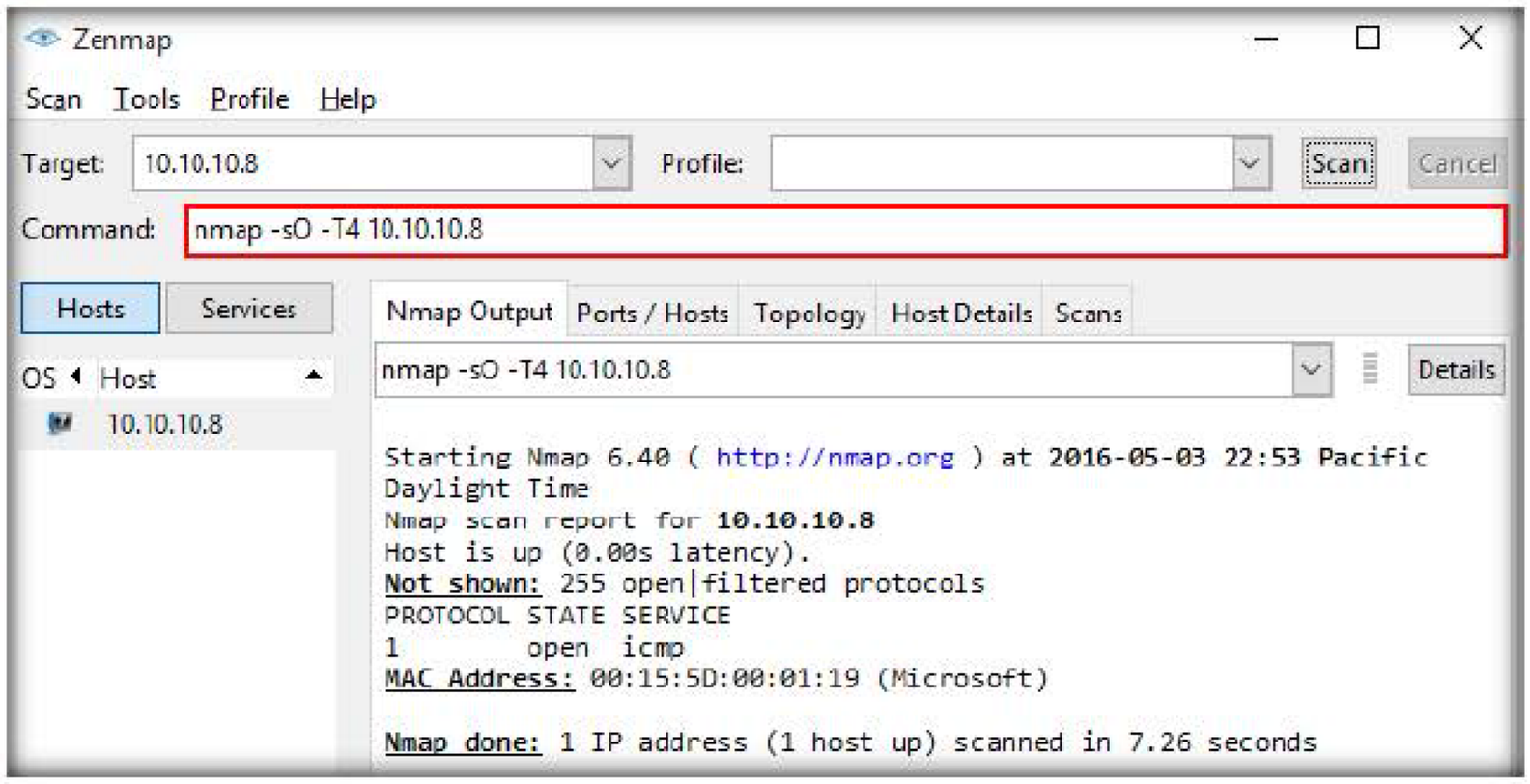



FIGURE 4.25: IP protocol scan attack implemented using NMAP

**Note:** The scan result might vary in your lab environment.

46. Now of the **total 256 protocols** present, it shows that **ICMP is open** and the rest of the **255 are either open or filtered** which indicates they never replied even after repeated transmissions.
47. To detect an ICMP protocol, use the code **icmp.type==8 or icmp.type==0**, which is used as an ICMP request and reply packet respectively.

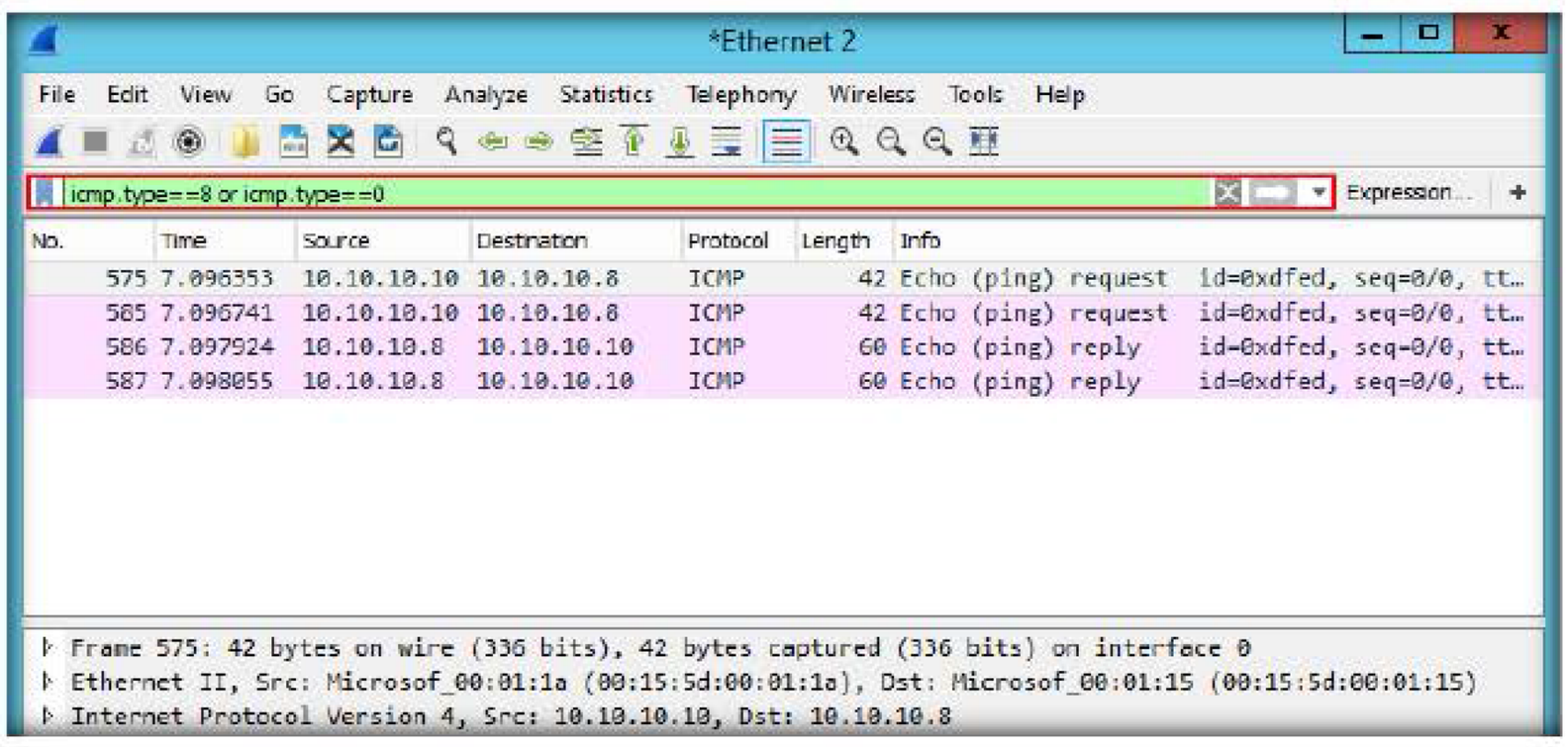



FIGURE 4.26: ICMP packet request and reply indicating that icmp protocol is used



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

**TASK 10**

**Detecting ACK scan attempt**

48. Now we shall demonstrate an **ACK scan attack**, which is used to know the **nature of a protocol** on the target machine.

Note: A protocol can be either **stateless or stateful**. A **stateless protocol only blocks SYN packets** from unidentified networks, but **allows ACK packets** because it thinks it might be an acknowledgement for an earlier packet. A **stateful** protocol keeps track of the connection and **blocks unsolicited ACK packets**, if there were no corresponding SYN packets for them.

**If a port replies with a RST packet**, the port is unfiltered, which means the **firewall was stateless**, and **no reply** indicates that the **firewall was stateful**.

49. Before beginning this lab task, start a new Wireshark packet capture in the Windows Server 2012.

50. Switch to the Windows 10 machine, launch Nmap, and type the command **nmap -sA -T4 10.10.10.8** (Windows Server 2008) in the **Command** field then click **Scan**.

This scan is different than the others discussed so far in that it never determines open (or even open|filtered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

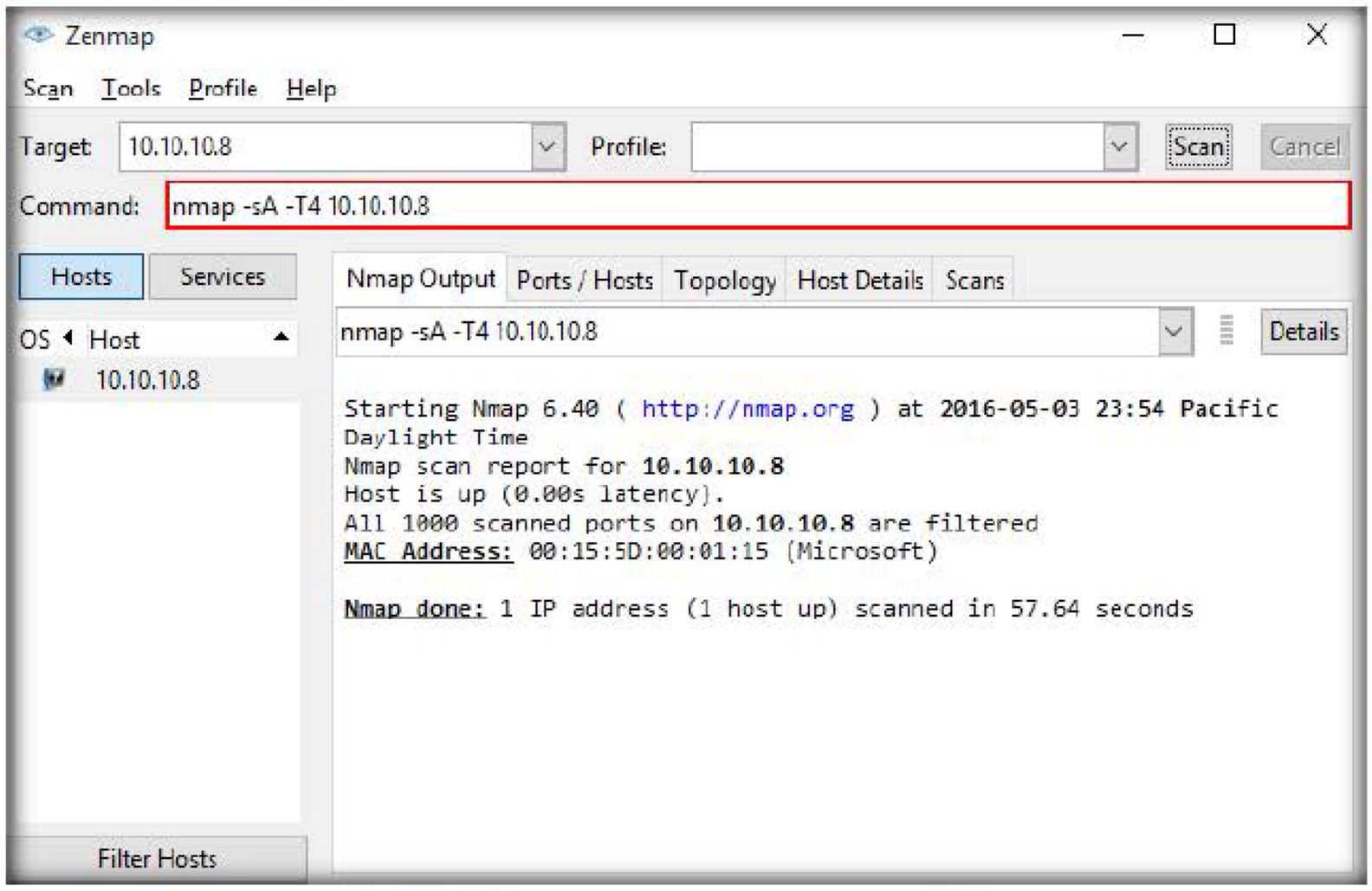



FIGURE 4.27: ACK attack implemented through NMAP

51. Switch to the Windows 10 machine, and stop the Wireshark packet capture, when the scan completes.

52. The reply shows **all ports are filtered**, which indicates the **firewall was stateful**. So there should not be any replies containing a RST packet.

53. Our primary task is to check for ACK packets sent from the attacker machine to the target machine. To check, type the syntax **tcp and ip.src==10.10.10.10** in the **Filter** field.



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

54. First check Wireshark using the code **tcp and ip.src==10.10.10.10** to look for ACK packets from the attacker to the victim.

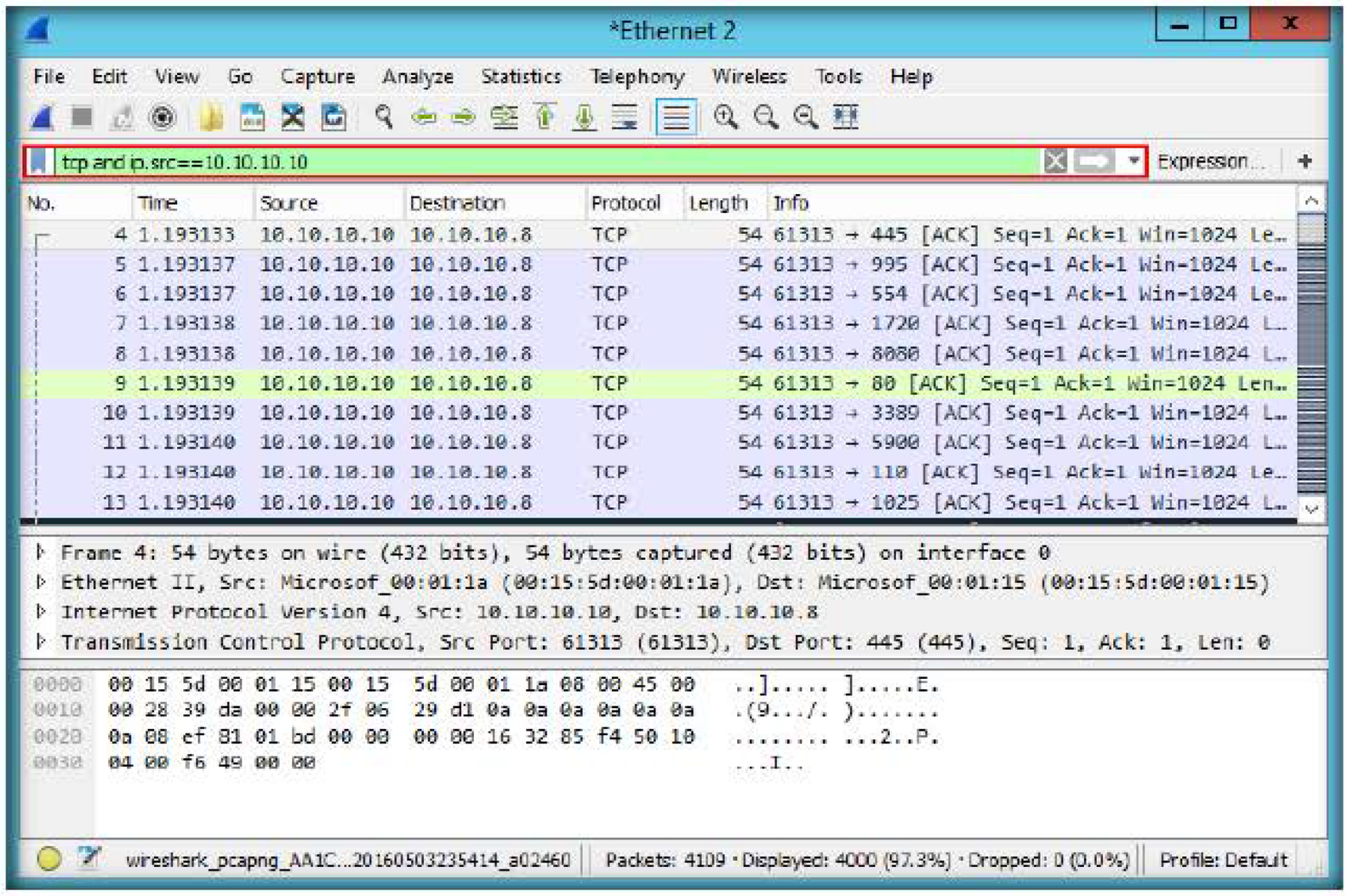



FIGURE 4.28: ACK packets from the attacker to the victim

55. Next, we must filter Wireshark for the RST packets from the victim to the attacker, which confirms that the firewall was a stateful firewall. Use code **ip.src==10.10.10.8 and ip.dst==10.10.10.10 and tcp.flags.reset==1**.

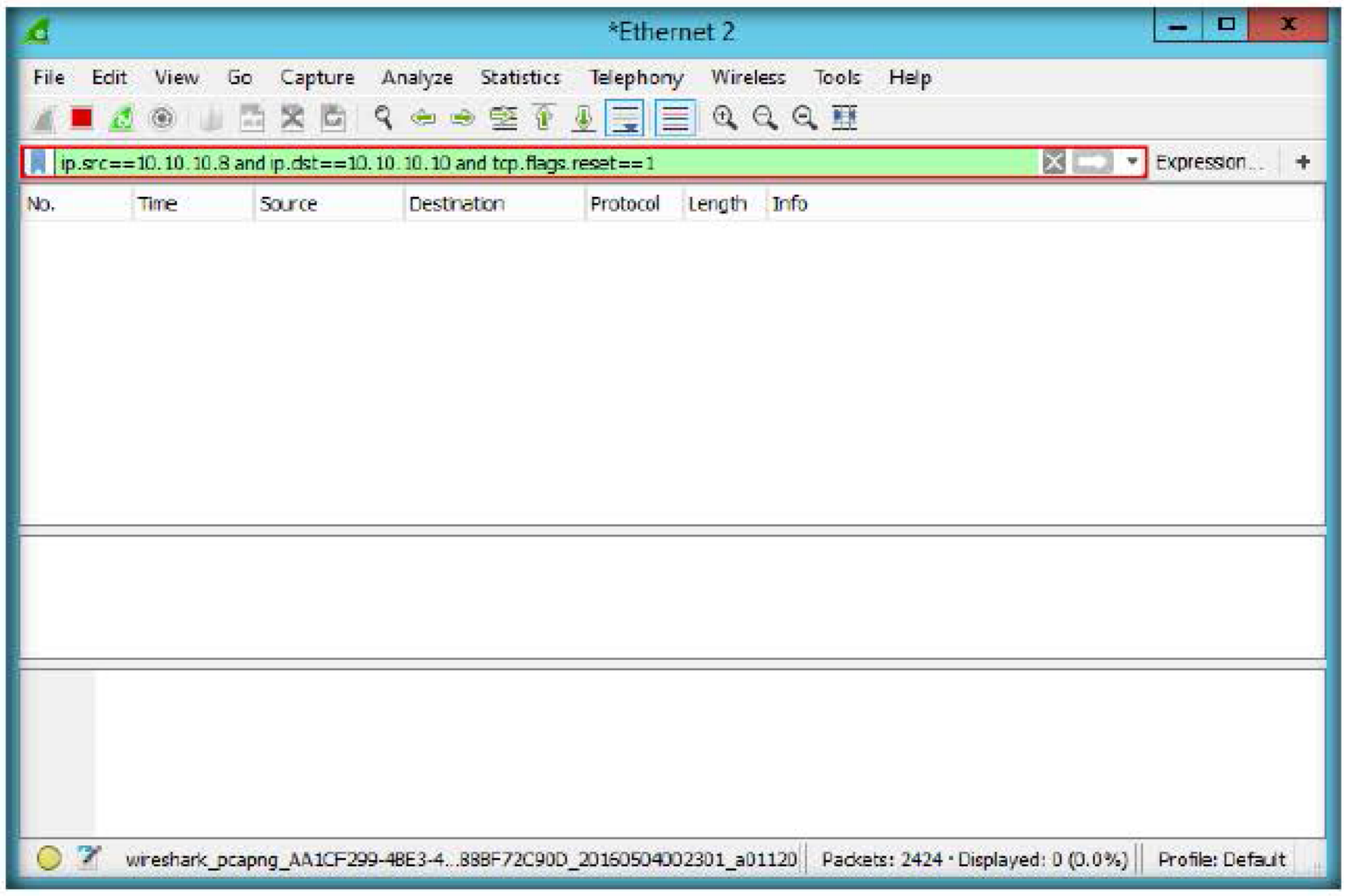



FIGURE 4.29: RST packets from victim to the attacker confirming the firewall was stateless


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

56. There is no trace of a RST reply, which concludes the firewall is in fact a stateful firewall.

**TASK 11**

**Detecting Nmap Maimon attempt**

57. Our next lab task is to perform a Nmap Maimon scan. In this type of scan, the attacker machine sends FIN/ACK packets to the target machine. The ports which respond with a RST packet are considered to be closed and the ports which do not reply and drop the packets are open.

58. Before beginning this lab task, start a new Wireshark packet capture in the Windows Server 2012.

59. Switch to the Windows 10 virtual machine, launch Nmap, type the command **nmap -sM -T4 10.10.10.8** (Windows Server 2008) in the **Command** field then click **Scan** to perform a Maimon scan.

The Maimon scan is named after its discoverer, Uriel Maimon. He described the technique in Phrack Magazine issue #49 (November 1996). Nmap, which included this technique, was released two issues later. This technique is exactly the same as the NULL, FIN, and Xmas scans, except that the probe is FIN/ACK.

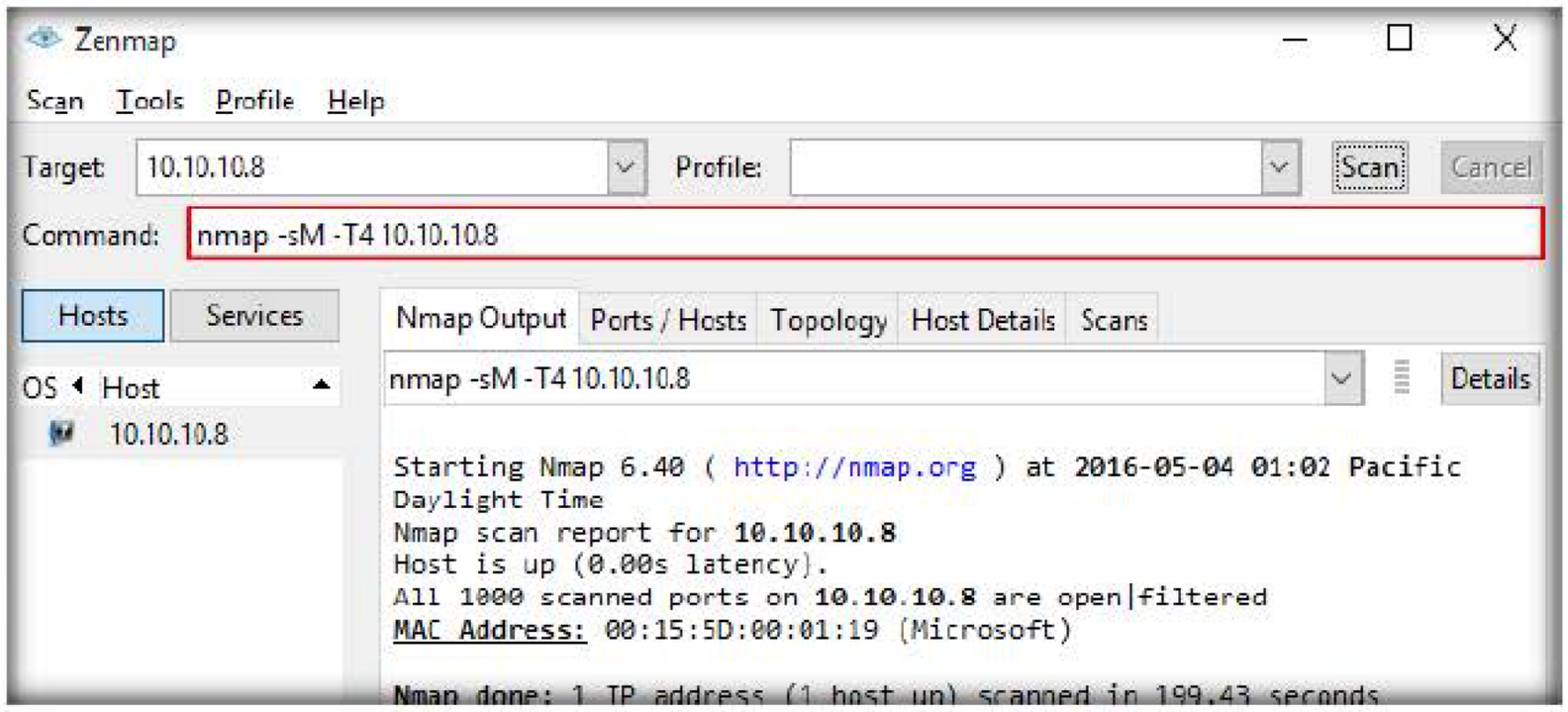



FIGURE 4.30: Maimon scan implemented using NMAP

60. The result says that all the ports are **open | filtered**, which signifies there is a firewall behind the host, and you cannot find any open ports.

61. Switch to the Windows Server 2012, stop the Wireshark packet capture, and issue the syntax **tcp.flags.fin==1 and tcp.flags.ack==1** in the **Filter** field.

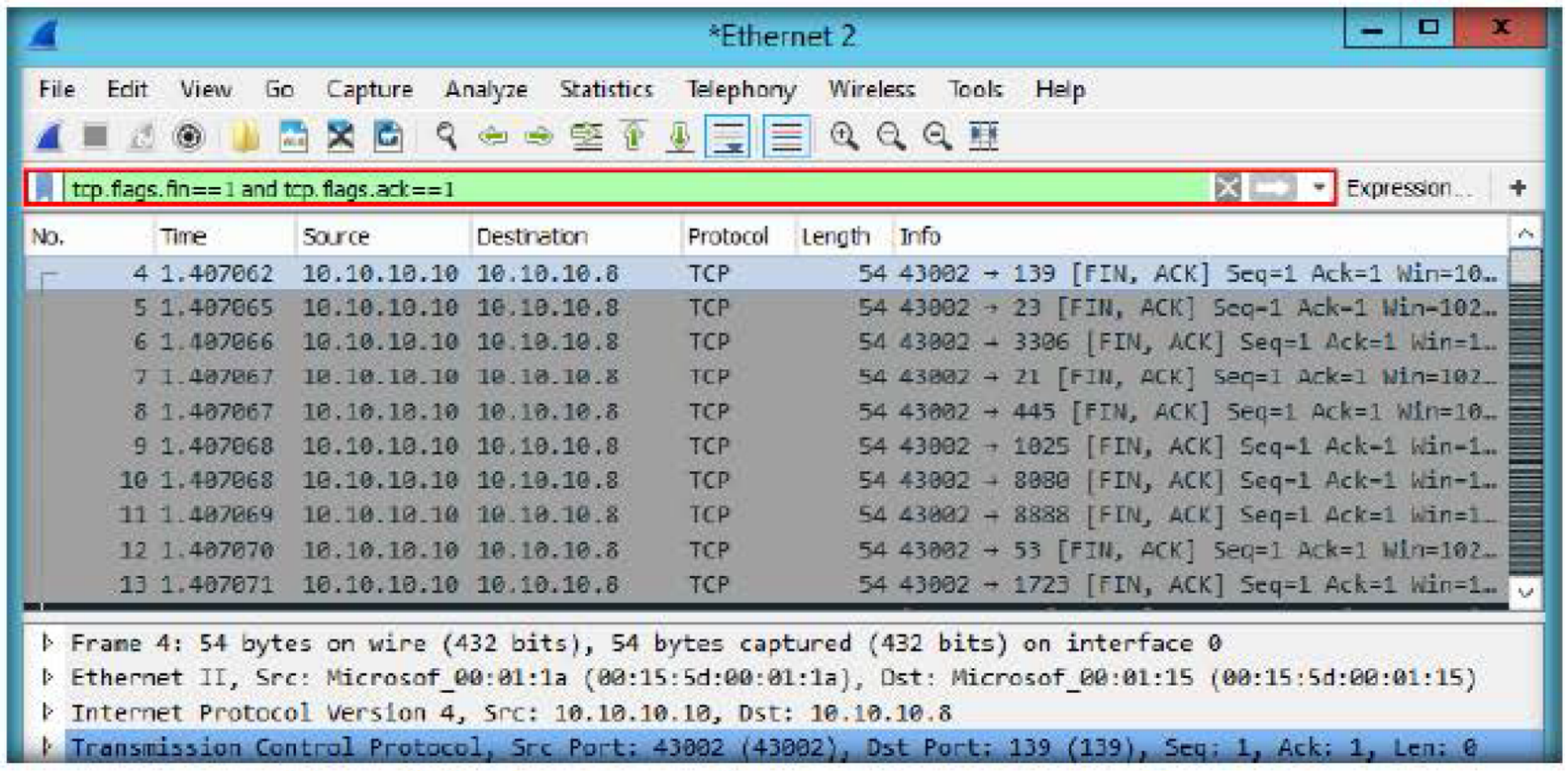



FIGURE 4.31: FIN/ACK packets sent as part of Maimon scan detected in Wireshark



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

**TASK 12**

**Detecting a null scan decoy attempt**

62. Next is the demonstration of the **Decoys option**. It is used with **-D switch in Nmap**. In this type of scan, you can merge a few other hosts along with you as decoys and perform a scan on any system. It does not hide your IP but makes it one among the decoys and difficult to guess as to who performed it.
63. Now we implement a Null scan using two Decoy IP addresses **10.10.10.11** and **10.10.10.12**.
64. Before beginning the lab task, start a new Wireshark packet capture in the Windows Server 2012.
65. Switch to the Windows 10, launch Nmap, type the command **nmap -sN -T4 -D 10.10.10.11,10.10.10.12 10.10.10.8** in the **Command** field then press **Scan** to implement the Null scan.

This Nmap syntax causes a decoy scan to be performed, which makes it appear to the remote host that the host(s) you specify as decoys are scanning the target network.

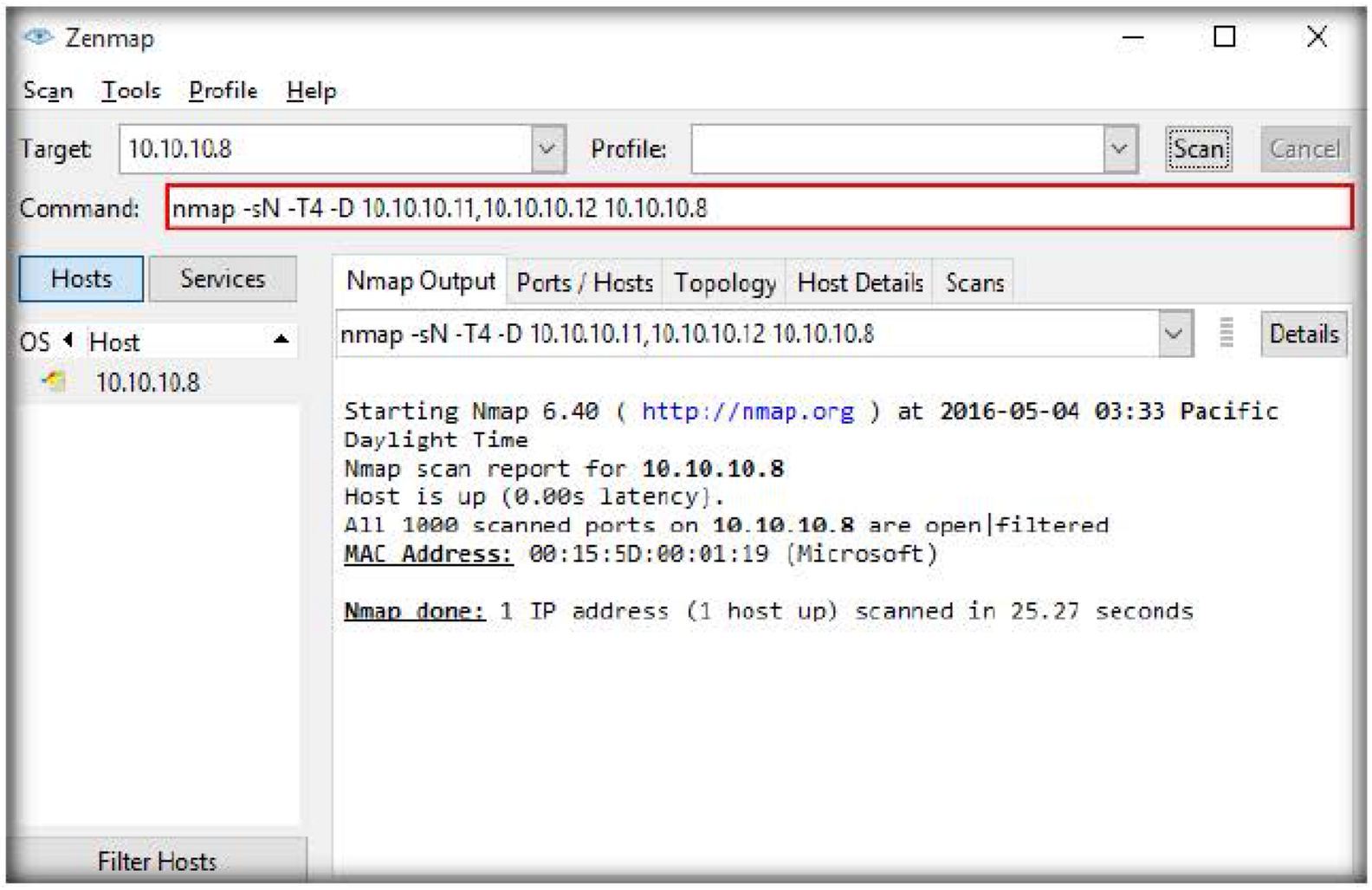



FIGURE 4.32: Decoys option used with two decoys in implementing a null scan

66. Since we are using decoy IP addresses, it will be difficult to identify the IP address from which the scan is being performed.
67. On completion of the scan, switch to the Windows server 2012 virtual machine and stop the Wireshark packet capture.


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

68. Filter the traffic captured by Wireshark to get all the TCP null packets by issuing the syntax **tcp.flags==0x00** in the **Filter** field.

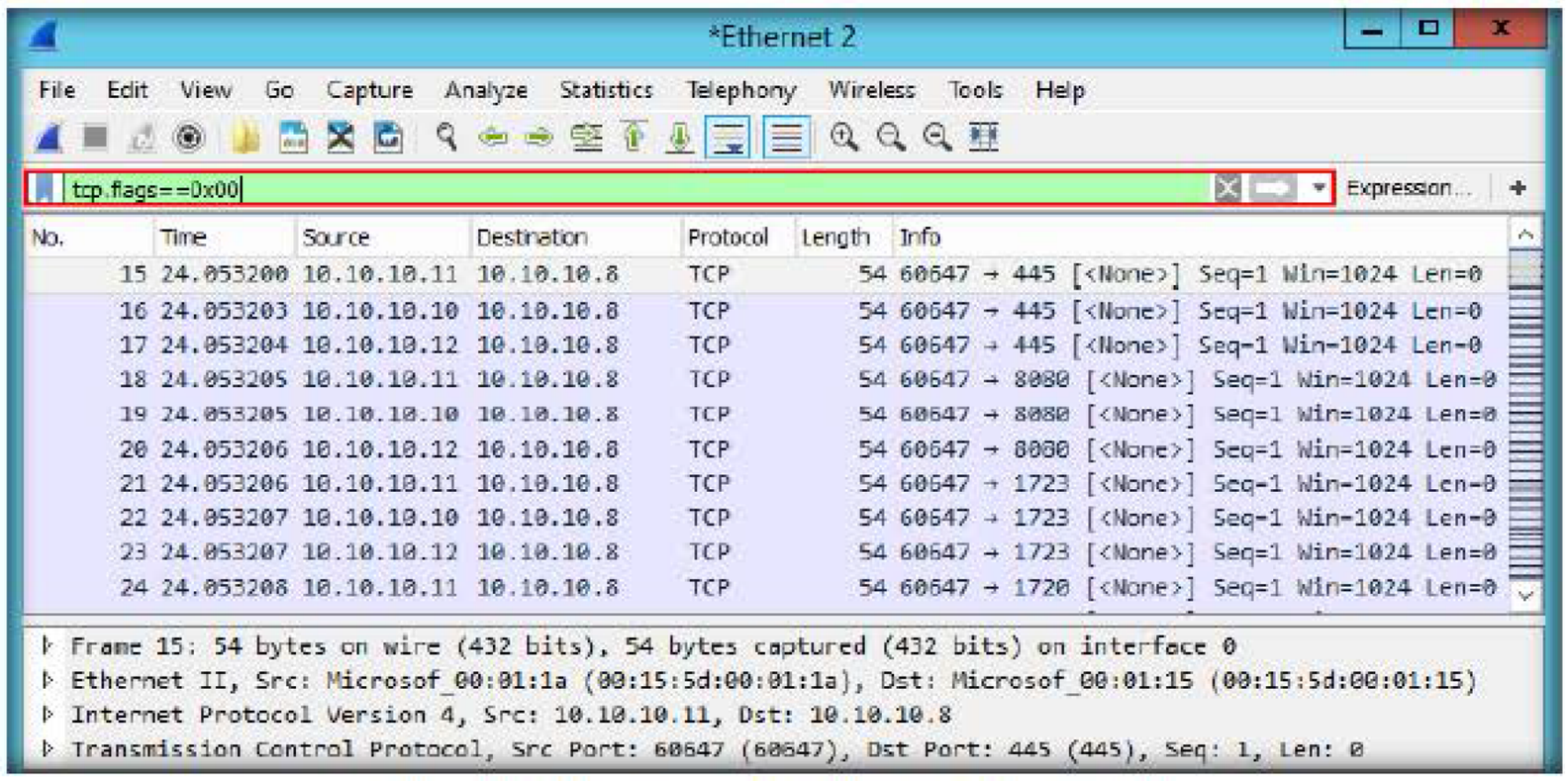



FIGURE 4.33: Decoys used to implement a Null scan attack

**Note:** You can use a large amount of decoys and with a lot more options to make the attacker more enigmatic.

69. Now we demonstrate the use of the verbosity option **-v**. The higher you set the level of verbosity the **more information is printed**. A verbose scan cannot be detected in Wireshark.

70. In the Windows 10 virtual machine, launch Nmap, type **nmap -sN -T4 -v -v -v -v -v -v 10.10.10.8** (or **nmap -sN -T4 -v5 10.10.10.8**) (10.10.10.8 is the IP address Windows Server 2008) in the **Command** field then click **Scan**.

71. When the scan completes, you will notice a clear scan result printed on the Nmap output as shown in the following screenshot:

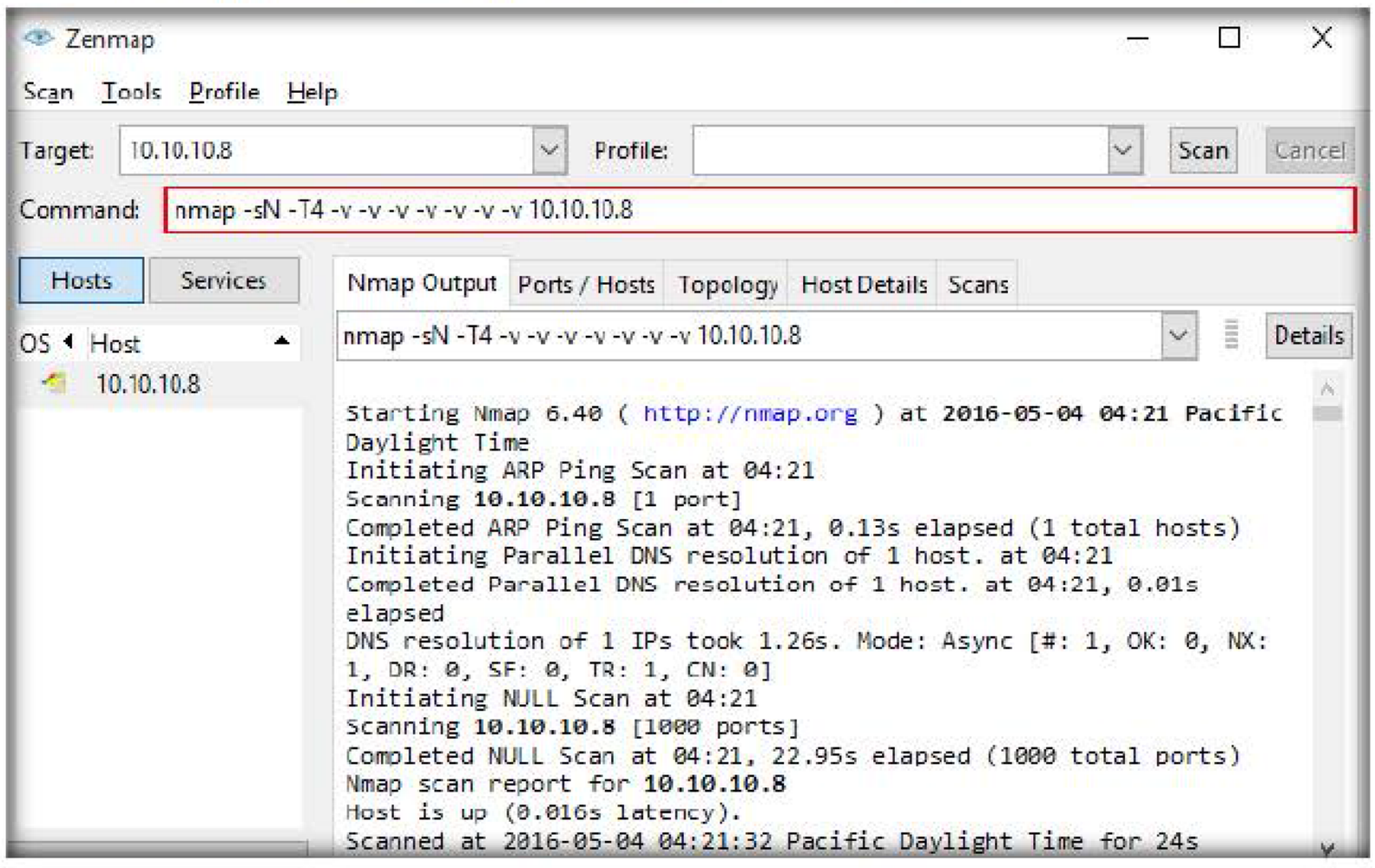



Figure 4.34: Verbosity option used to perform null scan attack



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

72. There is no special signature for detection in Wireshark

**TASK 13**

**Detecting OS fingerprinting attempt**

73. Next, we take a look at **OS detection or OS fingerprinting**. There are two types of OS detection. **Passive and Active detection**. **Passive** OS detection **does not send any** packet or probe to the victim and only sniffs the victim's traffic. It is difficult to detect and its results are unreliable. On the contrary **active** OS fingerprinting **sends a lot of probes** to the victim and has far better chances of giving accurate results as well as being detected by the firewall and IDS.
74. We demonstrate **TCP/IP based fingerprinting** using NMAP which is an active OS fingerprinting method
75. Before beginning this lab task, start the Wireshark packet capture in the Windows Server 2012
76. Switch to the **Windows 10** machine, launch Nmap, type **nmap -O -A 10.10.10.8** in the **Command** field then click **Scan**

After performing dozens of tests, Nmap compares the results to its nmap-os-db database of more than 2,600 known OS fingerprints and prints out the OS details if there is a match. Each fingerprint includes a freeform textual description of the OS, and a classification which provides the vendor name (e.g. Sun), underlying OS (e.g. Solaris), OS generation (e.g. 10), and device type (general purpose, router, switch, game console, etc).

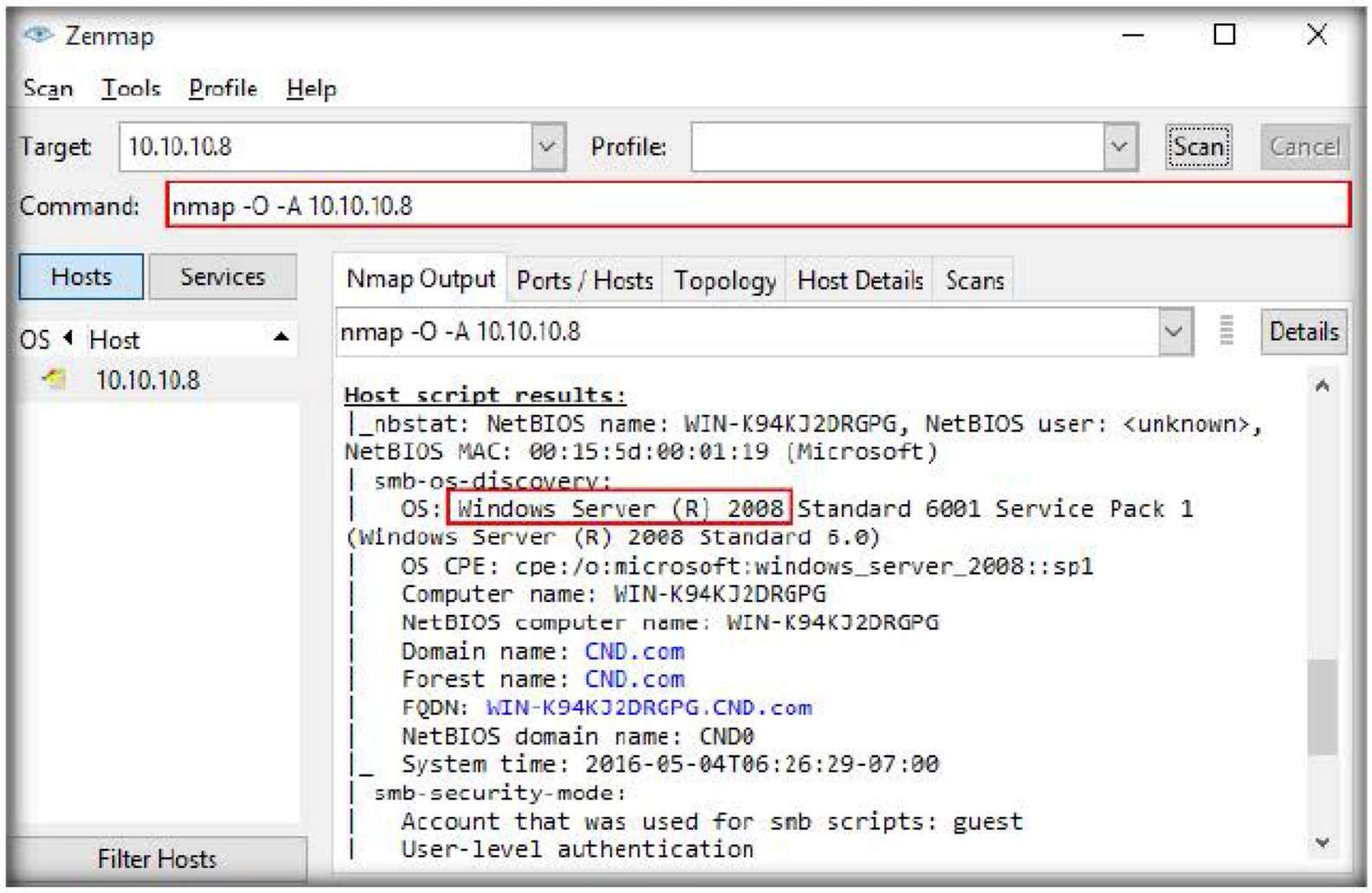



FIGURE 4.35: OS fingerprinting using NMAP


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

77. Switch back to the Windows Server 2012, and stop the Wireshark packet capture. Issuing the syntax **(tcp.flags==0x02) && (tcp.window_size <1025)** allows you to view the traffic associated with OS Fingerprinting as shown in the screenshot:

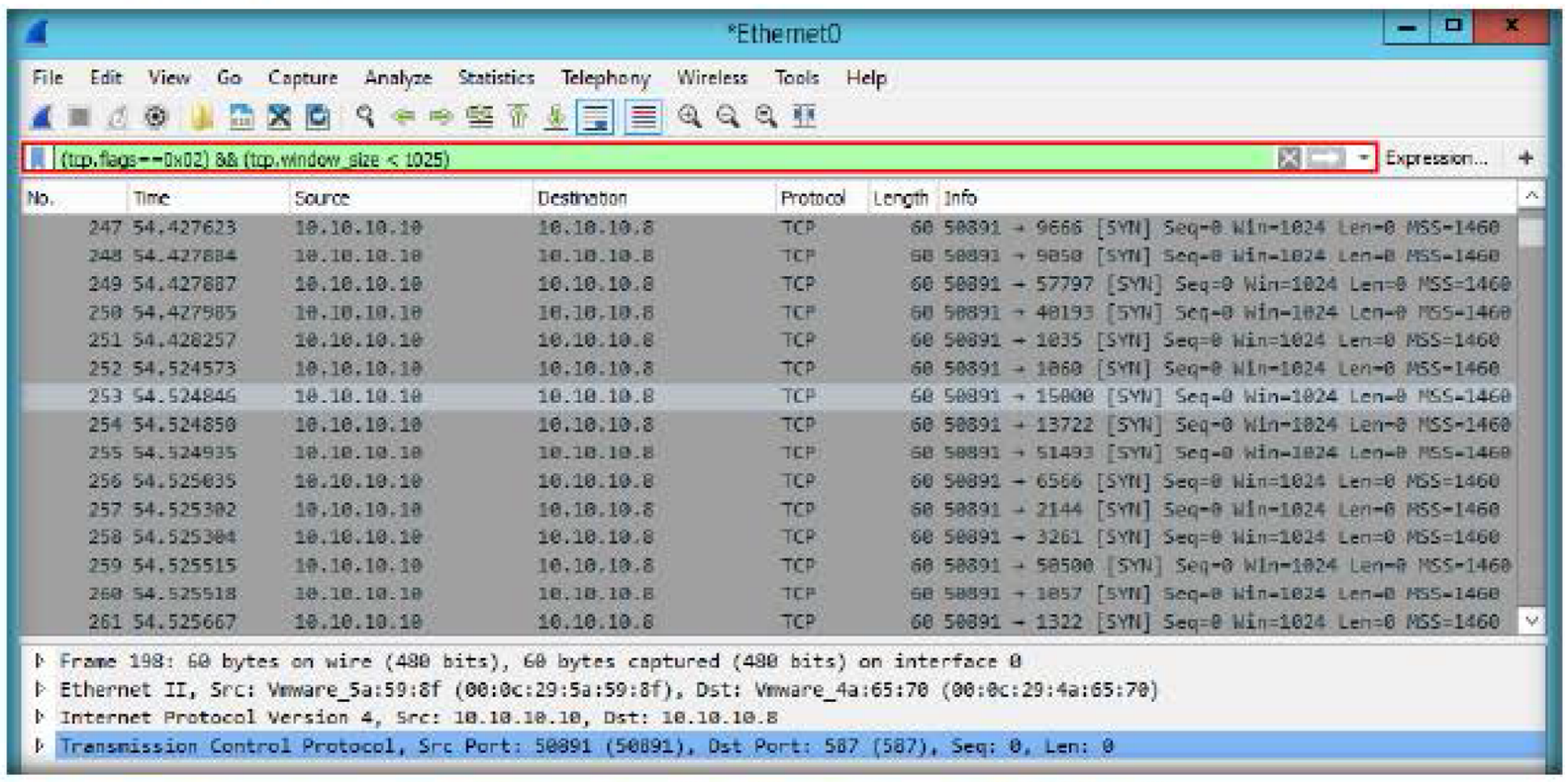



FIGURE 4.36: Detecting Nmap's OS fingerprinting attempt

**Note:** Although we have used both -O and -A options, just one of them will help in performing OS fingerprinting. -O switch is meant only for OS detection while -A is for OS detection, version detection, script scan and traceroute.

**TASK 14**

**Detecting Bruteforce Attempt**

78. The next lab task is to demonstrate a bruteforce attack on a FTP server and detect the attack using Wireshark.

79. Before beginning this lab task, ensure that a FTP website is running in the Windows Server 2008, and a new packet capture is begun in the Windows Server 2012.

80. Navigate to **Z:\CND-Tools\CND Module 11 Network Traffic Monitoring and Analysis\Bruteforce Tools\Brutus**, and double-click **BrutusA2.exe** to launch the application.

81. The Brutus GUI appears as shown in the following screenshot:

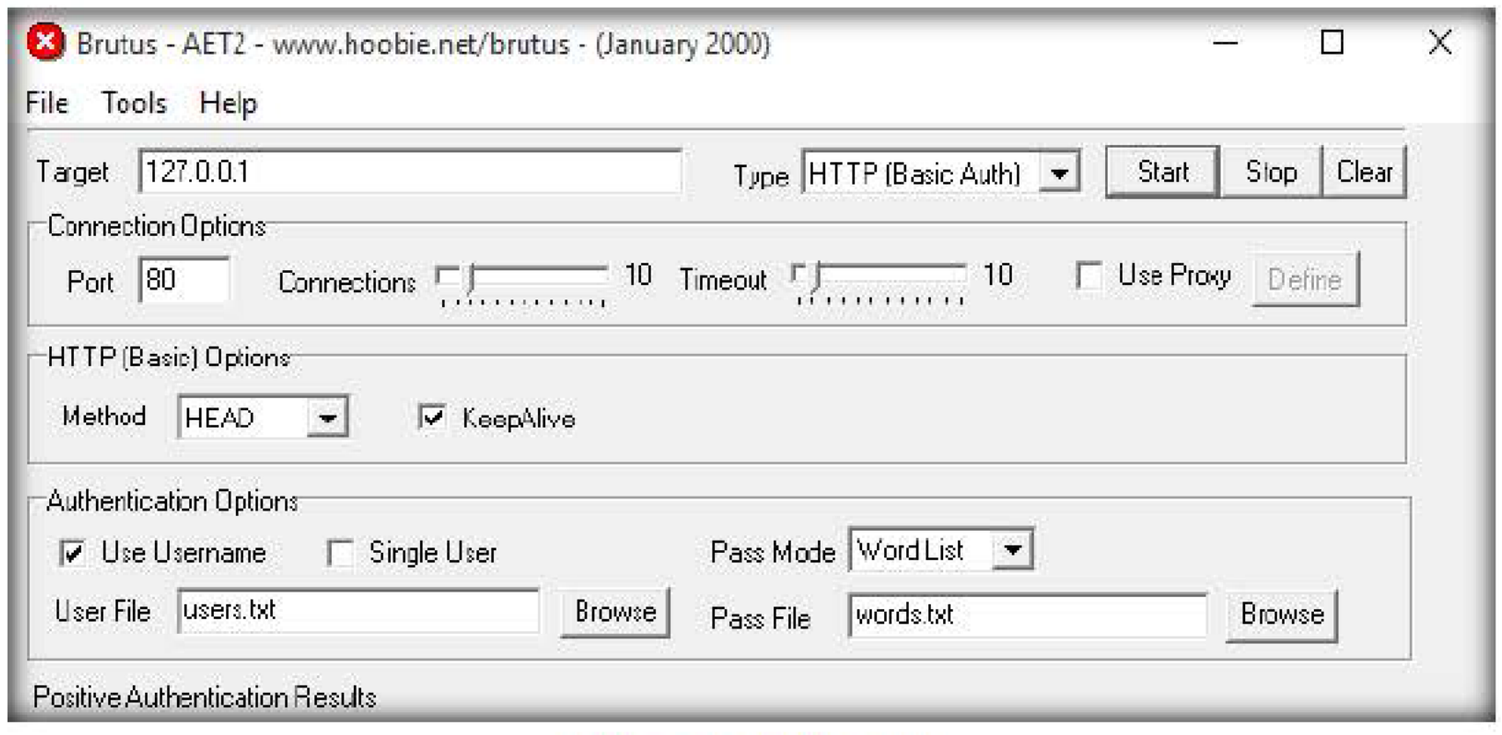



FIGURE 4.37: Brutus GUI


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

82. Assign the IP address of the Windows Server 2008 (**10.10.10.8**) in the **Target** field, select **FTP** from the **Type** drop-down list, leave the other options set to the default settings then click **Start**.

Brutus is a password cracking tool that supports HTTP (Basic Authentication), HTTP (HTML Form/CGI), POP3, FTP, SMB, Telnet and other types such as IMAP, NNTP, NetBus, etc. You can also create your own authentication types.

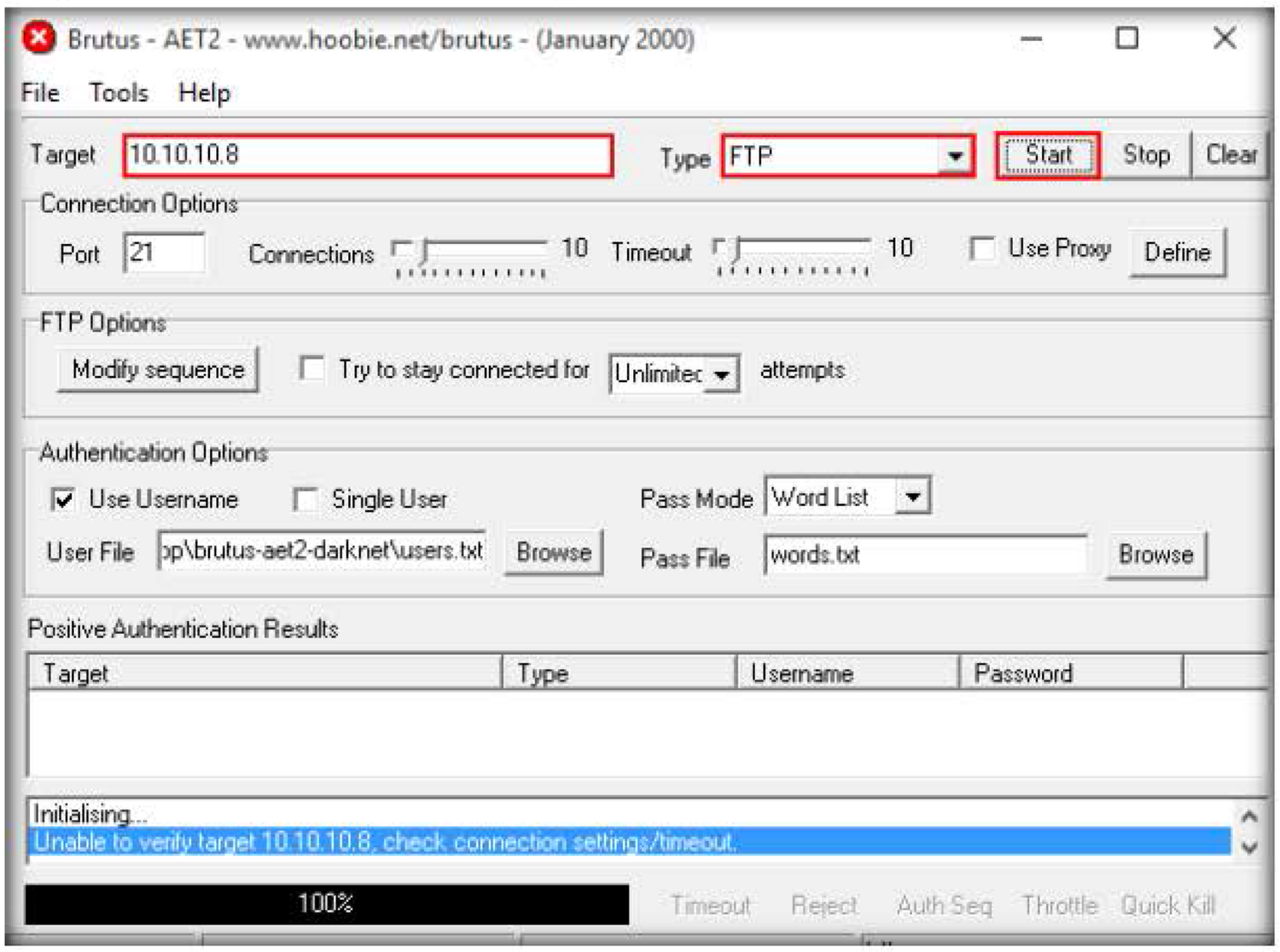



FIGURE 4.38: FTP attack with Brutus tool

83. Wait until the attack is completed

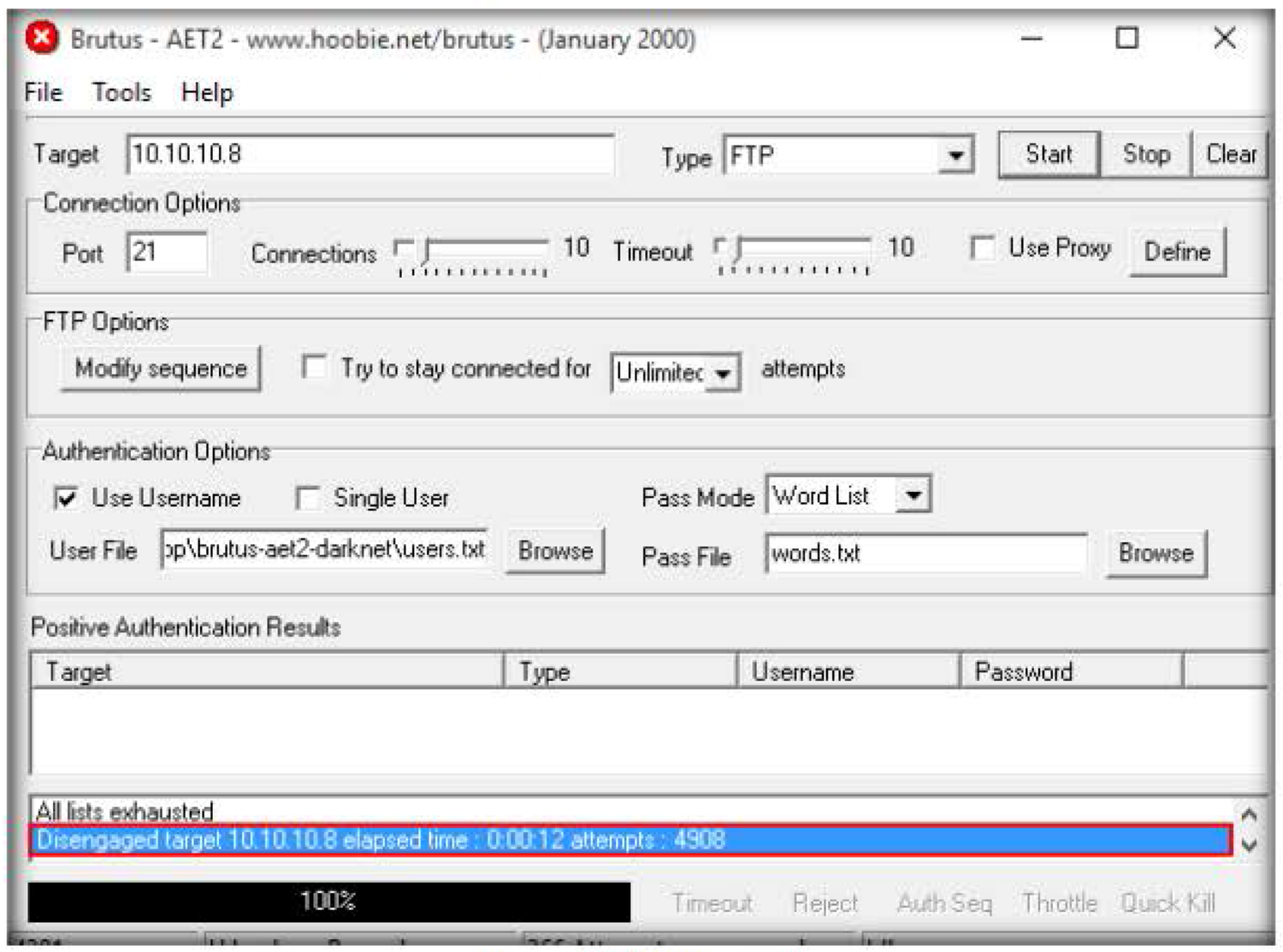



FIGURE 4.39: FTP attack completed



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

84. On completion of the attack, switch to the Windows Server 2012 and stop the Wireshark packet capture.

**Note**: In this lab, **4,908** attempts have been made to gain unauthorized access to the FTP server, but still failed. For every failed attempt, a packet containing the **response code 220** will be recorded in Wireshark.

85. Issue the filter **ftp.response.code == 220** in Wireshark **Filter** field

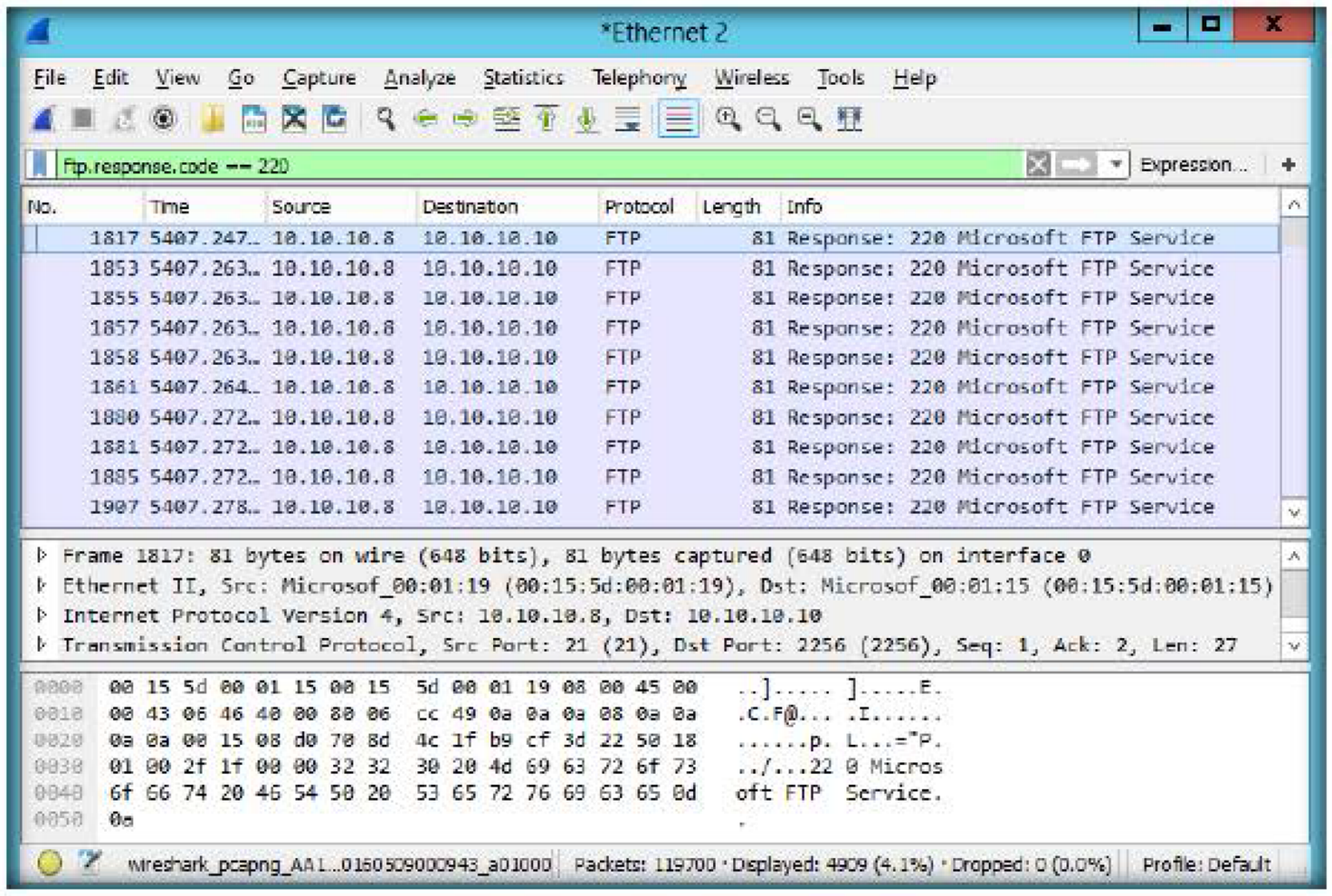



FIGURE 4.40: Brute force FTP attack

**Note**: It is evident that a huge number of failed logins have been recorded, which is confirmation that a brute force attack has been performed.

## Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on securing the wireless network using Linksys router

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

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



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

Lab 5

# Network Traffic Monitoring using PRTG

PRTG Network Monitor is a network traffic monitor that enables you to manage your network.

## Lab Scenario

The amount of traffic traversing through the organization's network keeps fluctuating, and cannot be predicted. The exceptional usage of network bandwidth, and performance bottlenecks may occur anytime, and it becomes difficult to spot them in time. As a network security administrator, you need to employ a network monitoring solution that enables you to manage your network, and avoid bandwidth and server performance bottlenecks; discover which applications use up the network bandwidth, and troubleshoot network problems.

ICON KEY

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

## Lab Objectives

This lab will help you understand how to monitor Network Traffic and Bandwidth in the Network using PRTG

## Lab Environment

To carry out the lab, you need:

- A virtual machine running Windows server 2012
- A web browser with internet access
- Administrative privileges to run the tools
- Since you will be installing the latest version of PRTG Network Monitor, screenshots and steps might differ in your lab environment

## Lab Duration

Time: 45 Minutes



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

# Overview of PRTG

PRTG is a network traffic and bandwidth monitoring tool. This tool can even monitor system health like CPU load, Memory on any system, etc. PRTG uses the concept of Sensors, and monitors every device using a sensor.

# Lab Tasks

**TASK 1**

**Download and install PRTG**

1. To begin this lab, you need to download and install PRTG Network Monitor.
2. To download the application, launch a web browser, type the URL www.paessler.com/prtg in the address bar and press **Enter**.
3. PRTG Network monitor download page appears, click **FREE TRIAL DOWNLOAD**. By selecting this option, you will be able to download and access the PRTG network monitor that has all features, but lasts for only 30 days.

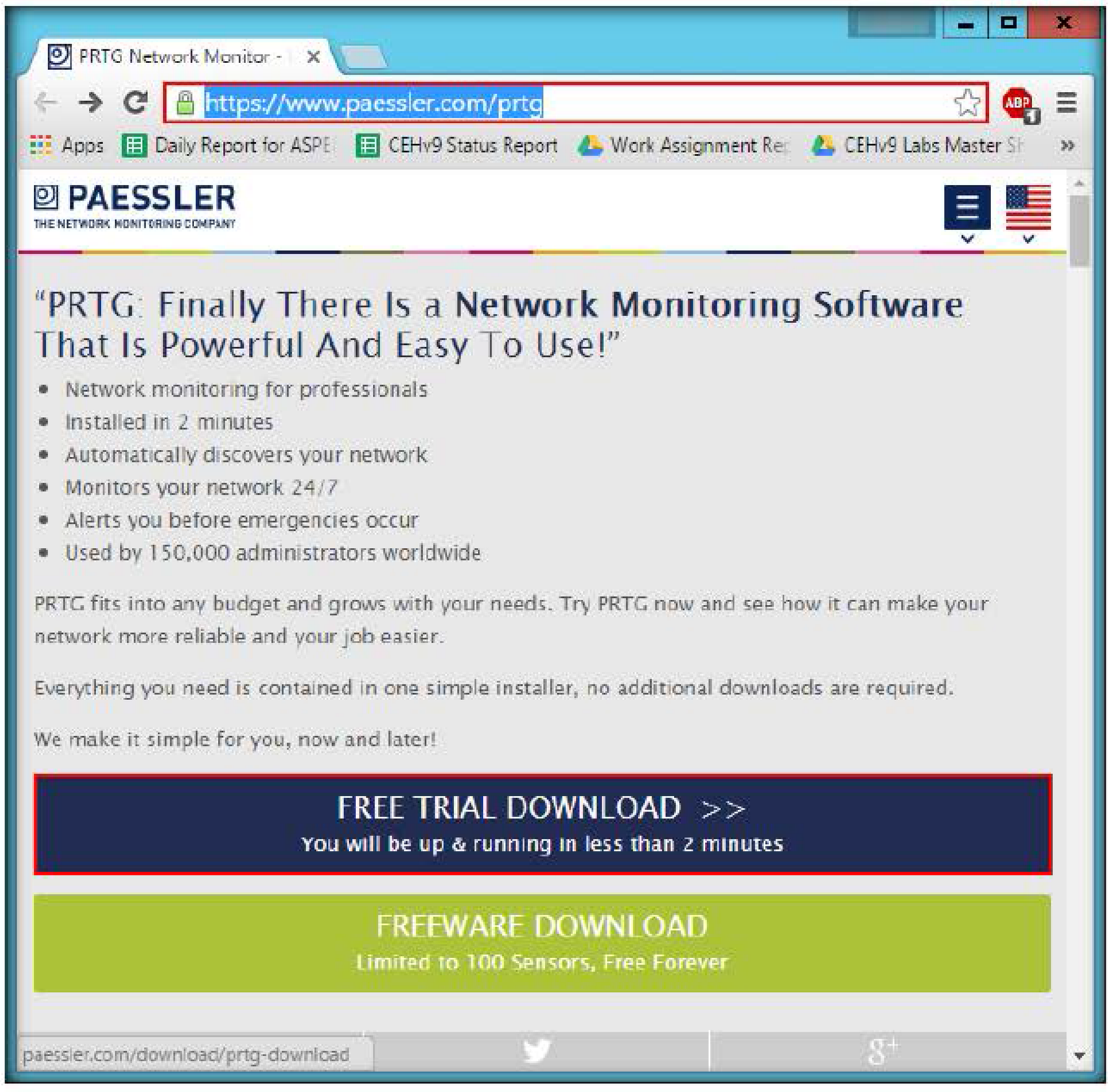



FIGURE 5.1: Paessler official Webpage to download PRTG

Paessler Router Traffic Grapher is a server up-time and utilization, network monitoring and bandwidth usage software package for server infrastructure from Paessler AG. It can monitor and classify bandwidth usage in a network using SNMP, Packet Sniffing and Netflow.

4. As soon as you click download, a **Save As** window appears; specify a download location and save the file.



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

5. Meanwhile, you will be redirected to a webpage containing the license key for the trial version of the tool. Make a note of the license key.

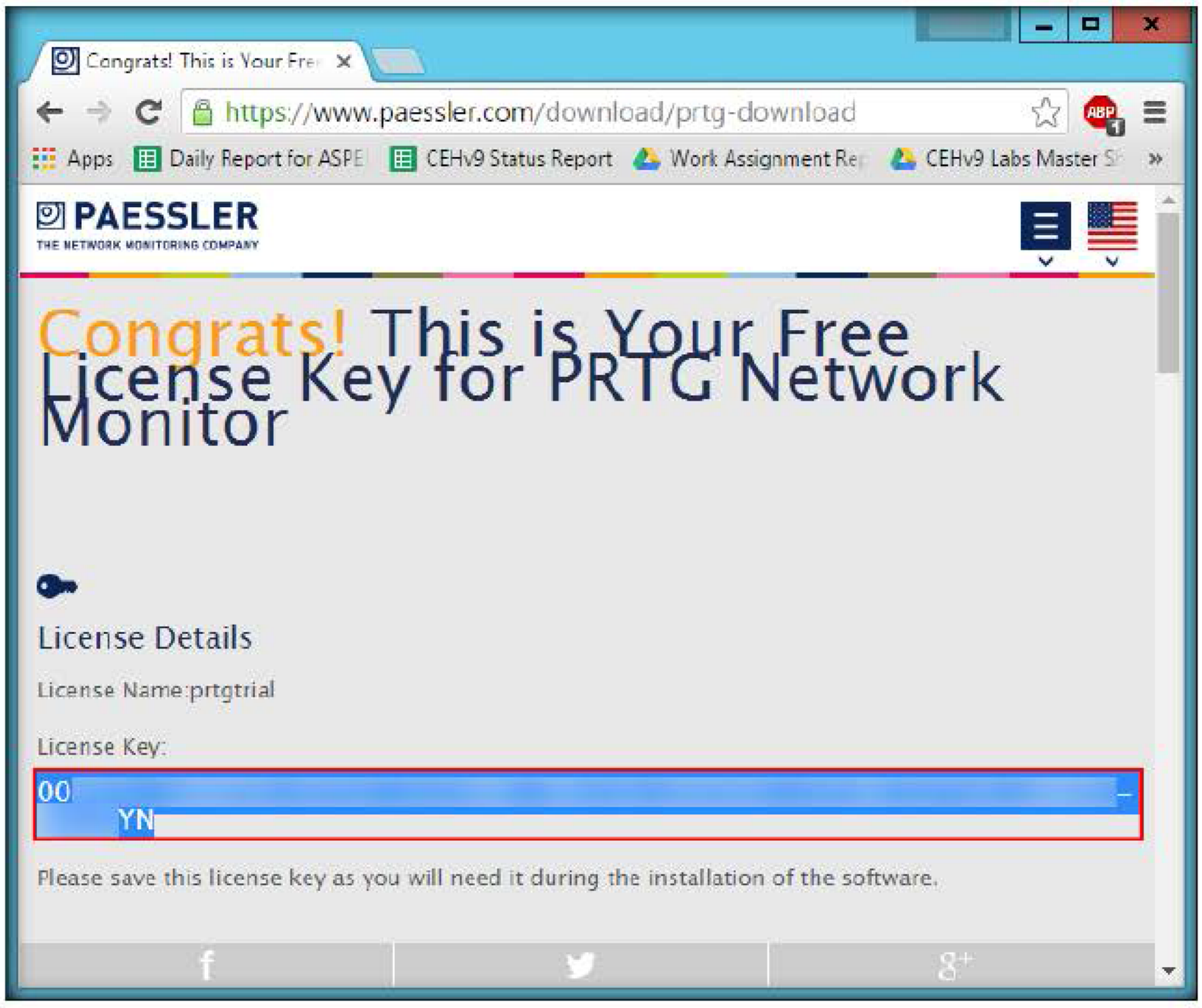



FIGURE 5.2: Copying the License Key

6. On completion of the download, navigate to the location where you have downloaded the file, and unzip the contents of the file to a folder named PRTG.

7. Open the PRTG folder, and double-click the setup file, to begin the installation. You will be asked to choose a language. Choose the language (here, English), and follow the wizard driven installation steps to install PRTG Network Monitor.




FIGURE 5.3: Selecting a Language

8. During the installation, you will be asked to enter an Email and the Product key, enter them.


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

9. On successful installation, the web console of PRTG Network monitor appears, click **Skip introduction**.

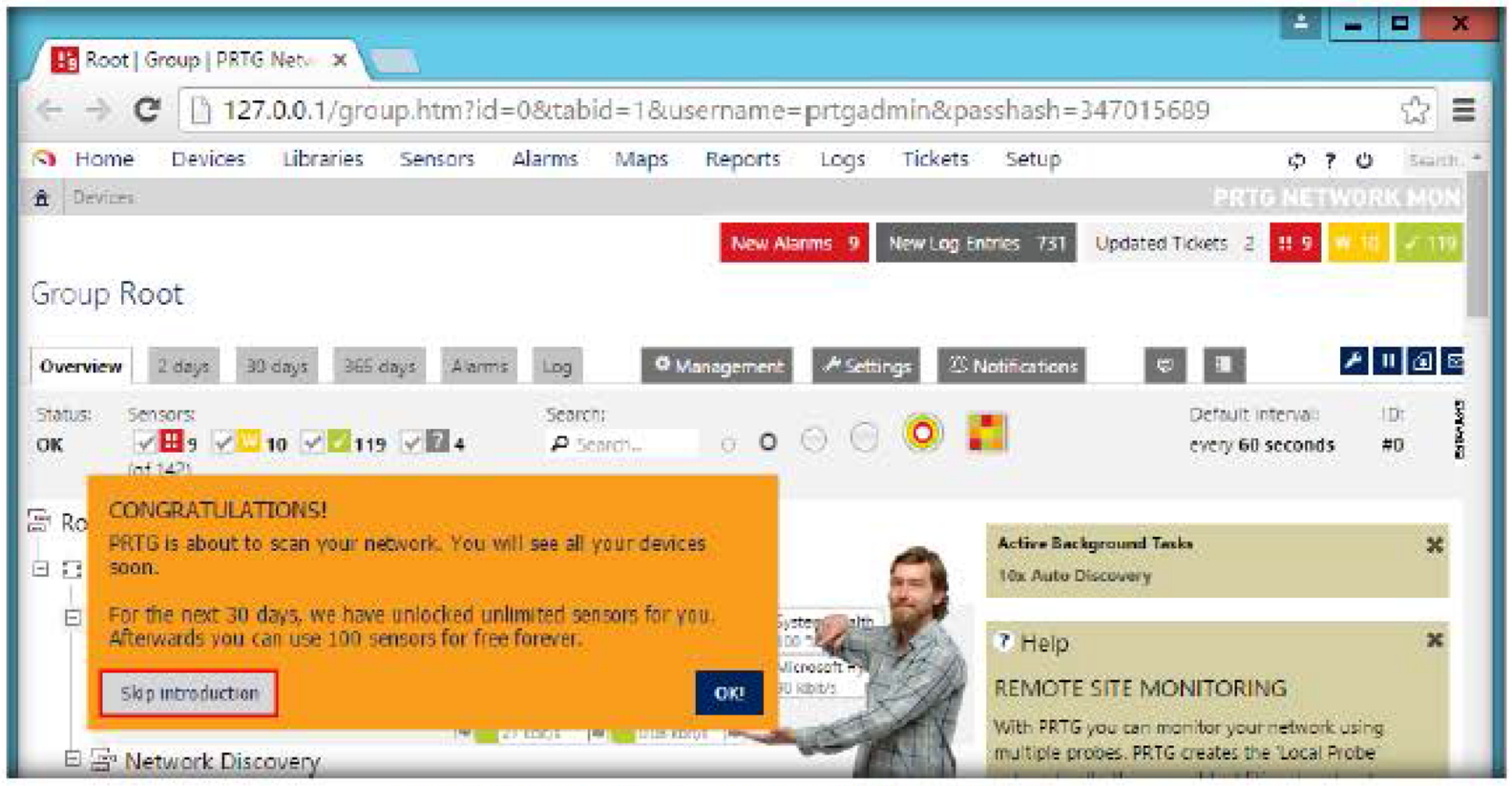



FIGURE 5.4: PRTG Network Monitor Main Window

**TASK 2**

**Setting up PRTG**

10. PRTG automatically discovers your subnets and you can add additional subnets as well.
11. Now, we will be accessing PRTG through the **browser interface** to set our initial settings.
12. First of all, click on the **devices** tab and then on the **settings** tab.

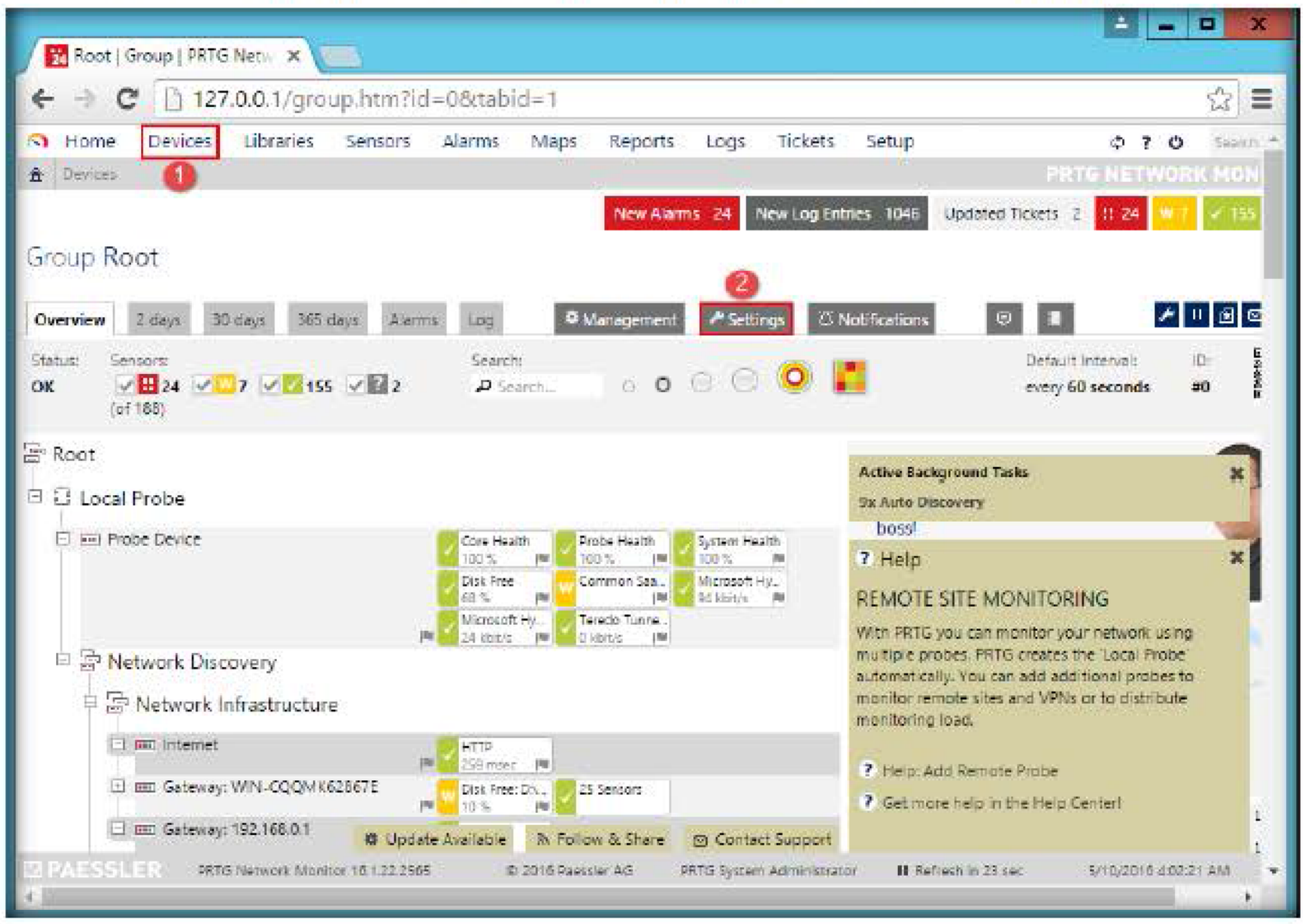



FIGURE 5.5: Navigating to the Settings Page of PRTG



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

13. Now on the settings page, scroll down to the "**credentials for windows systems**" section.

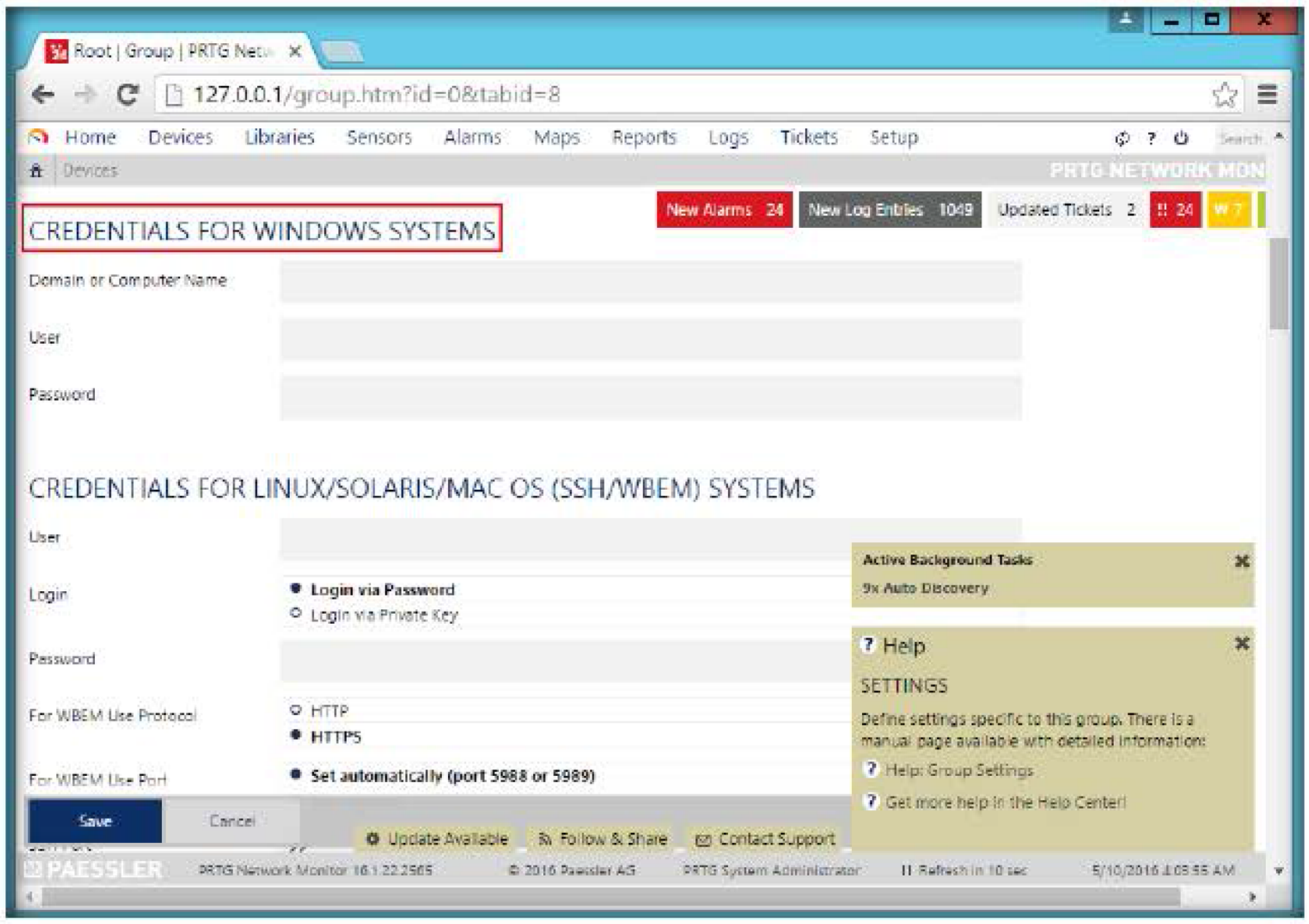



FIGURE 5.6: The Credentials Section of the Settings Page

14. You need to enter your active directory domain here which will be responsible for all windows access controls. If you do not have such a domain, you can make any PC responsible for windows access. We make the local PC itself responsible for access control.

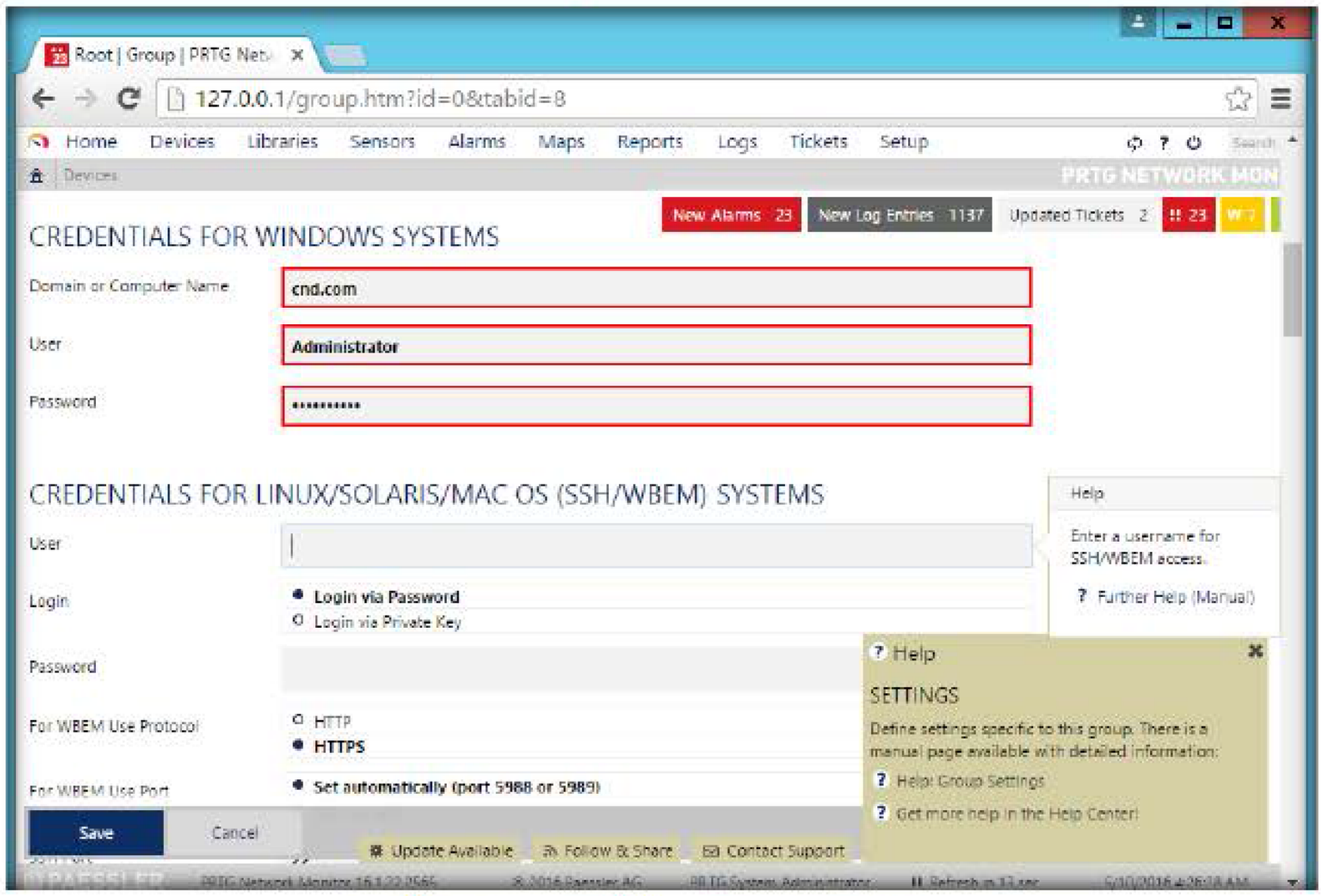



FIGURE 5.7: Credentials Entered for Windows Systems

The alarms list shows all sensors that are currently in a Down, Down (Partial) Down (Acknowledged), Warning, or Unusual status. Sensors in other states (for example, Up, Paused, or Unknown) do not appear here. This is useful to keep track of all irregularities in your network.



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

15. Similarly, like Windows, if you have other platforms in your organization like the Linux, Solaris, MAC or VMware server, and you want to configure an Administrator account for them as well. You can do so by scrolling down.

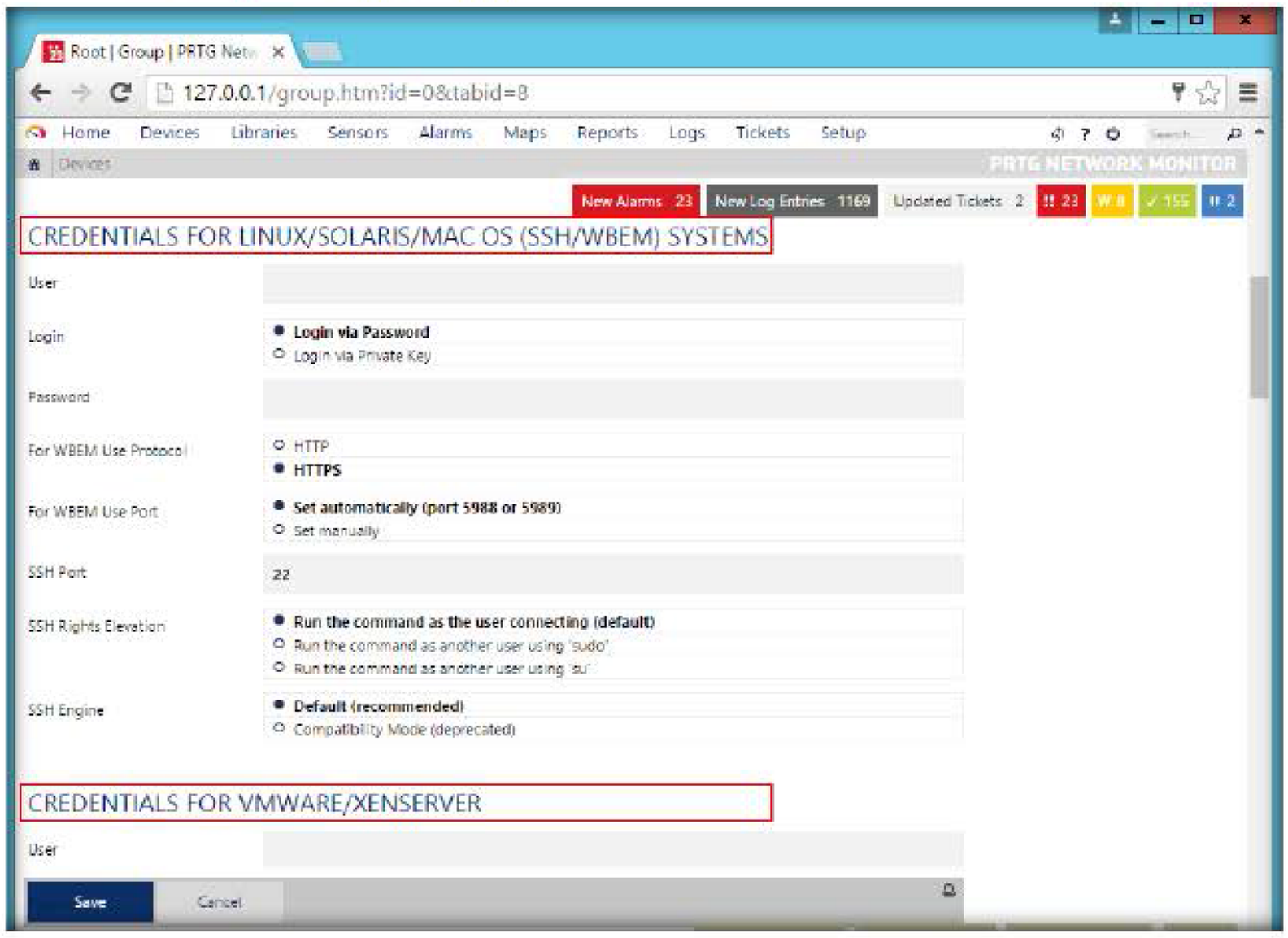



FIGURE 5.8: Credentials for Administrator systems of other platforms

The Logs list shows all past activities and events of your PRTG monitoring setup. This is useful to research past user activities, system events, and, for example, to check whether messages were sent. In a typical setup, a huge amount of data is produced here. Because the activity of every single object is recorded, you can use this information to check if your setup works exactly as desired.

16. You may configure the SNMP devices, DBMS and Cloud

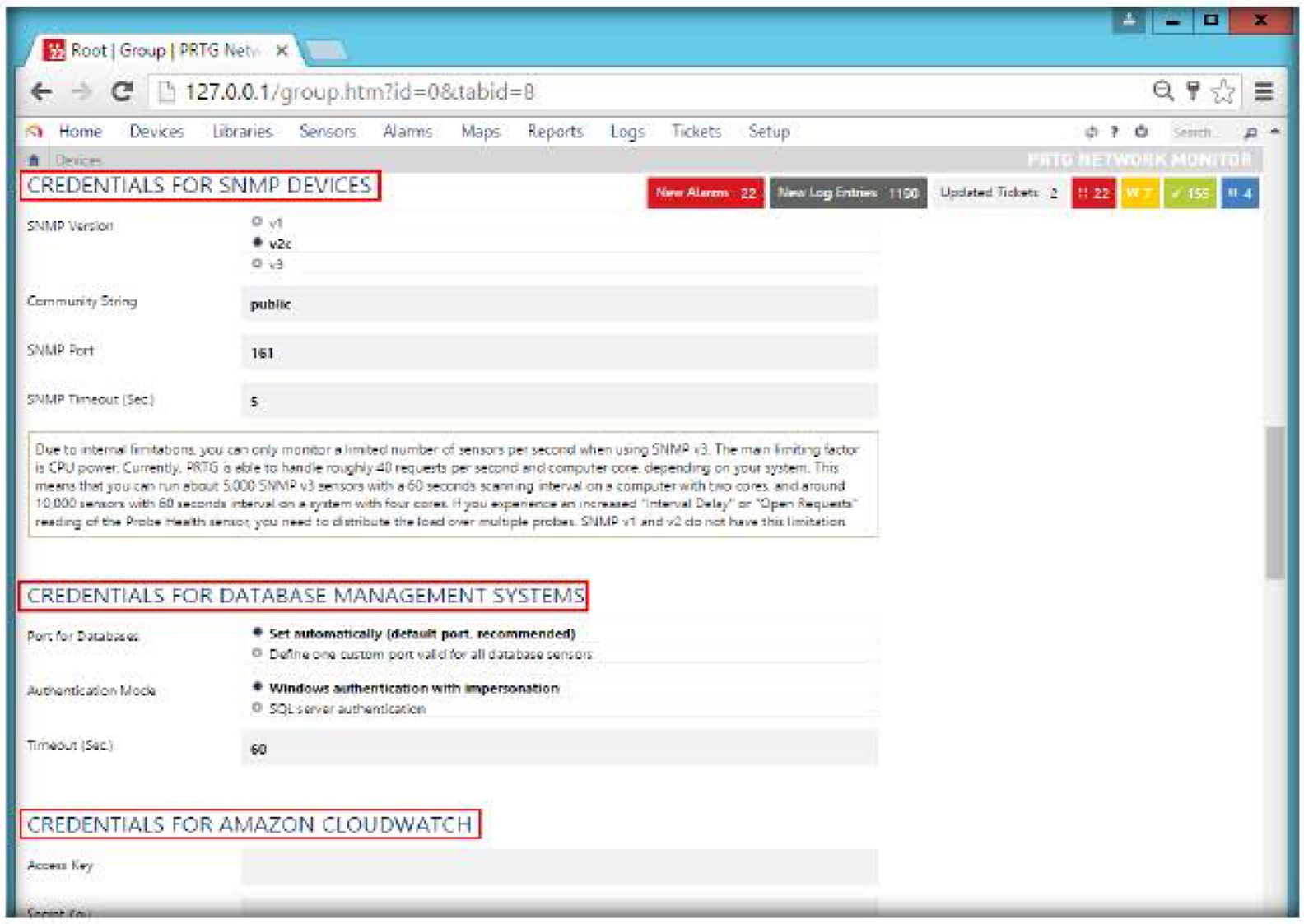



FIGURE 5.9: Credentials for SNMP, DBMS and Cloud



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

17. Now, in SNMP based devices you have a password like entity known as a **community string** which has a default value of **public**. If your devices use the same, then do not alter it and SNMP can be any of the three versions. **v1** is the basic version and **v2** has some additional features like the 64 bit counters and the most advanced **v3** even supports authentication and encryption.
18. If you want to monitor the **SQL server**, configure it with a port number and authentication of the database. If you want to use **PRTG's cloud sensors**, then enter AWS access key and AWS secret key.
19. There are even the **WINDOWS COMPATIBILITY OPTIONS** and the **SNMP COMPATIBILITY OPTIONS**. Unless you encounter problems with any particular device, it is advisable to keep the default settings unchanged in these sections

The Hyper-V Host Server sensor monitors a Microsoft Hyper-V host server via Windows Performance Counters or Windows Management Instrumentation (WMI), as configured in the "Windows Compatibility Options" of the parent device.

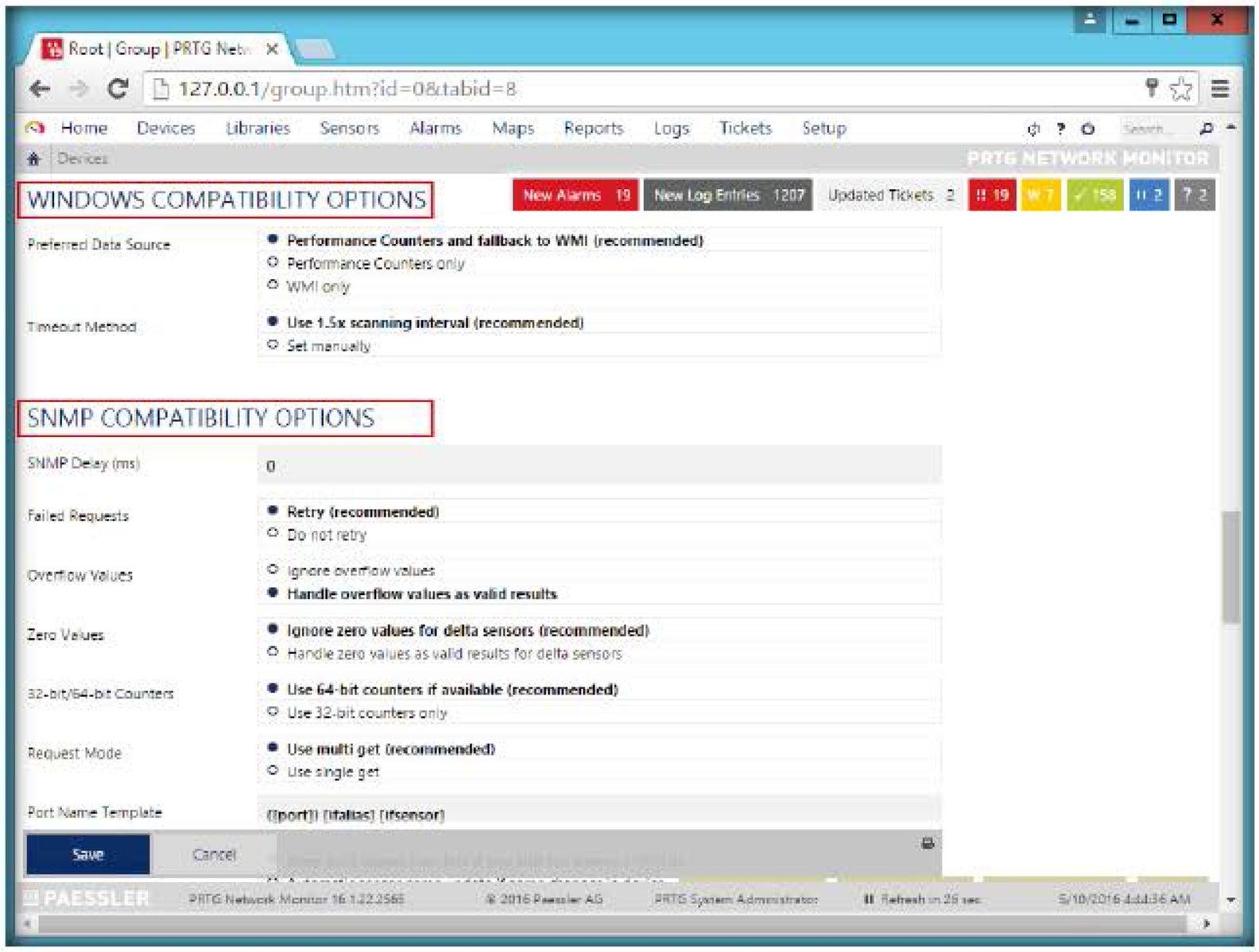



FIGURE 5.10: Windows and SNMP Compatibility Section of PRTG

20. Moving on to the next section, if you want the sensors to monitor data over a **proxy server** enter the details of the proxy server and the next section which deals with the **monitoring interval,** enter the frequency at which you want the scans to take place. Also choose the action you want to be performed when you discover a faulty system.


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

21. You may scroll down the webpage to view the **schedules, dependencies, and Maintenance** section, which should only be used when you are performing gradations or maintenance and you do not want monitoring to be done. So you can disable monitoring during these times with this option.

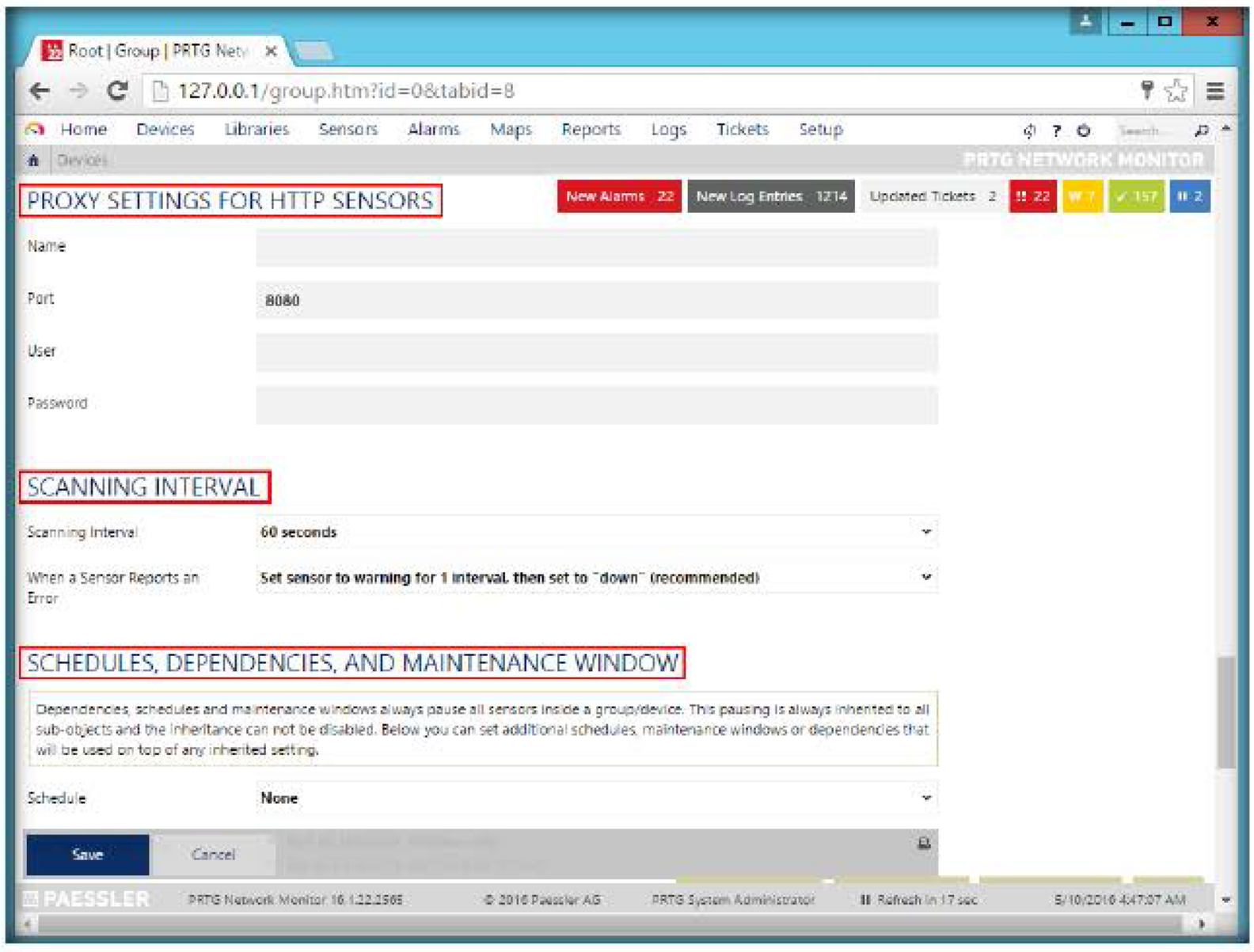



FIGURE 5.11: Proxy Settings and Scanning Intervals Sections of PRTG

15. Next, is **Access rights**, which governs the read, write and full permissions and which should be granted to groups and users. The **channel unit configuration** section deals with units like Kilobytes and Megabytes in which various sensors measure their data.


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

16. The final section called **Automatic monitoring data analysis** deals with unusual detection which displays the unusual values of a sensor and the similar sensors sub section. When enabled this provisions the detection and display of similar sensor values. It is advisable to have both these enabled. Finally click on **Save** after all settings are done. Do not click save now since we have not yet configured the two sections at the top.

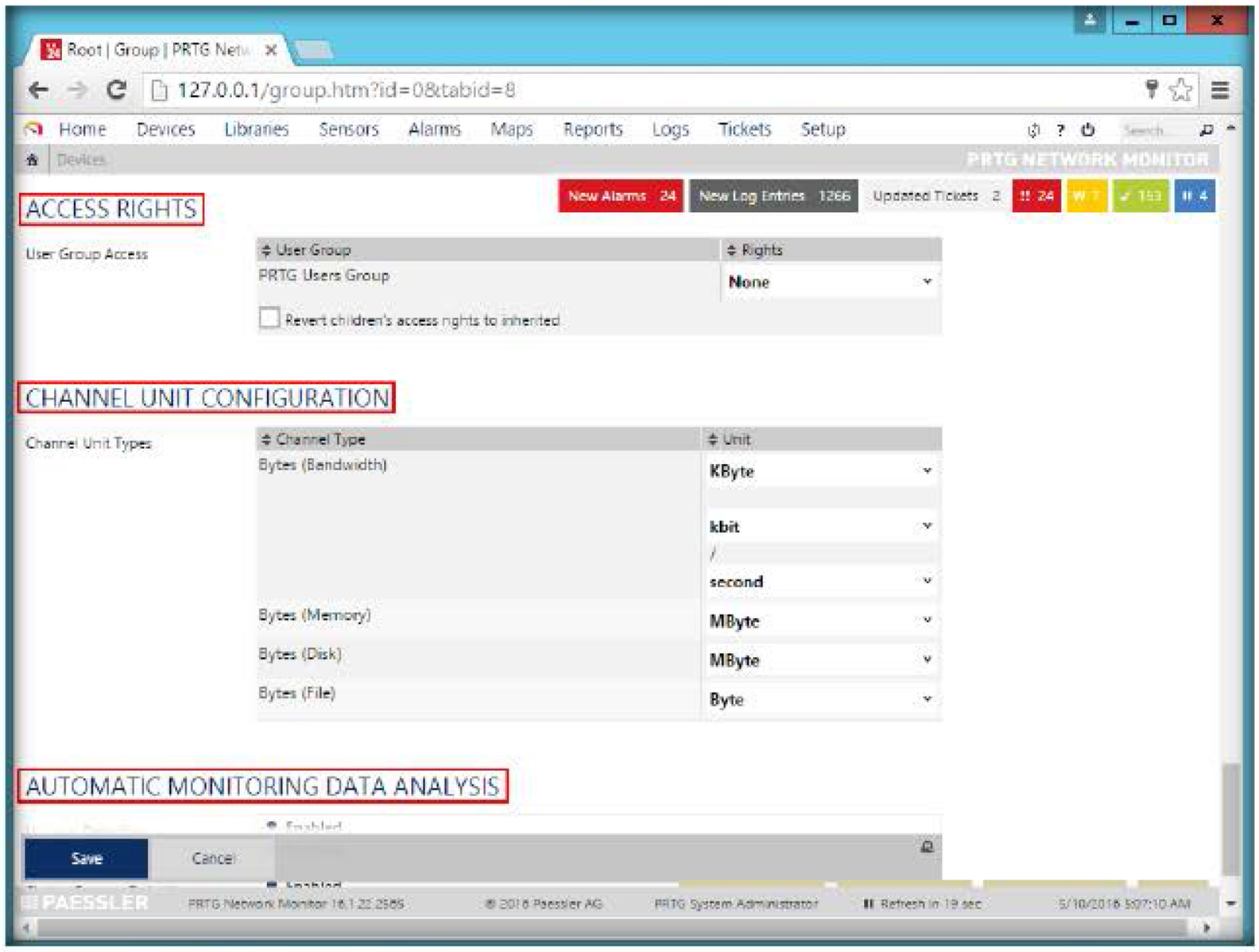



FIGURE 5.12: Access Rights, Channel Unit and Automatic Monitoring Data Analysis Sections of PRTG

17. Now, scroll back to the top and look for the Basic group settings. The settings we have configured belong to this Root group. The Name can be changed. All other devices and sensors inherit settings from here. You can override the inheritance of any setting for a sensor as well, which we will see later on.


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

18. In the Location section you need to enter the **Geographic Location** of the PRTG server. Normally your location is auto detected, but if there is a wrong detection, you can change it manually. Scroll down the web page, and click **Save**.

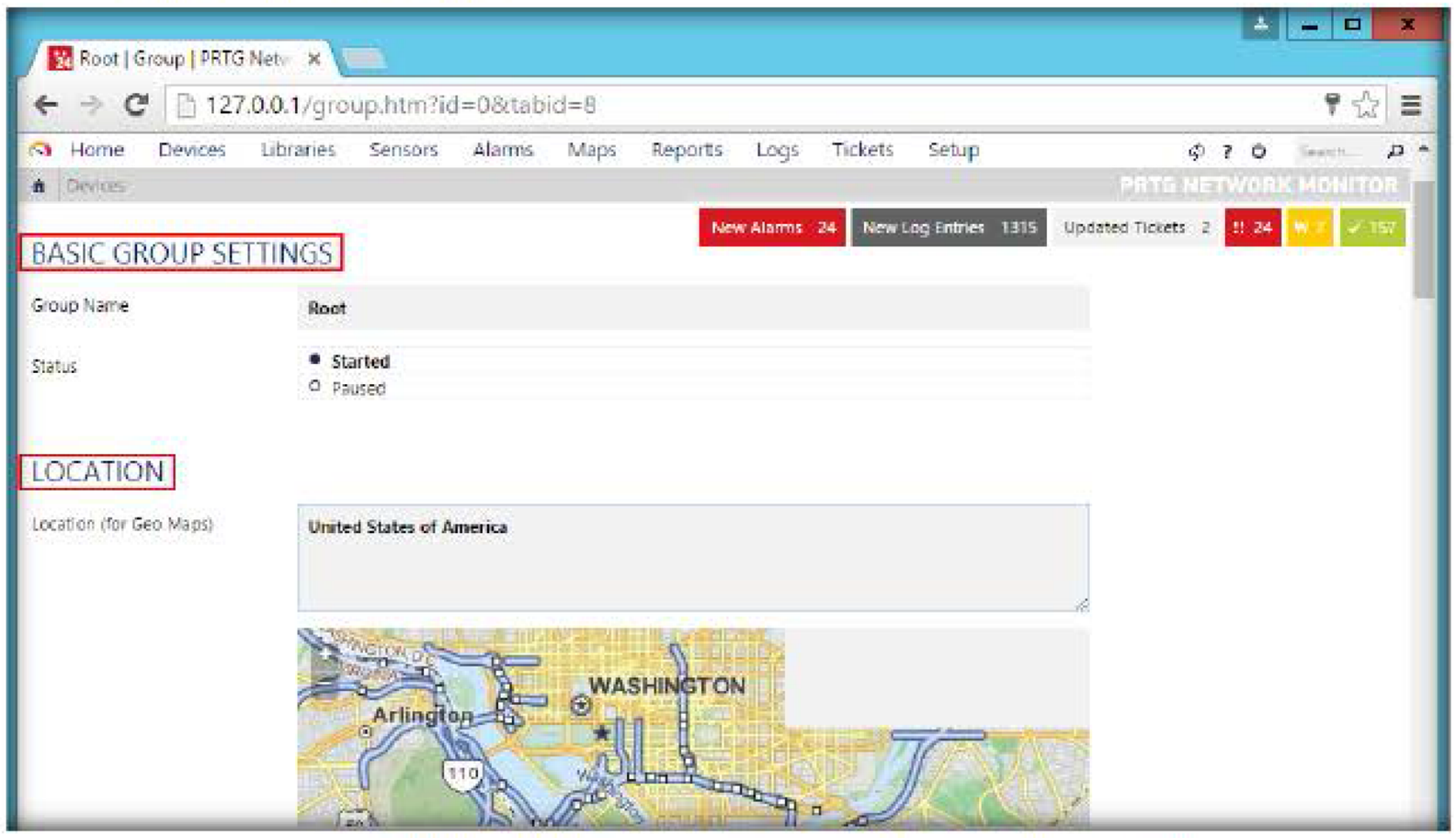



FIGURE 5.13: Basic Group Setting and Location Sections of PRTG

19. Upon installation, PRTG network monitor automatically assigns a username and password of its own. So, it is recommended to change the user credentials.

20. To change the user credentials, hover the mouse cursor on **setup**, hover the cursor on **Account settings** and then select **My Account** from the drop down list.

In the My Account settings you can define values regarding your (currently logged in) PRTG user. All settings in this section are user-specific. Some account options may not available, but restricted to the administrator.

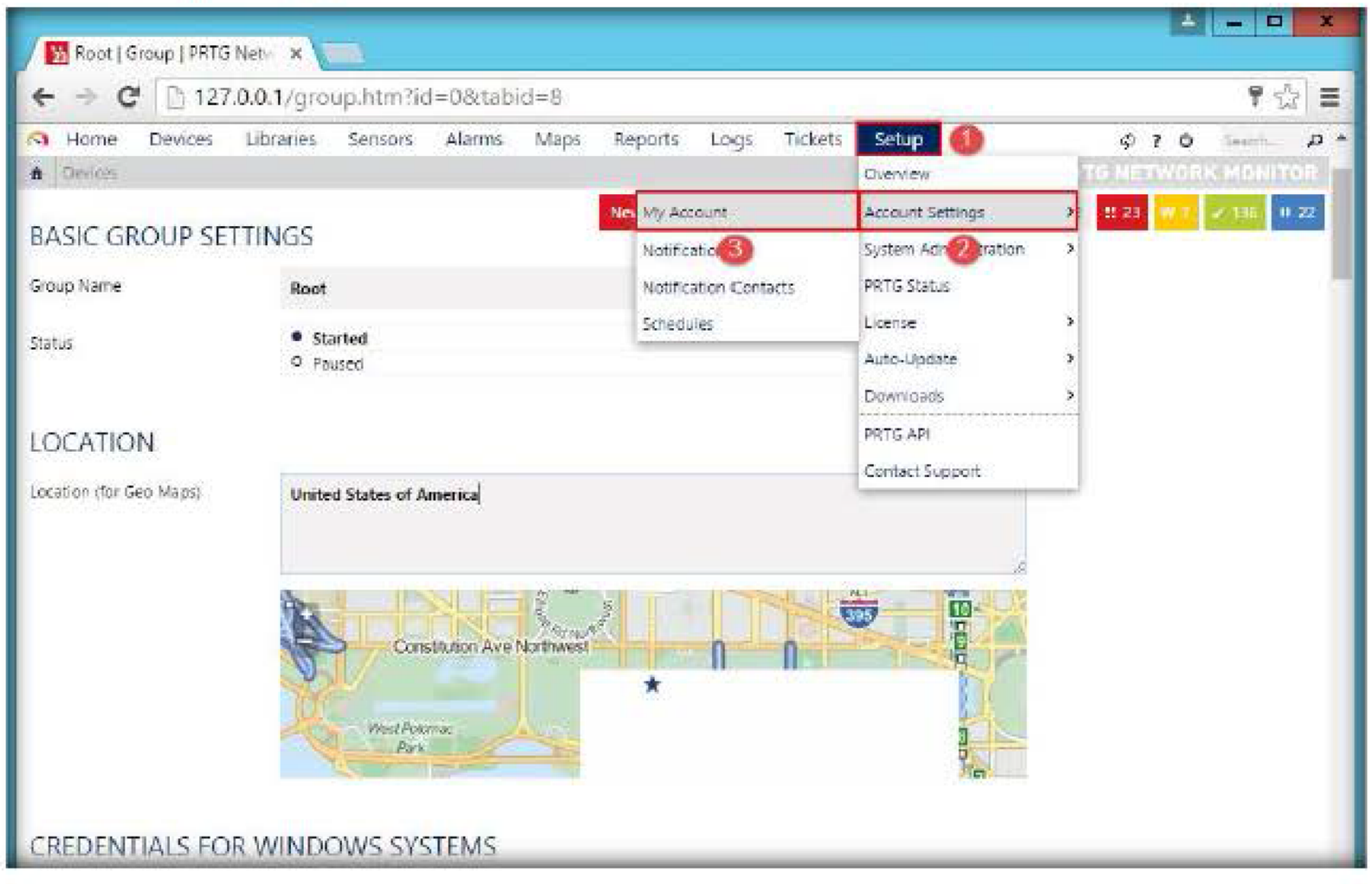



FIGURE 5.14: Entering the Account settings page of PRTG



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

**TASK 3**

**Administrator account setup**

21. The Account Settings web page appears, change the login name to Administrator, click the Specify new password radio button, specify the Old Password as **prtgadmin**, enter a strong password in the **New Password** field and re-enter the same in the **Retype Password** field.

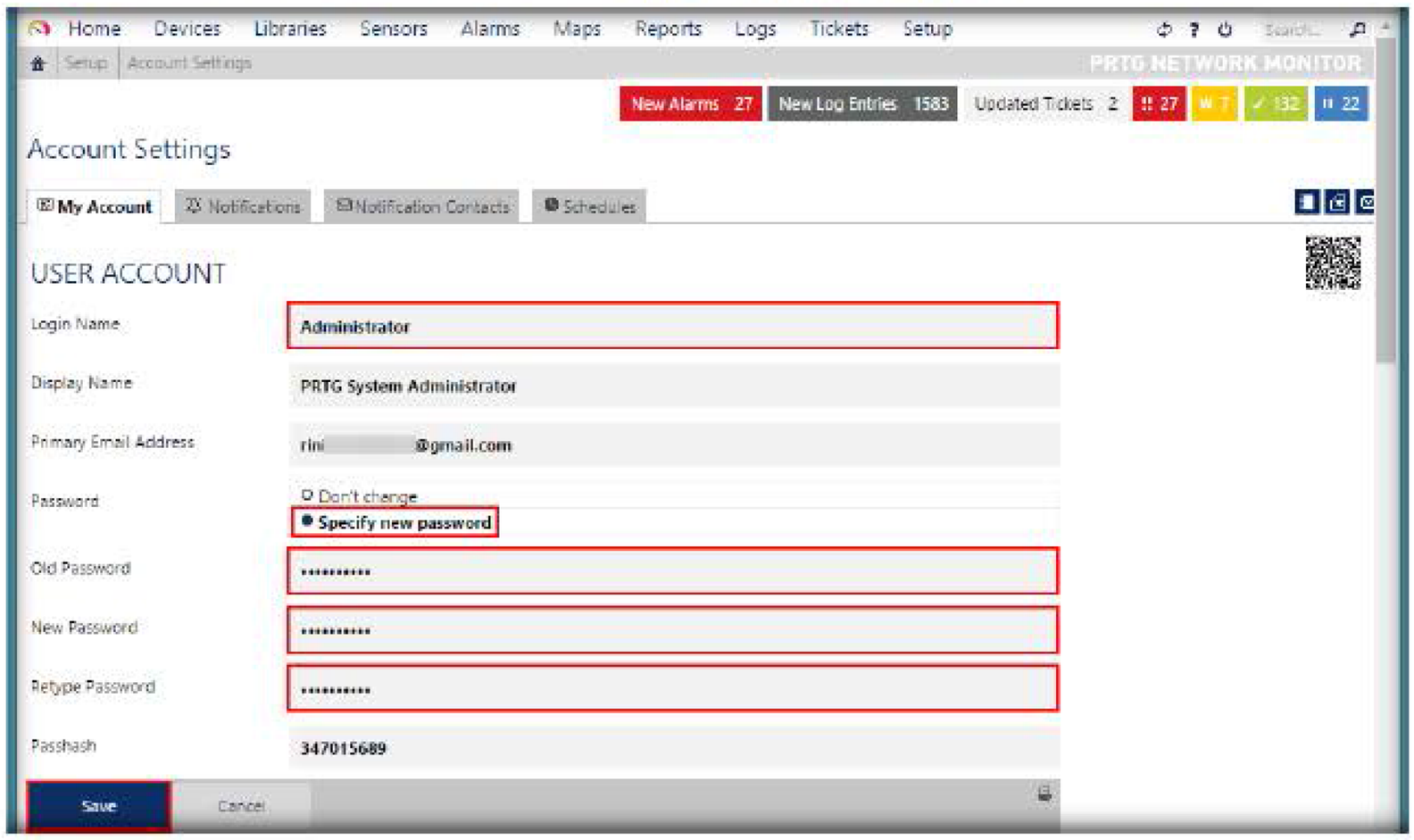



FIGURE 5.15: Administrator Accounts Section of PRTG

22. Now in the **ACCOUNT CONTROL** section, select the **PRTG Administrators** account in the **Primary Group** drop-down list. This is the main account of which all the other groups have to be a part of. Usually it is better to have an Administrator account as a primary account. The **Status** and **Last Login** field's values cannot be edited for a default Administrator account.

23. The **USER GROUPS** section shows all the groups, in which the current user holds up a membership. This section cannot be edited.

24. The **AUTO REFRESH AND ALERTING** section provides you with an option as to how frequently (**Auto refresh interval**) the content of the PRTG web page is to be refreshed automatically. You can also disable automatic refresh if required. Additionally, you may even configure the **Play Audible Alarms**.

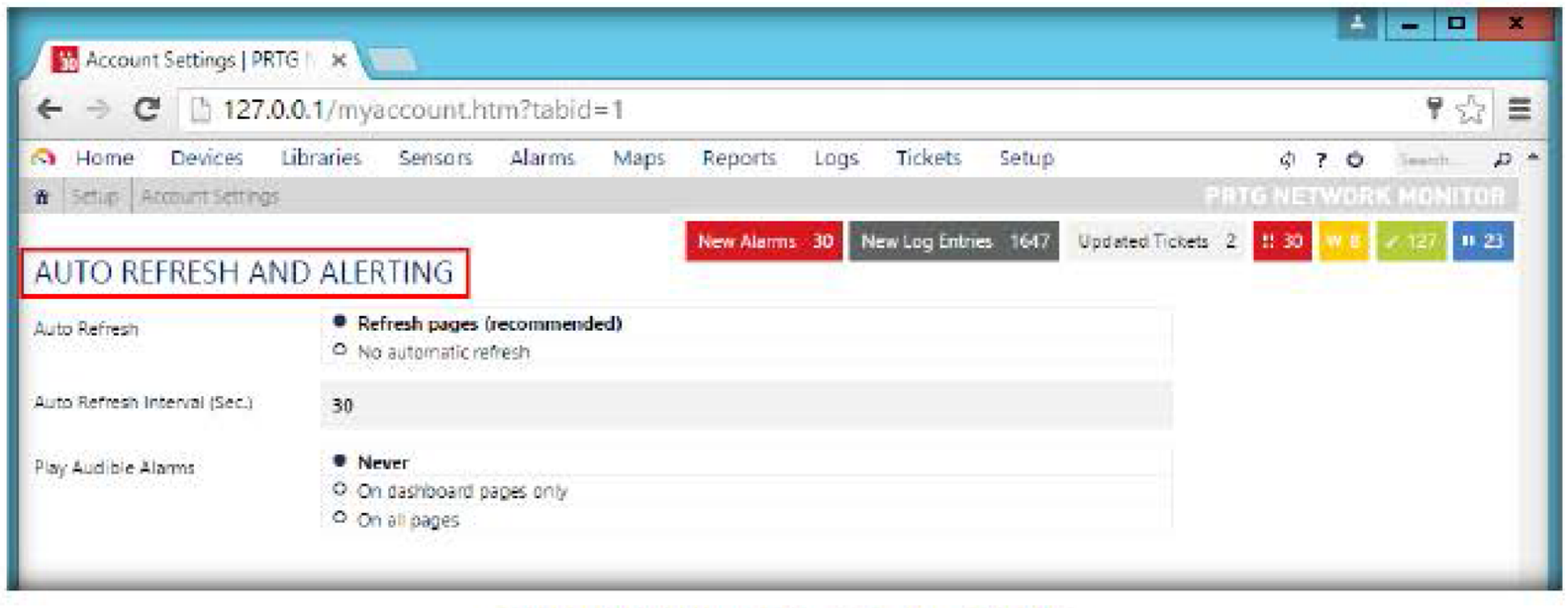



FIGURE 5.16: Auto Refresh Section of PRTG



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

25. The **WEB INTERFACE** section contains the homepage URL which is the page displayed immediately after login. The Max. Groups/Devices per Group section defines the number of groups and devices that can be shown before reduction of a group or device can be performed.
26. The next sub section Max. Sensors per Device defines the maximum number of sensors that can be shown before performing the reduction. The time zone can be changed to your local area time and the date format can be kept the same as the system date
27. The **TICKET SYSTEM** section, which if enabled, generates an email every time a ticket is assigned to the administrator or the user group, or an assigned ticket's status is changed.
28. Leaving all these section's configurations set to default, click **Save**.

PRTG uses notifications to send you alerts whenever PRTG discovers a defined status, such as slow or failing sensors, or when sensor channels breach threshold values. You can define an unlimited number of notifications allowing to use one, or more, of several communication channels like email, text messaging, push notifications to Android and iOS devices, and many more.

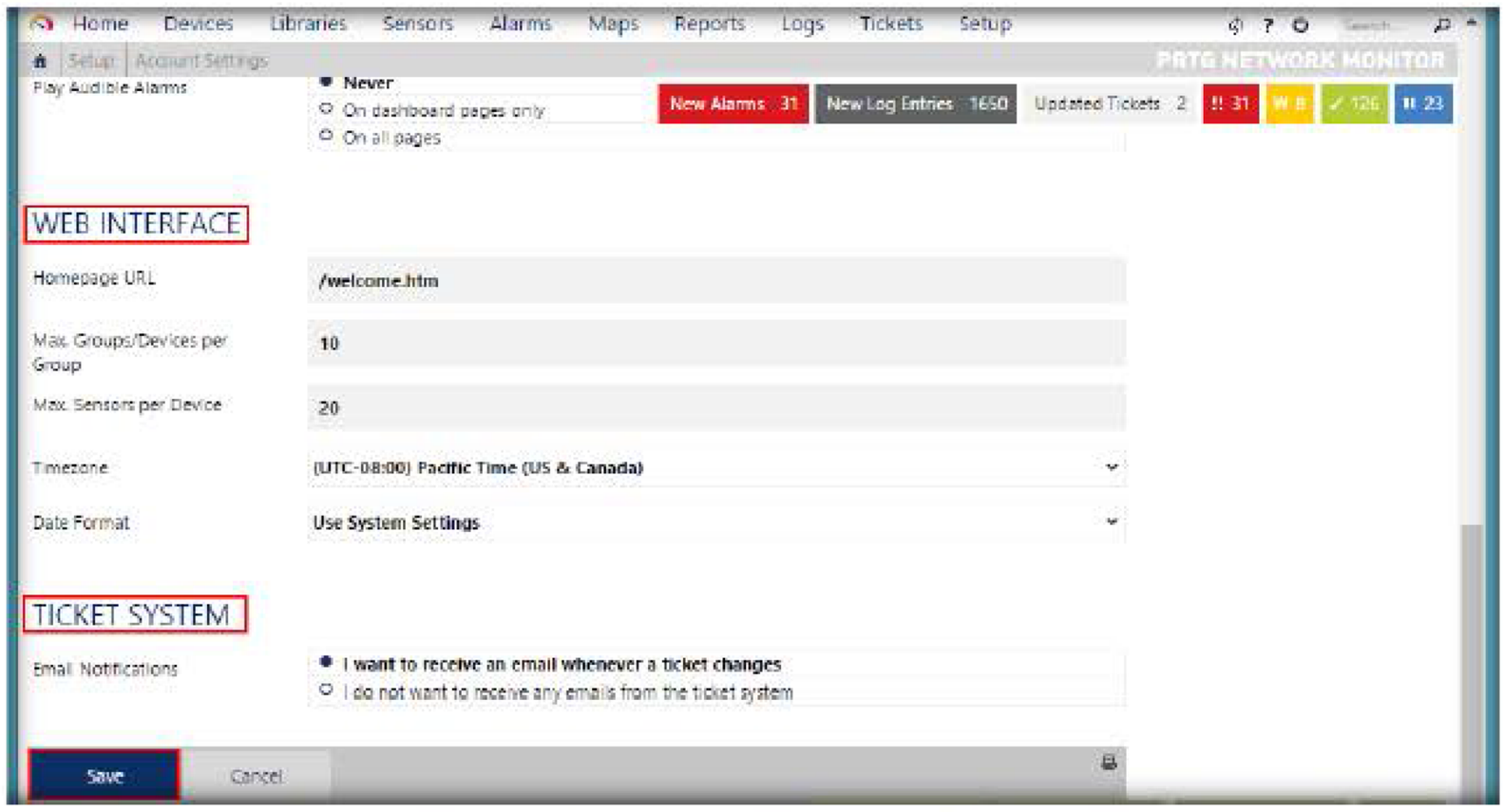



FIGURE 5.17: Web Interface and Ticket System Sections of PRTG

29. Now we shall explore the **notification** section of the PRTG. Notifications are meant to send out a message when something abnormal is detected in the network. It can be sent in the form of a mail or a text message to a predefined number.
30. Navigate to **Setup → account settings → notifications** in PRTG.

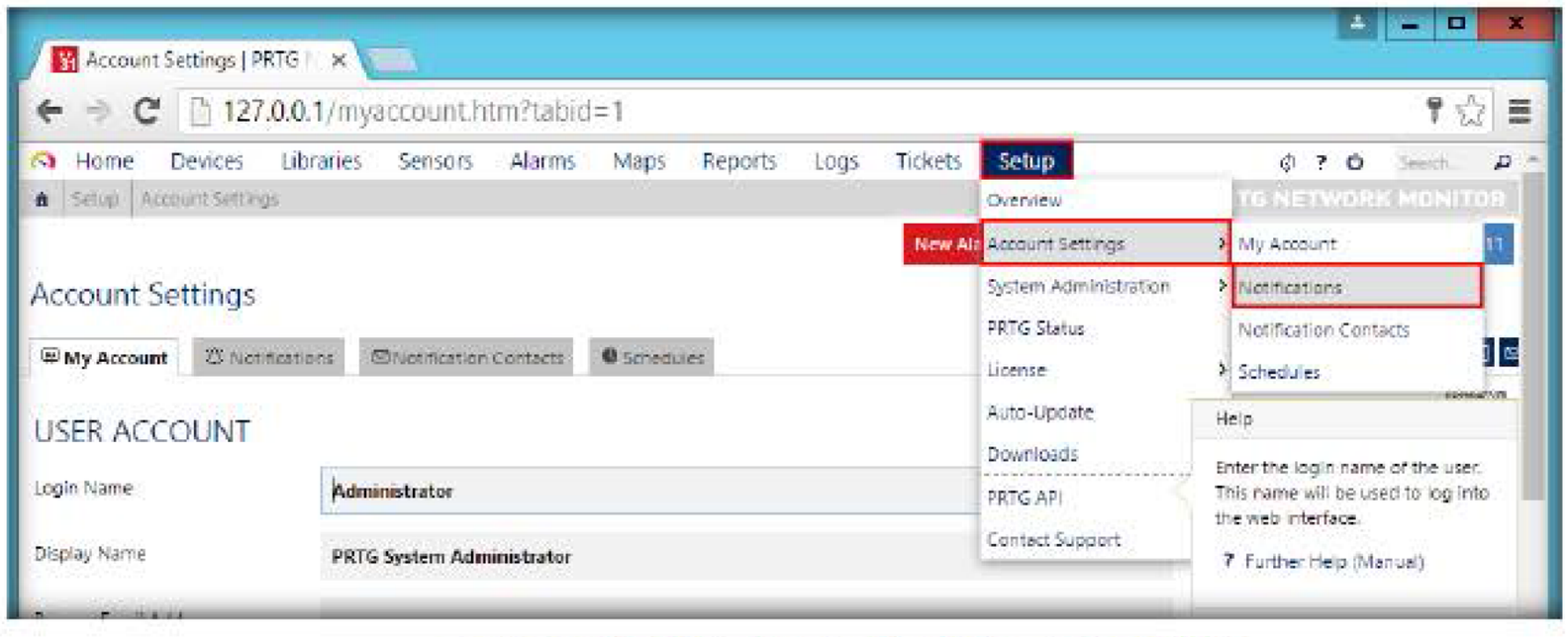



FIGURE 5.18: Navigating to the Notifications Section of PRTG


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

31. You are left with three notification options which are mailing to the Administrator, mailing to PRTG user group members and ticket notification. To make changes to any of the existing notifications click on edit button.

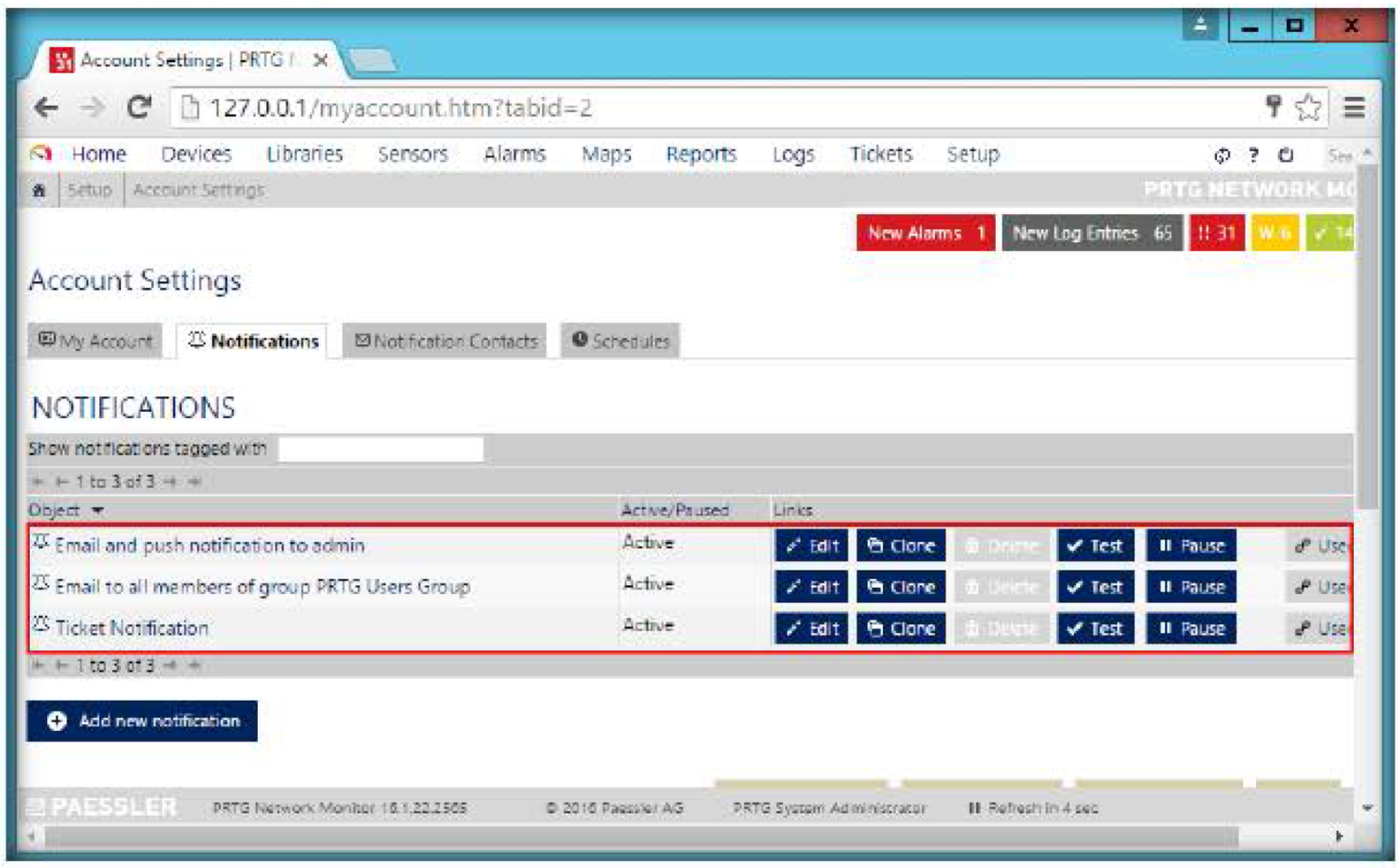



FIGURE 5.19: Notification Section of PRTG

32. Now in the **BASIC NOTIFICATION SETTINGS** section, you can change the default name of the notification, mention a few tags for filtering, change the state of the notification to be started or paused.

33. Next is the **Schedule** sub section, in which you can set up a schedule to receive notifications only on particular days and finally you also have an option to postpone notifications in which you can either collect them not at all, in paused state or collect them and send when reactivated.

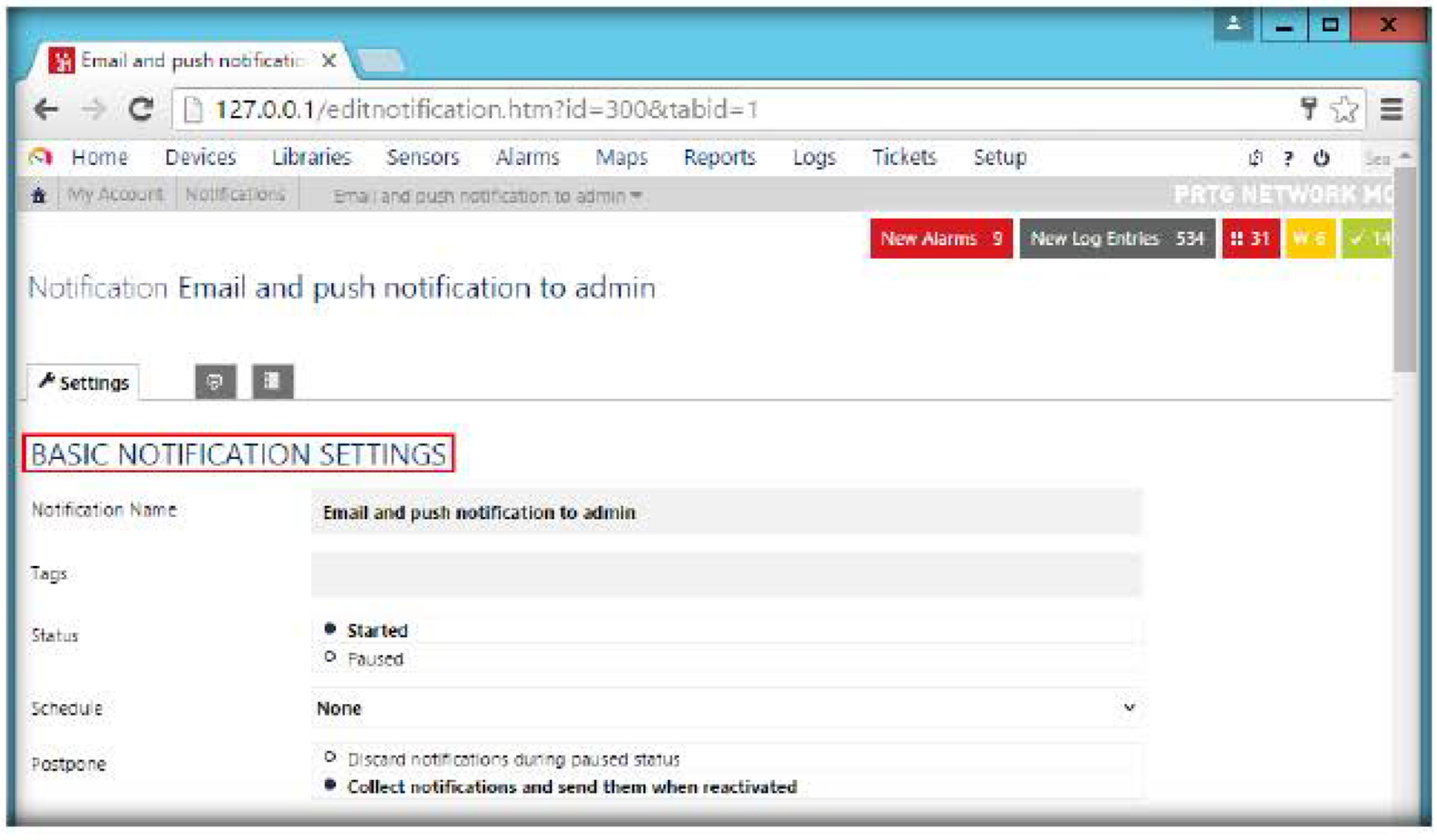



FIGURE 5.20: Various Settings in the Notifications Section


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

34. The **NOTIFICATION SUMMARIZATION** section provides different options which you can set PRTG to customize summary of the notifications with these options.
35. You can also set up a Subject line for summarized messages and set out the time frame (minutes) after which the summarization takes place.
36. The **ACCESS RIGHTS** section allows you to give various permissions (read, write and full) to different user groups.

Define which user can access what in your PRTG Network Monitor installation and manage all the user rights with the access rights system of PRTG.

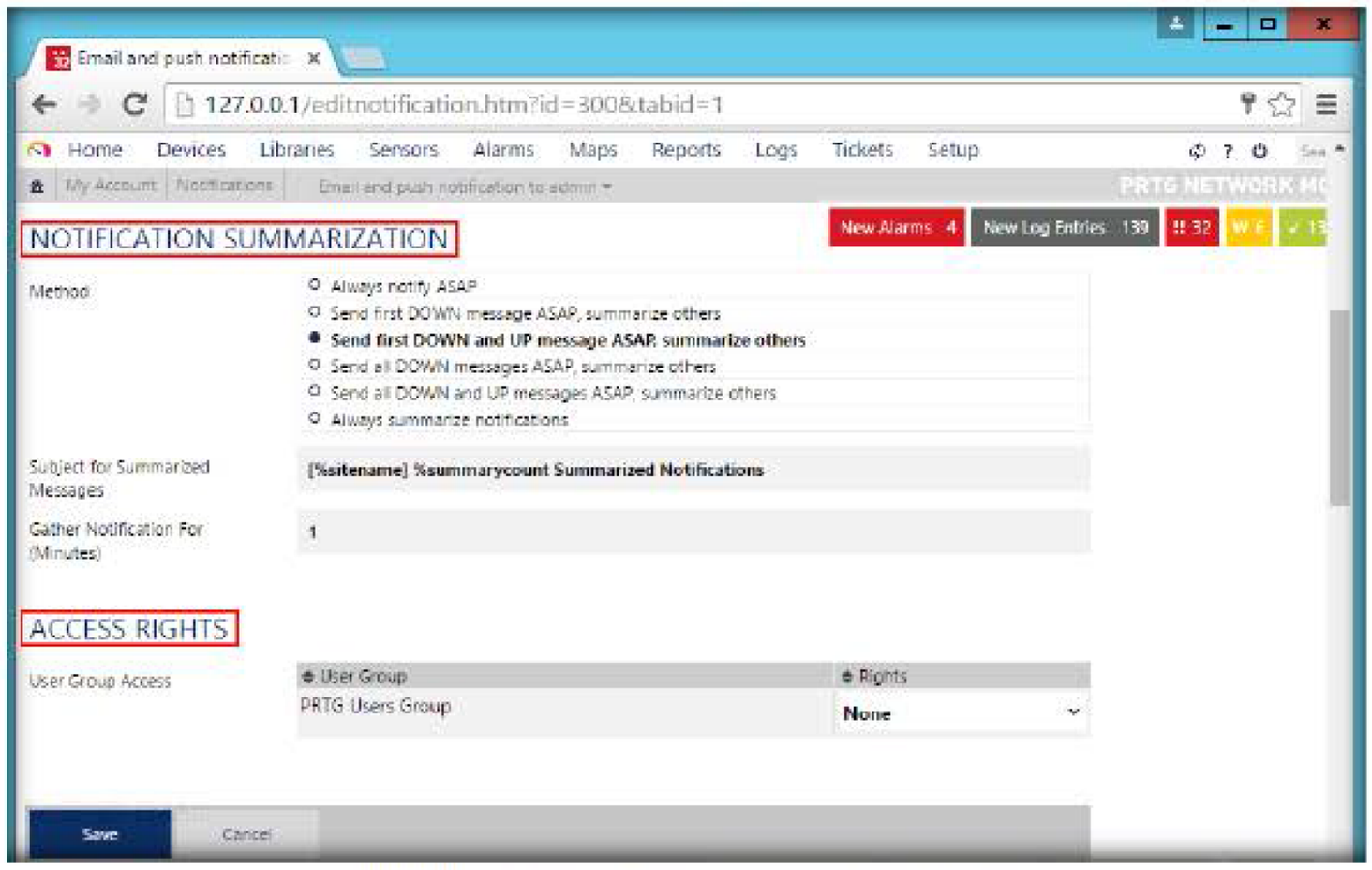



FIGURE 5.21: Various Settings in the Notifications Section

37. After this, you can configure the way you wish to be informed. There are quite a few methods like Email, Push Notification, SMS, SNMP trap and so on. After completing the update of your settings, click **Save**.

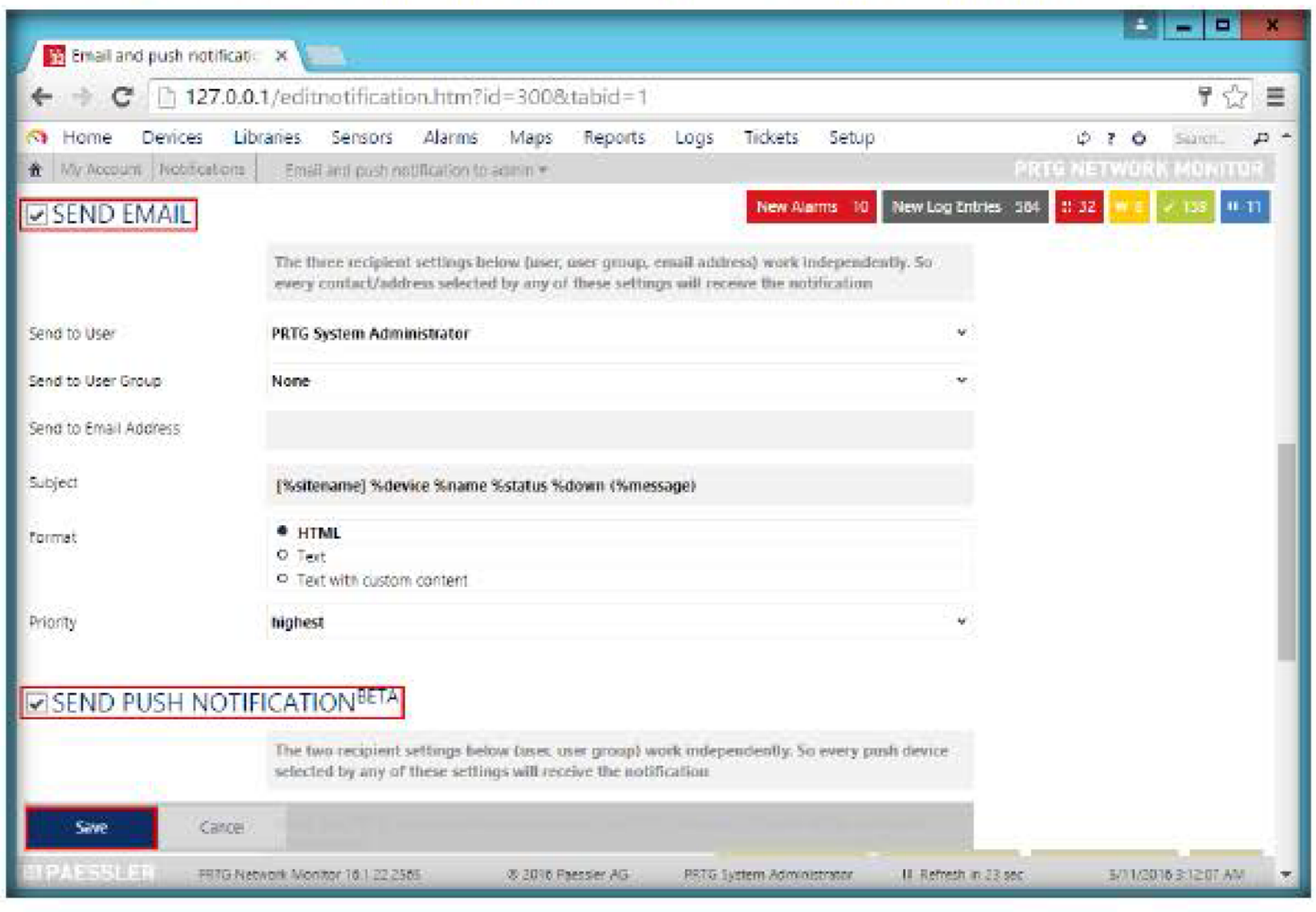
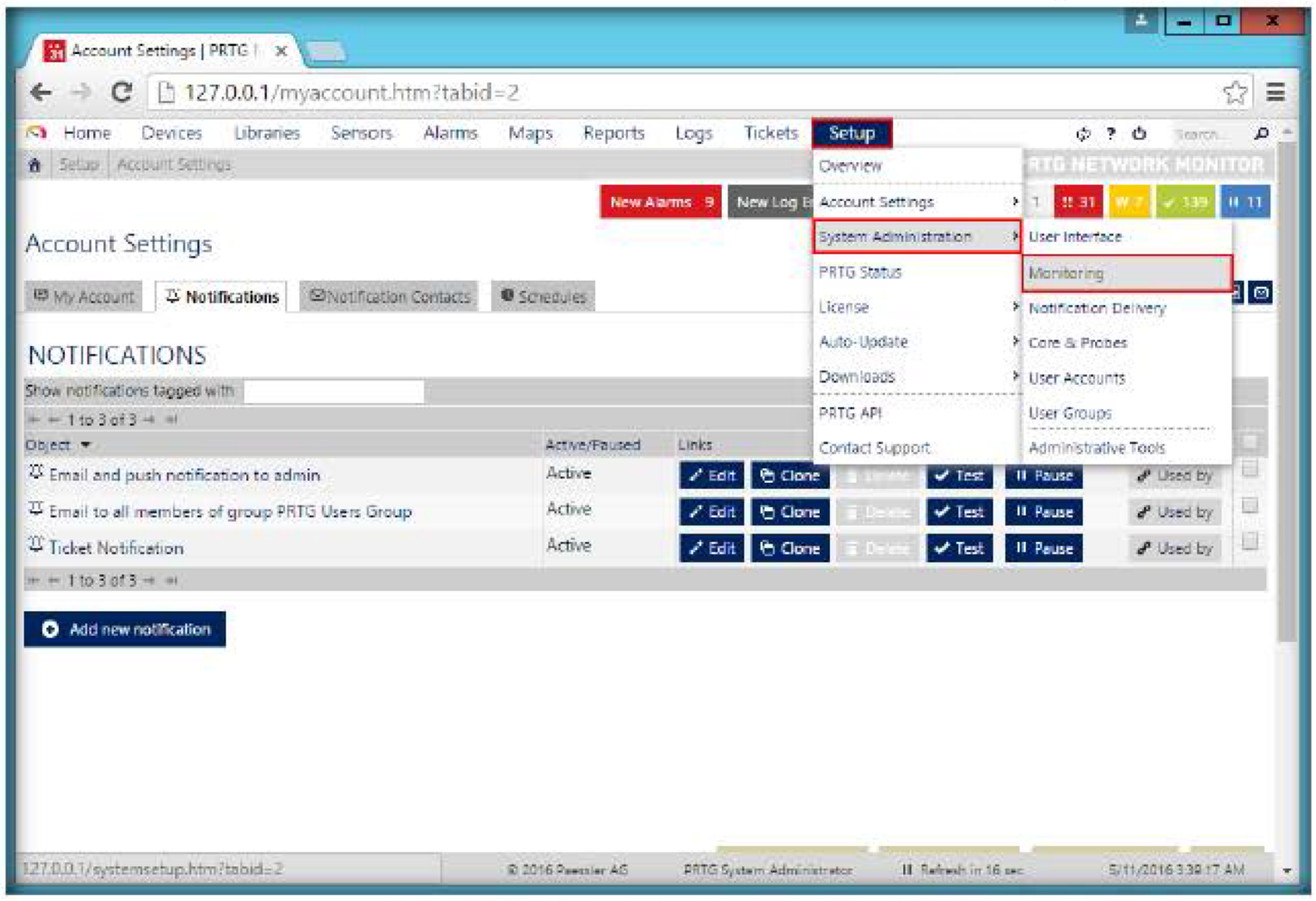



FIGURE 5.22: Various Methods through Which Notification is Received in PRTG



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

38. Next, we explore the monitoring options in the **System Administration** section. Hover the mouse cursor on **Setup**, hover the cursor on **System Administration** and then select **Monitoring** from the drop down list.




In the monitoring settings you can define global values regarding scanning intervals, unusual and similar sensors detection, auto-discovery, and uptime threshold.

FIGURE 5.23: Monitoring Sub Section in System Administration

39. The first section deals with the available **Monitoring Interval** time frame which can be configured in the settings section of every device tree.

40. The **UNUSUAL DETECTION** section has daily and hourly comparison methods. Daily average compares the previous day's average with other week days which have already passed. And hourly average compares previous hour average with other past hours of the same week, day and hour. You can set the percentage level which can be termed as unusual

41. The next two sections deal with **SIMILAR SENSORS DETECTION** and **RECOMMENDED SENSORS DETECTION**. Similar sensors can be configured to detect over primary channels only or all channels. But, it is recommended leaving it to the default settings.


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

42. Similarly **RECOMMENDED SENSOR DETECTION** which instructs the Administrator as to how he should deal with recommended sensors, which can be set to either always show or never show. However the best setting is the default recommended setting.

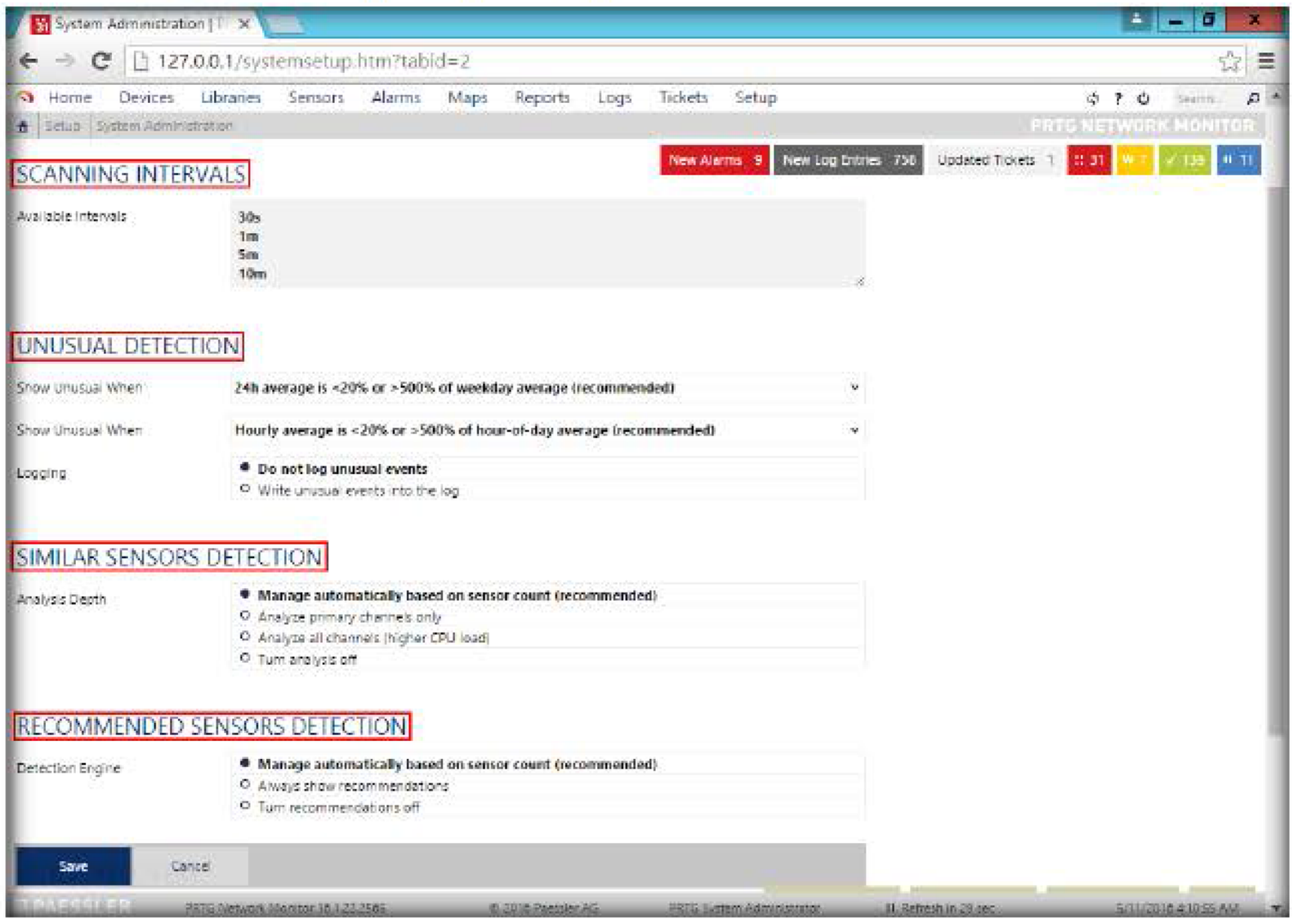



FIGURE 5.24: Monitoring Section in System administration settings

43. The **Auto-Discovery** section lets you to set a particular time in a day at which the auto discovery should take place and the **UPTIME TRESHOLD** section determines the minimum value below which a sensor's good requests fail and the sensor turns red. Maintain default values for both of these sections. Click **Save** after the settings are configured. In this lab, all the default settings have been chosen.

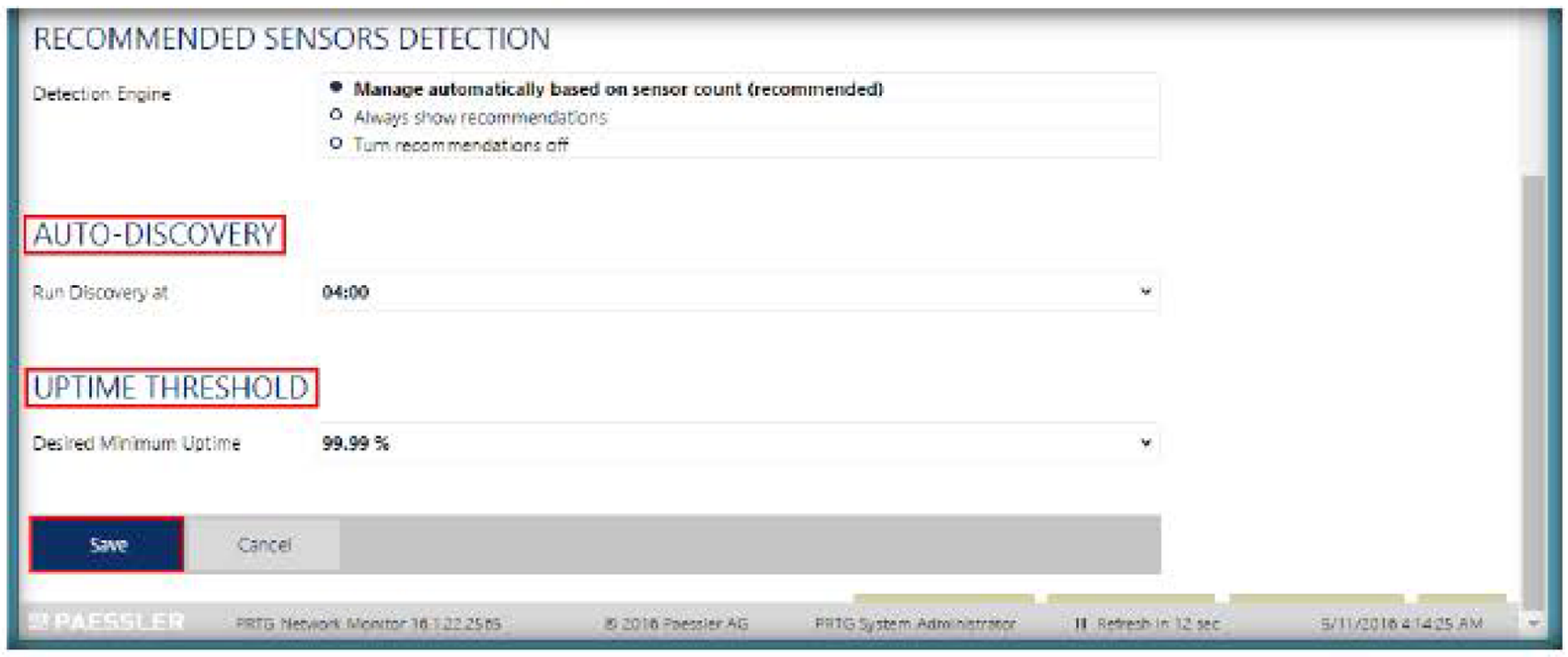



FIGURE 5.25: Auto Discovery and Uptime Sections in Monitoring



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

44. The next section is **Notification Delivery**. To go to the **Notification Delivery** section, hover the mouse cursor on **Setup**, hover the cursor on **System Administration** and then select **Notification Delivery** from the drop down list.

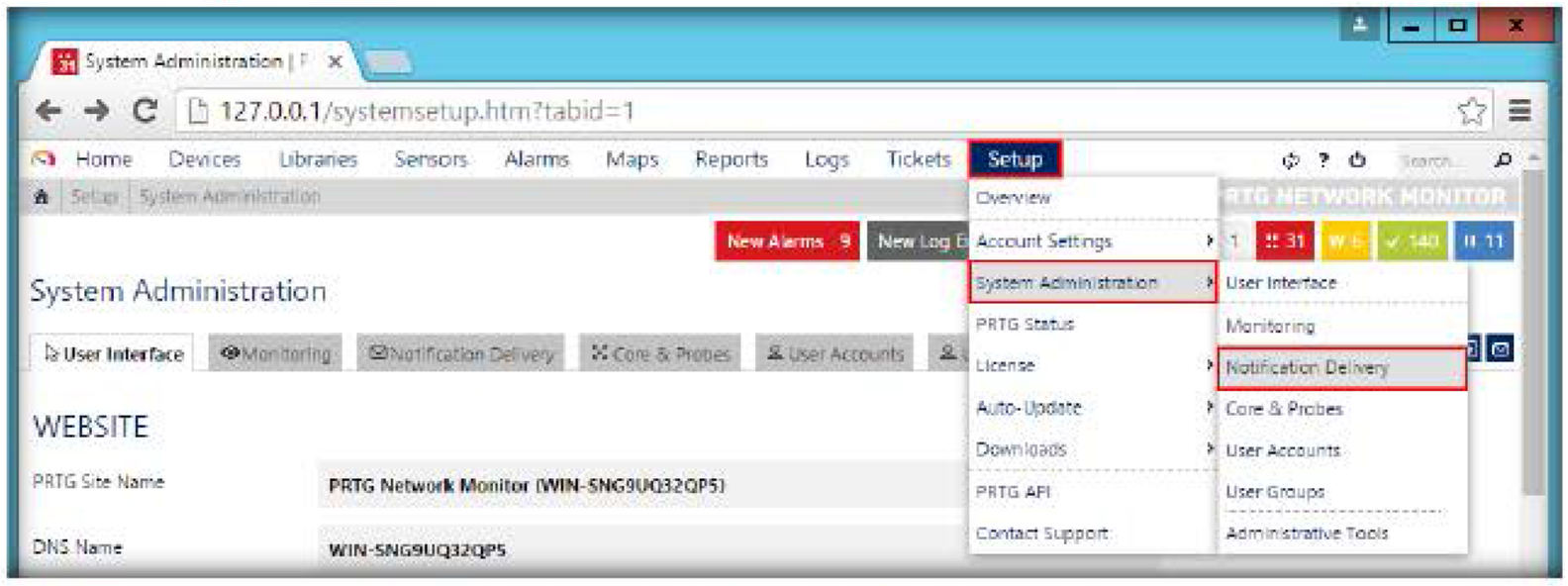



FIGURE 5.26: Notification Delivery in PRTG

In the notification delivery settings you can define global settings for notification delivery. If you do not want to use a specific notification method, just leave the respective fields empty.

45. The Notification Section deals with setting up the **SMTP Server and SMS DELIVERY**. The SMTP DELIVERY mechanism can be used to select the way in which the SMTP notification is delivered. You can also configure the sender's name and E-mail address

46. In the **HELO Ident** section you can set the DNS name which PRTG is running.

47. The SMS DELIVERY section can be used to select the correct configuration mode. Either select the sender from an existing list of service providers or select a new service provider. In the following sections you can set up various fields of service providers. Click **Save** when done.

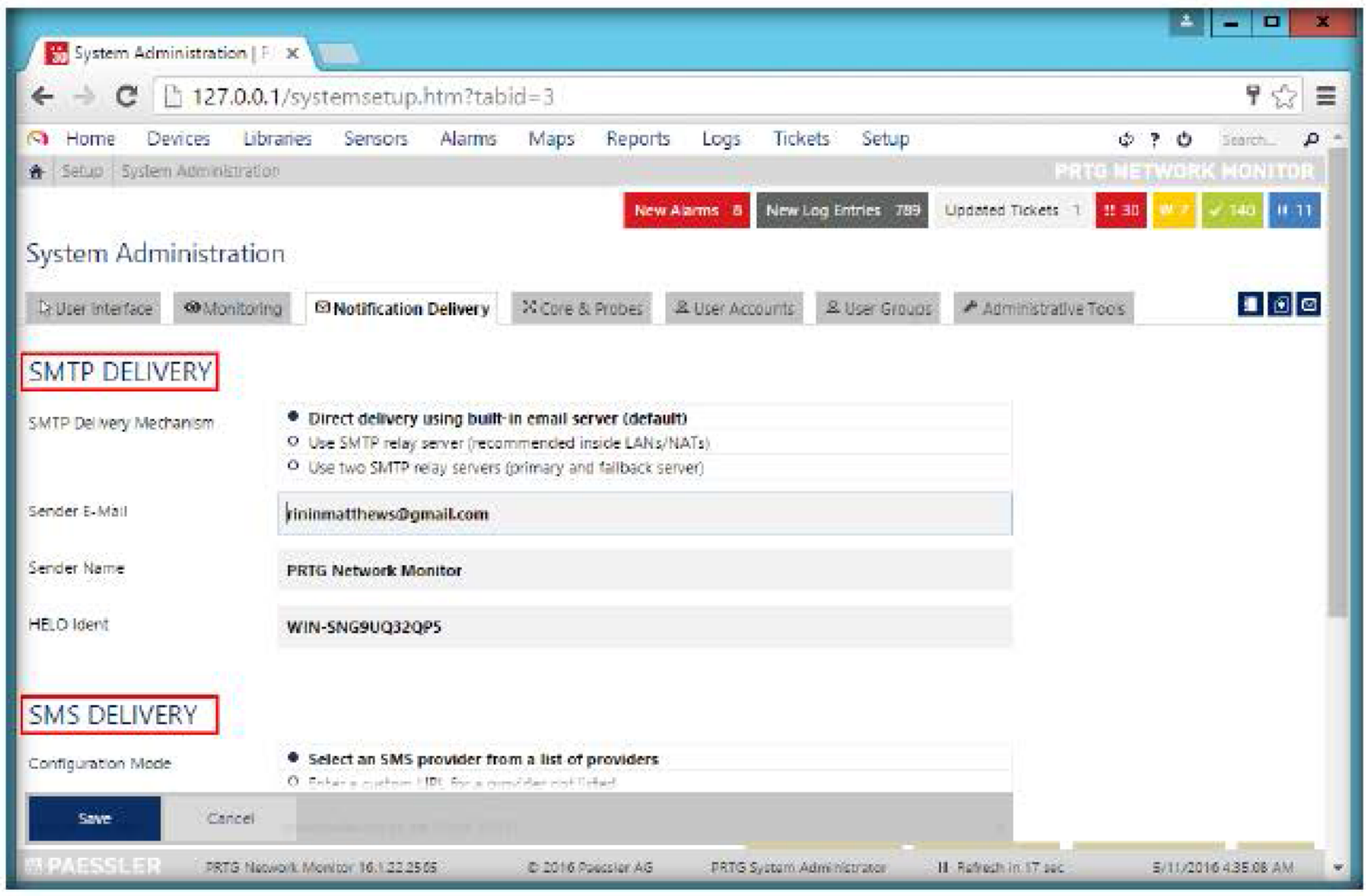



FIGURE 5.27: Notification Delivery in System Administration Section of PRTG



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

48. The **Core & Probes** section lets you configure the way in which a probe should be handled. If you are using a proxy server to get probes you can specify the details in the **PROXY CONFIGURATION** section or you can use the default option of no proxy. Click the **Core & Probes** tab in the webpage to view and configure the section.
49. In the **PROBE CONNECTION SETTINGS,** you have the probe connection IP's in which you can select which IP's to receive the probes (local 127.0.0.1, all IP's or specific IP's)
50. The next section is **Access Keys** which allow you to specify a set of passwords and any probe that needs to connect to PRTG should enter one of the passwords mentioned in this section.
51. The **Allow IP's** lets you specify a set of IP addresses from which the probes will be accepted and if it is left blank then only those probes originating from the local host are accepted.
52. Similarly the **Deny IP's** addresses lets you specify a set of IP addresses from which probes should not be accepted. If an IP address is in both the Allow and Deny list, then it will be denied.
53. In the **Deny GID's** section, you can define a set of Global ID's(GID) which can be denied access and any probe from this GID will not be accepted. The mini probes can be set up in the next section

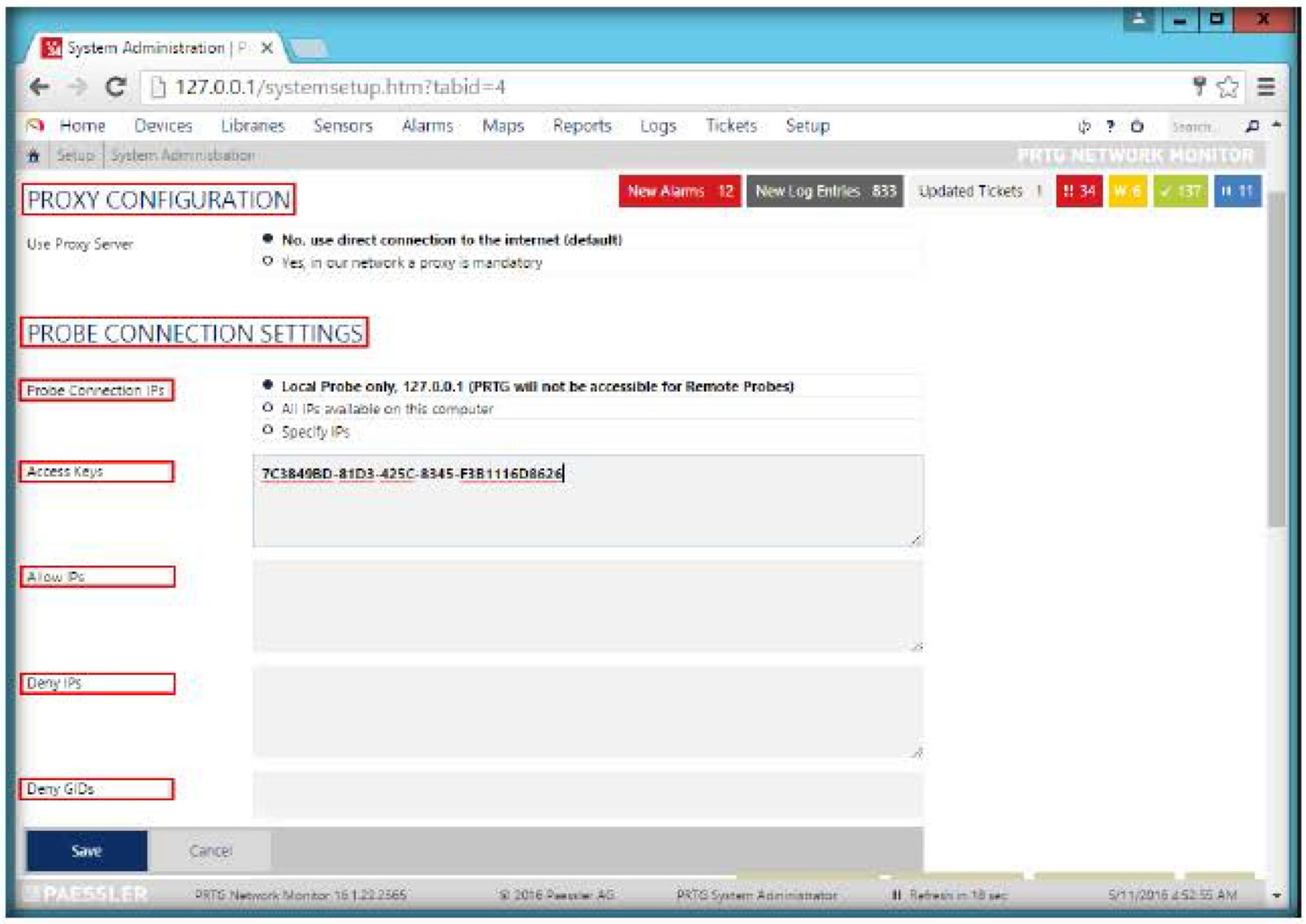



FIGURE 5.28: Probe Settings Section in Network Administration


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

54. If you have an active directory from where probes can be expected this can be configured in the active directory integration section. Historic data pruning allows you to specify the number of days the data for various protocols should be saved. You can use the default values in these cases.

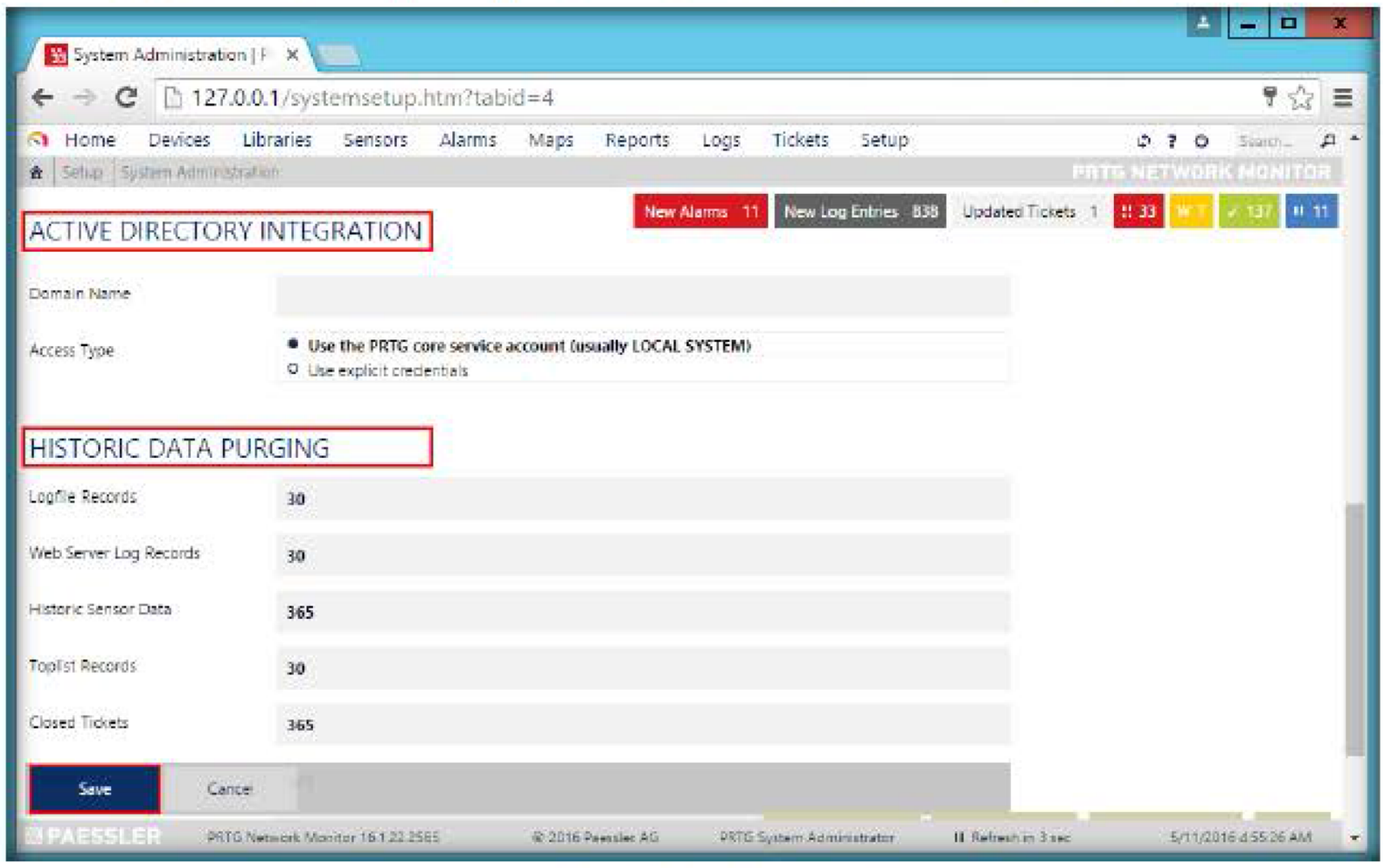



FIGURE 5.29: Probe Settings in PRTG

The Devices tab is your starting point for everyday use. The page is split into two parts. On the left hand side, it shows the tree-like device view which lists all configured PRTG core servers with their probes, groups, devices, and the sensors on the devices, in a hierarchical order. Next to each object you see an overview of the number of sensors, grouped by their current status.

55. Let us view the devices discovered by the PRTG Network Monitor. To view the devices, click on the **Devices** tab. The Devices window appears, displaying all the discovered devices as shown in the following screenshot:

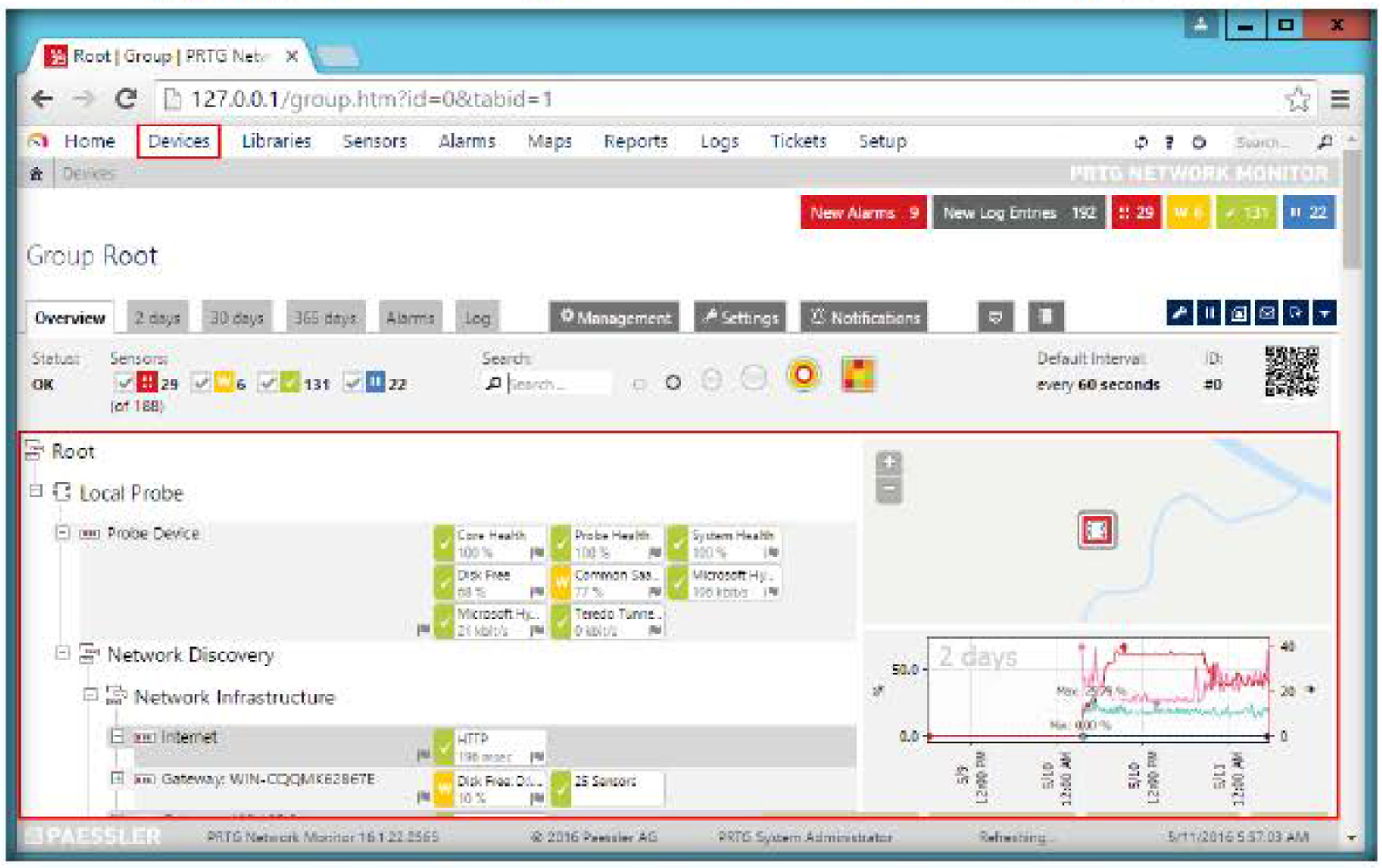



FIGURE 5.30: Various Types of Devices in the Network Shown in PRTG



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

56. PRTG discovers all the devices on the network but we do not want to monitor all of the devices in our network. We have our host machine and a few hyper-v virtual machines under it.
57. Let us add the **Windows Server 2008** virtual machine, in order to monitor the traffic flowing through the machine
58. Click the **Add Device** button under the **HyperV** section

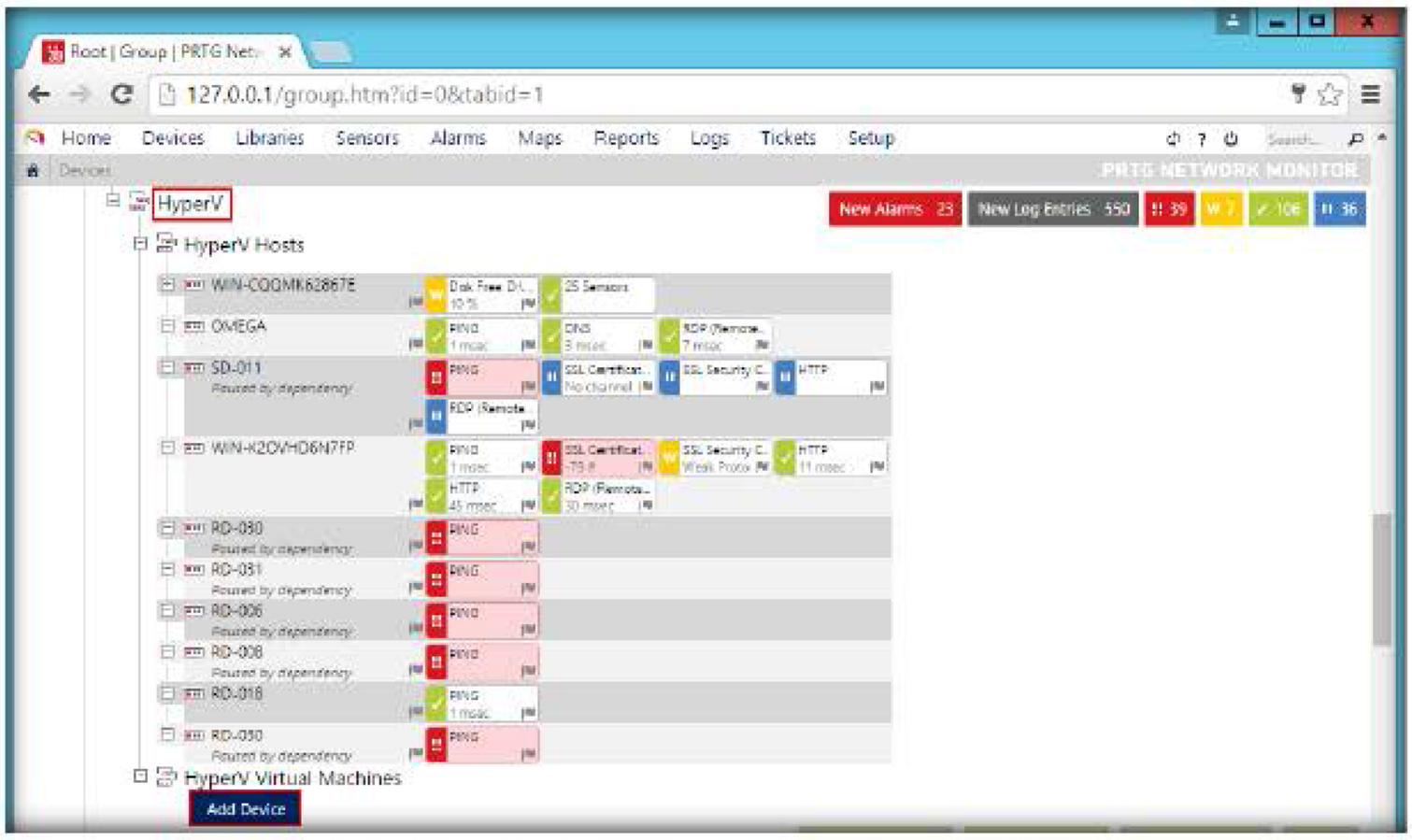



FIGURE 5.31: Various Types of Devices in the Network Shown in PRTG

59. The Add Device to Group Hyper-V Virtual Machines pop-up appears; enter the **Device Name** as **Windows Server 2008**, the IP address of the Windows Server 2008 i.e., **10.10.10.8**, and select the **Windows** icon in the **Device Icon** section.

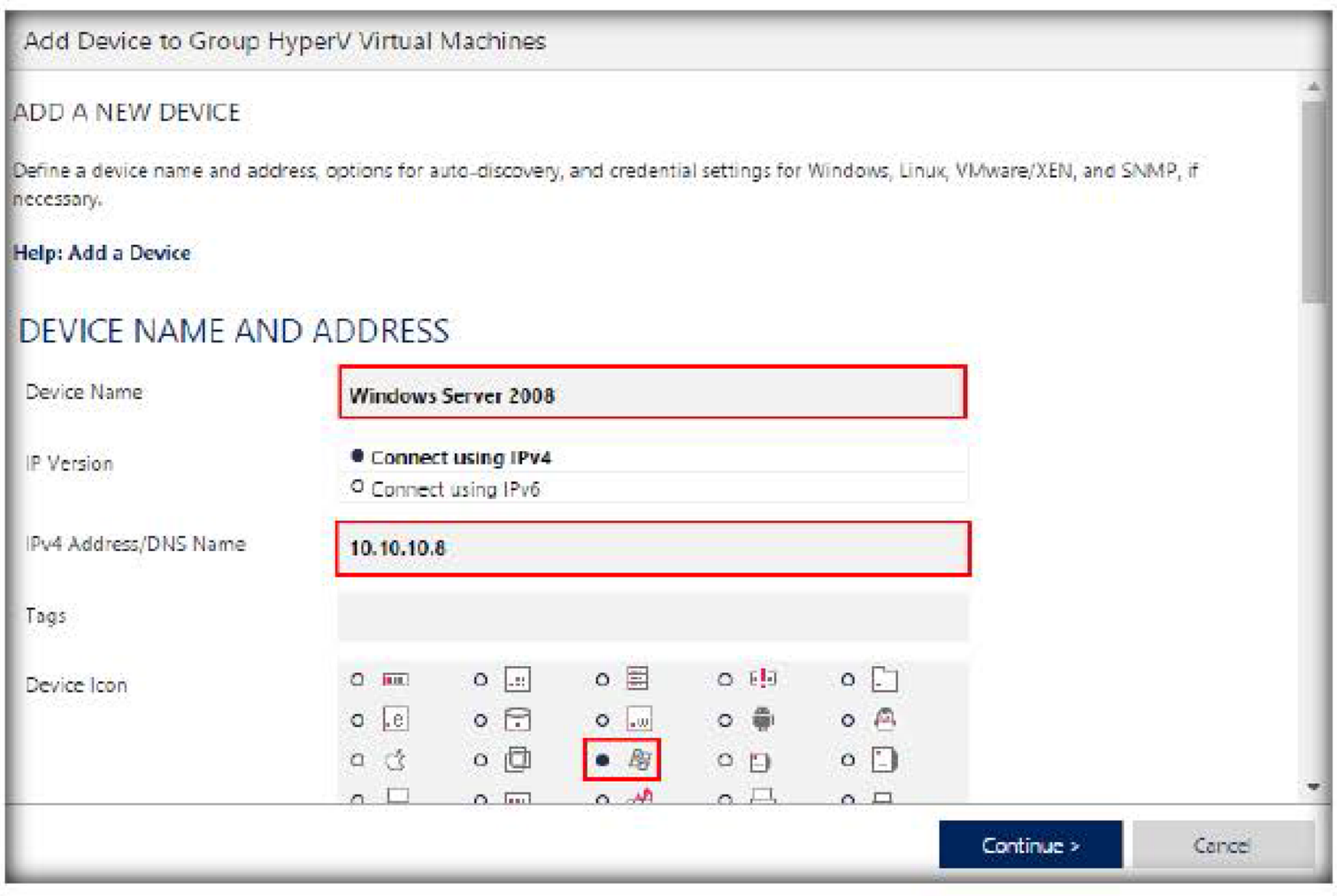



FIGURE 5.32: Adding a New Device in PRTG


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

60. Scroll the pop-up window down, select the **Automatic device identification (standard, recommended)** radio button under the **Sensor Management** section and click **Continue**.

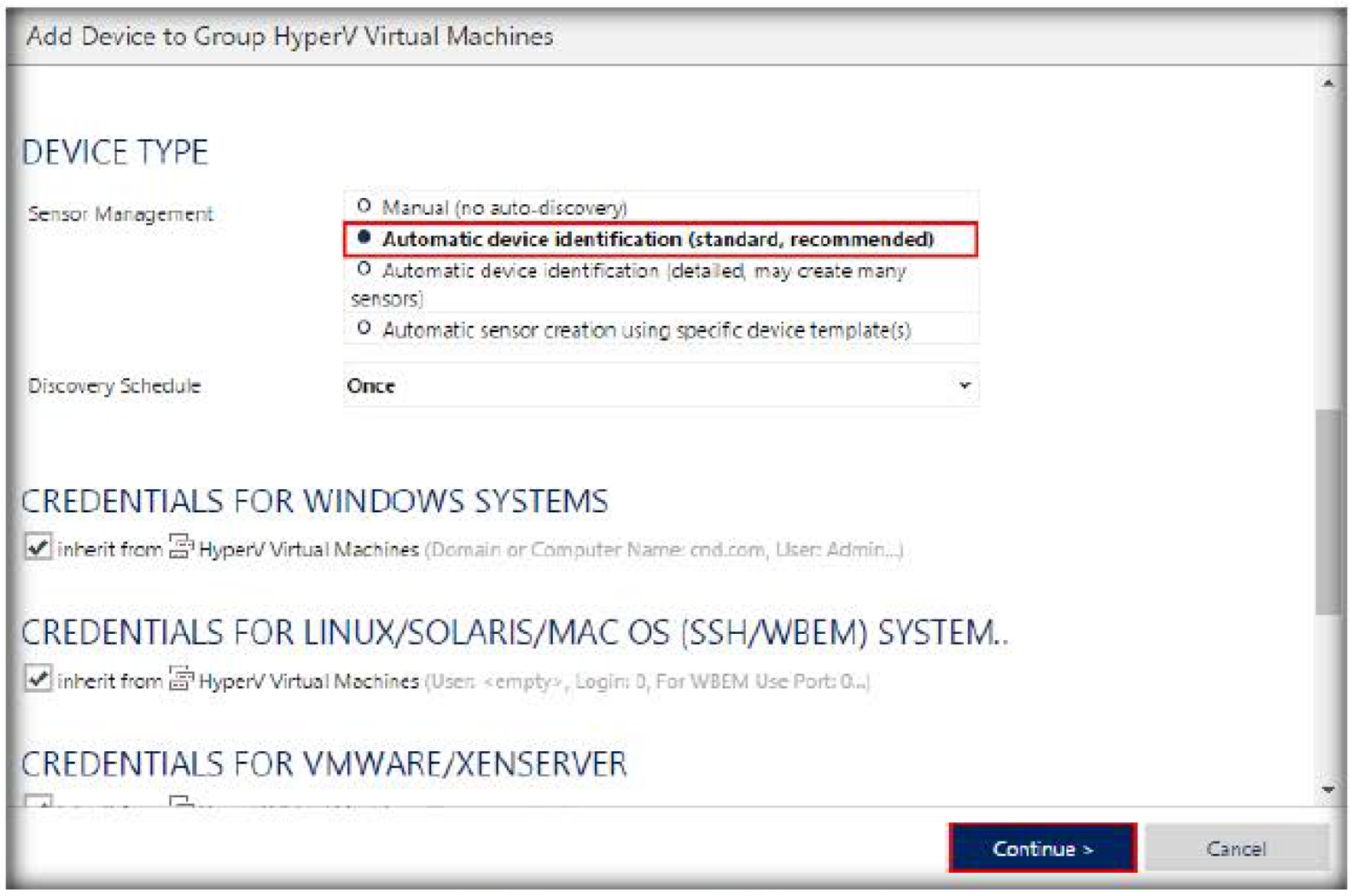



FIGURE 5.33: Configuring the New Device in PRTG

61. The added machine appears under the Hyper-V Virtual Machines section and PRTG monitor begins to perform auto-discovery on the machine as shown in the following screenshot:

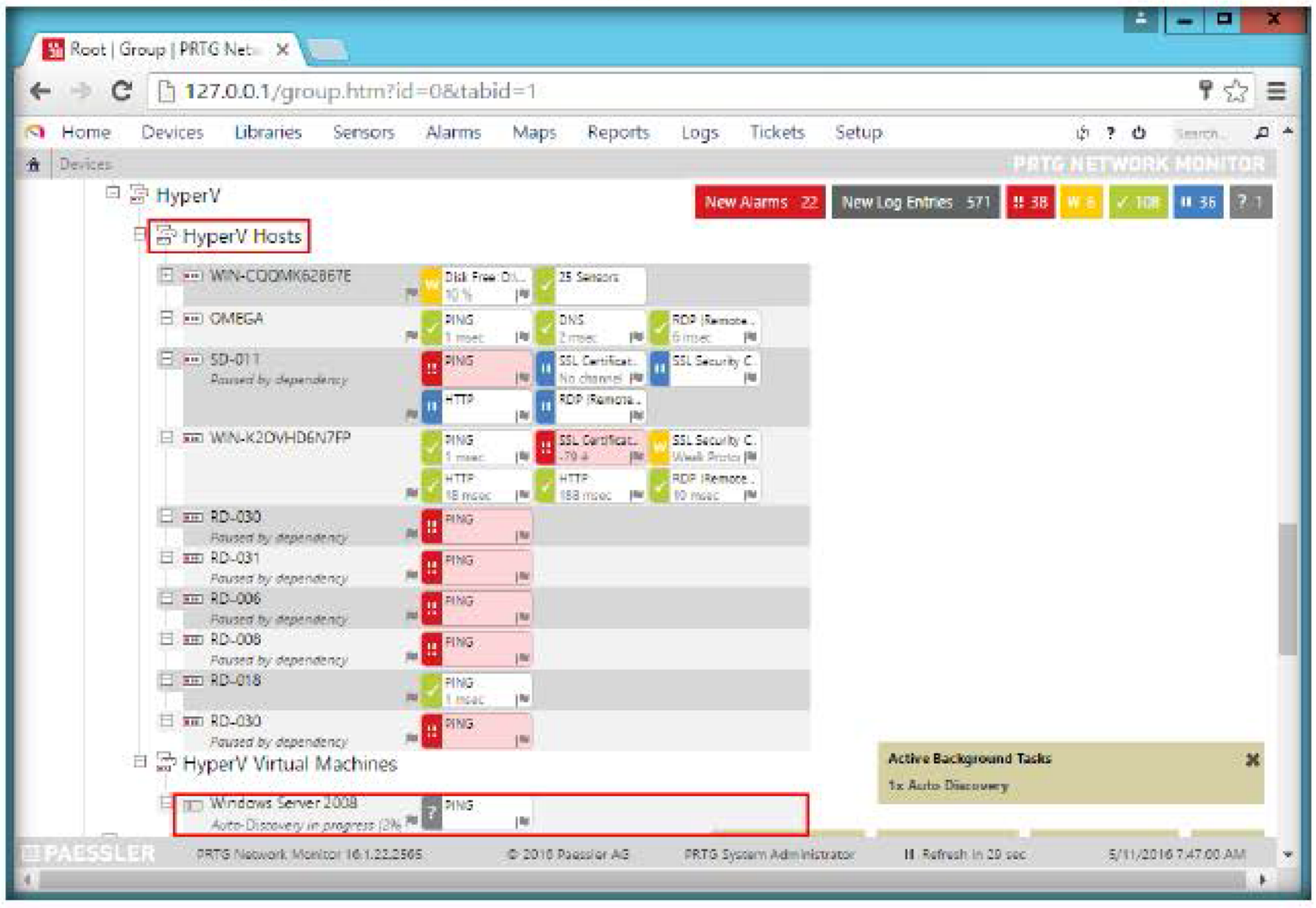



FIGURE 5.34: New Device Added in PRTG

The Hyper-V Host Server sensor monitors a Microsoft Hyper-V host server via Windows Performance Counters or Windows Management Instrumentation (WMI), as configured in the "Windows Compatibility Options" of the parent device.



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

62. It takes some time for the application to discover the machine. Upon successful discovery, PRTG network monitor adds a few sensors such as Ping, Memory, IIS, etc. to the machine as shown in the following screenshot:

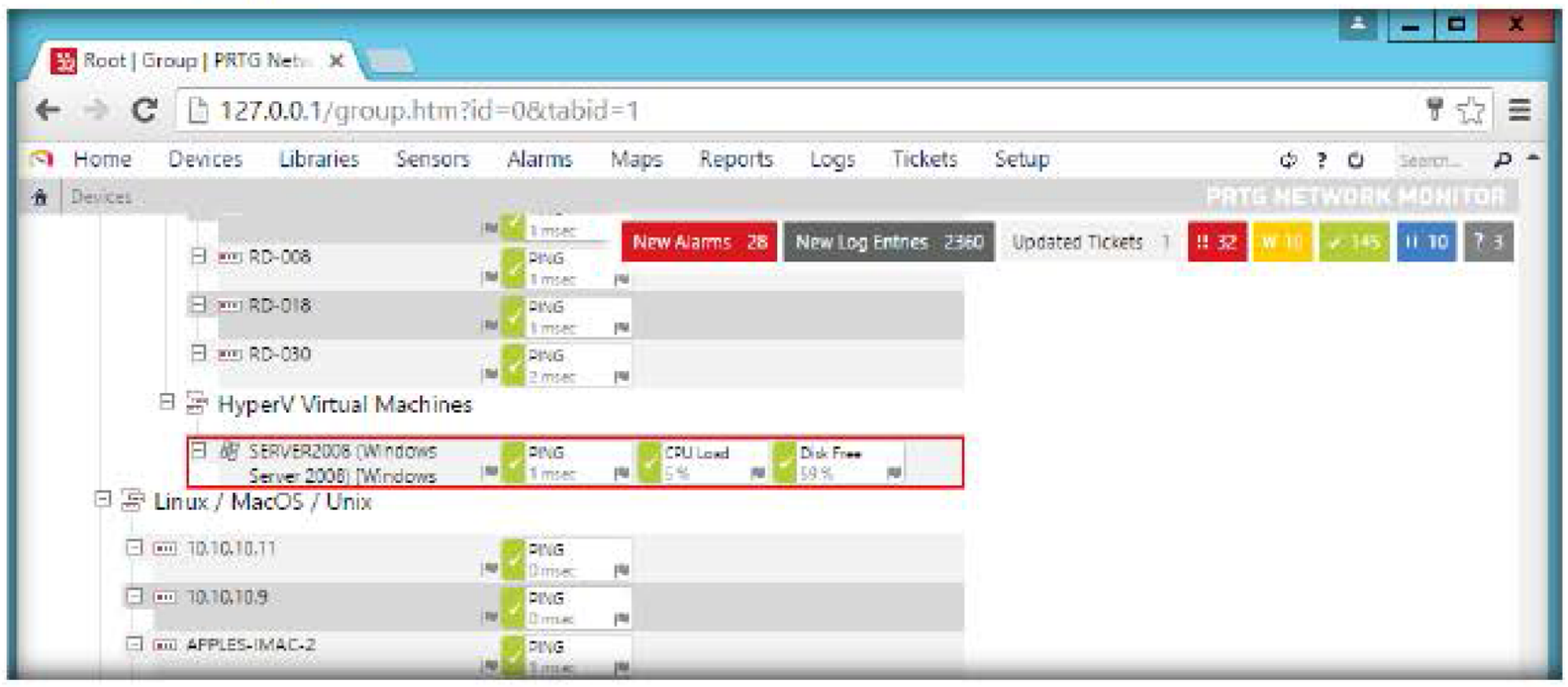



FIGURE 5.35: Sensors Running on the Newly Added Device

63. Now we see how to add a sensor to a device. **Sensors** are the basic elements of PRTG which make up an entire monitoring structure of PRTG.

64. A device can have any number of sensors and every sensor monitors a different aspect of the system.

65. To add a new sensor to the Windows Server 2008 device, right-click on **Windows Server 2008** and select **Add Sensor** from the context menu.

**TASK 5**

**Sensor Setup**

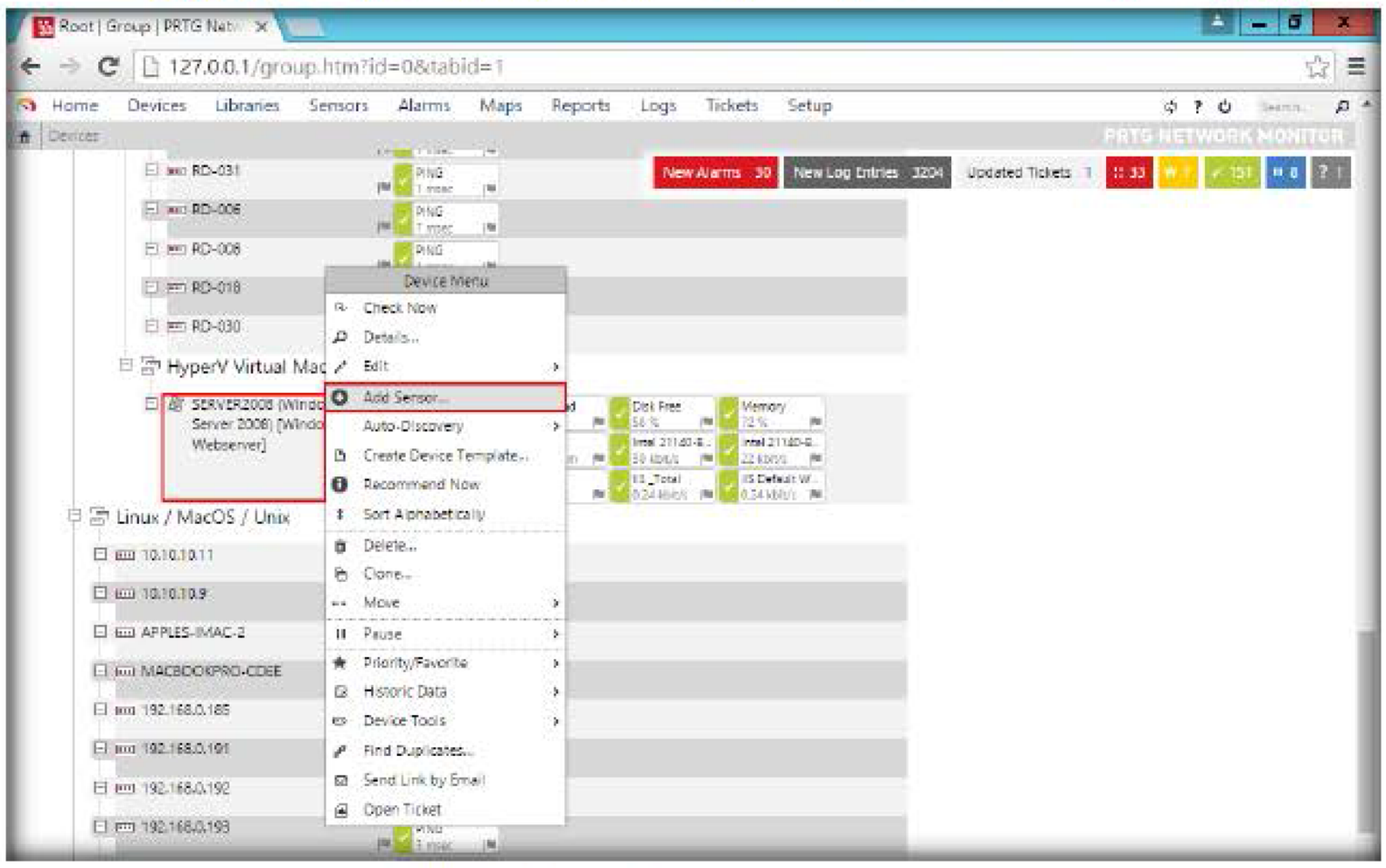



FIGURE 5.36: Initiating the process of new sensor addition

66. Now we shall select the traceroute sensor and this new sensor will be a part of the Windows client machine. To find the sensor, type the term "traceroute" in the **SEARCH** field.



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

67. While you are typing, the **Traceroute** sensor matching to the term appears in the search result. Select it.

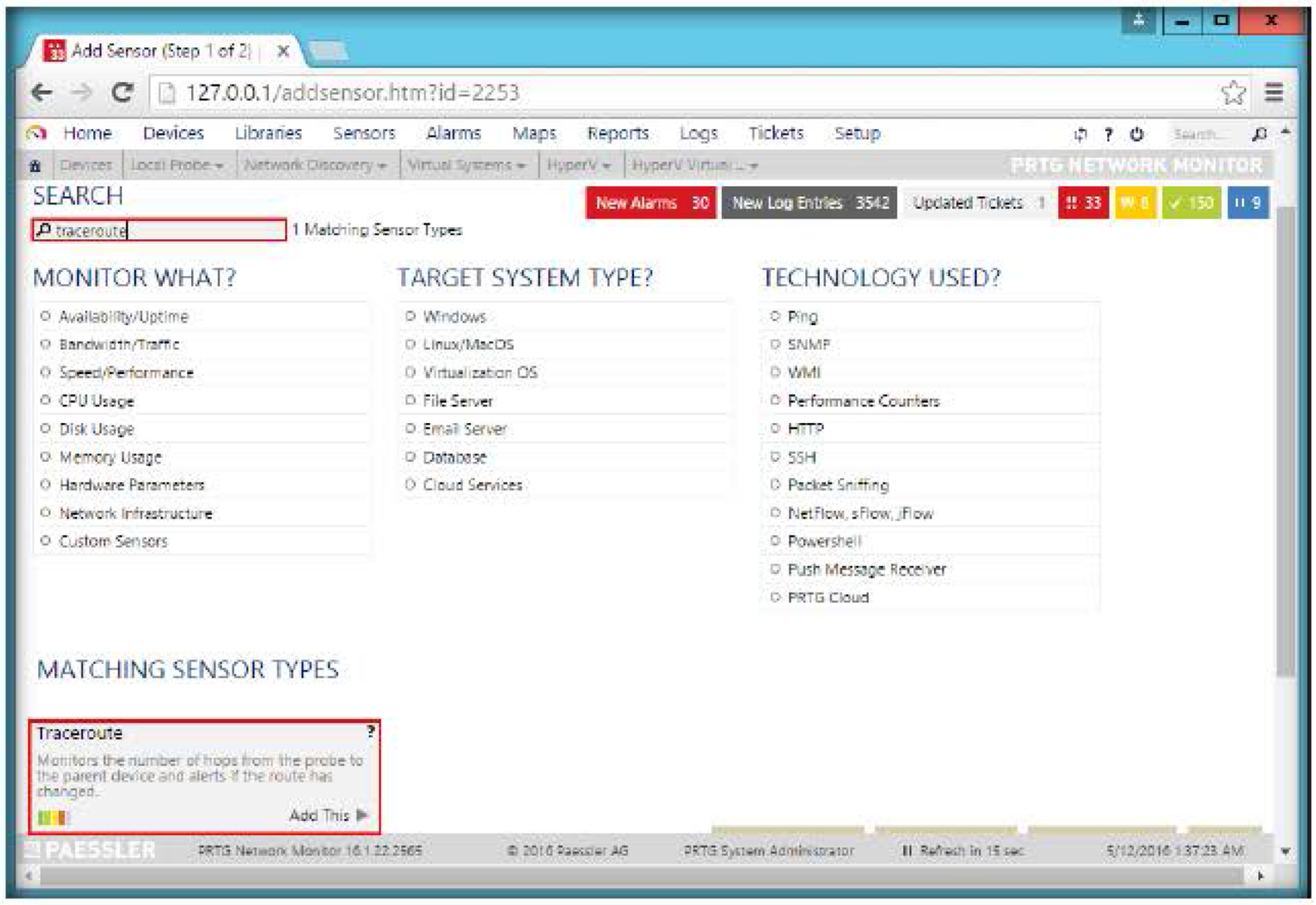



FIGURE 5.37: Adding a New Sensor

The Traceroute Hop Count sensor traces the number of hops needed from the probe system the sensor is running on to the IP Address/DNS Name defined in the sensor's parent device.

It shows the following:

- Execution time
- Number of hops.
- If the number of hops (the route) changes, you can additionally define another sensor status.

68. On selecting the sensor, the **BASIC SENSOR SETTINGS** window appears, where you need to configure the basic sensor settings like Name, Priority, tags, etc. of the selected sensor.

69. In the sensor setting, you need to define what action should be taken if a traceroute is altered. You can ignore it or set the sensor to a warning state or even an error state.

70. The final section is the scanning interval and it can either be inherited from the device or it can be reset. In this lab, the scanning interval is inherited from the device.


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

71. So, leave all the configurations set to the default and click **Continue**.

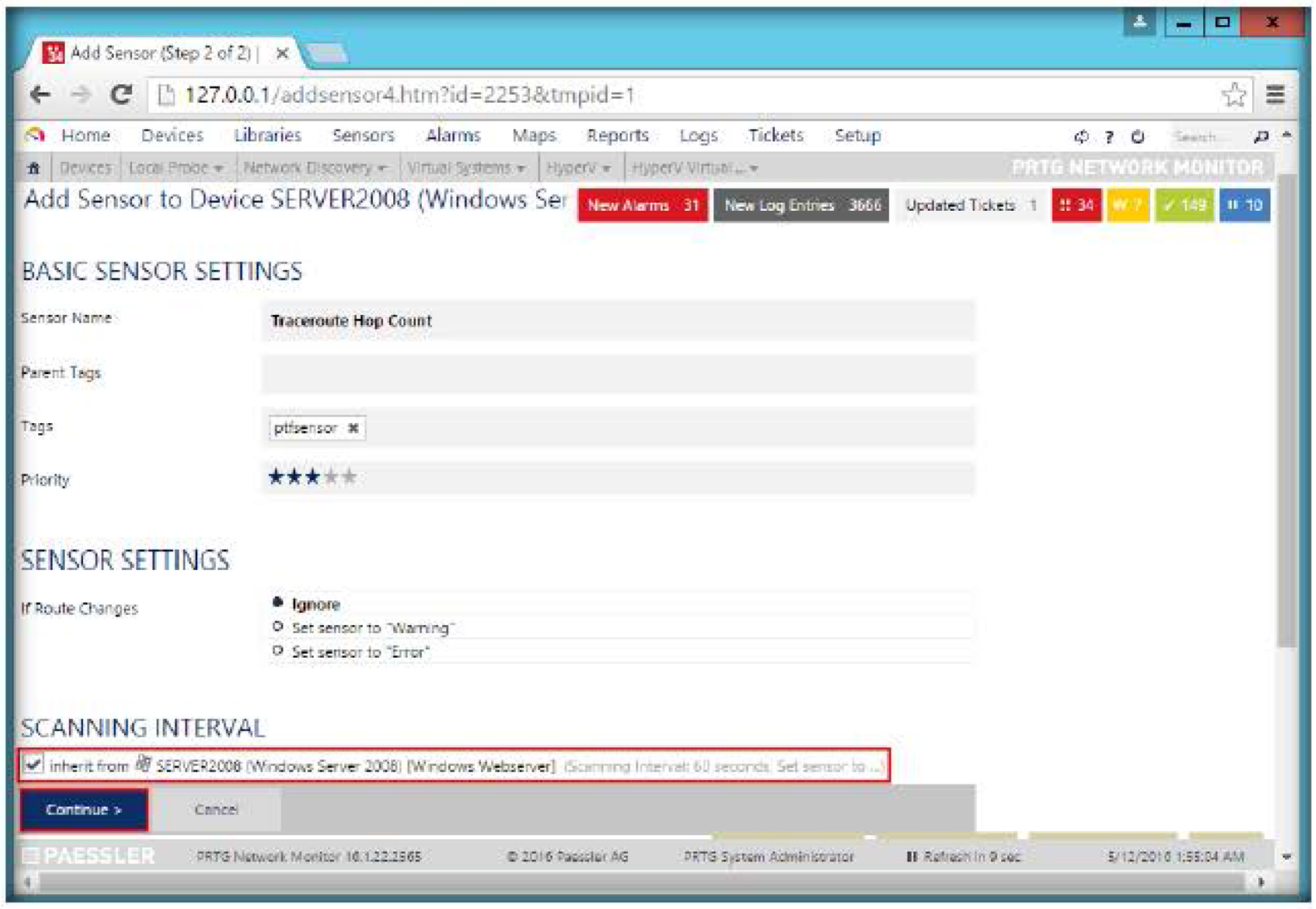



FIGURE 5.38: Setting up the Sensor for Use

72. Once you click Continue, you will be redirected to the Windows Server 2008 device overview webpage, displaying the status of the sensors. You may scroll the webpage down to view the added sensor. If you find the icon of the sensor in the color gray instead of green, right-click on the **Traceroute Hop Count** sensor and click **Check Now** from the **Sensor Menu**.

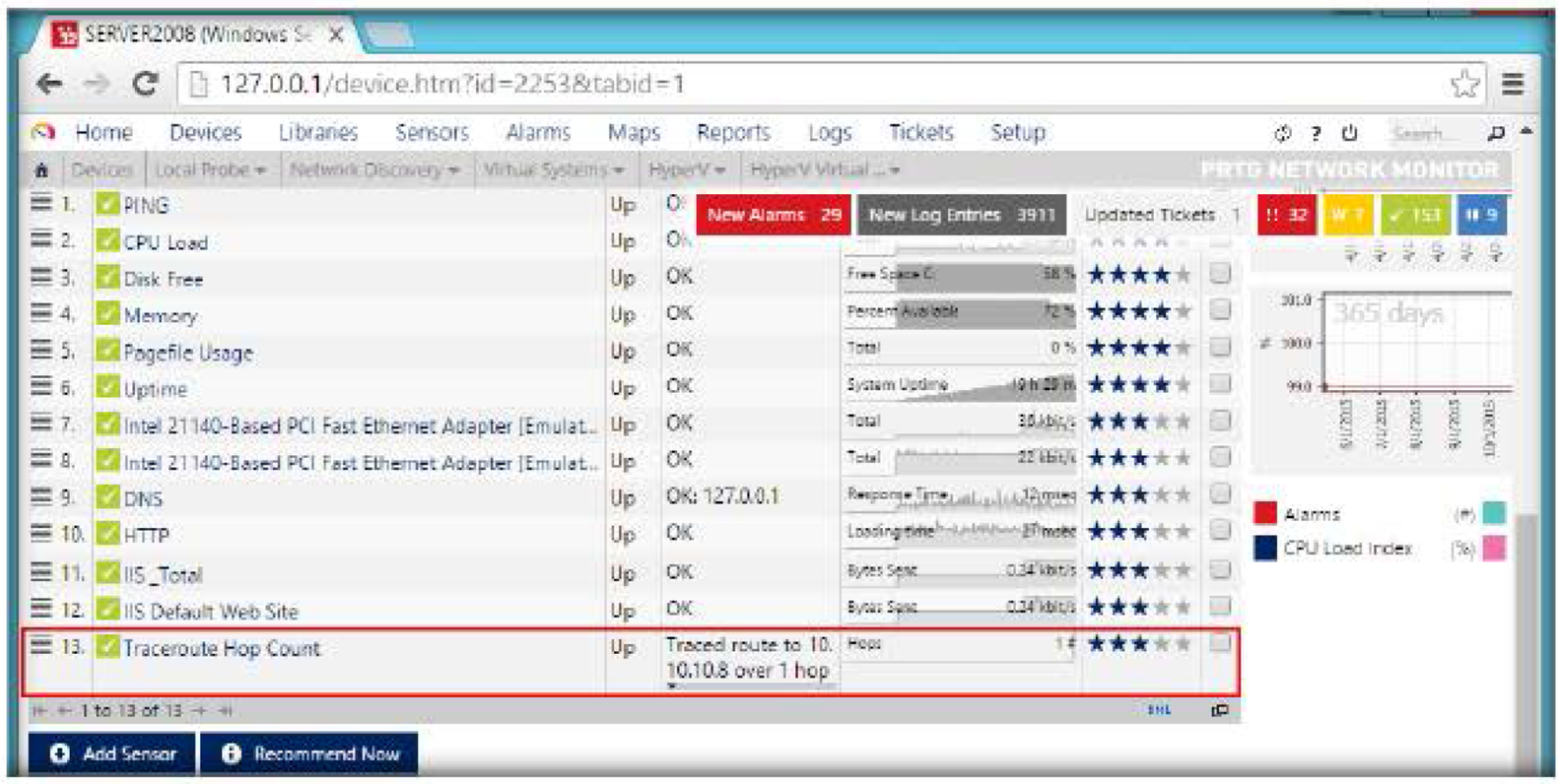



FIGURE 5.39: New Sensor Traceroute Shown Up Against its Device

73. Now, we explore the sensor colors. A sensor can either be red, yellow, green, blue or orange depending on its state. All these can be found at the top right corner of the browser



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

74. A red color indicates the sensor is in an error state, yellow indicates a warning state, green indicates the sensor is working fine, blue indicates the sensor is paused and it is not monitoring

75. The orange indicates an unusual value, the one whose statistical values are not usual but cannot yet be deemed as a warning or error, but might or might not be in the future




FIGURE 5.40: Sensor State Reflected in Colors

**Note:** The status of the sensors might vary in your lab environment

76. Now once we have set up the sensors we need to configure them with **upper and lower threshold values** and when the sensor reads any value not in the range of the specified threshold an alarm is triggered.


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

77. For setting the threshold value we need to specify a **parameter (channel)** for a sensor (here, **Traceroute Hop Count**) for which the threshold is being defined. To set up values in the **Traceroute Hop Count** sensor, click on the sensor and click anywhere on the elliptical path (click on highlighted area).

The Traceroute Hop Count sensor traces the number of hops needed from the probe system the sensor is running on to the IP Address/DNS Name defined in the sensor's parent device.

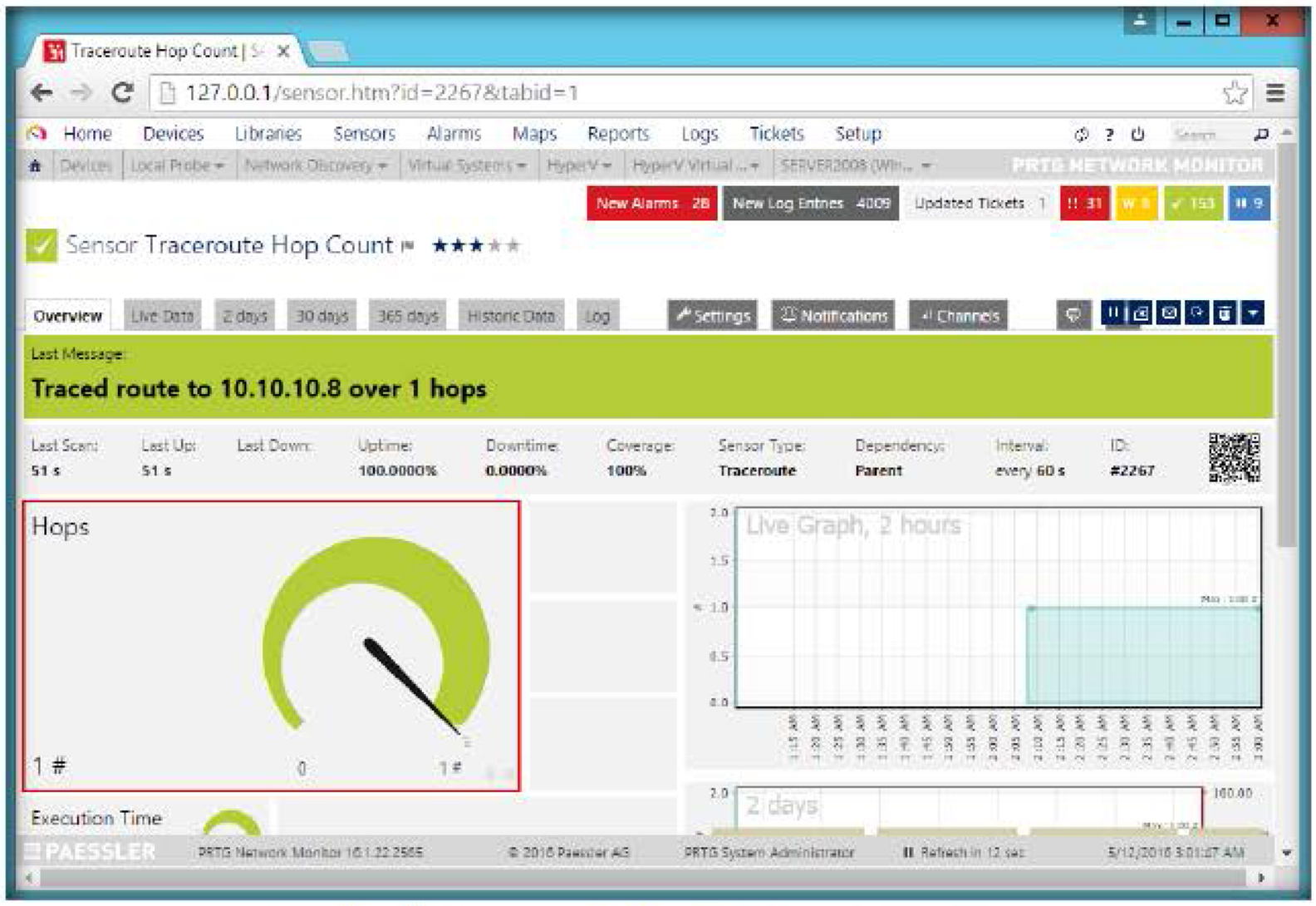



FIGURE 5.41: Area to be Clicked to Enter the Threshold Settings of Sensor

78. You can **select a channel** from the available list of channels at the top section. In this lab, we will be selecting the **number of hops** as our **channel** for the sensor **Traceroute**. Now go to the bottom section called **limits** and click on enable limits

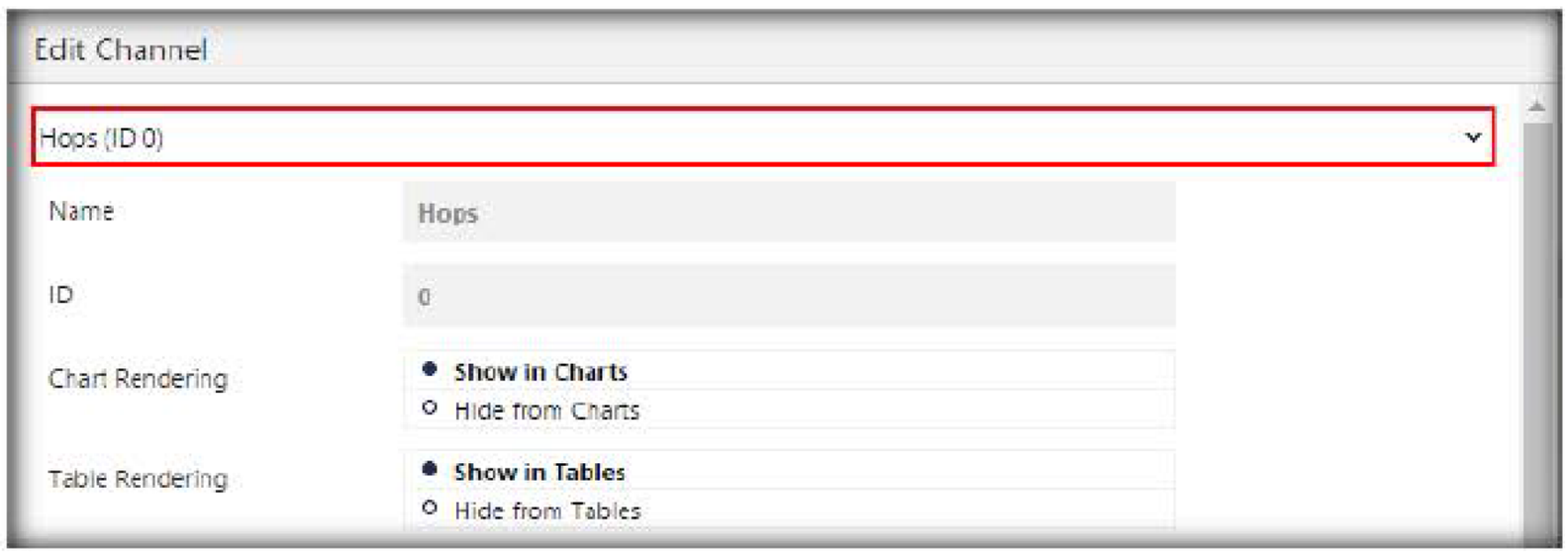



FIGURE 5.42: Selecting a Channel to Set Threshold Values

79. We have selected the **number of hops** as our **channel** for the sensor **Traceroute**. Now go to the bottom section called **limits** and click on enable limits

Note: **Hop count** defines **number of devices** that a packet has to pass to reach its destination, less the number of hops quicker the web page is loaded and more hops the slower the web page is loaded


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

80. So we will set out an upper error limit when maximum hop exceeds **25** and an upper warning limit when it exceeds **20**. We are not concerned about the lower level of the threshold, since a smaller number of hops the quicker the webpage is loaded. So we keep **lower values blank**. We can also write custom error messages for both error state and warning state. So, write some random Error Limit Message and Warning Limit Message. Once done, click **Apply** and then, click **OK**.

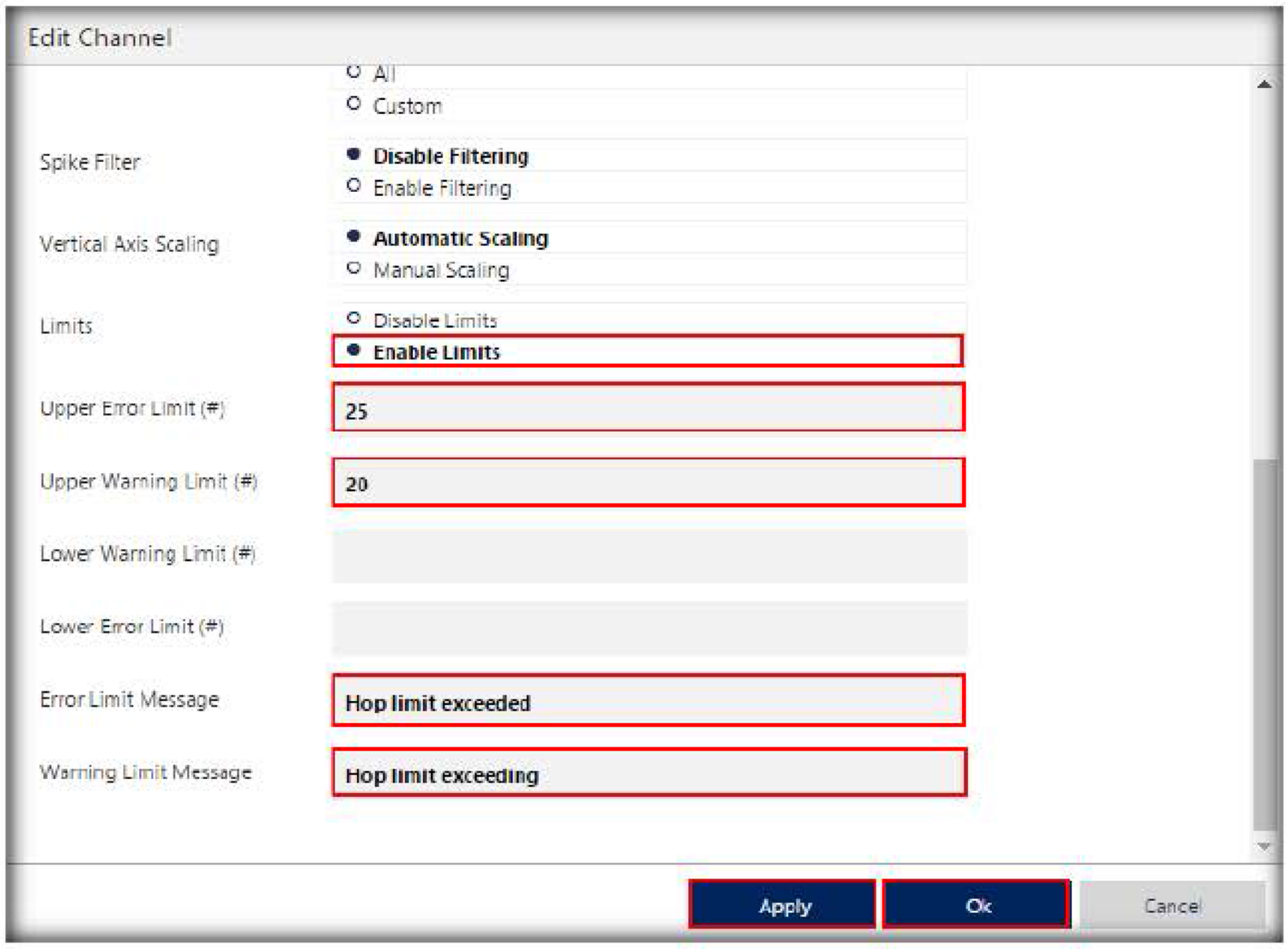



FIGURE 5.43: Setting the Threshold Values of Traceroute Sensor


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

81. Now you can see the ellipse in three different colors for **Warning (yellow), Error (red)** and **Good (green)**. You can also know the status of the sensor by looking at the position of the arrow if it is in a green, red or yellow zone.

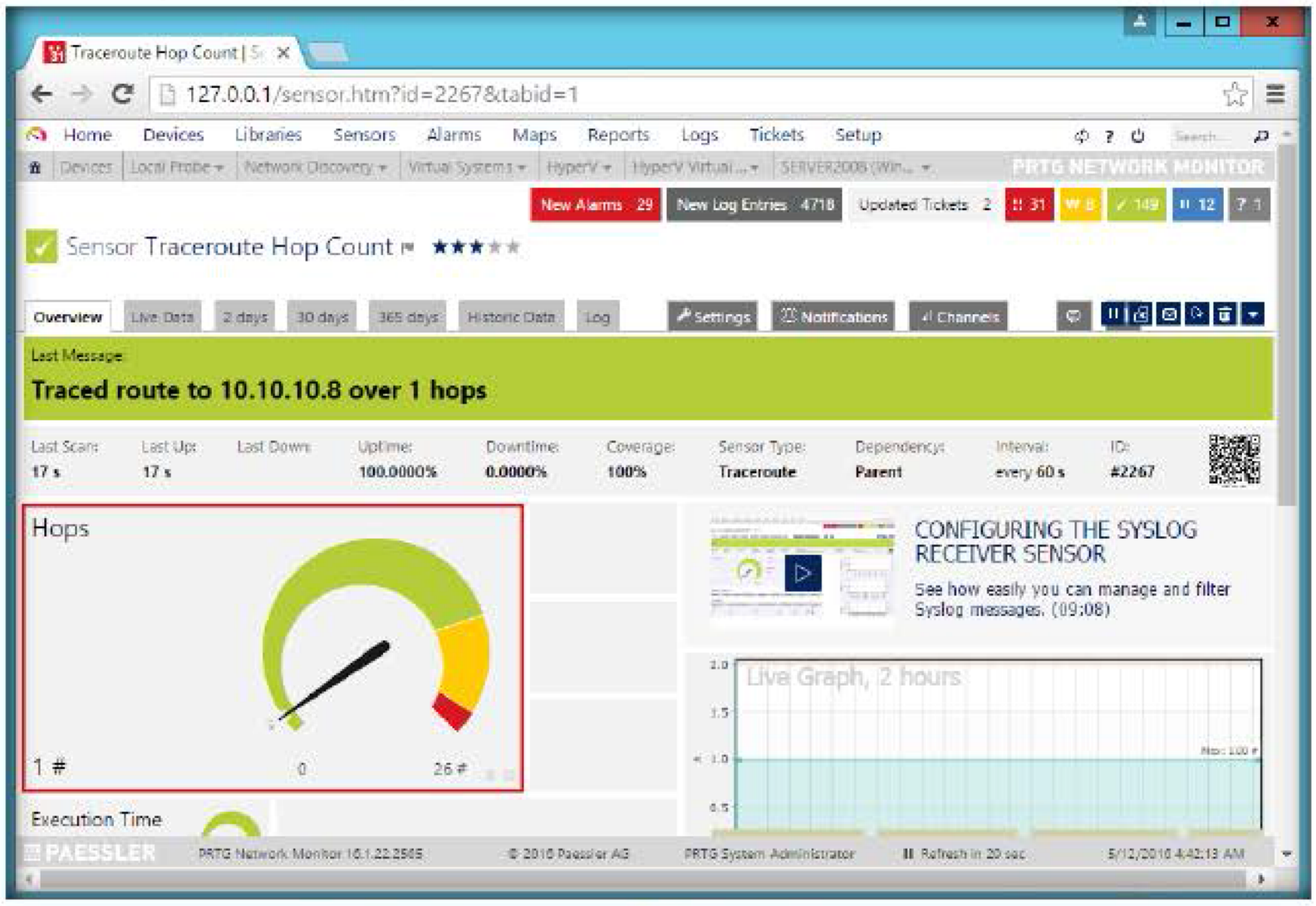



FIGURE 5.44: Analyzing the Health Status of the Traceroute Sensor

82. Now we look at how to analyze the **previous data** of a sensor. The value which we saw was an **overview**. To know the details of a sensor at this moment, click on **live data**, if you want to view the previous data you have the option of **2 days, 30 days and 365 days**.




FIGURE 5.45: Analyzing Previous Data of Traceroute Sensor



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

**Note**: You can also get customized historic data of a sensor by configuring the historic data tab. To configure, click **Historic Data** tab in the webpage.

83. Now, we shall perform **bandwidth monitoring**. PRTG has already built sensors for this task. We need to only add them to the device and configure them to start the monitoring process. Let's see how the **network sniffer** works.
84. We first use the Network sniffer sensor. It can be used in **three** ways:
    a. To sniff the traffic of an entire network
    b. To create a disk mirror and switch PRTG to this mirror and connect to sniff all of the data
    c. If you have multiple switches you can use additional hardware and integrate them and get all the switch data to PRTG
85. We will use the first option, and monitor an entire network using the network sniffer sensor.
86. Select the Devices tab on the webpage. When a list of devices appears on the webpage, right-click on **Probe Device** under **Local Probe** section and select **Add Sensor...** from the **Device Menu**.

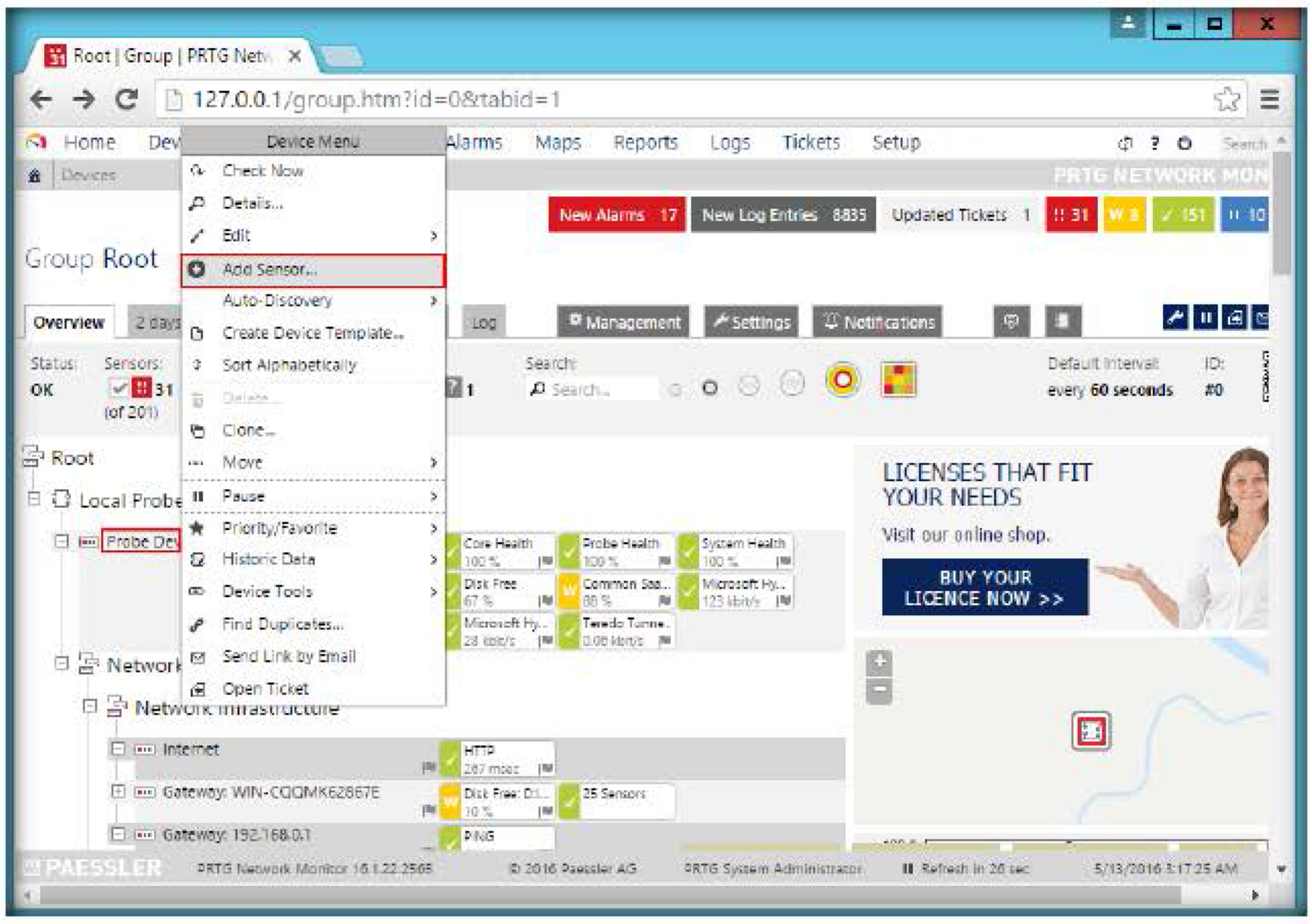



FIGURE 5.46: Adding a Packet Sniffer Sensor to Local Probe Device


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

87. Now from the sensor list page, enter **packet sniffer** in the search tab. The matching sensors appear in the lower section of the page. Select **Packet Sniffer** from the list of results. Notice that there is also a custom packet sensor next to packet sniffer. We will discuss this in further steps.

The Packet Sniffer sensor monitors the headers of data packets that pass a local network card using built-in packet sniffer. You can choose from predefined channels. The sensor analyzes only header traffic.

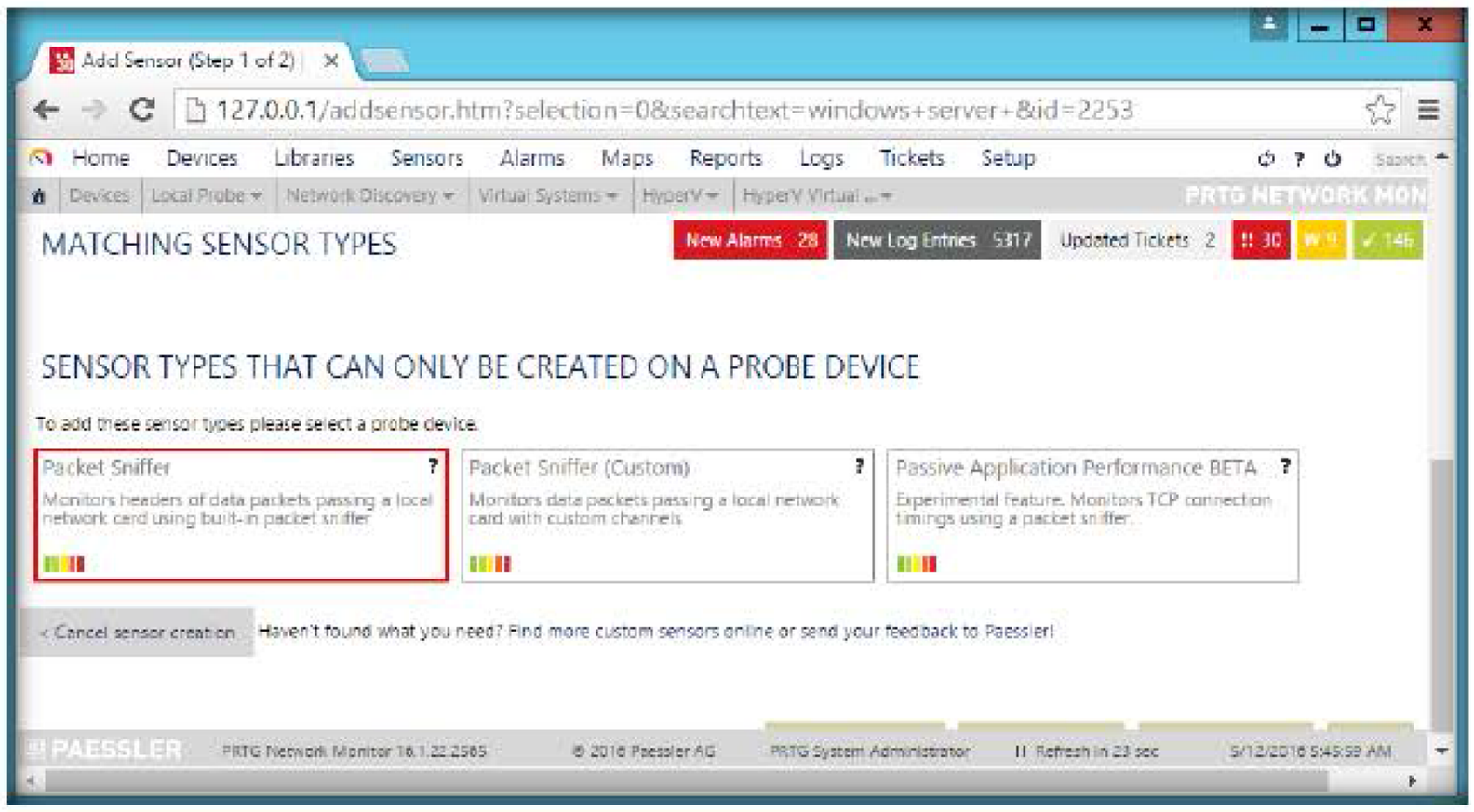



FIGURE 5.47: Adding the Packet Sniffer Sensor to Local Probe Device

88. Now in the next page, enter a custom name, tags and priority levels for the sensor. Next is what filters to include and exclude. An **Include filter** lets you to customize the traffic that enters the sensor. You can use various filters to either get packets from one particular IP or a particular port and so on.

89. If you do not want to get packets from any port or IP or MAC, just mention it in the **Exclude Filter** list. For now, we keep both these fields blank, so that we get the complete network traffic.

90. The network adapter has the IP address from where PRTG sniffs the traffic. The log stream allows you to define what data is written to the disk. If you select **None** no additional log files will be written, **only for the other channel** option writes log files of only the data which is not filtered and **all stream data** writes log files for all data received.


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

91. In this lab, choose the network adapter that is associated with the **10.10.10.*** network and click **Continue**.

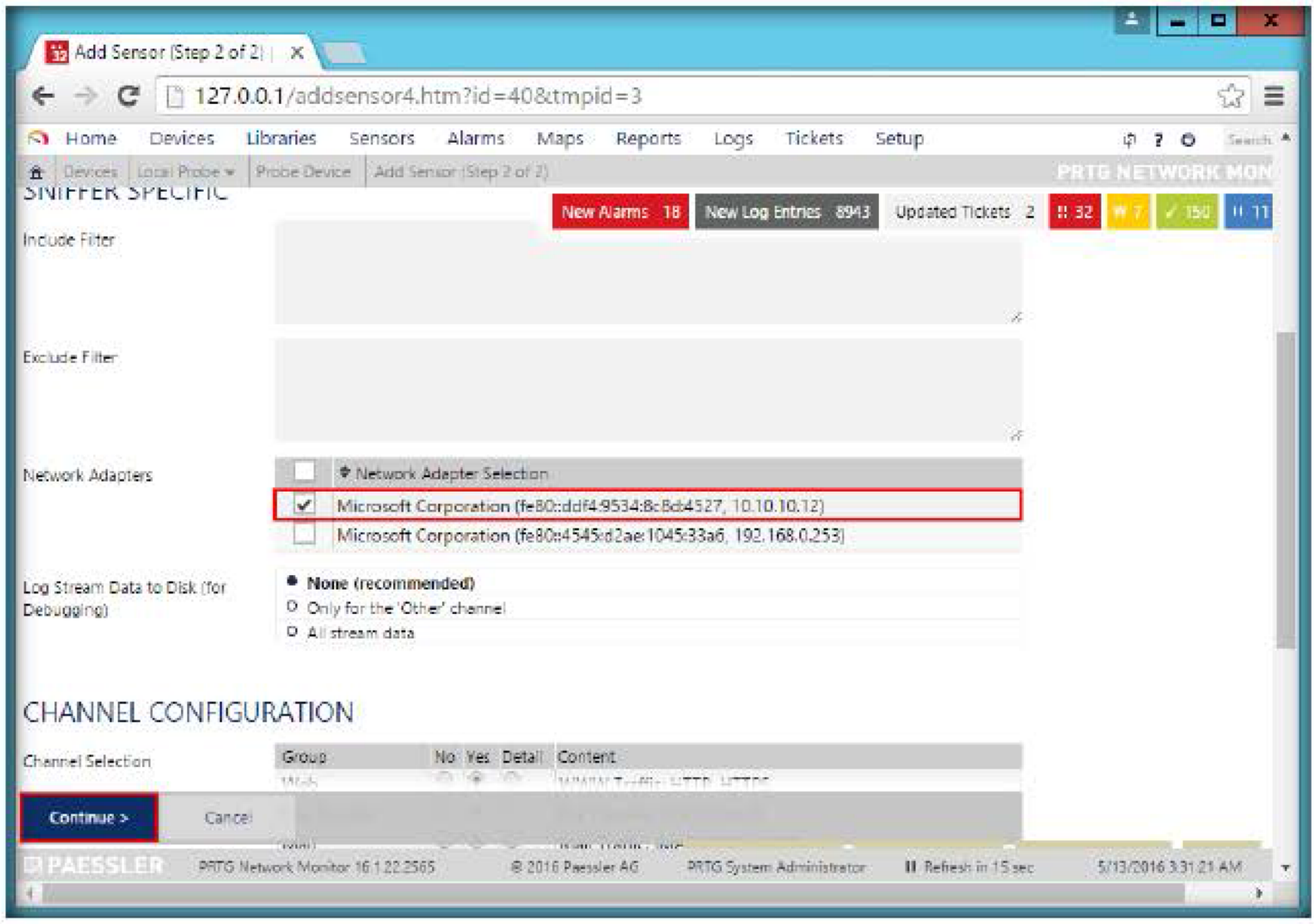



FIGURE 5.48: Setting Up the Packet Sniffer Sensor

92. Now go to the **Devices** section, wait until the state of the **Packet Sniffer** sensor under the **Probe Device** section turns green. If the state of the sensor does not turn green and running, right-click on it and select **Check Now** under **Sensor Menu**.

93. Once the sensor is up and running, click on it

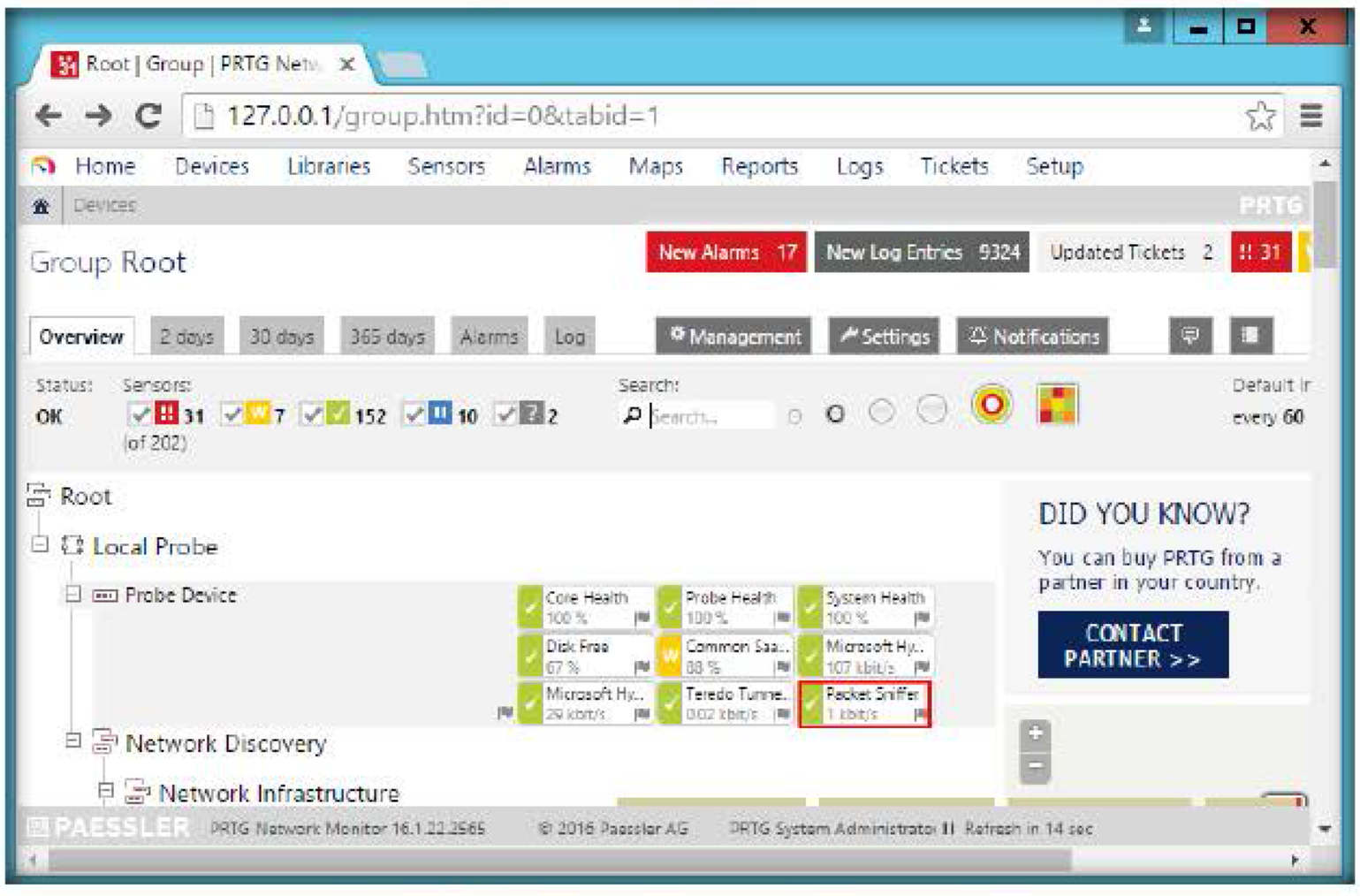



FIGURE 5.49: Packet Sniffer Sensor in SENSORS LIST



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

94. When you click on the sensor it opens up showing the various parameters. (It might be grey for you initially after immediate creation.)

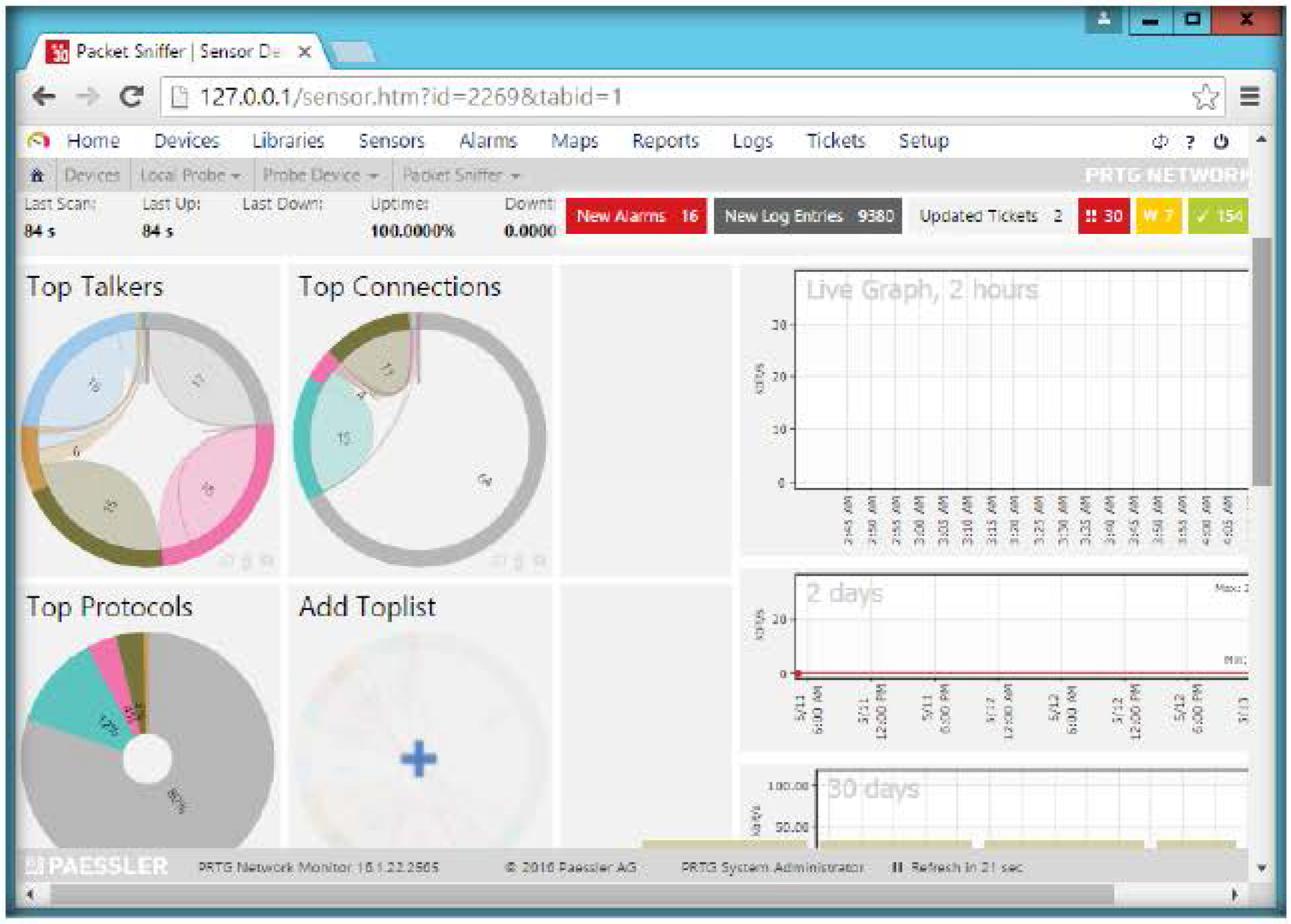



FIGURE 5.50: Various Parameters of the Packet Sniffer Sensor

95. If you scroll the webpage down, you will see the total aggregated traffic on the left side in the **Total** section and individual traffic in **small eclipses** on the right side with names like Infrastructure, WWW, NetBIOS and so on.

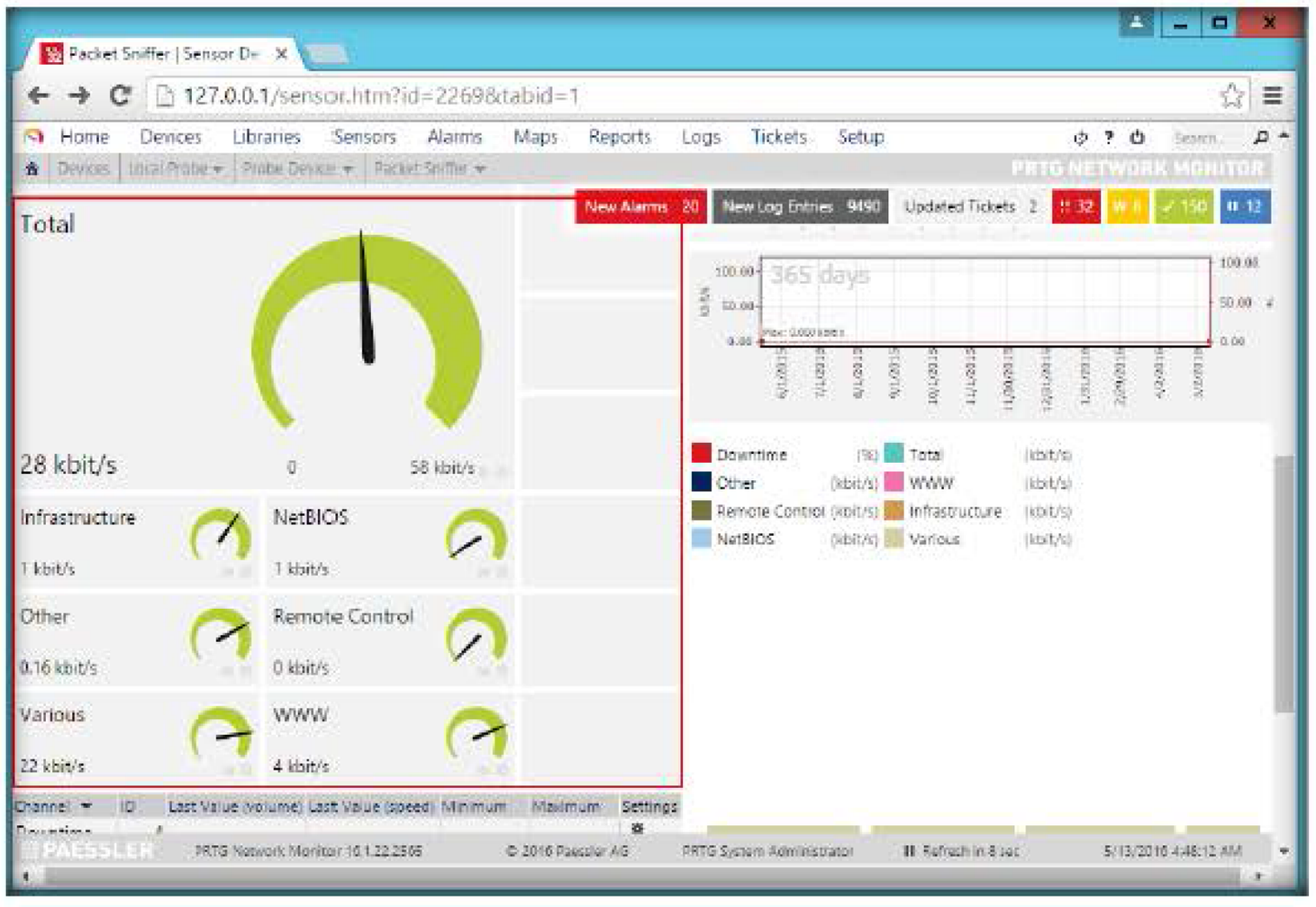



FIGURE 5.51: Various Parameters of the Packet Sniffer Sensor



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

96. Scroll the webpage up and click the **Top Talkers** link. This section shows which device IP's caused maximum traffic in the network.

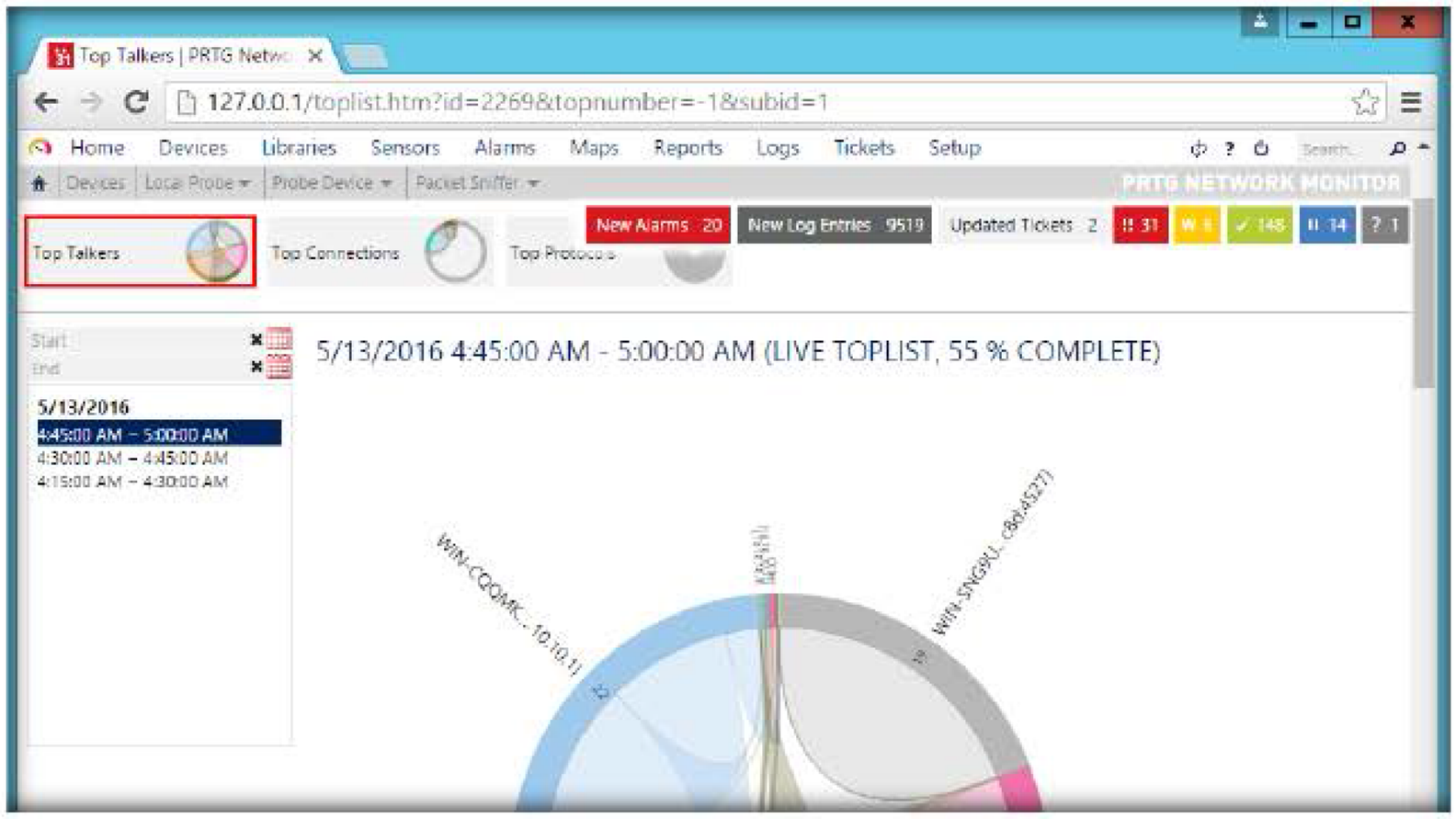



FIGURE 5.52: The Top Talkers Graph Expanded

97. In the same way, you may analyze the **Top connections** and **Top Protocols**. The Top Connections section displays the connections which are using most of the bandwidth and the **Top Protocols** section shows which protocols use the most bandwidth. Click on any one to expand them.

98. After expanding any graph if you scroll down you get a detailed view of all source and destination IP's. You can also create a new top list with your custom IP protocols etc. by using the **Add Toplist** option.

99. You can also view the live data for the past two hours by clicking on the graph at the right or on the Live data tab.

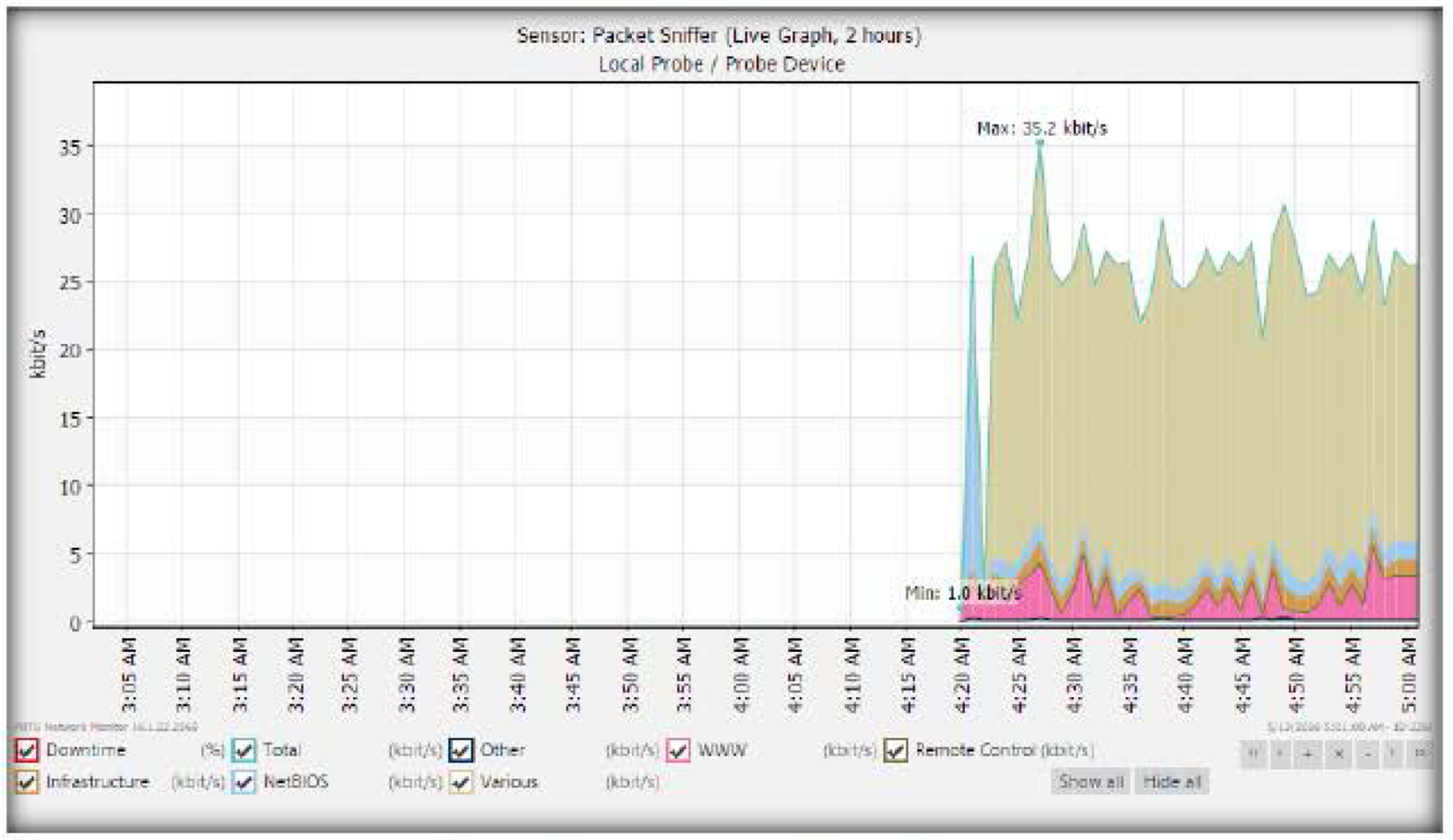



FIGURE 5.53: Live Network Traffic Data



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

100. We now see how to setup **Maps** in a PRTG. A Map is a graphical representation of a network structure. Hover the mouse cursor on the Maps tab and click **Add maps**.

With PRTG's Maps feature (some people might call this 'dashboards') you can create web pages with up-to-the-minute monitoring status information in a customizable layout. Using this unique concept, you can also make your overview pages of live data publicly available, if you like.

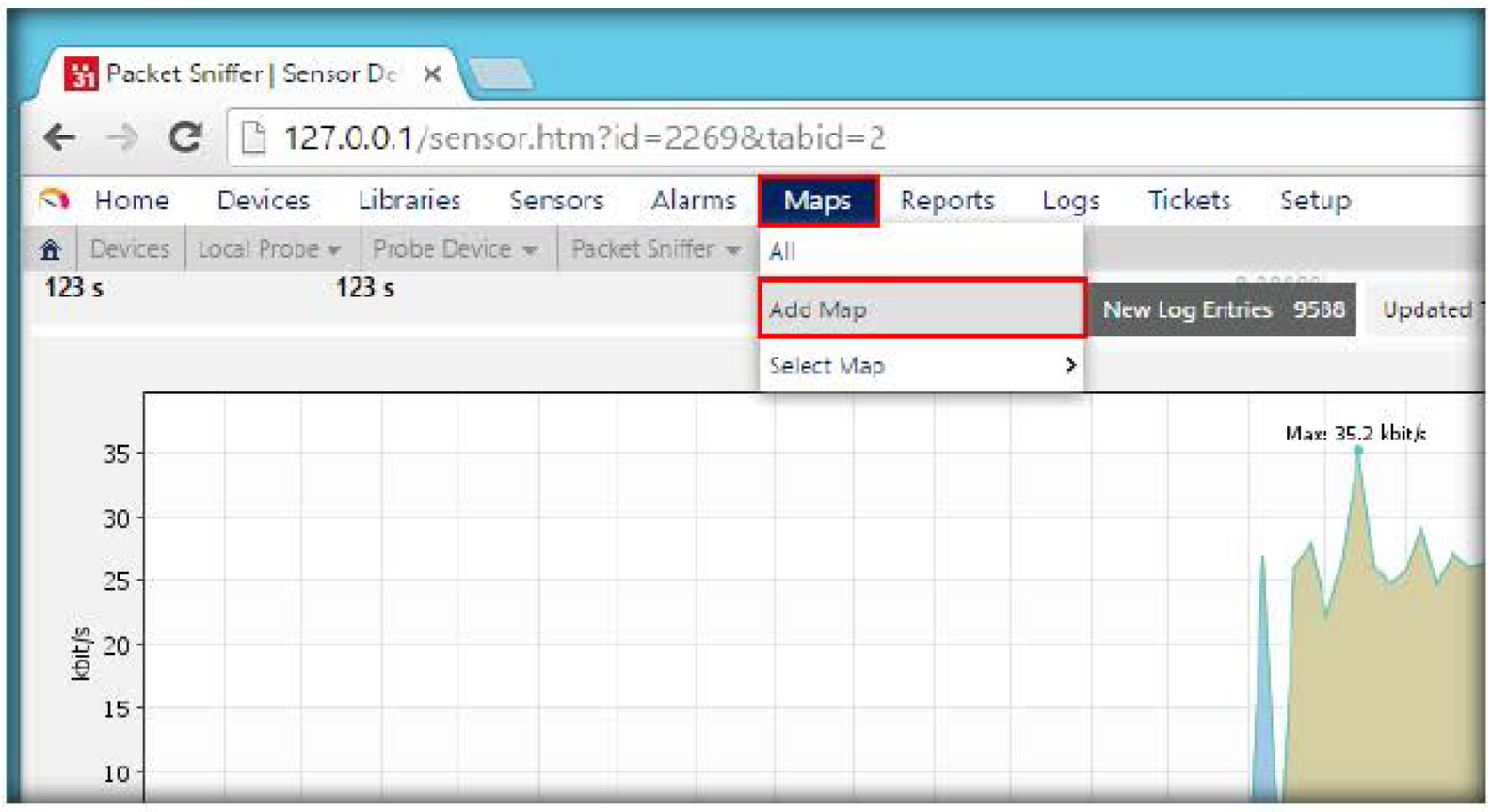



FIGURE 5.54: Navigating to the Map Section

101. Enter the values for map name, its layout dimensions, an optional background image and whether you want the map to be publicly accessed or specifically accessed only by authentication. In this lab, all the default options are chosen. Click on **Continue**.

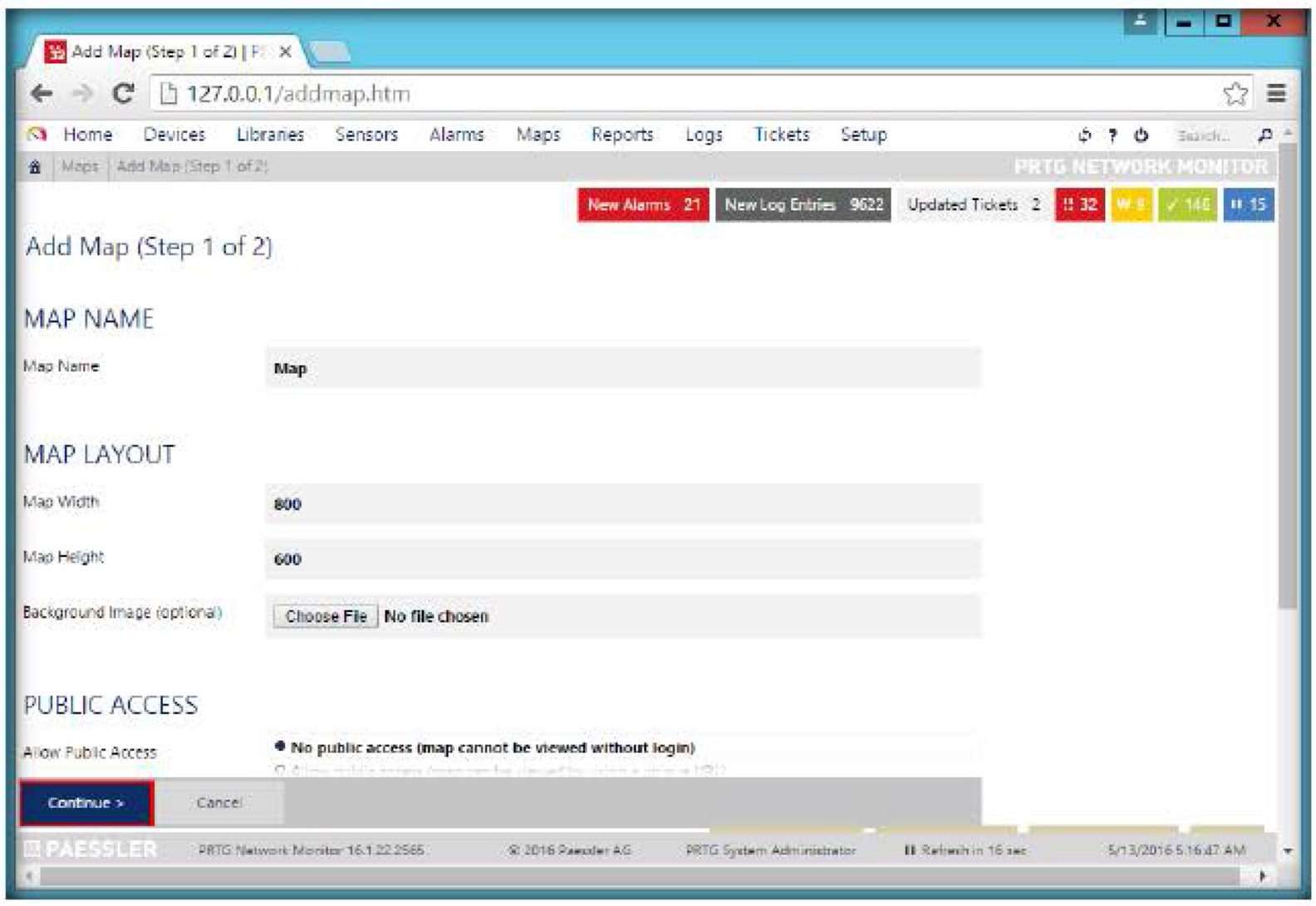



FIGURE 5.55: Configuring a Map



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

102. On the results page, you can drag and drop items from the left pane or the right pane into the center pane.

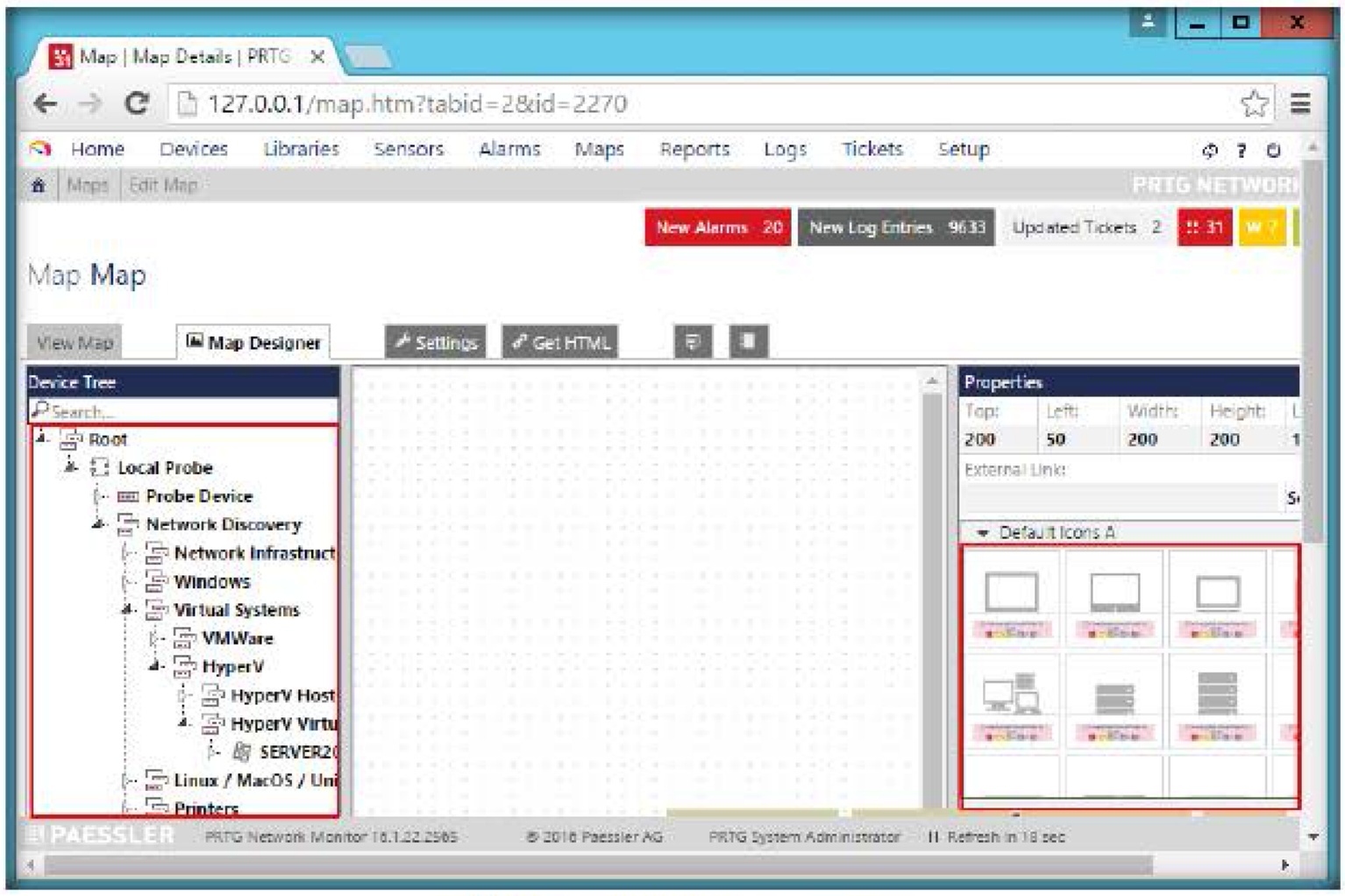



FIGURE 5.56: Various Parts of the Map

103. Now as soon as we drag and drop an item it shows the number of sensors in that device and their respective states.

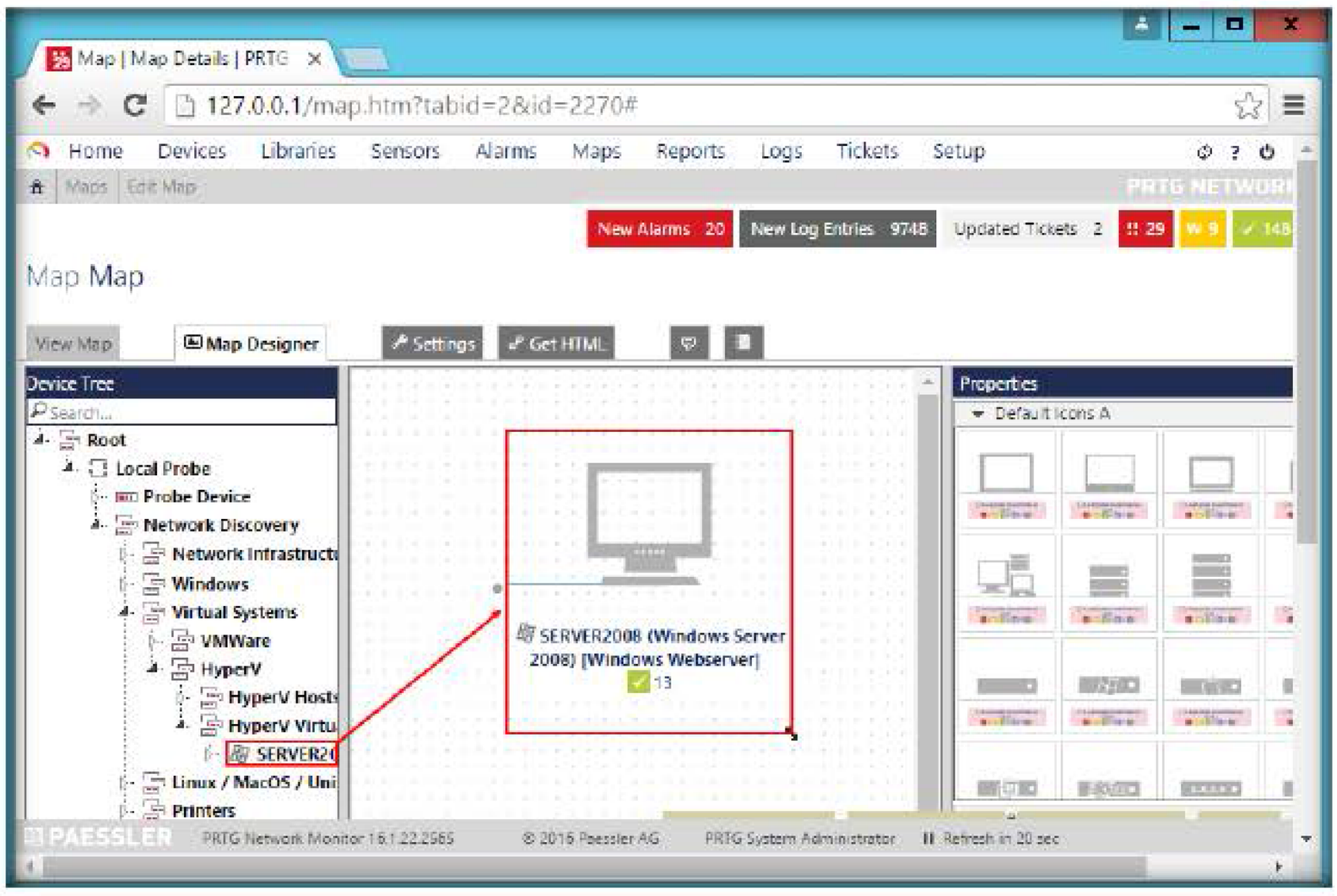



FIGURE 5.57: Windows Device with Sensor States



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

104. In our setup mentioned earlier, we have a host machine which has three virtual machines under it so we added the three virtual machines under the host.

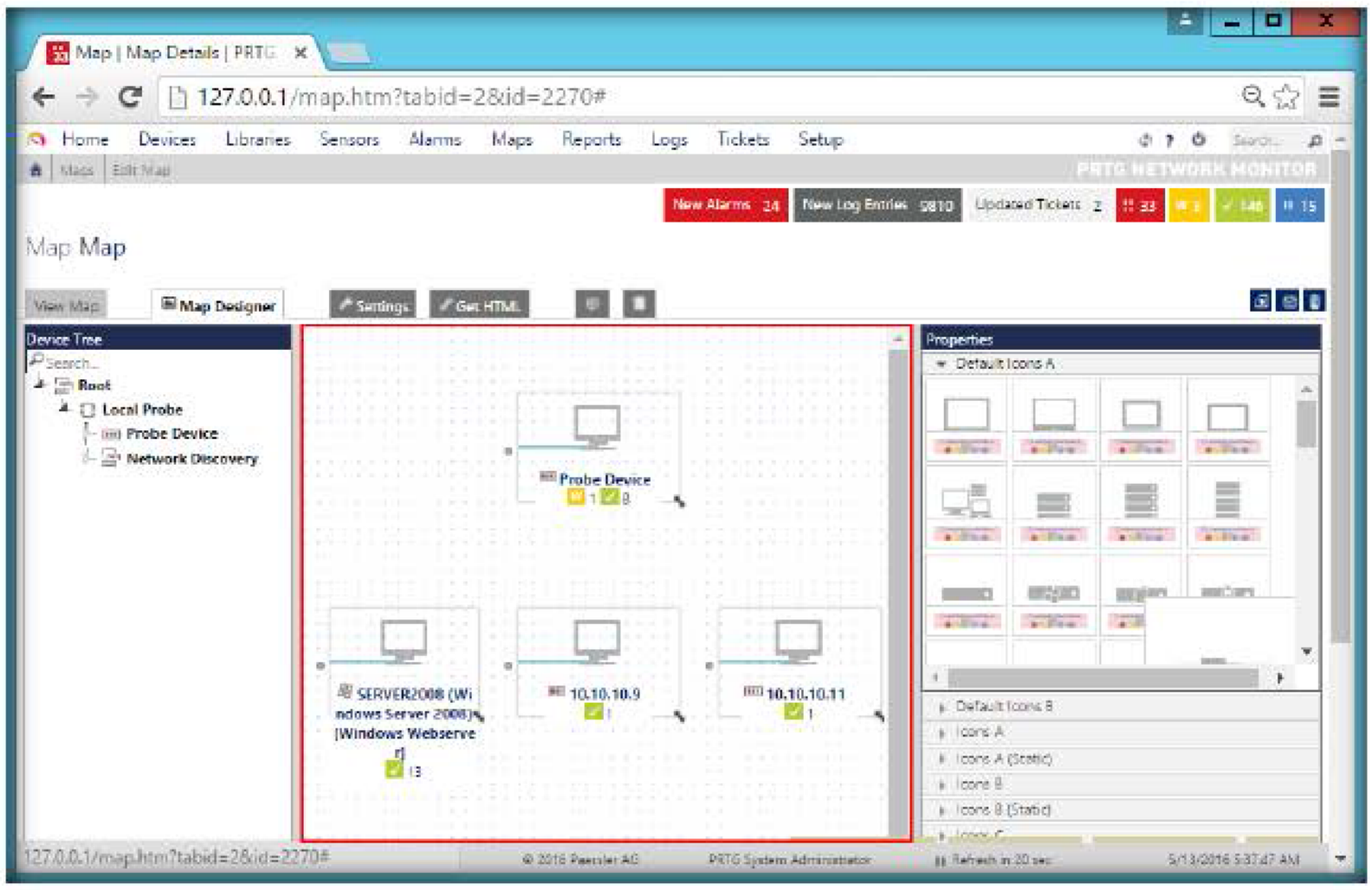



FIGURE 5.58: Creating the Basic Network Structure

105. You can show a connection between devices by interconnecting them. Click on the dot at the left end and drag to the device you want it to connect to.

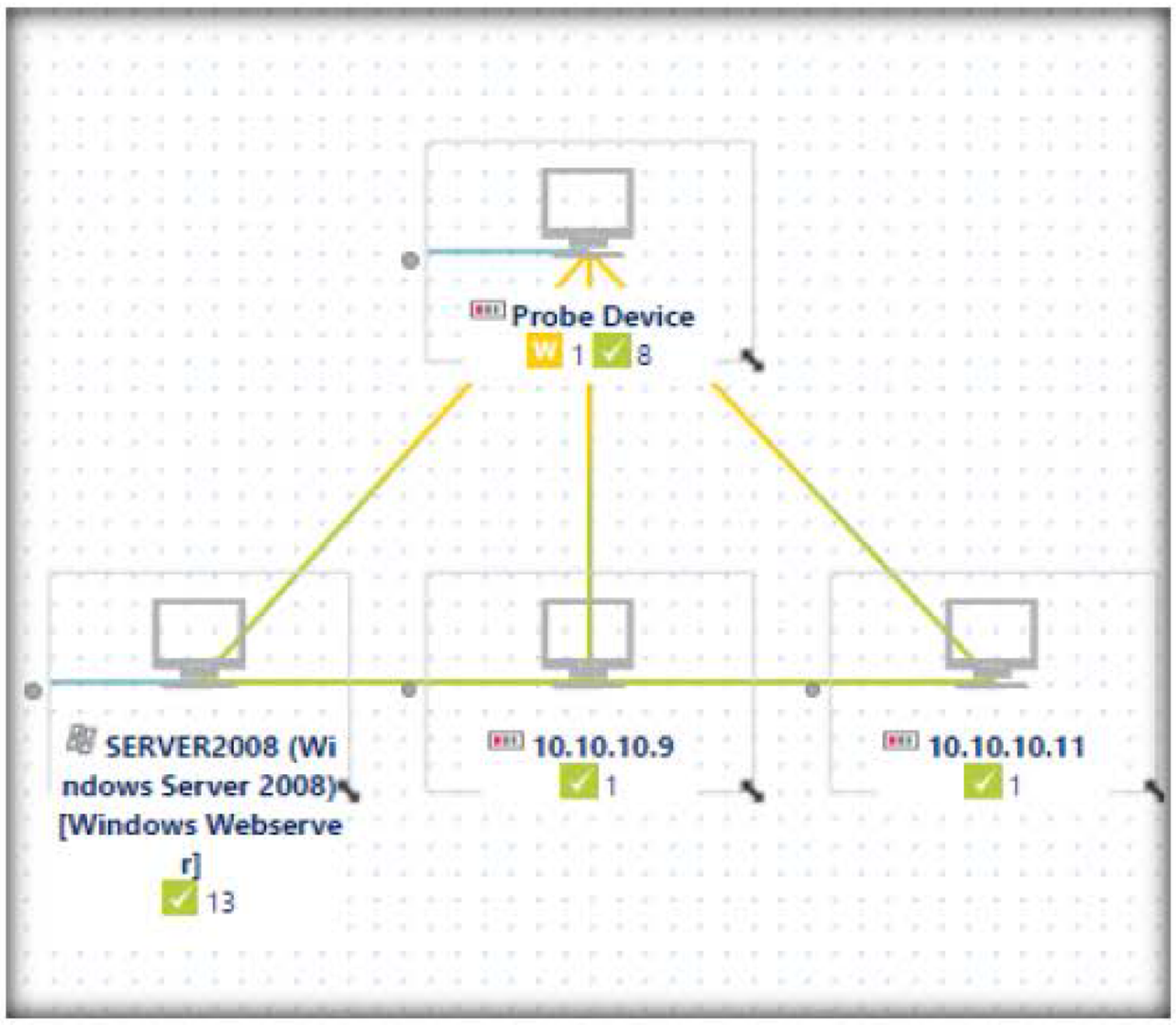



FIGURE 5.59: Map connections Set Up


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

106. To view the map, click the **View Map** tab at the top left corner of the webpage. Once the map is finalized, click Get HTML

107. You have several options for opening the map. You can open it **with or without a login**, by using the respective URL's or you can also show the map as an **Iframe** if you use the third option. Click on the link present under Option 2 to view the map.

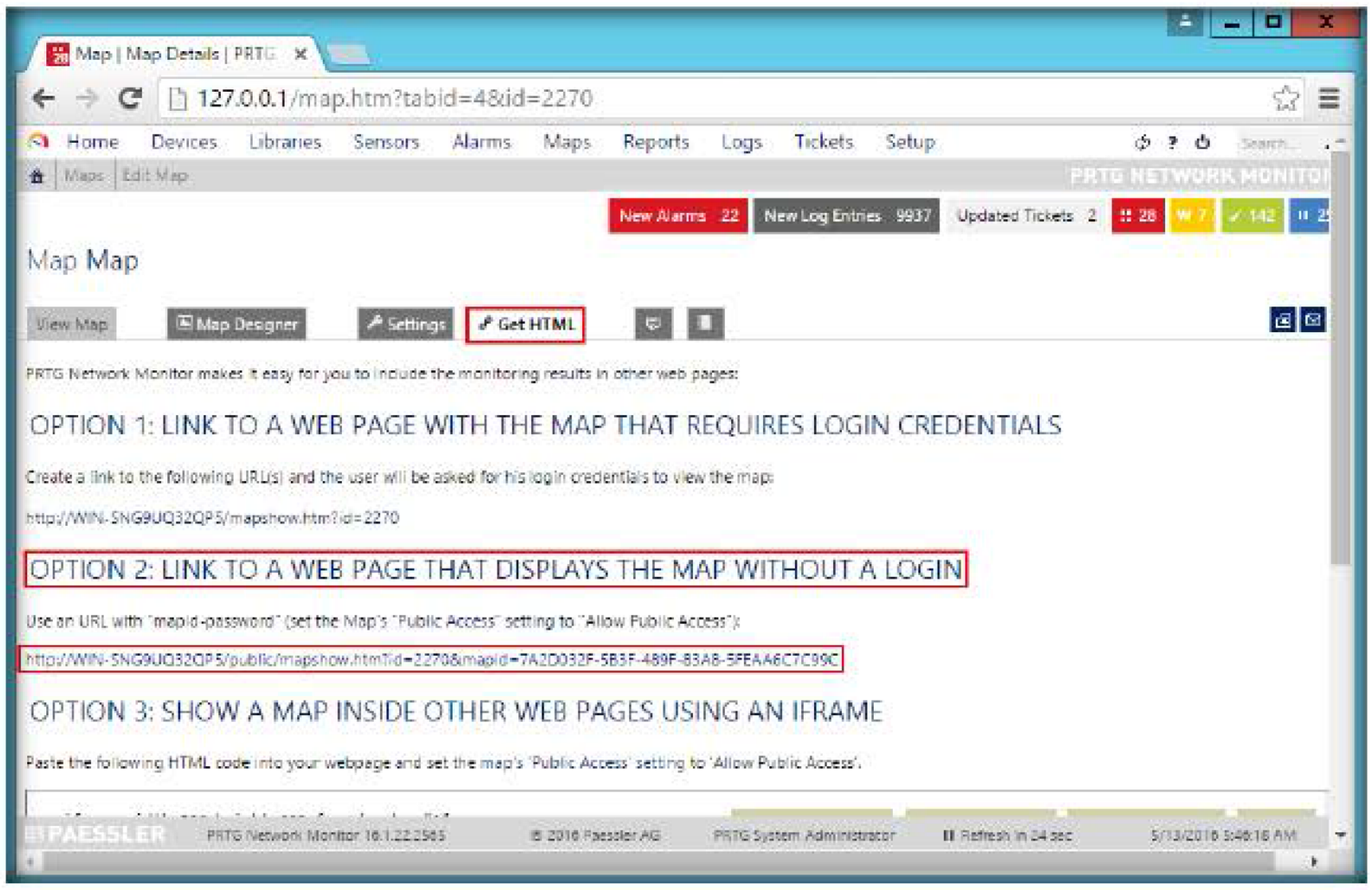



FIGURE 5.60: Map Opened Up in a New Tab

108. The map appears as shown in the following screenshot:

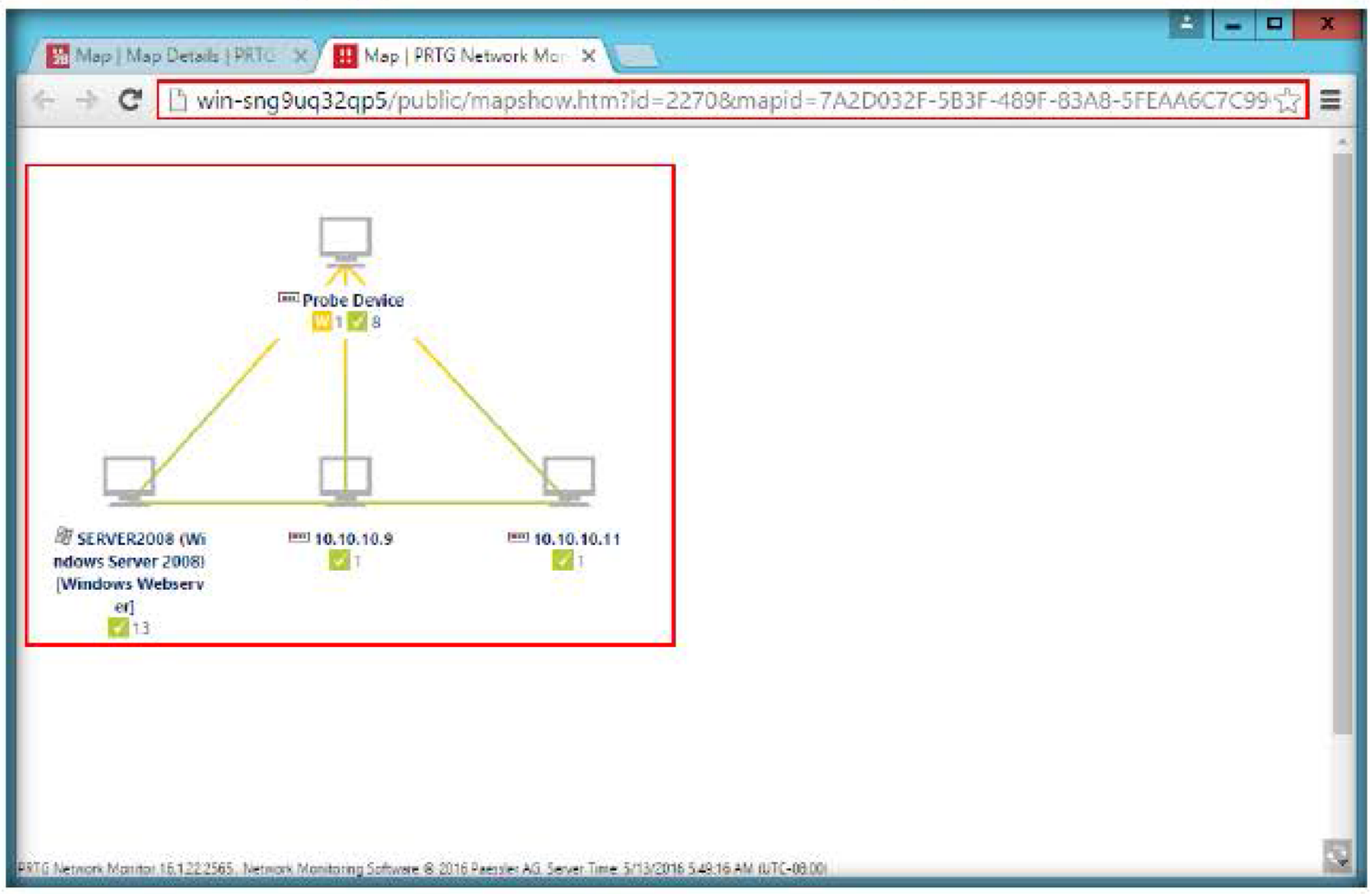



FIGURE 5.61: Map Opened Up in a New Tab


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

109. The **alarm** section. This section shows which sensors that are either in an error state, warning state or an unusual state. Go to the Alarm tab and click on **All**.

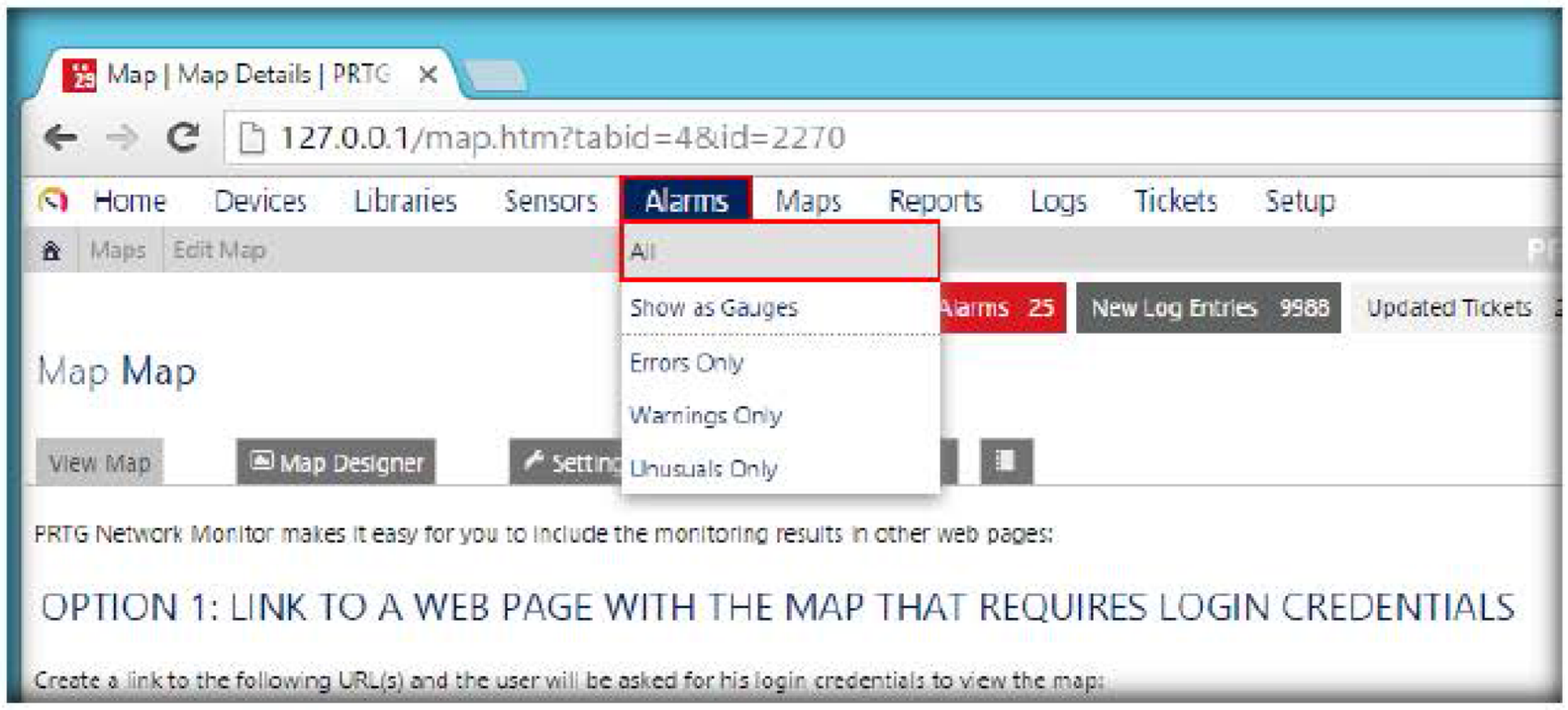



FIGURE 5.62: Navigating to Alarms Section

110. Now you get a list of sensors with their respective states and the devices to which they belong to.

The alarms list shows all sensors that are currently in a Down, Down (Partial), Down (Acknowledged , Warning, or Unusual status. Sensors in other states (for example Up, Paused, or Unknown) do not appear here. This is useful to keep track of all irregularities in your network.

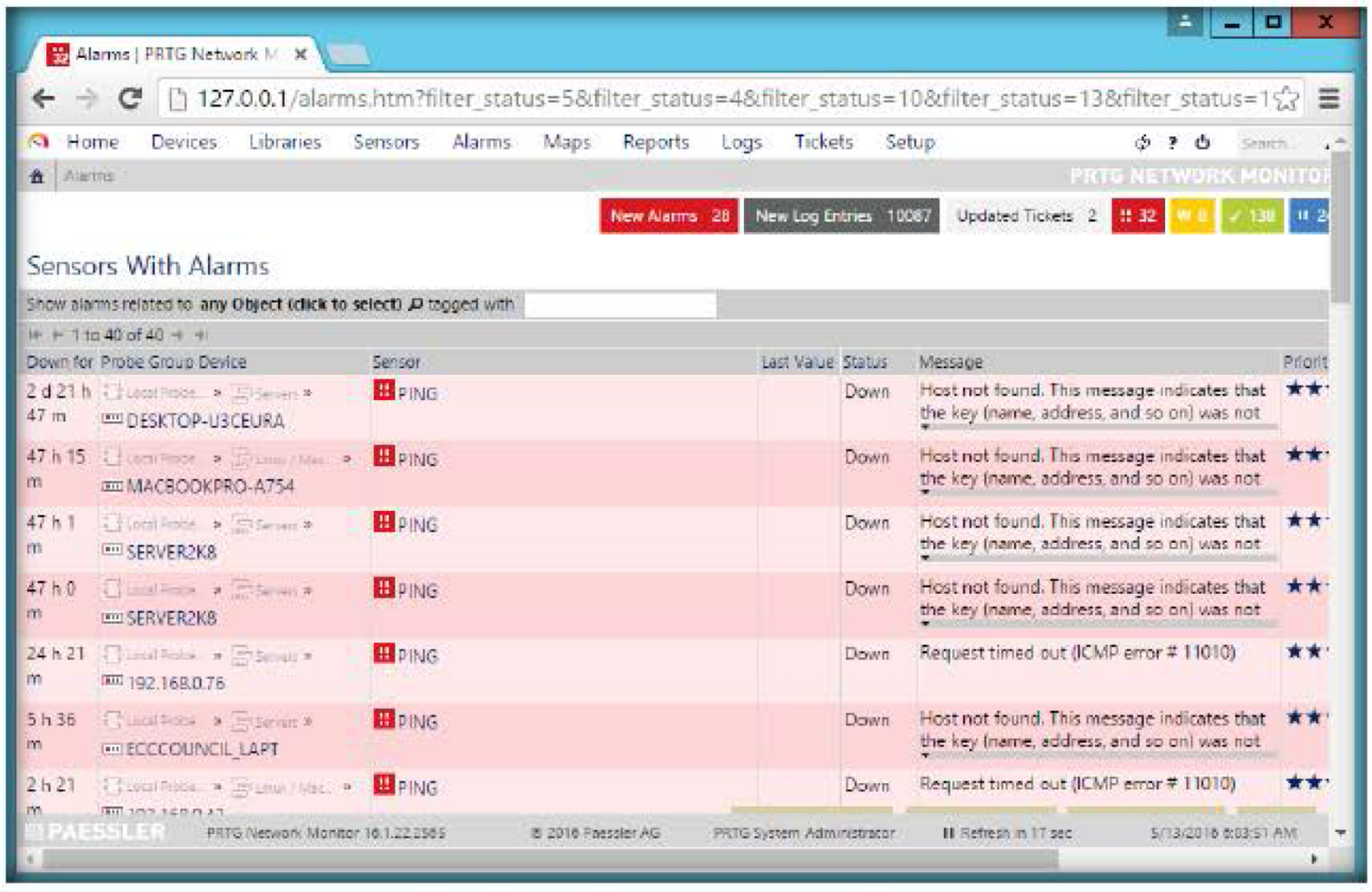



FIGURE 5.63: Sensors Not Functioning Properly

111. You can see what is wrong with the sensor by carefully analyzing the data in the Message section and take necessary action to correct.

112. You can also have a look at the **sensors as a gauge** or view only the sensors that are in an **error state (errors only)** or **warning state (warnings only)** or **unusual state (unusual only)** by clicking on other options under the **Alarms** tab



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

113. Now we shall analyze the Logs section. This section shows all the past activities and events of the PRTG setup. To view logs, hover the mouse cursor on **Logs** and click **All**.

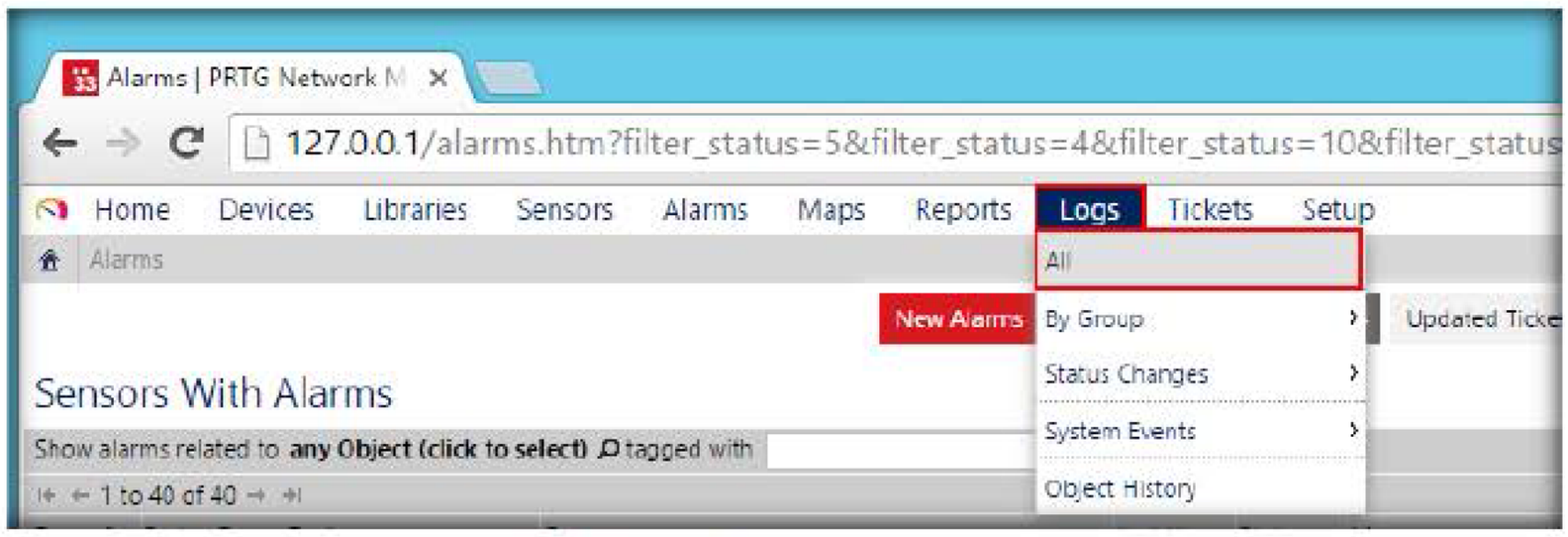



FIGURE 5.64: Navigating to the Log Records

114. This is where you get the complete list of log records. Notice the item in the top right corner which highlighted. This is the **Select Range**.

The Logs list shows all past activities and events of your PRTG monitoring setup. This is useful to research past user activities, system events, and, for example, to check whether messages were sent. In a typical setup, a huge amount of data is produced here. Because the activity of every single object is recorded, you can use this information to check if your setup works exactly as desired.

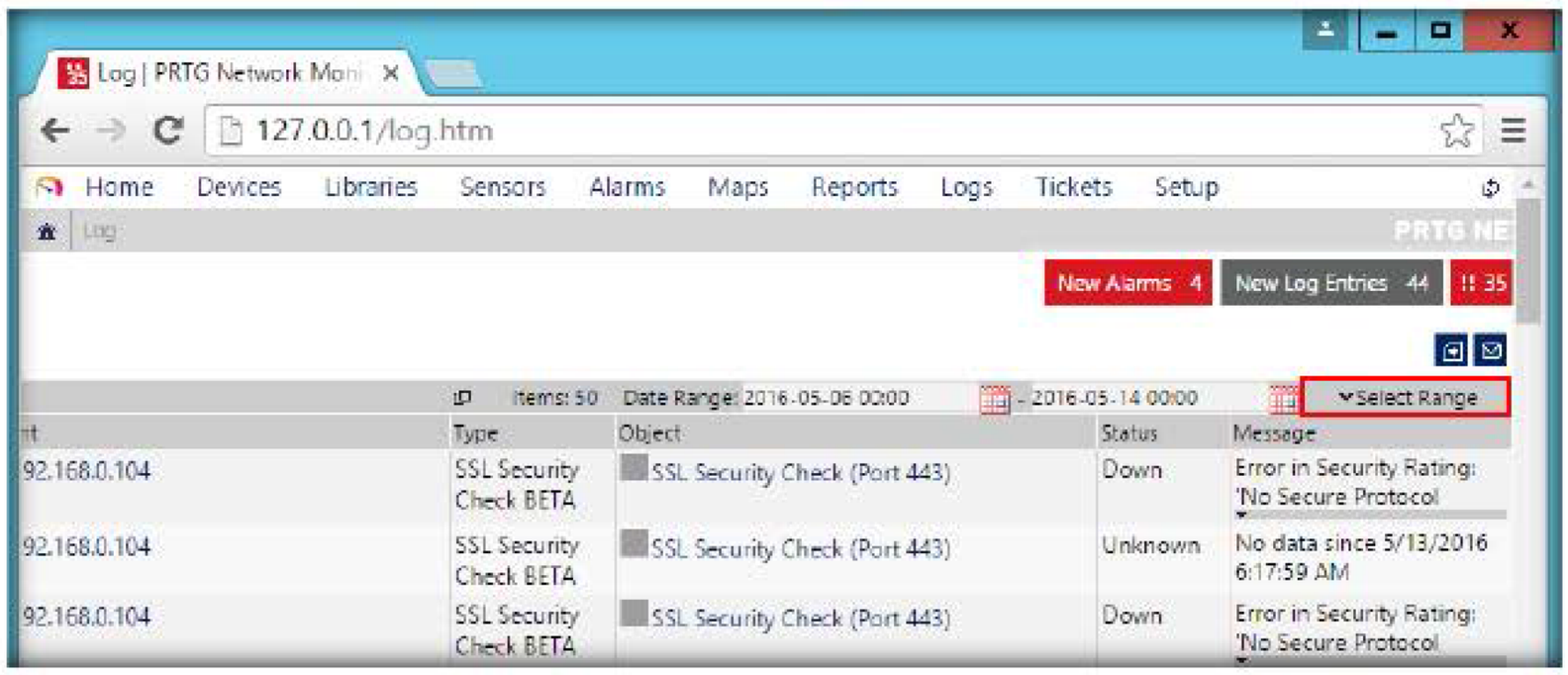



FIGURE 5.65: Log Records

115. Now you can select the range tab and choose how many days of data you want to see. We can select the **Today** option, to show only today's records or any other option for more records. You can also set a **Date Range** between which you want to see the records.

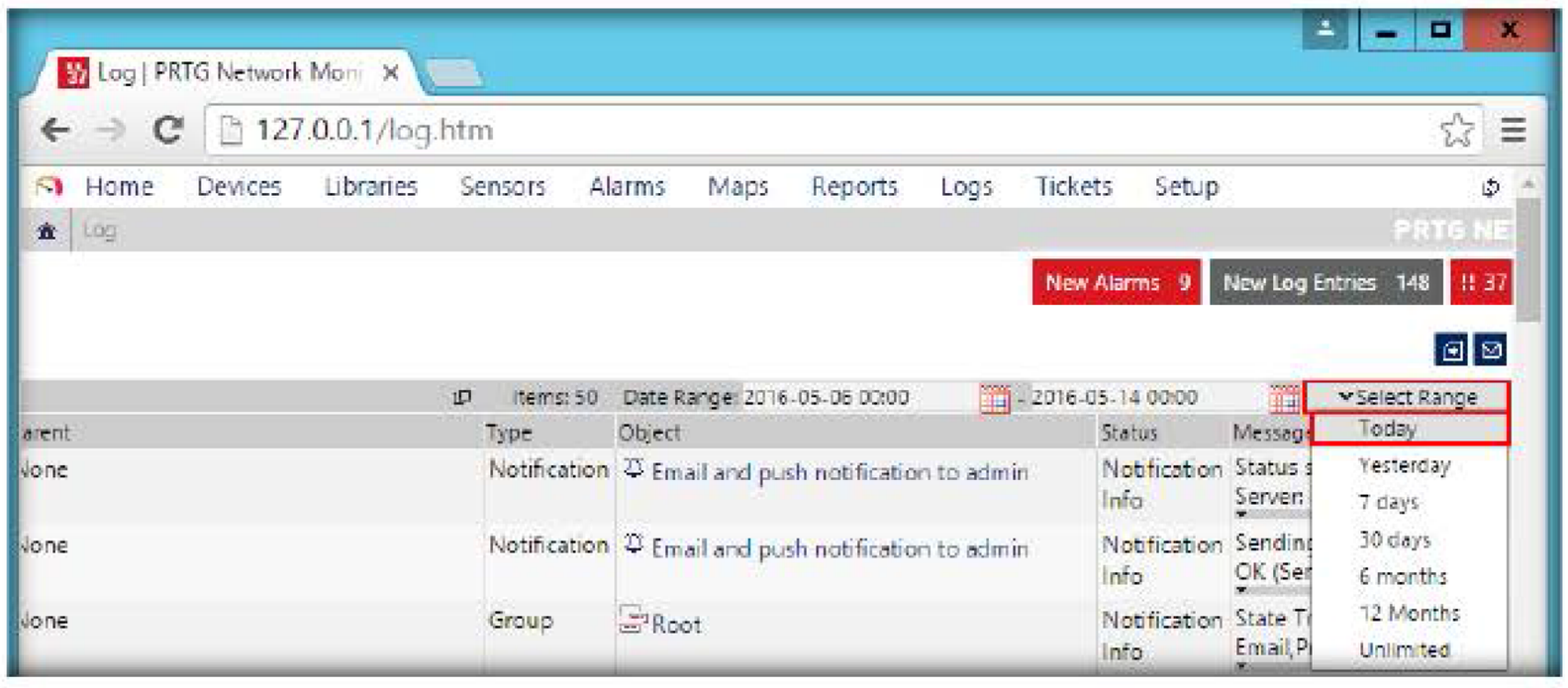



FIGURE 5.66: Selecting Today's Log Records



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

116. If you want to view log records for a **particular system** (windows machine in this case), go the following location as shown below

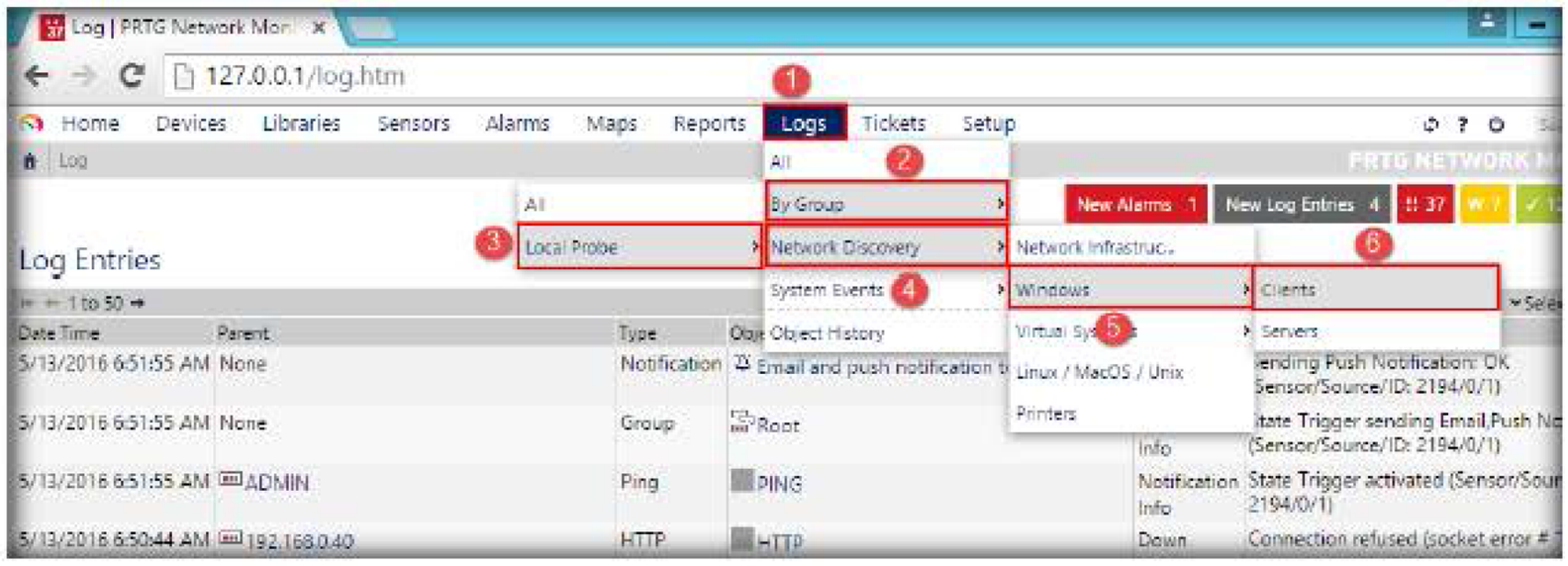



FIGURE 5.67: Filtering the Log with a Particular System

117. The filtered data is shown below. Look at the parent section of the filtered record.

PRTG Network Monitor includes its own ticket system. With tickets you can manage and maintain various issues which may appear while monitoring a network. A ticket in PRTG contains information about recent events in your PRTG installation which need a closer look by the administrator or another responsible person. You can see each ticket as a task for a particular PRTG user.

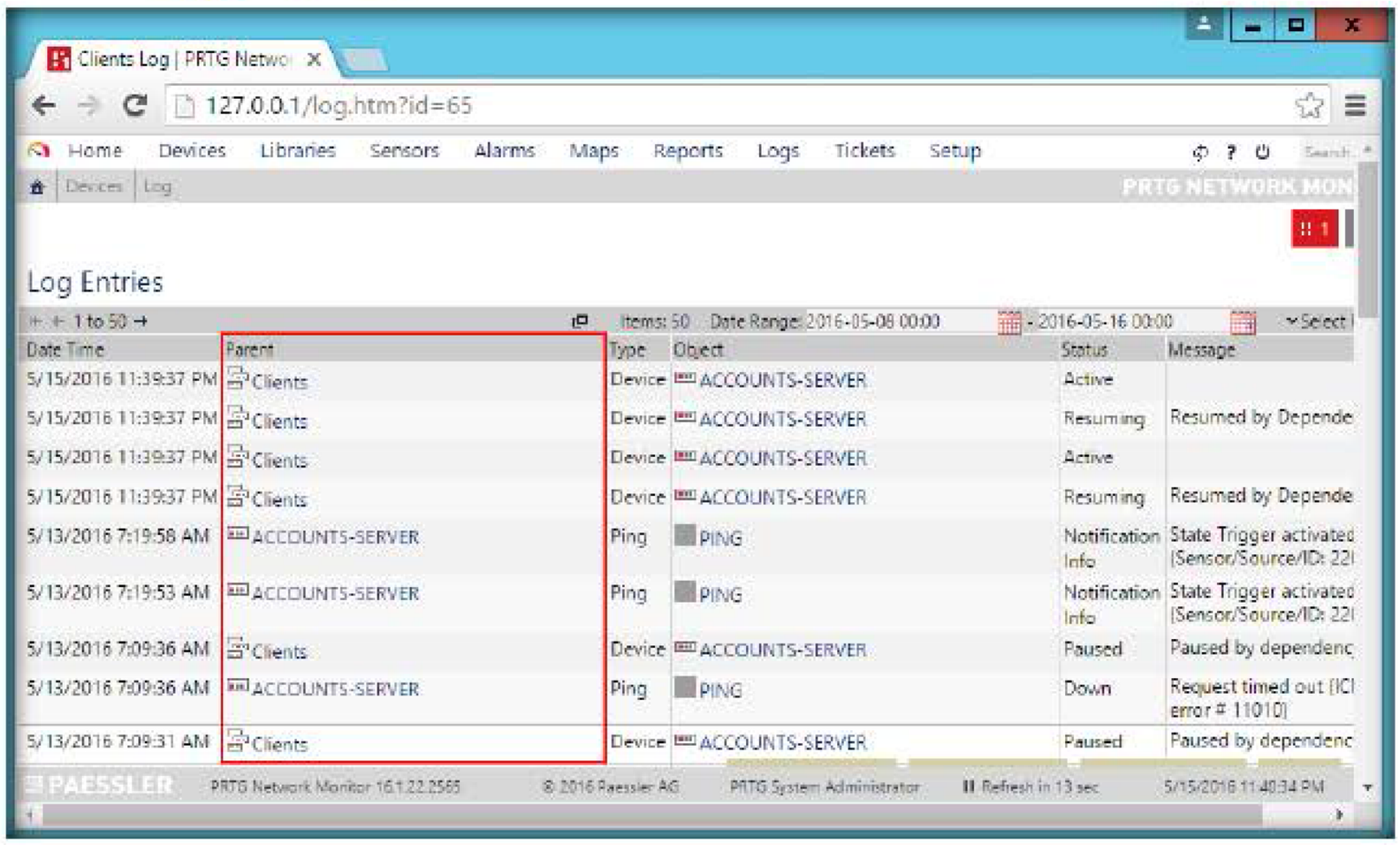



FIGURE 5.68: Log Data Filtered Based On Device

118. You can use other options and filter the log records on various parameters.

119. Next, we will explore the **Ticket** section of PRTG. Tickets contain information about recent activity in the network, on which the administrator has to have a look. It could be a new installation, an addition or deletion or a real issue.



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

120. Hover the mouse cursor on the **Tickets** tab and select **All** to view all the tickets.

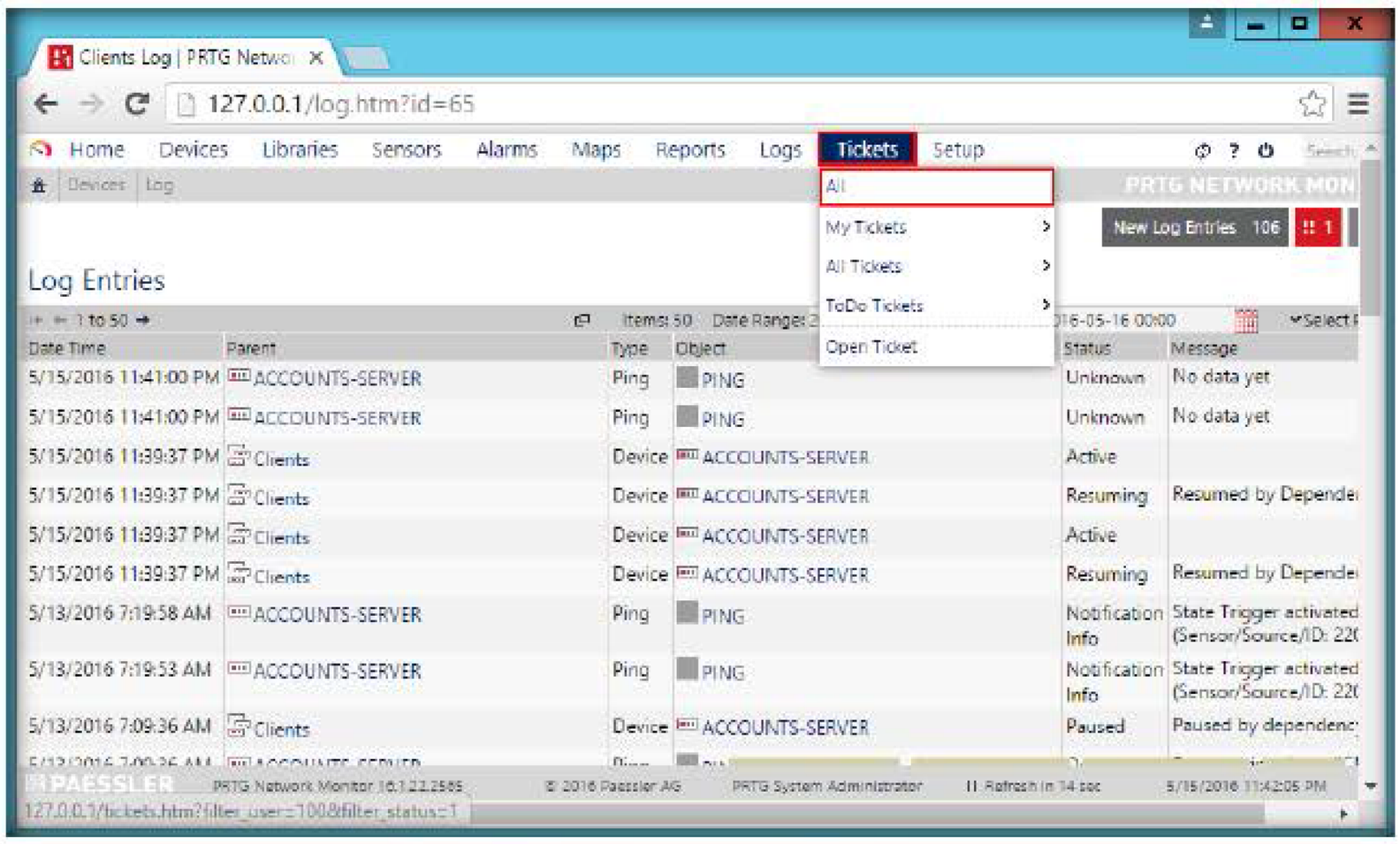



FIGURE 5.69: Navigating to the Tickets Section

121. You can see that there are various parameters to apply filters at the top section. The actions you can take against a ticket are in the right hand section of the web page, which are **Edit**, **Assign**, **Resolve** and **Close**.

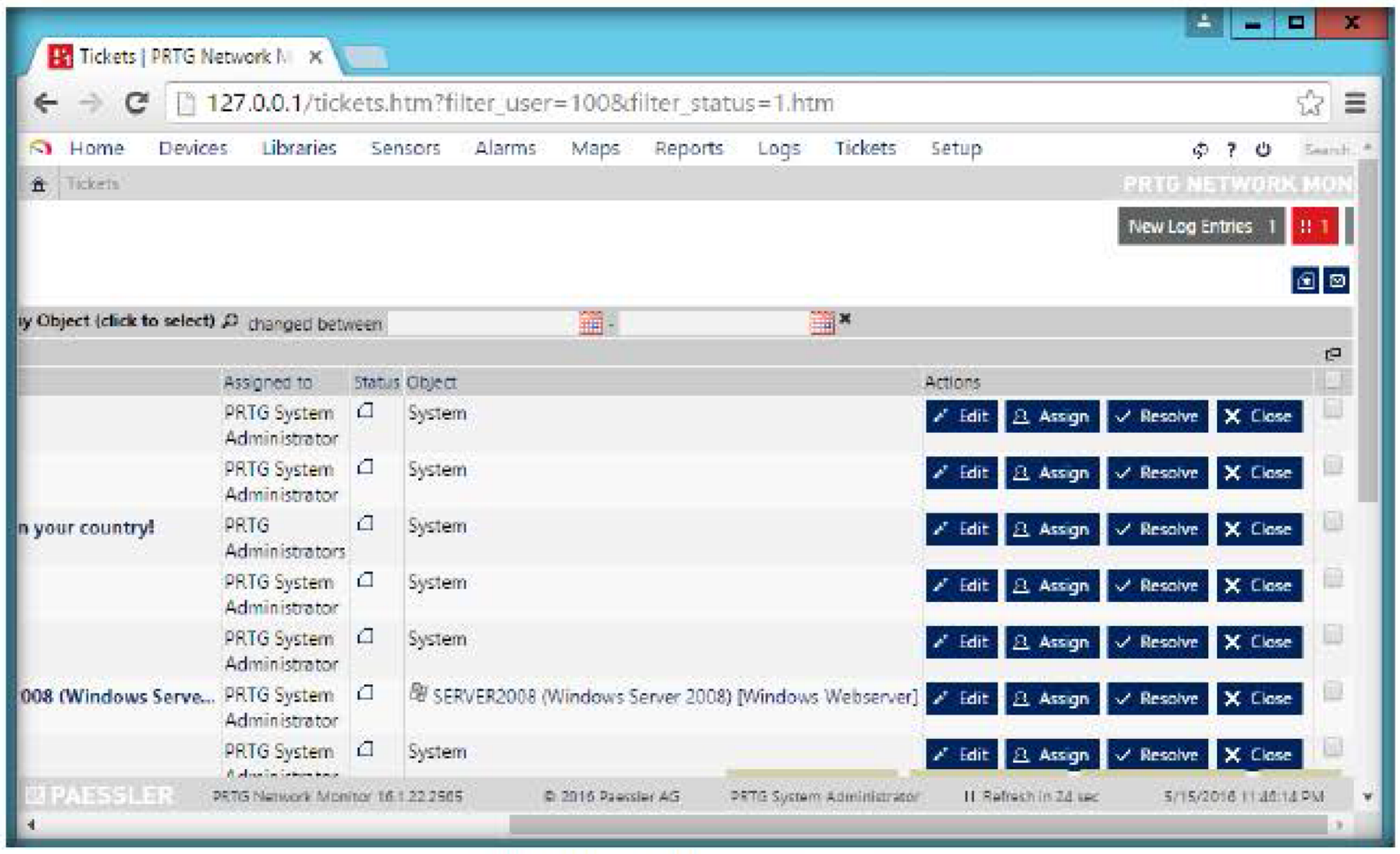



FIGURE 5.70: Tickets in the System



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

122. If you want to view only those tickets which are related to one of the **virtual machines**, click on the **related to any Object (click to select)** tab and select the virtual machine from the list. You can also select a particular sensor as well for the selected device. Click on **Save** when done.

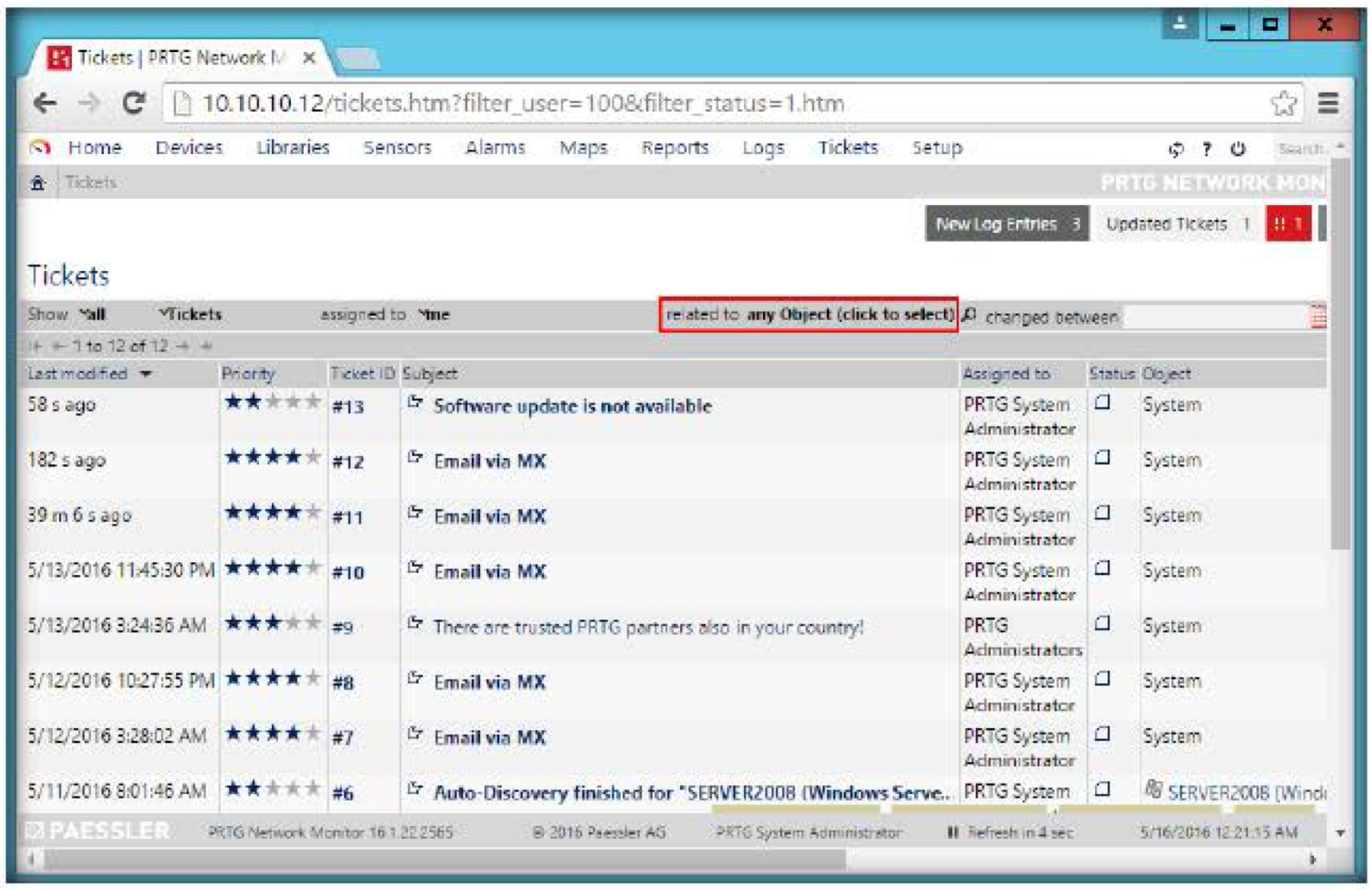



FIGURE 5.71: Selecting an Object

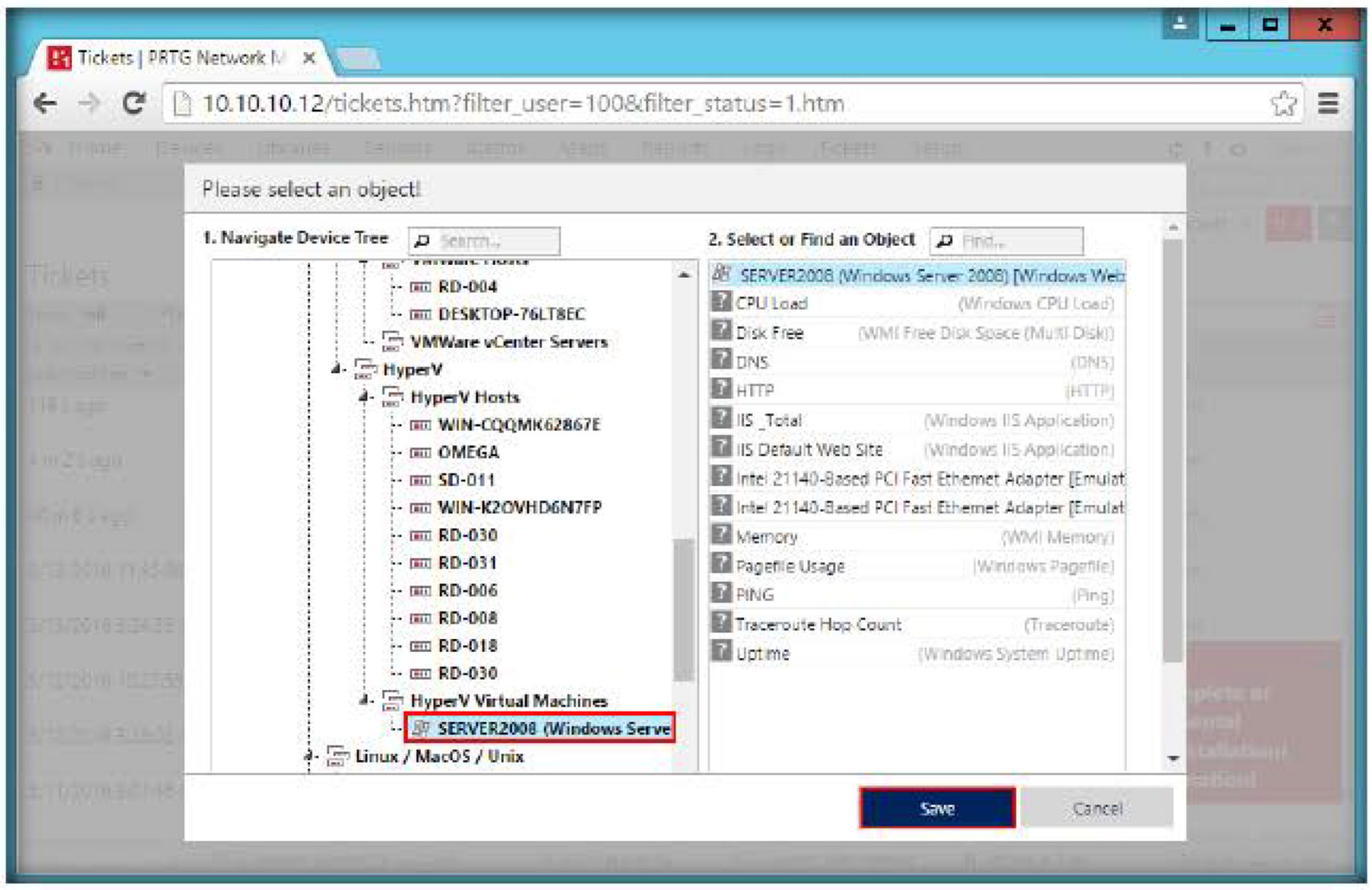



FIGURE 5.72: Selecting a Device to View its Tickets


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

123. You get only those tickets related to the particular device as follows:

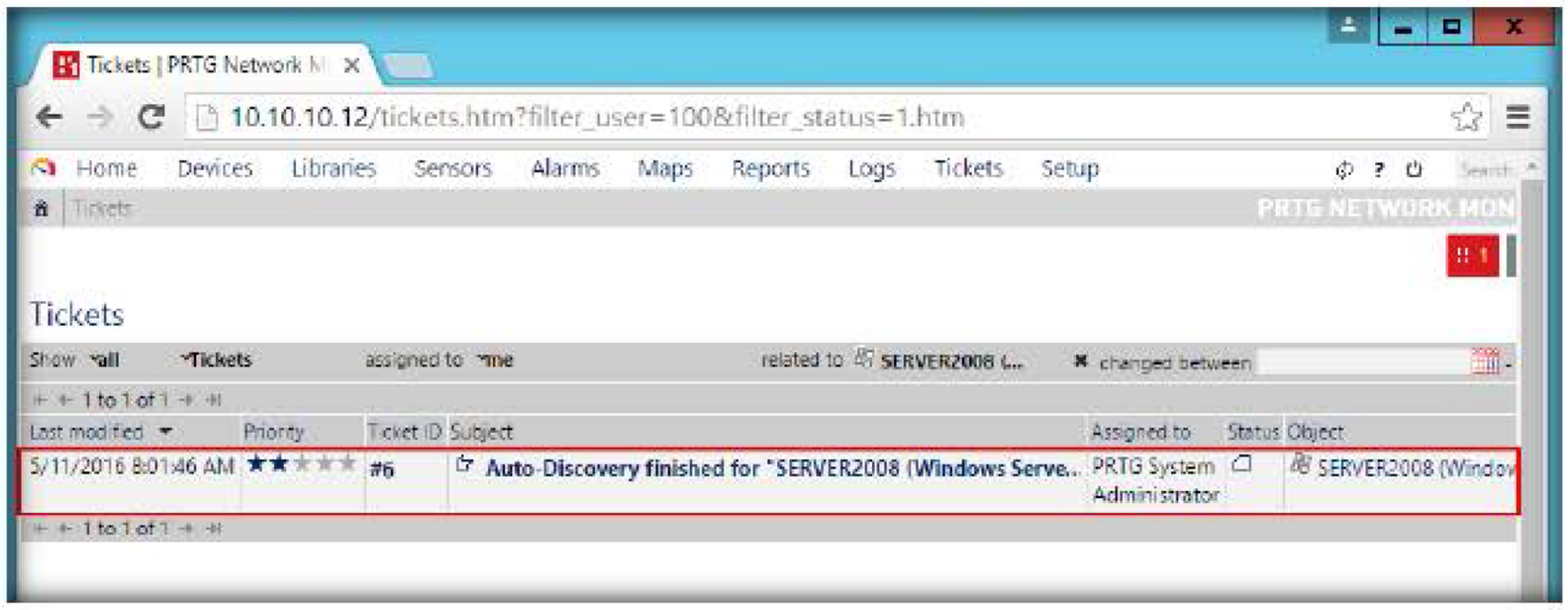



FIGURE 5.73: Tickets filtered by a particular device

124. You can change the ticket name, assignee or priority using the **edit** option, assign the ticket to someone else using the **assign** option. You can use the **resolve** or **close** options to end the ticket if you feel the issue has been solved.

125. The last section is the report section which allows you to create custom reports based on various parameters. To add a report, hover the mouse cursor on the **Reports** tab and click on **Add report** to create a new one.

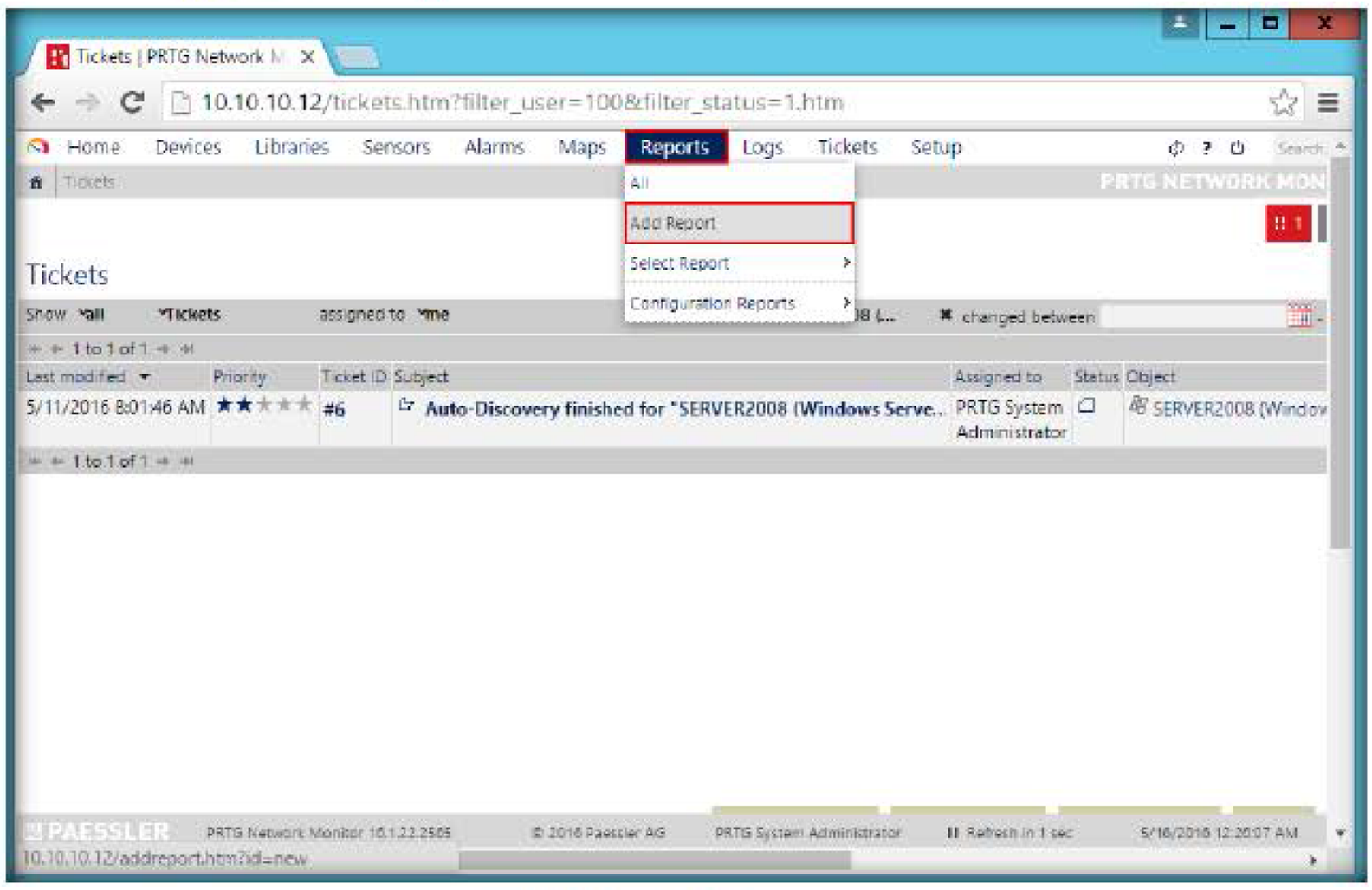



FIGURE 5.74: Adding a new report


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

126. In the basic settings of the report, provide a report name (here, **Test Report**), and select a template from the drop-down list (here, **Graph 1h interval, table 1h interval** template has been chosen). Security context deals with the Administrator account. Leave the other sections with the default options set, click **Continue**.

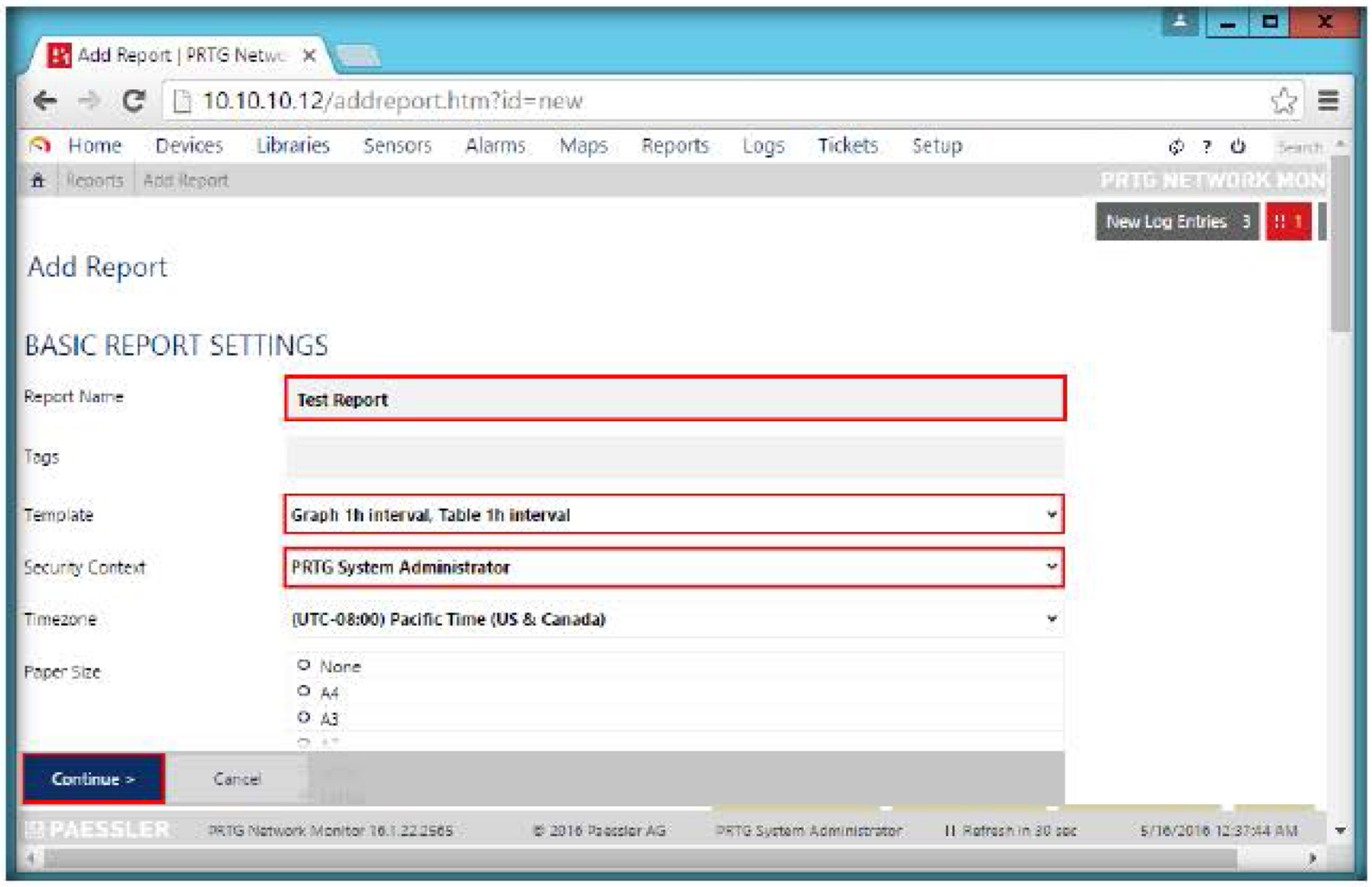



FIGURE 5.75: Basic Settings in Report

**Note**: You may configure the other settings like the **SENSORS** that are to be included in the report, **SCHEDULE** as to when you want the report to be generated, **PERIOD** during which the data should be collected, which forms the part of the report, etc.


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

127. The next step is the selection of individual sensors. Make any changes to sensors and click on **Run Now** at the top left corner of the webpage.

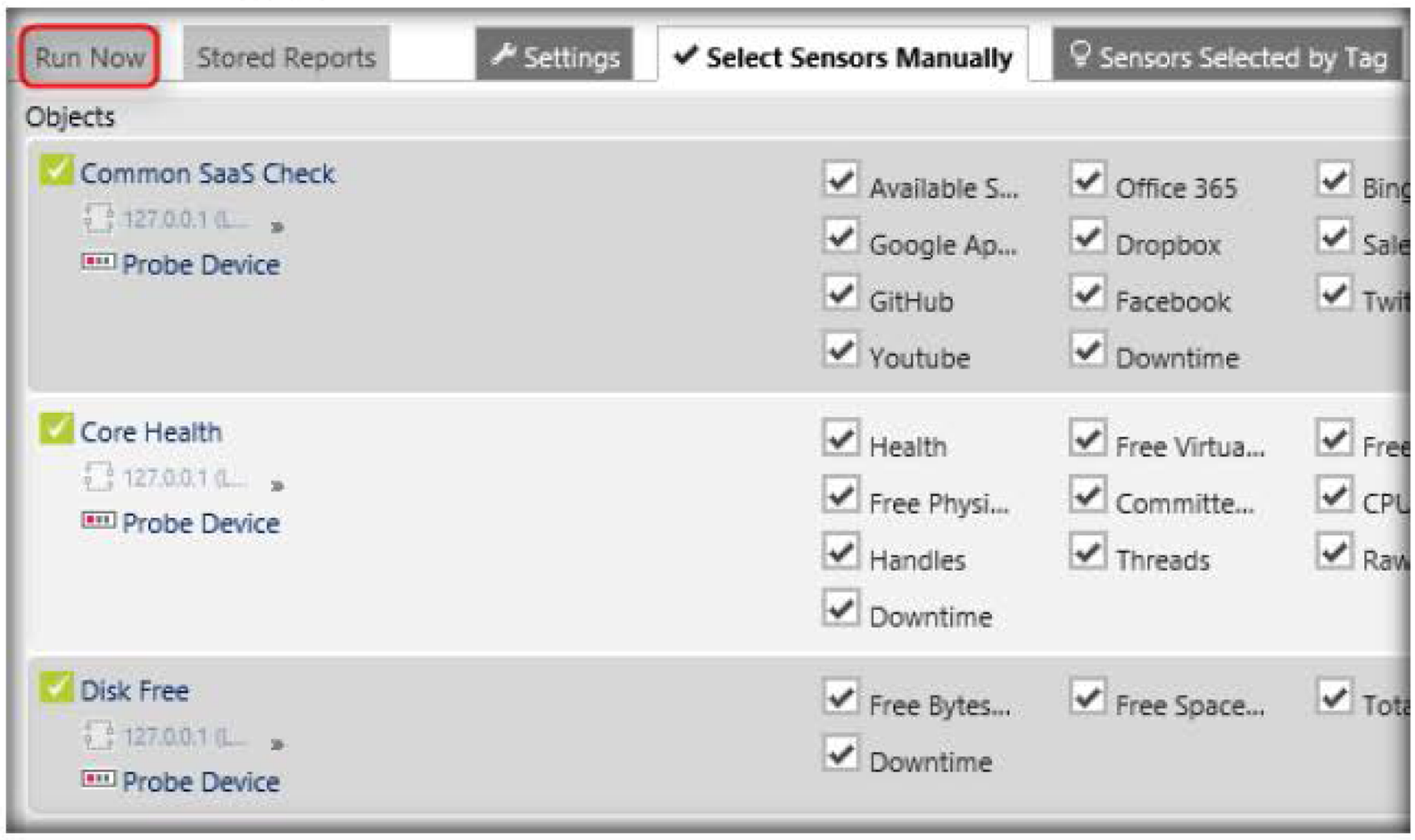



FIGURE 5.76: Selecting Sensors Manually

128. Use the **processing options** item to select the start and end dates for the report as well as the report format.

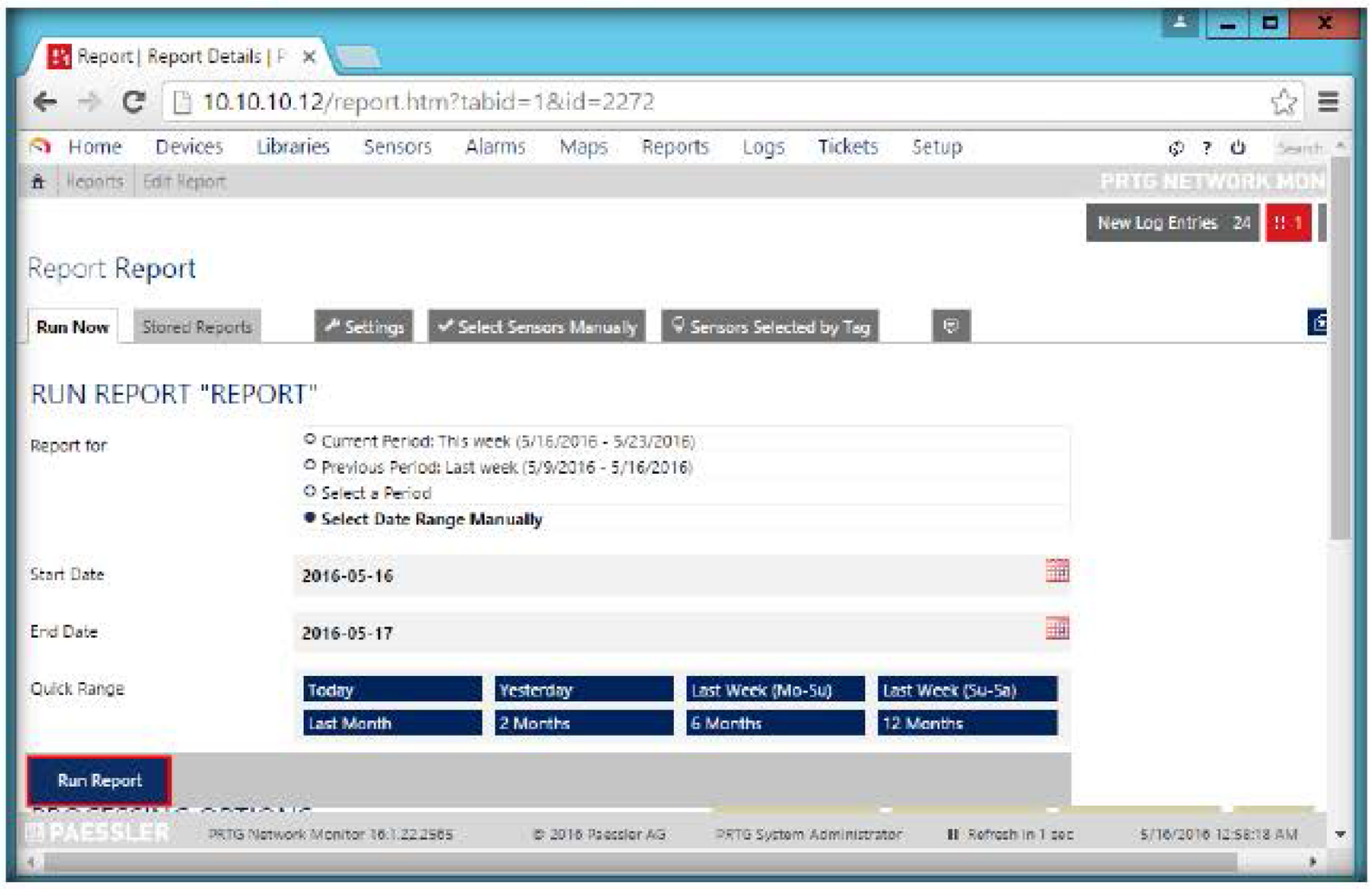



FIGURE 5.77: Finalizing the report settings


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

129. The report has both a data table and graph. You can scroll the report down and find every parameter in detail.

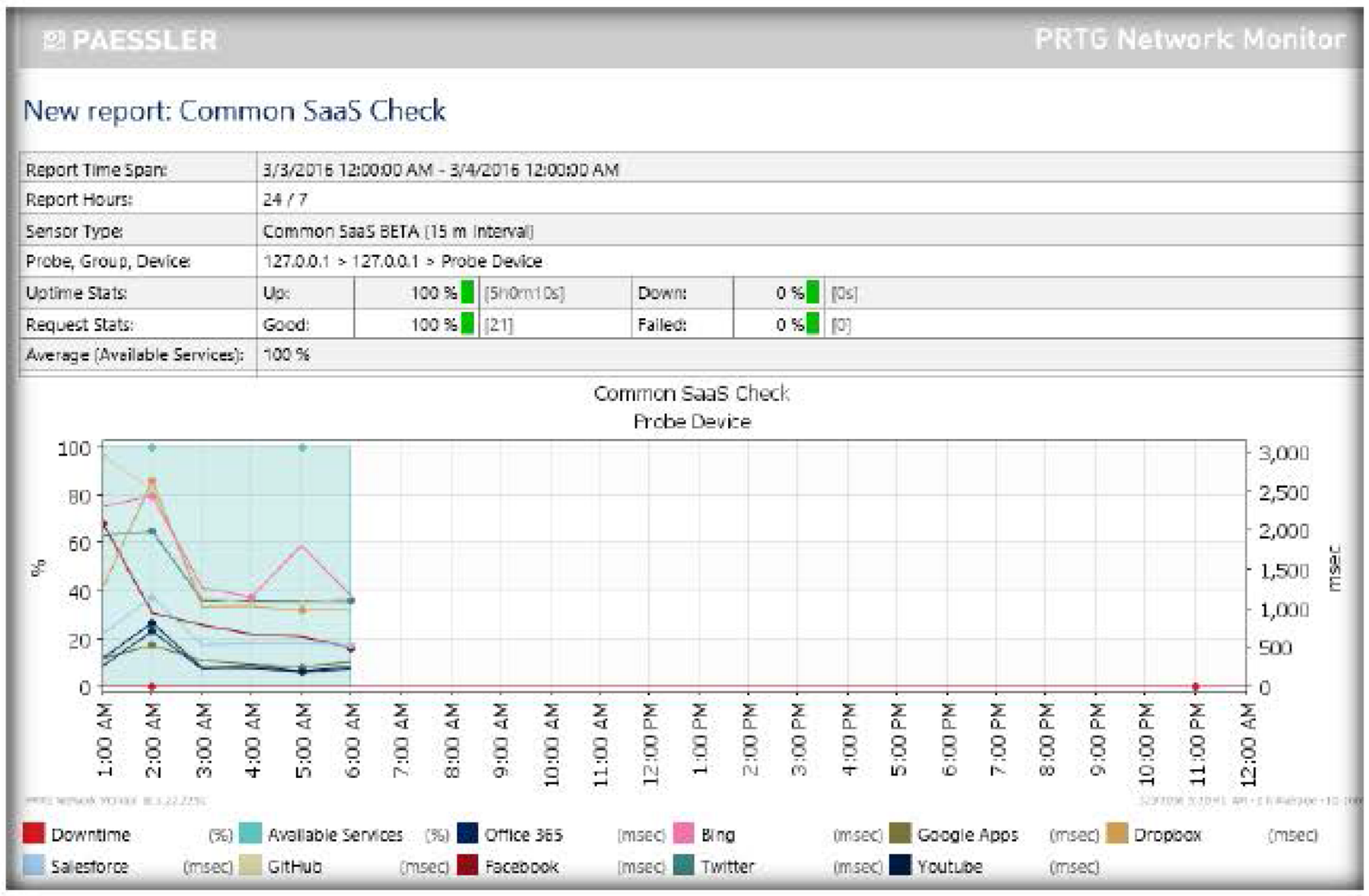



FIGURE 5.78: Report generated

## Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on securing the wireless network using Linksys router

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

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


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

Lab

6

# Web-based Traffic Analysis and Flow Collection Using ntopng

ntopng is a network traffic probe that shows network usage.

## Lab Scenario

Organizations host web servers, switches, routers, etc. in order to provide network access to personnel. Large amounts of traffic is flowing through the network, which needs to be examined by following the network policies implemented by the organization.

As a network administrator, it is essential to know how to log the network traffic; and examine the information flowing through the network as well as the network status.

ICON KEY

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

## Lab Objectives

This lab will demonstrate how to monitor Network Traffic using ntopng.

## Lab Environment

To carry out the lab, you need:

- A virtual machine running Network Security Toolkit (NST)
- A virtual machine running Windows server 2012
- A web browser with Internet access
- Administrative privileges to run the tools

## Lab Duration

Time: 20 Minutes



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

# Overview of ntopng

ntopng is a network traffic probe that shows the network usage. ntopng users can use a web browser to navigate through ntopng (that acts as a web server) traffic information and get a dump of the network status.

# Lab Tasks

**TASK 1**

**Login to NST**

1. Before beginning this lab, ensure you are logged into the Windows 10, Windows Server 2012, Windows Server 2008 and Ubuntu virtual machines.
2. To begin this lab, launch the VMware Workstation and Power On the **NST** virtual machine.
3. To login to the machine, select **Other...** from the NST User drop-down list.

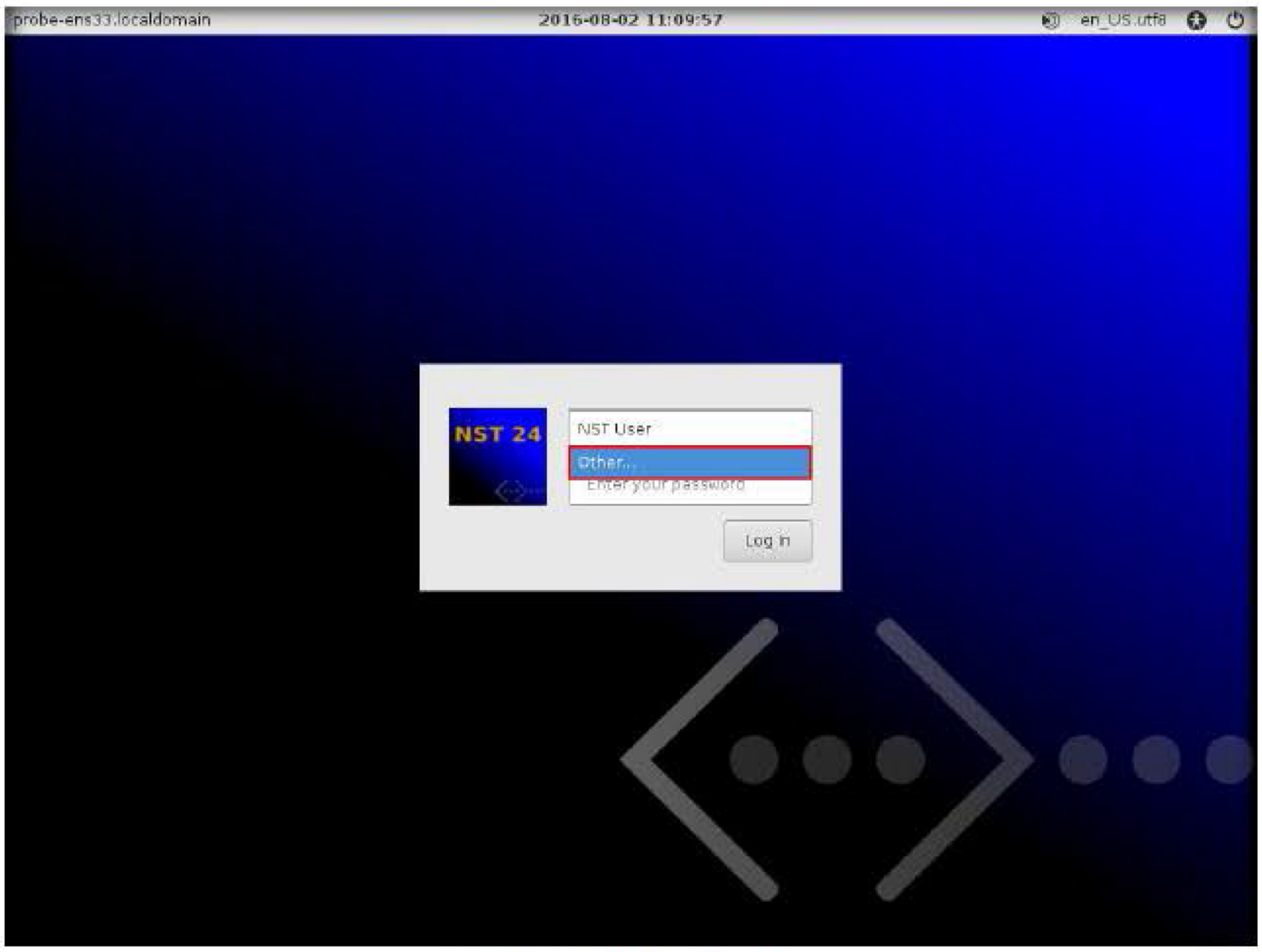



FIGURE 6.1: NST Login Window


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

4. Type **root** in the username field, **Pa$$w0rd** in the password field and click the **Log In** button.

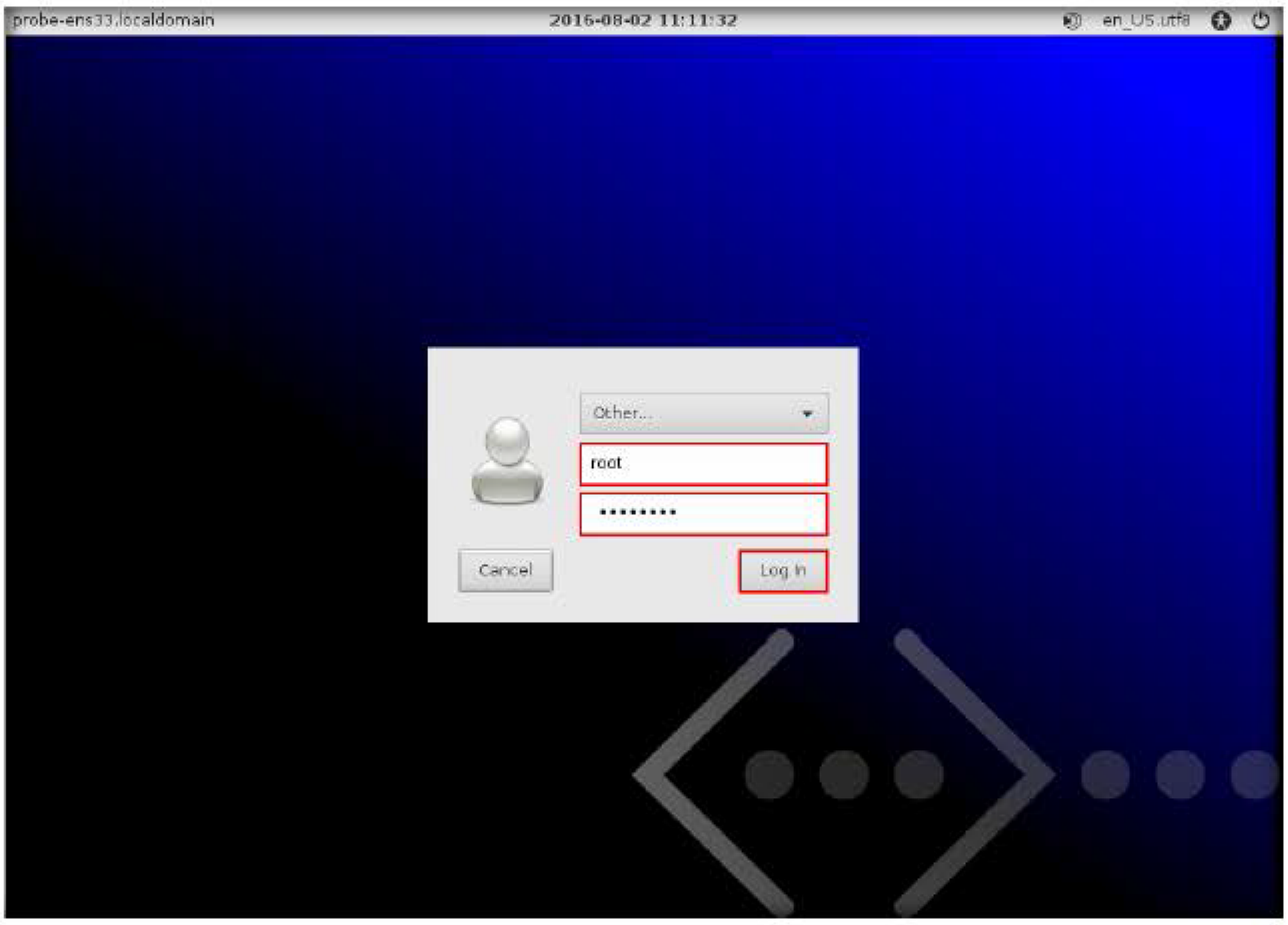



FIGURE 6.2: NST Login Window

**TASK 2**

**Login to NST WUI**

5. On successful login, the NST Desktop appears, click the **Firefox** icon in the Taskbar to launch the web browser.

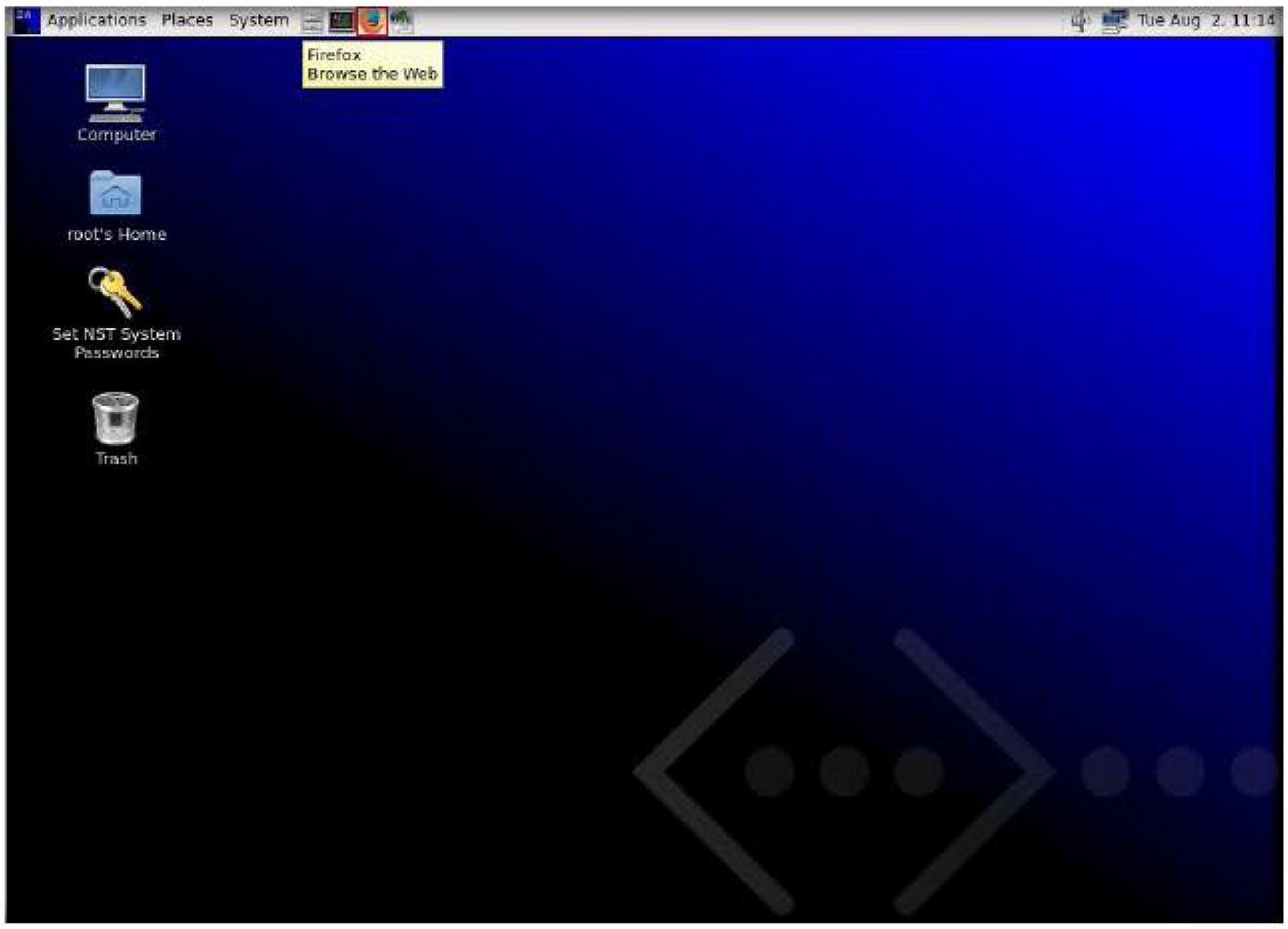



FIGURE 6.3: Launching Web Browser


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

6. An **Authentication Required** window (to access **http://127.0.0.1:9980**) appears, type **root** in the User Name field, **Pa$$w0rd** in the Password field and click **OK**.

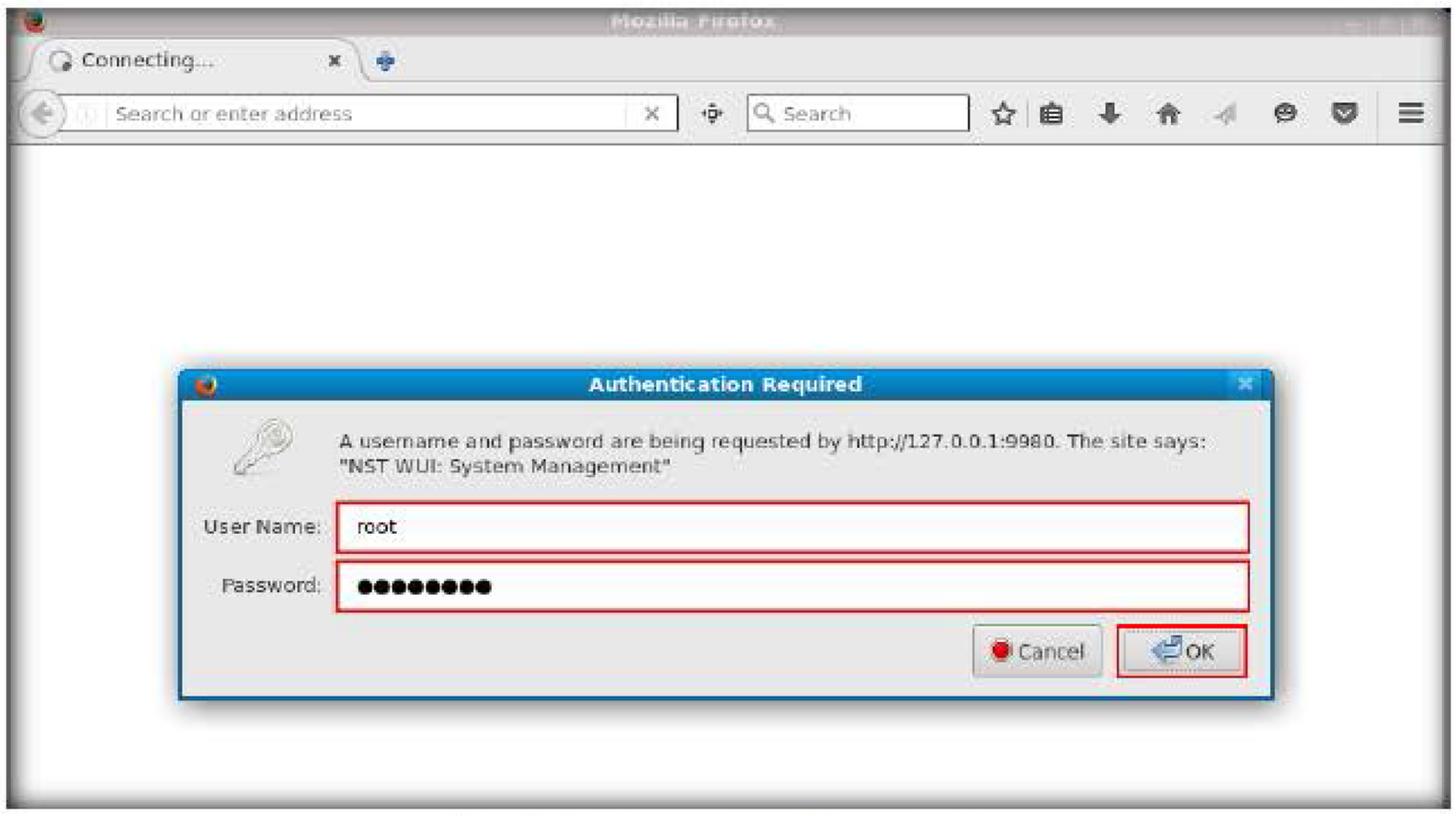



FIGURE 6.4: Authentication Required Window

**TASK 3**

**Login to ntopng**

7. NST homepage appears, go to **Network → Monitors → ntopng UI (HTTPS)**

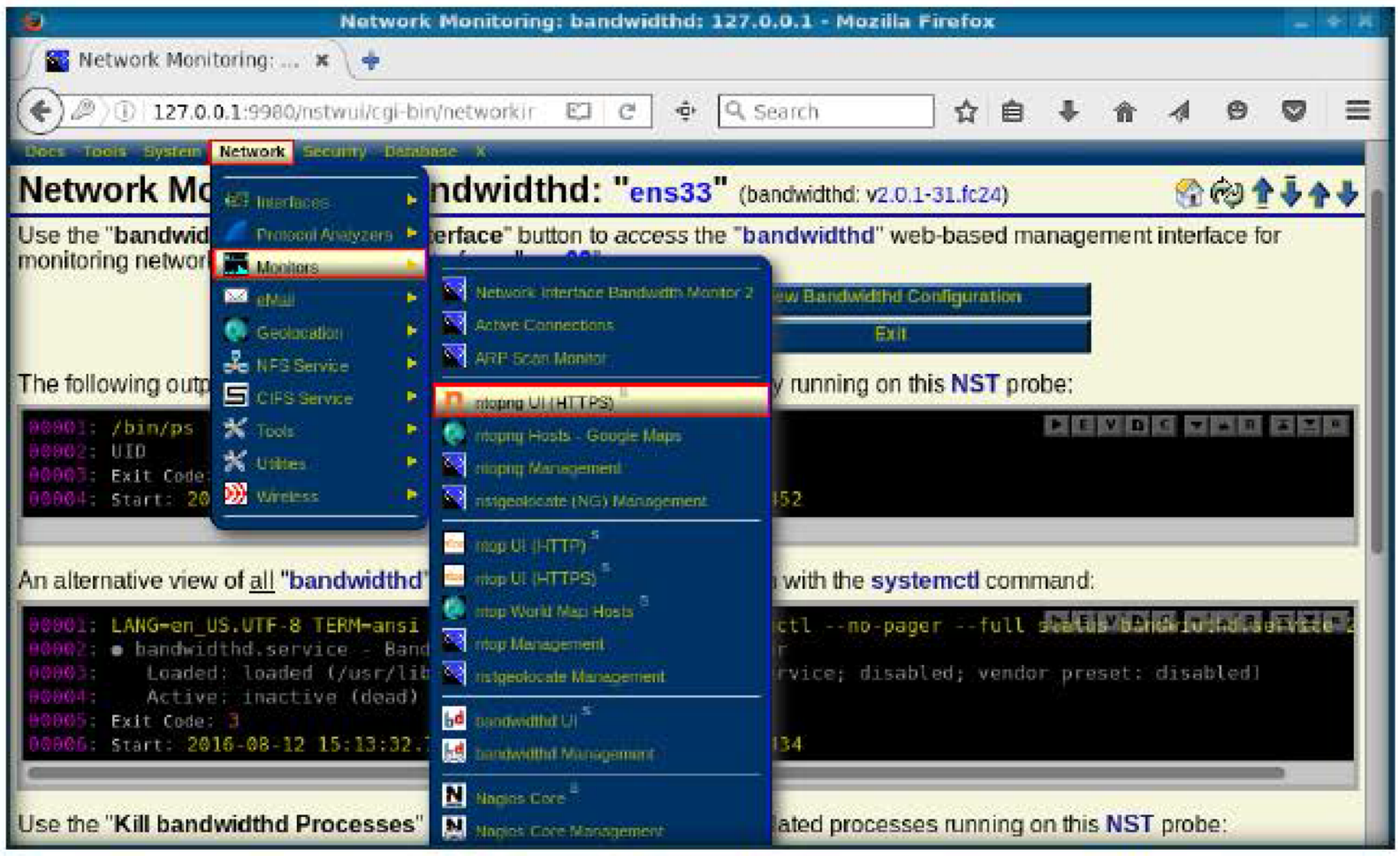



FIGURE 6.5: Launching ntopng UI



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

8. ntopng is a detailed network traffic usage monitor. One can use a web browser to navigate through a comprehensive set of rendered ntop network traffic views and analysis pages depicting the overall network traffic status.

9. **ntopng Setup Management** page appears, scroll down the page and click **Startup ntopng Session** to initialize the application

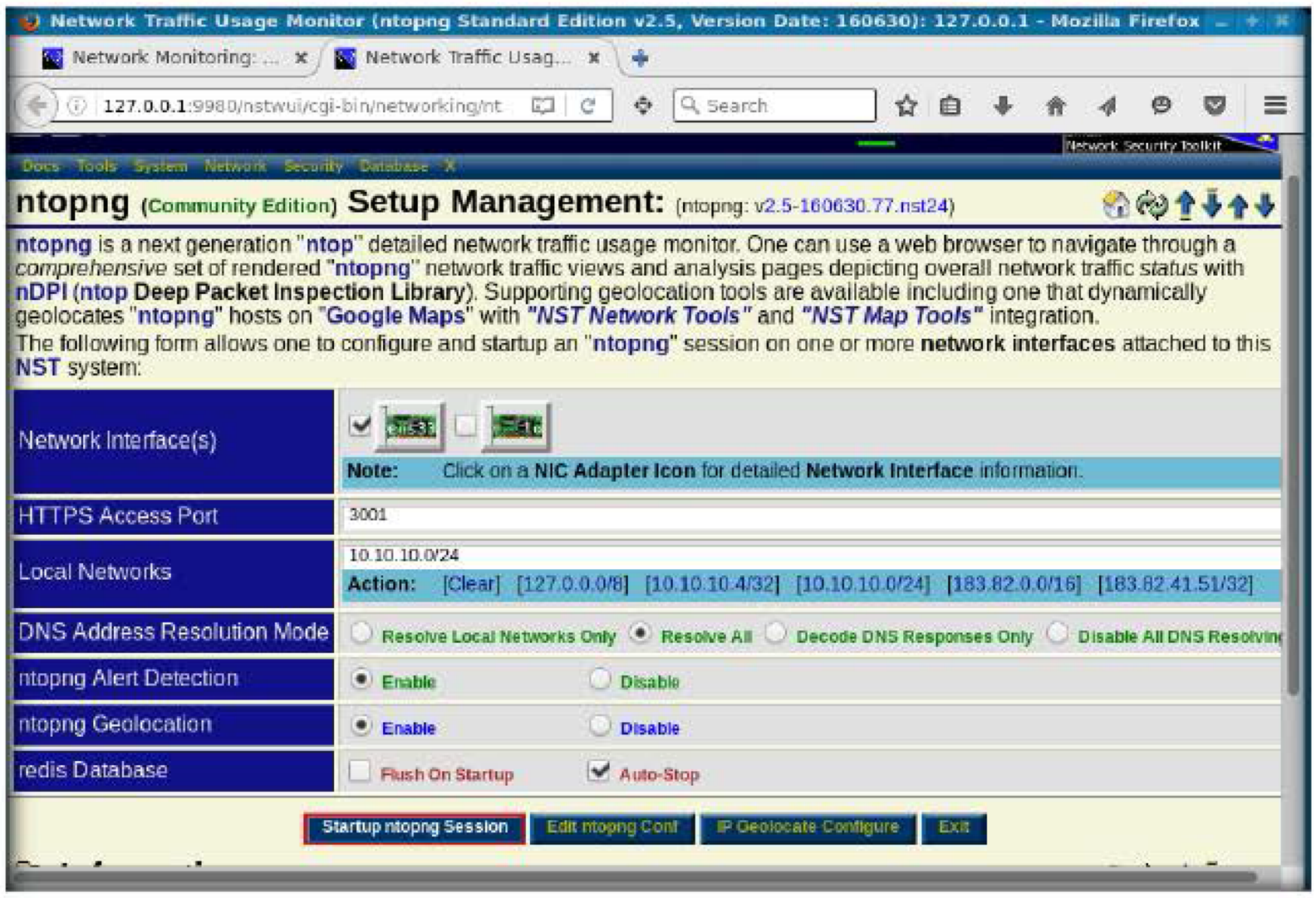



FIGURE 6.6: Initializing ntopng

10. ntopng begins to initialize in the background. Click **Return** to check the startup progress.

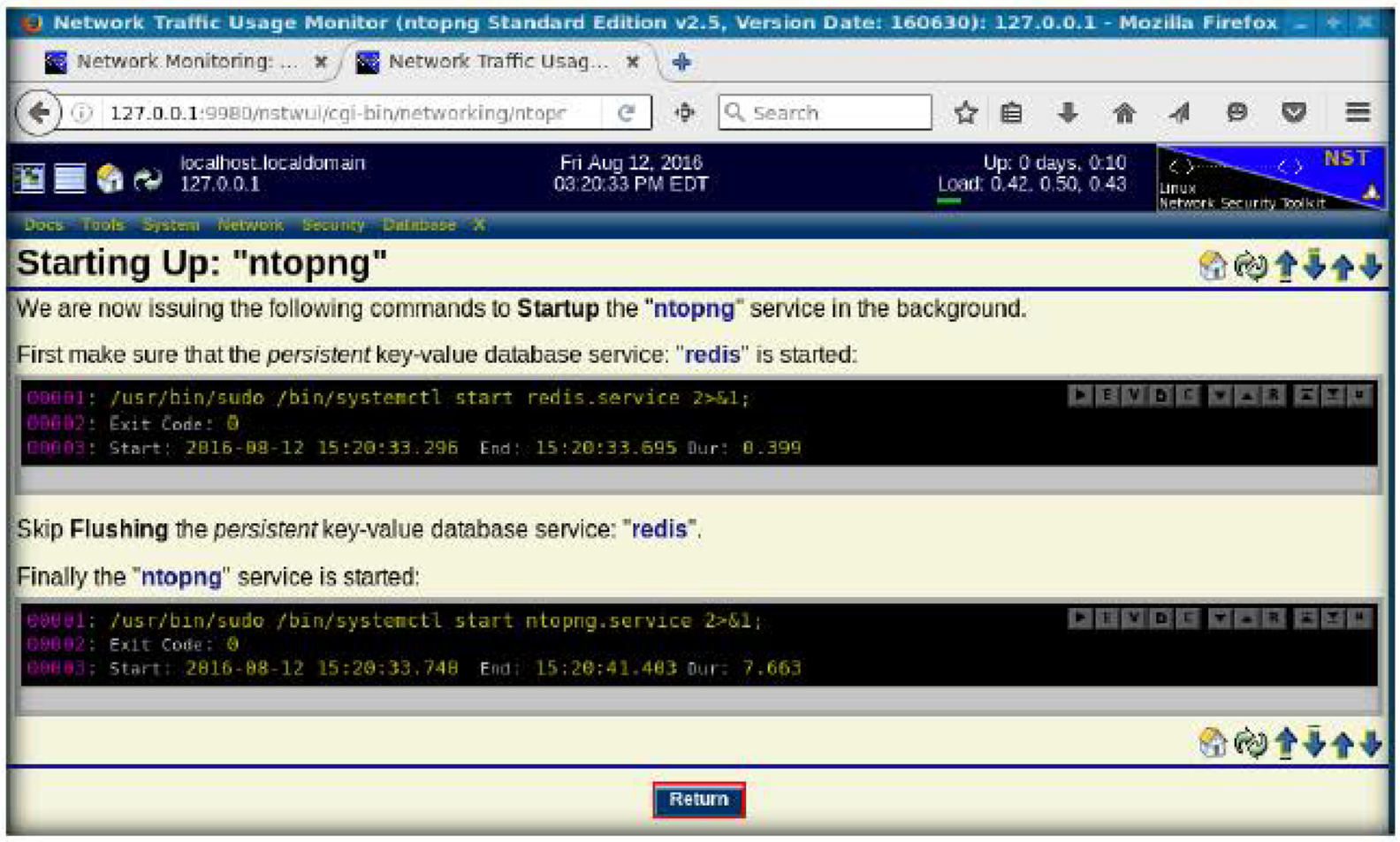



FIGURE 6.7: Checking the startup progress



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

11. Once the ntopng application is successfully initialized, it displays the ntop Service Control status as **Running**. Now, click **Use ntop Interface (HTTPS)** button to enter the ntop web-based user management interface.

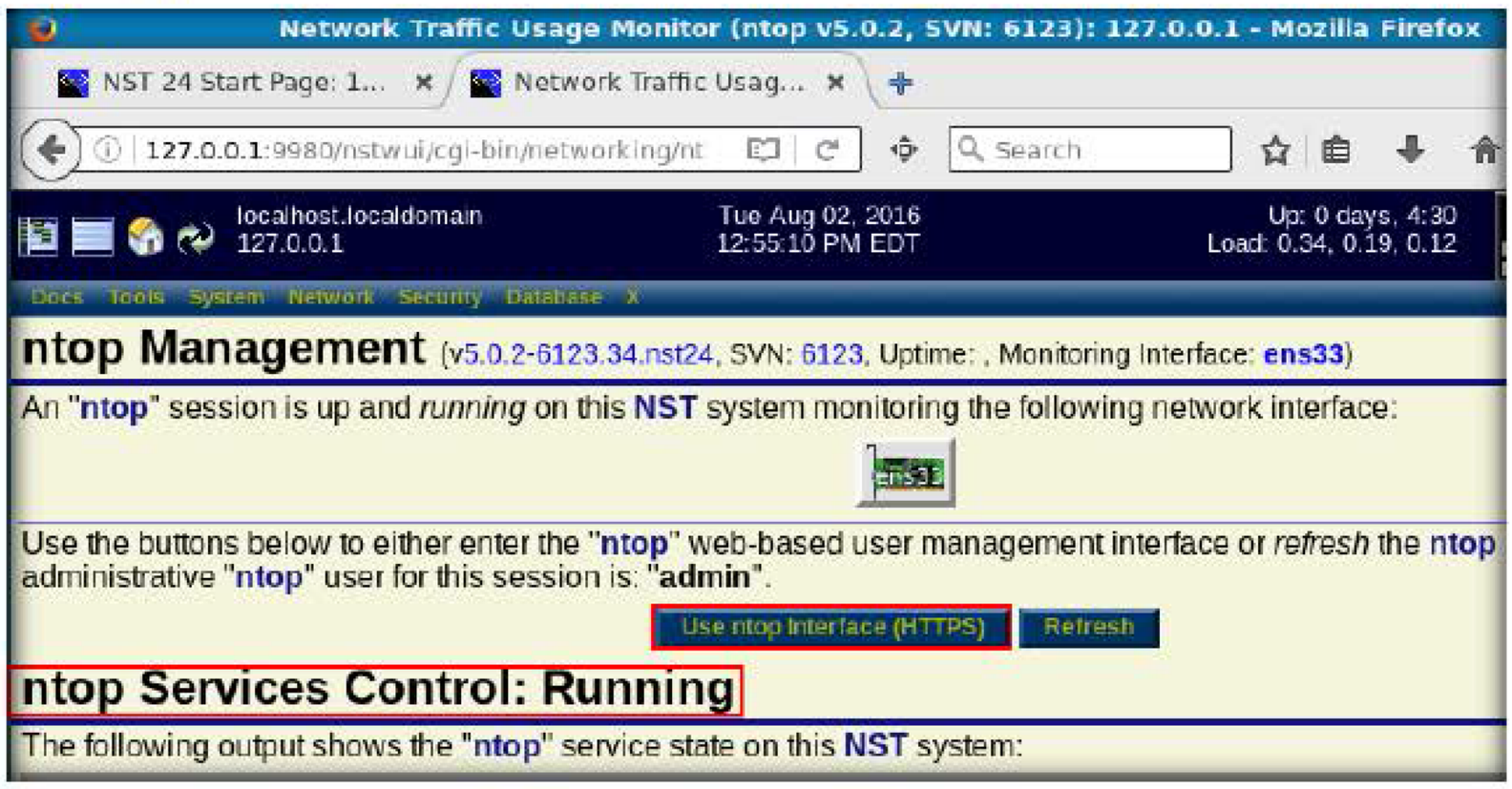



FIGURE 6.8: Using ntopng GUI

12. ntop runs on port **3001** by default. A webpage appears, stating the connection is not secure. To access the page, click **Advanced**.

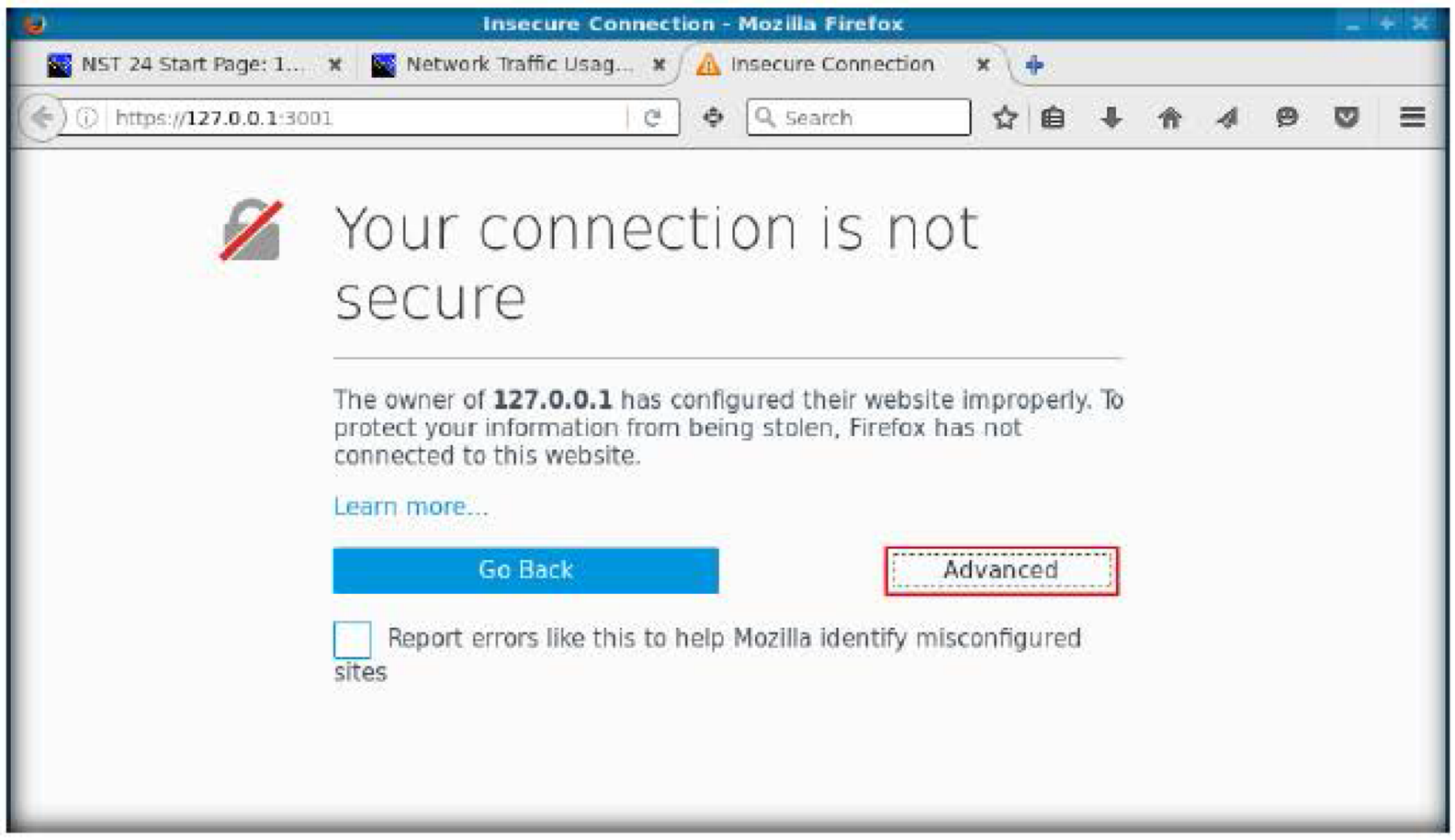



FIGURE 6.9: Connection Untrusted Webpage


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

13. Click **Add Exception...** to add access the ntop webpage.

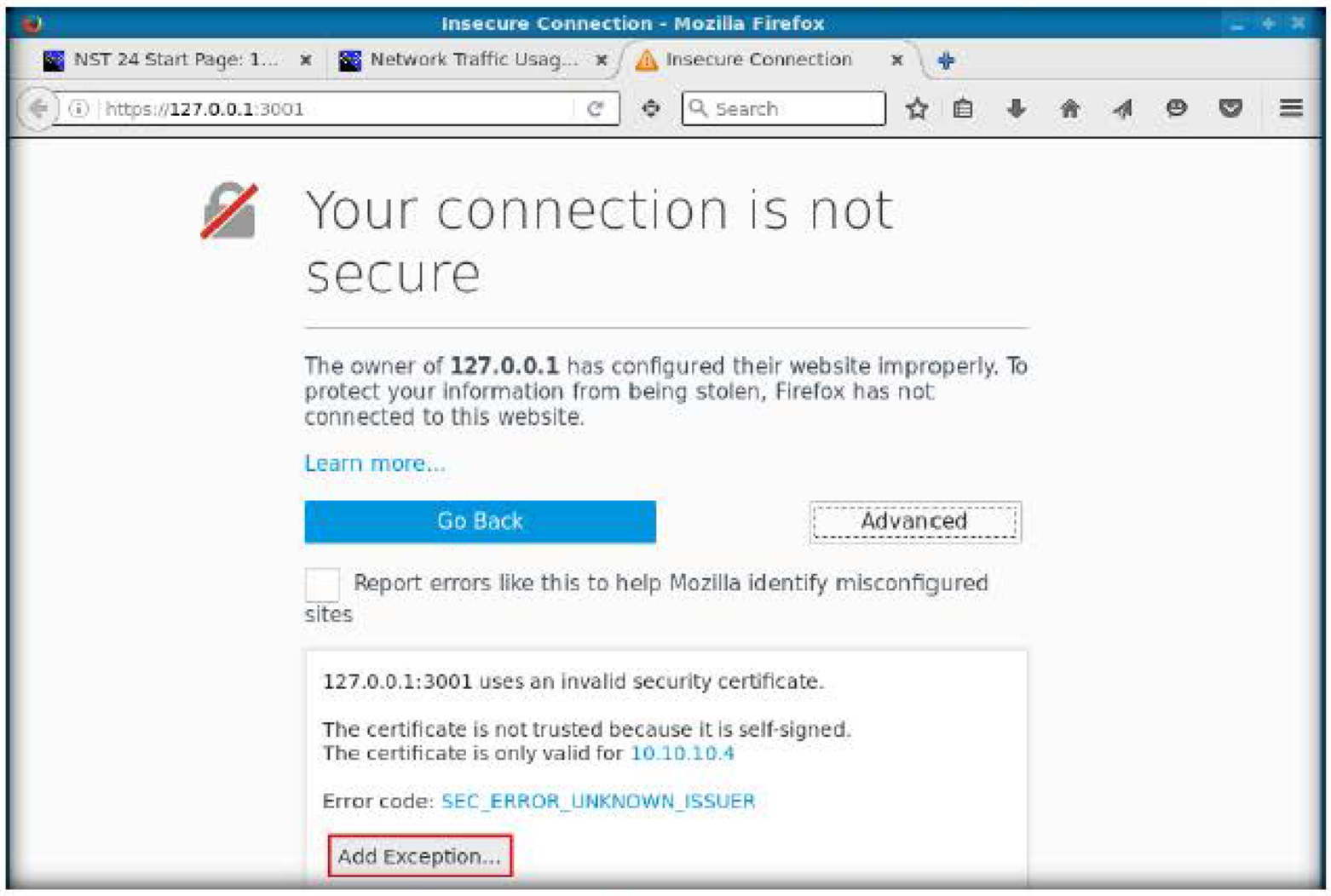



FIGURE 6.10: Adding Security Exception

14. The **Add Security Exception** window appears, click the **Confirm Security Exception**.




FIGURE 6.11: Confirming Security Exception


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

**TASK 4**

**Monitor Network Using ntop**

15. The ntopng login page appears, type the following credentials and click **Login**:

    Username: **admin**

    Password: **admin**

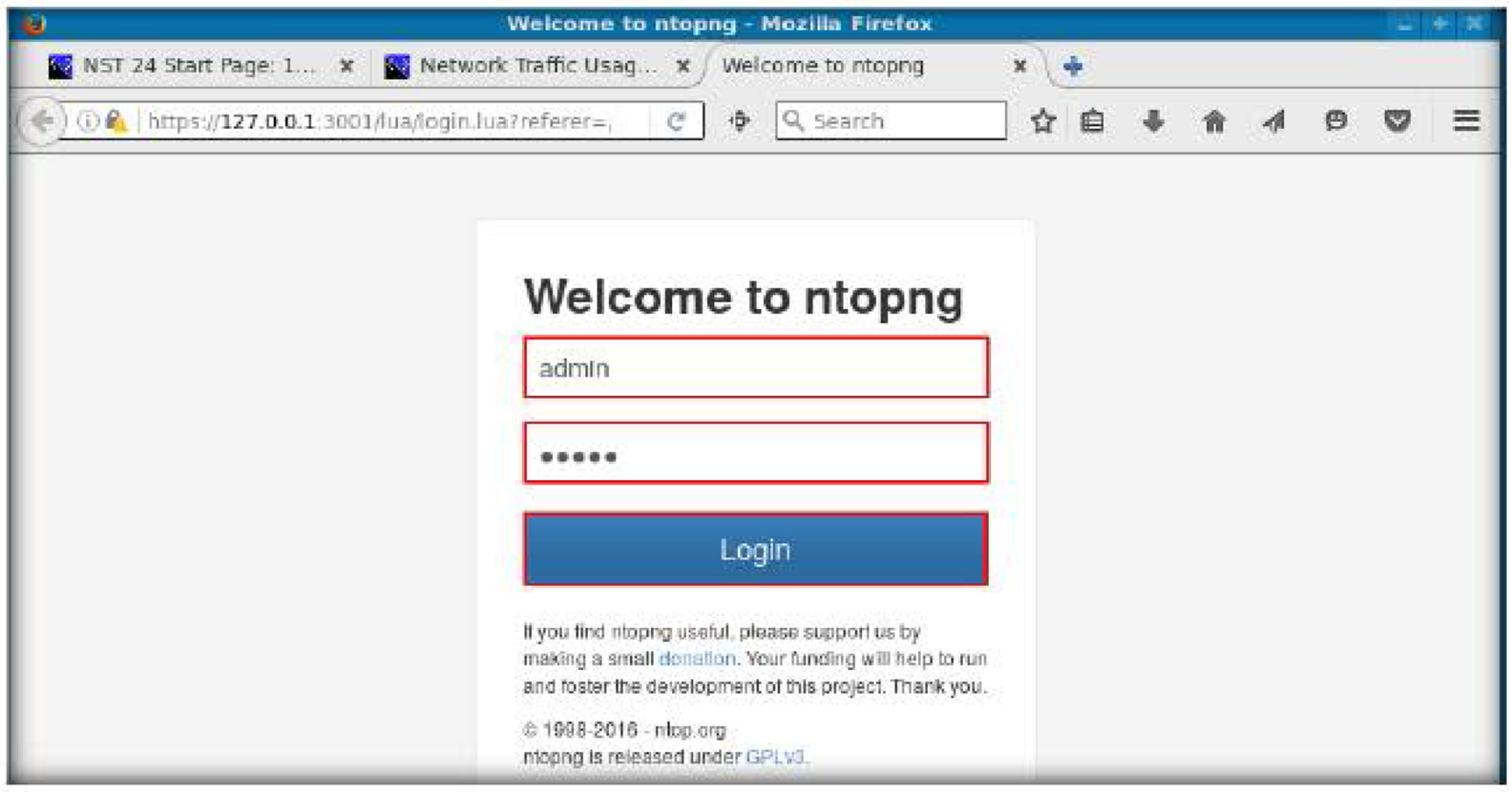



FIGURE 6.12: ntopng Login Page

16. Once logged in to the application, switch to each virtual machine and browse websites such as https://www.google.com.

17. After browsing the websites, switch back to the NST machine. View the ntop dashboard. The ntop dashboard displays the **Top Flow Talkers** under the **Talkers** webpage as shown in the screenshot.

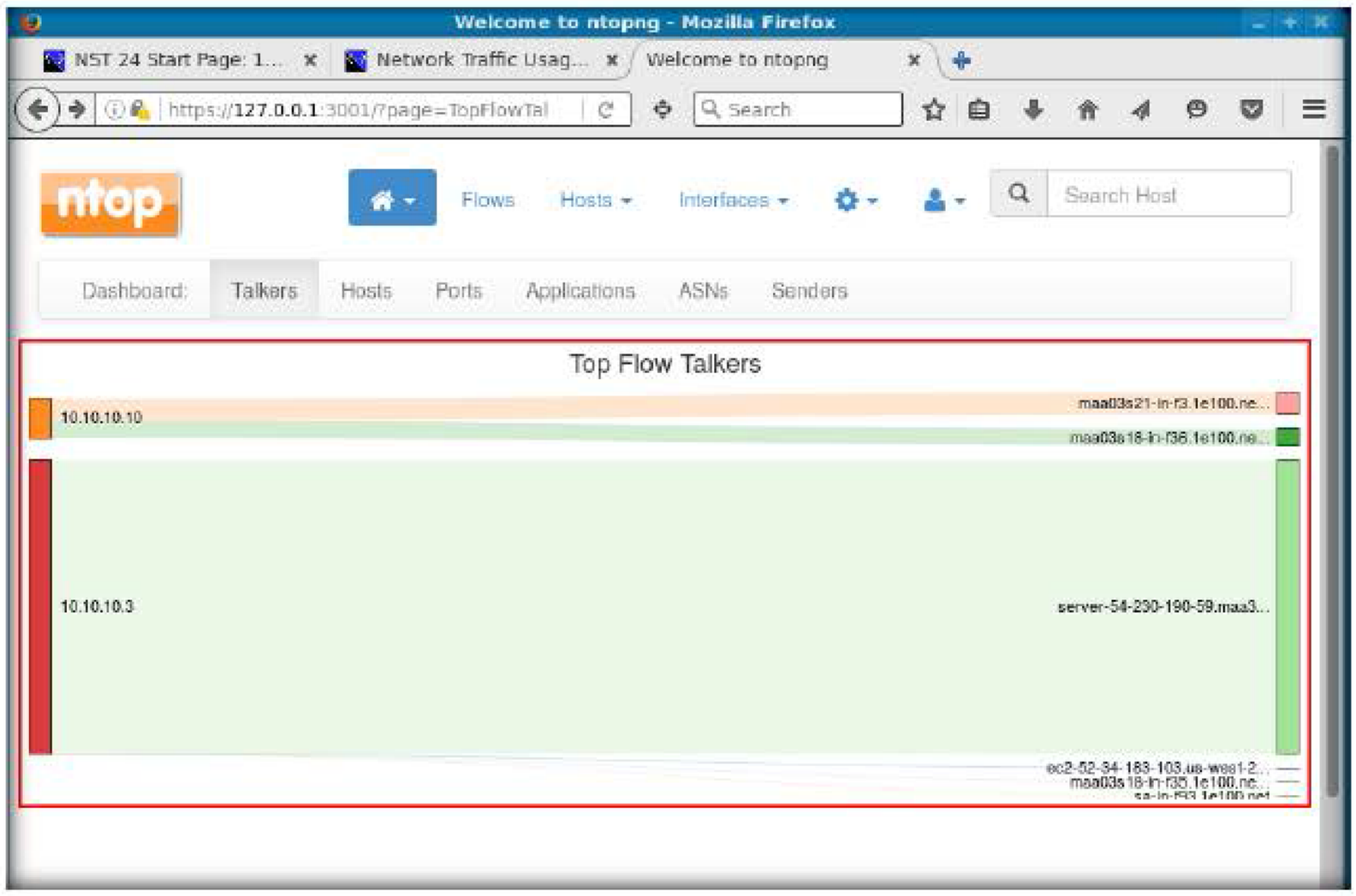



FIGURE 6.13: Network Traffic Displayed in ntop



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

18. Talkers are those hosts in a network, which communicate with the machines/software/web applications remotely.
19. Click the **Hosts** tab to view the top hosts that consume the most bandwidth compared to other hosts on the network.

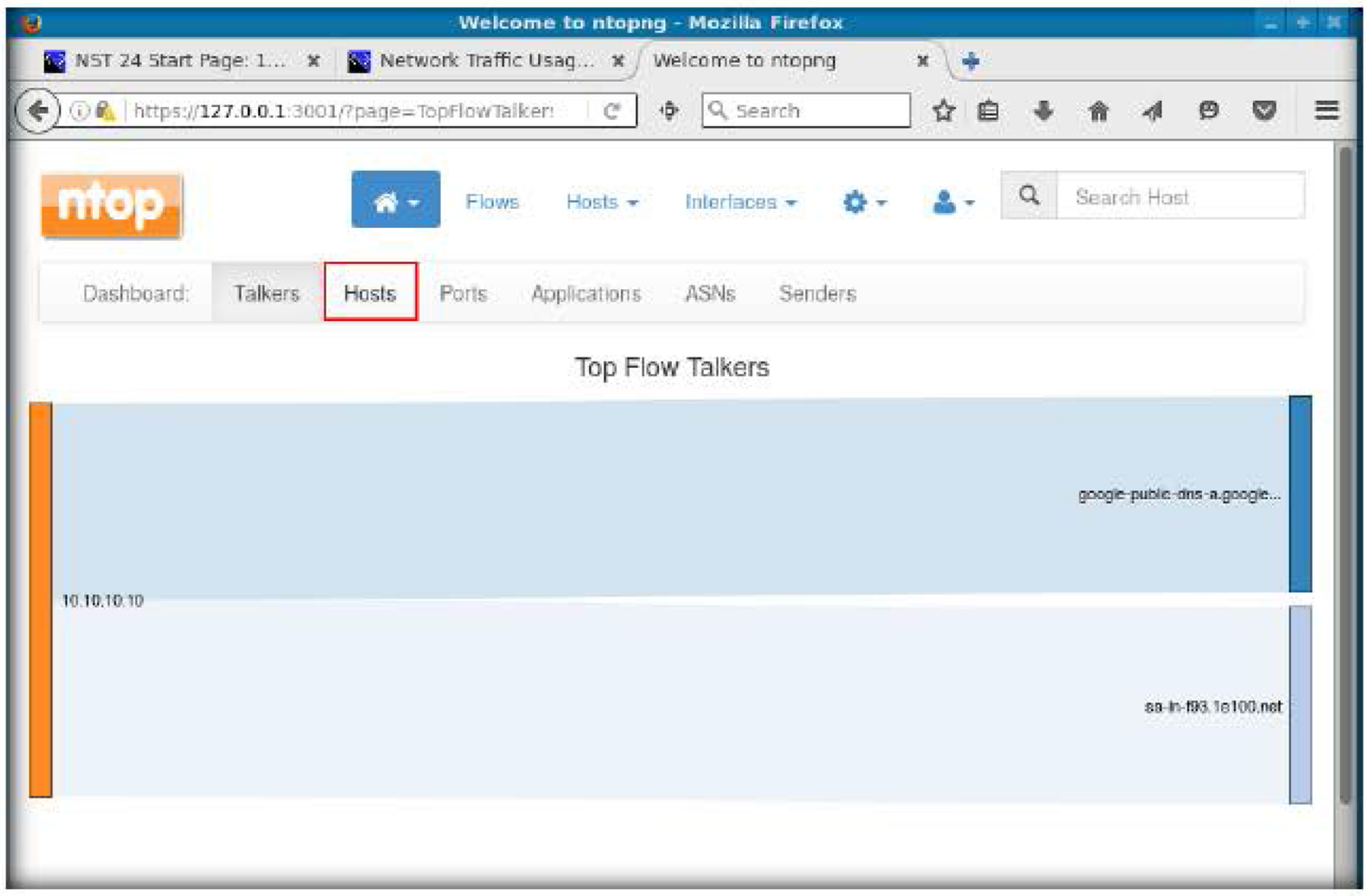



FIGURE 6.14: Viewing hosts in the network

20. The **Top Hosts** webpage appears displaying the percentage of bandwidth consumed by every local host as shown in the screenshot.

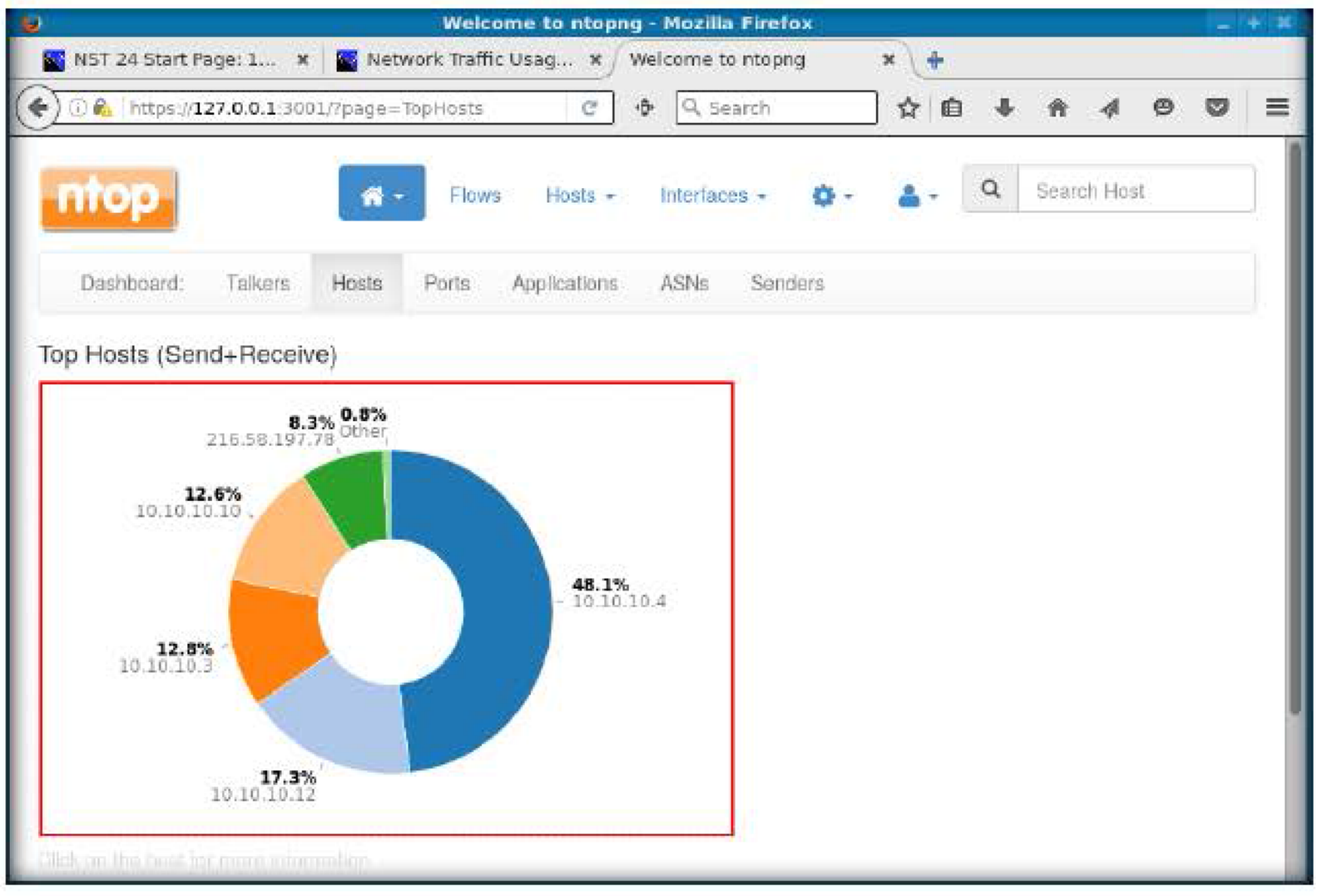



FIGURE 6.15: Top Hosts in the Network


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

21. All the ports, applications, ASNs and Senders associated with the top talkers can be viewed.

22. By default, ntop tracks all hosts that it sees from packets captured via various NICs. The next task is to view all the hosts (local and remote) the network communication took place between. To view, hover the mouse cursor on the **Hosts** drop-down list and click **Hosts**.

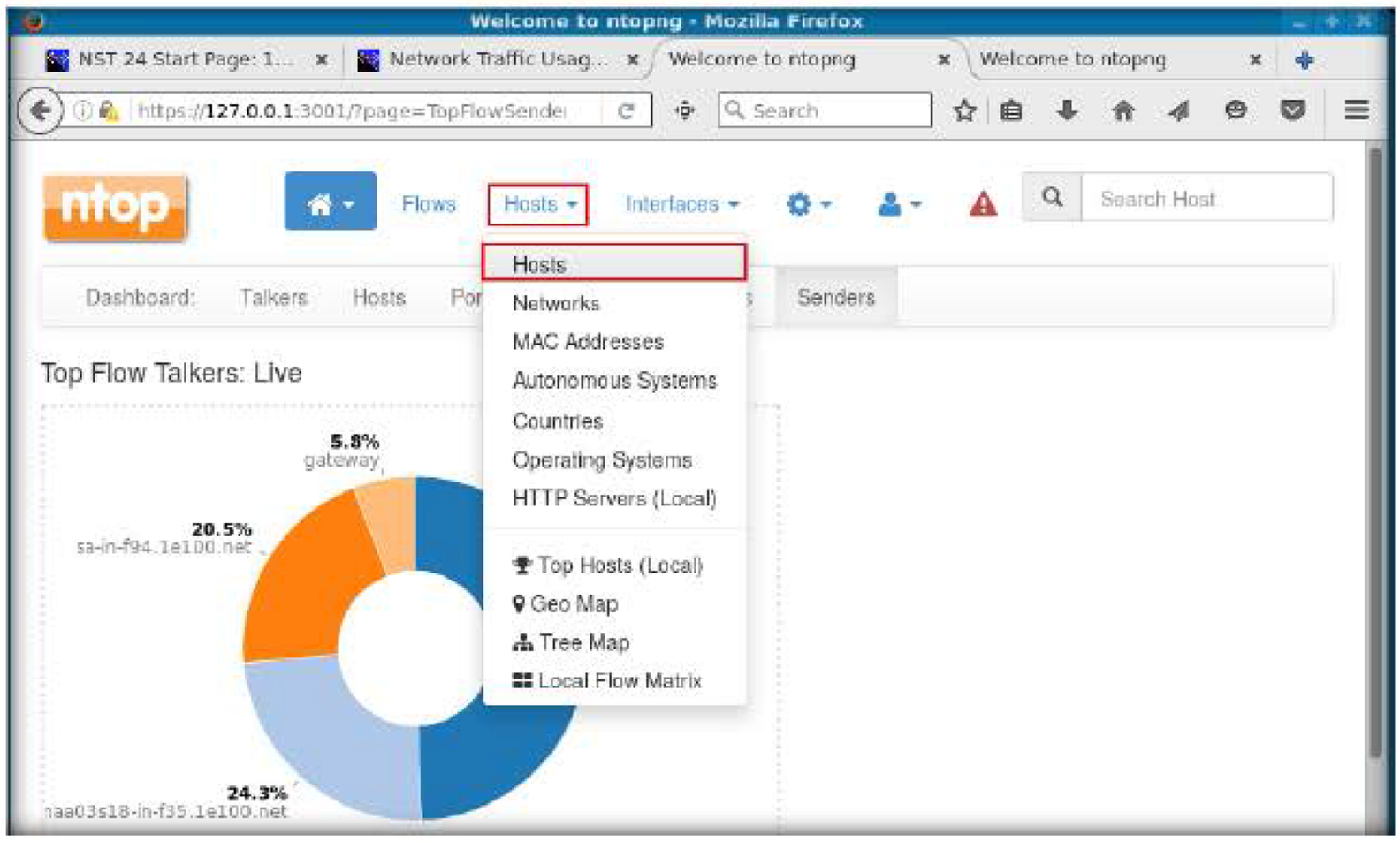



FIGURE 6.16: Viewing All Local and Remote Hosts

23. ntop displays all the hosts, along with the type of host (local or remote), time since the host is seen, amount of traffic through the host, etc. as shown in the screenshot.

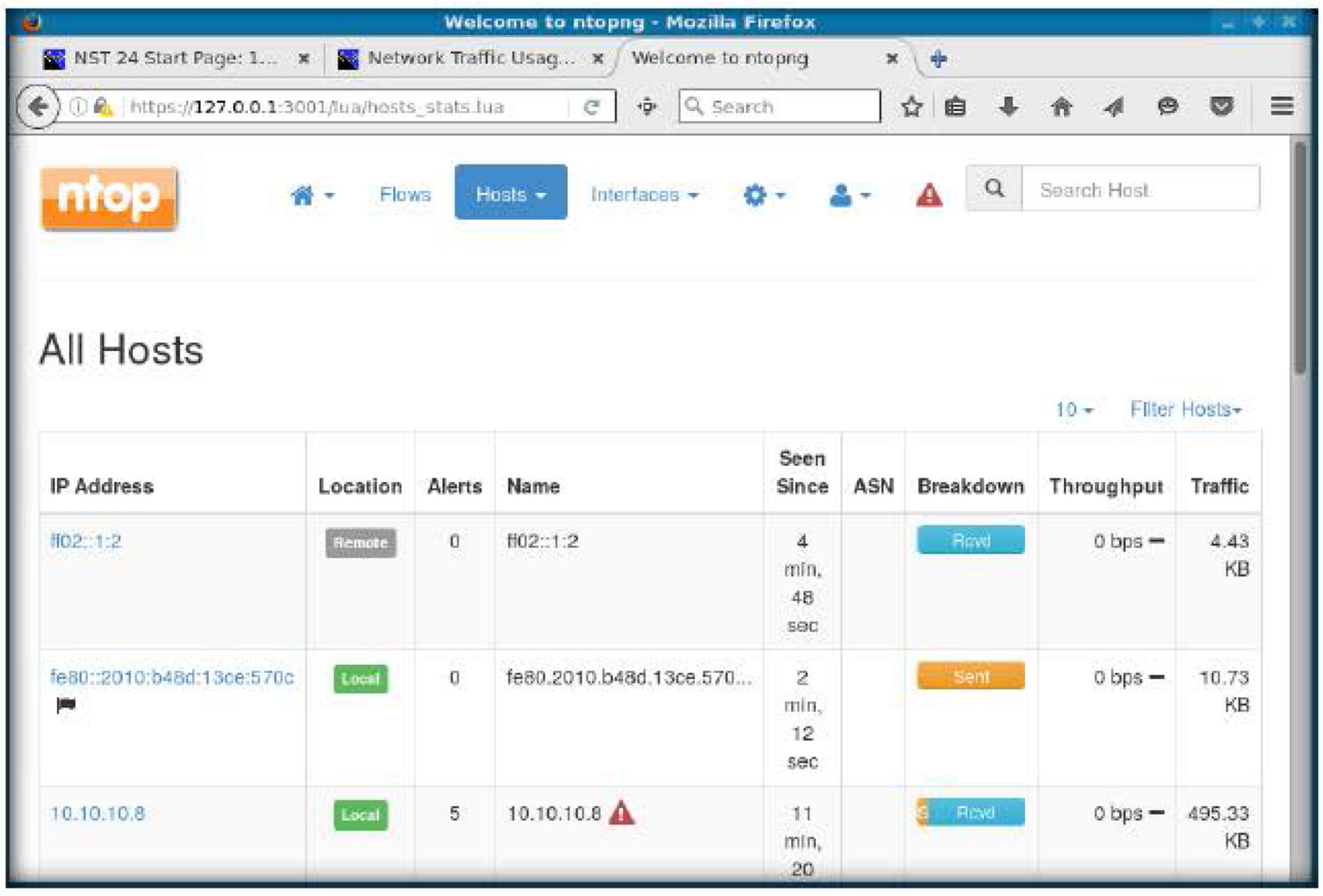



FIGURE 6.17: Examining All Local and Remote Hosts



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

24. You may view either local hosts alone, remote hosts alone or local networks by filtering them from the **Filter Hosts** drop-down list.

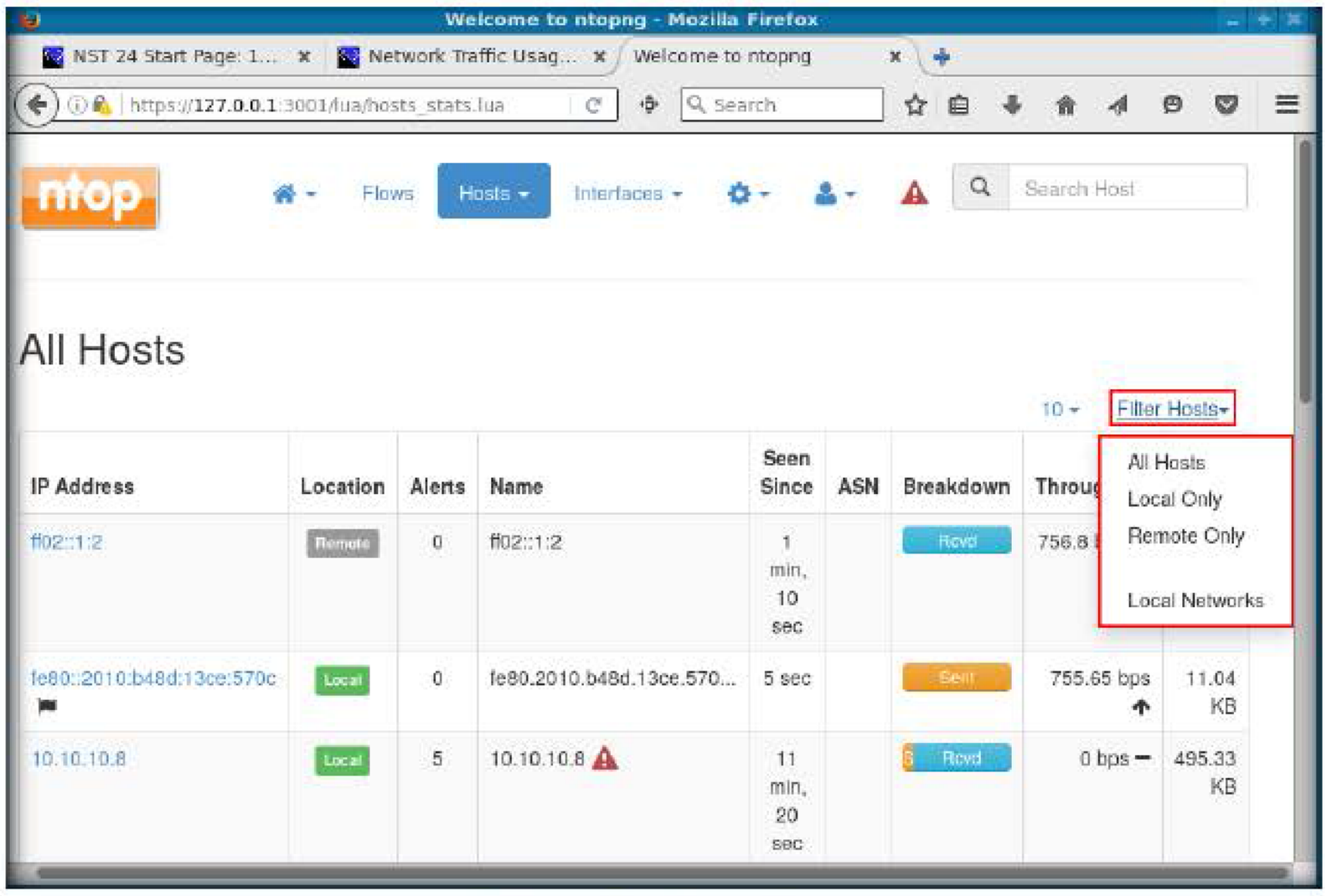



FIGURE 6.18: Filtering Hosts

25. There are other options under the **Hosts** drop-down list which can be used for monitoring the network.

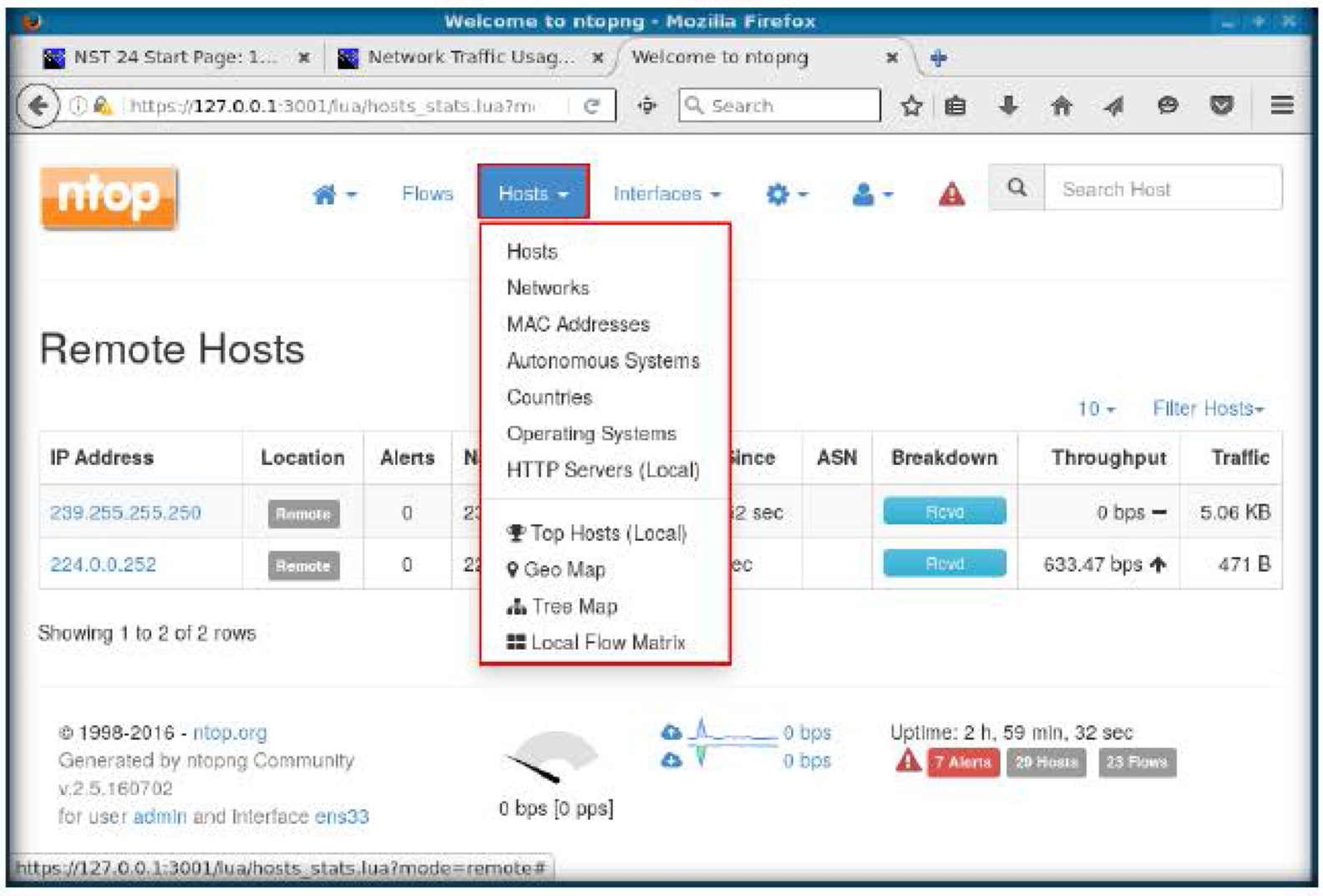



FIGURE 6.19: Examining Hosts


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

26. The various options under the Hosts drop-down list are:
    a. **Networks**: Displays all the networks discovered by ntop.
    b. **MAC Addresses**: Displays a list of Level-2 Addresses for the hosts identified.
    c. **Autonomous Systems**: Displays all autonomous systems discovered by ntop.
    d. **Countries**: Provides all the countries discovered by ntop. Any country can be clicked on to be redirected to a page containing the full list of hosts localized for that country.
    e. **Operating Systems**: Displays a list of the operating systems detected by ntop. They can be clicked on to see the detailed list of hosts.
    f. **HTTP Servers (Local)**: Lists all the local HTTP Servers. Multiple distinct virtual hosts may refer to the same HTTP server IP, which is specified in the second column.
    g. **Top Hosts (Local)**: Provides a host's activity based on time. The page should be kept open in order to allow the graph to dynamically update with freshly collected data for each host.
    h. **Geo Map**: Provides a world map where hosts are arranged according to their geographical position.
    i. **Tree Map**: Provides a tree map of all monitored hosts. By clicking on the hosts it is possible to visit the corresponding 'Host Details' page.
    j. **Local Flow Matrix**: This page visualizes a matrix of local hosts versus local hosts. Each cell contains the amount of traffic exchanged between each.
27. The **Flows** entry in the top toolbar can be selected to view real traffic information on the currently active flows. A flow can be thought of as a logical, bi-directional communication channel between two hosts. Multiple simultaneous flows can exist between the same pair of hosts.
28. To view the network flows, click **Flows** in the ntop menu.




FIGURE 6.20: Viewing Active Flows


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

29. ntop displays all the active flows in the network as shown in the screenshot.

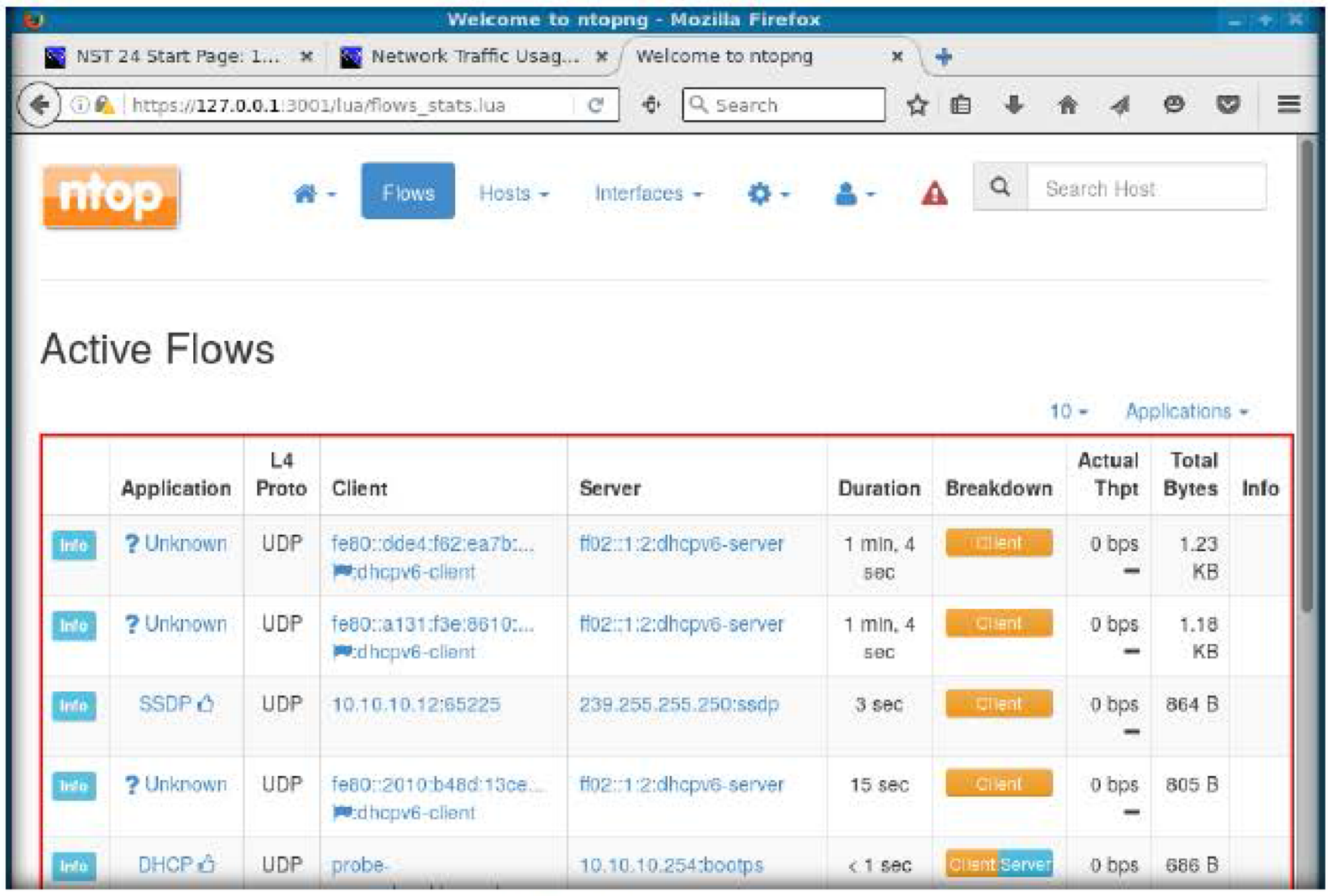



FIGURE 6.21: Examining Active Flows

30. ntop allows you to view the network flows and statistics from the traffic captured by the ntop server.

## Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on securing the wireless network using Linksys router

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

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



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

Lab 7

# Traffic capturing with an OSSIM

*Packet capture is a computer networking term for intercepting the traffic flowing through a network. Once a packet is captured, it is stored temporarily so that it can be analyzed.*

## Lab Scenario

Traffic flowing through a network contains various pieces of data. This data includes traffic associated with various protocols such as http, telnet, tcp, ftp, udp, etc. It is the responsibility of a CND to use packet capturing tools and capture traffic flowing through an organization's network.

ICON KEY

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

## Lab Objectives

This lab will demonstrate how to capture traffic using an OSSIM.

## Lab Environment

To carry out the lab, you need:

- OSSIM virtual machine
- A virtual machine running Windows Server 2008
- A Web browser with an Internet connection
- **Administrative** privileges to run tools

## Lab Duration

Time: 20 Minutes

## Overview of OSSIM

OSSIM (Open Source Security Information Management) is an open source security information and event management system, which comes integrated with a selection of tools designed to aid network administrators in computer security, intrusion detection, and prevention.



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

# Lab Tasks

**TASK 1**

**Logon 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 login screen appears.
3. In the login 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.




FIGURE 7.1: 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 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.

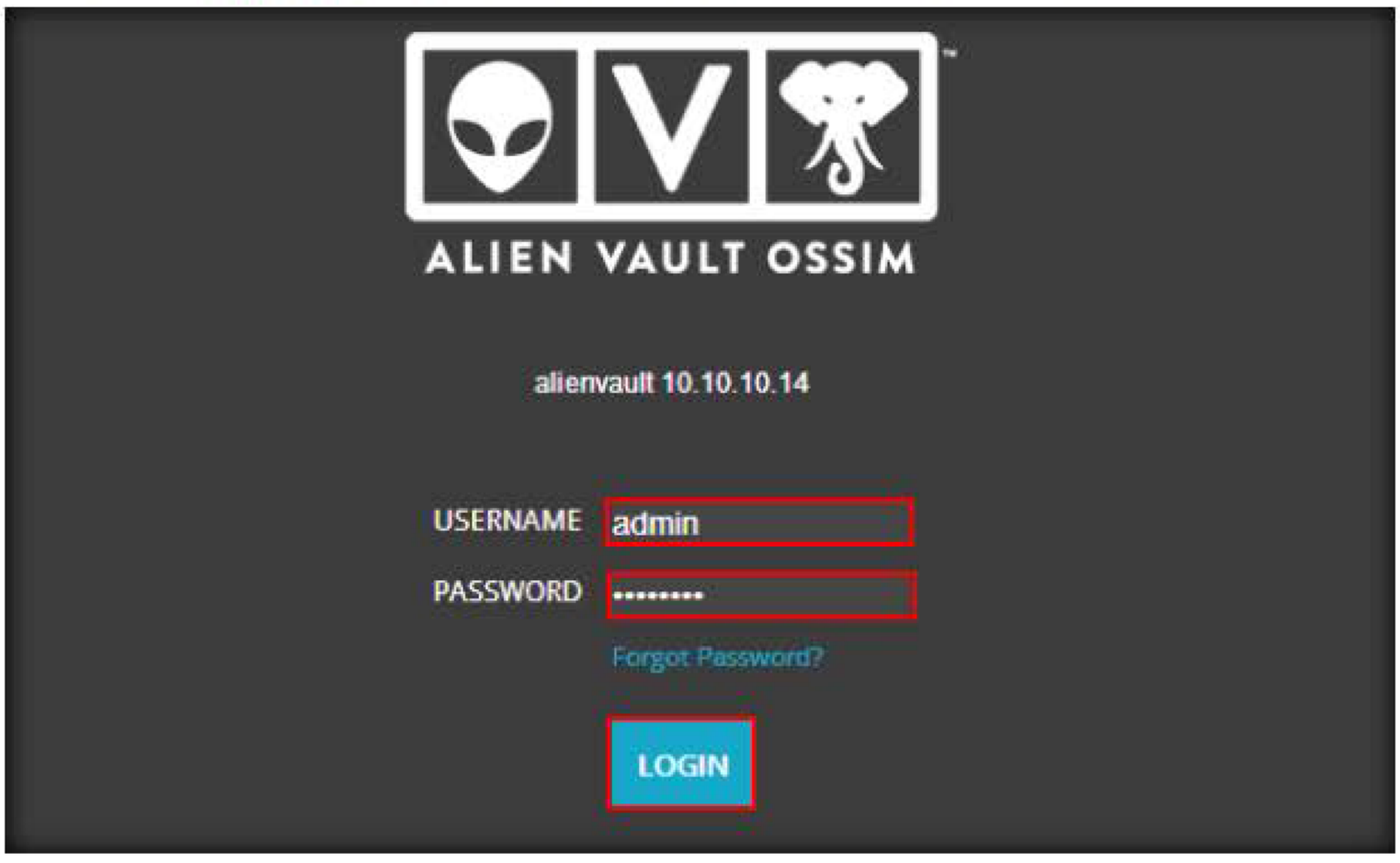



FIGURE 7.2: Logging in to Alien Vault


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

**TASK 2**

**Capture Traffic Flowing from Windows Server 2008**

7. Before starting the Traffic Capture of the Windows Server 2008 machine in OSSIM, log into Windows Server 2008 and browse random webpages to generate traffic.
8. To capture the traffic on the host, hover the mouse cursor on **ENVIRONMENT** and click **TRAFFIC CAPTURE**.




FIGURE 7.3: Capturing the Traffic

9. In the Destination field type the Windows Server 2008 or select from the Assets list by expanding and click **LAUNCH CAPTURE**.

   **Note**: If you receive any error while capturing the traffic, switch to the OSSIM virtual machine and select the Reboot Appliance option to restart the machine.

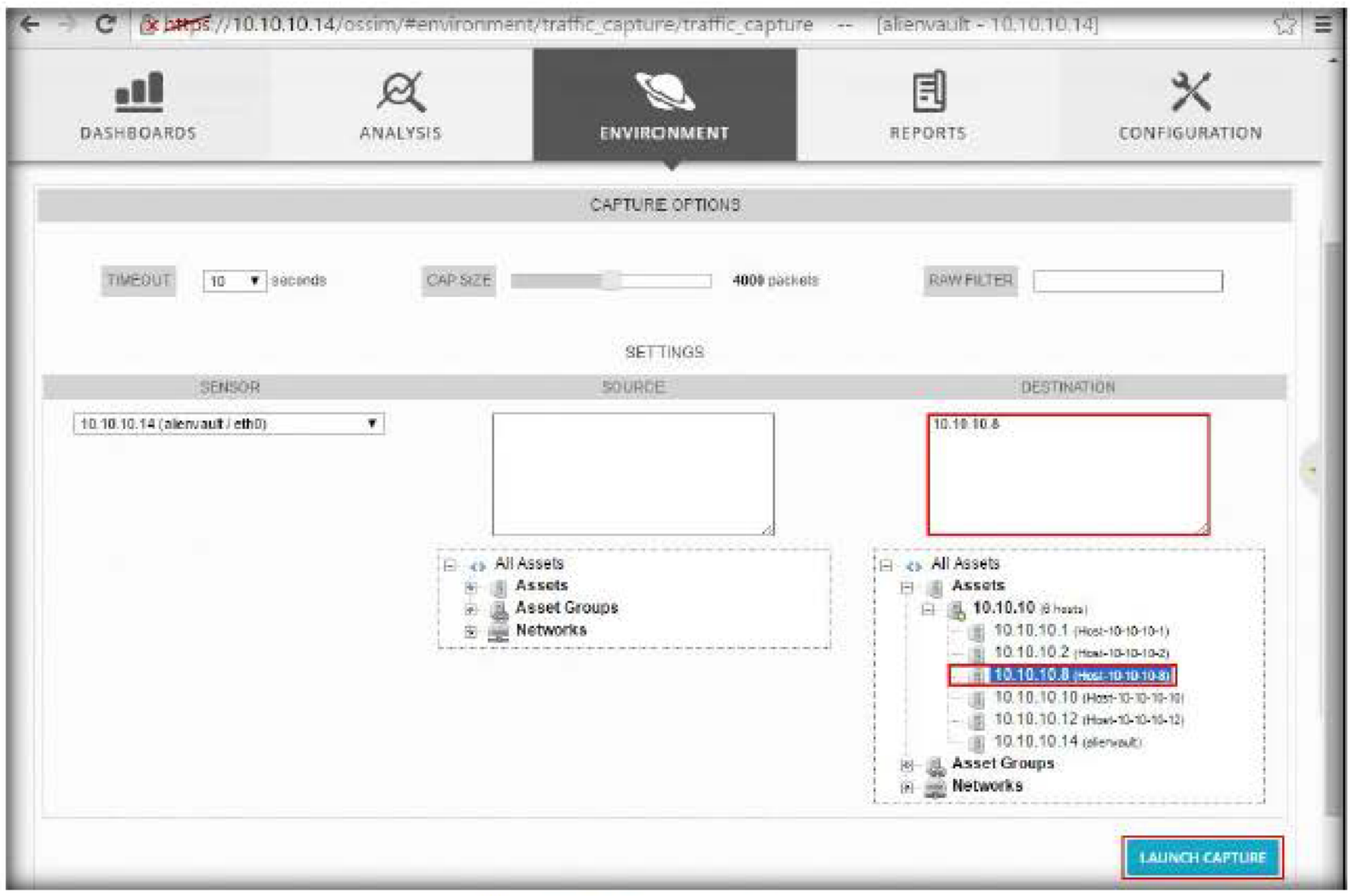



FIGURE 7.4: Launching the Capture



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

10. OSSIM starts capturing the network traffic, which is generated by Windows Server 2008.

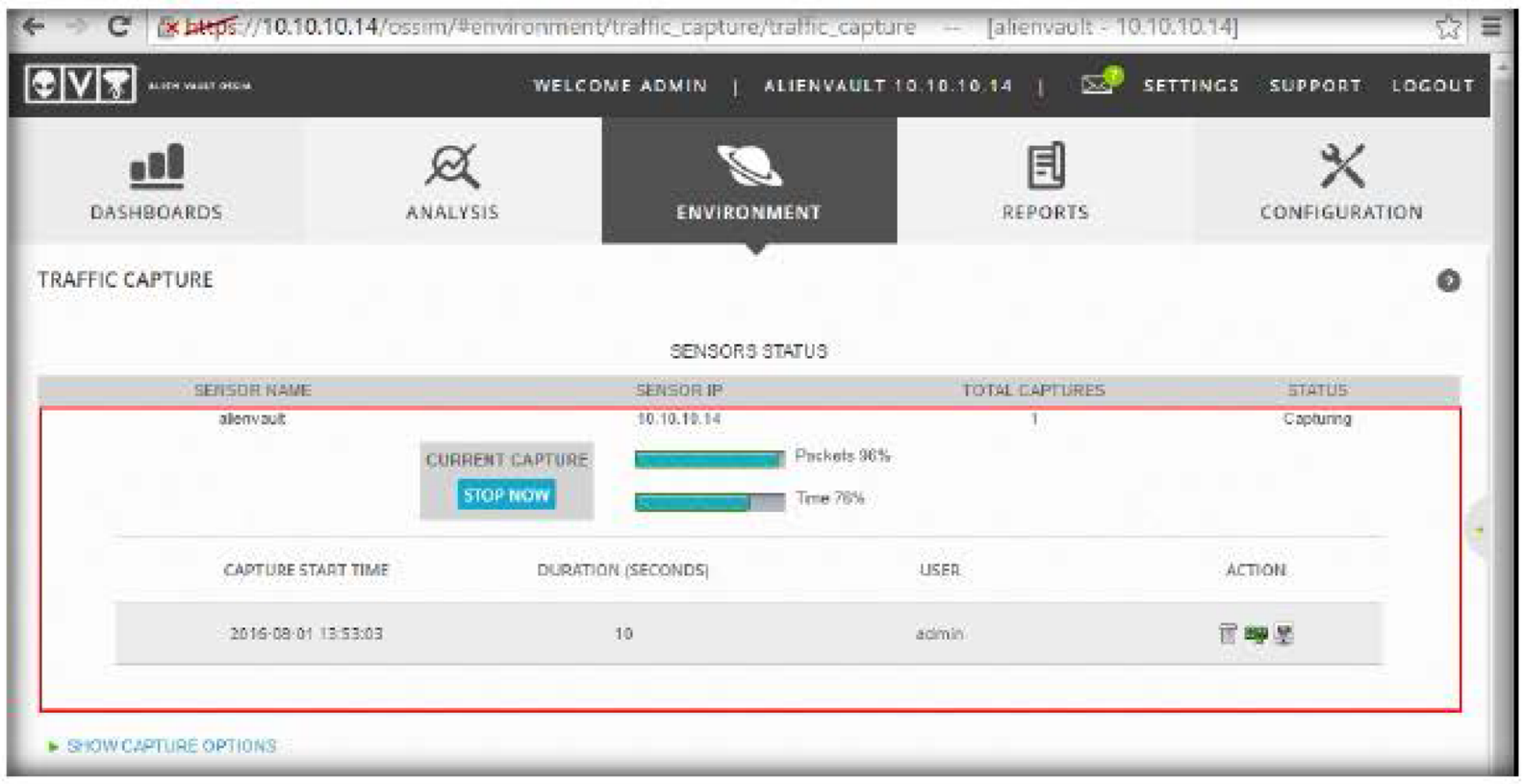



FIGURE 7.5: Sensor Status

11. Wait for the capture to complete. In the case of multiple captures, the latest capture report is present at the bottom.




FIGURE 7.6: Capture Reports

12. Click **View Payload** under **ACTION** as shown in the screenshot.




FIGURE 7.7: Viewing Capture Report


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

13. A new tab with the name of **SharkVault** opens. You can view the captured traffic here.

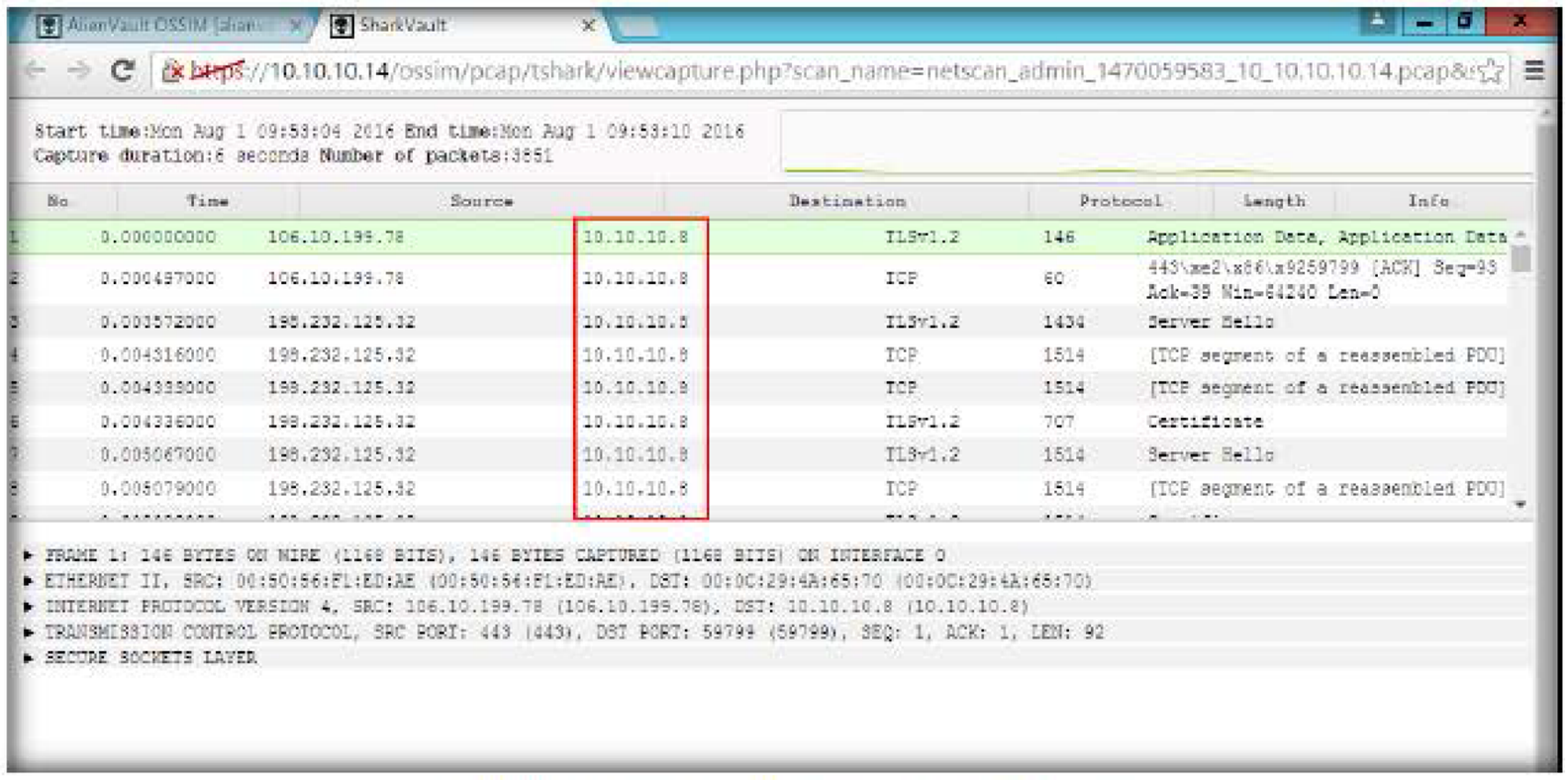



FIGURE 7.8: Shark Vault Showing Captured Packets

14. Click the **Graphs** button in the extreme right corner of SharkVault to view a graphical representation of the captured traffic.




FIGURE 7.9: Graphical View

15. The **Graphs: All Traffic** pop-up appears, after observing the traffic; you can close the Graphs pop-up and SharkVault tab.

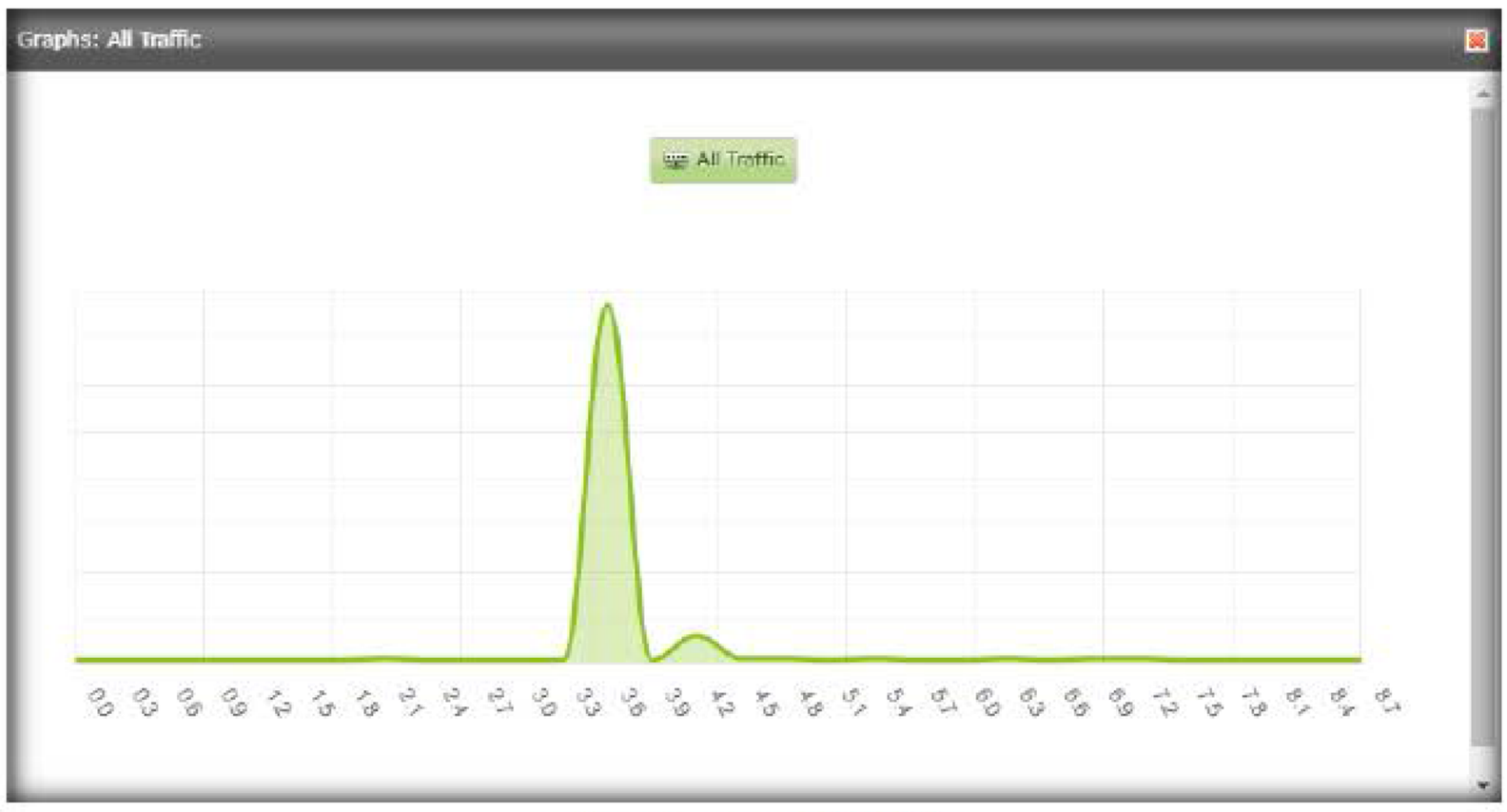



FIGURE 7.10: Graphical View


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

# 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 |



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

Lab 8

# Network Traffic Analysis Using Capsa

*Capsa is a network analyzer which helps network specialists detect and troubleshoot network problems, improve network performance, and enhance network security.*

## Lab Scenario

As the number of hosts in a network increases, the chances for anomalies increase as well. To avoid such anomalies, a chief network defender needs to deploy a network analyzer which can perform packet capture, accurate protocol decoding and analysis, and automatic diagnosis of network events. Using this data, you can detect and troubleshoot network problems to improve network performance and enhance network security.

ICON KEY

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

## Lab Objectives

This lab will demonstrate how to use network analyzers for network maintenance.

## Lab Environment

To carry out the lab, you need:

- Register at the link given below to get the setup file for the Capsa Enterprise Edition demo version

  http://www.colasoft.com/download/products/download_capsa.php

- If you decide to download the latest version, the screenshots shown in the lab might differ
- A computer running Windows Server 2012 as a Host (Administrator) machine
- A virtual machine running Windows 10
- A Web browser with an Internet connection
- **Administrative** privileges to run tools

You can download Wireshark from http://www.wireshark.org.



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

# Lab Duration

Time: 25 Minutes

# Overview of Network Analysis

Network/packet analysis is a process of capturing the traffic flowing through a network and examining each packet to detect network anomalies.

# Lab Tasks

**TASK 1**

**Download and Install Capsa**

1. Log on to the **Windows Server 2012** virtual machine
2. Go to http://www.colasoft.com/download/products/download_capsa.php
3. Enter your details, uncheck the **Subscribe to our newsletter** option, and click **FREE TRIAL DOWNLOAD**.

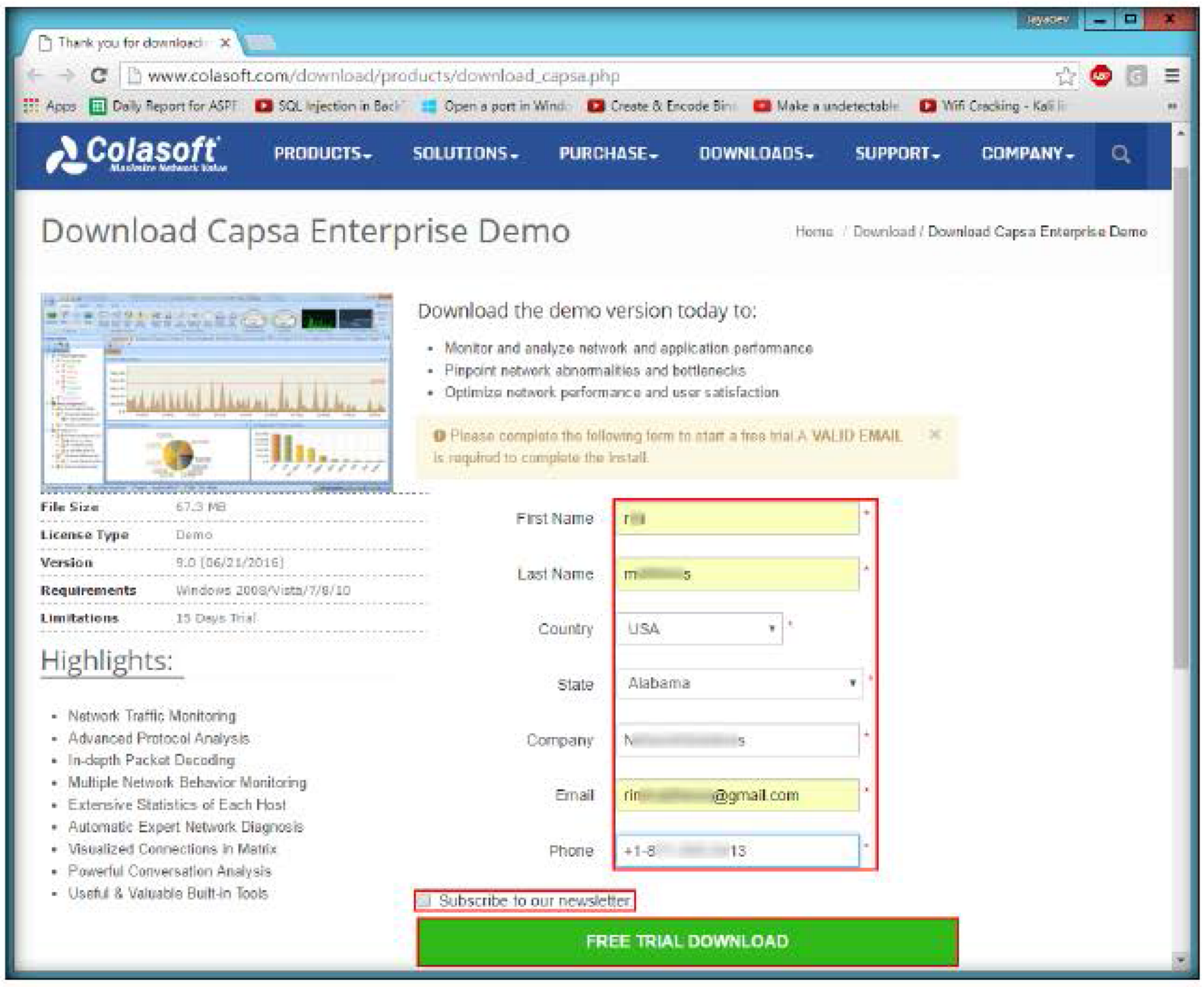



FIGURE 8.1: Registering for Capsa



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

4. Once you click **FREE TRIAL DOWNLOAD**, the system prompts you to save the installer through a **Save As** window. Save the installer on the **Desktop**.

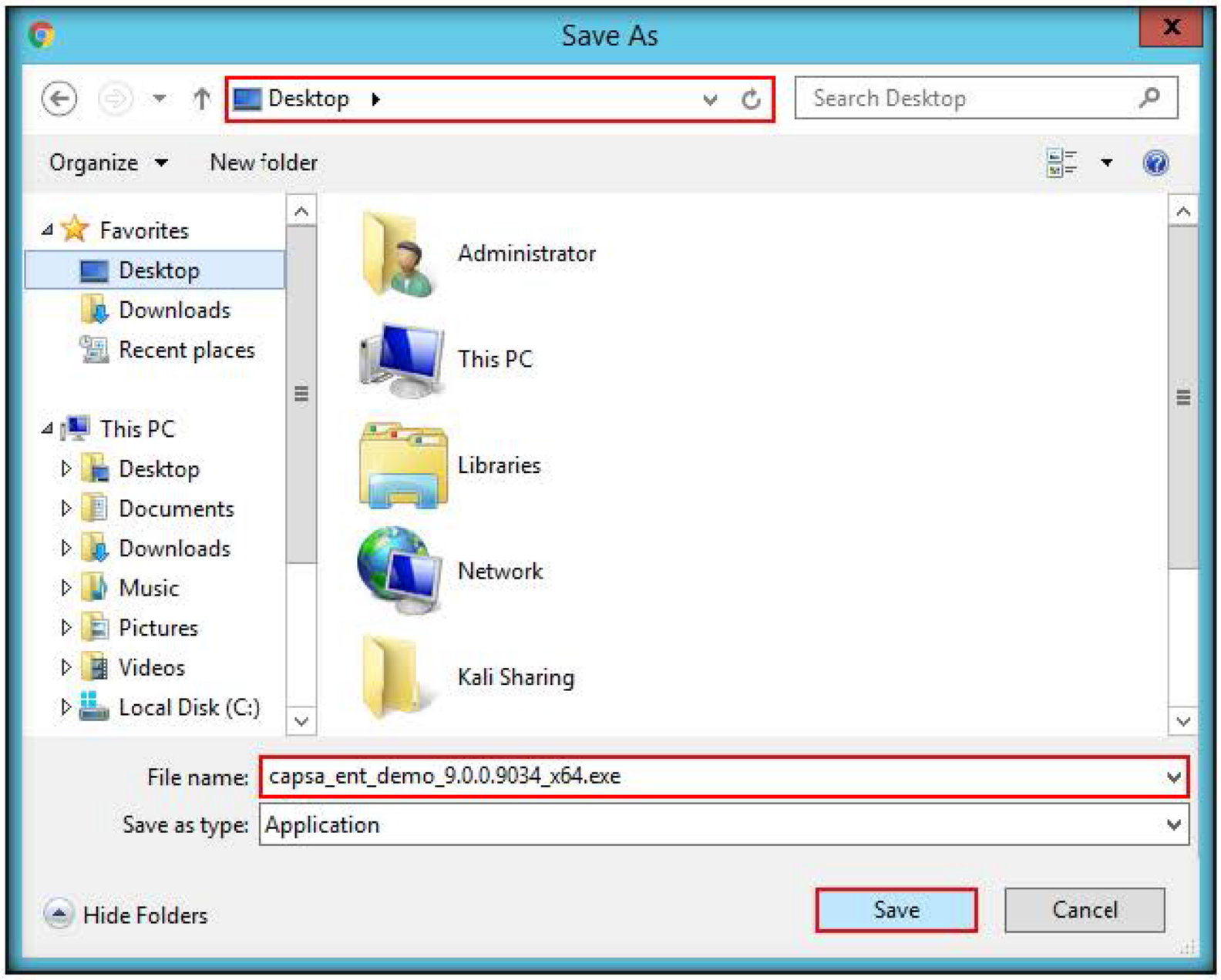



FIGURE 8.2: Downloading Colasoft tool

5. Navigate to your download location, double-click the installer file and follow the wizard installation steps to install the application.

   **Note:** In this lab, the version of Capsa downloaded is **capsa_ent_demo_9.0.0.9034_x64.exe**. If you are running this lab using a different version of Capsa, screenshots and steps may differ in your lab environment.

   During installation, if a **Windows Security** pop-up appears, click **Install**.

   In the final step of installation, check the **Launch Program** option and click **Finish**.


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

6. The **Colasoft Capsa 9 Enterprise Demo** window appears, click **OK**.

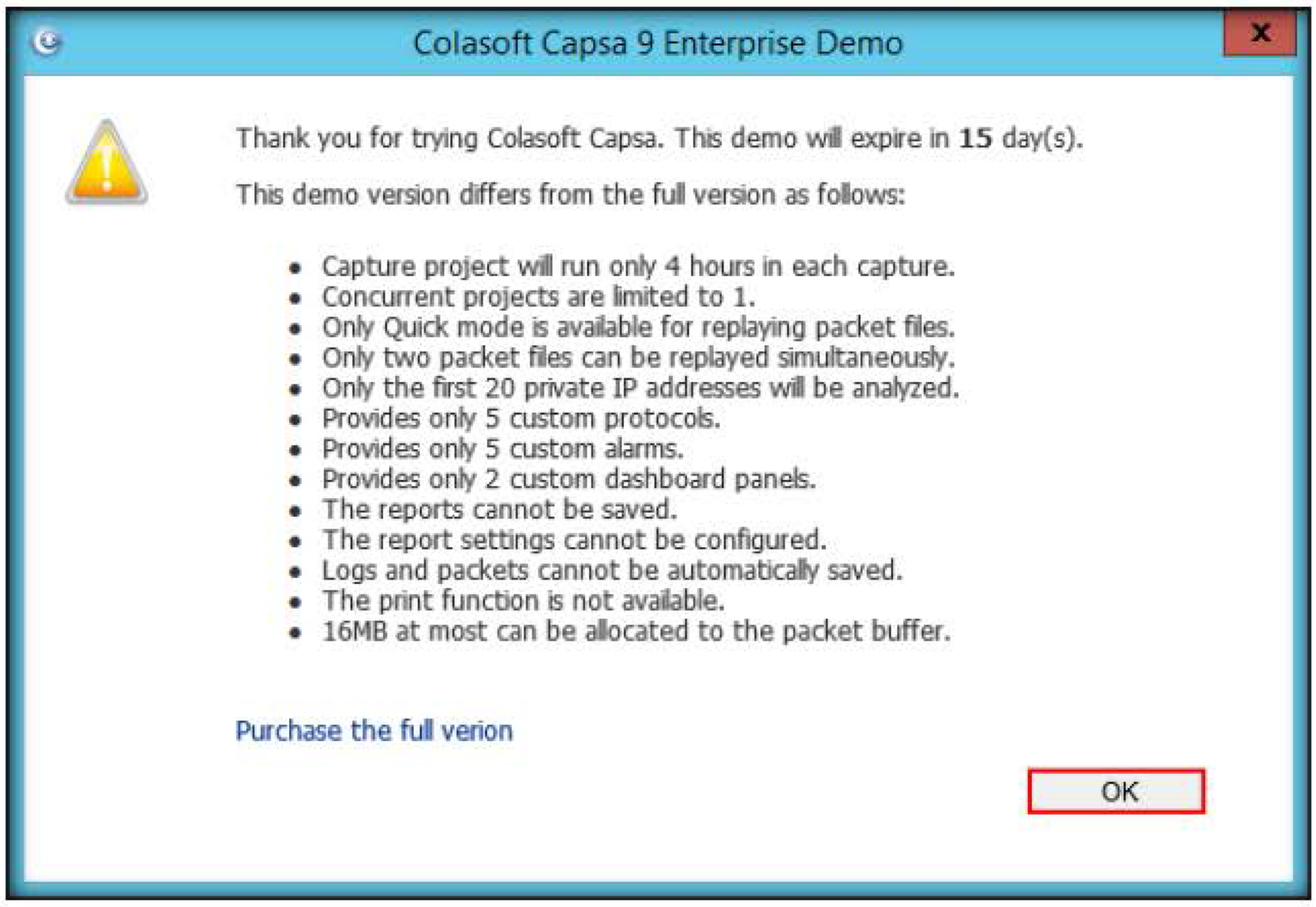



FIGURE 8.3: Colasoft capsa demo

**TASK 2**

**Begin Traffic Monitor**

7. The **Colasoft Capsa 9 Enterprise Demo** window appears as shown in the screenshot.

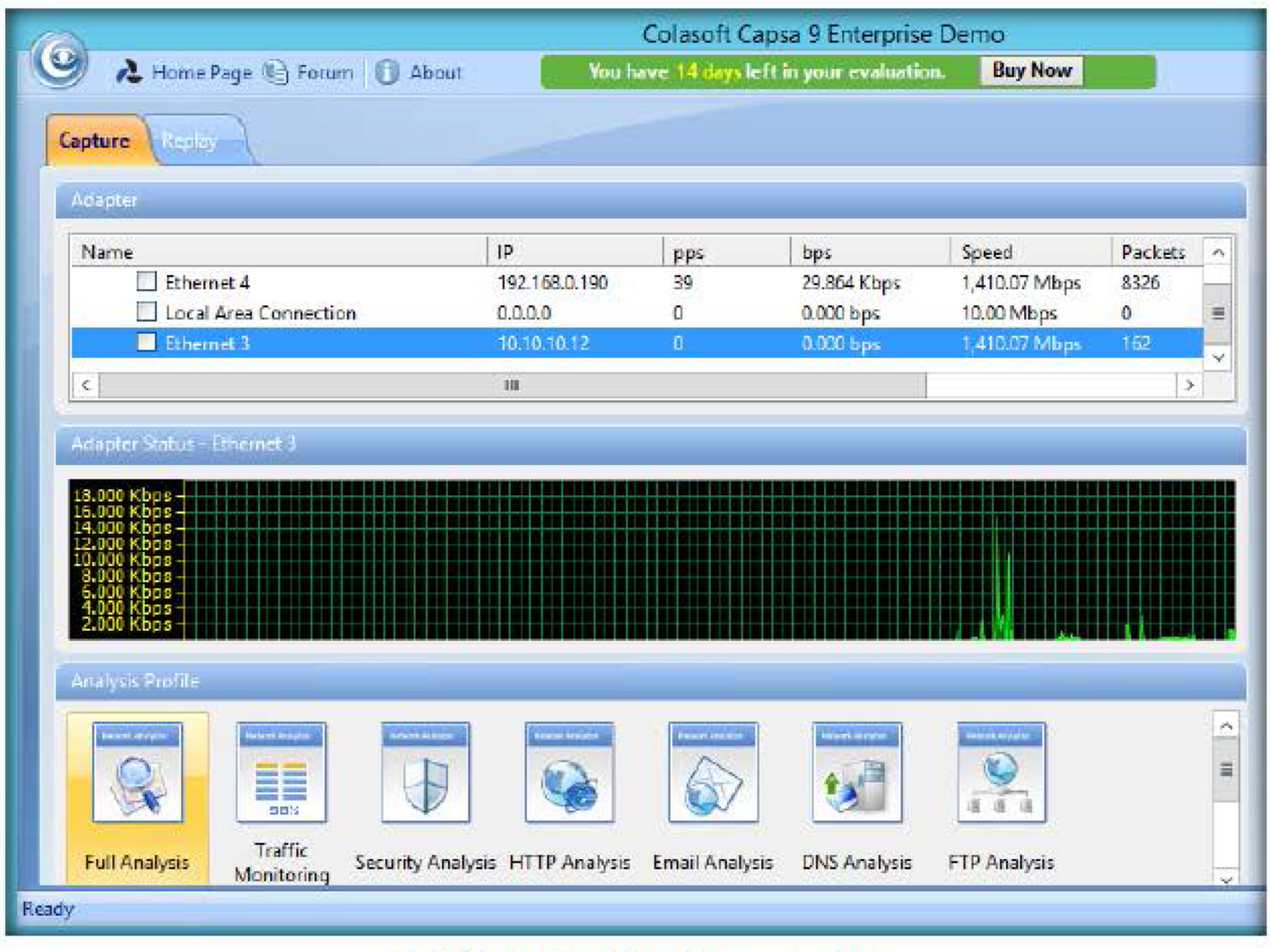



FIGURE 8.4: Colasoft capsa Enterprise Demo


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

8. In the **Analysis Profile** section, click **Traffic Monitoring**.

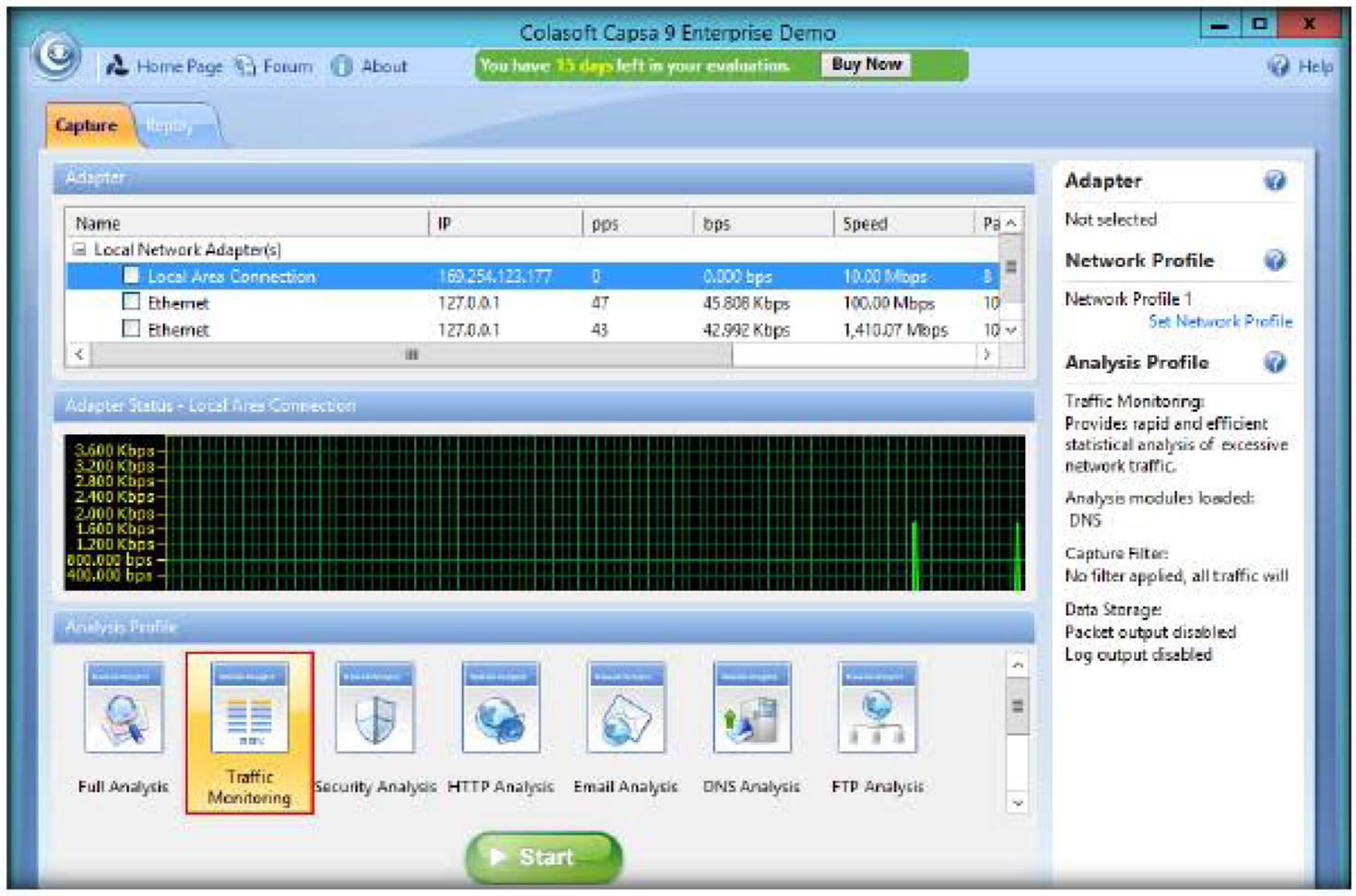



FIGURE 8.5: Navigating to Traffic monitoring profile

9. Under the **Capture** tab, check the adapter associated with the IP Address of the **Window Server 2012** virtual machine (i.e., **10.10.10.12**).

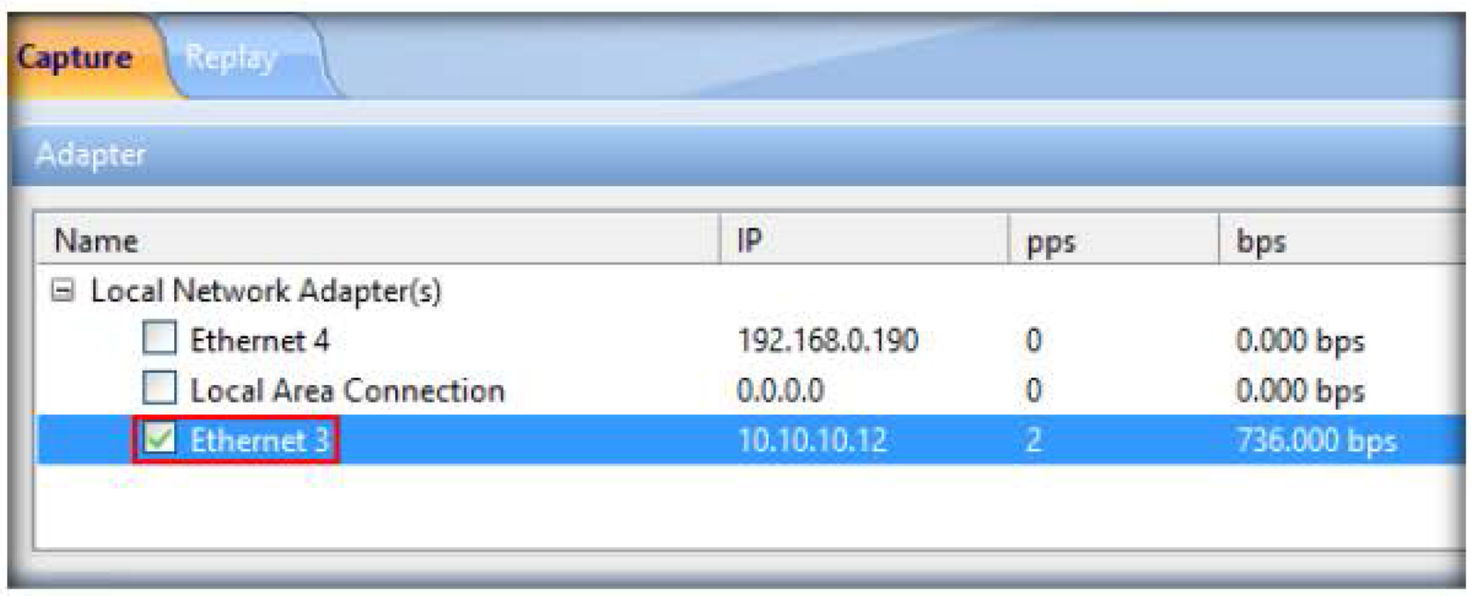



FIGURE 8.6: Selecting network interfaces

10. Scroll down and click **Start**.

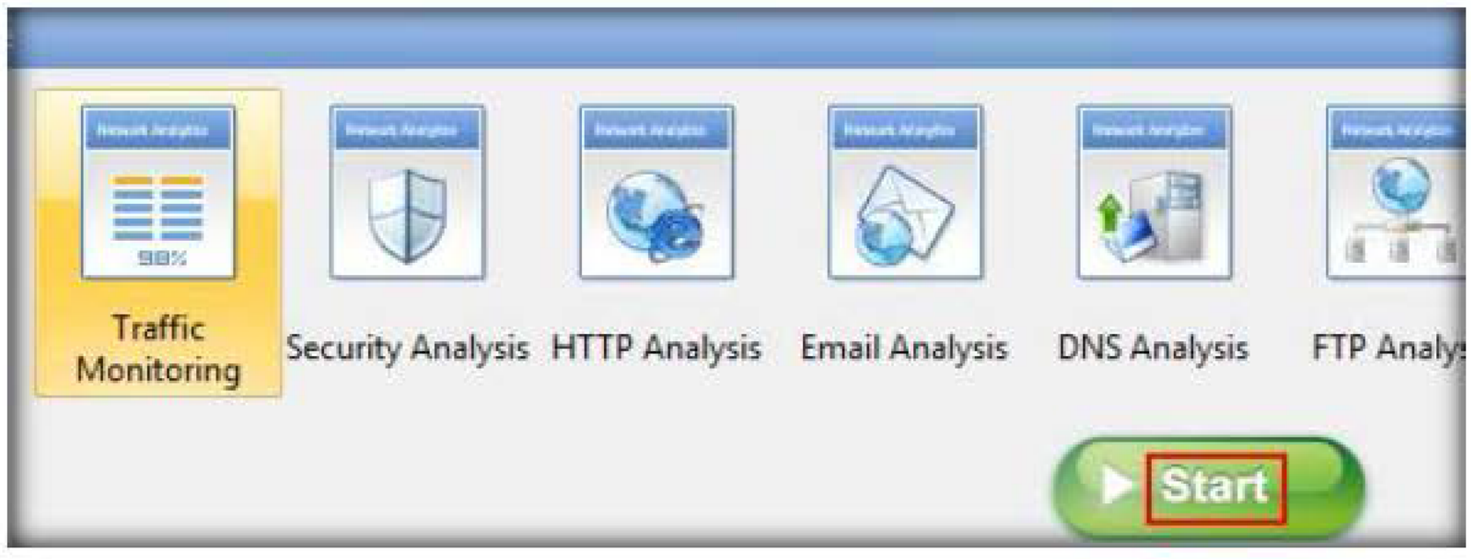



FIGURE 8.7: starting the traffic monitoring


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

11. Launch the **Windows 10** machine and log in as the Local Administrator. Browse some sites to generate traffic.
12. After a few minutes, click **Stop**.




FIGURE 8.8: stopping the traffic

13. Switch back to **Windows Server 2012**.

**TASK 3**

**Examine Network Traffic**

14. You can view the total traffic size in the **Total Traffic by Bytes** widget.

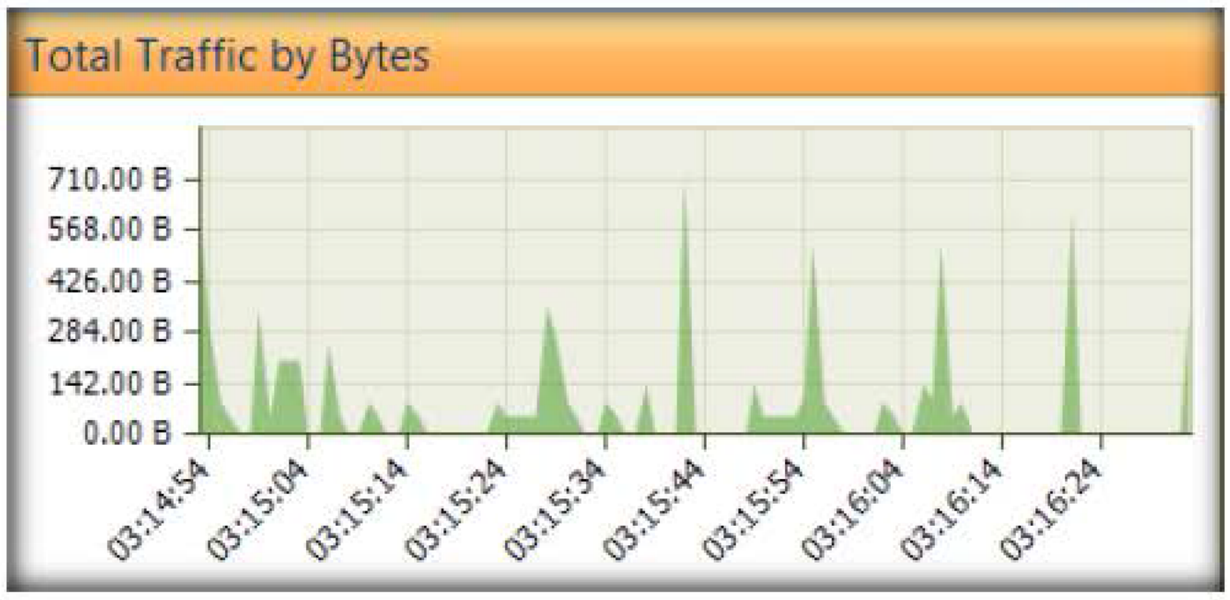



FIGURE 8.9: Viewing total traffic

15. You can view the IP addresses which consumed the maximum amount of memory in the **Top IP addresses by Bytes** widget.

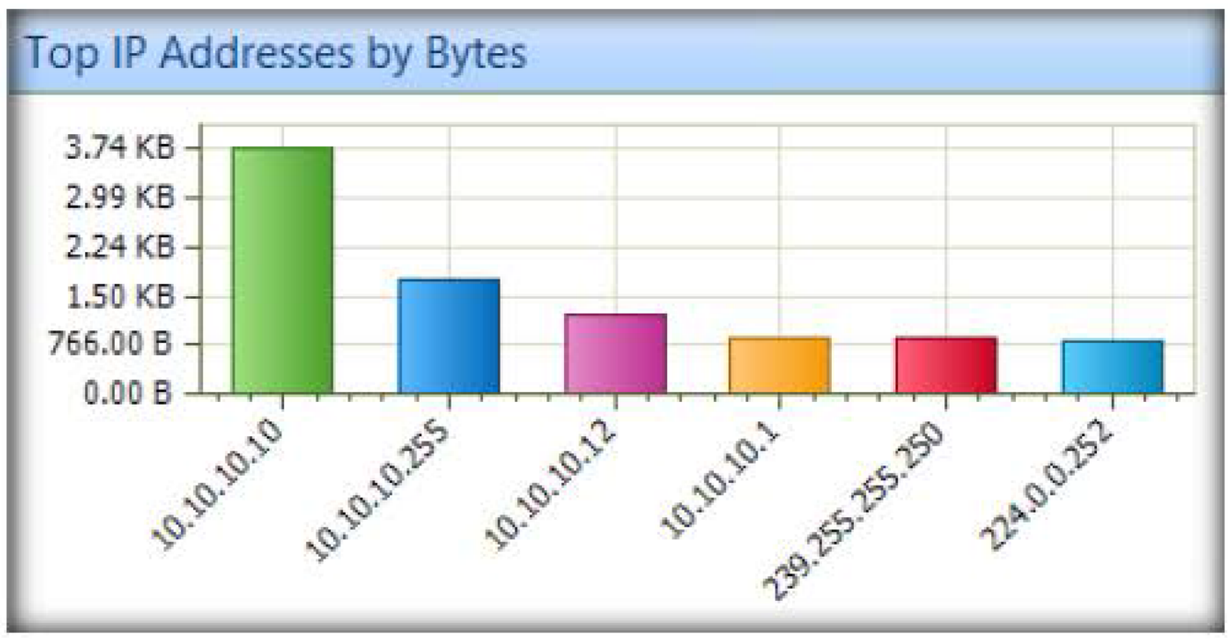



FIGURE 8.10: Viewing IP address in bytes


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

16. The protocol applications which consumed the most memory is available in **Top Application Protocols by Bytes** widget.

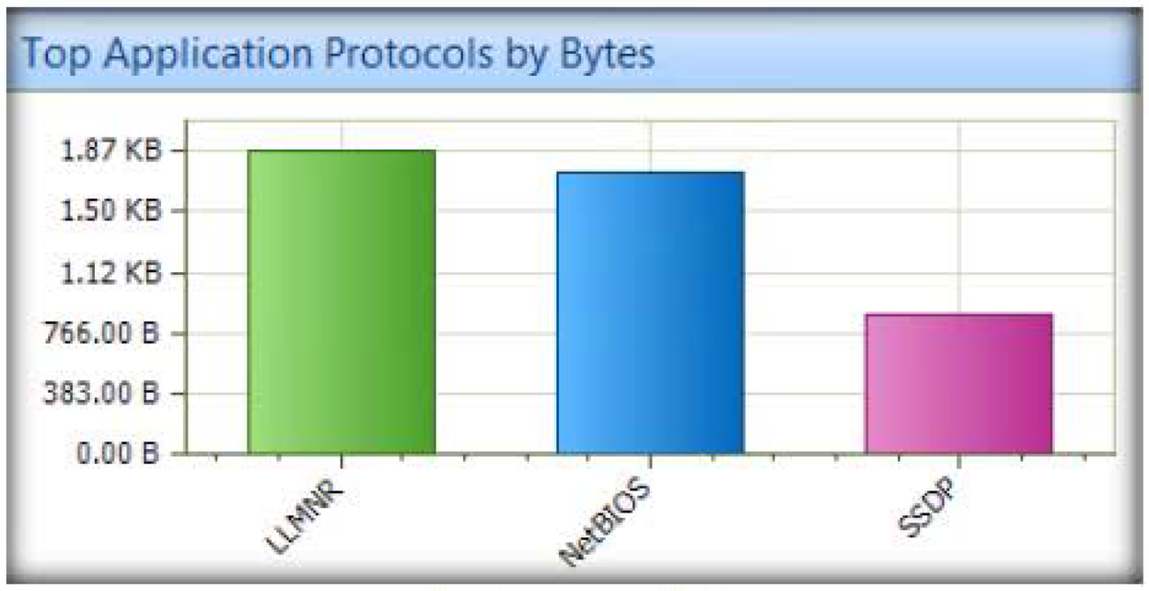



FIGURE 8.11: Protocols by bytes

17. Click the **Packets** tab.

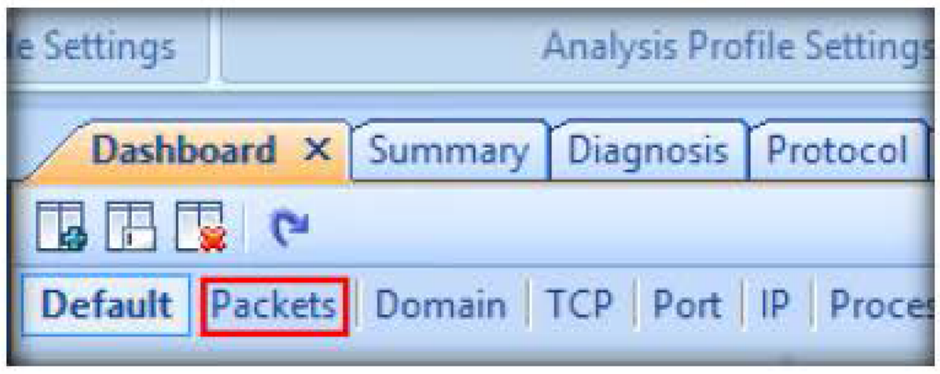



FIGURE 8.12: Navigating to packets tab

18. The **Global** widget is available in Packet tab.

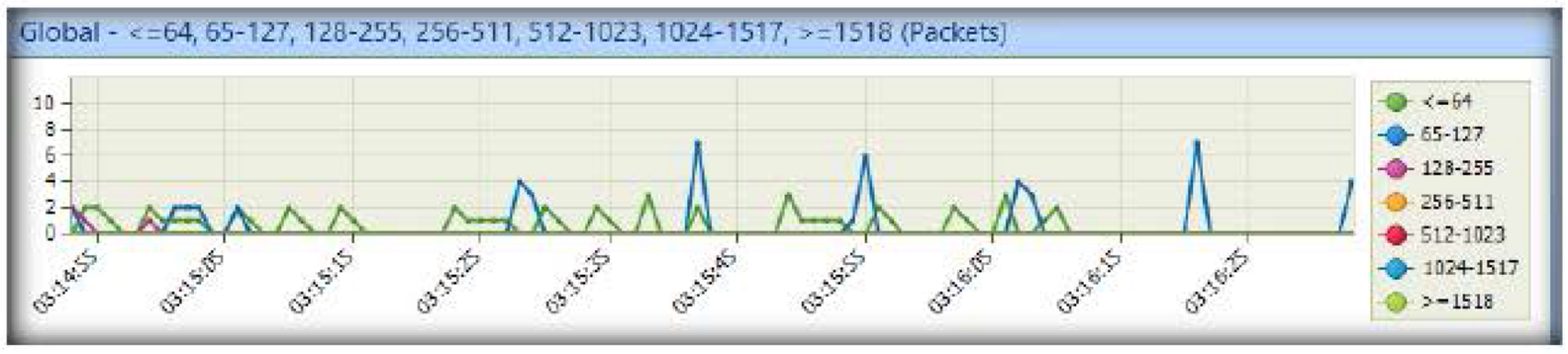



FIGURE 8.13: Global widget

19. The **Global - Broadcast, Multicast (packets)** widget shows the packets which were broadcast and multicast.

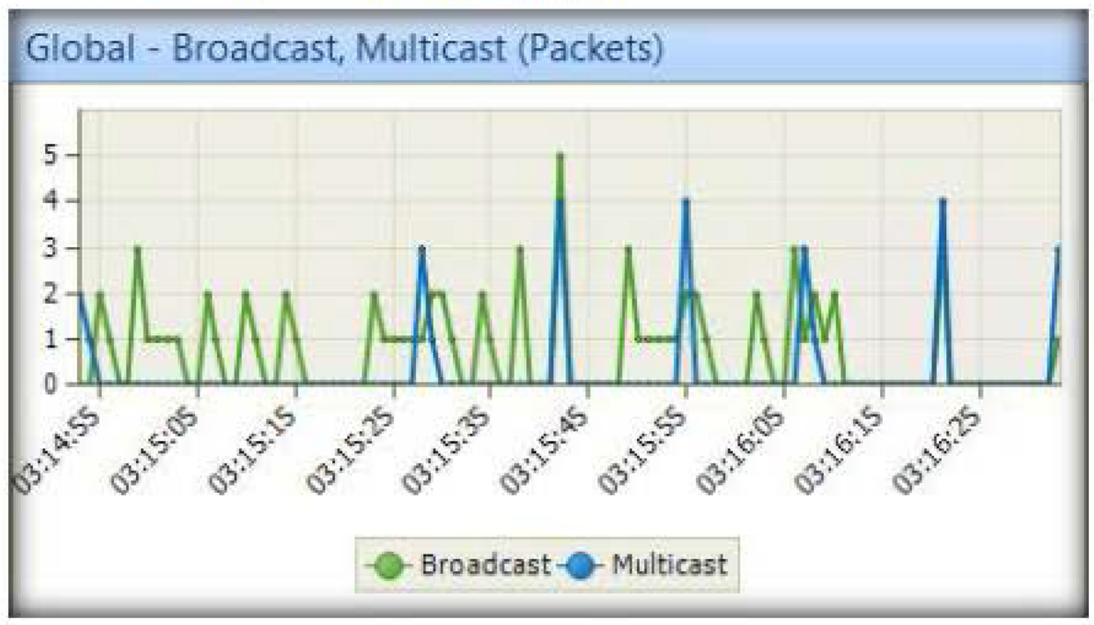



FIGURE 8.14: Global multicast and broadcast packets



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

20. The **Domain** tab has widgets if more than one domain is used.
21. Click the **TCP** tab to view various TCP flag related statistics.

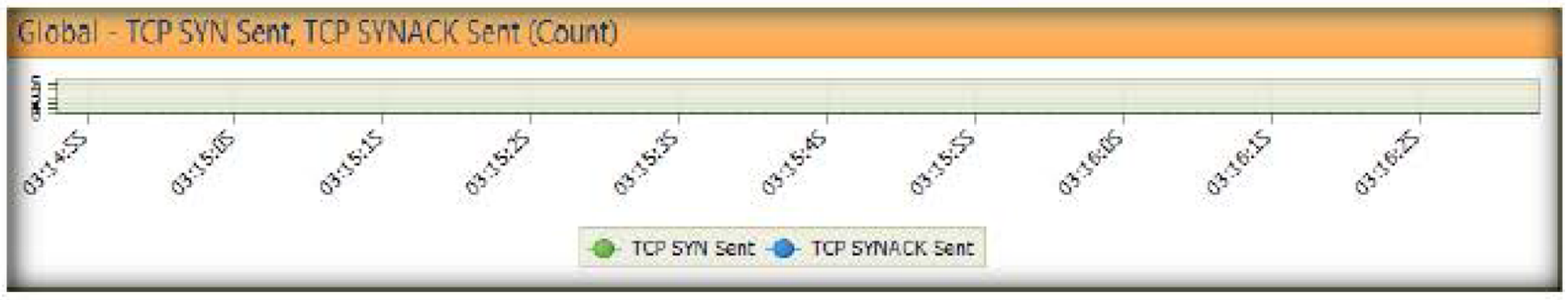



FIGURE 8.15: Global TCP SYN and ACK packets

22. You can also view widgets that show when the TCP FIN flag and RST flags are set.
23. Click the **Port** tab. You can view the top ports used in the network traffic.

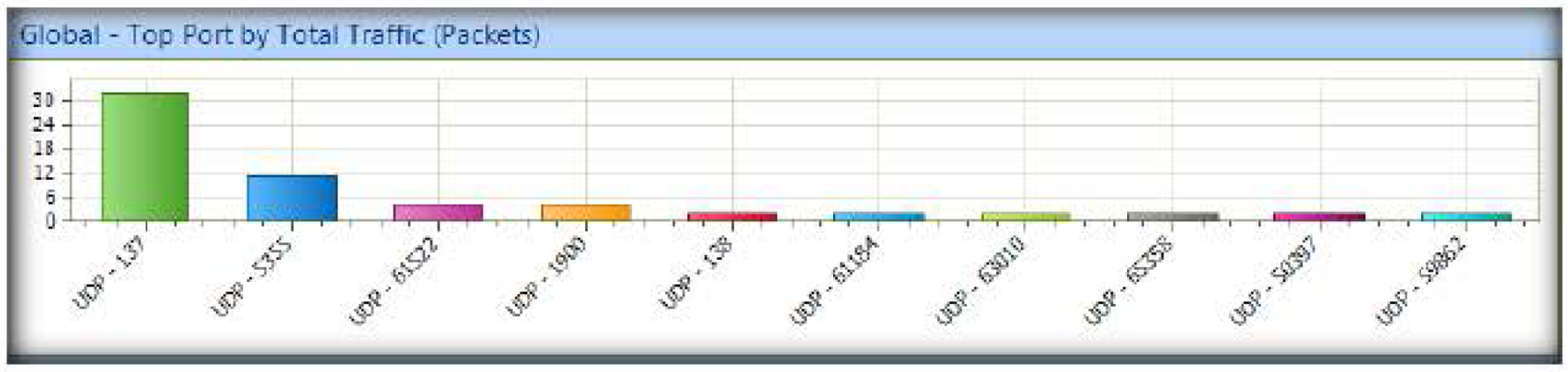



FIGURE 8.16: Global ports used

24. You can also view a separate widget each for TCP and UDP ports used. The UDP port widget is shown here.

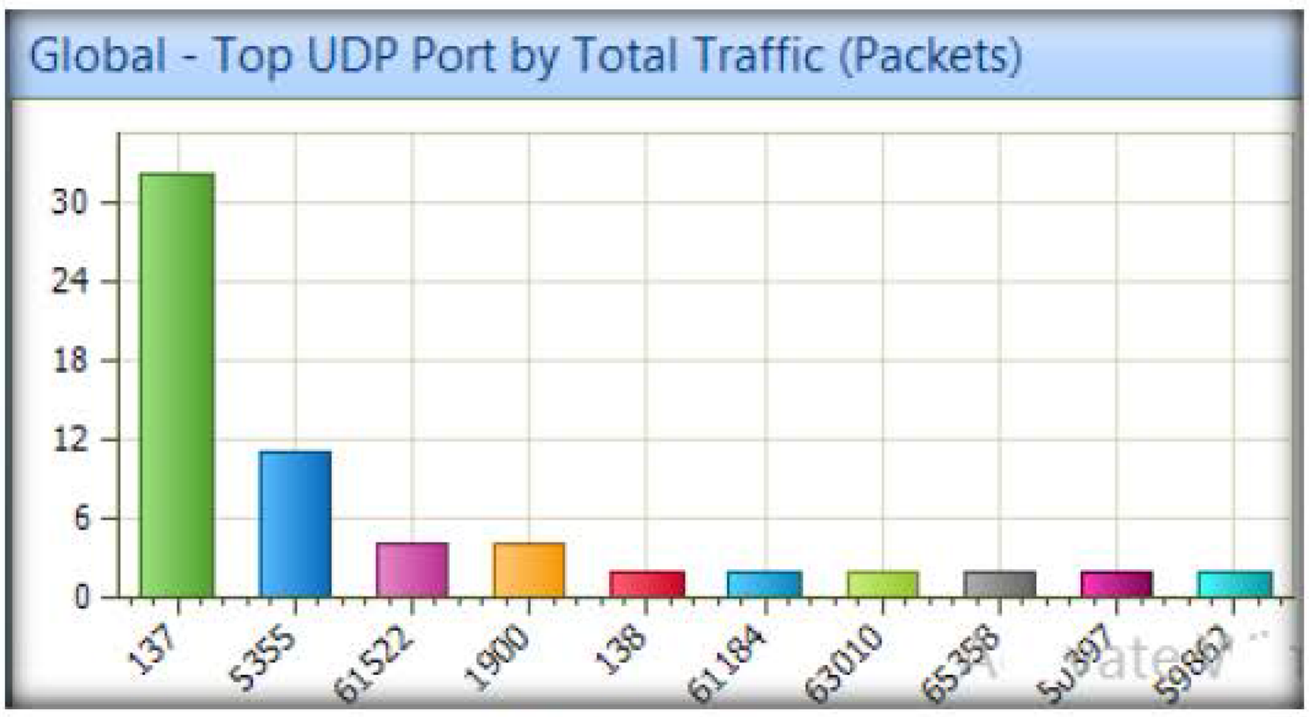



FIGURE 8.17: Global UDP ports used

25. Click the **IP** tab. You can view the top IP groups which generated the most traffic.

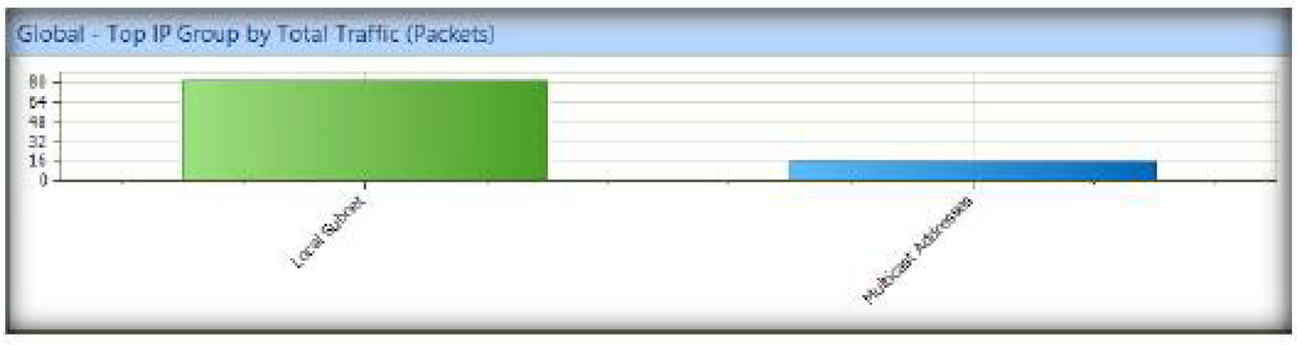



FIGURE 8.18: Global IP traffic


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

26. You can also view the top local IP address, which generated the most of the traffic.

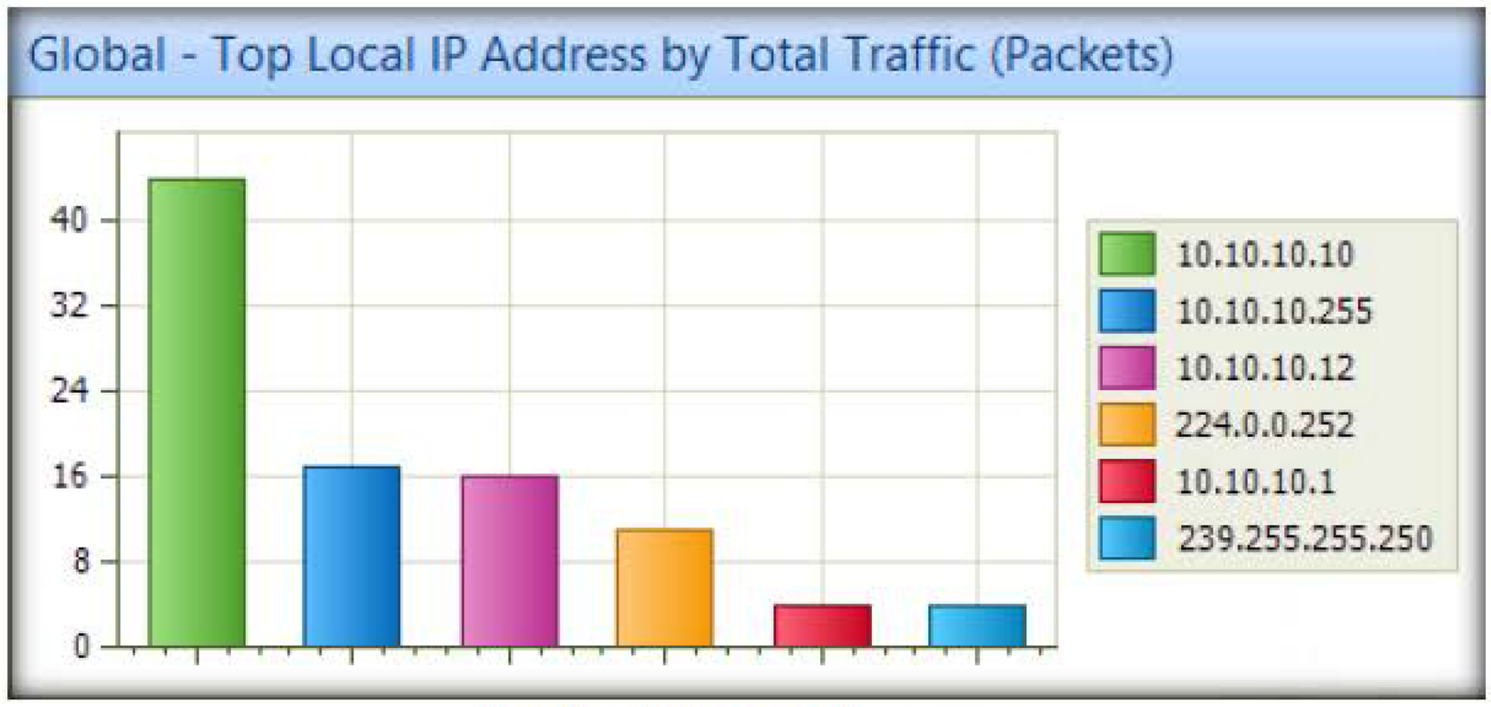



FIGURE 8.19: Local IP with most traffic

27. Next, click the **Close Project** button to close the window.

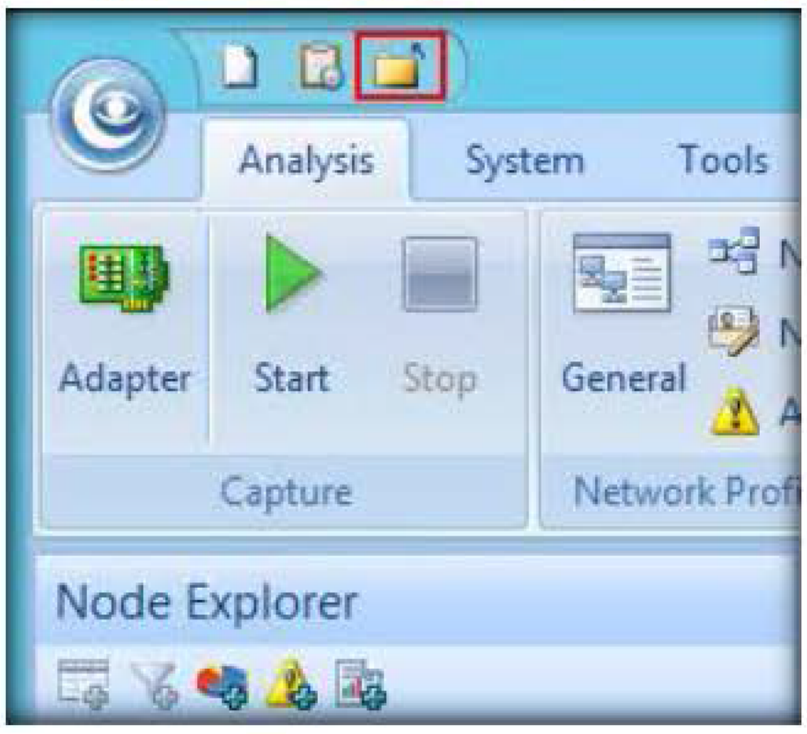



FIGURE 8.20: Closing the project

28. If a **Colasoft Capsa** pop up window appears, click **No**.

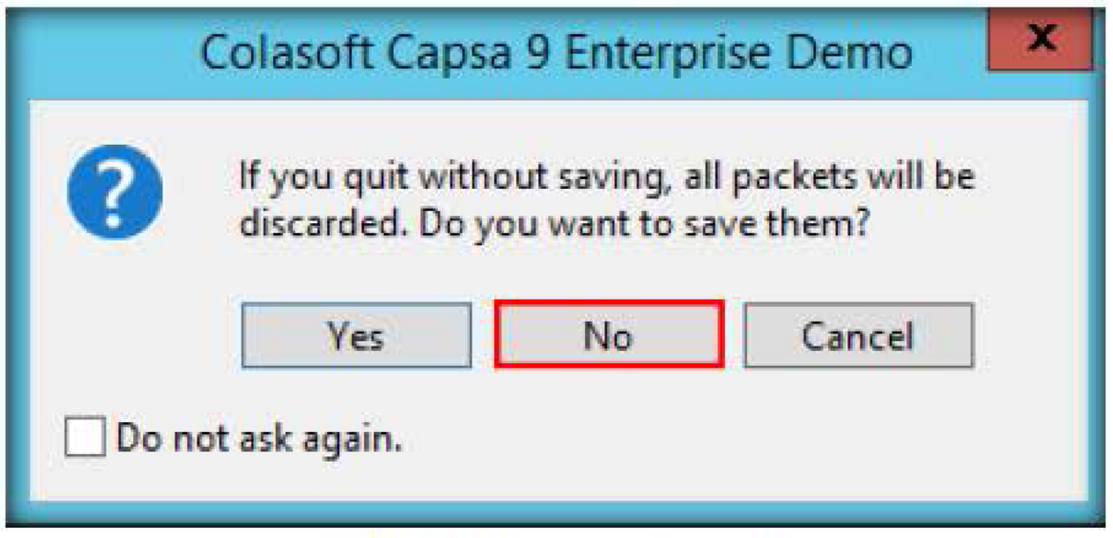



FIGURE 8.21: Not saving the packets


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

**TASK 4**

**Perform Security Analysis**

29. Click **Security Analysis** and click **Start**.

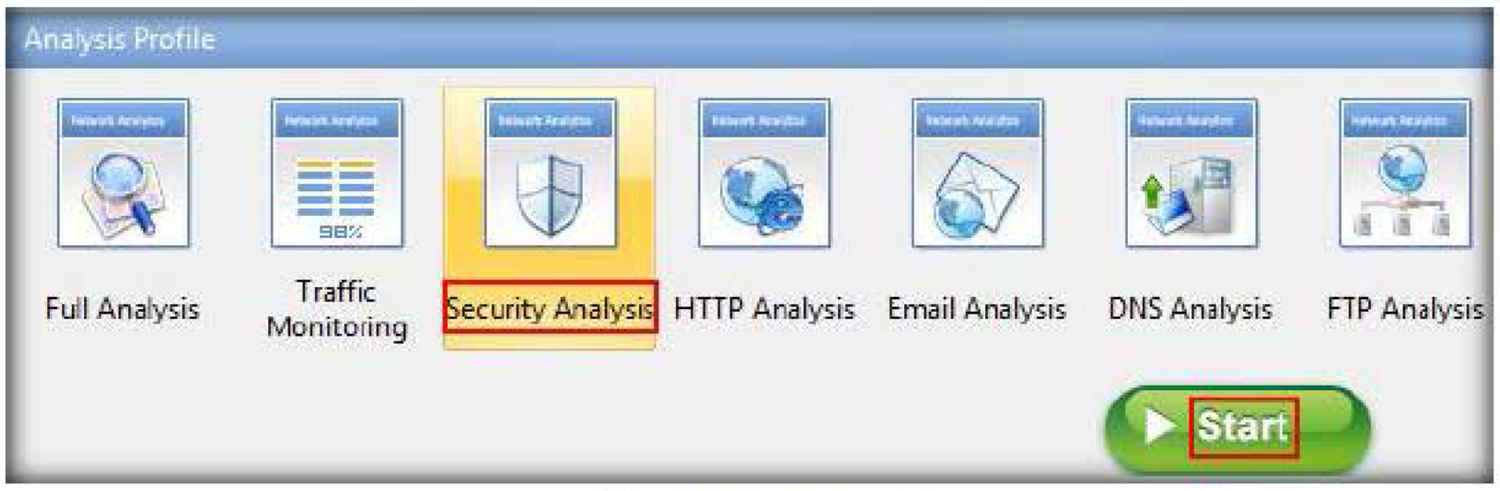



FIGURE 8.22: Security analysis

30. Switch to the **Windows 10** machine and browse web sites to generate traffic.
31. Switch back to **Windows Server 2012** and click **Stop** to stop the packet capture.




FIGURE 8.23: stopping the traffic

32. The **Summary** window appears. You can see a summary of the attacks or suspicious activities.

**TASK 5**

**Examine the Output**

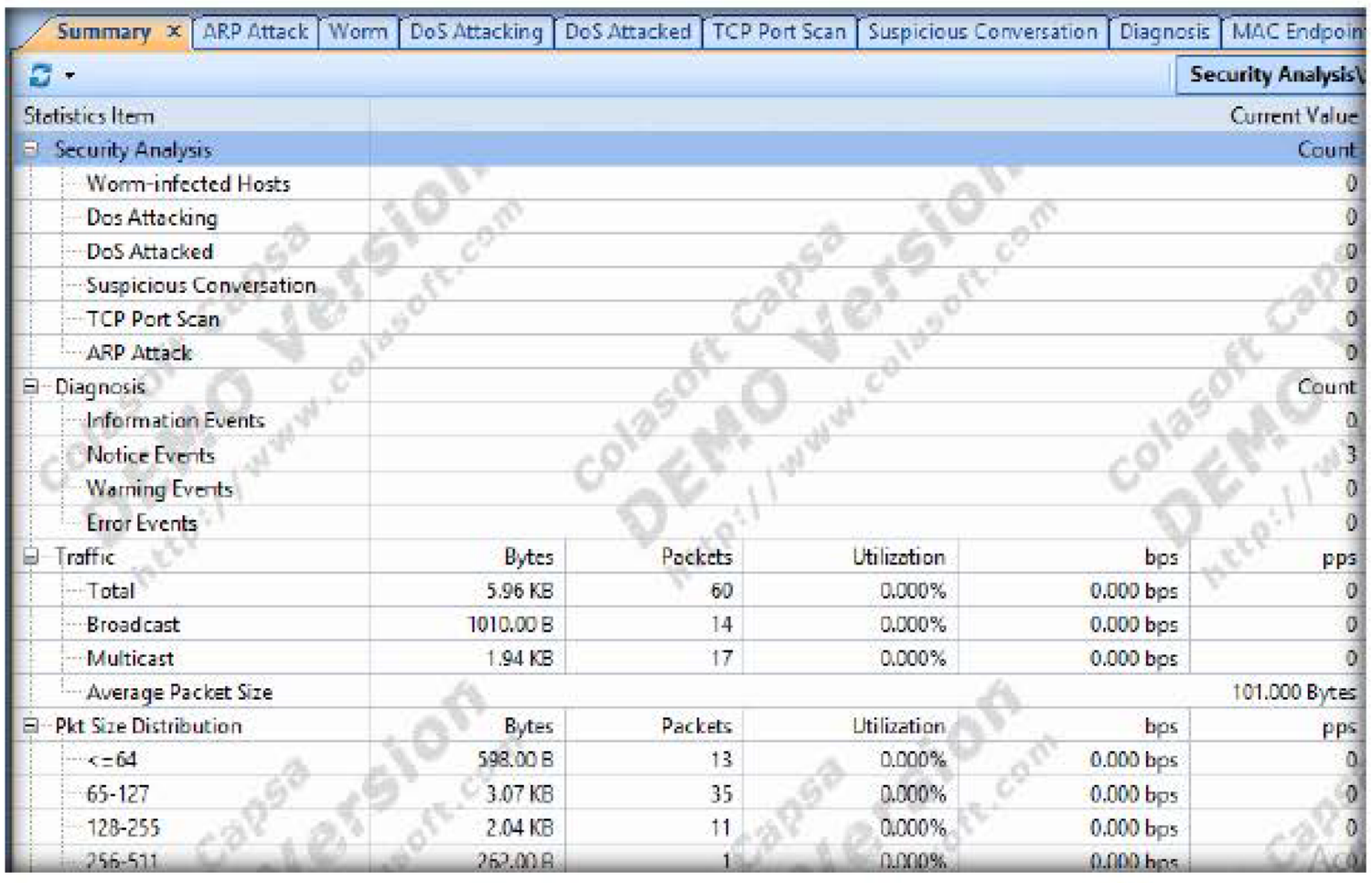



FIGURE 8.24: Summary of security



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

33. The next few tabs such as **ARP Attack**, **Worm**, **DoS Attacking** and so on show data only if relevant attack packets are found.

34. Click the **Diagnosis** tab to view any network defects.

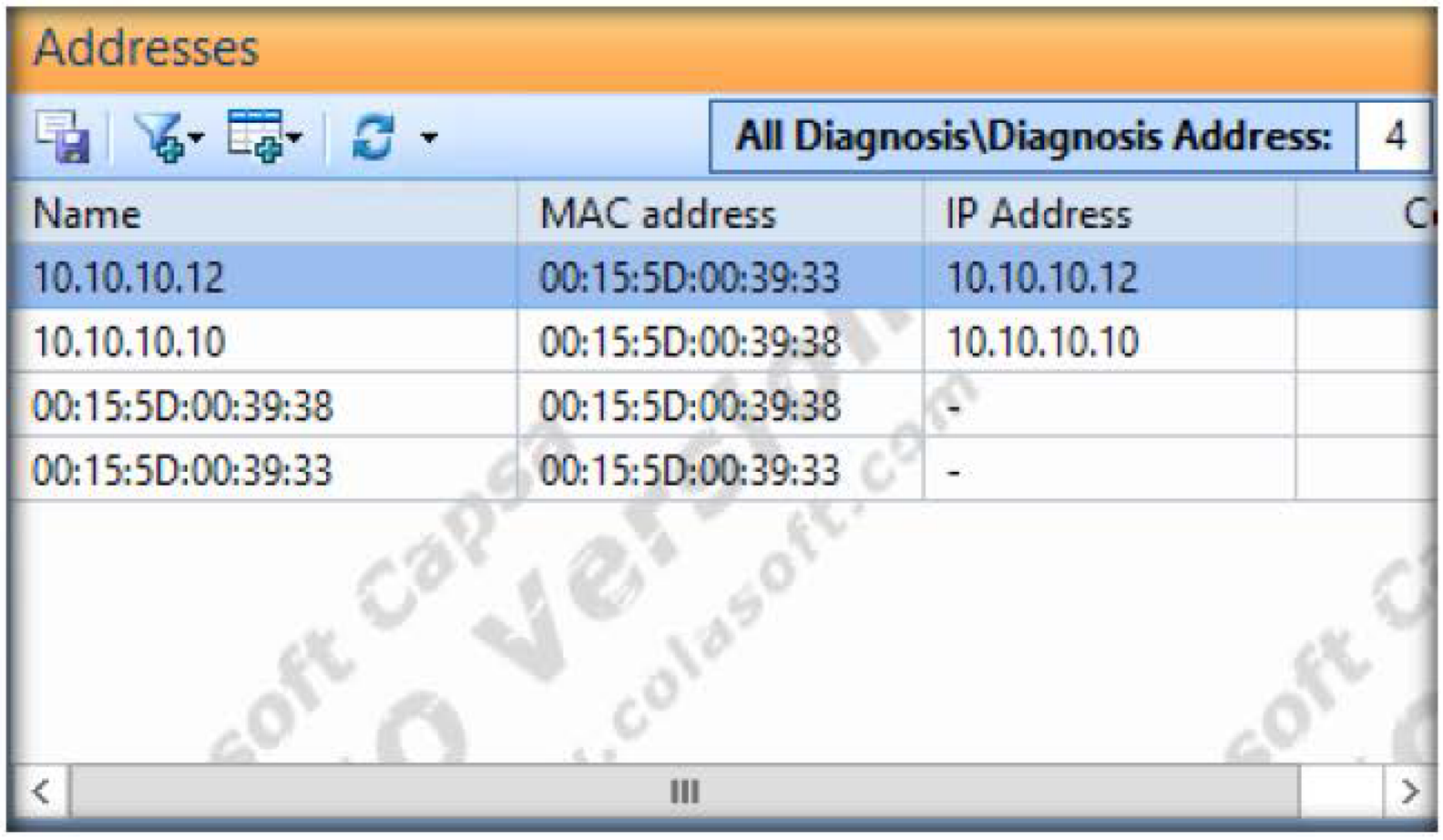



FIGURE 8.25: Diagnosis by IP address

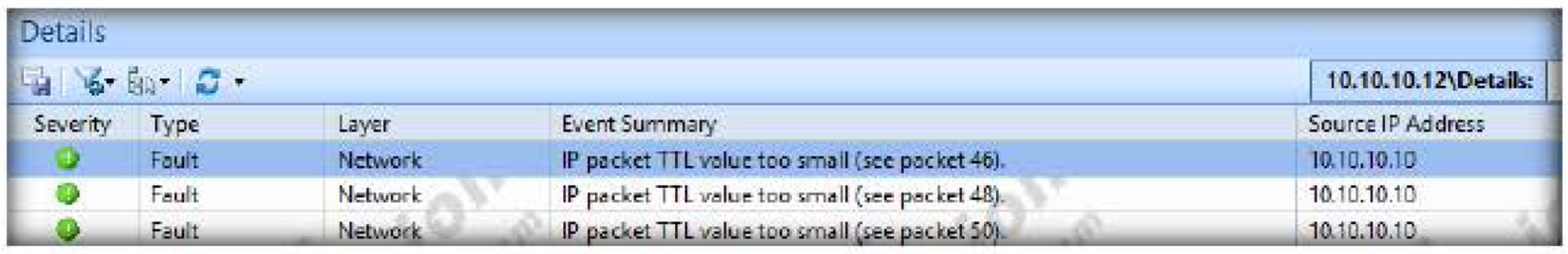



FIGURE 8.26: Diagnosis by details

35. Click the **MAC Endpoint** tab to view the MAC address endpoints and MAC conversations.

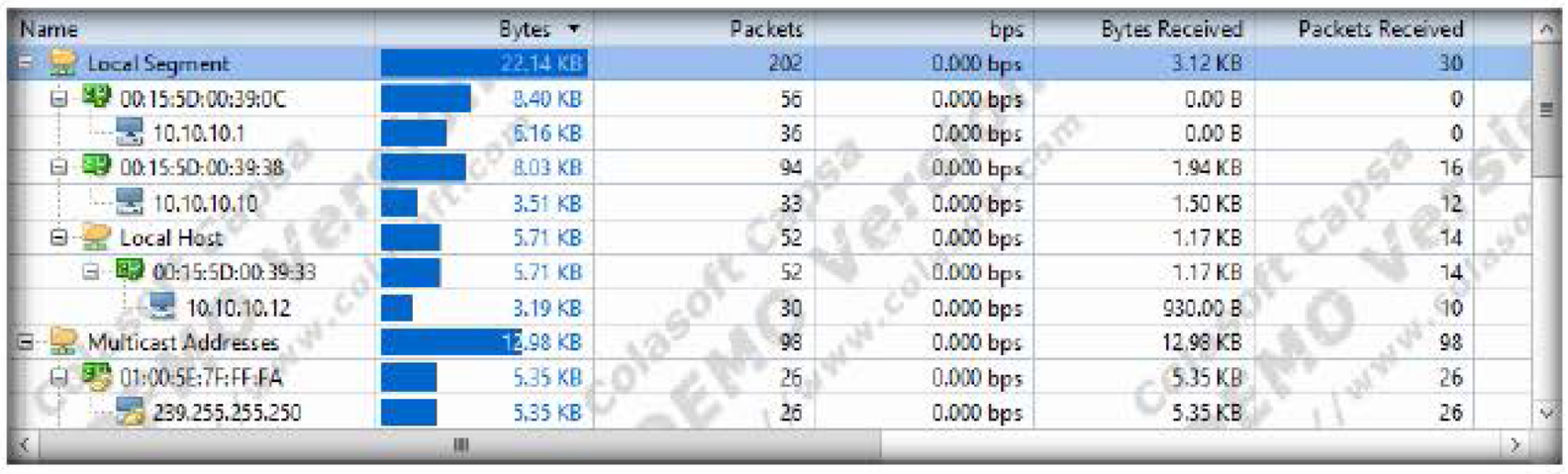



FIGURE 8.27: MAC endpoints

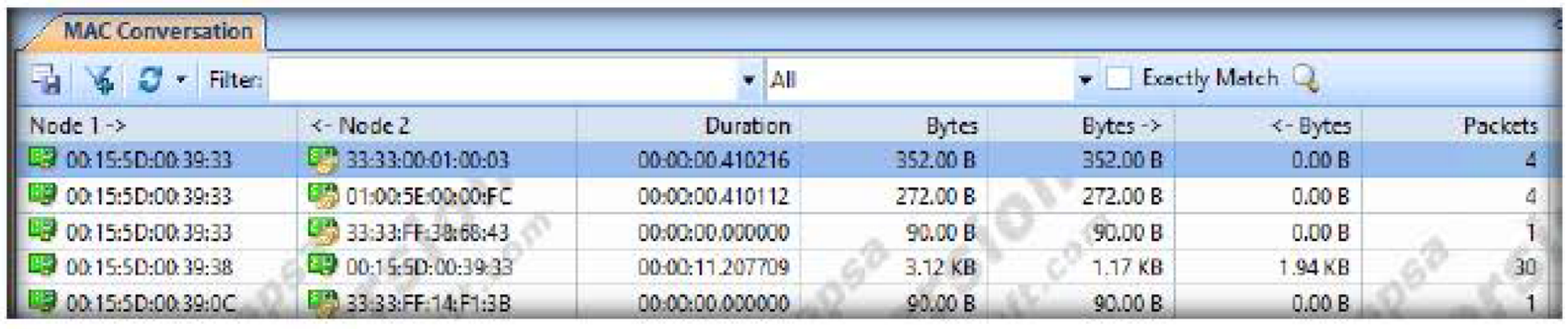



FIGURE 8.28: MAC conversations



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

36. Click **IP Endpoint** to view IP address end points and IP conversations (further sub divided based on protocols).

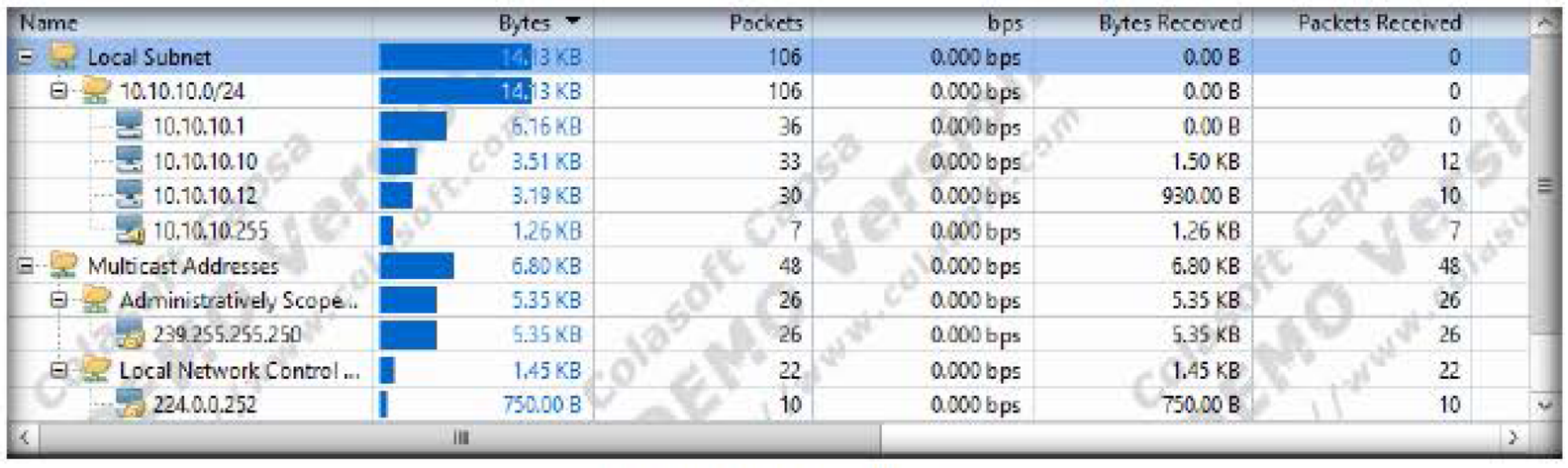



FIGURE 8.29: IP endpoints

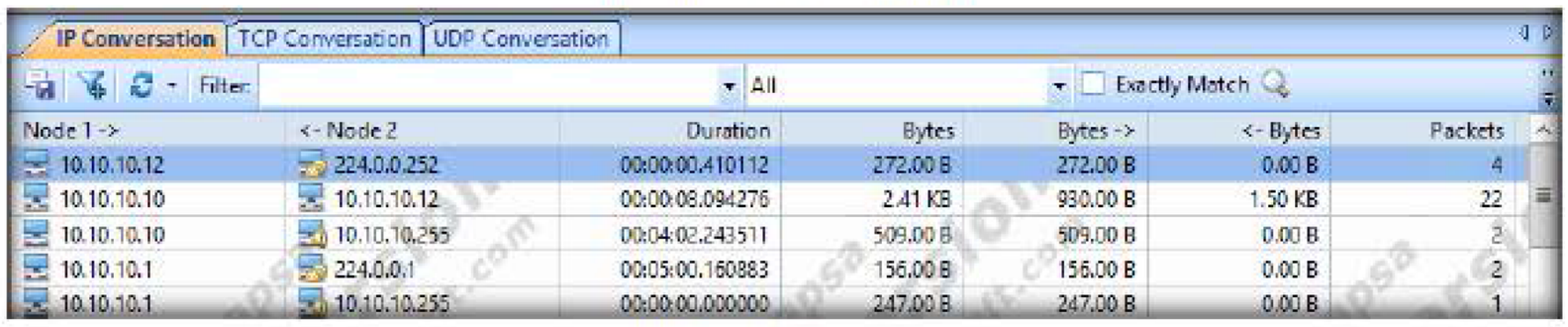



FIGURE 8.30: IP conversations

37. Click the **Close Project** button to close the window.




FIGURE 8.31: Closing the project

38. If a **Colasoft Capsa** pop up window appears, click **No**.

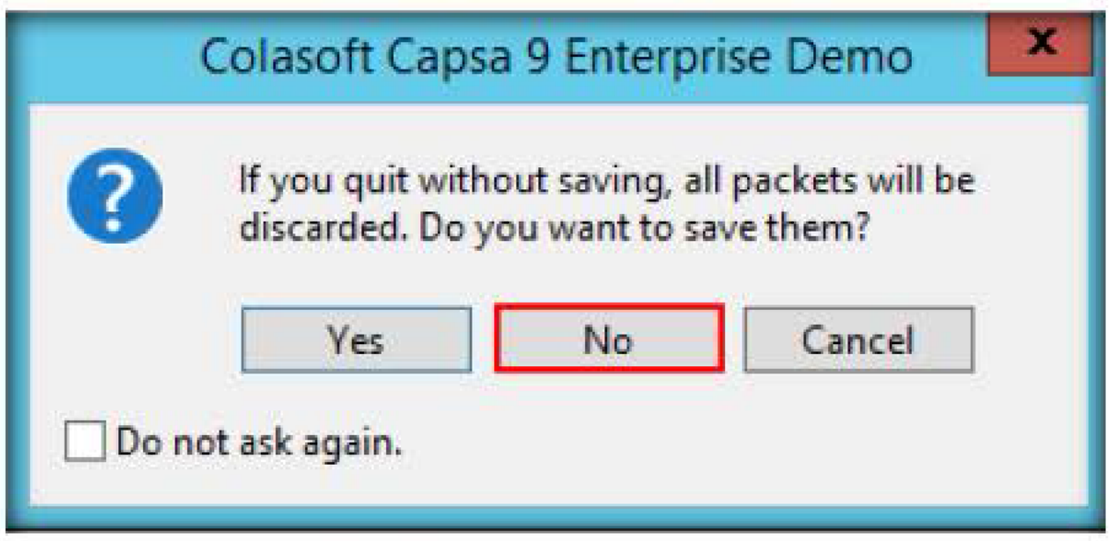



FIGURE 8.32: Not saving the packets


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

**TASK 6**

**Perform HTTP Analysis**

39. Click **HTTP Analysis** then click **Start**.

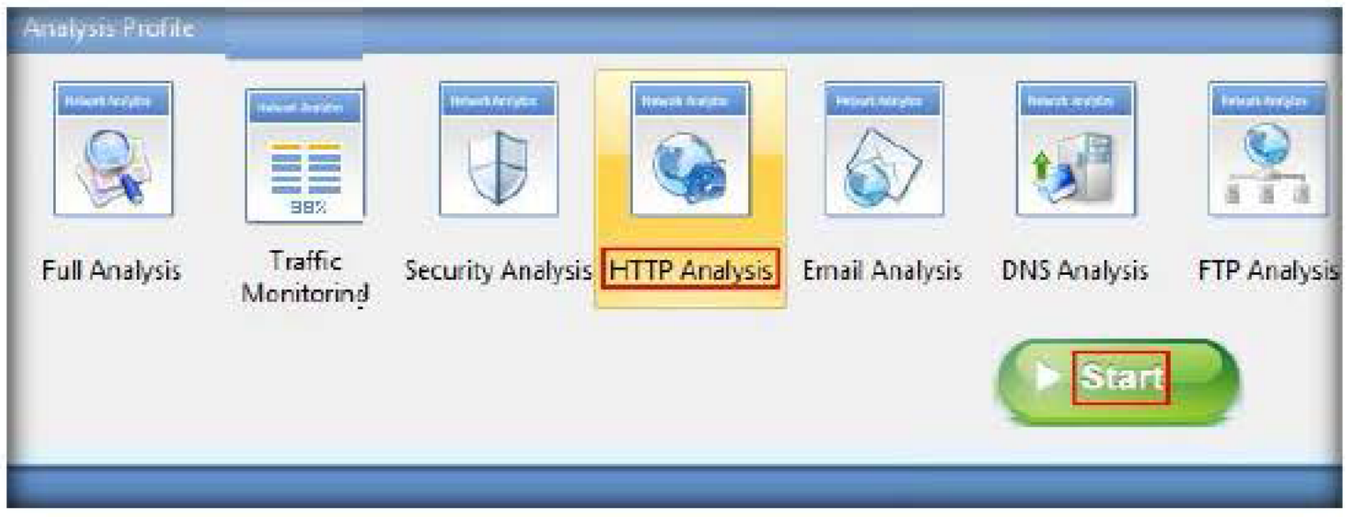



FIGURE 8.33: HTTP analysis

40. Switch to the **Windows 10** machine and browse web sites to generate traffic.
41. Switch back to **Windows Server 2012** and click **Stop**.

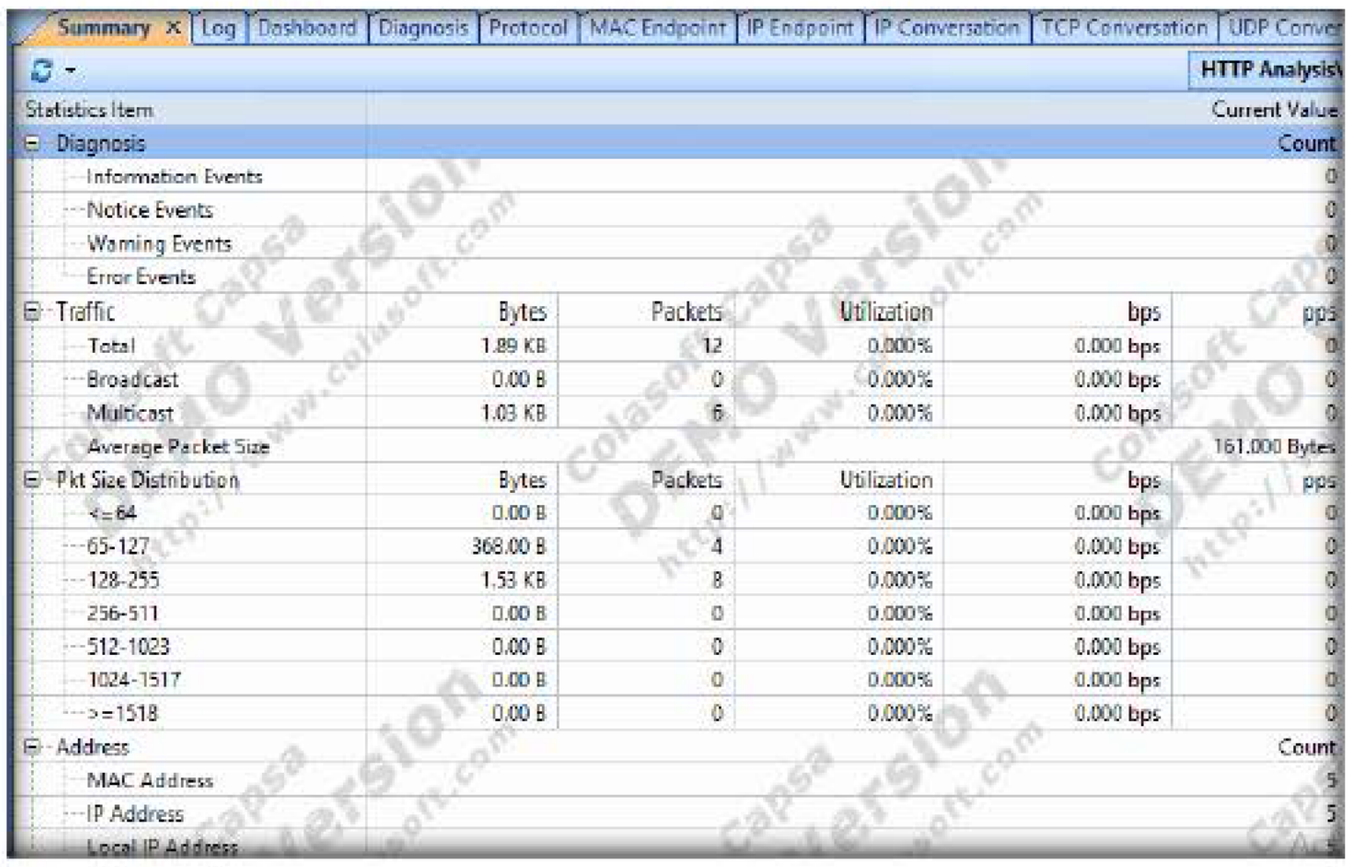



FIGURE 8.34: Stopping the traffic

**TASK 7**

**Examine the Output**

42. The **Summary** tab shows a summary of the packets.



Summary | Log | Dashboard | Diagnosis | Protocol | MAC Endpoint | IP Endpoint | IP Conversation | TCP Conversation | UDP Conver

HTTP Analysis\

| Statistics Item | | | | | |
|---|---|---|---|---|---|
| Diagnosis | | | | | Count |
| Information Events | | | | | 0 |
| Notice Events | | | | | 0 |
| Warning Events | | | | | 0 |
| Error Events | | | | | 0 |
| Traffic | Bytes | Packets | Utilization | bps | pps |
| Total | 1.89 KB | 12 | 0.000% | 0.000 bps | 0 |
| Broadcast | 0.00 B | 0 | 0.000% | 0.000 bps | 0 |
| Multicast | 1.03 KB | 6 | 0.000% | 0.000 bps | 0 |
| Average Packet Size | | | | | 161.000 Bytes |
| Pkt Size Distribution | Bytes | Packets | Utilization | bps | pps |
| <=64 | 0.00 B | 0 | 0.000% | 0.000 bps | 0 |
| 65-127 | 368.00 B | 4 | 0.000% | 0.000 bps | 0 |
| 128-255 | 1.53 KB | 8 | 0.000% | 0.000 bps | 0 |
| 256-511 | 0.00 B | 0 | 0.000% | 0.000 bps | 0 |
| 512-1023 | 0.00 B | 0 | 0.000% | 0.000 bps | 0 |
| 1024-1517 | 0.00 B | 0 | 0.000% | 0.000 bps | 0 |
| >=1518 | 0.00 B | 0 | 0.000% | 0.000 bps | 0 |
| Address | | | | | Count |
| MAC Address | | | | | 5 |
| IP Address | | | | | 5 |
| Local IP Address | | | | | 5 |

FIGURE 8.35: Summary of packets



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

43. The **Dashboard** and **Diagnosis** tabs have the same widgets as shown above. Click the **Protocol** tab. You can view number of packets (amount of traffic in **Bytes**) generated by different protocols.

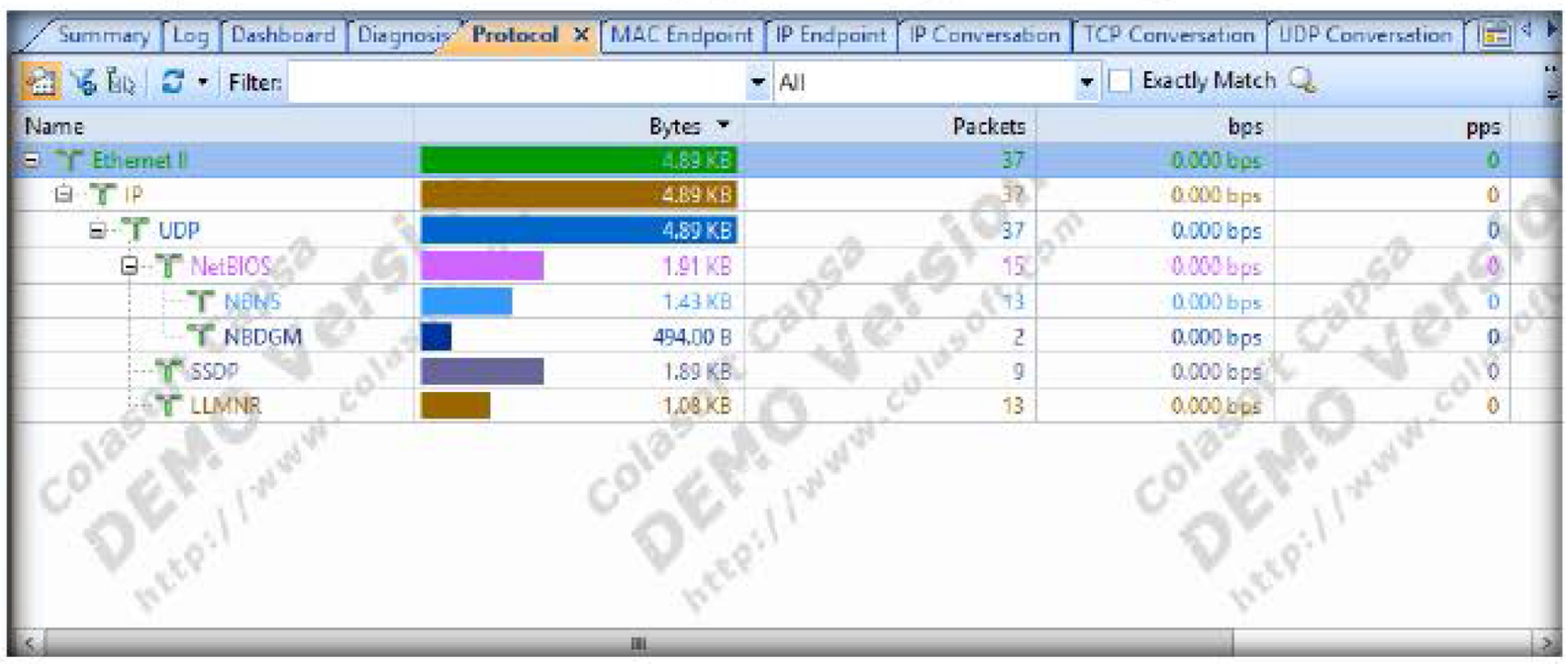



FIGURE 8.36: Protocol summary

44. Follow steps **37** and **38** to close the project.
45. In addition, other components can be analyzed as shown in the **Analysis** section.

## 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 |


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