Denial-of-Service

Module 10

Denial of Service

Denial of Service (DoS) is a type of attack on a computer or network that prevents legitimate use of its resources.

Lab Scenario

In computing, a denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users. Although the means, motives, and targets of a DoS attack may vary, it generally consists of the efforts of one or more people to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit-card payment gateways, and even root nameservers.

One common method of attack involves saturating the target machine with external communications requests, so that it cannot respond to legitimate traffic, or it responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload. DoS attacks can essentially disable your computer or your network. DoS attacks can be lucrative for criminals; recent attacks have shown that DoS attacks are a way for cyber criminals to profit.

As an expert Ethical Hacker or Pen Tester, sound knowledge of Denial of Service and Distributed Denial of Service attacks is must in order to detect and neutralize attack handlers and mitigate such attacks. The labs in this module give a hands-on experience in auditing a network against DoD and DDoS attacks.

Lab Objectives

The objective of this lab is to help students learn to perform Denial of Service attacks and test a network for DoS flaws.

In this lab, you will:

- Perform a DoS attack by sending a large number of SYN packets continuously
- Perform a HTTP flooding attack
- Perform a DDoS attack
- Detect and analyze DoS attack traffic

Lab Environment

To complete this lab, you will need:

- Window Server 2016 running in virtual machine
- Windows 10 running in virtual machine
- Windows Server 2012 running in virtual machine
- Windows 8 running in virtual machine
- Kali Linux running in virtual machine
- A web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 60 Minutes

Overview of Denial of Service

Denial of Service (DoS) is an attack on a computer or network that prevents legitimate use of its resources. In a DoS attack, attackers flood a victim's system with illegitimate service requests or traffic to overload its resources and prevent it from performing intended tasks.

Lab Tasks

Recommended labs to assist you in Denial of Service:

- **SYN Flooding** a Target Host using **Metasploit**
- SYN Flooding a Target Host using **hping3**
- Performing Distributed Denial of Service Attack using **HOIC**
- Detecting and Analyzing DoS Attack Traffic using **KFSensor** and **Wireshark**

Lab Analysis

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

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

Lab 1

SYN Flooding a Target Host using Metasploit

A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target machine in an attempt to exhaust its resources and make it unresponsive to legitimate incoming traffic.

Lab Scenario

DoS attacks are a kind of security break that does not generally result in the theft of information. However, these attacks can harm the target in terms of time and resources. On the other hand, failure might mean the loss of a service such as email. In a worst-case scenario, a DoS attack can mean the accidental destruction of the files and programs of millions of people who happen to be surfing the Web at the time of the attack.

Though the chances of successful SYN flooding are fewer because of advanced networking devices and traffic control mechanisms, attackers can launch SYN flooding attacks easily using a packet-crafting tool. As an ethical hacker or pen tester, you must assess your network resources for a SYN flooding attack.

Lab Objectives

The objective is to help students understand how to:

- Spoof IP Address of the Attacker Machine
- Perform SYN Flooding on the Target Machine

Lab Environment

To perform this lab, you need:

- Windows Server 2016 machine
- Kali Linux virtual machine
- Windows 10 virtual machine

- **Wireshark** located at **Z:\CEH-Tools\CEHv10 Module 10 Denial-of-Service\Wireshark**
- The latest version of Wireshark can be available at **https://www.wireshark.org/download.html**
- Administrative Privileges to run the tools
- If you decide to download the latest tools, screenshots might differ

Lab Duration

Time: 15 Minutes

Overview of the Lab

A TCP Session establishes a connection using a three-way handshake mechanism. The source sends a SYN packet to the destination. The destination, on receiving the SYN packet, responds by sending a SYN/ACK packet back to the source. This SYN/ACK packet confirms the arrival of the first SYN packet to the source. In conclusion, the source sends an ACK packet for the ACK/SYN packet sent by the destination. In a SYN attack, the attacker exploits the three-way handshake method. First, the attacker sends a fake TCP SYN request to the target server, and when the server sends a SYN/ACK in response to the client (attacker) request, the client never sends an ACK response. This leaves the server waiting to complete the connection.

Lab Tasks

Note: Before beginning this lab, log on to the **Windows 10** virtual machine and ensure that the firewall is turned off.

1. Log into the **Kali Linux** virtual machine.
2. In this lab, we are going to perform **SYN flooding** on the Windows 10 machine through **port 21**.
3. So, let us determine whether port 21 is open or not. We shall be using Nmap to determine state of the port.
4. Type the command **nmap -p 21 [IP Address of Windows 10]** and press **Enter**.

Note: The IP address of **Windows 10** used in this lab is **10.10.10.10,** which might vary in your lab environment.

5. The result returned by Nmap states that the port is **open**.

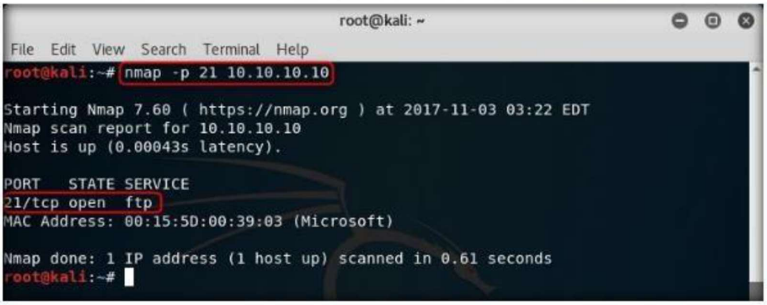

FIGURE 1.1: Checking for Open Port

Note: If the port turns out to be closed, look for the other open ports using Nmap.

6. Now that the result stating the port is open, perform SYN flooding on the victim machine (Windows 8) using port 21.
7. In this lab, use an auxiliary module named **synflood** to perform DoS attack on the machine. Launch this module from **msfconsole**.
8. Type **msfconsole** from a command-line terminal, and press **Enter** to launch msfconsole.

FIGURE 1.2: Launching msfconsole

9. Type the command **use auxiliary/dos/tcp/synflood** and press **Enter**.

FIGURE 1.3: Using the Auxiliary Module

10. This launches the synflood module.
11. Let us determine which module options need to be configured to begin the DoS attack.
12. So, type **show options** and press **Enter**. This displays all the options associated with the auxiliary module.

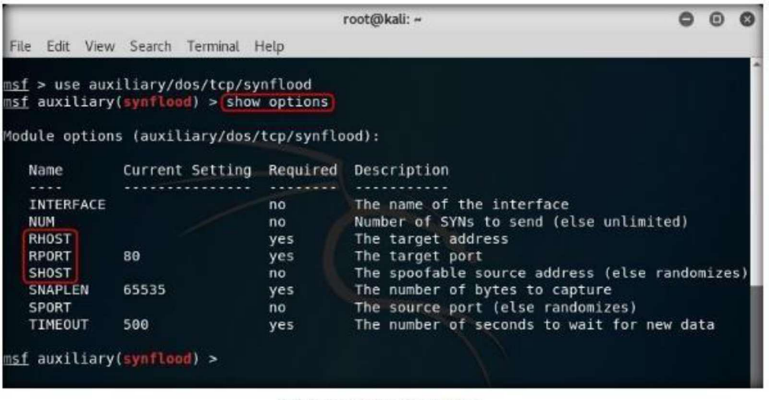

FIGURE 1.4: Viewing Options

13. Here, SYN flooding on port **4444** of the **Windows 10** machine will be performed by spoofing the IP Address of **Kali Linux** with that of the **Windows Server 2016** machine.

14. Issue the following commands:

    a. **set RHOST [IP Address of Windows 10]**

    b. **set RPORT 21**

    c. **set SHOST [IP Address of Windows Server 2016]**

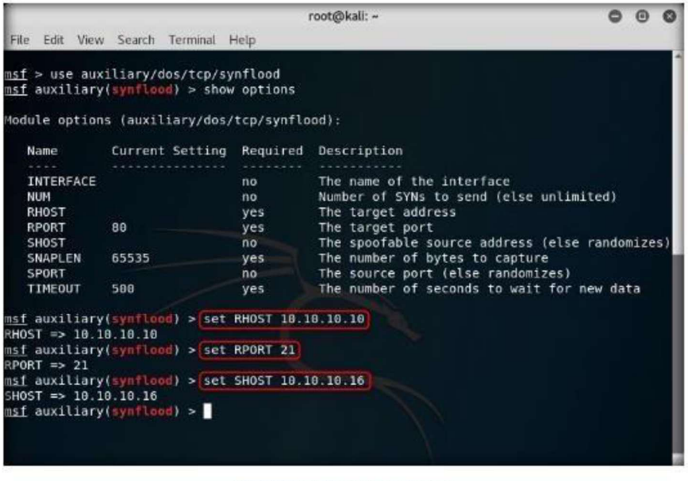

FIGURE 1.5: Configuring Options

15. By setting the SHOST option to **[IP Address of Windows Server 2016]**, you are spoofing the IP Address of Kali Linux machine with that of **Windows Server 2016**.

16. Once the auxiliary module is configured by setting the required options, start the DoS attack on **Windows 10** machine.

17. To begin, type **exploit** and press **Enter**.

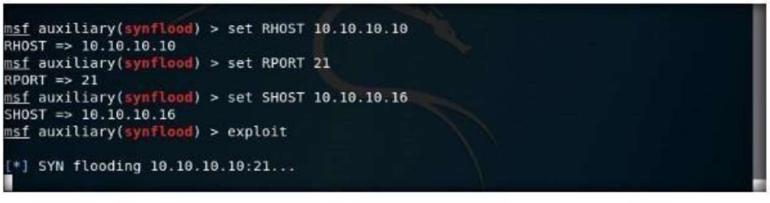

FIGURE 1.6: Initiating DoS Attack

18. This begins the syn flooding on the **Windows 10** machine.
19. To confirm, switch to the **Windows 10** machine, launch the **Wireshark** application, select an interface, and click **Start**.

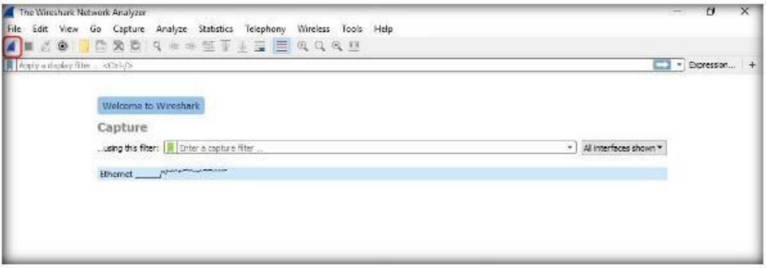

FIGURE 1.7: Capturing Traffic through Wireshark

20. Wireshark displays the traffic coming from the machine, as shown in the screenshot:

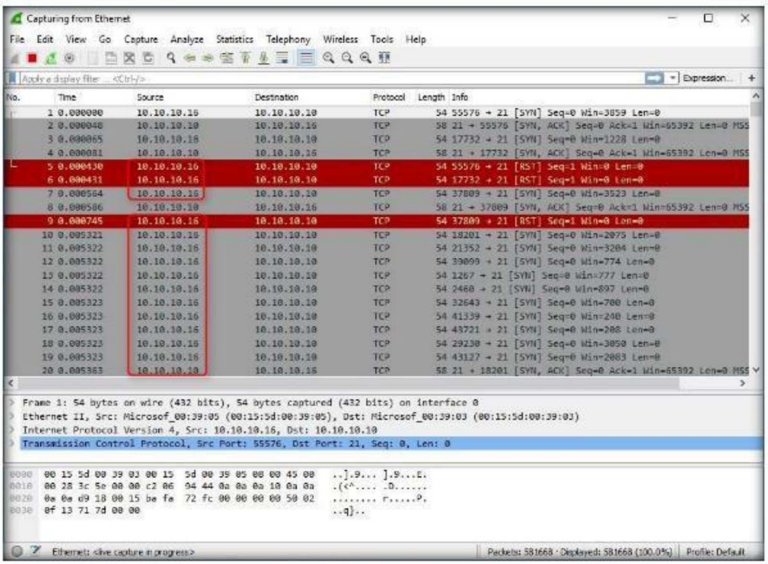

FIGURE 1.8: Analyzing the Traffic

21. Here, you can observe that the source IP address is that of the Windows Server 2016 machine. This implies that the IP Address of Kali Linux has been spoofed.
22. Now, open **Task Manager** in the machine, and click **Performance** tab. Wait for **10-15 seconds**; you will observe that the CPU usage has increased drastically, which implies that the DoS attack is in progress on the machine. If the attack is continued for some time, the machine's resources would be completely exhausted, and it will stop responding.

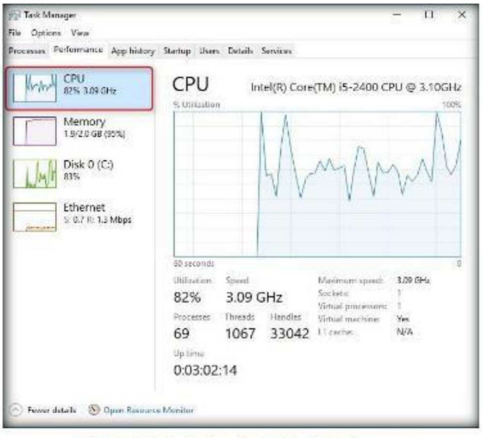

FIGURE 1.9: Analyzing the Machine's Performance

23. Once the performance analysis of the machine is done, switch to the Kali Linux machine and press **Ctrl+C** to terminate the attack.

```
msf auxiliary(synflood) > set RHOST 10.10.10.10
RHOST => 10.10.10.10
msf auxiliary(synflood) > set RPORT 21
RPORT => 21
msf auxiliary(synflood) > set SHOST 10.10.10.16
SHOST => 10.10.10.16
msf auxiliary(synflood) > exploit

[*] SYN flooding 10.10.10.10:21...
^C[-] Auxiliary interrupted by the console user
[*] Auxiliary module execution completed
msf auxiliary(synflood) >
```

FIGURE 1.10: Terminating the Attack

24. Thus, you have successfully spoofed the IP address and performed the DoS attack on the victim machine.

Lab Analysis

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

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

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

Lab

2

SYN Flooding a Target Host using hping3

hping3 is a command-line oriented TCP/IP packet assembler/analyzer.

Lab Scenario

A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to the target's system to consume enough server resources to make the system unresponsive to legitimate traffic.

A SYN flood attack works by not responding to the server with the expected ACK code. The malicious client can either not send the expected ACK, or spoof the source IP address in the SYN, causing the server to send the SYN-ACK to a falsified IP address—which will not send an ACK because it "knows" that it never sent a SYN. The server will wait for the acknowledgement for some time, as simple network congestion could also be the cause of the missing ACK, but in an attack increasingly large numbers of half-open connections will bind resources on the server until no new connections is be made, resulting in a denial of service to legitimate traffic. Some systems may also malfunction badly or even crash if other operating system functions are starved of resources in this way.

As an expert Ethical Hacker or Security Administrator of an organization, you should have sound knowledge of DoS and DDoS attacks and should be able to detect and neutralize attack handlers. You should use SYN cookies as a countermeasure against the SYN flood, which eliminates the resources, allocated on the target host.

Lab Objectives

The objective of this lab is to help students learn to perform DoS attacks and test the network for DoS flaws.

In this lab, you will:

- Perform DoS attacks
- Send huge amount of SYN packets continuously

Lab Environment

To complete this lab, you will need:

- Windows 10 as the victim machine
- Kali Linux virtual machine as the attacker machine
- Wireshark is located at **Z:\CEH-Tools\CEHv10 Module 10 Denial-of-Service\Wireshark**

Lab Duration

Time: 5 Minutes

Overview of hping3

hping3 is a network tool able to send custom TCP/IP packets and to display target replies in the same way that a ping program does with ICMP replies. hping3 handles fragmentation, arbitrary packets' body and size, and can be used to transfer files encapsulated under supported protocols.

Lab Tasks

1. Before beginning this lab, log in to the **Windows 10** virtual machine and keep the machine intact.
2. Log in to the **Kali Linux** virtual machine.
3. Launch the **hingp3** utility from the Kali Linux Applications menu.
4. To launch, go to **Applications → 01 - Information Gathering → Live Host Identification → hping3**.

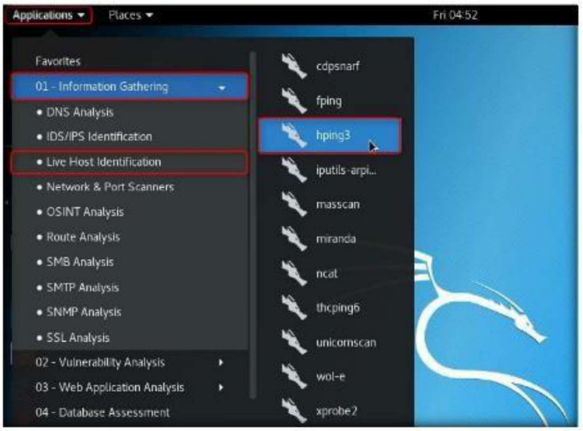

Figure 2.1: Launching hping3 from Kali Linux Menu

5. The **hping3** utility starts in command shell as shown in the screenshot:

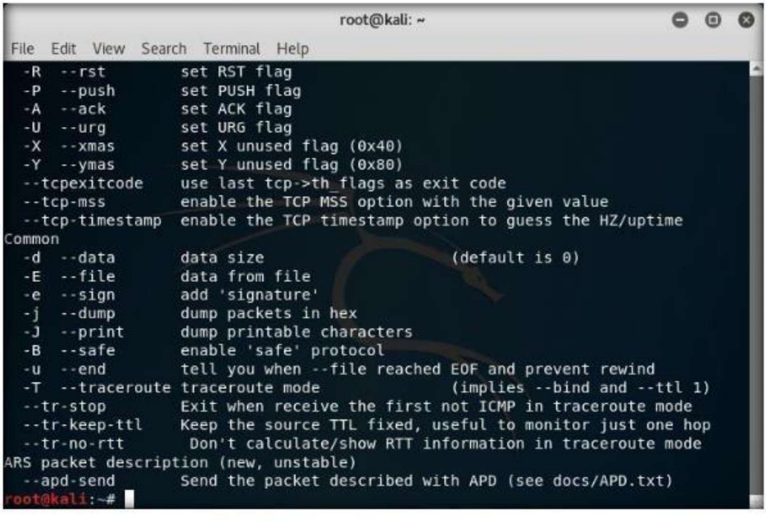

FIGURE 2.2: Kali Linux Command Shell with hping3

6. In command shell, type **hping3 -S [IP Address of Windows 10] -a 10.10.10.11 -p 22 --flood** and press **Enter**.

Note: In this lab, the IP Address of Windows 10 (victim) machine is **10.10.10.10**; this might vary in your lab environment.

10.10.10.11 refers to the IP address of the attacker machine i.e., Kali Linux; and the IP Address of this machine might vary in your lab environment.

FIGURE 2.3: Launching flooding attack using hping3

7. This initiates the SYN flooding on Windows 10.

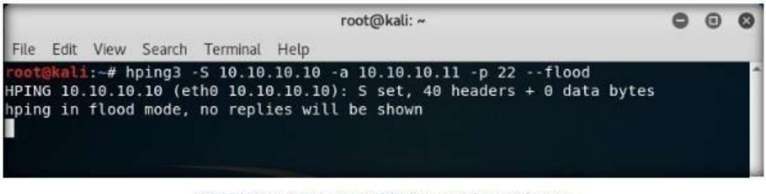

FIGURE 2.4: Attack successfully launched from Kali Linux

8. Hping3 floods the victim machine by sending bulk **SYN packets** and **overloading** victim resources.

9. Switch to the victim's machine (**Windows 10**). Install and launch Wireshark, select an interface, and start capturing.
10. You will observe that the application captures traffic, as shown in the screenshot:

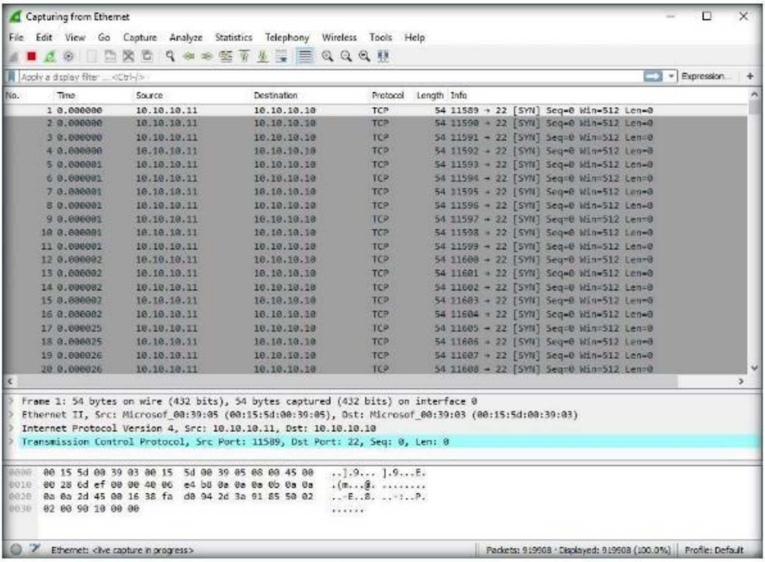

FIGURE 2.5: Wireshark with Packets Traffic

11. You sent huge number of **SYN packets**, which caused the victim's machine to **crash**.

Lab Analysis

Document the results gathered during this lab.

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

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

Lab

3

Performing Distributed Denial of Service Attack Using HOIC

A distributed denial of service (DDoS) attack involves a group of compromised systems usually infected with Trojans used to perform a DoS attack on a target system or network.

Lab Scenario

A distributed denial of service (DDoS) attack is a more sophisticated form of DoS attack in which, in some cases, it is difficult to trace the attackers. A DDoS attack is a large-scale, coordinated attack on the availability of services on a victim's system or network, launched indirectly through many compromised computers on the Internet.

A DDoS attack uses many computers to launch a coordinated DoS attack against one or more targets. Using client/server technology, the perpetrator is able to multiply the effectiveness of the DoS significantly by harnessing the resources of multiple unwitting accomplice computers, which serve as attack platforms. The flood of incoming messages essentially forces the target system to shut down, thereby denying service to legitimate users.

These attacks come from various machines that can be in the same location or various other locations. As large numbers of "zombies" participate in this attack, an enormous amount of traffic is directed onto the victim machine, resulting in temporary or permanent damage of its resources.

As an expert Ethical Hacker and Penetration Tester, you must be aware of all types of DoS attempts and prevent them from affecting information systems.

Lab Objectives

The objective of this lab is to help students learn how to perform a DDoS attack—in this case, HTTP Flooding.

Lab Environment

To complete this lab, you will need:

- **HOIC** tool located at **Z:\CEH-Tools\CEHv10 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\High Orbit Ion Cannon (HOIC)**
- You can download the latest version of HOIC from the link **http://sourceforge.net/projects/highorbitioncannon/**
- If you decide to download the latest version, then screenshots shown in the lab might differ
- Windows Server 2012, Windows 10 and Windows 8 virtual machines as attacker machines
- Kali Linux virtual machine as target machine
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of HOIC

"High Orbit Ion Cannon" or HOIC for short is a network stress testing tool for launching DDoS attacks. HOIC causes DoS through the use of HTTP floods. HOIC has a built-in scripting system that accepts .hoic files called "boosters," allowing a user to implement some anti-DDoS randomization countermeasures, as well as increase the magnitude of the attack.

Lab Tasks

1. Before beginning this lab, log into the **Windows 10**, **Windows Server 2012**, **Windows 8**, and **Kali-Linux** virtual machines.
2. In the **Windows 8** virtual machine, navigate to **Z:\CEH-Tools\CEHv10 Module 10 Denial-of-Service\DoS and DDoS Attack Tools** and copy the **High Orbit Ion Cannon (HOIC)** folder onto the **Desktop**.

Note: To perform the DDoS attack, run this tool from various virtual machines at once. So, when you run the tool directly from Z: (in virtual machines at a time), errors might occur. To avoid errors, copy the folder **High Orbit Ion Cannon (HOIC)** individually onto each machine, and then run the tool.

3. Similarly, follow the previous step and copy the **High Orbit Ion Cannon (HOIC)** folder onto the other virtual machines' respective Desktops.

4. Now, switch to the **Window 10** virtual machine.
5. Navigate to the **Desktop**, open **High Orbit Ion Cannon (HOIC)**, and double-click **hoic2.1.exe**.
6. HOIC GUI appears on the screen, click "**+**" (below **TARGETS**).

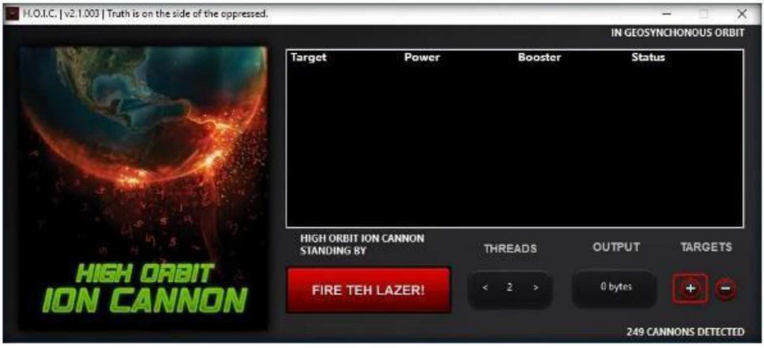

FIGURE 3.1: HOIC GUI

7. The **HOIC - [Target]** pop-up appears. Type the target URL **http://[IP Address of the target machine]** in the URL field, slide the power bar to **High**, select **GenericBoost.hoic** booster from the drop-down list, and click **Add**.

Note: The IP address entered in this lab is that of the Kali-Linux virtual machine and might differ in your lab environment.

FIGURE 3.2: HOIC - [Target] pop-up

8. Set the **THREADS** value to **20** by clicking the **>** button until the value is reached.

FIGURE 3.3: Setting the THREADS value

9. Now, switch to **Windows Server 2012** and **Windows 8** virtual machine and follow the **steps 5-8** to launch HOIC and configure it.
10. Once HOIC is configured on all the machines, switch to each machine and click **FIRE TEH LAZER!**.

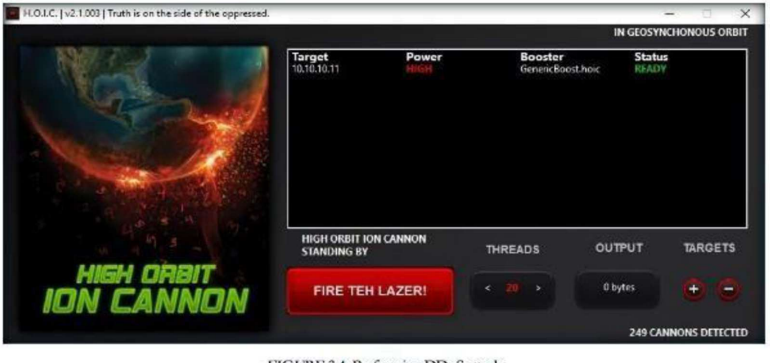

FIGURE 3.4: Performing DDoS attack

11. This initiates the DDoS attack on the target **Kali Linux** machine.
12. Switch to the **Kali Linux** virtual machine, and launch the command-line terminal.
13. Type **wireshark** in the terminal, and press **Enter**.

FIGURE 3.5: Launching Wireshark

14. If an **Error** pop-up appears, click **OK**.

FIGURE 3.6: Error pop-up

15. The Wireshark GUI appears; select a network interface and click **Start**.

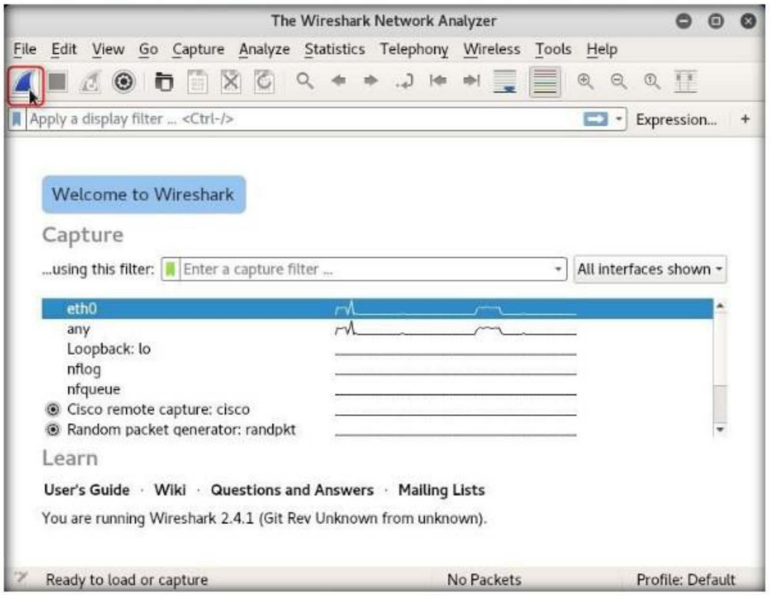

FIGURE 3.7: Starting Wireshark Capture

16. Observe that Wireshark starts capturing a large volume of packets, which means the machine is experiencing a huge number of incoming packets. These packets are coming from the **Windows Server 2012**, **Windows 10**, and **Windows 8** virtual machines.

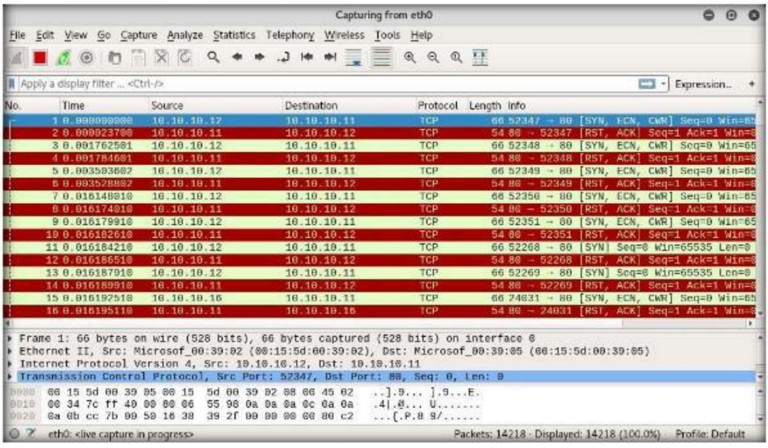

FIGURE 3.8: Wireshark Capturing the Packets

17. Leave the machine intact for 5–10 minutes, and then open it again. You will observe that the performance of the machine is slightly affected, and its response slowing down.

18. In this lab, only three machines are demonstrated flooding a single machine. If there are a large number of machines performing flooding, then the target Kali Linux machine's resources are completely consumed and the machine is overwhelmed.

19. In real time, a group of hackers operating hundreds or thousands of machines configure this tool on their machines, communicate with each other through IRCs, and simulate the DDoS attack by flooding a target machine/website at the same time. The target is overwhelmed and stops responding to user requests or starts dropping packets coming from legitimate users. The larger the number of attacker machines, the higher the impact of the attack on the target machine/website.

20. On completion of the lab, click **FIRE TEH LAZER!** again, and then close the HOIC window in all the attacker virtual machines. Also, close the Wireshark window in Kali Linux.

Lab Analysis

Analyze and document the results related to this lab exercise.

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

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

Lab

4

Detecting and Analyzing DoS Attack Traffic using KFSensor and Wireshark

KFSensor is a Network Intrusion Detection Tool that is equipped with several mechanisms to counter DOS attacks. The tool allows you to determine the maximum number of connections to the machine per IP address.

Lab Scenario

KFSensor is a Windows-based honeypot Intrusion Detection System (IDS). It acts as a honeypot to attract and detect hackers and worms by simulating vulnerable system services and Trojans. By acting as a decoy server, it can divert attacks from critical systems and provides a higher level of information than firewalls and NIDS alone.

KFSensor is designed for use in a Windows-based corporate environment and contains many innovative and unique features such as remote management, a Snort compatible signature engine and emulations of Windows networking protocols. As an ethical hacker or security administrator, you can use KFSensor to audit your network infrastructure against DoS attacks.

Lab Objectives

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

- Detect DoS attack using KFSensor
- Examine the incoming packet dump using Wireshark

Lab Environment

To perform this lab, you will need:

- Windows Server 2016 machine
- Kali Linux virtual machine
- Windows 10 virtual machine

- **KFSensor** located at **Z:\CEH-Tools\CEHv10 Module 10 Denial-of-Service\Honeypot Tools\KFSensor**
- The latest version of KFSensor can be available at **http://www.keyfocus.net/kfsensor/download**
- **Wireshark** located at **Z:\CEH-Tools\CEHv10 Module 10 Denial-of-Service\Wireshark**
- The latest version of Wireshark can be available at **https://www.wireshark.org/download.html**
- Administrative Privileges to run the tools
- If you decide to download the latest tools, screenshots might differ

Lab Duration

Time: 20 Minutes

Overview of the Lab

KFSensor's rule base signature engine can identify known attack patterns, which helps in analyzing the nature of an event. It contains a Windows networking/ NetBIOS/SMB/CIFS emulation honeypot. This unique feature enables it to detect the nature of attacks on file shares and Windows administrative services, currently the most prevalent and damaging on the Internet.

This lab demonstrates the process of DoS attack detection. Here, we will first search for an open port on the target machine (here, Windows 10) and perform DoS attack through an open port on the machine. Later, we will use KFSensor to detect the attack, and then examine the packets that were logged by KFSensor.

Lab Tasks

Note: Launch the **Windows 10** and **Kali Linux** virtual machines before beginning this lab.

1. In **Windows 10** virtual machine, navigate to **Z:\CEH-Tools\CEHv10 Module 10 Denial-of-Service\Honeypot Tools\KFSensor** and double-click **kfsens40.msi**.
2. If a **User Account Control** pop-up appears, click **Yes**.

3. The **KFSensor Evaluation Setup** window appears; follow the wizard-driven installation steps to install the application.

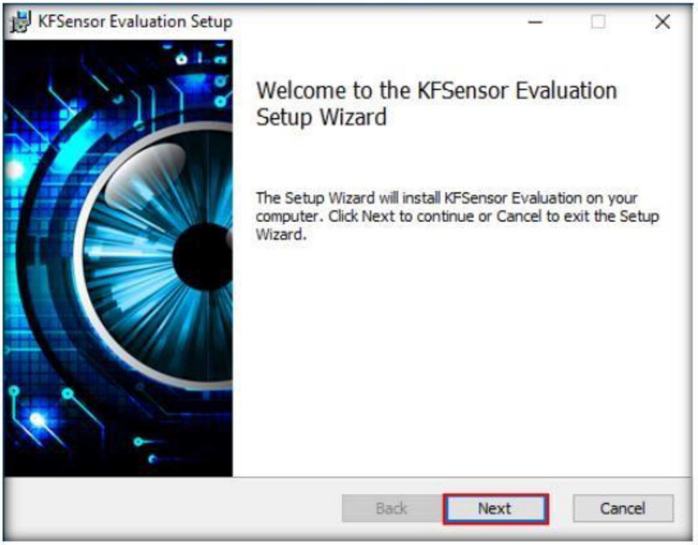

FIGURE 4.1: KFSensor setup Window

4. Completed the **KFSensor Evaluation Setup** wizard appears, **uncheck Launch KFSensor** option and click **Finish**.

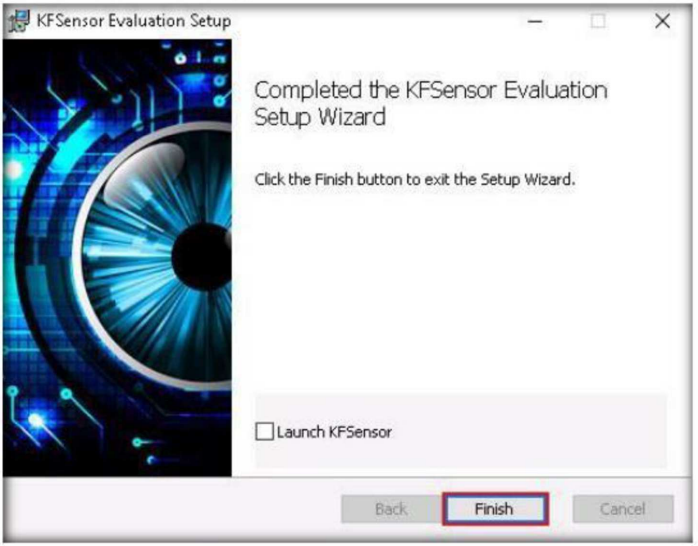

FIGURE 4.2: KFSensor Evaluation Setup window

5. Launch KFSensor as Administrator, navigate to **Start → KFSensor** and right-click on **KFSensor → More → Run as administrator** as shown in the screenshot.

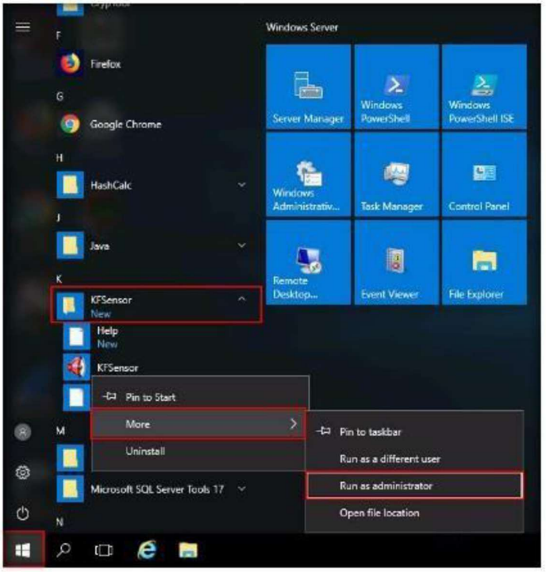

FIGURE 4.3: Launching KFSensor as an Administrator

6. If the **User Account Control** pop-up appears, click **Yes**.

7. When the application is being launched for the first time, the KFSensor **Set Up Wizard** window appears; click **Cancel** button.

FIGURE 4.4: KFSensor Set Up Wizard window

8. In the KFSensor application window, click **Settings** from the menu-bar and click **Set Up Wizard...** as shown in the screenshot:

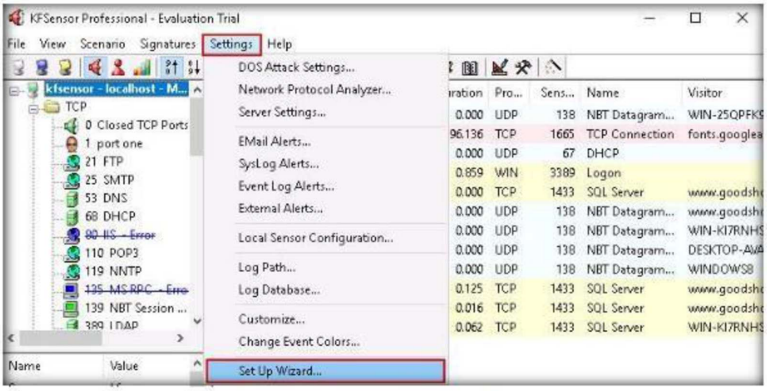

FIGURE 4.5: Launching KFSensor Set Up Wizard...

9. The KFSensor **Set Up Wizard** appears; click **Next** button.

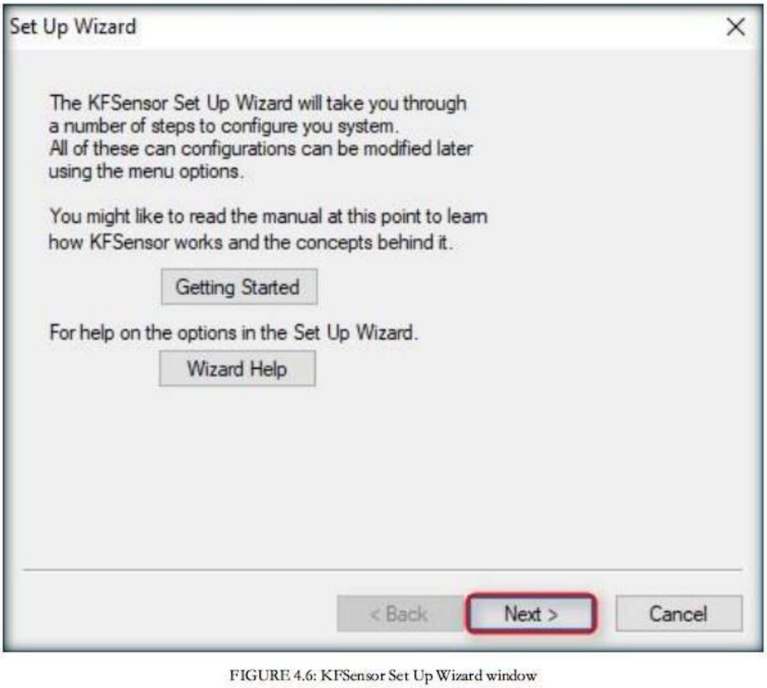

FIGURE 4.6: KFSensor Set Up Wizard window

10. In the **Set Up Wizard - Port Classes** window, check all the port classes to include, and click **Next.**

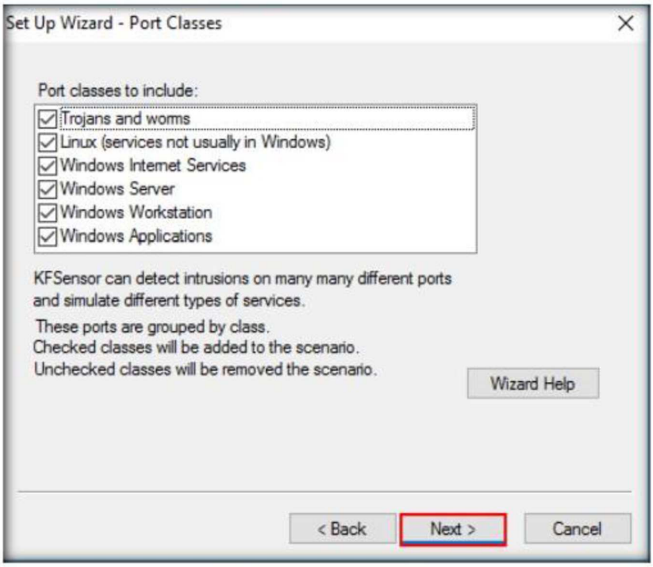

FIGURE 4.7: Port Classes Wizard

11. In the **Set Up Wizard - Native Services** wizard, check all the ports with all active native services, and click **Next.**

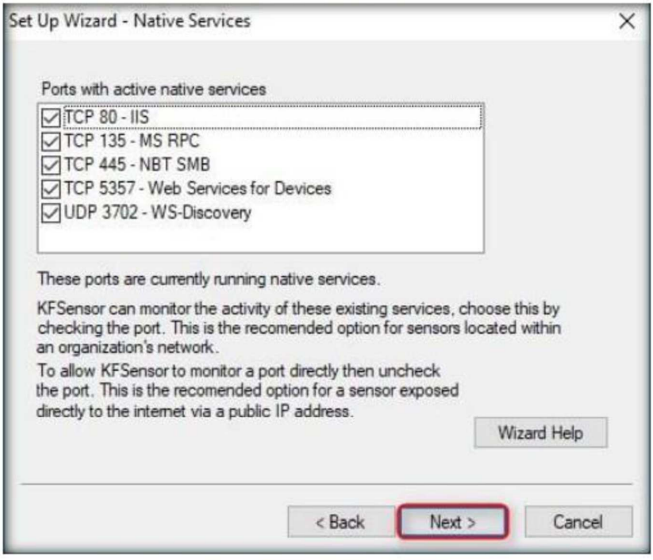

FIGURE 4.8: Native Services Wizard

12. In the **Set Up Wizard - Domain** window, leave the **Domain Name** field set to default, and click **Next**.

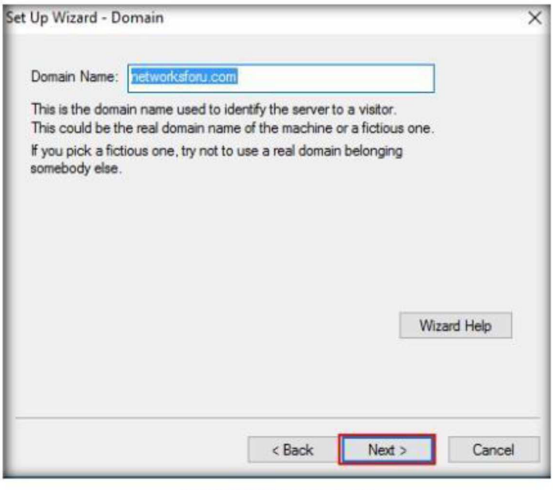

FIGURE 4.9: Domain wizard

13. In the **Set Up Wizard - EMail Alerts** window, leave the options set to default, and click **Next**.

FIGURE 4.10: EMail Alerts Wizard

14. In the **Set Up Wizard - Options** wizard:
    a. Select **Cautious** from **Denial Of Service Options** drop-down list
    b. Select **Enable packet dump files** from the **Network Protocol Analyzer** drop-down list
15. Click **Next**.

16. This sets the DoS options to Cautious mode and saves the packet dump files at the time of the DoS attack.

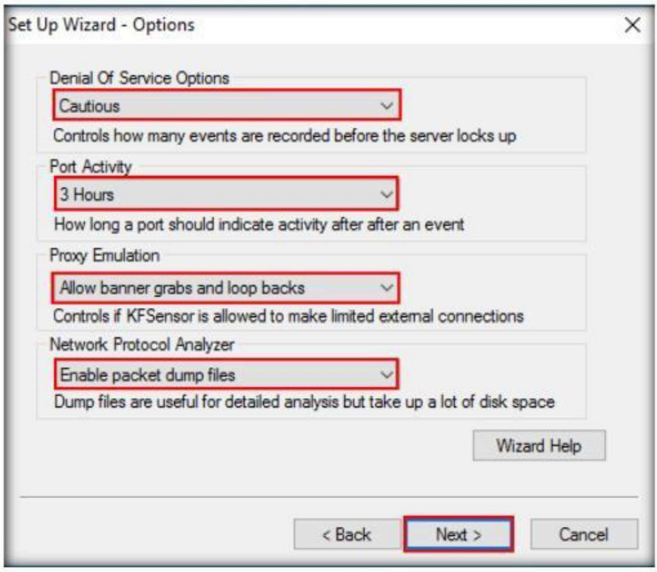

FIGURE 4.11: Options Wizard

17. In the **Set Up Wizard - Systems Service** wizard, leave the option set to default, and click **Next**.

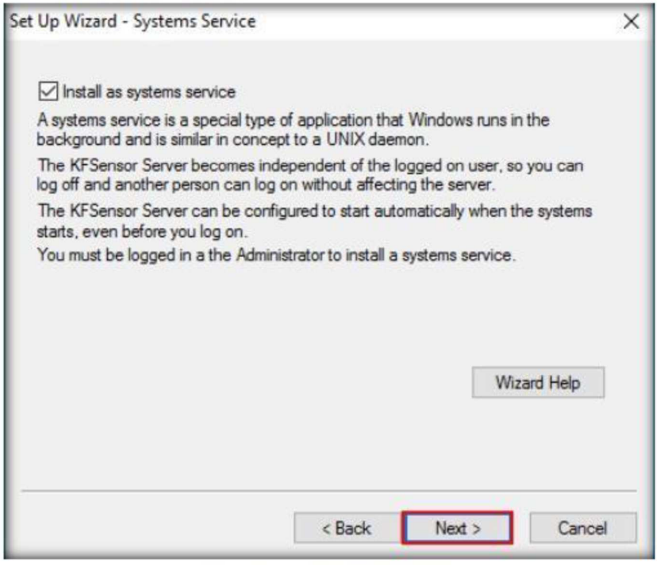

FIGURE 4.12: Systems Service Wizard

18. In the final step of the **Set Up Wizard** wizard, click **Finish**.

FIGURE 4.13: End of Wizard

19. The **KFSensor Professional** window appears. Click **FTP** under **TCP**.

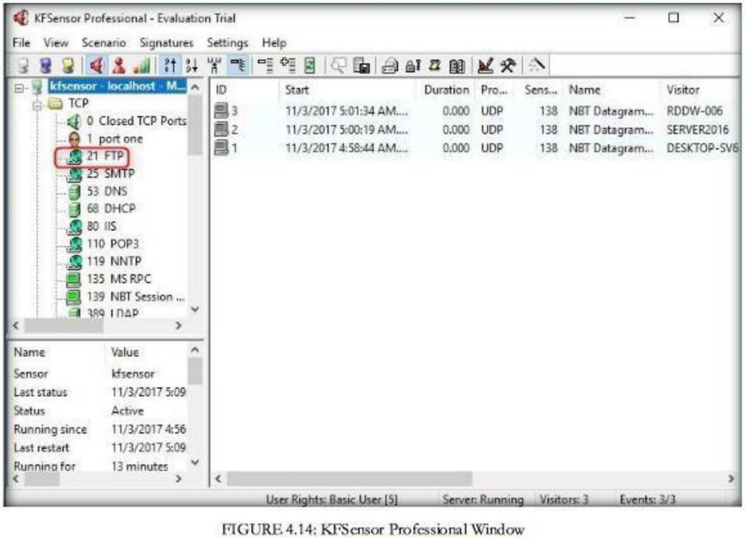

FIGURE 4.14: KFSensor Professional Window

20. If the FTP icon is green, and the FTP section is empty, it means currently there is no traffic through port 21.

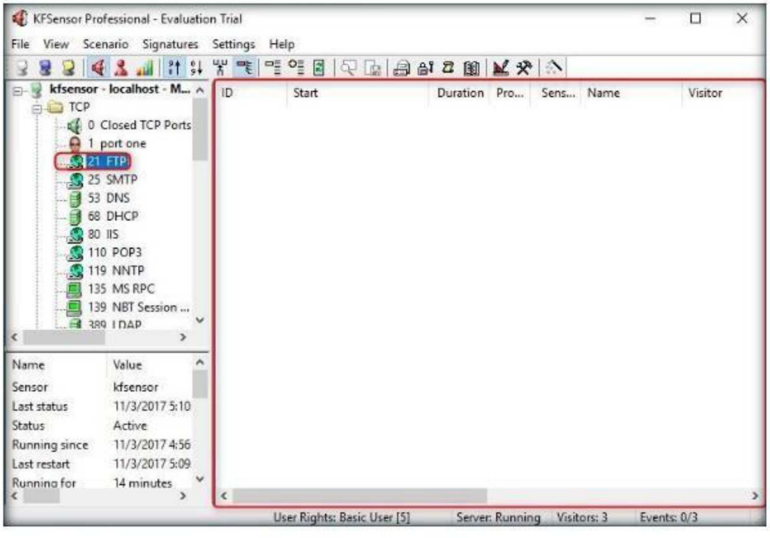

FIGURE 4.15: Viewing FTP Section

21. Now, KFSensor is configured to detect the DoS attacks that would be performed on the **Windows 10** machines from this point forward.

22. So, perform a DoS attack on this machine through **port 21** from an attacker machine, **Kali Linux**.

23. Switch to the **Kali Linux** virtual machine and open a command prompt. First task is to check whether **port 21** is open on the target machine by using Nmap.

24. The command used to check the status of this port is **nmap -p 21 [IP Address of Windows 10]**.

Note: The IP Address of **Windows 10** machine in this lab is **10.10.10.10,** which might differ in your lab environment.

25. Observe that **port 21** is open, as shown in the screenshot:

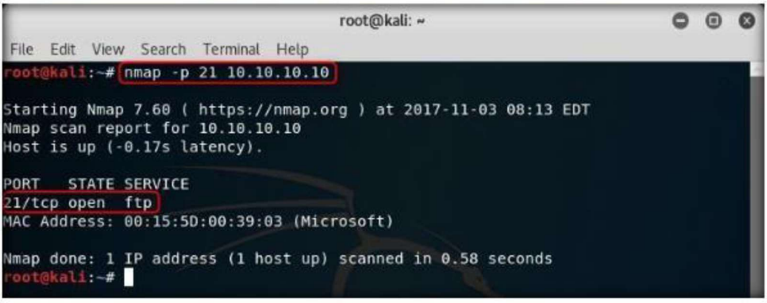

FIGURE 4.16: Testing FTP Port

26. Use this port to flood the victim machine.
27. Perform **SYN** flooding on the victim machine using hping3.
28. To begin flooding, type the command **hping3 -d 100 -S –p 21 --flood [IP Address of Windows 10]** and press **Enter**.

    Note: The IP address of Windows 10 machine is **10.10.10.10**.

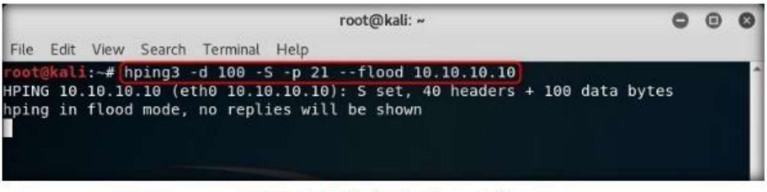

FIGURE 4.17: Flooding the Victim Machine

29. Here, we are performing SYN flooding (**-S**) onto the victim machine through port 21 (**-p 21**), where the data size of each packet going to the machine is 100 bytes (**-d 100**).

30. Once you enter the command, switch to the **Windows 10** machine and try to explore it. Observe that the machine's screen is frozen, which means that the resources of Windows 10 are completely exhausted. This means that the DoS attack is being successfully performed.

FIGURE 4.18: Victim Machine Failed to Respond

31. Now, switch to the **Kali Linux** machine, and press **Ctrl+C** to terminate SYN flooding.

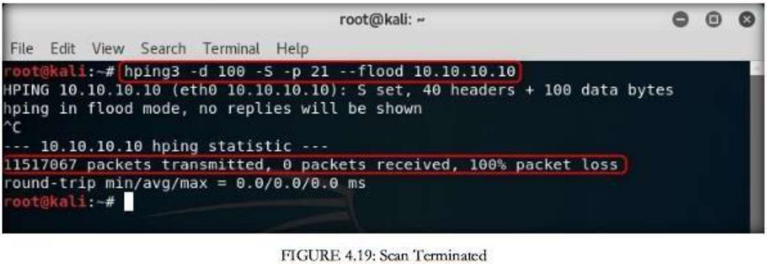

FIGURE 4.19: Scan Terminated

32. Switch to the **Windows 10** machine; you should now be able to access it.
33. Now the FTP icon in the left pane changes to red, and the FTP section in the right pane is flooded with a list of events.
34. Scroll down the section; you can see an event with the name **DOS Attack**.

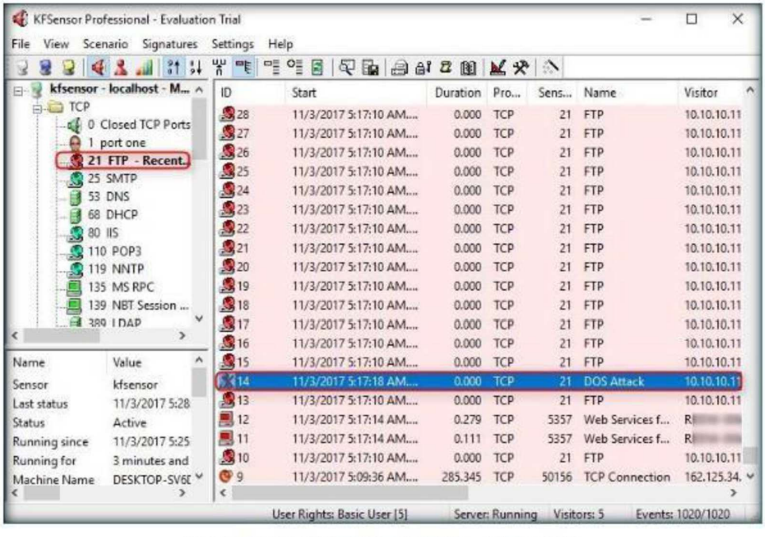

FIGURE 4.20: FTP Section Flooded with DOS Attack Events

35. This concludes that a DOS KFSensor has detected the DoS attack.
36. Choose a random event, right-click on it, and select **Event Details...** to view details of the selected event.

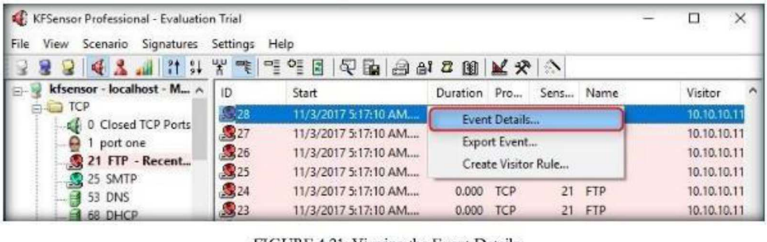

FIGURE 4.21: Viewing the Event Details

37. An **Event** window appears, displaying the event summary (on the **Summary** tab), which contains the severity level of the event (**High**), the description of the event (**Syn Scan**), the visitor of the event (**attacker machine's IP address**), the name of the sensor (**FTP**), and so on, as shown in the screenshot:

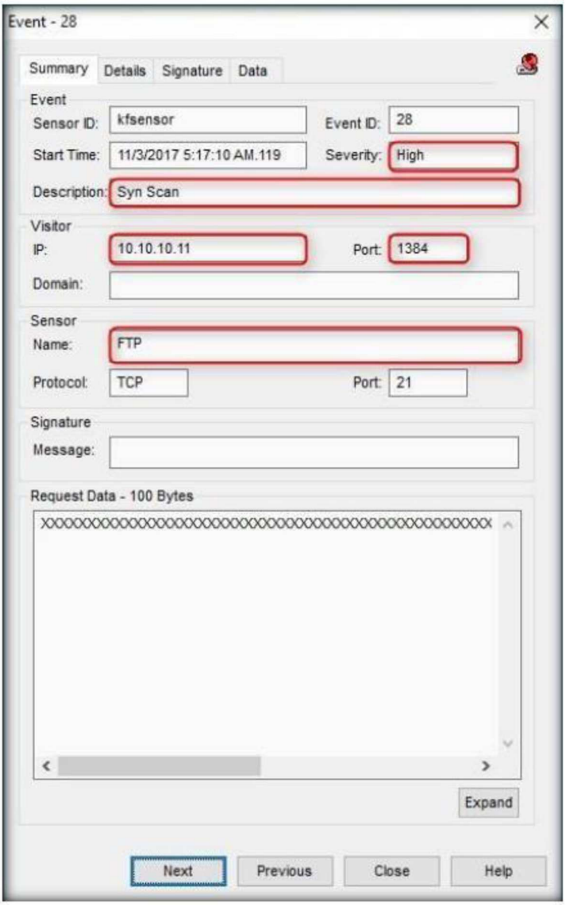

FIGURE 4.22: Viewing the Event Details

38. You may click the other tabs to analyze additional information related to the event.

39. Now, analyze the packet dump file containing the traffic captured during the DoS attack. KFSensor stores the packet dump file in **C:\kfsensor\dumps** by default.

40. To view the packet dump, use a packet capturing application such as Wireshark.

41. Install and launch Wireshark, located at **Z:\CEH-Tools\CEHv10 Module 10 Denial-of-Service\Wireshark**. If the application is already installed, launch it from the **Apps** screen.

42. Click **File** in the menu bar, and then click **Open**.

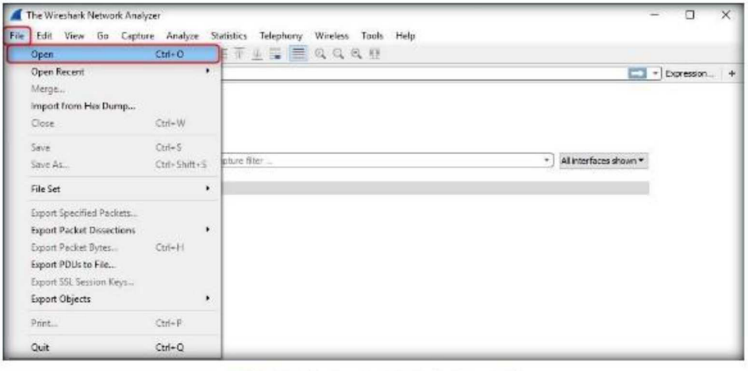

FIGURE 4.23: Opening the Packet Dump File

43. The **Wireshark: Open Capture File** window appears; navigate to **C:\kfsensor\dumps**, select the packet dump file, and click **Open**.

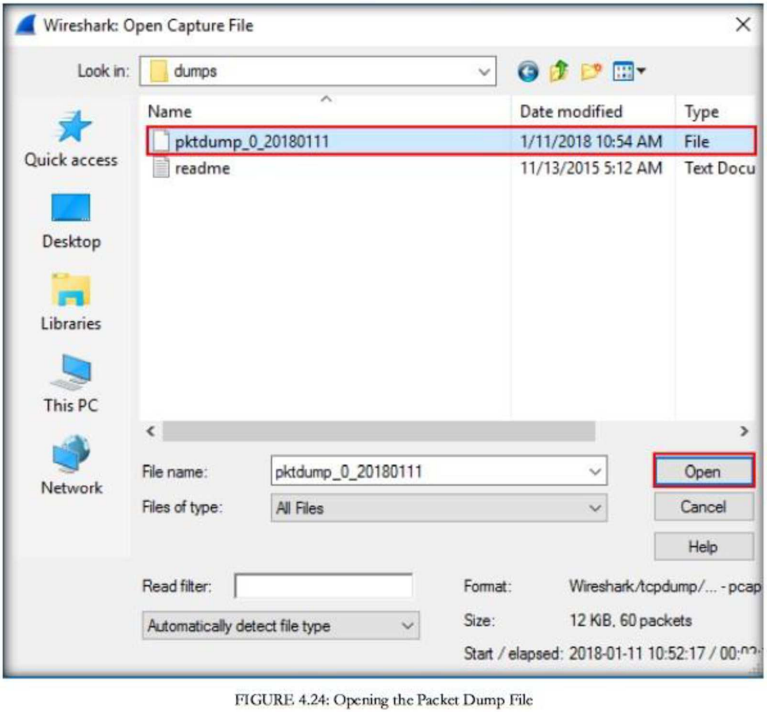

FIGURE 4.24: Opening the Packet Dump File

44. Wireshark loads the file and displays the packet's details, as shown in the screenshot:

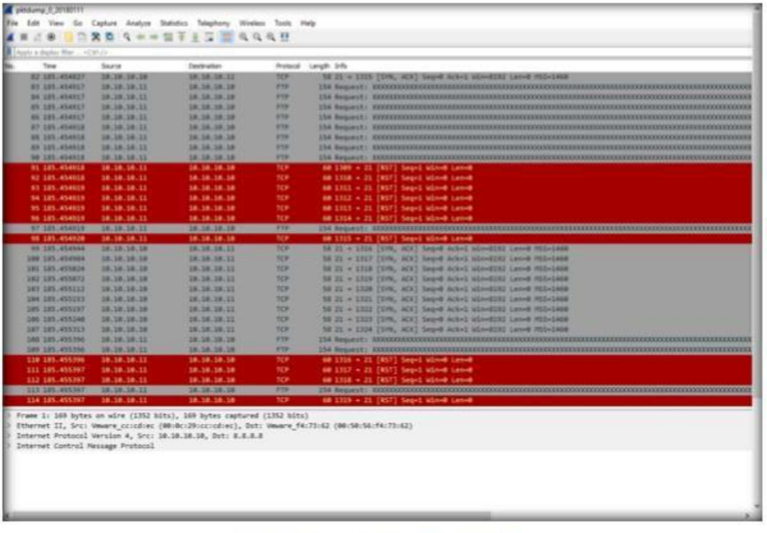

FIGURE 4.25: Analyzing the Packet Dump File

45. You may analyze the packets to get information related to headers of the packets, source IP Address, and so on.

Lab Analysis

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

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

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