Denial-of-Service

Module 09

Denial of Service

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

ICON KEY

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

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, you should have sound knowledge of Denial of Service and Distributed Denial of Service attacks in order to detect and neutralize attack handlers and mitigate such attacks. The labs in this module will give you 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

Tools demonstrated in this lab are available in C:\CEH-Tools\CEHv9 Module 09 Denial of Service

Lab Environment

To complete this lab, you will need:

- A computer running Window Server 2012 as host machine
- Windows 8.1 running in virtual machine
- Windows Server 2008 running in virtual machine
- Windows 7 running in virtual machine
- Kali Linux running in virtual machine
- A web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 75 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.

TASK 1

Overview

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**
- HTTP Flooding using **DoSHTTP**
- Implementing DoS Attack on a Router using **Slowloris** Script
- 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. Provide 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.

ICON KEY

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

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 of this lab is to help students understand how to:

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

Lab Environment

To perform this lab, you need:

- A computer running with Windows Server 2012 as Host machine
- Kali Linux running as a virtual machine
- Windows 8.1 running as a virtual machine

- **Wireshark** located at **D:\CEH-Tools\CEHv9 Module 09 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 sent by the source, 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 back 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 8.1** virtual machine.

TASK 1

Test for Open Port

1. Log into the **Kali Linux** virtual machine.
2. In this lab, we are going to perform **SYN flooding** on the Windows 8.1 machine through **port 4444**.
3. So, let us determine whether port 4444 is open or not. We shall be using nmap to determine state of the port.
4. Type the command **nmap -p 4444 [IP Address of Windows 8.1]** and press **Enter**.

Note: The IP address of **Windows 8.1** used in this lab is **10.0.0.4,** which might vary in your lab environment.

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

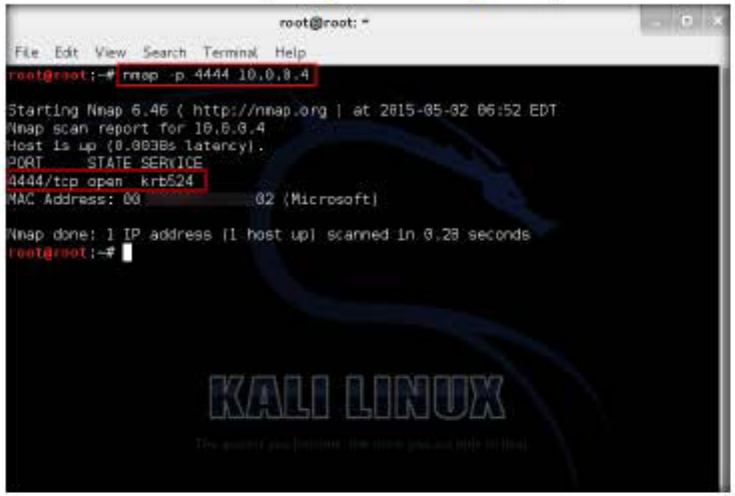


FIGURE 1.1: Checking for Open Port

6. Now that we got the result stating the port is open, let us begin to perform SYN flooding on the victim machine (Windows 8.1) using port 4444.
7. In this lab, we shall be using an auxiliary module named **synflood** to perform DoS attack on the machine. We need to launch this module from **msfconsole**.
8. Therefore, before launching msfconsole, you make sure that you have started postgresql and metasploit services.
9. If you have already started these services, skip to **step 10**.

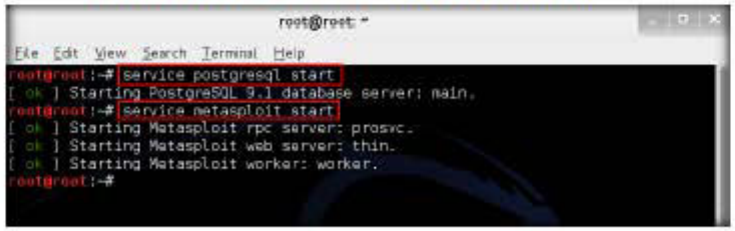


FIGURE 1.2: Starting Services

TASK 2

Perform DoS Attack

10. Type **msfconsole** from a command-line terminal, and press **Enter** to launch msfconsole.

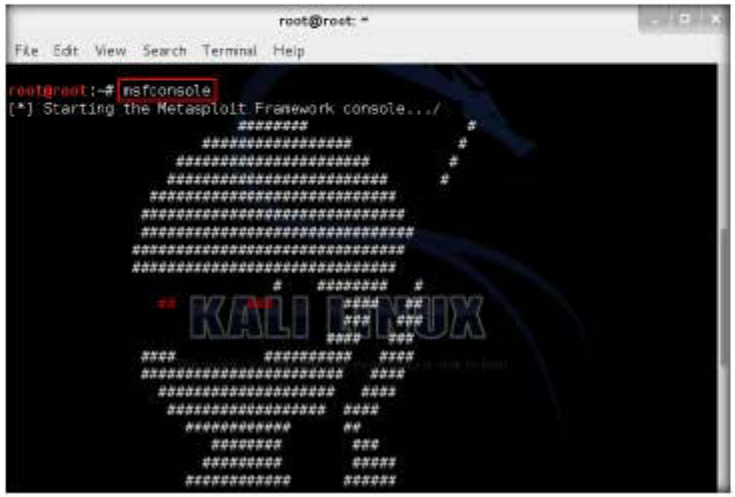


FIGURE 1.3: Launching msfconsole

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

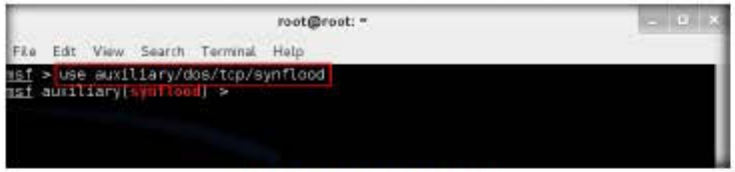


FIGURE 1.4: Using the Auxiliary Module

12. This launches the synflood module.
13. Let us determine what all module options need to be configured to begin the DoS attack.

14. So, type **show options** and press **Enter**. This displays all the options associated with the auxiliary module.

```
root@root: ~
File  Edit  View  Search  Terminal  Help
msf > use auxiliary/dos/tcp/synflood
msf auxiliary(synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   NUM                         no        Number of SYNs to send (else unlimited)
   RHOST                       yes       The target address
   RPORT      80               yes       The target port
   SHOST                       no        The spoofable source address (else rand
onizes)
   SNAPLEN    65535            yes       The number of bytes to capture
   SPORT                       no        The source port (else randomizes)
   TIMEOUT    500              yes       The number of seconds to wait for new d
ata

msf auxiliary(synflood) >
```

FIGURE 1.5: Viewing Options

15. Here, we shall be perform SYN flooding on port **4444** of the **Windows 8.1** machine by spoofing the IP Address of **Kali Linux** with that of the **Windows Server 2012** machine.

16. Issue the following commands:

    a. **set RHOSTS [IP Address of Windows 8.1]**

    b. **set RPORT 4444**

    c. **set SHOST [IP Address of Windows Server 2012]**

```
root@root: ~
File  Edit  View  Search  Terminal  Help
msf auxiliary(synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   NUM                         no        Number of SYNs to send (else unlimited)
   RHOST                       yes       The target address
   RPORT      80               yes       The target port
   SHOST                       no        The spoofable source address (else rand
onizes)
   SNAPLEN    65535            yes       The number of bytes to capture
   SPORT                       no        The source port (else randomizes)
   TIMEOUT    500              yes       The number of seconds to wait for new d
ata

msf auxiliary(synflood) > set RHOST 10.0.0.4
RHOST => 10.0.0.4
msf auxiliary(synflood) > set RPORT 4444
RPORT => 4444
msf auxiliary(synflood) > set SHOST 10.0.0.2
SHOST => 10.0.0.2
msf auxiliary(synflood) >
```

FIGURE 1.6: Configuring Options

17. By setting the SHOST option to **[IP Address of Windows Server 2012]**, you are spoofing the IP Address of Kali Linux machine with that of **Windows Server 2012**.
18. Now, you have configured the auxiliary module by setting the required options. Let us begin the DoS attack on **Windows 8.1** machine.
19. To begin, type **exploit** and press **Enter**.

```
msf auxiliary(synflood) > set RHOST 10.0.0.4
RHOST => 10.0.0.4
msf auxiliary(synflood) > set RPORT 4444
RPORT => 4444
msf auxiliary(synflood) > set SHOST 10.0.0.2
SHOST => 10.0.0.2
msf auxiliary(synflood) > exploit

[*] SYN flooding 10.0.0.4:4444...
```

FIGURE 1.7: Initiating DoS Attack

20. This begins the syn flooding on the **Windows 8.1** machine.

TASK 3

Examine the DoS Attack

21. To confirm, switch to the **Windows 8.1** machine, launch the **Wireshark** application, select an interface, and click **Start**.

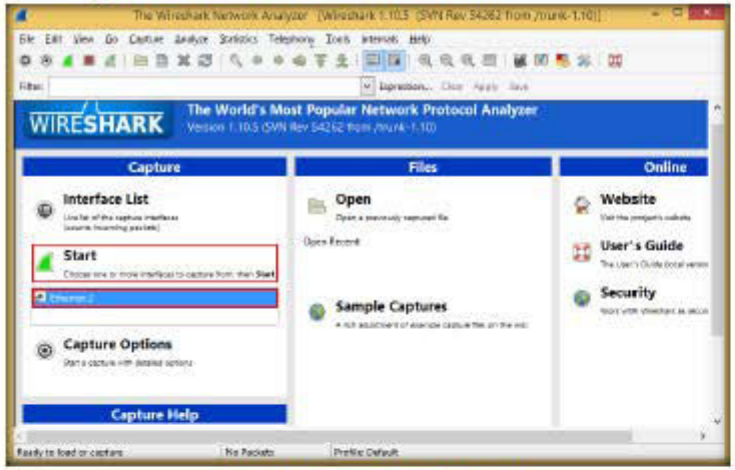


FIGURE 1.8: Capturing Traffic through Wireshark

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

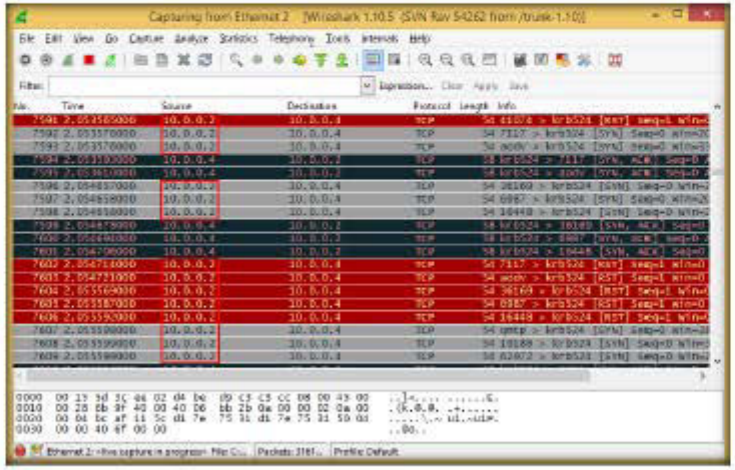


FIGURE 1.9: Analyzing the Traffic

23. Here, you can observe that the source IP address is that of the Windows Server 2012 machine. This implies that the IP Address of Kali Linux has been spoofed.

24. 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.

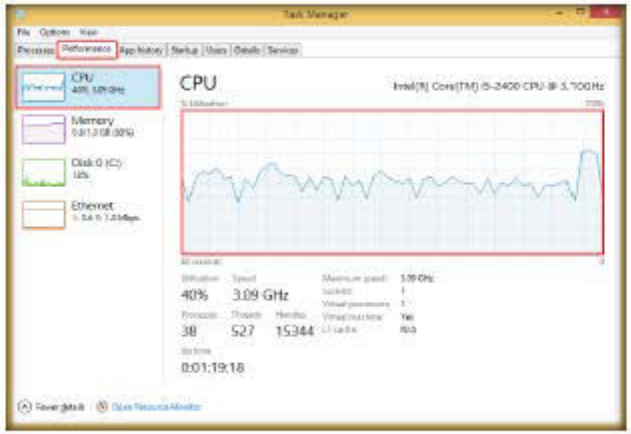


FIGURE 1.10: Analyzing the Machine's Performance

25. Once done on analyzing the performance of the machine, switch to the Kali Linux machine and press **Ctrl+C** to terminate the attack.

```
msf auxiliary(synflood) > exploit

[*] SYN flooding 10.0.0.4:4444...
^C[-] Auxiliary interrupted by the console user
[*] Auxiliary module execution completed
msf auxiliary(synflood) >
```

FIGURE 1.11: Terminating the Attack

26. 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. Provide 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

Lab 2

SYN Flooding a Target Host Using hping3

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

ICON KEY

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

Lab Scenario

A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt 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 simply not send the expected ACK, or by spoofing 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 can 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

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

First, type a simple command and see the result: #hping3 0.0-alpha-1> hping resolve www.google.com 66.102.9.104.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
  -R  --rst        set RST flag
  -P  --push       set PUSH flag
  -A  --ack        set ACK flag
  -U  --urg        set URG flag
  -X  --xmas       set X unused flag (0x40)
  -Y  --ymas       set Y unused flag (0x80)
  --tcpexitcode    use last tcp->th_flags as exit code
  --tcp-mss        enable the TCP MSS option with the given value
  --tcp-timestamp  enable the TCP timestamp option to guess the HZ/uptime
Common
  -d  --data       data size                    (default is 0)
  -E  --file       data from file
  -e  --sign       add 'signature'
  -j  --dump       dump packets in hex
  -J  --print      dump printable characters
  -B  --safe       enable 'safe' protocol
  -u  --end        tell you when --file reached EOF and prevent rewind
  -T  --traceroute traceroute mode                (implies --bind and --ttl 1)
  --tr-stop        Exit when receive the first not ICMP in traceroute mode
  --tr-keep-ttl    Keep the source TTL fixed, useful to monitor just one hop
  --tr-no-rtt       Don't calculate/show RTT information in traceroute mode
ARS packet description (new, unstable)
  --apd-send       Send the packet described with APD (see docs/APD.txt)
root@kali:~#
```

FIGURE 2.2: Kali Linux Command Shell with hping3

6. In command shell, type **hping3 -S 10.0.0.4 -a 10.0.0.6 -p 22 –flood** and press **Enter**.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# hping3 -S 10.0.0.4 -a 10.0.0.6 -p 22 --flood
```

FIGURE 2.3: Launching flooding attack using hping3

7. In the above command, **10.0.0.4 (Windows 8.1)** is the **victim** machine's IP address, and **10.0.0.6 (Kali Linux)** is the **attacker** machine's IP address. This initiates the SYN flooding on Windows 8.1.

The hping3 command should be called with a subcommand as a first argument and additional arguments according to the particular subcommand.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# hping3 -S 10.0.0.4 -a 10.0.0.6 -p 22 --flood
HPING 10.0.0.4 (eth0 10.0.0.4): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

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 8.1**). Install and launch Wireshark, select an interface, and start capturing.
10. You will observe that the application captures traffic, as shown in the screenshot:

hping3 was mainly used as a security tool in the past. It can be used in many ways by people who don't care for security to test networks and hosts. A subset of the things you can do using hping3:

- Firewall testing
- Advanced port scanning
- Network testing, using various protocols, TOS, fragmentation
- Manual path MTU discovery
- Advanced traceroute, under all the supported protocols
- Remote OS fingerprinting
- Remote uptime guessing
- TCP/IP stacks auditing

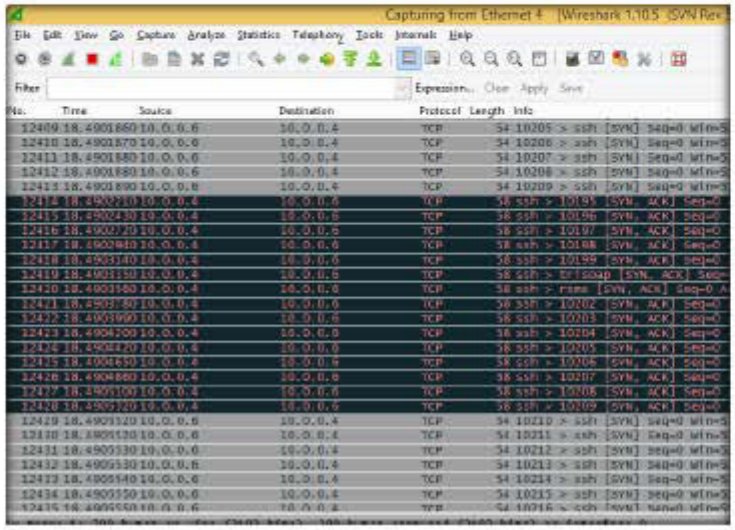


FIGURE 2.5: Wireshark with Packets Traffic

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

Lab Analysis

Document all the results gather 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

HTTP Flooding using DoSHTTP

DoSHTTP is an HTTP Flood Denial of Service (DoS) testing tool for Windows. DoSHTTP includes port designation and reporting.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise

Lab Scenario

HTTP flooding is an attack that uses enormous useless packets to jam a Web server. In this lab, we use hidden semi-Markov models (HSMM) to describe Web-browsing patterns and detect HTTP flooding attacks. We first use a large number of legitimate request sequences to train an HSMM model and then use this legitimate model to check each incoming request sequence. Abnormal Web traffic whose likelihood falls into unreasonable range for the legitimate model would be classified as potential attack traffic and should be controlled with special actions such as filtering or limiting the traffic. Finally, we validate our approach by testing the method with real data. The result shows that our method can detect the anomaly Web traffic effectively.

In the previous lab, you have learnt SYN flooding using hping3 and the countermeasures that can be implemented to prevent such attacks. Another method that attackers can use to attack a server is by using HTTP flood approach.

As an expert Ethical Hacker and Penetration Tester, you must be aware of all types of hacking attempts on a web server. For HTTP flooding attack, you should implement an advanced technique known, as "Tarpitting" which once established successfully will set connections window size to few bytes. According to TCP/IP protocol design, the connecting device will initially only send as much data to target as it takes to fill the window until the server responds. With "Tarpitting," there will be no response back to the packets for all unwanted HTTP requests, thus protecting your web server.

Lab Objectives

The objective of this lab is to help students learn how an HTTP Flooding DoS attack works.

Lab Environment

To carry out this lab, you will need:

- **DoSHTTP** tool located at **D:\CEH-Tools\CEHv9 Module 09 Denial of Service\DoS and DDoS Attack Tools\DoSHTTP**
- You can also download the latest version of DoSHTTP from the link http://www.socketsoft.net/
- If you decide to download the latest version, then screenshots shown in the lab might differ
- A computer running Windows Server 2012 as host machine
- Windows 8.1 running on virtual machine as attacker machine
- A web browser with an Internet connection
- Administrative privileges to run tools

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 09 Denial of Service

Lab Duration

Time: 5 Minutes

Overview of DoSHTTP

DoSHTTP is an HTTP Flood DoS Testing Tool for Windows. It includes URL Verification, HTTP Redirection and performance monitoring. DoSHTTP uses multiple asynchronous sockets to perform an effective HTTP Flood. DoSHTTP can be used simultaneously on multiple clients to emulate a Distributed Denial of Service (DDoS) attack. This tool is used by IT professionals to test web server performance.

Lab Tasks

TASK 1

Install and Configure DoSHTTP

1. Before beginning this lab, log in to **Windows 8.1** virtual machine.
2. Launch the **Wireshark** network protocol analyzer, select an interface, and start capturing.
3. Switch back to the host machine (Windows Server 2008), navigate to **D:\CEH-Tools\CEHv9 Module 09 Denial of Service\DoS and DDoS Attack Tools\DoSHTTP**, double-click **doshttp_setup.exe,** and follow the wizard-driven installation steps to install **DosHTTP**.

Note: If the **open File - Security Warning** pop-up appears, click **Run**.

DoSHTTP is an easy to use and powerful HTTP Flood Denial of Service (DoS) Testing Tool for Windows. DoSHTTP includes URL Verification, HTTP Redirection, Port Designation, Performance Monitoring and Enhanced Reporting

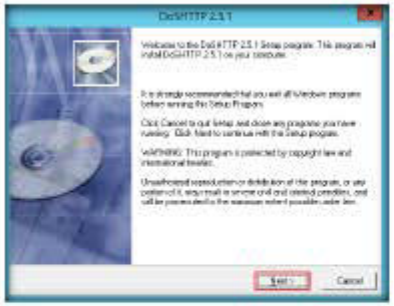


FIGURE 3.1: DoSHTTP installation wizard

4. On completing the installation, launch **DoSHTTP 2.5** from the **Apps** screen.

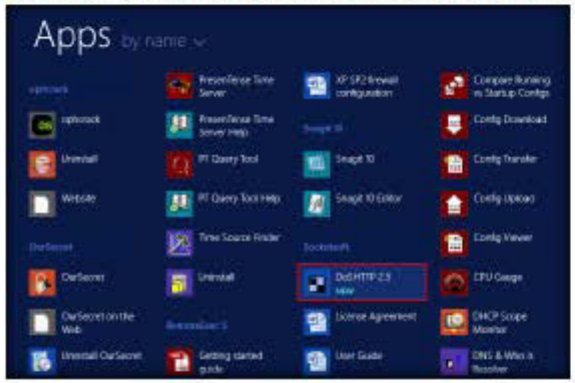


FIGURE 3.2: Launching application from Apps screen

5. A **license Agreement** window appears; click **I Accept**.

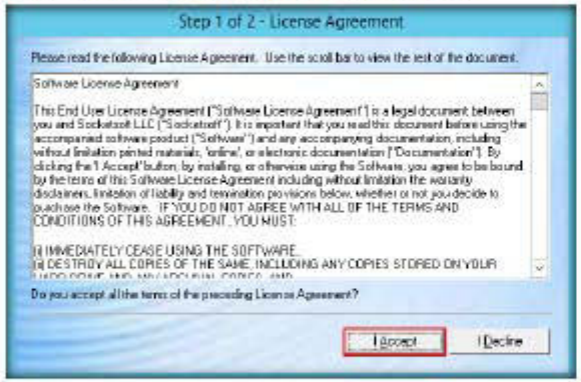


FIGURE 3.3: license Agreement window

6. A **Legal Disclaimer** window appears; click **I Accept**.

FIGURE 3.4: Legal Disclaimer window

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 09 Denial of Service

7. It takes some time for DoSHTTP to load as well as check for updates when you launch it the first time.
8. The DoSHTTP main window appears, along with a **DoSHTTP Registration** dialog box. Click **Try**.

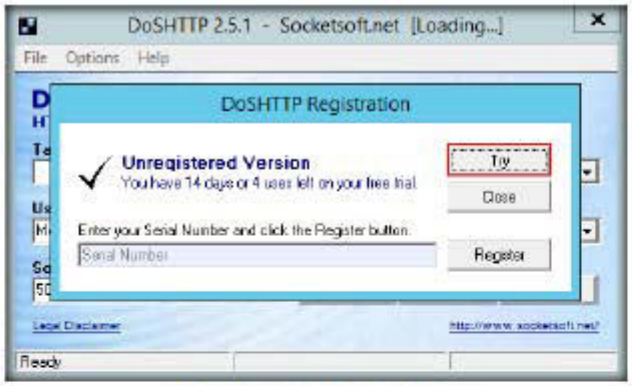


FIGURE 3.5: DoSHTTP Registration dialog box

DoSHTTP includes Port Designation and Reporting.

9. The DoSHTTP main window appears; enter the IP address of the target machine (**Windows 8.1** virtual machine) in the **Target URL** text field.

TASK 2

Perform HTTP Flooding

DoSHTTP uses multiple asynchronous sockets to perform an effective HTTP Flood. DoSHTTP can be used simultaneously on multiple clients to emulate a Distributed Denial of Service (DDoS) attack.

10. Leaving the other options set to default, click **Start Flood** to begin HTTP flooding on the target machine.

FIGURE 3.6: DoSHTTP main window

Note: **10.0.0.4** is the IP address of **Windows 8.1** virtual machine, which may differ in your lab environment.

11. The **DoSHTTP** evaluation pop-up appears; click **OK**.

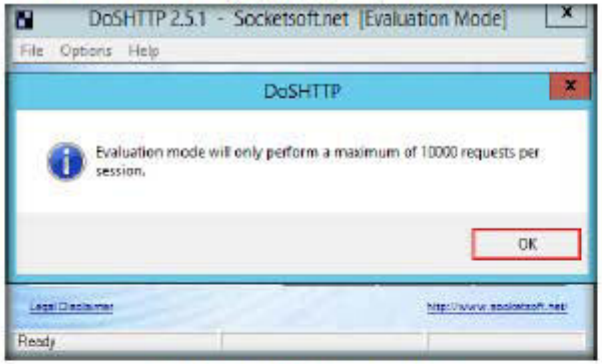


FIGURE 3.7: DoSHTTP Evaluation mode pop-up

DoSHTTP can help IT Professionals test web server performance and evaluate web server protection software. DoSHTTP was developed by certified IT Security and Software Development professionals.

12. DoSHTTP sends **asynchronous** sockets and performs **HTTP flooding** on the target network.
13. It returns an **HTTP Flood Test Report,** displaying results such as request rate, duration, target port, number of packets sent, and so on.

14. **Close** the Report.

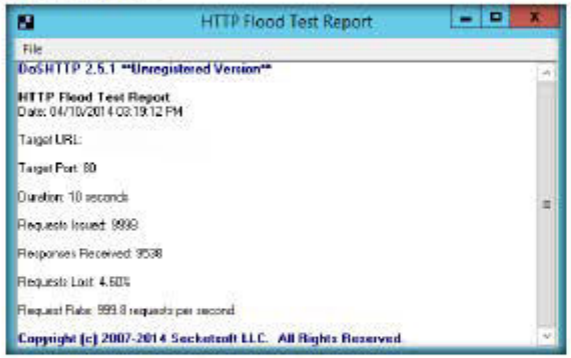
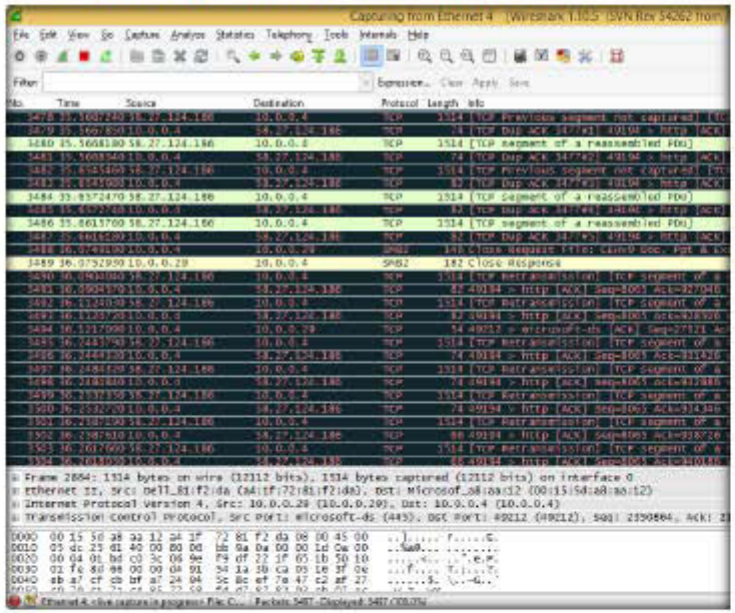


FIGURE 3.8: HTTP Flood Test Report

15. Switch back to the **Windows 8.1** virtual machine. You will observe that the application captures a lot of traffic as shown in the screenshot:



DoSHTTP can be used simultaneously on multiple clients to emulate a Distributed Denial of Service (DDoS) attack.

FIGURE 3.9: Wireshark window displaying traffic

16. You can conclude that many HTTP packets are **flooded** onto the host machine.

17. In real time, attackers choose a target and perform a DoS attack on it, causing the target to stop responding to any more requests coming from others and starts dropping packets coming even from legitimate users.

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

Implementing DoS Attack on a Router Using Slowloris Script

Slowloris script opens and maintains numerous "half-HTTP" connections until the server runs out of resources, leading to a denial of service.

Lab Scenario

As an ethical hacker and pen tester, you can use Slowloris script to audit your network against DoS attacks. When a successful DoS is detected, the script stops the attack and returns these pieces of information (which may be useful to tweak further filtering rules):

- Time taken until DoS
- Number of sockets used
- Number of queries sent

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise

Lab Objectives

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

Lab Environment

To complete this lab, you will need:

- **Slowloris.pl** file located at **D:\CEH-Tools\CEHv9 Module 09 Denial of Service\DoS and DDoS Attack Tools\Slowloris**
- A computer running Windows Server 2012 as host machine
- Kali Linux running on virtual machines as Attacker machine
- Administrative privileges to run tools

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 09 Denial of Service

Lab Duration

Time: 10 Minutes

Overview of Lab

The Slowloris script opens two connections to the server, each without the final CRLF. After 10 seconds, second connection sends additional header. Both connections then wait for server timeout. If second connection gets a timeout 10 or more seconds after the first one, we can conclude that sending additional header prolonged its timeout and that the server is vulnerable to Slowloris DoS attack.

A "LIKELY VULNERABLE" result means a server is subject to timeout-extension attack, but depending on the http server's architecture and resource limits, a full denial of service is not always possible. Complete testing requires triggering the actual DoS condition and measuring server responsiveness..

Lab Tasks

TASK 1

Log In to Virtual Machines

1. Launch the **Kali Linux** virtual machine from **Hyper-V Manager,** and log into it.
2. Before starting this lab, launch Wireshark to capture DoS traffic. To launch Wireshark, open a command terminal, type **wireshark** and press **Enter**.

FIGURE 4.1: Launching Wireshark

3. The **Lua: Error during loading** pop-up appears; click **OK** to continue.

FIGURE 4.2: Lua: Error during loading pop-up

4. The **Running as User root window** appears; check **Don't show this message again,** and click **OK** to continue.

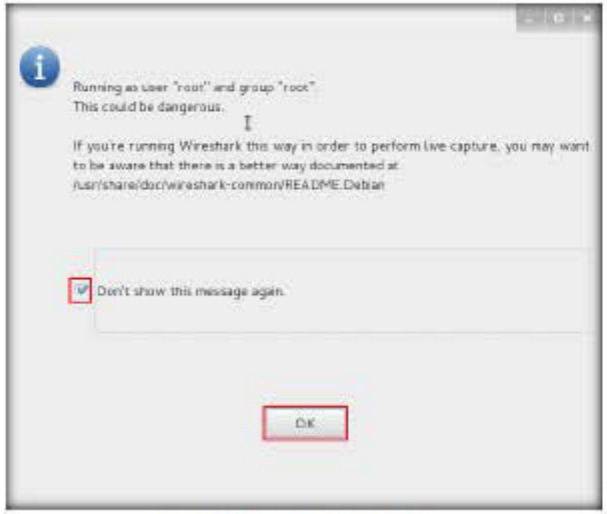


FIGURE 4.3: Running as User root Window

5. The Wireshark main window appears; choose the **interface**, and then click **Start** to capture the traffic.
6. After clicking **Start** to capture the traffic, leave the Wireshark window **open** or **minimize** the window.

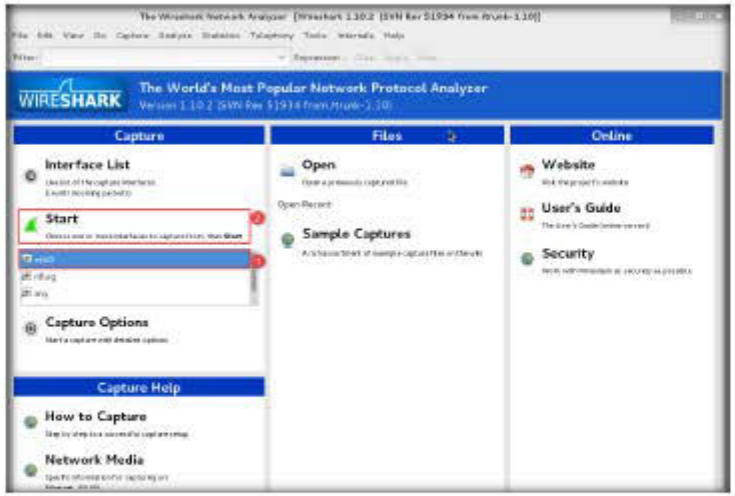


FIGURE 4.4: Starting Capture

7. Now, navigate to the **Desktop,** and double-click **Computer**.

FIGURE 4.5: Launch Computer

8. The **Computer** window appears; click **Go** from the menu bar, and select **Location...**.

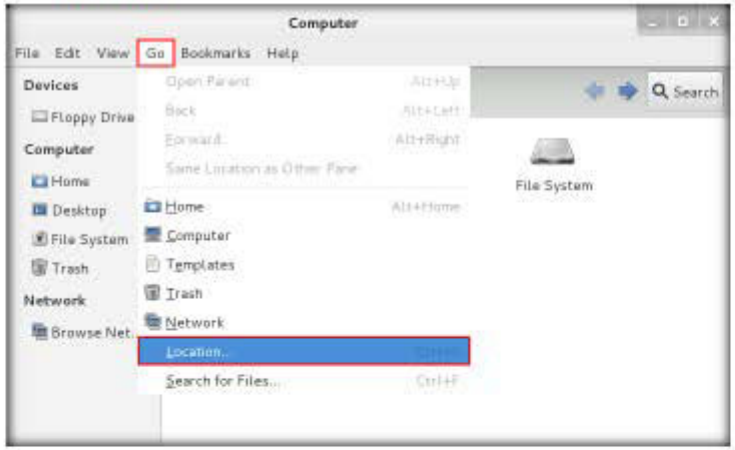


FIGURE 4.6: Go to Location

9. Type **smb://[IP address of Windows Server 2012]** in the **Go To** field, and press **Enter**.

   Note: In this lab, the IP Address of **Windows Server 2012** is **10.0.0.2**, which might differ in your lab environment.

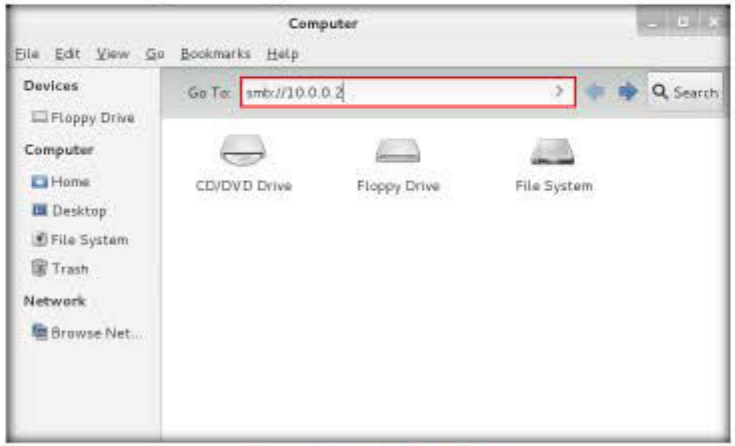


FIGURE 4.7: Connect Through Samba Share

   Note: If you are asked to enter credentials, input the credentials for Windows Server 2012, click **Remember forever,** and click **Connect**.

10. A window appears, displaying the **CEH-Tools** shared network drive.

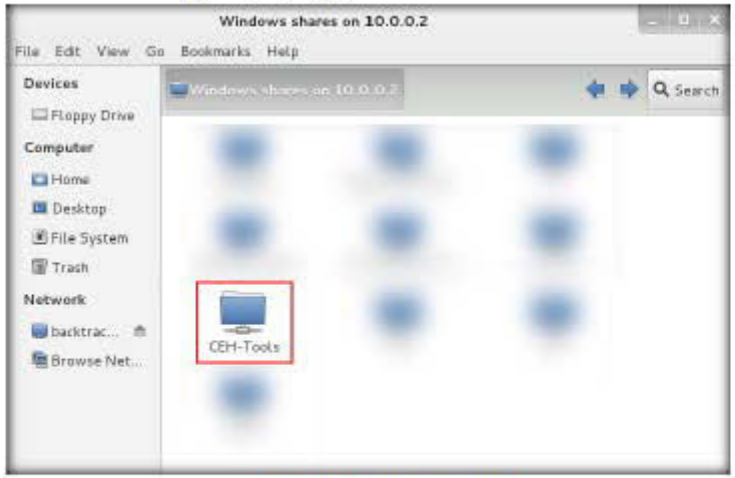


FIGURE 4.8: CEH-Tools Shared Network Drive

11. Double-click **CEH-Tools** network drive, and navigate to **CEHv9 Module 09 Denial of Service → DoS and DDoS Attack Tools → Slowloris,** right-click **slowloris.pl,** and choose **Copy** from the context menu and paste the file on Kali Linux Desktop.

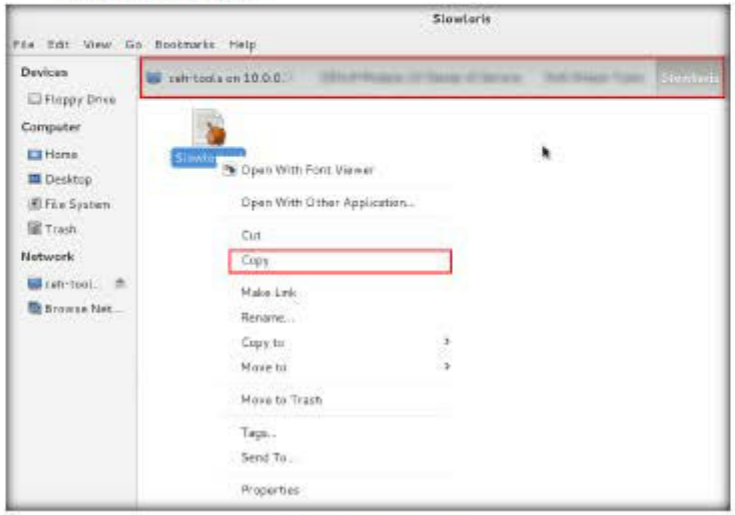


FIGURE 4.9: Copying the File

12. The **Slowloris.pl** file is pasted on your Kali Linux desktop, as shown in the following figure.

FIGURE 4.10: Pasting the File

13. Now, open a command terminal, type **cd Desktop** and press **Enter** to change the directory to the Desktop.

FIGURE 4.11: Changing Directory

14. Set full permissions to Slowloris.pl file by using the **chmod** command.

15. Now, type **chmod 777 Slowloris.pl** and press **Enter**. This command will set **Read**, **Write**, and **Execute** permissions for the file.

```
root@kali:~/Desktop# chmod 777 Slowloris.pl
root@kali:~/Desktop#
```

FIGURE 4.12: Changing Permissions

16. Check the list of files available on desktop by typing **ls** and pressing **Enter**.

```
root@kali:~/Desktop# chmod 777 Slowloris.pl
root@kali:~/Desktop# ls
Slowloris.pl
root@kali:~/Desktop#
```

FIGURE 4.13: Viewing the File

17. Perform the DoS attack on your router IP address by running this command: **./Slowloris.pl -dns <IP address of the Target Router>** (type the command and press **Enter**).

18. In this lab, we are using our local router, with the IP address **10.0.0.1**.

    Note: The IP address may differ in your lab environment.

```
root@kali:~/Desktop# chmod 777 Slowloris.pl
root@kali:~/Desktop# ls
Slowloris.pl
root@kali:~/Desktop# ./Slowloris.pl -dns 10.0.0.1
```

FIGURE 4.14: Performing Attack

19. Once you press **Enter**, the pearl script displays scrolling text, as shown in the screenshot.

```
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Sending data.
Current stats:  Slowloris has now sent 514 packets successfully.
This thread now sleeping for 100 seconds...

                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
```

FIGURE 4.15: Performing Attack

20. Maximize the Wireshark window, and observe the DoS traffic.

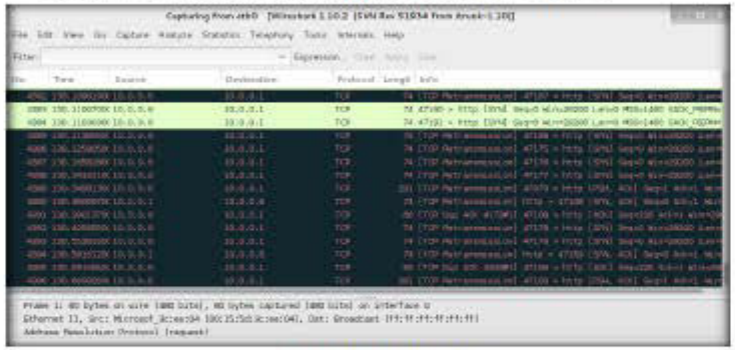


FIGURE 4.16: Checking DoS Traffic

21. Now, open a web browser in your Kali Linux machine, type your router IP address, and press **Enter**.

22. In this lab, the router IP address is **10.0.0.1**. As you have performed the DoS attack, it should not open as shown in the figure.

FIGURE 4.17: Browsing Router Web Panel

23. To stop the DoS attack, press **Ctrl+C** in the Slowloris.pl command terminal.

FIGURE 4.18: Stopping the Attack

24. Once you press **Ctrl+C,** you can access your router page, as shown in the screenshot.

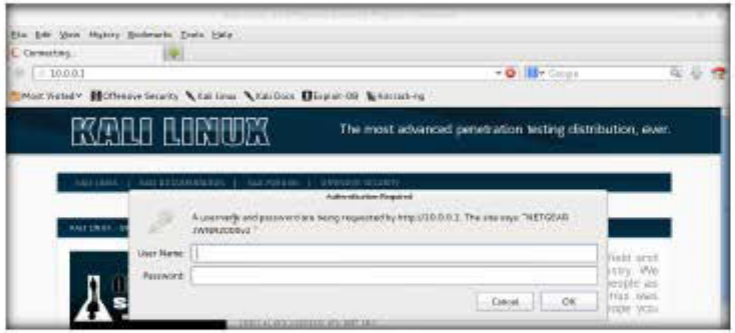


FIGURE 4.19: Accessing Router

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 5

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

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise

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 to the target system essentially forces it 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 **D:\CEH-Tools\CEHv9 Module 09 Denial of Service\DoS and DDoS Attack Tools\Hoic Version 2.1**
- You can also 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
- A computer running Windows Server 2012 as host machine
- Windows Server 2008, Windows 8.1 and Windows 7 running on virtual machines as attacker machines
- Kali Linux running on virtual machines as target machine
- Administrative privileges to run tools

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 09 Denial of Service

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

TASK 1

Log In to Virtual Machines

1. Before beginning this lab, log into the **Windows 8.1**, **Windows Server 2008**, **Windows 7,** and **Kali-Linux** virtual machines.
2. In the **Windows 8.1** virtual machine, navigate to **Z:\CEHv9 Module 09 Denial of Service\DoS and DDoS Attack Tools** and copy the **Hoic Version 2.1** folder onto the **Desktop**.

Note: To perform the DDoS attack, you will be running 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, you need to copy the folder *containing* the folder Hoic Version 2.1 individually onto each machine, and then run the tool.

3. Similarly, follow the previous step and copy the **Hoic Version 2.1** folder onto the other virtual machines' respective Desktops.

TASK 2

Configure HOIC

4. Now, switch to the **Window 8.1** virtual machine.
5. Navigate to the **Desktop**, open **Hoic Version 2.1,** and double-click **hoic2.1.exe**.
6. HOIC GUI appears on the screen, click "**+**" (below **TARGETS**).

FIGURE 5.1: 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.

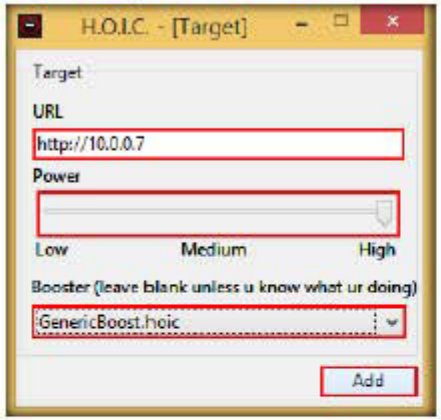


FIGURE 5.2: HOIC - [Target] pop-up

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

FIGURE 5.3: Setting the THREADS value

9. Now, switch to **Windows Server 2008** and **Windows 7** virtual machine and follow the **steps 5-8** to launch HOIC and configure it.

TASK 3

Perform DDoS Attack

10. Once you have configured HOIC on all the machines, switch to each machine and click **FIRE THE LAZER!**.

FIGURE 5.4: 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**.

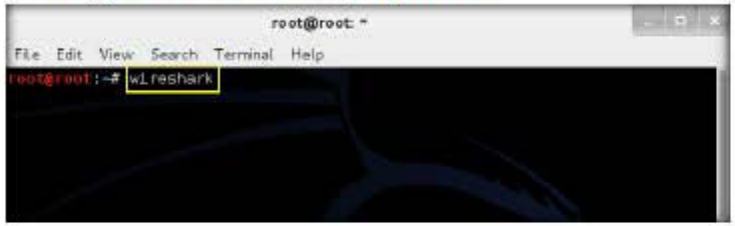


FIGURE 5.5: Launching Wireshark

14. An **Error** pop-up appears; click **OK**.

FIGURE 5.6: Error pop-up

15. Another dialog box appears; click **OK**.

FIGURE 5.7: Clicking OK in the dialog-box

16. The Wireshark GUI appears; select the network interface **eth0** and click **Start**.

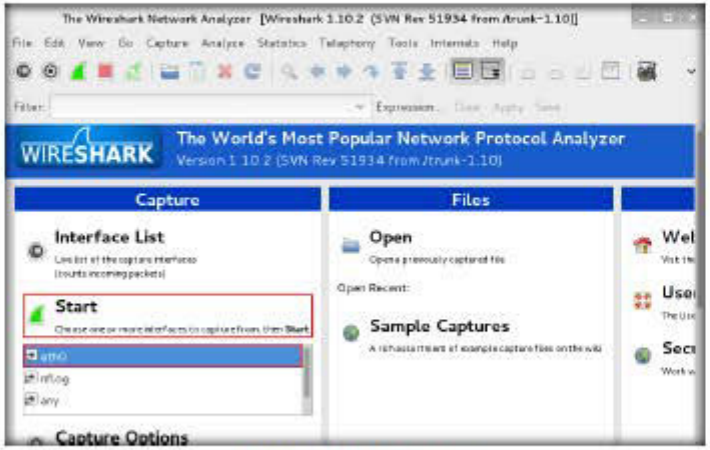


FIGURE 5.8: Starting Wireshark Capture

17. 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 2008**, **Windows 8.1** and **Windows 7** virtual machines.

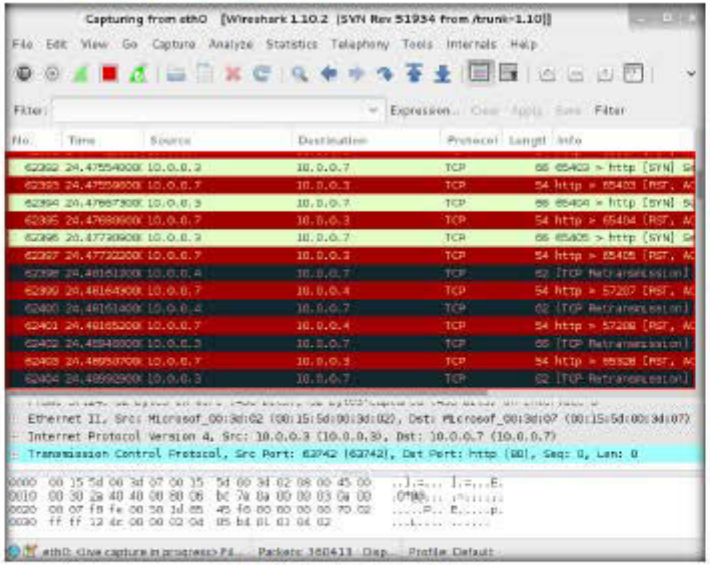


FIGURE 5.9: Wireshark Capturing the Packets

18. 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, its response slowing down.
19. In this lab, only three machines are demonstrated to perform flooding onto a single machine. If there are a large number of machines performing this flooding, then the target Kali Linux machine's resources are completely consumed and the machine is overwhelmed.
20. 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 specific 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.
21. On completion of the lab, click **FIRE THE 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

6

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.

ICON KEY

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

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 provide a higher level of information than can be achieved by using 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:

- A computer running with Windows Server 2012 as Host machine
- Kali Linux running as a virtual machine

- Windows 8.1 running as a virtual machine
- **KFSensor** located at **D:\CEH-Tools\CEHv9 Module 09 Denial of Service\DoS and DDoS Protection Tools\KFSensor**
- The latest version of KFSensor can be available at http://www.keyfocus.net/kfsensor/download
- **Wireshark** located at **D:\CEH-Tools\CEHv9 Module 09 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 8.1) 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 8.1** and **Kali Linux** virtual machines before beginning this lab.

TASK 1

Install KFSensor

1. In **Windows 8.1** virtual machine, navigate to **Z:\CEHv9 Module 09 Denial of Service\DoS and DDoS Protection Tools\KFSensor** and double-click **kfsens40.exe**.
2. If a **User Account Control** pop-up appears, click **Yes**.
3. If a **Windows Security** dialog-box appears asking you to enter network credentials, enter the credentials of **Windows Server 2012**.

4. The **KFSensor setup** window appears; follow the wizard-driven installation steps to install the application.

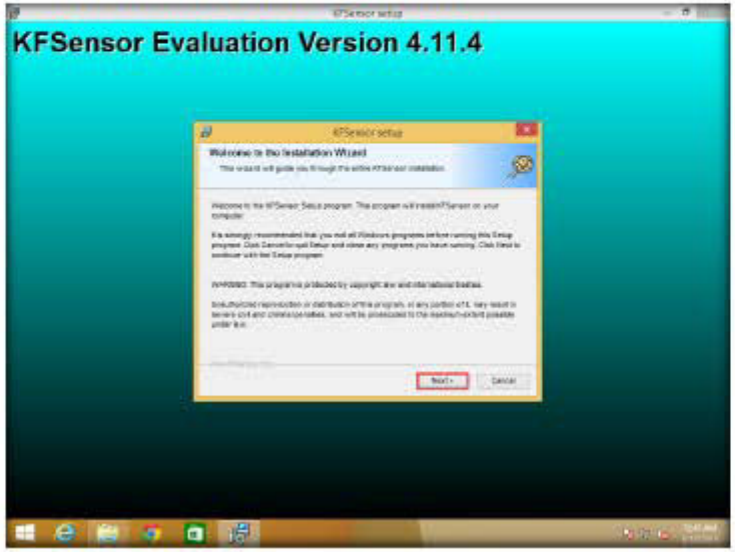


FIGURE 6.1: KFSensor setup Window

5. On completing the installation, you will be asked to reboot the computer for complete installation to occur.
6. So, select **Yes, reboot my computer now** and click **Next**.

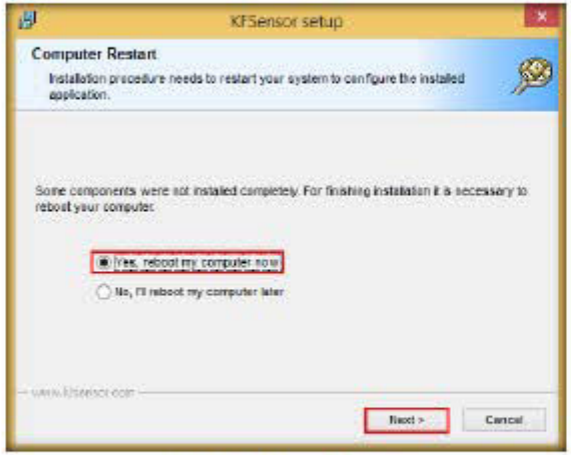


FIGURE 6.2: Rebooting the Machine

7. Wait for the machine to reboot.
8. After the reboot, log in to the machine. The KFSensor main window appears, along with a KFSensor dialog box stating that you need to run the application as an administrator. Click **Yes**.

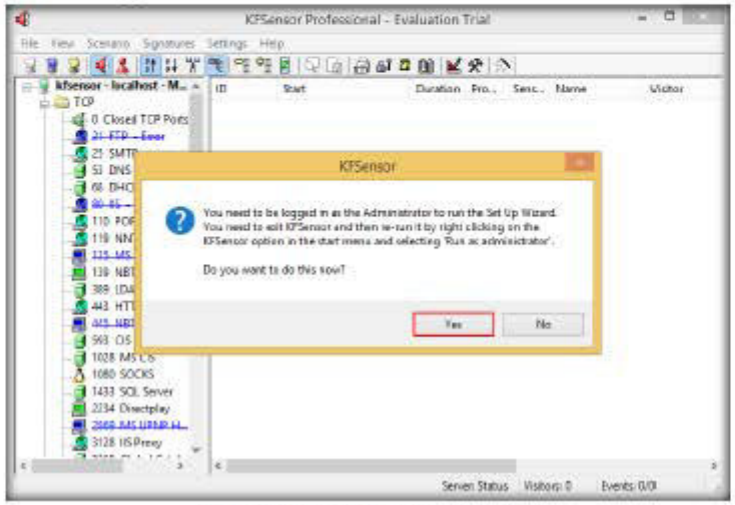


FIGURE 6.3: Launching KFSensor as an Administrator

9. Go to the **Apps** screen, right click on **KFSensor** application and click on **Run as administrator** (at the bottom of the screen).

FIGURE 6.4: Launching KFSensor as an Administrator

TASK 2

Configure KFSensor

10. If the **User Account Control** pop-up appears, click **Yes**.
11. When the application is being launched for the first time, the **KFSensor setup wizard** appears; click **Next** button.

FIGURE 6.5: KFSensor Setup Wizard

12. In the **Port Classes** window, check all the **port classes** to include, and click **Next**.

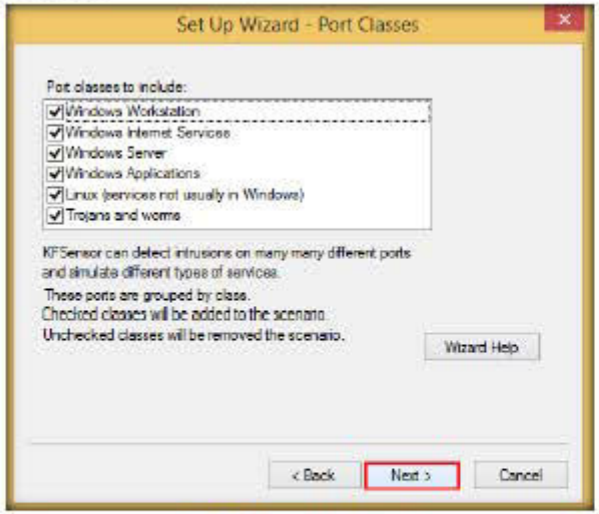


FIGURE 6.6: Port Classes Wizard

13. In the **Native Services** wizard, check all the ports with all active native services, and click **Next**.

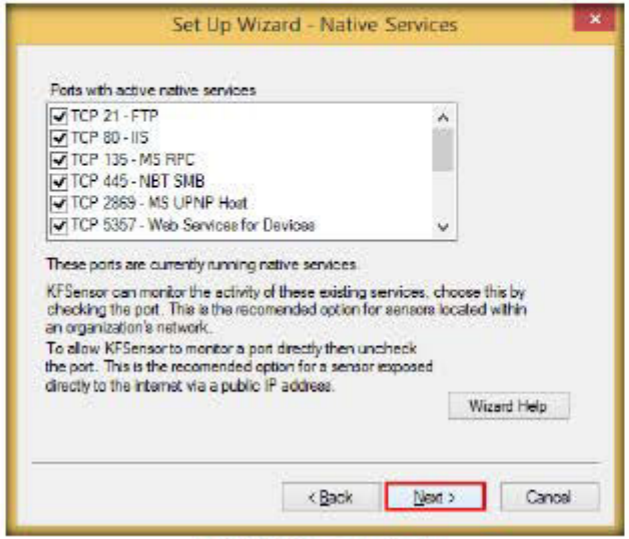


FIGURE 6.7: Native Services Wizard

14. In the **Domain** window, leave the **Domain name** field set to default, and click **Next**.

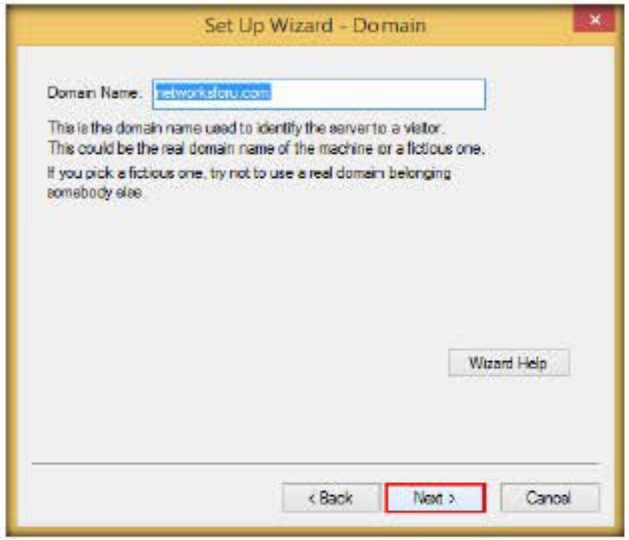


FIGURE 6.8: Domain wizard

15. In the **EMail Alerts** window, leave the options set to default, and click **Next**.

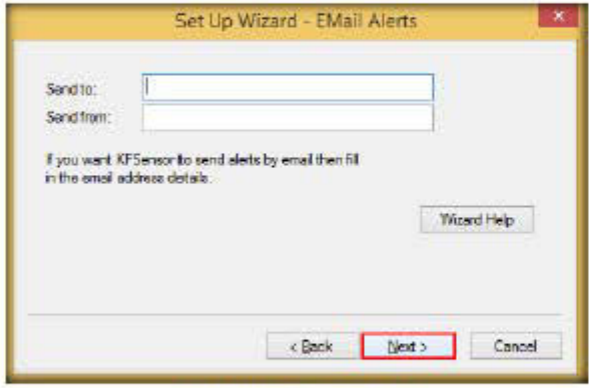


FIGURE 6.9: EMail Alerts Wizard

16. In the **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
17. Click **Next**.
18. This sets the DoS options to Cautious mode and saves the packet dump files at the time of the DoS attack.

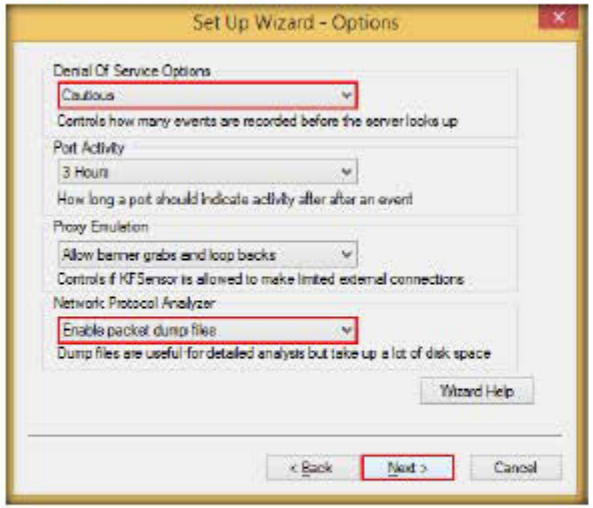


FIGURE 6.10: Options Wizard

19. In the **Systems Service** wizard, leave the option set to default, and click **Next**.

FIGURE 6.11: Systems Service Wizard

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

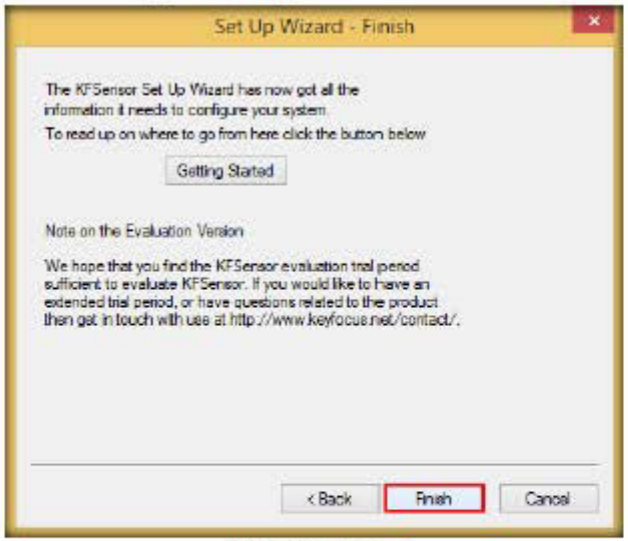


FIGURE 6.12: End of Wizard

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

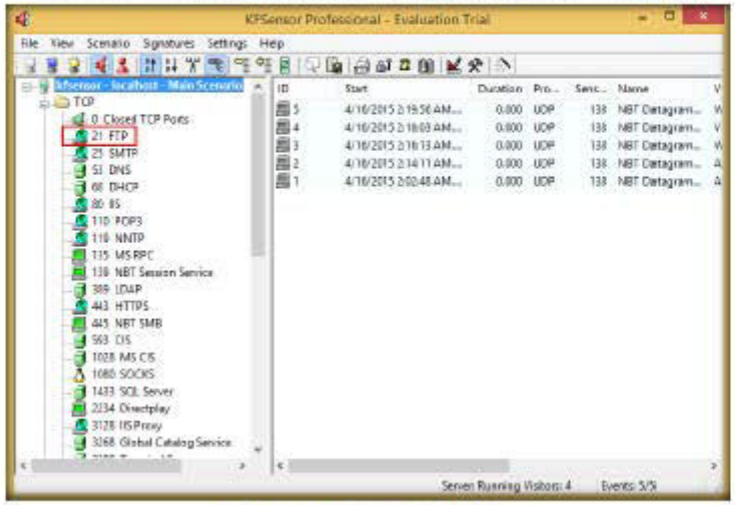


FIGURE 6.13: KFSensor Professional Window

22. Observe that the color of FTP icon is green, and the FTP section is empty, which means there is currently no traffic through port 21.

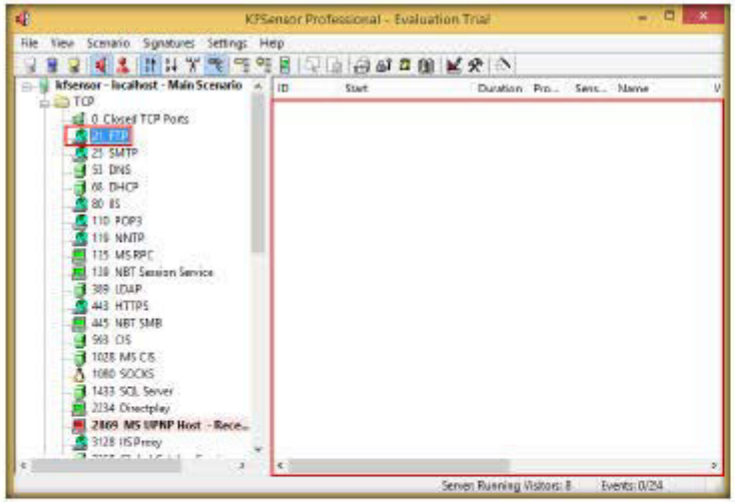


FIGURE 6.14: Viewing FTP Section

23. Now, KFSensor is configured to detect the DoS attacks that would be performed on the **Windows 8.1** machines from this point forward.

TASK 3

Perform DoS Attack

24. So, we will perform a DoS attack on this machine through **port 21** from an attacker machine, Kali Linux.
25. Switch to the **Kali Linux** virtual machine and open a command prompt. Our first task is to check whether **port 21** is open on the target machine by using nmap.
26. The command used to check the status of this port is **nmap -p 21 [IP Address of Windows 8.1]**.

Note: The IP Address of **Windows 8.1** machine in this lab is **10.0.0.4,** which might differ in your lab environment.

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

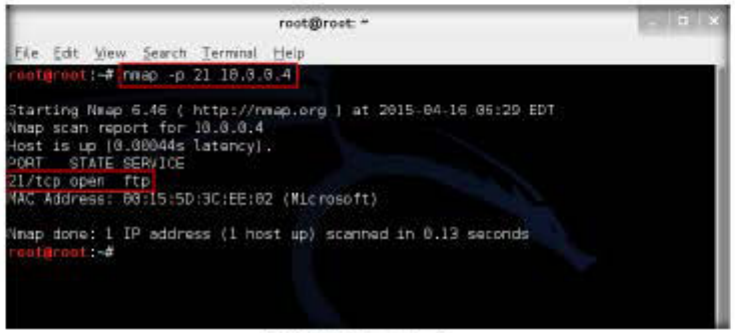


FIGURE 6.15: Testing FTP Port

28. So, you will be using this port to flood the victim machine.
29. We will be performing **SYN** flooding on the victim machine using hping3.
30. To begin flooding, type the command **hping3 -d 100 -S -p --flood [IP Address of Windows 8.1]** and press **Enter**.

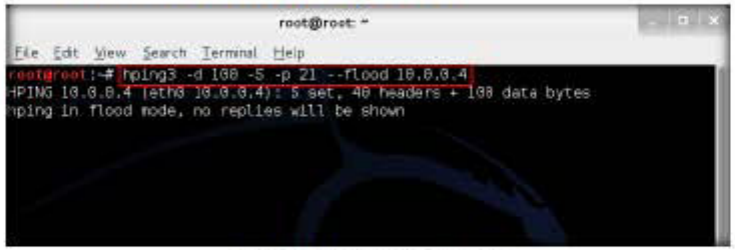


FIGURE 6.16: Flooding the Victim Machine

31. 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**).

32. Once you enter the command, switch back to the **Windows 8.1** machine and try to explore it. Observe that the machine's screen is frozen, which means that the resources of Windows 8.1 are completely exhausted. This means that the DoS attack is being successfully performed.

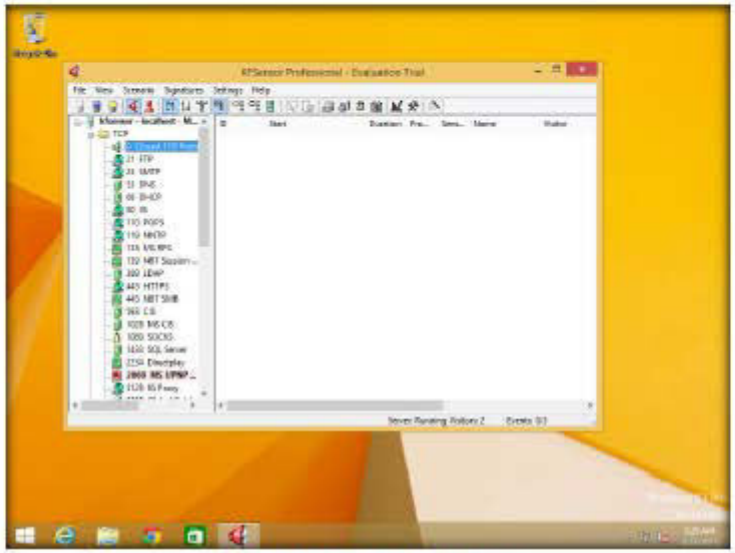


FIGURE 6.17: Victim Machine Failed to Respond

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

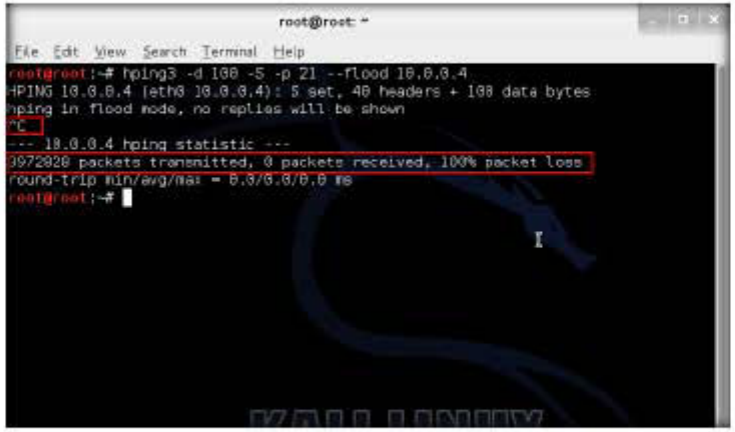


FIGURE 6.18: Scan Terminated

TASK 4

Detect DoS Attack

34. Switch back to the **Windows 8.1** machine; you should now be able to access it.
35. Observe that the color of the FTP icon in the left pane has changed to red, and the FTP section in the right pane is flooded with a list of events.
36. Scroll down the section; you can see an event with the name "DOS Attack."

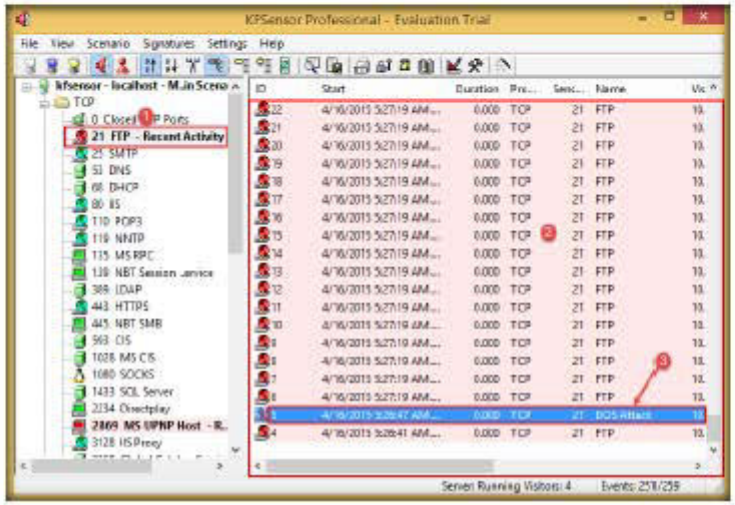


FIGURE 6.19: FTP Section Flooded with DOS Attack Events

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

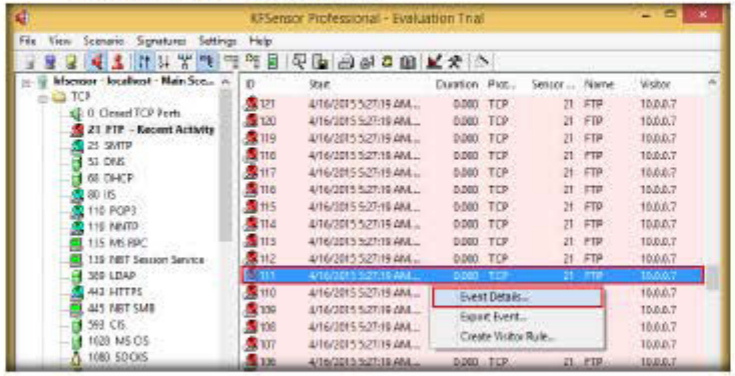


FIGURE 6.20: Viewing the Event Details

39. 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:

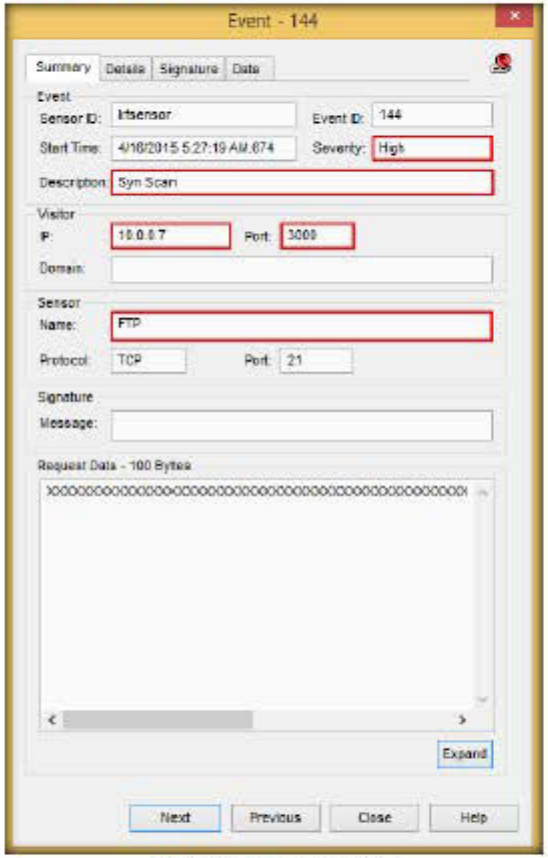


FIGURE 6.21: Viewing the Event Details

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

41. Now, we will 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.

42. To view the packet dump, you need to use a packet capturing application such as Wireshark.

43. Install and launch Wireshark, located at **D:\CEH-Tools\CEHv9 Module 09 Denial of Service\Wireshark**. If the application is already installed, simply launch it from the **Apps** screen.

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

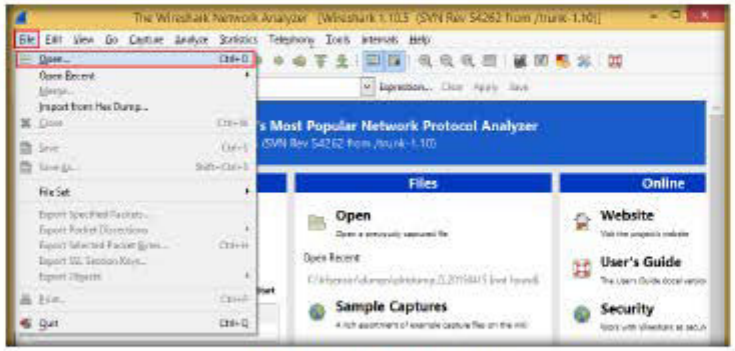


FIGURE 6.22: Opening the Packet Dump File

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

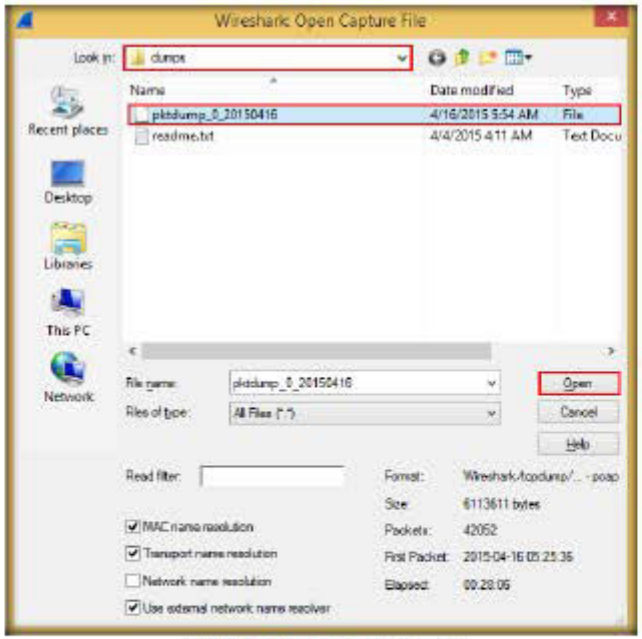


FIGURE 6.23: Opening the Packet Dump File

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

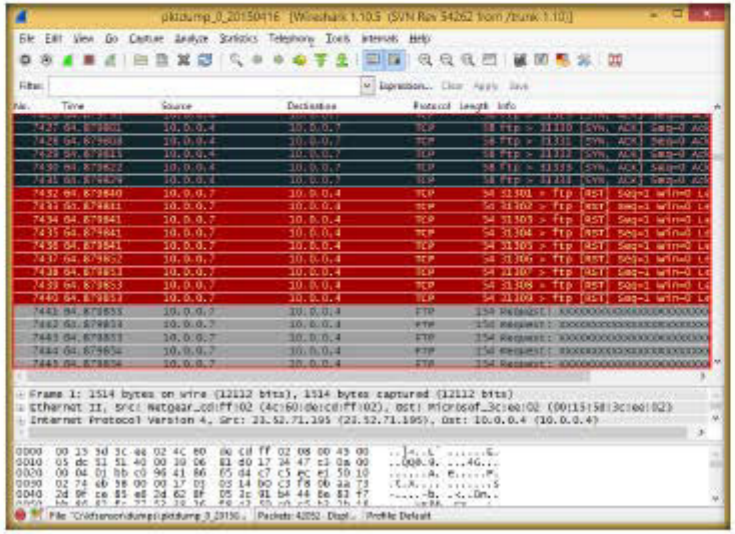


FIGURE 6.24 Analyzing the Packet Dump File

47. 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. Provide 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