

Lab 8: Performing a Denial of Service Attack from the WAN

Objective:

1. TCP Flood
2. UDP Flood
3. HTTP Flood

Takeaways:

1. “tcpdump” is a command-line packet analyzer tool in Kali Linux used for capturing and displaying network packets, allowing users to inspect and analyze network traffic for troubleshooting, security analysis, or diagnostic purposes.
2. Low Orbit Ion Cannon (LOIC) is a network stress testing tool available in Kali Linux, primarily used for conducting Distributed Denial of Service (DDoS) attacks by flooding target servers or websites with high volumes of traffic, causing disruption or downtime.
3. “capinfos” is a command-line tool used for analyzing and providing information about packet capture (PCAP) files, offering insights into network traffic details like protocols, packet counts, and timestamps.
4. A UDP flood attack involves sending a high volume of User Datagram Protocol (UDP) packets to a target server or network, overwhelming its capacity to handle incoming UDP traffic, leading to service disruption or denial of service.
5. An HTTP flood attack involves overwhelming a web server with a high volume of seemingly legitimate HTTP GET or POST requests, exhausting its resources and causing service disruption or denial of service.

Challenges:

Sign in | saintpeters.blackboard - Search | Week 5: 9-Social Engineering | Performing a Denial of Service | ChatGPT

https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ZSHQZGAEU

Ethical Hacking and Systems Defense

Performing a Denial of Service Attack from the WAN

KA bytes:1200 (1.1 KiB) TX bytes:1200 (1.1 KiB)

9 Notice the sample flag of 999818. Click on the Challenge icon and type the flag number into the answer box. This is just to show you how to capture Challenge Flags you will see throughout this lab.

→ SAMPLE CHALLENGE

View the sample flag number for the ip2.txt. Type the Flag number displayed.

99818

Submit Skip

→ CHALLENGE #1

10 Type the following command and press Enter, so your system will not have

← PREVIOUS → NEXT →

INT-KALI-FINAL-INFOSEC-sni View Fullscreen Send Ctrl+Alt+Delete Reboot

```
root@kali:~# cat ip2.txt
eth0
Link encap:Ethernet  HWaddr 08:00:27:00:07:1c
inet addr:192.168.1.100  Bcast:192.168.1.255  Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fe37:71c/64 Scope:Link
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:7435 errors:0 dropped:0 overruns:0 frame:0
TX packets:40 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1827238 (807.8 KiB)  TX bytes:8908 (7.8 KiB)

lo
Link encap:Local Loopback
inet addr:127.0.0.1  Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING  MTU:65536  Metric:1
Sample Flag: 999818
TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:1200 (1.1 KiB)  TX bytes:1200 (1.1 KiB)

root@kali:~#
```

Feels colder Now

Search

9:18 AM 1/8/2024

Sign in | saintpeters blackboard - Search | Week 5-9-Social Engineering | Performing a Denial of Service Attack from the WAN | ChatGPT

https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ZSHUQZGAEU

Ethical Hacking and Systems Defense

Performing a Denial of Service Attack from the WAN

SAMPLE CHALLENGE

→ CHALLENGE #1

Get the flag information from ip3.txt using the same technique you used above. Type the Flag number displayed.

123457

Submit **Skip**

10 Type the following command and **press** Enter, so your system will not have an IP Address.

```
root@kali2:~# ifconfig eth0 0.0.0.0 up
```

root@kali2:~# ifconfig eth0 0.0.0.0 up

← PREVIOUS **NEXT** →

35°F Mostly sunny 9:39 AM 1/8/2024

Console | Infosec Learning - Personal - Microsoft Edge

https://lab.infoseclearning.com/console/3628771/123

INT-KALI-FINAL-INFOSEC-sniff **View Fullscreen** **Send Ctrl+Alt+Delete** **Reboot**

```
root@kali2:~# cat ip3.txt
Link encap:Ethernet (Macaddr: 08:00:29:07:07:3e)
inet addr: 192.168.1.100 Bcast:192.168.1.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:7429 errors:0 dropped:0 overruns:0 frame:0
TX packets:40 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:827228 (807.8 KiB) TX bytes:1290 (1.1 KiB)

Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
UP LOOPBACK RUNNING MTU:65536 Metric:1
Flag:123457
TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:1280 (1.1 KiB) TX bytes:1290 (1.1 KiB)
```

Sign in | saintpeters blackboard - Search | Week 5-9-Social Engineering | Performing a Denial of Service Attack from the WAN | ChatGPT

https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ZSHUQZGAEU

Ethical Hacking and Systems Defense

Performing a Denial of Service Attack from the WAN

CHALLENGE #2

WIN-2K8SP1-INFOSEC-sniff **View Fullscreen** **Send Ctrl+Alt+Delete** **Reboot**

Flag:774556

36°F Sunny 9:42 AM 1/8/2024

Local Disk (C:)

Name	Date modified	Type	Size
Recycle Bin	1/15/2009 4:45 AM	File Folder	
Boot	9/10/2012 10:01...	File Folder	
Documents and Settings	1/12/2009 7:59 AM	File Folder	
recycle	2/2/2009 11:12 PM	File Folder	
PerfLogs	1/15/2009 5:40 AM	File Folder	
Program Files	5/3/2008 12:09 AM	File Folder	
ProgramData	5/3/2008 12:09 AM	File Folder	
shared	5/3/2008 11:17...	File Folder	
System Volume Information	2/3/2009 11:39 PM	File Folder	
Users	1/16/2013 10:22...	File Folder	
Windows	6/10/2008 9:45 PM	File Folder	
hmap	12/20/2009 3:05...	File Folder	
Autobrevet.txt	5/12/2008 5:42 PM	Windows Batch File	1 KB
bootmgr	1/15/2009 3:45 AM	System File	328 KB
BOOTMGR.BAT	9/10/2012 10:01...	Batch File	9 KB
config.sys	9/10/2008 5:40 PM	System File	1 KB
Opera Mail-1.0-1048...	6/25/2018 10:25...	Application	11,819 KB
paperfile.txt	6/17/2018 5:40 PM	System File	1,394.25...
Windows-Server-20...	2/3/2009 11:15 PM	PDF Image	18 KB
Windows-Server-20...	2/3/2009 11:37 PM	PNG Image	208 KB

Sign in | https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ZSHQZGAEU

Ethical Hacking and Systems Defense

Performing a Denial of Service Attack from the WAN

CHALLENGE #3

Find the flag4.txt file in the list. Open the file and type the Flag number displayed.

345678

Submit Skip

WIN-2K8SPI-INFOSEC-sniff View Fullscreen Send Ctrl+Alt+Delete Reboot

Flag: 345678

36°F Sunny 9:44 AM 1/8/2024

Sign in | https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ZSHQZGAEU

Ethical Hacking and Systems Defense

Performing a Denial of Service Attack from the WAN

25 Double-click on the logs folder (directories are listed alphabetically).

CHALLENGE #4

Find the flag5.txt file in the list. Open the file and type the Flag number displayed.

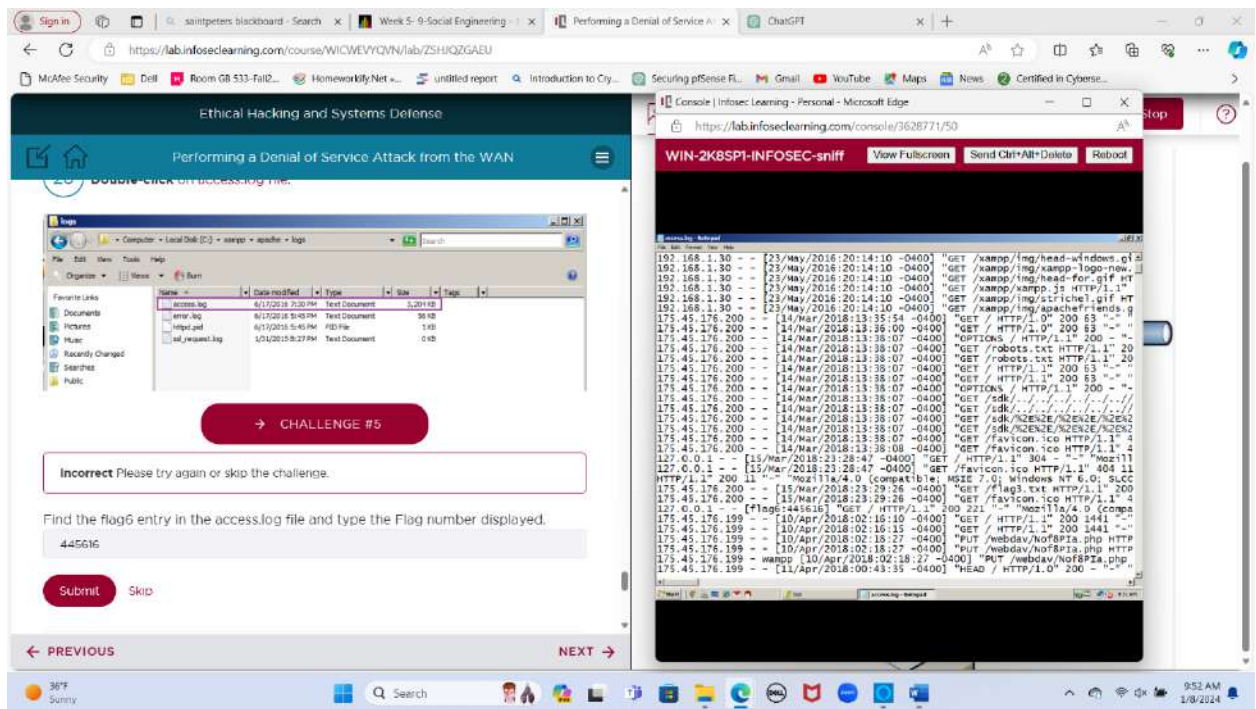
818772

Submit Skip

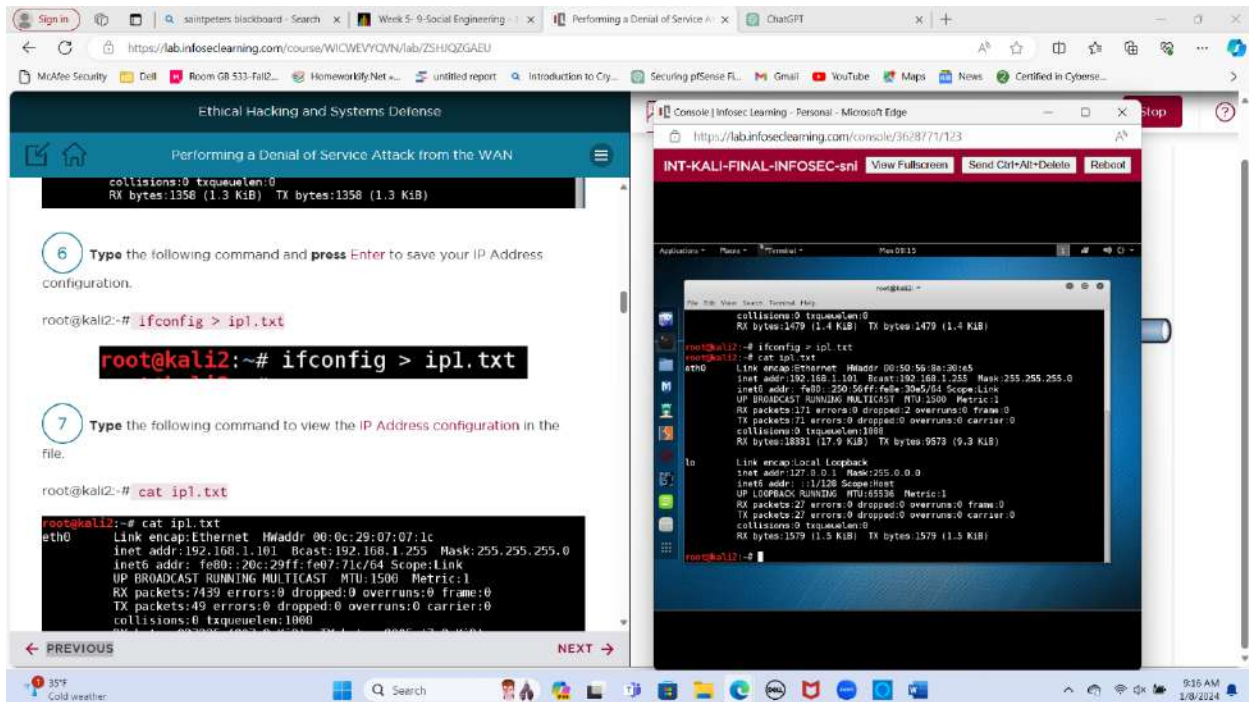
WIN-2K8SPI-INFOSEC-sniff View Fullscreen Send Ctrl+Alt+Delete Reboot

Flag: 818772

36°F Sunny 9:45 AM 1/8/2024



Screenshots:



Sign in | saintpeters.blackboard - Search | Week 5-9-Social Engineering | Performing a Denial of Service | ChatGPT

https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ZSHQZGAEU

McAfee Security | Dell | Room GB 533-Fall2... | HomeworkKillyNet... | untitled report | Introduction to Cry... | Security | Console | Infosec Learning - Personal - Microsoft Edge

https://lab.infoseclearning.com/console/3628771/123

INT-KALI-FINAL-INFOSEC-sni View Fullscreen Send Ctrl+Alt+Delete Reboot

Ethical Hacking and Systems Defense

Performing a Denial of Service Attack from the WAN

10 Type the following command and press Enter, so your system will not have an IP Address.

```
root@kali2:~# ifconfig eth0 0.0.0.0 up
```

```
root@kali2:~# ifconfig eth0 0.0.0.0 up
```

11 Type the following command and press Enter, to verify that no IPv4 address is listed for eth0.

```
root@kali2:~# ifconfig
```

```
root@kali2:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:9a:be:c1
          inet6 addr: fe80::20c:29ff:fe9a:bec1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:943 errors:0 dropped:0 overruns:0 frame:0
          TX packets:58 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:85927 (83.9 KiB)  TX bytes:8595 (8.3 KiB)
```

PREVIOUS NEXT

35°F Mostly sunny 9:20 AM 1/8/2024

Sign in | saintpeters.blackboard - Search | Week 5-9-Social Engineering | Performing a Denial of Service | ChatGPT

https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ZSHQZGAEU

McAfee Security | Dell | Room GB 533-Fall2... | HomeworkKillyNet... | untitled report | Introduction to Cry... | Security | Console | Infosec Learning - Personal - Microsoft Edge

https://lab.infoseclearning.com/console/3628771/123

INT-KALI-FINAL-INFOSEC-sni View Fullscreen Send Ctrl+Alt+Delete Reboot

Ethical Hacking and Systems Defense

Performing a Denial of Service Attack from the WAN

12 Type the following command and press Enter, to see all of the available options for tcpdump.

```
root@kali2:~# tcpdump --help
```

```
tcpdump version 4.6.2
libpcap version 1.6.2
OpenSSL 1.0.1k 8 Jan 2015
Usage: tcpdump [-aAbdDefHIJKLnOopqRStuVvxX#] [-B size] [-c count]
       [-C file_size] [-E algo:secret] [-F file] [-G seconds]
       [-i interface] [-j timestamp] [-M secret] [--number]
       [-O in/out/inout]
       [-r file] [-s snaplen] [--time-stamp-precision precision]
       [-T type] [--version] [-V file]
       [-w file] [-W filecount] [-y datalinktype] [--z command]
       [-Z user] [expression]
```

13 Type the following command and press Enter, to start tcpdump sniffing on the eth0 interface.

```
root@kali2:~# tcpdump -i eth0 -nntttt -s 0 -w TCPcapture.cap
```

```
root@kali2:~# tcpdump -i eth0 -nntttt -s 0 -w TCPcapture.cap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

PREVIOUS NEXT

35°F Mostly sunny 9:22 AM 1/8/2024

Sign in | saintpeters blackboard - Search | Week 5-9-Social Engineering | Performing a Denial of Service | ChatGPT

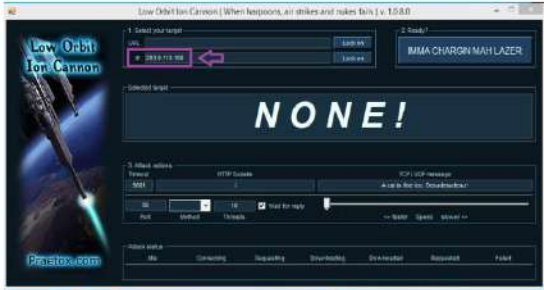
https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ZSHIQZGAEU

McAfee Security | Dell | Room GB 533-Fall2... | HomeworkKitty.Net | untitled report | Introduction to Cry... | Securing pfSense FL... | Gmail | YouTube | Maps | News | Certified in Cybers...

Ethical Hacking and Systems Defense

Performing a Denial of Service Attack from the WAN

16 In the Low Orbit Ion Cannon IP box, type **203.0.113.100**.



17 click the button that says Lock on. 203.0.113.100 will appear as the Selected

← PREVIOUS NEXT →

35°F Mostly sunny 9:24 AM 1/8/2024

Sign in | saintpeters blackboard - Search | Week 5-9-Social Engineering | Performing a Denial of Service | ChatGPT

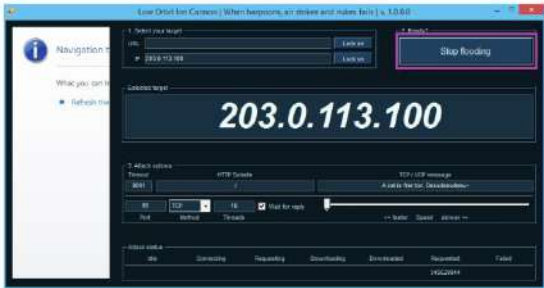
https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ZSHIQZGAEU

McAfee Security | Dell | Room GB 533-Fall2... | HomeworkKitty.Net | untitled report | Introduction to Cry... | Securing pfSense FL... | Gmail | YouTube | Maps | News | Certified in Cybers...

Ethical Hacking and Systems Defense

Performing a Denial of Service Attack from the WAN

20 Wait about 30 seconds, then click the Stop flooding button.



21 Click on the internal Linux Sniffer icon on the topology.

← PREVIOUS NEXT →

35°F Mostly sunny 9:25 AM 1/8/2024

Sign in | saintpeters blackboard - Search | Week 5-9-Social Engineering | Performing a Denial of Service | ChatGPT

https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ZSHQZGAEU

Ethical Hacking and Systems Defense

Performing a Denial of Service Attack from the WAN

23 Type the following command and press Enter, to view the total number of packet in the TCPcapture file.

```
root@kali2:~# capinfos TCPcapture.cap
```

```
File name: TCPcapture.cap
File type: Wireshark/tcpdump/... - pcap
File encapsulation: Ethernet
Packet size limit: file hdr: 262144 bytes
Number of packets: 1511 k
File size: 1233 MB
Data size: 1209 MB
Capture duration: 86 seconds
Start time: Fri Jun 17 00:05:11 2016
End time: Fri Jun 17 00:06:37 2016
Data byte rate: 14 MBps
Data bit rate: 112 Mbps
Average packet size: 800.06 bytes
Average packet rate: 17 kpackets/sec
SHA1: 4ba9244becd0c8637984f821951d499c70fdb3
d4c9ba1a14b9516d3df0d042c2a688b661547c7b
RIPEND160: 5ba3fe18f75511b451d386a9a979798013ad0
MD5: b85293e0e9cf27f1bd62fc35927d2975
Strict time order: True
```

PREVIOUS NEXT

35°F Mostly sunny

Console | Infosec Learning - Personal - Microsoft Edge

https://lab.infoseclearning.com/console/3628771/123

INT-KALI-FINAL-INFOSEC-sni View Fullscreen Send Ctrl+Alt+Delete Reboot

```
root@kali2:~# capinfos TCPcapture.cap
```

```
File name: TCPcapture.cap
File type: Wireshark/tcpdump/... - pcap
File encapsulation: Ethernet
Packet size limit: file hdr: 262144 bytes
Number of packets: 5148 k
File size: 3443 MB
Data size: 3361 MB
Capture duration: 245 seconds
Start time: Mon Jan 8 09:21:33 2024
End time: Mon Jan 8 09:25:38 2024
Data byte rate: 13 MBps
Data bit rate: 109 Mbps
Average packet size: 652.91 bytes
Average packet rate: 21 kpackets/sec
SHA1: 2123657899688977262e4e3067b7b9629877d39c
5ba3fe18f75511b451d386a9a979798013ad0
RIPEND160: 5ba3fe18f75511b451d386a9a979798013ad0
MD5: 5ba3fe18f75511b451d386a9a979798013ad0
Strict time order: False
```

Sign in | saintpeters blackboard - Search | Week 5-9-Social Engineering | Performing a Denial of Service | ChatGPT

https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ZSHQZGAEU

Ethical Hacking and Systems Defense

Performing a Denial of Service Attack from the WAN

UDP Flood

1 Type the following command and press Enter, to start tcpdump sniffing on the eth0 interface.

```
root@kali2:~# tcpdump -i eth0 -nntttt -s 0 -w UDPcapture.cap
```

```
root@kali2:~# tcpdump -i eth0 -nntttt -s 0 -w UDPcapture.cap
tcpdump: listening on eth0, link-type EN10B (Ethernet), capture size 262144 bytes
```

2 Click on the external Windows 8.1 attack machine in the topology.

Windows 8.1 Attack Machine
External Address
175.45.176.200
(North Korea)

PREVIOUS NEXT

35°F Mostly sunny

Console | Infosec Learning - Personal - Microsoft Edge

https://lab.infoseclearning.com/console/3628771/123

INT-KALI-FINAL-INFOSEC-sni View Fullscreen Send Ctrl+Alt+Delete Reboot

```
root@kali2:~# tcpdump -i eth0 -nntttt -s 0 -w UDPcapture.cap
```

```
File name: UDPcapture.cap
File type: Wireshark/tcpdump/... - pcap
File encapsulation: Ethernet
Packet size limit: file hdr: 262144 bytes
Number of packets: 3643 k
File size: 3443 MB
Data size: 3361 MB
Capture duration: 245 seconds
Start time: Mon Jan 8 09:21:33 2024
End time: Mon Jan 8 09:25:38 2024
Data byte rate: 13 MBps
Data bit rate: 109 Mbps
Average packet size: 652.91 bytes
Average packet rate: 21 kpackets/sec
SHA1: 2123657899688977262e4e3067b7b9629877d39c
5ba3fe18f75511b451d386a9a979798013ad0
RIPEND160: 5ba3fe18f75511b451d386a9a979798013ad0
MD5: 5ba3fe18f75511b451d386a9a979798013ad0
Strict time order: False
```


Sign in | saintpeters blackboard - Search | Week 5: 9-Social Engineering | Performing a Denial of Service Attack | ChanSPT


https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ZSHIQZGAEU

McAfee Security | Dell | Room 0B 533-Fall... | HomeworkifyNet | untitled report | Introduction to Cry... | Securing pSense FL... | Gmail | YouTube | Maps | News | Certified in Cybers...


Ethical Hacking and Systems Defense

Performing a Denial of Service Attack from the WAN

3 Select UDP for the Protocol in the Method dropdown list.



4 Click the IMMA CHARGIN MAH LAZER button.



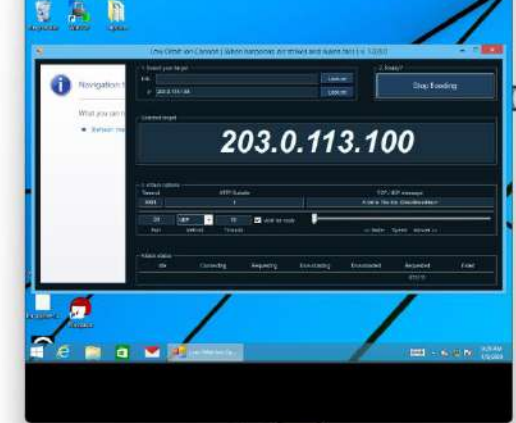
PREVIOUS NEXT

35°F Mostly sunny 9:29 AM 1/8/2024

Console | Infosec Learning - Personal - Microsoft Edge

https://lab.infoseclearning.com/console/3628771/67

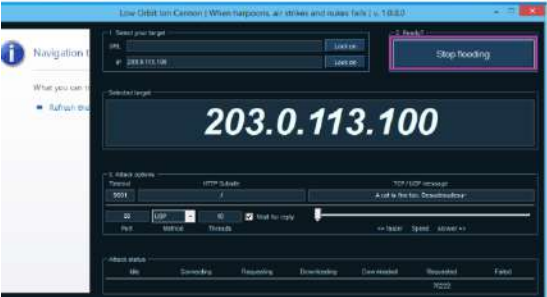
EXT-WIN8-FINAL-INFOSEC View Fullscreen Send Ctrl+Alt+Delete Reboot



Ethical Hacking and Systems Defense

Performing a Denial of Service Attack from the WAN

5 Wait about 30 seconds. Click the Stop flooding button.



6 Click on the internal Linux Sniffer icon on the topology.

Linux Sniffer

PREVIOUS NEXT

F my 9:30 AM 1/8/2024

Sign in | saintpeters blackboard - Search | Week 5-9-Social Engineering | Performing a Denial of Service | ChatGPT

https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ZSHIQZGAEU

McAfee Security | Dell | Room GB 533-Fall2... | HomeworkKillyNet... | untitled report | Introduction to Cry... | Security | Console | Infosec Learning - Personal - Microsoft Edge

Ethical Hacking and Systems Defense

Performing a Denial of Service Attack from the WAN

7 Press Control+c to stop the capture.

```
root@kali2:~# tcpdump -i eth0 -nntttt -s 0 -w UDPcapture.cap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C33049 packets captured
33049 packets received by filter
0 packets dropped by kernel
```

8 Type the following command and press Enter, to view the total number of packet in the UDPcapture file.

```
root@kali2:~# capinfos UDPcapture.cap

root@kali2:~# capinfos UDPcapture.cap
File name:          UDPcapture.cap
File type:          Wireshark/tcpdump/... - pcap
File encapsulation: Ethernet
Packet size limit:  file hdr: 262144 bytes
Number of packets:  3303 k
File size:          297 MB
Data size:          244 MB
Capture duration:   98 seconds
Start time:         Mon Jan 8 09:28:26 2024
End time:           Mon Jan 8 09:30:04 2024
Data byte rate:     2494 kbps
Data bit rate:      19 Mbps
Average packet size: 74.00 bytes
Average packet rate: 33 packets/sec
SHA1:               38ec877e9b132c223e6d7b6f4938c1f94e015d03e
RIPEMD160:           7120a23078c819e62bf62af4beed6a935a71c0e
MD5:                27c6b791f82a3bf97014b568124584e
Strict time order:  True
```

← PREVIOUS NEXT →

36°F Cold weather | Search | 9:31 AM 1/8/2024

Sign in | saintpeters blackboard - Search | Week 5-9-Social Engineering | Performing a Denial of Service | ChatGPT

https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ZSHIQZGAEU

McAfee Security | Dell | Room GB 533-Fall2... | HomeworkKillyNet... | untitled report | Introduction to Cry... | Security | Console | Infosec Learning - Personal - Microsoft Edge

Ethical Hacking and Systems Defense


Performing a Denial of Service Attack from the WAN

1 Type the following command and press Enter, to start tcpdump sniffing on the eth0 interface.

```
root@kali2:~# tcpdump -i eth0 -nntttt -s 0 -w HTTPcapture.cap

root@kali2:~# tcpdump -i eth0 -nntttt -s 0 -w HTTPcapture.cap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C7513 packets captured
7513 packets received by filter
0 packets dropped by kernel
```

2 Click on the external Windows 8.1 Attack Machine in the topology.



Windows 8.1 Attack Machine
External Address
175.45.176.200
(Ninjabot, France)

← PREVIOUS NEXT →

36°F Cold weather | Search | 9:33 AM 1/8/2024

Sign in | saintpeters blackboard - Search | Week 5-9-Social Engineering | Performing a Denial of Service | ChatGPT


https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ZSHIQZGAEU

McAfee Security | Dell | Room GB 533-Fall2... | HomeworkKittyNet | untitled report | Introduction to Cry... | Securing pfSense FL... | Gmail | YouTube | Maps | News | Certified in Cybers...

Ethical Hacking and Systems Defense

Performing a Denial of Service Attack from the WAN

3 Select HTTP for the Protocol in the Method dropdown list.



4 Click the IMMA CHARGIN MAH LAZER button.

← PREVIOUS NEXT →

36°F Sunny 9:33 AM 1/8/2024

Sign in | saintpeters blackboard - Search | Week 5-9-Social Engineering | Performing a Denial of Service | ChatGPT

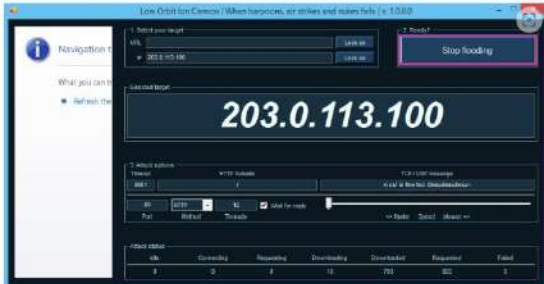
https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ZSHIQZGAEU

McAfee Security | Dell | Room GB 533-Fall2... | HomeworkKittyNet | untitled report | Introduction to Cry... | Securing pfSense FL... | Gmail | YouTube | Maps | News | Certified in Cybers...

Ethical Hacking and Systems Defense

Performing a Denial of Service Attack from the WAN

5 Wait about 30 seconds. Click the Stop flooding button.



6 Click on the internal Linux Sniffer icon on the topology.

← PREVIOUS NEXT →

Feels colder Now 9:34 AM 1/8/2024

Sign in | saintpeters.blackboard - Search | Week 5-9-Social Engineering | Performing a Denial of Service | ChatGPT

https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ZSHQZGAEU

McAfee Security | Dell | Room GB 533-Fall2... | HomeworkKitty.Net | untitled report | Introduction to Cry... | Secu... | Console | Infosec Learning - Personal - Microsoft Edge

https://lab.infoseclearning.com/console/3628771/123

INT-KALI-FINAL-INFOSEC-sni View Fullscreen Send Ctrl+Alt+Delete Reboot

Ethical Hacking and Systems Defense

Performing a Denial of Service Attack from the WAN

7 Press Control+c to stop the capture.

```
root@kali2:~# tcpdump -i eth0 -nntttt -s 0 -w HTTPcapture.cap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C7513 packets captured
7513 packets received by filter
0 packets dropped by kernel
```

8 Type the following command and press Enter, to view the total number of packet in the HTTPcapture.cap file.

```
root@kali2:~# capinfos HTTPcapture.cap

root@kali2:~# capinfos HTTPcapture.cap
File name: HTTPcapture.cap
File type: Wireshark/tcpdump/... - pcap
File encapsulation: Ethernet
Packet size limit: file hdr: 262144 bytes
Number of packets: 7513
File size: 1061 kB
Data size: 941 kB
Capture duration: 315 seconds
```

PREVIOUS NEXT

Feels colder Now

Search

9:35 AM 1/8/2024

Sign in | saintpeters.blackboard - Search | Week 5-9-Social Engineering | Performing a Denial of Service | ChatGPT

https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ZSHQZGAEU

McAfee Security | Dell | Room GB 533-Fall2... | HomeworkKitty.Net | untitled report | Introduction to Cry... | Securing pTSense FL | Gmail | YouTube | Maps | News | Certified in Cybers... | Console | Infosec Learning - Personal - Microsoft Edge

https://lab.infoseclearning.com/console/3628771/167

EXT-WIN8-FINAL-INFOSEC View Fullscreen Send Ctrl+Alt+Delete Reboot

Ethical Hacking and Systems Defense

Performing a Denial of Service Attack from the WAN

10 Type the following command and press Enter, to start tcpdump sniffing on the eth0 interface.

```
root@kali2:~# tcpdump -i eth0 -nntttt -s 0 -w HTTP2capture.cap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

11 Click on the Windows 8.1 Attack Machine in the topology. Uncheck the Wait for reply button next to HTTP.

Selected target

203.0.113.100

3 Attack options

Timeout: 9001 HTTP Subdata: TGP / UDP message: A cat is free too. Desires:desire

PREVIOUS NEXT

Feels colder Now

Search

9:36 AM 1/8/2024

