autopsy tool

volatility (extension .elf ,

binwalk (android +)

mobsf.live (android) | genymotion (ios) – apk analyzer

foremost tool – recover lost files

sleuth kit- data extraction

hURL (understand cyphers and decode it)

file (command to get file details)

exiftool (command for exif data)

strings (command to convert in string)

binwalk (command to get hidden file)

10> get - command to download

11> xxd -to open file in hex format

xxd -b binary format

12> file- command to get type of file

13> hydra - password attack

14> for root uid = 0 on Linux & 500 for windows

15> exploit-db - exploit code for

16> permission chmod/ chown

17> msfconsole – Metasploit framework

18> fcrackzip - tool to crack zip file

19> useful pattern -> '() { :; }; /bin/sh' (shell shock string)

20> msf_create_pattern (special pattern which is a process)

21> gdb -> debugger

22> msf-pattern_offset

23> pty package (python)

24> /bin/bash -i

25> x

26> msf-pattern_offset -q <address> (to see where its crashing)

27> ghidra- mobile reverse engineering

29> immunity debugger

30> msf-venum (to create little endian string of code for getting shell access)

31> debugger says 00 for bad characters.

32> zixem.altervista.org

33> pentestmonkey

1> TCP flags

2> 3way handshake -> TLS/SSL -> communication (start communication)

3> 4way handshake (close comm)

4> OSI model

5> nmap - to find open ports

6> working of nmap

  a>ping sweep

  b> DNS lookup

  c> Reverse DNS lookup

  d> Find open ports

  e> NSE (Nmap scripting engine)

7> switches of nmap

8> types of nmap scans

  a> sT

  b> sS

  c> sF

  d> sX

9> if port 80 is open try crawling that and visit robots.txt

robots.txt

cryptii.com: used for various cryptographic algos

wireshark: used to monitor network traffic

mobilefish.com: used for steganography

futureboy.us: same as above

wordlist, rockyou.txt: stores passwords

johny: used to crack linux passwords after unshadowing

crunch: used to generate combinations for passwords

hashcat: used to crack passwords

rtgen: similar to crunch, generate rainbow hashes

rtsort: sort the hashes

rcrack: crack hashes by matching with the ones generated in rtgen

xerxes: DoS attack

wafw00f: check if site uses security firewall

lbd: check if site uses load balancing

hping3: used to perform a SYN attack

maltego: check where a site links to

nmap: used to check port details for an ip

ravana: used for phishing

camphish: used to hack camera

exiftool: to get metadata from file

virustotal.com: check if website is safe

cookie stealing

ettercap: ARP poisoning

burpsuit: intercept packets between device and server SQL injection, Client and Server Side Scripting

dirb url -X .txt -> looks for all txt files in url, can be used without txt to find directories

crunch minlength maxlength -t template -o output.txt-> generate passwords of some length

fcrackzip -D -p dict.txt encrypted.zip -u -> unzip with a list of passwords in dict.txt

pypykatz -> used to analyze dump files

Metasploit:

msfconsole

search ssh_login

use x (x is index num displayed)

show options

set required options

run

sssions (to show active sessions)

sessions -u x (to get meterpreter shell for index x)

sessions -i x (use meterpreter)

shell (to get shell in that machine)

python -c "import pty; pty.spawn("/bin/bash")" (to get interactive shell

After leaving session and coming back to msf

use post/multi/manage/autoroute (routes an ip to another ip)

search ping_sweep (similar to arp-scan)

search portscan (searches open ports)

search ftp/anonymous (checks whether anonymous ftp login is allowed)

pyrhon -m SimpleHTTPServer (starts a server on some port)

sudo -l (check what accesses i have)

nmap : Here are all the arguments for nmap:

Scan Types

-sS: TCP SYN scan (half-open scan)

-sT: TCP connect scan (full-open scan)

-sU: UDP scan

-sP: Ping scan (check if host is up)

-sF, -sX, -sN: TCP FIN, Xmas, and Null scans (stealthy scans)

-sA: TCP ACK scan (checks for firewalls)

-sW: TCP Window scan (checks for open ports without sending data)

-sM: TCP Maimon scan (checks for open ports on Solaris systems)

Target Specification

<target>: Hostname or IP address to scan

-iL <inputfile>: Scan targets listed in a file

-iR <num>: Scan random targets (use with caution)

Port Specification

-p <port>: Scan specific port(s) (e.g., 22, 80)

-p-: Scan all ports (1-65535)

-p <port>-<port>: Scan a range of ports (e.g., 1-1024)

Timing and Performance

-T<0-5>: Set timing template (0: paranoid, 5: insane)

--min-rate <num>: Set minimum scan rate

--max-rate <num>: Set maximum scan rate

OS Detection

-O: Enable OS detection

--osscan-guess: Guess OS based on open ports

Version Detection

-sV: Enable version detection

--version-all: Detect all versions (not just most common ones)

Script Scanning

-sC: Enable script scanning (default scripts)

--script=<script>: Run a specific script

--script-args=<args>: Pass arguments to scripts

Output

-oN <outputfile>: Save output to a file in normal format

-oX <outputfile>: Save output to a file in XML format

-oG <outputfile>: Save output to a file in grepable format

Miscellaneous

-v: Increase verbosity

-d: Increase debugging level

--open: Show only open ports

--packet-trace: Show packet-level debugging information

Note: Some arguments may have overlapping functionality or be deprecated. Always check the nmap documentation for the most up-to-date information.