SCANNING NETWORK USING NMAP

Scanning network Live Host (ping sweep)	nmap -sP IP/CIDR
Scanning Live Host withouth port scan (ARP)	nmap -PR -sn IP/CIDR
Scripts+Version running on target	nmap -sC -sV IP/CIDR
OS of the target	nmap -O IP
All open ports of the target	nmap -p- IP/CIDR
Specific port scan of the target	nmap -p <port-number> IP/CIDR
Aggressive scan	nmap -A IP/CIDR
Scanning using NSE scripts	nmap --scripts <script_name> -p <port> IP/CIDR
Scripts+Version+Ports+OS scan	nmap -sC -sV -p- -A -v -T4 IP/CIDR

SERVICE ENUMERATION

FTP>SNMP>SMB>RDP>NetBIOS

FTP

```
nmap -sC -p 21 <ip>
hydra -L /usr/share/wordlists/metasploit/ -P <ip> ftp
hydra -L /usr/share/wordlists/metasploit/common_users.txt -P /usr/share/wordlists/metasploit/unix_passwords.txt <ip> ftp
ftp <ip>
get file.txt (to download it)
ls
cat file.txt
```

SNMP

nmap -sP <ip>	
snmp-check <ip>	snmp processes
nmap -sU -p 161 --script=snmp-processes <target>	https://nmap.org/nsedoc/scripts/
msfconsole	Find valid strings using metasploit
search snmp	

use auxiliary/scanner/snmp/snmp_login	
show options	
ip a	
set RHOSTS <ip>	
show options	
exploit	
exit	
nmap -sU -p 161 --script=snmp-interfaces <target>	https://nmap.org/nsedoc/scripts/snmp-interfaces.html
snmp-check <ip>	

SMB

nmap -p 445 --script smb-enum-shares <ip>	Shares details with permissions
File manager>Network>Windows Network>	Connect SMB GUI
On the bar (smb://<ip>)	https://youtu.be/T55Z0spbweY?t=1656
nmap -p 445 --script smb-enum-users <ip>	Enumerating users
nmap -p 445 --script smb-enum-users --script-args smbusername=<user>, smbpassword=<pass> <ip>	
nmap -p 445 --script smb-enum-groups --script-args smbusernname=<user>, smbpassword=<pass> <ip>	Enumerating groups
nmap -sC -sV -A -T4 -p 445 <ip>	Enumerating security level
nmap -p 445 --script smb-enum-services --script-args smbusername=<user>, smbpassword=<pass> <ip>	Enumerating services

RDP

nmap <ip>	Find port with RDP
msfconsole -q	Confirm port
search rdp	
use auxiliary/scanner/rdp/rdp_scanner	
show options	
set RHOSTS <ip>	
set RPORT <port> (3333?)	
exploit	
exit	
hydra -L /usr/share/metasploit-framework/data/wordlists/	Brute force RDP
hydra -L /usr/share/metasploit-framework/data/wordlists/commom_users.txt -P /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt rdp://<ip>	

xfreerdp /u:<user> /p:<passwd> /v:<ip>:<port>	Xfreerdp to create RDP session

NetBIOS

ip a	
nmap -sP <ip+*>	Enum network (last octet wildcard)
nmap -sV --script nbstat.nse <found ip>	Enum ip
	Enum netbios

WIRESHARK (traffic sniffing)

	https://youtu.be/2lchMa5VKnw?t=316
tcp.flags.syn==1	Filtering packets (DoS attack)
left click frame>Follow>HTTP Stream	Follow Streams TCP/HTTP
left click frame>Follow>TCP Stream	Red part SENT blue RESPONSE from server
Stream button on right bottom 1,2..	Walkthrough stream numbers
Flag cypher for text	decipher algorithms (not required in the exam, **just the FLAG**)
File>Export Objects>HTTP>filter by Content Type>text/plain>Save	Find files
Select frame>left bottom icon near request number	Find comments
CTRL+F	Finding Strings
	Could have a flag

DOS/DDOS

Statistics>Conversations	
Select IPV4>Select Bytes	The ip with the most requests are the ones attacking
Could be IPV6 too	

STEGANOGRAPHY

SNOW (hiding and extracting hidden data from txt file)	**OPENSTEGO** (hiding and extracting hidden data from image file)
	COVERT TCP (hiding data TCP/IP packet headers)

SNOW

Open in terminal (or powershell)	https://youtu.be/aNHW1A_rpNs?t=218

dir	
SNOW.EXE -C -m "secret_msg" -p "<passwd>" <name file in dir> <name output file>	Hiding data
SNOW.EXE -C -p "<passwd> " <name output file>	Extract data

Openstego

Hide data>message file (browse&select txt file to hide)	Hiding text into image
Cover file (browse the image to hide the txt inside)	
Name output file	https://youtu.be/aNHW1A_rpNs?t=512
Hide data button	
Extract data (browse image)	Extract
Output select open	
Password if needed	
Extract data	
if hash> hashes.com	

Covert TCP

cc -o covert_tcp covert_tcp.c	https://youtu.be/aNHW1A_rpNs?t=845
./cover_tcp -dest <Dest-IP> -source <Source-IP> -source_port 9999 -dest_port 8888 -server -file /path/to/file.txt	For receiving/listening (need to be root)
./cover_tcp -dest <Dest-IP> -source <Source-IP> -source_port 8888 -dest_port 9999 -server -file /path/to/file.txt	For sending (need to be root)

CRYPTOGRAPHY

Hashmyfiles (calculating and comparing hashes of files)	**Cryptool** (encryption/decryption of hex data manipulating key length)
CryptoForge (encrypting/decrypting the files)	**VeraCrypt** (hiding and encrypting disk partitions)
	BcTextEncoder (encoding/decoding txt in file (.hex)

HashMyFiles

Drag files into hashmyfiles	check if tampered by comparing hashes

	https://youtu.be/DtWjUsbuMtk?t=219

CryptoForge

Left click file, option "Encrypt"	encrypt
Window with passphrase	https://youtu.be/DtWjUsbuMtk?t=374
Click on the file, passphrase to decrypt it	decrypt hash on hashes.com

BcTextEncoder

Write text on Decoded plain>Encode>passwd	Encode
Write text on Encoded text>Decode>passwd	Decode and hashes.com
	https://youtu.be/DtWjUsbuMtk?t=495

Cryptool

File options>open>select file	hex format of the file
Analysis>select symmetric Encryption>Keylenght>start	find flag or hashes.com
	https://youtu.be/DtWjUsbuMtk?t=632

VeraCrypt

Create volume>create encrypted file container>hidden veracrypt volume>	https://youtu.be/DtWjUsbuMtk?t=789
select file>select algorithm>select space>passwd outer partition>	
scroll mouse>format>next hidden volume>select space (smaller than outer)>	
>passwd>next>format>ok>next>cancel window	
mount partition>select device>passwd related to the partition	

WEB

SQLMap (finding SQL injection vulnerabilities)	**Wpscan** (scanning and finding issues wordpress websites)
Burpsuite (analysing and manipulating the traffic)	**ADB** (connecting android devices to pc and binary analysis)

SQLMap

ping -c 3 <ip>	command execution
ping -c 3 <ip> | pwd	

id=	Find SQLi
	Intercept with burp
Intercept with burp, save item (req.txt)	
cd dir saved file	
sqlmap -r <req.txt> --dbs	
sqlmap -r <req.txt> -D <dbs>	
sqlmap -r <req.txt> -D <dbs> --tables	
sqlmap -r <req.txt> -D <dbs> --tables --columns	
sqlmap -r <req.txt> -D <dbs> --dump	

WpScan

ping <ip>	
wpscan --url <url> --enumerate u	wpscan -h info

ADB

adb connect <ip>:<port>	adb devices?
adb shell	
ls, whoami	
cd sdcard/	find secret.txt
cat secret.txt	

https://github.com/hunterxxx/CEH-v12-Practical