Appointment

VERY EASY

Machine Pwned

1- What does the acronym SQL stand for?
https://www.w3schools.com/sql/sql_intro.asp

2- What is one of the most common type of SQL vulnerabilities?
https://portswigger.net/web-security/sql-injection

3- What does PII stand for?
https://www.nist.gov/publications/guide-protecting-confidentiality-personally-identifiable-information-pii

4- What does the OWASP Top 10 list name the classification for this vulnerability?
https://owasp.org/www-project-top-ten/

5- What service and version are running on port 80 of the target?
nmap -sC -sV -p80 {IP}

6- What is the standard port used for the HTTPS protocol?:
https://opensource.com/article/18/10/common-network-ports

7- What is one luck-based method of exploiting login pages?
https://owasp.org/www-community/attacks/Brute_force_attack

8- What is a folder called in web-application terminology?
https://en.wikipedia.org/wiki/Web_directory

9- What response code is given for "Not Found" errors?:
https://httpstatuses.com/

10- What switch do we use with Gobuster to specify we're looking to discover directories, and not subdomains?
https://github.com/OJ/gobuster

11- What symbol do we use to comment out parts of the code?
http://www.gavilan.edu/csis/languages/comments.html

12- Submit root flag:
Burp y https://github.com/payloadbox/sql-injection-payload-list

Sequel

VERY EASY

1- What does the acronym SQL stand for?
https://www.w3schools.com/sql/sql_intro.asp

2- During our scan, which port running mysql do we find?
nmap -sC -sV {IP}

3- What community-developed MySQL version is the target running?
https://www.opensourceforu.com/2016/04/mariadb-the-community-developed-fork-of-mysql/

4- What switch do we need to use in order to specify a login username for the MySQL service?
https://dev.mysql.com/doc/refman/8.0/en/connecting.html

5- Which username allows us to log into MariaDB without providing a password?
https://book.hacktricks.xyz/pentesting/pentesting-mysql

6- What symbol can we use to specify within the query that we want to display eveything inside a table?
https://www.w3schools.com/mysql/mysql_select.asp

7- What symbol do we need to end each query with?
https://www.sqlmdfviewer.org/fix-error-sql-syntax.html

8- Submit root flag
mysql -u {user} -h {IP}

1- What nmap scanning switch employs the use of default scripts during a scan?
https://hackertarget.com/nmap-cheatsheet-a-quick-reference-guide/

2- What service version is found to be running on port 21?

```
nmap -sV {IP}
```

3- What FTP code is returned to us for the "Anonymous FTP login allowed" message?

```
ftp anonymous@{IP}
```

4- What command can we use to download the files we find on the FTP server?
https://www.cs.colostate.edu/helpdocs/ftp.html

5- What is one of the higher-privilege sounding usernames in the list we retrieved?

```
cat allowed.userlist*
```

6- What version of Apache HTTP Server is running on the target host?

```
nmap -sV -p80 {IP}
```

7- What is the name of a handy web site analysis plug-in we can install in our browser?
https://addons.mozilla.org/es/firefox/addon/wappalyzer/

8- What switch can we use with gobuster to specify we are looking for specific filetypes?
https://github.com/OJ/gobuster

9- What file have we found that can provide us a foothold on the target?

```
gobuster dir -u http://{IP}-w /usr/share/wordlists/dirb/common.txt -x php,txt,html
```

10- Submit root flag

```
hydra -l user -P allowed.userlist.passwd {IP} http-post-form
"/login.php:username=^USER^&password=^PASS^:Warning! Incorrect information." -vV -f
```

With Love:

Ixbalanque
https://www.linkedin.com/in/willeonardo/