**COSC 566 – Hack The Box Challenge**

**Giuseppe Schintu**

**--- TIER 0 ---**

A screenshot of a computer

Description automatically generated with medium confidence

Connect to target machine using telnet, then use ls and cat commands to see what text file has the root flag.

|  |  |
| --- | --- |
| Question | Answer |
| What does the acronym VM stand for? | Virtual Machine |
| What tool do we use to interact with the operating system in order to issue commands via the command line, such as the one to start our VPN connection? It's also known as a console or shell. | Terminal |
| What service do we use to form our VPN connection into HTB labs? | Openvpn |
| What is the abbreviated name for a 'tunnel interface' in the output of your VPN boot-up sequence output? | Tun |
| What tool do we use to test our connection to the target with an ICMP echo request? | Ping |
| What is the name of the most common tool for finding open ports on a target? | Nmap |
| What service do we identify on port 23/tcp during our scans? | telnet |
| What username is able to log into the target over telnet with a blank password? | Root |
| Submit root flag | b40abdfe23665f766f9c61ecba8a4c19 |

Graphical user interface

Description automatically generated

This challenge is about FTP and basic commands to ultimately CTF to complete the level

|  |  |
| --- | --- |
| Question | Answer |
| What does the 3-letter acronym FTP stand for? | File Transfer Protocol |
| Which port does the FTP service listen on usually? | 21 |
| What acronym is used for the secure version of FTP?  What is the command we can use to send an ICMP echo request to test our connection to the target? | sftp |
| From your scans, what version is FTP running on the target? | vsftpd 3.0.3 |
| What is the command we need to run in order to display the 'ftp' client help menu? | ftp -h |
| What is username that is used over FTP when you want to log in without having an account? | anonymous |
| What is the response code we get for the FTP message 'Login successful'? | 230 |
| There are a couple of commands we can use to list the files and directories available on the FTP server. One is dir. What is the other that is a common way to list files on a Linux system. | ls |
| What is the command used to download the file we found on the FTP server? | get |
| Submit root flag | 035db21c881520061c53e0536e44f815 |

Graphical user interface

Description automatically generated

This challenge is about SMB(Server Message Block). With smbclient we can see private and public share, and ultimately list access with ls/get the flag.txt file.

|  |  |
| --- | --- |
| Question | Answer |
| What does the 3-letter acronym SMB stand for? | Server Message Block |
| What port does SMB use to operate at? | 445 |
| What is the service name for port 445 that came up in our Nmap scan? | Microsoft-ds |
| What is the 'flag' or 'switch' we can use with the SMB tool to 'list' the contents of the share? | -L |
| How many shares are there on Dancing? | 4 |
| What is the name of the share we are able to access in the end with a blank password? | Workshares |
| What is the command we can use within the SMB shell to download the files we find? | get |
| Submit root flag | 5f61c10dffbc77a704d76016a22f1664 |

Graphical user interface, application, Teams

Description automatically generated

This challenge is about redis (a cache data server). With some basic commands using the redis-cli (select, list, keys, and get) we can inspect data and ultimately CTF.

|  |  |
| --- | --- |
| Question | Answer |
| Which TCP port is open on the machine? | 6379 |
| Which service is running on the port that is open on the machine? | Redis |
| What type of database is Redis? Choose from the following options: (i) In-memory Database, (ii) Traditional Database | In-memory database |
| Which command-line utility is used to interact with the Redis server? Enter the program name you would enter into the terminal without any arguments. | Redis-cli |
| Which flag is used with the Redis command-line utility to specify the hostname? | -h |
| Once connected to a Redis server, which command is used to obtain the information and statistics about the Redis server? | info |
| What is the version of the Redis server being used on the target machine? | 5.0.7 |
| Which command is used to select the desired database in Redis? | select |
| How many keys are present inside the database with index 0? | 4 |
| Which command is used to obtain all the keys in a database? | Keys \* |
| Submit root flag | 03e1d2b376c37ab3f5319922053953eb |

**--- TIER 1 ---**

A screenshot of a video game

Description automatically generated

This Challenge is about Web and SQL Injection. There are scanning tools like gobuster that can identify exploitable files. The current instructions do not mention that git clone will use the current folder when cloning any project.

﻿gobuster dir --url http://{Target IP}/ --wordlist SecLists/Discovery/Web-Content/directory-list-2.3-small.txt

Graphical user interface, text

Description automatically generated

|  |  |
| --- | --- |
| Question | Answer |
| What does the acronym SQL stand for? | Structured Query Language |
| What is one of the most common type of SQL vulnerabilities? | Sql Injection |
| What does PII stand for? | Personally Identifiable Information |
| What is the 2021 OWASP Top 10 classification for this vulnerability? | A03:2021-Injection |
| What does Nmap report as the service and version that are running on port 80 of the target? | Apache httpd 2.4.38 ((Debian)) |
| What is the standard port used for the HTTPS protocol? | 443 |
| What is a folder called in web-application terminology? | directory |
| What is the HTTP response code is given for 'Not Found' errors? | 404 |
| Gobuster is one tool used to brute force directories on a webserver. What switch do we use with Gobuster to specify we're looking to discover directories, and not subdomains? | dir |
| What single character can be used to comment out the rest of a line in MySQL? | # |
| If user input is not handled carefully, it could be interpreted as a comment. Use a comment to login as admin without knowing the password. What is the first word on the webpage returned? | Congratulations |
| Submit root flag | e3d0796d002a446c0e622226f42e9672 |

Graphical user interface

Description automatically generated

This challenge is about understanding the basics of MySQL (MariaDB) commands and structure. Ultimately, we will use simple commands (SHOW, SELECT) to capture the flag; which is in the htb table.

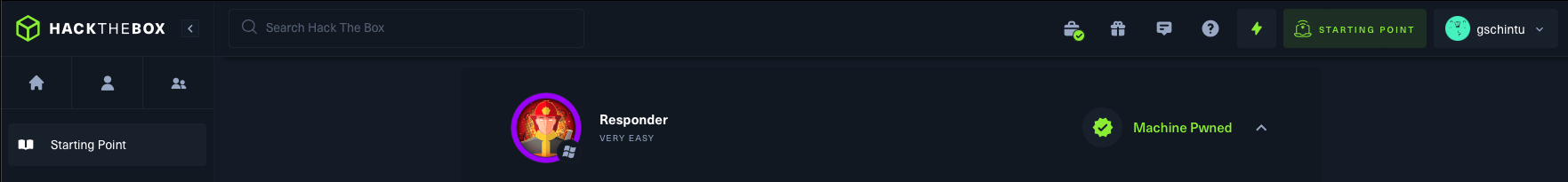
|  |  |
| --- | --- |
| Question | Answer |
| During our scan, which port do we find serving MySQL? | 3306 |
| What community-developed MySQL version is the target running? | MariaDB |
| When using the MySQL command line client, what switch do we need to use in order to specify a login username? | -u |
| Which username allows us to log into this MariaDB instance without providing a password? | root |
| In SQL, what symbol can we use to specify within the query that we want to display everything inside a table? | \* |
| In SQL, what symbol do we need to end each query with? | ; |
| There are three databases in this MySQL instance that are common across all MySQL instances. What is the name of the fourth that's unique to this host? | htb |
| Submit root flag | 7b4bec00d1a39e3dd4e021ec3d915da8 |

Graphical user interface

Description automatically generated with low confidence

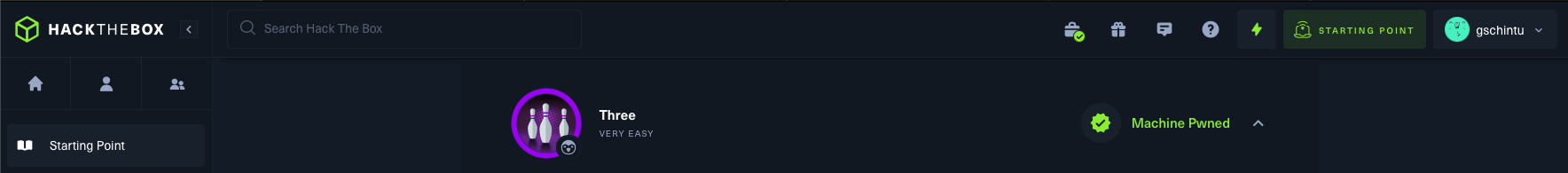
This challenge is about using basic ftp through vsftpd (secure ftp module). The additional caveat is to use gobuster to inspect and look for scripts like php and use the information from ftp files to gain access to password protected sites. Ultimately, we need to use the ls and get commands to search folders and download the file that has the flag.

|  |  |
| --- | --- |
| Question | Answer |
| What Nmap scanning switch employs the use of default scripts during a scan? | -sC |
| What service version is found to be running on port 21? | vsftpd 3.0.3 |
| What FTP code is returned to us for the "Anonymous FTP login allowed" message? | 230 |
| After connecting to the FTP server using the ftp client, what username do we provide when prompted to log in anonymously? | anonymous |
| After connecting to the FTP server anonymously, what command can we use to download the files we find on the FTP server? | get |
| What is one of the higher-privilege sounding usernames in 'allowed.userlist' that we download from the FTP server? | admin |
| What version of Apache HTTP Server is running on the target host? | apache httpd 2.4.41 |
| What switch can we use with Gobuster to specify we are looking for specific filetypes? | -x |
| Which PHP file can we identify with directory brute force that will provide the opportunity to authenticate to the web service? | Login.php |
| Submit root flag | c7110277ac44d78b6a9fff2232434d16 |



This challenge focuses on file inclusion vulnerability on a webpage being served on a windows machine that can be exploited to collect the NetNTLMv2 challenge of the user that is running the web server. Additionally, it uses a utility called Responder to capture a NetNTLMv2 hash and later use a utility known as john the ripper to test millions of potential passwords to see if they match the one used to create the hash. With the password at hand we can finally use a tool called Evil-WinRM to remote into the target machine and look into folders and find suspicious files that may contain the root flag for this challenge.

|  |  |
| --- | --- |
| Question | Answer |
| When visiting the web service using the IP address, what is the domain that we are being redirected to? | Unika.htb |
| Which scripting language is being used on the server to generate webpages? | php |
| What is the name of the URL parameter which is used to load different language versions of the webpage? | page |
| Which of the following values for the `page` parameter would be an example of exploiting a Local File Include (LFI) vulnerability | ../../../../../../../../windows/system32/drivers/etc/hosts |
| Which of the following values for the `page` parameter would be an example of exploiting a Remote File Include (RFI) vulnerability | //10.10.14.6/somefile |
| What does NTLM stand for? | New Technology Lan Manager |
| Which flag do we use in the Responder utility to specify the network interface? | -I |
| There are several tools that take a NetNTLMv2 challenge/response and try millions of passwords to see if any of them generate the same response. One such tool is often referred to as `john`, but the full name is what?. | John The Ripper |
| What is the password for the administrator user? | badminton |
| We'll use a Windows service (i.e. running on the box) to remotely access the Responder machine using the password we recovered. What port TCP does it listen on? | 5985 |
| Submit root flag | ea81b7afddd03efaa0945333ed147fac |



This challenge is about a brief introduction to the AWS CLI that will be used for attempt to exploit poor configuration in the Amazon AWS environment, specifically the AWS file hosting features S3. The final phase of this challenge will implement a reverse shell to navigate contents in the s3 target endpoint.

|  |  |
| --- | --- |
| Question | Answer |
| How many TCP ports are open? | 2 |
| What is the domain of the email address provided in the "Contact" section of the website? | Thetoppers.htb |
| In the absence of a DNS server, which Linux file can we use to resolve hostnames to IP addresses in order to be able to access the websites that point to those hostnames? | /etc/hosts |
| Which sub-domain is discovered during further enumeration? | s3.thetoppers.htb |
| Which service is running on the discovered sub-domain? | Amazon s3 |
| Which command line utility can be used to interact with the service running on the discovered sub-domain? | awscli |
| Which command is used to set up the AWS CLI installation? | Aws configure |
| What is the command used by the above utility to list all of the S3 buckets? | Aws s3 ls |
| This server is configured to run files written in what web scripting language? | php |
| Submit root flag | a980d99281a28d638ac68b9bf9453c2b |

**--- TIER 2 ---**

A screenshot of a computer

Description automatically generated with medium confidence

In this challenge we can exploit a misconfiguration in Microsoft SQL Server with a reverse shell. For this, we will get familiarized with the use of basic use of Impacket and winPEAS tools in order to further attack some services. We will use the reverse shell to transfer and execute a couple of .exe that will enable us to read the windows configuration and identify exploitable files with potential credentials.

|  |  |
| --- | --- |
| Question | Answer |
| Which TCP port is hosting a database server? | 1433 |
| What is the name of the non-Administrative share available over SMB? | backups |
| What is the password identified in the file on the SMB share? | M3g4c0rp123 |
| What script from Impacket collection can be used in order to establish an authenticated connection to a Microsoft SQL Server? | mssqlclient.py |
| What extended stored procedure of Microsoft SQL Server can be used in order to spawn a Windows command shell? | Xp\_cmdshell |
| What script can be used in order to search possible paths to escalate privileges on Windows hosts? | winPEAS |
| What file contains the administrator's password? | ConsoleHost\_history.txt |
| Submit user flag | 3e7b102e78218e935bf3f4951fec21a3 |
| Submit root flag | b91ccec3305e98240082d4474b848528 |