Tom Hills
CS566, Dr. Ruoti
Project 7: Hack the Box Intro
04/26/2022

TIER 0:

- Meow:
    1. What does the acronym VM stand for?
       Virtual Machine.
    2. What tool do we use to interact with the operating system in order to start our VPN connection?
       Terminal.
    3. What service do we use to form our VPN connection?
       openvpn.
    4. What is the abbreviated name for a tunnel interface in the output of your VPN boot-up sequence output?
       tun.
    5. What tool do we use to test our connection to the target?
       ping.
    6. What is the name of the tool we use to scan the target's ports?
       nmap.
    7. What service do we identify on port 23/tcp during our scans?
       telnet.
    8. What username ultimately works with the remote management login prompt for the target?
       Root.
    9. Submit root flag?
       b40abdfe23665f766f9c61ecba8a4c19.
- Fawn:
    1. What does the 3-letter acronym FTP stand for?
       File transfer protocol.
    2. What communication model does FTP use, architecturally speaking?
       client-server model.
    3. What is the name of one popular GUI FTP program?
       filezilla.
    4. Which port is the FTP service active on usually?
       21 tcp.
    5. What acronym is used for the secure version of FTP?
       sftp.
    6. What is the command we can use to test our connection to the target?
       ping.
    7. From your scans, what version is FTP running on the target?
       vsftpd 3.0.3.
    8. From your scans, what OS type is running on the target?
       unix.
    9. Submit root flag
       035db21c881520061c53e0536e44f815.
- Dancing:
    1. What does the 3-letter acronym SMB stand for?
       server message block.

2. What port does SMB use to operate at?
   445.
3. What network communication model does SMB use, architecturally speaking?
   client-server model.
4. What is the service name for port 445 that came up in our nmap scan?
   microsoft-ds.
5. What is the tool we use to connect to SMB shares from our Linux distribution?
   smbclient.
6. What is the `flag` or `switch` we can use with the SMB tool to `list` the contents of the share?
   -L.
7. What is the name of the share we are able to access in the end?
   WorkShares.
8. What is the command we can use within the SMB shell to download the files we find?
   get.
9. Submit root flag
   5f61c10dffbc77a704d76016a22f1664.

TIER 1:

- Appointment:
  1. What does the acronym SQL stand for?
     structured query language.
  2. What is one of the most common type of SQL vulnerabilities?
     sql injection.
  3. What does PII stand for?
     personally identifiable information.
  4. What does the OWASP Top 10 list name the classification for this vulnerability?
     A03:2021-Injection.
  5. What service and version are running on port 80 of the target?
     Apache httpd 2.4.38 ((Debian)).
  6. What is the standard port used for the HTTPS protocol?
     443.
  7. What is one luck-based method of exploiting login pages?
     brute-forcing.
  8. What is a folder called in web-application terminology?
     directory.
  9. What response code is given for "Not Found" errors?
     404.
  10. What switch do we use with Gobuster to specify we're looking to discover directories, and not subdomains?
      dir.
  11. What symbol do we use to comment out parts of the code?
      #.
  12. Submit root flag
      e3d0796d002a446c0e622226f42e9672.

Tom Hills
CS566, Dr. Ruoti
Project 7: Hack the Box Intro
04/26/2022

- Sequel:
    1. What does the acronym SQL stand for?
       structured query language.
    2. During our scan, which port running mysql do we find?
       3306.
    3. What community-developed MySQL version is the target running?
       MariaDB.
    4. What switch do we need to use in order to specify a login username for the MySQL service?
       -u.
    5. Which username allows us to log into MariaDB without providing a password?
       root.
    6. What symbol can we use to specify within the query that we want to display everything inside a table?
       *.
    7. What symbol do we need to end each query with?
       ;.
    8. Submit root flag
       7b4bec00d1a39e3dd4e021ec3d915da8.
- Crocodile:
    1. What nmap scanning switch employs the use of default scripts during a scan?
       -sC.
    2. What service version is found to be running on port 21?
       vsftpd 3.0.3.
    3. What FTP code is returned to us for the "Anonymous FTP login allowed" message?
       230.
    4. What command can we use to download the files we find on the FTP server?
       get.
    5. What is one of the higher-privilege sounding usernames in the list we retrieved?
       admin.
    6. What version of Apache HTTP Server is running on the target host?
       2.4.41.
    7. What is the name of a handy web site analysis plug-in we can install in our browser?
       wappalyzer.
    8. What switch can we use with gobuster to specify we are looking for specific filetypes?
       -x.
    9. What file have we found that can provide us a foothold on the target?
       login.php.
    10. Submit root flag
        c7110277ac44d78b6a9fff2232434d16.
- Responder:
    1. How many TCP ports are open on the machine?
       3.
    2. When visiting the web service using the IP address, what is the domain that we are being redirected to?

unika.htb.

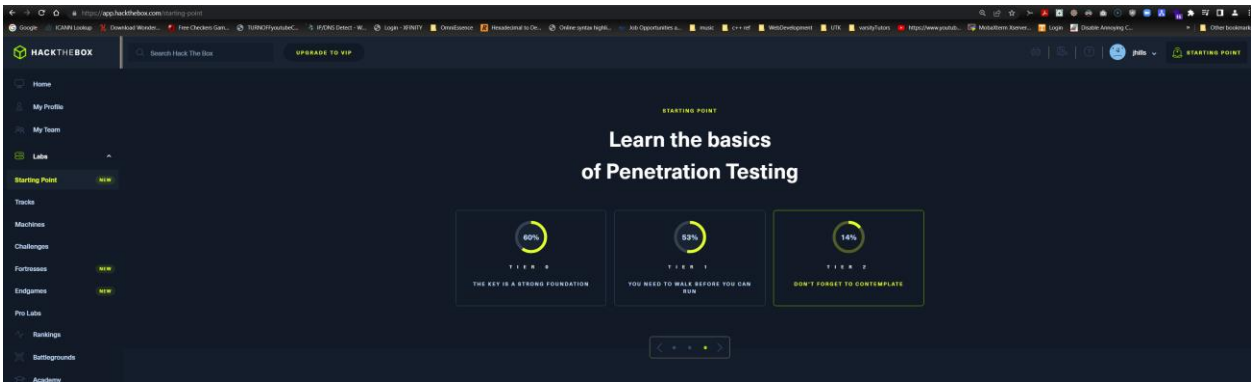
3. Which scripting language is being used on the server to generate webpages?
   php.
4. What is the name of the URL parameter which is used to load different language versions of the webpage?
   page.
5. Which of the following values for the `page` parameter would be an example of exploiting a Local File Include (LFI) vulnerability: "french.html", "//10.10.14.6/somefile", "../../../../../../../../windows/system32/drivers/etc/hosts", "minikatz.exe"
   ../../../../../../../../windows/system32/drivers/etc/hosts.
6. Which of the following values for the `page` parameter would be an example of exploiting a Remote File Include (RFI) vulnerability: "french.html", "//10.10.14.6/somefile", "../../../../../../../../windows/system32/drivers/etc/hosts", "minikatz.exe"
   //10.10.14.6/somefile.
7. What does NTLM stand for?
   New Technology Lan Manager.
8. Which flag do we use in the Responder utility to specify the network interface?
   -i.
9. 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.
10. What is the password for the administrator user?
    badminton.
11. 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.
12. Submit root flag
    ea81b7afddd03efaa0945333ed147fac.

TIER 2:

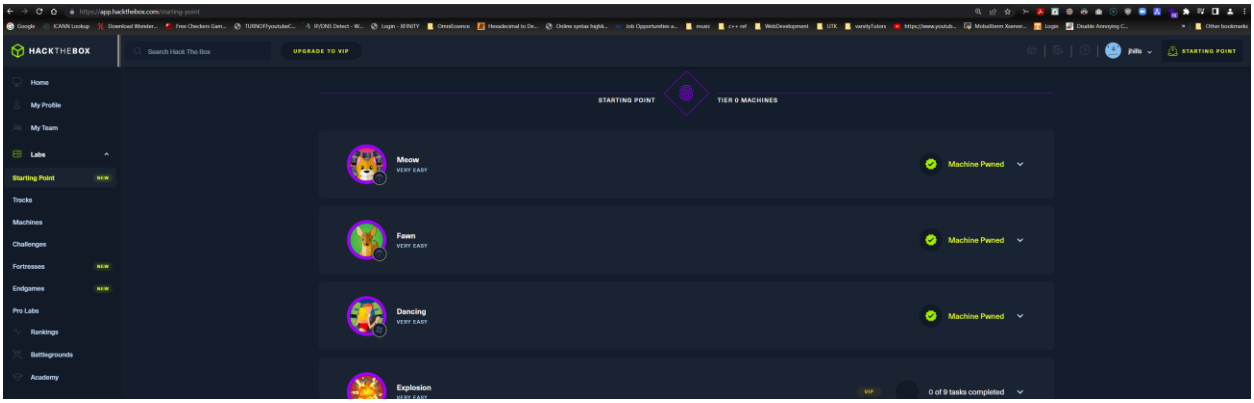
- Archetype:
  1. Which TCP port is hosting a database server?
     1433.
  2. What is the name of the non-Administrative share available over SMB?
     backups.
  3. What is the password identified in the file on the SMB share?
     M3g4c0rp123.
  4. What script from Impacket collection can be used in order to establish an authenticated connection to a Microsoft SQL Server?
     mssqlclient.py.
  5. What extended stored procedure of Microsoft SQL Server can be used in order to spawn a Windows command shell?
     xp_cmdshell.

6. What script can be used in order to search possible paths to escalate privileges on Windows hosts?
   winpeas.
7. What file contains the administrator's password?
   ConsoleHost_history.txt.
8. Submit user flag
   HTB{3e7b102e78218e935bf3f4951fec21a3}.
9. Submit root flag
   b91ccec3305e98240082d4474b848528.

Overview:



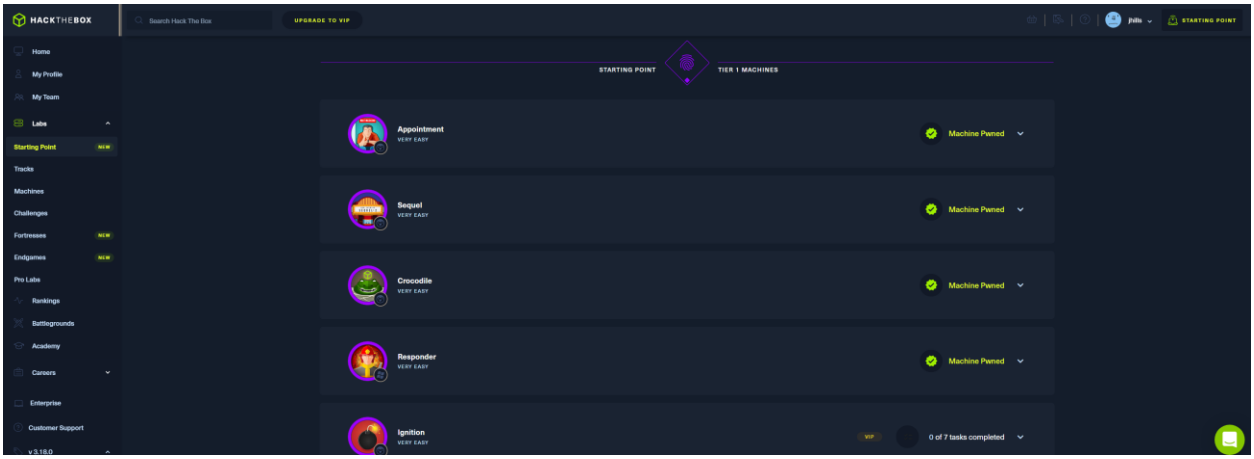
Tier 0:



(continues next page)

Tom Hills
CS566, Dr. Ruoti
Project 7: Hack the Box Intro
04/26/2022

Tier 1:



Tier 2: