Starting Point Tier 0

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 install the following using Homebrew on your terminal.

- brew install nmap
- brew install telnet
- brew install lftp (FTP)
- brew install samba (smbclient)

NOTES:
service FTP uses FTP
service microsoft-ds uses SMB
service redis uses redis-cli

Meow

Task 1: VM stands for ‘Virtual Machine’
Task 2: The ‘terminal’ is used to interact with the OS
Task 3: ‘OpenVPN’ is used to form my vpn connection into HTB labs
Task 4: ‘ping’ is used to test our connection to the target with an ICMP echo request
Task 5: ‘nmap’ is the name of the most common tool for finding open ports on a target
Task 6: ‘telnet’ is the service we identify on port 23/tcp during scans
Task 7: ‘root’ is the username able to log into the target over telnet with a blank password

ROOT FLAG captured via my terminal using the following steps…

- nmap <target-ip> (port 23 is open)
- telnet <target-ip> (connect to login)
- *Meow login:* root (login with blank password)
- ls (list content in dir)
- cat flag.txt

Fawn

Task 1: FTP stands for ‘File Transfer Protocol’
Task 2: FTP usually listens on port ’21’
Task 3: ‘SFTP’ is a later more secure protocol similar to FTP
Task 4: ‘ping’ is used to test our connection to the target with an ICMP echo request

Task 5: From my scans, version ‘vsftpd 3.0.3’ was running on the target
Task 6: ‘Unix’ was running on my target
Task 7: ‘ftp -?’ displays the FTP client help menu
Task 8: ‘anonymous’ is used over FTP to log in without an account
Task 9: The response code for Login successful is ‘230’
Task 10: ‘ls’ lists the files and directories available on the FTP server
Task 11: ‘get’ is the command to download the file found

ROOT FLAG captured via my terminal with the following steps…

- nmap -sV <target-ip> (port 21 is open with ftp services running version vsftpd 3.0.3)
- ftp anonymous@<target-ip>
- ls
- get flag.txt
- exit
- cat flag.txt

Dancing

Task 1: SMB stands for ‘Server Message Block’
Task 2: SMB operates on port ‘445’
Task 3: ‘microsoft-ds’ is the service name that came up on nmap scan
Task 4: ‘-L’ is used with the smbclient to list the available shares on Dancing
Task 5: there were ‘4’ shares on Dancing
Task 6: ‘WorkShares’ allows us to access with a blank password
Task 7: ‘get’ is used within the SMBs shell to download the files found

ROOT FLAG captured via my terminal using the steps below…

- nmap -sV <target-ip>
- smbclient -L //<target-ip>/
- smbclient //<target-ip>/<sharename>
- ls
- cd James.P
- ls
- get flag.txt
- cat flag.txt

Redeemer

Task 1: TCP port ‘6379’ is open on the machine
Task 2: ‘redis’ service is running on the port
Task 3: Redis is a ‘In-memory Database’
Task 4: Redis uses ‘redis-cli’ to interact with the server
Task 5: ‘-h’ is used to specify the hostname
Task 6: ‘info’ command is used to find more information about the server
Task 7: ‘5.0.7’ version is being used on the target machine

Task 8: ‘select’ command is used to select the database in redis
Task 9: ‘4’ keys are present inside the database
Task 10: ‘KEYS *’ command is used to obtain all the keys in the database

ROOT FLAG captured via my terminal using the following steps below…

- nmap -p- <target-ip>
- redis-cli -h <target-ip> -p 6379
- info
- keys *
- get flag

Explosion (VIP)
Preignition (VIP)
Mongod (VIP)
Synced (VIP)