

Forum:[Hack Forums](#)

Thread: [Hack the Box - Starting Point: "The Key Is A Strong Foundation"](#)

Zenthara - May 17, 2025, 5:12 pm

Chapter 1: "The Key Is A Strong Foundation"

Hack The Box Learning Outcomes

In the first tier, you will gain essential skills in the world of cybersecurity pen-testing. You'll start by learning how to connect to various services, such as FTP, SMB, Telnet, Rsync, and RDP anonymously. Next, you'll discover the power of Nmap, a valuable tool for identifying open ports on target systems, allowing you to assess their vulnerabilities. Lastly, you'll explore connecting to a MongoDB server, adding a valuable layer to your penetration testing knowledge. This tier will lay a strong foundation for your journey into the realm of cybersecurity. Learn how to connect FTP, SMB, Telnet, Rsync and RDP anonymously.

Learn how to use Nmap to identify open ports.

Learn how to connect to a MongoDB server.

This post will be broken down into four sections, for each of the FREE HackTheBox machines - these will be in order of how they appear on the HackTheBox website.

Steps to Perform On Setup Only

Connect to the HackTheBox Network

In order to be able to attack the machines you will first need to be on the same Network as the Target machine. HackTheBox provides two methods for accomplishing this: Pwnbox (Recommended) - You will be able to interact with a Virtual Machine through your Web Browser (fully configured & networked). You get two hours for free. This is enough time to complete these challenges.

OpenVPN (Legacy) - If you would rather use your own environment, or you have burned through the free two hours you should configure your own environment. This will be explained in further depth below.

Configuring your own Environment (OpenVPN) This step is only necessary if you wish to use OpenVPN ([Click to View](#))

Step 1: Download Required Software

If you would rather complete these tasks in your own custom environment you should download the following tools: [VMWare](#) (Recommended) // [License Keys for VMware Workstation PRO](#)

[Parrot Security Linux \(OS\)](#) Step 2: Extract the VMDK File from the downloaded ZIP

You can use [WinRAR](#) or [7-zip](#) to extract this file.

At the time of writing, the contained file is named "Parrot-security-6.3.2_amd64.vmdk"

Step 3: Create a new Virtual Machine

Open up VMWare Workstation and click on "Create a New Virtual Machine", if this button is not visible navigate to the top left of the screen and click File -> New Virtual Machine (or press the CTRL + N keybind).

You will have a choice between Typical and Custom within the setup wizard. You should pick Typical.

You will then be prompted for your choice of Operating System, click "I will install the operating system later".

You will then get an additional prompt to provide further information on the Operating System you will be installing, select "Linux" as the Guest Operating System and "Debian 11x 64-bit" as the

version.

You can name the Virtual Machine whatever you would like but I would recommend naming it "ParrotOS"

You can leave the disk size at its default (20GB). You should also keep the "Split virtual disk into multiple files" enabled.

Review the overview and ensure it is accurate. Then click "Finish".

Step 4: Configure the Virtual Machine

Enter the Virtual Machine Settings by doing ANY ONE of the following: Right click the "ParrotOS" Virtual Machine on the sidebar

Click on "ParrotOS" and use the CTRL + D shortcut

Navigate to VM -> Configure on the topbar.

Click on the "Hard Drive" shown on the left hand list, and then click on the "Remove" button at the bottom of the left hand list.

Click "Add" and click "Hard Drive", proceed to the next page.

Keep the Virtual Disk Type set to SCSI (Recommended)

You will then be prompted to select what disk you would like to use, select "Use an existing virtual disk".

Click on "Browse" and select the previously downloaded and unpacked "Parrot-security-6.3.2_amd64.vmdk" file.

Click "Finish".

You may be prompted with a message stating "Convert existing virtual disk image to newer format?" select "Keep Existing Format".

You should now navigate to the "Options" tab.

Select "Shared Folder"

Under the "Folder Sharing" settings select "Always enabled"

Create a path for the Shared Folder (remember this location, you'll need it later) and click "Next"

The only Additional Attribute needed is "Enable this share" and click "Finish".

Select "Advanced" in the options menu

Under "Firmware Type" select "UEFI"

Click "OK".

Step 5: Power on the Virtual Machine

You can start the machine by either: Clicking on "ParrotOS" on the left hand menu and then pressing the CTRL + B shortcut.

Click on "ParrotOS" on the left hand menu and clicking the "Power on this virtual machine" button

You may be prompted with a menu stating "Cannot connect to virtual device ide1:0 because no corresponding..." you should select "Yes" on this menu.

If you get a selection of different versions. Press Enter and it will just select the default one.

Step 6: Configuring the Machine for Attacks

By this point you should now be presented with the ParrotOS desktop, you may be asked if you would like to scan for updates, you should select "Yes".

? This will take a while.

Once the updates have concluded go back onto the HackTheBox website (ensure that you open this INSIDE OF PARROTOS) and navigate [this page](#) and select the Box you would like to complete (Meow, Fawn, Dancing or Redeemer), click on the box and you will be presented with their first step. You should select "Connect with OpenVPN" and the default parameters provided will be fine for this project.

Click on "Download VPN". You will be prompted to download an OVPN file, download this file, and open up a new Terminal window and execute the following commands: `cd /home/user/Downloads`
`sudo openvpn starting_point_YOURNAME.ovpn`

If this was all a success your screen should be [looking something like this](#).
You are now ready to communicate with the HTB machines.

Step to Perform for all Boxes

Spawn Target Machine

Once you have your environment ready and connected to the network you should spawn the Target machine. This can be done on the Learning Outcome with the ["Spawn Target" button](#). This will generate an IP Address, this will be the Target you are attacking.

Table of ContentBox 1: Meow

Box 2: Fawn

Box 3: Dancing

Box 4: Redeemer

[Box 1: Meow](#)

Tags: Telnet, Protocols, Reconnaissance, Weak Credentials, Misconfiguration

[Video Walkthrough: Produced by HackTheBox](#)

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?

To identify the running services on the Network the most common tool to utilise is Nmap, and as such we will use it here, open a new Terminal and execute the following command "nmap VICTIM_IP" and the following output will be returned:

Code Starting Nmap 7.94SVN (<https://nmap.org>) at 2025-05-17 21:59 UTC

Nmap scan report for VICTIM_IP

Host is up (0.037s latency).

Not shown: 999 closed tcp ports (conn-refused)

PORT STATE SERVICE

23/tcp open telnet

Nmap done: 1 IP address (1 host up) scanned in 0.66 secondsAs it can be seen, the only active

port is port 23, and it is running the Telnet service.

Task 7: What username is able to log into the target over telnet with a blank password?
If you need to anonymously login using Telnet the root account should be used.

Submit Flag: Submit Root Flag

Utilising the knowledge we've gained from the previous tasks we know we need to login anonymously on the root account using Telnet on port 23. To do this open up a Command Prompt and execute the following commands: [sudo apt update

[sudo apt-get install telnet

telnet VICTIM_IP

You should then be prompted for "Meow login" ([as shown here](#)), and as we already know, if we want to login without a password, we can attempt to use the "root" account. Once this command has been executed we will be given the following output:

Code +-[user@parrot]-[~]

+-? \$telnet VICTIM_IP

Trying VICTIM_IP...

Connected to VICTIM_IP.

Escape character is '^'.

```
? ?    ??  ??? ?    ?????
???? ?? ???? ???? ? ???? ???? ???? ???? ???
? ? ??? ??? ???? ? ? ? ???  ???? ???? ???
```

Meow login: root

Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-77-generic x86_64)

[list]

[*]Documentation: <https://help.ubuntu.com>

[*]Management: <https://landscape.canonical.com>

[*]Support: <https://ubuntu.com/advantage>

[/list]

System information as of Sat 17 May 2025 10:19:08 PM UTC

```
System load:      0.06
Usage of /:       41.7% of 7.75GB
Memory usage:     4%
Swap usage:       0%
Processes:        135
Users logged in:   0
IPv4 address for eth0: VICTIM_IP
IPv6 address for eth0: dead:beef::250:56ff:fe94:e0bb
```

[list]

[*]Super-optimized for small spaces - read how we shrank the memory footprint of MicroK8s to make it the smallest full K8s around.

[/list]

<https://ubuntu.com/blog/microk8s-memory-optimisation>

75 updates can be applied immediately.

31 of these updates are standard security updates.

To see these additional updates run: `apt list --upgradable`

The list of available updates is more than a week old.

To check for new updates run: `sudo apt update`

Last login: Mon Sep 6 15:15:23 UTC 2021 from 10.10.14.18 on pts/0

root@Meow:~# The part we are most interested in is the line showing "root@Meow:~#" this indicates that we can now run commands on this system. We now need to look for a flag, and initially we can scan the folder we are currently in with the "ls" command.

Code root@Meow:~# ls

flag.txt snap This shows us that we have two things contained within our current folder, a directory called snap/ and a file called flag.txt, to view this file we can use the "cat" command.

Code root@Meow:~# cat flag.txt

b40abdf23665f766f9c61ecba8a4c19 This is flag for the Meow Box! Submit it and this Box is completed!

[Box 2: Fawn](#)

Tags: FTP, Protocols, Reconnaissance, Anonymous/Guest Access

[Video Walkthrough: Produced by HackTheBox](#)

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: FTP sends data in the clear, without any encryption. What acronym is used for a later protocol designed to provide similar functionality to FTP but securely, as an extension of the SSH protocol?

SFTP (a.k.a. Secure File Transfer Protocol)

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?

As was done in the previous box, we will use an Nmap scan to look for open ports and view their relevant banners.

This task however would like to know what version of software is running, to get the Software Version banners we can use the "-sV" parameter for nmap.

Code +-[user@parrot]-[~]

+---? \$nmap -sV VICTIM_IP

Starting Nmap 7.94SVN (<https://nmap.org>) at 2025-05-17 22:34 UTC
Nmap scan report for VICTIM_IP
Host is up (0.035s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 3.0.3
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 1.33 secondsAs can be seen from this scan, the version of FTP running is "vsftpd 3.0.3".

Task 6: From your scans, what OS type is running on the target?
The above scan shows that the Operating System in use is the "Unix" OS within the "Service Info" heading.

Task 7: What is the command we need to run in order to display the 'ftp' client help menu?
ftp -?

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'?
To utilise the FTP commands we must first install it, execute the "sudo apt install ftp -y" command, once this has completed its execution it will now be ready for use.

We know from research on Google that we can login to FTP anonymously using the anonymous account. Once prompted for the password just press Enter and do not provide one.

```
Code +-[user@parrot]-[~]  
+--? $ftp anonymous@VICTIM_IP  
Connected to VICTIM_IP.  
220 (vsFTPd 3.0.3)  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp>From this login we can see that the success code is "230".
```

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. Similarly to Linux we can use the "ls" command to list the files in the current directory.
Code ftp> ls
229 Entering Extended Passive Mode (|||41997|)
150 Here comes the directory listing.

-rw-r--r-- 1 0 0 32 Jun 04 2021 flag.txt

Task 11: What is the command used to download the file we found on the FTP server?

The "get" command is what is utilised in FTP for downloading files. As we know from Task 10, there is a flag.txt file that we would want to see the contents of, let's download that.

Code tp> get flag.txt

local: flag.txt remote: flag.txt

229 Entering Extended Passive Mode (|||38253|)

150 Opening BINARY mode data connection for flag.txt (32 bytes).

100%

[*][b]**[/b]| 32 35.03 KiB/s 00:00 ETA

226 Transfer complete.

32 bytes received in 00:00 (1.05 KiB/s)

Submit Flag: Submit Root Flag

We now have the flag downloaded, it automatically downloads into the Home directory (/home/user/flag.txt), we can view its contents by opening a new Terminal and running the "cat" command.

Code -[user@parrot]-[~]

+-? \$cat /home/user/flag.txt

035db21c881520061c53e0536e44f815This is our flag and we just need to submit it on HackTheBox and we've completed this box!

[Box 3: Dancing](#)

Tags: Protocols, SMB, Reconnaissance, Anonymous/Guest Access

[Video Walkthrough: Produced by FindingUrPasswd](#)

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

Similarly to how we have done it in the last boxes we run an Nmap scan with the "-sV" parameters

Code +-[user@parrot]-[~]

+-? \$nmap -sV VICTIM_IP

Starting Nmap 7.94SVN (https://nmap.org) at 2025-05-17 22:57 UTC

Nmap scan report for VICTIM_IP

Host is up (0.035s latency).

Not shown: 997 closed tcp ports (conn-refused)

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds?

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 8.68 secondsThe service name can be seen as "microsoft-ds".

Task 4: What is the 'flag' or 'switch' that we can use with the smbclient utility to 'list' the available shares on Dancing?

To utilise the smbclient commands we must first install it, execute the "sudo apt install smbclient -y" command, once this has completed its execution it will now be ready for use.

We can then use the -L parameter to list the available shares.

Code +-[?]-[user@parrot]-[~]

+++? \$smbclient -L VICTIM_IP

Password for [WORKGROUP\user]:

```
<pre>[code]Sharename      Type      Comment
-----
```

```
ADMIN$      Disk      Remote Admin
```

```
C$          Disk      Default share
```

```
IPC$        IPC       Remote IPC
```

```
WorkShares  Disk</pre>
```

Reconnecting with SMB1 for workgroup listing.

do_connect: Connection to VICTIM_IP failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)[/code]

When prompted for the password we login anonymously and just press Enter opting not to provide one.

Task 5: How many shares are there on Dancing?

4

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?

Firstly we need to login to the WorkShares anonymously by just pressing Enter opting to not provide a password.

Code +-[user@parrot]-[~]

+++? \$smbclient \\VICTIM_IP\WorkShares

Password for [WORKGROUP\user]:

Try "help" to get a list of possible commands.

smb: > help

```
?          allinfo      altname      archive      backup<br />
blocksize  cancel        case_sensitive cd            chmod<br />
chown      close        del          deltree      dir<br />
du         echo         exit         get          getfacl<br />
geteas     hardlink     help         history      iosize<br />
lcd        link         lock         lowercase    ls<br />
l          mask         md           mget         mkdir<br />
mkfifo     more         mput         newer        notify<br />
open       posix        posix_encrypt posix_open    posix_mkdir<br />
posix_rmdir posix_unlink posix_whoami  print        prompt<br />
put        pwd          q            queue        quit<br />
readlink   rd           recurse      reget        rename<br />
```

```

reput      rm      rmdir      showacls    setea<br />
setmode    scopy    stat      symlink    tar<br />
tarmode    timeout  translate unlock     volume<br />
vuid       wdel      logon     listconnect showconnect<br />
tcon       tdis      tid       utimes     logoff<br />
..

```

!
After looking through the list of commands the most useful will be "ls" for listing file content, "cd" for changing the directory and "get" for downloading files.

Submit Flag: Submit Root Flag

Code +-[user@parrot]-[~]

+++? \$smbclient \\VICTIM_IP\WorkShares

Password for [WORKGROUP\user]:

Try "help" to get a list of possible commands.

smb: > ls

```

.                D      0 Mon Mar 29 08:22:01 2021
..               D      0 Mon Mar 29 08:22:01 2021
Amy.J            D      0 Mon Mar 29 09:08:24 2021
James.P          D      0 Thu Jun  3 08:38:03 2021

```

<pre>[code] 5114111 blocks of size 4096. 1754167 blocks available</pre>

smb: > cd Amy.J\

smb: \Amy.J> ls

```

.                D      0 Mon Mar 29 09:08:24 2021
..               D      0 Mon Mar 29 09:08:24 2021
worknotes.txt    A     94 Fri Mar 26 11:00:37 2021

```

<pre>Code 5114111 blocks of size 4096. 1754167 blocks available</pre>

smb: \Amy.J> cd ..

smb: > cd James.P\

smb: \James.P> ls

```

.                D      0 Thu Jun  3 08:38:03 2021
..               D      0 Thu Jun  3 08:38:03 2021
flag.txt         A     32 Mon Mar 29 09:26:57 2021

```

<pre>Code 5114111 blocks of size 4096. 1754167 blocks available</pre>

smb: \James.P> get flag.txt

getting file \James.P\flag.txt of size 32 as flag.txt (0.3 KiloBytes/sec) (average 0.3 KiloBytes/sec)[/code]

Now that we have the flag.txt file downloaded, it will be downloaded to the home directory (/home/user/flag.txt), we can view it with the "cat" command.

Code +-[user@parrot]-[~]

+++? \$cat /home/user/flag.txt

5f61c10dffbc77a704d76016a22f1664Now that the flag has been acquired we just submit this in HackTheBox and this box is completed!

[Box 4: Redeemer](#)

Tags: Redis, Vulnerability Assessment, Databases, Reconnaissance, Anonymous/Guest Access

[Video Walkthrough: Produced by CryptoCat](#)

Task 1: Which TCP port is open on the machine?

As usual let's attempt to run an Nmap scan and see what results we get back.

```
Code +-[?]-[user@parrot]-[~]
```

```
+--? $nmap VICTIM_IP
```

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-17 23:27 UTC
```

```
Nmap scan report for VICTIM_IP
```

```
Host is up (0.044s latency).
```

```
All 1000 scanned ports on VICTIM_IP are in ignored states.
```

```
Not shown: 1000 closed tcp ports (conn-refused)
```

Nmap done: 1 IP address (1 host up) scanned in 0.75 secondsThis is new. Nmap hasn't detected any open ports! This however is common as it only checks a small number of ports by default. If we however specify the "-p1-65535" it'll scan every single port that could be open.

```
Code +-[user@parrot]-[~]
```

```
+--? $nmap -p1-65535 VICTIM_IP
```

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-17 23:29 UTC
```

```
Nmap scan report for VICTIM_IP
```

```
Host is up (0.031s latency).
```

```
Not shown: 65534 closed tcp ports (conn-refused)
```

```
PORT    STATE SERVICE
```

```
6379/tcp open  redis
```

Nmap done: 1 IP address (1 host up) scanned in 15.03 secondsWe have found an open TCP port on "6379".

Task 2: Which service is running on the port that is open on the machine?

We can also see from the above Nmap scan that "Redis" is the service running on the port.

Task 3: What type of database is Redis? Choose from the following options: (i) In-memory Database, (ii) Traditional Database

Redis is an "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"
```

This can be installed through running the following command: "sudo apt install redis-tools -y"

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"
```

```
Code +-[?]-[user@parrot]-[~]
```

```
+--? $redis-cli -h VICTIM_IP
```

VICTIM_IP:6379> info

[b]Server[/b]

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
arch_bits:64
multiplexing_api:epoll
atomicvar_api:atomic-builtin
gcc_version:9.3.0
process_id:754
run_id:3cf8deecffe2b9765c98009eb0229e81ee3e462c
tcp_port:6379
uptime_in_seconds:675
uptime_in_days:0
hz:10
configured_hz:10
lru_clock:2694415
executable:/usr/bin/redis-server
config_file:/etc/redis/redis.conf

[b]Clients[/b]

connected_clients:1
client_recent_max_input_buffer:2
client_recent_max_output_buffer:0
blocked_clients:0

[b]Memory[/b]

used_memory:859624
used_memory_human:839.48K
used_memory_rss:5894144
used_memory_rss_human:5.62M
used_memory_peak:859624
used_memory_peak_human:839.48K
used_memory_peak_perc:100.12%
used_memory_overhead:846142
used_memory_startup:796224
used_memory_dataset:13482
used_memory_dataset_perc:21.26%
allocator_allocated:1570200
allocator_active:1892352
allocator_resident:9101312
total_system_memory:2084024320
total_system_memory_human:1.94G

used_memory_lua:41984
used_memory_lua_human:41.00K
used_memory_scripts:0
used_memory_scripts_human:0B
number_of_cached_scripts:0
maxmemory:0
maxmemory_human:0B
maxmemory_policy:noeviction
allocator_frag_ratio:1.21
allocator_frag_bytes:322152
allocator_rss_ratio:4.81
allocator_rss_bytes:7208960
rss_overhead_ratio:0.65
rss_overhead_bytes:-3207168
mem_fragmentation_ratio:7.21
mem_fragmentation_bytes:5076528
mem_not_counted_for_evict:0
mem_replication_backlog:0
mem_clients_slaves:0
mem_clients_normal:49694
mem_aof_buffer:0
mem_allocator:jemalloc-5.2.1
active_defrag_running:0
lazyfree_pending_objects:0

[b]Persistence[/b]

loading:0
rdb_changes_since_last_save:4
rdb_bgsave_in_progress:0
rdb_last_save_time:1747524204
rdb_last_bgsave_status:ok
rdb_last_bgsave_time_sec:-1
rdb_current_bgsave_time_sec:-1
rdb_last_cow_size:0
aof_enabled:0
aof_rewrite_in_progress:0
aof_rewrite_scheduled:0
aof_last_rewrite_time_sec:-1
aof_current_rewrite_time_sec:-1
aof_last_bgrewrite_status:ok
aof_last_write_status:ok
aof_last_cow_size:0

[b]Stats[/b]

total_connections_received:6
total_commands_processed:6
instantaneous_ops_per_sec:1
total_net_input_bytes:306
total_net_output_bytes:11572

instantaneous_input_kbps:0.03
instantaneous_output_kbps:7.05
rejected_connections:0
sync_full:0
sync_partial_ok:0
sync_partial_err:0
expired_keys:0
expired_stale_perc:0.00
expired_time_cap_reached_count:0
evicted_keys:0
keyspace_hits:0
keyspace_misses:0
pubsub_channels:0
pubsub_patterns:0
latest_fork_usec:0
migrate_cached_sockets:0
slave_expires_tracked_keys:0
active_defrag_hits:0
active_defrag_misses:0
active_defrag_key_hits:0
active_defrag_key_misses:0

[b]Replication[/b]

role:master
connected_slaves:0
master_replid:18739e05b904198b4c960c14d5fa8c53a51acf26
master_replid2:0000000000000000000000000000000000000000
master_repl_offset:0
second_repl_offset:-1
repl_backlog_active:0
repl_backlog_size:1048576
repl_backlog_first_byte_offset:0
repl_backlog_histlen:0

[b]CPU[/b]

used_cpu_sys:0.585340
used_cpu_user:0.485129
used_cpu_sys_children:0.000000
used_cpu_user_children:0.000000

[b]Cluster[/b]

cluster_enabled:0

[b]Keyspace[/b]

db0:keys=4,expires=0,avg_ttl=0

Task 7: What is the version of the Redis server being used on the target machine?
As shown from the information above, the Redis version is 5.0.7

Task 8: Which command is used to select the desired database in Redis?
The "select" command.
Code VICTIM_IP:6379> select 0
OK

Task 9: How many keys are present inside the database with index 0?
4
Code VICTIM_IP:6379> keys *

```
[list=1]
[*]"numb"
[*]"flag"
[*]"temp"
[*]"stor"/list]
```

Task 10: Which command is used to obtain all the keys in a database?
"keys *"

Submit Flag: Submit Root Flag

Now that we have all the prerequisites we can run the "get" command on the flag key.

Code VICTIM_IP:6379> get flag

"03e1d2b376c37ab3f5319922053953eb" We now have the flag and can submit this to HackTheBox
- and that concludes this box.

Syndicate - May 17, 2025, 5:14 pm

Thanks for posting this brother! I'm sure someone will find it helpful :)

StinkButt420 - May 17, 2025, 6:20 pm

Man, this would have been DOPE to have when I was just starting out. I read the official writeups,
LIKE A NERD!

DramaKing - May 17, 2025, 6:20 pm

Labeling it 'spoilers' or 'walkthrough' would be expected.

Zenthara - May 17, 2025, 6:33 pm

(May 17, 2025 06:20 PM) DramaKing Wrote: [\[CITE\]](#) Labeling it 'spoilers' or 'walkthrough' would be expected. There's a few things I wish I could change but once I was posting them my posts all got merged into one single post - I'll keep it in mind for the next post though.