**TryHackMe – Mr Robot CTF**

**Victim**: 10.10.125.184

**Kali**: 10.8.180.190

**N****map**

A computer screen shot of white text

Description automatically generated

**Viewing Scan**

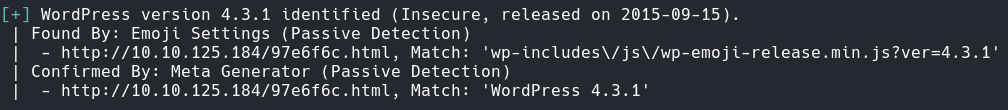


A screenshot of a computer

Description automatically generatedWhen I looked at the URL I noticed the ending would change to fit the command. I then thought about adding a custom command “LS” to try and list contents. However I got some useful information.

**WPScan**





A close up of a computer screen

Description automatically generated

**HTTPie**

A screen shot of a computer

Description automatically generated

A computer screen shot of a computer program

Description automatically generated

There was this hash value and there was a dictionary downloaded.

**FFUF**

Nothing was found.

A screenshot of a computer screen

Description automatically generated**Gobuster**

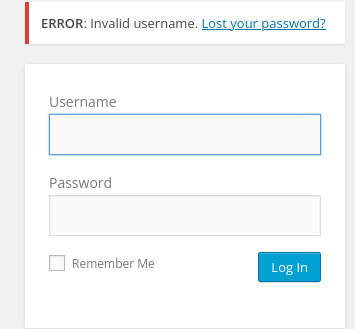




A screenshot of a computer

Description automatically generated

Nothing really of interest has been found.

After looking at the login page for a bit, I started testing some usernames and passwords. I realised that information about the username was given.

**Hydra**

A screenshot of a login box

Description automatically generated

The reason why the password test was used because I want to discover the valid username. This is only possible because of the ERROR message that is displayed telling us that either the username or password is incorrect.

It’s a post request because I looked at burp suit and saw a post request to submit the username & password. The last part of the command shows success based on the error message produced.

Password discovered was ER28-0652. (forget to get a screenshot).

Exploitation

A screenshot of a menu

Description automatically generatedIn the dashboard I went to appearance, then editor. Next, I went to archives.

A screenshot of a computer

Description automatically generated

I then replaced the existing PHP code with my own reverse shell from pen test monkey.

A screenshot of a computer

Description automatically generated

Setup netcat, this will allow you to connect.

A computer screen with white text

Description automatically generatedGo to the site above.

Now I am in.

**Upgrade Shell**

A computer screen shot of a program code

Description automatically generated

LinPEAS

I then downloaded linPEAS onto the victim machine.

A screenshot of a computer program

Description automatically generated

A computer screen shot of a computer

Description automatically generatedI was able to obtain a hash for the next account (lateral movement).

**Crackstation**

I was able to crack the hash (abcdefghijklmnopqrstuvwxyz).

|  |
| --- |
|  |

A close up of a black background

Description automatically generated

**Flag 2**

A computer screen with white text

Description automatically generated

A computer screen with white text

Description automatically generatedI will try to use the kernel exploit (dirtycow).

A computer screen shot of a computer code

Description automatically generated

It didn’t work.

A computer screen shot of a computer code

Description automatically generated**Find SUID Binaries**

Nmap is an interesting one.

I read that you can spawn a shell using nmap, once you have entered interactive mode.

A blue background with white text

Description automatically generated



A black background with white text

Description automatically generatedBash spawning didn’t work.

A screen shot of a computer

Description automatically generatedShell spawning gave me root.

A computer code with white text

Description automatically generated**Flag 3**