Stapler

Status in-progress

+ Add a Property

Add a comment...

Figuring out the machine IP address

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

Bash

Nmap Scanning on the IP address

```bash
nmap -Pn -p- 192.168.99.100 -e eth1 -oN nmap nmap -A -sC -
sV -p20,21,22,53,80,137,139,3306,12380 192.168.99.100 -e
eth1 -oN nmap-detailed
```

Bash

nmap.txt 0.5KB

Resuts of the nmap scan in normal format

nmap-detailed.txt 3.1KB

Possible network attack vectors and explanations

Name	Status	Reason
21 FTP	info-gathering	Got few files using anonymous login
80 HTTP	not-exploited	Got nothing out of the server
139 SMB	info-gathering	Got few files from this system as well
3306 MySQL	not-exploited	Unable to login to the system
12380 HTTPS	exploited	Got the page to the internal wordpress website

COUNT 5

12380 HTTPS - Internal Index Page

Wit[illegible]

```bash
/a[illegible]
WordPress
```

Exploit the `Advanced Video plugin` to get output of the `/etc/passwd` file to get usernames to enumerate for ssh logins. Used `hydra and top-20 ssh passwords` to check for valid logins and was able to find 2. Using 1 of the logins, I ran `LinEnum.sh` to get information and was able to find `passwords for 2 more users` one of which had `sudo-ed` recently, using this I read the `/root/flag.txt` file and got flag.

Box solved.

Tricky points were to use hydra for password cracking after getting usernames for the machine, as there was no other vector to attack, at least the one I know of.