W1R3S

Status   complete

+ Add a Property

Add a comment...

Figuring out the machine IP address

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

Nmap Scanning on the IP address

```bash
nmap -Pn -e eth1 -oN nmap 192.168.99.102 nmap -Pn -p- -e
eth1 -oN nmap-all 192.168.99.102 nmap -A -sC -sV -p
21,22,80,3306 -e eth1 -oN nmap-detailed 192.168.99.102
```

📎 nmap 0.4KB

📎 nmap-all 0.4KB

📎 nmap-detailed 1.6KB

Possible network attack vectors and explanations

Aa Name	⊘ Status	☰ Reason
21 FTP	not-exploited	Found few useless files
22 SSH	exploited	Used LFI from Cuppa and logged into get shell
80 HTTP	exploited	Exploited CuppaCMS exploit and got LFI to get `PASSWD` and use `w1r3s` account and `shadow` file hash to get password and login to the shell and then `sudo -i` to get root.

Important Tips and Tricks

+ New

- `curl -s --data-urlencode`

COUNT 3

`http://192.168.1.106/administrator/alerts/alertConfigField.php`