

# Pluck

▼ 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 -e eth1 -oN nmap 192.168.99.100 nmap -Pn -p- -e  
eth1 -oN nmap-all 192.168.99.100 nmap -A -sC -sV -p  
22,80,3306,5355 -e eth1 -oN nmap-detailed 192.168.99.100
```




Bash ▼

 nmap 0.4KB

 nmap-all 0.4KB

 nmap-detailed 0.9KB

**Possible network attack vectors and explanations**

 Name	 Status	 Reason
<u>22 SSH</u>	exploited	Tried HYDRA with common passwords and usernames extracted from /etc/passwd but no combination see to work.
<u>80 HTTP</u>	exploited	Extracted all the files using PHP LFI using php:// as well as there was a native LFI in the code itself which was easier to exploit.

## 80 HTTP

Exploited LFI with the `page` parameter and extracted the `backup.tar` which I got the reference from

`/usr/local/etc/passwd` this was because I was `root` `user` and in the `backup.tar` I found `keys for SSH for paul`. I had to fix permissions for all the files to make them work and the `permission was 0400 or all the files`.

I was greeted with the `pdmenu` and to escape i had to use `VIM shell escape trick` and it got me shell after that I had to use `DirtyCow exploit (40616)` to get root.