四 情报收集

实验目的

1、 掌握系统信息等基本信息收集方法；

2、 理解网络安全攻击与防御策略。

实验环境

1、 Metasploitable2 虚拟机；

2、 Kali 虚拟机。

实验讲解

渗透测试是一种通过模拟恶意黑客攻击的技术与方法。渗透测试主要依据CVE(Common Vulnerabilities and Exposures)已经发现的安全漏洞，模拟入侵者的攻击方法对网站应用、服务器系统和网络设备进行破坏性质的攻击性测试。

渗透测试执行流程如下：

1. 前期交互阶段
2. 情报收集阶段
3. 威胁建模阶段
4. 漏洞分析阶段
5. 渗透攻击阶段
6. 后渗透攻击阶段
7. 报告阶段

其中，信息收集是进行渗透攻击的前提，通过信息收集可以有针对性的指定模拟攻击测试计划，提高模拟攻击的成功率，同时可以有效的降低攻击测试对系统正常运行造成的不利影响。

一、 系统信息收集

1. whois

whois 用于查询域名 IP 及所有者等信息的传输协议，如可用于查询域名是否已经被注册，以及注册域名的详细信息的数据库(域名所有人、域名注册信息等)。如：

```
whois baidu.com
```

2. dmitry

dmitry 是一个由 C 语言编写的 UNIX/Linux 命令行工具，可用于收集主机相关信息，如子域名、Email 地址、系统运行时间等。如：

```
dmitry baidu.com
```

3. whatweb

whatweb 可用于网站指纹识别。如：

```
whatweb baidu.com
```

4. 其它

其它如网站目录扫描 dirsearch，域名枚举 dnsenum，子域名爆破 subDomainsBrute 等。

二、 端口扫描

Nmap 是 Linux 下的网络扫描和嗅探工具包，是使用最广泛的端口扫描工具，可用于主机发现、端口扫描、版本侦测、操作系统探测等用途。

语法：nmap [Scan Type(s)] [Options] {target specification}

Nmap 常见参数：

选项	功能
-sL	List Scan 列表扫描，仅将指定的目标的IP列举出来，不进行主机发现
-sn	Ping Scan 只进行主机发现，不进行端口扫描
-Pn	将所有指定的主机视作开启的，跳过主机发现的过程
-PS/PA/PU/PY [portlist]:	使用TCP SYN/ACK或SCTP INIT/ECHO方式进行发现
-PE/PP/PM:	使用ICMP echo, timestamp, and netmask 请求包发现主机
-PO[protocollist]	使用IP协议包探测对方主机是否开启
-n/-R	-n表示不进行DNS解析；-R表示总是进行DNS解析。
--dns-servers <serv1[,serv2],...>	指定DNS服务器
--system-dns	指定使用系统的DNS服务器
--traceroute	追踪每个路由节点

1. 主机发现

```
nmap -sn 192.168.254.1-255
```

```
root@bogon:/# nmap -sn 192.168.254.1-255
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-12 21:08 CST
Nmap scan report for bogon (192.168.254.1)
Host is up (0.00042s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for bogon (192.168.254.2)
Host is up (0.00024s latency).
MAC Address: 00:50:56:E3:0B:7A (VMware)
Nmap scan report for bogon (192.168.254.128)
Host is up (0.00047s latency).
MAC Address: 00:0C:29:4C:1E:39 (VMware)
Nmap scan report for bogon (192.168.254.254)
Host is up (0.00082s latency).
MAC Address: 00:50:56:EA:8D:D4 (VMware)
Nmap scan report for bogon (192.168.254.129)
Host is up.
Nmap done: 255 IP addresses (5 hosts up) scanned in 2.01 seconds
```

图 4.1 主机发现

2. TCP 端口扫描

nmap －sS 192.168.254.128

```
root@bogon:/# nmap -sS 192.168.254.128
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-12 21:13 CST
Nmap scan report for bogon (192.168.254.128)
Host is up (0.0031s latency).
Not shown: 977 closed ports
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
```

图 4.2 TCP 端口扫描

3. 版本侦测

nmap -sV 192.168.254.128

```
root@bogon:~# nmap -sV 192.168.254.128
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-12 21:24 CST
Nmap scan report for bogon (192.168.254.128)
Host is up (0.00091s latency).
Not shown: 977 closed ports
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?
513/tcp  open  login?
```

图 4.3 TCP 版本侦测

4. 操作系统侦测

nmap -O 192.168.254.128

```
MAC Address: 00:0C:29:4C:1E:39 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

图 4.4 操作系统侦测

5. 防火墙探测

nmap -sA 192.168.254.128

```
root@bogon:/# nmap -sA 192.168.254.128
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-12 21:21 CST
Nmap scan report for bogon (192.168.254.128)
Host is up (0.0039s latency).
All 1000 scanned ports on bogon (192.168.254.128) are unfiltered
MAC Address: 00:0C:29:4C:1E:39 (VMware)
```

图 4.5 防火墙探测

三、 漏洞扫描

漏洞扫描技术建立于端口扫描基础之上，在端口扫描后得知目标主机开启的端口及端口上的网络服务，并将相关信息与漏洞扫描系统提供的漏洞裤及进行匹配，查看是否有满足匹配条件的漏洞。

个人常见漏洞扫描工具有：AWVS、Nessus、OpenVAS、Burpsuite、Nikto 等。

Nikto 是一款开源的网页服务扫描器，包含超过 3300 种有潜在危险的文件 CGIs，超过 625 种服务器版本，超过 230 种特定服务器问题，可对网页服务器进行全面的多种扫描。

1. Nikto 升级与更新插件

```
nikto –update
```

2. 查看插件

```
nikto –list-plugins
```

3. 扫描主机

```
nikto –host 192.168.254.128
```

4. 扫描主机及端口

```
nikto –host 192.168.254.128 –port 80
```

实验内容

1、 根据系统中命令帮助或查询互联网，查询靶机或特定主机基本信息；

2、 使用 nmap 命令，查询靶机更多信息；

3、 使用漏洞扫描工具（自定），扫描靶机可疑漏洞。