实验 2 Nmap扫描器应用

实验目的

1.掌握Nmap扫描器的使用方法。
2.借助Nmap实现网内主机探测、服务探测、系统探测和漏洞探测。

实验内容

1.Nmap基本命令学习；
2.识别活跃的主机；
3.查看打开端口；
4.系统指纹信息识别；
5.服务的指纹识别；
6.追踪路由信息；
7.保存结果到文件
8.TCP 扫描与UDP扫描
9.检查是否有防火墙

实验前提

完成本实验，需要事先安装：

- kali 201902虚拟机，假设其IP地址为：10.10.10.130
- owasp bwa v1.2 虚拟机或者其它可用于扫描的靶机。假设其IP地址为：10.10.10.135

实验步骤

Nmap 常用参数速查表

- -sT
  TCP connect()扫描，这种方式会在目标主机的日志中记录大批的链接请求以及错误信息。
- -sP
  ping扫描，加上这个参数会使用ping扫描，只有主机存活，nmap才会继续扫描，一般最好不加，因为有的主机会禁止ping，却实际存在。

- -sS
  半开扫描，一般不会记入日志，不过需要root权限。
- -sU
  udp扫描，但是一般不可靠，
- -sA
  用来穿过防火墙的规则集，速度慢。
- -sV
  端口服务及版本
- -A
  包含了-sV，-O，全面系统检测，启动脚本检测，扫描等。
- -P0
  扫描之前不使用ping，适用于防火墙禁止ping，比较有用。
- -v
  显示扫描进程
- -O
  探测目标系统的漏洞，容易误报
- -oN/-oX/-oG
  将报告写入文件，格式分别为正常（自定义.txt）,XML,grepable.
- -iL
  扫描主机列表
- -sC　--script=default
  默认的脚本扫描，主要是搜集各种应用服务的信息

Nmap扫描实验 1 识别活跃的主机

使用nmap查看主机是否在线，执行命令如下：

```
# 扫描单个主机IP
nmap -sP 10.10.10.135

# 扫描整个子网
nmap 10.10.10.0/24

# 扫描多个主机
namp 10.10.10.135 10.10.10.136

# 扫描一个小范围
nmap 10.10.10.135-200

# 扫描某个文件（txt）内的ip列表
nmap -iL text.txt

# 扫描除某个目标外
nmap 10.10.10.135/24 -exclude 10.10.10.130
# 扫描除某个目标文件外的ip
nmap 10.10.10.135/24 --exclude targets.txt

# 设置扫描强度，最快为T5 ， 最慢为T1
nmap -T5 10.10.10.135/24
```

Nmap扫描实验 2 查看打开端口

常用命令如下：

```
# 使用nmap查看10.10.10.135上常用的1-1000号端口
nmap 10.10.10.135

# 扫描指定扫描端口（指定扫描100-1000范围内的端口）
nmap -p 20-25,80,443 10.10.10.135

# 使用 -F 快速扫描参数，扫描1-100号端口
nmap -F 10.10.10.135

# 扫描特定端口3389
nmap -p 3389 10.10.10.135

# 扫描所有端口
nmap -p 10.10.10.135
```

Nmap扫描实验 3 系统指纹信息识别

常用命令如下：

```
# 加-O参数用于识别操作系统,如:
nmap -O 10.10.10.135

# 使用 -A 参数提供更多信息
nmap -A 10.10.10.135
```

Nmap扫描实验 4 服务的指纹识别

```
# 使用选项 -sV可以查看端口服务版本信息
nmap -sV 10.10.10.135
```

Nmap扫描实验 5 追踪路由信息

```
# 使用 --traceroute，完成路由追踪
nmap --traceroute 某个域名

# 显示主机接口和路由
nmap --iflist
```

Nmap扫描实验 6 保存结果到文件

```
# 保存到文本文件中,使用 -oN 路径
nmap -oN <path where you want to save file> 某个域名
# 或者用 > (重定向符)
nmap 10.10.10.135 > output.txt

# 保存到xml文件，使用 -oX 路径
nmap -oX <path where you want to save file> 某个域名
```

Nmap扫描实验 7 TCP 扫描与UDP扫描

```
# 使用-sS 表示TCP SYN 扫描、-sU表示 UDP扫描
 nmap -sS -sU -PN 192.168.0.164

# Fin scan
nmap -sF 192.168.7
```

Nmap扫描实验 8 检查是否有防火墙

```
# 使用-sA 即ACK扫描
nmap -sA 192.168.1.254

# 使用 -PN
nmap -PN 192.168.1.1

# 如果有防火墙，阻碍icmp ping探测，可以尝试下列命令
nmap -PS 192.168.1.1
nmap -PS 80,21,443 192.168.1.1
nmap -PA 192.168.1.1
nmap -PA 80,21,200-512 192.168.1.1

**The following scan types exploit a subtle loophole in the TCP and good for testing security of common attacks:

## TCP Null Scan to fool a firewall to generate a response ## ## Does not set any bits (TCP flag header is 0) ##

Command: nmap -sN 192.168.1.254

## TCP Fin scan to check firewall ## ## Sets just the TCP FIN bit ##

Command:nmap -sF 192.168.1.254

## TCP Xmas scan to check firewall ## ## Sets the FIN, PSH, and URG flags, lighting the packet up like a Christma

Command: nmap -sX 192.168.1.254
```

Nmap扫描实验 7 扫描 IPv6

```
# 使用 -6 参数 表示地址为ipv6
nmapp -6 ipv6 address here
```

其中，'-6' 将开启 ipv6 扫描.

Nmap扫描实验 8 显示 nmap 端口扫描结果的判断依据

```
# 使用 --reason
nmap --reason 192.168.0.1

# 显示所有发出和收到的数据包
nmap --packet-trace 192.168.1.1
```

Nmap扫描实验 9 Nmap的多种扫描方法

```
# Scan a host using ip protocol ping
nmap -PO 192.168.1.1

# Scan a host using UDP ping
nmap -PU 192.168.1.1
nmap -PU 2000.2001 192.168.1.1

# Scan for IP protocol
nmap -sO 192.168.1.1
```

选学内容：Nmap扫描更多实例

以下内容可以选作。

```
# 获取远程主机信息（-sS 为TCP SYN扫描，-Po 允许icmp，-sV 服务版本检测，-O 识别os）
nmap -sS -Po -sV -O <target>

# 获取指定且open端口的服务信息
nmap -sT -p 80 -oG – 192.168.1.* | grep open

# 找出192.168.0.网段内所有活跃设备
nmap -sP 192.168.0.*

# 找出给定子网内没使用的ips
nmap -T4 -sP 192.168.2.0/24 && egrep “00:00:00:00:00:00” /proc/net/arp

# 扫描LAN中有 Conficker 病毒的主机
nmap -PN -T4 -p139,445 -n -v –script=smb-check-vulns –script-args safe=1
192.168.0.1-254


# 扫名 Rouge Network可用的服务
nmap -A -p1-85,113,443,8080-8100 -T4 –min-hostgroup 50 –max-rtt-timeout
2000 –initial-rtt-timeout 300 –max-retries 3 –host-timeout 20m
–max-scan-delay 1000 -oA wapscan 10.0.0.0/8

# 使用代理(-D 192.168.0.2)，以隐藏自身
sudo nmap -sS 192.168.0.10 -D 192.168.0.2
```

实验报告要求

至少完成7个上述NMAP实验内容，截图记录执行结果，填写实验报告。