# Nmap多年積累實操經驗分享

發布: 2023年2月14日10:17:50

## 全量端口基礎方案簡單梳理

21 FTP弱密码
22 SSH弱密码
23 telnet弱密码
25 邮件伪造,vrfy/expn查询邮件用户信息,可使用smtp-user-enum工具来自动跑
53 DNS溢出、远程代码执行、允许区域传送,dns劫持,缓存投毒,欺骗以及各种基于dns隧道的远控
69 尝试下载目标及其的各类重要配置文件
80 IIS6 RCE
80-89 应用服务器端口
110 POP3 可尝试爆破,嗅探
111 NFS 权限配置不当
137 SMB
143 IMAP 爆破
161 SNMP 爆破默认团队字符串,搜集目标内网信息
139 SMB嗅探
161 SNMP默认团体名/弱口令漏洞
389 LDAP注入、匿名访问、弱口令
443 POODLE漏洞、应用服务器端口
445 ms17-010、ms08-067
464 kpasswd Kerberos 口令和钥匙改换服务
512,513,514 Linux rexec爆破,rlogin登陆
554 RTSP
873 RSYNC
1080 shadowsocks 可以尝试使用ss代理工具进行代理
1194 OpenVPN 想办法钓VPN账号,进内网
1352 Lotus 弱口令,信息泄漏,爆破
1433 mssql (sql server) 注入,提权,sa弱口令,爆破
1500 ISPmanager 弱口令
1521 Oracle tns爆破,注入,弹shell…
1723 PPTP 爆破,想办法钓VPN账号,进内网
2082,2083 cPanel 弱口令
2049 NFS 权限配置不当
2181 Zookeeper
2375 docker
2601,2604 Zebra 默认密码zerbra
3000 grafan
3128 Squid 弱口令
3306 mysql弱密码
3312,3311 kangle 弱口令
3389 ms12-020、Windows rdp shift后门[需要03以下的系统]、爆破
3690 svn泄露,未授权访问
4848 GlassFish 弱口令
4899 radmin

```
5000 Flask、Sybase/DB2 爆破,注入
5432 postgresql 爆破,注入,弱口令
5900,5901,5902 VNC 弱口令爆破 VNC提权
5984 couchdb
5985 SOAP
6379 redis未授权访问
6443 Kubernetes
7001 weblogic、websphere
7002 WebLogic Java反序列化一大堆,弱口令
7778 Kloxo 主机面板登录
8000 Ajenti 弱口令
8069 Zabbix 远程执行,SQL注入
8080 jenkins、GeoServer、Kubernetes、JBOSS、libssh、poodle
8180 libssh - cve-2018-10933、JBOSS
8393、8983、8081、80、443、8080 solr
8443 Plesk 弱口令
8440-8450,8080-8089 应用服务器端口（可尝试经典的topn,vpn,owa,webmail,目标oa,各类Java控制台,各类服务器Web管理面板,各类Web中间件漏 洞利用,各类Web框架漏洞利用等等……）
8161 ActiveMQ后台弱密码(admin/admin)漏洞以及put写shell
9080-9081,9090 WebSphere（应用服务器） Java反序列化/弱口令
9043 、9443 poodle
9200，9300 Elasticsearch未授权访问漏洞、elasticsearch远程命令执行、Elasticsearch任意文件读取
11211 memcache
27017，27018 mongodb
43958 Serv-U
50070，50030 hadoop
61616 ActiveMQ
```

複製

# 初階

## 一.主機發現

### 四層傳輸（TCP+UDP協議）

```
nmap -sP -PS[端口1，端口2...或端口范围][目标]（TCP SYN Ping）
nmap -sP -PY[端口1，端口2][目标]（SCTP INIT Ping）
nmap -sP -PA[端口1，端口2][目标]（TCP ACK Ping）
nmap -sP -PU[端口1，端口2][目标]（UDP Ping）发送空UDP到端口31和338，默认使用40125端口
```

複製

## 二.端口掃描

### 端口範圍（0~65535）

```
0~1023  有的系统可以改变，有的系统协议使用的是固定的
特点：有的系统可以改变，有的系统协议使用的是固定的
WWW默认80端口；FTP默认21端口；139专用于NetBIOS与TCP/IP之间的通信

1024~49151
特点：一般不固定分配某种服务，而是根据程序申请

49152~65535
特点：进程主要是用户所安装的应用程序
```

複製

### 基礎知識

```
TCP     FTP数据连接
TCP     FTP控制连接
```

```
TCP|UDP Secure Shell（SSH）服务
TCP     Telnet服务（远程登陆）
TCP     Simple Mail Transfer Protocol（SMTP，简单邮件传输协议）
TCP|UDP Windows Internet Name Service(WINS,Windows网络名称服务)
TCP|UDP Domain Name System（DNS，域名系统）
UDP     DHCP服务
UDP     DHCP客户端
UDP     Trivial File Transfer Protocol（TFTP，普通文件传输协议）
TCP|UDP Hypertext Transfer Protocol（HTTP，超文本传输协议）
TCP     Post Office Protocol3（POP3，邮局协议版本3）
TCP     Network News Transfer Protocol（NNTP，网络新闻传输协议）
UDP     Network Time Protocol（NTP，网络时间协议）
TCP|UDP Microsoft RPC
TCP|UDP NetBIOS Name Service（NetBIOS名称服务）
TCP|UDP NetBIOS Datagram Service（NetBIOS数据流服务）
TCP|UDP NetBIOS Session Service（NetBIOS会话服务）
TCP|UDP Interent Message Access Protocol（IMAP，Internet邮件访问协议）
TCP|UDP Simple Network Management Protocol（SNMP，简单网络管理协议）
TCP|UDP Simple Network Management Protocol Trap（SNMP陷阱）
TCP|UDP Lightweight Directory Access Protocol（LDAP，轻量目录访问协议）
TCP|UDP Hypertext Transfer Protocol over TLS/SSL（HTTPS，HTTP的安全版）
TCP     Server Message Block（SMB，服务信息块）
TCP|UDP Lightweight Directory Access Protocol over TLS/SSL（LDAPS）
TCP     Remote File Synchronization Protocol（rsync，远程文件同步协议）
TCP     Interent Message Access Protocol over TLS/SSL（IMAPS）
TCP     Post Office Protocol3 over TLS/SSL（POP3S）
TCP     Microsoft SQL Server Database
TCP     Oracle数据库
TCP     MySQL数据库
TCP     Microsoft Terminal Server/Remote Desktop Protocol（RDP）
TCP     Virtual Network Computing web interface（VNC，虚拟网络计算机web界面）
TCP     Virtual Network Computing Remote desktop（VNC，虚拟网络计算机远程界面）
```

複製

### nmap端口掃描原理

实施TCP连接扫描　‘-sT’表示实施TCP连接扫描；‘-p-’表示扫描所有端口；‘-PN’表示不进行Ping扫描
TCP SYN扫描（半开放扫描）　该扫描方式一般不留下主机记录；‘-s’表示nmap运行哪种类型扫描；‘-S’表示执行TCP SYN扫描
TCP窗口扫描（和其他的不一样；开：返回RST包；关：不返回包）　　这种扫描方式可能有的系统不支持会报错；‘-sW’表示实施TCP窗口扫描
TCP Maimon扫描（和隐蔽扫描方式一样）　　‘-sM’表示使用TCP Maimon扫描
TCP ACK扫描（和其他的不一样；开：返回TCP RST包；关：不返回包）　‘-sA’表示实施TCP ACK扫描
自定义TCP扫描　　‘--scanflags’可指定任意TCP标志位，也可以设置TCP扫描类型；例：--scanflags SYNURG[目标]（表示设置SYN和URG的标志位）
IP协议扫描　　‘-sO’表示使用IP协议扫描；

隐蔽扫描方式：（可躲避包过滤和可检测进入限制端口的SYN包）
1.TCP FIN扫描
2.TCP Xmas Tree（树）扫描（FIN、PSH、URG的标记置为打开）
3.TCP Null（空）扫描（与树扫描相反没有任何标记）

指定扫描端口：目标的UDP端口53和111，TCP端口21-25和80进行扫描　‘-sU’在既扫描UDP又扫描TCP时使用；‘-p’用来指定扫描端口；‘-sS’表示使用TCP SYN扫描
快速扫描：只扫描100多个端口，速度比较快
不按顺序随机扫描

实施UDP端口扫描　‘-sU’表示UDP端口扫描

複製

## 三.指紋識別

**識別操作系統指令**

1.nmap -O[目标]
识别目标操作系统

2.nmap -O --osscan-guess或--fuzzy[目标]
推测操作系统

3.nmap -O/-A --osscan-limit[目标]
指定识别某个目标主机的操作系统（条件：目标上必须有一个开和一个关的TCP端口）

複製

**識別防火牆指令**

1.nmap -sA[目标]
对目标实施ACK扫描（确定防火墙是否开启和关闭）

2.nmap -sS[目标]
对目标实施SYN扫描（确定防火墙是否开启和关闭）

複製

## 四.防火牆和IDS規避

**規避掃描指令**

**（1）分片（分片后防火牆和IDS檢測到的可能性下降）**

1.nmap -f[目标]
将包分片成每个小包，小包的字节上限为8，如：一个20字节包分成三个包，两个8字节和一个4字节

2.nmap --send-eth[目标]
避开IP层而直接发送原始的以太网帧
nmap -mtu[number][目标]
自定义偏移量大小，偏移量‘number’必须是8的倍数
例：nmap -f 192.168.1.103 对目标192.168.1.103实施分片扫描
nmap -mtu 16 192.168.1.103 对目标192.168.1.103实施设置偏移量为16的分片扫描

複製

**（2）IP誘騙（誘餌主機必須在工作狀態，否則造成拒絕服務攻擊，誘餌適用PING掃描和-O，不適用版本檢測或TCP掃描）**

nmap -D[decoy1，decoy2...|RND:number][目标]
‘-D’表示指定一个或多个诱饵的IP地址；‘RND’表示随机生成几个地址作为诱饵；
例：nmap -D RND:10 192.168.1.102 随机生成10个地址作为诱饵对目标192.168.1.102进行扫描
nmap -D 192.168.1.103，192.168.1.109，ME 192.168.1.102 指定103和109为诱饵实施对目标192.168.1.102的扫描，ME代表可以收到指定

複製

**（3）IP偽裝(指通過任何一個地址，對目標主機實施掃描)**

nmap -e[接口] -S[IP_Address] -Pn[目标]
‘-e’表示用来指定发送数据包的网络接口；‘-S’用来指定伪装的IP地址；‘-Pn’用来表示不进行PING扫描
例：nmap -e eth0 -S 192.168.1.103 -Pn 192.168.1.102 以192.178.1.103为伪装地址对目标192.168.1.102的eth0接口进行发送包，从事实现非Ping扫描

複製

**（4）指定源端口(目標機上的開放端口被指定為源端口)**

nmap --source-port[端口]或-g[端口][目标]
‘--source-port’和‘-g’选项都是用来指定发送数据包的源端口
例：nmap -g 22 -O 192.168.1.103 指定22号端口为源端口对目标192.168.1.103进行操作系统识别

複製

**（5）掃描延時（延時可降低防火牆審查強度，實現規避）**

nmap --scan-delay[time][目标]
‘time’代表延时的时间 例：nmap --scan-delay 5s scanme.insecure.org
对目标scanme.insecure.org做到延时5秒钟的扫描

複製

**其他規避方法**

1.指定发送包的长度（在原报文上附加随机数据，使处理变慢，而规避防火墙和IDS）
nmap --data-length[number][目标] ‘number’指的是指定的附加的包长度，单位为字节
例：nmap --data-length 25 192.168.1.102 向目标192.168.1.102发送附加25个字节大小的包

2.伪装MAC地址（指定伪装的MAC地址进行扫描）
nmap --spoof-mac [mac address/vendor/0 name][目标] ‘--spoof-mac’指用来指定伪装的MAC地址，其可选用的参数包括0（随机生成一个MAC地址），MAC Address（手动生成一个MAC地址）和Vendor Name（厂商生成一个MAC地址）
例：nmap -sT -PN --spoof-mac 0 192.168.1.1 随机生成一个MAC地址，对目标192.168.1.1实施TCP扫描

3.指定TTL（用来指定IP包被路由器丢弃之前允许通过的最大网段数量）
nmap --ttl[val][目标] ‘val’表示指定的TTL值，TTL值的范围为0~255
例：nmap --ttl 20 scanme.insecure.org 通过指定的TTL值为20，扫描目标主机scanme.insecure.org

4.使用错误校验和（错误校验和可以使比较差的系统产生响应）
nmap --badsum[目标] ‘--badsum’代表使用错误校验和指令
例：nmap --badsum 192.168.1.103 使用错误校验和扫描目标192.168.1.103

複製

## 五.nmap擴展

**使用NES腳本實施掃描**

nmap --script[script.nse][目标]
‘script.nse’指用来指定扫描的脚本，可以同时指定多个脚本，或者指定脚本种类实施扫描。每个脚本间用逗号分隔
例：nmap --script vuln 102.168.1.103 用nes对目标192.168.1.103中存在的漏洞进行扫描

複製

**服務枚舉工具Amap**

nmap -bq 192.168.41.13650-100 指定端口50-100之间，测试目标192.168.41.136上正在运行的应用程序

複製

---

# 進階

# 一.網絡基礎服務：

## DHCP類服務類（動態主機配置協議）

**DHCP默認端口：67**

1.广播DHCP请求包（向局域网中所有主机发送广播包）
nmap --script broadcast-dhcp-discover.nse
使用broadcast-dhcp-discover脚本向局域网中发送DHCP Request请求包

2.DHCP发现
nmap -sU -p 67 --script=dhcp-discover 192.168.1.1
发送DHCPINFORM请求到路由器的UDP端口67，获取所有本地配置参数

3.IGMP协议发现 （IGMP：组管理协议）

```
nmap --script broadcast-igmp-discovery
```

扫描局域网中的IGMP协议

```
nmap --script broadcast-igmp-discovery --script-args 'broadcast-igmp-discovery.version=all'
```

指定所有协议发包（使用了IGMPv1版本发送数据包）

複製

### DNS服務類（域名解析協議）

#### DNS默認端口：53

1.获取DNS信息（使用dns-nsid脚本发送ID请求） （DNS：域名解析）

```
nmap -sSU -p 53 --script dns-nsid 192.168.1.104
```

获取192.168.1.104主机RHEL6.4上的DNS信息（-sSU表示进行UDP和TCP SYN扫描）

2.DNS服务发现协议（使用broadcast-dns-service-discovery脚本发送DNS-SD广播包）

```
nmap --script=broadcast-dns-service-discovery
```

使用broadcast-dns-service-discovery脚本发送DNS-SD广播包获取服务列表

3.探测主机是否允许DNS递归查询（使用dns-recursion脚本查询递归情况）

```
nmap -sU -p 53 --script=dns-recursion 192.168.1.104
```

探测目标192.168.1.104主机RHEL6.4是否允许DNS递归查询（recursion）

4.枚举DNS服务器的主机名（使用dns-brute脚本枚举DNS服务器主机名）

```
nmap --script dns-brute www.baidu.com
```

枚举DNS服务器www.baidu.com的主机名

5.DNS缓存探测（使用dns-cache-snoop脚本探测DNS缓存）

```
nmap -sU -p 53 --script=dns-cache-snoop.nse 192.168.1.104
```

探测目标192.168.1.104主机RHEL6.4上的DNS缓存条目

6.探测主机是否支持黑名单列表（使用dns-blacklist脚本查看支持黑名单列表）

```
nmap -sn --script dns-blacklist 192.168.1.104
```

探测目标192.168.1.104是否支持防止DNS反垃圾和打开proxy黑名单列表

複製

## 二.WEB服務

### HTTP服務類（超文本傳輸協議）

#### HTTP服務默認端口：80

1寻找HTTP服务

```
nmap 192.168.1.102
```

查看目标192.168.1.102是否开启了HTTP服务

2.识别HTTP版本

```
nmap -sV -p 80 192.168.1.102
```

识别目标主机192.168.1.102的HTTP服务版本

3.基本认证信息（使用http-auth脚本查看认证信息）

```
nmap --script http-auth 192.168.1.1
```

获取路路由器的认证信息

4.默认账户（使用http-default-accounts脚本检查web服务是否允许默认账户登录）

```
nmap --script http-default-accounts -p 8180 192.168.1.106
```

扫描目标主机（Metasploit2）上的web程序是否允许默认账户登录

5.检查是否存在风险的方法（使用http-methods脚本查看服务器可能存在风险的方法）

```
nmap --script http-methods 192.168.1.102
```

扫描目标主机192.168.1.102的RHEL6.4上的HTTP是否存在有风险的方法

6.探测访问一个网页的时间

```
nmap --script http-chrono -p 80 192.168.1.106
```

探测访问目标主机RHEL6.4上Apache服务的时间

7.提取HTTP注释信息（http-comments-displayer脚本从HTTP响应中提取HTML注释）

```
nmap -p 80 --script http-comments-displayer.nse 192.168.1.104
```

探测目标192.168.1.104上RHEL6.4上Apache服务的时间

8.从类HTTP服务获取时间（http-date脚本可以从类HTTP服务上获取时间）

```
nmap -p 80 --script http-date 192.168.1.104
```

从目标192.168.1.104上RHEL6.4上的Apache服务获取时间

9.枚举HTTP服务网页目录

```
nmap --script http-enum 192.168.1.104 -p 80
```

枚举目标192.168.1.104上Apache服务的网页目录

10.获取访问网站的错误页（http-errors脚本通过爬行访问http的错误页）

```
nmap --script http-errors 192.168.1.104 -p 80
```

获取目标192.168.1.104的http错误页面

11.获取HTTP头信息（http-headers脚本获取HTTP头信息）

```
nmap -sV --script http-headers 192.168.1.104 -p 80
```

获取目标192.168.1.104的http头信息，其中-sV代表显示服务版本信息

12.获取HTTP的目录结构（http-sitemap-generator脚本获取HTTP目录结构）

```
nmap  --script http-sitemap-generator -p www.baidu.com
```

获取百度网址的目录结构（other-其他；gif-图片；html-html网页；png-图片；css-页面；xml-页面；svg-可缩放向量图形）

13.检测是否启用TRACE方法（http-trace脚本发送HTTP TRACE请求）

```
nmap --script http-trace -d 192.168.1.104 -p 80
```

获取目标192.168.1.104是否开启trace方法；-d表示如果trace开启时会显示文件的头部字段信息

14.探测主机是否允许爬行（http-useragent-tester脚本看是否允许网络爬虫）
（最好先看是否允许爬行，如果不允许，那么获取HTTP头信息及目录结构等将无法实现）

```
nmap -p 80 --script http-useragent-tester.nse 192.168.1.104
```

看目标192.168.1.104是否允许爬行

15.搜索WEB虚拟主机（http-vhosts脚本发送HEAD请求，搜索web虚拟主机）

```
nmap --script http-vhosts www.baidu.com
```

搜索百度的虚拟主机

16.探测web服务是否容易受slowloris DoS攻击（慢攻击slowhttptest的一种方式）

```
nmap --script http-slowloris --max-parallelism 400 192.168.1.104
```

探测目标192.168.1.104上RHEL6.4上web是否容易受到slowloris DoS攻击

17.获取路由跟踪信息（targets-traceroute脚本可以获取经过路径）
（newtargets表示在输出结果中显示到目标主机经过的跳数）

```
nmap --script targets-traceroute --script-args newtargets --traceroute
192.168.1.104 -p 80                                    获取目标上的80端口的路由跟踪信息
```

18.路由跟踪位置（traceroute-geolocation脚本列举每一跳的地址位置）

```
nmap --traceroute --script traceroute-geolocation www.baidu.com
```

探测百度服务器的路由跟踪位置信息

複製

## AJP服務（Apache JServ Protocol定向包協議）

**AJP服務默認端口：8009**

1.获取AJP服务的头部信息

```
nmap -sV --script=ajp-headers -p 8009 192.168.1.106
```

获取主机Metasploitable2上AJP服务的头部信息

2.在AJP服务上请求连接

```
nmap -sV --script=ajp-request -p 8009 192.168.1.106
```

向主机的Metasploitable2上AJP服务请求一个URL

複製

### SSL/TLS協議(中間人劫持/ARP劫持)內網（SSL：安全套接層TLS：傳輸層安全）

#### ssl服務的默認端口是：443

1.枚举SSL秘钥

```
nmap --script ssl-enum-ciphers www.baidu.com -p 443
```

枚举百度服务器支持的SSL协议秘钥算法

2.获取SSL证书

```
nmap --script ssl-cert，ssl-google-cert-catalog -p 443 www.baidu.com
```

通过ssl-enum-ciphers脚本查询google的证书目录，查到百度的SSL证书

複製

## 三.遠程服務

### Telnet服務類（遠程登錄服務）

#### telnet服務默認端口：23

1.探测Telnet服务是否支持加密（telnet-encryption脚本探测是否加密）

```
nmap -p 23 --script telnet-encryption 192.168.104
```

探测目标的RHEL6.4上Telnet服务是否支持加密

2.破解Telnet服务密码(telnet-brute脚本破解密码)

```
nmap -p 23 --script telnet-brute 192.168.104
```

破解目标主机上的Metasploitable2上的Telnet密码

複製

### SSH服務類（安全殼協議）

#### SSH服務默認端口：22

1.查看SSH服务密钥信息（full-完整密钥；bubble-模糊输出；visual-ASCII码；all-详细信息）

```
nmap --script ssh-hostkey --script-args ssh_hostkey=full 192.168.1.104 -p 22
```

查看目标主机RHEL6.4上SSH服务的完整密钥信息

```
nmap --script ssh-hostkey --script-args ssh_hostkey='visual bubble' 192.168.1.104 -p 22
```

以visual和bubble格式输出目标上SSH服务的密钥信息

2.查看SSH2支持的算法（ssh2-enum-alogs脚本查看ssh2服务）

```
nmap --script ssh2-enum-algos 192.168.1.104 -p 22
```

查看目标主机RHEL6.4,SSH2协议支持的算法

複製

### VNC服務（VNC：虛擬網絡計算機；vnc-info腳本查看VNC信息）

#### VNC服務默認端口：5900

1.查看目标metasploitable2中的VNC服务的详细信息

```
nmap --script vnc-info -p 5900 192.168.1.103
```

複製

## 四.數據庫服務

## MySQL數據庫服務類

### MySQL服務默認端口：3306

1.检查MySQL空密码（mysql-empty-password脚本检查MySQL是否有空密码）如果存在空密码，任何人都可以登录
nmap --script mysql-empty-password 192.168.1.106
检查目标中mysql服务是否允许空密码访问

2.获取MySQL密码散列（mysql-dump-hashes脚本获取MySQL的Hash）
nmap -p 3306 192.168.1.103 --script mysql-dump-hashes --script-args='username=root，password=123456'
获取目标中MySQL用户的密码散列（hash值）

3.查询MySQL数据库信息（mysql-query脚本查询mysql信息,其实就是利用数据库）
nmap -p 3306 --script mysql-query --script-args='query="select host,user from mysql.user",username=root,password=123456' 192.168.1.103
查询数据库user表中的host，user字段值

4.查询MySQL数据库中的用户（mysql-users脚本查询MySQL的用户）
nmap -sV -p 3306 --script=mysql-users --script-args=mysqluser=root 192.168.1.104

5.破解MySQL用户密码（mysql-brute脚本破解MySQL用户密码）
nmap --script mysql-brute -p 3306 192.168.1.104
破解主机RHEL6.4上MYSQL数据库的密码

6.枚举MySQL用户信息（mysql-enum脚本枚举MySQL用户信息）
nmap --script=mysql-enum -p 3306 192.168.1.104
枚举目标主机RHEL6.4上的Mysql用户信息

7.获取MySQL数据库信息（mysql-info脚本可以连接MySQL）
nmap --script mysql-info 192.168.1.104 -p 3306
探测目标主机上数据库的信息信息

複製

## MSSQL Server（sqlserver）數據庫服務類

### MSSQL Server服務默認端口：1433

1.破解MS SQL Server数据库用户名密码（ms-sql-brute脚本破解MS SQL Server用户名密码）
nmap -p 1433 --script ms-mysql-brute --script-args userdb=/root/user.txt,passdb=/root/pass.txt 192.168.1.108
破解windows7上MS SQL Server数据库用户名密码

2.获取MS SQL Server数据库信息（ms-sql-info脚本破解MS SQL Server数据库信息）
nmap -p 1433 --script ms-mysql-info --script-args mssql.instance-port=1433 192.168.1.108
破解windows7上MS SQL Server数据库服务信息

3.查询MS SQL Server数据库实例（ms-sql-config脚本查询MS SQL Server数据库实例）
nmap -p 1433 --script ms-sql-config --script-args mssql.username=sa,mssql.password=123456 192.168.1.108
查询windows7上MS SQL Server数据库实例信息

4.查询MS SQL Server数据库条目（ms-sql-query脚本查询MS SQL Server数据库条目，其实就是利用数据库）
nmap -p 1433 --script ms-mysql-query --script-args mssql.username=sa，mssql.password=123456,ms-sql-query.query="SELECT*FROM master..syslogins" 192.168.1.108
查询目标SQL Server中master数据库中syslogins表信息

複製

### LDAP數據庫服務（LDAP:輕量目錄訪問協議）

#### LDAP服务默认端口：389

1.获取LDAP根DSE条目(ldap-rootdse脚本获取LDAP根目录DSE条目)
nmap -p 389 --script ldap-rootdse 192.168.1.103
获取目标主机LDAP服务的根DSE条目

2.LDAP查询（ldap-search脚本查询LDAP）
nmap -p 389 --script ldap-search 192.168.1.103
查询主机上LDAP服务中的条目

CN：用户名 OU：组织单元 DC：组织

复制

## 五.其他服务

### FTP服务类（文本传输协议）

#### FTP服务默认端口21

1.寻找FTP服务
nmap 192.168.1.102
扫描目标主机上是否开启了FTP服务
2.识别FTP服务版本
nmap -sV -p 21 192.168.1.102
扫描目标主机上FTP服务版本
3.检查FTP匿名登录（ftp-anon脚本来检查是否允许FTP匿名登录）
nmap --script ftp-anon 192.168.1.102
检查目标主机上是否允许ftp匿名登录

复制

### SMB服务类（信息服务块，文件共享和打印机功能）

#### SMB服务默认端口445，137（UDP端口）,139（TCP端口）

1.SMB安全信息模式（smb-security-mode脚本获取SMB安全信息模式）
nmap --script smb-security-mode.nse -p 445 192.168.1.108
扫描目标主机上SMB服务的安全模式信息

2.是否启用SMBv2协议（smbv2-enabled脚本检测是否支持SMBv2协议）
nmap --script smbv2-enabled.nse -p 445 192.168.1.108
检测目标主机windows7上是否支持SMBv2协议

3.获取windows信息（smb-mbenum脚本可以用户获取管理类信息）
nmap -p 445 --script smb-mbenum 192.168.1.109
获取windowsXP上的管理类信息

4.获取共享文件（smb-enum-shares脚本获取SMB共享文件）
nmap --script smb-enum-shares.nse -p 445 192.168.1.109
获取目标上的共享文件及文件的详细信息

5.枚举系统域名（smb-enum-domains脚本枚举系统域名）
nmap --script smb-enum-domains -p 445 192.168.1.109
枚举目标中的域名

6.检查是否有SMB漏洞（smb-vuln-cve2009-3130脚本检查是否存在cve2009-3130漏洞）
139端口是NetBIOS提供的Samba服务，用于共享
nmap --script=smb-vuln-cve2009-3130.nse -p 139 192.168.1.102
检查目标是否存在cve2009-3130漏洞

7.枚举Samba用户（smb-enum-users脚本检查Samba用户）

```
nmap --script smb-enum-users 192.168.1.102
```

枚举目标主机上所有的Samba用户

8.SMB服务密码破解（smb-brute脚本破解SMB服务密码）

```
nmap --script smb-brute.nse -p 445 192.168.1.102
```

破解目标主机Metasploitable上SMB服务的密码

复制

## SMTP服务（简单邮件传输协议）

### SMTP服务默认端口25

1.枚举邮件用户（smtp-enum-users脚本用来枚举远程系统的所有用户）

```
nmap --script smtp-enum-users.nse -p 25 192.168.1.104
```

枚举目标主机上的邮件服务用户

2.收集邮件地址（http-grep脚本可以进行网络爬虫，收集邮件地址）

```
nmap --script=http-grep -p 80 192.168.1.103
```

通过HTTP80端口对目标实行网络爬虫收集邮件地址

3.收集目标主机支持的SMTP命令（smtp-commands脚本可以收集目标所支持的SMTP命令）

```
nmap --script smtp-commands.nse -p T:25 192.168.1.103
```

收集目标主机支持的SMTP命令

复制

## SNMP服务（简单网络管理协议）

### SNMP服务默认端口161

1.枚举网络接口（snmp-interfaces脚本通过SNMP协议枚举网络接口）

```
nmap -sU -p 161 --script=snmp-interfaces 192.168.1.108
```

枚举目标主机上的网络接口信息

2.获取网络连接状态（snmp-netstat脚本查看网络连接状态）

```
nmap -sU -p 161 --script=snmp-netstat 192.168.1.108
```

获取windows7中网络连接状态

3.枚举目标主机程序的进程（snmp-processes查看主机程序进程）

```
nmap -sU -p 161 --script=snmp-processes 192.168.1.108
```

枚举windows7上所有运行程序的进程号

4.提取系统信息（snmp-sysdescr脚本提取系统信息）

```
nmap -sU -p 161 --script=snmp-sysdescr 192.168.1.108
```

提取系统信息

5.枚举Windows服务（snmp-win32-services脚本枚举Windows服务）

```
nmap -sU -p 161 --script=snmp-win32-services 192.168.1.108
```

枚举Windows7系统上的服务

6.枚举Windows用户（snmp-win32-users脚本枚举Windows用户）

```
nmap -sU -p 161 --script=snmp-win32-users 192.168.1.108
```

枚举Windows7系统上的用户

7.枚举Windows共享文件（snmp-win32-shares脚本枚举共享Windows文件）

```
nmap -sU -p 161 --script=snmp-win32-shares 192.168.1.108
```

枚举Windows7系统上的共享文件

8.枚举Windows安装的软件（snmp-win32-software脚本枚举安装的软件）

```
nmap -sU -p 161 --script=snmp-win32-software 192.168.1.108
```

枚举Windows7系统上的软件

9.SNMP服务密码破解（snmp-brute脚本破解SNMP服务密码，SNMP默认密码public）

```
nmap -sU --script=snmp-brute 192.168.1.108
```

破解系统Windows7上的SNMP服务密码

复制

## NetBIOS服务（为应用程序编程接口（API）提供请求低级服务的统一命令集）

### NetBIOS服务默认端口137

1.获取NetBIOS服务名称和MAC地址（nbstat脚本获取目标NetBIOS名称和MAC地址）

```
nmap -sU --script nbstat -p 137 192.168.1.108
```

获取目标主机NetBIOS名称和MAC地址

2.浏览广播包发现主机（broadcast-netbios-master-browser脚本发现局域网中主机）

```
nmap --script=broadcast-netbios-master-browser
```

发现局域网中的主机

复制

## NTP服务信息（网络时间协议）

### NTP服务默认端口123

1.从NTP服务器上获取基本信息（ntp-info脚本）

```
nmap -sU -p 123 --script ntp-info 192.168.1.108
```

对目标实施NTP服务基本信息扫描

复制

## RPC服务详细信息（远程过程调用协议；通过网络向远程计算机发请求的服务）

### RPC服务默认端口111

1.扫描目标的RPC服务信息（rpcinfo脚本）

```
nmap -p 111 --script rpcinfo 192.168.1.103
```

扫描目标的RPC服务基本情况
获取所有开放服务（banner）

2.获取所有目标主机上开放的服务信息（banner脚本）

```
nmap -sV --script=banner 192.168.1.108
```

获取目标上所有开放服务信息

复制

## DICT服务信息（词典网络协议）

### DICT服务默认端口2628

1.查看一台词典服务信息（dict-info脚本查看词典服务信息）

```
nmap -p 2628 --script dict-info 216.18.20.172
```

查看美国一台词典方服务的信息

复制

## IRC服务信息（网络聊天室）

### IRC服务默认端口：6667

1.获取目标IRC服务信息（irc-info脚本查看IRC服务）
获取目标主机上的IRC服务信息

```
nmap --script irc-info 192.168.1.106 -p 6667
```

复制

# 六.OS操作系统

## os操作系统发现：通过SMB协议

**SMB服务默认端口：445**

1.操作系统发现（smb-os-discovery.nse脚本发现操作系统）
nmap --script smb-os-discovery.nse -p 445 192.168.1.108 发现目标操作系统

复制

## MTU发现（最大传输单元MTU）

1.MTU发现（path-mtu脚本可以方发现目标最大传输单元值）
nmap --script path-mtu 192.168.1.104 发现目标最大传输单元是多少

复制

## 探测防火墙规则

1.探测防火墙的规则（firewalk脚本可以探测防火墙的规则）
nmap --script=firewalk --traceroute 192.168.1.104 探测目标主机上的防火墙规则

复制

## 唤醒远程主机

1.唤醒远程主机（broadcast-wake-on-lan脚本唤醒远程主机）
nmap --script broadcast-wake-on-lan --script-args broadcast-wake-on-lan.MAC='00:12:34:56:78:9A' 唤醒MAC地址为00:12:34:56:78:9A的主机

复制

## WSDD服务协议

**（web服务动态协议，WS-Discovery）**

1.WSDD服务协议（broadcast-wsdd-discover脚本定位web服务）
nmap --script broadcast-wsdd-discover 获取局域网内支持web服务动态协议的设备

复制

## 嗅探目标

1.嗅探目标，扫描局域网中活动的主机（targets-sniffer脚本嗅探目标）
nmap -sL --script=targets-sniffer --script-args=newtargets，targets-sniffer.timeout=5s,targets-sniffer.iface=eth0 指定扫描接口eth0，扫描时间5s，对局域网内活动的主句进行扫描

复制

## 监听广播包

1.监听局域网中通过接口eth0的所有广播包，并对收到的包进行解码（broadcast-listener脚本监听广播包）
nmap --script broadcast-listener -e eth0 监听局域网中通过接口eth0的所有广播包，并对收到的包进行解码

复制

# 七.nmap的MISC杂项使用及配套工具

## 探测TP-Link路由器是否存在漏洞

1.探测型号为WR1041N的TP-Link无线路由器是否存在漏洞(http-tplink-dir-traversal脚本)
nmap -p 80 --script http-tplink-dir-traversal 192.168.1.1

2.利用路由器中的漏洞，读取配置文件/etc/topology.conf中的内容

```
nmap -p 80 --script http-tplink-dir-traversal --script-args
rfile=/etc/topology.conf 192.168.1.1
```

复制

## 反向索引

### （一种索引结构）

1.利用反向索引扫描目标上运行的服务（reverse-index脚本反向索引）

```
nmap --script reverse-index 192.168.1.104
```

复制

## 单元测试

1.对所有NSE库进行单元测试（unittest脚本可对所有NSE库进行单元测试，unittest.run代表进行测试）

```
nmap --script unittest --script-args unittest.run
```

复制

## VMWare认证进程破解

### VMWare-authd程序端口：902

1.破解windows7上VMWare-authd程序的认证信息

```
nmap -p 902 --script vmauthd-brute 192.168.1.100
```

复制

## 探测目标是否启用了IP转发

1.探测目标是否开启了IP转发（ip-forwarding脚本）

```
nmap -sn --script ip-forwarding --script-args='target=mail.benet.com'192.168.1.104
```

复制

## 获取ASN列表

### 描述一种对数据进行表示，编码，传输和解码的数据格式

1.获取ASN列表（targets-asn脚本获取ASN列表）

```
nmap --script targets-asn --script targets-asn.asn=32
```

复制

## 枚举EAP提供的认证方法

### EAP无线网络或点对点连接认证框架

1.枚举EAP提供的认证方法（eap-info脚本用于枚举eap认证）

```
nmap -e wlan2 --script eap-info
```

复制

## 枚举服务

### DNS枚举（域名解析）

1.DNSenum
通过谷歌和字典查询域名

```
dnsenum --enum benet.com
```

使用dnsenum工具检查DNS枚举 '--threads[number]'：设置用户同时运行多个进程数
'-r'：允许用户启用递归查询
'-d'：允许用户设置WHOIS请求之间时间延迟数
'-o'：允许用户指定输出位置
'-w'：允许用户启用WHOIS请求

2.fierce
对子域名进行扫描和收集信息的 fierce可以获取一个目标主机上所有IP地址和主机信息

```
fierce -dns baidu.com
检查百度的IP地址和主机信息
```

复制

### SNMP枚举（简单网络管理协议）

```
1.Snmpwalk
使用GETNEXT请求，查询OID数信息，显示给用户
snmpwalk -c public[目标] -v 2c   使用snmpwalk命令测试主机

2.snmpcheck
将结果以可读的方式输出
snmpcheck [目标] 使用snmpcheck获取主机信息
```

复制

### SMTP枚举（简单邮件传输协议）

```
1.smtp-user-enum
针对SMTP协议的25号端口，探测存在的邮箱用户
smtp-user-enum -M VRFY -U /tmp/users.txt -t 192.168.41.138
扫描192.168.41.138主机的详细信息
```

复制

## 测试网络范围

```
测试网络范围
0            最大网络数量           IP地址范围                最大主机数
A类地址   126（2^7-2）      0.0.0.0-127.255.255.255    16777214
B类地址   16384(2^14)      128.0.0.0-191.255.255.255       65534
C类地址   2097152(2^21)    192.0.0.0-223.255.255.255       254
D类地址
E类地址
```

复制

### 域名查询工具DMitry

```
用来查询IP或域名WHOIS信息
dmitry -wnpb rzchina.net
用DMitry收集rzchina.net的信息
netmask -s rzchina.net
使用netmask将域名转化为标准子网掩码格式
```

复制

### 跟踪路由工具Scapy

```
包嗅探，网扫，网发现，发包，包应答反馈

1.启动scapy工具
ans，unans=sr（IP（dst=“www.rzchina.net/30”，ttl=（1,6））/TCP（））
2.使用sr（）函数实现发送和接收数据包
ans.make_table(lambda(s,r):(s.dst,s.ttl,r.src))
3.以表的形式查看数据包数据包发送情况
res，unans=traceroute(["www.google.com","www.kali.org","www.rzchina.net"],dport=
[80,443],maxttl=20,retry=2)
4.使用scapy查看TCP路由跟踪信息
res，graph（）
5.使用res.graph（）函数以图的形式显示结果
res，graph（target=“>/tmp/graph.svg”）
6.将显示图保存在/tmp/graph.svg目录中
exit（）或者Crtl+D
7.退出scapy程序
```

复制

## 分析密码

**ettercap：制造一个欺骗的包，绑定监听数据到一个本地端口等**

```
locate etter.conf
1.查找到Ettercap配置文件的保存位置

vi /etc/ettercap/etter.conf
2.使用Vim编辑器编辑etter.conf配置文件，将ec_uid和ec_gid配置项修改为0，并将Linux部分
IPTABLES行的注释去掉
ettercap -G

3.启动Ettercap

4.使用中间人攻击方式，收集目标上的各种重要信息
```

复制

**metasploit（msf）： search_email_collector模塊可以通過Google，Bing，Yahoo三個網站收集郵箱信息，幫助破解**

```
msfconsole
1.打开msfconsole
search email_collector
2.查询search_email_collector模块
use auxiliary/gather/search_email_collector
3.使用辅助模块search_email_collector
show options
4.查看search_email_collector模块下的有效选项
set DOMAIN gmail.com
5.gmail.com是需要检索的邮箱地址，现在是配置了DOMAIN选项
gmail.com
set outfile /root/email.txt
6.设置OUTFILE选项，将搜索到的邮件地址保存在email.txt文件 中
/root/email.txt
run
7.实施渗透攻击（会显示目标邮箱所有邮件发送记录的地址，将信息保存在email.txt文件中）
备注：    可能会出现报错，因为是运用国外网站收集信息，可以挂VPN来实现
```

複製

**相關文章**


央媒談“文盲演員”引發飯圈甩鍋大戰

央媒談“文盲演員”引發飯圈甩鍋大戰


野生大熊貓深夜遛達鏡頭前呆萌打卡

野生大熊貓深夜遛達鏡頭前呆萌打卡


張萌談演員到底需不需要有文化

張萌談演員到底需不需要有文化


情人節多地迎領證高峰

情人節多地迎領證高峰


婚房爛尾10年業主住進毛坯房

婚房爛尾10年業主住進毛坯房


多地首套房貸利率降至4%以下為什麼急於提前還貸

多地首套房貸利率降至4%以下為什麼急於提前還貸