域内扫描

主机探测

NetBIOS

这是一款用于扫描Windows网络上NetBIOS名字信息的程序。该程序对给出范围内的每一个地址发送NetBIOS状态查询，并且以易读的表格列出接收到的信息，对于每个响应的主机，NBTScan列出它的IP地址、NetBIOS计算机名、登录用户名和MAC地址。但只能用于局域网,NBTSCAN可以取到PC的真实IP地址和MAC地址，如果有"ARP攻击"在做怪，可以找到装有ARP攻击的PC的IP/和MAC地址。但只能用于局域网

下载地址`http://www.unixwiz.net/tools/nbtscan.html`

用法：nbtscan.exe + IP

```
C:\>nbtscan.exe 192.168.41.0/24
192.168.41.1    WORKGROUP\DAOER                 SHARING
192.168.41.10   HACK\DC                         SHARING DC
192.168.41.20   HACK\PC-2008                    SHARING
192.168.41.30   HACK\PC-2003                    SHARING
*timeout (normal end of scan)
```

ICMP

除了利用NetBIOS探测内网，还可以利用ICMP协议探测内网。依次对内网中的每个IP地址执行ping命令，可以快速找出内网中所有存活酌主机。在渗透刹试中，可以使用如下命令循环探测整个C段

```
for /L %I in (1,1,254) DO @ping -w 1 -n 1 192.168.1.%I | findstr "TTL="
```

```
C:\>for /L %I in (1,1,254) DO @ping -w 1 -n 1 192.168.41.%I | findstr "TTL="
来自 192.168.41.1 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.41.2 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.41.10 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.41.20 的回复: 字节=32 时间=1ms TTL=128
来自 192.168.41.30 的回复: 字节=32 时间=1ms TTL=128
```

ARP

```
apr -t IP
```

```
C:\>arp.exe -t 192.168.41.0/24
Reply that 00:50:56:C0:00:08 is 192.168.41.1 in 12.029100
Reply that 00:50:56:F4:B3:58 is 192.168.41.2 in 14.693300
Reply that 00:0C:29:58:D6:E0 is 192.168.41.10 in 15.485400
Reply that 00:0C:29:D4:E2:A4 is 192.168.41.20 in 0.225000
Reply that 00:0C:29:7B:EF:B5 is 192.168.41.30 in 15.285200
Reply that 00:50:56:F5:F7:69 is 192.168.41.254 in 1.138500
Reply that 00:0C:29:D4:E2:A4 is 192.168.41.255 in 0.235200
```

端口探测

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
```

```
Scan of 254 IPs started at Thu Mar 31 19:20:14 2022

--------------------------------------------------------------------------------
192.168.41.1
Responds with ICMP unreachable: No
TCP ports: 135 443


--------------------------------------------------------------------------------
192.168.41.10
Responds with ICMP unreachable: No
TCP ports: 135


--------------------------------------------------------------------------------
```

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
```

```
C:\>telnet 192.168.41.10 22
正在连接192.168.41.10...无法打开到主机的连接。 在端口 22: 连接失败
```