https://micropoor.blogspot.com/

## ICMP简介:

它是TCP/IP协议族的一个子协议,用于在IP主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据,但是对于用户数据的传递起着重要的作用。

# nmap扫描:

```
1 root@John:∼# nmap -sP -PI 192.168.1.0/24 -T4
```

```
root@John:~# nmap -sn -PE -T4 192.168.1.0/24

Starting Nmap 7.40 ( https://nmap.org ) at 2017-12-04 06:33 EST
Nmap scan report for 192.168.1.1
Host is up (0.0088s latency).
MAC Address:
Nmap scan report for 192.168.1.100
Host is up (0.028s latency).
MAC Address:
Nmap scan report for 192.168.1.101
Host is up (0.040s latency).
MAC Address:
Nmap scan report for 192.168.1.107
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 1.82 seconds
```

```
1 root@John:~# nmap -sn -PE -T4 192.168.1.0/24
```

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-12-04 07:14 EST
Nmap scan report for 192.168.1.1
Host is up (0.0017s latency).
MAC Address:
Nmap scan report for 192.168.1.100
Host is up (0.030s latency).
MAC Address:
Union of 192.168.1.101
Host is up (0.068s latency).
MAC Address:
Nmap scan report for 192.168.1.101
Host is up (0.068s latency).
MAC Address:
Nmap scan report for 192.168.1.107
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.31 seconds
root@John:~#
```

#### CMD下扫描:

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

```
C:\Users\John>for /L %P in <1,1,254> DO @ping -w 1 -n 1 192.168.1.%P ¦ findstr
TTL="
来自 192.168.1.1 的回复: 字节=32 时间=6ms TTL=64
来自 192.168.1.100 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.101 的回复: 字节=32 时间=144ms TTL=64
```

## powershell扫描:

```
powershell.exe -exec bypass -Command "Import-Module ./Invoke-TSPingSwe ep.ps1

invoke-TSPingSweep -StartAddress 192.168.1.1 -EndAddress 192.168.1.2

invoke-TSPingSweep -StartAddress 192.168.1.1 -EndAddress 192.168.1.1

invoke-TSPingSweep -StartAddress 192.168.1.1

invoke-TSPingSweep -StartAddre
```

```
D:\>powershell.exe -exec bypass -Command "Import-Module ./Invoke-TSPingSweep.ps1; Invoke-TSPingSweep.ps1; Invoke-TSPingSweep.p
```

1 D:\>tcping.exe -n 1 192.168.1.0 80

```
D:\>tcping.exe -n 1 192.168.1.0 80

Probing 192.168.1.0:80/tcp - No response - time=2022.805ms

Ping statistics for 192.168.1.0:80
1 probes sent.
0 successful, 1 failed.

Was unable to connect, cannot provide trip statistics.

D:\>
```

# 附录:

powershell脚本与tcping (来源互联网,后门自查)

链接:https://pan.baidu.com/s/1dEWUBNN 密码:9vge

• Micropoor