专注APT攻击与防御

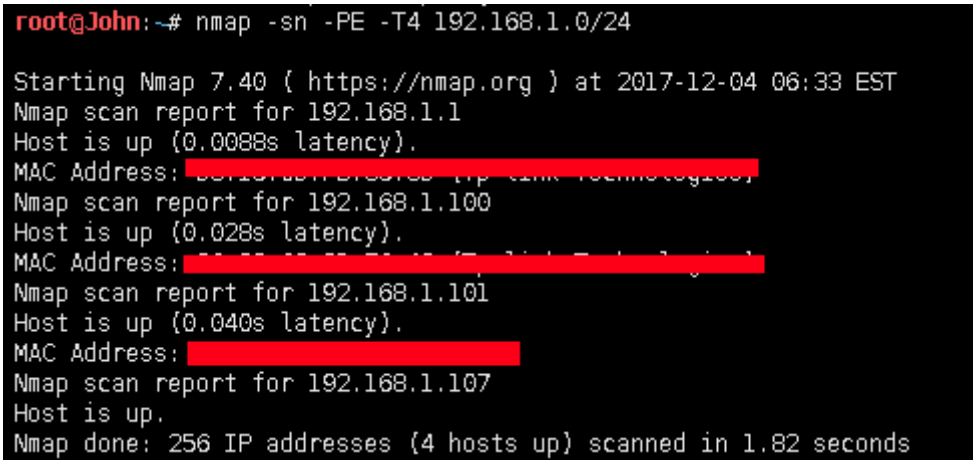
https://micropoor.blogspot.com/

ICMP简介：

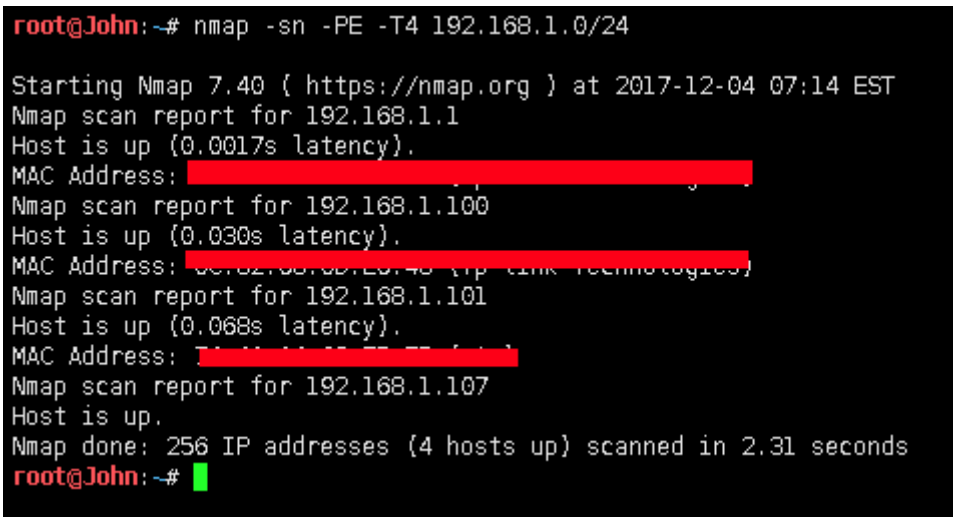
它是TCP/IP协议族的一个子协议，用于在IP主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要的作用。

nmap扫描：

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




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



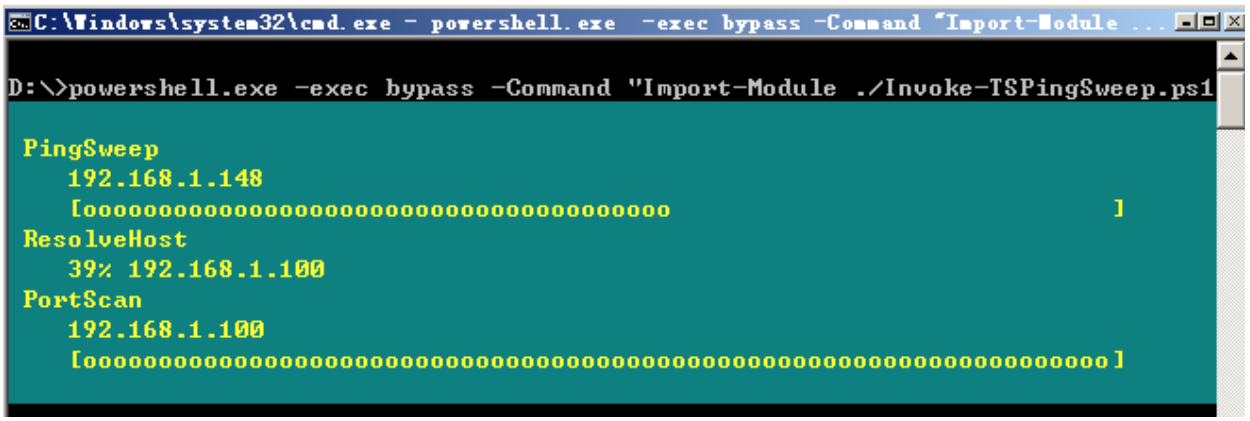
CMD下扫描：

```
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-TSPingSweep.ps1
; Invoke-TSPingSweep -StartAddress 192.168.1.1 -EndAddress 192.168.1.254 -Resolv
eHost -ScanPort -Port 445,135"
```




```
D:\>powershell.exe -exec bypass -Command "Import-Module ./Invoke-TSPingSweep.ps1
; Invoke-TSPingSweep -StartAddress 192.168.1.1 -EndAddress 192.168.1.254 -Resolv
eHost -ScanPort -Port 445,135"

IPAddress                HostName                 Ports
---------                --------                 -----
192.168.1.1              John-PC                  {}
192.168.1.100            John-PC                  {445, 135}
```

```
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