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：

1 root@John:~# nmap ‐sP ‐PI 192.168.1.0/24 ‐T4

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

CMD下扫描：

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

powershell扫描：

1 powershell.exe ‐exec bypass ‐Command "Import‐Module ./Invoke‐TSPingSwe ep.ps1

2 ; Invoke‐TSPingSweep ‐StartAddress 192.168.1.1 ‐EndAddress 192.168.1.2

54 ‐Resolv

3 eHost ‐ScanPort ‐Port 445,135"

1 D:\>tcping.exe ‐n 1 192.168.1.0 80

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