主动信息收集

防知焉 攻知未

PTES渗透测试标准

- 前期交互阶段
- 情报收集阶段
- 威胁建模阶段
- 漏洞分析阶段
- 渗透攻击阶段
- 后渗透攻击阶段
- 渗透测试报告阶段

为什么需要主动信息收集？

- 被动信息收集的结果可能已经过时
- 使用主动信息收集对被动信息收集的结果进行验证

主动信息收集

- 直接与目标系统进行通信
- 无法避免留下访问痕迹
  - 使用受控的第三方电脑进行探测
    - 代理或肉鸡
  - 使用噪声迷惑目标，淹没真实的探测流量

主机发现

- 识别存活的主机
  - 潜在的被攻击目标
- 二、三、四层发现

二层发现

- ARP协议
  - 扫描速度快，扫描结果可靠
  - 不可路由

问题：什么时候会用到二层发现？

二层发现

- Arping命令——arp级别的ping工具
- arping 192.168.80.128
- arping 192.168.80.128 –c 1
- arping 192.168.80.12 –c 3

使用wireshark抓包查看数据流。

二层发现

- Netdiscover
  - 只用于二层发现
  - 支持主动探测和被动探测
- 主动探测
  - netdiscover -i eth0 –r 192.168.80.0/24
- 被动探测
  - 混杂模式：接收所有经过它的数据流，而不论目的地址是否是它
  - netdiscover –p

使用wireshark抓包查看数据流。

三层发现

- IP，ICMP协议
  - 速度比二层发现慢
  - 可路由
  - 容易被边界防火墙过滤

三层发现

- Ping命令——向目标主机发送icmp数据包
  - type8：ping请求
  - type0：ping应答
- ping 192.168.80.128
- ping 192.168.80.128 –c 1

- traceroute Linux系统
- tracert Windows系统

使用wireshark抓包查看数据流。

三层发现

- fping
  - 支持对整个网段进行主机发现

- fping -g 192.168.80.0/24

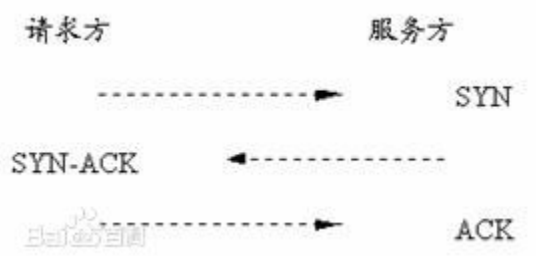
- fping -g 192.168.80.0/24 >> result.txt
- cat result.txt | grep alive

四层发现

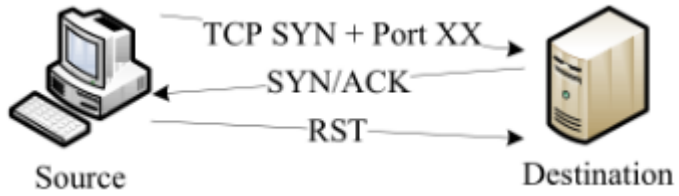
- TCP、UDP协议
  - 可路由
  - 不太可能被防火墙过滤，结果相对可靠
  - 速度慢

四层发现

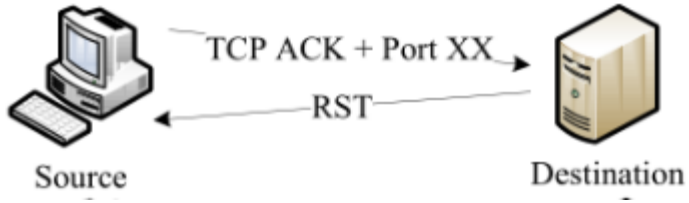
- 三次握手



- SYN Ping扫描，目的端口80
  - –PS参数
  - nmap -sn –PS80 www.baidu.com



- ACK Ping扫描，目的端口80
  - –PA参数
  - nmap -sn -PA www.baidu.com

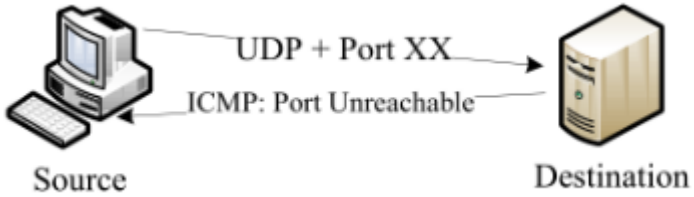


使用wireshark抓包查看数据流。

四层发现

- Nmap
- UDP Ping扫描，目的端口40125
  - -PU参数
  - nmap -sn -PU www.baidu.com

- 测试了一下，大多数设备不会响应...



端口扫描

- 主机发现的下一步是要进行端口扫描
- 端口对应网络服务
- 通过服务的漏洞攻击进入目标主机

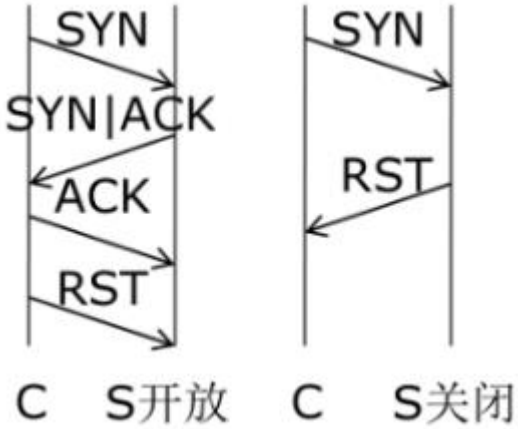
端口扫描

- Nmap所识别的6个端口状态
  - open(开放的)
  - closed(关闭的)
  - filtered(被过滤的)
  - unfiltered(未被过滤的)
  - open|filtered(开放或者被过滤的)
  - closed|filtered(关闭或者被过滤的)

端口扫描

- TCP connect()扫描
  - 调用connect()函数
  - 端口开放：与目标主机建立完整的三次握手
  - 端口关闭：收到RST
- -sT参数
  - 默认扫描常用的1000个端口
  - nmap -sT 192.168.80.201

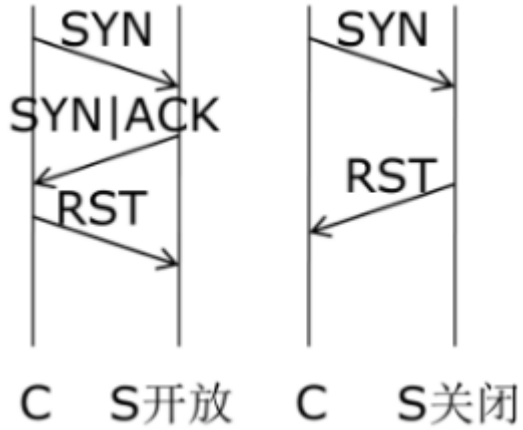
  - nmap -sT -p80 192.168.80.201
  - nmap -sT -p800 192.168.80.201
  - wireshark抓包分析



端口扫描

- TCP SYN扫描(半开扫描)
  - Nmap默认的扫描方式
  - 不建立完整的三次握手，较隐蔽
  - 端口开放：收到SYN/ACK并回复RST
  - 端口关闭：收到RST
- -sS参数
  - 默认扫描常用的1000个端口
  - nmap -sS 192.168.80.201

  - nmap -sS -p80 192.168.80.201
  - nmap -sS -p800 192.168.80.201
  - wireshark抓包分析



端口扫描

- UDP扫描
  - 端口开放：没有回复(UDP是无连接协议)
  - 端口关闭：ICMP port-unreachable
- -sU，UDP扫描
  - 默认扫描常用的1000个端口
  - nmap –sU 192.168.80.201 –p1-100
  - nmap –sU 192.168.80.201 –p53
  - nmap –sU 192.168.80.201 –p800
  - wireshark抓包分析

注意：如果既扫描TCP又扫描UDP，必须指定-sU以及至少一个TCP扫描类型(-sT/-sS)

```
nmap -sT -sU -p T:53,U:53 192.168.80.201
```

服务扫描

- 服务的类型
- 服务的版本
  - 已知的漏洞和弱点

服务扫描

- Nmap
  - -sV参数
  - nmap 192.168.80.201 -p1-100 -sV

操作系统识别

- 操作系统类型
- 操作系统版本
  - 已知的缓冲区溢出、代码执行漏洞

操作系统识别

- 通过TTL值判断操作系统
  - Linux 64 (1-64)
  - Windows 128 (65-128)
  - Unix 255

操作系统识别

- Nmap
  - -O参数
  - nmap –O 192.168.80.201

SNMP扫描

- SNMP(简单网络管理协议)
  - 容易被配置错误，黑客喜欢的攻击目标
  - Security is Not My Problem
  - 代理进程:UDP 161，管理进程:UDP 162
  - community，管理进程和代理进程之间的认证口令，默认为public

- 防护措施
  - 升级SNMPv3

SNMP扫描

- onesixtyone
  - /usr/share/doc/onesixtyone/dict.txt
  - onesixtyone –c dict.txt 192.168.80.132暴力猜解community

- snmpwalk
  - snmpwalk 192.168.80.132 -c admin -v 2c 查询详细信息

SNMP扫描

- Nmap
  - nmap -sU -p161 --script="snmp-brute" 192.168.80.132
  - nmap -sU -p161 --script="snmp-netstat" 192.168.80.132
  - nmap -sU -p161 --script="snmp-win32-services" 192.168.80.132

- -sC参数，根据端口识别的服务,调用默认脚本
  - nmap -sU -sC -p161 192.168.80.132

SMB扫描

- 微软历史上出现安全问题最多的协议

- Nmap
  - nmap -p139,445 --script="smb-vuln-ms08-067" 192.168.80.132
  - nmap -p139,445 --script="smb-vuln-ms17-010" 192.168.80.132

FTP扫描

- FTP匿名登录

- nmap -p21 --script="ftp-anon" 192.168.80.201
- ftp 192.168.80.201

WAF识别

- Web应用防火墙
- wafw00f
  - wafw00f -l 列出支持的waf类型
- nmap

Nmap其它参数

- -D，IP地址欺骗
  - nmap -p21 -D 192.168.80.1,192.168.80.2,192.168.80.3 192.168.80.201
  - nmap -p21 -D RND:10 192.168.80.201
- --spoof-mac，MAC地址欺骗
  - 数字”0”表示随机分配一个mac地址
  - nmap -p21 --spoof-mac 0 192.168.80.201

Nmap其它参数

- --traceroute 路由追踪
  - nmap --traceroute 223.5.5.5
- -iR 随机扫描
  - nmap -iR 200 -p21 --open
- -Pn不检测主机存活，默认目标主机存活
- -n，禁止对目标ip作反向域名解析
- --script-help 脚本使用帮助
- --scan-delay，设置扫描延迟时间
  - nmap 192.168.80.201 --scan-delay=1
- -A，OS识别,版本探测,脚本扫描,traceroute的组合

谢谢大家