

网络安全 – 网络侦查技术

曹越

国家网络安全学院

武汉大学

yue.cao@whu.edu.cn

信息收集

网络扫描

网络监听

口令破解

信息收集

网络扫描

网络监听

口令破解

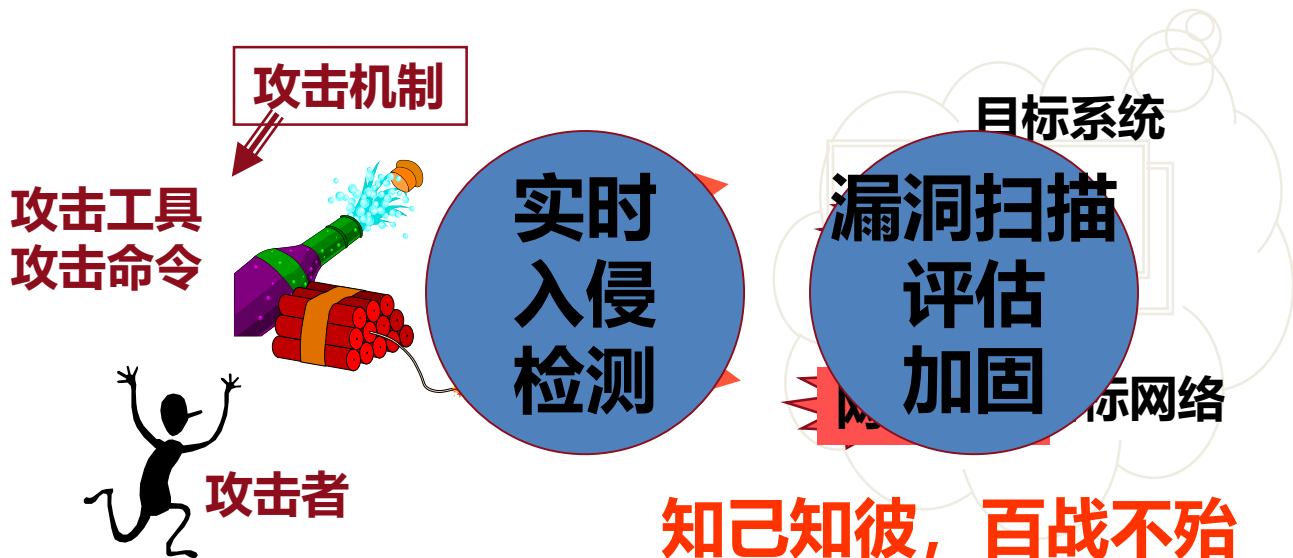
信息收集 – 章节分解

1. 为什么要信息收集
2. 信息收集的过程
3. 信息收集方法

为什么要信息收集

信息收集技术也是一把双刃剑

1. 黑客在攻击之前需要收集信息，才能实施有效的攻击
2. 管理员用信息收集技术来发现系统的弱点



信息收集的过程

信息收集是一个综合过程

- **从一些社会信息入手**
- **找到网络地址范围**
- **找到关键的机器地址**
- **找到开放端口和入口点**
- **找到系统的制造商和版本**
- **.....**

社会信息

DNS域名

- 网络实名
- 网站的网页中

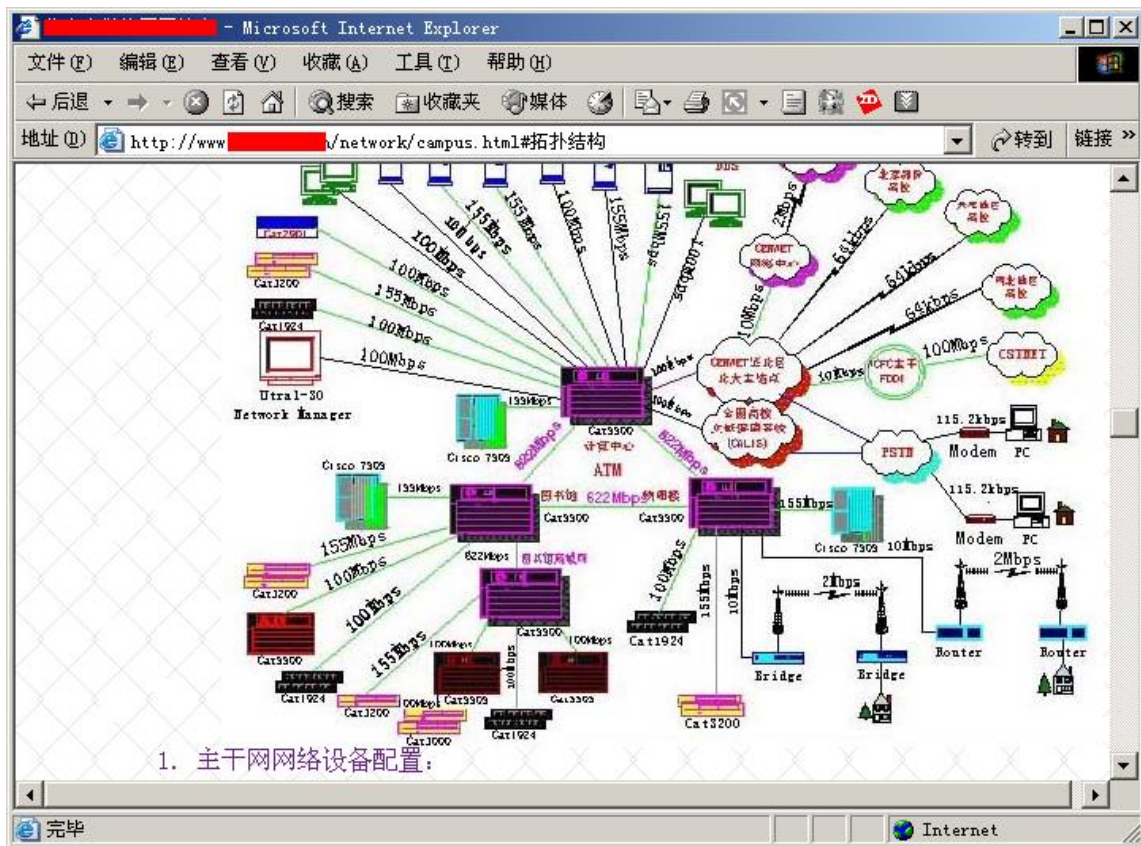
新闻报道

- 例如：XX公司采用XX系统，...

这样的信息可以合法地获取



例：来自网站的公开信息



非网络技术的探查手段

社会工程

- 通过一些公开的信息，获取支持人员的信任
- 假冒网管人员，骗取员工的信任（安装木马、修改口令等）

查电话簿、XX手册(指南)

- 在信息发达的社会中，只要存在，就没有找不到

通过搜索引擎可以获取到大量的信息

- 搜索引擎提供的信息的有效性？

信息收集方法

Whois

- 为Internet提供目录服务，包括名字、通讯地址、电话号码、电子邮箱、IP地址等信息

Client/Server结构

- Client端
 - 发出请求，接受结果，并按格式显示到客户屏幕上
- Server端
 - 建立数据库，接受注册请求
 - 提供在线查询服务

客户程序

- UNIX系统自带whois程序
- Windows也有一些工具
- 直接通过Web查询

基于Web的Whois示例

NAME SPACE SMART WHOIS RESULTS - Microsoft Internet Explorer

文件(E) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)

地址(D) <http://name.space.xs2.net/cgi-bin/whois.pl>

• PRO Domain Web and Email package is only \$179.00 per year! 2 POP Email, aliases, forwarding, 50M WEB account, INCLUDES DOMAIN NAME FOR FREE!

• [Download the latest ROOT ZONE file](#)

Registrant:
AltaVista Company ([ALTAVISTA16-DOM](#))
1070 Arastradero Road
Palo Alto, CA 94304
US

Domain Name: [ALTAVISTA.COM](#)

Administrative Contact:
AltaVista Domain Administration ([AD14996-OR](#)) dns-admin@AV.COM
AltaVista Company
c/o AltaVista Legal Department
1070 Arastradero Rd
Palo Alto, CA 94304
US
650-320-7700
Fax- 650-320-6433

Technical Contact:
AltaVista Company ([AO111-ORG](#)) dns-technical@AV.COM
AltaVista Company
1070 Arastradero Road
PALO ALTO, CA 94304
US
650-320-7700 fax: 650-330-6433

Billing Contact:
AltaVista Domain Billing ([AD14996-OR](#)) dns-billing@AV.COM
AltaVista Company
1070 Arastradero Road
Palo Alto, CA 94304
US
650-320-7700
Fax- 650-320-6433

Record last updated on 15-Mar-2002.
Record expires on 10-Feb-2007.
Record created on 10-Feb-2000.
Database last updated on 24-Apr-2002 10:33:00 EDT.

Domain servers in listed order:

NS1.ALTAVISTA.COM	209.73.164.76
NS2.ALTAVISTA.COM	209.73.164.7
NS3.ALTAVISTA.COM	209.73.176.204

信息收集：nslookup

关于DNS

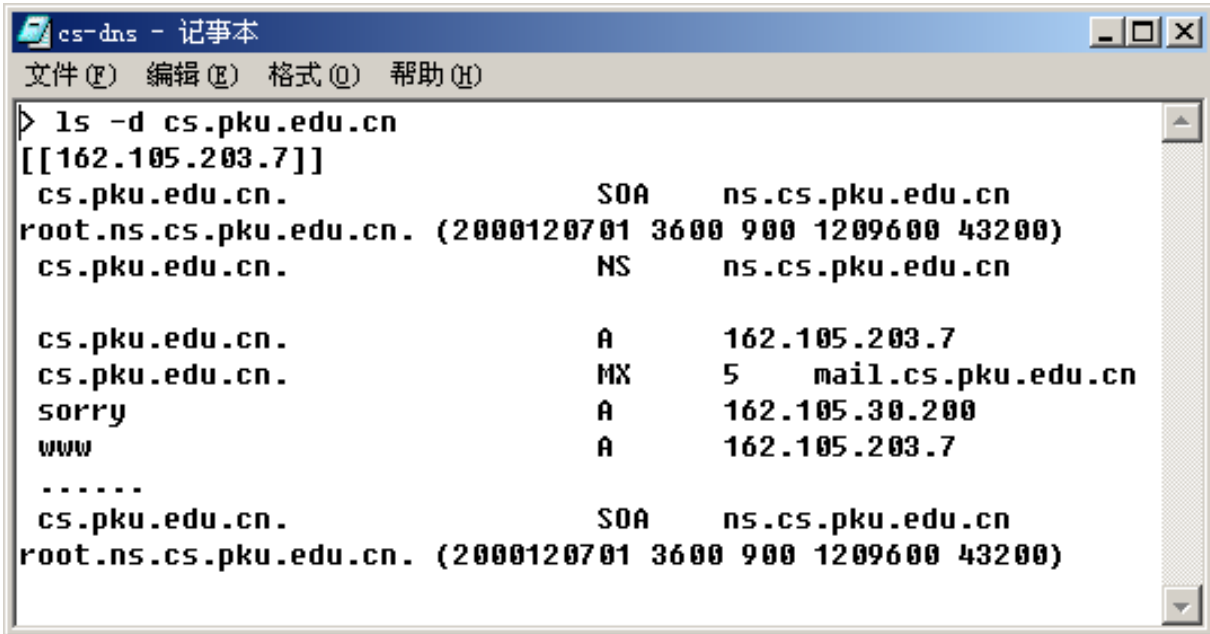
- 是一个全球分布式数据库，对于每一个DNS节点，包含有该节点所在的机器的信息、邮件服务器的信息、主机CPU和操作系统等信息
- nslookup是一个功能强大的客户程序

熟悉nslookup，就可以把DNS数据库中的信息挖掘出来

- 分两种运行模式
 - 非交互式，通过命令行提交命令
 - 交互式：可以访问DNS数据库中所有开放的信息

UNIX/LINUX环境下的host命令有类似的功能

DNS节点的例子



```
cs-dns - 记事本
文件(F) 编辑(E) 格式(O) 帮助(H)

> ls -d cs.pku.edu.cn
[[162.105.203.7]]
cs.pku.edu.cn.                SOA      ns.cs.pku.edu.cn
root.ns.cs.pku.edu.cn. (2000120701 3600 900 1209600 43200)
cs.pku.edu.cn.                NS       ns.cs.pku.edu.cn

cs.pku.edu.cn.                A        162.105.203.7
cs.pku.edu.cn.                MX       5      mail.cs.pku.edu.cn
sorry                          A        162.105.30.200
www                            A        162.105.203.7
.....
cs.pku.edu.cn.                SOA      ns.cs.pku.edu.cn
root.ns.cs.pku.edu.cn. (2000120701 3600 900 1209600 43200)
```

DNS & nslookup

通过nslookup可以做什么？

- 区域传送：可以列出DNS节点中所有的配置信息
- 这是为了主DNS和辅DNS之间同步复制才使用的
- 查看一个域名，根据域名找到该域的域名服务器
- 反向解析，根据IP地址得到域名名称

从一台域名服务器可以得到哪些信息？

- 如果支持区域传送，全部可查
- 否则的话，至少可以发现以下信息
 - 邮件服务器的信息，在实用环境中，邮件服务器往往在防火墙附近，甚至就在同一台机器上
 - 其他，比如ns、www、ftp等，这些机器可能被托管给ISP

信息收集

网络扫描

网络监听

口令破解

网络扫描 – 章节分解

1. 扫描器
2. 地址扫描
3. 端口扫描
4. 漏洞扫描
5. 扫描器发展历史

扫描器介绍

扫描器是一种自动检测远程或本地主机安全性弱点的程序

- 通过使用扫描器可以发现远程服务器是否在线
- 它对外开放的各种TCP端口的分配及提供的服务
- 它所使用的软件版本(如操作系统或其他应用程序的版本)
- 所存在可能被利用的系统漏洞

扫描器的重要性

扫描器能够暴露网络上潜在的脆弱性

无论扫描器被管理员利用，或者被黑客利用，都有助于加强系统的安全性

- **它能使得漏洞被及早发现，而漏洞迟早会被发现的**

扫描器除了能扫描端口，往往还能够

- **发现系统存活情况，以及哪些服务在运行**
- **用已知的漏洞测试这些系统**
- **对一批机器进行测试，简单的迭代过程**
- **有进一步的功能，包括操作系统辨识、应用系统识别**

操作系统辨识

操作系统辨识的动机

- 许多漏洞是系统相关的，而且往往与**相应版本**对应
- 从操作系统或者应用系统的具体实现中，发掘出来的攻击手段都需要辨识系统
- 操作系统的信息还可以与其他信息结合起来，比如漏洞库，或者社会诈骗(社会工程， social engineering)

如何辨识一个操作系统

- 一些端口服务的提示信息，例如，telnet、http、ftp等服务的提示信息
- TCP/IP栈指纹
- DNS泄漏出OS系统

地址扫描

C:\>ping WWW.163.com

Pinging WWW.163.com[202.108.42.91]with 32bytes of data:

Reply from 202.108.42.91: bytes=32 time=331ms TTL=46

Reply from 202.108.42.91: bytes=32 time=320ms TTL=46

Reply from 202.108.42.91: bytes=32 time=370ms TTL=46

Reply from 202.108.42.91: bytes=32 time=361ms TTL=46

Ping statistics for 202.108.42.91:

Packets: Sent=4, Received=4, Lost=0 (0%loss),

Approximate round trip times in milli-seconds:

Minimum=320ms, Maximum=370ms, Average=345ms

关于Ping

可以用来发现一台主机是否Active

为什么不能ping成功?

- 没有路由，网关设置?
- 网卡没有配置正确
- Timeout值
- 防火墙阻止掉了

“Ping of death”

- 发送特大ping数据包(>65535字节)导致机器崩溃

缺点?

- 针对单台主机，面对大量主机，效率低。

网络扫描 – 端口扫描

基于TCP/IP协议，对各种网络服务，无论是主机或者防火墙、路由器都适用

端口扫描可以确认各种配置的正确性，避免遭受不必要的攻击

用途，双刃剑

- **管理员可以用来确保自己系统的安全性**
- **黑客用来探查系统的入侵点**

端口扫描的技术已经非常成熟，目前有大量的商业、非商业的扫描器

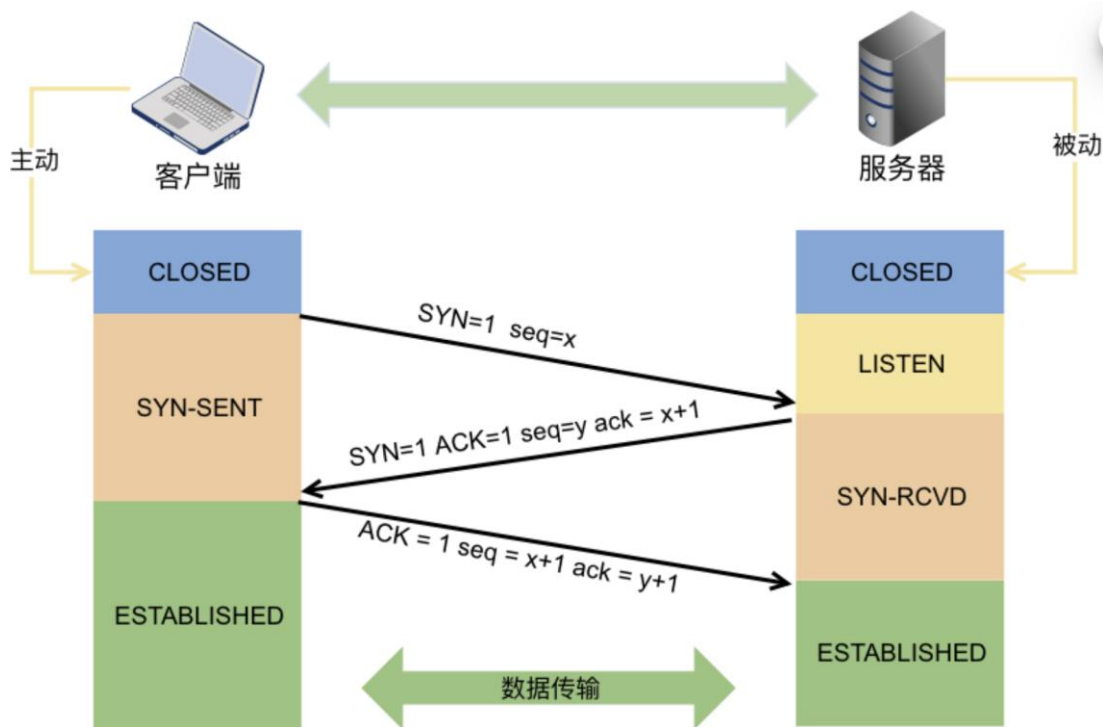
端口扫描

- 熟知端口 (0 ~ 1023)
- 注册端口 (1024 ~ 49151)
- 专用端口 (49152 ~ 65535)

方法

- 基本扫描
 - Connect, SYN, FIN, Xmas树, 空扫描, ACK, Windows, RPC, UDP
- 高级扫描
 - Ident, FTP Bounce

回顾：TCP连接的建立和终止时序图



TCP连接知识

TCP数据包6个标志位

- URG: 紧急数据包
- ACK: 确认
- PSH: 请求急迫操作
- RST: 连接复位
- SYN: 连接请求
- FIN: 结束

TCP/IP的一些实现原则

- 当一个SYN或者FIN数据包到达一个关闭端口，丢弃数据包的同时发送一个RST数据包
- 当一个RST数据包到达一个监听端口，RST被丢弃
- 当一个包含ACK的数据包到达一个监听端口时，数据包被丢弃，同时发送一个RST数据包
- 当一个不包含SYN位的数据包到达一个监听端口时，数据包被丢弃
- 当一个SYN数据包到达一个监听端口时，正常的三阶段握手继续，回答一个SYN|ACK数据包
- 当一个FIN数据包到达一个监听端口时，数据包被丢弃

端口扫描技术

基本的TCP connect()扫描

TCP SYN扫描 (半开连接扫描, half open)

TCP Fin扫描 (秘密扫描, stealth)

TCP ftp proxy扫描 (bounce attack)

用IP分片进行SYN/FIN扫描 (躲开防火墙检测)

UDP ICMP端口不可达扫描

Reverse-ident扫描

TCP connect()扫描

做法

- 扫描器调用socket的connect()函数发起一个正常的连接
 - 如果端口是打开的，则连接成功
 - 否则，连接失败

优点

- 简单，不需要特殊的权限

缺点

- 服务器可以记录下客户的连接行为，如果同一个客户轮流对每一个端口发起连接，则一定是在扫描

TCP SYN扫描

做法

- 向目标主机的特定端口发送一个SYN包
 - 如果应答包为RST包，则说明该端口是关闭的
 - 否则，应答包为一个SYN/ACK包
 - 扫描客户端发送一个RST包，停止建立连接
- 由于连接没有完全建立，所以称为“半开连接扫描”

优点

- 很少有系统会记录这样的行为，更隐蔽

缺点

- 在UNIX平台上，需要root权限才可以建立这样的SYN数据包

TCP FIN扫描 (秘密扫描)

做法

- 扫描器发送一个FIN数据包
 - 如果端口关闭，则丢弃该包，并送回一个RST包
 - 否则的话，丢弃该包，不回送

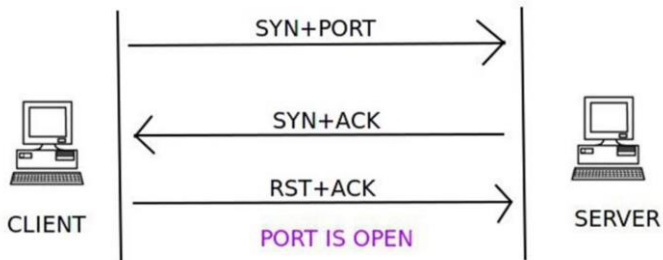
优点

- 相对TCP SYN扫描更隐蔽 (可用防火墙技术检查未被允许访问的端口扫描)
- 不是TCP建立连接的过程，所以比较隐蔽 (针对打开端口)

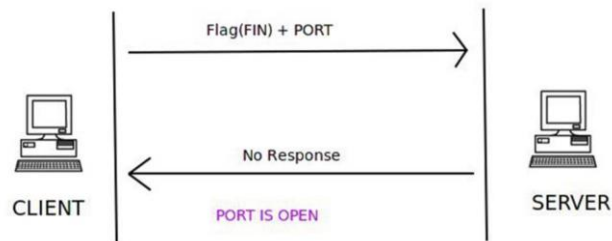
缺点

- 与SYN扫描类似，也需要构造专门的数据包

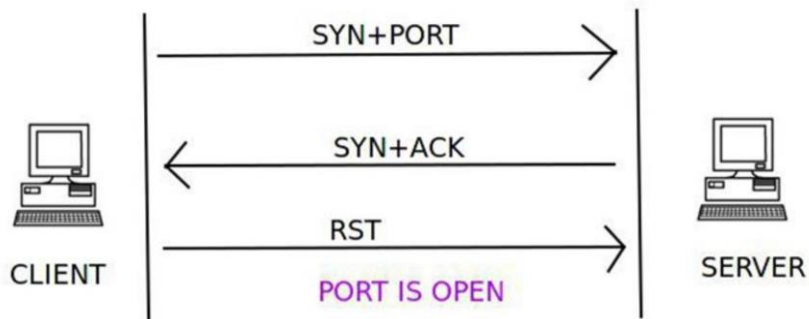
示例



Connect



FIN



SYN

分片扫描

本身并不是一种新的扫描方法，而是其他扫描技术的变种，特别是SYN扫描和FIN扫描

通过把TCP包分成很小的分片，从而让它们能够通过包过滤防火墙

- 注意，有些防火墙会**丢弃太小的包**
- 而有些服务程序在处理这样的包时会出现异常，或者性能下降，或者出现错误

Reverse-Ident扫描

Ident协议使得攻击者可以发现任何一个通过TCP连接的进程的所有者的用户名，即使该进程并没有发起连接

- **只有在TCP全连接之后才有效**
- **TCP端口113**

例如

- **可以先连接到80端口，然后通过ident来发现服务器是否在root下运行**

建议关闭ident服务，或者在防火墙上禁止，除非是为了审计的目的

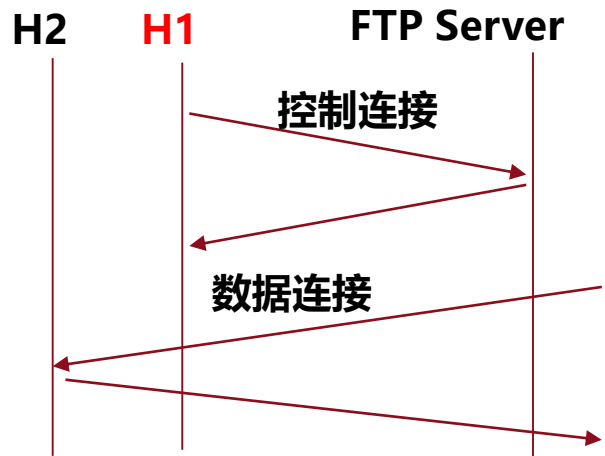
TCP FTP Proxy扫描

方法

- 在FTP协议中，数据连接可以与控制连接位于不同的机器上
- FTP Server 与 目标主机建立连接，且目标主机端口可以指定
- 如果端口打开，则可以传输否则，返回"425 Can't build data connection: Connection refused."
- FTP这个缺陷还可以被用来向目标（邮件，新闻）传送匿名信息

优点：这种技术可以用来穿透防火墙

缺点：慢，且有些FTP Server禁止这种特性



UDP ICMP端口扫描

利用UDP协议

做法

- 向目标端口发送UDP分组
- 对于关闭的UDP端口，会送回一个ICMP Port Unreach错误

缺点

- 速度慢，而且UDP包和ICMP包都不是可靠的
- 需要root权限，才能读取ICMP Port Unreach消息
- 网络状态不好？

漏洞扫描

漏洞扫描是指使用漏洞扫描程序，对目标系统进行信息查询

漏洞扫描器是一种自动检测远程、或本地主机安全性弱点的程序

外部扫描

- 端口，软件

内部扫描

- 系统配置，漏洞

扫描器历史

早期

- 80年代，网络没有普及，上网的好奇心驱使许多年轻人通过Modem拨号进入到UNIX系统中。这时候的手段需要大量的手工操作
- 于是，出现了War Dialer——自动扫描，并记录下扫描的结果
- 现代的扫描器要先进得多

SATAN: Security Administrator's Tool for Analyzing Networks

- 1995年4月发布，引起了新闻界的轰动
- 界面上的突破，从命令行走向图形界面 (使用HTML界面)
- 两位作者的影响 (Dan Farmer写过网络安全检查工具COPS，另一位Weitse Venema是TCP_Wrapper的作者)

Nmap

- 技术上，是最先进的扫描技术大集成
- 结合了功能强大的通过栈指纹，来识别操作系统的众多技术

经典的网络扫描器 - 1

主要功能有：

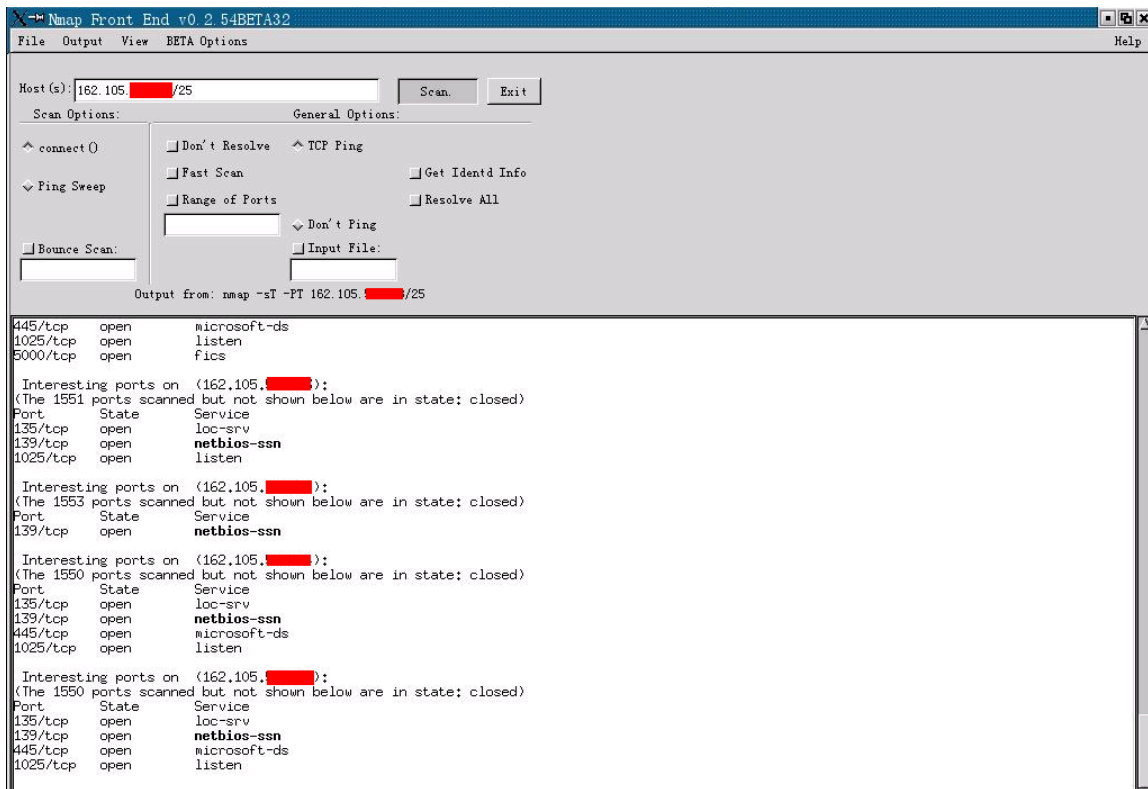
- **检测活跃在网络上的主机（主机发现）**
- **检测主机上开放的端口（端口发现或枚举）**
- **检测到相应的端口（服务发现）的软件和版本**
- **检测操作系统，硬件地址，以及软件版本**

经典的网络扫描器 - 2

Nmap

- www.nmap.org
- UDP、TCP connect、TCP SYN（半开）、Ftp Proxy（跳跃攻击）、Reverse-ident、ICMP (ping)、FIN、ACK sweep、Xmas Tree、SYN sweep和NULL扫描
- 通过TCP/IP来鉴别操作系统类型、秘密扫描、动态延迟和重发、平行扫描、通过并行的Ping侦测下属的主机、欺骗扫描、端口过滤探测、直分布扫描、灵活目标选择以及端口的描述

Nmap用于扫描 - 1



Nmap用于扫描 - 2

```
[root@supersnake nides]# nmap -sS www.██████████
```

Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/)
Interesting ports on (██████████):
(The 1521 ports scanned but not shown below are in state: closed)

Port	State	Service
7/tcp	open	echo
9/tcp	open	discard
13/tcp	open	daytime
19/tcp	open	chargen
21/tcp	open	ftp
23/tcp	open	telnet
25/tcp	open	smtp
37/tcp	open	time
80/tcp	open	http
111/tcp	open	sunrpc
199/tcp	open	smux
512/tcp	open	exec
513/tcp	open	login
514/tcp	open	shell
543/tcp	open	klogin
544/tcp	open	kshell
986/tcp	open	unknown
987/tcp	open	unknown
2401/tcp	open	cvspsrver
6000/tcp	open	X11
6112/tcp	open	dtspc

Nmap run completed -- 1 IP address (1 host up) scanned in 1 second
[root@supersnake nides]# █

经典的网络扫描器 - 2

Nessus

- www.nessus.org
- Nessus是图形化界面，使得它使用起来相当简便，它还对扫描出的漏洞给出详细的利用方法和补救方法。所以，Nessus是攻击者和网管都应该学会使用的漏洞检查利器

X-scan

- <http://xfocus.org>
- 提供了图形界面和命令行两种操作方式
- 远程操作系统类型及版本、标准端口状态及端口banner信息、CGI漏洞、RPC漏洞、SQL-SERVER默认帐户、弱口令，NT主机共享信息、用户信息、组信息、NT主机弱口令用户

最近的扫描器

地址端口扫描

- **ScanPort, Ghost Port Scanner, nbtscan, Dr. Morena, IP Restrictions Scanner, Arp-scan, Cheops-ng**

特征扫描

- **Xprobe, LDistFP, TelnetFP**

系统扫描

- **Security Administrators Integrated Network Tool , VLAD , NetPing, HostScan**

无线扫描

- **NetStumbler, WirelessMon, WiFi Hopper, Vistumbler**

信息收集

网络扫描

网络监听

口令破解

网络监听 – 章节分解

1. 共享式以太网
2. 交换式以太网
3. 防范&检测方法

网络监听

网络监听的目的是截获通信的内容

监听的手段是对协议进行分析

当黑客成功地登录进一台网络上的主机，并取得了root权限之后，而且还想利用这台主机去攻击同一网段上的其它主机时，这时网络监听是一种最简单而且最有效的方法，它常常能轻易地获得用其他方法很难获得的信息

网络监听 – 共享以太网

什么是共享以太网？

unicast, broadcast, multicast, promiscuous

Sniffer

- 中文可以翻译为嗅探器，可以监视网络的状态、数据流动情况以及网络上传输的信息
- 当信息以明文的形式在网络上传输时，便可以使用网络监听的方式来进行攻击

网络监听 - 交换式以太网

交换机能根据数据帧中的目的MAC地址，将数据帧准确地送到目的主机的端口，而不是所有的端口。

所以交换式网络环境在一定程度上能抵御Sniffer攻击

在交换环境中，Sniffer的简单的做法就是伪装成为网关

ARP欺骗

➤ **ARPredirect**

□ **冒充网关，窃取消息**

网络监听 - 交换式以太网 - 示例

A主机, 网关, IP 192.168.0.1

B主机, 用户端, IP 192.168.0.2

C主机, 入侵者, IP 192.168.0.3

受网关控制, C无法监听A-B通信

C采用ARP欺骗攻击: ARPredirect - t 192.168.0.2 192.168.0.1

告诉B主机, C主机是网关

破绽?

网络监听 - 防范&检测方法

网络监听的防范方法

- 确保以太网的整体安全性（设备端）
- 采用加密技术（数据端）

检测网络监听的手段

- 反应时间
- DNS测试
- 利用Ping进行监测
- 利用ARP数据包进行监测

信息收集

网络扫描

网络监听

口令破解

口令破解

黑客攻击目标时常常把破译普通用户的口令作为攻击的开始

字典文件

- **用户的名字、生日、电话号码、身份证号码、所居住街道的名字等**

口令破解

口令攻击类型

- 字典攻击
- 强行攻击 (传统暴力破解, 费时)
- 组合攻击 (yuecao2021)

口令破解器

- 一般通过判断数据加密后和要解密的原数据是否一致
- A (尝试破解的口令) + B (加密算法) = C (被解密的口令)

注册码

- 需已知注册码算法即可破译安装

口令破解 - Windows 口令破解

➤ Windows 的口令存放

- SAM (Security Account Manager)

- LM (Lan Manager) 口令散列算法

- NTLM (Windows LAN Manager) 盘问相应验证机制

安全标识在账号创建就同时创建，一旦账号被删除，安全标识也同时被删除。即便是相同用户名，在每次创建是标识都是不同的

➤ Windows 口令破解程序

- L0phtcrack (www.10pht.com)

- NTSweep (www.packet.securify.com)

- PWDump2 (www.doubleupsoftware.com)

口令破解 - Unix口令破解

➤ /etc/passwd

□ LOGNAME : PASSWORD : UID : GID :
USERINFO : HOME : SHELL

➤ /etc/shadow: 把passwd中口令领域分离, 增强

➤ CrackLib

□ CrackLib

□ John、Crack

□ 禁用root远程登录

课后习题

1. 扫描有几种类型？简述它们的功能
2. 什么是网络监听？
3. 简述以太网的网络监听
4. 如何防范网络监听？

谢谢!