



网络攻击与防御

CH03—信息收集与防御

BitSec(张立江)

中国矿业大学 网络空间安全系

is.cumt.edu.cn



扫描技术

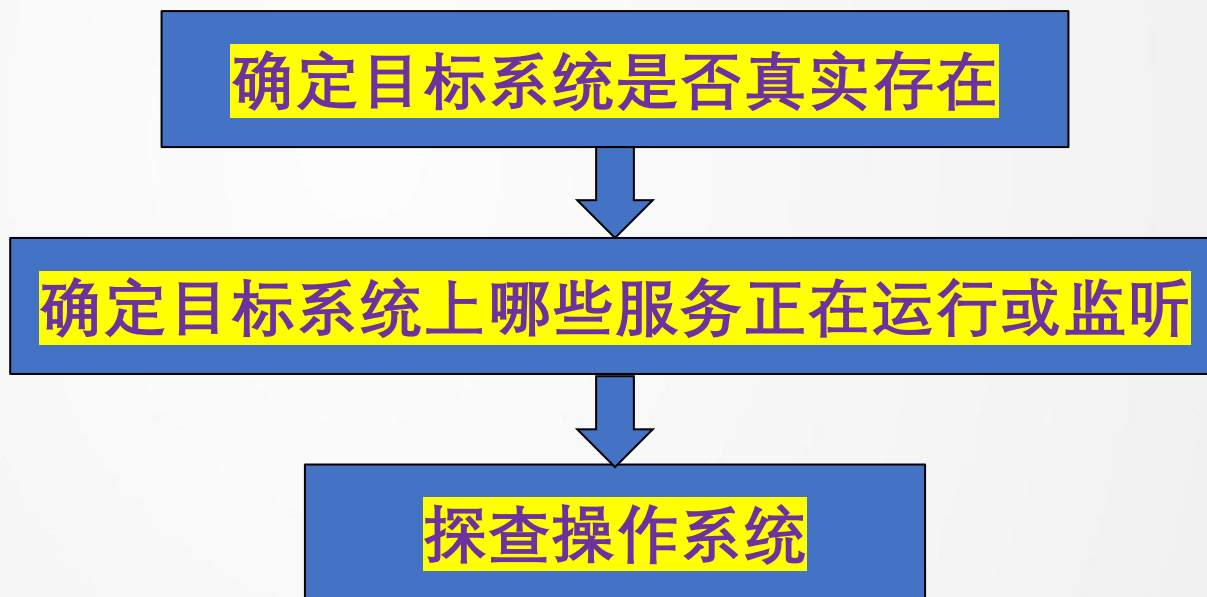
查点技术

扫描与查点的防御

网络嗅探与防御

扫描技术概述

- 扫描的基本步骤:



确定目标系统是否真实存在

- 基本方法：**ping 扫描**
 - （传统意义上）**ping**：向目标发**ICMP ECHO**（类型8）数据包，如返回 ICMP ECHO_REPLY数据包（类型0），说明目标系统真实存在
 - ✓ ping
 - ✓ **nmap -sP**：Linux + windows，GUI版本为Zenmap
 - （现在的）**ping**：可利用 ICMP，TCP，UDP

```
root@kali: ~# nmap -sP 58.218.185.156
```

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-08-15 09:01 CST  
Nmap scan report for 58.218.185.156  
Host is up (0.00081s latency).  
Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

```
root@kali: ~# nmap -sP www.cumt.edu.cn
```

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-08-15 08:58 CST  
Nmap scan report for www.cumt.edu.cn (58.218.185.156)  
Host is up (0.0020s latency).  
Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```


- **Q:** 目标站点阻断了ICMP数据包，怎么办？

- **A:** 使用TCP，UDP进行ping扫描

- ✓ **nmap -PT:** 对“-PT”选项指定的端口（通常是80端口）进行TCP ping扫描；该选项向目标网络发出**TCP ACK**数据包并根据返回的**RST**数据包判断活跃主机

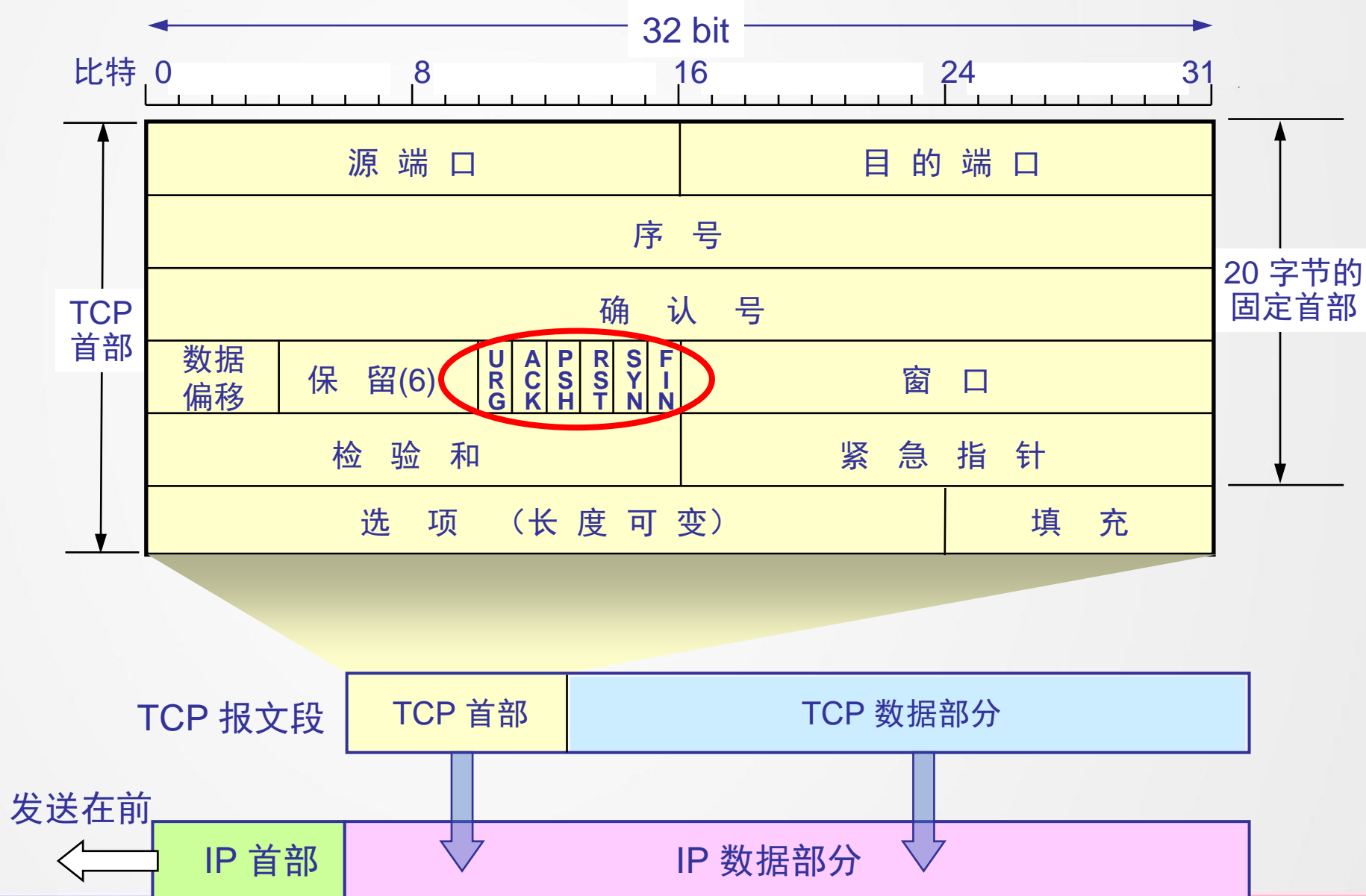
```
root@kali:~# nmap -sP -PT80 www.163.com
```

- ✓ **problem:** 为什么选用发出ACK数据包？

- ✓ **answer:** 绝大多数无状态（non-stateful）防火墙产品（如Cisco IOS系列）通常都会放行这种数据包

确定目标系统上哪些服务正在运行或监听

- **端口扫描：** 主动连接目标系统的TCP和UDP端口以确定哪些服务正在运行或处于LISTENING（监听）状态
- **主要目的：**
 - 确定运行的TCP/UDP服务
 - 确定操作系统的**具体**类型
 - 确定提供服务的应用程序名称和版本



❖ TCP的6个标志位

- URG: 紧急数据包
- ACK: 确认
- PSH: 请求急迫操作; 接收方应尽快将数据包交给应用层
- RST: 连接复位; 重建连接
- SYN: 连接请求
- FIN: 结束

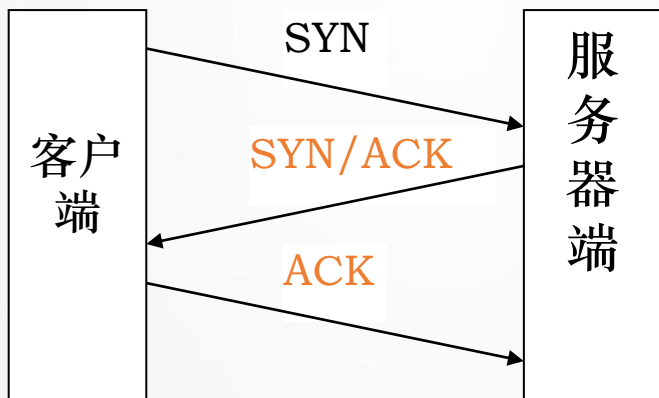
❖ TCP/IP的一些实现原则

- SYN或FIN数据包到达一关闭的端口, 丢弃数据包同时发送一个RST数据包
- RST数据包到达一监听端口/关闭端口, RST被丢弃

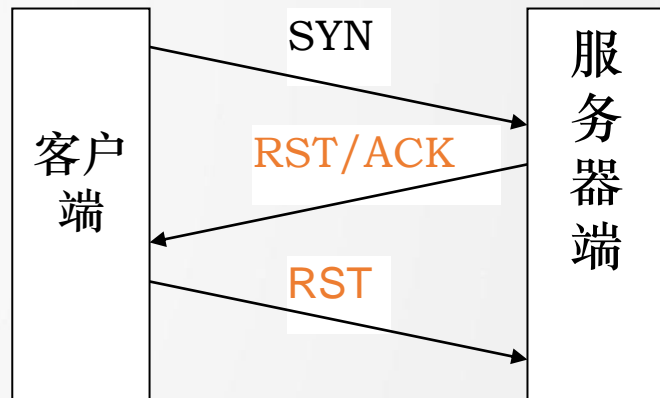
- 包含ACK的数据包到达一个监听端口时, 数据包被丢弃, 同时发送一个RST数据包
- 不包含SYN位的数据包到达一个监听端口时, 数据包被丢弃
- SYN数据包到达一个监听端口时, 正常的三阶段握手继续, 回答一个SYN|ACK数据包
- FIN数据包到达一个监听端口时, 数据包被丢弃

• 扫描类型:

1. TCP连接扫描 (TCP Connect () 扫描; `nmap -sT`) : 连接目标端口并完成一次完整的三次握手过程; 很容易被目标系统觉察



建立连接成功 (目标端口开放)



未建立连接成功(目标端口关闭)

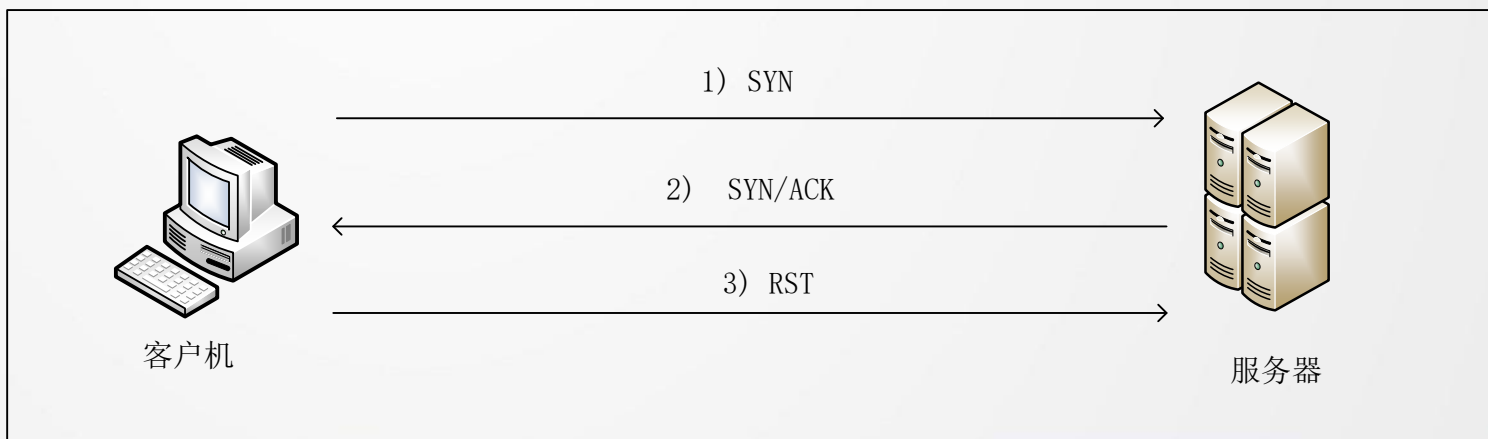
2. TCP SYN扫描(半开扫描; `nmap -sS`)：向目标端口送SYN数据包

- 返回SYN/ACK数据包，可以断定该端口处于监听状态
- 返回RST/ACK数据包，通常表明该端口不在监听状态

然后，扫描者送出一个RST/ACK数据包（使通信双方永远不会建立一条完整连接）

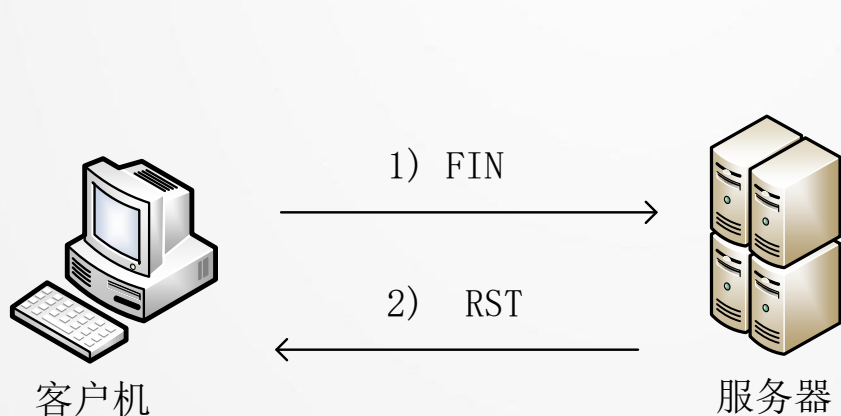
优点：更隐秘，目标系统一般不会将其记入日志

缺点：半开连接过多时，会形成一种“拒绝服务”条件而引起对方的警觉

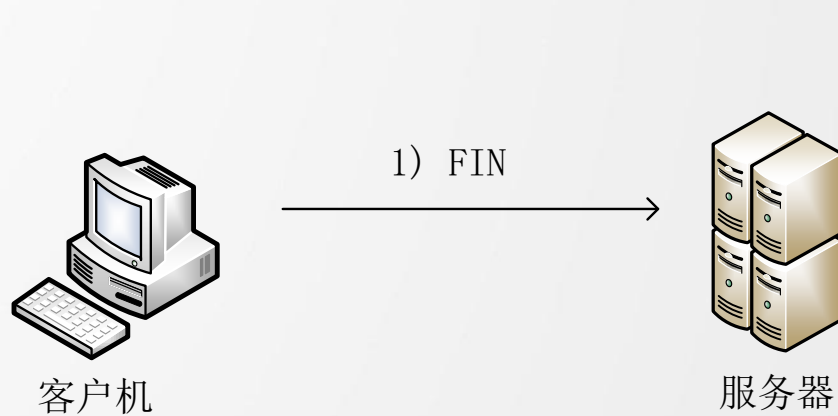


3. TCP FIN扫描 (秘密扫描; `nmap -sF`) : 向目标端口发送FIN数据包

- 如果目标端口关闭, 目标系统应该返回一个RST数据包, 否则丢弃该包。通常只对UNIX/LINUX系统的TCP/IP栈有效 (Window平台总是返回RST包)
- 由于不包含TCP三次握手协议的任何部分, 所以无法被记录下来, 从而比SYN扫描隐蔽
- FIN数据包能通过监测SYN包的包过滤器 (秘密扫描)



(a)端口关闭的情况



(b)端口开放的情况

秘密扫描的两个变体：

3.1 TCP Xmas扫描（圣诞树扫描；`nmap -sX`）：TCP包包头设置所有标志位（1）

- 目标端口关闭，目标系统应该返回一个RST数据包

3.2 TCP Null扫描（空扫描；`nmap -sN`）：关掉所有的标志位（0）

- 目标端口关闭，目标系统应该返回一个RST数据包

- **Remark:** 使用这些组合的目的是通过FIN标记监测器的过滤

- ✓ **Remark:** 主要用于UNIX/Linux/BSD的TCP/IP的协议栈；不适用于Windows系统

4. **TCP ACK扫描** (`nmap -sA`): 测试防火墙的规则集。判断防火墙是简单的**包过滤防火墙**; 还是高级的、具备数据包过滤功能的**状态 (stateful) 防火墙**
 - 不能用来确定端口是否开放或者关闭
5. **TCP窗口扫描** (`nmap -sW`): 测试特定目标系统 (如**AIX**和**FreeBSD**系统) 上的端口是否开放、被过滤——会导致目标系统返回不同的TCP窗口长度值

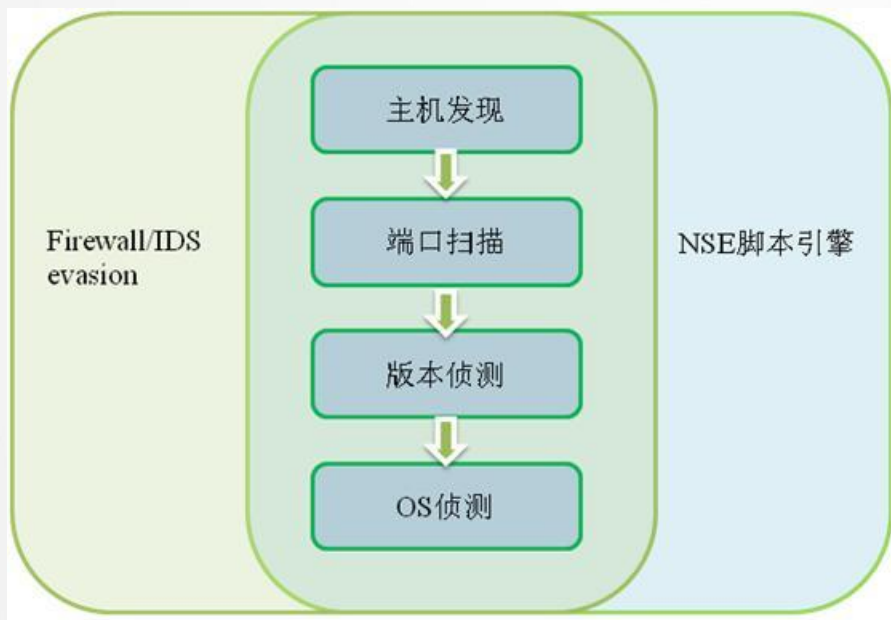
6. **TCP Maimon扫描**(**nmap -sM**) : 探测报文改为FIN/ACK外, 其原理与TCP FIN扫描一样; 无论端口是否开放, 都应响应RST报文。Uriel注意到如果端口开放, 许多基于BSD的系统只是丢弃该报文
7. **UDP扫描**(**nmap -sU**) : 向目标端口发出UDP数据包
- 如果返回“ICMP port unreachable” 出错消息, 表明端口关闭
 - 如果没有收到该消息, 端口可能开放
 - **remark:** UDP不要求必须建立一条连接, 所以扫描的准确性取决于与目标网络的使用情况和过滤机制有关的许多因素 (**扫描结果不可靠**)

扫描工具-NMAP (Network Mapper)



• NMAP (扫描之王) :

- 主机扫描技术
- 端口扫描技术
- 远程主机OS指纹识别
- 防火墙/IDS规避
- 脚本引擎NSE



Ping扫描: **nmap -sP**

缺省时同时发送icmp和对80端口
发送ack来探测

可以用**nmap -sP -P0** 不发送icmp
消息

TCP connect扫描: **nmap -sT**

TCP SYN扫描: **nmap -sS**

TCP FIN, XMAS, NULL扫描:

nmap -sF

nmap -sX

nmap -sN

UDP扫描: **nmap -sU**

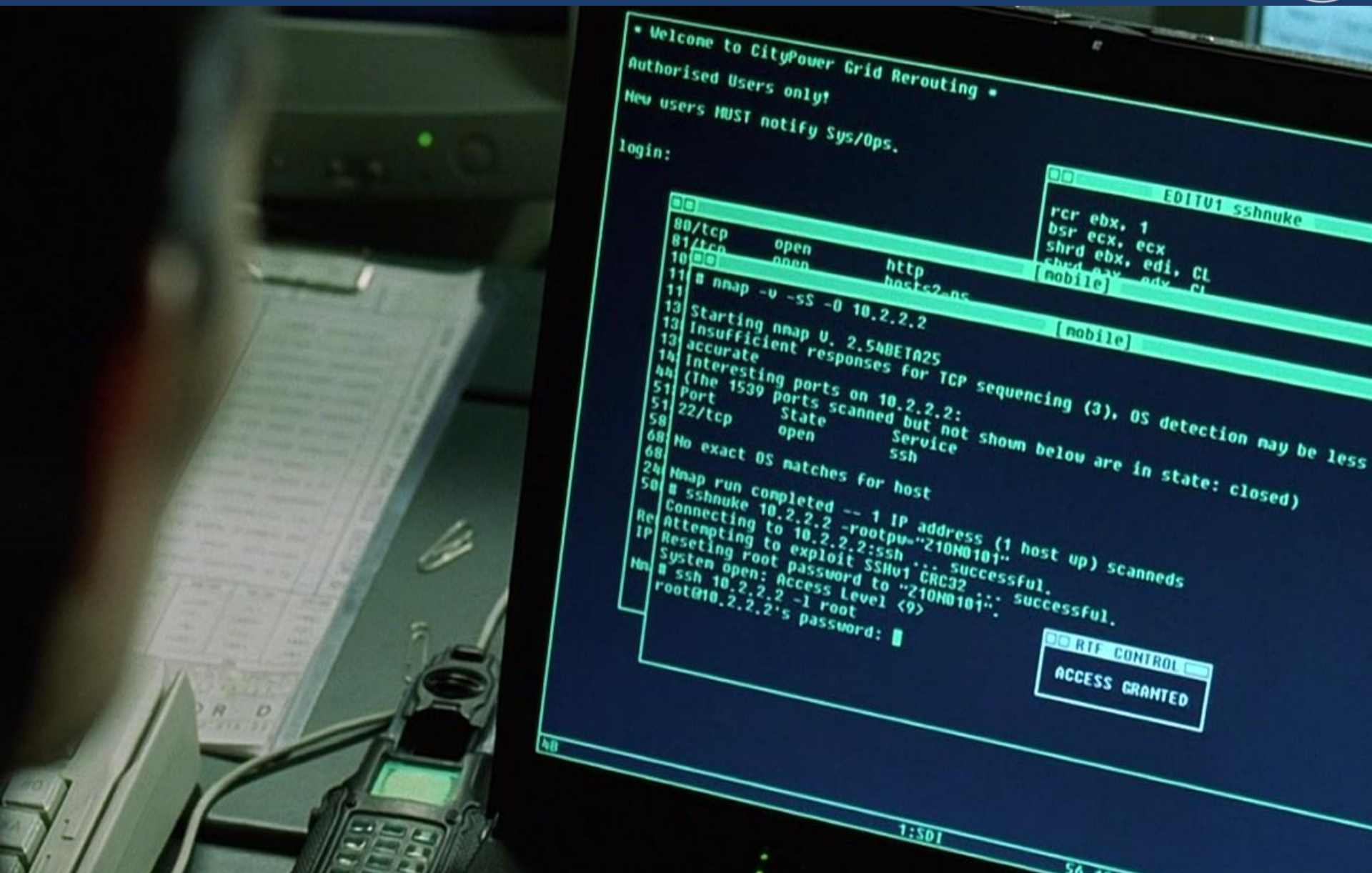
激进扫描: **nmap -A**

控制时间:

nmap -T(0-5) #数字代表激进程度



The Matrix- 《黑客帝国》





The Matrix- 《黑客帝国》

- nmap: `//man nmap` 查看如何使用
- `nmap -sS` : TCP SYN端口扫描

```
root@kali: ~# nmap -sS 58.218.185.156
root@kali: ~# nmap -sS mail.cumt.edu.cn

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-08-15 09:14 CST
Nmap scan report for mail.cumt.edu.cn (58.218.185.21)
Host is up (1.2s latency).
Not shown: 988 closed ports
PORT      STATE      SERVICE
25/tcp    open      smtp
80/tcp    open      http
110/tcp   open      pop3
111/tcp   open      rpcbind
143/tcp   open      imap
465/tcp   open      smtps
514/tcp   filtered  shell
993/tcp   open      imaps
995/tcp   open      pop3s
2222/tcp  open      EtherNetIP-1
5989/tcp  open      wbem-https
9900/tcp  open      iua

Nmap done: 1 IP address (1 host up) scanned in 475.87 seconds
```

DNMAP(KALI): 基于Nmap的分布式框架，使用客户端/服务端架构，服务器接收命令并发送至客户端进行Nmap安全扫描，扫描完毕后，客户端返回扫描结果

• 其他扫描工具：

- **natcat (nc) [unix, windows]***：能够完成的任务非常之多，业界称之为信息安防人员的“**瑞士军刀**”
- **SuperScan [windows]**：不再更新
- **X-Scan [windows]**：更新至2010年

```
root@kali:~# nc -v -z -w2 www.163.com 1-140
Warning: inverse host lookup failed for 58.222.18.97: Unknown server error : Connection timed out
Warning: inverse host lookup failed for 58.221.56.5: Unknown server error : Connection timed out
163.xdwscache.glb0.lxdns.com [58.222.18.97] 135 (loc-srv) : Connection timed out
163.xdwscache.glb0.lxdns.com [58.222.18.97] 89 (?) open
163.xdwscache.glb0.lxdns.com [58.222.18.97] 88 (kerberos) open
163.xdwscache.glb0.lxdns.com [58.222.18.97] 80 (http) open
```

-v：生成详尽的输出报告；

-vv：生成非常详尽的输出报告；

-z：零模式I/O，即端口扫描；

-w2：设定各条连接的倒计时超时值

探查操作系统

- **主要技术：**

- 旗标抓取技术（查点部分）
- 协议栈指纹分析技术（更准确），可分为：
 - 主动式协议栈指纹分析技术
 - 被动式协议栈指纹分析技术

- **协议栈指纹分析技术的工作原理：**

- 不同厂家的IP协议栈实现存在着许多细微的差别
- 探查这些差异，就能对目标系统做出有依据的判断

- 可用的探查技术：

- **FIN探查**：向某个打开端口发出FIN数据包。根据RFC 793的规定，目标系统应该不做任何响应。但许多实现如Windows会返回FIN/ACK数据包
- **无效标志探查**：在SYN数据包的TCP报头置位一个未定义的TCP标志。某些操作系统（如Linux）会在响应数据包里置位这个标志
- **ISN（Initial Sequence Number，初始序列号）采样**：TCP协议在响应一个连接请求时，返回的ISN呈现不同的模式
- **DF标志位监控**：某些操作系统会置位DF位（Don't Fragment）以改善性能

• 可用的探查技术（续）：

- **TCP初始数据窗长度**：目标系统返回数据包的初始窗口大小不同
- **ACK值**：不同的IP协议栈在往ACK字段里填写序列号时会采用不同的做法，有的原封不动地送回，有的则会先加1、再送回来
- **ICMP出错消息抑制**（有些OS会对送出ICMP出错消息的频率做出限制）/**ICMP消息内容**（不同OS在ICMP返回消息里给出的文字内容不一样）/**ICMP出错消息——请求/响应是否匹配**（某些实现在返回ICMP出错消息时会改变请求数据包的IP报头）
- **数据包拆分处理**：协议栈在处理数据包分片时采取不同的做法。在重新组合数据包时，协议栈会用后收到的新数据覆写先收到的老数据（或者相反）



扫描技术—操作系统探测

```
root@kali:~# ping -c 4 192.168.40.128
PING 192.168.40.128 (192.168.40.128) 56(84) bytes of data:
64 bytes from 192.168.40.128: icmp_seq=1 ttl=64 time=0.052 ms
64 bytes from 192.168.40.128: icmp_seq=2 ttl=64 time=0.064 ms
64 bytes from 192.168.40.128: icmp_seq=3 ttl=64 time=0.048 ms
64 bytes from 192.168.40.128: icmp_seq=4 ttl=64 time=0.055 ms
111/tcp open rpcbind
443/192.168.40.128 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt/min/avg/max/mdev = 0.048/0.055/0.064/0.006 ms

root@kali:~# ping -c 4 192.168.40.130
PING 192.168.40.130 (192.168.40.130) 56(84) bytes of data:
64 bytes from 192.168.40.130: icmp_seq=1 ttl=128 time=0.533 ms
64 bytes from 192.168.40.130: icmp_seq=2 ttl=128 time=0.645 ms
64 bytes from 192.168.40.130: icmp_seq=3 ttl=128 time=0.448 ms
64 bytes from 192.168.40.130: icmp_seq=4 ttl=128 time=0.645 ms
Nmap done: 1 IP address (1 host up) scanned in 204.42 seconds

root@kali:~# ping -c 4 192.168.40.130
PING 192.168.40.130 (192.168.40.130) 56(84) bytes of data:
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt/min/avg/max/mdev = 0.263/0.448/0.645/0.149 ms
```

**ubuntu linux、
Win 7**

**windows
XP**

扫描技术—操作系统探测

❖ **主动协议栈指纹分析技术**：向目标系统发送数据包去探查网络协议栈的独有特点，推测操作系统

✓ **nmap -O**：同时使用以上技术（“数据包拆分处理”和“ICMP 出错消息队列”除外）进行探查

```
root@kali: ~# nmap -O 192.168.40.130

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-08-15 09:24 CST
Nmap scan report for 192.168.40.130
Host is up (0.00057s latency).
Not shown: 985 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
143/tcp   open  imap
389/tcp   open  ldap
443/tcp   open  https
445/tcp   open  microsoft-ds
465/tcp   open  smtps
993/tcp   open  imaps
995/tcp   open  pop3s
1025/tcp  open  NFS-or-IIS
6000/tcp  open  X11
MAC Address: 00:0C:29:2A:10:F3 (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP2 or SP3
Network Distance: 1 hop
```

扫描技术—操作系统探测

❖ 被动协议栈指纹分析技术： 通过被动地监控网络通信推测目标的操作系统

◆ 成功取决于攻击者必须位于网络的通信枢纽，以及必须有一个可用来捕获数据包的端口

◆ (部分)被动式特征:TTL/窗口大小/DF位

✓ siphon的指纹数据库文件
osprints.conf

```
# Send new fingerprints to siphon@subterrain.net
```

```
# Window:TTL:DF:Operating System
```

```
# DF = 1 for ON, 0 for OFF.
```

```
7D78:64:1:Linux 2.1.122 - 2.2.14
```

```
77C4:64:1:Linux 2.1.122 - 2.2.14
```

```
7BF0:64:1:Linux 2.1.122 - 2.2.14
```

```
7BC0:64:1:Linux 2.1.122 - 2.2.14
```

```
832C:64:1:Linux 2.0.34 - 2.0.38
```

```
7FE0:64:0:Linux 2.0.34 - 2.0.38
```

```
0B68:64:1:Linux 2.0.32 - 2.0.34
```

```
4470:64:0:FreeBSD 2.2.1 - 4.0
```

```
4470:64:1:FreeBSD 2.2.1 - 4.0
```

```
43E0:64:1:FreeBSD 2.2.1 - 4.0
```

```
4074:64:0:OpenBSD 2.x
```

```
43E0:64:0:OpenBSD 2.x
```

```
4000:64:0:NetBSD 1.3 - 1.33 / AIX 4.3.X
```


• 查点技术——**旗标抓取**

• telnet

```
root@kali: ~# telnet mail.cumt.edu.cn 25
Trying 58.218.185.21...
Connected to mail.cumt.edu.cn.
Escape character is '^]'.
220 cumt.edu.cn Anti-spam GT for Coremail System (cumt[20141130])
Connection closed by foreign host.
```

盈世 | Coremail
引领邮件技术 沟通创造价值

```
root@kali: ~# telnet www.sina.com.cn 80
Trying 202.102.75.162...
Connected to newsnj.sina.com.cn.
Escape character is '^]'.
GET / HTTP/1.1
```

```
HTTP/1.1 403 Forbidden
Server: squid/2.7.STABLE5
Date: Tue, 09 Sep 2014 07:00:58 GMT
Content-Type: text/html
Content-Length: 117
X-Squid-Error: ERR_ACCESS_DENIED 0
X-Cache: MISS from 202.102.75.162
```

squid-cache.org
Optimising Web Delivery


```
root@kali:~# telnet www.cumt.edu.cn 80
```

```
Trying 58.218.185.156...
```

```
Connected to sudy.cumt.edu.cn.
```

```
Escape character is '^['.
```

```
get / /http 1.1
```

```
HTTP/1.1 408 Request Time-out
```

```
Date: Sun, 04 Sep 2016 08:31:47 GMT
```

```
Server: YxlinkWAF
```

```
Content-Length: 223
```

```
Connection: close
```

```
Content-Type: text/html; charset=iso-8859-1
```

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
```

```
<html><head>
```

```
<title>408 Request Time-out</title>
```

```
</head><body>
```

```
<h1>Request Time-out</h1>
```

```
<p>Server timeout waiting for the HTTP request from the client.</p>
```


```
</body></html>
```

```
Connection closed by foreign host.
```

→ 铱迅Web应用防护系统

- netcat:

```
root@kali: ~# nc -v 163.com 80
Warning: inverse host lookup failed for 123.58.180.8: Unknown host
Warning: inverse host lookup failed for 123.58.180.7: Unknown host
163.com [123.58.180.8] 80 (http) open
ls
<html>
<head><title>400 Bad Request</title></head>
<body bgcolor="white">
<center><h1>400 Bad Request</h1></center>
<hr><center>nginx</center>
</body>
</html>
```



Nginx (“engine x”)：一个高性能的 HTTP 和 反向代理 服务器，
也是一个 IMAP/POP3/SMTP 服务器

• HTTP:

POST index.jsp 200 OK mail.cumt.edu.cn

头信息 Post 响应 HTML 缓存 Cookies

响应头信息

原始头信息

Cache-Control no-cache
Content-Language zh-CN
Content-Type text/html; charset=GBK
Date Sat, 15 Aug 2015 03:53:21 GMT
Expires Thu, 01 Jan 1970 00:00:00 GMT
Pragma No-cache
Server Apache-Coyote/1.1
Transfer-Encoding chunked

Firefox
Firebug

请求头信息

原始头信息

Accept text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding gzip, deflate
Accept-Language zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Connection keep-alive
Cookie safedog-flow-item=832D12B6F7C8D4C92B4C0963F92A28C6; uid=cumt
Host mail.cumt.edu.cn
Referer http://mail.cumt.edu.cn/
User-Agent Mozilla/5.0 (Windows NT 10.0; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0

头(header)	类型	说明
User- Agent	请求	关于浏览器和它平台的信息，如Mozilla5.0
Accept	请求	客户能处理的页面的类型，如text/html
Accept-Charset	请求	客户可以接受的字符集，如Unicode-1-1
Accept-Encoding	请求	客户能处理的页面编码方法，如gzip
Accept-Language	请求	客户能处理的自然语言，如en(英语)，zh-cn(简体中文)
Host	请求	服务器的DNS名称。从URL中提取出来，必需。
Authorization	请求	客户的信息凭据列表
Cookie	请求	将以前设置的Cookie送回服务器，可用来作为会话信息
Date	双向	消息被发送时的日期和时间
Server	响应	关于服务器的信息，如Microsoft-IIS/6.0
Content-Encoding	响应	内容是如何被编码的（如gzip）
Content-Language	响应	页面所使用的自然语言
Content-Length	响应	以字节计算的页面长度
Content-Type	响应	页面的MIME类型
Last-Modified	响应	页面最后被修改的时间和日期，在页面缓存机制中意义重大
Location	响应	指示客户将请求发送给别处，即重定向到另一个URL
Set-Cookie	响应	服务器希望客户保存一个Cookie

- **Web 页面盗窃：**通过对网页源码的分析，找出可能的缺陷和脆弱点；方式包括：
 - **手工扫描：**（具有讽刺意义的是）**往往规范化的编程风格会提供给攻击者更多的信息：**规范的代码往往会有很多帮助性的注释，以帮助用户或者测试人员在代码运行错误时进行处理
 - **自动扫描：**逐页读取目标站点的网页，通过搜索特定关键字，来找出可能的漏洞
 - 出于运行效率考虑，往往采取将目标站点镜像到本地、指定扫描条件、指定扫描细度等方法
 - 自动扫描脚本或工具往往由资深攻击者开发后在网络上共享，攻击者不需要太多的攻击知识就可以使用
 - 自动扫描具有很高的页面处理速度，因此对Web站点的安全性构成极大的威胁
- **Web盗窃通过正常的Web访问来试图寻找漏洞，因此无法完全屏蔽**

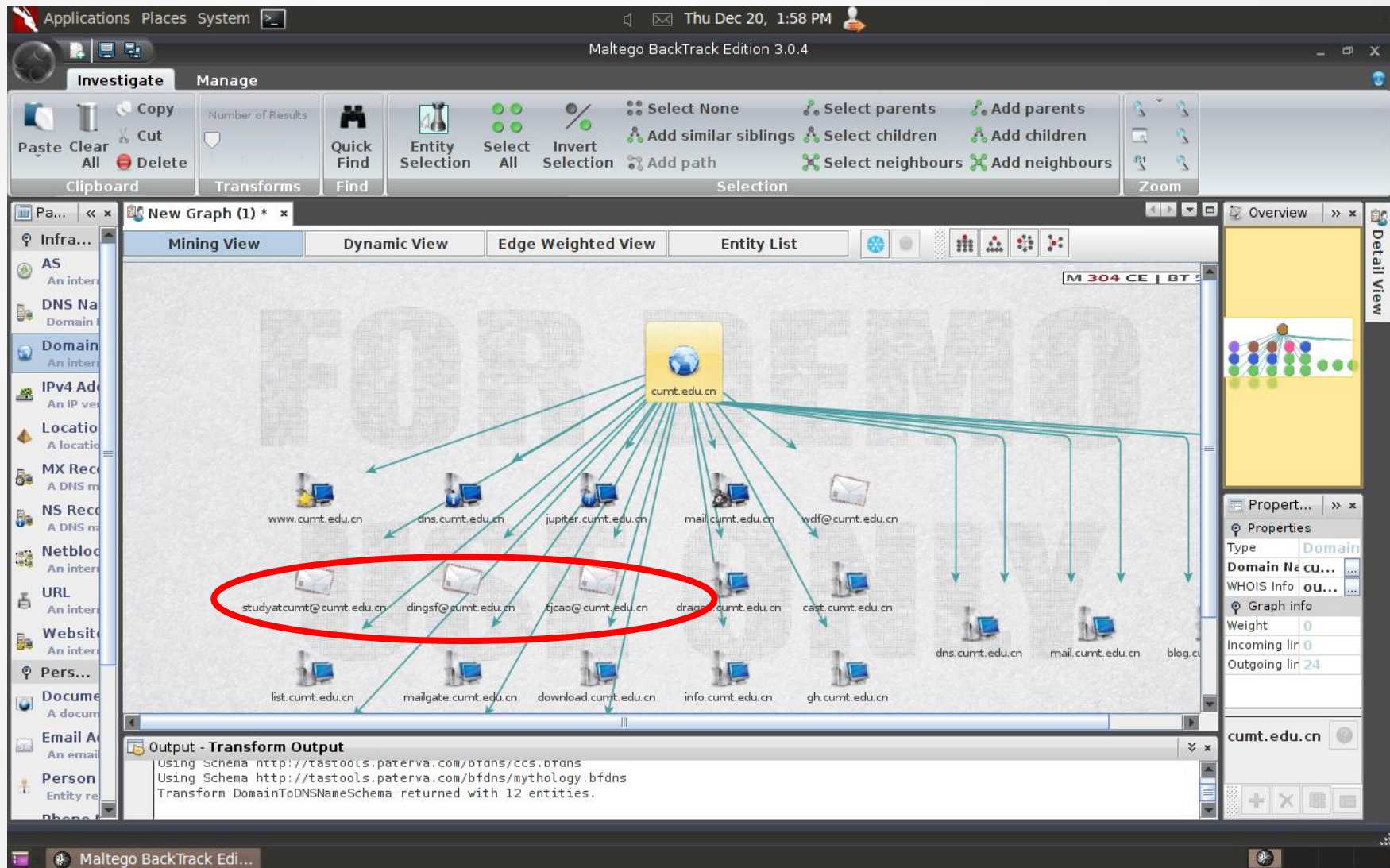
查点

- 一个“规范”的HTML代码

逐页扫描的不足：
效率太低

```
<script language=javascript><!--
  if (top.location != self.location)top.location=self.location;
// —>
</script>
<!--
' =====
' -----
' 转发时请保留此声明信息,这段声明不并会影响你的速度!
' ***** 凹丫丫网站管理系统 *****
' 作者:满载而归
' 网站:http://www.oyaya.cn
' 电子邮件:lovecswh@163.com
' 交流社区: http://www.oyaya.net
' = qq: 232706573
' =技术讨论: qq群号: 9994750
' 版权声明: 版权所有, 源代码公开, 各种用途均可免费使用, 但是修改后必须把修改后的文件
' 发送一份给作者. 并且保留作者此版权信息
' *****
' -----
' -----
--\
```


• 综合智能信息收集：maltego(BT5、KALI)



与联

- **漏洞扫描：**分析确认目标主机中可以被利用的漏洞

- ✓ **手动分析：**过程复杂、技术含量高、效率较低

- ✓ **自动分析：**人为干预过程少，效率高。如 **Nessus**、**OpenVAS**、**X-Scan**等综合型漏洞检测工具及专用扫描工具



- **Nessus:**

- ✓ 功能强大、简单易用的网络安全扫描工具，不可多得的审核堵漏工具
- ✓ 2000/03/06年，Nmap发起“**Top 50 Security Tools**”、“**Top 75 Security Tools**”、“**Top 100 Security Tools**”评选活动，Nessus“战胜”众多的商业化漏洞扫描工具而三次夺魁
- ✓ **黑客的血滴子，网管的百宝箱**
- ✓ **工作原理:** 通过插件模拟黑客攻击，对目标系统进行攻击性的安全漏洞扫描，如测试弱口令等。若模拟攻击成功，则表明目标主机系统存在安全漏洞
- ✓ 可完成多项安全工作，如扫描选定范围内的主机的端口开放情况、提供的服务、是否存在安全漏洞等

- **Nessus:**

- ✓ **免费(对个人用户)**

- ✓ 基于多种安全漏洞的扫描，避免扫描不完整的情况

- ✓ **插件体制**：扩展性强，支持及时的在线升级，可以扫描自定义漏洞或者最新安全漏洞

- ✓ **客户端/服务端机制**：容易使用、功能强大

- 主机扫描技术

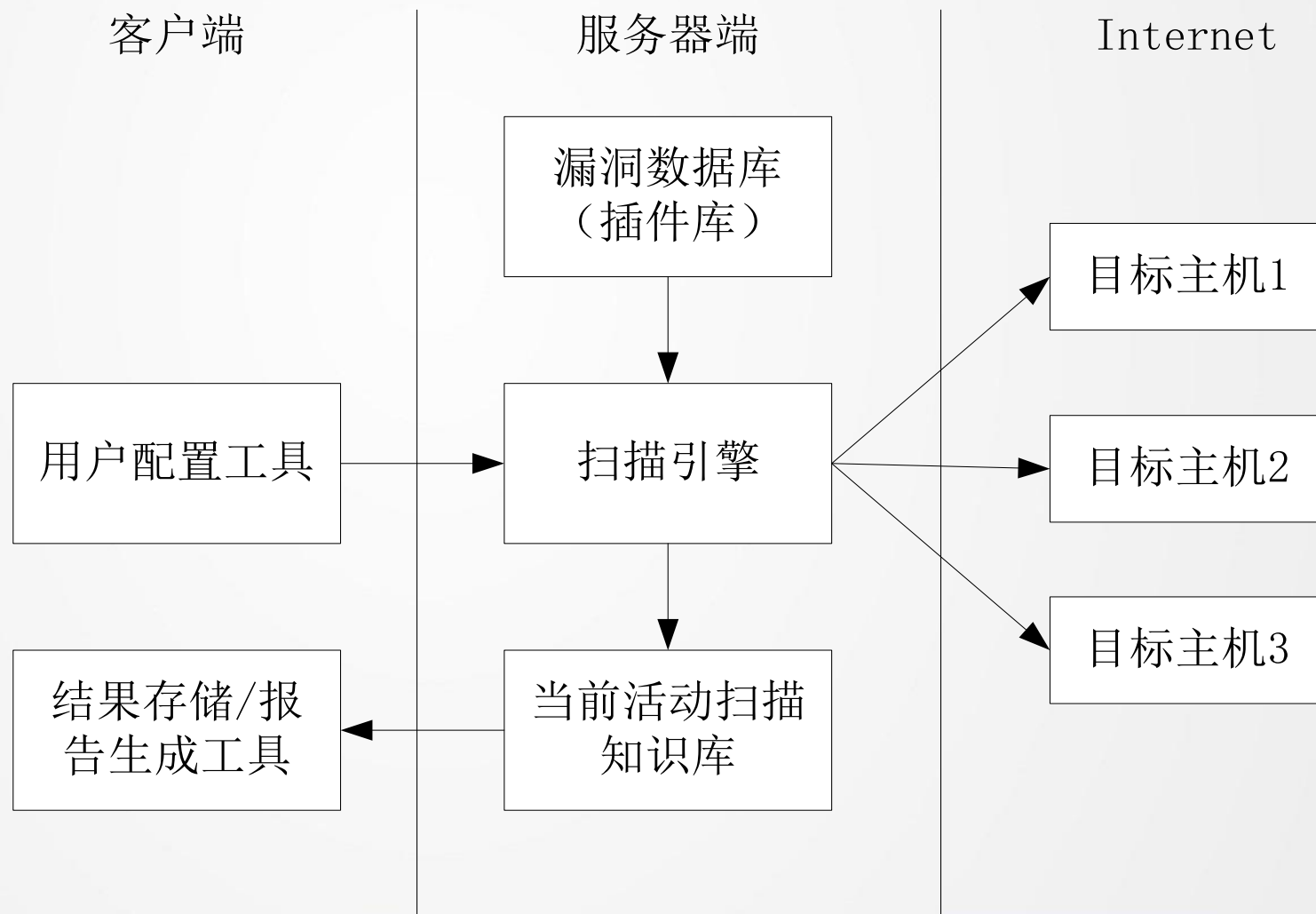
- 端口扫描技术

- 远程主机OS识别

- **漏洞扫描技术**

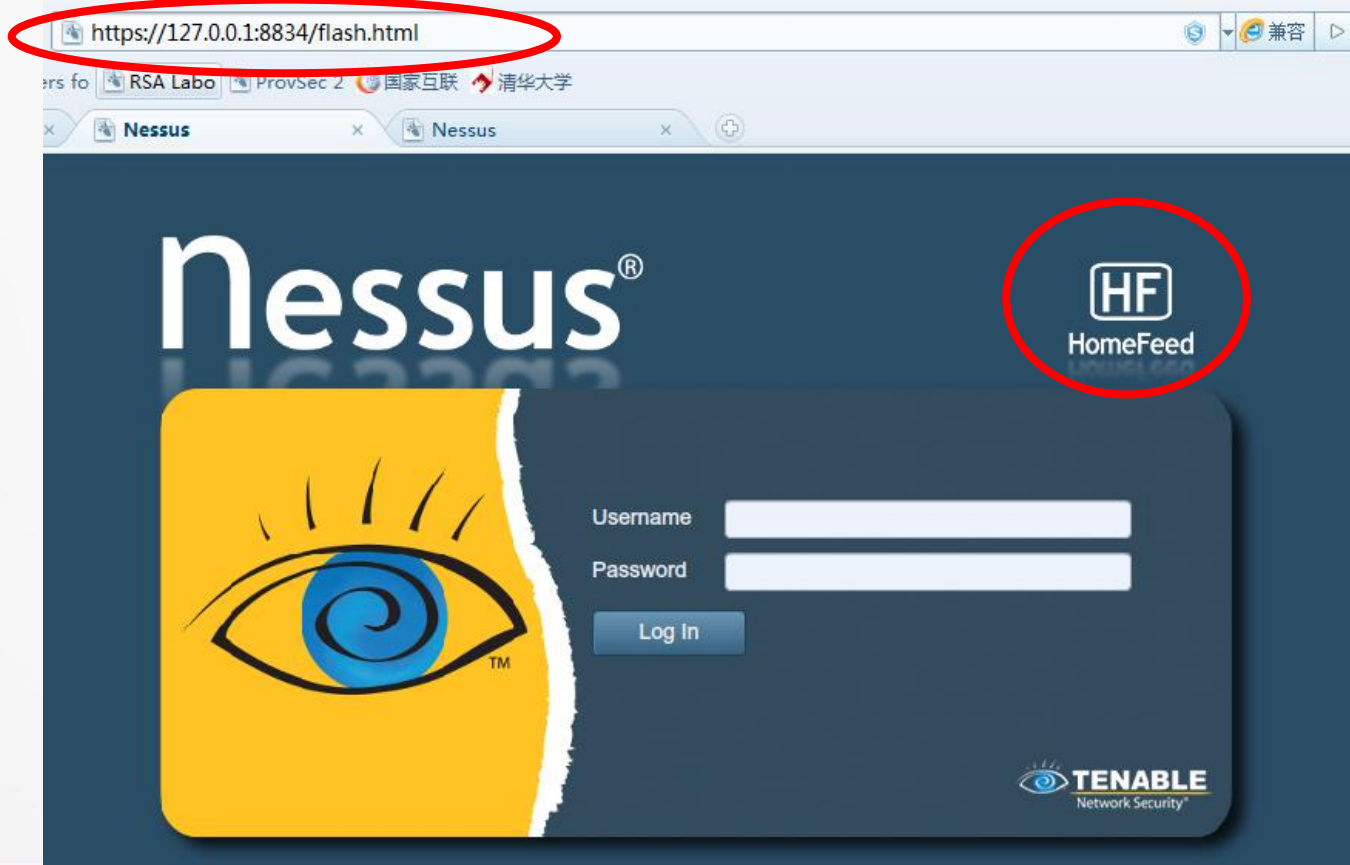
- ◆ 自带上万个扫描插件

- Nessus的结构:

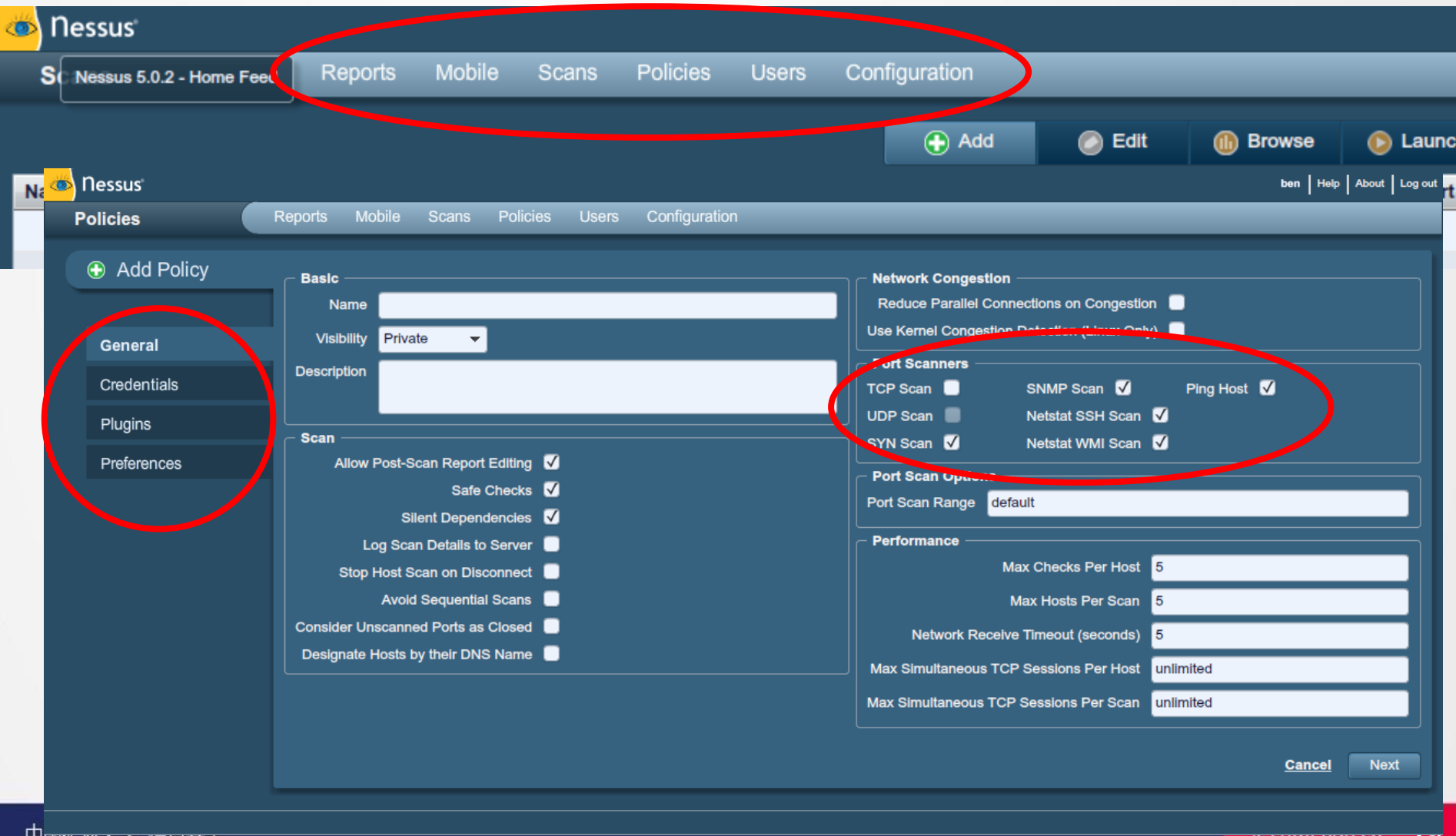


- **Nessus使用:**

- C/S模式，安装完成后在URL中输入：
https://[server IP]:8834/
进入Nessus的GUI界面

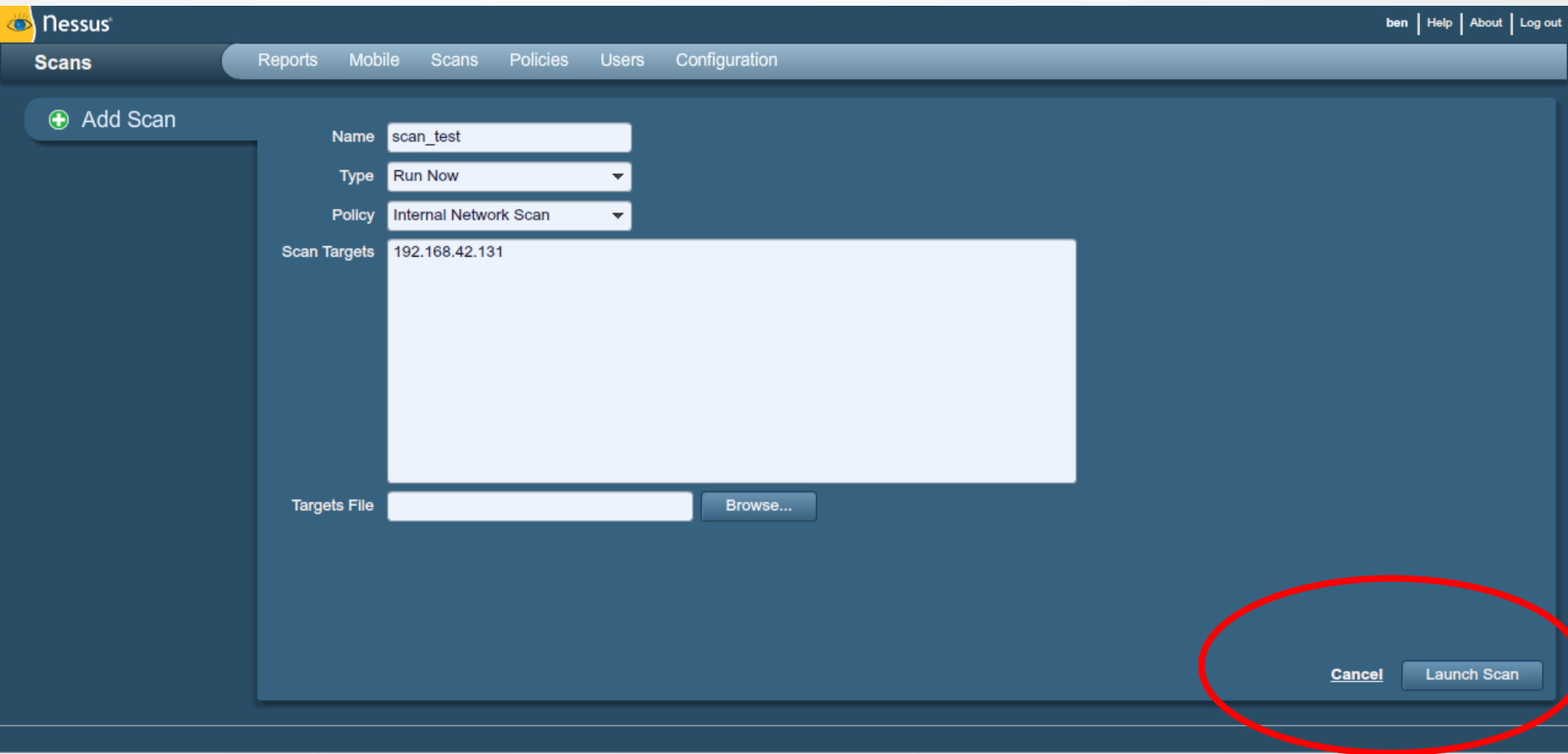


- 登录成功后，进入



The screenshot shows the Nessus 5.0.2 - Home Feed interface. The top navigation bar includes links for Reports, Mobile, Scans, Policies, Users, and Configuration. The left sidebar contains links for Add Policy, General, Credentials, Plugins, and Preferences. The main content area displays the 'Add Policy' form, which is divided into several sections: Basic, Network Congestion, Port Scanners, Port Scan Options, and Performance. The 'Port Scanners' section is highlighted with a red circle, showing options for TCP Scan, UDP Scan, SYN Scan, SNMP Scan, Netstat SSH Scan, Netstat WMI Scan, and Ping Host. The 'Performance' section shows settings for Max Checks Per Host, Max Hosts Per Scan, Network Receive Timeout (seconds), Max Simultaneous TCP Sessions Per Host, and Max Simultaneous TCP Sessions Per Scan. The 'Basic' section includes fields for Name, Visibility, and Description. The 'Scan' section includes checkboxes for Allow Post-Scan Report Editing, Safe Checks, Silent Dependencies, Log Scan Details to Server, Stop Host Scan on Disconnect, Avoid Sequential Scans, Consider Unscanned Ports as Closed, and Designate Hosts by their DNS Name. The 'Network Congestion' section includes checkboxes for Reduce Parallel Connections on Congestion and Use Kernel Congestion Detection (Linux Only). The 'Port Scan Options' section includes a field for Port Scan Range. The 'Performance' section includes fields for Max Checks Per Host, Max Hosts Per Scan, Network Receive Timeout (seconds), Max Simultaneous TCP Sessions Per Host, and Max Simultaneous TCP Sessions Per Scan. The interface also includes a 'Cancel' button and a 'Next' button at the bottom right.

- 扫描:



The image shows the Nessus Scans interface. At the top, there is a navigation bar with the Nessus logo and links for Reports, Mobile, Scans, Policies, Users, and Configuration. Below this, there is a sidebar with a '+ Add Scan' button. The main area contains a form for creating a new scan. The form has the following fields:

- Name: scan_test
- Type: Run Now (dropdown menu)
- Policy: Internal Network Scan (dropdown menu)
- Scan Targets: 192.168.42.131 (text area)
- Targets File: (text input field) with a Browse... button

At the bottom right of the form, there are two buttons: Cancel and Launch Scan. The Launch Scan button is circled in red.

- 查看扫描报告:

Nessus

ben | Help | About | Log out

Reports

Reports | Mobile | Scans | Policies | Users | Configuration

Nessus

ben | Help | About | Log out

Reports

Reports | Mobile | Scans | Policies | Users | Configuration

xp2 Vulnerability Summary | Host Summary

Completed: Nov 21, 2012 18:48

Download Report

Remove Vulnerability | Audit Trail

Filters

No Filters

+ Add Filter

Clear Filters

Plugin ID	Count	Host	Port
33822	2	192.168.42.131	80 / tcp
10678	2	192.168.42.131	443 / tcp
11213	2		
26920	1		
26928	1		
31705	1		
42873	1		
45411	1		
51192	1		
57582	1		
57608	1		
11219	7		
22964	5		
10107	2		

Plugin ID: 33822

Port / Service: www (80/tcp)

Severity: High

Plugin Name: XAMPP Example Pages Detection

Synopsis

The remote web server allows access to its example pages.

Description

The remote web server makes available example scripts from XAMPP, an easy-to-install Apache distribution containing MySQL, PHP, and Perl. Allowing access to these examples is not recommended since some are known to disclose sensitive information about the remote host and others may be affected by vulnerabilities such as cross-site scripting issues. Additionally, some pages have known cross-site scripting, SQL injection, and local file inclusion vulnerabilities.

Solution

Consult XAMPP's documentation for information about securing the example pages as well as other applications if necessary.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

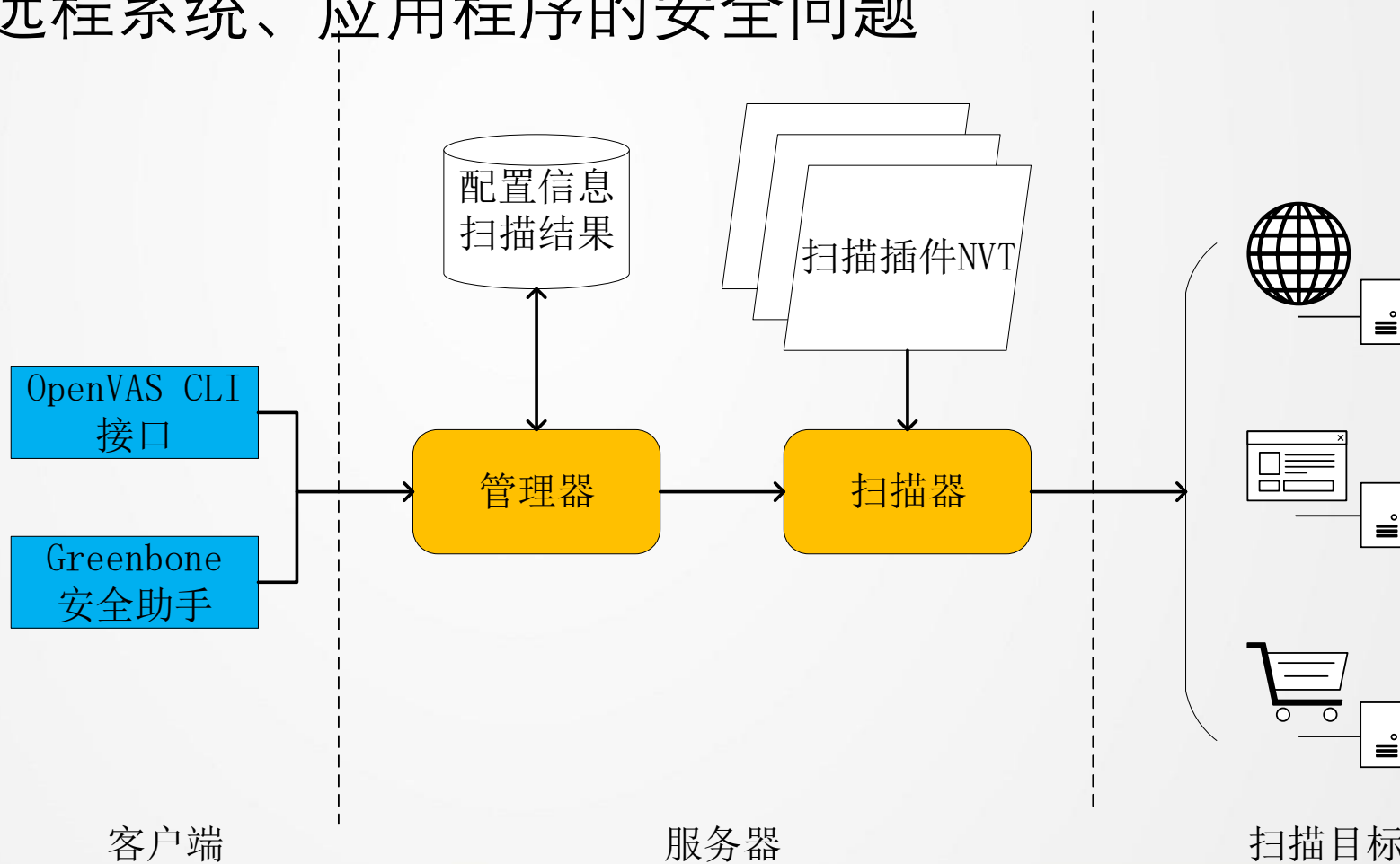
Plugin Output

Nessus was able to access XAMPP's examples using the following URL :

中国矿业大学 信息安全

is.cumt.edu.cn 41

- **OpenVAS:** 开放式漏洞评估系统，网络扫描器。核心是一个服务器，包括一套网络漏洞测试程序，可以检测远程系统、应用程序的安全问题



http:// Result Details ? [Menu] [Download]

Task: Immediate scan of IP 192.168.202.130 ID: e67a4486-91f7-42c3-a8e3-e793ac5fc3aa

Vulnerability	Severity	QoD	Host	Location	Actions
Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Remote	10.0 (High)	98%	192.168.202.130	445/tcp	[Details] [Star]

Summary
This host is missing a critical security update according to Microsoft Bulletin MS09-001.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation could allow remote unauthenticated attackers to cause denying the service by sending a specially crafted network message to a system running the server service. Impact Level: System/Network

Solution
Solution type: VendorFix

Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, <http://www.microsoft.com/technet/security/bulletin/ms09-001.msp>

Affected Software/OS
Microsoft Windows 2K Service Pack 4 and prior. Microsoft Windows XP Service Pack 3 and prior. Microsoft Windows 2003 Service Pack 2 and prior.

Vulnerability Insight
The issue is due to the way Server Message Block (SMB) Protocol software handles specially crafted SMB packets.

Vulnerability Detection Method
Details: [Vulnerabilities in SMB Could Allow Remote Code Execution \(958687\) - Remote \(OID: 1.3.6.1.4.1.25623.1.0.900233\)](#)
Version used: \$Revision: 3183 \$

References
CVE: [CVE-2008-4114](#), [CVE-2008-4834](#), [CVE-2008-4835](#)
BID: 31179
Other: <http://www.milw0rm.com/exploits/6463>

Navigation:

- Scan M
 - Task
 - New
 - Note
 - Over
 - Perf
- Config
 - Scan
 - Targ
 - Cred
 - Ager
 - Esca
 - Sche
 - Repe
 - Slav
- Admin
 - User

Buttons: [X] [Download]

NeXpose

EN ▼ Blog Support Contact Sign In

RAPID7

Products ▼

Services ▼

Partners ▼

Research

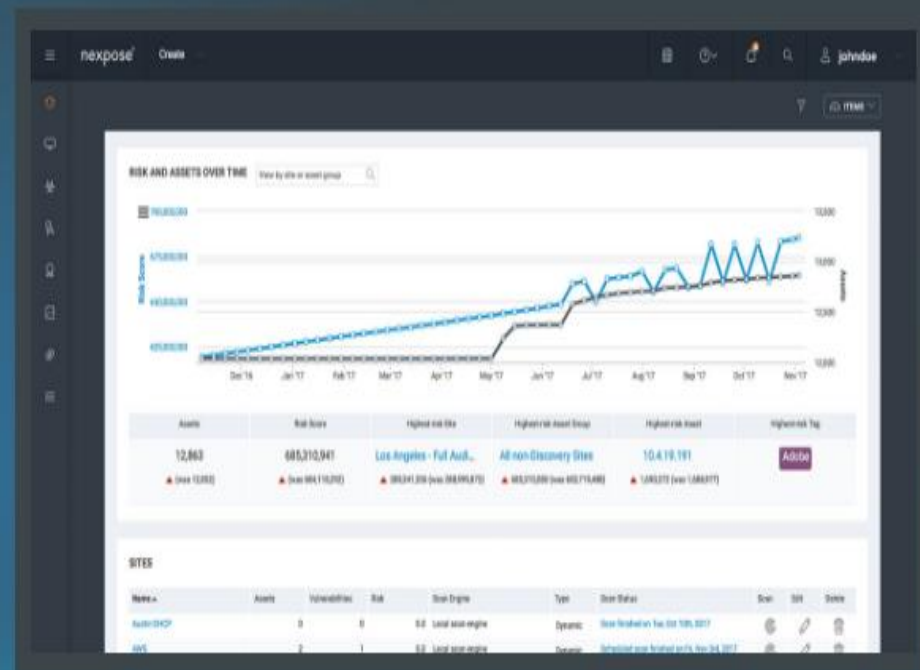
FREE TRIAL

Home | Products | Nexpose

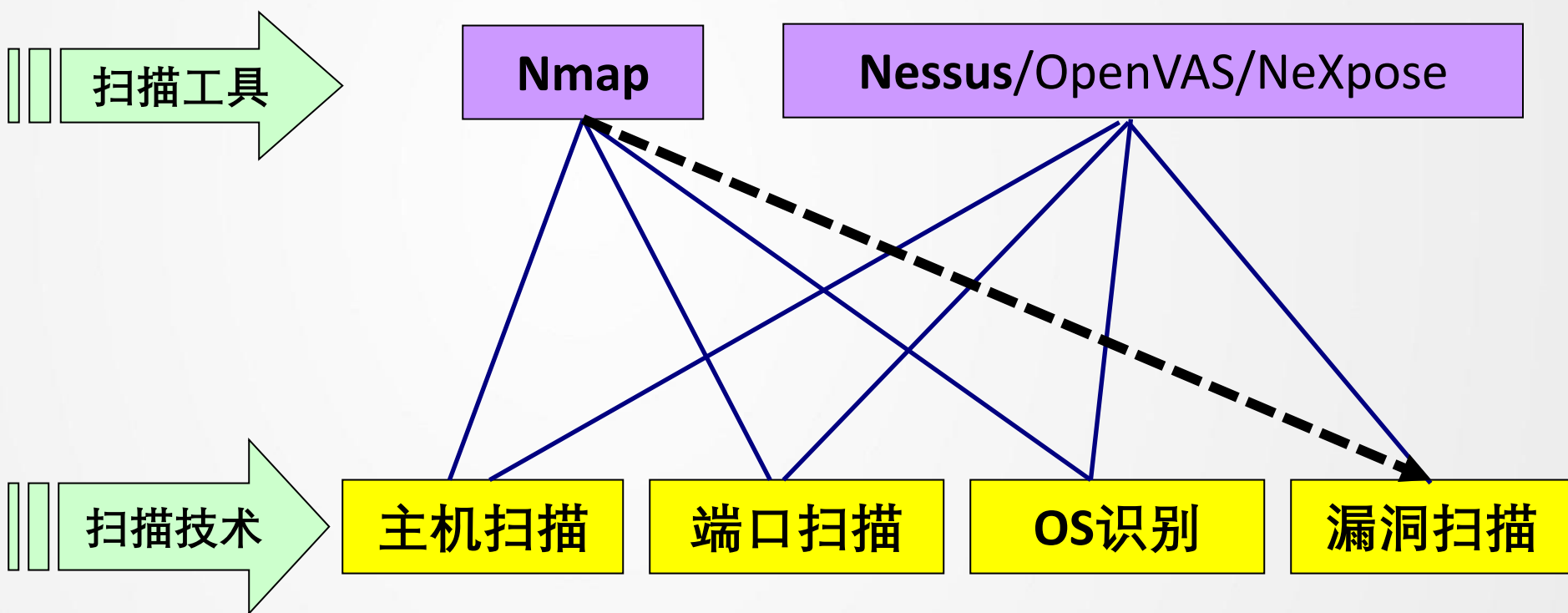
nexpose

Your on-prem vulnerability scanner

GET STARTED



常用扫描工具比较



- **端口扫描监测：**

- ✓（最简单） **在某个不常用的端口进行监听**：如发现对该端口的连接请求，就认为有端口扫描。一般这些工具都会对连接请求的来源进行反探测，同时弹出提示窗口

- ✓ **混杂模式下抓包（wireshark）** 并进一步分析判断

- ✓ **蜜罐系统（Honeypot）**

- **审计技术 (Auditing) :**

- ✓ 使用系统记录下的**使用时间、敏感操作和违纪操作**等，为系统进行事故原因查询、事故发生后的实时处理提供详细可靠的依据或支持
- ✓ 记录网络连接的请求、返回等信息，从中识别出扫描行为
- ✓ **如：**Web服务器的**日志记录**能帮助跟踪客户端IP地址，确定其地理位置信息，检测访问者所请求的路径和文件，了解访问状态，检查访问者使用的浏览器版本和操作系统类型等

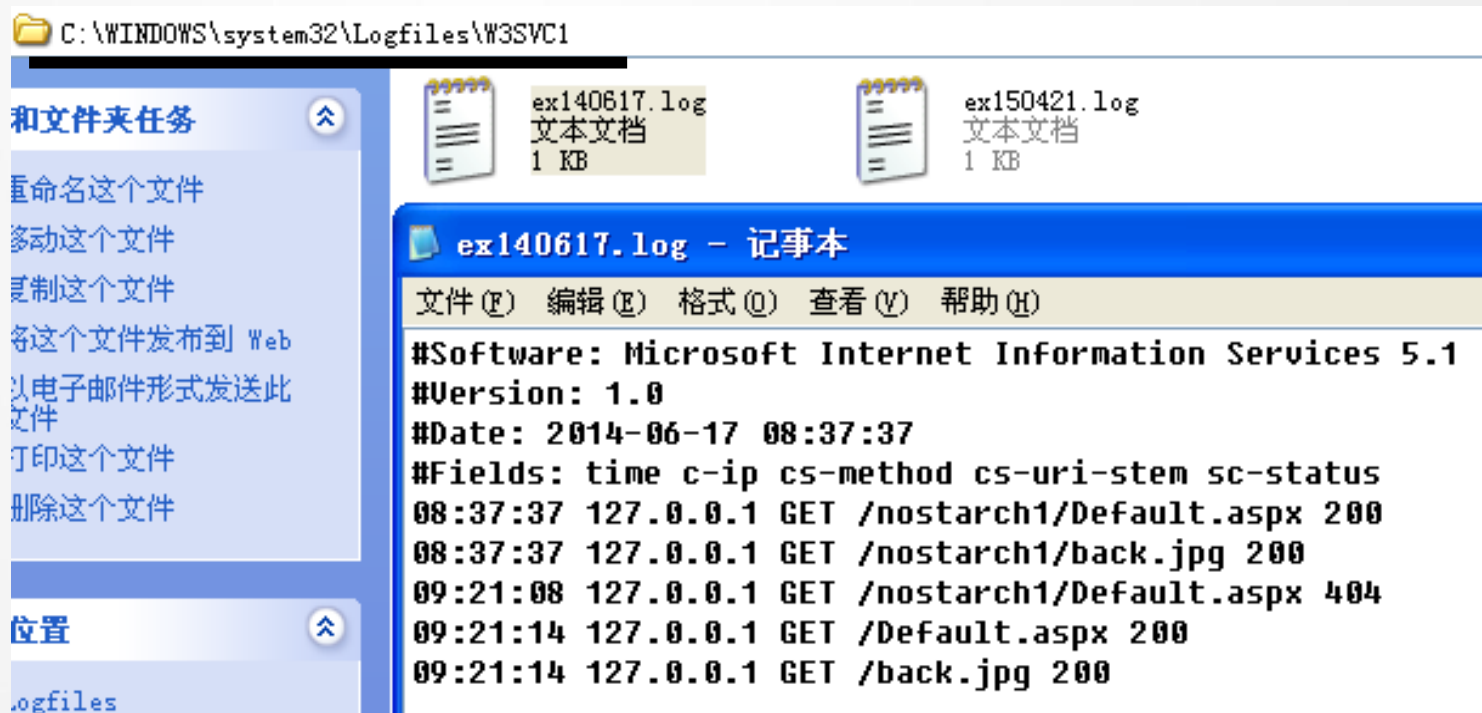
扫描的防御

• 审计技术例—IIS服务器的日志记录:

✓“%SystemRoot%/System32/LogFiles”目录存放关于WWW、FTP、SMTP等服务的日志目录

□WWW服务的日志目录: **W3SVCn**, “n”表示第n个WWW网站 (虚拟主机)

□FTP服务的日志目录: **MSFTPSVCn**



- IIS服务器的日志格式：
 - ✓ Microsoft IIS Log File Format (IIS日志文件格式, 一个固定的ASCII格式)
 - ✓ NCSA Common Log File Format (NCSA通用日志文件格式)
 - ✓ **W3C Extended Log File Format (W3C扩展日志文件格式, 可让用户设置的ASCII格式, 默认格式)**
 - ✓ ODBC Logging
- 日志文件一般记录对方IP地址、使用的HTTP方法、URI资源及其传递的CGI参数字符串等信息。通常设置使用W3C Extended Log File Format, 可以记录更多更细致的信息, 有助于更好的审计入侵行为

扫描的防御

- **审计技术举例—Apache服务器的日志记录：**

- ✓默认情况下，Apache会使用两个标准的日志文件：

- access_log**：所有对Apache Web服务器访问的活动记录

- error_log**：运行期间所有的状态诊断信息，包括对Web服务器的错误访问记录

- 一般在**/usr/local/apache/logs**目录下

```
bitsec@ubuntu:/opt/lampp/logs$ ls
access_log  error_log  php_error_log  ssl_request_log
```


- 扫描：目标系统是否存活、端口扫描、OS探测
 - ping、nmap
 - 端口扫描原理/OS探测技术
- 查点：旗标抓取/漏洞扫描等
 - telnet、natcat、maltego、Nessus、OpenVAS、NeXpose

- **网络监听(网络嗅探、Network Sniffing)**: 在他方未察觉的情况下捕获其通信报文、通信内容的技术
- 对**网络攻击与防范**双方都有重要意义, 是一把**双刃剑**
 - ✓ **网络管理员**: 了解网络运行状况的有力助手
 - ✓ **黑客**: 有效收集信息的手段
- 网络监听技术的能力范围**只限于局域网**



- **网卡的工作模式:**

1. **广播模式(Broadcast Mode):** 网卡能够接收网络中的广播信息
2. **组播模式(Multicast Mode):** 网卡能够接收组播数据
3. **单播模式(Unicast Mode):** 只接收目的地址匹配本机MAC地址的数据帧
4. **混杂模式(Promiscuous Mode, 监听模式):** 网卡接收一切数据帧, 无论其目的MAC地址是什么

• 例：用Wireshark嗅探163邮箱密码

Microsoft [Wireshark 1.6.5 (SVN Rev 40429 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
48	2.675069	49.68.54.181	220.181.75.116	TCP	62	slm-api > http [ACK] Seq=1 Ack=1 win=17
49	2.676048	49.68.54.181	220.181.75.116	TCP	1478	[TCP segment of a reassembled PDU]
50	2.676168	49.68.54.181	220.181.75.116	HTTP	218	POST /login.jsp?type=1&url=http://entry
51	2.712178	220.181.75.116	49.68.54.181	TCP	62	http > slm-api [ACK] Seq=1 Ack=1417 win=

p%3A%2F%2Fmail.163.com%2Ferrorpage%2Ferr_163.htm&username=netsecur&password=cumt123456&selType=-1

Offset	Hex	ASCII
0000	e0 24 7f 93 c2 af 00 26 c7 60 43 6c 88 64 11 00	.\$.....& .`cl.d..
0010	60 89 00 c6 00 21 45 00 00 c4 14 90 40 00 40 06!E.@.@.
0020	95 81 31 44 36 b5 dc b5 4b 74 06 46 00 50 99 06	..1D6... Kt.F.P..
0030	75 7a 57 68 2f 94 50 18 10 e0 ad c9 00 00 76 65	uzwh/.P.ve
0040	72 69 66 79 63 6f 6f 6b 69 65 3d 31 26 73 74 79	rifycook ie=1&sty
0050	6c 65 3d 2d 31 26 70 72 6f 64 75 63 74 3d 6d 61	le=-1&pr oduct=ma
0060	69 6c 31 36 33 26 73 61 76 65 6c 6f 67 69 6e 3d	il163&sa velogin=
0070	26 75 72 6c 32 3d 68 74 74 70 25 33 41 25 32 46	&url2=ht tp%3A%2F
0080	25 32 46 6d 61 69 6c 2e 31 36 33 2e 63 6f 6d 25	%2Fmail. 163 .com%
0090	32 46 65 72 72 6f 72 70 61 67 65 25 32 46 65 72	%2Ferrorp age%2Fer
00a0	72 5f 31 36 33 2e 68 74 6d 26 75 73 65 72 6e 61	r_163.ht m&userna
00b0	6d 65 3d 6e 65 74 73 65 63 75 72 26 70 61 73 73	me=netse cur&pass
00c0	77 6f 72 64 3d 63 75 6d 74 31 32 33 34 35 36 26	word=cum t123456&
00d0	73 65 6c 54 79 70 65 3d 2d 31	selType= -1

- 交换式局域网的监听技术：

- 溢出攻击

- 交换机要维护一张MAC地址与端口的映射表（CAM）
 - 维护该表的内存有限。如用大量的错误MAC地址的数据帧对交换机进行攻击，交换机就可能出现溢出
 - 交换机就回到**广播方式**——向所有的端口发送数据包（**ARP过载, MAC泛洪**）

- **ARP欺骗**（欺骗章节详细介绍）

- 计算机维护一个IP-MAC地址对应表，该表随**ARP请求/响应**不断更新
 - **ARP欺骗**：改变表里的对应关系，攻击者成为被攻击者与交换机之间的“中间人”，使交换式局域网中的所有数据包都流经攻击者的网卡



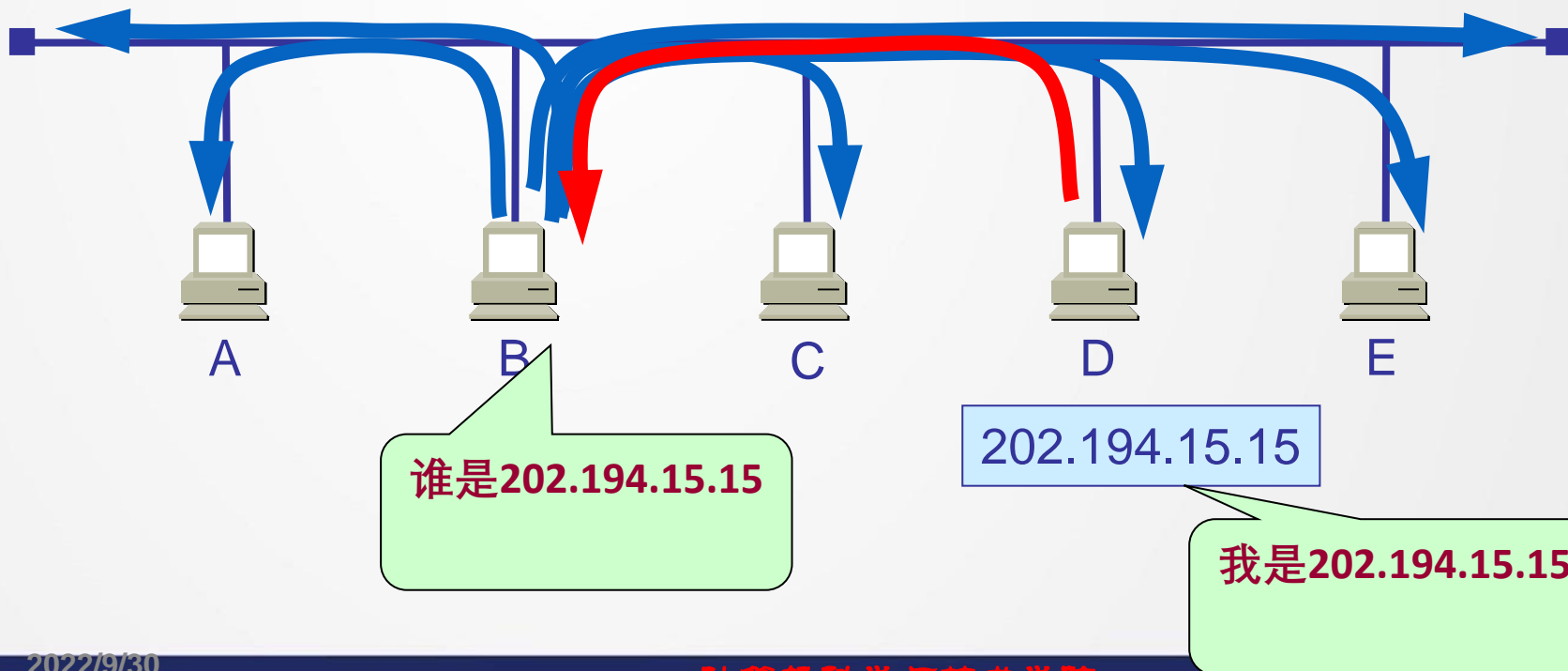
ARP基础知识

- ARP(Address Resolution Protocol): 地址解析协议, 用于将IP地址 (32位) 转化为网卡的物理地址 (MAC地址 48位), 属于数据链路层的协议。
- 在以太网中, 数据帧从一个主机到达局域网内的另一台主机是根据48位的以太网地址 (MAC地址) 来确定的, 而不是根据IP地址。

- ARP地址解析的工作原理:

IP地址 $\xrightarrow{\text{ARP}}$ MAC地址

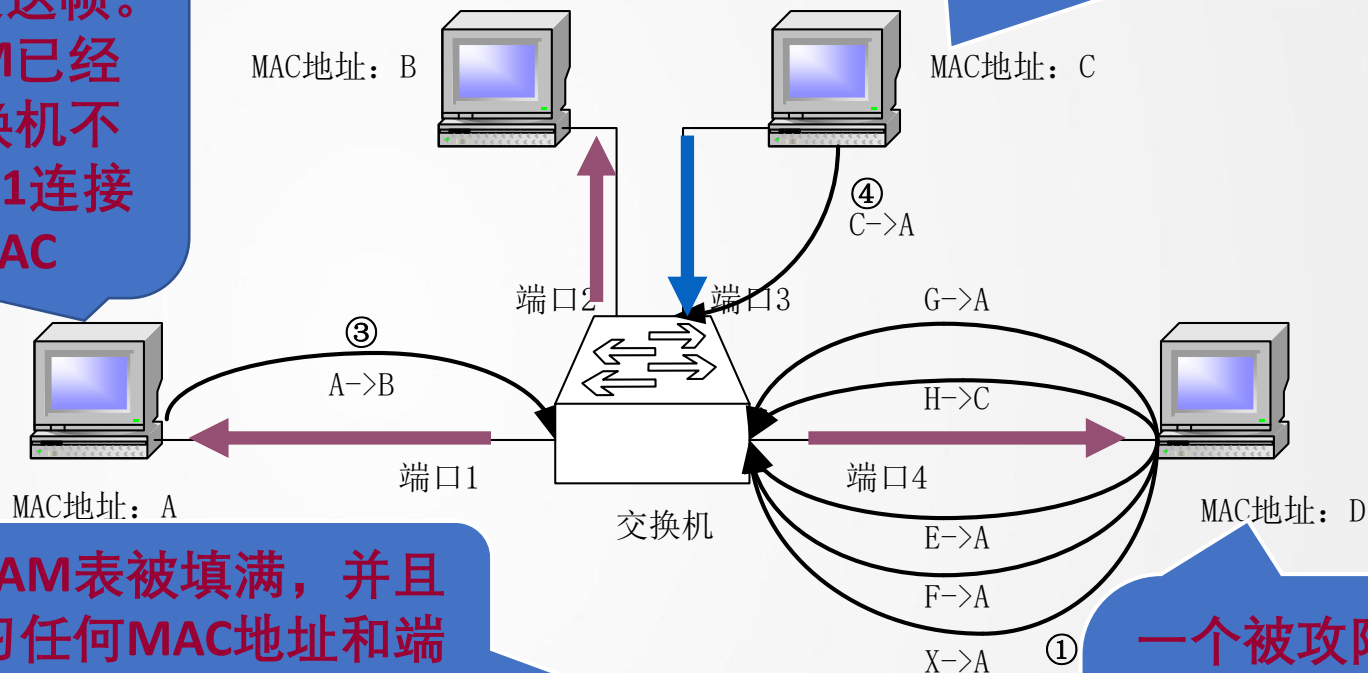
建立在网络互相信任的基础上



MAC泛洪

A向B主机发送帧。
但因为CAM已经
填满，交换机不
能学习端口1连接
的A的MAC

C给A发送一个帧，但是交换机的
CAM表中没有A的地址，所以交
换机泛洪到所有端口



交换机的CAM表被填满，并且
不能再学习任何MAC地址和端
口映像

一个被攻陷的主机连接端口4.来源
于G、H、E和F的假MAC地址
的帧和真MAC地址D的帧在端
口4发送

端口	MAC地址
1	A
2	B
3	C
4	D

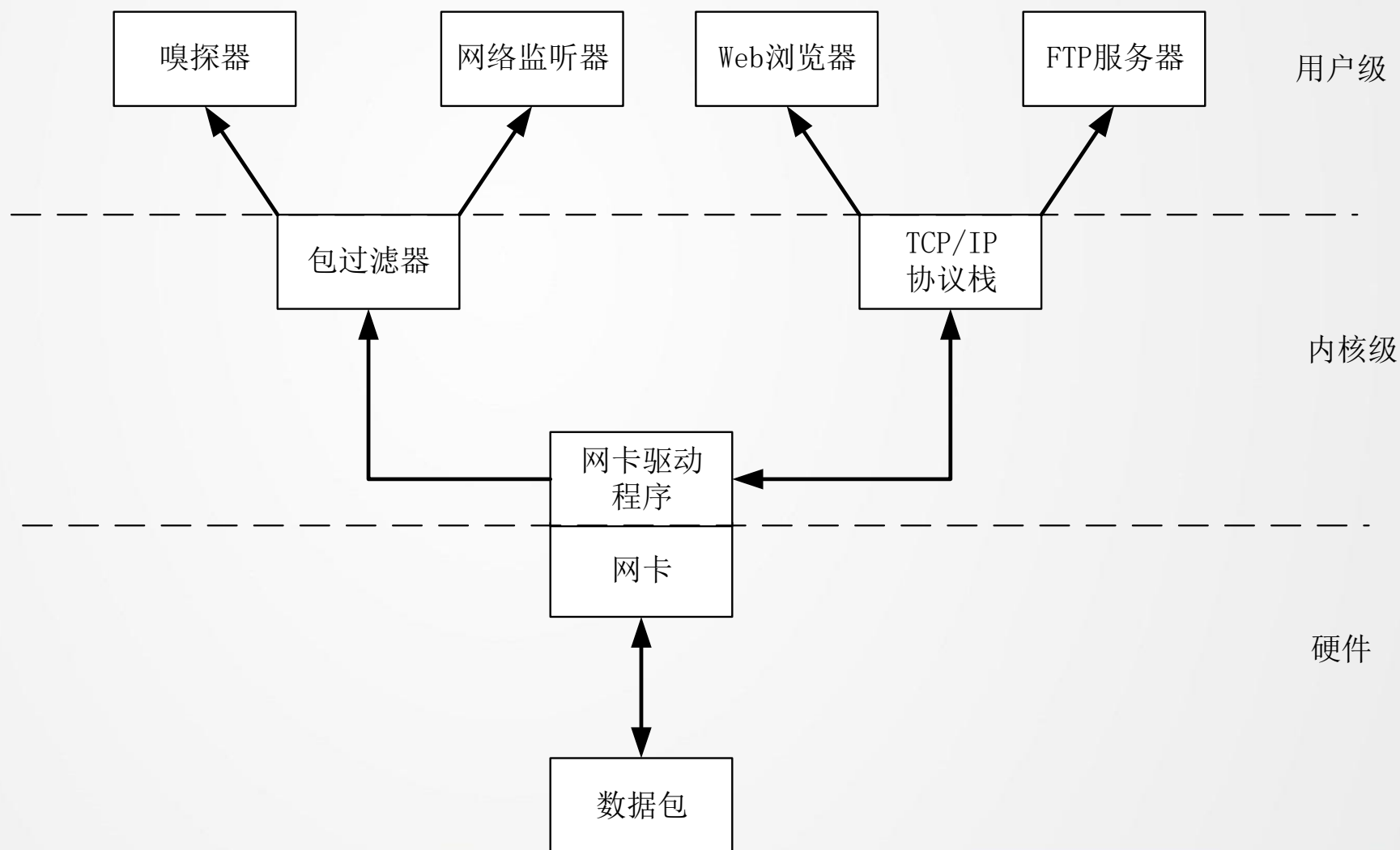
②攻击后

端口	MAC地址
4	D
4	G
4	H
4	E
4	F
4	X

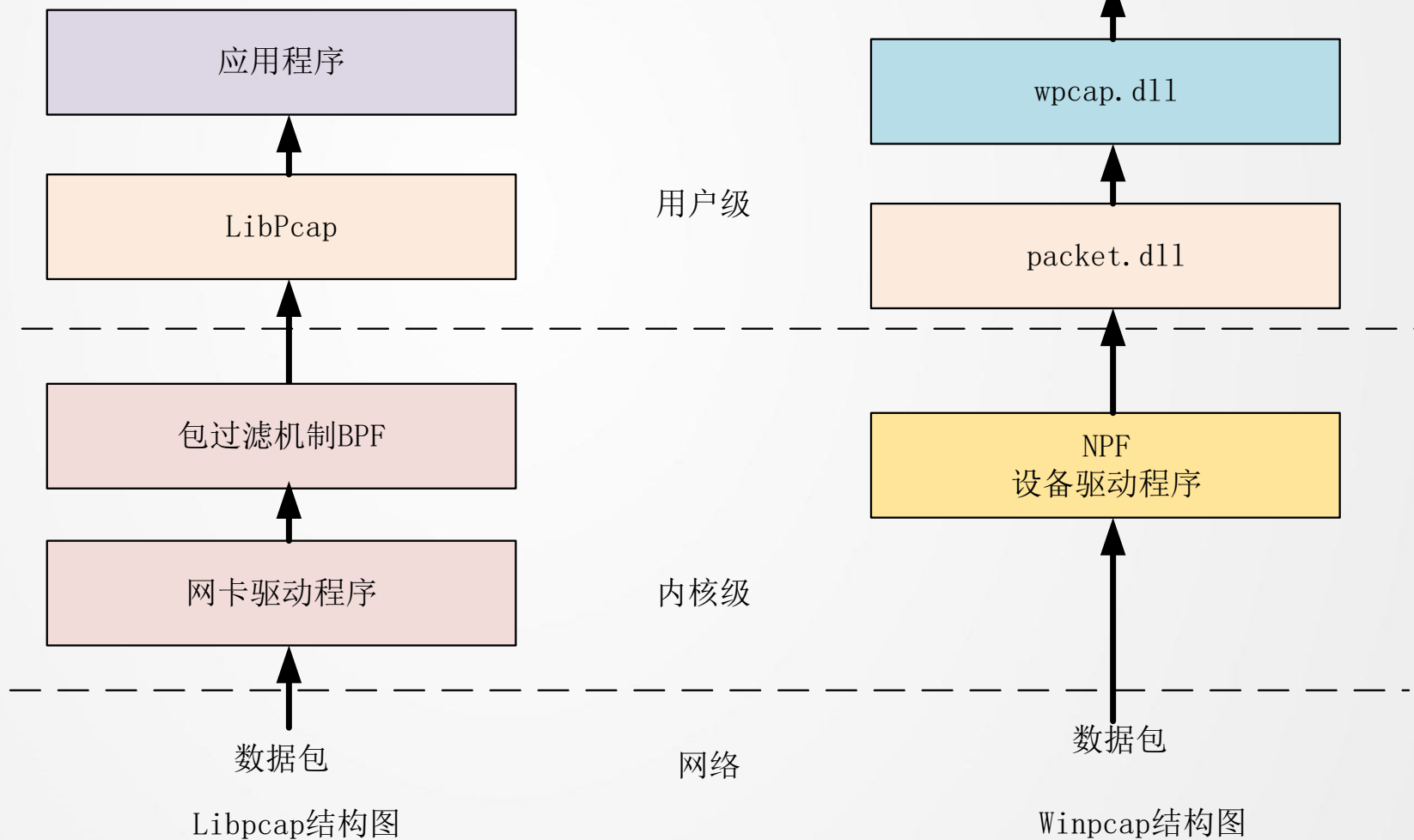
• 嗅探的工作机制:

- ✓ **驱动程序支持**: 直接与网卡驱动程序接口的驱动模块, 作为网卡驱动与上层应用的“中间人”, 将网卡设置成**混杂模式**, 捕获数据包并从上层接收各种抓包请求
- ✓ **分组捕获过滤机制**: 对来自网卡的数据帧进行过滤, 将符合要求的数据交给上层
 - 网卡上传的数据帧有两个去处: **正常的协议栈**或**分组捕获过滤模块**, 对于非本地的数据包, 前者会丢弃, 后者则根据上层应用要求来决定是否丢弃
 - 许多操作系统都提供分组捕获机制:
 - ◆ **UNIX类型的OS**中主要有3种:
 - BSD系统中的BPF(Berkeley Packet Filter)
 - SVR4中的DLPI(Data Link Interface)
 - Linux中的SOCK_PACKET类型套接字
 - ◆ **Windows平台**上主要有NPF过滤机制

• 共享式局域网的监听实现方法：



• 相关开发库:





- ❖ **开发库libpcap**：对开发者而言，网卡驱动程序和BPF捕获机制是透明的，需要掌握的是libpcap库的使用
- ❖ libpcap隐藏了用户程序和操作系统内核交互的细节，完成如下工作：
 - 向用户程序提供一套功能强大的抽象接口
 - 根据用户要求生成过滤指令
 - 管理用户缓冲区
 - 负责用户程序和内核的交互

- **基于Windows系统的WinPcap**

- 比libpcap多一些功能，如WinPcap可以发送数据，但libpcap不行

□WinPcap的架构：

- **内核级的数据包监听设备驱动程序NPF：**把设备驱动增加在Windows，直接从数据链路层取得网络数据包不加修改地传递给应用程序，也允许用户发送原始数据包
- **低级动态链接库packet.dll：**运行在用户层，把应用程序和数据包监听设备驱动程序隔离开，使得应用程序可以不加修改地在不同Windows系统上运行
- **高级系统无关库Wpcap.dll：**和应用程序编译在一起，它使用低级动态链接库提供的服务，向应用程序提供完善的监听接口，不同Windows平台上的高级系统无关库是相同的

- 使用Winpcap的流程

打开网卡接口，设置为混杂模式

Pcap_open_live

设置过滤器(捕获前过滤)

Pcap_setfilter

捕获数据

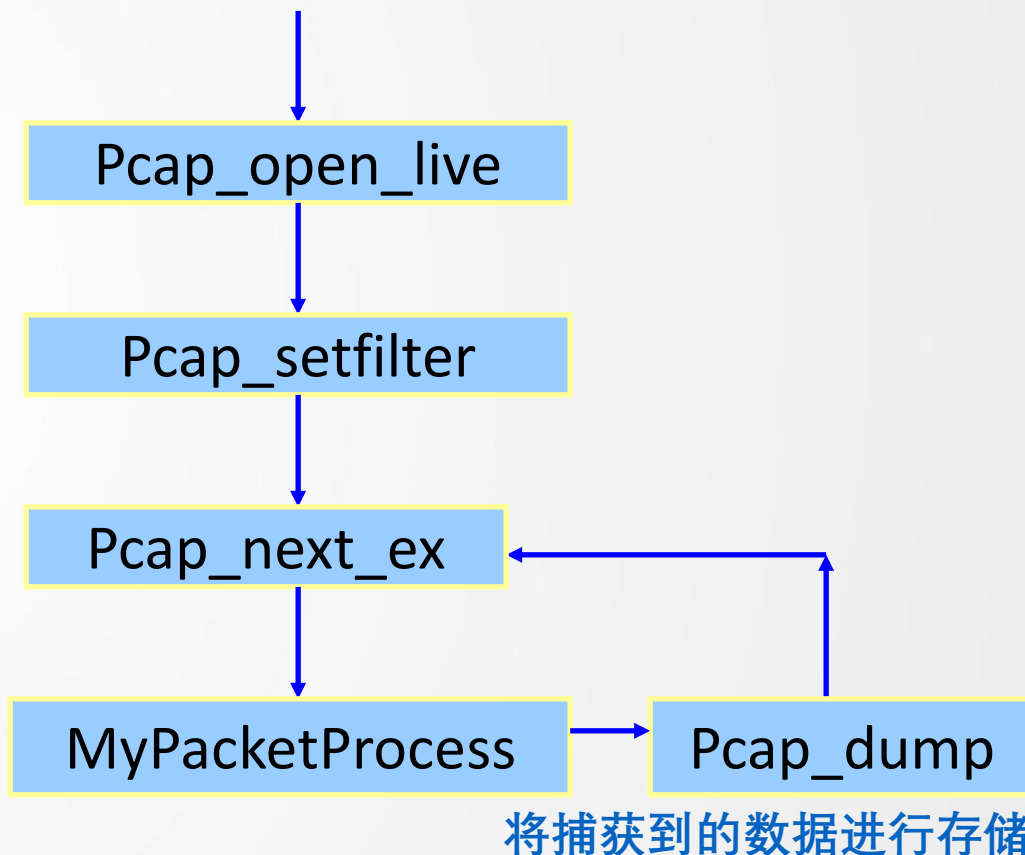
Pcap_next_ex

对捕获到的数据进行处理

MyPacketProcess

Pcap_dump

将捕获到的数据进行存储



• 常用的网络监听工具

✓ Wireshark

- ❑ 免费开源的网络数据包分析工具，可在Linux、Solaris、Windows等多平台运行
- ❑ 允许从网络中捕捉数据包并进行分析，详细探究数据包的协议字段信息和会话过程
- ❑ 很好的可扩展性，能自由地增加插件以实现额外功能
- ❑ 支持多种通讯接口（如Ethernet、Token-ring、X.25等）及数据包协议类型（如ARP、TCP、UDP等），可以组合TCP上的封包且显示出以ASCII或是EBCDIC型态的数据（TCP Stream），捕获的封包可以被存储
- ❑ 支持Capture Filter（捕获前过滤）和Display Filter（捕获后过滤）功能

✓ Tcpdump/Windump

过滤表达式

Wireshark · 显示过滤器表达式

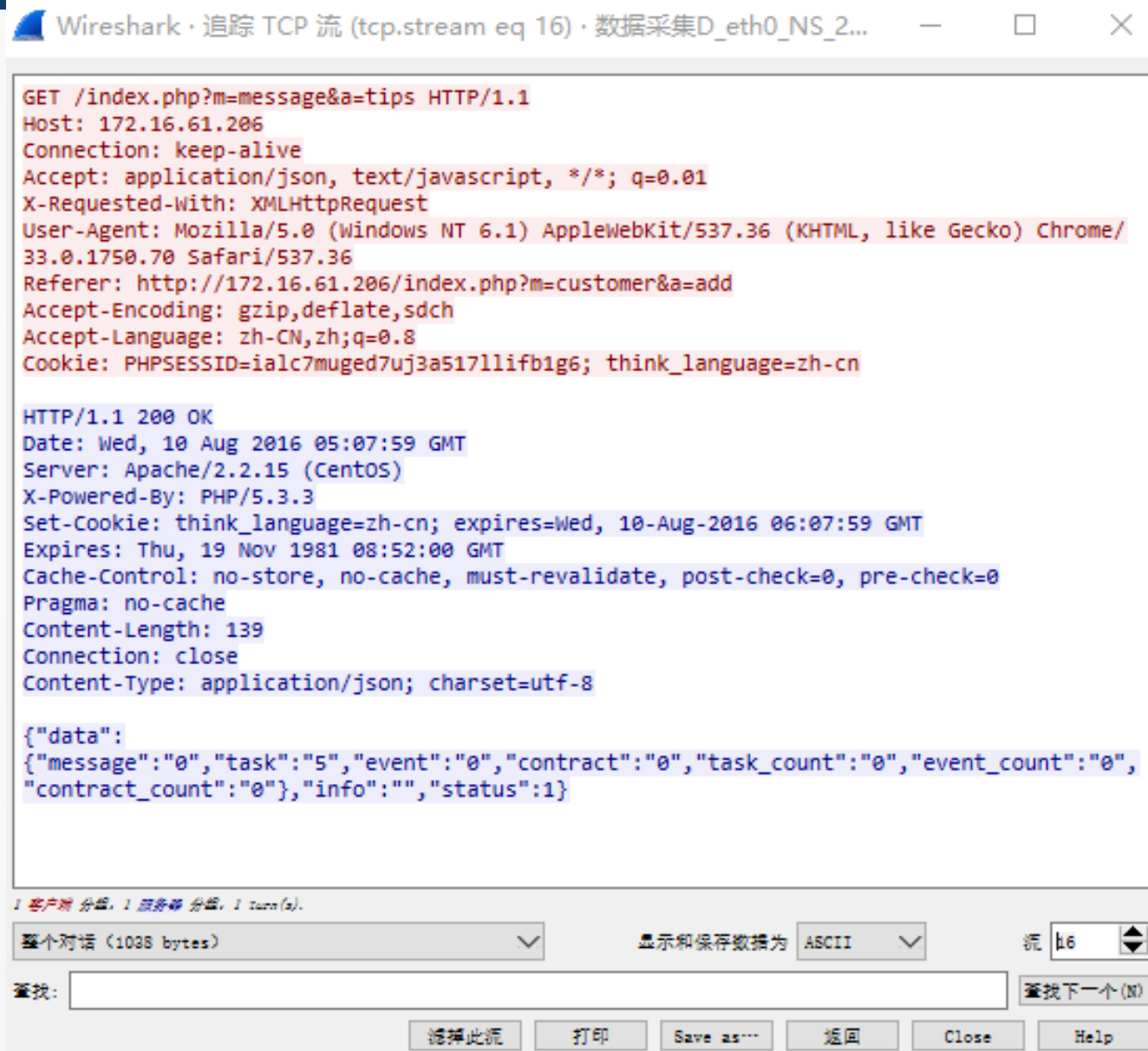
字段名称	关系	值 (IPv4 address)	预定义的值	范围 (偏移:长度)
ip.addr	==	192.168.10.99		

ip.addr == 192.168.10.99

点击确定插入此过滤器



追踪TCP流





网络监听及防御技术

协议统计分析

Wireshark · 协议分级统计 · 流量中的线索

协议	按分组百分比	分组	按字节百分比	字节	比特/秒	End Packets	End Bytes	End Bits
▼ Frame	100.0	212	100.0	107506	35 k	0	0	0
▼ Ethernet	100.0	212	2.8	2968	978	0	0	0
Link Layer Discovery Protocol	0.5	1	0.3	318	104	1	318	104
▼ Internet Protocol Version 6	0.5	1	0.1	131	43	0	0	0
▼ User Datagram Protocol	0.5	1	0.0	8	2	0	0	0
DHCPv6	0.5	1	0.1	83	27	1	83	27
▼ Internet Protocol Version 4	97.6	207	3.9	4140	1365	0	0	0
▼ User Datagram Protocol	28.8	61	0.5	488	160	0	0	0
Wireless Session Protocol	0.5	1	0.0	5	1	1	5	1
Simple Service Discovery Protocol	3.3	7	0.7	707	233	7	707	233
Domain Name System	25.0	53	3.2	3463	1141	53	3463	1141
▼ Transmission Control Protocol	68.9	146	88.4	95007	31 k	133	90378	29 k
Secure Sockets Layer	4.2	9	5.7	6160	2031	9	6160	2031
▼ Hypertext Transfer Protocol	1.9	4	81.1	87232	28 k	2	460	151
Line-based text data	0.9	2	80.4	86388	28 k	2	86586	28 k
Data	0.5	1	0.1	144	47	1	144	47
Address Resolution Protocol	0.9	2	0.1	56	18	2	56	18

无显示过滤器。

Close

复制

Help



常用的网络监听工具

tcpdump

```
root@kali:~# tcpdump
```

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

```
02:07:02.017488 IP6 fe80::d1aa:bec5:25dc:abab > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s), length 28  
02:07:02.017508 IP 192.168.238.1 > igmp.mcast.net: igmp v3 report, 1 group record(s)  
02:07:02.033908 IP6 fe80::d1aa:bec5:25dc:abab > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s), length 28  
02:07:02.034003 IP 192.168.238.1 > igmp.mcast.net: igmp v3 report, 1 group record(s)  
02:07:02.034359 IP6 fe80::d1aa:bec5:25dc:abab > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s), length 28  
02:07:02.034363 IP 192.168.238.1 > igmp.mcast.net: igmp v3 report, 1 group record(s)  
02:07:02.034499 IP6 fe80::d1aa:bec5:25dc:abab > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s), length 28  
02:07:04.368101 IP kali.41190 > gateway.domain: 32201+ PTR? 22.0.0.224.in-addr.arpa. (41)  
02:07:06.389665 IP kali.60302 > gateway.domain: 8662+ PTR? 2.238.168.192.in-addr.arpa. (44)  
02:07:06.392196 IP gateway.domain > kali.60302: 8662 NXDomain 0/1/0 (117)  
02:07:06.392319 IP kali.58991 > gateway.domain: 18938+ PTR? 135.238.168.192.in-addr.arpa. (46)
```

Mission（不需要提交）：

- 开发基于WinPcap的嗅探器，掌握嗅探器的工作原理，熟悉WinPcap的使用，掌握基于WinPcap网络嗅探器的开发过程
- 具体要求：
 - 了解基于libpcap、winPCap开发嗅探器的工作原理，编写网络监听程序，获取数据包，并对数据包进行解析

纸上得来终觉浅，绝知此事（hacking）要躬行

❖ 监听（被动技术，难以发现）的防御：

- ❖ 被动防御措施，如采用**安全的网络拓扑结构**和**数据加密技术**。
注意重点区域的安全防范
 - **网络分段**越细，嗅探器收集的信息越少。将网络分成一些小的网络，数据包只能在该网段内部被嗅探。嗅探器不能跨过的网络设备：**交换机、路由器**。网络分段需要昂贵的硬件设备，只适应于中小的网络
 - **VLAN**：使网络隔离不必要的数据传送，一般可采用20个工作站为一组，是比较合理的数字

- **监听的防御：**

- **数据通道加密：** 数据通过事先建立的加密通道进行传输，账号、口令等敏感信息将受到严密保护。主要有
 - **SSH** (Secure Shell)
 - **SSL** (Secure Socket Layer, 安全套接字应用层)
 - **VPN**
- **数据内容加密：** 采用被证实较为可靠的加密机制对传输的邮件和文件进行加密
 - **PGP**等

- **交换网络下防监听：**

- 主要防止ARP欺骗及ARP泛洪

- **交换网络下防范监听的措施主要包括：**

- 不要把信任关系建立在单一的IP或MAC基础上，理想的关系应该建立在IP-MAC的对应关系上
- 使用静态ARP或IP-MAC对照表代替动态的ARP或IP-MAC对应表——禁止自动更新，使用手动更新
- 定期检查ARP请求：使用ARP监视工具如ARPWatch等监视并探测ARP欺骗
- 制定良好的安全管理策略，加强用户安全意识



感谢聆听

中国矿业大学 网络空间安全系

is.cumt.edu.cn