企业秘密保护与陷阱网络

吴鲁加<wulujia@unnoo.com>

提纲

- 简单陷阱网络的构建与应用实例
- 企业／组织对秘密保护的要求
- 攻击路径假想
- 自防御型陷阱网络
- 总结与展望

用户需求与目标

- 需求
  - 服务器上保存有重要数据
  - 必须允许远程接入
  - 经常遇到大量扫描尝试
- 目标
  - 将进行扫描的 IP 地址屏蔽
  - 必要时研究该 IP 的址的目标

配置

- 工具
  - portsentry
  - rinetd
  - VMWare
- 思路
  - 默认启动 portsentry 对扫描行为进行监视
    - KILL_RUN_CMD=”/usr/sbin/rinetd”
  - 发现攻击企图后，启动 rinetd 转向 ViruteHoneynet
    - 0.0.0.0 1433 192.168.0.55 1433
    - logfile /var/log/rinetd.log

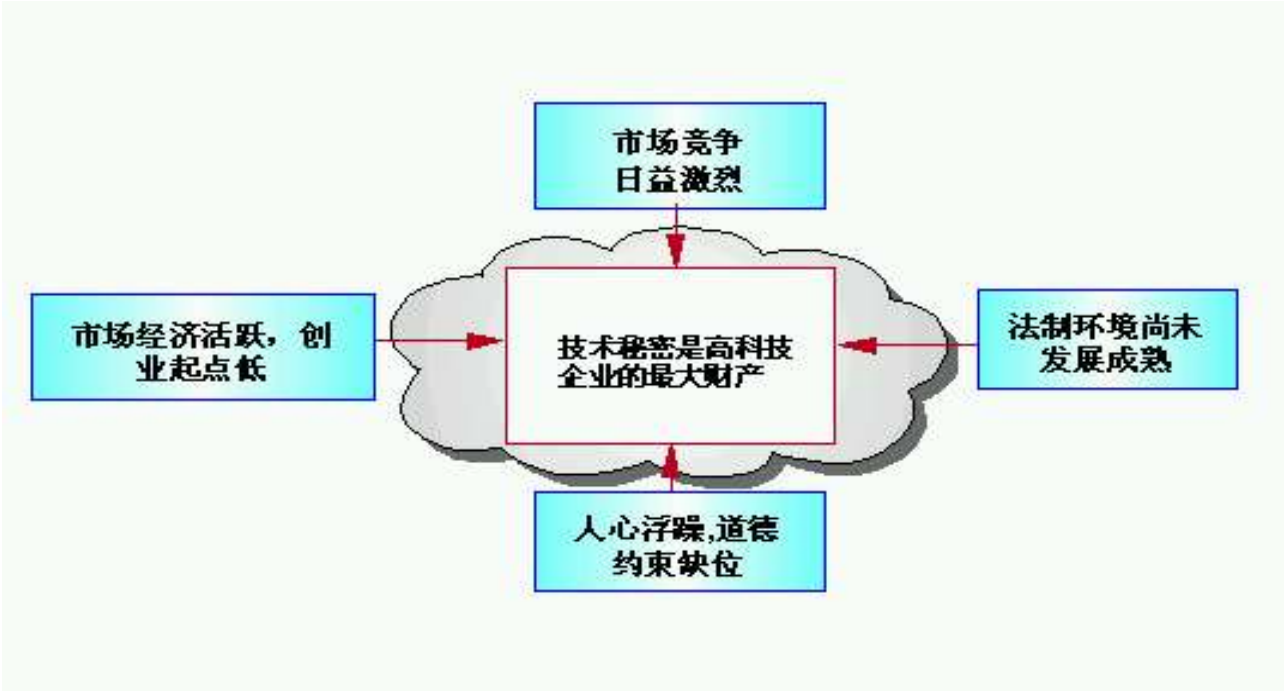
效果

- 攻击
  - 攻击者对 MSSQL 服务器进行攻击
  - sa 密码为 123456
- 记录
  - Portsentry、 rinetd 日志
  - MSSQL 操作日志
  - 截图

典型高科技企业的知识产权结构

- 金字塔结构
  - 专利权
  - 著作权
  - 商业秘密

企业技术秘密的窥视者


市场竞争
日益激烈
市场经济活跃，创
业起点低
技术秘密是高科技
企业的最大财产
法制环境尚未
发展成熟
人心浮躁,道德
约束缺位

技术秘密的保护标准

- 法律的要求：“权利人采取保密措施”
  - 保护标准：除非经权利人许可，否则他人不能以合法渠道获得
  - 保护基线：只需采取基本的、适度的保密措施即可，如保密协议、保密管理规定

- 管理的要求：他人不能从权利人获得
  - 保护标准：除非经权利人许可，否则他人不能获得
  - 保护基线：需要采取大量系统化的保护措施

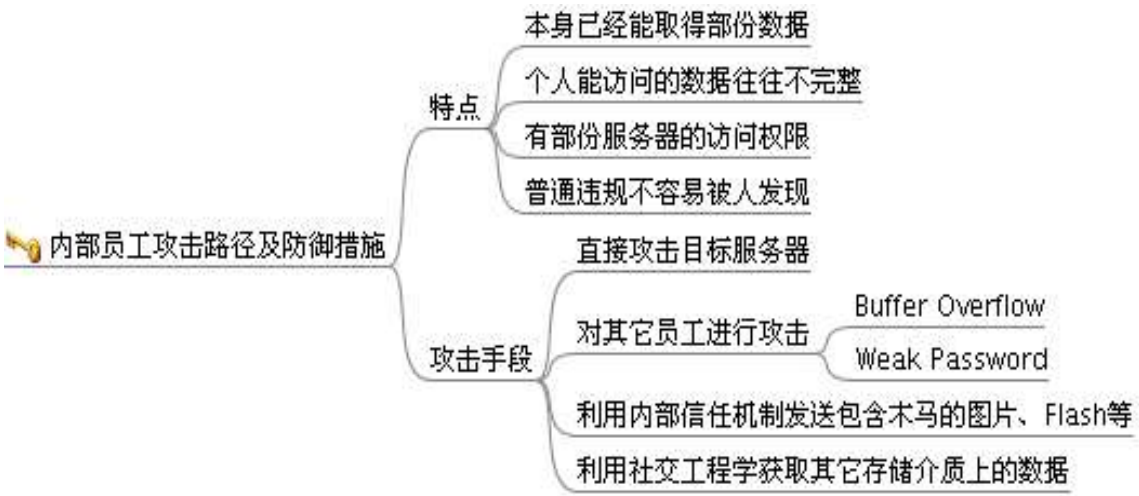
企业对技术秘密的保护要求

- 要求
  - 不该获得的人不能获得
  - 获得的人拿不出去
  - 拿出去的必然合法及合乎企业规范
  - 非法拿出去必须有痕迹
- 防护措施
  - 技术（我们的重心），陷阱网络能做到
    - 避免信息被“非法”获取
    - 减少信息被“骚扰”的机率
    - 保证“非法”获取有记录
  - 管理

外部黑客的攻击手段


外部黑客攻击路径及防御措施
特点
不了解企业网络
真正攻击前有大量尝试
攻击手段
缓冲区溢出
弱口令猜测
SQL注入
旁路攻击
同一机房的其它设备
同一域名旗下的其它主机
分支机构服务器
客户端攻击
浏览器
邮件客户端
即时聊天工具
OFFICE文档(MS & OO & SUN)
社交工程学

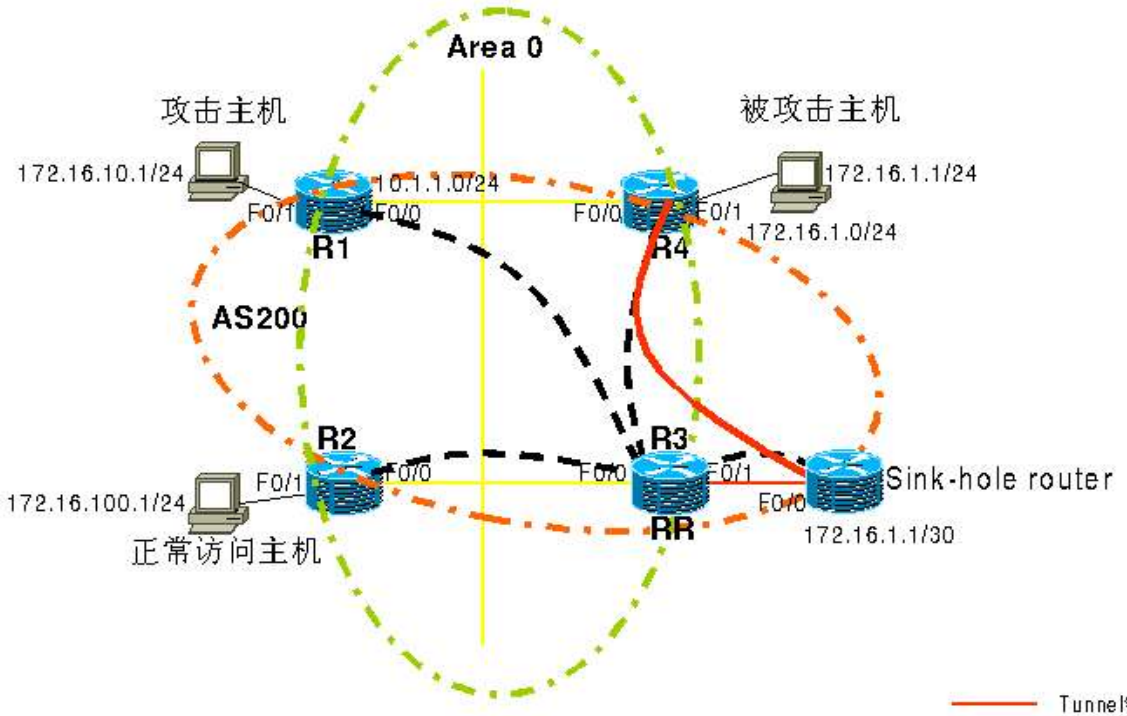
内部员工攻击手段


内部员工攻击路径及防御措施
特点
本身已经能取得部份数据
个人能访问的数据往往不完整
有部份服务器的访问权限
普通违规不容易被人发现
攻击手段
直接攻击目标服务器
对其它员工进行攻击
Buffer Overflow
Weak Password
利用内部信任机制发送包含木马的图片、Flash等
利用社交工程学获取其它存储介质上的数据

自防御型陷阱网络思路

- 从前面简单的 Honeypot 设置进一步设想
- 从各种 AntiDDoS 设备的宣传
  - 下水道路由

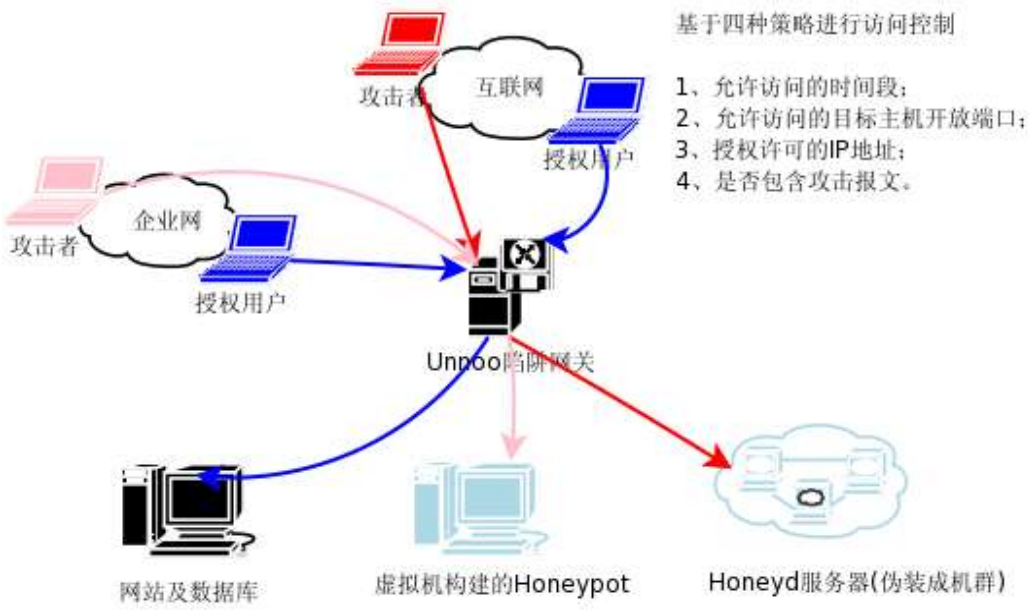
ADDN 网络抵御 DDoS 攻击



1、保证R4和sink-hole路由器之间的TUNNEL是通的。
2、sink-hole路由器不参加AS内部的IGP路由。只有到R3和R4的静态路由。
3、 sink-hole路由器参加AS200的IBGP路由。
4、我们假定R3充当BGP RR路由器。

来源：ADDN 网络抵御 DDoS 攻击（刘闻欢）

自防御型陷阱的基本设计



三个技术核心部份

- Unnoo 陷阱网关
- Honeyd 服务器构成的虚拟网络
- 虚拟机构成的 Honeypot 组

自防御型 NAT 陷阱网关的构成

- 策略控制
  - Snort 、 SnortSam
- NAT
  - iptables
- 数据分析
  - Sebek

基于时间的控制

- 主要应用范围
  - 保密单位
  - 访问策略可以按时间定义的网络
- 技术实现
  - crontab 添加及删除规则
- 应用特点
  - 内容级 Honeypot
  - 主要对象是内部“违规者”

虚拟机

- VMWare
- UML(UserModLinux)

基于协议和开放端口的控制

- 主要应用范围
  - 网络协议固定的单位（银行、证券、运营商等）
  - 前提是需要做好应用及端口管理
- 技术实现
  - iptables 直接将访问目标无效协议端口的数据 NAT 转发
- 应用特点
  - 网络级 Honeypot，可以与 Honeyd 结合应用
  - 主要对象是已经进入内部网络的“渗透者”

Honeyd(1)

```
create router
set router personality "Cisco 3000 Series VPN Concentrator"
set router default tcp action block
set router default udp action block
add router tcp port 23 "/usr/bin/perl scripts/cisco/router-telnet.pl"
bind 192.168.1.111 router
```

```
$ nmap -p 1-100 192.168.1.111 -O

Starting nmap 3.75 ( http://www.insecure.org/nmap ) at 2005-04-02
Warning:  OS detection will be MUCH less reliable because we did
Interesting ports on 192.168.1.111:
(The 99 ports scanned but not shown below are in state: filtered)
PORT    STATE SERVICE
23/tcp open  telnet
MAC Address: 00:0C:41:16:94:59
Aggressive OS guesses: Cisco 3000 Series VPN Concentrator (95%),
ft Windows XP Pro RC1+ through final release (91%), Cisco 3000-se
 3Com 4924 GigE Switch (90%), NetBSD 1.6.1 (Alpha) (90%), OpenBSD
%), Netopia DSL router (88%)
No exact OS matches for host (test conditions non-ideal).
```

Nmap Scan of Cisco

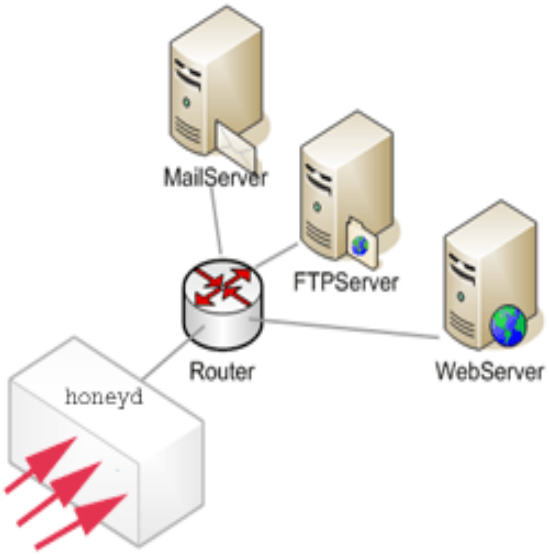
```
$ telnet 192.168.1.111
Trying 192.168.1.111...
Connected to 192.168.1.111.
Escape character is '^]'.
Welcome to rabbitHole.matrix.com cisco router!
PLEASE LOG OFF IF YOU ARE NOT AUTHORIZED TO USE
THIS SYSTEM!

Users (authorized or unauthorized) have no explicit or
implicit expectation of privacy.  Any or all uses of this
system may be monitored, inspected, copied, intercepted,
audited, recorded, and disclosed to authorized site.
By using this system, the user consents to such
monitoring, interception, recording, copying, auditing,
inspection, and disclosure at the discretion of authorized
site.
User Access Verification

Username: _
```

Telnet to fake Cisco Machine

honeyd(2)



基于 IP 地址的控制

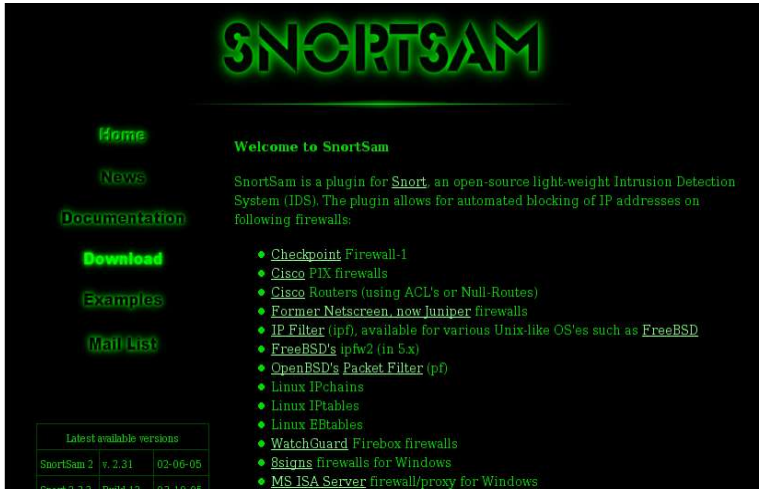
- 主要应用范围
  - 特定高安全级别的设备及网络，如网管
- 技术实现
  - 直接采用 iptables 设置 NAT 规则
- 应用特点
  - 应用对象是所有有意无意的“试探者”

基于扫描和攻击的访问控制

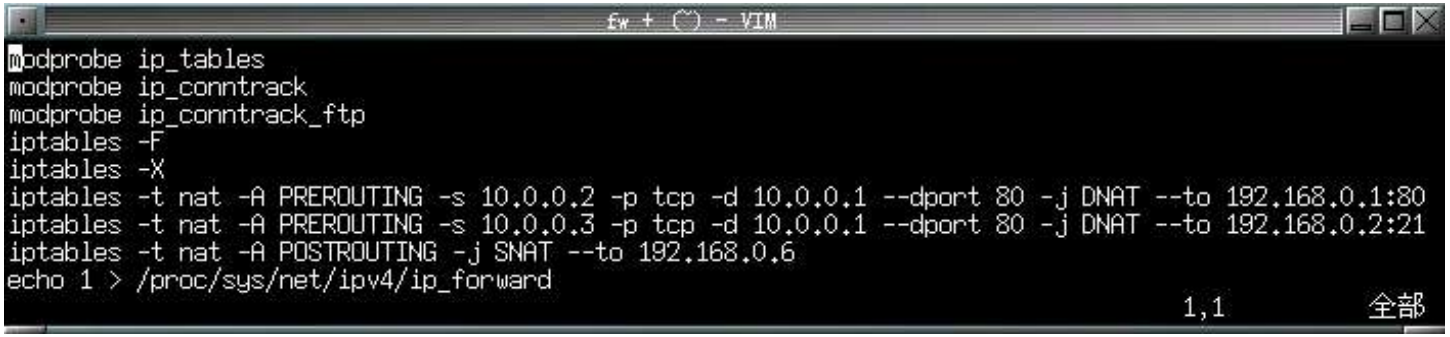
- 主要应用范围
  - 保密单位、实验机构等
  - 技术研究组织更倾向于研究这类型的攻击
- 技术实现
  - 发现工具
    - 扫描： portsentry
    - 攻击： Snort
  - 联动工具
    - SnortSam
- 应用特点
  - 应用对象是所有目的明确的“攻击者”

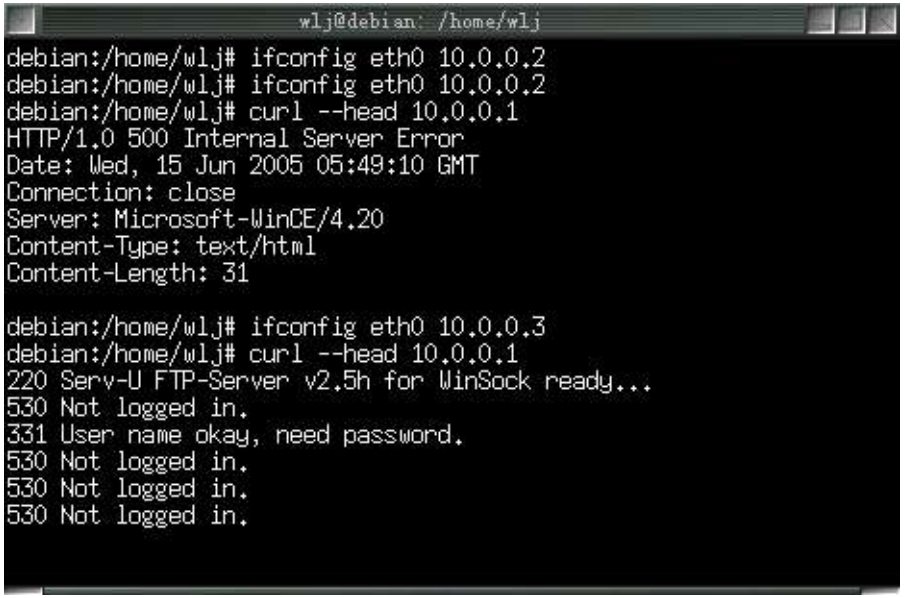
SnortSam 和 iptables

- SnortSam
  - ssp_iptables.c
  - 基于攻击报文的 NAT
  - 能够结合 Checkpoint 等
- iptables
  - 灵活高效，有大量的配置工具

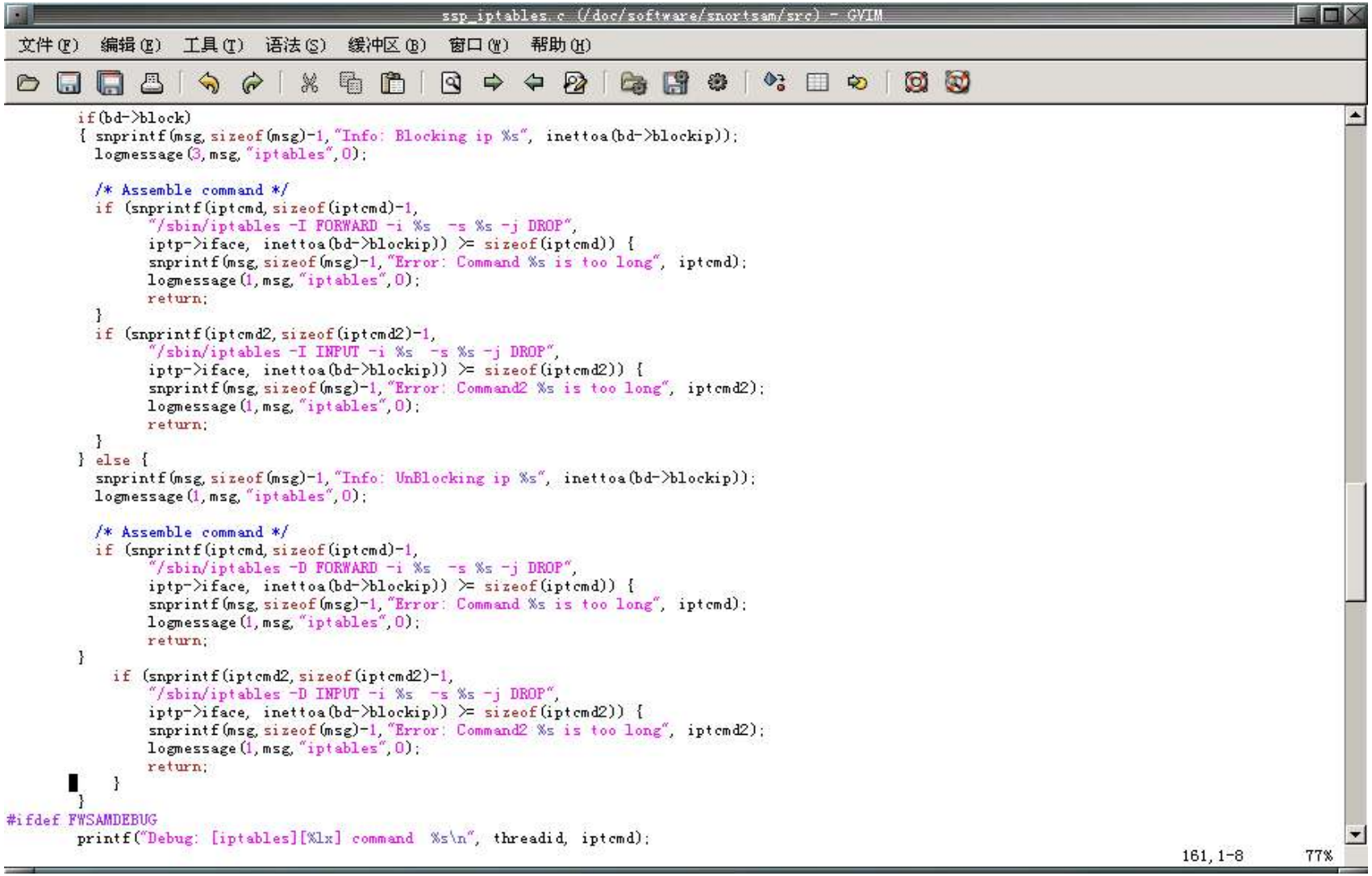


iptables 配置与连接效果





SnortSam 可以调整的部份



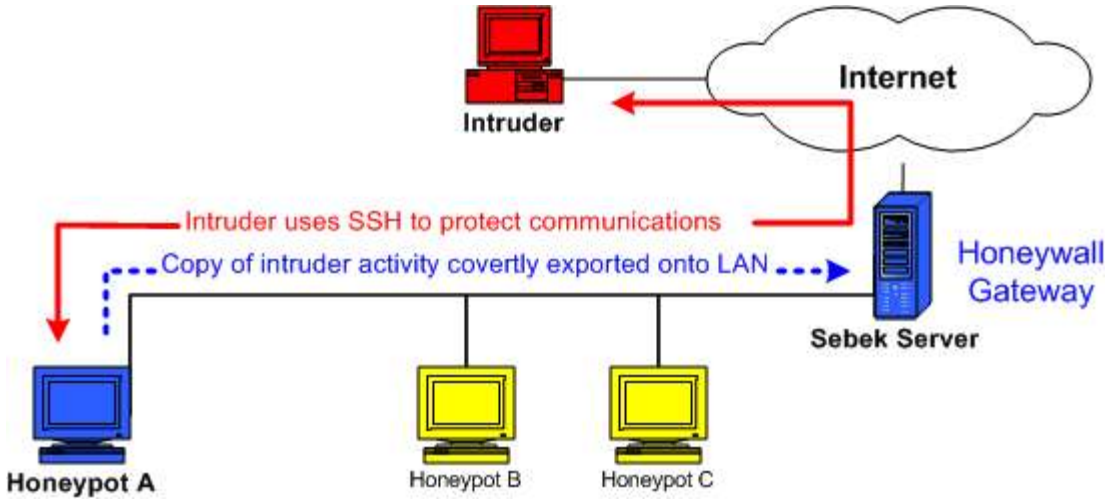

```
        if(bd->block)
        { snprintf(msg,sizeof(msg)-1,"Info: Blocking ip %s", inettoa(bd->blockip));
          logmessage(3,msg,"iptables",0);

          /* Assemble command */
          if (snprintf(iptcmd,sizeof(iptcmd)-1,
                "/sbin/iptables -I FORWARD -i %s  -s %s -j DROP",
                iptp->iface, inettoa(bd->blockip)) >= sizeof(iptcmd)) {
                snprintf(msg,sizeof(msg)-1,"Error: Command %s is too long", iptcmd);
                logmessage(1,msg,"iptables",0);
                return;
          }
          if (snprintf(iptcmd2,sizeof(iptcmd2)-1,
                "/sbin/iptables -I INPUT -i %s  -s %s -j DROP",
                iptp->iface, inettoa(bd->blockip)) >= sizeof(iptcmd2)) {
                snprintf(msg,sizeof(msg)-1,"Error: Command2 %s is too long", iptcmd2);
                logmessage(1,msg,"iptables",0);
                return;
          }
        } else {
          snprintf(msg,sizeof(msg)-1,"Info: UnBlocking ip %s", inettoa(bd->blockip));
          logmessage(1,msg,"iptables",0);

          /* Assemble command */
          if (snprintf(iptcmd,sizeof(iptcmd)-1,
                "/sbin/iptables -D FORWARD -i %s  -s %s -j DROP",
                iptp->iface, inettoa(bd->blockip)) >= sizeof(iptcmd)) {
                snprintf(msg,sizeof(msg)-1,"Error: Command %s is too long", iptcmd);
                logmessage(1,msg,"iptables",0);
                return;
        }
            if (snprintf(iptcmd2,sizeof(iptcmd2)-1,
                "/sbin/iptables -D INPUT -i %s  -s %s -j DROP",
                iptp->iface, inettoa(bd->blockip)) >= sizeof(iptcmd2)) {
                snprintf(msg,sizeof(msg)-1,"Error: Command2 %s is too long", iptcmd2);
                logmessage(1,msg,"iptables",0);
                return;
        }
        }
#ifdef FWSAMDEBUG
        printf("Debug: [iptables][%lx] command  %s\n", threadid, iptcmd);
```

对攻击报文的分析

- Sebek



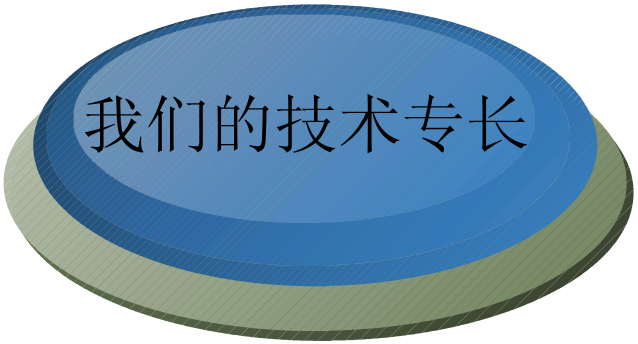
总结

- 企业秘密保护的要求
- 陷阱网络对企业秘密保护的意义
  - 实现“内容级”的 Honeypot
  - 隐藏真实目标
  - 及时发现和处理小规模恶意事件
  - 攻击者分类及分别对待（试探、违规、攻击、渗透）
- 自防御型陷阱网络的构成

展望

- 对自防御型 NAT 陷阱的完善
  - 融合、统一控制及数据分析
  - roo CDROM [Honeynet project]
- 其它类型陷阱网络
  - 客户端陷阱（针对内网用户的客户端攻击）
  - 帐号口令陷阱（针对网络钓鱼）

关于大成天下（http://www.unnoo.com）



渗透测试（ Penetration testing ）
网络架构评估设计（ Architecture review and design ）
应用审计（ Application audit ）
源代码审计（ Source code review ）
黑箱测试（ Online or Binary Black box testing ）
审计、追踪与数据恢复（ Forensics ）
协议分析（ Protocol analysis ）

我们的产品

游刃基线安全系统
铁卷信息监控平台

我们的服务

网络安全评估
网络安全培训
信息安全监理
软件定制开发

谢谢！