基于嗅探技术的内部网络安全研究*

徐 鸿[1],杨云江[2]

(1.贵州大学 计算机科学与信息学院,贵州 贵阳 550025;
2.贵州大学 信息化管理中心,贵州 贵阳 550025)

摘 要:网络边界处的防火墙系统可以有效防御一些来自外网的攻击,在入侵检测系统的实时保护下,理论上可以保障内网安全无忧。然而,内部网络的非法操作更隐蔽、更有威胁。针对这种情况,通过嗅探技术对内网进行实时的流量监控和数据包分析,较好地加强和保障了内网的安全。

关键词:嗅探技术;流量监控;数据包分析

中图分类号:TP393.08 **文献标识码**:A **文章编号**:1674-7720(2011)01-0038-03

The study of intranet security based on sniffer technology

Xu Hong[1], Yang Yunjiang[2]

(1.College of Computer Science and Information, Guizhou University, Guiyang 550025, China;
2.Information Management Center, Guizhou University, Guiyang 550025, China)

Abstract: The firewall system in network boundary can effectively prevent some of the attacks from the external network, which can protect the internal network secure in the intrusion detection system. but the malicious operations in intranet are more subtle and more threatening. In response to such a situation, this paper monitors the real-time traffic of intranet and analyzes data-packets by sniffer technology, which can strengthen and protect the intranet's security.

Key words: sniffer technology; monitoring traffic; analyzing data-packets

由于TCP/IP协议族本身存在许多安全漏洞,使复杂的网络安全难以保障。网络安全一般来说分为网络外部安全和网络内部安全两方面,这两方面出现的安全问题的比例约为3:7,显然,最普遍的安全威胁主要来自内部。内网由大量的终端组成,内网任何一部分的安全问题,都可能导致整个内部网络的瘫痪。内网的安全通常依靠主机防护系统、入侵检测系统(IDS)及漏洞扫描技术等来保证[1]。针对使用入侵检测系统的内网,由于网络传输速率的大大加快,使IDS的负担加重,造成了IDS的高虚警率,且IDS在应对对自身的攻击时,对其他传输的检测也会被抑制。因此本文通过嗅探技术加强对内网的实时监控管理,一定程度上加强了内网安全。

1 嗅探技术及Omni peek

网络嗅探是指利用计算机的网络接口截获目的地为其他计算机的数据报文的一种手段。网络嗅探技术不主动向网络发送数据包,而是监听、提取和解析网络中正在传输的数据包。网络嗅探技术是一把双刃剑,其正当用途主要是分析网络的流量及性能,以便找出网络中潜在的问题,但不可用于窃取私密信息[2]。如果某时段一个网段运行不畅,造成信息包的发送比较慢,丢包现象严重,而网络管理员又不知道问题所在,此时就可以用嗅探软件作出较准确的判断。

Omni peek是出自WildPackets的著名抓包软件,其功能与Sniffer Pro有相似之处,是一款网管和应用故障诊断分析软件。针对复杂的网络环境,执行管理、监控、分析、除错及最佳化的工作。Omni peek软件v6.02提供更好的图形用户界面,不管是在有线网络还是在无线网络中,它都能够给予网络管理人员实时的网络监视、数据包捕获以及故障诊断分析能力。

2 实时网络监控

2.1 协议分析

在共享网络环境下,即由集线器组成的局域网环境,只需将网卡设置成混杂模式,即可监听到所有经过

*基金项目:贵州省科学技术基金项目(黔科J字[2009]2116号)

该网卡的数据包。而在交换网络环境,设置网卡接收模式就不可行了。因此,在一个交换式的局域网中,在其任一台主机上安装网络嗅探工具,无论其嗅探功能如何强大,也无能为力。这时,它只能嗅探到从本机进出的数据包。而若把嗅探工具安装在代理服务器上便可解决这一问题。对内网的实时监控,不是为了实时记录网络状态,而是为了发现异常和攻击。本文分析了一些常见的内网安全问题(正常的数据包就不再此阐释),通过运行 Omni peek,捕获数据包,经查看发现内网主机 192.168.0.136 的数据包可疑,刚开机不久便向 IP 地址为 24.89.201.200 发送大量数据包,且这台主机发出的所有数据包协议都基于 HTTP,如图 1 所示。

图 1 发送的数据包协议

通过查看某个捕获的数据包的源码,解码后如表 1 所示。

表 1 通过查看某个捕获的数据包的源码解码

00 19 D1 79 3B 98	目的 MAC 地址	00 19 D1 79 4D 42	源 MAC 地址
0800(0x0800)	IP 协议代码	00 80 06 A6 AD	其中 06 是 TCP 代码
C0 A8 00 88	192.168.0.136	18 59 C9 C8	24.89.201.200
00 00 00 00 00	ACK 数量为 0	FF FF	窗口大小为 65 535

由于 HTTP 是基于请求/响应范式的,信息交换过程分为 4 个部分:建立连接、发送请求、发送响应、关闭连接。但捕获到的内网 IP 为 192.168.0.136 的主机所发出的数据包却很可疑,ACK 确认的数量值全为 0。图 2 是通过 Omni peek 软件对 TCP 的解析,发现所有数据包均是 SYN 包,而 SYN 包是主机要发起 TCP 连接时发出的数据包,也就是这台内网主机不断地向外网中的某主机建立 HTTP 连接,但没有得到任何回应,既未收到 ACK 确认包,也没有 FIN 释放连接[3]。

图 2 通过 Omni peek 软件对 TCP 的解析

在 30 s 内,内网主机 192.168.0.136 从网络收到的数据包数只有 5 个,但其向外网发出的数据包却有 904 个,如图 3 所示。

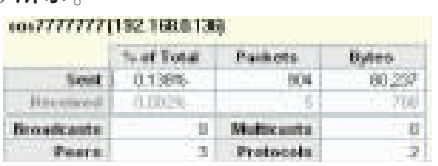

图 3 在 30 s 内,内网主机 192.168.0.136 从网络收到的数据包数

这时用 Omni peek 节点分析功能,查看 192.168.0.136 节点的详细资料统计,如图 4 所示,发现 HTTP 协议占了整个通信协议的 99.386%。

图 4 192.168.0.136 节点的详细资料统计

通过对上述情况的分析,可以推测 192.168.0.136 所收到的 5 个包是来自别的节点的 DNS 包(从图 3 可以看出总共有 3 个节点与它通信,并且图 4 的协议中 DNS 数据包占了 0.614%)。

当单独查看 IP 地址为 192.168.0.136 与 24.89.201.200 的主机通信协议时,则 100%都是 HTTP 协议,如图 5 所示。它与 IP 地址为 24.89.201.200 的主机通信全是基于 HTTP 的,但没有收到一个回包。这对 HTTP 来说显然是不正常的,HTTP 是基于 TCP、是有连接的,不会只发不收。因此判断该主机可能是感染了病毒,是造成 TCP SYN 泛洪(Flood)攻击所需的“肉鸡”。

图 5 当单独查看 IP 地址为 192.168.0.136 与 24.89.201.200 的主机通信协议

然而对于被攻击主机来说,由于 SYN 泛洪攻击所使用的 IP 地址并不是真实的地址,而是代理服务器的公共 IP 地址,所以被攻击者最多只能追踪到内网代理服务器的 IP 地址为 210.40.20.76(假设未使用二级以上代理),而要确定攻击终端很难,黑客通常利用这种攻击的隐蔽性肆意破坏。所以,内网管理员应该立即确定这台内网主机,对其进行下线处理,再进行扫描杀毒,以免造成不可避免的损失。

2.2 流量监控

一般进行流量监控时,首先要关注那些流量最大的终端节点。某一时段,丢包现象严重,网络性能下降,通过 Omni peek 软件分析发现网络阻塞,如图 6 所示。

图 6 通过 Omni peek 软件分析发现网络阻塞

经查看发现,内网 IP 为 192.168.0.162 的主机流量最大,且比例一直在持续增加,这是造成网络阻塞的重要原因。本文先分析网络流量的流向[4],通过 Omni peek 的 peer map 捕获发现,确定 192.168.0.162 向外网很多终端发送大量的数据包,如图 7 所示。再对数据包的传输协议进行查看,发现均为基于 UDP 的数据包。UDP 是一个无连接、不可靠和缺乏安全性的传输层协议。通过对内网 IP 为 192.168.0.162 的主机进行单点分析,其在

图 7 192.168.0.162 向外网很多终端发送大量的数据

短时间内向 257 外网终端发出了 7 863 个数据包，其中 UDP 数据包占了 91.4%，如图 8 所示。

图 8 通过对内网 IP 为 192.168.0.162 的主机进行单点分析

主机向外网发出大量 UDP 数据包，虽然 UDP 数据包不像 TCP 建立连接需“3 次握手”，可以被人利用 SYN 消耗一方资源，但如果利用大量 UDP 包冲击服务器，可能会造成 UDP FLOOD 攻击，也会使网络瘫痪。一般出现下面两种可能：(1)“肉鸡”终端不断向外网发送大量无意义的 UDP 数据包，利用 UDP 协议漏洞，在两台主机的网段之间产生大量没有实际意义的 UDP 数据流。这些数据流将占尽服务器的网络带宽资源，从而导致系统无法正常提供服务功能，造成 DoS 攻击[5]。(2)某种 P2P 下载软件的共享功能从图 8 得知，它收到了 2 642 个数据包。有关调查表明，P2P 业务不断增加，造成了网络带宽的巨大消耗，引起网络拥塞，降低其他业务的性能。经查找证实，该内网终端确实在使用 P2P 软件 Emule。在这种情况下，应对该终端进行限速处理，恢复网络通畅。

2.3 防止内网 ARP 欺骗攻击

在局域网中，最常见的攻击是 ARP 欺骗攻击。由于 ARP 使主机不会验证包的来源是否合理，使得一台主机在从未收到 ARP 请求包时，也可以发送 ARP 应答包。一旦某台主机收到 ARP 应答包，即使它从未向发送此应答包的主机发送过 ARP 请求包，仍会对本地的 ARP 缓存进行更新，将应答包中的 IP 和 MAC 地址存储在 ARP 缓存中，所以很多人利用这种缺陷，通过发送伪造的 ARP 应答包给发出请求的主机，从而改变它们之间的数据传输过程[6]。造成这种情况主要是因为 ARP 的基础就是信任局域网内所有的人，这样就很容易实现在以太网上的 ARP 欺骗。被 ARP 攻击的主要现象有：局域网内频繁性区域掉线，网速时快时慢，同时能够在网络中产生大量的 ARP 数据包通信量使网络阻塞。

某时段，发现捕获的数据包不显示目的 IP 地址及源 IP 地址，查看其数据包协议为 ARP 的应答包，如图 9 所示，分析证实必然是某台主机发送 ARP 欺骗数据包。

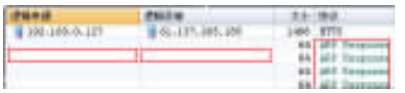

图 9 某时段其数据包协议为 ARP 的应答色

在 MS-DOS 环境下使用 arp - a 命令来查看 ARP 缓存，正常情况下，每一个内网 IP 都有唯一的 MAC 地址与之对应。某主机窜改 MAC 地址(人为或是病毒)(如图 10 所示)，主机 192.168.0.105 伪造代理服务器 192.168.0.1 的 MAC 地址。

```
Interface: 192.168.0.124 --- 0x10003
  Internet Address      Physical Address
  192.168.0.1           00-19-d1-79-3b-98
  192.168.0.105         00-19-d1-79-3b-98
```

图 10 某主机窜改 MAC 地址

同时 Omni peek 软件的 ARP 数据包分析功能也发现异样，如图 11 所示，幅度较大的部分是 ARP Response 包的频率值，从图得知这个时段内有大量的 ARP 应答包，应答包数量大大超过请求包，经分析得知，图中大部分的应答包是 192.168.0.105 的终端发出的，以达到欺骗的目的。

图 11 Omni peek 软件的 ARP 数据包分析功能也发现异样

内网管理员可以通过 Omni peek 软件第一时间察觉到 ARP 攻击，立即对恶意主机进行下线处理。

在基于代理服务器的环境下，通过网络嗅探软件 Omni peek 可以很方便地对内网进行实时监控管理。本文对常见的内网安全问题进行了分析和阐述，特别是第一种，由于内网主机本身没有真实 IP 地址，通过代理服务器的公共 IP 地址隐藏终端来攻击外网主机，而被攻击者又很难确定这台没有真实 IP 地址的终端。从被攻击者的角度，如何确定没有固定IP 地址的终端，即非真实 IP 地址网络终端定位方法的有待进一步的研究。

参考文献

[1] 杨云江.计算机网络管理技术[M].第 2 版，北京：清华大学出版社，2009.

[2] 蔡林.网络嗅探技术在信息安全中的应用[J].计算机时代，2008(6)：16-18.

[3] RICHARD S W.TCP/IP illustrated volume 1[M].北京：机械工业出版社，2002.

[4] DABIR A, MATRAWY A. Bottleneck analysis of traftic monitoring using wireshark [C]. 4th International Conference on Innovations in Information Technology, 2007, IEEE

Innovations′07, 2007:158-162.

[5] OADEER M A. Network traffic analysis and intrusion detection using packet sniffer[C]. 2010 Second International Conference on Communication Software and Networks, 2010:313-317.

[6] 孙谦,黄家林,傅军.基于协议分析的ARP欺骗病毒源自动定位[J].现代计算机,2008,289:136-139.

(收稿日期:2010-06-02)

作者简介:

徐鸿,男,1986年生,硕士研究生,主要研究方向:网络安全。

杨云江,男,1955年生,教授,硕士生导师,主要研究方向:网络应用,网络安全。