

园区网 ARP 欺骗攻击防御模式设计与实现

赵晓峰,汪精明,王平水

(安徽财经大学 网络中心,安徽 蚌埠 233041)

摘 要:地址解析协议(ARP)工作于 OSI 参考模型第二层,在园区网 VLAN 中实现 IP 地址到网络接口硬件地址(MAC)的映射功能,攻击者利用 ARP 协议安全缺陷,在网关与主机(整个网段)之间实施 ARP 欺骗攻击,将会对 VLAN 内主机产生巨大安全威胁。针对此类攻击设计与实现的网络防御模式,通过 IP 地址与接入层交换机端口绑定、定期在 VLAN 广播网关 MAC 地址等方法,可有效阻止该类攻击发生。

关键词:交换网络;ARP 欺骗;网络攻击;网络防御

中图分类号:TP393.08

文献标识码:A

文章编号:1673-629X(2007)07-0152-04

Design and Implementation of Defense System for ARP Spoofing in Campus Network

ZHAO Xiao-feng, WANG Jing-ming, WANG Ping-shui

(Anhui University of Finance & Economics, Bengbu 233041, China)

Abstract: Address Resolution Protocol(ARP) works in Layer 2 of the OSI reference model. It implements the mapping between IP and MAC in VLAN of campus network. The attacker uses the ARP shortage of security, implements the ARP spoofing attack between the gateway and the host computer, will be serious threat to the security of host computer in VLAN. Design and implementation of defense system for this kind of attack, through IP address and switch port binding, broadcast gateway MAC address and so on methods, can prevent this kind of attack to occur effectively.

Key words: switch network; ARP spoofing; network attack; network defense

0 引 言

目前,园区网普遍采用核心交换机+汇聚交换机+接入交换机结构构建,并通过 VLAN 将整网划分若干子网,在交换机上基于端口方式实现 VLAN。网管人员通常将服务器、交换机、互联网出口分别划分 VLAN,其它普通用户按楼宇或部门划分 VLAN,这样划分 VLAN 好处是简单、易于实现、易于管理,但在安全方面存在很大缺陷,其中最大安全威胁是 ARP 欺骗问题。

ARP 协议工作于 OSI 参考模型第二层,在园区网 VLAN 中实现 IP 地址到网络接口硬件地址(MAC)映射功能,ARP 欺骗利用 ARP 协议安全缺陷,通过向被欺骗主机发送伪造 ARP 请求或应答,使目标主机将数据报发往攻击者希望的 MAC 地址。ARP 欺骗攻击方式很多,主要有中间人攻击、拒绝服务攻击、克隆攻击,

这些攻击会造成被攻击主机受监听、会话劫持或无法对外连接。园区网 VLAN 内主机之间相互访问较少,主机与网关之间数据交换频繁,主机依赖网关转发与接收数据报,才能访问互联网或园区网服务器。因此,攻击者通常选择在网关与主机之间实施 ARP 欺骗攻击。

随着图形化 ARP 欺骗工具与基于 ARP 欺骗木马的出现,使得实施该类攻击门槛降低,园区网安全受到进一步威胁。如何阻止该类攻击发生,成为保障园区网安全一项刻不容缓的重要课题。

1 ARP 欺骗原理和实现方式

园区以太网中,每台联网主机具有两种地址:IP 地址和网卡地址(MAC),IP 地址用于 VLAN 间通信,VLAN 内部通过 MAC 地址通信,在 Windows 等操作系统中,联网主机使用高速 ARP 缓存存放最近的 IP-MAC 映射对,以下情况下主机会主动更新 ARP 缓存:

- 1)映射对生存期已过会被删除。
- 2)收到发往本机 IP 地址 ARP 请求或应答时,

收稿日期:2006-09-03

基金项目:安徽省 2006 年教育厅自然科学基金项目(2006kj017C)

作者简介:赵晓峰(1970-),男,安徽蚌埠人,实验师,研究方向为网络管理、网络安全。

ARP 缓存中没有相应映射对,将新建该映射。如有旧映射对,且新映射对 MAC 地址与旧映射对 MAC 地址不同,新 MAC 地址将更新旧 MAC 地址。

3)收到发往本网段 ARP 请求或应答广播帧时,如 ARP 缓存中已有相应映射对,且与广播帧所含映射 MAC 地址不同,缓存中映射对 MAC 地址会被新 MAC 地址更新。ARP 缓存中没有相应映射对,不新建该映射。

ARP 协议是无状态协议,主机收到 ARP 数据帧,不论该帧是否源于真正源主机,都将新建或替换相应映射对。ARP 欺骗核心思想就是向目标主机发送伪造了源 IP-MAC 映射的 ARP 请求或应答,诱使目标主机更新其 ARP 缓存,从而使目标主机将报文发送给错误对象。如图 1 所示,攻击主机 B 对 A 实施 ARP 欺骗,A 本要发往 C 的报文会发送到攻击者指定主机 D,主机 A 对此一无所知^[1]。

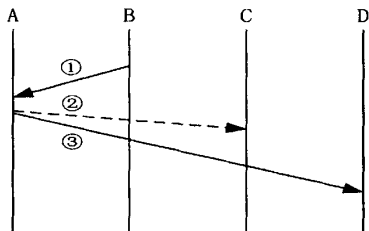


图 1 ARP 欺骗原理

注:D 为任意或根本不存在的主机。

①B 向 A 发送 ARP 应答(请求),将 A 缓存中关于 C 映射对 MAC 地址改为 D 的 MAC 地址。

②A 向 C 发送报文。

③B 对 A 欺骗成功,A 发向 C 的报文将被错误地发往 D。

在 VLAN 中当攻击者选择在网关与主机(整网段)之间进行 ARP 欺骗,会对整个 VLAN 内主机产生巨大安全威胁。

2 攻击者在网关与主机(整网段)实施 ARP 欺骗攻击的方式

ARP 欺骗中,中间人攻击是最主要,也是最危险的攻击方式,攻击者将自己主机插入网关与目标主机通信路径之间,成为两者通信的中继,为了转发两者的数据报,攻击主机要启动路由转发功能,攻击过程如图 2 所示。

注:B 为任一主机或整网段。

①A 向网关发送 ARP 请求(应答),网关将 B 的 IP 映射为 A 的 MAC 地址。

②A 向 B 发送 ARP 请求(应答),B 将网关的 IP 映

射为 A 的 MAC 地址。

③网关发往 B 的报文,要经 A 转发。

④B 发往网关的报文,要经 A 转发。

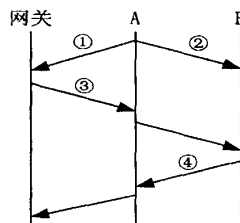


图 2 中间人攻击

攻击者通过中间人攻击再辅助于嗅探监听^[2],就可在交换网络截获网段内任一主机明文密码(E-MAIL, TELNET, FTP 等),通过会话劫持,可冒充被攻击主机登录远程服务器,利用 DNS 欺骗,可骗取某些加密码令等。

中间人攻击时,如攻击者忘记或故意不打开路由转发功能,会造成拒绝服务攻击效果。对截获的目标主机某些管理数据报进行修改加工,然后再重新发出,可造成克隆攻击效果。

3 防御模式设计

3.1 对网关欺骗的防御

图 3 假设某 VLAN 有 A, B, C 三台主机,分别接入交换机 1, 2, 3 号端口。

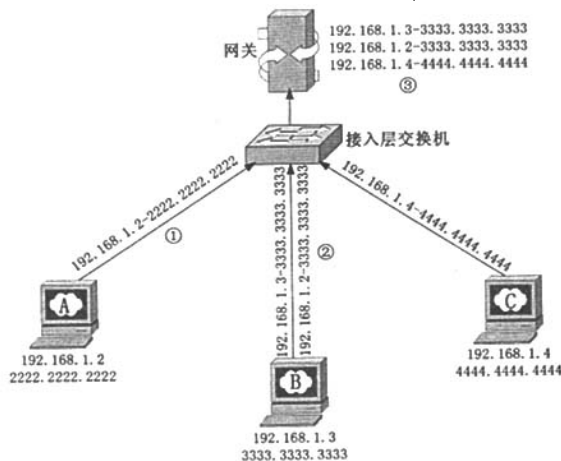


图 3 欺骗网关示例

注:A 为被攻击主机,B 为攻击主机,C 为其它任意主机。

①主机 A 经网关转发数据报,网关建立 A 主机正确 IP-MAC 映射。

②主机 B 对 A 实施 ARP 欺骗。

③主机 A 在网关的正常 IP-MAC 映射被改变。

接入层交换机端口具有自学习功能,主机只要有

网络访问数据发送,其上连交换机端口将记住帧源 MAC 地址,图 3 中,A,B,C 所连交换机 1,2,3 号端口分别学习到 2222.2222.2222,3333.3333.3333,4444.4444.4444 三个 MAC 地址,此时,如果 B 在实施 ARP 欺骗的同时,也经网关向外访问,网关 ARP 缓存中将出现 3333.3333.3333 映射两个 IP 地址情况。B 如只实施 ARP 欺骗,不经网关向外访问,网关 ARP 缓存中相关 B 的映射只有一个 192.168.1.2 - 3333.3333.3333,但不论 B 是否经网关向外访问,其针对 A 实施欺骗的映射在网关 ARP 缓存中都将存在。根据交换机端口学习的 MAC,比对网关 ARP 缓存,将发现本该是 192.168.1.2 - 交换机端口 1 的对应关系,变成 192.168.1.2 - 交换机端口 2。通过以下过程将 IP 地址与交换机端口绑定可阻止该种欺骗。

1)将 VLAN 内主机 IP 地址与其上连交换机端口对应关系存入数据库。

2)定期采集网关 ARP 映射表及接入交换机端口自学习 MAC 地址。

3)根据端口自学习 MAC 地址,比对网关 ARP 缓存中映射 IP,与数据库中端口对应 IP 是否相符。

不相符有两种可能:一是 IP 地址盗用,二是正在进行 ARP 欺骗,关闭接入交换机端口将阻止这两种恶意网络行为。

3.2 对主机欺骗的防御

对主机欺骗防御有两种方法:

1)编写防御网关 ARP 欺骗的程序,主机安装该程序后,即将 ARP 缓存中网关映射设为静态映射,当收到来自于网关的 ARP 帧,将帧中所含映射 MAC 地址,与预先定义网关正确 MAC 地址比对,如不相符,拒绝更新网关映射,并发出警报。

2)按某一频率,不断向 VLAN 发送含有网关正确映射 ARP 应答,主动更新 VLAN 内存活主机网关映射 MAC 地址,当攻击者实施欺骗攻击时,主机 ARP 缓存网关映射不断被改回正确状态,受此干扰,攻击不能成功进行。为了防范对整网段拒绝服务攻击,还需对网关 ARP 请求或应答广播帧进行分析,发现有不正确 ARP 请求或应答,即报警。

4 防御系统具体实现

根据防御模式设计原理,在 LINUX 下分两大模块实现防御系统。

4.1 防御对网关欺骗的模块

能够实时采集网关 ARP 映射表与接入交换机端口自学习 MAC 地址信息,成为模式设计中 IP 地址与端口绑定的关键,这两个关键信息可通过启动核心交

换机与接入交换机 SNMP 服务获取,RFC1213 定义的 MIB-2 IP 组有一个 ipNetToMediaTsble 表^[3,4],该表的 ipNetToMediaPhysAddress 存储了系统 ARP 缓存所有映射对,该项 OID 值为 1.3.6.1.2.1.4.22.1.2,防御系统通过向网关 SNMP 代理服务该 OID 项,发送 GetBulkRequest 请求报文,即可获取网关 ARP 缓存所有 IP-MAC 映射信息。RFC1493 定义的 BRIDGE-MIB 中 dot1dTp 组的 dot1dTpFdbTable 表存储了交换机端口自学习 MAC 地址信息,其 OID 为 1.3.6.1.2.1.17.4.3,该表由三个表项构成:dot1dTpFdbAddress 项存储了交换机自学习所有 MAC 地址,dot1dTpFdbPort 项存储了自学习 MAC 对应端口,dot1dTpFdbStatus 项表明端口获取 MAC 的方式,如没有做 MAC 地址绑定,值为 3,即 learned 自学习。防御系统只要对某接入交换机,发送该 OID 的 GetBulkRequest 请求报文,即可获取该交换机各端口自学习 MAC 地址,去掉上连端口学习的 MAC 地址,剩下部分即为要获取的端口自学习 MAC 地址。通过端口自学习 MAC 地址查找网关 ARP 映射表该 MAC 地址对应 IP,比对数据库中预先存储的该端口绑定 IP,如不相符即关闭该端口。RFC1213 定义的 MIB-2 接口组 iftable 中 ifadminstatus 表示端口管理状态,其 OID 为 1.3.6.1.2.1.2.2.1.7,值为 1,表示端口打开,值为 2 表示端口关闭,值为 3 表示测试,该值可以使用读写权限团体名修改。防御系统向交换机需关闭端口 OID 发送值为 2 的 setrequest 请求报文,即可关闭该端口,同时将关闭该端口相关信息记录下来。

4.2 防御对主机欺骗的模块

在模式设计中提到对主机欺骗,防御可通过两种方法实现。

方法一:在主机端对所接收 ARP 帧进行欺骗分析,关键是能够抓取 ARP 帧,园区网主机大部分用的是 Windows 系统,因此,通过 WinPcap 编程,实现 ARP 帧抓取。下面是使用 WinPcap 实现 ARP 帧抓取关键代码,其中省略了错误检查^[5]。

```
Pcap_if_t * alldevs; Pcap_if_t * d; Pcap_t * adhandle;
Struct bpf_program foode;
Pcap_findalldevs(&alldevs, errbuf); /* 返回系统中可用接口列表
*/
Adhandle = pcap_open_live(d -> name, /* 选择抓取帧接口名称
*/
65536, /* 表示抓取整个帧 */
0, /* 因只抓取发往本机的帧,网卡设为正常模式 */
1000, /* 超时值为 1000 毫秒 */
errbuf); /* 错误信息缓冲区 */
pcap_datalink(adhandle); /* 检查是否为以太网 */
```

```
pcap_compile(adhandle, &fcode, "arp", 1, netmask); /* 设置仅抓取 ARP 帧 */
pcap_setfilter(adhandle, &fcode); /* 为接口设置过滤器 */
pcap_freealldevs(alldevs); /* 释放接口列表, 当接收到 ARP 帧时, 调用回调函数 packet_handler, 对抓取的帧处理就可在函数中完成 */
Pcap_loop(adhandle, 0, packet_handler, NULL);
```

方法一虽然可行,但并不实用,因为让园区网所有主机都安装该程序不太现实,且攻击者如果冒充某台主机向防御系统发送大量报警,将会对管理员的判断、处理产生严重影响。

方法二:实现方法二关键有三点:a.如何将广播帧传向 VLAN;b.如何生成广播帧;c.如何获取 VLAN 广播帧。

VLAN 信息通过 802.1Q 协议(CISCO 专有协议为 ISL)封装与解封,设置为 trunk 模式端口可传送 802.1Q 数据报,如通过 trunk 发送 802.1Q 数据报 VLANID 为 52,即意味着该数据报发往 VLAN52。因此,只要将防御系统与交换机连接端口设为 trunk 模式,防御系统具有处理 802.1Q 数据报能力,即可对发送或接收任意 VLAN 网关 ARP 广播帧。因防御系统使用 LINUX 系统,通过 vconfig 配置虚拟接口,即可处理 802.1Q 数据报,例如要发送与接收 VLAN52 的网关 ARP 广播帧,可通过以下命令配置虚拟接口:

```
vconfig add eth0.52
ifconfig eth0.52 up
```

LINUX 下通过 libnet 编程,实现向外发送 ARP 广播帧。下面使用 libnet 编程实现向 VLAN52 发送合法网关广播帧关键代码,其中省略了错误检查(注:网关 IP 为 192.168.52.1,MAC 地址为 0006.d605.1cfc)。

```
libnet_t *l;
char brocast[6] = {0xff,0xff,0xff,0xff,0xff,0xff};
u_char eg_src[6] = {0x00,0x06,0xd6,0x05,0x1c,0xfc};
u_char e52ip_src[4] = {0xc0,0xa8,0x34,0x01};
u_char hz[6] = {0x00,0x00,0x00,0x00,0x00,0x00};
u_char ipz[4] = {0x00,0x00,0x00,0x00};
l = libnet_init(LIBNET_LINK_ADV, /* 设定基于链路层发送方式 */
"eth0.52", /* 设定发送接口 */
errbuf); /* 错误信息缓冲区 */
libnet_build_arp(ARPHRD_ETHER, ETHERTYPE_IP, 6, /*
MAC 地址长度 */
```

```
4, /* IP 地址长度 */
ARPOP_REPLY, /* 操作类型为应答 */
eg_src, /* 网关 MAC 地址 */
e52ip_src, /* 网关 IP 地址 */
hz, /* 目标硬件地址,因是广播可全为 0 */
ipz, /* 目标 IP 地址,因是广播可全为 0 */
NULL, 0, 1, 0);
libnet_autobuild_ethernet(brocast, /* 以太网目标地址为广播地址 */
ETHERTYPE_ARP, /* 以太网协议类型为 ARP */
libnet_write(l); /* 将 l 中描述数据报发送出去 */
libnet_destroy(l); /* 释放 l 所占内存 */
```

使用本程序按某一频度,主动更新 VLAN52 存活主机 ARP 缓存网关映射,即可阻止或干扰攻击者欺骗攻击。配置好其它 VLANID 虚拟接口,在程序中增加向新加 VLAN 虚拟接口 ARP 广播,即可对一个以上 VLAN 实施防护。至于对 ARP 广播帧捕获分析,只要将方法一中使用 WinPcap 实现的程序,稍加改动移植到防御系统中,改用 libpcap 实现在相应虚拟接口捕捉来自于网关的 ARP 广播帧即可实现。只不过捕获 ARP 广播帧后,先要判断是否是防御系统自己发出的,如不是再判断是否有 ARP 广播欺骗存在。

5 结 语

针对园区网攻击者最感兴趣的网关与主机之间 ARP 欺骗问题,在对攻击原理与实现分析基础上,总结出一套方便有效的攻击防御方法,实现的系统可有效阻止中间人与克隆攻击,对拒绝服务攻击也有一定防御作用。在此系统上添加和完善相应功能,可将其作为轻型 IDS 使用。

参考文献:

- [1] 郑文兵,李成忠. ARP 欺骗原理及一种防范算法[J]. 江南大学学报:自然科学版,2003,2(6):574-577.
- [2] 李海鹰,程 灏,吕志强,等. 针对 ARP 攻击的网络防御模式设计与实现[J]. 计算机工程,2005,31(5):170-171.
- [3] Richard S W. TCP/IP 详解(卷 1:协议)[M]. 北京:机械工业出版社,2000.
- [4] Stallings W. SNMP 网络管理[M]. 北京:中国电力出版社,2001.
- [5] 陈 辉,陶 洋. 基于 WinPcap 实现对 ARP 欺骗的检测和恢复[J]. 计算机应用,2004,24(10):67-85.

《计算机技术与发展》欢迎投稿,欢迎订阅。