

IP 源地址欺骗

刘凯 2015140014
黄锦雨 2015140011

/ 工作流程

Step01

IP欺骗原理

Step02

实际操作

Step03

如何防止IP欺骗

/IP欺骗原理

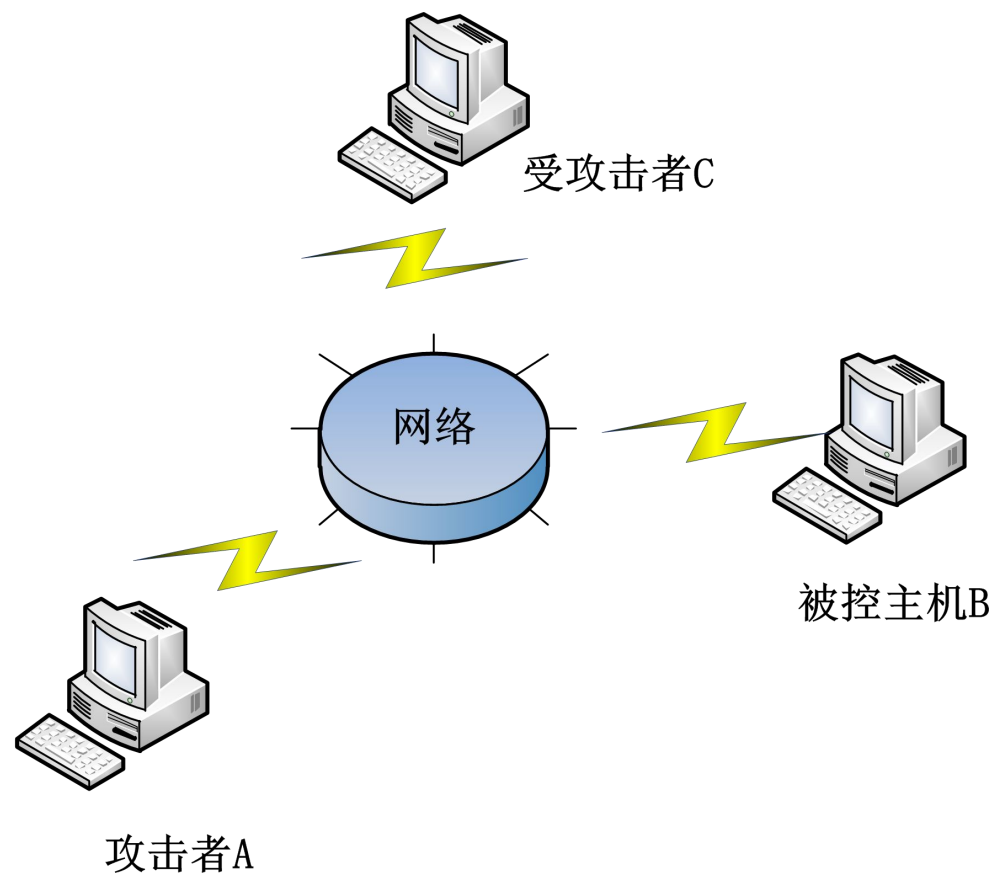


图1 网络连接图

/IP欺骗原理

1.1、IP地址欺骗基本原理

- 攻击者选取那些与被攻击主机C存在信任关系的主机作为跳板，如主机B，将发给主机C的数据包中的IP源地址改为主机B的IP地址，从而不会被C发现发送数据包的真实主机，即主机A。

1.2、IP地址伪造方法

- 编写raw socket程序，改变数据包中的IP源地址，需root权限；
- 使用nmap等工具构造具有指定IP源地址的数据包。

/IP欺骗原理

1.3、IP欺骗攻击过程

- 攻击者A利用工具发现与受害者C存在信任关系的主机B；
- 主机A使用LAND、SYN洪水等攻击方法使B主机瘫痪，目的是防止B主机收到有效网络数据将IP欺骗揭穿；
- 预测受害者主机C的数据包序列号；
- 主机A通过IP欺骗伪装成主机B，并向主机C的513端口（rlogin）发送请求连接；
- 主机A接着向C发送ACK信号，企图与主机C建立连接；
- 主机A篡改主机C的/.rhosts文件，使得所有用户无密码登录主机C。

/IP欺骗原理

1.4、如何估计初始序列号ISN

TCP三次握手可能会使得主机A无法与受攻击主机C进行连接，关键在于如何估计主机C的初始序列号ISN。如何预测？

- 首先与主机C的某个端口建立正常连接，重复N次，计算出往返时间的平均值；
- 由往返平均时间就可以推算出ISN；

/IP欺骗原理

1.5、如何建立连接

- 主机A伪装成主机B向主机C的513端口（ rlogin ）发送连接请求；
- 主机C发送SYN+ACK包给主机B而不是主机A确认请求；
- 主机A在先前估计的序列号上加1，并向主机C发送ACK包，若序列号估计正确，则连接建立；
- 留下后门，如篡改主机C的/.rhosts文件获得一个shell。

/ 实际操作

2.1、工具

- a) 两台主机，分别为CentOS 6.6 和Windows 7；
- b) Nmap；
- c) Wireshark。

/实际操作

2.2、操作过程

a) Nmap使用

```
[root@malo ~]# nmap -sS -p 8080 10.210.84.103 -D 10.210.84.15

Starting Nmap 5.51 ( http://nmap.org ) at 2015-11-07 23:40 CST
Nmap scan report for 10.210.84.103
Host is up (0.091s latency).
PORT      STATE      SERVICE
8080/tcp   filtered  http-proxy
MAC Address: 68:A3:C4:D0:EE:B3 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.12 seconds
[root@malo ~]#
```

图2 Nmap使用过程

/ 实际操作

图中命令为

```
nmap -sS -p 8080 10.210.84.103 -D 10.210.84.15 ;
```

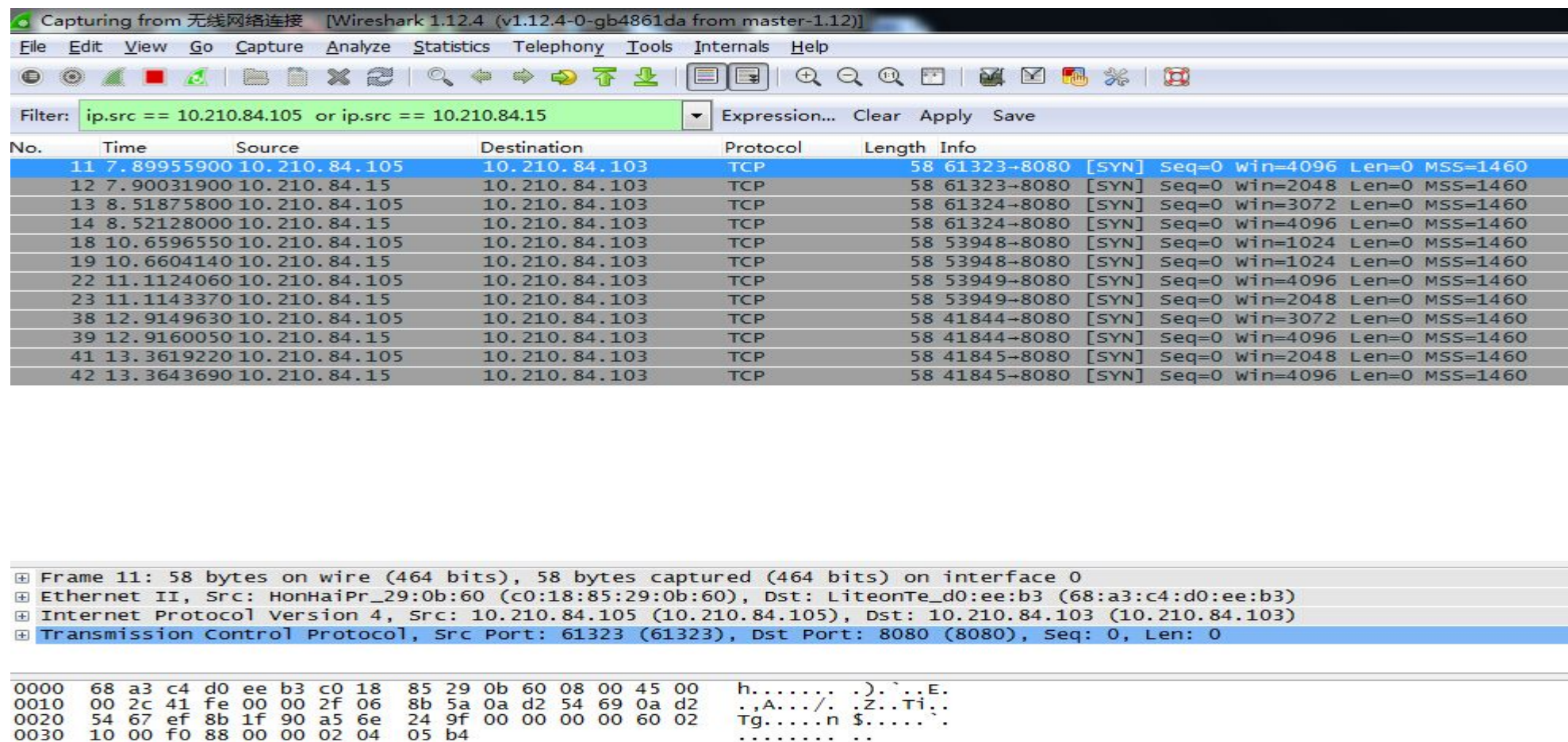
其中10.210.84.103为目标主机地址，10.210.84.15为发送数据包时伪造的IP地址，真实IP地址为10.210.84.105，同时探测端口8080，发送多次。

b) 使用wireshark捕捉数据包

首先使用wireshark的过滤功能,设定

```
ip.src == 10.210.84.15 or ip.src == 10.210.84.105。
```

/ 实际操作



Capturing from 无线网络连接 [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: `ip.src == 10.210.84.105 or ip.src == 10.210.84.15` Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
11	7.89955900	10.210.84.105	10.210.84.103	TCP	58	61323→8080 [SYN] Seq=0 win=4096 Len=0 MSS=1460
12	7.90031900	10.210.84.15	10.210.84.103	TCP	58	61323→8080 [SYN] Seq=0 win=2048 Len=0 MSS=1460
13	8.51875800	10.210.84.105	10.210.84.103	TCP	58	61324→8080 [SYN] Seq=0 win=3072 Len=0 MSS=1460
14	8.52128000	10.210.84.15	10.210.84.103	TCP	58	61324→8080 [SYN] Seq=0 win=4096 Len=0 MSS=1460
18	10.6596550	10.210.84.105	10.210.84.103	TCP	58	53948→8080 [SYN] Seq=0 win=1024 Len=0 MSS=1460
19	10.6604140	10.210.84.15	10.210.84.103	TCP	58	53948→8080 [SYN] Seq=0 win=1024 Len=0 MSS=1460
22	11.1124060	10.210.84.105	10.210.84.103	TCP	58	53949→8080 [SYN] Seq=0 win=4096 Len=0 MSS=1460
23	11.1143370	10.210.84.15	10.210.84.103	TCP	58	53949→8080 [SYN] Seq=0 win=2048 Len=0 MSS=1460
38	12.9149630	10.210.84.105	10.210.84.103	TCP	58	41844→8080 [SYN] Seq=0 win=3072 Len=0 MSS=1460
39	12.9160050	10.210.84.15	10.210.84.103	TCP	58	41844→8080 [SYN] Seq=0 win=4096 Len=0 MSS=1460
41	13.3619220	10.210.84.105	10.210.84.103	TCP	58	41845→8080 [SYN] Seq=0 win=2048 Len=0 MSS=1460
42	13.3643690	10.210.84.15	10.210.84.103	TCP	58	41845→8080 [SYN] Seq=0 win=4096 Len=0 MSS=1460

Frame 11: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface 0

Ethernet II, Src: HonHaiPr_29:0b:60 (c0:18:85:29:0b:60), Dst: LiteonTe_d0:ee:b3 (68:a3:c4:d0:ee:b3)

Internet Protocol Version 4, Src: 10.210.84.105 (10.210.84.105), Dst: 10.210.84.103 (10.210.84.103)

Transmission Control Protocol, Src Port: 61323 (61323), Dst Port: 8080 (8080), Seq: 0, Len: 0

0000	68 a3 c4 d0 ee b3 c0 18	85 29 0b 60 08 00 45 00	h..... .).`..E.
0010	00 2c 41 fe 00 00 2f 06	8b 5a 0a d2 54 69 0a d2	.,A.../. .Z..Ti..
0020	54 67 ef 8b 1f 90 a5 6e	24 9f 00 00 00 00 60 02	Tg.....n \$......
0030	10 00 f0 88 00 00 02 04	05 b4

图3 Wireshark捕捉数据包

/ 实际操作

图中可以发现每发送一次，wireshark会捕捉到真实IP和伪造IP各一条，这是因为在探测目标主机端口8080会将真实IP发送出去，如只是选择发送伪造数据包是不会出现真实IP地址。捕捉到伪造的IP地址10.210.84.15，说明IP源地址伪造成功。

/预防方法

- 使用随机化的初始序列号
- 使用网络层安全传输协议
- 避免采用IP地址信任的策略
- 在路由器和网关上实施包过滤

Thank you
