华中科技大学
计算机网络实验报告

实验名称 lab02-SYN flood 攻击及 SYN cookie 原理分析

姓　名	专业	学　　号	贡献百分比	得 分
王科俨	人工智能自动化	M202072949	1	

注：团队成员贡献百分比之和为 1

教师评语：

一. 环境（详细说明实验运行的操作系统，网络平台，机器的配置）

操作系统：SEEDUbuntu-16.04-32bit

网络拓扑模拟：GNS3

虚拟机：VirtualBox

抓包工具：wireshark

二. 实验目的

通过 VirtualBox 创建 2 台虚拟机并用 GNS3 搭建网络拓扑结构，对目标主机发起 SYN 泛洪攻击，然后修改目标主机 linux 内核相关参数后再次对目标主机发起 SYN 泛洪攻击，使用 wireshark 在目标主机上观察对比两次攻击产生的报文，通过本次实验理解 SYN 泛洪攻击以及 SYN Cookie 的原理。

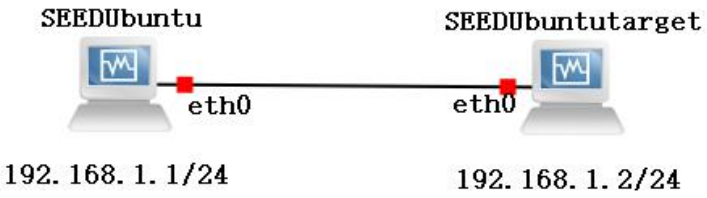
三. 实验步骤（包括主要流程和说明）

I. 使用 VirtualBox 创建虚拟机

新建一个虚拟机，名称为 SEED Ubuntu，类型为 Linux，版本选择 Ubuntu(32-bit)，内存 1G，使用实验提供的虚拟硬盘文件创建，使用该主机发起 SYN 泛洪攻击。同理创建另一个名为 SEED Ubuntu target 的主机作为 SYN 泛洪攻击的目标。结果如下图所示：

II. 使用 GNS3 搭建网络拓扑结构

打开GNS3,新建一个名称为Lab02的项目,在首选项中找到VirtualBox VMs处，通过 New 新建 SEED Ubuntu 和 SEED Ubuntu target 模版，然后搭建如下的网络拓扑结构（将 SEED Ubuntu 的 eth0 网卡和 SEED Ubuntu target 的 eth0 网卡相连）：



III. 配置虚拟机 IP 地址及路由

搭建完网络拓扑结构后，运行虚拟机，使用

sudo ip address add {NETWORK/MASK} dev {ADAPTOR}

命令按下表配置 IP 地址:

	SEED Ubuntu	SEED Ubuntu target
IP 地址	192.168.1.1/24	192.168.1.2/24

即在 SEED Ubuntu 的终端输入

sudo ip address add 192.168.1.1/24 dev eth0

上命令为 SEED Ubuntu 的 eth0 网卡添加 192.168.1.1/24 的 IP 地址，使用 *ip address|grep eth0* 查看 IP 地址结果如下:

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdi
sc pfifo_fast state UP group default qlen 1000
    inet 192.168.1.1/24 scope global eth0
```

同理为 SEED Ubuntu target 配置 IP 地址

使用命令 *sudo ip route add default via 192.168.1.1* 将 SEED Ubuntu 的 IP 地址作为 SEED Ubuntu target 的默认路由，使用 *ip route* 查看 target 的路由信息，结果如下:

```
default via 192.168.1.1 dev eth0
169.254.0.0/16 dev eth0  scope link  metric 1000
192.168.1.0/24 dev eth0  proto kernel  scope link  src
192.168.1.2
```

在 target 主机上 *ping 192.168.1.1*，结果如下:

```
[12/09/20]seed@VM:~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=1.26
ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=1.04
ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.831
 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=0.774
 ms
```

至此 IP 地址和路由配置完毕

IV. 发起 SYN Flood 攻击

在 SEED Ubuntu target 上启动 telnet 服务:

service openbsd-inetd start

先在 SEED Ubuntu 上使用 *telnet 192.168.1.2* 测试:

```
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-gener
ic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

1 package can be updated.
0 updates are security updates.
```

成功登录!

在 SEED Ubuntu 上使用 *netwox 76 -i 192.168.1.2 --dst-port 23* 对 target 进行 SYN Flood 攻击，在 target 上使用 wireshark 观察攻击报文，结果如下:

1	2020-…	192.168.1.2	242.142.115…	TCP	60	40425 → 23 [SYN] Seq=291526…
2	2020-…	242.142.115…	192.168.1.2	TCP	58	23 → 40425 [SYN, ACK] Seq=1…
3	2020-…	192.168.1.2	247.4.234.51	TCP	60	7998 → 23 [SYN] Seq=3612438…
4	2020-…	247.4.234.51	192.168.1.2	TCP	58	23 → 7998 [SYN, ACK] Seq=27…
5	2020-…	192.168.1.2	158.189.52.1	TCP	60	29466 → 23 [SYN] Seq=230364…
6	2020-…	158.189.52.1	192.168.1.2	TCP	58	23 → 29466 [SYN, ACK] Seq=1…
7	2020-…	192.168.1.2	72.57.94.109	TCP	60	23399 → 23 [SYN] Seq=162081…
8	2020-…	72.57.94.109	192.168.1.2	TCP	58	23 → 23399 [SYN, ACK] Seq=8…
9	2020-…	192.168.1.2	191.28.67.58	TCP	60	36186 → 23 [SYN] Seq=202347…
10	2020-…	191.28.67.58	192.168.1.2	TCP	58	23 → 36186 [SYN, ACK] Seq=3…
11	2020-…	192.168.1.2	145.234.249…	TCP	60	16126 → 23 [SYN] Seq=371808…
12	2020-…	145.234.249…	192.168.1.2	TCP	58	23 → 16126 [SYN, ACK] Seq=2…

在 target 主机上输入命令 *netstat -tn*，结果如下：

```
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Add
ress         State
tcp        0      0 192.168.1.2:23          9.59.96.246
:34894       SYN_RECV
tcp        0      0 192.168.1.2:23          187.209.72.
126:33443    SYN_RECV
tcp        0      0 192.168.1.2:23          40.101.178.
214:45992    SYN_RECV
tcp        0      0 192.168.1.2:23          157.64.158.
245:46324    SYN_RECV
tcp        0      0 192.168.1.2:23          15.169.229.
221:43303    SYN_RECV
tcp        0      0 192.168.1.2:23          96.117.204.
212:5370     SYN_RECV
tcp        0      0 192.168.1.2:23          108.237.239
.48:18951    SYN_RECV
tcp        0      0 192.168.1.2:23          220.148.67.
0:6055       SYN_RECV
tcp        0      0 192.168.1.2:23          242.142.115
```

此时在 SEED Ubuntu 上 *telnet 192.168.1.2* 依旧出现了登录提示

```
[12/09/20]seed@VM:~$ telnet 192.168.1.2
Trying 192.168.1.2...
Connected to 192.168.1.2.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login:
Login timed out after 60 seconds.
Connection closed by foreign host.
[12/09/20]seed@VM:~$
```

V. 配置 linux 内核 tcp syn cookie 相关参数

在 target 主机上使用 *echo 0>/proc/sys/net/ipv4/tcp_syncookies* 关闭 syn cookie 机制，使用 *sysctl -w net.ipv4.tcp_max_syn_backlog=5* 将半开链接上限设置为 5。

VI. 再次发起 SYN Flood 攻击

同步骤 IV，通过 wireshark 观察报文结果如下：

```
    1 2020-… 192.168.1.2  111.164.75.… TCP      60 46463 → 23 [SYN] Seq=3139170
    2 2020-… 111.164.75.… 192.168.1.2  TCP      58 23 → 46463 [SYN, ACK] Seq=30
    3 2020-… 192.168.1.2  64.81.77.215 TCP      60 32521 → 23 [SYN] Seq=3126820
    4 2020-… 64.81.77.215 192.168.1.2  TCP      58 23 → 32521 [SYN, ACK] Seq=17
    5 2020-… 192.168.1.2  162.41.183.… TCP      60 63067 → 23 [SYN] Seq=3738384
    6 2020-… 162.41.183.… 192.168.1.2  TCP      58 23 → 63067 [SYN, ACK] Seq=32
    7 2020-… 192.168.1.2  77.99.107.38 TCP      60 17066 → 23 [SYN] Seq=1245876
    8 2020-… 77.99.107.38 192.168.1.2  TCP      58 23 → 17066 [SYN, ACK] Seq=28
    9 2020-… 192.168.1.2  144.71.243.… TCP      60 57235 → 23 [SYN] Seq=3169377
   10 2020-… 144.71.243.… 192.168.1.2  TCP      58 23 → 57235 [SYN, ACK] Seq=39
   11 2020-… 192.168.1.2  158.81.242.… TCP      60 49096 → 23 [SYN] Seq=6014117
   12 2020-… 192.168.1.2  208.149.235… TCP      60 23545 → 23 [SYN] Seq=1546148
   13 2020-… 192.168.1.2  227.184.253… TCP      60 57382 → 23 [SYN] Seq=8179645
   14 2020-… 192.168.1.2  12.69.53.57  TCP      60 18591 → 23 [SYN] Seq=2436747
   15 2020-… 192.168.1.2  76.161.114.… TCP      60 16967 → 23 [SYN] Seq=1676495
```

Netstat -tn 结果如下,仅有 5 条连接:

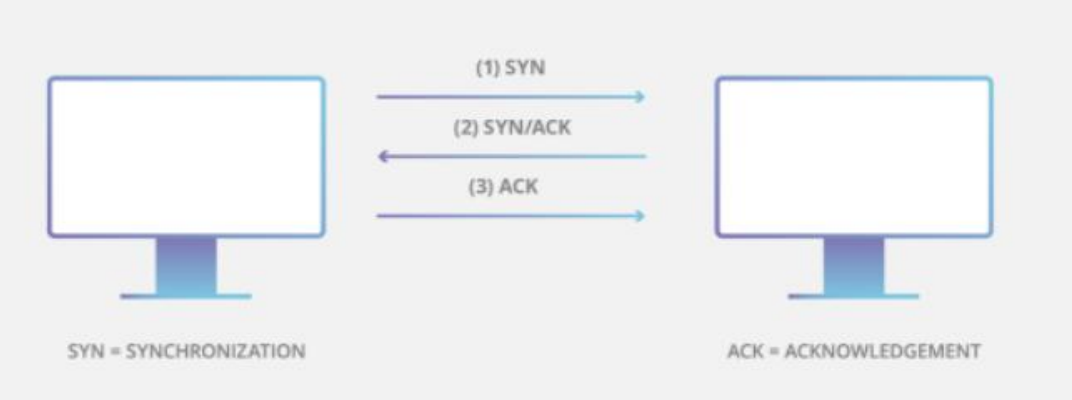
```
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Add
ress         State
tcp        0      0 192.168.1.2:23          77.99.107.3
8:17066      SYN_RECV
tcp        0      0 192.168.1.2:23          162.41.183.
74:63067     SYN_RECV
tcp        0      0 192.168.1.2:23          64.81.77.21
5:32521      SYN_RECV
tcp        0      0 192.168.1.2:23          111.164.75.
170:46463    SYN_RECV
tcp        0      0 192.168.1.2:23          144.71.243.
127:57235    SYN RECV
```

在 SEED Ubuntu 上 telnet 192.168.1.2，无法建立连接

```
[12/09/20]seed@VM:~$ telnet 192.168.1.2
Trying 192.168.1.2...
telnet: Unable to connect to remote host: Connection ti
med out
```

四. 实验结果和分析

I. TCP 三次握手



一个完整的 TCP 连接包括三个过程:

① 客户端向服务器发送 SYN 报文启动连接

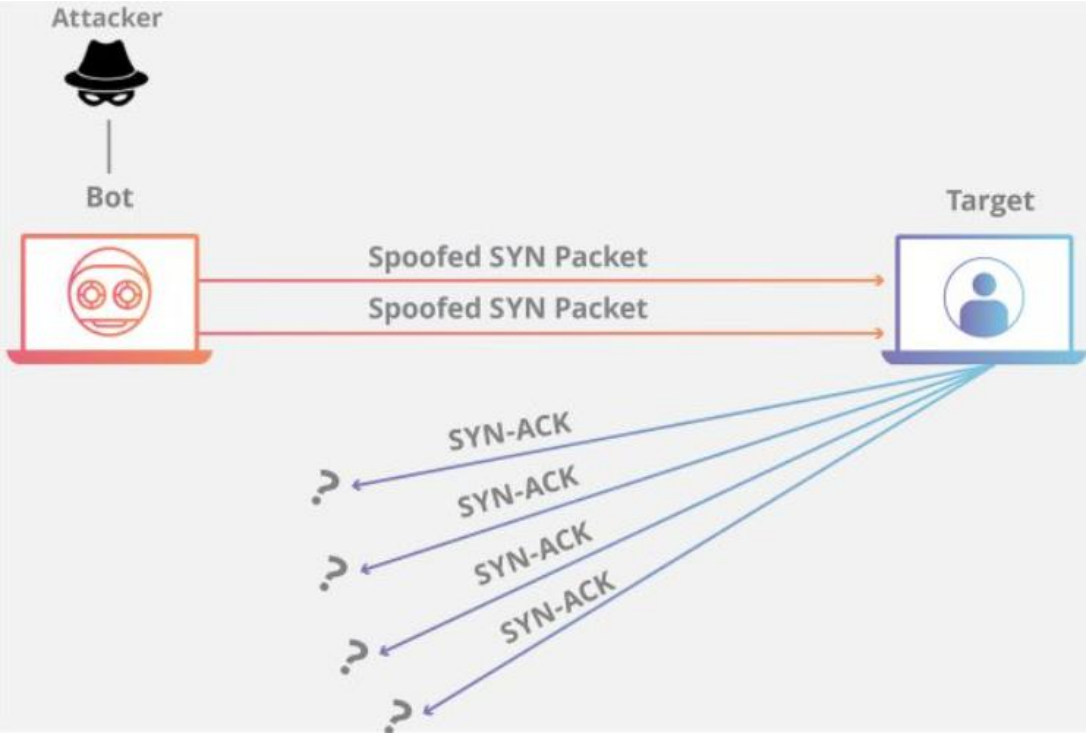
② 服务器向客户端发送 SYN/ACK 报文回应，确认通信，此时 TCP 连接处于 SYN_RCVD 状态

③ 客户端返回 ACK 报文确认从服务器接收到报文。完成此报文发送和接受序列后，TCP 连接处于 ESTABLISHED 状态，能够发送和接收数据。

II. SYN Flood 攻击原理

SYN 泛洪攻击是一种 DoS 攻击。在收到 SYN 数据包后，服务器将发送 SYN/ACK 数据包进行回应，等待来自客户的 ACK 报文段。如果某客户不发送 ACK 来完成三次握手的最后一步，最终服务器将终止该半开连接并回收资源。

攻击者通过发送大量的 TCP SYN 报文段，而不完成第三次握手，服务器会不断地为这些半开连接分配资源，即使从未使用，直至服务器资源消耗殆尽。



在第二次泛洪攻击中，将内核参数设置为 tcp_syncookies=0，tcp_max_syn_backlog=5，由于泛洪攻击，服务器一直维持着 5 个半开连接，

使用 *watch -n 0.1 netstat -tn* 观察发现，半开连接在经过大约一分钟后被终止但服务器又会收到新的 SYN 报文然后继续维持上限 5 的半开连接，一旦处于 SYN_RCVD 状态的 TCP 连接达到上限 tcp_max_syn_backlog 即 5 个时，新的 SYN 报文将会被服务器丢弃，所以在 SEED Ubuntu 上无法建立 telnet 连接。

III. SYN Cookies 原理

启用 SYN Cookies 后，在收到一个 SYN 报文段时，服务器不会为该报文段生成一个半开连接，而是生成一个初始 TCP 序列号，它是 SYN 报文段源地址、目的地址、端口号以及服务器上的秘密数的复杂函数。这种序列号被称为“cookie”，服务器不记忆该 cookie 或任何对应于 SYN 的其他状态信息。

服务器使用 cookie 检验客户是否合法，合法则生成一个全开连接，若客服不返回 ACK 报文段，因为服务器并没有分配任何资源因此也不会对服务器造成危害。

第一次泛洪攻击由于开启了 Cookie，因此服务器资源没有被耗尽，从而成功地建立了 telnet 连接。