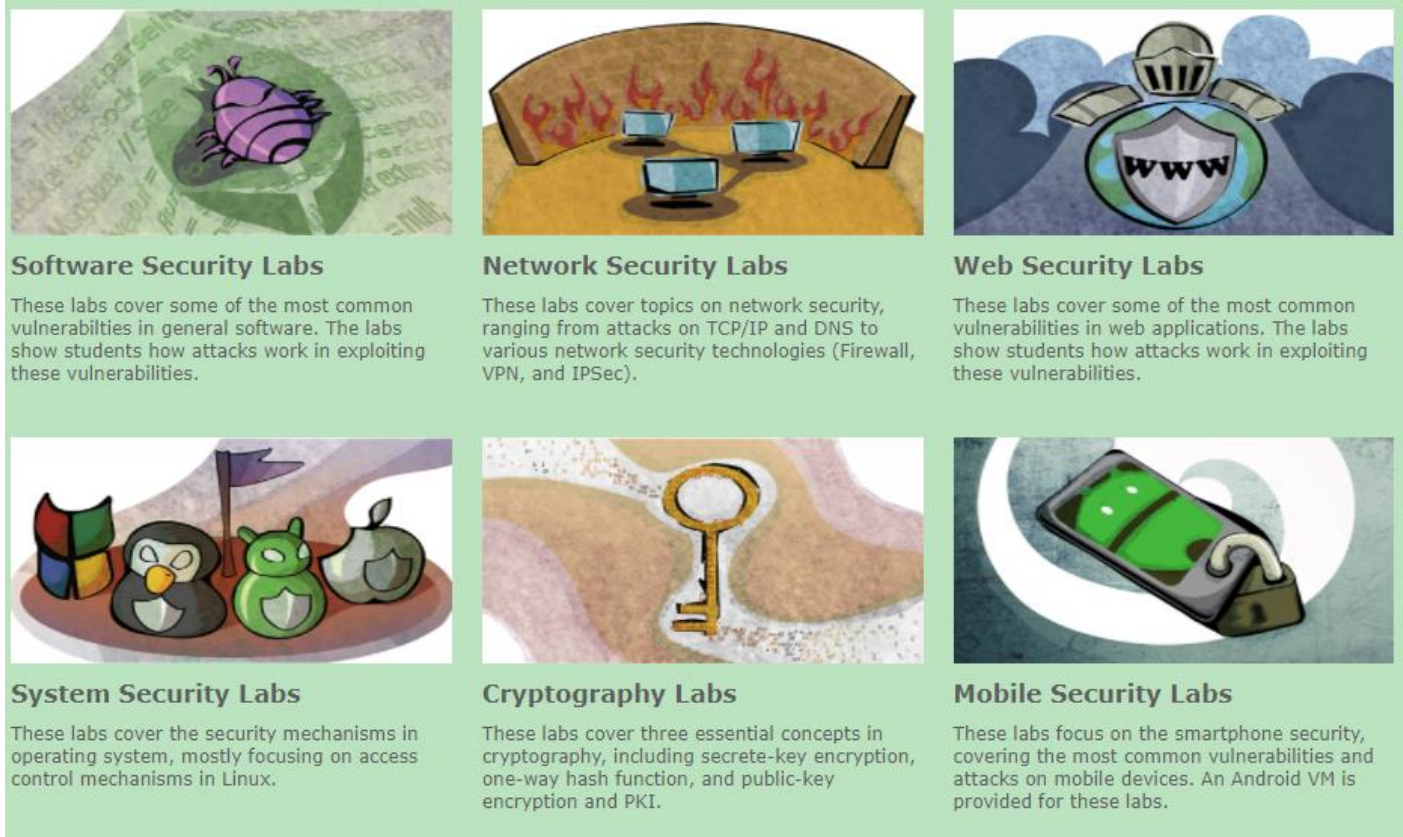
SYN flood攻击及SYN cookie原理分析

1.简介

- SEED：计算机安全教育的教学实验平台
- http://www.cis.syr.edu/~wedu/seed/
- 纽约雪城大学 杜文亮 (Du, Wenliang)教授设计和实现，从2002年开始得到NSF 1.2M$的资助
-

1.简介

- SEED内容包含一下几类：



Software Security Labs

These labs cover some of the most common vulnerabilties in general software. The labs show students how attacks work in exploiting these vulnerabilities.

Network Security Labs

These labs cover topics on network security, ranging from attacks on TCP/IP and DNS to various network security technologies (Firewall, VPN, and IPSec).

Web Security Labs

These labs cover some of the most common vulnerabilities in web applications. The labs show students how attacks work in exploiting these vulnerabilities.

System Security Labs

These labs cover the security mechanisms in operating system, mostly focusing on access control mechanisms in Linux.

Cryptography Labs

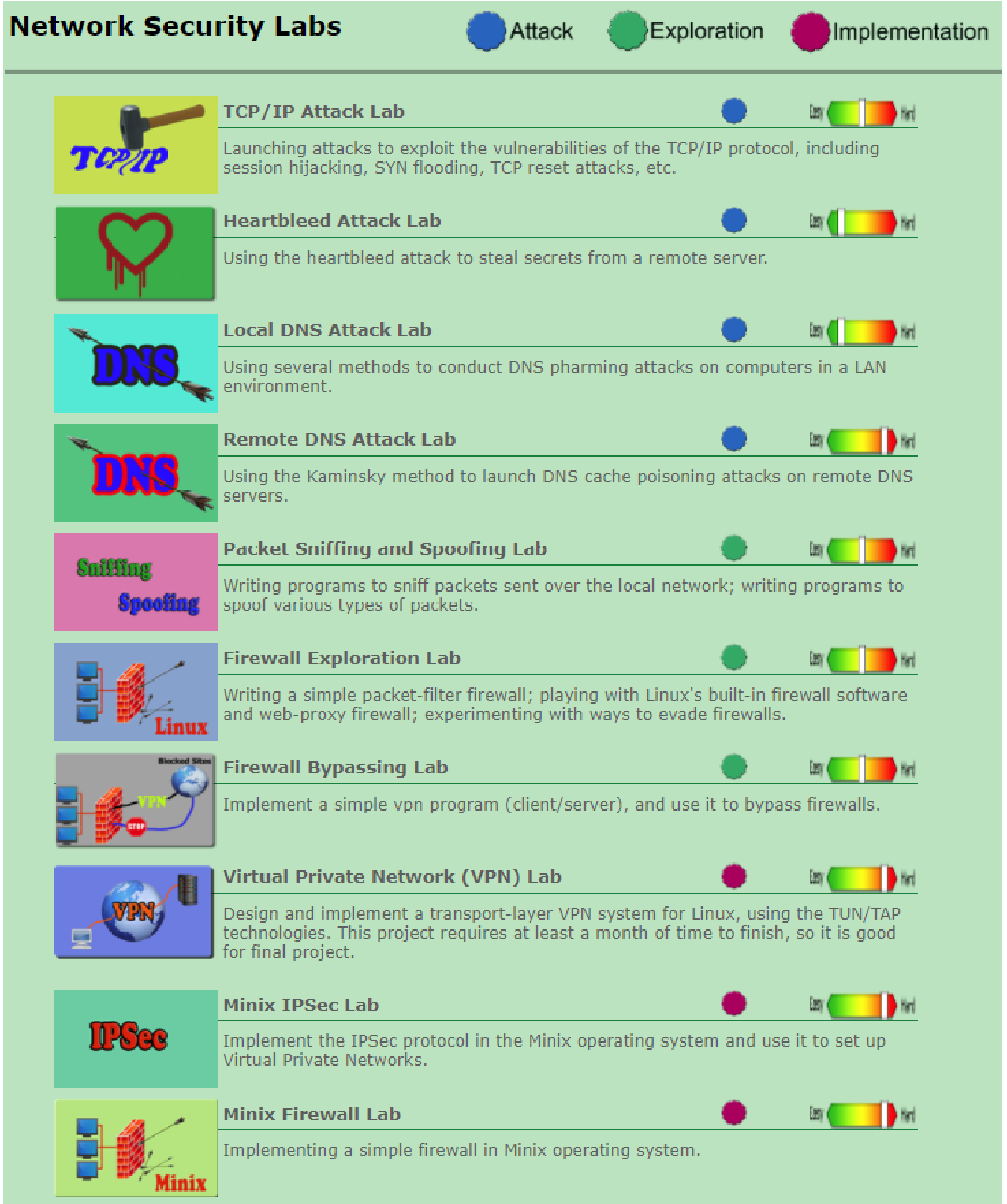
These labs cover three essential concepts in cryptography, including secrete-key encryption, one-way hash function, and public-key encryption and PKI.

Mobile Security Labs

These labs focus on the smartphone security, covering the most common vulnerabilities and attacks on mobile devices. An Android VM is provided for these labs.

1.简介

- 网络安全主要包括10大实验
- 分为攻击类、破解类、实现类
- 难度越大，消耗的时间越长



Network Security Labs ● Attack ● Exploration ● Implementation

TCP/IP Attack Lab ●

Launching attacks to exploit the vulnerabilities of the TCP/IP protocol, including session hijacking, SYN flooding, TCP reset attacks, etc.

Heartbleed Attack Lab ●

Using the heartbleed attack to steal secrets from a remote server.

Local DNS Attack Lab ●

Using several methods to conduct DNS pharming attacks on computers in a LAN environment.

Remote DNS Attack Lab ●

Using the Kaminsky method to launch DNS cache poisoning attacks on remote DNS servers.

Packet Sniffing and Spoofing Lab ●

Writing programs to sniff packets sent over the local network; writing programs to spoof various types of packets.

Firewall Exploration Lab ●

Writing a simple packet-filter firewall; playing with Linux's built-in firewall software and web-proxy firewall; experimenting with ways to evade firewalls.

Firewall Bypassing Lab ●

Implement a simple vpn program (client/server), and use it to bypass firewalls.

Virtual Private Network (VPN) Lab ●

Design and implement a transport-layer VPN system for Linux, using the TUN/TAP technologies. This project requires at least a month of time to finish, so it is good for final project.

Minix IPSec Lab ●

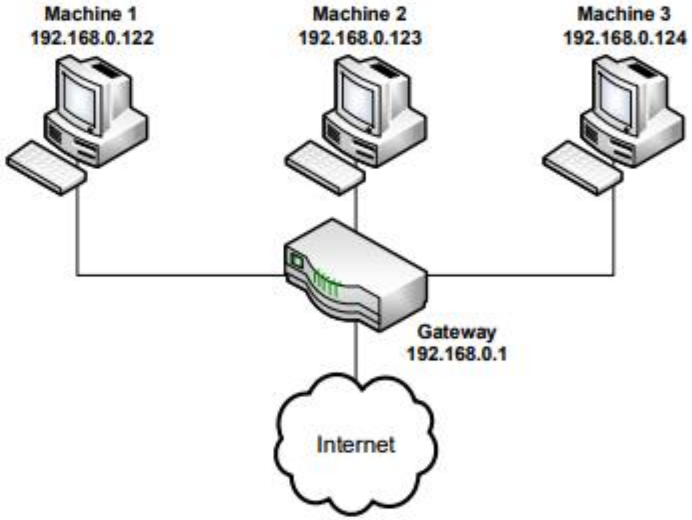
Implement the IPSec protocol in the Minix operating system and use it to set up Virtual Private Networks.

Minix Firewall Lab ●

Implementing a simple firewall in Minix operating system.

2.TCP/IP Attack Lab

- Netwox Tools作为报文生成工具
- Wireshark 报文截获工具
- 启动 ftp and telnet Servers



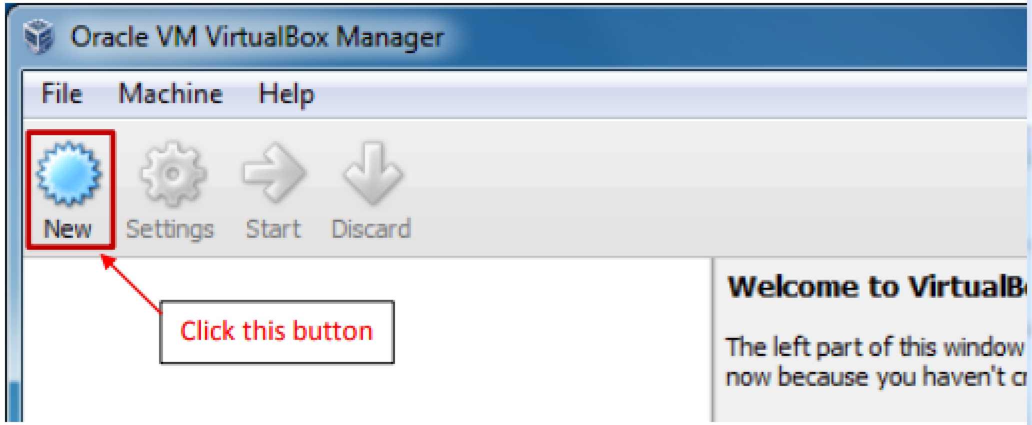
- Task 1 : SYN Flooding Attack
- Task 2 : TCP RST Attacks on telnet and ssh Conr
- Task 3 : TCP RST Attacks on Video Streaming Applications
- Task 4 : TCP Session Hijacking
- Task 5 : Creating Reverse Shell using TCP Session Hijacking
- 注意：攻击者可以观察到被攻击者的流量

2.TCP/IP Attack Lab

- netwox Tools一共提供了200多个工具
- 运行netwox，进入界面后
- 选项3搜索工具
- 选项4显示帮助

2.使用步骤

- VirtualBox新建虚拟机

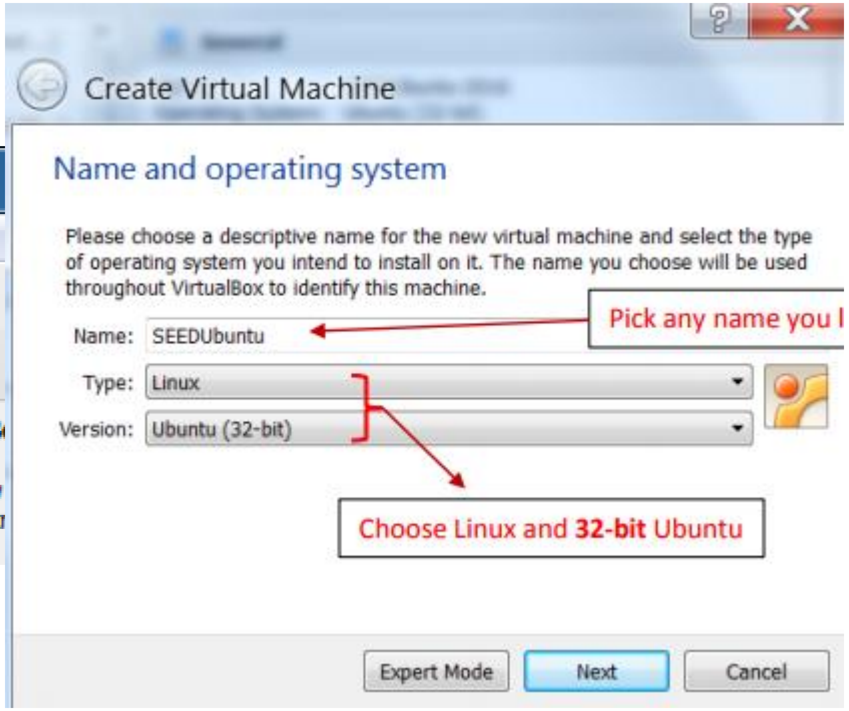


Oracle VM VirtualBox Manager

Click this button

Welcome to VirtualB

The left part of this window
now because you haven't cr



Create Virtual Machine

Name and operating system

Please choose a descriptive name for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name: SEEDUbuntu

Type: Linux

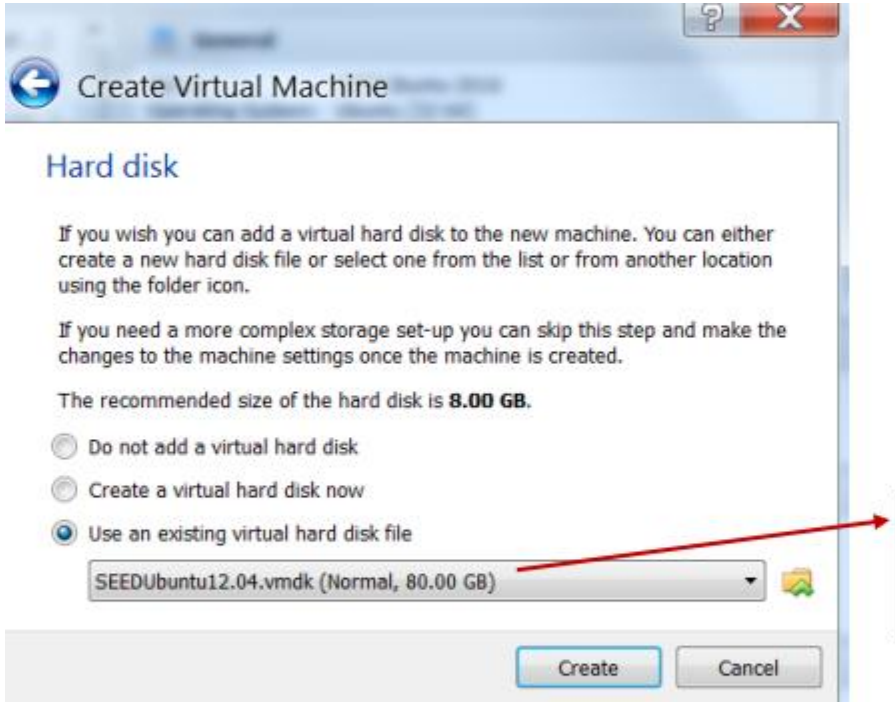
Version: Ubuntu (32-bit)

Pick any name you l

Choose Linux and **32-bit** Ubuntu

2.使用步骤

- 导入SEED 虚拟机镜像文件， 运行虚拟机



Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard disk is **8.00 GB**.

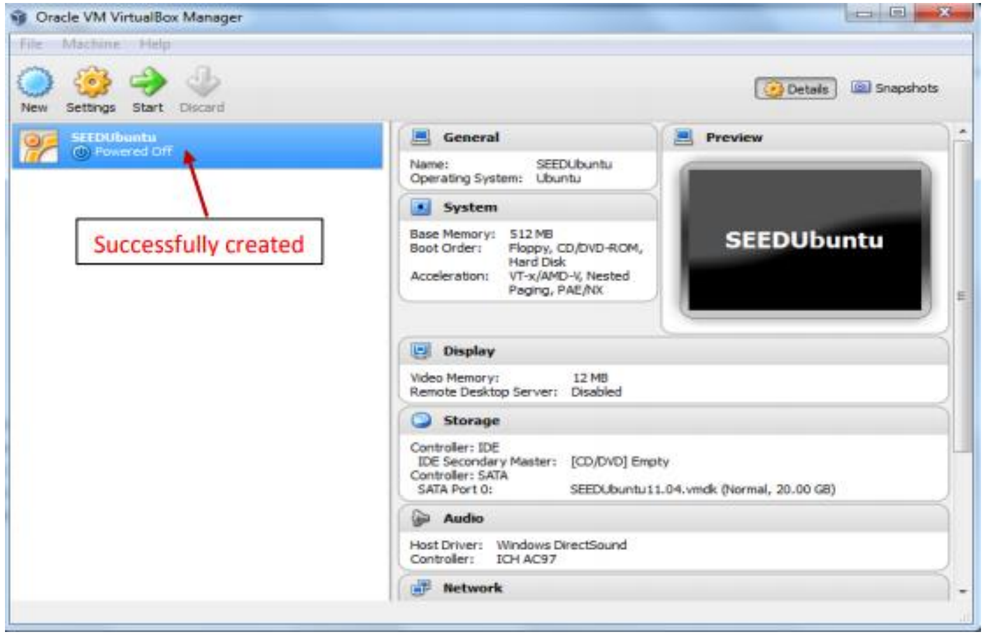
○ Do not add a virtual hard disk

○ Create a virtual hard disk now

● Use an existing virtual hard disk file

SEEDUbuntu12.04.vmdk (Normal, 80.00 GB)

Pick the **SEEDUbuntu12.04.vmdk** file



Successfully created

General

Name: SEEDUbuntu
Operating System: Ubuntu

System

Base Memory: 512 MB
Boot Order: Floppy, CD/DVD-ROM, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX

Display

Video Memory: 12 MB
Remote Desktop Server: Disabled

Storage

Controller: IDE
IDE Secondary Master: [CD/DVD] Empty
Controller: SATA
SATA Port 0: SEEDUbuntu11.04.vmdk (Normal, 20.00 GB)

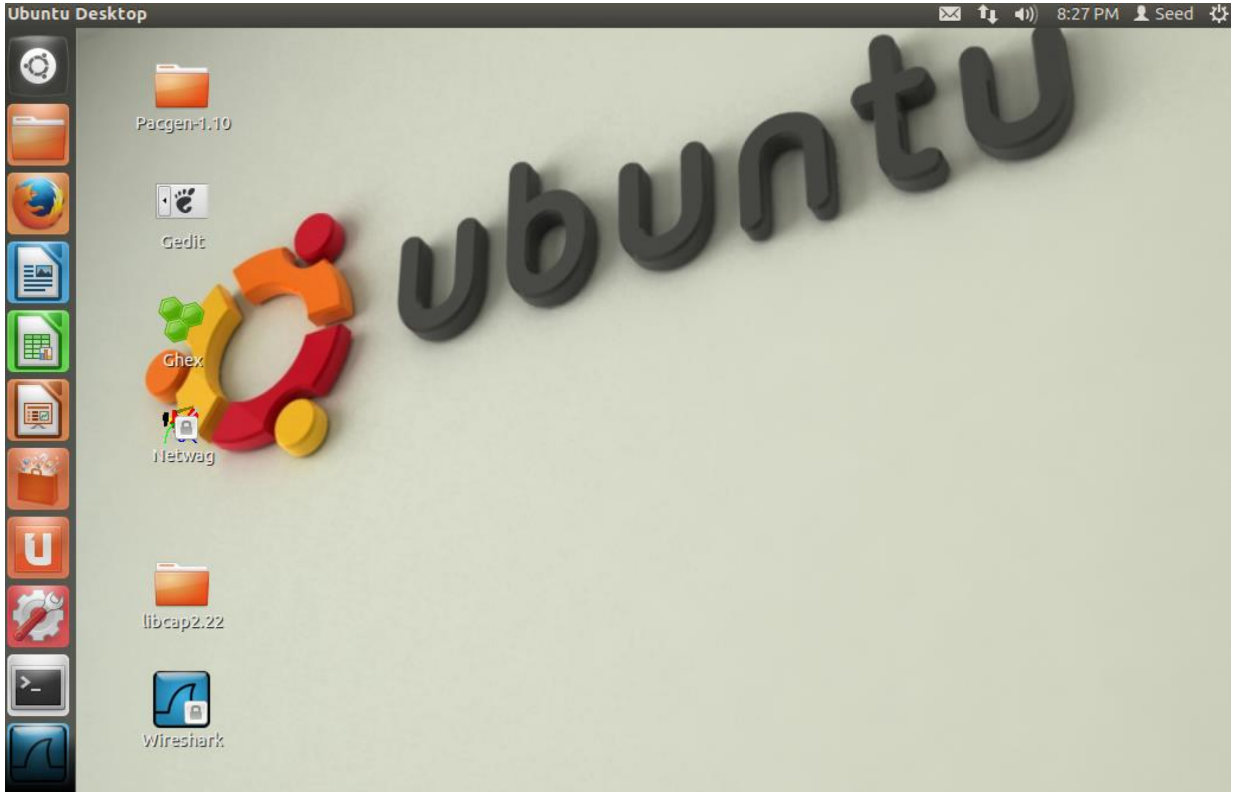
Audio

Host Driver: Windows DirectSound
Controller: ICH AC97

Network

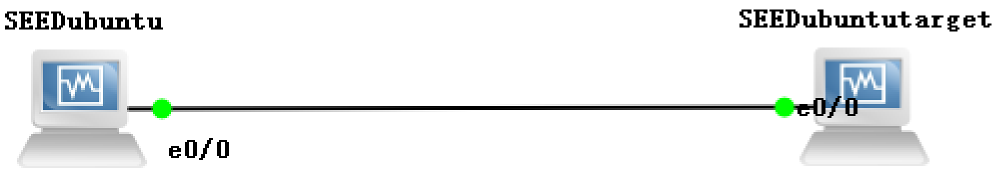
2.使用步骤

- 普通用户登陆，有特权操作再su
- 超级用户 User ID: root, Password: seedubuntu.
- 普通用户 User ID: seed, Password: dees



2.使用步骤

- 利用GNS3配置如图网络
- SEED ubuntu 攻击 SEED Ubuntu target
- 配置好两台主机的地址和路由



2.使用步骤

- ###配置IP地址命令：
- ip address显示地址
- sudo ip address add 192.168.1.1/24 dev eth0 添加IP
- sudo ip address del 192.168.1.1/24 dev eth0 删除IP

- ####增加路由
- ip route显示路由
- sudo ip route add 192.168.1.0/24 dev eth0
- sudo ip route del 192.168.1.0/24 dev eth0

- ####增加路由
- ip route add {NETWORK/MASK} via {GATEWAYIP}
- ####增加默认路由
- ip route add default via 192.168.1.1

- 永久修改网络配置，图形界面配置

2.使用步骤

- SEED Ubuntu target上启动telnet服务:

service service openbsd-inetd start

- 攻击命令:

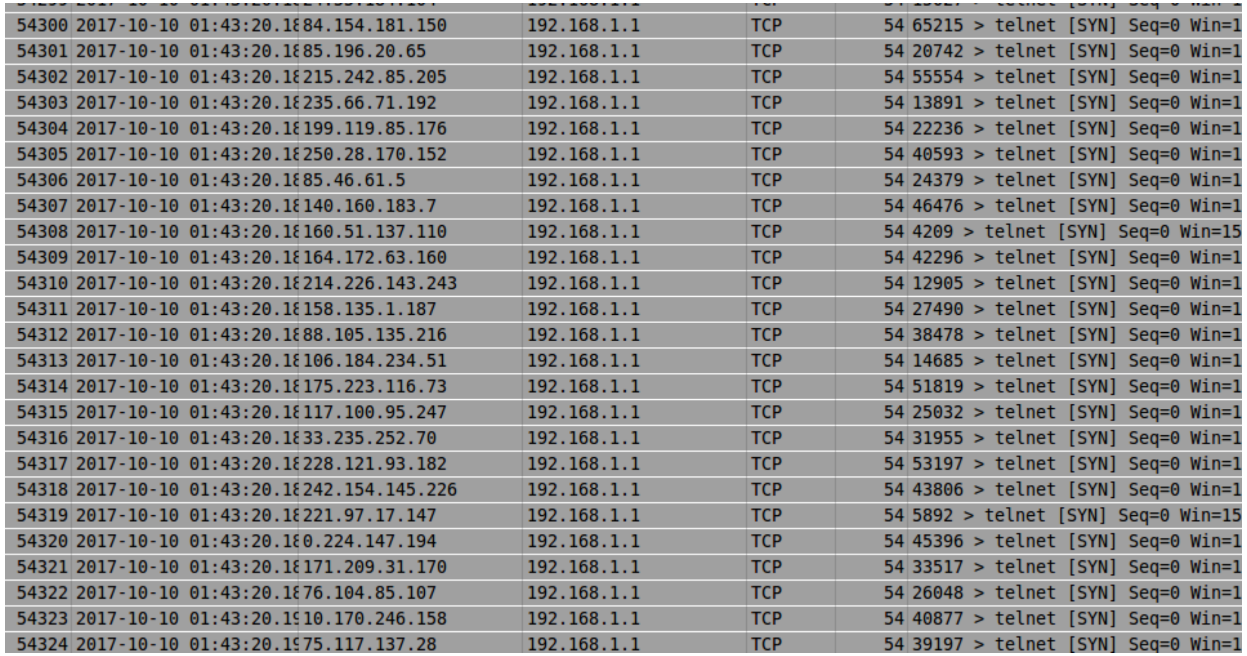
netwox 76 -i 192.168.1.1 --dst-port 23

- 可以在SEED ubuntu 或者 SEED Ubuntu target 上用tcpdump或者wireshark观察攻击报文:

如左图

- 可以在SEED ubuntu 或者 SEED Ubuntu target 上用tcpdump或者wireshark观察建立连接:

netstat –n --tcp



```
54300 2017-10-10 01:43:20.18 84.154.181.150    192.168.1.1   TCP   54 65215 > telnet [SYN] Seq=0 Win=1
54301 2017-10-10 01:43:20.18 85.196.20.65      192.168.1.1   TCP   54 20742 > telnet [SYN] Seq=0 Win=1
54302 2017-10-10 01:43:20.18 215.242.85.205    192.168.1.1   TCP   54 55554 > telnet [SYN] Seq=0 Win=1
54303 2017-10-10 01:43:20.18 235.66.71.192     192.168.1.1   TCP   54 13891 > telnet [SYN] Seq=0 Win=1
54304 2017-10-10 01:43:20.18 199.119.85.176    192.168.1.1   TCP   54 22236 > telnet [SYN] Seq=0 Win=1
54305 2017-10-10 01:43:20.18 250.28.170.152    192.168.1.1   TCP   54 40593 > telnet [SYN] Seq=0 Win=1
54306 2017-10-10 01:43:20.18 85.46.61.5        192.168.1.1   TCP   54 24379 > telnet [SYN] Seq=0 Win=1
54307 2017-10-10 01:43:20.18 140.160.183.7     192.168.1.1   TCP   54 46476 > telnet [SYN] Seq=0 Win=1
54308 2017-10-10 01:43:20.18 160.51.137.110    192.168.1.1   TCP   54 4209 > telnet [SYN] Seq=0 Win=15
54309 2017-10-10 01:43:20.18 164.172.63.160    192.168.1.1   TCP   54 42296 > telnet [SYN] Seq=0 Win=1
54310 2017-10-10 01:43:20.18 214.226.143.243   192.168.1.1   TCP   54 12905 > telnet [SYN] Seq=0 Win=1
54311 2017-10-10 01:43:20.18 158.135.1.187     192.168.1.1   TCP   54 27490 > telnet [SYN] Seq=0 Win=1
54312 2017-10-10 01:43:20.18 88.105.135.216    192.168.1.1   TCP   54 38478 > telnet [SYN] Seq=0 Win=1
54313 2017-10-10 01:43:20.18 106.184.234.51    192.168.1.1   TCP   54 14685 > telnet [SYN] Seq=0 Win=1
54314 2017-10-10 01:43:20.18 175.223.116.73    192.168.1.1   TCP   54 51819 > telnet [SYN] Seq=0 Win=1
54315 2017-10-10 01:43:20.18 117.100.95.247    192.168.1.1   TCP   54 25032 > telnet [SYN] Seq=0 Win=1
54316 2017-10-10 01:43:20.18 33.235.252.70     192.168.1.1   TCP   54 31955 > telnet [SYN] Seq=0 Win=1
54317 2017-10-10 01:43:20.18 228.121.93.182    192.168.1.1   TCP   54 53197 > telnet [SYN] Seq=0 Win=1
54318 2017-10-10 01:43:20.18 242.154.145.226   192.168.1.1   TCP   54 43806 > telnet [SYN] Seq=0 Win=1
54319 2017-10-10 01:43:20.18 221.97.17.147     192.168.1.1   TCP   54 5892 > telnet [SYN] Seq=0 Win=15
54320 2017-10-10 01:43:20.18 0.224.147.194     192.168.1.1   TCP   54 45396 > telnet [SYN] Seq=0 Win=1
54321 2017-10-10 01:43:20.18 171.209.31.170    192.168.1.1   TCP   54 33517 > telnet [SYN] Seq=0 Win=1
54322 2017-10-10 01:43:20.18 76.104.85.107     192.168.1.1   TCP   54 26048 > telnet [SYN] Seq=0 Win=1
54323 2017-10-10 01:43:20.19 10.170.246.158    192.168.1.1   TCP   54 40877 > telnet [SYN] Seq=0 Win=1
54324 2017-10-10 01:43:20.19 75.117.137.28     192.168.1.1   TCP   54 39197 > telnet [SYN] Seq=0 Win=1
```

3.进一步观察linux内核tcp syn cookie机制

配置内核参数的两种方式:

- cat /proc/sys/net/ipv4/tcp_syncookies
- echo 0 > /proc/sys/net/ipv4/tcp_syncookies
- sysctl –a | grep net.ipv4.tcp_max_syn_backlog
- sysctl -w net.ipv4.tcp_max_syn_backlog = 5

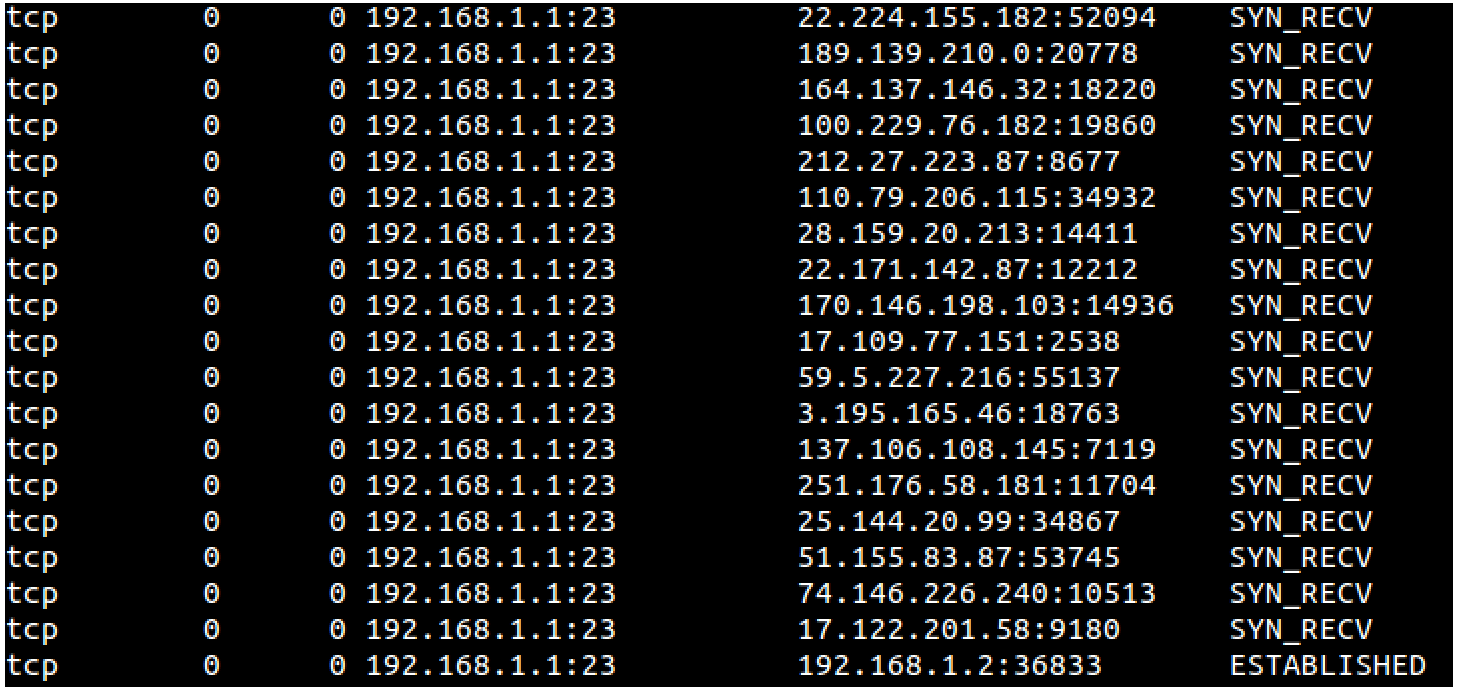
3.进一步观察linux内核tcp syn cookie机制

比较打开和关闭SEED Ubuntu target内核tcp syn cookie参数，syn flood攻击的效果：

1. 设置SEED Ubuntu target上， net.ipv4.tcp_max_syn_backlog=5
2. 设置SEED Ubuntu target上， net.ipv4. tcp_syncookies=0
3. 从SEED Ubuntu 上用netwox的syn flood攻击SEED Ubuntu target
4. 同时从SEED Ubuntu 上用telnet 主机 SEED Ubuntu target，看能否建立连接？

3.进一步观察linux内核tcp syn cookie机制

打开SEED Ubuntu target内核tcp syn cookie参数，同时从SEED Ubuntu 上用 telnet 主机 SEED Ubuntu target，看能否建立连接？



```
tcp        0      0 192.168.1.1:23          22.224.155.182:52094    SYN_RECV
tcp        0      0 192.168.1.1:23          189.139.210.0:20778     SYN_RECV
tcp        0      0 192.168.1.1:23          164.137.146.32:18220    SYN_RECV
tcp        0      0 192.168.1.1:23          100.229.76.182:19860    SYN_RECV
tcp        0      0 192.168.1.1:23          212.27.223.87:8677      SYN_RECV
tcp        0      0 192.168.1.1:23          110.79.206.115:34932    SYN_RECV
tcp        0      0 192.168.1.1:23          28.159.20.213:14411     SYN_RECV
tcp        0      0 192.168.1.1:23          22.171.142.87:12212     SYN_RECV
tcp        0      0 192.168.1.1:23          170.146.198.103:14936   SYN_RECV
tcp        0      0 192.168.1.1:23          17.109.77.151:2538      SYN_RECV
tcp        0      0 192.168.1.1:23          59.5.227.216:55137      SYN_RECV
tcp        0      0 192.168.1.1:23          3.195.165.46:18763      SYN_RECV
tcp        0      0 192.168.1.1:23          137.106.108.145:7119    SYN_RECV
tcp        0      0 192.168.1.1:23          251.176.58.181:11704    SYN_RECV
tcp        0      0 192.168.1.1:23          25.144.20.99:34867      SYN_RECV
tcp        0      0 192.168.1.1:23          51.155.83.87:53745      SYN_RECV
tcp        0      0 192.168.1.1:23          74.146.226.240:10513    SYN_RECV
tcp        0      0 192.168.1.1:23          17.122.201.58:9180      SYN_RECV
tcp        0      0 192.168.1.1:23          192.168.1.2:36833       ESTABLISHED
```

4. 实验报告要求

1. 写出完整的实验配置过程，包括拓扑结构和配置命令
2. 用截图的方式描述实验结果
3. 描述tcp syn cookie的原理
4. 交实验报告，2018-12-20之前以附件形式发送到邮箱 **hust_network@163.com**，报告文件名称：学院专业-学号-名字-实验二.doc