Lab6

57117221 姚远

Linux Firewall Exploration Lab

Task 1: Using Firewall

Machine A的IP地址：192.168.43.123 Machine B的IP地址：192.168.43.159

阻止A对B进行telnet连接；阻止B对A进行telnet连接

未进行任何操作时，A和B可以互相连接：

```
[09/17/20]seed@VM:~$ telnet 192.168.43.159
Trying 192.168.43.159...
Connected to 192.168.43.159.
Escape character is '^]'.
```

```
[09/17/20]seed@VM:~$ telnet 192.168.43.123
Trying 192.168.43.123...
Connected to 192.168.43.123.
```

在主机A处开启防火墙——sudo ufw enable

```
[09/17/20]seed@VM:~$ sudo ufw enable
Firewall is active and enabled on system startup
```

此时主机B无法对A进行telnet连接

```
[09/17/20]seed@VM:~$ telnet 192.168.43.123
Trying 192.168.43.123...
telnet: Unable to connect to remote host: Connection timed out
```

同理，在主机B处开启防火墙，主机A也无法对B进行telnet连接

```
[09/17/20]seed@VM:~$ telnet 192.168.43.159
Trying 192.168.43.159.,
telnet: Unable to connect to remote host: Connection timed out
```

阻止A访问某个外部网页

以www.baidu.com为例，先ping一下百度查看其ip地址

```
[09/17/20]seed@VM:~$ ping www.baidu.com
PING www.a.shifen.com (36.152.44.95) 56(84) bytes of data.
64 bytes from 36.152.44.95: icmp_seq=1 ttl=56 time=24.4 ms
64 bytes from 36.152.44.95: icmp_seq=2 ttl=56 time=40.8 ms
64 bytes from 36.152.44.95: icmp_seq=3 ttl=56 time=33.1 ms
```

添加规则

```
[09/17/20]seed@VM:~$ sudo ufw deny out to 36.152.44.95
Rule added
```

此时再去ping百度，如果ping的是该IP地址，会被拒绝访问.

```
[09/17/20]seed@VM:~ $ ping www.baidu.com
PING www.a.shifen.com (36.152.44.95) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
```

```
[09/17/20]seed@VM:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
36.152.44.95               DENY OUT    Anywhere
36.152.44.96               DENY OUT    Anywhere
```

Task 2: Implementing a Simple Firewall

使用LKM和Netfilter来实现包过滤模块。 在监测点NF_INET_PRE_ROUTING设置阻止主机B的任何访问，故代码如下：

```
#include <linux/kernel.h>
#include <linux/skbuff.h>
#include <linux/ip.h>
#include <linux/netfilter.h>
#include <linux/netfilter_ipv4.h>

static struct nf_hook_ops nfho;
static unsigned char *drop_ip = "\xc0\xa8\x2b\x9f";

unsigned int hook_func(unsigned int hooknum ,
                        struct sk_buff **skb ,
                        const struct net_device *in ,
                        const struct net_device *out ,
                        int (*okfn)(struct sk_buff *))
{
    struct sk_buff *sb = *skb;
    if(ip_hdr(sb)->saddr == *(unsigned int *)drop_ip)
    {
        return NF_DROP;
    }else{
        return NF_ACCEPT;
    }
}

int init_module()
{
    nfho.hook = (nf_hookfn * )hook_func;
    nfho. hooknum = NF_INET_PRE_ROUTING;
    nfho.pf = PF_INET;
    nfho.priority = NF_IP_PRI_FIRST;
    nf_register_hook(&nfho);
    return 0;
}
```

*drop_ip为阻止访问主机的IP地址 注意指针的写法，可能seed的gcc编译较为严格，容易报错。

```
[09/17/20]seed@VM:~$ make
make -C/lib/modules/4.8.0-36-generic/build/ M=/home/seed modules
make[1]: Entering directory '/usr/src/linux-headers-4.8.0-36-generic'
  Cc [M]  /home/seed/hook.0
  Building modules, stage 2.
  MODPOST 1 modules
  LD [M]  /home/seed/hook.ko
make[1]: Leaving directory '/usr/src/linux-headers-4.8.0-36-generic'
[09/17/20]seed@VM:~$ sudo insmod hook.ko
[09/17/20]seed@VM:~$ lsmod
Module                  Size  Used by
hook                   16384  0
vboxsf                 45056  0
```

在内核中加载模块，上图为成功的结果。然后在主机B中尝试连接A，失败。可见阻止成功。

```
[09/17/20]seed@VM:~$ ping 192.168.43.123
PING 192. 168. 43.123 (192.168. 43.123) 56(84) bytes of data.
From 192.168 .43.159 icmp_seq=9 Destination Host Unreachable
From 192. 168.43.159 icmp_seq=10 Destination Host Unreachable
From 192.168 .43.159 icmp_seq=11 Destination Host Unreachable
From 192.168 .43.159 icmp_seq=12 Destination Host Unreachable
From 192.168 .43.159 icmp_seq=13 Destination Host Unreachable
```

Task 3: Evading Egress Filtering

主机A（192.168.43.123）已经设定防火墙，阻止了所有对外telent访问

```
[09/17/20]seed@VM:~$ sudo ufw status
Status: active
To                          Action       From
--                          ------       ----
23/tcp                      REJECT OUT   Anywhere
23/tcp (v6)                 REJECT OUT   Anywhere (v6)
```

主机B（192.168.43.115）不设定防火墙 主机C（192.168.43.159）作为telnet服务器

Task 3.a Telnet to Machine B through the firewall

令主机A穿过防火墙对主机B进行telnet访问。 方法：令A向C发起SSH访问请求，然后以其为跳板telnet访问B

```
root@ubuntu:~# ssh -L 8000: 192.168.43.159:23 root@192.168.43.115
The authenticity of host '192.168.43.115 (192.168.43.115)' can't be
established.
ECDSA key fingerprint is SHA256 : BWfh0ICyunx4S
tCOQYAbWoHZ8de0iph0A53CbUTYQEs.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.43. 115' (ECDSA) to the list of known
hosts.
root@192.168.43.115's password:
Last login: Thu_Sep 17 04:34:25 2020 from 192.168.43.123
```

然后进行telnet连接，成功。

Task 3.b: Connect to Facebook using SSH Tunnel

使用SSH请求连接一个被禁止访问的网址，这里以www.seu.edu.cn为例：

```
[09/17/20]seed@VM:~$ sudo ufw deny out to 121.194.14.142
Rule added
[09/17/20]seed@VM:~$ ping www.seu.edu.cn
PING seu-ipv6.cache.saaswaf.com (121.194.14. 142) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
```

通过SSH通道将主机B作为跳板

```
root@ubuntu:~# ssh -D 9000 -C root@192.168.43.115
root@192.168.43.115's password:
Last login: Thu_Sep 17 04:36:08 2020 from 192.168.43.115
```

此时可以顺利与www.seu.edu.cn通信

退出SSH后，又不可访问

```
root@VM:/home/seed# ping www. seu. edu. cn
PING seu-ipv6.cache.saaswaf.com (121.194.14.142) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
```

Task 4: Evading Ingress Filtering

在主机A中阻止外部对其80端口和22端口的连接 然后通过指令建立ssh通道

```
root@VM:/home/seed# ssh -fCNR 192.168.43.115:917: 192.168.43.123:918
root@192.168.43.115
```

这样主机B就可以反向通过该通道访问到主机A的80端口