Subject: Invisible Server Service **Lecturer: Jirawat Thaenthong** **Organization: Faculty of Technology and Environment, PSU, Phuket Campus.** **Date: 19/5/60** **Version: 1.0** **Objective:** 1. Trainees study basic of invisible server service (door-knock pattern). 2. Trainees practice and use 'knock' and 'iptables' programs to hide service from hacker.	**Approved**

Instructions& Prerequisites:

- Trainees should have basic skill of Linux commands and iptables program.
- Ubuntu 16.04 Virtual machine (VirtualBox/VMware)

Concepts:

- Nmap is a scanner program.
- Nmap refers to closed ports as those that do not have a daemon listening behind them.
- Nmap refers to filtered ports, it means that a firewall of some kind is preventing access to the IP address that is scanning
- Nmap reports three states, such as unfiltered, open/filtered, and closed/filtered.
- Nmap, https://nmap.org/book/man-port-scanning-basics.html
- iptables DROP is different from iptables REJECT
    - Use REJECT rule when you want the other know the port is unreachable, and use DROP rule for connections to hosts you don't want people to see.
- Use iptables to block some port with '–j REJECT' pattern ← This generates an ICMP Port Unreachable response. Hacker will learn the port was blocked with '-j REJECT'
- Use 'iptables' to response the ports are scanning that are unused and closed, and also not filtered as follows:
    - –j REJECT-reject-with tcp-reset ← This is better.

Task 1: Install and configure knockd (Linux-based)

1. Update apt package

   $ sudo apt update ← We use this command instead of apt-get

2. Install knockd package

   $ sudo apt install knockd

3. Open main configuration file **"/etc/knockd.conf"** with some editor (e.g. nano, pico). Look at an example of configuration

```
[options]
        UseSyslog

[openSSH]
        sequence    = 7000,8000,9000
        seq_timeout = 5
        command     = /sbin/iptables -A INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
        tcpflags    = syn

[closeSSH]
        sequence    = 9000,8000,7000
        seq_timeout = 5
        command     = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
        tcpflags    = syn
```

4. Change TCP port sequence as you need, e.g. 1111, 2222, 3333, 4444

   sequence = 1111, 2222, 3333, 4444

5. Change default log file from **/var/log/syslog** to **/var/log/portknocking.log**

   LogFile = /var/log/portknocking.log

Finally, you have this

```
[options]
       UseSyslog
       LogFile = /var/log/portknocking.log

[openSSH]
       sequence    = 1111,2222,3333
       seq_timeout = 5
       command     = /sbin/iptables -A INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
       tcpflags    = syn

[closeSSH]
       sequence    = 3333,2222,1111
       seq_timeout = 5
       command     = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
       tcpflags    = syn
```

6. Start the Service
   6.1. Open knockd initialization file **(/etc/default/knockd**)
   6.2. Change 0 -> 1

   START_KNOCKD=1

   6.3. Fix the default network interface, e.g. ens33 (assume your server use this interface)

   KNOCKD_OPTS="-i ens33"

   6.4. Restart service

   $ sudo systemctl restart knockd

7. Test Your Install
   7.1. From server, you can monitor the knock log file (/var/log/portknocking.log).

   $ sudo tail –f /var/log/portknocking.log

   7.2. From client,

   Install knock

   $ sudo apt update

   $ sudo install knockd

7.3. Run knock

$ knock [options] <host> <port [:proto] > <port[:proto]> <port[:proto]>

From your default configuration (/etc/knockd.conf), you can test connect to server as following example

$ knock 172.16.94.133 1111:tcp 2222:tcp 3333:tcp ←Assume server ip addr = 172.16.94.133

What did you see on server?

$ knock 172.16.94.133 3333:tcp 2222:tcp 1111:tcp

What did you see on server?

8. Testing your iptables

8.1. Make sure all connections from localhost are allowed.

$ sudo iptables –A INPUT –s 127.0.0.0/8 –j ACCEPT

8.2. Keep track of associated connections and to ensure any existing connections are acknowledged and responsed

$ sudo iptables –A INPUT –m state --state ESTABLISHED, RELATED –j ACCEPT

8.3. Make sure you block all inbound traffic to server

$ sudo iptables –A INPUT –j DROP

8.4. Verify your iptables rules

$ sudo iptables -nvL

9. Saving iptables rules

Now, you have knock service for sshd. However, you have to save all iptables rules that run from calling knock service.

$ sudo apt install iptables-persistent

$ sudo iptables-save

Iptables rules are kept at /etc/iptables

Task 2: Test invisible server service

1. From client
   1.1. Use “nmap” to scan your service on server

   $ nmap 172.16.94.133

   Nmap seems to think the sshd service is not run on server.

   1.2. Test connect server with ssh client

   $ ssh simon@172.16.94.133 ←Server IP address = 172.16.934.133, and account=simon

   You cannot connect to server because the iptables rule blocks your connection

   1.3. Knock server to open sshd

   $ knock 172.16.94.133 1111:tcp 2222:tcp 3333:tcp

   1.4. Test ssh connection

   $ ssh simon@172.16.94.133

   Now, you can connect to server with ssh client

   1.5. Knock server to close sshd when you do not need service.

   $ knock 172.16.94.133 3333:tcp 2222:tcp 1111:tcp

Self-Study:

You have to repeat all tasks in lab sheet several times to understand the solution. Write down your own report and share with your friends.

Homework

You have no homework, but you should try to make invisible service on real server and try use different service.

Remark:

Do activity by yourself. Good Luck