Exercise: Using FWKnop to deactivate SSH Available from the World

Steps

1. On your Kali system, start a shell by hitting `Alt-F2`, then typing `lxterminal` and hitting `Enter`.
2. We'll start by configuring `fwknop`. Let's create a client configuration with a shared secret:

   ```
   fwknop -A tcp/22 -D mrrobot --key-gen --use-hmac --save-rc-stanza
   ```

3. Take a look at the client configuration you just created:

   ```
   cat /home/lockthisdown/.fwknoprc
   ```

4. Highlight the `KEY_BASE64` and `HMAC_KEY_BASE64` lines, then hit `Ctrl-Shift-C` to copy them:

   ```
   Hit Ctrl-Shift-c
   ```

5. Now, let's `ssh` into the MrRobot virtual machine, where we'll set up the server.
6. Start up a new tab by hitting `Ctrl-Shift-T`.

   ```
   Hit Ctrl-Shift-t
   ```

7. If there isn't an SSH daemon running on MrRobot, please use the Getting SSH Access on the MrRobot Virtual Machine instructions to start an SSH daemon.
8. `ssh` into the MrRobot virtual machine as the user `robot`, using the password `abcdefghijklmnopqrstuvwxyz`

   ```
   ssh robot@mrrobot
   abcdefghijklmnopqrstuvwxyz
   ```

9. If you haven't completed the MrRobot exercise where you put the `robot` user into the sudoers group, please use the Getting SSH Access on the MrRobot Virtual Machine instructions to do this.
10. Use `sudo` to run as the `root` user, using the `root` user's normal environment.

```
sudo su -
```

11. Synchronize the virtual machine's clock with an NTP server:

    ```
    ntpdate time1.google.com
    ```

12. Edit the `access.conf` file:

    ```
    nano /etc/fwknop/access.conf
    ```

13. Scroll down in this file almost to the end until you find the uncommented `KEY_BASE64` and `HMAC_KEY_BASE64` lines.

14. Replace the `KEY_BASE64` and `HMAC_KEY_BASE64` lines with the text you copied from the client:

    ```
    Place the cursor on the KEY_BASE64 line and hit Ctrl-K twice.
    Hit Ctrl-Shift-V to paste in the KEY_BASE64 and HMAC_KEY_BASE64 lines from the client
    ```

15. Hit `Ctrl-X` to exit, then `Y` to acknowledge the file write, then `Enter` to confirm the filename.

    ```
    Hit Ctrl-X
    Hit Y
    Hit the Enter key
    ```

16. Let's activate `fwknop` to run on boot. Rename the disabled Upstart job file:

    ```
    cd /etc/init
    mv fwknop-server.conf.disabled fwknop-server.conf
    ```

17. Now, start the `fwknopd` server via Upstart's `initctl` command:

    ```
    initctl start fwknop-server
    ```

18. Take a look at the iptables configuration, which has gained a new chain called `FWKNOP_INPUT`:

    ```
    iptables-save | grep FWKNOP
    ```

19. Switch back to the tab that is on the Kali system.

20. Now, run an `fwknop` command on the client, asking the mrrobot machine to allow access from `10.23.58.30` to port `22`:

    ```
    fwknop -n mrrobot -a 10.23.58.30 -A tcp/22
    ```

21. Now, quickly before you miss it, switch back over to your `ssh` session with the `mrrobot` virtual machine and look at the iptables configuration:

    ```
    iptables-save | grep FWKNOP
    ```

22. Observe a new rule allowing `10.23.58.30` to access TCP port `22`. If you don't see this, detour to the troubleshooting section of this exercise. When troubleshooting is done, repeat the last two steps.

23. Now, let's see the transient nature of this rule. Wait a full minute, then look at the iptables configuration again:

    ```
    iptables-save | grep FWKNOP
    ```

24. Take a look at the log messages you see from `fwknop`:

    ```
    grep fwknopd /var/log/syslog
    ```

25. Change your Slack status to `:thumbsup:`.

26. Suspend the virtual machines:

    ```
    sudo /scripts/suspend-all-vms.sh
    ```

Troubleshooting

In one of our tests, we found that the `fwknopd` daemon wasn't opening firewall rules because of a 4 minute difference in the system times on the Kali host and the MrRobot guest. If you run into the same problem, update the time on the `mrrobot` virtual machine and your Kali system:

```
# On Kali:
systemctl start ntp

# On MrRobot:
ntpdate time1.google.com
```

Troubleshooting - Missing FWknop client

If the `fwknop` client is not on your Kali system, install it with:

```
apt install fwknop-client
```