Activity File: firewalld Configuration

In this activity, you'll continue to be an SOC analyst at Better Buys, Inc.

- You will be working with a server that is used to remotely administer other machines on the network using Telnet and SSH.
- You've been asked to update the firewall in order to implement different rules for different zones. Since this is challenging to do with UFW, you've decided to use firewalld to organize rules for your different zones.
- You've decided to implement multi-zone-based firewall filtering for specific services. Specifically, you will create four zones: one each for HTTP, HTTPS, and SSH, and one for all other traffic.
- In addition to configuring rules, you'll use firewalld to verify your firewall rules by inspecting which services are running in each zone.

Note: Feel free to use online resources and man pages to help you with this activity.

- Use `sudo /etc/init.d/firewalld` start to start firewalld.
- Use `sudo firewall-cmd --list-all-zones` to list all current zones.
- Use `sudo firewall-cmd --zone=home --change-interface=eth0` to bind together interfaces.
- Use `sudo firewall-cmd --get-services` to list currently configured services.
- Use `sudo firewall-cmd --zone=home --list-all` to list all currently configured services for a specific zone.
- Use `sudo firewall-cmd --zone=home --add-rich-rule=` to add specific rules to specific zones

Set Up

- You will need to uninstall UFW for firewalld to work properly. Run the following commands:

    - `sudo apt remove ufw` to uninstall ufw.
    - `service firewalld status` to verify firewalld is running.
    - `service firewalld start` to start it if needed.
- Verify firewalld is running:
    - Run: `service firewalld status`.
    - Run: `service firewalld start` to start it if needed.
- Log into the firewalld VM using the following credentials:
    - Username: `sysadmin`
    - Password: `cybersecurity`

Instructions

Open a terminal window and start firewalld.

1. List all available zones.
2. Set your `eth0` interface to your `home` zone.
   `sudo /etc/init.d/firewalld`
3. Verify the home zone is set to `eth0`.
4. Display all active home zone services.

```
sysadmin@ufw-host:~$ sudo firewall-cmd --zone=home --list-all
home (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth0
  sources:
  services: ssh mdns samba-client dhcpv6-client
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

- What is the status of IVP6, SSH and Telnet?

- Are we able to connect via SSH or Telnet?

5. Log into the UFW VM using the following credentials:

    - Username: `sysadmin`
    - Password: `cybersecurity`
6. Type the SSH command that connects to `firewalld IP`.

7. Test the Telnet connection to `firewalld IP`.

    - What does the `no route to host` message mean?
8. Test pings to the `firewalld IP`.

9. Go back to your firewalld machine and block pings and ICMP requests in your `home` zone.

10. List all the rules that are in place in your `home` zone.

    - Are all our rules are in place?
11. Switch back to the UFW VM.

    Run the command for `ping` that sends four packets to the `firewalld` machine.

    - Are your ping requests blocked?

Bonus:

11. Switch back to the firewalld machine.

    - Using `rich-rules`, block the UFW server's IP address.
12. Test if the UFW server's connection is blocked by testing your `rich-rule` by trying to SSH into `firewalld IP`.

    - Why do you think you're not able to connect?