Metropolitan State University
CYBR 490 – Cybersecurity for Medical Devices
Lab 1: Infusion Pump Environment Security Controls – Firewall

Overview

Russell Medical (Device Overview 1) decided to apply endpoint protection, hardening, and data protection in their wireless pumps. The general guidance and customized approaches include disabling unused or unnecessary ports and services.

This Labtainers exercise illustrates the use of iptables on a firewall to limit network access to an infusion pump server from a client computer, as illustrated in figure 1. When properly configured, the firewall will only allow selected traffic from the client/workstations (doctor, nurse, and admin) to the server.

1.0 Background

You will setup firewall rules to prevent unauthorized users from accessing the pump server or isolate the pump server as a protected server and only permit specific users to use it. In addition, the server is only accessible to traffic from the hospital network, which is blocked from the public network. It may be possible to secure a server against unwanted access by restricting the kinds of network traffic that is transmitted to the server. For instance, if the server has an unprotected service accessible through its network interface, using that service will be more challenging if something is preventing traffic from reaching it.

There are numerous methods and solutions available for restricting IP network traffic between computers. You will use Linux iptables to restrict IP traffic in this lab. On the firewall component, use the following command to view the manpage for Iptables:

man iptables
man iptables-extensions

2.0 Lab Environment

This lab runs in the Labtainers framework, available at http://my.nps.edu/web/c3o/labtainers. Labtainers are linked to a pre-built virtual machine in this lab. Labtainers can be used on any Linux host that supports Docker containers. Start the lab using your labtainer-student directory using this command.

```
labtainer infusion
```

A link to this lab manual will be displayed.

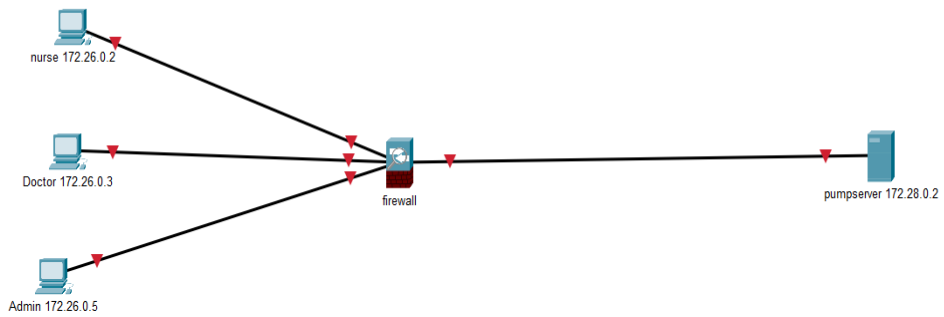

Figure 1 lab environment

3.0 Lab tasks

3.1 Explore

1. The Wireshark utility is installed on the firewall. Use it to view network traffic through the firewall, and to debug your firewall rules. Start it from the firewall terminal.
2. On The firewall, a Wireshark tool is installed. Use it to inspect network traffic that is passing through the firewall. From the firewall terminal, run this command to start the wireshark.

   wireshark &
3. Then select the eth0 interface.
4. On the nurse terminal use the nmap command to list some of the open ports on the pump server:

   nmap pumpserver

   ***Obtain a screen shot of the open ports and save to a Word document indicating it is for Section 3.1, Step 4. You will be capturing several screen shots throughout the rest of the lab in the word document.

5. Use wget command to verify that the server responds to HTTP requests:

   wget pumpserver &

***Obtain a screen shot of the server response and save to the Word document indicating it is for Section 3.1, Step 5.

6. Verify a SSH service is available; you don't have to log in when requested; simply press the Ctrl C key to exit after receiving a response from the server.ssh pumpserver.

   ***Obtain a screen shot of the SSH service availability and save to the Word document indicating it is for Section 3.1, Step 6.

7. Finally, confirm that telnet is available. You don't need to log in to this as well.

   telnet pumpserver

   ***Obtain a screen shot of the telnet availability and save to the Word document indicating it is for Section 3.1, Step 7.

8. Take note of the source IP addresses and destination ports that the clients used to connect to the server as you watched the traffic in Wireshark.

   ***Include the source IP address and destination ports in the Word document indicating it is for Section 3.1, Step 8.

3.2 Use iptables to limit traffic

The iptables utility is installed on the "firewall" component. Use it to prevent the firewall from forwarding any traffic to the server other than SSH and HTTP and allow only the doctor, nurse, and admin computer to access the server remotely.

1. On the firewall, block all the ports on the pumpserver using this command.
   sudo iptables -P FORWARD DROP
   sudo iptables -P INPUT DROP
   sudo iptables -P OUTPUT DROP
2. Use this command to save your changes.

   sudo iptables-save
3. On the nurse's workstation use the nmap command again to verify the pumpserver ports are closed.

   ***Include a screen shot of the indication the ports are open in the Word document indicating it is for Section 3.2, Step 2.

4. Then configure the firewall to allow ssh traffic from the nurse's computer using this command.

sudo iptables -A FORWARD -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

sudo iptables -A FORWARD -p tcp --dport 22 -s 172.26.0.3 -j ACCEPT

***Take a screen shot of the command typed in and the result after running it and include in the Word document indicating it is for Section 3.2, Step 3.

5. Allowed clients (doctor, nurse, and admin) should only be able to reach the pumpserver on HTTP and SSH ports. Configure these clients to be able to reach the pumpserver on HTTP and SSH ports.
6. Modify the IP tables SSH from the doctor, nurse, and admin computers to demonstrate that the firewall only allows the desired traffic.

   ***Include a screen shot of the modified tables and include in the Word document indicating it is for Section 3.2, Step 3.

4.0 Submission

- After finishing the lab, go to the terminal on your Linux system that was used to start the lab and type:

  Stoplab
- Submit the Word document to the appropriate Assignment box (Lab 1) in D2L.