Using iptables to limit application services

Background

This Labtainer exercise illustrates the use of iptables to limit which application services, (ports), will be forwarded through a component serving as a firewall.

You will configure the firewall within this topology:

client <============> firewall <============> server

such that the client can only access SSH and HTTP services on the server.

It is assumed that you have already learned about iptables elsewhere, e.g., in a course or independent study. You can learn about the iptables command via the manpage:

```
man iptables
```

and there are also plenty of resources on the internet.

Performing the lab

The lab is started from the labtainer working directory on your Linux host, e.g., a Linux VM. From there, issue the command:

```
labtainer iptables
```

The resulting virtual terminals will include bash shells on two components: a client computer and a "firewall".

Tasks

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 sessions.

Demonstrate that you have done this by running this command on the client computer:

```
nmap -n 172.25.0.3
```

the resulting display should indicate that SSH and HTTP are the only ports that are open.

Stop the labtainer

When the lab is completed, or you'd like to stop working for a while, run:

```
stoplab
```

from the host labtainer working directory. You can always restart the lab to continue your work. When the labtainer is stopped, a zip file is created and copied to a location displayed by the stoplab command. When the lab is complete, send that zip file to the instructor.

This lab was developed for the Labtainer framework by the Naval Postgraduate School, Center for Cybersecurity and Cyber Operations under National Science Foundation Award No. 1438893. This work is in the public domain, and cannot be copyrighted.