Telnet Lab Exercise

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.

Overview

This labtainer exercise illustrates the use of a telnet client to access resources on a server. It is a simple lab intended to illustrate basic client server networking and the transmission of plaintext passwords over a network by telnet.

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 telnetlab
```

The resulting virtual terminals include one connected to a client comptuer, and a terminal connected to a server.

Tasks

1. **Determine the server IP address**

In the server window, type "`ifconfig`" to view the IP address of the server. The server IP address will follow the "`inet adddr:`" label.

2. **Telnet to telnet server and display a file on the server**

On the client comptuer, use the telnet command to access the server using its IP address:

```
    telnet <IP>
```

You will be prompted for a user ID and then a password. Both of them are "`ubuntu`"

There is a pre-created file on the server named "`filetoview.txt`".

View the file content by typing:

```
    cat filetoview.txt
```

Exit the telnet session on the client via the "`exit`" command.

3. **View plaintext passwords.**

On the server, start tcpdump to display TCP network traffic with this command:

```
    sudo tcpdump –i eth0 –X tcp
```

On the client start a telnet session, but when prompted for the password type “`mydoghasfleas`” (as you know this password is incorrect). As you type each letter of the password, observe the tcpdump of the traffic. Keeping in mind that every other packet is an “`ack`”, do you see the password. What do you notice?

4. **Use SSH to protect communications with the server**

From the client computer, use the SSH command to access the server using its IP address:

```
ssh <IP>
```

The first time you SSH to a server, SSH will warn you that the “`authenticity of  the host… can’t be established`”. Type “`yes`” at the prompt.

View the file content by typing:

```
cat filetoview.txt
```

Observe the tcpdump output, and note that there is no readable plain text.

Stop the Labtainer

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

```
stoplab telnetlab
```

from the host labtainer working directory. You can always restart the labtainer and continue your work where you left off. When the Labtainer is stopped, a zip file is created and saved to a location displayed beneath the stoplab. When you are completely finished send that file to your instructor.