The nmap-ssh lab

Overview

This labtainer exercise uses nmap and other skills to identify and exploit a weakness in a system.

You are performing ad-hoc security testing for a client who believes their internal SSH server is relatively secure, but you would like to confirm the validity of this. Your goal is to attempt to remotely access that SSH server and disclose the content of a selected file.

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 nmap-ssh
```

The resulting virtual terminal will include a bash shell on a computer called "`MyComputer`". The nmap utility is pre-installed on that computer. You will also have a virtual terminal connected to a "router", and a bash shell there. You have been told that the router sits between the organization's client workstations and the servers.

Tasks

You have been told the target SSH server IP address is 172.25.0.2 and the SSH port number changes frequently within the range of 2000-3000. you have been given an account, "analysis" on the client computer called MyComputer and on the router.

Client computers <===> [Router]<===> servers

your goal is to successfully SSH from "`MyComputer`" into the "`ubuntu`" account on the SSH server and find and display the contents of the secret file.

Hints:

- nmap is installed on MyComputer. Use it to search the target network for the mystery port, as well as any other traffic that might include passwords
- tshark and tcpdump are installed on the router. Use tcpdump on the router to capture traffic from the ethernet interface attached to the target network. Capture only traffic from a service that might contain a password and send the output to a file with a .pcap extension.
- Use tshark to follow tcp streams to look for usernames and passwords. Use the -r option to read the file you created above. Use the tshark man page to find how to display a tcp stream. You may have to follow more than one stream.

Use the username and password you find to login to the SSH server on the secret port.
Find the secret file and display it using the cat command.

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 labtainer 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 completed send that zip file to the instructor.