Lab-6 Report: Mitnick Attack

Shrikant Kale - 700727822

**Lab Environment Setup**

* Created Lab environment using docker containers.
* To execute docker container, I have used docker-compose commands.
  + dcbuild (docker-compose build) – to build the docker container image
  + dcup (docker-compose up) – to run the docker container
  + dcdown (docker-compose down) – to shut down the container

**Task 1) SYN Flooding Attack**

Pinging the trusted-server-10.9.0.6. In order to have it in the arp cache. And then taking down the trusted server to replicate the SYN attack

**Text

Description automatically generated**

Taking the trusted server down in order to simulate SYN attack

**Text

Description automatically generated**

Adding the cm flag, by running the “ARP -S IP MAC” command

**Text

Description automatically generated**

**TASK 2): SPOOF TCP CONNECTIONS AND RSH SESSIONS**

2.1: PYTHON SCRIPT FOR SPOOFING SYN PACKET.

**Text

Description automatically generated**

PYTHON SCRIPT FOR SNIFFING THE SYN+ACK PACKET. AND TO SEND THE ACK PACKET.

**Text

Description automatically generated**

ESTABLISHING THE TCP CONNECTION BY RUNNING THE SNIFF AND SPOOF CODE.

**A close-up of a document

Description automatically generated with medium confidence**

**A close-up of a document

Description automatically generated with low confidence**

**Graphical user interface, text, application

Description automatically generated**

**TASK #2.2: SPOOF THE SECOND TCP CONNECTION**

PYTHON CODE FOR ESTABLISHING TCP CONNECTION WITH X-TERMINAL

**Text

Description automatically generated**

After sending ACK packet

**Text

Description automatically generated**

Python code for spoofing the second connection

**Text

Description automatically generated**

Establishing the connection, by running the python code.

**Text

Description automatically generated**

Spoofing the second connection, by running the python command.

**Text

Description automatically generated with low confidence**

WIRESHARK TRAFFIC VERIFYING THE ATTACK

**Graphical user interface

Description automatically generated with medium confidence**

WE ARE ABLE TO VERIFY THAT THE FILE HAS BEEN CREATED. SCREENSHOT BELOW

**Text

Description automatically generated**

**TASK 3: SETTING UP A BACKDOOR**

PYTHON CODE FOR SPOOFING, SNIFFING, & ESTABLISHING TCP CONNECTION WITH THE X-TERMINAL 10.9.0.5

**Text

Description automatically generated**

After Sending ACK packet

**Text

Description automatically generated**

Python code for spoofing the second connection

**Text

Description automatically generated**

Establishing the connection by running the python code. screenshot below:

**Text

Description automatically generated**

Running the second python command to spoof the second connection

**Text, letter

Description automatically generated**

Verifying the attack with WIRESHARK

**Table

Description automatically generated with low confidence**

Checking the rhost file. verifying that our payload has worked successfully

**Text

Description automatically generated with low confidence**

From the attacker (connecting the x-terminal). Screenshot below:

**Text

Description automatically generated**