Instructions for setting up and trying seth

Preamble

The purpose of this optional exercise is to examine the process of using a script to execute a MITM attack. This exercise is intended to increase your exposure to MITM attacks

NOTE: Two videos demonstrating this technique have been added to your course shell under the heading Attacking Microsoft RDP with Seth (1) and Attacking Microsoft RDP with Seth (2). Watch these videos first before proceeding. I have also added a link to a Kali Linux Tutorial on Seth.

Requirements

For this assignment you will need to perform each of the following:

1. Set up a network of three VMs consisting of (1) a Windows host (HOST1) acting as an RDP Server with RDP enabled, (2) a Windows client (CLIENT) that can login to HOST1. Depending on your set up, this might be the machine hosting the hypervisor or it could be another Windows VM, and (3) a VM running Kali and Seth which will perform the MITM attack.

2. Establish a user account on HOST1 (the RDP Host) with a weak password and enable RDP. ***DO NOT FORCE NETWORK LEVEL AUTHENTICATION.***

3. Ensure that Seth is installed on your kali host.

4. Run Seth on your kali host, giving it the correct interface, attacker IP, victim IP and RDP server IP. Attacker is your kali machine and victim is the CLIENT.

5. Using CLIENT, login to HOST1 via RDP.

6. Once successful, take a screen shot showing that Seth has captured the password to get into HOST1

Command execution example: ./seth.sh eth0 192.168.1.{4,7,10}

In the above example the hosts are:

- 192.168.1.4 Kali Attacker
- 192.168.1.7 Host2 (CLIENT victim)
- 192.168.1.10 HOST 1 (Windows RDP Server)

Optional tasks (for fun):

- Run a remote command on the RDP host (i.e. calc)
- Test the ability of Seth to capture keystrokes from the CLIENT.
- Visit the github and examine the source code of Seth