**Lab 1: Reverse Shell**

**Objective:**

* Gain practical experience in using cybersecurity tool (Moriarty Matrix) and conducting cyber-attacks (including network ones) on a target machine
* Develop skills in network monitoring using Wireshark and implementing measures to secure a network.

**Equipment:**

* Two or three virtual machines running on a host computer, such as VirtualBox or VMware
* Linux or Windows work for the Target and Attacker Machine
* Wireshark or similar network monitoring tool
* Basic knowledge of networking and Linux command line

**Part 1: Setting up the Environment:**

1. Install and configure Virtual Machine on the attacker machine and a Linux or Windows distribution as the victim machine.
2. The two machines do not need to be on the same NAT network but need to identify their IP addresses and open ports to use.
3. Install and configure Wireshark on a third machine, the host machine, or the victim machine.

**Part 2: Conducting a Network Attack:**

1. On the attacker machine, start the listening program and obtain the IP address of the victim machine.
2. Initiate a reverse shell connection from the attacker machine to the victim machine.
3. Use the reverse shell connection to retrieve, edit, and delete files on the victim machine, and execute personal Python programs on the victim machine.
4. Perform reconnaissance on the target, starting with the IP address.
5. Monitor the network traffic using Wireshark to identify any suspicious activities.
6. Document any changes made from attacker machine to the target machine and identify if there are any noticeable themes showing that the victim machine is affected (such as slowing down, ports being used, outside connections, etc…).

**Part 3: Securing the Network**

1. Identify the ports and connections used by the attacker machine.
2. Use the firewall on the victim machine to block these ports and connections.
3. Verify that the ports and connections are blocked using Wireshark or other network monitoring tools.
4. Document what the attacker could have done keep his connection and what the victim machine could have done to prevent initial connections.

**Rubric:**

* Successful completion of Part 1: Setting up the Environment: 20 points
* Successful completion of Part 2: Conducting a Network Attack: 50 points
* Successful completion of Part 3: Securing the Network: 20 points
* Quality of documentation and explanation of steps taken: 10 points

**Optional additional steps:**

1. Delivery Process:

- How was the malware delivered? Phishing, disposable email address

1. With the reverse shell was any other malware added such as a keylogger or virus