Matthew Moltzau

Ryan Vacca

Julia Vrooman

**Final Project : Cyber Security Programming**

**Project 6. Spoofed ARP Detector.**The goal of this project is to develop a tool that detects ARP spoofing in LANs and WLANs. You must demo your tool in a testbed LAN.

**Overview:**

ARP Spoofing is a malicious technique in which an attacker sends a compromised / spoofed Address Resolution Protocol (ARP) on a Local Area Network (LAN). The goal of the attacker is to embed their Media Access Control (MAC) address with the Internet Protocol (IP) address of another host located on the LAN. This allows the attacker to intercept the traffic intended for the correct target host IP.

ARP Spoofing is a gateway to enable other attacks such as Denial of Service (DOS), Man-in-the-Middle (MITM), and Session Hijacking. ARP is a communications protocol in which the internet layer IP addresses are resolved into link layer MAC addresses. The means of attack in ARP spoofing comes from the lack of host authentication of the packet that was received by the victim.

**Project Goal:**

The goal of this project will be to detect the ARP spoofing in a LAN and/or WLAN. Our program will be used as a tool to supplement the victims firewall to notify the victim when a possible IP/MAC address hijacking has occurred. We would like to have the python programming running in the background and when we simulate an ARP spoof, the process in the victim’s node will then be brought to the foreground alerting the victim they may have potentially been exposed. This is the goal we aim to achieve coupled with appropriate accuracy.

**Deliverables:**

1. Source Code – This will be a directory with multiple .py files.
2. ReadMe – This file will explain configuration in which to set up the VLAN and execute python code.
3. Virtual Machine images. Kali Linux and/or Windows Server

**Timeline:**

SEP: Discuss program architecture, python version lockdown.

OCT: Configure Virtual network(s), research ARP python spoofing, develop prototype.

NOV: Polish prototype into final product, testing, documentation.

DEC: Prepare products for turn-in, practice delivery mechanism for class presentation.

**Project Breakdown:**

We will be using virtual machines to simulate the different nodes involved.

1 node simulating the router, 1 node the attacker, and 1 node the victim. The router node is the connection to which the victim and attacker communicate through. Our goal will be to first successfully take on the role of the attacker in which we attempt to spoof our victim. By studying the means of attack, we can begin thinking like the attacker. Once we have successfully placed our attacker in-between the router and the victim, we can then reverse engineer the process in which to harden our defenses. We feel as if this approach is favorable and will ultimately make our ARP spoofing detector more robust since we have taken the time to research / implement the attack. This will also set up our unit tests to which we can run our tool against to gauge our success in detection.