Lab 03 - COMP8670 Advanced Computer Networks

February 25, 2025

Purpose

This lab is designed to introduce students to practical aspects of network protocol security analysis. It provide hands-on experience with network protocols security analysis.

Objectives

- Understand and implement an ARP poisoning attack.
- Analyze DHCP protocol security using Finite State Machines and STRIDE methodology.

Prerequisites

- Scapy: A powerful Python-based tool for network packet manipulation and sniffing.
- Virtual Machines (VMs): One VM to act as the victim (Metasploitable), and the second VM to execute the attack (Kali). VirtualBox or VMware can be used to set up these VMs. You may use setup with VirtualBox or VMware
- Target virtual machine (Metasploitable),, click here to download
- Network sniffing tool (e.g., Wireshark) for analysis

Part 1: ARP Poisoning Attack

Practice and demonstrate an ARP poisoning attack using Scapy and virtual machines, disrupting communication between two hosts.

Tasks

1. **Environment Setup**: Create a simple network with two virtual machines (VM1 and VM2) connected through a virtual switch or host-only network. Ensure both VMs can ping each other, confirming network connectivity. **[10 POINTS]**
2. **ARP Security Testing**: Write a script using Scapy to perform ARP security testing (pentesting), follow the STRIDE methodology we applied in the class to test and verify the identified vulnerabilities.**[20 POINTS]**
3. **Mitigation and Report**: Discuss and implement basic mitigation strategies against ARP poisoning, such as static ARP entries or using ARP spoofing detection tools. **[10 POINTS]**

Report Requirements

[**10 POINTS**] Include the following in your report:

- Network configurations and ARP tables before and after the attack.
- Scapy scripts used.
- Screenshots demonstrating the success of the attack, including Wireshark captures.
- Discussion on mitigation strategies.

Part 2: Security Analysis of The DHCP

DHCP stands for Dynamic Host Configuration Protocol. It is a network management protocol used on IP networks whereby a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network. This is to ensure that all devices have a unique IP address and can communicate with other networks. The DHCP process involves four main steps:

1. Discover: The client device sends out a broadcast message (DHCPDISCOVER) to discover available DHCP servers.
2. Offer: DHCP servers receive the discover message and respond with a DHCP offer (DHCPOFFER) message, which contains an IP address offer and other configuration information like subnet mask, default gateway, and DNS server addresses.
3. Request: The client receives the offer(s) and sends back a request message (DHCPREQUEST) to the selected DHCP server, asking for the offered IP address and configuration details.
4. Acknowledgment: The DHCP server acknowledges (DHCPACK) the client's request and finalizes the IP address lease. The server may also send a negative acknowledgment (DHCPNAK) if the requested configuration is not valid or the IP address is no longer available.

DHCP allows devices to join a network smoothly and with minimal manual configuration, making it a crucial service in large networks and for devices that frequently join or leave a network, such as laptops, smartphones, and other portable devices. The DHCP (Dynamic Host Configuration Protocol) does not inherently provide Confidentiality, Integrity, and Availability (CIA) features.

Tasks

1. Start Wireshark open the enclosed pcap trace file and list all the DHCP packets in the trace. Use screenshots to support your answer. [**5 POINTS**]
2. Create a Finite State Machine model for the DHCP process. This model should include states such as "Discover", "Offer", "Request", and "Acknowledge". Use diagrams to represent the FSM. [**15 POINTS**]
3. Apply the STRIDE methodology to the FSM model of DHCP to identify potential security threats. For each STRIDE element, identify possible vulnerabilities in the DHCP process. [**15 POINTS**]
4. Propose mitigation strategies for each identified vulnerability. This could involve protocol enhancements, configuration changes, or additional security mechanisms. [**5 POINTS**]

Report Requirements

Submit a comprehensive report detailing their FSM model, STRIDE analysis, identified vulnerabilities, and proposed mitigations. Use the attached report template. [**10 POINTS**]

Submission Guidelines

- The deadline for the task is **Wednesday, 5/03/2025, 11:59 PM**
- Format your reports clearly and legibly, adhering to the provided structure, and don't forget the cover page as the previous task.
- Submit your report as a PDF document through the submission form that will be sent to you.
- Ensure that all sections of the lab are completed and thoroughly documented.