TCP Session Hijacking Lab Assignment

CSCI 297E: Ethical Hacking

Due Date: 2024-05-15

Objective

Understand and demonstrate the techniques of TCP session hijacking within a controlled lab environment using virtual machines.

Tools Required

- VirtualBox
- Ubuntu VMs on an internal network
- Networking tools: Wireshark, Ettercap, tcpdump

Preparatory Steps

Ensure you have set up your virtual environment as per the instructions provided:

- Virtual Environment Setup Instructions
- Using tcpdump for Network Monitoring

Assignment Tasks

1. **Environment Setup Verification**
   Verify that all VMs can communicate. Use `ping` to ensure connectivity. Document the IP configurations and connectivity test results.
2. **ARP Poisoning and Traffic Capture**
   Perform ARP poisoning between the Victim and Server VMs using Ettercap. Capture the traffic with tcpdump on the Attacker VM. Detailed instructions are available in the tcpdump guide.
3. **Session Hijacking**
   Analyze the captured traffic to identify a TCP session. Modify packets to hijack the session and redirect traffic or alter communications. Document the steps and results of your hijacking attempt.
4. **Analysis and Reporting**
   Analyze the impact of your hijacking on the communication between the Victim and Server. Identify potential signs of the attack and how it could be detected.
5. **Mitigation and Defense**
   Implement and test mitigation strategies to protect against similar attacks. Evaluate the effectiveness of these strategies.

Deliverables

Submit a comprehensive lab report covering:

- Setup and connectivity verifications.
- Steps taken during ARP poisoning and session hijacking.
- Analysis of the hijacking impact and mitigation strategies.
- Reflections on what was learned and potential real-world applications.

Evaluation Criteria

- Accuracy and completeness of setup and execution.
- Depth of analysis in the hijacking and mitigation process.
- Clarity and thoroughness in reporting and documentation.