Network Forensics Testbed - Instruction and Usage Guide

This guide provides detailed instructions on how to set up and use the Network Forensics Testbed for educational purposes. This testbed allows students to simulate real-world network attacks, capture network traffic, and analyze data for forensic purposes. It is designed to be simple, reusable, and accessible for students with basic networking knowledge.

Prerequisites

1. Docker and Docker Compose installed on your machine.
2. Basic understanding of Linux commands and networking concepts.

Installation

1. Clone the repository:

   git clone https://github.com/student/network-forensics-testbed.git

   cd network-forensics-testbed

2. Make the scripts executable:

   chmod +x scripts/*.sh cleanup.sh setup.sh

3. Build and run the testbed:

   docker-compose up -d --build

Usage

1. Start the Testbed:

   Use the docker-compose command to start all the containers.

2. Simulate Attacks:

   - Perform ARP spoofing to initiate a MITM attack.
   - Scan the network for live devices.

3. Capture Network Traffic:

- Use tcpdump on the target container to capture packets.

4. View and Analyze Logs:

- Access the logs collected by the logger.

- Copy the packet capture file for offline analysis.

Cleanup

To stop and remove all containers, volumes, and logs:

./cleanup.sh

Troubleshooting

- If logs are not being written, ensure the logs directory has the correct permissions.

- If the attacker cannot find tools (like arpspoof), make sure the Docker image is properly built.

- Restart the testbed if containers fail.

Conclusion

This testbed provides a practical environment for learning network forensics. It enables students to gain hands-on experience with real-world attack scenarios, making it an essential tool for anyone pursuing a career in cybersecurity.