CURRICULUM

Technology-Facilitated Gender-Based Violence (TFGBV) and

Cybersecurity Labwork

Duration: 2 Hours

Instructor: Protection/Technology Specialist: Dr. Lela Mirtskhulava

Tools:

- **Wireshark**: Network protocol analyzer for real-time packet capture and traffic analysis.
- **Cisco Packet Tracer**: Network simulation tool for building and troubleshooting virtual network environments.
- **Social Media and Smartphone Security Tools**: Focus on securing social media platforms (e.g., Facebook) and smartphones from TFGBV threats.

Lab Objectives:

By the end of this lab session, students will:

- Understand how to capture and analyze network traffic using Wireshark.
- Design and simulate a network using Cisco Packet Tracer.
- Detect abnormal activities such as unauthorized access and hacking attempts related to TFGBV.
- Learn techniques for securing Facebook and other social media platforms.
- Learn best practices for securing smartphones from hacking and cyber-harassment.

Lab Structure

Part 1: Network Simulation and Traffic Analysis (60 minutes)

Step 1: Build a Basic Network in Cisco Packet Tracer (20 minutes)

- **Objective**: Set up and simulate a basic network using Cisco Packet Tracer.
    1. **Network Setup**:
        - Create a network with two PCs (victim and attacker), a router, and a switch.
        - Assign IP addresses to devices (e.g., 192.168.1.2 for the victim and 192.168.1.3 for the attacker).

        - Configure basic routing for the network.

    2. **Normal Traffic Simulation**:

        - Generate normal traffic (ping test, file transfers) between the two PCs to understand baseline network behavior.

Step 2: Capture and Analyze Network Traffic with Wireshark (20 minutes)

- **Objective**: Capture and analyze traffic using Wireshark to identify potential threats.

    1. **Wireshark Setup**:

        - Start Wireshark and capture live traffic generated from the Cisco Packet Tracer network.

    2. **Traffic Analysis**:

        - Apply filters to detect any abnormal traffic (e.g., large amounts of pings indicating a DoS attack or unauthorized login attempts).

Step 3: Simulating a Network Breach and Detection (20 minutes)

- **Objective**: Simulate a network breach (e.g., cyberstalking, unauthorized access) and analyze it.

    1. **Network Breach Simulation**:

        - From the attacker's PC, simulate a DoS attack or unauthorized Telnet login attempts targeting the victim.

    2. **Detecting the Breach**:

        - Use Wireshark to capture the attack traffic and analyze the packets to identify the source of the attack.

Part 2: Securing Social Media Platforms and Smartphones (60 minutes)

Step 4: Securing Facebook and Other Social Media Platforms (30 minutes)

1. **Objective**: Understand how to secure Facebook and other social media platforms from common TFGBV-related threats such as account hacking and harassment.

    - **Account Security Settings**: Demonstrate how to:

        - Enable **two-factor authentication (2FA)** on Facebook and other platforms.

        - Set up **strong passwords** and avoid using the same password for multiple accounts.

        - Use Facebook's **privacy settings** to restrict access to personal information.

        - **Review login activity** and log out of any suspicious sessions.

- **Securing Against Harassment**:
    - How to block, report, or mute harassing users.
    - Enable options to prevent non-friends from sending private messages or accessing your profile.

2. **Lab Activity**:
    - Students will create a **secure social media environment** by configuring Facebook account security settings on a test account.
    - **Scenario**: A simulated TFGBV case where an attacker attempts to gain unauthorized access to a Facebook account. Students will use security measures to protect the account from the attack.

Step 5: Securing Smartphones from Cyber-Harassment (30 minutes)

1. **Objective**: Learn best practices to secure smartphones from threats like hacking, spyware installation, and cyber-harassment related to TFGBV.
    - **Smartphone Security Settings**:
        - Enable **device encryption** and **screen lock** (PIN, fingerprint, or face recognition).
        - Use **secure Wi-Fi connections** and avoid public Wi-Fi networks for sensitive activities.
        - Keep the operating system and apps **up-to-date** to ensure the latest security patches are applied.
    - **App Security**:
        - Review **app permissions** and revoke access to sensitive data (e.g., location, contacts) from apps that don't need it.
        - Install apps only from trusted sources (e.g., Google Play Store, Apple App Store).
        - Use anti-malware apps to scan for and remove spyware or other malicious software.
    - **Securing Against Harassment**:
        - How to block unknown callers or message senders.
        - Enable **call screening** or use apps that prevent unwanted calls and messages.
2. **Lab Activity**:

    - Students will perform a **security audit** on a test smartphone:
        - Check the **app permissions** and revoke unnecessary access.
        - Set up **screen lock** and **encryption** for the device.
        - Install an anti-malware app and perform a **security scan**.

Lab Wrap-Up (10 minutes)

1. **Review**:
    - Recap key concepts such as securing social media platforms, detecting network breaches, and smartphone security best practices.
2. **Q&A**:
    - Address any questions related to the lab work, tools, or real-world application of cybersecurity measures to combat TFGBV.

Assessment:

- **Lab Report**:
  Students will submit a brief report detailing:
    - The network configuration in Cisco Packet Tracer.
    - The Facebook and smartphone security measures implemented.
    - Analysis of captured network traffic and detection of the simulated breach.
    - Recommendations for securing personal devices and online accounts against TFGBV.

This curriculum ensures students gain hands-on experience in using digital forensic tools and understanding how to secure social media platforms and smartphones, which are commonly targeted in TFGBV cases.

References

1. **Laura Chappell & Gerald Combs** (2019). *Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide*.
   ISBN: 978-1893939940.
2. https://www.geeksforgeeks.org/what-is-cisco-packet-tracer