DIGITAL FORENSICS AND CYBERSECURITY

YEAR 3

SEMESTER 2

SEMESTER 2 GROUP PROJECT PROPOSAL

GROUP MEMBERS:

DENYS RUDENKO B00156766

PRATHAM RAINA B00158273

MUHAMMAD MUNEEB NADEEM B00158381

Project Title:

"Understanding Cybersecurity Threats: An Integrated Approach to Social Engineering, Malware, and Vulnerability Analysis"

Introduction:

In today's interconnected world, cybersecurity threats continue to grow in complexity, targeting individuals, organizations, and governments. This project focuses on addressing these threats by combining three critical aspects of cybersecurity: **social engineering**, **malware analysis**, and **vulnerability analysis**.

Our goal is to provide a comprehensive understanding of how attacks are conducted and how they can be mitigated. By integrating these topics, we aim to highlight the lifecycle of a cyberattack—from exploiting human vulnerabilities to analysing malware behaviour, and finally, identifying and addressing system weaknesses.

Objectives:

1. **Demonstrate Cybersecurity Attacking Techniques:**
   - Simulate a **social engineering** attack using a **cloned website** to gather user credentials.Analyze **malware** using **njRAT** to showcase the impact of remote access trojans.
2. **Demonstrate a Defensive Strategy:**
   - Perform a **vulnerability analysis** on a system and propose effective mitigation strategies.
3. **Provide Educational Value:**
   - Document the theoretical concepts of each module to help others understand the concepts and methods.
4. **Showcase Integration:**
   - Combine offensive and defensive cybersecurity methods into a project to show the interplay between attacks and defensive approaches.

Project Overview

The project is divided into three interconnected sections, each addressing a key cybersecurity area:

Section 1: Social Engineering

- **Description:** Social engineering exploits human psychology to obtain sensitive information. This module will cover the theory behind social engineering and demonstrate a phishing attack by cloning a website using the **Social Engineering Toolkit (SET)**.
- **Expected Outcome:** A practical demonstration of how attackers can trick users into sharing sensitive information.

Section 2: Malware Analysis

- **Description:** Malware is one of the most pervasive cybersecurity threats. This module will simulate a remote access trojan (RAT) attack using **njRAT**. We'll demonstrate its capabilities, such as keystroke logging and file access, to show how attackers can control compromised systems.
- **Expected Outcome:** A clear understanding of how malware operates and the potential risks it poses.

Section 3: Vulnerability Analysis

- **Description:** Defensive cybersecurity focuses on identifying and mitigating system weaknesses. This module will involve scanning a system or a vulnerable web app for vulnerabilities using tools like **Nessus** or **OpenVAS**.
- **Expected Outcome:** A report detailing vulnerabilities and steps to prevent exploitation

Methodology

1. **Research and Planning:**
   - Study the theoretical background of social engineering, malware, and vulnerability analysis.
   - Plan the project structure and assign responsibilities among team members.

2. **Integration:**
    - Perform each **practical** demonstration in a step-by-step manner, documenting the process thoroughly.
    - Combine the three section as one project system to demonstrate how offensive and defensive techniques are interconnected.
3. **Documentation:**
    - Prepare detailed reports for each module, including theoretical explanations, practical steps, and mitigation strategies.

Tools and Technologies

- **Social Engineering Toolkit (SET):** For cloning websites and simulating phishing attacks.
- **njRAT:** For demonstrating malware capabilities in a controlled environment.
- **Nessus/OpenVAS:** For vulnerability scanning and analysis.
- **Python and Bash Scripts:** For automation and customization where necessary.

Deliverables

1. **Practical Demonstrations:**
    - A step-by-step implementation of a phishing attack.
    - A malware simulation showcasing the impact of remote access trojans.
    - A vulnerability assessment with detailed recommendations for mitigation.
2. **Documentation:**
    - A project report covering theoretical and practical aspects of each module.
3. **Presentation:**
    - A presentation summarizing the project, including demonstrations and key findings.