TIMOTHY SEWE OGODE(CSSA0423076)

CYBER SHUJAA

WEEK 2

INTRODUCTION TO CYBERSECURITY

Table of Contents

[INTRODUCTION 2](#_Toc136526043)

[1. INTRO TO OFFENSIVE SECURITY 2](#_Toc136526044)

[i. Hacking your First machine 2](#_Toc136526045)

[ii. What is Offensive Security 2](#_Toc136526046)

[iii. Careers in Cyber Security 2](#_Toc136526047)

[2. WEB APPLICATION SECURITY 3](#_Toc136526048)

[i. Introduction 3](#_Toc136526049)

[ii. Web Application Security Risks 3](#_Toc136526050)

[iii. Example of Web Application Security 3](#_Toc136526051)

[3. Digital Forensics 4](#_Toc136526052)

[i. Introduction 4](#_Toc136526053)

[ii. Digital Forensics Process 4](#_Toc136526054)

[iii. Example of Digital Forensics 4](#_Toc136526055)

[4. CONCLUSION 5](#_Toc136526056)

# INTRODUCTION

Cybersecurity is a crucial field focused on protecting computer systems, networks, and data from unauthorized access, theft, damage, or disruption. It encompasses various practices, technologies, and strategies aimed at safeguarding digital information and ensuring the confidentiality, integrity, and availability of data. In today's interconnected world, cybersecurity plays a vital role in defending against cyber threats such as malware, phishing attacks, data breaches, and hacking attempts. Professionals in cybersecurity work to identify vulnerabilities, implement security measures, monitor systems for potential threats, and respond effectively to incidents. By staying ahead of evolving threats and constantly adapting to new technologies, cybersecurity professionals contribute to maintaining the security and trustworthiness of digital environments for individuals, organizations, and society as a whole.

# INTRO TO OFFENSIVE SECURITY

Offensive security is a proactive and authorized approach to assessing computer systems, networks, and applications for vulnerabilities. By simulating real-world attacks, offensive security professionals aim to identify weaknesses and improve the overall security of a system. Activities such as penetration testing, vulnerability assessment, social engineering, and exploit development are carried out to uncover potential vulnerabilities before malicious actors can exploit them. The goal is to help organizations understand their vulnerabilities, strengthen their defence mechanisms, and enhance their overall cybersecurity posture. Through offensive security practices, organizations can better protect their systems, data, and infrastructure from potential threats and attacks.

## Hacking your First machine

To begin hacking the fake bank application called FakeBank, we need to use the command-line application GoBuster to find hidden directories and pages. Firstly, open a terminal on the machine provided. Next, execute the GoBuster command in the terminal, specifying the website URL (http://fakebank.com) and the wordlist file (wordlist.txt) to search for potentially hidden pages. GoBuster will scan the website and display the discovered pages, denoted by a "Status: 200" response. Once you have identified a secret bank transfer page (/bank-transfer), input this page's URL into the FakeBank website. This page allows you to transfer money between accounts, and as an ethical hacker, you would identify such vulnerabilities and report them to the bank for remediation. For the task at hand, transfer $2000 from account 2276 to your own account (account number 8881).

## What is Offensive Security

Offensive security is the act of hacking into computer systems, taking advantage of software flaws, and locating security gaps in software to obtain unauthorized access to them. To defeat a hacker, you must act in a hacker-like manner by identifying flaws and suggesting remedies before a cybercriminal does. Defensive security is the act of defending a company's computer network and systems against any potential digital attacks. In a defensive cyber job, you can be searching for cybercriminals, tracing down compromised systems or devices, or keeping an eye on infrastructure for nefarious activities.

## Careers in Cyber Security

Careers in cybersecurity provide diverse opportunities to protect against cyber threats. Roles include security analysts, penetration testers, incident responders, and consultants. Professionals identify vulnerabilities, implement security measures, and safeguard systems. The growing demand for skilled experts makes cybersecurity a rewarding and challenging career path.

# WEB APPLICATION SECURITY

## Introduction

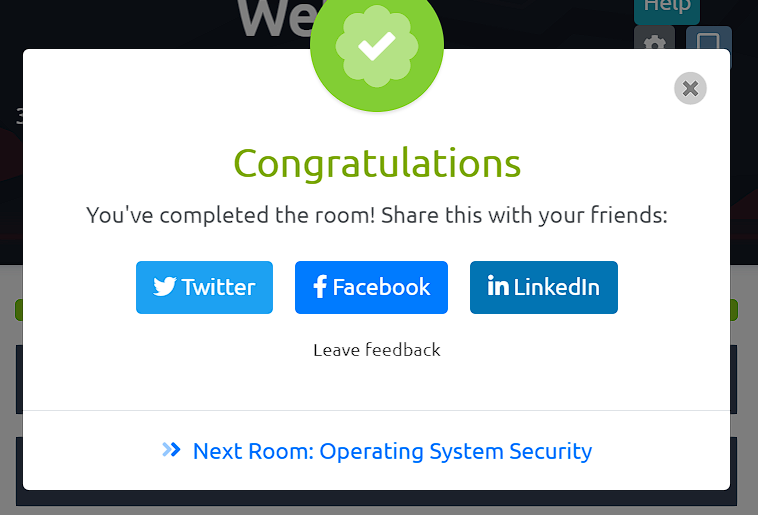
Web applications provide the convenience of using programs without the need for installation. They run on remote servers and can be accessed through web browsers. Examples include webmail, online office suites, and online shopping platforms. Web applications retrieve data from database servers to provide information and services. However, the security of web applications is crucial, as a vulnerability can lead to significant losses for companies and customers. Bug bounty programs are offered by companies to reward individuals who discover and report security vulnerabilities in their systems.

## Web Application Security Risks

Online shops have certain functions like logging in, searching for products, adding to the cart, and providing payment details. However, these steps can be vulnerable to attacks. Attackers may try to discover passwords through brute force or exploit weaknesses in search functions to access unauthorized data or execute unauthorized programs. Payment details may be at risk if not properly encrypted. Common vulnerabilities include identification/authentication failures, broken access control, injection attacks, and cryptographic failures. Understanding these vulnerabilities is crucial for securing web applications.

## Example of Web Application Security

This task focuses on a vulnerable website that suffers from Insecure Direct Object References (IDOR), a form of Broken Access Control. IDOR occurs when a web application fails to validate user permissions for accessing specific objects, allowing unauthorized access. For example, a user might access files or data by guessing sequential object names or IDs. This vulnerability can lead to the exposure of sensitive information or unauthorized actions.



# Digital Forensics

## Introduction

Forensics is the scientific application used to investigate crimes and uncover facts. As technology has become more prevalent, digital forensics emerged as a specialized field to investigate digital crimes. In scenarios where law enforcement encounters digital devices and media at a crime scene, questions arise regarding the collection, handling, and analysis of digital evidence. Procedures must be followed to collect evidence from running devices, transfer it securely, and analyze vast amounts of data stored on personal devices. Digital forensics applies computer science techniques to examine digital evidence for legal purposes, serving both public-sector investigations conducted by government agencies and law enforcement and private-sector investigations initiated by corporate entities to address policy violations.

## Digital Forensics Process

Primary goal is to collect, preserve, and analyse digital evidence in a secure and systematic manner. After obtaining legal authorization, you must acquire the relevant digital devices and establish a chain of custody to ensure the integrity of the evidence. Safely transporting the evidence to the lab, you create forensic copies of the data to work with, preserving the original evidence. The investigation process involves using validated tools and techniques to process and analyse the digital evidence. Finally, the findings are documented in a comprehensive report, presenting the discovered evidence and conclusions. Adhering to these principles ensures the integrity, reliability, and reproducibility of the digital forensics investigation.

## Example of Digital Forensics

By converting the document to PDF format and using the program pdf info, we can extract metadata such as the creator, producer, creation date, modification date, and PDF version. In this case, the metadata reveals that the document was created using Microsoft Word for Office 365 on October 10, 2018. This information can provide insights into the source and potential clues about the perpetrator. Analysing file metadata is just one aspect of digital forensics that helps uncover evidence and unravel the details of a case.

A screenshot of a computer

Description automatically generated with medium confidence

# CONCLUSION

This report explored the methodologies and techniques employed in offensive security, understanding the need for ethical hacking to identify and mitigate vulnerabilities. In the context of web application security, we discussed common threats and countermeasures, emphasizing the significance of secure coding practices and vulnerability testing. Additionally, we explored the field of digital forensics, highlighting the process of collecting and analysing digital evidence for investigative purposes. Through these discussions, we have gained valuable insights into the various aspects of cybersecurity, reinforcing the importance of proactive measures and a comprehensive approach to protect digital assets and investigate potential incidents.