Google Developer Student Clubs
Faculty Of Sciences Of Tunis (FST)

Introduction to Cybersecurity

Alaa Brahim

October 27, 2023

Contents

Chapter 1

Introduction

1.1 Welcome to Cybersecurity

Welcome to the GDSC FST Cybersecurity Introduction session! In this session, we will explore the fascinating world of cybersecurity and the critical role it plays in safeguarding computer systems, networks, and data. Cybersecurity is a rapidly evolving field, and understanding its fundamentals is essential in today's interconnected digital landscape.

1.2 What is Cybersecurity?

Cybersecurity is the practice of protecting computer systems, networks, and data from theft, damage, or unauthorized access. It encompasses a wide range of strategies and techniques designed to safeguard sensitive information and maintain the integrity of digital assets. In an age where technology is deeply integrated into our lives, cybersecurity is more important than ever to ensure the privacy and security of individuals, organizations, and governments.

Chapter 2

Common Cybersecurity Terminology

2.1 Vulnerabilities

Vulnerabilities refer to weaknesses or flaws in computer systems, software, or networks that can be exploited by malicious actors.

These vulnerabilities can vary in complexity, from highly sophisticated to rather simple. Some common examples of simple vulnerabilities include:

- Weak Passwords: Using easily guessable passwords such as "password" or "123456" is a straightforward way to compromise security.

- Outdated Software: Running outdated software or operating systems with known security flaws can expose your systems to exploitation.

Identifying and addressing vulnerabilities is a crucial aspect of cybersecurity to prevent potential breaches and attacks.

2.2 Attack

An attack in cybersecurity refers to unauthorized access or harm to computer systems, networks, or data. It's the malicious act that exploits vulnerabilities to compromise the security and integrity of digital assets. Some examples of attacks include:

- Brute Force Attack: involves repeatedly trying passwords or encryption keys to gain unauthorized access. It's a method of systematically checking all possible combinations until the correct one is found.

2.3 Types of Attacks

Cyberattacks come in various forms. They can broadly be categorized into the following:

2.3.1 Physical Attacks

Physical attacks involve direct, unauthorized access to a computer system, network, or hardware. These attacks often require physical proximity to the target and can include break-ins to server rooms or the theft of physical devices.

2.3.2 Remote Attacks

Remote attacks occur when hackers exploit vulnerabilities from a distance, often over the internet. These attacks can be executed without physical access to the target systems. Examples include phishing attacks through email or fake websites.

2.4 Malware

Malware, short for malicious software, encompasses a wide range of harmful software types designed to compromise computer systems, networks, or data. Two common examples of malware are:

- Ransomware: a type of malware that encrypts data on the victim's system and demands a ransom in exchange for the decryption key. It can lead to data loss and financial extortion.

- Virus: a specific type of malware that often attaches to legitimate programs or files and executes when the host program is run.

Chapter 3

Capture The Flag (CTF)

3.1 What is a CTF?

A Capture The Flag (CTF) competition is a cybersecurity challenge where participants solve a series of puzzles and tasks to find hidden "flags." These flags are typically strings of text or codes hidden within the challenges. CTFs come in various difficulty levels, making them suitable for both beginners and experienced cybersecurity enthusiasts.

3.2 Beginner-Friendly Platforms

If you're new to CTFs, there are several beginner-friendly platforms to get you started. One notable platform is "picoCTF," which offers a wide range of challenges that cater to novice participants. These challenges are designed to teach fundamental cybersecurity concepts and gradually increase in complexity as you progress.

3.3 CTF Categories

CTFs feature challenges from various categories, each focusing on a different aspect of cybersecurity. Here are some common CTF categories:

3.3.1 Cryptography

In CTFs, cryptography challenges involve encoding and decoding messages using various techniques. One common simple method is "ROT13", a letter substitution cipher that shifts each letter in the alphabet by 13 positions. For example, the quote by John Perry Barlow, "When cryptography is outlawed, bayl bhgynjf jvyy unir cevinpl," becomes "When cryptography is outlawed, only outlaws will have encryption" after decoding.

You might also encounter binary encoding challenges in CTFs. Binary encoding represents text using ones and zeros. For instance, decoding "01000111 01000100 01010011 01000011" reveals the original text "GDSC."

Cryptography challenges test your ability to identify and apply encoding and encryption methods to uncover hidden messages or flags.

3.3.2 Web Exploitation

Web exploitation challenges in CTFs often involve identifying and exploiting vulnerabilities in web applications. These challenges can require a keen eye for detail and an understanding of web technologies.

One common technique in web exploitation challenges is to leave clues in the website's source code. For example, in the script.js file of alaabrahim.github.io/gdsc-cyber-intro-web, you will find code like this:

```
// Check if the hash matches ’GDSC{Y0u_f0und_y0ur_f1rst_fl4g!}’
// note to self: remove this comment
if (
  hashHex ===
  "e248689043d9761a616c73839049467e69430516c0a7791c7d6f2eba8c284aca"
) {
  alert("Congratulations! You won!");
} else {
  alert("Try again.");
}
```

3.3.3 Open Source Intelligence (OSINT)

OSINT challenges involve gathering information from publicly available sources, such as social media, websites, or public records, to uncover insights and identify potential security risks.

3.3.4 Steganography

Steganography challenges in CTFs involve the art of hiding secret information within seemingly innocuous files or data, making it challenging to detect and extract concealed content. Two common examples are:

- Adding data directly to the end of a file. You can practice this concept by visiting alaabrahim.github.io/gdsc-cyber-intro-web and exploring the website logo.

- Encoding a secret message in the least significant bit (LSB) of pixels in images. By subtly altering the color of individual pixels, hidden messages can be embedded within an image without noticeably affecting its appearance.

3.3.5 Forensics

Forensics challenges in CTFs involve analyzing and recovering information from digital artifacts. This can include examining log files, analyzing network traffic, or investigating incidents to find hidden flags. Log files, for example, record various activities and events in a system or application, making them valuable sources of information for cybersecurity analysts.

- Example: Consider the following log entries (log.txt): In this example, the log entries show user activity, and it's possible to detect that the user "TurboSlayer" is attempting to brute force the web challenge by attempting multiple flags. Analyzing log files like this can provide insights into suspicious or noteworthy actions that are essential for investigating and resolving cybersecurity incidents.

3.4 Reverse Engineering

Reverse engineering in CTFs often involves the analysis of precompiled binaries or programs to understand their functionality, uncover vulnerabilities, or extract hidden information. This process aims to get as close as possible to the original source code, even when it's not available.

- Example: Consider a scenario where you have a compiled program without access to the original source code. The program checks for a flag:

```
#include <stdio.h>
#include <string.h>

char *flag = "GDSC{this_is_a_flag}";
char input[100];

int main() {
    printf("Enter the flag: ");
    scanf("%99s", input);
    if (strcmp(input, flag) == 0)
```

```
        printf("Correct!\n");
    else
        printf("Wrong!\n");
    return 0;
}
```

While the source code is hidden, artifacts remain in the binary that can provide insights. By opening the binary in a text editor or using the strings command in Linux, you can find all the strings defined in the code, including the hidden flag.

3.4.1 Other Categories

CTFs often include additional categories like mobile application security,buffer overflows and more. The goal is to provide a diverse set of challenges to test your skills and encourage learning.

CTFs are an excellent way to enhance your cybersecurity knowledge and problem-solving abilities. As you progress, you'll gain a deeper understanding of various aspects of cybersecurity and develop the skills needed to protect and secure digital systems.

Chapter 4

Special Topics

In this special chapter, we will delve into advanced topics in cybersecurity that expand on the concepts covered earlier in this document.

4.1 Physical Attacks with ATtiny85

The ATtiny85 is a microcontroller capable of being used for various purposes, including as a tool in physical attacks. One of its applications is emulating HID (Human Interface Device) devices, such as keyboards or mice, to execute malicious actions on a target computer. This technique is known as "Bad USB." Bad USB can be used to inject keystrokes or execute predefined scripts on the target system. Here is how you can make your own using a cheap microcontroller like the attiny85: link.

Understanding Bad USB attacks involves recognizing the potential risks of plugging untrusted USB devices into your computer, as they can act as keyboard emulators and compromise your system's security. Mitigating this risk requires awareness and protective measures.

4.2 Remote Attacks with Metasploit

Metasploit is a popular penetration testing tool used by both cybersecurity professionals and malicious actors. It offers a wide range of exploits, payloads, and post-exploitation tools to compromise remote systems. While it's an essential tool for cybersecurity professionals, it can also be used to generate malware for remote attacks.

Using Metasploit to create malware allows attackers to craft malicious payloads and propagate them to target systems. Understanding these techniques is crucial for cybersecurity professionals to defend against such threats.

It's essential to stay vigilant and take steps to secure your systems against potential Metasploit-based attacks. Here is a youtube playlist for those of you interested in learning more about the Metasploit framework: link.

This special chapter highlights the dual nature of technology, where powerful tools can serve both defensive and offensive purposes. It emphasizes the importance of responsible and ethical use of cybersecurity knowledge to protect digital environments and infrastructure.

Remember that cybersecurity is a constantly evolving field, and staying informed about the latest trends and threats is essential for effectively defending against cyberattacks.

Chapter 5

Conclusion

In this guide, we've delved into the essential realm of cybersecurity, covering fundamental concepts, practical applications, and real-world challenges. We've explored various facets of cybersecurity, from terminology and vulnerability analysis to capture the flag (CTF) competitions and reverse engineering.

We've seen the importance of staying informed about emerging threats and evolving security strategies, and the dual nature of tools like Metasploit and ATtiny85. As we conclude, remember that cybersecurity is an ever-changing field that demands continuous learning and a strong commitment to ethical practices.

Your journey in cybersecurity has just begun. Use your knowledge to contribute to digital security, protect data, and defend against cyber threats. We hope this guide has equipped you with the foundation needed to excel in the ever-connected world of cybersecurity.