1. Introduction to Cybersecurity

Introduction

Information is typically characterized by the highest possible degree of certainty, assumed to be accurate and valid, and available to individuals or groups. The most important feature of information is that it provides us with meaning and context about the world around us. For example, when we read a book or talk to someone, we learn new information and use this information to shape our thoughts and behaviors.

Information Security

Information security involves protecting information from unauthorized use, disclosure, destruction, alteration, damage, or preventing unauthorized access to it. We can also define information security as the set of measures taken to prevent information from being harmed in the wrong hands.

Principles of Information Security: The CIA Triad

Confidentiality: Ensures that information is accessible only to authorized individuals and prevents others from viewing it.

Integrity: Means that information remains accurate and unchanged, preventing it from being accidentally or intentionally altered.

Availability: Ensures that information is easily accessible to authorized users when needed.

Information security encompasses the protection of both physical documents and electronic data. This includes a wide range of measures, from encryption techniques to access control systems and antivirus software.

Today, especially with the widespread use of the internet, information security is of vital importance for both individuals and organizations.

Hacker

The concept of "hack" is a versatile term used in various fields and can carry different meanings depending on the context. Generally, it can be described as using or modifying a system in unintended ways.

A hacker is a skilled computer expert with in-depth technical knowledge of computer systems and networks, capable of utilizing this knowledge for various purposes.

Hackers are often curious, problem-solving individuals who think creatively and have a keen interest in technology.

Types of Hackers

Hackers are categorized into three types based on their approaches and behaviors.

White Hat: White hat hackers are well-intentioned hackers who know the techniques and methods used by cyber criminals and recognize the tools and software used during hacker activities. White hat hackers work to enhance system security. They collaborate with companies to identify security vulnerabilities and help them fix these issues.

Black Hat: Black hat hackers are malicious hackers who harm systems, steal information, and gain unauthorized access to systems. Often depicted as the "bad guys" in the media, these hackers breach security systems for personal gain or other harmful intentions. Their actions include data theft, spreading malware, and other cybercrimes.

Gray Hat: Gray hat hackers know the techniques and methods used by malicious hackers and recognize the tools and software used during hacker activities. They are computer experts who sometimes may violate the law but generally operate within legal bounds and uphold ethical standards. This group stands somewhere between ethical and unethical hacking. They may access systems without authorization but usually report the security vulnerabilities they find to the respective organization to show goodwill. Their intentions may not be entirely malicious, but their methods are questionable.

Ethical Hacker

Ethical hackers fall under the category of white hat hackers.

The role of ethical hackers is to test and strengthen the security of computer systems, networks, and data. In addition to having deep technical knowledge, being an ethical hacker requires strong ethical values and a sense of responsibility. Ethical hackers typically enhance their skills through specialized training and certifications.

Ethical hackers perform penetration tests to identify potential security vulnerabilities, conduct vulnerability analysis, and perform risk assessments. Their goal is to uncover weaknesses that attackers could exploit and make recommendations to fix them.

In the cybersecurity world, the role of ethical hackers is becoming increasingly important. As technology becomes more integrated into our lives, the demand for these experts in ensuring the security of the digital world also increases.

"To be a hacker is to bring the impossible within reach through unexpected behaviors."

- Anonymous

Question

Q: What is the sum of the squares of the numbers from 1 to 100?

A: 338350

Explanation: The first method that might come to mind to solve this problem is to take the squares of each number from 1 to 100 and sum them up one by one. However, using the formula

n * (n + 1) * (2 * n + 1) / 6

allows for a much faster solution, stepping outside the usual approach—what we can call a mathematicalhack.

Sub-Fields of Cybersecurity

Cybersecurity is a concept that represents our security in the digital world. To ensure our security in the digital realm, cybersecurity encompasses many critical sub-fields. Each area is a specialized domain and a crucial part of protecting our systems.

Let's take a closer look at the important sub-fields of cybersecurity.

Application Security

Application security focuses on ensuring the security of applications from the development stage onward. This area includes identifying and fixing software bugs and other security vulnerabilities. Security tests and secure coding standards are important components of this field.

Web Application Security

Web application security focuses on detecting, preventing, and mitigating threats to web-based applications. In this field, vulnerabilities such as SQL Injection, XSS, CSRF, and IDOR are among the most common. Web application security is essential for protecting user data, maintaining application performance, and preserving the reputation of enterprises.

Regular penetration tests (pentests) are conducted to identify and address security vulnerabilities in web applications.

Network Security

Network security involves protecting network resources to prevent, detect, and respond to malicious threats and attacks. Technologies such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and virtual private networks (VPN) are used in this field.

Network security is crucial for ensuring the secure transmission of data and preventing unauthorized access.

Reverse Engineering

Reverse engineering involves analyzing software, devices, or systems to understand how they work, both statically and dynamically. This field can be used to find security vulnerabilities, analyze malware, and bypass licensing or other protection mechanisms.

Cloud Security

Cloud security ensures the protection of data, applications, and infrastructure in cloud computing services. This includes identity and access management (IAM), data encryption, firewalls, and other cloud-based security protocols. Cloud security ensures that data is stored, processed, and transmitted securely in the cloud.

Mobile Application Security

Mobile application security encompasses security measures specific to mobile devices and applications. This includes protection against malware, preventing data leaks, and implementing end-to-end encryption techniques.

IoT Security

IoT (Internet of Things) security involves ensuring the security of smart devices, sensors, and other IoT devices. This area covers device security, data protection, and network security. IoT security is critically important for protecting the expanding IoT ecosystem from threats.

Digital Forensics

Digital forensics includes technical and legal procedures for investigating and analyzing cybercrimes. This field focuses on practices such as data recovery, electronic evidence collection, and investigating cybercrimes. Digital forensics plays a vital role in criminal investigations and legal processes.

<u>Threat Intelligence</u>

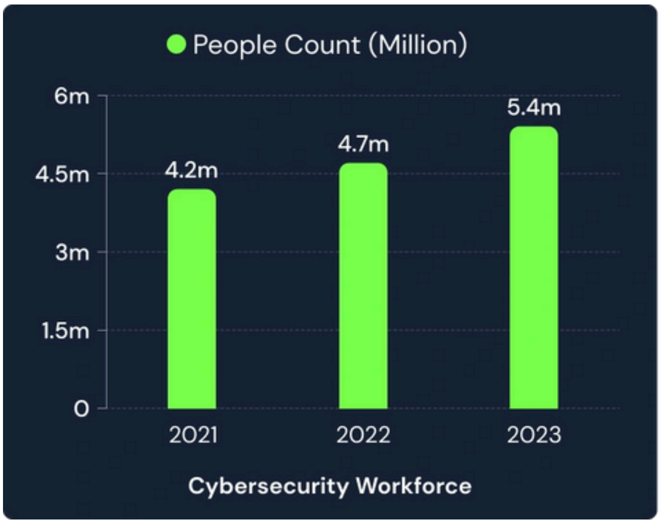
Threat intelligence involves gathering and analyzing information about cyber threats. This information is used to prevent, detect, and respond to threats. Threat intelligence provides security teams with the ability to anticipate attacks and take proactive measures.

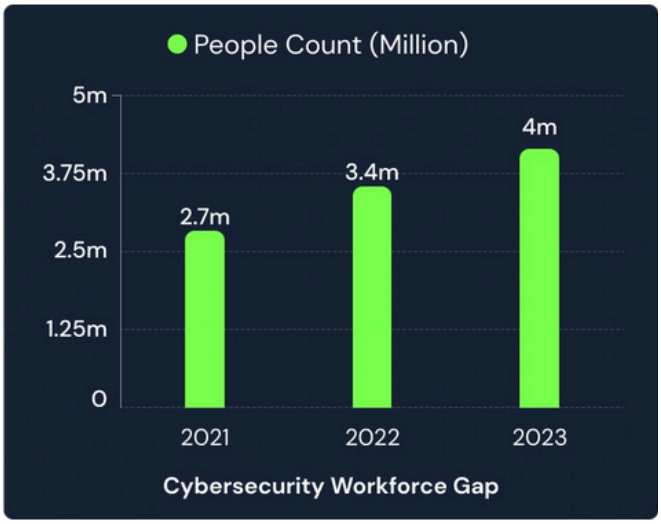
Career

As cyber attacks and threats increase every day, interest and employment in the field of cybersecurity continue to grow. Companies invest in this field to protect their reliability and reputation, while countries also invest similarly to prepare for potential cyber warfare.

The increase in investments in cybersecurity drives both technological innovation and the expansion of job opportunities in the sector.

Below, you can see graphs showing employment numbers and workforce gaps in the cybersecurity sector.





The data were obtained from (ISC)^2 (International Information System Security Certification Consortium) reports.

As seen in the above graphs, although there is an increasing employment rate in recent years, the workforce gap also grows each year.

Various positions in cybersecurity include developing defense and attack strategies, hardening systems to enhance security, or performing penetration tests to improve the security of institutions.

Career Journey

Anyone considering a career in cybersecurity will encounter many challenges and opportunities on this journey. The key to success in this process is undoubtedly regular and focused discipline.

Since cybersecurity requires deep technical knowledge, you may occasionally feel inadequate. However, aside from these challenges, the sector offers high financial rewards and flexible working conditions, such as remote work, making it an attractive field.

It is important to network and meet experienced professionals in this field to advance. Connecting with these individuals through online forums, professional networks like LinkedIn, Discord channels, or cybersecurity conferences and workshops can provide significant benefits in terms of knowledge exchange.

As you expand your network and enhance your technical skills, don't forget to develop your social skills, which are often overlooked but crucial for cybersecurity professionals. Communication skills, responsibility, team collaboration, and problem-solving abilities are among the essential social characteristics needed for success in this field.

As someone starting or considering starting a career in cybersecurity, you should ask yourself the following questions:

- How strong is my interest in technology and innovation?
- How open am I to learning new information?
- Do I trust myself in solving problems I encounter?
- Am I a team player?
- How do I react under stress, and how can I manage it?
- Am I ready to work long hours if needed to complete projects on time?

Cybersecurity is a constantly evolving field that presents new challenges. Therefore, you must be prepared for the challenges you will encounter and continually learn and adapt to succeed in your cybersecurity career.

Teams

Cybersecurity is a field with many sub-disciplines. The teams listed below help organizations counter cyber threats and ensure the organization's security. Although each team has different roles and responsibilities, they all serve a common goal: strengthening the organization's cybersecurity posture.

Red Team

The Red Team is a group that acts from the attacker's perspective to test an organization's cybersecurity. Their aim is to discover potential vulnerabilities and security gaps, exploit these weaknesses, and realistically test the organization's cyber defense capabilities. Red Team operations include various methods such as attack scenarios, penetration tests, and social engineering tactics. Their work helps understand how well the organization's defenses are prepared for real-world threats.

Blue Team

The Blue Team is responsible for strengthening and maintaining the organization's cybersecurity defenses. This team defends the organization against the Red Team's attack attempts, continuously monitors and improves security measures to prevent and detect security breaches. The Blue Team's duties include monitoring and managing firewalls, intrusion detection systems, and other security solutions, incident response, implementing security policies, and providing security awareness training to employees.

Purple Team

The Purple Team aims to maximize the organization's cybersecurity capabilities by combining the efforts of the Red and Blue teams. Serving as a bridge between the Red and Blue teams, the Purple Team allows both sides to learn from each other and develop their skills. They guide the Blue Team on how to address vulnerabilities discovered by the Red Team and provide feedback to enhance the effectiveness of defense strategies.

Bug Bounty

Bug Bounty is a defense strategy for companies and a revenue source for cybersecurity researchers that has gained significant popularity in recent years. In bug bounty programs, cybersecurity researchers who discover security vulnerabilities within the specified scope and report these vulnerabilities are rewarded with money. Through these programs, organizations become more resilient to cyber attacks while cybersecurity researchers can earn income.

Penetration Testing (Pentest)

Penetration testing is the process of identifying potential security vulnerabilities in an organization's software, systems, and IT infrastructure by simulating real-world cyber attacks. These tests help organizations strengthen their defenses, identify critical vulnerabilities ahead of time, and minimize the impact of a potential security breach.

Penetration tests are conducted within the framework of a contract signed between the organization requesting the test and the organization performing the test. This contract ensures that the test activities are conducted legally and defines the scope of the test. Only the components specified in the contract may be tested, ensuring that the process adheres to both legal and ethical standards.

Professionals involved in penetration testing are usually referred to as "pentesters," "penetration testers," or "cybersecurity experts." These professionals conduct tests within the scope of their given authority using an ethical hacker approach and report the security vulnerabilities they identify.

Types of Penetration Testing

Penetration tests can be classified into three main categories based on the level of information provided: White Box, Grey Box, and Black Box.

White Box

The team conducting the test is given comprehensive information and authority about the system. This approach allows for an in-depth analysis and testing of the system.

Grey Box

The team performing the test is provided with partial information and authority about the system. This creates a more realistic test scenario and demonstrates how pentesters can progress with partial information.

Black Box

The test team conducts the test without any prior knowledge about the system. This offers the most realistic scenario from the perspective of an actual attacker.

Penetration Testing Methodologies

Penetration testing methodologies are standardized approaches used to systematically identify and assess security vulnerabilities. These methodologies enhance both the effectiveness and efficiency of penetration tests.

OWASP

The Open Web Application Security Project (OWASP) is a global initiative focused on improving the security of web applications. The OWASP penetration testing methodology provides a framework for identifying, assessing, and mitigating security vulnerabilities in web applications and services. This methodology guides both developers and security experts in ensuring application security.

OSSTMM

The Open Source Security Testing Methodology Manual (OSSTMM) provides a methodology for information security testing and can be applied to a wide range of areas such as network security, application testing, and physical security audits. OSSTMM offers a detailed methodology that ensures security tests are conducted transparently, objectively, and repeatably. It also provides guidance for measuring security performance and continuously improving the security posture.

NIST

The National Institute of Standards and Technology (NIST) penetration testing methodology provides standards and best practices, particularly for government agencies and large-scale organizations. NIST's cybersecurity methodology encompasses risk management, the assessment of security vulnerabilities, and post-breach incident management processes. This methodology helps organizations conduct comprehensive security assessments and meet compliance requirements.

Basic Information

Port

Ports are virtual or physical connection points used for data transfer between computers.

Physical Ports

Physical ports are hardware-based connection points found on computers. Examples include USB, Ethernet, HDMI, and DisplayPort, which are used to connect various devices to the computer and facilitate data transfer.

Virtual Ports

Virtual ports are numbered between 0 and 65535 and are used for communication over a network. Each port number is associated with specific services or protocols, and all data transfer over the internet occurs through these virtual ports.

For example, when visiting websites, we connect to port 80 or 443 on the server hosting the website.

Commonly used services and protocols operate on specific ports. Below is a table of some frequently used ports and services:

Port Number	**Service / Protocol**
21	FTP
22	SSH
23	Telnet
25	SMTP
53	DNS
80	HTTP
443	HTTPS
3306	MySQL
3389	RDP
5432	PostgreSQL

Vulnerability

A vulnerability refers to security weaknesses in computer systems. These weaknesses can be exploited by attackers to gain unauthorized access, steal data, or use the system for malicious purposes.

OWASP TOP 10: A list ranking the most critical security vulnerabilities in web applications.

CVE (Common Vulnerabilities and Exposures): A public directory that identifies known security vulnerabilities and exposures.

CVSS (Common Vulnerability Scoring System): A scoring system used to measure the severity of security vulnerabilities.

Exploit

An exploit is the code or technique that enables the malicious use of a vulnerability. This allows attackers to gain unauthorized access or control over systems.

PoC (Proof of Concept): Demo content demonstrating the exploitability of a vulnerability.

Zero Day: Security vulnerabilities that are not yet patched and are generally unknown to the public.

Shell

A shell is a computer program that provides users with an interface to use the services of an operating system.

Gaining a shell on a system allows an attacker to execute commands on the target system through an interface.

Bind Shell: A type of shell where the attacker opens a port on the target machine and connects to it to execute commands.

Reverse Shell: A type of shell where the target machine connects back to the attacker's machine, allowing the execution of commands.

Web Shell: A type of shell that includes a malicious script running on a web server, giving the attacker remote command execution capabilities.

IP (Internet Protocol) Address

An IP address is a unique number that identifies devices on the internet and facilitates communication between them.

IPv4: Uses a 32-bit addressing system and provides approximately 4.3 billion unique addresses.

IPv6: Developed due to the insufficient addressing capacity of IPv4, it uses a 128-bit addressing system.