This is a brief review of the book. If you're interested in purchasing, feel free to contact me.

The path to the world of Cybersecurity

based on

Google Cybersecurity Courses

created by

Adham Al-Saadi

This is a brief review of the book. If you're interested in purchasing, feel free to contact me.

This is a brief review of the book. If you're interested in purchasing, feel free to contact me.

The courses of the program are as follows:

1. **Foundations of Cybersecurity**
   Explore the cybersecurity profession, including significant events that led to the development of the cybersecurity field and its continued importance to organizational operations. Learn about entry-level cybersecurity roles and responsibilities.

2. **Play It Safe: Manage Security Risks**
   Identify how cybersecurity professionals use frameworks and controls to protect business operations, and explore common cybersecurity tools.

3. **Connect and Protect: Networks and Network Security**
   Gain an understanding of network-level vulnerabilities and how to secure networks.

4. **Tools of the Trade: Linux and SQL**
   Explore foundational computing skills, including communicating with the Linux operating system through the command line and querying databases with SQL.

5. **Assets, Threats, and Vulnerabilities**
   Learn about the importance of security controls and developing a threat actor mindset to protect and defend an organization's assets from various threats, risks, and vulnerabilities.

6. **Sound the Alarm: Detection and Response**
   Understand the incident response lifecycle and practice using tools to detect and respond to cybersecurity incidents.

7. **Automate Cybersecurity Tasks with Python**
   Explore the Python programming language and write code to automate cybersecurity tasks.

8. **Put It to Work: Prepare for Cybersecurity Jobs**
   Learn about incident classification, escalation, and ways to communicate with stakeholders. This course closes out the program with tips on how to engage with the cybersecurity community and prepare for your job search.

This is a brief review of the book. If you're interested in purchasing, feel free to contact me.

This is a brief review of the book. If you're interested in purchasing, feel free to contact me.

Foundations of Cybersecurity

Course content:

- ## Module 1: Welcome to the exciting world of cybersecurity
  Begin your journey into cybersecurity! You'll explore the cybersecurity field, and learn about the job responsibilities of cybersecurity professionals.

- ## Module 2: The evolution of cybersecurity
  You will explore how cybersecurity threats have appeared and evolved alongside the adoption of computers. You will also understand how past and present cyber attacks have influenced the development of the security field. In addition, you'll get an overview of the eight security domains.

- ## Module 3: Protect against threats, risks, and vulnerabilities
  You will learn about security frameworks and controls, which are used to mitigate organizational risk. You'll cover principles of the CIA triad and various National Institute of Standards and Technology (NIST) frameworks. In addition, you'll explore security ethics.

- ## Module 4: Cybersecurity tools and programming languages
  You'll discover common tools used by cybersecurity analysts to identify and eliminate risk. You'll learn about security information and event management (SIEM) tools, network protocol analyzers, and programming languages such as Python and SQL.

This is a brief review of the book. If you're interested in purchasing, feel free to contact me.

❖ Welcome to the exciting world of cybersecurity

Imagine that you're preparing for a storm. You've received notification that a storm is coming. You prepare by gathering the tools and materials you'll need to stay safe. You make sure your windows and doors are secure. You assemble a first aid kit, tools, food and water. You're prepared.

The storm hits and there are powerful winds and heavy rain. The storm is using its force to try and breach your home. You notice some water leaks and begin patching them quickly in order to minimize any risk or potential damage.

Handling a security incident is no different. Organizations must prepare for the storm by ensuring they have the tools to mitigate and quickly respond to outside threats. The objective is to minimize risk and potential damage.

As a security analyst, you'll work to protect your organization and the people it serves from a variety of risks and outside threats. And if a threat does get through, you and your team will provide a solution to remedy the situation.

Cybersecurity (or security) : is the practice of ensuring confidentiality, integrity, and availability of information by protecting networks, devices, people, and data from unauthorized access or criminal exploitation.

As ChatGPT defines, **Cybersecurity** is the practice of defending computer systems, networks, and sensitive information from digital attacks, theft, and damage. It involves implementing technologies, processes, and controls to protect data, reduce risks, and prevent unauthorized access. Key goals include safeguarding data privacy, maintaining data integrity, and ensuring reliable access to resources for authorized users.

For example, requiring complex passwords improves confidentiality and makes it more difficult for threat actors to compromise them.

Threat actor : is any person or group who presents a security risk.

This is a brief review of the book. If you're interested in purchasing, feel free to contact me.

Benefits of security

- Protects against external and internal threats
- Meets regulatory compliance
- Maintains and improves business productivity
- Reduces expenses
- Maintains brand trust

Technology is rapidly changing, and so are the tactics and techniques that attackers use. As digital infrastructure evolves, security professionals are expected to continually grow their skills in order to protect and secure sensitive information.

So, what do security analysts do?.. Security analysts are responsible for monitoring and protecting information and systems.

Security analyst responsibilities:

- **Protecting computer and network systems**
  Requiring an analyst to monitor an organization's internal network is crucial. If a threat is detected, then an analyst is generally the first to respond. Analysts also often take part in exercises to search for weaknesses in an organization's own systems. For example, a security analyst may contribute to penetration testing or ethical hacking. The goal is to penetrate or hack their own organization's internal network to identify vulnerabilities and suggest ways to strengthen their security measures.
- **Installing prevention software**
  For the purposes of identifying risks and vulnerabilities.
- **Conducting periodic security audits**
  A security audit is a review of an organization's security records, activities, and other related documents.

There are two groups of skills that are particularly useful for a security analyst:

Transferable skills: skills from other areas that can apply to different careers
Such as Communication, Collaboration, Analysis and Problem solving.

Technical skills: skills that require knowledge of specific tools, procedures, and policies
Such as Programming languages, Security incident and event management (SIEM) tools, and Computer forensics.

This is a brief review of the book. If you're interested in purchasing, feel free to contact me.

Security professionals protect assets, manage risks, and ensure business continuity. Strong security measures are crucial to prevent data breaches that can harm reputation and erode trust by exposing personally identifiable information.

Personally Identifiable Information (PII) : Any information used to infer an individual's identity. PII includes someone's full name, date of birth, physical address, phone number, email address, or IP address and similar information.

Sensitive Personally Identifiable Information (SPII) : A specific type of PII that falls under stricter handling guidelines. SPII includes social security numbers, medical or financial information, and biometric data, such as facial recognition.

If SPII is stolen, this has the potential to be significantly more damaging to an individual than if PII is stolen. PII and SPII data are key assets that a threat actor will look for if an organization experiences a breach. When a person's identifiable information is compromised, leaked, or stolen, identity theft becomes the primary concern.

Identity theft : the act of stealing personal information to commit fraud while impersonating a victim, and the primary objective of identity theft is financial gain.

❖ The evolution of cybersecurity

The security industry is constantly evolving, but many present-day attacks are not entirely new. Attackers often alter or enhance previous methods. Understanding past attacks can provide direction for how to handle or investigate incidents in your job as a security analyst. First, let's go over a couple of key terms that will support your understanding of the attacks we'll discuss.

Computer virus : Malicious code written to interfere with computer operations and cause damage to data and software.

Worm : Malware that can duplicate and spread itself across systems on its own.
Malware : Software designed to harm devices or networks.

This is a brief review of the book. If you're interested in purchasing, feel free to contact me.

In 1986, the Alvi brothers created the **Brain virus**. Although the intention of the virus was to track illegal copies of medical software and prevent pirated licenses, the virus had unexpected consequences. Once a person used a pirated copy of the software, the virus infected their computer. Subsequently, any disk that was inserted into the infected computer would also become infected. The virus continued to spread to new computers whenever someone used one of the infected disks. Undetected, the virus rapidly spread globally within a couple of months. While the intention was not to destroy data or hardware, the Brain virus significantly impacted productivity and disrupted business operations. This event fundamentally altered the computing industry, highlighting the importance of implementing security measures to maintain both security and productivity.

In 1988, Robert Morris developed a program to assess the size of the internet. The program crawled the web and installed itself onto other computers to tally the number of computers connected to the internet. However, the program had a flaw and failed to keep track of the computers it had already compromised. As a result, it continued to re-install itself on those computers, causing them to run out of memory and crash. Approximately 6,000 computers, which represented 10% of the internet at the time, were affected by this attack. The consequences were severe, resulting in millions of dollars in damages due to business disruptions and the significant efforts required to remove the worm from the affected systems.

After the **Morris worm**, Computer Emergency Response Teams, known as CERTs® were established to respond to computer security incidents. CERTs still exist today, but their place has expanded to include more responsibilities.

As a security analyst, you will follow and maintain strategies put in place to ensure your organization has a plan to keep their data and people safe.

To better understand attacks in the digital age, we'll discuss two notable attacks that relied on the internet: the **LoveLetter attack** and the **Equifax breach**.

In the year 2000, Onel De Guzman created the LoveLetter malware to steal internet login credentials. This attack spread rapidly and took advantage of people who had not developed a healthy suspicion for unsolicited emails. Users received an

email with the subject line, "I Love You." Each email contained an attachment labeled, "Love Letter For You." When the attachment was opened, the malware scanned a user's address book. Then, it automatically sent itself to each person on the list and installed a program to collect user information and passwords. Recipients would think they were receiving an email from a friend, but it was actually malware. The LoveLetter ended up infecting 45 million computers globally and is believed to have caused over $10 billion dollars in damages. The LoveLetter attack is the first example of social engineering.

Social engineering : a manipulation technique that exploits human error to gain private information, access, or valuables.

After the LoveLetter, attackers understood the power of social engineering. The number of social engineering attacks is increasing with every new social media application that allows public access to people's data. Today, it's common for employees to receive training on how to identify social engineering attacks. Specifically, phishing through the emails they receive.

Phishing : the use of digital communications to trick people into revealing sensitive data or deploying malicious software.

In 2017, attackers successfully infiltrated the credit reporting agency, Equifax, resulting in one of the largest known data breaches of sensitive information. Over 143 million customer records were stolen, and the breach affected approximately 40% of all Americans. The stolen records included personally identifiable information such as social security numbers, birth dates, driver's license numbers, home addresses, and credit card numbers.

From a security standpoint, the breach occurred due to multiple failures on Equifax's part. It wasn't just one vulnerability that the attackers took advantage of, there were several. In the end, Equifax settled with the U.S. government and paid over $575 million dollars to resolve customer complaints and cover required fines. These are just a couple of well-known incidents that have shaped the security industry. Knowing about them will help you in your security career.

This is a brief review of the book. If you're interested in purchasing, feel free to contact me.

Understanding different types of malware and social engineering attacks will allow you to communicate about security risks during future job interviews. As a future security professional, constantly adapting and educating yourself on threat actors' tactics and techniques will be a part of your job.

As the tactics of threat actors evolve, so do the roles of security professionals. Having a solid understanding of core security concepts will support your growth in this field. One way to better understand these core concepts is by organizing them into categories, called security domains.

As of 2022, **CISSP** has defined eight domains to organize the work of security professionals. It's important to understand that these domains are related, and gaps in one domain can result in negative consequences for an entire organization. Additionally, understanding the domains can help you better comprehend your career goals and your role within an organization.

CISSP defines eight domains in total :

1. **Security and risk management** : Defines security goals and objectives, risk mitigation, compliance, business continuity, and the law.
2. **Asset security** : Secures digital and physical assets. It's also related to the storage, maintenance, retention, and destruction of data.
3. **Security architecture and engineering** : Optimizes data security by ensuring effective tools, systems, and processes are in place.
4. **Communication and network security** : Manage and secure physical networks and wireless communications
5. **Identity and access management** : Keeps data secure, by ensuring users follow established policies to control and manage physical assets, like office spaces, and logical assets, such as networks and applications.
6. **Security assessment and testing** : Conducting security control testing, collecting and analyzing data, and conducting security audits to monitor for risks, threats, and vulnerabilities.
7. **Security operations** : Conducting investigations and implementing preventative measures.

This is a brief review of the book. If you're interested in purchasing, feel free to contact me.

8. **Software development security** : Uses secure coding practices, which are a set of recommended guidelines that are used to create secure applications and services.

As an entry-level analyst, you will continue to develop your skills by learning how to mitigate risks and ensure the safety of people and data. While you don't need to be an expert in all domains, having a basic understanding of them will greatly assist you in your journey as a security professional.