The Information Security Field

The Information Security Field

- **How does this support my pentesting career?**

  - Knowing the information security field
  - Career opportunities
  - Talking with colleagues

1.1 Infosec Culture

- **Information Security** has deep roots in the **underground hacking scene**, which still looks at computer systems with curiosity, trying to figure out new ways to use and break them!

- The term *hacker* was born in the sixties in the MIT community.

- It refers to people who prefer to understand how a system works rather than just using it. These people are **curious, highly intelligent and strongly motivated to pursue knowledge!**

1.1 Infosec Culture

- Approaching systems with curiosity lets hackers and infosec professionals find new ways to use computer systems, bypassing the restrictions imposed by software vendors or programmers and deeply understanding any security pitfall of any kind of implementation.

- Being able to perform an attack also means being able to deeply understand the technology and the functioning of the target system.

1.1 Infosec Culture

- Being a hacker means being pushed by curiosity and having a hunger for knowledge. Hackers explore and improve their skills daily.

- This aspect is still valid in the modern information security field; **there is always something new** to learn, something interesting to try or something exciting to study!

1.1 Infosec Culture

- The history of hacking could easily be an entire book or a course by itself. If you do a quick Internet search on hacking, you will find that it is not necessarily related to computers only.

- Hacking is more of an approach, or a lifestyle, applied to telephone lines, people and software development.

https://en.wikipedia.org/wiki/John_Draper
https://www.mitnicksecurity.com/about/kevin-mitnick-worlds-most-famous-hacker-biography

1.1 Infosec Culture

- *The Conscience of a Hacker*, also known as *The Hacker's Manifesto* written by *The Mentor*, is a document that gives an idea about the ideals of the underground hacking community.

- Being an information security professional means pursuing knowledge, being honest with yourself and never stop challenging yourself and your colleagues.

http://phrack.org/issues/7/3.html

1.2 Career Opportunities

- Nowadays, companies of all sizes, as well as government bodies are using advanced technologies to store and process a great deal of confidential data on computers and mobile devices.

- Data is not only stored but also transmitted across private and public networks to other computers. Therefore, it is a **must** to protect sensitive information. Companies pay a premium to safeguard their data and ensure that their systems are protected. Or, at least they should.

1.2 Career Opportunities

- An even more important sector is national security. Recently, governments have to face a broad range of cyber-threats: global cyber syndicates, hackers for hire, hacktivists, terrorists and state-sponsored hackers.

- With critical infrastructure like power plants, trains or dams being controlled by computers, using hacking skills for good has become critical for the safety of nations.

1.2 Career Opportunities

- Companies and governments need to implement hardware and software defensive systems to protect their digital assets.

- Additionally, they also need to train their entire organization to make sure:
  - Secure applications are developed,
  - Proper defensive measures are taken, and
  - That proper use of the company's data is in place.

- IT Security is a very difficult game! A way to ensure that a system is secure from cyber-attacks is by **hiring a penetration tester**.

1.2 Career Opportunities

- **Penetration testers** (also called pentesters) are professionals who are hired to simulate a hacking attack against a network, a computer system, a web application or the entire organization.

- They master the same tools and techniques that malicious hackers use to discover any (and all) vulnerability in the systems they test.

1.2 Career Opportunities

+ These highly skilled professionals often work:

  - As freelancers
  - In an IT Security services company
  - As in-house employees

1.2 Career Opportunities

+ Moreover, as IT is a broad knowledge domain, they can specialize in specific infosec sectors such as:
  - Systems attacks
  - Web applications
  - Malware analysis
  - Reverse engineering
  - Mobile applications
  - Other

1.2 Career Opportunities

- The demand for penetration testers is on a steady growth.
- Being passionate, skilled and hungry for knowledge are fundamental characteristics for a successful pentesting career.
- By starting this course, you have made a big step in the right direction! We'll now introduce some of the jargon used by information security professionals.

1.3 Information Security Terms

- Speaking the **domain language** is **fundamental** in any field. It helps you to better understand the industry and better communicate with your colleagues.

- We will now review a list of important terms to know. Keep this chapter as a reference while studying.

1.3.1 White Hat Hacker

- A **white hat hacker** is a professional penetration tester or ethical hacker who performs authorized attacks against a system helping the client solve their security issues.

- White hat hackers do not perform illegal actions.

1.3.2 Black Hat Hacker

- A **black hat hacker** is a hacker who performs unauthorized attacks against a system with the purpose of causing damage or gaining profit.

- There is also a category of black hat hackers called **crackers**.

1.3.3 Users and Malicious Users

- A **user** is a computer system user. It can be an employee of your client or an external user.
- A **malicious user** is a user who misuses or attacks computer systems and applications.

1.3.4 Root or Administrator

- The **root** or **administrator** users are the users who manage IT networks or single systems.
- They have the maximum privileges over a system.

1.3.5 Privileges

- In a computer system, **privileges** identify the action that a user is allowed to do.
- The higher the privileges, the more the control over a system a user has.

1.3.6 Security Through Obscurity

- **Security through obscurity** is the use of secrecy of design, implementation or configuration in order to provide security.

- In this course, you will learn that security through obscurity cannot stop a skilled and motivated attacker.

1.3.7 Attack

+ An **attack** is any kind of action aimed at misusing or taking control over a computer system or application.

+ Some examples of attacks are:
  - Getting unauthorized access to an administration area
  - Stealing a user's password
  - Causing denial of service
  - Eavesdropping on communications

1.3.8 Privilege Escalation

- **Privilege escalation** is an attack where a malicious user gains elevated privileges over a system.

1.3.9 Denial of Service

- With a **denial of service (DoS)** attack, a malicious user makes a system or a service unavailable.
- The attack could be carried out by making the service crash or by saturating the service resources, thus making it unresponsive for legitimate users.

1.3.10 Remote Code Execution

+ During a **remote code execution** attack, a malicious user manages to execute some attacker-controlled code on a victim remote machine.

+ Remote code execution vulnerabilities are very dangerous because they can be exploited over the network by a remote attacker.

1.3.11 Shell Code

- A **shellcode** is a piece of custom code which provides the attacker a shell on the victim machine.
- Shellcodes are generally used during remote code execution attacks.

1.3.11 Shell Code

+ Now that you know a little more about the information security field, it is time to start learning some technical skills!

References

- Captain Crunch: https://en.wikipedia.org/wiki/John_Draper
- Biography of Kevin Mitnick: https://www.mitnicksecurity.com/about/kevin-mitnick-worlds-most-famous-hacker-biography
- The Conscience of a Hacker: http://phrack.org/issues/7/3.html