Penetration Testing Student

The INE Penetration Testing Student Guide To Prepare EJPT Certification.

Made by @beyrouthterminus for educational purpose.

1. Prerequisites

[1.1] The Information Security Field

1.1.1 Infosec Culture

• **Information security** has deep roots in the **underground hacking scene**. The term hacker was born in the sixties in the MIT community.

• 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 perfrom an attack also means being able to **deeply understand the technology and the functioning** of the target system.

• Hackers **explore and improve their skills daily**.

• *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 underground hacking community.

1.1.2 Career Opportunities

• Nowadays, companies and governement 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.

• Governements have to face a broad range of cyber-threats, 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**.

• Companies and governments need to implement **hardware and software defensive systems** to protect their digital assets. They also need to train their enitre organization to make sure **secure applications are developed, proper defensives 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 system is secure from cyber-attacks is **by hiring a penetration tester.**

• Penetration testers are professionals who are hired to simulate a hacking attack against a network, a computer system, a web application or the entire organization. T**hey master the same tools and techniques that malicious hackers** use to discover any vulnerability.

• Moreover, as IT is a broad knowledge domain, they can specialize in specific infosec sectors such as:
- ☑ *System attacks*
- ☑ *Web applications*
- ☑ *Malware Analysis*
- ☑ *Reverse engineering*
- ☑ *Mobile applications*
- ☑ *Other*

• **Being passionate, skilled and hungry for knowledge** are fundamental characteristics **for a succesfull pentesting career.**
•

1.1.3 Information Security Terms

• ***White hat hacker:*** A professional penetration tester or ethical hacker who performs authorized attacks against a system.

• ***Black hat hacker:*** Who performs unauthorized attacks against a system with the purpose of causing damage or gaining profit.

• ***User:*** Computer system user, can be an employee of your client or external user.

• ***Malicious User:*** User who misuses or attacks computer systems and applications.

• ***Root:*** The root or administrator users are the users who manage IT networks or single systems with maximum privileges.

• ***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.

• ***Security Through Obscurity:*** The use of secrecy of design, implementation or configuration to provide security.

• ***Attack:*** Any kind of action aimed at misusing or taking control over a computer system or application.

• ***Privilege Escalation:*** Attack where a malicious user gains elevated privileges over a system.

• ***Denial Of Service:*** Attack where a malicious user makes a system or a service unavailable by crashing it or saturating services ressources.

• ***Remote Code Execution:*** Attack where a malicious user manages to execute some attacker-controller code on a victim remote machine.

• ***Shell code:*** Piece of custom code wich provides the attacker a shell on the victim machine.

[1.2] Cryptography & VPNs

1.2.1 Clear-text Protocols

• **Clear-text protocols** transmit data over the network without any kind of transformation (encryption). This lets an attacker **eavesdrop** on the communication, as well as perform other malicious actions.

• Because of their nature, clear-text protocols **are easy to intercept, eavesdrop and mangle.** They should not be used to transmit critical or private information.

• If there is **absolutely no alternative** to a clear-text protocol, you should use it **only on trusted networks.**

1.2.1 Cryptographic Protocols

• On the other hand, cryptographic protocols transform (encrypt) the information transmitted to protect the communication.

• One of the goal of these protocols is to **prevent eavesdropping.** If an attacker intercepts the traffic, they will not be able to understand it.

• If you need to transmit private information, you should **always use a cryptographic protocol** to protect the communication over the network.

• If you need to run a clear-text protocol on an untrusted network, **you can wrap (tunnel)** a clear-text protocol into a cryptographic one. A great example of protocol tunneling is a **VPN**.

2. Preliminary Skills & Programming

3. Basics

4. References

4.1 Useful references*:*

-INE
-eJPT
-Cherrytree