I WANT TO BE A PENTESTER, NOW WHAT?

by Ivan Puccinelli*

*Pentester at Open-Sec. He has cybersecurity certifications such as eJPT and eWPT. He also has experience in web application development and penetration testing in the field of infrastructure (internal/external), web applications and PCI DSS segmentation. (https://www.linkedin.com/in/ivan-puccinelli-mendiola-36ab16274)

Although pentesting is a complex task that requires a group of abilities and specific technology knowledge, there are certain essential qualities and abilities that every good pentester should have. If you find yourself reading this article, it is because you are interested in knowing these fundamental skills that you should have in your new career.

Being a pentester is not easy, you need to have technical abilities, knowledge and skills that can be acquired through formal education or practical experience. In this article, I'll show you 7 abilities that every "wannabe" pentester must possess.

1. Programming Knowledge

A big part of the pentesters must have a strong knowledge in programming. It is very important to have a high comprehension of programming languages such as Python, C++, Ruby y Perl, and more. You have to be able to understand the root code, identify vulnerabilities, automate tests, work out exploits, among other applications.

2. Network Knowledge

Networks are the base of everything related to information security. It 's necessary to know how they work, how they communicate with the devices and how information is delivered. It is also important to understand the network topology, the communication protocols, the network structure and the physical security.

3. Operating Systems Knowledge

A pentester must have a good comprehension of the operating systems such as Linux, Windows and macOS. They got to know the system commands, the security configurations, the file management and the process handling.

4. Ability to Identify Vulnerabilities

A pentester must be able to identify vulnerabilities in systems and networks. This involves having scoped thinking and being able to think out of the box. Also, a pentester must be able to identify the security gaps and evaluate the risk associated with them.

5. Security Tools Knowledge

Existen muchas herramientas de seguridad que los pentester utilizan para identificar vulnerabilidades y proteger sistemas y redes. Se debe tener un conocimiento profundo de estas herramientas y saber cómo utilizarlas de manera efectiva. Algunas de las herramientas comunes son Nmap, Wireshark, Metasploit, John the Ripper, Aircrack-ng, entre otras, y cada una de ella tiene un propósito específico.

6. Documentation Ability

Documentation is very important. We must be able to document what we find, the tests done and the identified vulnerabilities. In addition, we should be able to create clear and detailed reports that explain the scope of the problem, the severity and the possible solutions, always keeping in mind to which kind of professional this report is being aimed.

7. Work Team Ability

Information security is a collaborative effort. A pentester must be able to work in a team and communicate efficiently with the other members of the crew. Apart from it, a pentester must be able to work also with other TI professionals, such as system managers and software developers.

One pentesters must have a thorough knowledge on programming, networks, operating systems, security tools and critical thinking skills. Additionally, as a pentester, you must be able to keep record of the discoverments, work with a team and communicate in an effective way. If you are interested in becoming into a pentester, Si estás interesado en convertirte en un pentester, make sure to acquire these essential skills and never stop learning.