RE: the InfoSec Africa event

Scope:

- ***Penetration testing*** aims to evaluate the security of a particular target, such as a system, network, or application. It entails actively looking for security flaws and exploiting them to gain unauthorised access, simulate attacks, and assess how well security measures are working.
- **Ethical hacking**: The term "ethical hacking" refers to a variety of security-related tasks that have a wider range of applications. Penetration testing is just one aspect of it; other aspects include vulnerability analyses, security audits, risk analysis, and incident response.

Authorization:

- **Penetration Testing**: Penetration testing is typically carried out with the owner of the target system or organisation's proper authorization and consent. A prior agreement is made regarding the limitations, rules of engagement, and testing scope.
- **Ethical hackin**g: In a broad sense, ethical hacking refers to the responsible use of hacking tools and techniques to find security flaws. Beyond penetration testing, it may involve things like research, knowledge sharing, and community involvement.

Methodology:

- Planning, reconnaissance, scanning, exploitation, and post-exploitation phases are all included in the structured methodology of **penetration testing**. It aims to pinpoint weaknesses, weigh the consequences, and offer remediation advice.
- **Ethical hacking:** A broader range of techniques and activities are included in ethical hacking. It may involve a number of strategies, including cryptography analysis, wireless network testing, web application security assessment, and social engineering, among others.

Objective:

- **Penetration Testing**: The primary objective of penetration testing is to identify vulnerabilities and assess the security posture of the target system or organization. The focus is on identifying weaknesses that could be exploited by attackers and providing recommendations for improving security.

- **Ethical Hacking**: Ethical hacking encompasses a broader objective of improving overall security. It aims to proactively identify vulnerabilities, develop secure systems and practices, and raise awareness about potential security risks.

Reporting:

- **Penetration Testing**: Penetration testing includes detailed reporting of identified vulnerabilities, their impact, and recommendations for remediation. The report provides a comprehensive assessment of the security posture and helps organisations prioritise and address the identified issues.
- **Ethical Hacking**: Ethical hacking may involve reporting vulnerabilities and providing recommendations, but it can also involve other activities such as research, knowledge sharing, and collaborating with the security community.

RESOURCES:

- Open Source tools
- More Tools:
- Job Description Template
- Blueprint