HOW MUCH DO YOU KNOW ABOUT

PEN TESTING

Penetration testing or ethical hacking is testing an organization's systems for exploitable vulnerabilities and weaknesses. Such testing is crucial to understanding whether the organization's information systems are hardened or not.

PENETRATION TEST

Crucial component to network security because it helps us identify:

- Security vulnerabilities before a hacker does
- Gaps in information security compliance
- Actionable remediation guidance

The pen testing process can be broken down to these stages.

#1

PLANNING AND RECONNAISSANCE: Defining the scope and goals of a test, including the systems to be addressed and the testing methods to be used. Plus, gathering intelligence to better understand how a target works and its potential vulnerabilities.

#2

SCANNING: Understand how the target application will respond to various intrusion attempts. This is typically done using Static and Dynamic analysis,

#3

GAINING ACCESS: To use Web application attacks, such as cross-site scripting, SQL injection and backdoors, to uncover a target's vulnerabilities. Testers then try and exploit these vulnerabilities to understand the damage they can cause.

#4

MAINTAINING ACCESS: See if the vulnerability can be used to achieve a persistent presence in the exploited system - long enough for a bad actor to gain in - depth access. The idea is to imitate advanced persistent threats.

#5

ANALYSIS: The results of the penetration test are then compiled into a detailed report. This information is analyzed by security personnel to help configure an enterprise's system and protect against future attacks.

WECODE