

PENETRATION TESTING

A penetration test, or pen test, is an attempt to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities. These vulnerabilities may exist in operating systems, service and application flaws, improper configurations, or risky end-user behavior. Such assessments are also useful in validating the efficacy of defensive mechanisms, as well as, end-user adherence to security policies.

- **Setting up your virtual lab**
- **Using kali Linux**
- **Programming**
- **Using the metasploit framework**
- **Assessments**
- **Information gathering**
- **Finding vulnerabilities traffic**
- **Exploitation**
- **Password attacks**
- **Client-side exploitation social engineering**
- **Bypassing antivirus application**
- **Post exploitation**
- **Web application testing**
- **Wireless attacks**
- **Exploit development**
- **A stack-based buffer overflow in Linux**
- **A stack-based buffer overflow in windows**
- **Structured exception handler overwrites**
- **Fuzzing, porting exploits, and metasploit modules**
- **Using the smart phone pentest framework**

