Course: Certificate Course in Vulnerability Assessment & Penetration Testing in Information Security

Duration: 60 Hrs (2hrs/day)/6 weeks

Fee: Rs 3,000

Abstract

Vulnerability assessment & Penetration Testing (VAPT) is the method through which we assess the security of the organization before it is going to be exploited by the hackers. The main goal behind VAPT is to find vulnerabilities in the system in a controlled manner by using various tools and techniques. By doing this course Students shall be aware of the various ways through which hackers' attempts to compromise an Application, Service, Desktop or a server. Also we see its countermeasures. This course is going to help students to understand the basic of vulnerability assessment & penetration testing and various tools and techniques used in VAPT through Linux.

Prerequisite

Understanding the basics of networking, OSI reference model, TCP/IP and IP addressing scheme.

Outcome of the course

The students shall have hand on experience on various tools & techniques of vulnerability assessment & penetration testing used in Linux and shall pursue a career in penetration testing domain.

Syllabus

1. **Information security Basics.** (10 hrs)
   - Elements of information security
   - Security challenges
   - Hacking concepts
   - Phases of hacking
   - Vulnerability research

2. **Introduction to penetration testing.** (10 hrs)
   - Penetration testing concepts i.e. what why & how we do pen test?
   - Penetration testing methodology
   - Types of penetration testing
   - Tools and techniques used in penetration testing
   - Limitations of penetration testing tools

3. **Introduction to Linux.** (10 hrs)
   - Features of Linux why we use it?
   - Installation of Linux on VM(virtual machine)
   - Linux file system
   - Basic Linux commands
   - Editing files on command line using vi & nano editor
   - Searching text in file(cut,awk.grep)etc
   - Search update and delete tools using apt
   - Comparing files.

4. **Hand on practise on tools used in penetration testing.** (30 hrs)
   - scanning and its types(network, port and vulnerability scanning)
   - Nmap and live scanning on ports and networks
   - Netcat usage on TCP/UDP ports
   - Wireshark basics and capturing data
   - NFS ,SMB ,SMTP enumeration
   - Vulnerability scanning overview
   - Different types of vulnerability scanning
   - Nessus installation and configuration
   - Vulnerability scanning with Nessus
   - Web application assessment with nikto & burp suite
   - Vulnerability analysis with Metasploit framework