iGNITE Technologies

POWERED BY IGNITE TECHNOLOGIES

INFRASTRUCTURE PENETRATION TESTING

TRAINING & PROGRAM

Enroll Now

www.ignitetechnologies.in

+91 959 938 7841

iGNITE Technologies

INFRASTRUCTURE PENETRATION TESTING

Infrastructure penetration testing involves detecting and investigating the vulnerabilities and flaws present in the computer systems and the devices that are connected to the network, cloud etc. in an effort to ensure maximum security. In layman terms, it is the process of unearthing the loopholes in an organization's security framework.

Furthermore, if an organization wants to ensure that they are compliant with the information security policies and analyze their level of response to any cyber-based risks, they can make use of this methodology.
It is usually performed in collaboration with other methodologies like External, Internal, Wireless, Cloud and Virtualization Penetration Testing.

PREREQUISITES

This course has been designed for professionals and therefore anyone who wishes to take up this course should have their fundamentals and concepts regarding network; the components involved in designing an organization's network server or its infrastructure. Additionally, you should be aware of the Linux and Windows basic commands & Kali Linux Framework & its well-known tools.

COURSE DURATION: 35 to 40 HOURS

www.ignitetechnologies.in
+91 959 938 7841

Why to choose Ignite Technologies?

Ignite believes in “Simple Training makes Deep Learning” which help us in Leading International CTF market.

• Ignite Technologies is leading Institute which provides Cyber Security training from Beginner to Advance as mention below:

1. Networking
2. Ethical hacking
3. Bug Bounty
4. Burp Suite for Pentester
5. Windows for Pentester
6. Linux for Pentester
7. Computer Forensic
8. CTF-2.0
9. Privilege Escalation
10. Red Team Operations
11. Infrastructure Penetration Testing
12. API Penetration Testing
13. Android Penetration Testing

• World RANK -1st, in Publishing more than 400 walkthroughs (Solution) of CTFs of the various platform on our reputed website “www.hackingarticles.in”.

• We Provide Professional training that includes real-world challenges.

• Ignite’s Students are placed in a TOP reputed company in the overworld.

• Hands-on Practice with 80% Practical and 20% Professional Documentation.

• ONLINE classes are available

Career in IT Security Domain:

Chief Information Security Officer
Senior Security Consultant
Cryptographer
Penetration Tester
Researcher
Incident Analyst | Responder
Software code Analyst
Risk Controller
Security Architect
Exploit Developer
Information Security Analyst
Digital Forensic Expert
International Trainer
Security Engineer
Ethical Hacker

COURSE OVERVIEW

PRE-ENGAGEMENT INTERACTIONS

- Introduction to Scope
- Metrics for Time Estimation
- Questionnaires
- Specify Start and End Dates
- Specify IP Ranges and Domains
- Dealing with Third Parties
- Payment Terms
- Report delivery

INTERNAL & EXTERNAL PENETRATION SCANNING

- Information Gathering
- Map the internal network
- Advance port Scanning
- Server OS Testing
- Service Fingerprinting
- RDP MITM Attack
- Attempt to Establish null Sessions
- Hands-on Ideal Vulnerability Assessment Tools

APPLICATION SERVER MAPPING

- OWASP Standard and Top 10 Vulnerability
- Manual Vulnerability Assessment
- Application Fingerprinting
- Web Directory Brute Force
- Code Injection
- Automated Testing
- Vulnerability Scanning
- Fuzzing
- Hash Cracking
- Tomcat Penetration Testing
- SSL/TLS Security Testing
- Challenge 1: CMS Penetration Testing
- Challenge 2: Web Server Hacking

DATABASE PENETRATION TESTING

- MySQL Exploitation
- PostgreSQL Exploitation
- Couch DB Exploitation
- MS-SQL Exploitation

iGNITE Technologies

LINUX FOR PENTESTER

- Reverse Shell
- File transfer Technique
- Abusing Network Shares
- Bypass Restricted Shell
- Abusing sudo rights
- Misconfigured SUID Permissions
- Pivoting

WINDOWS FOR PENTESTER

- OS Fingerprinting
- Bypasses Whitelisting Programs
- Privilege Escalation
- Active Directory Exploitation
- Lateral Movement
- Domain Persistence Attack

DOCKER FOR PENTESTER

- Fundamental of Docker
- Assemble Your Penetration Testing Laboratory
- Exploiting Docker Containers
- Container Vulnerability Assessment
- Poisonous Docker Image

NETWORK DEVICE SECURITY AUDIT

- Router
- Switches
- Firewall
- Data leak Prevention

VOIP PENETRATION TESTING

- SIP Protocol Enumeration
- Extension Brute force
- Extension Registration
- Call Spoofing
- Sniffing Calls

BONUS SECTION

- Android Application Penetration
- CI|CD penetration Testing
- Introduction to Threat Hunting
- Introduction to Incident Response