



NANO SCIENTIFIC RESEARCH CENTRE PVT.LTD

AN ISO 9001:2008 CERTIFIED COMPANY



ETHICAL HACKING SYLLABUS



ETHICAL HACKING

1. Introduction to Ethical Hacking

- Overview of Ethical Hacking
- Hackers Vs Ethical Hackers
- Different Types of Hackers
- World Top Hacker's History
- Terminologies Used in Hacking
- Skills Required to Become a Hacker
- OWASP Top 10 Application Security Risks

2. Essentials for Ethical Hacking

- Basics of Programming Languages
- Basics of Networking
- Linux and Windows Commands
- Tools and Installations of Kali Linux

3. Foot printing, Information Gathering, Reconnaissance

- What is Information Gathering
- Active & Passive Information Gathering
- Google as an Information Gathering Agent
- Addons and Tool Based Foot Printing
- Site for Foot Printing

4. System Virtualization & Cloning

- Virtualization
- VmWare
- VirtualBox
- Backup & Restore
- Cloning



5. Scanning Networks

- Overview of TCP/IP 3-way Handshake
- Nmap Scanning Methods
- Nmap Script Engine
- Online Scanning
- Some Useful Scanners
- Introduction to Enumeration
- SNMP Enumeration
- Banner Grabbing

6. Hiding Identify (Proxy & VPN)

- Over view of proxy
- Online Proxy
- Proxy Tools
- VPNs & Bypass Restrictions
- Using Proxy and VPNs

7. Vulnerability Analysis

- Introduction to Vulnerability
 CVEs
 NVDs
- Introduction to VA-PT
 Nessus
 Acunetix
 Netsparker
 IBM AppScan



8. System Hacking

- Using Protocols

- SSH

- FTP

- Telnet

- HTTP/HTTPS

- VNC

- SMB

9. Network Attacks & Security

- DOS & DDOS Attack
- Buffer overflow (Brief Intro)
- Packet Sniffing
- IDS and Honeypot

10. Website Hacking

- Bypass Authentication
- Session Hijacking
 - Using URL
 - Using QR Code
- SQL Injection
- Dumping Passwords

11. Social Engineering

- Email Hacking
- Phishing Attacks
 - Social Media



12. System and Application Password Hacking

- Password Cracking
- Password Resetting
- Login Without Entering Password
- Linux password Resetting
- Password in Plain Text
- Securing System
- Rar,Pdf, Ms-Office & Zip password Cracking

13. Steganography & Cryptography

- Introduction to Stenography & Cryptography
- Data Hiding behind Images, Videos Files Etc...
- Data Hiding Tools
- ADS
- Cryptography

14. Penetration Testing

- Pen Testing Methodology
- Approaches
- Vulnerability Assessments Vs. Penetration Testing
- Internal Penetration Assessments
- Layered Security Approach
- Common Attacker Methods
- Password Security
- Network Architecture
- Physical Security & Security Awareness
- Isolation/Mitigation of known vulnerabilities



15. Viruses, Trojans, Worms and Malwares

- Introduction to viruses, worms, and Trojans
- Hacking by using some Viruses, Trojans and Worms
- Botnets
- Key Logging
- Overview of Malware Analysis
- Countermeasures

16. Wireless Password Cracking

- WEP Cracking
- WPA/WPA2 Password Cracking
- WI-FI Router Password Cracking

17. Introduction to Mobile Hacking

- Android Architecture
- Android Development
- Reverse Engineering & Tools
- Mobile Pen Testing



NANO SCIENTIFIC RESEARCH CENTRE PVT LTD

OUR RECRUTERS



XILINX

AMD



ALSTOM
Shaping the future



ademtech

PALADION
HIGH SPEED CYBER DEFENSE

mindlance moschip

ELVEEGO
CIRCUITS

Infosys

Address:

NANO SCIENTIFIC RESEARCH CENTRE PVT LTD
(AN ISO 9001:2008 CERTIFIED)

#601 & 604, Siri Estates, Opp to Karur Vysya Bank,
Opp Lane to R.S.Brothers, Ameerpet, Hyderabad.

www.nanocdac.com

+91 96406 48777- Aravind Reddy.K
+91 82975 78555- Mallikarjun.V