AEGIS ETHICAL HACKING

An ethical hacker is a computer and networking expert who systematically attempts to penetrate a computer system or network on behalf of its owners for the purpose of finding security vulnerabilities that a malicious hacker could potentially exploit. The purpose of ethical hacking is to evaluate the security of a network or system's infrastructure. It entails finding and attempting to exploit any vulnerabilities to determine whether unauthorized access or other malicious activities are possible. Vulnerabilities tend to be found in poor or improper system configuration, known and unknown hardware or software flaws, and operational weaknesses in process or technical countermeasures.

Course Contain :-

- **Computer Security Basics**
- **Most Common Attacks**
- **ASCII Code**
- **Networking Basics and Security**
- **IANA, Allotment of IP Address**
- **Ping and Ping Sweep**
- **Foot-Printing Techniques**
- **Detecting Victim, OS**
- **Detecting Firewall**
- **Domain Name and DNS**
- **ICANN**
- **Top Level Domains**
- **DNS Delegation**
- **Hacking Mailing Clients**
- **Instant Messengers Hacking (gtalk, yahoo, etc)**
- **Port Scanning**
- **Detecting Open Ports**
- **Intellectual Property Theft**
- **Trojan attack and countermeasure**
- **Hacking by Key loggers**

- **Steganography and Steganalysis**
- **Identity Attacks**
- **Proxy Server Attacks**
- **Password Cracking**
- **Sniffer and Wireless Hacking**
- **Call Spoofing**
- **Google Hacking**
- **Email Security**
- **Buffer Overflow**
- **DOS and DDOS Attacks**
- **Honeypots**
- **0-day Attacks**
- **XSS Attacks**
- **Windows and System Hacking**
- **Social Engineering Attacks**
- **Defacing Website and Security Standards**
- **Web Jacking**
- **SQL Injection**
- **Finding Loopholes**
- **Phishing Techniques**
- **Cyber Law and Consulting**
- **Cyber Forensics and Investigations**
- **IT Act, 2000**
- **CERT-IND and AO**
- **Case Studies**
- **Earning Money Online**
- **Adsense and Adwords**
- **IP and malware**
- **IP Analysis**

- **Types of Malwares**
- **Foot-Printing Techniques**
- **Information Gathering**
- **ICANN Guidelines**
- **Hosting Servers**
- **Registrant and Hosting Panels**
- **Static and Dynamic Websites**
- **Pre-Penetration Steps**
- **Information Scanning**
- **Hacking using Google**
- **Finding Control Panel of Websites**
- **Attacking Systems**
- **Windows Hacking**
- **Phishing**
- **Session Hijacking**
- **Password Cracking, Penetration Testing**
- **Web Foot-Printing**
- **DNS Hijacking**
- **Sub-Domains Scanner**
- **Information about target on Web App**
- **Webserver Hacking**
- **Metasploit**
- **Privilege Escalation Attack**
- **Rooting**
- **Shell coding**
- **Encryption / Decryption**
- **Web Application Penetration Testing**
- **Social Engineering Penetration Testing**
- **WEP and WPA Attacks**
- **XSS Attacks**

- Persistent and Non-Persistent Attacks
- CRPF
- Securing XSS Attacks
- SQL Penetration Testing
- Blind SQLi
- Attacks on SQL Server
- Securing SQLi
- Database Penetration Testing
- Different types of CMS identifications
- Attacks on CMS
- Joomla Exploits
- Wordpress Exploits
- Vbulletin Exploits
- Wireless Penetration Testing
- WEP and WPA Attacks
- Security Measures
- LAN Penetration Testing
- Client Side Exploits
- MITM Attacks
- Sniffing Attacks (http, https)
- Trojans, Virus and Backdoors Detection
- Vulnerability Assessments
- Assessment tools (acunetix, dywa)
- Testing Reports and Post Testing Actions
- Cyber Law and Acts

AEGIS I-NET PVT. LTD.
TRAINING SERVICES CONSULTANT