# AEGIS I-NET

## ACEH Course Content

- 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.
- Shellcoding
- 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
- Standards and Compliance
- Cyber Law and Acts
- CERT-IND and AO
- Cyber Forensics and Investigations.