ARMOURINFOSEC

577, Gold Plaza, Punjab Jewelers, M.G. Road,
Opp. Treasure Island Mall,
Indore, Madhya Pradesh 452001, INDIA

+91-99777-47-168

info@armourinfosec.com

WE ARE A LEARNING PLATFORM

About Us

Armour Infosec is a piece of knowledge and technical security solutions providing Company. We are a part of the Genext Group. We are delivering technology services and training to students and professionals. We are specialized in IT Security, Ethical Hacking, Cyber Security, Network Security, Website Security, Wireless Security, Web Designing And Development, Search Engine Optimization, Android Application Development, Network Support And Annual Maintenance Contract, Hardware & Networking and more. We give students the best of our knowledge which helps them for their bright future.

Ethical hackers use their knowledge to secure and improve the technology of organizations. They provide an essential service to these organizations by looking for vulnerabilities that can lead to a security breach.

An ethical hacker reports the identified vulnerabilities to the organization. Additionally, they provide remediation advice. In many cases, with the organization's consent, the ethical hacker performs a re-test to ensure the vulnerabilities are fully resolved.

We believe in quality, client and student's satisfaction more than anything else. Education is very necessary for all and we are providing it in a manner that our trainees get the best in the industry.

ARMOURINFOSEC

WHY CHOOSE US

- Our Quality Training and Professional Services.
- Necessary Theory and Maximum Practical.
- We teach Manual Methods Instead of Automate tools.
- Evening, Morning and Weekend batches available.
- Network administration and Development in Core.
- Amazing Ambience with skillful Trainees.
- We Provide Study Material with Necessary Tools and Practical Sessions.
- We held Workshops and Seminars on the Current topics of system Hacks.

Penetration Testing

Source Code Review

Forensic Science

Secure Server Development
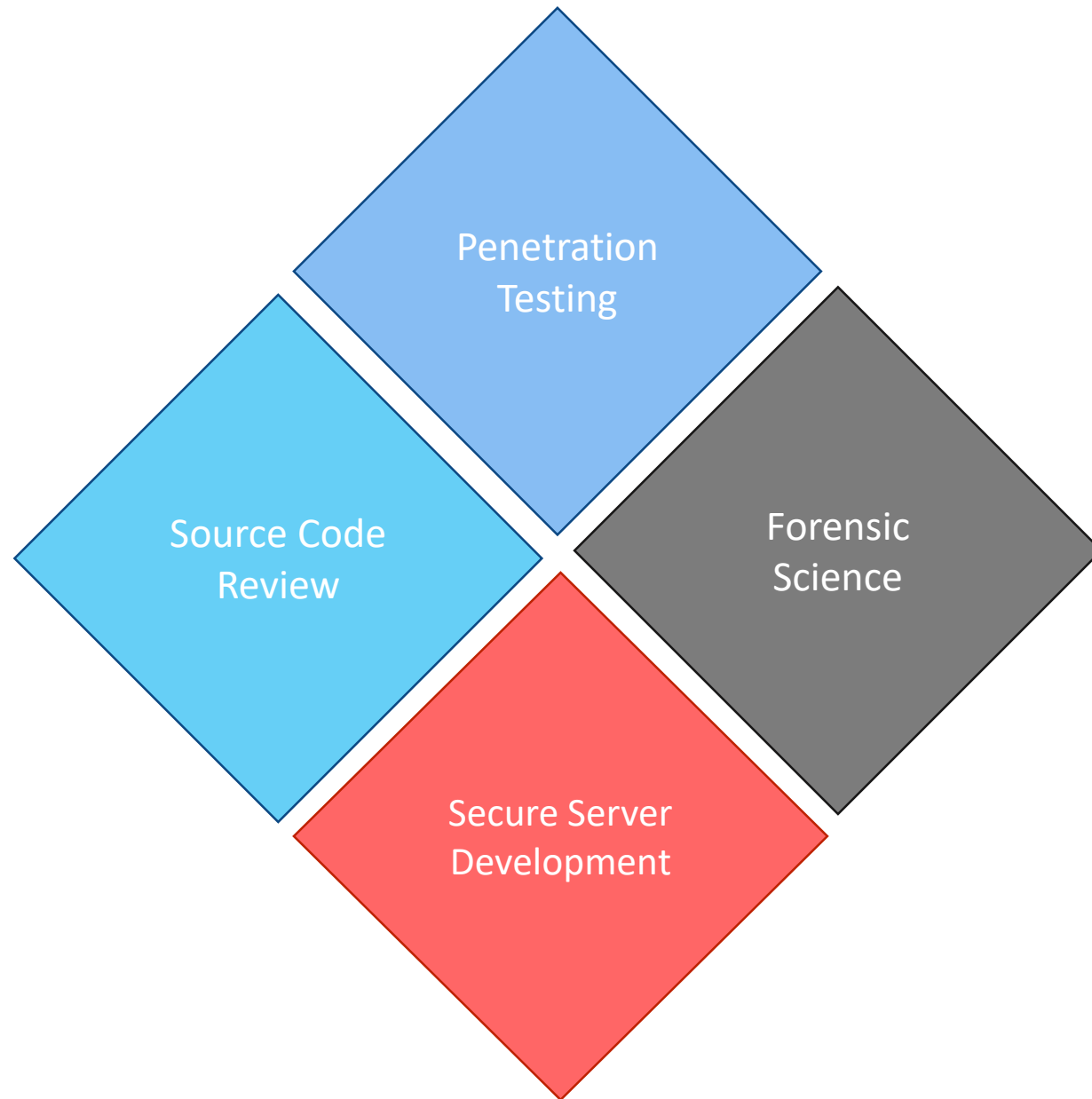
ARMOURINFOSEC

OUR COURSES
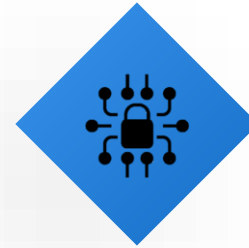
Certified Information Security Expert

Armour Infosec Certified Ethical Hacking Penetration Testing Expert

Armour Infosec Certified Computer Hacking & Forensic Expert

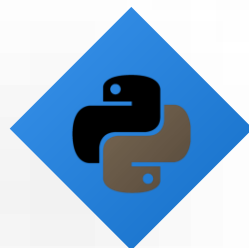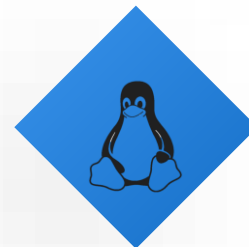Certified Network Security Expert

Certified Web Security Expert

Certified Wireless Security Expert

Python for Hackers

Certified Linux Server Administrator

Certified Windows Server Administrator

ARMOURINFOSEC

Certified Network Security Expert

A Certified Network Security Expert / Penetration Tester is a network security consuitant that tries to break a network and find possible exploits in different computer systems and softwares. In short you can say them ethical hacker. They generally are expected to run a number of tests and fill out assessment reports about what they have discovered during penetration. In this course students will learn Penetration Testing, Linux Fundamentals, Information Gathering, Detecting Live System, Enumeration, Vulnerability Assessments, Malware Goes Undercover, Windows Hacking, Hacking UNIX/Linux, Advanced Exploitation Techniques, Networks, Sniffing, IDS.

DURATION

2 hours/ day X 75 days

ENROLL NOW

ARMOURINFOSEC

Certified Information Security Expert

What are the Objectives of the course?

- Implement technical strategies, tools, and techniques to secure data and information for your organization.
- Adhere to ethical security behavior for risk analysis and mitigation
- Understand security in cloud computing architecture in depth
- Comprehend legal requirements, privacy issues and audit process methodologies within the cloud environment
- Focus on IT compliance and the integrity of enterprise systems to establish a more secure enterprise IT framework

What are the Required Skillsets?

- Information security analysts must have strong analytical skills. They have to be able to study computer systems, assess any potential risks, and consider possible solutions.
- Creativity is critical for information security analysts. They must be able to anticipate cyber-attacks, always thinking one step ahead of a cyber threat. This kind of forward-thinking takes creativity.
- Threats to cybersecurity are always changing, as are solutions. Information security analysts have to constantly update their knowledge on the latest data-protection news, cyber-security legislation, and practices and techniques.

What are the career benefits of this training?

- Cybersecurity is vital for career roles such as penetration tester, cybersecurity analyst, network analyst, cybersecurity auditor, cybersecurity architect, forensics investigator, and many more.

- There are 2000+ cybersecurity jobs in India and 40,000+ in the US (Indeed.com). Cybersecurity job roles are expected to rise to six million worldwide by 2019.

- Expertise your skills in the management side of information security, including topics like governance, program development, and program, incident, and risk management.

Units Covered

Windows Server

Red Hat Linux Server

WordPress

Secure Development in PHP

Python for Hackers

Ethical Hacking & Penetration Testing

ARMOURINFOSEC

Ethical Hacking & Penetration Testing

You will learn how to patch these networks as well as web applications with input validation using regular expressions. You will learn a security design pattern to avoid introducing injection vulnerabilities by input validation and replacing generic system calls with specific function calls. You will learn how to hack web apps with SQL injection vulnerabilities and retrieve user profile information and passwords. You will learn how to patch them with input validation and SQL parameter binding. Understand the better view of network application pentesting, Web Application Pentesting followed by reverse engineering and buffer-overflow. You will learn the hacking methodology, Nessus tool for scanning vulnerabilities, Kali Linux for penetration testing, and Metasploit Framework for gaining access to vulnerable Windows Systems, deploying keylogger, and performing Remote VNC server injection. You will learn security in memory systems and virtual memory layout, and understand buffer overflow attacks and their defenses.

MODULE 01: KALI LINUX FUNDAMENTALS

- Kali Linux history and introduction
- Kali Linux GUI desktops
- Kali Linux Commands
- Tar and zips
- Compiling programs
- Identifying software packages
- Installing and removing software

- User account management
- Changing a user account password
- Passwd & Shadow file formats
- File permissions
- Directory permissions
- Octal representation
- Changing permissions

- Setting default permissions
- Internet addressing
- Network services
- Commonly available services
- Fundamental network configuration files
- Network control scripts

MODULE 02: INTRODUCTION TO PENETRATION TESTING & ETHICAL HACKING

Hacking Concepts
- Introduction to Hacking
- Hacking vs. Ethical Hacking
- Effects of Hacking on Business
- Who is a Hacker?
- Hacker Classes
- Hacktivism
- Hacking Phases
- Defense in Depth

Vulnerability Assessment & Penetration Testing
- Vulnerabilities
- Vulnerability Research
- Vulnerability Research Websites
- What is Penetration Testing?
- Why Penetration Testing
- Penetration Testing Methodology
- Security Policies
- Types of Security Policies

- Steps to Create and Implement Security Policies

Disaster Recovery & Risk Management
- Defining Risk Management
- Strategies for Managing Risk
- How to Analyze Risk
- Disaster Recovery Strategies
- Plan Testing and Execution

ARMOURINFOSEC

Ethical Hacking & Penetration Testing

MODULE 03: FOOTPRINTING AND RECONNAISSANCE

Footprinting Concepts and Methodology
- Footprinting Terminology
- What is Footprinting?
- Why Footprinting?
- Objectives of Footprinting
- Footprinting Threats

Footprinting using Search Engines
- Finding Company's External and Internal URLs
- Public and Restricted Websites
- Collect Location Information
- People Search
- People Search Online Services
- People Search on Social Networking Services
- Gather Information from Financial Services
- Footprinting through Job Sites
- Monitoring Target Using Alerts

Website Footprinting
- Mirroring Entire Website
- Website Mirroring Tools
- Extract Website Information from http://www.archive.org
- Monitoring Web Updates Using Website Watcher

Email Footprinting
- Tracking Email Communications

- Collecting Information from Email Header
- Email Tracking Tools

Footprinting using Google
- Footprint Using Google Hacking Techniques
- What a Hacker can do with Google Hacking?
- Google Advance Search Operators
- Finding Resources Using Google Advance Operator
- Google Hacking Tools

WHOIS Footprinting
- WHOIS Lookup
- WHOIS Lookup Result Analysis
- WHOIS Lookup Tools
- WHOIS Lookup Online Tools

DNS Footprinting
- Extracting DNS Information
- DNS Interrogation Tools
- Using Nslookup
- Dig for Unix / Linux

Network Footprinting
- Locate the Network Range
- Determine the Operating System
- Traceroute
- Traceroute Analysis

- Traceroute Tools

Footprinting using Social Engineering
- Footprinting through Social Engineering
- Collect Information Using Eavesdropping, Shoulder Surfing, and Dumpster Diving
- Collect Information through Social Engineering on Social Networking Sites

Footprinting using Social Networking Sites
- Collecting Facebook Information
- Collecting Twitter Information
- Collecting Linkedin Information
- Collecting Youtube Information
- Tracking Users on Social Networking Sites

Footprinting Tools
- Maltego
- Domain Name Analyzer Pro
- Web Data Extractor
- Additional Footprinting Tools

ARMOURINFOSEC

Ethical Hacking & Penetration Testing

MODULE 04: SCANNING NETWORKS

Scanning Networks Concepts and Methodology
- Network Scanning
- Scanning Methodology

Check for Live Systems
- ICMP Scanning
- Ping Sweep
- Ping Sweep Tools

Banner Grabbing
- Banner Grabbing Tools
- Banner Grabbing Countermeasures: Disabling or Changing Banner
- Hiding File Extensions from Web Pages

Check for Open Ports
- Three-Way Handshake
- TCP Communication Flags
- Create Custom Packet Using TCP Flags

- Scanning IPv6 Network
- Scanning Tool
- Hping2 / Hping3
- Hping Commands
- Scanning Techniques
- Nmap
- TCP Connect / Full Open Scan
- Stealth Scan (Half-open Scan)
- Xmas Scan
- FIN Scan
- NULL Scan
- IDLE Scan
- ICMP Echo Scanning/List Scan
- UDP Scanning
- Inverse TCP Flag Scanning
- ACK Flag Scanning

Scanning Beyond IDS
- IDS Evasion Techniques
- SYN/FIN Scanning Using IP Fragments

Scan for Vulnerability
- Security Alerts
- Vulnerability Scanning
- Vulnerability Scanning Tool
- IBM Appscan
- GFI Languard
- Network Vulnerability Scanners
- Analyzing the Scan Results
- Generating Reports
- Remediation
- Patch Management

MODULE 05: PROXIES, VPNS AND TOR

- Proxy Servers
- Why Attackers Use Proxy Servers?
- Use of Proxies for Attack
- Proxy Chaining
- Proxy Tools

- Free Proxy Servers
- HTTP Tunneling Techniques
- Why do I Need HTTP Tunneling
- HTTP Tunneling Tool
- SSH Tunneling

- SSH Tunneling Tools
- Spoofing IP Address
- IP Spoofing Detection Techniques
- Tor: anonymous internet access
- How tor works

ARMOURINFOSEC

Ethical Hacking & Penetration Testing

MODULE 06: ENUMERATION

Enumeration Concepts
- What is Enumeration?
- Techniques for Enumeration
- Services and Ports to Enumerate

NetBIOS Enumeration
- NetBIOS Enumeration Tools
- Enumerating User Accounts
- Enumerate Systems Using Default Passwords

FTP Enumeration
- Banner Grabbing
- TFTP Enumeration
- Metasploit Modules

SSH Enumeration
- Version Scanning
- Banner Grabbing
- Scripts to enumerate
- Bruteforce

MSSql Enumeration
- Information Gathering
- SQL Users Enumeration
- Bruteforcing mssql
- Interactive database shell

VNC Enumeration

- Cracking Password
- Connecting to VNC

SNMP Enumeration
- SNMP (Simple Network Management Protocol) Enumeration
- Working of SNMP
- Management Information Base (MIB)
- SNMP Enumeration Tools

UNIX/Linux Enumeration
- UNIX/Linux Enumeration Commands
- Linux Enumeration Tools

LDAP Enumeration
- LDAP Enumeration Tools

Telnet Enumeration
- Scripts Scanning
- Banner Grabbing
- Brute forcing

Web Enumeration
- HTTP Method Enumeration
- HTTP Basic Authentication
- Checking Running Service Version

MySql Enumeration
- Basic Commands

- MySql BruteForcing

NTP Enumeration
- NTP Enumeration Commands

SMTP Enumeration
- SMTP Enumeration Tools

DNS Enumeration
- DNS Zone Transfer Enumeration Using NSLookup
- DNS Enumeration Tools

SMB Enumeration
- SMB Enumeration Tools
- Null sessions
- Syntax for a null session
- Viewing shares

NFS Enumeration
- Script Scan
- Enumerate NFS share
- Escalate the Privileges by NFS

Remote Desktop Enumeration
- Login with known credentials
- Nmap Scripts
- Brute-force
- Adding User to RDP group

ARMOURINFOSEC

Ethical Hacking & Penetration Testing

MODULE 07: SYSTEM HACKING

Windows Hacking &Security
- Introducing Operating System
- Introduction of Windows Hacking
- Bootloader
- File system
- Windows command & Powershell
- Special or shell folder in windows
- Windows Registry
- Group Policies
- Batch Programming & Windows Scripting

Cracking Passwords
- Password Cracking
- Password Complexity
- Password Cracking Techniques
- Types of Password Attacks
- Passive Online Attack
- Active Online Attack
- Distributed Network Attack
- Elcomsoft Distributed Password Recovery
- Non-Electronic Attacks
- Default Passwords
- Manual Password Cracking (Guessing)
- Stealing Passwords Using USB Drive
- Stealing Passwords Using Keyloggers
- Microsoft Authentication
- How Hash Passwords Are Stored in Windows SAM?

- What Is LAN Manager Hash?
- LM "Hash" Generation
- LM, NTLMv1, and NTLMv2
- NTLM Authentication Process
- Kerberos Authentication
- Salting
- PWdump7 and Fgdump
- L0phtCrack
- Ophcrack
- Cain & Abel
- Winrtgen and rtgen
- RainbowCrack
- Password Cracking Tools
- LM Hash Backward Compatibility
- How to Disable LM HASH
- How to Defend against Password Cracking
- Implement and Enforce Strong Security Policy

Executing Applications
- Executing Applications: RemoteExec
- Executing Applications: PDQ Deploy
- Executing Applications: DameWare NT Utilities

Spyware
- What Does the Spyware Do?
- Types of Spywares
- Desktop Spyware
- Email and Internet Spyware

- Child Monitoring Spyware
- Screen Capturing Spyware
- USB Spyware
- Audio Spyware
- Video Spyware
- Print Spyware
- Telephone/Cellphone Spyware
- GPS Spyware
- How to Defend Against Spyware
- Anti-Spywares

Keylogger
- Types of Keystroke Loggers
- Methodology of Attacker in Using Remote Keylogger
- How to Defend Against Keyloggers
- Anti-Keylogger

Hiding Files
- Rootkits
- Types of Rootkits
- How Rootkit Works
- Detecting Rootkits
- Steps for Detecting Rootkits
- How to Defend against Rootkits
- Anti-Rootkit

ARMOURINFOSEC

Ethical Hacking & Penetration Testing

MODULE 07: SYSTEM HACKING

NTFS Data Stream
- How to Create NTFS Streams
- NTFS Stream Manipulation
- How to Defend against NTFS Streams
- NTFS Stream Detectors

What is Steganography?
- Application of Steganography
- Classification of Steganography
- Technical Steganography
- Linguistic Steganography
- Steganography Techniques
- ow Steganography Works
- Types of Steganography

- Whitespace Steganography Tool
- Image Steganography
- Least Significant Bit Insertion
- Masking and Filtering
- Algorithms and Transformation
- Image Steganography Tools
- Document Steganography Tools
- Video Steganography Tools
- Audio Steganography Tools
- Folder Steganography Tools
- Spam/Email Steganography
- Natural Text Steganography
- Issues in Information Hiding

- Steganalysis
- Steganalysis Methods/Attacks on Steganography
- Detecting Text and Image Steganography
- Detecting Audio and Video Steganography
- Steganography Detection Tools

Covering Tracks
- Why Cover Tracks?
- Covering Tracks
- Ways to Clear Online Tracks
- Disabling Auditing
- Covering Tracks Tool
- Track Covering Tools

MODULE 08: PRIVILEGE ESCALATION

Escalating Privileges
- Privilege Escalation
- Privilege Escalation Tools
- How to Defend Against Privilege Escalation
- How to Do Privilege Escalation in Linux and Windows
- Tools that can help identify potential privilege escalation vulnerabilities on a system.
- How to create users

Linux Privilege Escalation

- Manual Enumeration
- User Details
- Operating System & Kernel Details
- Network Details
- Applications & Services Details
- User home directory enumeration
- Automated Enumeration
- Kernel Exploits
- Service Exploits

- Password Mining
- Linux File Permissions
- PATH Variable (Path abusing)
- Sudo (Shell Escape Sequences and Abusing Intended Functionality)
- Capabilities
- Cron Jobs & Systemd Timers
- NFS Root Squashing

ARMOURINFOSEC

Ethical Hacking & Penetration Testing

MODULE 08: PRIVILEGE ESCALATION

Windows Privilege Escalation
- Manual Enumeration
- User Details
- Operating System & Kernel Details
- Network Details
- Applications & Services Details

- User home directory enumeration
- Automated Enumeration
- Kernel Exploits
- Service Exploits
- Registry Exploits
- Password Mining

- Scheduled Tasks
- mimikatz
- Impersonation and Potato Attacks
- Startup Apps

MODULE 09: MALWARE THREATS

Trojan Concepts
- What is a Trojan?
- Purpose of Trojans
- What Do Trojan Creators Look For
- Indications of a Trojan Attack
- Common Ports used by Trojans

Types of Trojans
- Command Shell Trojans
- GUI Trojans
- Document Trojans
- E-mail Trojans
- Defacement Trojans
- Botnet Trojans
- Proxy Server Trojans
- FTP Trojans
- VNC Trojans

- HTTP/HTTPS Trojans
- ICMP Tunneling
- Remote Access Trojans
- Covert Channel Trojan
- E-banking Trojans
- Banking Trojan Analysis
- Destructive Trojans
- Notification Trojans
- Credit Card Trojans
- Data Hiding Trojans (Encrypted Trojans)
- Trojan Analysis: Flame
- Flame C&C Server Analysis
- Trojan Analysis

Trojan Detection
- How to Detect Trojans
- Scanning for Suspicious Ports

- Port Monitoring Tools
- Process Monitoring Tools
- Scanning for Suspicious Registry Entries
- Registry Entry Monitoring Tools
- Scanning for Suspicious Device Drivers
- Device Drivers Monitoring Tools
- Scanning for Suspicious Windows Services
- Windows Services Monitoring Tools
- Scanning for Suspicious Startup Programs
- Windows Startup Registry Entries
- Startup Programs Monitoring Tools
- Scanning for Suspicious Files and Folders
- Files and Folder Integrity Checker
- Scanning for Suspicious Network Activities
- Detecting Trojans and Worms with Capsa Network Analyzer

ARMOURINFOSEC

Ethical Hacking & Penetration Testing

MODULE 09: MALWARE THREATS

Trojan Infection
- How to Infect Systems Using a Trojan
- Wrappers
- Wrapper Covert Programs
- Different Ways a Trojan can Get into a System
- How to Deploy a Trojan
- Evading Anti-Virus Techniques

Anti-Trojan Software
- Anti-Trojan Software's

Virus and Worms Concepts
- Introduction to Viruses
- Virus and Worm Statistics
- Stages of Virus Life
- Working of Viruses: Infection Phase
- Working of Viruses: Attack Phase
- Why Do People Create Computer Viruses
- Indications of Virus Attack
- How does a Computer Get Infected by Viruses
- Common Techniques Used to Distribute Malware on the

Web
- Virus Hoaxes and Fake Antiviruses
- Virus Analysis

Types of Viruses
- System or Boot Sector Viruses
- File and Multipartite Viruses
- Macro Viruses
- Cluster Viruses
- Stealth/Tunneling Viruses
- Encryption Viruses
- Polymorphic Code
- Metamorphic Viruses
- File Overwriting or Cavity Viruses
- Sparse Infector Viruses
- Companion/Camouflage Viruses
- Shell Viruses
- File Extension Viruses
- Add-on and Intrusive Viruses
- Writing a Simple Virus Program

- Terabit Virus Maker
- JPS Virus Maker and DELmE's Batch Virus Maker

Worms
- How is a Worm Different from a Virus?
- Worm Analysis: Stuxnet
- Worm Maker: Internet Worm Maker Thing

Malware Analysis
- What is Sheep Dip Computer?
- Anti-Virus Sensors Systems
- Malware Analysis Procedure: Preparing Testbed
- Malware Analysis Procedure
- Virus Analysis Tool: IDA Pro
- Online Malware Testing: VirusTotal
- Online Malware Analysis Services

Detection Methods
- Virus and Worms
- Companion Antivirus
- Anti-virus Tools

ARMOURINFOSEC

Ethical Hacking & Penetration Testing

MODULE 10: SNIFFERS

Sniffing Concepts
- Wiretapping
- Packet Sniffing
- Sniffing Threats
- How a Sniffer Works
- Types of Sniffing Attacks
- Passive Sniffing
- Active Sniffing
- Protocols Vulnerable to Sniffing
- SPAN Port

MAC Attacks
- MAC Flooding
- MAC Address/CAM Table
- How CAM Works
- What Happens When CAM Table is Full?
- Mac Flooding Switches with macof
- MAC Flooding Tools
- How to Defend against MAC Attacks

DHCP Attacks
- How DHCP Works
- DHCP Request/Reply Messages
- IPv4 DHCP Packet Format
- DHCP Starvation Attack

- Rogue DHCP Server Attack
- How to Defend Against DHCP Starvation and Rogue Server Attack

ARP Poisoning
- What is Address Resolution Protocol (ARP)?
- ARP Spoofing Techniques
- ARP Spoofing Attack
- How Does ARP Spoofing Work
- Threats of ARP Poisoning
- ARP Poisoning Tools
- How to Defend Against ARP Poisoning
- ARP Spoofing Detection: XArp

Spoofing Attack
- Spoofing Attack Threats
- MAC Spoofing/Duplicating
- MAC Spoofing Technique: Windows
- MAC Spoofing Tool: SMAC
- IRDP Spoofing
- How to Defend Against MAC Spoofing

DNS Poisoning
- DNS Poisoning Techniques
- Intranet DNS Spoofing
- Proxy Server DNS Poisoning

- DNS Cache Poisoning
- How to Defend Against DNS Spoofing

Sniffing Tools
- Sniffing Tool: Wireshark
- Follow TCP Stream in Wireshark
- Display Filters in Wireshark
- Additional Wireshark Filters
- Sniffing Tool: Tcpdump/Windump
- Packet Sniffing Tool: Capsa Network Analyzer
- Network Packet Analyzer: OmniPeek Network Analyzer
- Network Packet Analyzer: Observer
- Network Packet Analyzer: Sniff-O-Matic
- Network Packet Analyzer: JitBit Network Sniffer
- Chat Message Sniffer: MSN Sniffer 2
- TCP/IP Packet Crafter: Colasoft Packet Builder
- How an Attacker Hacks the Network Using Sniffers

Sniffer Detection Technique
- How to Defend Against Sniffing
- How to Detect Sniffing
- Sniffer Detection Technique: Ping Method
- Sniffer Detection Technique: ARP Method
- Sniffer Detection Technique: DNS Method
- Promiscuous Detection Tool: PromqryUI

ARMOURINFOSEC

Ethical Hacking & Penetration Testing

MODULE 11: SOCIAL ENGINEERING

Social Engineering Concepts
- What is Social Engineering?
- Behaviors Vulnerable to Attacks
- Factors that Make Companies Vulnerable to Attacks
- Why Is Social Engineering Effective?
- Warning Signs of an Attack
- Phases in a Social Engineering Attack
- Impact on the Organization
- "Rebecca" and "Jessica"
- Common Targets of Social Engineering

Social Engineering Techniques
- Introduction of Social Engineering

- Types of Social Engineering
- Human-based Social Engineering
- Technical Support
- Authority Support
- Human base
- Human base: Eavesdropping and Shoulder Surfing
- Human base: Dumpster Diving
- Computer based Attacks
- Computer based Attacks: Pop-Ups
- Computer based Attacks: Phishing
- Computer based Attacks: Spear Phishing
- Computer based Attacks: Using Social Media

Mobile based
- Mobile based: Publishing Malicious Apps
- Mobile based: Repackaging Legitimate Apps
- Mobile based: Fake Security Applications
- Mobile based: Using SMS
- Insider Attack
- Disgruntled Employee
- Preventing Insider Threats
- How to Detect Phishing Emails
- Anti-Phishing Toolbar: Netcraft
- Anti-Phishing Toolbar: PhishTank
- Identity Theft

MODULE 12: DENIAL OF SERVICE

DoS/DDoS Concepts
- What is a Denial of Service Attack?
- What are Distributed Denial of Service Attacks?
- How Distributed Denial of Service Attacks Work
- Symptoms of a DoS Attack
- Cyber Criminals
- Organized Cyber Crime: Organizational Chart

DoS Attack Techniques
- Bandwidth Attacks
- Service Request Floods
- SYN Attack

- SYN Flooding
- ICMP Flood Attack
- Peer-to-Peer Attacks
- Permanent Denial-of-Service Attack
- Application Level Flood Attacks

Botnet
- Botnet Propagation Technique
- Botnet Ecosystem
- Botnet Trojan: Shark
- Poison Ivy: Botnet Command Control Center
- Botnet Trojan: PlugBot

- Botnet Trojans: Illusion Bot and NetBot Attacker

Denial of Service Attack Detection Techniques
- Activity Profiling
- Wavelet Analysis
- Sequential Change-Point Detection
- Post-Attack Forensics
- Techniques to Defend against Botnets
- DoS/DDoS Protection at ISP Level
- Enabling TCP Intercept on Cisco IOS Software
- Advanced DDoS Protection Appliances

ARMOURINFOSEC

Ethical Hacking & Penetration Testing

MODULE 13: ADVANCED EXPLOITATION TECHNIQUES

Web server Concepts
- Web server Market Shares
- Open Source Web server Architecture
- IIS Web server Architecture
- Understanding How Web Servers Are Hacked
- The Impact of Hacking
- Web Servers versus Web Applications
- The Role of Cloud

Discovering Risks & Misconfiguration in Web Servers
- Crawling, Enumeration, and Directory Traversal
- Mirroring Websites
- Reconnaissance and Footprinting
- HTTP Fingerprinting
- Social Engineering
- Internal Leakage
- Debug Settings
- Excessive Access Rights
- Misconfigured SSL
- Weaknesses in Default Configurations
- Other Attacks against Web Servers

Website Defacement
- HTTP Response Splitting
- Web Cache Poisoning
- Brute Forcing Authentication Schemes
- Streamline Testing with Automation
- Hacking Web Applications

Web server Security Tools

- Syhunt Dynamic
- N-Stalker Web Application Security Scanner
- Wikto
- Acunetix Web Vulnerability Scanner
- HackAlert
- QualysGuard Malware Detection
- Managing and Hardening Web Servers

What is Patch Management?
- Identifying Appropriate Sources for Updates and Patches
- Installation of a Patch
- Implementation and Verification of a Security Patch or Upgrade
- Patch Management Tools
- Designing for Network Segmentation
- Sandboxing

Web server Concepts
- Web server Market Shares
- Open Source Web server Architecture
- IIS Web server Architecture
- Understanding How Web Servers Are Hacked
- The Impact of Hacking
- Web Servers versus Web Applications
- The Role of Cloud

Discovering Risks & Misconfiguration in Web Servers
- Crawling, Enumeration, and Directory Traversal
- HTTP Fingerprinting
- Social Engineering

- Internal Leakage
- Debug Settings
- Excessive Access Rights
- Misconfigured SSL
- Weaknesses in Default Configurations
- Other Attacks against Web Servers

Website Defacement
- HTTP Response Splitting
- Web Cache Poisoning
- Brute Forcing Authentication Schemes
- Streamline Testing with Automation
- Hacking Web Applications

Injection
- HTML Injection
- OS Command Injection
- OS Command Injection – Blind
- PHP Code Injection
- Server-Side Includes (SSI) Injection
- SQL Injection – Double Query
- Based
- XML/XPath Injection

ARMOURINFOSEC

Ethical Hacking & Penetration Testing

MODULE 13: ADVANCED EXPLOITATION TECHNIQUES

Web server Security Tools

- Syhunt Dynamic
- N-Stalker Web Application Security Scanner
- Wikto
- Acunetix Web Vulnerability Scanner
- HackAlert

- QualysGuard Malware Detection
- Managing and Hardening Web Servers

What is Patch Management?

- Identifying Appropriate Sources for Updates and Patches
- Installation of a Patch
- Implementation and Verification of a Security Patch or

- Upgrade
- Patch Management Tools
- Support and End of Life
- Locking Down Services
- Designing for Network Segmentation
- Sandboxing

MODULE 14: EVADING IDS, FIREWALLS, AND HONEYPOTS

- Introduction of Working with Firewalls
- Understanding Firewalls
- Firewall Architectures
- Types of Firewalls
- Evading Firewalls
- Configuring Proxy
- Evading Firewalls using Tunneling
- Evading Firewalls using External Systems
- Evading Firewalls using miTM Attacks
- Firewalls Evation Tools
- Firewall Bypassing & Penetration Testing
- Firewalls Evation Tools Continued
- Honeypots Defined
- Types of Honeypots
- Detecting Honepots

- Honeypot using Atomic Software
- Introduction to IDS
- Intrusion Detection Systems
- Introduction to Evading IDS
- Encryption & Flooding
- Obfuscating
- Fragmentation Attacks
- Overlapping Fragments
- Points of Vulnerabilities in IDS
- How to avoid IDS Demo
- Insertion Attacks
- Evasion Attacks
- Denial of Service Attacks
- Application Layer- Attacks
- Time to Live Attacks

- False Positive Generation
- Urgency Flag
- Session Splicing
- Pre Connection SYN
- Post Connection SYN
- Snort
- More tools
- Ways to Detect
- ADMmutate
- Other Evading Tools
- Centralized Security Management
- IDS Penetration Testing

ARMOURINFOSEC