INFOSECTRAIN

OFFENSIVE CYBER SECURITY ENGINEER

COURSE CONTENT

sales@infosectrain.com | www.infosectrain.com

Index

Security Fundamentals : Eccouncil CEH / CEH(Practical)

This course would be covering the essentials of security, touching base on security terminologies, various attack methodologies and techniques used by offenders/hackers in the real world. Advancing forward, it also covers in-depth, various aspects of the cybersecurity field. The course also provides hands-on experience on various industrial tools used for these purposes.

- CEH
  - **Module 01:** Introduction to Ethical Hacking
  - **Module 02:** Footprinting and Reconnaissance
  - **Module 03:** Scanning Networks
  - **Module 04:** Enumeration
  - **Module 05:** Vulnerability Analysis
  - **Module 06:** System Hacking
  - **Module 07:** Malware Threats
  - **Module 08:** Sniffing
  - **Module 09:** Social Engineering
  - **Module 10:** Denial-of-Service
  - **Module 11:** Session Hijacking
  - **Module 12:** Evading IDS, Firewalls, and Honeypots
  - **Module 13:** Hacking Web Servers
  - **Module 14:** Hacking Web Applications
  - **Module 15:** SQL Injection
  - **Module 16:** Hacking Wireless Networks
  - **Module 17:** Hacking Mobile Platforms
  - **Module 18:** IoT Hacking
  - **Module 19:** Cloud Computing
  - **Module 20:** Cryptography

Advanced Pentest : InfosecTrain APT

This is an advanced level course designed by experts for InfosecTrain. The course imparts a very high level of understanding of various components of infrastructure, including OS, IDS/IPS, firewalls, etc., determining vulnerabilities in these systems and using them to break into a secured system without being discovered. The course also focuses on providing an understanding and usage of a variety of tools.

Domain 1.0: Planning and Scoping

1.1 Explain the importance of planning for an engagement.

- Understanding the target audience
- Rules of engagement
- Communication escalation path
- Resources and requirements
  - Confidentiality of findings
  - Known vs. unknown
- Budget
- Impact analysis and remediation timelines
- Disclaimers
  - Point-in-time assessment
  - Comprehensiveness
- Technical constraints
- Support resources
  - WSDL/WADL
  - SOAP project file
  - SDK documentation
  - Swagger document
  - XSD
  - Sample application requests
  - Architectural diagrams

1.2 Explain key legal concepts.

- Contracts
  - SOW
  - MSA
  - NDA
- Environmental differences
  - Export restrictions
  - Local and national government restrictions
  - Corporate policies
- Written authorization
  - Obtain signature from proper signing authority
  - Third-party provider authorization when necessary

1.3 Explain the importance of scoping an engagement properly.

- Types of assessment
  - Goals-based/objectives-based
  - Compliance-based
  - Red team
- Special scoping considerations
  - Premerger
  - Supply chain
- Target selection
  - Targets
    - Internal
      - On-site vs. off-site
    - External
    - First-party vs. third-party hosted
    - Physical
    - Users
    - SSIDs
    - Applications
  - Considerations
    - White-listed vs. black-listed
    - Security exceptions
      - IPS/WAF whitelist
      - NAC
      - Certificate pinning
      - Company's policies
  - Supply chain
- Threat actors
  - Adversary tier
    - APT
    - Script kiddies
    - Hacktivist
    - Insider threat
  - Capabilities
  - Intent
  - Threat models
- Strategy
  - Black box vs. white box vs. gray box
- Risk acceptance
- Tolerance to impact
- Scheduling
- Scope creep

1.4 Explain the key aspects of compliance-based assessments.

- Compliance-based assessments, limitations, and caveats
  - Rules to complete assessment
  - Password policies
  - Data isolation
  - Key management
  - Limitations
    - Limited network access
    - Limited storage access
- Clearly defined objectives based on regulations

Domain 2.0: Information Gathering and Vulnerability Identification

2.1 Given a scenario, conduct information gathering using appropriate techniques.

- Scanning
- Enumeration
  - Hosts
  - Networks
  - Domains
  - Users
  - Groups
  - Network shares
  - Web pages
  - Applications
  - Services
  - Tokens
  - Social networking sites
- Packet crafting
- Packet inspection
- Fingerprinting
- Cryptography
  - Certificate inspection
- Eavesdropping
  - RF communication monitoring

- Sniffing
  - Wired
  - Wireless
- Decompilation
- Debugging
- Open Source Intelligence Gathering
  - Sources of research
    - CERT
    - NIST
    - JPCERT
    - CAPEC
    - Full disclosure
    - CVE
    - CWE

2.2 Given a scenario, perform a vulnerability scan.

- Credentialed vs. non-credentialed
- Types of scans
  - Discovery scan
  - Full scan
  - Stealth scan
  - Compliance scan
- Container security
- Application scan
  - Dynamic vs. static analysis
- Considerations of vulnerability scanning
  - Time to run scans
  - Protocols used
  - Network topology
  - Bandwidth limitations
  - Query throttling
  - Fragile systems/non-traditional assets

2.3 Given a scenario, analyze vulnerability scan results.

- Asset categorization
- Adjudication
  - False positives
- Prioritization of vulnerabilities
- Common themes

- Vulnerabilities
- Observations
- Lack of best practices

2.4 Explain the process of leveraging information to prepare for exploitation.

- Map vulnerabilities to potential exploits
- Prioritize activities in preparation for penetration test
- Describe common techniques to complete attack
  - Cross-compiling code
  - Exploit modification
  - Exploit chaining
  - Proof-of-concept development (exploit development)
  - Social engineering
  - Credential brute forcing
  - Dictionary attacks
  - Rainbow tables
  - Deception

2.5 Explain weaknesses related to specialized systems.

- ICS
- SCADA
- Mobile
- IoT
- Embedded
- Point-of-sale system
- Biometrics
- Application containers
- RTOS

Domain 3.0: Attacks and Exploits

3.1 Compare and contrast social engineering attacks.

- Phishing
  - Spear phishing
  - SMS phishing
  - Voice phishing
  - Whaling

- Elicitation
  - Business email compromise
- Interrogation
- Impersonation
- Shoulder surfing
- USB key drop
- Motivation techniques
  - Authority
  - Scarcity
  - Social proof
  - Urgency
  - Likeness
  - Fear

3.2 Given a scenario, exploit network-based vulnerabilities.

- Name resolution exploits
  - NETBIOS name service
  - LLMNR
- SMB exploits
- SNMP exploits
- SMTP exploits
- FTP exploits
- DNS cache poisoning
- Pass the hash
- Man-in-the-middle
  - ARP spoofing
  - Replay
  - Relay
  - SSL stripping
  - Downgrade
- DoS/stress test
- NAC bypass
- VLAN hopping

3.3 Given a scenario, exploit wireless and RF-based vulnerabilities.

- Evil twin
  - Karma attack
  - Downgrade attack

- Deauthentication attacks
- Fragmentation attacks
- Credential harvesting
- WPS implementation weakness
- Bluejacking
- Bluesnarfing
- RFID cloning
- Jamming
- Repeating

3.4 Given a scenario, exploit application-based vulnerabilities.

- Injections
  - SQL
  - HTML
  - Command
  - Code
- Authentication
  - Credential brute forcing
  - Session hijacking
  - Redirect
  - Default credentials
  - Weak credentials
  - Kerberos exploits
- Authorization
  - Parameter pollution
  - Insecure direct object reference
- Cross-site scripting (XSS)
  - Stored/persistent
  - Reflected
  - DOM
- Cross-site request forgery (CSRF/XSRF)
- Clickjacking
- Security misconfiguration
  - Directory traversal
  - Cookie manipulation
- File inclusion
  - Local
  - Remote
- Unsecure code practices
  - Comments in source code
  - Lack of error handling
  - Overly verbose error handling
  - Hard-coded credentials
  - Race conditions
  - Unauthorized use of functions/unprotected APIs
  - Hidden elements
  - Sensitive information in the DOM
  - Lack of code signing

3.5 Given a scenario, exploit local host vulnerabilities.

- OS vulnerabilities
  - Windows
  - Mac OS
  - Linux
  - Android
  - iOS
- Unsecure service and protocol configurations
- Privilege escalation
  - Linux-specific
    - SUID/SGID programs
    - Unsecure SUDO
    - Ret2libc
    - Sticky bits
  - Windows-specific
    - Cpassword
    - Clear text credentials in LDAP
    - Kerberoasting
    - Credentials in LSASS
    - Unattended installation
    - SAM database
    - DLL hijacking
  - Exploitable services
    - Unquoted service paths
    - Writable services
  - Unsecure file/folder permissions
  - Keylogger
  - Scheduled tasks
  - Kernel exploits
- Default account settings
- Sandbox escape
  - Shell upgrade
  - VM
  - Container
- Physical device security
  - Cold boot attack
  - JTAG debug
  - Serial console

3.6 Summarize physical security attacks related to facilities.

- Piggybacking/tailgating
- Fence jumping
- Dumpster diving
- Lock picking
- Lock bypass
- Egress sensor
- Badge cloning

3.7 Given a scenario, perform post-exploitation techniques.

- Lateral movement
  - RPC/DCOM
    - PsExec
    - WMI
    - Scheduled tasks
  - PS remoting/WinRM
  - SMB
  - RDP
  - Apple Remote Desktop
  - VNC
  - X-server forwarding
  - Telnet
  - SSH
  - RSH/Rlogin
- Persistence
  - Scheduled jobs
  - Scheduled tasks
  - Daemons
  - Back doors
  - Trojan
  - New user creation
- Covering your tracks

Domain 4.0: Penetration Testing Tools

4.1 Given a scenario, use Nmap to conduct information gathering exercises.

- SYN scan (-sS) vs. full connect scan (-sT)
- Port selection (-p)
- Service identification (-sV)
- OS fingerprinting (-O)
- Disabling ping (-Pn)
- Target input file (-iL)
- Timing (-T)
- Output parameters
  -oA
  -oN
  -oG
  -oX

4.2 Compare and contrast various use cases of tools.

(**The intent of this objective is NOT to test specific vendor feature sets.)

- Use cases
  - Reconnaissance
  - Enumeration

- Vulnerability scanning
- Credential attacks
  - Offline password cracking
  - Brute-forcing services
- Persistence
- Configuration compliance
- Evasion
- Decompilation
- Forensics
- Debugging
- Software assurance
  - Fuzzing
  - SAST
  - DAST

- Tools
  - Scanners
    - Nikto
    - OpenVAS
    - SQLmap
    - Nessus
  - Credential testing tools
    - Hashcat
    - Medusa
    - Hydra
    - Cewl
    - John the Ripper
    - Cain and Abel
    - Mimikatz
    - Patator
    - Dirbuster
    - W3AF
  - Debuggers
    - OLLYDBG
    - Immunity debugger
    - GDB
    - WinDBG
    - IDA
  - Software assurance
    - Findbugs/findsecbugs
    - Peach
    - Dynamo
    - AFL
    - SonarQube
    - YASCA
  - OSINT
    - Whois
    - Nslookup
    - Foca
    - Theharvester
    - Shodan
    - Maltego
    - Recon-NG
    - Censys
  - Wireless
    - Aircrack-NG
    - Kismet
    - WiFite
  - Web proxies
    - OWASP ZAP
    - Burp Suite
  - Social engineering tools
    - SET
    - BeEF
  - Remote access tools
    - SSH
    - NCAT
    - NETCAT
    - Proxychains
  - Networking tools
    - Wireshark

- Hping
- Mobile tools
  - Androzer
  - APKX
  - APK studio
- MISC
  - Searchsploit
  - Powersploit
  - Responder
  - Impacket
  - Empire
  - Metasploit framework

4.3 Given a scenario, analyze tool output or data related to a penetration test.

- Password cracking
- Pass the hash
- Setting up a bind shell
- Getting a reverse shell
- Proxying a connection
- Uploading a web shell
- Injections

4.4 Given a scenario, analyze a basic script (limited to Bash, Python, Ruby, and PowerShell).

- Logic
  - Looping
  - Flow control
- I/O
  - File vs. terminal vs. network
- Substitutions
- Variables
- Common operations
  - String operations
  - Comparisons
- Error handling
- Arrays
- Encoding/decoding

Domain 5.0: Reporting and Communication

5.1 Given a scenario, use report writing and handling best practices.

- Normalization of data
- Written report of findings and remediation
  - Executive summary
  - Methodology
  - Findings and remediation
  - Metrics and measures
    - Risk rating
  - Conclusion
- Risk appetite
- Storage time for report
- Secure handling and disposition of reports

5.2 Explain post-report delivery activities.

- Post-engagement cleanup
  - Removing shells
  - Removing tester-created credentials
  - Removing tools
- Client acceptance
- Lessons learned
- Follow-up actions/retest
- Attestation of findings

5.3 Given a scenario, recommend mitigation strategies for discovered vulnerabilities.

- Solutions
  - People
  - Process
  - Technology
- Findings
  - Shared local administrator credentials
  - Weak password complexity
  - Plain text passwords
  - No multifactor authentication
  - SQL injection
  - Unnecessary open services

- Remediation
  - Randomize credentials/LAPS
  - Minimum password requirements/password filters
  - Encrypt the passwords
  - Implement multifactor authentication
  - Sanitize user input/parameterize queries
  - System hardening

5.4 Explain the importance of communication during the penetration testing process.

- Communication path
- Communication triggers
  - Critical findings
  - Stages
  - Indicators of prior compromise
- Reasons for communication
  - Situational awareness
  - De-escalation
  - De-confliction
- Goal reprioritization

Active Directory Pentest: Offensive cyber Security Engineer

Active Directory Pentest

- Course Introduction and Overview
- Active Directory Overview
- Physical, Logical Active Directory Components
- Building Active Directory Lab

Attacking Active Directory

- Introduction
- LLMNR Poisoning Overview
- Capturing NTLMv2 Hashes with Responder
- Password Cracking with Hashcat
- LLMNR Poisoning Defenses
- SMB Relay Attacks Overview
- Quick Lab Update

- Discovering Hosts with SMB Signing
- SMB Relay Attack Demonstration
- SMB Relay Attack Defenses
- Gaining Shell Access

Post-Compromise Enumeration

- Introduction
- PowerView Overview
- Domain Enumeration with PowerView
- Bloodhound Overview and Setup
- Grabbing Data with Invoke-Bloodhound
- Enumerating Domain Data with Bloodhound

Post-Compromise Attacks

- Introduction
- Pass the Hash / Password Overview
- Installing crackmapexec
- Pass the Password Attacks
- Dumping Hashes with secretsdump.py
- Cracking NTLM Hashes with Hashcat
- Pass the Hash Attacks
- Pass Attack Mitigations
- Token Impersonation Overview
- Token Impersonation with Incognito
- Token Impersonation Mitigation
- Kerberoasting Overview
- Kerberoasting Walkthrough
- Kerberoasting Mitigation

- GPP / cPassword Attacks Overview
- Abusing GPP: Part 1
- Abusing GPP: Part 2
- Mimikatz Overview
- Credential Dumping with Mimikatz
- Golden Ticket Attacks

Post Exploitation

- Introduction
- File Transfers Review
- Maintaining Access Overview
- Pivoting Lab Setup
- Pivoting Walkthrough
- Cleaning Up

Exploit Development Basics (Python Shell Script)

Linux Stack Smashing

- Introduction to the basics of Linux stack overflow vulnerabilities and the required debugging toolset
- Linux fundamentals
- stack overflow exploitation
- Linux exploit mitigations related to stack overflow exploitation
- Understanding Return Oriented Programming
- Learning how to write Linux shellcode from scratch, including cases such as Egghunting, encoding, etc.

ISO 27001 Fundamental /PCI-DSS

- Understanding Standard and regulatory framework
- Fundamental principles of information security
- Information Security Management System (ISMS)
- Understanding Audit Principals
- Understanding Onsite Audit Activities
- Closing an Audit

INFOSECTRAIN

sales@infosectrain.com | www.infosectrain.com