INFOSECTRAIN

AI Powered Course

RED TEAM

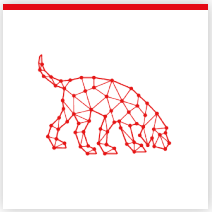
Operations Professional

Online Training

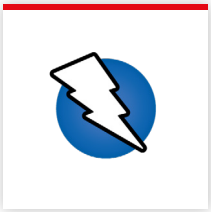
INFOSECTRAIN

Top Tools Covered

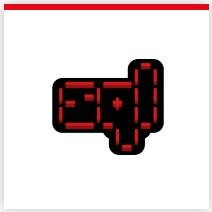
Browser Exploitation Framework (BeEF)



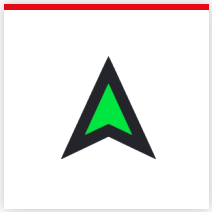
BloodHound



OWASP ZAP (Zed Attack Proxy)

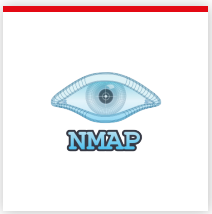


Sqlmap



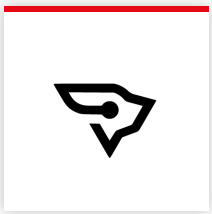
XSStrike

Metasploit Framework



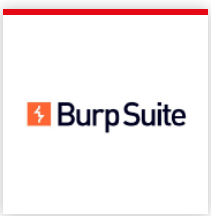
Nmap

Nessus

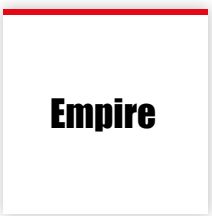


SharpHound

Sliver



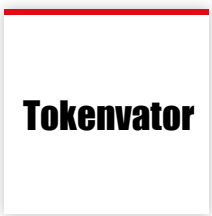
Burp Suite



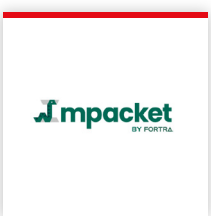
Empire

LaZagne

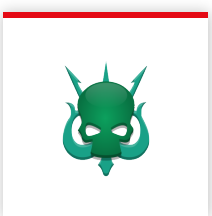
Mimikatz



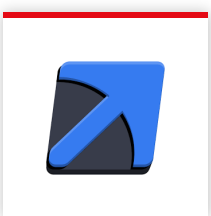
Tokenvator



Impacket



CrackMapExec



Responder

INFOSECTRAIN

Course Highlights

- **60-Hour** Instructor-Led Training
- Learn from Experienced **Offensive Security Experts**
- **Hands-on Labs** with Realistic Attack Simulations
- **OSINT, Exploitation**, Persistence & Lateral Movement Exercises
- Detection-Aware Setup **Custom Lab**
- **Interview Preparation** for Red Team Roles
- **Purple Team Collaboration** Tips & Tradecraft Insights
- **Post-Course Mentorship** & Community Access
- Access to **Recorded Sessions**

INFOSECTRAIN

About Course

The Red Team Operations Professional Training course by InfosecTrain blends theory and practical labs to help professionals master the art of red team operations while adhering to strict legal and ethical guidelines. Through structured modules, learners explore the entire red team engagement lifecycle—planning, exploitation, persistence, C2 operations, and advanced tradecraft. The program emphasizes real-world adversary emulation, operational security, and collaboration with blue teams, ensuring participants walk away with skills to execute impactful, stealthy, and professional red team engagements.

Course Objectives

Upon successful completion of the course, participants will be able to:

- Execute Initial Access techniques such as phishing, malicious documents, and exploiting misconfigurations.
- Perform Reconnaissance and Enumeration including Active Directory mapping, user hunting, and asset profiling.
- Leverage Credential Access attacks like Kerberoasting, AS-REP Roasting, DCSync, and token theft.
- Conduct Lateral Movement using Pass-the-Hash, RDP hijacking, SMB relay, and WinRM abuse.
- Apply Privilege Escalation techniques such as UAC bypass, DLL hijacking, and kernel exploits.
- Implement Evasion and OPSEC methods including AV/EDR bypass, LOLBAS, and living-off-the-land techniques.
- Operate Command & Control (C2) frameworks like Covenant, Sliver, Mythic, staging, and persistence modules.
- Deliver Reporting and Debrief sessions by crafting impactful reports, mapping findings to MITRE, and effectively communicating results.
- LLM Penetration Testing involves assessing AI models to identify vulnerabilities such as data poisoning and model poisoning.

INFOSECTRAIN

Target Audience

The training is ideal for:

- Penetration Testers transitioning into Red Team roles
- SOC Analysts and Blue Teamers seeking adversarial insight
- Security Engineers and Architects building detection strategies
- Cybersecurity students and enthusiasts with a strong technical foundation
- Professionals preparing for CREST, OSCP, CRTO, or similar certifications

Pre-Requisites

- Good understanding of networking concepts (TCP/IP, common protocols)
- Familiarity with advanced Linux command line and regular expressions
- Good scripting knowledge (e.g., Python, PowerShell, Bash)
- Understanding of common operating systems (Windows, Linux)

INFOSECTRAIN

Course Content

Theoretical

Module 1 — Red Teaming Fundamentals and Ethics

- Introduction to Red Teaming
- What is Red Teaming?
- Red Teaming vs Penetration Testing
- Benefits of Red Teaming for Organizations
- Types of Red Team Engagements (e.g., Full Scope, Specific Objective)
- Red Team Engagement Lifecycle
  - Planning and Scoping (Understanding Objectives, Constraints, ROE)
  - Reconnaissance (OSINT, Passive, Active)
  - Initial Compromise
  - Establish Foothold and Persistence
  - Internal Reconnaissance and Privilege Escalation
  - Lateral Movement
  - Data Exfiltration
  - Post-Engagement Activities (Reporting, Lessons Learned)
- Legal and Ethical Considerations
- Importance of Written Authorization (Get out of Jail Free card)
- Ethics in Offensive Security
- Understanding Legal Frameworks (e.g., CFAA, GDPR, Mention Local Regulations for India if Relevant, Though the Course is General)
- Professionalism and Responsible Disclosure
- Operational Security (OPSEC) for Red Teams
- Protecting your Tools, Infrastructure, and Identity

- Maintaining Stealth and Avoiding Detection
- Tradecraft Considerations

Practical

Module 2 — Reconnaissance and Open Source Intelligence (OSINT)

- OSINT Methodologies
- Public Records, Social Media, News Archives
- Google Dorking, Shodan, Censys
- Whois, DNS Records
- Company Websites, Employee Profiles (LinkedIn)
- Dark Web Monitoring (Brief Overview, Ethical Considerations)
- Passive Reconnaissance
  - DNS Enumeration (Dig, Host, nslookup, Fierce, dnsenum)
  - Subdomain Enumeration (sublist3r, assetfinder, Amass)
  - Email Gathering (theHarvester, hunter.io)
  - Web Application Reconnaissance (Wappalyzer, builtwith)
- Active Reconnaissance (Stealthy Approaches)
  - Port Scanning
  - Vulnerability Scanning (Introduction to Nessus)
  - Network Mapping (Maltego, Custom Scripts)

INFOSECTRAIN

Practical

Module 3 Initial Access and Exploitation

- Client-Side Attacks
  - Phishing and Spear Phishing (Payload Delivery, Social Engineering)
  - Malicious Documents (Macros, OLE Objects)
  - Browser Exploitation (Drive-by Downloads, Ethical Warning)
  - Watering Hole Attacks (Conceptual)
- Web Application Exploitation (Red Team Focus)
  - OWASP Top 10 Revisited (Focus on Initial Compromise Vectors)
  - SQL Injection for Initial Access (Blind SQLi, Out-of-band)
  - Cross-Site Scripting (XSS) for Cookie Stealing/Credential Harvesting
  - File Upload Vulnerabilities
  - Deserialization Vulnerabilities
- Network-Based Exploitation
  - Exploiting Vulnerable Services (SMB, RDP, SSH, FTP)
  - Metasploit Framework (Advanced Usage, Custom Modules)
  - Exploiting Public-facing Vulnerabilities (CVE Research, PoC Adaptation)
- Bypassing Defenses (Introduction)
  - Antivirus Evasion Techniques
  - Firewall Bypass (Port Forwarding, Tunneling)
  - IDS/IPS Evasion (Fragmentation, Encryption)

Module 4 Establishing Foothold and Persistence

- Windows Persistence
  - Registry Run Keys
  - Startup folders
  - Scheduled Tasks and Services
  - WMI Event Subscriptions
  - DLL Hijacking
- Linux Persistence
  - Cron Jobs
  - Systemd Services
  - Startup Scripts (/etc/rc.local, init.d)
  - SSH Authorized Keys
  - Rootkits (Conceptual, Ethical Considerations)
- Cross-Platform Persistence Techniques
  - Backdoored Executables
  - Web Shells (for Web Server Persistence)
  - Implant Deployment (C2 agents - e.g., Covenant, Empire, Sliver)
- Covert Channels for C2
  - DNS Tunneling (iodine, dnscat2)
  - ICMP Tunneling
- Windows Internal Reconnaissance
  - Active Directory Enumeration (BloodHound, PowerView)
  - Local User and Group Enumeration
  - Network Share Discovery
  - Installed Software and Patches

- Firewall Rules and Network Configurations
- Kerberoasting and AS-REP Roasting

- Linux Internal Reconnaissance
  - Kernel Vulnerabilities
  - SUDO Misconfigurations
  - SUID/SGID Binaries
  - Cron Job Misconfigurations
  - Writable Files and Directories
  - Password Reuse

- Common Privilege Escalation Techniques
  - Unquoted Service Paths
  - Insecure Service Permissions
  - Kernel Exploits
  - Credential Harvesting (Mimikatz, LaZagne)
  - Token impersonation
  - Pass-the-Hash/Pass-the-Ticket

- Windows Lateral Movement
  - SMB (PsExec, wmiexec, CrackMapExec)
  - WMI
  - RDP
  - Scheduled Tasks
  - Service Creation
  - Domain Controller Attacks (Golden/Sliver Tickets)

- Linux Lateral Movement
  - SSH (sshpass, SSH Tunneling)
  - Exploiting Shared Directories

- Pivoting and Tunneling
  - SSH Tunneling (Local, Remote, Dynamic Port Forwarding)
  - SOCKS Proxies (proxychains)
  - Chisel, Ligolo-ng
  - Port Forwarding (socat, netcat)
  - Double Pivoting Scenarios
- Evading Network Defenses
  - Network Segmentation Bypass (Conceptual)
  - Traffic Obfuscation
  - Low-and-slow Techniques

Module 5 Data Exfiltration Impact

- Identifying Sensitive Data
  - Financial Data, PII, Intellectual Property
  - Configuration Files, Source Code
  - Password hashes, credentials
- Exfiltration Techniques
  - Direct HTTP/S Transfers
  - DNS Exfiltration
  - ICMP Exfiltration
- Covering Tracks and Anti-Forensics (Ethical Considerations)
  - Clearing Logs (Event Logs, Shell History)
  - Timestamp Manipulation (Touch)
  - Shredding Files
  - Emphasis on Understanding These for Blue Team Defense
- Impact Simulation
  - Ransomware Simulation (No Actual Encryption, Just Demonstrating Capability)
  - Data Manipulation/Deletion

Module 6 Command and Control (C2) Frameworks and Infrastructure

- Introduction to C2 Frameworks
  - Types of C2 (HTTP, DNS, SMB, Custom)
  - Common C2 Frameworks: Cobalt Strike, Mythic, Covenant, Empire, Sliver
- Metasploit (Multi/Handler)
  - Choosing the Right C2 for the Engagement
- C2 Infrastructure Setup
  - Domain Fronting
  - Redirectors (Apache, Nginx, Haproxy)
  - Malleable C2 Profiles
  - Cloud C2 Infrastructure (AWS, Azure, DigitalOcean, Ethical Considerations and Cost)
  - Obfuscating C2 Traffic
- Advanced C2 Evasion
  - Customizing C2 Implants
  - Network Indicator Removal (Removing Unique Strings)
  - Payload Encryption and Obfuscation
  - Domain Name Registration and Reputation
  - Using Legitimate Services for C2 (e.g., Slack, GitHub, High Risk, Ethical Discussion)
- C2 Post-Exploitation Modules
  - Leveraging C2 Built-in Features for Recon, Lateral Movement, Persistence Scripting within C2 Frameworks

INFOSECTRAIN

Module 7 Adversary Simulation and Advanced Tradecraft

- Develop an Adversary Emulation Plan Based on Real-world Threat Actors
- Implement Advanced Tradecraft to Bypass Mature Defenses
- Threat Intelligence and Adversary Emulation
- MITRE ATT&CK Framework for Red Teaming
- Mapping TTPs to Threat Actors (e.g., APT29, FIN7)
- Developing an Adversary Emulation Plan
- Purple Teaming Concept
- Advanced Evasion Techniques
  - ✓ Memory Injection Techniques (Process Hollowing, Reflective DLL Injection)
  - ✓ Abusing Legitimate Tools and Processes (Living Off The Land - LOLBins/LOLBAS)
  - ✓ Code Signing Abuse
  - ✓ Sandbox Evasion
- Post-Engagement Activities
  - ✓ Debriefing with the Blue Team
  - ✓ Detailed Reporting (Executive Summary, Technical Findings, Recommendations)
  - ✓ Lessons Learned and Continuous Improvement
  - ✓ Metrics for Red Teaming

INFOSECTRAIN

AI For Red Team

- Introduction to LLM
- OWASP Top 10 LLM
- Using AI for Network Discovery
- Gyoithon for web server intelligence gathering
- Audio Deepfake Development
- Visual deepfake
- AI Injection: Using AI for SQL Exploits
- Using AI in the phases of pentesting
- Understanding RAG (Retrieval-Augmented Generation) Architecture: Components (Retriever, Generator, Knowledge Base)
- Threats to RAG Pipelines:
  - **Knowledge Base Poisoning:** Injecting malicious or biased information
  - **Retrieval Manipulation:** Directing the retriever to unsafe or irrelevant documents
  - **Generator Vulnerabilities:** Prompt injection, jailbreaking through RAG context
  - **Integration Points:** API security between components, data exfiltration from knowledge base or generated content
  - **Denial of Service:** Overloading the retriever or generator
  - Defense Strategies for RAG

INFOSECTRAIN

Red Team Operations Tool List

1 Reconnaissance and OSINT

- Google Dorking, Shodan, Censys
- whois, dig, host, nslookup, fierce, dnsenum
- sublist3r, assetfinder, Amass
- theHarvester, hunter.io
- Wappalyzer, BuiltWith
- Maltego, SpiderFoot, Recon-ng

2 Initial Access and Exploitation

Client-Side Attacks

- Gophish, King Phisher, SET (Social-Engineer Toolkit)
- MacroPack, EvilClippy, SharpShooter
- Browser Exploitation Framework (BeEF)

3 Web Exploitation

- Burp Suite, OWASP ZAP
- sqlmap, XSStrike, Commix
- UploadScanner, Deserialization Exploitation Toolkit

4 Network Exploitation

- Metasploit Framework, ExploitDB, searchsploit
- Nmap, Nessus, OpenVAS
- Impacket, CrackMapExec, Responder

5 Persistence and Foothold

Windows

- PowerView, WinPEAS, Seatbelt
- WMI Explorer, Autoruns, Sysinternals Suite

Linux

- LinPEAS, Linux Exploit Suggester, pspy
- chkrootkit, rkhunter

Cross-Platform

- Covenant, Empire, Sliver, Mythic
- Web shells, backdoored binaries, SSH implants

Covert Channels

- iodine, dnscat2, ICMPExfil, Ptunnel

6 Internal Recon and Privilege Escalation

- BloodHound, SharpHound
- LaZagne, Mimikatz, Tokenvator
- Linux Exploit Suggester, GTFOBins
- SudoKiller, SUID3NUM, find, grep, awk

7 Lateral Movement and Pivoting

Windows

- PsExec, wmiexec.py, CrackMapExec
- RDP, Scheduled Tasks, Golden/Sliver Ticket tools

Linux

- sshpass, proxychains, Ligolo-ng, Chisel, socat, netcat

8 Data Exfiltration and Impact Simulation

- curl, wget, scp, rsync
- dns2tcp, ICMPExfil, exfiltration scripts
- touch, shred, log cleaner scripts
- Custom ransomware simulators (non-destructive)

9 C2 Frameworks and Infrastructure

- Cobalt Strike (licensed), Mythic, Empire, Sliver, Metasploit multi/handler
- Apache, Nginx, HAProxy (redirectors)

10 Advanced Tradecraft and Adversary Simulation

- Invoke-Obfuscation, NinjaCopy, Process
- Hollowing scripts
- Living Off The Land Binaries (LOLBAS)
- Code signing tools, sandbox evasion scripts
- MITRE ATT&CK Navigator, Threat Actor TTP mappers

11 AI for Red Teaming

- Gyoithon (web intelligence via AI)
- AInjection (AI-assisted SQLi)
- LLM-based recon tools (custom GPT wrappers)
- Deepfake generators: Descript, DeepFaceLab, Wav2Lip
- RAG pipeline simulators, LangChain, Haystack
- Prompt injection testers, RAG threat modeling scripts

INFOSECTRAIN
Educate. Excel. Empower.

Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on