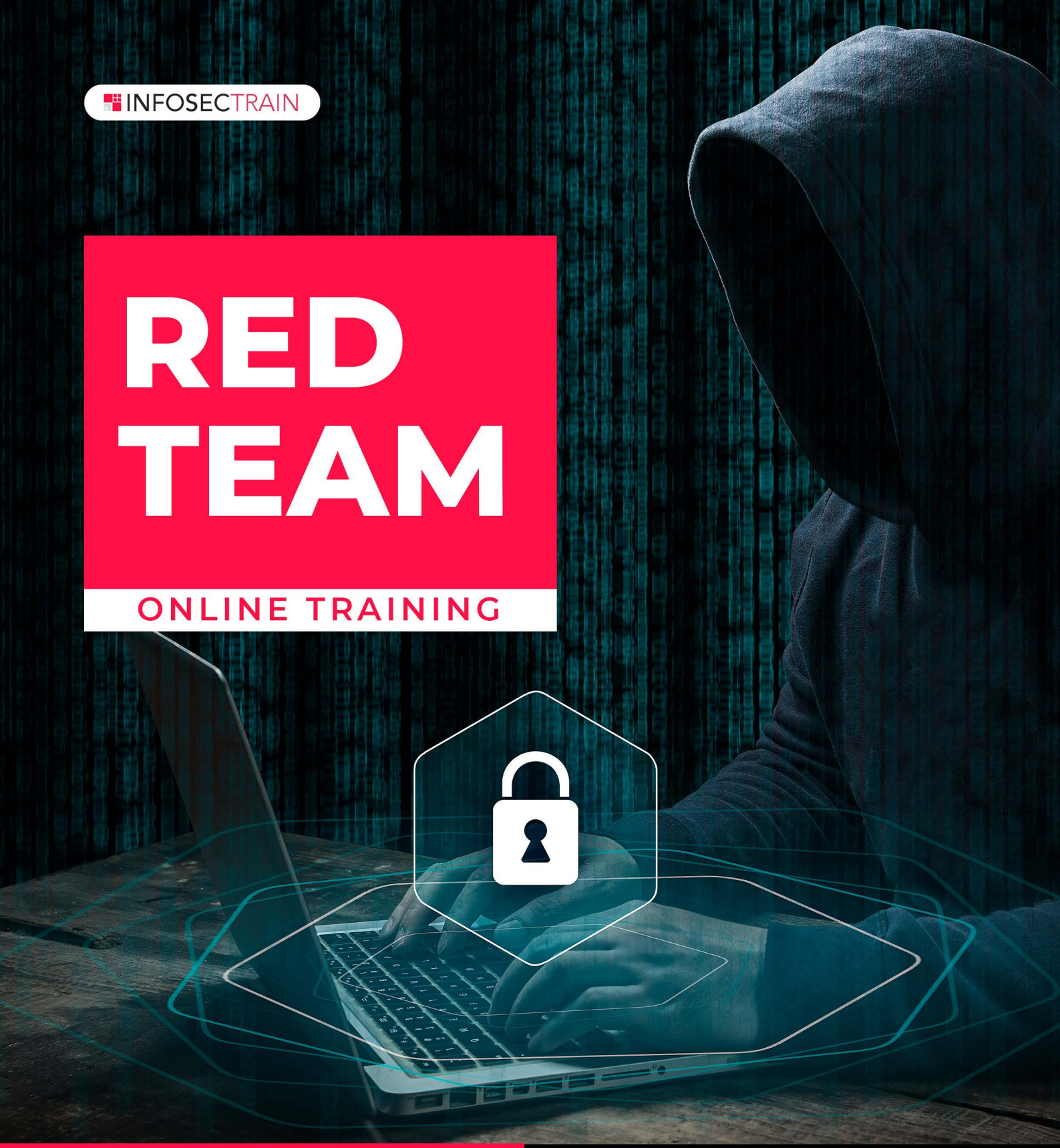
INFOSECTRAIN

RED TEAM

ONLINE TRAINING



- Network Pentest
- OS Pentest
- Web- Application Pentest
- Cloud Pentest
- Hands on RedTeam Assessment

COURSE HIGHLIGHTS

- 60 Hours of Instructor-led Training
- Certified & Highly Experienced Trainers
- Access to the recorded sessions
- Different Learning Modes to Choose from

www.infosectrain.com

sales@infosectrain.com

INFOSECTRAIN

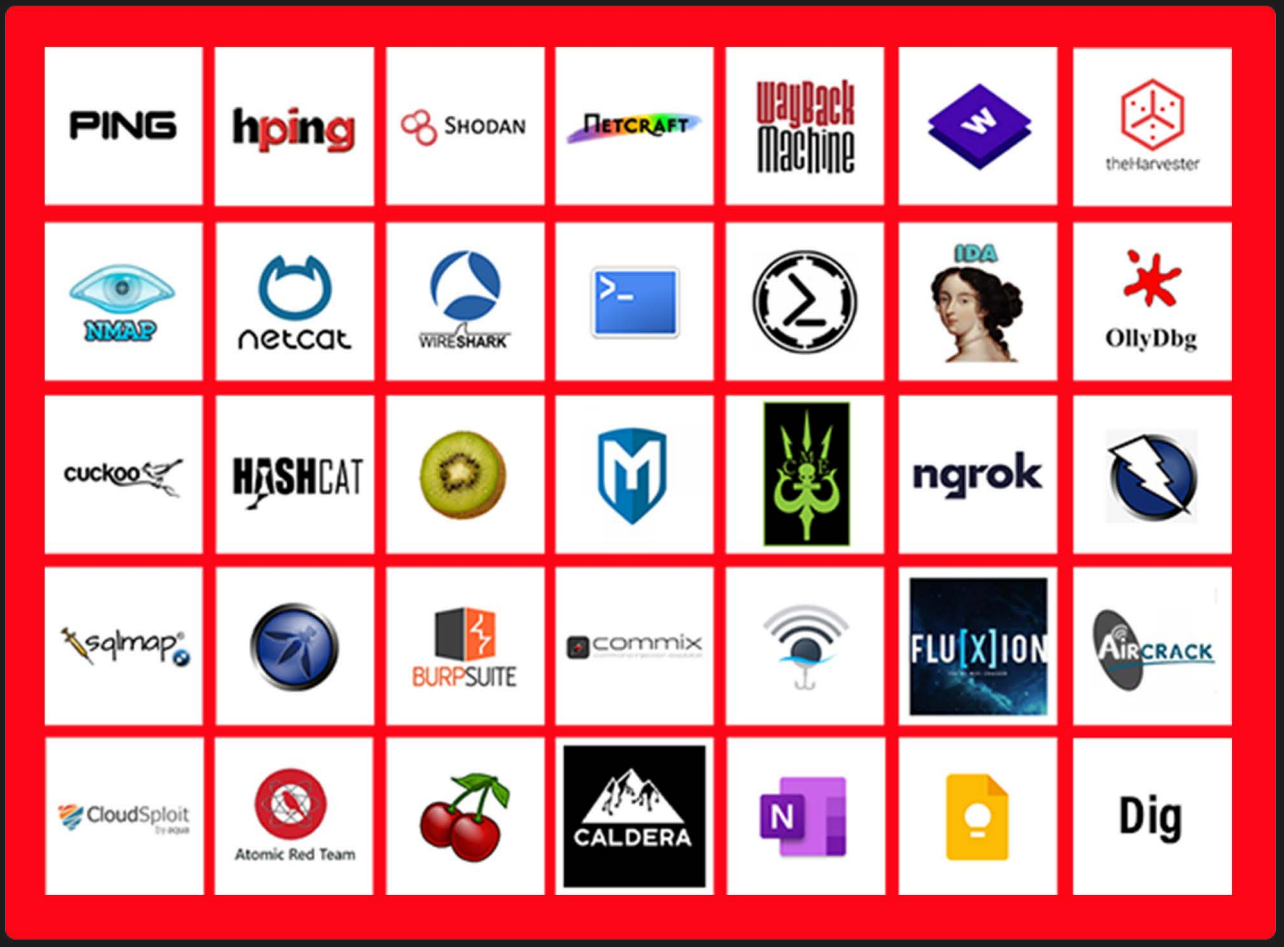
LEARNING PATH

LEARNING PATH

- Introduction to Pen-Testing
- Hands On with Linux
- Scripting Skills
- Introduction to Red Team's Plan and Execution
- Information Gathering & Enumeration
- Red Team Kill Chain
- Advanced Windows Exploitation
- Binary Analysis and Exploitation
- The Metasploit Framework
- Exploiting Overflows - Linux & Windows
- Privilege Escalation
- Lateral Movement & Pivoting Techniques
- Advanced Web Attacks
- Introduction to Wireless Security
- AWS Pen testing
- MITRE ATT&CK Red Teaming
- Deliverables - Report Writing

INFOSECTRAIN

TOOLS COVERED

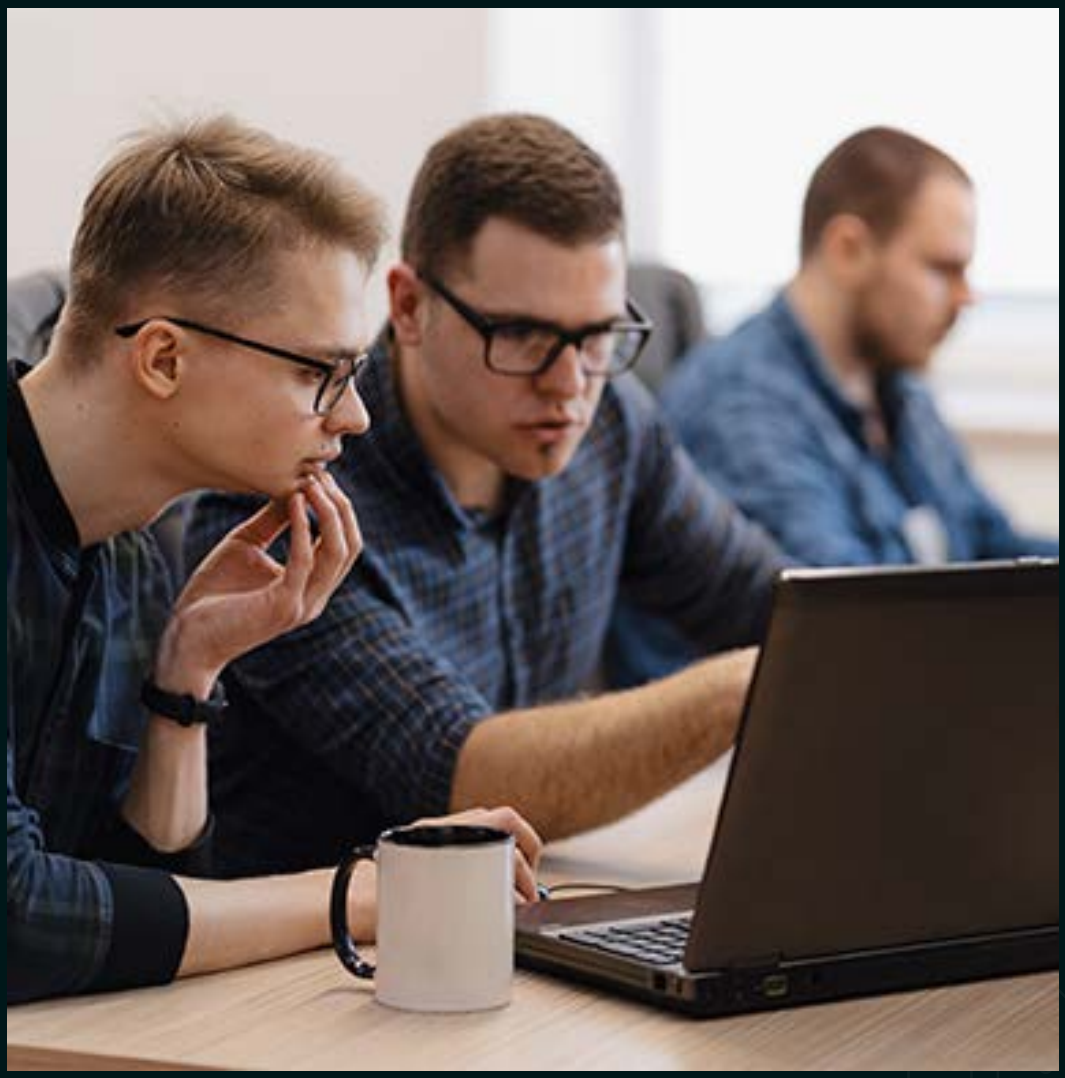


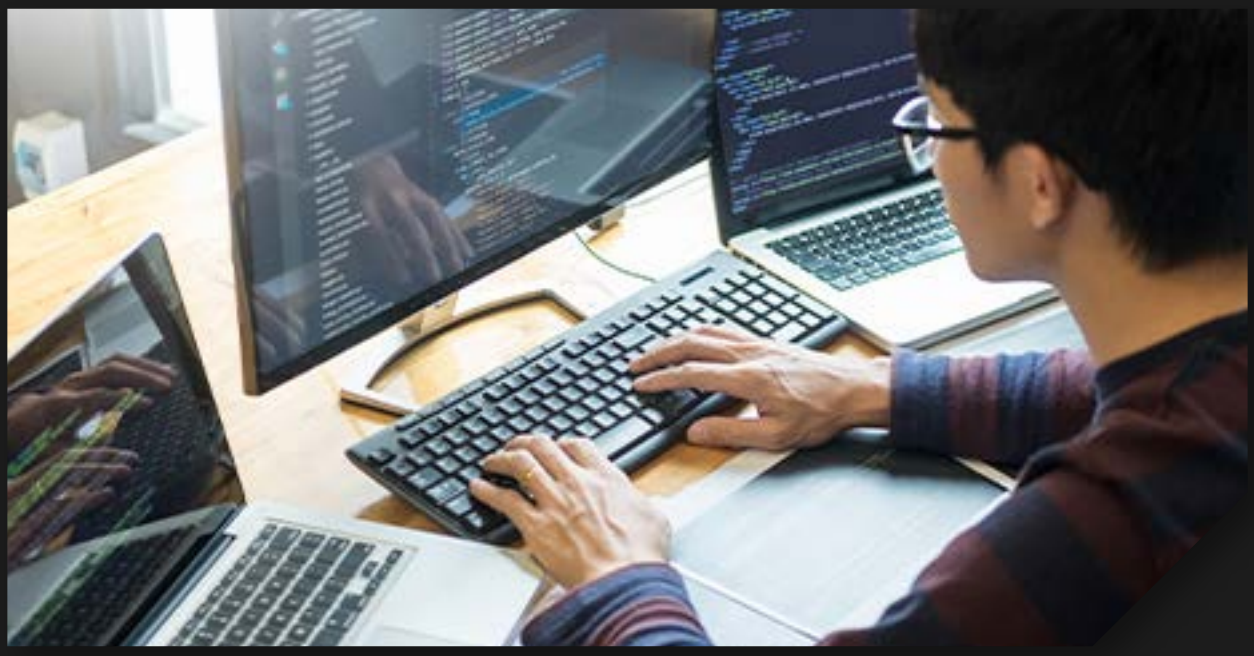
AND MORE...

INFOSECTRAIN

Introduction

The InfoSecTrain Red Team Certified Training is designed to make you an influential Red Team Hacking expert who can counter cyber threats and perform effective penetration testing to detect those threats. Our certified and structured Red Team Training course combines all the tools and techniques needed to become an effective Red Team Cyber Security expert. Learn to mimic the thought process and mindset of hackers & digital offenders and offensively safeguard sensitive IT Infrastructure with InfoSecTrain Red Team Hacking course!





Target Audience

- Red Teamers
- Bug Bounty Hunters
- Security Analysts
- Vulnerability Managers
- Penetration Testers
- IT Security Professionals
- Security Consultants
- Anyone who wants to learn the Offensive side of Cyber Security

Prerequisites

- A thorough understanding of Penetration Tests and Security Assessments
- Prior knowledge on OWASP TOP 10
- Understanding & Navigating Different OSes like Windows, Linux
- Knowledge of Active Directory
- Networking Basics
- Familiarity with PowerShell Scripts

Why Infosec Train?

Certified & Experienced Instructor

Flexible Schedule

Access to the recorded sessions

Post Training Support

Tailor Made Training

4 hrs/day in Weekend/ Weekday

COURSE OUTLINE

INFOSECTRAIN

Introduction to Pen-Testing

- Penetration Testing Benefits
- Types of Penetration Testing
- Penetration Testing Methodologies
- Law & Compliance
- Planning, Managing & Reporting

Hands On with Linux

- The Linux Filesystem
- Basic Linux Commands
- Finding Files in Linux
- Managing Linux Services
- Searching, Installing, and Removing Tools
- The Bash Environment
- Piping and Redirection
- Text Searching and Manipulation
- Backgrounding Processes (bg)
- Jobs Control
- Process Control
- File and Command Monitoring
- Downloading Files
- Persistent Bash Customization

Scripting Skills

- Introduction to Shell
  - Script Basics
  - Global Declarations
  - Variable basics
  - Escape characters
  - Basic redirection and pipe
  - Understanding Conditions
  - Understanding Loops
  - Recursion and Nested Functions
  - Function Attributes
  - The Linux Execution Environment with Scripts
  - Restricted Shells

- Introduction to Python
  - What is Python?
  - Python: Favourite of Hackers
  - Data Types and variables
  - Control Flow and Data structure
  - Functions, Functional Programming and File Handling
  - Exception Handling
  - Creating Managing File and Directory Access
  - Raw Socket basics
  - Socket Programming with Python
  - Servers and Clients architecture
  - Creating Sniffers (wired and wireless)
  - Creating packet injector

Introduction to Red Team's Plan and Execution

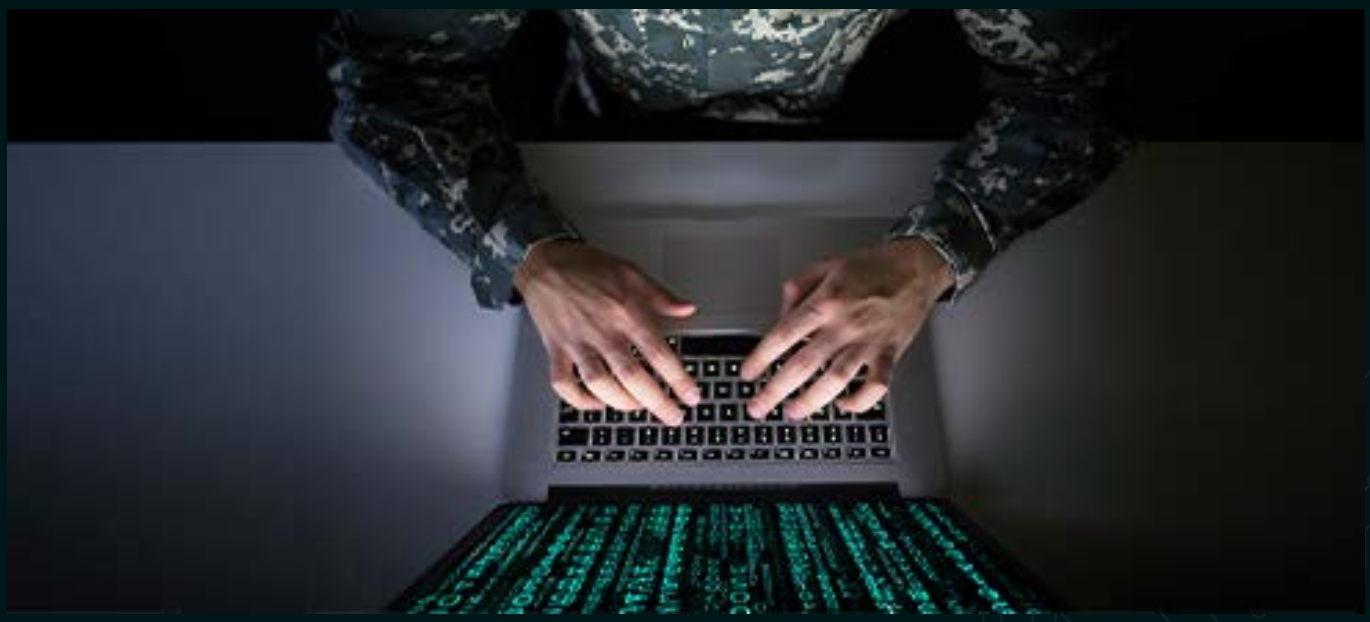
- What is Red Teaming?
- Red Team Attack Lifecycle (Phases)
- Red Team Infrastructure
- Enterprise Environment Overview
- Technologies Exploitation in Red Teaming
  - Web Technology
  - Network Technology
  - Physical Red Teaming
  - Cloud Technology
  - Wireless
- Why organizations need Red Team?
- Red Team Exercise Execution

Information Gathering & Enumeration

- Types of Information Gathering
- OSINT: Case Study
- Extensive OSINT Enumeration
- Google Search
- Google Hacking
- User Enumeration & Phishing
- Forward Lookup Brute Force
- Reverse Lookup Brute Force
- DNS Zone Transfers
- Port Scanning
  - Null Sessions
- Enum4Linux
- VRFY Script
- Python Port

Red Team Kill Chain

- Initial Access & Delivery
- Weaponization
- Command & Control
- Credentials Dumping
- Lateral Movement
- Establishing Persistence
- Data Exfiltration



Advanced Windows Exploitation

- Operating System and Programming Theory
- Win32 APIs
- Windows Registry
- What are Macros?
- Creating Dangerous Macros using Empire
- Microsoft Office Phishing using Macros
- Executing Shellcode in Word Memory
- PowerShell File Transfers
- VBA Shellcode Runner
- PowerShell Shellcode Runner
- Reflection Shellcode Runner in PowerShell
- Client-Side Code Execution with Windows Script Host
- Credential Replay Attacks
- Credential Discovery
- Hashing Concept
  - Pass the Hash (PTH)
  - Kerberoasting and AS-REP Roasting
  - Pass the Ticket (PTT)

Binary Analysis and Exploitation

- WinDbg and x86 Architecture
- Introduction to x86 Architecture
- Introduction to Windows Debugger
- Accessing and Manipulating Memory from WinDbg
- Introduction to IDA Pro
- Static-Dynamic Analysis Synchronization
- Double Pivoting
- Windows Defender Exploit Guard
- Binary diffing with BinDiff 5
- Visualizing code changes and identifying fixes
- Reversing 32-bit and 64-bit applications and modules

The Metasploit Framework

- Exploring Metasploit Framework
- Using Metasploit Auxiliary
- Using Exploit Modules
- Staged and Non-Staged Payloads
- Working with Multi Handler
- Working with Meterpreter Session

Exploiting Overflows – Linux & Windows

- Stack Overflows Introduction
- A Word About DEP, ASLR, and CFG
- Replicating the Crash
- Controlling EIP
- Stack Overflows and ASLR Bypass
- ASLR Introduction
- ASLR Implementation
- ASLR Bypass Theory
- Windows Defender Exploit Guard and ASLR
- Understanding SEH
- Exploiting SEH Overflows
- Understanding the low fragmentation heap
- Heap Overrun/Overflow

Privilege Escalation

- Windows Privilege Escalation
  - Understanding Windows Privileges and Integrity Levels
  - User Account Control (UAC) Bypass: fodhelper.exe Case Study
  - Insecure File Permissions: Serviio Case Study
  - Leveraging Unquoted Service Paths
  - Windows Kernel Vulnerabilities: USBPcap Case Study
- Linux Privilege Escalation
  - Understanding Linux Privileges
  - Insecure File Permissions: Cron Case Study
  - Insecure File Permissions: /etc/passwd Case Study
  - Kernel Vulnerabilities: Case Study

Lateral Movement & Pivoting Techniques

- Lateral Movement and Network Pivoting
- File-Less Lateral Movement Methodologies
- Understand Local, Remote Port Forwarding Using Chisel, various proxies etc
- Multi-level in-depth network pivoting in Windows & Linux OS
- Lateral Movement with SSH
- SSH Hijacking Using SSH-Agent and SSH Agent Forwarding

Advanced Web Attacks

- OWASP Standards
- Broken Web Application
- ATutor
- Web Traffic Inspection using Burpsuite
- Atmail Mail Server Appliance: from XSS to RCE
- Session Hijacking
- Session Riding
- Authentication Bypass and RCE
- Injection Attacks
- ATutor LMS Type Juggling Vulnerability
- Attacking the Loose Comparison
- Magic Hashes
- JavaScript Injection Remote Code Execution
- Cookie Deserialization RCE
- Server-Side Template Injection
- XSS and OS Command Injection
- Advanced XSS Exploitation
- RCE Hunting

Introduction to Wireless Security

- Cracking Wireless Encryptions
- Cracking WEP
- Cracking WPA, WPA2 & WPA3
- WIFI-Phishing
- Dos Attack: WIFI Jamming
- Securing WAP
- Auditing and Reporting

AWS Pen testing

- Building and setup AWS pen testing Environment
- Exploiting S3
- Understanding and exploiting Lambda Services
- Testing IAM privileges
- Case study For Capital One Attack.

MITRE ATT&CK Red Teaming

- Follow Mitre ATT&CK Framework
- Playing with Mitre
- Testing with Caldera
- Atomic Red Team Test for MITRE-ATT&CK
- Utilizing LOLBAS for stealth persistence & Data Exfiltration

Deliverables - Report Writing

- Defining Methodology
- Types of Reports
  - Executive Summary
  - Detailed Reports
- Adding Proof of Concept
- Creating Drafts
- Risk Rating Factors
- Automating Reports
- Report Writing Tools

www.infosectrain.com | sales@infosectrain.com