ONLINE TRAINING

# REDTEAM

Hacksudo®

- Network Pentesting
- OS Pentesting
- Web-Application Pentesting
- Cloud Pentesting
- Hands on ReadTeam Assm.

## Course Highlights

- 60 Hours of Instructor-led Training
- Access to the Recorded sessions

info@hacksudo.com

www.hacksudo.com

# About Company

## Industrial

Hack Sudo is a global enterprise for IT Security Training & Security Consultancy that focuses on solving IT Security issues. It is trusted standard for companies to protect their Products, Brand & Confidential information from various types of Cyber Attacks.

## Corporation

We provide training and education in the field of Ethical Hacking , VAPT , ReadTeam , Development & Information Security to the students as well as the corporate. These trainings can be provided at client locations and at Hack Sudo Centers.

## Learning Path

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

# 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

# COURSE OUTLINE

## 1. Introduction to Pen-Testing

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

## 2. 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

## 3. 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
- Why organizations need Red Team?

- Red Team Exercise Execution

1. Web Technology
2. Network Technology
3. Physical Red Teaming
4. Cloud Technology
5. Wireless

- Why organizations need Red Team?
- Red Team Exercise Execution

## 4. 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

1. Null Sessions
2. Enum4Linux
3. VRFY Script
4. Python Por

## 5. Red Team Kill Chain

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

## 6. 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

1. Pass the Hash (PTH)
2. Kerberoasting and AS-REP Roasting
3. Pass the Ticket (PTT)

## 7. 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

## 8. Privilege Escalation

- Windows Privilege Escalation

1. Understanding Windows Privileges & Integrity Levels
2. User Account Control (UAC) Bypass:fodhelper.exe Case Study

3. Insecure File Permissions: Serviio Case Study
4. Leveraging Unquoted Service Paths
5. Windows Kernel Vulnerabilities: USBPcap Case Study

- Linux Privilege Escalation

1. Understanding Linux Privileges
2. Insecure File Permissions: Cron Case Study
3. Insecure File Permissions: /etc/passwd Case Study
4. Kernel Vulnerabilities: Case Study

## 9. 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

## 10. 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

## 11. Introduction to Wireless Security

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

## 12. AWS Pen testing

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

## 13. 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

## 14. Deliverables - Report Writing

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

red team