

## ABOUT THE COURSE

Become a Software Security Professional with advanced skills in software security and transform your career in 10 weeks. The hands-on program teaches you secure software development lifecycle processes and methodologies using the latest tools to build and assess applications.

The training covers SDLC process and security deliverables such as Requirement Analysis, Security Architecture, and Design, Threat Modeling, 3<sup>rd</sup> Part Component Reviews, DAST, SAST, Vulnerability Assessment, Penetration Testing, Fuzzing, Exploit Development, and Risk Assessment.

**INSTRUCTOR-LED**

**DURATION: 80 HOURS**



## WHO SHOULD ATTEND ?



**DARKRELAY**

- Senior Penetration Testers
- Senior Security Engineers
- Senior Web Developers
- Senior Security Researchers
- Security Architects
- Engineering Managers
- Directors
- Software Architects

## SECURE SOFTWARE DEVELOPMENT PROFESSIONAL

**For more information**

Visit: [www.darkrelay.com](http://www.darkrelay.com)

Email: [training@darkrelay.com](mailto:training@darkrelay.com)



## Course Outline

### Software Security and SDLC

- Integrating Security into SDLC
- SDLC Phases
- Roles and Responsibilities
- Security Deliverables in SDLC
- Secure SDLC Drivers: Compliance and Standards

### Security Requirements Analysis

- Case Study: Student Information Management System(SIMS)
- SIMS Requirements Analysis
- SRS

### Architecture and Design Reviews

- Case Study: SIMS
- SIMS Architecture Review
- SDD

### Threat Modelling

- Microsoft Threat Model
- Case Study: SIMS
- SIMS Threat Modelling

### 3rd Party Component Analysis

- Introduction to 3rd party assessment
- Case Study: SIMS
- SIMS 3rd party Component Analysis

### Risk Assessment

- Introduction to Risk Assessment
- Case Study: SIMS
- SIMS Risk Management

### Penetration Testing

- Lab Setup
- Introduction to Kali Linux
- Linux Commands



- Kali Tools
- Introduction to Python
- Introduction to Bash
- Bash Automation
- Services in Kali

### Recon

- Active
- Passive

### Enumeration

- SMTP
- SNMP
- DNS
- NFS
- SMB
- FTP
- HTTP
- SSH
- TFTP







### Vulnerability Scanning

- Nessus
- Nmap

### Attacking Web Applications

- OWASP Top Ten
- SANS Top 25
- CWE
- Web Application Enumeration
- Injection Attacks
- File Inclusions
- Client Side Attacks
- Server Side Attacks
- File Upload Bypass

### DevSecOps

- CI/CD
- Gitlab

### Web Application Scanning (DAST)

- OWASP ZAP
- Burp Suite Pro

### Static Application Security Testing (SAST)

- XSS
- Input Validation
- SQL Injection
- OS Command Injection
- File Inclusion
- Buffer Overflow

### Thick Client Penetration Testing

- Introduction and Methodology
- Attack Surface Analysis
- DLL Hijacking
- EXE Hijacking
- Buffer Overflow
- Information Leakage
- IFEO
- Registry Attacks



### Antivirus Evasion

- Bad Byte Technique
- Avoiding Detectable Functions
- PowerShell Bypass
- Bypass Windows Defender

### Memory Corruption Bugs

- Introduction to x86
- Fuzzing
- Immunity Debugger
- GDB
- Windows Buffer Overflow
- Linux Buffer Overflow

### Exploit DB

- Choosing Exploits
- Fixing Exploits
- Updating Payload
- Compile & Deliver Exploit
- Execute Exploit



## Metasploit Framework

- Introduction
- Modules
- Payloads
- MsfVenom
- Meterpreter
- Multi Handler
- Post Exploitation

## Privilege Escalation

- Windows Privilege Escalation
- Linux Privilege Escalation

## Password Attacks

- Brute force with Wordlists
- Password Cracking
- Capturing Password Hashes
- Pass the Hash Attack



## Post Exploitation

- Autoroute
- Pivoting
- Lateral Movement

## Tunneling & Port Forward

- Local Port Forward
- Remote Port Forward
- Dynamic Port Forward

## Penetration Testing Labs

- Vuln Hub
- Build your lab

## Report Generation

- Maintaining Notes
- Creating Report Templates
- Generating Reports

## Cryptography

- Public Key Cryptography
- Weak SSL/TLS Ciphers
- Sensitive Information Over Unencrypted Channel

## Active Directory Attacks

- Introduction
- AD Enumeration
- AD Authentication
- AD Vulnerabilities
- AD Persistence
- Lateral Movement





## ABOUT DARKRELAY

DarkRelay is lead by Cybersecurity veterans who are SANS 760, GXPN, GPEN, OSCP, OSCE, CISSP certified with more than 16 years of experience in cyber security research and development. DarkRelay uses their perspective to build valuable security programs for the clients.

We are providing world class cyber security consulting and training services with a focus on offensive security training such as Web Application Security, Advanced Penetration Testing, Bug Bounty, Vulnerability Assessment, Fuzzing and Exploit Development.



## OUR TRAININGS

- Practical Penetration Testing
- Attacking Web Applications
- Fuzzing & Exploit Development
- Red Teaming
- Software Development Security
- Ethical Hacking
- Advanced Penetration Testing
- Vulnerability Assessment
- Malware Analysis
- Cloud Security



**DARKRELAY**

## SECURE SOFTWARE DEVELOPMENT PROFESSIONAL

**For more information**  
Visit: [www.darkrelay.com](http://www.darkrelay.com)  
Email: [training@darkrelay.com](mailto:training@darkrelay.com)