ABOUT THE COURSE

Ready to push yourself further into learning the art of cutting-edge hacking skills? If yes, the Advanced Penetration Testing course is the right course for you. Whether you are a senior penetration tester, security engineer, red teamer, or trying to better understand advanced vulnerability discovery and exploitation, enroll today!

The course covers a plethora of advanced penetration testing skills to enable you to assess and compromise Networks, Web Applications, Thick Client Applications, Operating Systems, Products, Active Directory, and Cloud Infrastructure.

INSTRUCTOR-LED

DURATION: 40 HOURS

WHO SHOULD ATTEND ?

- Penetration Testers
- Security Engineers
- Web Developers
- Information Security Engineers
- Security Researchers
- Security Architects
- Engineering Managers
- Security Interns

DARKRELAY

ADVANCED PENETRATION TESTING

For more information
Visit: www.darkrelay.com
Email: training@darkrelay.com

Course Outline

Introduction

- Approach & Methodology
- Threat Model Driven Penetration Testing
- MITRE ATT&CK

Network Attacks

- NAC Bypass
- OSPF Exploitation
- DDoS

Macro Attacks

- Introduction to Macros
- Undetectable Macro Malware
- Malware Delivery via Macro
- Attack via Microsoft Office Applications

Antivirus Evasion

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

Attacking Web Applications

- SSI
- Insecure Deserialization
- SSRF
- XXE
- No SQL
- OS Command Injection

Thick Client Penetration Testing

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

Active Directory Attacks

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

Fuzzing

- Introduction to AFL
- Fuzzing Source
- Fuzzing Binary
- Crash Analysis
- Exploit Analysis

Memory Corruption Bugs

- Fuzzing
- Windows Buffer Overflow
- Linux Buffer Overflow
- ASLR Bypass
- 3 Byte Overwrite

Advanced Privilege Escalation

- Hunting for Kernel Exploits
- Compiling Kernel Exploits
- Executing Kernel Exploits
- Token Manipulation
- Abusing DPAPI
- AD Privilege Escalation

Advanced Pivoting and Lateral Movement

- Pivoting Using Metasploit
- Internal Network Scanning
- Lateral Movement

CVE Case Studies

- Log4j
- Exif tool RCE
- Heartbleed
- Eternal blue
- PHP RCE
- Dirty Cow

CTF

- ROP Chaining
- Canary Bypass
- NX Bypass
- Reverse Engineering
- Crypto Challenges

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

ADVANCED PENETRATION TESTING

For more information
Visit: www.darkrelay.com
Email: training@darkrelay.com