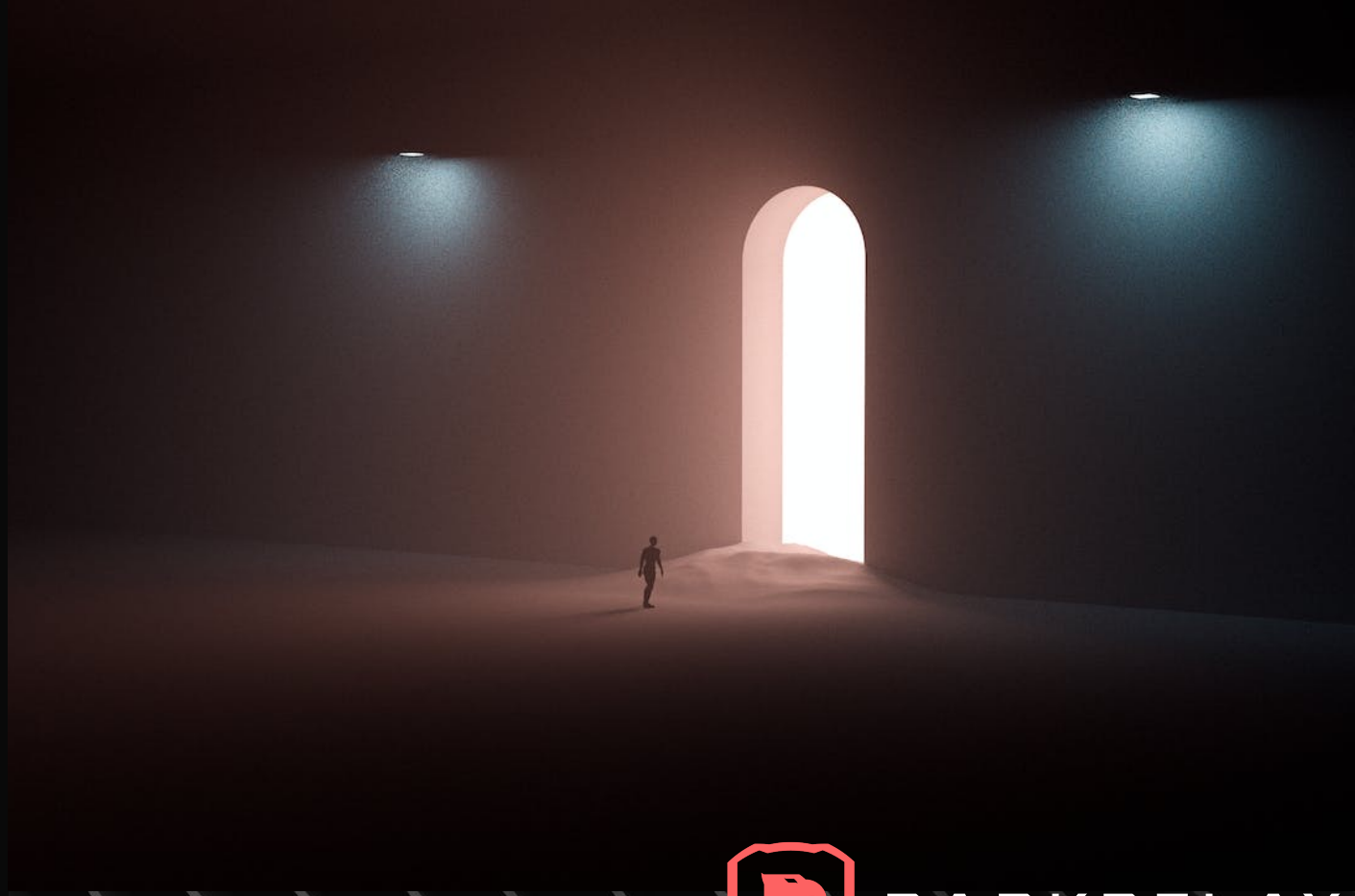
# ABOUT THE COURSE

The Professional Penetration Tester (**PENT**) training is our zero-to-hero course for intermediate to advanced understanding of offensive cyber security, equipping our students to learn professional grade Penetration Testing & Vulnerability ssessment (VA) skills by employing a practical and hands on approach to practice network and application enumeration, vulnerability scanning, exploitation, privilege escalation, and lateral movement while learning the soft skills needed to make it in offensive security. The PENT course helps you identify, detect, and exploit any vulnerability in the target applications, networks, thick client, and infrastructure.

**Instructor- Led Online**

Duration: 40 Hours



DARKRELAY

## WHO SHOULD ATTEND ?

- Penetration Testers
- Security Engineers
- Security Researchers
- Bug Hunters
- Information Security Engineers
- Engineering Managers
- Web Developers
- QA Engineers
- Software Developers

# Professional Penetration Tester (PENT)

**For more information**

**Visit**: www.darkrelay.com
**Email**: training@darkrelay.com

# COURSE OUTLINE

### Introduction

- Introduction to Cybersecurity
- Network Fundamentals
- Introduction to Penetration Testing
- Penetration Testing Methodology
- Lab Setup
- Introduction to Kali Linux & Tools
- Bash for Pentesters
- Python for Pentesters
- Note-taking: Chery Tree

### Information Gathering

- Passive Reconnaissance
- Active Reconnaissance

### Enumeration

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

### Vulnerability Scanning

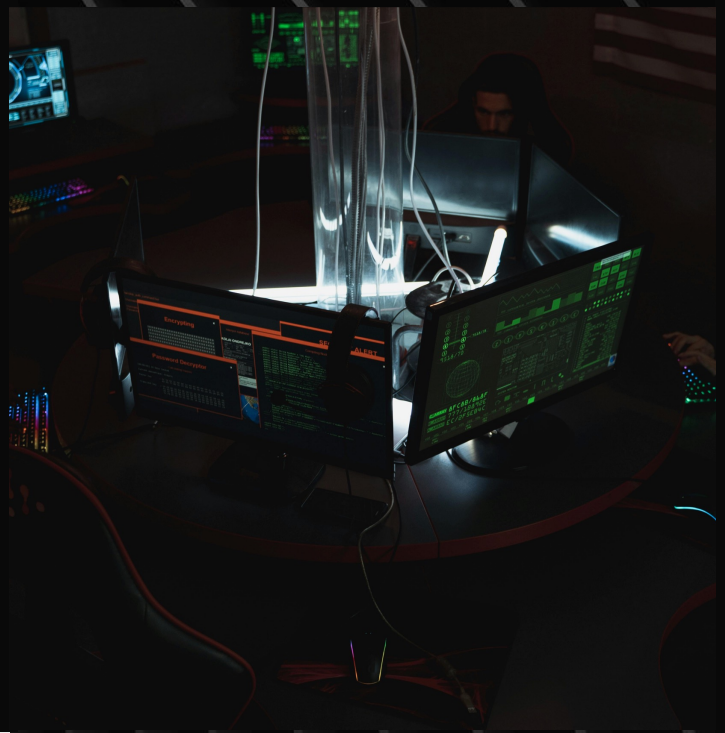
- Nessus
- CVSS Scoring

### Web Application Scanning (DAST)

- Introduction to ZAP & Burp Suite
- OWASP ZAP
- Burp Suite Pro

### Attacking Web Applications

- OWASP Top Ten
- CWE/SANS Top 25
- OWASP ASVS
- OWASP Testing Guide & Checklist
- Web Application Enumeration



- Injection Attacks
- File Inclusions
- Client-Side Attacks
- Server-Side Attacks
- File Upload Bypass

### Web API Attacks

- Injection Attacks
- IDOR
- Mass Assignment
- Open Redirection

### Buffer Overflow

- Introduction to x86
- Immunity Debugger
- Fuzzing
- Stack Overflow
- Buffer Overflow in Windows
- Buffer Overflow in Linux

### Exploit DB

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

### Metasploit Framework

- Introduction
- Modules
- Payloads
- MSFvenom
- Meterpreter
- Case Study: EternalBlue

### Privilege Escalation

- Windows Privilege Escalation
- Linux Privilege Escalation


### Password Attacks

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

### Tunnelling & Port Forwarding

- Local Port Forwarding
- Remote Port Forwarding
- Dynamic Port Forwarding

### Post Exploitation

- Autoroute
- Pivoting
- Lateral Movement

### Active Directory Attacks

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

### Penetration Testing Labs

- Setting up Vulnerable Machines
- Building containerized Vulnerable Machines

### Report Generation

- Penetration Testing Report Template
- Writing Professional Reports

### Conclusion

- Next Steps
- Certification Exam
- Building a better Resume
- Career Guidance

# ABOUT DARKRELAY

Founded in 2019, DarkRelay is led by Cybersecurity veterans who are **SANS 760, GXPN, GPEN, OSCP, OSCE**, and **CISSP** certified with 20+ years of experience in cyber security research and development. DarkRelay Security Labs uses global its perspective to build valuable security programs for its students.

Whether you are a beginner or an experienced cyber security professional, our training will address your every learning need, challenge, and career goal.

DARKRELAY

# 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

## Professional Penetration Tester (PENT)

**For more information**

**Visit**: www.darkrelay.com
**Email**: training@darkrelay.com