



RUN & GUN: NETWORK PENETRATION TESTING

Our aim is to train Information Security Professionals, IT Professionals or anyone interested in cultivating the **right skills and knowledge** to learn the process of **network penetration testing, network vulnerability assessments**, and ways to protect against cyberattacks.

Online Training	Hands-on Training	Right Methodology
You will learn and improve your Network Penetration Testing skills via Online Training using Microsoft Teams Meeting.	We will provide all the necessary tools to download for free and give you details to prepare one day before the training starts. There is no hidden or additional cost involved.	Learn our Network Penetration Testing methodology refined by experts with years of experience conducting Web Penetration Testing projects for thousands of clients.
Top Rated Trainer	Certificate of Attendance	100% Fully Claimable
80% practical hands-on training with a focus on skill development from a top-rated IT security expert trainer .	Get an e-certificate of attendance from leading Cybersecurity training provider.	Training is fully claimable under HRD Corp. (Human Resource Development Corporation).

be confident your system is in safe hands.



Run & Gun: Network Penetration Testing is two days of live virtual training with an emphasis on 90% practical hands-on training that focuses on developing network penetration testing skills.

In this training, we shall learn the process of network penetration testing, network vulnerability assessments and ways to protect against incoming threats in the manner of virtual hands-on training. **Optional 2-hour mentoring sessions** are included to help participants hone and practice their skills.

It's recommended that participants have prior experience setting up, managing, or securing an organization's network.

COURSE OUTLINE

Day 1

Module 1: Network Security - Overview

- 1.1 Policies, Standards, Procedures, Baselines, Guidelines
- 1.2 Security Models

Module 2: Network Protocols and Analysis

- 2.1 Internet Protocol (IP)
- 2.2 IP Addressing
- 2.3 Transmission Control Protocol (TCP)
- 2.4 Internet Control Message Protocol (ICMP)
- 2.5 Internet Group Management Protocol (IGMP)
- 2.6 Address Resolution Protocol (ARP)
- 2.7 Dynamic Host Configuration Protocol (DHCP)
- 2.8 User Datagram Protocol (UDP)
- 2.9 Domain Name Service (DNS)
- 2.10 Lightweight Directory Access Protocol (LDAP)
- 2.11 Telnet
- 2.12 File Transfer Protocol (FTP)
- 2.13 Trivial File Transfer Protocol (TFTP)
- 2.14 Simple Mail Transfer Protocol (SMTP)
- 2.15 Post Office Protocol (POP)
- 2.16 Internet Message Access Protocol (IMAP)
- 2.17 Simple Network Management Protocol (SNMP)
- 2.18 Voice over IP (VoIP)
- 2.19 Session Initiation Protocol (SIP)
- 2.20 Hyper Text Transfer Protocol (HTTP)
- 2.21 HTTPS

Module 3: Network Security Threats

- 3.1 Spam
- 3.2 Malware
- 3.3 Worm
- 3.4 Trojan
- 3.5 Drive-by download
- 3.6 Spyware
- 3.7 Keystroke logging
- 3.8 Adware
- 3.9 BOT
- 3.10 Social engineering
- 3.11 Phishing
- 3.12 Tabnabbing
- 3.13 Email spoofing
- 3.14 Password cracking
- 3.15 Denial-of-Service attack
- 3.16 Buffer Overflow
- 3.17 Network scanning
- 3.18 Information gathering
- 3.19 Port Scanning
- 3.20 Vulnerability Scanning

Day 2

Module 4: Network Vulnerability Assessment

- 4.1 Scan Types
- 4.2 Introduction to Vulnerability Assessment
- 4.3 Introduction to Metasploit

Module 5: Password Cracking

- 5.1 Introduction
- 5.2 Types of password cracking techniques
- 5.3 Password cracking with Hydra/ Ncrack
- 5.4 Generating custom password dictionaries

Day 1: 9am to 1pm

Day 2: 9am to 1pm

Day 2: 2pm to 4pm (optional)

Platform: Microsoft Teams Meeting

Duration: 8 hours + 2 hours mentoring (optional)

✓ **Certificate of Attendance**

Who Should Attend

- Network Administrator
- System Administrator
- IT Executive
- Information Technology Professionals
- Information Security Professionals
- Computer Network Professionals
- Other Business or IT Professionals who are responsible for Network Security and Data Protection.

- ✓ Trained by **award-winning Cybersecurity training provider** with top rated IT security specialist.
- ✓ **80% practical hands-on training** with focus on skill development to successfully learn how to conduct Network Penetration Testing.
- ✓ Get an **e-certificate of attendance** from leading Cybersecurity training provider.
- ✓ Training is **100% fully claimable** under HRD Corp. (Human Resource Development Corporation).
- ✓ Materials and **technical support provided** - Training guide, supporting materials and training access link.



www.condition-zebra.com

Condition Zebra (M) Sdn Bhd (701012-T)

Level 3-10, Block F, Phileo Damansara 1,
Jalan 16/11 Off Jalan Damansara,
46350 Petaling Jaya, Selangor, MY.

Email: info@condition-zebra.com
Phone: +603-7665 2021