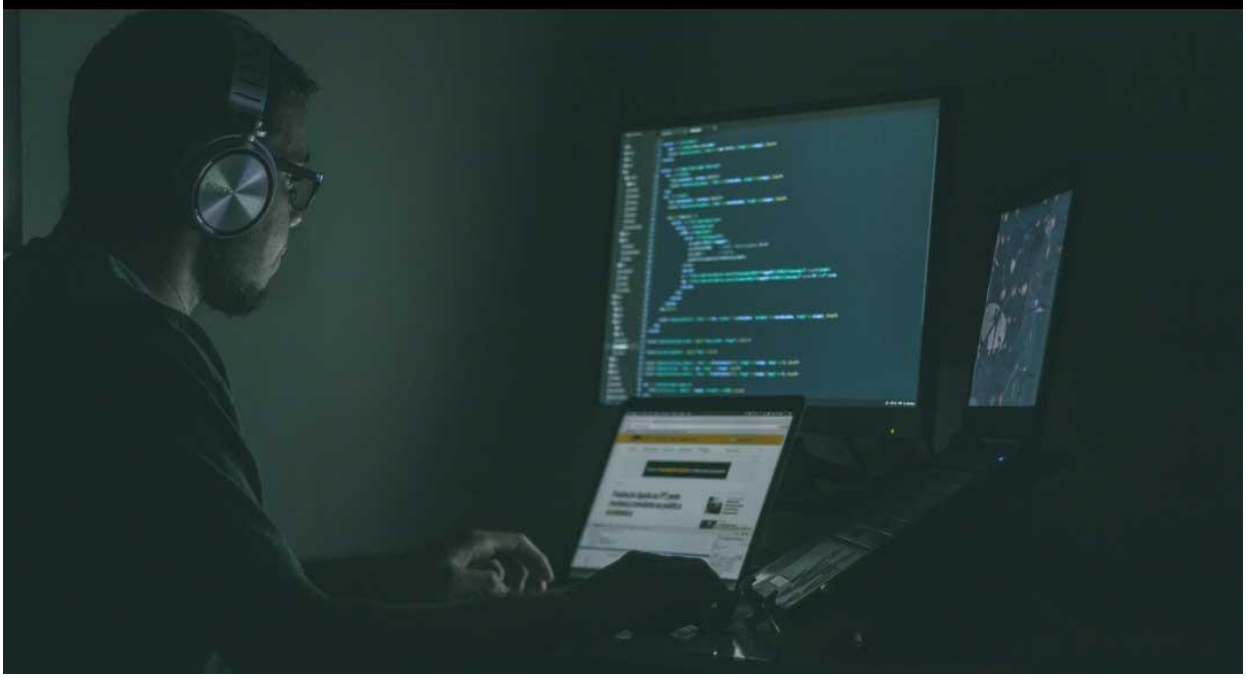
CONDITION ZEBRA

Beyond IT Security Training. We Train Differently

RUN & GUN: NETWORK PENETRATION TESTING



Cyber Security Online Training 2022

Run & Gun: Network Penetration Testing

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.

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

Training Details

Day 1: Monday, 9am to 1pm
Day 2: Tuesday, 9am to 1pm
Day 2: Tuesday, 2pm to 4pm (optional)
Platform: Microsoft Teams Meeting
Duration: 8 hours (4 hours a day) plus 2 hours mentoring session (optional)
Course Fee: **RM700 (*subject to 6% SST)**

[NOTE]: This is a paid training with *subject to HRDF claim for qualified HRDF contributing companies.

Benefits

- Trained by award-winning Cybersecurity Training Provider with Top Rated Network Pentester.
- 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.
- 100% HRDF (Human Resource Development Fund) claimable under SBL-KHAS
- Materials and technical support provided - Training guide, supporting materials and training access link.

What you will learn?

- The simplest way to master the fundamental of network security by learning from a top-rated Network Penetration Tester.
- Learn our 8-step Network Penetration Testing methodology refined by experts with years of experience conducting Pentest projects for thousands of clients.
- What are the latest 20 most dangerous Network Security Threats? Learn how to protect your company network against these threats.
- How to do passive and active information gathering like a Professional Hacker would do before launching their attacks.
- The secrets to avoiding network-based attacks that hackers don't want you to know about!
- What NEVER to do best practices so your network doesn’t expose high-security vulnerabilities that can be easily exploited by hackers.
- Do you know that most successful hackers use social engineering as their toolkit? Learn the techniques to stop them in their track.
- Do you know that email phishing is one of the techniques used by 80% of hackers? Learn more about this technique and how to protect against this!
- WARNING: We are not responsible for your action if you learn this. We will demonstrate how to easily crack passwords using Hydra / Ncrack for educational purposes.

Who should attend?

- Information Technology Professionals
- Information Security Professionals
- Computer Network Professionals
- Other Business or IT Professionals, who are responsible for IT or Network Security

Run & Gun: Network Penetration Testing Course Outline

Day 1 – Module 1 and 2

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

Day 1 – Module 3

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 and 5

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