In Network Penetration Testing training, we shall learn the process and conduct of network penetration testing in the manner of virtual hands-on training. This is a paid training with ***subject to HRDF claim** for qualified HRDF contributing companies.

Run & Gun: Network Penetration Testing

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

Run & Gun: Network Penetration Testing Course Outline

Day 1 – Module 1 to 3

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 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