

Beyond IT Security Training.
We Train Differently

Network Security & Penetration Testing



We assess your network to find vulnerability

Train you to fix

Secure your network

What is the uniqueness?

How will you learn?

How will it benefit you?

Pre-training

During the training

Post-training

Security Assessment with Analysis Report

No other training providers did this before and we are the first! Prior to the training, our security engineers will conduct a security assessment and provide a security analysis report on your network.

Understand Your Network

You will get a clear understanding on the security and the hidden risks of your network.

Hands-on Session

You will learn and improve your technical skills to test and secure a network.

Solution-Driven

You will have the opportunity to focus and get professional consultation from trainer based on the challenges you face in the security analysis report on your network.

Live Hacking and Penetration Testing

You will practice and sharpen your skills by applying it in live network.

Skills Application

You will be able to understand and fix the vulnerabilities of your network listed in the security analysis report.

Master Network Security

You will be able to master advanced techniques to secure and conduct security assessment on network.

Course Description

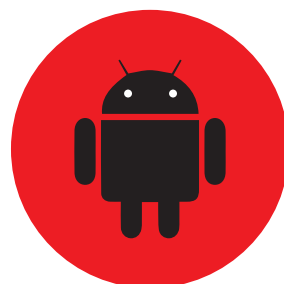
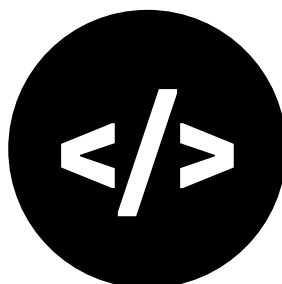
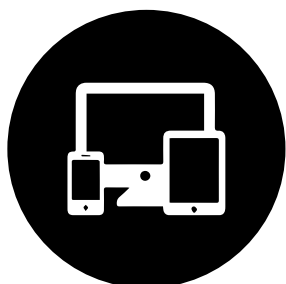
This network security training fully arms you to address the information security concerns within the organization for data protection.

You will gain in-depth understanding on the network hacking tools usage and how to conduct the network penetration testing in a careful and professional manner.

This training will also demonstrates various network hacking techniques as well as penetration testing methodologies to help you identify network security vulnerabilities.

Course Outline

- Overview of Network Security
- Network Protocol & Analysis
- Network Security Threats
- Network Vulnerability Assessment
- Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)
- Firewalls
- Hardening Operating Systems and Patch Management
- Hardening Physical Security
- Application Security
- e-mail Security
- Authentication: Encryption, Cryptography and Digital Signatures
- Virtual Private Network
- Log Analysis
- Wireless Network Security
- Incident Response



Learning Outcomes

- Enable you to understand and communicate the network security risks associated with hacking and other exploits
- Discover real-world network hacking techniques and countermeasures
- Sharpen up your technical skills and learn to fix the network vulnerabilities
- Learn to perform a network penetration testing on own deployment and evaluate network security threats and possible exploits

Enable you to develop and design a secure network

- Enable you to tackle real-life scenarios and apply new skills to the job with ease

Duration

4 Days

Exam Details

Number of Questions: 50

Passing Score: 70%

Test Duration: 85 mins Exam + 5 mins NDA

Test Format: Multiple Choice

Test Delivery: PVTc (Pearson VUE Test Center)

Exam Prefix: CZ 100



Who Should Attend

System engineers, network administrators, firewall administrators, IT managers, information security professionals, penetration testers, ethical hackers and anyone who is interested in network security and penetration testing

Certified Network Security Specialist (CNSS)



VISIONCORP
smart solutions for smart people

www.visioncorp.com.my
Tel: +6 03 7665 2021
Email: service@visioncorp.com.my