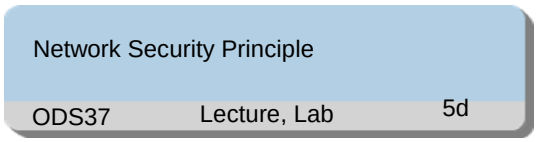
NETWORK SECURITY PRINCIPLE TRAINING

Training Path



Target Audience

Operation and maintenance engineer

Prerequisites

- Be familiar with Windows operating system
- Having a general knowledge of TCP/IP basics

Objectives

On completion of this program, the participants will be able to:

- Describe the definition of security in computers
- Describe the definition of security in networks
- Describe the definition of assurance, defense in depth and a threat
- Describe How do you define risks
- Describe the relation between security and being user friendly
- Describe what does CIATAN stand for?
- Describe security principles
- Describe security threats and risks
- Describe evil code
- Describe web security
- Describe e-mail threats
- Describe firewall, IDS and honeypot
- Describe what does CIATAN stand for?
- Describe virtual private networks
- Describe WLAN security

Training Content

ODS37 Network Security Principle

- Network Security Principles
  - What is security?
  - Terminology
  - Risks
  - Different security levels

- Security vs. user friendly
- The security process in a project
- Security policy
- Security principles

- Security Threats and Risks
  - Standards and Categorizations
  - Security Attack
  - Passive attack (Release of message contents, Traffic Analysis)
  - Active attack (Masquerade, Replay, Modification of messages, DoS)
  - Security Mechanism
  - Security Services
  - Attacker Motivation
  - Profile of an Attacker
- Evil Code
  - Malicious programs
  - Trapdoors (backdoors)
  - Trojan horses
  - Logic bombs
  - Viruses (definition, signature, prevention, example)
  - Worms
  - Zombies
  - Hoaxes
  - Modern malware
  - Virus Countermeasures
  - A Real Case
- Web Security
  - Web Browser Security (SSL/TLS, SET, 3D Secure)
  - Web Browser Security (CGI, Java Script, ActiveX, Plug-in)
  - Web Browser Security, Threats
  - Cookies, Hijacking Attack, Replay Attack, Registry Change
  - Spyware
  - Web Browser Parasite
  - Security Configuration
  - DNSSEC
- E-mail Threats

- E-mail & Protocols
- E-mail Attachment
- Man in the Middle Attack
- Phishing
- Spam (Motivation, technique, filters, solution, prevention)

- Firewall, IDS and Honeypot
  - Types of attacks
  - Tools and techniques for hacking
  - What hackers want to break?
  - Countermeasures
  - Firewalls
  - Firewalls, types and comparison
  - Intrusion Detection systems
  - IDS types
  - Intrusion Prevention Systems
  - Honeypots
- Cryptography
  - Cryptography, Goals and History
  - Cryptography Techniques
  - Secret Key Cryptography (Symmetric Cryptography)
  - Public Key Cryptography (Asymmetric Cryptography)
  - HASH Mechanisms
  - Digital Signature
  - Public Key Infrastructure (PKI)
  - Certificate Authority
  - PGP
  - Steganography
- Virtual Private Networks
  - Virtual Private Networks
  - IPSec
  - Security Policy
  - Security Association, SA
  - SPI (Security Parameter Index)
  - Key Exchange
  - SSL/TLS

- WLAN Security
  - Standards & Modes
  - Defense (SSID and MAC)
  - Wired Equivalent Privacy (WEP)
  - Wi-Fi Protected Access (WPA)
  - Standard 802.1x
  - PEAP
  - Standard 802.11i
  - WPA2
- Authentication
  - Authentication & Authorization
  - User and Computer Authentication
  - Pros & Cons
  - Password Encryption & salt
  - Guessing/hacking Password
  - Password file & Protection
  - Password disclosure/hacking
  - Spoofing attack & Defense
  - System Improvements
  - Challenge / Response
  - Radius, Diameter, Kerberos