

Network Security Fundamentals

Course Length: 2 Day

Course Code: 7600

Prerequisites: None

Course Overview: This course is offered to provide insight into Network Security – a growing topic of concern for IT, corporations, and users of network resources. *Network Security Fundamentals* is an overview of what Information Security involves strategies to maintain information integrity, sorting out misleading information in the news, and providing industry awareness.

Course Outline

Introduction

- What does Information Security mean?
- History
- Relevancy to Day-to-Day Life
 - Stolen Identity
 - Social Security Number
 - Credit Card Numbers
 - (Provide examples of missing information)
- Misunderstandings

Security Breaches

- Insider vs. outsider
- Intruder (Hacker)
- Unauthorized access
- Disgruntled employees
- Employee accidentally misplacing/ information
- Viruses
- Malware/worms
- phishing
- Exploits
- Denial of Service (DoS)



NetForce Solutions, Inc.
P.O. Box 1710
Denver, NC 28037

phone (301) 943-5062
fax (509) 757-1661

info@netforcesolutions.com

www.netforcesolutions.com

Network Security Fundamentals

Identification & Authentication

- Why authenticate?
- Authenticators
- Single-factor
 - Passwords/Pins
 - Complexity
- 2-factor
 - Tokens and keys
 - Smartcards
 - Certificates and digital IDs
 - Biometrics
 - Fingerprints
 - Retinal and iris scanning
 - Voiceprints
 - Body geometry

Network Devices

- Firewall Architecture
 - Firewall Types
 - Firewall placement
 - Untrusted vs. Trusted
 - Perimeter definition
 - DMZ
 - Pros and Cons
- Routers and Security
 - Router access
 - Physical security
 - Logins, passwords, privileges, and accounts
 - Remote access
 - Pros and Cons

VPN

- Secure Remote Access
 - Network layer-based (IPSec)
 - Data link layer-based (L2TP)
 - Non-IPSec
 - Authentication Header (AH)
 - Encapsulating Security Payload (ESP)
 - Internet Security Association Key Management Protocol (ISAKMP)

Network Security Fundamentals

IPS/IDS: Intrusion Prevention System/Intrusion Detection

- IDS
 - Discovery
 - Anomaly Detection
 - Signature Recognition
 - Deployment
 - Network Intrusion Detection Systems
 - In-line
 - Sniffer
 - Host-Based IDS (HIDS)
- IPS
 - Alerts the network administrator
 - Session Termination
 - Combination of IDS and an application layer firewall.
- Pros and Cons

Wireless Networks

- How to Secure
 - Change default admin password
 - SSID
 - Change default SSID
 - Restrict Broadcasting
 - MAC Filter and IP Scope Restriction
 - Encryption
 - WEP
 - WPA
 - TKIP

Security Fundamentals

- Least Privilege
- Separation of Duties
- Defense in Depth

Strategies (Corporate and Personal Focus)

- Documenting and Reviewing a Security Policy
 - Federal Government Regulations/Policies
 - Federal Information Processing Standards (FIPS)
 - National Institute of Standards and Technology (NIST)
- Reducing Frustration for Legitimate Users
- Accountability
- Best Practice