Hands-On

Network Security

IPsec / VPNs / Firewalls / Wireless

BTS
Real-World Experience

Course Description

This Hands-On course is designed to expand an attendees general knowledge of networking into leading edge technologies. Attendees will learn about the security risks all networks present and some of the key security solutions to meet these challenges needed for new and old technologies in service today. Specifically, the student will learn about secure networking via VLANs and VPNs delivered by tunneling or the hot new concept of MPLS VPNs.

Security inevitably involves trade-offs in practice. Real systems need to provide reliable operation while still offering sufficient effective system power.
Designing secure systems involves building systems that are difficult for an attacker to defeat. To understand this well, the course first demonstrates the most popular hacking techniques for compromising systems and then teaches how these techniques can be defeated by good design and security features.

Students Will Learn

- **How hackers locate machines and network components vulnerable to attack**
- **How to defeat port scanning attacks on your own network**
- **How hackers attack WiFi networks, gain access and control**
- **How to configure your own WiFi networks to defeat typical attacks**
- **How passwords can be captured by intruders from network traffic**
- **How to prevent the capture of passwords on your network**
- **How Phishing and man in the middle attacks are perpetrated against networks**
- **How to protect your network against phishing attacks**
- **How intruders defeat authentication systems to gain unauthorized access**
- **How to build authentication systems that are difficult to defeat**
- **How routes and addresses may be spoofed to gain access and deny service**
- **How to defeat spoofing attacks**
- **How sniffers can be used to capture users data**
- **How to implement tunneling, SSH and VPN technology to protect confidentiality**
- **And More...**

Target Audience

Anyone responsible for, or interested in a Real-World practical hands-on approach to Security in Data Networking Technologies, Modern Techniques, Applications and Design. This includes Telecom professionals, outside plant / field, network operations staff, central office technicians, technical marketing staff, help desk agents, project managers, network

engineers, network administrators, voice engineers, and those in charge of converging voice and data networks.

Prerequisites

Attendees should already be familiar with the TCP/IP protocol, routing and switching technologies in a network as well as common operating systems. Attendees should bring their own laptop computers to undertake the practical hands-on sessions in class.

Course Outline

Module I: Security Fundamentals

Locating what needs to be secured

Identifying the range of Network Vulnerabilities

Analyzing the consequences of successful network attacks

Applying MOM analysis of threats

Security efficiency tradeoffs

Footprinting and Intelligence Gathering

Acquiring target information

Locating useful and relevant information

Scavenging published data

Mining archive sites

Scanning and enumerating resources

Identifying Vulnerabilities

Correlating weaknesses and exploits

Researching databases

Determining target configuration

What hackers need to attack a network

Analyzing the hacking tools Hands-on

Evaluating Vulnerability Assessment tools

Leveraging opportunities for attack

Hands-on exercise capturing and analysing traffic

Module II: Addressing and Spoofing

Identifying addresses and names used in our network

Address duplication methods

MAC addresses duplication methods

IP address discovery and spoofing

Hands-on Exercise Spoofing addresses

Communications using TCP and UDP Ports

Firewall use of port filters

Discovering filtered ports

Manipulating ports to gain access

Connecting to blocked services

Hands-on exercise Port scanning

Defeating firewalls

Port scanning countermeasures

Hands-on exercise detecting port scanning

Module III: Naming

Domain Name Service issues

Poisoning DNS

Gaining control of browsers

Creating custom malware

Harvesting client information

Enumerating internal data

Spoofing names and the impact of spoofed name

Hands-on Exercise spoofing DNS names

Implementing countermeasures to DNS spoofing

Module IV: Authentication Systems

Pivoting and island hopping

Deploying portable media attacks

Routing through compromised clients

Forwarding and redirecting ports

Pilfering target information

Stealing password hashes

Hands-on exercise password scanning

Hands-on exercise defeating Password Scanning

Module V: External Connections

Testing Antivirus and IDS Security

Masquerading network traffic

Sidestepping perimeter defenses

Evading antivirus systems

Falsifying file headers to inject malware

Discovering the gaps in antivirus protection

Hands-on exercise analyzing external connections

Module VI: Using Confidentiality Techniques to Defeat Sniffers

Using service separation techniques to isolate risk

Separating services on LANs using VLANs

Hands-on exercise deploying VLANs

Separating services over WANs using MPLS Paths

Deploying VPN Security

Separating Services using Encrypted Tunnels

Deploying Authentication options

Encryption: Symmetric and Asymmetric

DES, RSA, AES

Exploiting IPSec for VPNs over the Internet

Using PPTP Tunnels

Authenticating using RADIUS and DIAMETER

L2TP

Key management

Public Key Infrastructures for Private Data Exchange

Corporate security policies

Hands-on Exercise using VPN to defeat sniffing

Module VII: Wireless Vulnerability

Analyzing how WiFi works

Security using WEP

Hiding access points

Hands-on Exercise scanning for access points

WEP vulnerabilities

Hands-on Exercise Hacking a Wireless Access Point using WEP

WiFi security countermeasures

Deploying IEEE 802 Security concepts

Understanding EAP, WPA and WPA-2

Deploying AAA

Hands-on exercise Implementing WPA to defeat hacking and testing vulnerability

Module VIII: Compromising operating systems

Examining Windows protection modes

Analyzing Linux/UNIX processes

Subverting Web applications

Injecting SQL and HTML code

Bypassing authentication mechanisms

Manipulating Clients to Uncover Internal Threats

Baiting and snaring inside users

Review and Evaluation

Delivery Method

1-877-Info-2-Day | www.BTStraining.com

Instructor-Led with numerous Hands-On labs and exercises.

Equipment Requirements
(This apply's to our hands-on courses only)

BTS always provides equipment to have a very successful Hands-On course. BTS also encourages all attendees to bring their own equipment to the course. This will provide attendees the opportunity to incorporate their own gear into the labs and gain valuable training using their specific equipment.

Course Length

3 Days