



## **Course 753: Security Boot Camp (5 days)**

### **Unit 1 - Security Introduction**

- Principals
- The Concept of Trust
- Threat Definition and Risk Analysis
- Defense Models
- Security Policy
- Auditing

### **Unit 2 - The Larger Picture**

- Security Policy
- Security Policy Development
- Security Management
- Auditing and Logging
- Physical Security

### **Unit 3 - Authentication and Authorization**

- Authentication
- Authorizations
- Kerberos
- Other Real World Systems

### **Unit 4 - OS Principles**

- Version and Change Control
- Patching

### **Unit 5 - Specifics for Different OS**

- Hardening Unix
- Hardening Linux
- Hardening Windows

### **Unit 6 - Server Hardening**

- Web servers
- E-mail
- Printers and Faxes

### **Unit 7 - Protocols and Security**

- TCP/IP Weaknesses
- SSH and TLS
- IPSec
- IP Telephony and Streaming Media



## **Unit 8 - Network Infrastructure**

- DNS
- Public Key Infrastructure
- Hardening Router
- Hardening Switches and Hubs

## **Unit 9 - Firewalls and Proxy Servers**

- Fire Taxonomy
- Other Functions Performed by Firewalls
- Proxy Servers
- DMZ
- Strengths and Weakness of Firewalls

## **Unit 10 - Intrusion Detection and Prevention**

- Concepts
- Host or Network Based?
- Detection Models

## **Unit 11 - Remote Access**

- puTTY and ssh
- AAA Model
- PBGate
- DACS

## **Unit 12 - VPN**

- Concepts
- IPsec Tunnel
- L2TP over IPsec
- PPTP
- Using SSL

## **Unit 13 - Programming Architectures**

- J2EE Security
- .NET Security

## **Unit 14 - Wireless Security**

- Frequency Security Basics
- Layer 1 Solutions
- Layer 2 Solutions
- Wireless IDS

## **Unit 15 - Messaging Security**

- RV
- EMS
- Recovering

## **Unit 16 - Attack and Response**

- Response Team
- Responding
- Recovering

## **Unit 17 - Legal Considerations**

- Workers Concerns
- US Code
- California State Laws