Cybersecurity Foundations

Duration: 5 Days   Course Code: 9701

Overview:

In this cybersecurity course, you will gain a global perspective of the challenges of designing a secure system, touching on all the cyber roles needed to provide a cohesive security solution. Through lecture, labs, and breakout discussion groups, you will learn about current threat trends across the Internet and their impact on organizational security. You will review standard cybersecurity terminology and compliance requirements, examine sample exploits, and gain hands-on experience mitigating controls. In a contained lab environment, you will work with live viruses, including botnets, worms, and Trojans.

Target Audience:

Cybersecurity professionals, including security analysts, intel analysts, policy analysts, security operations personnel, network administrators, system integrators, VARS, and security consultants

Objectives:

- **After completing this course you should be able to understand:**
- Current cyber threats and cybersecurity site references
- Government-mandated directives and compliance requirements
- Cyber roles required to successfully design secure systems
- The attack cycle perpetrated by malicious hackers
- Enterprise policy requirements
- Best strategies for securing the enterprise with layered defenses
- How security zones and detailed logging augment information assurance
- Forensic challenges and incident response planning
- Risk management process
- Goals achievable with auditing, scanning, and testing systems
- Industry recommendations for maintaining secure access control
- Standards-based cryptographic solutions for securing communications

Prerequisites:

Attendees should meet the following prerequisites:

- TCP/IP Networking or equivalent knowledge

Testing and Certification

Recommended as preparation for the following exams:

- There are no exams currently aligned to this course

Follow-on-Courses:

The following courses are recommended for further study:

- CEH - Certifed Ethical Hacker
- CISM - Certified Information Security Manager

Content:

The Cyber Battlefield

- Critical Business Security
- Worldwide Internet Growth
- Security Fundamentals
- Security Goals
- Terminology Threats and Exposures
- Exploits and Exposures
- Hackers and Crackers
- Attack Methods
- Social Engineering
- Common Attack Vectors
- Traffic Analysis
- Responding to Threats and Attacks
- Documents and Procedures to Manage Risk
- Vulnerability Scanners
- Penetration Testing
- The OSSTMM
- NIST
- Risks of Penetration Testing

The Structure of the Internet and TCP/IP

- CNCI
- Initiatives
- Legal Compliance Standards
- Acts
- Federal Agency Compliance
- Commercial Regulatory Compliance
- Internet Leadership IANA
- Regional Internet Registry
- Protocols and RFCs
- TCP/IP Model
- Network Access Layer
- Internet Layer
- Host-to-Host Layer
- Process Layer
- Domain Name Service

Vulnerability Assessment and Tools

- Vulnerabilities and Exploits
- Vulnerability Assessment Tools
- Application-Level Scanners
- System-Level Scanners
- System-Level Testing Tools
- Open Source System-Level Scanner Tools
- Commercial System-Level Scanner Tools
- Advanced Attack Techniques and Tools
- Commercial Exploit Tools
- Free Exploit Tool: Metasploit
- Free Exploit Tool: BeEF
- Fuzz Testing
- Preventing Exploits and Attacks
- Patch Management
- Common Vulnerabilities and Exposures
- Alerts and Software
- Tools
- Vulnerability Research
- Common Security Sites
- Patch Management
- Tools

Authentication and Cryptographic Solutions

- Authentication
- Authentication Issues
- Cryptosystems Password Authentication
- Hash Functions
- Kerberos Cryptographic Benefits
- Symmetric Key Encryption Asymmetric Encryption Digital Signatures PKI Components
- Models
- Policies
- Lifecycle
- Distribution

Firewalls and Edge Devices

- General Security Integration
- Services
- Needs for Services
- Security Zones
- Filtering
- Screened Subnets
- Trusted Zones
- Devices
- Routers
- Firewalls
- DMZ Hosts
- Other Security Considerations
- Business-to-Business Communications
- Exceptions to Policy
- Special Services and Protocols
- Configuration Management
- Software Development Security
- Certification and Accreditation
- Common Criteria
- Intrusion Detection and Prevention
- Defense in Depth
- Network Device Logging
- Host Monitoring and Logging
- Events Correlation
- Placement of IDS Monitors and Sensors
- Monitoring
- Host-Based and Network-Based Differences
- Policy Management
- Behavioral Signatures
- IDS and IPS Weaknesses
- Encryption
- Incorrect Configuration

Forensic Analysis

- Incident Handling
- Security Incident Response
- Time and Reaction Sensitivity
- Incident Handling Issues and Considerations
- Response Procedures
- Evidence
- Logging
- Log Analysis Tools
- Active Ports

Lab 6: Cyber Attacks and Passwords

- Crack Passwords via the GUI
- Crack Passwords via the CLI
- Hide Files with NTFS

Lab 7: Cyber Attacks and Backdoors

- Perform Netcat Banner Grabbing
- Perform Netcat Shoveling
- Use Netcat to Port Scan
- Create and Detect a Trojan

Lab 8: Risk Assessment

- Review Profile and Complete a Criticality Ranking
- Complete a Criticality Review
- Complete a Threat Profile
- Evaluate the Support Policy and Cost

Lab 9: Security Policies

- Review Security Policies
- Develop an Incident Response Policy

Lab 10: Host Security

- Use the RECUB Trojan
- Identify the RECUB Service
- Harden the System

Lab 11: Covert Communications

- Hide Messages Using S-Tools
- Use Spam Mimic

Lab 12: Authentication and Cryptography

- Use Ettercap
- Use Dsniff
- Explore Cain and Abel

Lab 13: Snort IDS

- Install Snort IDS
- Configure Eagle X IDS
- Configure Rule to Ignore Hosts in Snort

Lab 14: Forensic Analysis

- Examine an IIS Event Log and Identify Common
- Use CurrPorts to Identify Anomalies
- Use Jotti for Forensic Analysis

Lab 15: Business Continuity Plan

- Identify When a Disaster Has Occurred
- Determine Key Assets
- Identify Potential Controls

Cyber Awareness

- Social Engineering
- Social Engineering Goals
- What Makes Social Engineering Possible
- Targets
- Attacks
- Phishing
- Phishing via Email
- Online Attacks
- Statistical Data
- Sources of Security Breaches
- Preventing Social Engineering
- Cyber Awareness: Policies and Procedures
- Security Policy Topics
- Social Media
- Social Networking Sites

Cyber Attacks: Footprinting and Scanning

- Footprinting
- Gathering Information
- Unearthing Initial Information
- Internet Archive
- People Search
- Locations and Mapping
- Job Boards
- Financial Information
- Google and Search Operators
- Identifying the Target Network and Its Range
- WHOIS Utility
- DNS Online Search Tools
- Traceroute
- Footprinting Countermeasures
- Detecting Live Systems
- Bypassing Authentication
- War Dialing
- Wardriving
- ICMP: Ping
- Port Scanning
- Performing TCP and UDP Scans
- Port Numbers
- TCP Flags
- TCP ThreeWay Handshake
- Port Scanning Techniques
- TCP Full Connect Port Scan
- TCP HalfOpen (SYN) Scanning
- Nmap HalfOpen Scan
- UDP Port Scan
- Nmap Scan Types and Switches
- Port Scanning Tools
- OS Fingerprinting
- Active Stack Fingerprinting
- Passive Fingerprinting
- Proxies and Anonymizers
- Scanning Countermeasures

Cyber Attacks: Breaking and Entering

- Password Attacks
- Privilege Escalation
- Maintaining Access
- Windows Authentication
- SysKey Encryption
- LAN Manager Password Encryption
- Dependency Walker
- Log Maintenance

Disaster Recovery and Business Continuity

- Disaster Types
- Disaster Recovery Plan (DRP)
- DRP Goals
- Creating a DRP
- DRP Contents
- DRP Design Requirements
- DRP Priorities
- Recovery Strategies
- High Availability
- Data Collection Documentation
- DRP Testing
- Business Continuity Planning
- BCP Steps

Cyber Evolution

- Cyber Forces
- Cyber Terrorism
- Cyber Security: Crime, War, or Fear Mongering?
- Cyber Future 7 Compliance Initiatives
- Cyber Defense in Depth
- Education and Training

Labs

Lab 1: Lab Setup

- Access the Virtual Lab Environment
- Configure BackTrack and Redhat Security Spin
- Rebuild Your Physical Computer

Lab 2: Understanding TCP/IP

- Convert Binary to Decimal
- Convert Decimal to Binary
- Convert Hexadecimal to Decimal
- Analyze Wireshark Traffic

Lab 3: Vulnerability Assessment

- Use Nessus
- Identify Coding Issues

Lab 4: Cyber Awareness

- Identifying Social Engineering Attacks
- Detect Phishing Using Internet-Based Tools

Lab 5: Cyber Scanning

- Trace Domains and IP Addresses
- Map Web Site Content with Teleport Pro
- Use Cheops for Graphical Display of Network
- Use GFI LanGuard
- Scan Using Nmap

- Windows LAN Manager and NTLM Hashes
- Linux Password Encryption
- SAM Database Insecurities
- Password Extraction Cracking
- Password Cracking Techniques
- Password Cracking Tools
- LCP
- John the Ripper
- Cain and Abel
- Password Cracking Countermeasures
- Covering Tracks
- Principle of Exchange
- Clearing the Logs
- Hiding Tools, Files, and Programs
- NTFS Alternate Data Streaming
- Information Hiding: Methods
- Steganography
- Steganography Detection
- Rootkits
- Countermeasures: Rootkits

Cyber Attacks: Backdoors and Trojans

- Malware
- Trojans
- Trojan Infection Mechanisms
- Well-Known Trojans
- Distribution Methods Wrappers
- Trojan Autostart Methods
- Covert Communications
- Stealth Technique: Avoiding Detection
- Backdoor Countermeasures
- Malware Countermeasure
- Anti-Spyware Software
- Malware Countermeasure Practices

Cyber Assessment and Risk Management

- Risk Management Steps
- Determining ALE
- CRAMM Process
- Risk Management Lifecycle
- Protected Assets
- CIA Triad
- Quantitative Risk Assessment
- Threat Determination Process
- Risk Assessment
- Lifecycle
- Steps
- Vulnerability Categories
- Business Assets vs. Risk
- Benefits of Risk Management
- Policy
- Assessment

Security Policy Management

- Security Policy
- Use
- Importance
- Legal Issues
- Example
- Policy References
- Policies, Guides, Standards, Procedures, and Controls

- Scan Using Zenmap
- Perform Banner Grabbing

- Security Policy Coverage Matrix
- Example: Internet Security Coverage Matrix
- Granular View of a Security Matrix
- Basic Policies

Securing Hosts and Servers

- Types of Hosts
- General Configuration Guidelines
- Clean Systems
- Unnecessary Services
- Warning Banners
- Limiting Access
- Configuring and Logging
- Security Patches
- Security Baselines
- Traffic Filtering Monitoring
- DoS Vulnerabilities
- Server Hardening
- Web Server Hardening
- Mail Server Hardening
- FTP Server Hardening
- DNS Server Hardening
- Other Servers
- Workstation Considerations
- Network Appliances
- Wireless Access Hardening
- VLAN Security
- Software Attacks

Securing Communications

- Applying Cryptography to OSI Model
- Tunnels
- Securing Services
- Email
- FTP and Telnet
- SSL and TLS
- Gateway-to-Gateway VPN
- Host-to-Gateway VPN
- IP Security
- Wireless Access Communication
- Wireless Security

Further Information:

For More information, or to book your course, please call us on 00 966 92000 9278

training@globalknowledge.com.sa

www.globalknowledge.com/en-sa/

Global Knowledge - KSA, 393 Al-Uroubah Road, Al Worood, Riyadh 3140, Saudi Arabia