Cybersecurity Foundations

Duration: 5 Days **Course Code: 9701**

Overview:

When you consider just a few of the consequences of a security breach - your proprietary information completely accessible, hefty fines for security lapses, news headlines about your company's security breach, it becomes obvious: An in-depth and thorough understanding of cyber security fundamentals and best practices is absolutely necessary.
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.
In addition to technical cybersecurity components, you will learn and explore the non-technical aspects of cybersecurity necessary to mitigate risk and lessen exposure, including risk management, threat determination, disaster recovery, security policy management, and business continuity planning. This course provides an excellent foundation for those proceeding to CISSP, CEH, CISA, or CISM training.

Target Audience:

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

Objectives:

- 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:

Content:

1. 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

2. 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

3. 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

SysKey Encryption

- LAN Manager Password Encryption
- 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

7. 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

8. 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

9. Security Policy Management

- Security Policy
- Use

12. 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

13. 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

14. Forensic Analysis

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

4. 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

5. 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

6. Cyber Attacks: Breaking and Entering

- Password Attacks
- Privilege Escalation
- Maintaining Access
- Windows Authentication
- Importance
- Legal Issues
- Example
- Policy References
- Policies, Guides, Standards, Procedures, and Controls
- Security Policy Coverage Matrix
- Example: Internet Security Coverage Matrix
- Granular View of a Security Matrix
- Basic Policies

10. 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

11. 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
- Active Ports
- Dependency Walker
- Log Maintenance
- 15. 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
- 16. 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

Further Information:

For More information, or to book your course, please call us on 00 971 4 446 4987

training@globalknowledge.ae

www.globalknowledge.com/en-ae/

Global Knowledge, Dubai Knowledge Village, Block 2A,First Floor, Office F68, Dubai, UAE