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:

Network professionals looking to advance their knowledge and explore cybersecurity as a career path Executives and managers looking to increase their ability to communicate with security professionals and implement a robust security solution at the organizational level Individuals who want to improve their understanding of cybersecurity fundamentals, including threats, mitigating controls, and organizational responsbilities

Objectives:

- **After completing this course you should be able to:**
- Increase your awareness of security
- Interpret/analyze tool output for network mapping/footprinting
- Reduce attack surface of systems
- Review networking as it applies to security controls
- Explore different data protection principles
- Examine the role of PKI/certificates in building trusted relationships between devices in a network
- Implement login security and other identity management solutions
- Reduce attack surface of network devices
- Explore current malware threats and anti-malware solutions
- Explore social engineering threats, methods, and techniques
- Examine software vulnerabilities and security solutions for reducing the risk of exploitation
- Explain monitoring capabilities and requirements and how those may raise privacy concerns
- Identify physical security controls and the relationship between physical and IT security
- Explain incident response capabilities
- Identify legal considerations and investigative techniques when it comes to cybersecurity
- Research trends in cybersecurity

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:

- G013 - CompTIA Security+
- CEH - Certifed Ethical Hacker
- CISM - Certified Information Security Manager

Content:

Cybersecurity Awareness

- What is security?
- Confidentiality, integrity, and availability
- Security baselining
- Security concerns: Humans
- Types of threats
- Security controls
- What is hacking?
- Risk management
- Data in motion vs. data at rest
- Module review

Network Discovery

- Networking review
- Discovery, footprinting, and scanning
- Common vulnerabilities and exposures
- Security policies
- Vulnerabilities
- Module review

Systems Hardening

- What is hardening?
- Types of systems that can be hardened
- Security baselines
- How to harden systems
- Hardening systems by role
- Mobile devices
- Hardening on the network
- Analysis tools
- Authentication, authorization, and accounting
- Physical security
- Module review

Security Architecture

- Security architecture
- Network devices
- Network zones
- Network segmentation
- Network Address Translation
- Network Access Control
- Module review

Data Security

- Cryptography
- Principles of permissions
- Steganography
- Module review

Public Key Infrastructure

- Public key infrastructure
- Certification authorities
- Enabling trust
- Certificates
- CA management
- Module review

Environment Monitoring

- Monitoring
- Monitoring vs. logging
- Monitoring/logging benefits
- Logging
- Metrics
- Module review

Physical Security

- What is physical security?
- Defense in depth
- Types of physical security controls
- Device security
- Human security
- Security policies
- Equipment tracking
- Module review

Incident Response

- Disaster types
- Incident investigation tips
- Business continuity planning
- Disaster recovery plan
- Forensic incident response
- Module review

Legal Considerations

- Regulatory compliance
- Cybercrime
- Module review

Trends in Cybersecurity

- Cybersecurity design constraints
- Cyber driving forces
- How connected are you?
- How reliant on connectivity are you?
- Identity management
- Cybersecurity standards
- Cybersecurity training

Course Look Around

- Looking back
- Looking forward
- Planning your journey
- View More View More

Lab 1: Explore HR Security

Lab 2: Interpret Scanning Results

Lab 3: Harden Servers and Workstations

Lab:4 Security Architecture

Lab 6: Configure a PKI

Lab 7: Manage Passwords

Lab 8: Explore Hardening Recommendations and Known Vulnerabilities

Lab 9: Detect Malware

Lab 10: Social Engineering

Lab 11: Privilege Escalation

Lab 12: Monitor a System

Lab 13: Implement Physical Security

Lab 14: Incident Response

Lab 15: Review Legal Considerations

Identity Management

- What is identity management?
- Personally identifiable information
- Authentication factors
- Directory services
- Kerberos
- Windows NT LAN Manager
- Password policies
- Cracking passwords
- Password assessment tools
- Password managers
- Group accounts
- Service accounts
- Federated identities
- Identity as a Service
- Module review

Network Hardening

- Limiting remote admin access
- AAA: Administrative access
- Simple Network Management Protocol
- Network segmentation
- Limiting physical access
- Establishing secure access
- Network devices
- Fundamental device protection summary
- Traffic filtering best practices
- Module review

Malware

- What is malware?
- Infection methods
- Types of malware
- Backdoors
- Countermeasures
- Protection tools
- Module review

Social Engineering

- What is social engineering?
- Social engineering targets
- Social engineering attacks
- Statistical data
- Information harvesting
- Preventing social engineering
- Cyber awareness: Policies and procedures
- Social media
- Module review

Software Security

- Software engineering
- Security guidelines
- Software vulnerabilities
- Module review

Lab 5: Protect Data

Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 0113 242 5931

info@globalknowledge.co.uk

www.globalknowledge.com/en-gb/

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK