Cybersecurity Foundations

Duration: 5 Days   Course Code: 9701

Overview:

Exclusive - Investigate cybersecurity threats and master techniques needed to protect your network.
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 wants to improve their understanding of cybersecurity fundamentals, including threats, mitigating controls, and organizational responsibilities

Objectives:

- 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:

TCP/IP Networking or equivalent knowledge

Recommended courses:

- Understanding Networking Fundamentals
- TCP/IP Networking

Follow-on-Courses:

The following courses are recommended for further study:

Technical track (certifications)

- CND - Certified Network Defender
- CEH - Certifed Ethical Hacker

Management track (certifications)

- Comptia+ Security
- CISM - Certified Information Security Manager
- CISA - Certified Information Security Auditor

Content:

1. 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

2. Network Discovery

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

3. 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

4. Security Architecture

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

5. Data Security

- Cryptography
- Principles of permissions
- Steganography
- Module review

6. Public Key Infrastructure

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

12. Environment Monitoring

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

13. Physical Security

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

14. Incident Response

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

15. Legal Considerations

- Regulatory compliance
- Cybercrime
- Module review

16. 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

17. Course Look Around

- Looking back
- Looking forward
- Planning your journey

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

7. 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

8. 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

9. Malware

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

10. 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

11. 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 0800/84.009

info@globalknowledge.be

www.globalknowledge.com/en-be/