Cefi Informatica s.r.l.
Piazza di Porta Maggiore, 6 – 00185 Roma
Tel. 06.5921914 : Fax 06.54280485
P.Iva : 06373061008

SEDI di ROMA

Centro
Piazza di Porta Maggiore , 6

Eur
Viale Pasteur, 78
Viale Pasteur, 70

Appio
Piazza C. Cantù, 19

Tel.: 06 - 5921914
Fax : 06 -54280485

Mail: staff@cefi.it

Programma Didattico

Master Manager della Sicurezza Informatica

Network Security

- Explain the security function and purpose of network devices and technologies
  - Firewalls
  - Routers
  - Switches
  - Load Balancers
  - Proxies
  - Web security gateways
  - VPN concentrators
  - NIDS and NIPS (Behavior based, signature based, anomaly based, heuristic)
  - Protocol analyzers
  - Sniffers
  - Spam filter, all-in-one security appliances
  - Web application firewall vs. network firewall
  - URL filtering, content inspection, malware inspection
- Apply and implement secure network administration principles
  - Rule-based management
  - Firewall rules
  - VLAN management
  - Secure router configuration
  - Access control lists
  - Port Security
  - 802.1x
  - Flood guards
  - Loop protection
  - Implicit deny
  - Prevent network bridging by network separation
  - Log analysis
- Distinguish and differentiate network design elements and components
  - DMZ
  - Subnetting
  - VLAN
  - NAT
  - Remote Access
  - Telephony
  - NAC
  - Virtualization
  - Cloud Computing
    - o Platform as a Service
    - o Software as a Service
    - o Infrastructure as a Service
- Implement and use common protocols
  - IPSec
  - SNMP

- SSH
- DNS
- TLS
- SSL
- TCP/IP
- FTPS
- HTTPS
- SFTP
- SCP
- ICMP
- IPv4 vs. IPv6

- Identify commonly used default network ports

- FTP
- SFTP
- FTPS
- TFTP
- TELNET
- HTTP
- HTTPS
- SCP
- SSH
- NetBIOS

- Implement wireless network in a secure manner

- WPA
- WPA2
- WEP
- EAP
- PEAP
- LEAP
- MAC filter
- Disable SSID broadcast
- TKIP
- CCMP
- Antenna Placement
- Power level controls

Compliance and Operational Security

- Explain risk related concepts

- Control types

o Technical
o Management
o Operational

- False positives
- Importance of policies in reducing risk

o Privacy policy
o Acceptable use
o Security policy
o Mandatory vacations
o Job rotation
o Separation of duties
o Least privilege

- Risk calculation

o Likelihood
o ALE
o Impact

- Quantitative vs. qualitative
- Risk-avoidance, transference, acceptance, mitigation, deterrence
- Risks associated to Cloud Computing and Virtualization

- Carry out appropriate risk mitigation strategies

- Implement security controls based on risk
- Change management

- Incident management
- User rights and permissions reviews
- Perform routine audits
- Implement policies and procedures to prevent data loss or theft

- Execute appropriate incident response procedures
- Basic forensic procedures
  - Order of volatility
  - Capture system image
  - Network traffic and logs
  - Capture video
  - Record time offset
  - Take hashes
  - Screenshots
  - Witnesses
  - Track man hours and expense
- Damage and loss control
- Chain of custody
- Incident response: first responder

- Explain the importance of security related awareness and training
- Security policy training and procedures
- Personally identifiable information
- Information classification: Sensitivity of data (hard or soft)
- Data labeling, handling and disposal
- Compliance with laws, best practices and standards
- User habits
  - Password behaviors
  - Data handling
  - Clean desk policies
  - Prevent tailgating
  - Personally owned devices
- Threat awareness
  - New viruses
  - Phishing attacks
  - Zero days exploits
- Use of social networking and P2P

- Compare and contrast aspects of business continuity
- Business impact analysis
- Removing single points of failure
- Business continuity planning and testing
- Continuity of operations
- Disaster recovery
- IT contingency planning
- Succession planning

- Explain the impact and proper use of environmental controls
- HVAC
- Fire suppression
- EMI shielding
- Hot and cold aisles
- Environmental monitoring
- Temperature and humidity controls
- Video monitoring

- Execute disaster recovery plans and procedures
- Backup / backout contingency plans or policies
- Backups, execution and frequency
- Redundancy and fault tolerance
  - Hardware
  - RAID
  - Clustering
  - Load balancing
  - Servers

- High availability
- Cold site, hot site, warm site
- Mean time to restore, mean time between failures, recovery time objectives and recovery point objectives

-Exemplify the concepts of confidentiality, integrity and availability (CIA)

Threats and Vulnerabilities

- Analyze and differentiate among types of malware
- Adware
- Virus
- Worms
- Spyware
- Trojan
- Rootkits
- Backdoors
- Logic bomb
- Botnets

- Analyze and differentiate among types of attacks
- Man-in-the-middle
- DDoS
- DoS
- Replay
- Smurf attack
- Spoofing
- Spam
- Phishing
- Spim
- Vishing
- Spear phishing
- Xmas attack
- Pharming
- Privilege escalation
- Malicious insider threat
- DNS poisoning and ARP poisoning
- Transitive access
- Client-side attacks

- Analyze and differentiate among types of social engineering attacks
- Shoulder surfing
- Dumpster diving
- Tailgating
- Impersonation
- Hoaxes
- Whaling
- Vishing

- Analyze and differentiate among types of wireless attacks
- Rogue access points
- Interference
- Evil twin
- War driving
- Bluejacking
- Bluesnarfing
- War chalking
- IV attack
- Packet sniffing

- Analyze and differentiate among types of application attacks
- Cross-site scripting
- SQL injection
- LDAP injection
- XML injection
- Directory traversal/command injection
- Buffer overflow

- Zero-day
- Cookies and attachments
- Malicious add-ons
- Session hijacking
- Header manipulation

- Analyze and differentiate among types of mitigation and deterrent techniques
- Manual bypassing of electronic controls

o Failsafe/secure vs. failopen

- Monitoring system logs

o Event logs
o Audit logs
o Security logs
o Access logs

- Physical security

o Hardware locks
o Mantraps
o Video surveillance
o Fencing
o Proximity readers
o Access list

- Hardening

o Disabling unnecessary services
o Protecting management interfaces and applications
o Password protection
o Disabling unnecessary accounts

- Port security

o MAC limiting and filtering
o 802.1x
o Disabling unused ports

- Security posture

o Initial baseline configuration
o Continuous security monitoring
o remediation

- Reporting

o Alarms
o Alerts
o Trends

- Detection controls vs. prevention controls

o IDS vs. IPS
o Camera vs. guard

- Implement assessment tools and techniques to discover security threats and vulnerabilities

- Vulnerability scanning and interpret results
- Tools

o Protocol analyzer
o Sniffer
o Vulnerability scanner
o Honeypots
o Honeynets
o Port scanner

- Risk calculations

o Threat vs. likelihood

- Assessment types

o Risk
o Threat
o Vulnerability

- Assessment technique

o Baseline reporting
o Code review
o Determine attack surface
o Architecture

o Design reviews
- Within the realm of vulnerability assessments, explain the proper use of penetration testing versus vulnerability scanning
· Penetration testing
o Verify a threat exists
o Bypass security controls
o Actively test security controls
o Exploiting vulnerabilities
· Vulnerability scanning
o Passively testing security controls
o Identify vulnerability
o Identify lack of security controls
o Identify common misconfiguration
· Black box
· White box
· Gray box

Application, Data and Host Security

- Explain the importance of application security
· Fuzzing
· Secure coding concepts
o Error and exception handling
o Input validation
· Cross-site scripting prevention
· Cross-site Request Forgery (XSRF) prevention
· Application configuration baseline (proper settings)
· Application hardening
· Application patch management
- Carry out appropriate procedures to establish host security
· Operating system security and settings
· Anti-malware
o Anti-virus
o Anti-spam
o Anti-spyware
o Pop-up blockers
o Host-based firewalls
· Patch management
· Hardware security
o Cable locks
o Safe
o Locking cabinets
· Host software baselining
· Mobile devices
o Screen lock
o Strong password
o Device encryption
o Remote wipe/sanitization
o Voice encryption
o GPS tracking
· Virtualization
- Explain the importance of data security
· Data Loss Prevention (DLP)
· Data encryption
o Full disk
o Database
o Individual files
o Removable media
o Mobile devices
· Hardware based encryption devices
o TPM
o HSM

o USB encryption
o Hard drive
- Cloud computing

Access Control and Identity Management

- Explain the function and purpose of authentication services
- RADIUS
- TACACS
- TACACS+
- Kerberos
- LDAP
- XTACACS

- Explain the fundamental concepts and best practices related to authentication, authorization and access control
- Identification vs. authentication
- Authentication (single factor) and authorization
- Multifactor authentication
- Biometrics
- Tokens
- Common access card
- Personal identification verification card
- Smart card
- Least privilege
- Separation of duties
- Single sign on
- ACLs
- Access control
- Mandatory access control
- Discretionary access control
- Role/rule-based access control
- Implicit deny
- Time of day restrictions
- Trusted OS
- Mandatory vacations
- Job rotation

- Implement appropriate security controls when performing account management
- Mitigates issues associated with users with multiple account/roles
- Account policy enforcement
o Password complexity
o Expiration
o Recovery
o Length
o Disablement
o Lockout
- Group based privileges
- User assigned privileges

Cryptography

- Summarize general cryptography concepts
- Symmetric vs. asymmetric
- Fundamental differences and encryption methods
o Block vs. stream
- Transport encryption
- Non-repudiation
- Hashing
- Key escrow
- Steganography
- Digital signatures
- Use of proven technologies
- Elliptic curve and quantum cryptography

- Use and apply appropriate cryptographic tools and products
- WEP vs. WPA/WPA2 and preshared key

- MD5
- SHA
- RIPEMD
- AES
- DES
- 3DES
- HMAC
- RSA
- RC4
- One-time-pads
- CHAP
- PAP
- NTLM
- NTLMv2
- Blowfish
- PGP/GPG
- Whole disk encryption
- TwoFish
- Comparative strengths of algorithms
- Use of algorithms with transport encryption

o SSL
o TLS
o IPSec
o SSH
o HTTPS

- Explain the core concepts of public key infrastructure

- Certificate authorities and digital certificates

o CA
o CRLs

- PKI
- Recovery agent
- Public key
- Private key
- Registration
- Key escrow
- Trust models

- Implement PKI, certificate management and associated components

- Certificate authorities and digital certificates

o CA
o CRLs

- PKI
- Recovery agent
- Public key
- Private keys
- Registration
- Key escrow
- Trust models

CEFI
CENTRI DI FORMAZIONE INFORMATICA

Adobe CERTIFIED ASSOCIATE

Microsoft Office Specialist

ECDL

Organismo Accreditato da ACCREDIA

CERMET
SISTEMA DI GESTIONE CERTIFICATO
9001:2008