MUSA FORMAZIONE

Formazione a distanza
Team di professionisti
Tecnologia e-learning
Network

## PARTE 1 – COMPTIA SECURITY + (45 ORE)

### MODULO 1 – LE BASI

- Assessment test
- Introduzione alle Reti informatiche, Pacchetti, Indirizzi IP, Routing
- Indirizzamento, ARP, TCP, UDP, Firewall
- Topologie di rete
- La pila di OSI (Open Systems Interconnection Model)
- TCP/IP Suite
- IP Subnetting
- Le basi del protocollo: il modello TCP/IP
- TCP/IP Ports
- Comprendere i dispositivi di rete
- Il MAC Address
- Elementi di crittografia e metodi per creare password sicure
- Vulnerability Assessment
- Strumenti open source per analizzare le reti (sniffer)
- Open Vas: Vulnerability Scanner analisi di rete
- Wireshark
- Configurazione e uso di analizzatori di rete open source
- Studiare le comunicazioni con Wireshark
- Applicazioni Web-analisi dei Cookie
- Same Origin Policy (Politica della stessa origine)
- Studiare le Applicazioni Web e HTTP con Burp Suite
- Analisi Cloud sicuri e multicloud. Hexadecimal vs. Binary
- Intrusion Prevention e Intrusion Detection Systems
- Network Security
- Sistemi operativi
- Backup e Archiviazione

### MODULO 2 MISURARE E STIMARE IL RISCHIO

- Risk Assessment
    - Computing Risk Assessment
    - Agire sul Risk Assessment
    - Rischi associati al cloud computing
    - Rischi associati con la virtualizzazione
- Sviluppare Policies, Standards, e Guidelines
    - Implementare Policie aziendali
    - Risk Management e Best Practices

Formazione a distanza
Team di professionisti
Tecnologia e-learning
Network

- o   Disaster Recovery
- o   Business continuity

## MODULO 3 ANALISI E DIAGNOSTICA DELLE RETI

- Monitoraggio delle reti
- Comprendere l'Hardening e metodologie di gestione dei sistemi informativi aziendali
  - o   Lavorare con i servizi
  - o   Patches
  - o   User Account Control
  - o   File systems
- Mettere in sicurezza una rete
- Security Posture
  - o   Monitoraggio continuo della sicurezza
  - o   Impostare una Remediation Policy
- Evidenziare le falle nella Sicurezza
  - o   Alarm
  - o   Alerts
  - o   Trends
- Differenziare Detection Controls e Prevention Controls

## MODULO 4 DISPOSITIVI ED INFRASTRUTTURE

- Analisi sistemi TCP/IP
  - o   Studio della pila di OSI
  - o   Lavorare con la TCP/IP Suite
  - o   IPv4 and IPv6
  - o   Capire l'incapsulamento
  - o   Lavorare con protocolli e servizi
- Progettare una rete sicura:
  - o   DZ e Subnetting
  - o   Virtual Local Area Networks
  - o   Remote Access
  - o   Network Address Translation
  - o   Telephony
  - o   Network Access Control
- Dispositivi di rete
  - o   Firewall
  - o   Router
  - o   Switch
  - o   Load Balancers

MUSA
FORMAZIONE

Formazione a distanza
Team di professionisti
Tecnologia e-learning
Network

- o Proxy
- o Web Security Gateway
- o Concentratori VPNs e VPN
- o Intrusion Detection Systems
- o Comprendere Intrusion Detection Systems
- o IDS vs. IPS 110
- o Lavorare con una Network-Based IDS
- o Lavorare con una Host-Based IDS
- o Lavorare con NIPSs
- o Protocol Analyzers
- o Spam Filter
- o UTM Security Appliance

## MODULO 5 ACCESS CONTROL, AUTENTICAZIONE E AUTORIZZAZIONE

- Comprendere le basi dell'Access Control
  - o Identificazione vs. Autenticazione
  - o Autenticazione (Single Factor) e Autorizzazione
  - o Sicurezza e difesa
  - o Network Access Control
  - o Token
  - o Potenziali problemi di autenticazione e accesso
  - o Protocolli di autenticazione
  - o Policy aziendale
  - o Utenti con account ruoli Multipli
- Remote Access Connectivity
  - o Utilizzare il protocollo the Point-to-Point
  - o Lavorare con i protocolli di Tunneling
  - o Lavorare con RADIUS
  - o TACACS/TACACS+/XTACACS
  - o VLAN Management
  - o SAML
- Authentication Services
  - o LDAP
  - o Kerberos
- Access Control
  - o Mandatory Access Control
  - o Discretionary Access Control
  - o Role-Based Access Control
  - o Rule-Based Access Control
- Principali pratiche di Access Control
  - o Lista dei Privilegi
  - o Separation of Duties
  - o Time of Day Restrictions

![MUSA FORMAZIONE]

Formazione a distanza
Team di professionisti
Tecnologia e-learning
Network

- o User Access Review
- o Smart Cards
- o Access Control List
- o Port Security
- o Working with 802.1X
- o Flood Guards and Loop Protection
- o Preventing Network Bridging
- o Log Analysis
- o Configurazione sicura del Router

## MODULO 6 SICUREZZA DELLE RETI WIRELESS

- Lavorare con i sistemi Wireless
  - o IEEE 802.11x Wireless Protocols
  - o WEP/WAP/WPA/WPA2
  - o Wireless Transport Layer Security
- Dispositivi Wireless
- Wireless Access Points
  - o Extensible Authentication Protocol
  - o Lightweight Extensible Authentication Protocol
  - o Protected Extensible Authentication Protocol
- Reti Wireless: principali vulnerabilità
  - o Wireless Attack Analogy

## MODULO 7 SICUREZZA NEL CLOUD

- Lavorare con il Cloud Computing
  - o Software as a Service (SaaS)
  - o Platform as a Service (PaaS)
  - o Infrastructure as a Service (IaaS)
  - o Private Cloud
  - o Public Cloud
  - o Community Cloud
  - o Hybrid Cloud
- Utilizzare la virtualizzazione
  - o Snapshots
  - o Patch Compatibility
  - o Host Availability/Elasticity
  - o Security Control Testing
  - o Sandboxing
- Sicurezza nel Cloud
  - o Cloud Storage

## MODULO 8 HOST, DATA, E APPLICATION SECURITY

- Application Hardening
  - Databases and Technologies
  - Application Configuration Baselining
  - Operating System Patch Management
  - Application Patch Management
- Host Security
  - Permissions
  - Access Control List
  - Antimalware
  - Host Software Baselining
  - Hardening Web Servers
  - Hardening Email Servers
  - Hardening FTP Servers
  - Hardening DNS Servers
  - Hardening DHCP Services
- Application Security
- Best Practices for Security
  - Data Loss Prevention

## MODULO 9 CRITTOGRAFIA

- Crittografia: cenni storici
- Crittografia: prime applicazioni ed esempi
- Crittografia moderna
  - Symmetric Algorithms
  - Asymmetric Algorithms
  - Quale crittografia utilizzare?
  - comprendere l'Hashing
  - Algoritmi di Hashing
  - Rainbow Tables e Salt
  - Key Stretching
  - Quantum Cryptography
  - Cryptanalysis Methods
  - Wi-Fi Encryption
- Sistemi di crittografia
  - Confidentiality e Strength
  - Integrità
  - Digital Signatures
  - Authentication
  - Nonrepudiation

Formazione a distanza
Team di professionisti
Tecnologia e-learning
Network

- o   Key Features
- Crittografia standard e Protocolli
  - o   Le origini dello standard di crittografia
  - o   Public-Key Infrastructure X.509
  - o   Public-Key Cryptography Standards
  - o   X.509
  - o   SSL and TLS
  - o   Certificate Management Protocols
  - o   Secure Multipurpose Internet Mail Extensions
  - o   Secure Electronic Transaction
  - o   Secure Shell
  - o   HTTP Secure
  - o   Secure HTTP
  - o   IP Security
  - o   Tunneling Protocols
  - o   Federal Information Processing Standard
- Utilizzo delle Public-Key Infrastructure
  - o   Certificate Authority
  - o   Registration Authorities e Local Registration Authorities
  - o   Implementazione di Certificati
  - o   Comprendere la Certificate Revocation
  - o   Implementazione dei giusti Modelli
- crittografia in Pratica
- problemi di crittografia
- Applicazioni di crittografia
  - o

## MODULO 10 MALWARE, VULNERABILITÀ E MINACCE

- Malware
- Virus
  - o   Sintomi di infezione da virus
  - o   come funziona un virus
  - o   tipi di virus
  - o   Gestire lo Spam per evitare i Virus
  - o   Antivirus Software
- Comprendere le diverse tipologie di attacco
  - o   Identifying Denial-of-Service e Distributed Denial-of-Service
  - o   Spoofing Attacks
  - o   Pharming Attacks
  - o   Phishing, Spear Phishing, e Vishing Attacks
  - o   Xmas Attack
  - o   Man-in-the-Middle Attacks
  - o   Replay Attacks
  - o   Smurf Attacks

Formazione a distanza
Team di professionisti
Tecnologia e-learning
Network

- o Password Attacks
- o Privilege Escalation
- o Malicious Insider Threats
- o Transitive Access
- o Client-Side Attacks
- o Typo Squatting e URL Hijacking
- o Watering Hole Attack
- Identificare le tipologie di Application Attacks
  - o Cross-Site Scripting e Forgery
  - o SQL Injection
  - o LDAP Injection
  - o XML Injection
  - o Directory Traversal/Command Injection
  - o Buffer Overflow
  - o Integer Overflow
  - o Zero-Day Exploits
  - o Cookies e Attachments
  - o Locally Shared Objects e Flash Cookies
  - o Malicious Add-Ons
  - o Session Hijacking
  - o Header Manipulation
  - o Arbitrary Code e Remote Code Execution
- Tools per identificare le minacce
- Interpretare i risultati del test
  - o Tools da conoscere
  - o Risk Calculations e Assessment Types

## MODULO 11 SOCIAL ENGINEERING E ALTRI NEMICI

- Comprendere il significato di Social Engineering
  - o Tipologie di Social Engineering Attacks
  - o Motivazioni di un Attacco
  - o I principi alla base del Social Engineering
  - o Esempi di attacco di tipo Social Engineering
- Comprendere la sicurezza fisica
  - o Mantraps
  - o Video sorveglianza
  - o Fencing
  - o Access List
  - o Proper Lighting
  - o Signs
  - o Guards
  - o Barricades
  - o Biometrics
  - o Protected Distribution

MUSA
FORMAZIONE

Formazione a distanza
Team di professionisti
Tecnologia e-learning
Network

- - Alarms
  - Motion Detection
- Environmental Controls
  - HVAC
  - Environmental Monitoring
- Data Policies
  - Distruzione di una Flash Drive
  - Considerazioni
  - Dischi ottici

## MODULO 12 SECURITY ADMINISTRATION

- Third-Party Integration
  - Transitioning
  - Ongoing Operations
- Consapevolezza e formazione sulla sicurezza
  - Somministrare una opportuna formazione
  - Tematiche di sicurezza
  - Argomenti di formazione
- Classificare le informazioni
  - Informazione pubblica
  - Informazione privata
- Controlli di accesso all'informazione
  - Concetti di Security
- Rispetto delle normative sulla Privacy e sulla sicurezza note storiche
  - Gramm-Leach-Bliley Act
  - The Computer Fraud and Abuse Act
  - The Family Educational Rights and Privacy Act
  - The Computer Security Act of 1987
  - The Cyberspace Electronic Security Act
  - The Cyber Security Enhancement Act
  - The Patriot Act
- Dispositivi mobili
  - Problematiche legate al BYOD
- Metodi alternativi per limitare i rischi di sicurezza

## MODULO 13 DISASTER RECOVERY E INCIDENT RESPONSE

- Problemi connessi alla Business Continuity
  - Tipologie di Storage
  - Lavorare ad un piano di Disaster-Recovery
  - Incident Response Policies
  - Incident Response
  - Succession Planning

- Reinforcing Vendor Support
  - Accordi a livello di servizio
  - Accordi Code Escrow
- Penetration Testing
  - Cosa testare?
  - Vulnerability Scanning

![MUSA FORMAZIONE]

Formazione a distanza
Team di professionisti
Tecnologia e-learning
Network

## PARTE 2° - CERTIFIED ETHICAL HACKER C|EH (45 ORE)

### MODULO 1: INTRODUZIONE ALL'ETHICAL HACKING

- Information Security Overview
- Cyber Kill Chain Concepts
- Hacking Concepts
- Ethical Hacking Concepts
- Information Security Controls
- Information Security Laws and Standards

### MODULO 2: FOOTPRINTING AND RECONNAISSANCE

- Footprinting Concepts
- Footprinting Through Search Engines
- Footprinting Through Web Services
- Footprinting Through Social Networking Sites
- Website Footprinting
- Eamil Footprinting
- Whois Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting Through Social Engineering
- Footprinting Tools
- Footprinting Countermeasures

### MODULO 3: SCANNING NETWORKS

- Network Scanning Concepts
- Scanning Tools
- Host Discovery
- Port and Service Discovery
- OS Discovery (Banner Grabbing/OS Fingerprinting)
- Scanning Beyond IDS and Firewall
- Draw Network Diagrams

### MODULO 4: ENUMERATION

- Enumeration Concepts
- NetBIOS Enumeration
- SNMP Enumeration
- LDAP Enumeration
- SMTP and DNS Enumeration
- Other Enumeration Techniques

Formazione a distanza
Team di professionisti
Tecnologia e-learning
Network

- Enumeration Countermeasures

## MODULO 5: VULNERABILITY ANALYSIS

- Vulnerability Assessment Concepts
- Vulnerability Classification and Assessment Types
- Vulnerability Assessment Solutions and Tools
- Vulnerability Assessment Reports

## MODULO 6: SYSTEM HACKING

- System Hacking Concepts
- Gaining Access
- Escalating Privileges
- Maintaining Access
- Clearing Logs

## MODULO 7: MALWARE THREATS

- Malware Concepts
- APT Concepts
- Trojan Concepts
- Virus and Worm Concepts
- Fileless Malware Concepts
- Malware Analysis
- Countermeasures
- Anti-Malware Software

## MODULO 8: SNIFFING

- Sniffing Concepts
- Sniffing Technique: MAC Attacks
- Sniffing Technique: DHCP Attacks
- Sniffing Technique: ARP Poisoning
- Sniffing Technique: Spoofing Attacks
- Sniffing Technique: DNS Poisoning
- Sniffing Tools
- Countermeasures
- Sniffing Detection Techniques

## MODULE 09: SOCIAL ENGINEERING

- Social Engineering Concepts

- Social Engineering Techniques
- Insider Threats
- Impersonation on Social Networking Sites
- Identity Theft
- Countermeasures

## MODULE 10: DENIAL-OF-SERVICE

- Dos/DDos Concepts
- Dos/DDos Attack Techniques
- Botnets
- DDos Case Study
- Dos/DDos Attack Tools
- Countermeasures
- Dos/DDos Protection Tools

## MODULE 11: SESSION HIJACKING

- Session Hijacking Concepts
- Application Level Session Hijacking
- Network Level Session Hijacking
- Session Hijacking Tools
- Countermeasures

## MODULE 12: EVADING IDS, FIREWALLS AND HONEYPOTS

- IDS, IPS, Firewall and Honeypot Concepts
- IDS, IPS, Firewall and Honeypot Solutions
- Evading IDS
- Evading Firewalls
- IDS/Firewall Evading Tools
- Detecting Honeypots
- IDS/Firewall Evasion Countermeasures

## MODULE 13: HACKING WEB SERVERS

- Web Server Concepts
- Web Server Attacks
- Web Server Attack Methodology
- Web Server Attack Tools
- Countermeasures
- Patch Management
- Web Server Security Tools

## MODULE 14: HACKING WEB APPLICATIONS

FORMAZIONE

Formazione a distanza
Team di professionisti
Tecnologia e-learning
Network

- Web Application Concepts
- Web Application Threats
- Web Application Hacking Methodology
- Web API, Webhooks and Web Shell
- Web Application Security

## MODULE 15: SQL INJECTION

- SQL Injection Concepts
- Types of SQL Injection
- SQL Injection Methodology
- SQL Injection Tools
- Evasion Techniques
- Countermeasures

## MODULE 16: HACKING WIRELESS NETWORKS

- Wireless Concepts
- Wireless Encryption
- Wireless Threats
- Wireless Hacking Methodology
- Wireless Hacking Tools
- Bluetooth Hacking
- Countermeasures
- Wireless Security Tools

## MODULE 17: HACKING MOBILE PLATFORMS

- Mobile Platform Attack Vectors
- Hacking Android OS
- Hacking iOS
- Mobile Device Management
- Mobile Security Guidelines and Tools

## MODULE 18: IOT AND OT HACKING

- IoT Concepts
- IoT Attacks
- IoT Hacking Methodology
- IoT Hacking Tools
- Countermeasures
- OT Concepts
- OT Attacks
- OT Hacking Methodology
- OT Hacking Tools

Formazione a distanza
Team di professionisti
Tecnologia e-learning
Network

- Countermeasures

## MODULE 19: CLOUD COMPUTING

- Cloud Computing Concepts
- Container Technology
- Serverless Computing
- Cloud Computing Threats
- Cloud Hacking
- Cloud Security

## MODULE 20: CRYPTOGRAPHY

- Cryptography Concepts
- Encryption Algorithms
- Cryptography Tools
- Public Key Infrastructure (PKI)
- Email Encryption
- Disk Encryption
- Cryptanalysis
- Countermeasures