

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 multcloud. 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 Policies aziendali
 - Risk Management e Best Practices

- Disaster Recovery
- Business continuity

MODULO 3 ANALISI E DIAGNOSTICA DELLE RETI

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

MODULO 4 DISPOSITIVI ED INFRASTRUTTURE

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

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

MODULO 5 ACCESS CONTROL, AUTENTICAZIONE E AUTORIZZAZIONE

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

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

MODULO 6 SICUREZZA DELLE RETI WIRELESS

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

MODULO 7 SICUREZZA NEL CLOUD

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

MODULO 8 HOST, DATA, E APPLICATION SECURITY

- Application Hardening
 - Databases and Technologies
 - Application Configuration Baselineing
 - Operating System Patch Management
 - Application Patch Management
- Host Security
 - Permissions
 - Access Control List
 - Antimalware
 - Host Software Baselineing
 - 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

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

MODULO 10 MALWARE, VULNERABILITÀ E MINACCE

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

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

MODULO 11 SOCIAL ENGINEERING E ALTRI NEMICI

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

- 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

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

MODULO 1: INTRODUZIONE ALL'ETHICAL HACKING

- Hacking: l'evoluzione
- Chi è l'Ethical Hacker?

MODULO 2: FOOTPRINTING

- Gli step dell'Ethical Hacking
- Cosa è il Footprinting?
- Terminologia del Footprinting
- Minacce introdotte dal Footprinting
- Il processo di Footprinting
- OS Fingerprinting

MODULO 3: SCANNING

- Significato di Scanning
- Checking for Live Systems
- Analisi dello stato delle Porte
- Contromisure utilizzate
- Vulnerability Scanning
- Mapping the Network
- Usare sistemi Proxies
- Passaggi essenziali nei processi di penetration test

MODULO 4: ENUMERATION

- Cosa significa Enumeration in un penetration test
- Uso di "Windows Enumeration"
- Linux Basic
- Enumeration con SNMP
- Linux Enumeration
- LDAP in Enumeration
- Uso di NTP in Enumeration
- Uso di SMTP Enumeration

MODULO 5: SYSTEM HACKING

- Uso del "System Hacking"
- Passaggi essenziali nei processi di "Hacking"
- Analisi dei tipi di Malware
- Cosa sono gli Sniffers e loro uso

- Utilizzo dei “Network Sniffing”

MODULO 6: SOCIAL ENGINEERING

- Significato di “Social Engineering”
- Dal Social Networking al Gathering Information
- Minacce comunemente impiegate
- Furto d’Identità
- Phishing

MODULO 7: DENIAL OF SERVICE

- Analisi attacchi in DDoS
- DDoS Tools
- DoS Strategia di difesa
- DoS Considerazioni nel Pen-Testing

MODULO 8: SESSION HIJACKING

- Utilizzo di tecniche di “Hijacking”
- Browser Hijacking
- Strategia dell’attacco
- Tecniche e Strategie di difesa

MODULO 9: WEB SERVERS AND APPLICATIONS

- Analisi di un sistema “Client-Server “
- Utilizzo delle Web application
- Analisi dell’Application server
- Hacking Web application e Application server

MODULO 10: SQL INJECTION

- Introduzione a MySQL
- Analisi delle falle di sicurezza di un sistema
- Le applicazioni web e i DBMS SQL
- Introduzione alle tecniche del “SQL Injection”

MODULO 11: HACKING WI-FI AND BLUETOOTH

- Tecniche di Wireless Network
- Strumenti di hacking wireless
- Strumenti hacking bluetooth

MODULO 12: MOBILE DEVICE SECURITY

- Analisi dell'architettura dei modelli Mobile OS
- Elementi di "Mobile Security"
- Device Security Models
- Attacchi Security Mobile
- Uso di tools per attacchi e difesa

MODULO 13: EVASION

- Tecniche per l'uso degli Honeypot
- Distro honeypot
- Difesa con uso honey-D
- Strategie di intelligence informatica
- Uso Osint
- Uso dei Firewalls come difesa degli attacchi

MODULO 14: CLOUD TECHNOLOGIES AND SECURITY

- Cos'è un cloud
- Tipologie cloud
- Sicurezza nel cloud

MODULO 15: PHYSICAL SECURITY

- Introduzione Physical Security
- Leggi all'uso della sicurezza
- Uso delle regole per una buona Physical Security
- Protezioni delle aree di pertinenza

MODULO 16: MOBILE SECURITY

- Il sistema operativo Android
- Il sistema operativo Apple iOS
- Diversi tipi di applicazioni mobili
- Le principali applicazioni mobili per la sicurezza
- L'impatto della sicurezza delle applicazioni mobili
- La metodologia di test di penetrazione delle applicazioni mobili
- Legge privacy: BYOD
- Utilizzare la distro Santoku per l'analisi dei sistemi mobili
- Utilizzare la distro "Android Tamer 4" per Malware Analysis, Penetration Testing e Reverse Engineering.
- Emulatori per dispositivi mobili
- Analisi Forense dei dispositivi