ProconsulAcademy

Programma Corso di Formazione Digital Security

Tool e ambienti software utilizzati

- Distribuzioni Linux orientate alla security
- Cisco Packet Tracer (Design e simulazione di reti)
- Wireshark (Analisi di rete, sniffing, scomposizione data frame)
- NMAP (Identificazione Host e analisi dei servizi)
- IP Tables (Creazione e simulazione policy di firewalling)
- Saranno predisposte opportune sessioni *hands-on* su ambienti SIEM, SOAR e IAM le cui piattaforme di riferimento saranno identificate durante lo svolgimento del programma di formazione

Modulo 1 - Linux OS

Obiettivo di questo modulo è fornire le informazioni per installare, configurare e amministrare un sistema Linux. Fornire inoltre una base di preparazione sistemistica orientata ad amministratori di sistema, affrontare problematiche reali, confrontare Linux con altri sistemi operativi e fare diretti riferimenti al mondo Internet.

Contenuti:

Fondamenti di Linux

- Introduzione al SO, installazione e configurazione di base.
- Interazione con il FS.
- *User profilig*, *permissions* e *attributes*.
- Editing e manipolazione di testi.
- Gestione dei processi.
- Bash shell scripting.
- Gestione aggiornamenti e pacchetti.
- Virtualizzazione.
- Servizi (SSH, FTP ,…).
- Linux OS *client-server architectures*
- Amministrazione rete - Elementi base e comandi *Shell*

MODULO 2 – Infrastrutture di networking

Obiettivo di questo modulo e fornire tutte le competenze necessarie a supportare e implementare architetture di sistemi e reti aziendali operativamente sostenibili, altamente disponibili e soprattutto sicure. Verranno forniti gli strumenti per identificare e tradurre i requisiti in un'architettura tecnica completa. Durante tutto il modulo sarà posto sempre un particolare accento nell'ambito dell'identificazione e risoluzione degli incident di sicurezza. Verranno infine illustrate le metodologie di monitoraggio, di misurazione e il reporting delle prestazioni e della capacità dei sistemi aziendali.

ProconsulAcademy

Contenuti:

Foundamentals

- Networking Basics
- Network Architecture
- TCP-IP/OSI Model
- Comparison Between TCP-IP/OSI Model
- Binary To Decimal Conversion
- Basic Overview Of Ip
- Introduction To Ipv6
- Classfull Ip Address
- Introduction To Tcp-Ip First Lvl
- Computer Cables Intoduction
- Unshielded Twisted Pair Cable
- Shielded Twisted Pair Cable Fiber Optic Cable
- Network Devices Introduction Switch & Router
- Static Routing Theory
- Lab: Configure Static Routing Ipv4
- Configure Ipv6 Address
- Lab: Configure Static Routing Ipv6

Routing & switching

- Administrative Distance
- Dynamic Routing
- Protocol
- Interior Routing Protocol
- Link State
- Basi di Ospf
- Vlan
- Subnet
- Vlan Trunking

Advanced Routing & switching

- Distance Vector
- Routing Information Protocol
- Elementi avanzati di Ospf
- Introduction To Cisco Packet Tracer
- Lab: Cisco Packet Tracer
- Nat/Pat
- Lab: Cisco Packet Tracer
- Lab: Vlan Trunking

Application layer

- Arp, Icmp, Tcp
- Dns
- Dhcp
- Http/Https
- Ftp/Ftps

- Introduction To Virtualization
- Introduction To Windows
- Lab: Windows Networking

Principi di network & infrastructure security

- Computer Security: History
- Computer Security: Principles
- Mobile Security
- Introduction To Cryptography
- Symmetric Cryptography
- Lab: Sym Crypto
- Asymmetric Cryptography
- Lab: Asym Crypto
- Hash Function
- Lab: Hash Function
- Proxy
- Vpn
- Remote Access Vpn
- Site-To-Site Vpn

Cyber attacks – Analisys

- Introduzione al *Blue Teaming*
- Sw/Network Vulnerabilities & Threats
- Osi Lvl 2/3: Attacks
- Lab: Lvl 2/3 Attacks
- Dns Attacks
- Lab: Dns Attacks
- Linux Security: Os, Access Control Policy
- Windows Security: Os, Access Control Policy

Cyber attacks – Mitigation

- Malware Overview
- Malware Analysis/Threat Hunting
- Tcp/Udp Attacks
- Lab: Tcp/Udp Attacks
- Web Application Attacks
- Lab: Web Applications
- Linux Security: Os, Access Control Policy
- Windows Security: Os, Access Control Policy

Defensive Hardware & Software – fondamenti

- Secure Network Infrastructure
- Waf
- Npt, Procedure Checklist, Mitigation And Remediation
- Balancer
- Firewall Introduction
- Ids/Ips Introduction
- Piattaforme di *logging* e monitoraggio

Analisi e trattamento dei Data Breach

- gdpr introduction and privacy concerns
- risk assessment
- data protection and impact assessment
- dealing with data breaches
- cloud introduction
- cloud security
- gdpr: dealing with data in cloud
- penalties for non-compliance
- Configuration, Provisioning & Fine Tuning
- Logging And Advanced Troubleshooting

MODULO 3 – Alert Analysis

Durante lo svolgimento di questo modulo verranno sviluppati i temi relativi all'analisi di 1° e 2° livello relativamente ai concetti di base della gestione del rischio in un contesto infrastrutturale complesso. Obiettivo è descrivere l'architettura SOC, la tassonomia degli incidenti e illustrare le procedure di gestione degli eventi. Dettagliare i controlli di sicurezza, le logiche di gestione degli incidenti di sicurezza IT e Service Level Agreement (SLA) correlati. Verrà fornita inoltre una panoramica delle policy aziendali in merito a: l'utilizzo corretto delle risorse IT, la navigazione Web, le best practice e DO's & DONT's.

Contenuti:

Protocolli applicativi e porte

- Tipologia di porte e loro caratteristiche
- IANA
- HTTP/S
- FTP/S
- SSH
- SMTP

Strutture dati e piattaforme SO

- Dati non strutturati in ambiente Windows.
- Elementi di amministrazione e profilazione in ambiente Windows.
- Linux architetture & file system.
- Gestione dati non strutturati in ambiente Linux.
- Elementi di amministrazione e profilazione in ambiente Linux.

Modello di architettura e ruoli

- 3-Tiers *architecture model*
- Introduzione alle web application
- Front End
- Back End

- Client

Tipologie di attacchi

- Malware
- Adware
- Cookies Attacks
- DDos
- Phishing
- SQL Injection
- Cross-site scripting
- Sniffing
- Brute force attack
- User enumeration
- Social engineering

Defensive Hardware & Software

- Apparati Firewall
- Apparati IDS
- Antivirus
- ACL
- DMZ
- Proxy
- Balancer
- VPN

Detection, analysis e Recovery

- Piattaforme di monitoraggio e supporto (SIEM, SOAR, …)
- Breach and log analysis
- Threat Analysis
- Incident Response
- Ruoli e responsabilità, procedure di escalation e profili di intervento

Modulo 4 - Identity & Access Management

In questo modulo verranno fornite tutte quelle competenze necessarie a gestire l'intero processo (applicazione di policy appropriate, impiego di strumenti tecnologici e di integrazione - API) per gestire le informazioni riguardanti l'identità degli utenti e controllarne l'accesso alle risorse aziendali.

Contenuti:

Identity Management

- Introduzione IDM framework
- Customer Digital Identity e Workforce Digital Identity
- Life·cycle e trasformazione di una digital identity
- Trusted source e riconciliazione di identità
- Target system provisioning e riconciliazione di accounts
- Workflow approvativi
- Roles, Policies e regole SoD
- Access Review e Certification process

Access Management

- Introduzione AM framework
- Web Application protection
- Reverse proxy ed agent
- Identitystore ed LDAP
- Web Single Sign On
- Authentication e Authorization (RBAC/ABAC)
- Adaptive authentication (risk based)
- Multifactor authentication
- SAML Federation Identity e Service Provider
- Introduzione alle modalità di Passwordless Authentication
- Definizione e utilizzo di JWT Tokens
- Introduzione ai protocolli standard OAuth, OpenID, FIDO2

IAM Compliance Regulations

- Introduzione a: PSD2, GDPR, NIST, PCI DSS, SOX, HIPAA

Piattaforme IAM

- Installazione e configurazione di piattaforme di Identity Access Management
- Introduzione ed uso di piattaforme di Identity Access Management