ProconsulAcademy

Corso Formativo Cybersecurity Technician

Modulo 1: Sistemi Operativi (Linux e Windows)

1. **Introduzione ai Sistemi Operativi**: Definizione e funzione di un sistema operativo, introduzione ai principali OS (Linux, Windows) e al loro ruolo nella gestione delle risorse hardware e software.
2. **Architettura di Linux e Windows**Panoramica dell'architettura a strati dei sistemi operativi, con particolare attenzione alle differenze tra kernel monolitico (Linux) e ibrido (Windows).
3. **Installazione e configurazione di Linux**: Guida pratica all'installazione e configurazione di distribuzioni Linux comuni come Ubuntu, CentOS, gestione delle partizioni, e configurazioni iniziali.
4. **Installazione e configurazione di Windows Server**: Istruzioni per l'installazione di Windows Server, inclusa la configurazione di ruoli server come Active Directory e DNS.
5. **Gestione dei pacchetti in Linux**: Introduzione ai sistemi di gestione dei pacchetti (APT, YUM, RPM), installazione, aggiornamento e rimozione di software.
6. **File system e permessi in Linux**: Struttura del file system in Linux, gestione dei permessi e proprietà dei file, comandi chmod e chown.
7. **File system e permessi in Windows**: NTFS e FAT, gestione delle autorizzazioni nei file e cartelle, differenze tra permessi a livello di file system e permessi di condivisione.
8. **Gestione dei processi e multitasking**: Introduzione ai processi in esecuzione, gestione delle priorità dei processi e differenze tra multitasking cooperativo e preemptive.
9. **Virtualizzazione (Hyper-V, KVM, VMware)**: Tecnologie di virtualizzazione più comuni e come vengono implementate in Linux e Windows, vantaggi e usi pratici.
10. **Gestione degli utenti e gruppi**: Creazione e gestione di utenti e gruppi, gestione dei permessi di accesso e dei privilegi amministrativi.
11. **Controllo degli accessi in Linux**: Utilizzo di strumenti avanzati come SELinux e AppArmor per la gestione della sicurezza e dei permessi di accesso.
12. **Group Policy in Windows**: Strumenti di gestione centralizzata delle configurazioni e dei permessi tramite le Group Policy di Windows Server.
13. **Automazione con shell scripting**: Introduzione a Bash scripting in Linux e PowerShell in Windows per automatizzare attività di amministrazione e gestione.
14. **Monitoraggio e gestione delle risorse**: Uso di strumenti come top, htop per Linux e Task Manager per Windows per monitorare CPU, memoria e altre risorse di sistema.
15. **Backup e ripristino in Linux e Windows**: Strumenti e strategie per il backup e il ripristino dei dati, inclusi backup incrementali e pianificazione dei backup.
16. **Hardening del sistema operativo**: Tecniche per rafforzare la sicurezza del sistema operativo, inclusa la rimozione di servizi non necessari e la configurazione di firewall.

17. **Gestione dei log e troubleshooting**: Come visualizzare e interpretare i log di sistema per diagnosticare problemi e risolverli in modo efficiente.
18. **Servizi di rete di base** : Configurazione e gestione dei servizi di rete come SSH, DNS, FTP, NFS su Linux e SMB su Windows.
19. **Introduzione a Docker e containerizzazione**: Introduzione alla containerizzazione, come creare e gestire container Docker per l'isolamento e la portabilità delle applicazioni.
20. **Aggiornamenti e patch management**: Processi per mantenere un sistema aggiornato con le ultime patch di sicurezza, gestione degli aggiornamenti automatici.

Modulo 2: Networking

1. **Introduzione ai concetti di rete**: Panoramica sulle reti di computer, tipi di reti (LAN, WAN, MAN), e il ruolo dei protocolli di rete.
2. **Modello OSI e TCP/IP**: Descrizione dei livelli del modello OSI e il loro ruolo nelle comunicazioni di rete, con particolare attenzione alla suite di protocolli TCP/IP.
3. **Indirizzamento IP e subnetting**: Introduzione agli indirizzi IPv4 e IPv6, subnetting, e creazione di reti IP efficienti.
4. **Protocolli di rete (IP, TCP, UDP)**: Differenze tra i protocolli TCP e UDP, caratteristiche e usi dei principali protocolli di rete.
5. **Routing statico e dinamico**: Introduzione ai concetti di routing, differenze tra routing statico e dinamico, e configurazione di protocolli come OSPF e BGP.
6. **NAT e PAT (Network Address Translation)**: Come NAT e PAT permettono la mappatura degli indirizzi IP privati in indirizzi IP pubblici per consentire la comunicazione con Internet.
7. **VLAN e segmentazione di rete**: Introduzione alle VLAN per la segmentazione della rete e il miglioramento della sicurezza e dell'efficienza.
8. **Configurazione di switch e router**: Configurazione di base di switch e router Cisco (o altri vendor), inclusa la gestione di interfacce, VLAN e routing.
9. **DHCP, DNS, e configurazione di servizi di rete**: Configurazione di server DHCP per l'assegnazione dinamica degli indirizzi IP e configurazione di server DNS per la risoluzione dei nomi.
10. **Firewall e sicurezza perimetrale**: Concetti di firewall, tipi di firewall (stateful, stateless), e come implementare una sicurezza perimetrale efficace.
11. **VPN e tunneling**: Panoramica sulle Virtual Private Network (VPN) e le tecniche di tunneling per creare connessioni sicure su reti non affidabili.
12. **Reti wireless (Wi-Fi e sicurezza)**: Configurazione delle reti Wi-Fi, protocolli di sicurezza wireless (WPA, WPA2, WPA3), e come proteggere una rete wireless.
13. **Configurazione di reti IPv**: Introduzione a IPv6, indirizzamento e subnetting IPv6, e configurazione di reti utilizzando il nuovo protocollo.
14. **Troubleshooting di rete:** Strumenti di diagnostica di rete come ping, traceroute, e netstat per risolvere problemi di connettività.

15. **Analisi del traffico di rete (Wireshark)**: Utilizzo di strumenti di analisi del traffico di rete come Wireshark per monitorare e analizzare i pacchetti.
16. **QoS (Quality of Service):** Implementazione di QoS per garantire la priorità del traffico di rete critico, gestione della larghezza di banda e delle code.
17. **Load balancing e failover:** Configurazione di tecniche di bilanciamento del carico e failover per migliorare la disponibilità e la resilienza della rete.
18. **Reti SDN (Software-Defined Networking)**: Introduzione alle reti definite dal software e come permettono la gestione e la configurazione centralizzata delle reti.
19. **Tecniche di segmentazione e separazione di rete**: Come MPLS e VPN vengono utilizzati per segmentare e separare le reti e garantire prestazioni e sicurezza.
20. **Sicurezza di rete (IDS/IPS, NAC)**: Implementazione di tecnologie di sicurezza come Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), e Network Access Control (NAC).

Modulo 3: Cloud

1. **Introduzione al cloud computing:** Panoramica su cosa sia il cloud computing, i suoi vantaggi e svantaggi, e come ha trasformato l'IT moderno.
2. **Modelli di servizio: IaaS, PaaS, SaaS:** Differenze tra Infrastructure as a Service (IaaS), Platform as a Service (PaaS), e Software as a Service (SaaS) e quando utilizzarli.
3. **Modelli di deployment: Public, Private, Hybrid Cloud**: Confronto tra i vari modelli di implementazione del cloud e quali sono più adatti a determinati scenari aziendali.
4. **Introduzione ad AWS, Azure e Google Cloud**: Panoramica sui principali provider di cloud pubblico e sulle loro offerte di base.
5. **Creazione e gestione di istanze virtuali nel cloud**: Come creare, configurare e gestire istanze EC2 in AWS, VM in Azure e Compute Engine in Google Cloud.
6. **Storage nel cloud**: Introduzione ai diversi tipi di storage nel cloud come Amazon S3, Azure Blob Storage, Google Cloud Storage e concetti di archiviazione a lungo termine.
7. **Networking nel cloud**: Configurazione e gestione delle reti cloud, VPC (Virtual Private Cloud), subnet e gruppi di sicurezza per garantire la sicurezza e la connettività.
8. **Gestione delle risorse cloud (IAM, RUoli e permessi)**: Gestione degli utenti e dei ruoli nel cloud, concetti di Identity and Access Management (IAM).
9. **Load balancing e auto-scaling nel cloud**: Configurazione del bilanciamento del carico e l'auto-scaling per garantire alta disponibilità e scalabilità automatica.
10. **Backup e disaster recovery nel cloud**: Strategie di backup nel cloud e opzioni di ripristino in caso di disastri per garantire la continuità operativa.
11. **Monitoraggio e logging nel cloud**: Utilizzo di strumenti come AWS CloudWatch e Azure Monitor per il monitoraggio continuo delle risorse e la gestione dei log.
12. **Automazione e infrastruttura come codice (Terraform, CloudFormation)**: Introduzione all'automazione dell'infrastruttura con strumenti come Terraform e AWS CloudFormation.

13. **Serverless computing (Lambda, Functions)**: Introduzione al computing serverless, come AWS Lambda e Azure Functions, e i loro vantaggi per lo sviluppo rapido e scalabile.
14. **Microservizi e container nel cloud**: Come utilizzare Docker e Kubernetes per distribuire microservizi nel cloud in modo efficiente e scalabile.
15. **Sicurezza nel cloud**: Panoramica delle pratiche di sicurezza nel cloud, inclusa la crittografia, la gestione delle chiavi e la responsabilità condivisa.
16. **Gestione dei costi e ottimizzazione delle risorse nel cloud**: Come monitorare e ottimizzare l'utilizzo delle risorse cloud per ridurre i costi e migliorare le prestazioni.
17. **Introduzione al cloud ibrido e multi-cloud**: Come gestire ambienti multi-cloud e ibridi per garantire la flessibilità e ridurre la dipendenza da un singolo fornitore.
18. **Strategie di migrazione al cloud**: Pianificazione e implementazione della migrazione delle infrastrutture IT esistenti nel cloud, con attenzione a compatibilità e sicurezza.
19. **Database nel cloud (RDS, DynamoDB, Cosmos DB)**: Come configurare e gestire database nel cloud, inclusi servizi relazionali e non relazionali.
20. **Monitoraggio continuo e auditing nel cloud**: Implementazione di processi di monitoraggio e auditing per garantire che le risorse nel cloud siano sicure e conformi.

Modulo 4: DevOps

1. **Introduzione al DevOps**: Panoramica dei principi DevOps e del ciclo di vita del software.
2. **Principi di integrazione e distribuzione continua (CI/CD)**: Introduzione ai concetti di CI/CD e al loro ruolo nel migliorare l'efficienza del team di sviluppo.
3. **Versionamento del codice con Git e GitHub**: Uso di Git e GitHub per il versionamento del codice e gestione delle modifiche.
4. **Automazione con Jenkins, GitLab CI**: Implementazione di pipeline CI/CD automatizzate utilizzando Jenkins o GitLab CI per automatizzare la build e il testing del codice.
5. **Gestione dei container con Docker**: Introduzione a Docker per la creazione, gestione e distribuzione di container che facilitano la portabilità delle applicazioni.
6. **Orchestrazione con Kubernetes**: Introduzione a Kubernetes per l'orchestrazione dei container, gestione dei cluster e distribuzione automatica.
7. **Infrastruttura come codice (IaC) con Terraform**: Uso di Terraform per definire e gestire l'infrastruttura IT come codice, facilitando la scalabilità e l'automazione.
8. **Gestione della configurazione (Ansible, Chef, Puppet)**: Strumenti di gestione della configurazione per automatizzare la configurazione di server e ambienti.
9. **Pipeline di deployment e automazione**: Creazione di pipeline automatizzate per distribuire applicazioni in ambienti di produzione e staging.
10. **Gestione delle release e rollback :**Strategie di gestione delle release di software e tecniche di rollback sicuro in caso di problemi.

11. **Monitoraggio continuo (Prometheus, Grafana, ELK Stack):** Implementazione del monitoraggio continuo di applicazioni e sistemi utilizzando Prometheus, Grafana e lo stack ELK.
12. **Log management e centralizzazione**: Tecniche per raccogliere, analizzare e centralizzare i log delle applicazioni e dei sistemi per la diagnosi e il troubleshooting.
13. **Testing automatizzato (unit test, integration test):** Creazione di test automatizzati, come test unitari e test di integrazione, per migliorare la qualità del software.
14. **Gestione delle dipendenze:** Utilizzo di strumenti di gestione delle dipendenze come Maven o NPM per garantire la coerenza delle build del software.
15. **Strategie di gestione delle build (Maven, Gradle)**: Configurazione di build automatizzate con strumenti come Maven o Gradle per gestire il ciclo di vita del software.
16. **Cloud DevOps con AWS, Azure DevOps**: Strumenti e servizi specifici per il DevOps nel cloud, inclusi AWS CodePipeline e Azure DevOps.
17. **Security DevOps (DevSecOps)**: Introduzione a DevSecOps per integrare la sicurezza nel processo DevOps, con particolare attenzione al testing di sicurezza automatizzato.
18. **Continuous delivery e continuous deployment**: Differenze tra continuous delivery e continuous deployment e come implementare entrambe le strategie.
19. **Performance tuning e ottimizzazione**: Tecniche di ottimizzazione delle performance per garantire che il codice sia efficiente e scalabile.
20. **Feedback loop e miglioramento continuo**: Come implementare cicli di feedback rapidi e continui per migliorare i processi di sviluppo e distribuzione.

Modulo 5: Sicurezza Difensiva

1. **Introduzione alla sicurezza informatica:** Panoramica sui concetti fondamentali della sicurezza informatica, compresi i tipi di minacce e le contromisure di difesa.
2. **Principi di difesa in profondità**: Implementazione di strategie di sicurezza a più livelli per proteggere i sistemi IT da minacce diverse.
3. **Firewall e protezione perimetrale**: Configurazione e gestione dei firewall per proteggere le reti da traffico non autorizzato o dannoso.
4. **Intrusion Detection and Prevention Systems (IDS/IPS)**: Introduzione ai sistemi di rilevamento e prevenzione delle intrusioni per monitorare e bloccare attività sospette.
5. **Controllo degli accessi e autenticazione forte (2FA, MFA)**: Implementazione di misure di sicurezza avanzate per la gestione dell'autenticazione e del controllo degli accessi.
6. **Protezione delle reti wireless**: Best practice per proteggere le reti wireless, inclusa la configurazione sicura e l'uso di crittografia.
7. **Crittografia (AES, RSA, SSL/TLS)**: Introduzione ai principali algoritmi di crittografia e ai loro utilizzi per proteggere dati in transito e a riposo.
8. **Sicurezza delle applicazioni web (OWASP Top 10)**: Esplorazione delle principali vulnerabilità delle applicazioni web e come mitigarle.

9. **Sicurezza endpoint (antivirus, EDR)**: Tecniche di protezione per i dispositivi finali, inclusi antivirus, firewall personali, e soluzioni EDR (Endpoint Detection and Response).
10. **Incident response e gestione degli incidenti**: Creazione di un piano di risposta agli incidenti per affrontare attacchi informatici e violazioni della sicurezza.
11. **Analisi forense digitale**: Tecniche per raccogliere, analizzare e preservare prove digitali durante un'indagine post-attacco.
12. **Sicurezza dei database**: Metodi per proteggere i database da accessi non autorizzati e minacce interne, inclusa la crittografia dei dati.
13. **Backup sicuro e disaster recovery**: Strategie per la creazione di backup sicuri e la pianificazione del disaster recovery in caso di emergenza.
14. **Patch management e aggiornamenti di sicurezza**: Come gestire e applicare patch e aggiornamenti di sicurezza in modo tempestivo per mitigare vulnerabilità.
15. **Protezione dai malware e ransomware**: Strategie per prevenire, rilevare e mitigare le minacce malware, inclusi ransomware.
16. **Network Access Control (NAC)**: Implementazione di politiche di controllo degli accessi alla rete per garantire che solo dispositivi autorizzati accedano alle risorse.
17. **Sicurezza mobile e BYOD**: Protezione dei dispositivi mobili e gestione delle politiche Bring Your Own Device (BYOD) nelle organizzazioni.
18. **Compliance e normative (GDPR, PCI-DSS)**: Conformità alle normative di sicurezza e privacy, come il GDPR e lo standard PCI-DSS per la protezione dei dati sensibili.
19. **Penetration testing difensivo**: Tecniche per testare la sicurezza delle infrastrutture IT simulando attacchi reali per identificare vulnerabilità.
20. **Threat hunting e intelligence** : Introduzione alla ricerca delle minacce e all'uso dell'intelligence di sicurezza per anticipare attacchi informatici.

Modulo 6: Sicurezza Offensiva

1. **Introduzione all'hacking etico**: Panoramica sull'hacking etico e le sue finalità, con enfasi sulle responsabilità legali ed etiche.
2. **Metodologie di penetration testing (Recon, Scanning, Exploitation):** Le fasi di un penetration test, dalla ricognizione iniziale allo sfruttamento delle vulnerabilità.
3. **Ricognizione attiva e passiva**: Tecniche per raccogliere informazioni su obiettivi senza interagire direttamente con i sistemi (passiva) e con interazione (attiva).
4. **Vulnerability scanning e assessment (Nessus, OpenVAS)**: Utilizzo di strumenti di scanning per identificare vulnerabilità nei sistemi e valutare il rischio.
5. **Exploitation e sviluppo di exploit**: Tecniche per sfruttare le vulnerabilità e sviluppare exploit personalizzati per eseguire codice malevolo.
6. **Social engineering e phishing**: Tecniche di manipolazione psicologica, come il phishing, per ingannare le persone e ottenere informazioni sensibili.

7. **Attacchi di rete (ARP Spoofing, DNS Poisoning)**: Attacchi mirati alla manipolazione del traffico di rete, come l'ARP Spoofing e il DNS Poisoning.
8. **Password cracking e bruteforce**: Tecniche per forzare le password utilizzando attacchi di forza bruta o dizionari.
9. **Exploiting Web Application Vulnerabilities (SQL Injection, XSS)**: Tecniche per sfruttare vulnerabilità nelle applicazioni web, come SQL Injection e Cross-Site Scripting (XSS).
10. **Attacchi a reti wireless**: Tecniche per compromettere la sicurezza delle reti Wi-Fi, inclusi attacchi WEP/WPA cracking.
11. **Privilege escalation e pivoting**: Tecniche per ottenere privilegi più elevati in un sistema e spostarsi lateralmente all'interno di una rete compromessa.
12. **Post-exploitation e mantenimento dell'accesso**: Strategie per mantenere l'accesso a un sistema compromesso e nascondere l'attività malevola.
13. **Tecniche di evasione degli antivirus** : Tecniche avanzate per eludere i rilevamenti antivirus e altri sistemi di difesa.
14. **Attacchi a container e orchestratori (Docker, Kubernetes)**: Attacchi mirati a container Docker e orchestratori come Kubernetes, sfruttando configurazioni deboli.
15. **Attacchi a reti cloud**: Tecniche per compromettere ambienti cloud, sfruttando vulnerabilità specifiche delle infrastrutture cloud.
16. **Red teaming e simulazioni di attacchi** : Introduzione alle operazioni di Red Teaming, simulazioni di attacchi reali per testare la sicurezza dell'organizzazione.
17. **Scrittura di report di penetration testing**: Come scrivere report di penetration testing dettagliati, chiari e utili per i team di sicurezza.
18. **Strumenti di exploit (Metasploit, Burp Suite)**: Utilizzo di strumenti standard come Metasploit e Burp Suite per eseguire test di sicurezza offensivi.
19. **Reverse engineering e analisi di malware**: Tecniche per analizzare e comprendere il funzionamento di software malevolo attraverso il reverse engineering.
20. **Introduzione al bug bounty**: Panoramica sui programmi di bug bounty, come funzionano e come partecipare per trovare vulnerabilità.

Modulo 7: Sistemistica

1. **Introduzione alla gestione dei sistemi**: Panoramica sul ruolo dell'amministratore di sistema e delle tecnologie chiave per la gestione delle infrastrutture IT.
2. **Progettazione di infrastrutture IT**: Come progettare reti e sistemi informatici per supportare applicazioni aziendali e carichi di lavoro critici.
3. **Virtualizzazione avanzata (VMware, Hyper-V)**: Configurazione avanzata di ambienti virtualizzati utilizzando strumenti come VMware e Hyper-V per migliorare l'efficienza delle risorse.
4. **Gestione degli storage (SAN, NAS, RAID)**: Tecniche per configurare e gestire storage aziendali, inclusi Storage Area Networks (SAN), Network Attached Storage (NAS) e array RAID.

5. **Gestione avanzata delle reti (DHCP, DNS, VLAN)**: Configurazione e gestione avanzata di server DHCP e DNS, oltre alla segmentazione delle reti tramite VLAN.
6. **Active Directory e gestione delle identità**: Introduzione a Active Directory per la gestione centralizzata di utenti, gruppi e policy di sicurezza.
7. **Backup e ripristino (Veeam, Bacula**: Strategie per il backup e il ripristino dei dati, inclusi strumenti specifici come Veeam e Bacula.
8. **Monitoraggio dei sistemi (Nagios, Zabbix)**: Implementazione di sistemi di monitoraggio come Nagios e Zabbix per garantire la disponibilità e le prestazioni delle risorse IT.
9. **Pianificazione della capacità e scalabilità**: Tecniche per prevedere la capacità necessaria e scalare i sistemi per rispondere alla crescita aziendale.
10. **Gestione degli aggiornamenti e patching**: Come gestire e applicare aggiornamenti e patch per mantenere i sistemi sicuri e funzionanti.
11. **Automazione della gestione dei server (Ansible, Puppet)** : Utilizzo di strumenti di automazione come Ansible e Puppet per gestire in modo efficiente i server e distribuire configurazioni.
12. **Load balancing e alta disponibilità (HAProxy, F5)**: Implementazione di tecniche di bilanciamento del carico e alta disponibilità per garantire la continuità dei servizi.
13. **Bilanciamento del carico dei server web (Apache, Nginx)**: Configurazione di Apache e Nginx per distribuire il carico di traffico su più server e ottimizzare le prestazioni.
14. **Migrazione di dati e server**: Pianificazione e implementazione di migrazioni di server e dati tra ambienti fisici, virtuali e cloud.
15. **Troubleshooting e risoluzione dei problemi avanzata**: Tecniche avanzate per diagnosticare e risolvere problemi complessi su server e reti.
16. **Disaster recovery e continuità operativa**: Come pianificare ed eseguire strategie di disaster recovery per garantire la continuità operativa in caso di guasti.
17. **Ottimizzazione delle performance dei server**: Tecniche per monitorare e ottimizzare le prestazioni dei server, inclusa la gestione delle risorse e il tuning.
18. **Centralizzazione della gestione dei log (ELK Stack)**: Implementazione dello stack ELK (Elasticsearch, Logstash, Kibana) per raccogliere, analizzare e visualizzare i log di sistema.
19. **Monitoring del traffico di rete**: Utilizzo di strumenti per monitorare il traffico di rete e identificare problemi di connettività o prestazioni.
20. **Documentazione e best practices di gestione** : Creazione di documentazione accurata e seguire le best practices per garantire la gestione efficace e sicura dei sistemi.