PROVA SCRITTA - TRACCE D'ESAME

Profilo: Area dei Collaboratori, settore tecnico, informatico e dei servizi generali (Direzione Infrastrutture Digitali). **Formato:** Risposta aperta, massimo 1000 caratteri per domanda.

PROVA 1

Domanda 1: Architetture di rete e protocolli

Si descriva brevemente il concetto di VLAN (Virtual LAN) a livello 2 del modello OSI. Quali sono i vantaggi principali del suo utilizzo in una rete aziendale e in che modo è possibile far comunicare tra loro dispositivi appartenenti a VLAN differenti?

Domanda 2: Apparati di rete e di sicurezza

Quali sono le principali differenze architetturali e funzionali tra un Firewall tradizionale di tipo "Stateful Inspection" e un "Next-Generation Firewall" (NGFW)? Si citi inoltre la differenza operativa tra un sistema IDS e un IPS.

Domanda 3: Principi di sicurezza e D.Lgs. 138/2024

L'art. 24 del D.Lgs. 138/2024 richiede l'adozione di misure per la gestione dei rischi, includendo esplicitamente la "gestione degli incidenti" e la "continuità operativa". A livello sistemistico, quali pratiche o architetture consentono a un Ateneo di garantire il ripristino dei servizi in caso di grave attacco informatico (es. Ransomware)?

Domanda 4: Ambienti Microsoft e Identity Management

In un ambiente Microsoft, qual è la funzione di Active Directory Domain Services (AD DS) e per quale motivo è strettamente dipendente dal servizio DNS? Si accenni brevemente alla differenza tra l'infrastruttura AD locale (on-premise) e l'integrazione con Microsoft Entra ID.

Domanda 5: Ambienti virtualizzati

Si descrivano i ruoli fondamentali dei componenti di un'infrastruttura virtualizzata basata su VMware vSphere (es. ESXi e vCenter). Quali sono le accortezze da tenere presenti quando si utilizzano le *snapshot* nella gestione del ciclo di vita di una macchina virtuale?

Domanda 6: Monitoraggio della cybersecurity

Perché il monitoraggio continuo è cruciale nell'infrastruttura IT di un Ateneo? Si indichino almeno tre tipologie di log o eventi (di rete o di sistema) che dovrebbero essere prioritariamente raccolti in un sistema centralizzato (es. SIEM) per rilevare tempestivamente anomalie.

PROVA 2

Domanda 1: Architetture di rete e protocolli

Si spieghi lo scopo del *subnetting* in una rete IP. Inoltre, come viene utilizzata una Access Control List (ACL) a livello di un apparato di routing per filtrare e mettere in sicurezza il traffico tra due subnet differenti?

Domanda 2: Apparati di rete e di sicurezza

Si descriva il funzionamento generale di una Virtual Private Network (VPN). Qual è la differenza principale, in termini di casi d'uso e protocolli tipicamente impiegati, tra una VPN "Site-to-Site" e una VPN "Remote Access"?

Domanda 3: Principi di sicurezza e D.Lgs. 138/2024

Tra le misure previste dall'art. 24 del D.Lgs. 138/2024 figurano il controllo degli accessi e l'uso dell'autenticazione a più fattori (MFA). Si spieghi perché l'MFA è un requisito essenziale per gli account amministrativi. In questo contesto, come si inserisce il "Principio del Minimo Privilegio" (PoLP)?

Domanda 4: Ambienti Microsoft Windows

Si descriva sinteticamente il processo di assegnazione degli indirizzi IP tramite protocollo DHCP in un ambiente Windows (fasi DORA). In ambito gestione client, qual è l'utilità delle Group Policy Object (GPO) implementate tramite Active Directory?

Domanda 5: Ambienti virtualizzati (VMware)

In un cluster VMware vSphere, quali vantaggi offrono le funzionalità di *vMotion* e *High Availability* (HA)? Si spieghi la differenza di comportamento tra le due tecnologie in caso di guasto hardware improvviso di un host ESXi.

Domanda 6: Monitoraggio della cybersecurity

Nell'ambito del monitoraggio proattivo, qual è la differenza tecnica e procedurale tra un *Vulnerability Assessment* e un *Penetration Test*? Perché il Vulnerability Assessment dovrebbe essere un'attività ciclica in un'infrastruttura esposta?

PROVA 3

Domanda 1: Architetture di rete e protocolli

Facendo riferimento al modello OSI, si spieghi la differenza fondamentale tra l'inoltro di pacchetti a livello 2 (Switching) e a livello 3 (Routing). Quali informazioni (header) vengono lette dagli apparati per prendere le decisioni di inoltro in questi due livelli?

Domanda 2: Apparati di rete e di sicurezza

In una moderna architettura enterprise, quando è necessario e tecnicamente giustificato utilizzare uno switch "Layer 3" rispetto a un tradizionale switch "Layer 2"? Quali sono vantaggi e svantaggi nell'utilizzare protolli di livello 3 o di livello 2?

Domanda 3: Principi di sicurezza e D.Lgs. 138/2024

L'art. 24 del D.Lgs. 138/2024 impone l'adozione di politiche sull'uso della crittografia. Si definisca la differenza tra la protezione dei "dati a riposo" (Data at Rest) e dei "dati in transito" (Data in Transit). Quali tecnologie o protocolli si implementano per soddisfare queste due esigenze?

Domanda 4: Ambienti Microsoft Windows

Il servizio DNS è fondamentale in ambiente Microsoft. Si descrivano brevemente le funzioni dei record DNS di tipo "A", "CNAME" e "MX". Quale strumento a riga di comando si utilizza comunemente in Windows per testare la risoluzione dei nomi?

Domanda 5: Ambienti virtualizzati (VMware)

Si illustri il concetto di Virtual Switch (vSwitch) in un ambiente VMware vSphere. In che modo un vSwitch si interfaccia con le schede di rete fisiche (uplink) del server host per far comunicare le macchine virtuali con la rete fisica di Ateneo?

Domanda 6: Monitoraggio della cybersecurity

Se il sistema di monitoraggio rileva un'esecuzione sospetta e una rapida crittografia dei file su un file server (potenziale attacco Ransomware), quali sono le primissime azioni tecniche e di contenimento che un sistemista dovrebbe eseguire?