Compito n. 2

Il candidato risponda alle seguenti domande a risposta multipla

1. In un cloud pubblico con organizzazione multi-account (come AWS Organizations o Azure Management Groups), il modo più efficace per impedire globalmente l'uso di servizi non autorizzati, indipendentemente dai ruoli locali, è:
   A. Tag obbligatorie sugli account
   B. Policy a livello di singolo progetto/resource group
   C. Ruoli "Owner" ovunque ma con audit severo
   D. Implementazione di un ruolo unico di super-amministratore in ogni account membro
   E. Guardrail a livello di organizzazione (Service Control Policies / Deny ereditati)

2. In un Active Directory moderno su VM, quale meccanismo mitiga il rischio di USN rollback dopo il ripristino di uno snapshot?
   A. Disabilitare NTP
   B. Aumentare RID pool a mano
   C. VM-Generation ID: rigenera invocationID e forza non-authoritative sync
   D. Deframmentazione offline del database NTDS
   E. Bloccare la replica in entrata/uscita per 24 ore e usare il comando repadmin /force

3. Qual è la funzione del record CNAME in un dominio DNS?
   A. Specifica i nomi dei server mail principali da contattare per l'invio e la ricezione di posta elettronica.
   B. Mappa un nome di dominio su un altro nome canonico per creare un alias per l'host.
   C. Definisce la priorità con un valore numerico per i server MX (Mail Exchanger) in caso di failover.
   D. Indica la durata massima di caching per la risposta di tutti i record sul resolver DNS (Time To Live).
   E. Mappa un nome di dominio su un indirizzo IP numerico (IPv4) utilizzato per la risoluzione diretta.

4. Quale organo e' responsabile del perseguimento delle finalità dell'Università secondo criteri di qualità e nel rispetto dei principi di efficacia, efficienza, trasparenza e promozione del merito?

A. il Rettore

B. il Direttore generale

C. il Collegio dei revisori

D. il Presidio di Qualità

E. Il Presidente del Nucleo di valutazione

5. La normativa universitaria prevede che il Senato accademico:

A. se previsto come organo dallo Statuto di un'università statale deve essere soppresso, e le sue attribuzioni trasferite al Consiglio di amministrazione

B. è un organo che deve essere previsto dallo Statuto di tutte le università statali

C. è un organo facoltativo di tutte le università con sede nel territorio italiano

D. è un organo che prevede la partecipazione di un componente regionale

E. è un organo che prevede la partecipazione di un componente comunale

Il candidato risponda alla seguente domanda

L'Ateneo sta subendo un attacco informatico significativo. I primi segnali sono: traffico anomalo in uscita, il sito web principale, che si trova nella DMZ principale, è rallentato e il Firewall segnala numerosi tentativi di accesso non autorizzato verso l'indirizzo IP del server di posta, che si trova in una DMZ secondaria.

Il candidato:

- Individui sinteticamente i primi passi da compiere per mitigare l'attacco, isolare la minaccia e mitigare l'impatto sul sito web, utilizzando il Firewall e il Reverse Proxy. Spieghi la configurazione del Firewall (regole di ACL o Stateful Inspection) necessaria per proteggere la DMZ secondaria e il server di posta.
- Descriva brevemente come utilizzerebbe le competenze di analisi e controllo dei log (provenienti dal Firewall, dal server di posta e dagli Switches di rete) per identificare la natura e la fonte dell'attacco e stabilire se vi sia stata una compromissione interna.
- In risposta all'attacco, si rende necessario bloccare temporaneamente il traffico TCP in ingresso sulla porta 8080 sul *server di posta* in DMZ secondaria e verificare le sessioni attive sul router che interfaccia il GARR:

- Fornisca i **comandi Linux (iptables)** necessari per bloccare il traffico in ingresso sulla porta 8080 del server di posta.
- Fornisca il **comando Cisco IOS (o equivalente)** che utilizzerebbe sul **router di accesso al GARR** per visualizzare lo stato delle interfacce e i pacchetti scartati o gli errori.