UNIVERSITÀ DEGLI STUDI DI MILANO

CONCORSO PUBBLICO, PER TITOLI ED ESAMI, A N. 3 POSTI DI CATEGORIA C - AREA TECNICA, TECNICO-SCIENTIFICA ED ELABORAZIONE DATI, CON RAPPORTO DI LAVORO SUBORDINATO A TEMPO INDETERMINATO PRESSO L'UNIVERSITÀ DEGLI STUDI DI MILANO - DIREZIONE ICT, DI CUI N. 1 POSTO DA RISERVARE, PRIORITARIAMENTE, ALLE CATEGORIE DI CUI AL DECRETO LEGISLATIVO N.66/2010 - CODICE 22266

La Commissione giudicatrice della selezione, nominata con Determina Direttoriale n. 8923 del 31.5.2023, composta da:

Prof.ssa Elena Pagani	Presidente
Sig. Giancarlo Galluzzi	Componente
Dott. Massimo Frisoli	Componente
Dott.ssa Desiree Paolina Celeste Forcolini	Segretaria

comunica i quesiti relativi alla prova orale:

Quesiti – Gruppo 1

1. Il candidato definisca le caratteristiche e l'utilità di una VLAN (virtual LAN).
2. Il candidato descriva a cosa serve il parametro *netmask* presente nelle tabelle di instradamento di IP.
3. Il candidato illustri cosa si intende per attacco zero-day.
4. Il candidato illustri le differenze tra i meccanismi di protezione realizzati con Access Control List e con firewall.

Lettura e traduzione – lingua inglese
Tratto da NIST CSWP 20 – Planning for a Zero Trust Architecture: *A Planning Guide for Federal Administrators*

The enterprise monitors and measures the integrity and security posture of all owned and associated resources. This tenet deals with the aspects of cyber hygiene for both enterprise-owned resources and those that may not be owned, but used in an enterprise workflow such as configuration, patching, application loading, etc. The state of resources should be monitored, and appropriate action taken when new information such as a new vulnerability or attack is reported or observed. The confidentiality and integrity of data on the resource should be protected. This requires enterprise admins to know how resources are configured, maintained, and monitored.

Quesiti – Gruppo 2

1. Il candidato illustri in cosa consiste lo schema di indirizzamento CIDR (Classless Inter-Domain Routing) usato da IP.
2. Il candidato illustri il formato degli indirizzi di rete utilizzati dal protocollo IPv4.
3. Il candidato spieghi in che cosa consiste un attacco Man-in-the-Middle.
4. Il candidato motivi perché è più facile portare un attacco Denial-of-Service usando il protocollo UDP piuttosto che il protocollo TCP.

Lettura e traduzione – lingua inglese
Tratto da NIST CSWP 20 – Planning for a Zero Trust Architecture: *A Planning Guide for Federal Administrators*

All resource authentication and authorization are dynamic and strictly enforced before access is allowed. A typical enterprise has a wide collection of network identities: end users, accounts used by processes and services, etc. Some end users may have multiple network identities, and some identities may only be used by hardware/software components. The enterprise needs to have a governance policy and structure in place so that only authorized operations are performed, and only when the identity has properly authenticated itself. The enterprise needs to consider if their current identity governance policies are mature enough and where and how are authentication and authorization checks currently performed.

Dynamic enforcement means that other factors such as endpoint and environmental factors impact authentication and authorization policies.

Quesiti – Gruppo 3

1. Il candidato discuta le differenze tra uno switch e un router.
2. Il candidato descriva il funzionamento e l'utilità di NAT (Network Address Translation).
3. Il candidato illustri cosa è e come opera una Access Control List di un router.
4. Il candidato definisca che cosa è un *ransomware*.

Lettura e traduzione – lingua inglese
Tratto da NIST CSWP 20 – Planning for a Zero Trust Architecture: *A Planning Guide for Federal Administrators*

Access to individual enterprise resources is granted on a per-session basis. In an ideal zero trust architecture, every unique operation would undergo authentication and authorization before the operation is performed. For example, a delete operation following a read operation to a database should trigger an additional authentication and authorization check. This level of granularity may not always possible and other mitigating solutions such as logging and backups, may be needed to detect and recover from unauthorized operations. Enterprise administrators will need to plan how to enforce fine grain access policies on individual resources. If the security tools used by the enterprise do not allow this, other solutions such as logging, versioning tools, or backups may help achieve the desired access control outcome and manage this risk.

Milano, 23 giugno 2023

La Commissione

Prof.ssa Elena Pagani - Presidente

Sig. Giancarlo Galluzzi - Componente

Dott. Massimo Frisoli - Componente

Dott.ssa Desiree Paolina Celeste Forcolini - Segretaria