NSS Quiz

Date: 27 April, 2023

Q.) CRL = Certificate Revocation List (CRL)

Q.) Kerberos is \_\_\_\_\_\_\_\_\_\_\_ Protocol = **Authentication**

Q.) If there are N realms, then there must be **N(N –1)/2** secure key exchanges so that each realm can interoperate with all other Kerberos realms.

Q.) **Public-key certificate** offers solution of the issue discussed.

Weakness :

Anyone can forge such a public announcement.

That is, an attacker could pretend to be Bob and send a public key to another participant or broadcast such a public key.

Until such time as Bob discovers the forgery and alerts other participants, the forger is able to read all encrypted messages intended for Bob and can use the forged keys for authentication.

Q.) They allow an “end user” certificate to sign another certificate = **Proxy Certificate**

Q.) Securing Wireless Transmissions / Securing Wireless Network = Turn off identifier broadcasting:

Q.) ESS transition: Here, station moves from one ESS to another ESS

Q.) Association: -> Establishes an initial association between a station and an AP.

Q.) Discovery phase: An AP uses messages called Beacons and Probe Responses to advertise its IEEE 802.11i security policy.

Q.) Master agents : It is program that provides the interface between an SNMP Network Manager and a subagent.

----10----

Q.) can support a range of policies: centralized administration – A small number of privileged users may grant and revoke access rights. ownership-based administration - The owner (creator) of a table may grant and revoke access rights to the table. decentralized administration – In addition to granting and revoking access rights to a table, the owner of the table may grant and revoke authorization rights to other users, allowing them to grant and revoke access rights to the table.

Q.) records (rows) or columns (attributes) – best - also need attribute indexes to help data retrieval

Q.) Cloud Deployment Models: Public, Private, Community & Hybrid.

Q.) Cloud Provider: Iaas, Paas, Saas

Q.) In-network Processing is faster as Compared to Centralized Processing

Q.) **Privacy** is the control over the extent, timing, and circumstances of sharing oneself (physically, behaviourally, or intellectually) with others.

Q.) **Privacy Homomorphism** is encryption transformation that allows direct computation on encrypted data.

Q.) 12 protection bits: UNIX File Access Control

Q.) 1 is the sticky bit (only owner can remove, delete, …, a directory)

Q.) **Many-to-many** relationship between users and roles

----20----

Q.) RBAC0: min functionality

Q.) RBAC1: RBAC0 plus role (permission) inheritance

Q.) Biba Integrity Model: Modify, Observe, Execute, Invoke

Q.) BLP Mode Access Modes: Read, Append, Write & Execute

Q.) multiple full operating system instances execute in parallel = full virtualization

Q.) Increasing RAM is Not a Security Measure

Q.) True / False

Q.) True / False

Q.)

Q.)