Exam C

Saturday, October 21, 2023 5:53 PM

Ssh = port 22
RDP = 3389
DNS - TCP/UDP 53
LDAP = 389
NTP = UDP 123

"block SQL inject over internet connection" = IPS
    Internet connection
    Compared to "browser-based app" = WAF

Diffusion = one character changes and very diff hash
Confusion = encrypted data is drastically different than plaintext

Registration authority RA = verify entity requesting cert

Legal hold = create backups of customer data

EDR = endpoint detection and response = protect against malware and threats

MAC spoofing = ARP poisoning
    Duplicate MAC addresses would be sign

Stored procedures = execute on server side rather than client

Tokenization = functional
    Masking =/= functional

TCP port 23 = telnet

ISO 27701 = PIMS

Certificate pinning = prevent SSL proxy examination in MITM attacks
    App trusts only a set of digital certs
    SSL proxy can't use its own certificate for MITM
    Prevent break in chain of trust

Switch log = rogue access point detection

DaaS = desktop as a service

Simulations would require "changes in infrastructure"
    Tabletop exercise would not require

Firewall default = implicit deny ALL traffic

HA = high availability
    Ex: UPS

VPN concentrator = used as an endpoint to endpoint VPN solution
    Aggregate and manage multiple VPN connections
    Central point for connecting remote or branch offices to private network

"Most important part of off-boarding"
    Archive decryption keys associated with user account
    "user's account will be disabled so audit of privileges wont be useful"

Weak cipher suite = easy to decrypt hashes

OS access to web server executable = service account

"maintains a scheduling app and database in virtualized cloud environment"
    Backup method = snapshot
    Much more efficient than doing full backups which would individually copy all files

Admin = label in MAC

SSO typically just for the org
    Federation = 3rd party

Continuous delivery automates testing
    =/= prod

Risk matrix or heat map = visual summary of a risk assessment
Risk register = identification of risk at each step of a project plan
Risk control assessment = list of cybersecurity requirements based on id risk
Risk awareness = ongoing group discussions regarding cybersecurity

Kerberos = tickets

Wireless jamming = wireless spectrum

Electronic code book = block cipher mode where each block is encrypted with same key

HMAC = commonly used with the AH field of Ipsec

Heuristic = AI based that detects with no prior signature
Behavior-based = detects bad behavior like trying to attempt a SQL injection
Signature-based = traffic flow based

Netstat = linux too

Diamond model = summarize the aftermath of an intrusion
    Adversary
    Capability
    Infrastructure
    Victim

Laptop can have remote wipe but not good for preserving data

Even when MAC filtering is enabled people are still unauth access
    Enable WPA3 encryption

MAC address can be spoofed to get around filter
For proper auth, use WPA3

XSS = use scripts at one site to execute commands on other sites

Protected distribution = physically secure cabled network