Practice test 7

Tuesday, October 17, 2023 1:11 PM

FTPES = explicit secure; uses AUTH TLS to upgrade unsecure connection on port 21 to secure one

SSTP = secure sockets tunneling protocol microsoft, PPP layer 2 frames over TLS for remote access through VPN

multipathing - configure multi I/O paths between server nodes and storage arrays in single device to remove single point of failure

SOC 2 type II = "highly detailed and designed to be restricted"

27K

- 27001 = cert
- 27002 = guidelines + controls
- 27701 = personal data and privacy

cybersecurity framework

ISO 31k (3100) = enterprise risk management ERM

SOC3 - less detailed report certifying compliance w/ SOC2

freely distributed

EAP-TTLS = can use any tunneling prot while PEAP can only use MSCHAPv2 or EAP-GTC

indoor positioning system IPS - find device location by triangulate prox [illegible] like WiFi AP

device location by triangulation
to other radio sources like WiFi AP
or bluetooth beacons

data masking = code
tokenization ≠ code?

find OS-level files during acq

- cache
- pagefile/swap
- RAM

firmware has hardware-level abstraction
but does not have OS files

Which are cloud-based

- backdoor or virtual platforms
- RAT or web servers

API keys on database as plaintext
is not fault of CSP

is not fault of CSP

nmap also for "test system's connectivity by examine TCP/UDP ports"

boot attestation - transmit boot log report signed by TPM via trusted process to remote server like NAC

measured boot - uses platform configuration registers PCRs in TPM at each stage of boot process to verify measures of key system state data

secure boot - prevent pc from being hijacked by malicious OS

UEFI configured with digicerts of valid OS vendors

UEFI - provides to allow host to boot OS

configure boot integrity checks

- can enforce boot integrity checks

- htaccess file
  - apache server
  - high-level config of website
  - can be edit to redirect

CSRF - exploit apps that use cookies to auth users and track sessions

kerberos

1. Client
   - check pword/PIN
   - properly auth users
   - user input correct creds

2. KDC server
   - TGT is time-stamped

- TGT is time-stamped
  max age of 10 hours
  must sync w/in 5 min

- verify time on pc matches time zone of server

- KDC uses port 88 TCP/UDP

- certify time and port

3. App server

- to access app server resources need a Service Ticket and Service session key

  both used by TGS

- client use service ticket to auth to app server

- app server verify service ticket and service session key
- mutual auth
- then client must be authorized via ACL
- Service ticket/session key + ACL