Exam B

Friday, October 20, 2023 6:28 PM

RAID

RAID 0 = striping - alt copied to mult drives

needs 2 drives

fails on loss of 1

no parity data

RAID 1 = mirroring - duplicated across multiple drives

needs 2 drives

no parity

can survive 1 drive fail

RAID-5

needs 3 drives

Striping + parity ; no mirror

can survive 1 drive fail

RAID-6

needs 4 drives

Striping + parity ; no mirror

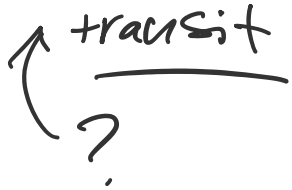
can survive 2 drive fail

RAID 10

needs 4 drives

striping + mirror

switches in data center 802.1Q trunk



auth program does task of passwds

in use

IPS detects SQL inject

in transit

Validate PIN before allowing deposit

in use

backup tapes transported

at rest

implement phone usage for gov projects

biggest concern = photo/video

NAC - access control based on health check or posture assessment

Jump server can go to internal as

jump scare

well

weak encryption ≠ plaintext

WPS

- only 11000 possible PIN
- weak to brute force
- spoofing does not affect WPS

"disable any breached user accounts"

this is apparently recovery task

VPN ≠ monitoring

AH = hash packet data for integrity

"provide details about attackers location"

- tracert = route to IP

- tracert = route to IP
- dig = reverse lookup of IP

AIS = STIX TAXII

WPA3 enterprise + 802.1x

"creds provided from server could not be validated"

either

- host CA ≠ server CA
- host doesnt have CA installed

harden web servers

- prevent packet capture = HTTPS
- prevent on path = create web server cert and sign w/ CA

DNSSEC good for validate IP of device

DNSSEC good for validate IP of device
not for on-path

diffusion - encryption where changing
one char will cause many output
char changes

"worst" security concern for computer
internet facing server

diamond model = "applies scientific
principles to provide post-event
analysis of intrusion"

MITRE Attack = TTP

"using laptop to circumvent org sec
w/ mobile hotspot"

w/ mobile hotspot"

- HIPS
- Host firewall

XUTM is deep in network
X WAF usually for web servers
X NGFW wouldnt see comms outside net

mobile app = ECC ?

maybe AES

Netflow gives net traffic analysis that can be used to see lateral movement

TPM

- burned-in crypto keys
- built in protect from brute force
  dict attacks against FDE
  login creds

electromagnetic interference EMI