Exam A

Thursday, October 19, 2023 4:14 PM

Library protection

Server room

- locking cabinets for physical equip
- Video surveillance
- env sensor

employee laptops offsite

- FDE
- biometric reader

Loading systems onsite

- smart card lease onsite

Open area laptops users

- cable locks

Network protocols

"website" = HTTPS

Sync time = NTP

"access switch w/ CLI" = SSH

calls = SRTP

"gather metrics from remote routers" = SNMPv3

Auth methods

Sign a sign-in sheet = something you can do

only login through VPN = somewhere you are

Firewall rules

Source | Dest | Protocol | Port # | Allow/Block

10.... 10.... TCP or UDP 443

TCP 389 = LDAP

TCP 3389 = RDP

Backdoor testing = active recon

SRTP = AES

file storage subsystem

- Partition data
- Temp file systems

kernel stats = stored in mem

ROM = type of mem storage

process table = stored in RAM

ROM retains data on power off/reboot

ex: BIOS

multifunction device MFD

ex: all in one printer

ISO 27001 = standard for info sec manage systems

ISO 27002 = controls + guide

ISO 27701 = PII

ISO 31000 = risk manage

how to prevent external device data exfil

create OS rule to block use of removable media

can block write to removable media

host firewall and UTM do not
monitor removable devices

apps ≠ removable devices

SIEM
- save log info
- create audit reports from single db

archive encryption keys after account
disable is good for if data needs
to be retrieved

botnet would not include trojan

on-path = mitm would not be able
valid SSL ticket

to provide valid SSL ticket

"unsecure connection"

"using creds from another site" = federation

MTBF = how often will fail between repairs

CASB

- visibility of app use
- data security policy use
  ex: verify encrypted data transfers

X net reports

X VPN

security

VPN concentrator - provide security connectivity

"reset file system and reboot"

stuck rebooting over and over

supposed to be sign that race condition occurred

not resource exhaustion because not a storage/memory issue

login banner - "lets people know you are watching logins"

usage policies + legal restrict

different control

non-cred scan can see version of web server software

- x file perms
- x OS files
- x local users

nmap

802.1X = central auth server
can use username/pword

curl to retrieve, grep to search

Scanless = port scan w/ proxy

Separation of duties = dual control

Rainbow tables

Rainbow tables

- built prior to attack
- if diff hashing tech used, must make a new table
- wont be useful if salt

SSID broadcast suppression = hide SSID from list of available net but can still connect

lack of vendor support and not EoL because it was "a new product"

DNS sinkhole - redirect and id devices that try to reach C2 server

segment devices infected w/ malware

Log files

Log files

- dump = contents of sys memory
- web = all web pages accessed
- packet = net comms
- DNS = which domains were accessed by internal sys

Maybe *

trusted boot = verify OS

secure boot = bootloader

POST power-on self test - hardware check before booting OS

"deploying a new mobile app"

VDI might be correct if it is talking about the app only

is talking about the app only

"track progress of parts as they are used on assembly line" = blockchain

Volatility

- CPU registers
  cache
- router table
  ARP cache
  process table
  kernel stats
  memory
- temp file systems
- Disk
- remote logging/monitor data
- physical config, net topology

- physical config, net topology
- archival media

QA ≠ baseline test

Split knowledge – limit knowledge any 1 person knows

dual control – 2 people must be present

traceroute – maps each hop by increment TTL during each request

"number of sessions from IP with TTL = 0"

vuln scans are specific and

vuln scans are specific

won't get info if TTL=0

DNS TTL ≠ 0

banner grabbing can be good recon

get type, version, and config of services

TTL ≠ 0

"provide creds in morning and not have to for rest of day"

Kerberos - ticket based system for SSO

no SSO:

- TACACS+

- LDAPS
- 802.1X

Setting up VLAN does not need extra resources

Connect to org VPN and cant print to home printer

* VPN is full tunnel because traffic is being redirected through VPN rather than in split tunnel

* could maybe be filtered by VPN client but "not common"

digital sig = add trust to cert

digital sig = add trust to cert

X.509 - defines structure of cert

everyone can view contents of cert

data custodian =? set access rights and controls

TPM = encryption keys

User Agent header = user device

the agent might not be cause of IPS alert

1 OR 1=1;--

random net access from external IP

backdoor

ARP poisoning = local

polymorphic virus - changes itself on each download

trojan wouldn't be the source

SMIME = encrypt between email clients

IMAP = does encrypt info downloaded from server but not outgoing

SSL would encrypt server to server, not clients