Practice test 3

Wednesday, October 11, 2023 3:08 PM

"begin with" risk management

- id
- prio
- classification

Cloud access management

- private subnets - allow services and compute resources to interact w/ each other

  AWS uses VPC to isolate & segment net traffic

- Storage encryption = FPE
- container namespaces = prevent 1 container read/write to another

Wildcards - cloud resources configure read/write access, and using wildcard breaks p of least priv

Setup WPA2 enterprise

- 802.1x
  uses EAP to pass creds to RADIUS
- RADIUS
  wireless controller connects to RADIUS
  w/ shared secret key

Why might drop a vendor?

- vendor lacks expertise
- servers are incompatible

Updating Cisco routers router security

- iOS
- block source routed packets
  prevent spoofed IP addresses
  from bypassing router/firewall filter

  Source-routed packets - specify what
  path packet should take through
  net

  - shared

ver

- message authentication - shared secret configured on each device

make sure message/data isn't tampered with

IPv6 usually enabled by default

SNMP traps - alert messages for certain events info, warn, crit

CPU, mem, state failed, disk capacity, fan speeds, temp

infrared used prox sensors

hashcat = pword cracker

corrective

- containment of threat
- quarantine of infected host(s)

Site risk assessment - evaluates exposure to safety concerns related to area-related risks: disaster, utility disrupt, health/safety

first step of DRP = id crit systems and mission essential functions

Prod, dev, stage, test

test = pen test + vuln scanning

staging = dynamic analysis

Response and recovery controls - policies, procedures, resources to guide entity in responding to outage/disaster

Crypto-erase - secure erase; encrypts all data on drive using media encrypt key, then deletes the key

ineffective secrets manage + input validation

ineffective secrets manage + input validation

- API attacks
- SQL injection
- resource exhaustion - use privilege escalation to deplete resources from ineffective secrets manage

CSRF does not come from input valid

TXT = DNS

SPAN is not separate hardware

TAP = active / passive

SPAN = active

Tape is less expensive than disk

SAN = access other storage devices from

servers

block level

NAS = data access to common group of clients

SAN vs NAS

SAN = servers

NAS = users

playbook = checklist

runbook automates playbook

Standard method for creating CSP

Cloud/follow sec competencies

Cloud control matrix

"immediately escalated" = critical data

PII also an answer but incorrect

LDAP injection - exploits either unauthenticated

client app

LDAP injection - exploits either [illegible]
access of a vulnerability in client app
to submit arbitrary directory queries

XML injection - takes advantage of data
sent with no encryption and input
validation to inject arbitrary code
to return contents like /etc/config

Continuity of operation planning COOP
backup methods of functioning in
the event IT support absent

Common constraints of embedded systems

- crypto capability
- Network range
- Compute power

isolation

- black holes
- sandbox
- air gap

segmentation

- sinkhole

MDM

- remote wipe
- camera usage

MAM

- deployment of workspace
- use of containers

enterprise workspace - collection of corpo apps bundled and placed in containers

active/active = during failover, performance is degraded

active/passive = performance not affected but costs are higher

application-layer load balancers can use

persistence to keep client connected
set cookie

always-on - VPN connection that does not require initiation by client

file metadata
- when create, access, modify
- ACL
- copyright
- tags

mobile metadata
- CDR call detail records
- data transfer volume
- cell tower connections

Email data
- header

- addresses
- servers handling spam
- spam check results

Web metadata
- autho into
- cookies
- data type of resource

Outline password attack = interact with auth system

Wireless controller - centralized management and monitoring app for WAP

need to protect from Rogue AP from connect

"split segments between VPCs" to isolate data

network segment

- performance & load balance
- isolate/protect data
- compartment data access for diff departments

Security group - collection of firewall rules that can be applied to one or more instances

virtual host firewall

monitor virtual instances = logging/monitor

3rd party NGFW probably too hard to implement in cloud

API considerations - code that enables data transmission between one product to another

auto-
product to another

SSO

Hybrid warfare = social media

not messaging app

OT = operational technology

OT-DDoS = disrupt embedded sys

DNS poison = layer 7

transit gateway - interconnect VPC and on-premise

NAT gateway - cloud resources of private IP access internet

Cloud storage security - integrate

Cloud storage gateway - integrate cloud storage w/ on premise servers

gateway endpoint - route to service in VPC route table to connect to AWS

fake telemetry - false but realistic data to trick attackers

DNS sinkhole - intercept DNS requests attempting to connect to known malicious or unwanted domains and return fake IP

PKI

Crypto key and cert management are critical and org's top prio

pinning - several techniques to ensure when client inspects cert presented by server/app, it is correct

"prevent malicious certs from entering chain of trust"

"minimize risk for all sites" = use multi certs

trust issues occur if CN in Subject field does not match FQDN

ex: if it is a test site w/ same cert then FQDN likely not included in certs subject field