Practice test 2

Tuesday, October 10, 2023 3:41 PM

SIEM

- correlation
- Sens
- trends

protected distributed system PDS - wire or fiber optic system w/ safeguards to permit use for trans of unencrypted info through area of lesser classification

Sideloading apps

file corruption is not a concern

- in most cases app wont install if corrupt
- corruption will affect performance and usability, not sec

personality-trait based auth = something

personality-trait based auth - [illegible]

you exhibit

behavioral based

inherent risk is result of qual/quant assess

prevent data exposure

- encryption
- code obfuscation
- code sign

data execution

prevent w/ security feature built into OS that prevents code from being executed in storage area marked as non-exec

code reuse may introduce dead code

code normalization - string is stripped of illegal chars and converted to acceptable

illegal chars and converted to ASCII char set

prepending email means adding text like "RE:..." to add familiarity

hybrid warfare - suite of tech to influence target; usually political agenda

- espionage
- disinfo
- hacking

Powershell = Windows admin

TLS 1.2 - added SHA 256 + improvement to cipher suite negotiation process and protection against known attacks

LEAP = vuln to pword cracking because it uses MSCHAP and not V2

EAP-FAST = Cisco, no certs and uses protected access credential PAC

DNSSEC

mitigate against spoofing and poisoning attacks

authoritative server for zone creates package of resource records called RRset signed w/ private key known as zone signing key

Test access point TAP - copies signals from physical layer to DL layer

no not or transport logic so every frame is received

Switched port analyzer SPAN - port mirroring

mirroring

layer 3|4

dropped frames not copied

Configure DMZ to deploy 2 load balanced web servers

- VIP
- scheduling algoritum
- bastion hosts - any servers configured w/ minimal services to run in DMZ wont be config w/ any data that could be sec risk

UTM

- scan web traffic
- Block URLS
- Block malware

IaaS = provider is <u>not</u> responsible for

IaaS = provider is NOT responsible for availability of software

Access policies

- right to log on to pc
- install software
- change network config

Account permissions

determine number of rights and privileges user has to r, w, create, share files

Account disable

- by admin
- "impossible travel"

CSP responsible for security of infra

Trusted operating system

TOS - OS

- must now reqs for sec

Host-based [illegible]

that meets gov reqs for sec

MAC

tracert or traceroute use ICMP packets to report round trip time

RTT

pathping gives connection details like latency or packet loss

Single CA vs hierarchy

- root cert is self signed
- Entire PKI collapses if CA is compromised

Hierarchy only

- Offline CA
- intermediate CA

weak patch management

weak patch management
- undocumented processes
- non-centralized deployment
  ex: Micro endpoint config manage can schedule, monitor, and auto-deploy patches

SAN - access to block-level data storage that can be access by mult users

flex, available, performance

Network attached storage NAS - file-level data storage that provides access to common group of clients

Single storage over ethernet

ease of use for consumers

Managerial control - oversight of info system risk id + tool for evaluation and selection of sec controls

selection of sec controls

"oversees and monitors other controls"

OAuth - protocol for authn/authz for REST API

sharing of resources w/in user profile sites

CASB = software tool

USB cable attack - accessing users after they plug into malicious USB plug or cable

only black hat move laterally

interview witnesses = establish what they did at scene

non-discretionary privileged management

non-discretionary privileges

mitigate problem of regulating access control of privileged admin accounts

STIX = what to say

TAXII = where to send

threat map - graphic showing source, target, and type of attacks detected by CTI

walkthrough = pc + demonstrate what action they would take

tabletop = no pc + describe course of action

CVE

- dict of vulns
- scores

Credit card fraud = id theft

privacy breach = PII not collected, stored, processed in compliance

operational control = guard as training programs

data masking = secure coding tech

tokenization = db de-id

Networked embedded system - connected to physical net wired/wireless to provide output to connected device

Ex: ATM

Stand alone embedded system - no host analog/digital data

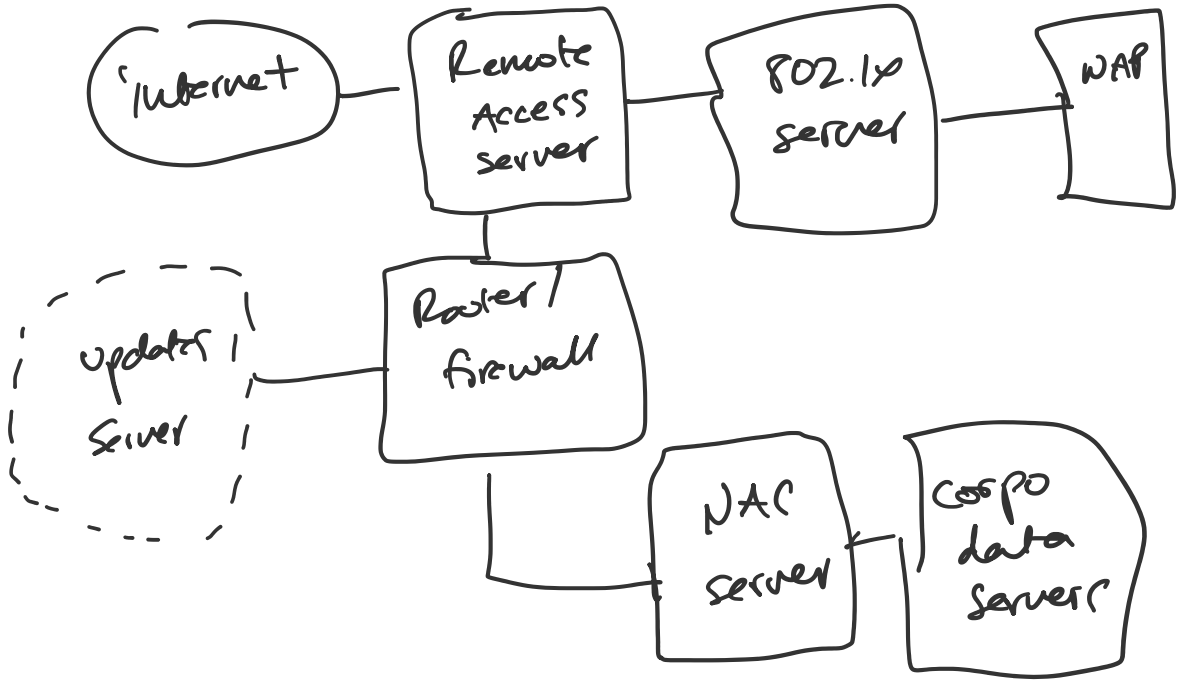
SDN = ABAC

Serverless architecture - removes responsibility of consumer to provision, scale, maintain server/storage by using functions and microservices

Services integration - orchestration of multiple services being performed through sequence of tasks

Scripts + API

Service Oriented Architecture SOA - allows services to comm w/ each other across diff platforms and languages w/ loose coupling



-T4 = fast

-T0/-T1 = slow

"allow files access before verdict"

archives & docs = work files

"not released until verdict"

ex: quarantine app and wait

Apps ≃ scripts

deleting files flagged is not good,
should at least quarantine

risk if you allow downloaded file
to receive verdict after releasing
it to user