Practice test 4

Thursday, October 12, 2023 5:21 PM

time-based login = log in for x amount of time

time-of-day login = log in during certain hours

User certs = AD

email cert w/ SMIME

email addr used for CN or SAN

pivot - bypass net boundary and compromise servers on net

remote access / tunneling protocols

persistence = maintain connection to host as RAT or backdoor

CRC

protected distribution system PDS - wire w/ safeguards

protected distribution system

or fiber optic system w/ safeguards for transmission of unencrypted info through area of lesser classification

Next-gen SWG + CASB = "wholly cloud hosted platform for client access"

Next-gen SWG - proxy-based firewall, content filter, IDS/IPS for access to internet sites and services

Netskope - SWG w/ CASB

VPC endpoint - publishing service so instances can access other instances in other VPCs using AWS internal net and private IP

On-demand resources = cloud resources for peaks

for peaks

Containers allow for CI/CD

Hypervisor - software that creates, runs, manages VM on physical system

allows VMs to share resources

VPC - pool of shared resources isolated from but hosted within public cloud

Risk heatmap - graphical table indicating likelihood and impact of risk factors identified for workflow, project, or dept for stakeholders

does not have counter-measures

MAC cloning - spoofing; changed hardware address configured on adapter interface or asserts use of arbitrary MAC addr

or asserts use of arbitrary

ARP poisoning - uses packet crafter like Ettercap to broadcast unsolicited ARP reply packets

update MAC:IP address cache table w/ spoofed address

embedded system may run firmware located on programmable logic controller PLC

PHI very popular on black market

blackmail / insurance fraud

Setup device w/

- WPS
- 8-digit PIN

activating WPS on router & adapter associates them with PIN

associates them with PIN

then associates adapter w/ access point using WPA2

random SSID & PSK generated

fog computing - decentralized local access w/ fog nodes

analyze data on network edge to avoid transfer unnecessary data back to LAN

send data to LAN level and process w/ IoT sensor

at net edge, closer to data sources but not on the devices itself

edge computing - distributed model accomplished at or near source

of data

enable prio

best for low latency

HSTS = force secure browsing

content security policy CSP = header option that mitigates clickjacking, script injecting, client side attacks

cache-control = prevent caching

secure cookies = mitigate session hijacking and data exposure

SetCookie

CHAP - handshake repeated w/ diff challenge messages throughout session

updates session timestamp and guards against replay attacks

Usually only one-way auth

unless w/ 2 Cisco routers

Repeated challenges prevent replay

Baseband update - modify firmware of radio modem used for cellular, Wi-Fi, Bluetooth, NFC, GPS

nslookup - query name records for given domain using DNS resolver

Windows

dig - test network or linux to see if DNS service is misconfigured

"newest wireless security tech available"

WPA3

- 4-way handshake auth mechanism with prots based on Diffie-

SAE

- enterprise auth requires 192-bit AES, personal can use 128/192-bit

File transfer protocol explicit secure FTPES

uses AUTH TLS to upgrade unsecure connection

Secure sockets tunneling protocol SSTP

Microsoft protocol that tunnels PPP layer 2 frames over TLS for remote access over VPN

No recon in white box

implied trust - any system that is connected is authorized

token key - auto pword that can be used once

context-aware notification - 2FA method uses multi means to auth: time of day, type of device, loc...

ICS industrial control system

flow analyzers generate flow records

timestamp + IP

DNS servers have logs for all requests

throughput records - bandwidth monitors or flow analyzers; but no file generated

GDPR

sensitive = harm subject or make prejudice decisions about them

prejudice decisions about them

private = id

Cybersecurity insurance - product offered to protect from cyber incident consequences

tags to help users search for incidents later

- email
- office 365
- spear phishing (not sure how its not whaling)
- fraud

Spoofing = pretending to be legit email and website

"high level" = email campaign and fraud site

criminal syndicate = $$; even if from another country

target regions = location of email account

Maximum tolerable downtime MTD

how long business can go without unrecoverable failure

RPO - how much data loss org can handle in time

if last backup = 12 hours ago

and RPO = 10 hours

then there is 2 hours of missing data

Repairable assets = MTBF

$$MTBF = \frac{\text{devices} \times \text{hours}}{\#\text{ of failures}}$$

ex: total devices = 3

failed devices = 2

$$\frac{3 \times 1000}{2} = 1500$$

"repairable" = server w/ failed hard drives

Non repairable assets = MTTF

$$\text{MTTF} = \frac{\text{devices} \times \text{hours}}{\#\text{ of devices}}$$

ex: 8 devices

$$\frac{8 \times 1000}{8} = 1000$$

"non-repairable" = failed hard drives

MTTR = measure of time taken to restore systems to full operation

RPO is not achievable based on 2 hours of missing data

last backup 12 hours

RPO = 10 hours

Work recovery time WRT - time to get back to business

WRT + RTO <?> MTD