Practice test 1

Monday, October 9, 2023 5:00 PM

Non persistent VDE - system reverts back to previous state on log off

Type 1 hypervisors - run directly on system hardware

suffers breach and learns lesson on proper approach of maintain archived data

focus on which areas of report?

- Lessons learned
- retention policies

geotagging - add location metadata onto data - files or devices

help ensure app is secure before release

- proper auth/auth
- error handling
- input validation

app audits - occur after app's first commission or when app gets upgraded and at regular intervals

help ensure not vuln to new threats

Check status of online cert w/out revealing id of cert requester

OCSP stapling

OCSP responder - accepts requests

OCSP w/out stapling means requestor

OCSP w/out stapling means requestor goes to responder directly

production = end users have access

junior pen tester in black box env = testing as external threat

Lessons learned = review and anal response and possibly integrate changes

NXlog - open source log normalization tool Windows

journalctl

systemd - manage log files

journald - format to write logs from processes

journalctl view logs

syslog - open format/proto/server software for logging event messages

Rsyslog - update to syslog; can work over TCP and use secure connection

identification = who stakeholders and point of contact for IR team

data at rest = keys need to be stored for longer

application layer = most processing capacity needed

network layer = firewall store connection

transport layer = firewall state connection states and use rules to allow established or related traffic

AAA

- access through smart card
- access data w/ privileges
- all events recorded in logs

OWASP = info of critical app sec risks

transit gateway - cloud net hub that allows users to interconnect VPC and on-prem nets through console

NAT gateway - allows cloud resources

NAT gateway - allows cloud resources access to internet w/out revealing IP to inc internet connections

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

Cloud storage gateway - integrate cloud storage repos w/ on-prem servers as infra

How can site auto upload imag to world map?

- geotagging
- geo location

curl command = download files to or from server

MitB - compromise browser by install plug-ins, scripts, or intercept API calls

HTTP response splitting - craft malicious URL and convince user to submit to web server

locally shared objects or LSOs - flash cookies stored on pc from Adobe may be able to track users browsing behavior

data steward = quality of data

- ensure labels
- id w/ appropriate metadata
- collected and stored in format containing values that comply w/ laws/regs

data owner - label asset and ensure protected w/ correct controls

data custodian - manage system on which data assets are stored

data processor - entity engaged by data controller to assist w/ collection, storage, and tasks

VLAN = separate net resources or dep

level

"does not run code" = compiler

NFC = "bump" + no encryption

IV - used in stream ciphers
ensures key produces unique cipher
from same plaintext

ECC

- asymm
- more efficient

homomorphic - allows computation
directly on encrypted data w/out
secret key

NIDS + sensors

Correlation engine - part of SIEM

push noti = app not SMS

multiparty - adverse event impacts multi orgs

flow analysis

- IPFix or NetFlow
- collect metadata about net traffic w/out capture frames
- good for trend analysis

namespaces - isolate containers; prevent read/write between containers

Control groups - ensure one container can't overwhelm others in DoS

public subnets - allow service or container to connect directly w/ internet gateway

Sniff all traffic on net = APP poison to reroute traffic to Attacker's MAC addr

TCP/IP hijacking - attacker det's host then replaces w/ their machine; spoof hosts IP addr

machine; spoof hosts IP addr

MSA = measurement systems anal =
quality management process

LTE = base band radio; support
higher bandwidth

narrowband - low power version of
LTE

Field programmable Gate Arrays FPGA
semiconductor devices that have
programmable logic blocks

Zigbee - two way wireless radio frq
comm between sensor and control
system

UAVs can drop USB

EV certs can't be issued for wildcards

TXT record - DNS record used for variety of reasons

may provide strings of chars for verify

Most clients can trust multiple root CAs

CA brought online to add or update intermediate CAs

HSM - perform centralized PKI key gen, or key escrow

manage, key gen, or key escrow

can be implemented as plug-in PCIe adapter card

TPM - spec for hardware-based storage of encryption keys, hashed passwords, other user/platform Id info

motherboard

Continuous integration - commit and test updates often

Continuous deployment - making changes to prod env

Continuous delivery - staging, testing infra that supports app

Continuous monitoring - detect service failures and incidents

Continuous validation - revalidate after every change

port security - allows certain # of MAC addr to access port

flood guard - feature of circuit-level firewall that prevents maliciously open connections from forming

data controller - entity responsible for determine why/how data is stored, collected, and used

WPA vs WPA2

WPA2 uses AES rather than

- WPA2 uses AES rather than RC4
- WPA2 reqs much longer passwords

Metadata associated w/ CDR

call detail records

- list of towers connected to
- SMS text timestamps
- call durations

HTTP strict transport security HSTS

forces browsers to connect via HTTPS only

mitigates downgrade attacks like SSL Stripping

content security policy CSP - mitigates

Content security policy CSP - mitigates clickjacking, script inject, and other client-side attacks

Cache-control - determines if browser can cache responses

good for when device is shared

Secure cookies - defend against client-side attacks like session hijacking and data exposure

Secure attr of cookie can prevent from being sent over http

Secure multifunction printers

- delete queued data

- disclosure of

- delete queued
  protect from disclosure of info stored on hard drive
- change default pword
- enable logging to review sys activity

software compliance and licensing - legally binding agreement to only use software in accordance w/ conditions of usage

terms of agree = user data collect

inherent risk - level of risk before any measures in place

any

result of qual/quant analysis

SLA contains cloud right to audit

forensics investigation organisation

apply tags

timestamps help w/ timeline
to establish provenance of
evidence and non-rep but
not for organize

folders with read access for everyone

default settings

web server hardening

upload files

web

- use SSH to upload files
- use config templates provided
- Secure a guest account

most web servers must allow guests

Evil twin = WiPhishing

Registration Authority RA - function of cert enrollment

combined w/ CA in single CA hierarchy

validates and submit request on behalf of end use

Conditional access to system

- UAC

- sudo restrictions

non-discretionary - each subject accessil has no right to mod ACL, only system owner

playbook

- query strings to id incident types

Signatures

- when to report compliance incident
- incident cat and def

Two-person integrity/control - continuous surveillance and control of controlled ecv or material by min of 2 auth individuals

attackers take advantage of company site redirects

- add redirects to .htaccess file

.htaccess file contains high-level config of site

runs on apache server and can be edit to redirect users

- craft phishing links

baseline configuration - documented and agreed upon sets of specs for info systems

change management - process for system mods/upgrades to ensure changes are documented

configuration control - manage system related docs

Configuration control - deliverables and related docs throughout lifecycle of system

benchmarking - measure business metrics and practices and comparing to improve

local replication - replicates data in single data center region where storage account was created

TACACS+ - auth process w/ multi challenge/response between client server
Used when controlling multi network switches/routers

att to Kerberos

on cloud platform, attacker only needs 1 account, service, or host to gain access to an entire platform

NMAP

basic syntax of nmap is to provide IP subnet (or IP addr) to scan

default behavior w/out switches is to ping and send TCP ACK packet to port 80 and 443 to determine if host is present

on local network segment will

also do ARP and ND
(neighbor discovery) sweeps

When host is detected will
perform port scan against host
and report on state of each
port scanned for each IP

then user can run service discovery
scans on active IPs

-A - fingerprinting w/

- OS type
- service versions

- traceroute

default scan will scan 1000 ports

-T4 = fast, stable, speed
helps w/ efficient
net maintain

-T0/-T1 = slow; help
intruders evade
IDS & defenses

-p - scan entire sobnet for
a port

nmap 192.168.1.0/24 -p80

-PR - send ARP requests since
generally not blocked by

generally not

firewalls like usual scans

-sn - discovery only; show only hosts responding to probes

no port scan

-F - fast port scan of 100 ports instead of 1000

-sA - stealthy, evasive, scan take advantage of TCP handshake

sends TCP ACK to reveal firewall rulesets, which ports are filtered, and if firewall is stateful

Network Diagram

remote access server accepts connections from public internet and auth as NAC client

802.1x switch - accepts wired connections for low-privilege workstations and auth as NAC client

WAP - accepts connections from low-privilege wireless connections and auth as NAC client

router/firewall - applies routing and security policies to each interface

Remediation Server (update server)

allows hosts that have not met health policy to update

isolated from other network

in captive portal

NAC server - operates as type of AAA server

- Centralizes account info
- processes auth requests and health policy attestation reports passed from

Supplicants = user devices passed to it by

NAC clients = remote access AP

NAC clients = remote servers, switches, APs

Active directory AD server - stores user auth data but can't assume that it does health policy checks

Troubleshooting Kerberos

1. Principe (client user)

goal = verify user creds

task 1 = verify password/PIN

task 2 = properly auth users

2. KDC server (auth & TGS)

ticket granting ticket TGT or

ticket granting ticket

User ticket is time-stamped

default max age of 10 hours

workstations and servers on net must sync w/in five min

verify time on pc syncs w/ server

key distribution center KDC operates on port 88 TCP/UDP

Certify time and port connectivity establishes valid connection

3. Application Server

Client must obtain service ticket and service session

issued by

ticket ...

key which are issued by

TGS

uses service ticket to auth to

app server which verifies

ticket has valid service

session key

principle & app can then do

mutual auth

access to app server is decided

by ACL