# Practice test 6

Monday, October 16, 2023 5:53 PM

OTA = over the air
update baseband

non-discretionary PAM = mitigate problem of regulating ac of privilege accounts

SEAndroid = MAC + sandbox

UEM can include MAM

context-aware authentication can disable screen locks for ex in trusted loc or check net location

Security content automation protocol SCAP allows compatible scanners to determine if pc meets config baseline

offset = UTC or DST ...

clock synchronization - sync to NTP

important for auth and audit systems

Nikto - web app scanner that looks for exploits: SQL, XSS, ...

manag SIEM events in centralized way

deploy listeners

management servers can be set up as listener or collector to parse before sending to SIEM

app-aware filtering = firewall

NGFW

not antivirus/malware

XML = data exchange

- spoofing
- request forgery
- inject arbitrary code

↑ w/out encryption

USB on the go OTG - allows port to function as host or device

ex: phone port for external drive

SDN = "control model that dictates access based on ABAC"

reconfig net w/ exe files instead of hardware

software-defined visibility SDV

assessment and incident response

functions

real-time collection, aggregation, and reporting of data about net traffic

IaC model

abstract network model = SDN for policy decisions on traffic prio and switching

network functions virtualization NFV

architecture support rapid deployment of virtual net using general purpose VMs and containers

SDN = net traffic handling are implemented by network controller app, which interfaces w/

network controller app APIs

network controller app

Encapsulation security payload ESP

confidentiality + auth and integrity for payload or header of data packet in IPsec

password lockout

- vuln to DoS
- increases workload for admin
- more secure than reset

rollback to known config = baseline

revert to known state = saved system state at point in time

security guidance - best practice summary and unique challenges of cloud env

and unique challenges of cloud-based
and on-premise control