Practice test 8

Tuesday, October 17, 2023 5:44 PM

Carving = data recovery = analysis of disk/disk image for file frags retained in slack space

frags may be deleted/overwritten files

DHCP spoofing - attacker attempts to respond to DHCP requests

DHCP snooping = inspect traffic on Access ports to ensure host isn't spoofing MAC addr

Victim play as blue team?

test env does not fully simulate prod

E-discovery - filter relevant evidence and storing it in db so can

and storing it in db so can be used in courtroom

serverless architecture - cloud model where apps hosted by 3rd party

remove responsibility of consumer to provision, scale, and maintain servers/storage w/ functions + microservice

microservice architecture - app is collection of independent of one another and structured around business capabilities

service oriented architecture SOA - allow services to comm w/ each other across diff platforms and languages w/ loose coupling tech

Type 1 hypervisor run directly on system hardware; do not require OS in vm

Ping can scan all IP addresses of subnet

Risk and control assess RCA = id risk and assess effectiveness of controls

risk heatmap = likelihood + impact

hybrid warfare

- espionage
- social media
- soft power - using diplomatic & cultural assets to achieve obj can influence ops of orgs in target country
- exploitation = no code exe in

data execution = no code exe in data storage area

bastion hosts - any servers config w/ min services to run in DMZ

NIST 5 functions

- Identify
- Protect
- Detect
- Respond
- Recover

CIS = 20 CIS controls

Zigbee = home auto

- two way wireless radio
- IEEE 802.15.4

Control risk - how much less effective a sec control has become over time

NAC = AAA