Pre assessment 21

Monday, July 24, 2023 9:18 PM

21. Org wants to combine security controls to control incoming and outgoing traffic. Should include stateless inspection, malware inspection, and a content filter

A. VLAN
B. NAT
[✓ C.] UTM
D. DNSSEC
C. WAF

Unified threat management

UTM - advance firewall that combines multiple controls together like stateless inspection, malware analysis, and content filter

no other answers provide these

VLAN is for network segmentation on switch

Network Address Translation

NAT - converts public to private IP addresses and vice versa

DNSSEC provides validation for DNS responses

- protects

Web app firewall WAF - pro
web server from internet based attacks

22. Deploying Linux server in screened subnet. Want to manage from pc in private network.

A. Forward proxy server
B. Reverse proxy server
C. web app firewall
D. Jump server

Jump server - placed between security zones and is used to manage devices in the other zone

could connect to jump server using SSH, then linux server using SSH forwarding

forward proxy for outgoing internet traffic

reverse proxy for incoming internet traffic

23. Several attacks against servers in DMZ. Which will prevent?

A. IPS

A. Anomaly based IPS

[✓ B.] inline IPS

C. Passive IDS

D. Signature-based IPS

inline IPS only one that will <u>prevent</u>

24. Coffee shop <u>stopped</u> broadcasting SSID for wireless network. Turn on laptop and see the SSID, what is the attack?

A. Rogue AP

[✓ B.] Evil twin

C. Jamming

D. Bluejacking

evil twin - a rogue Access point (AP) with the same or similar service set identifier SSID

jamming - not allowing anybody to connect to wireless network

bluejacking - related to bluetooth

25. Must put smartphone in conductive metal box before entering area. Which is greatest risk to ID this mitigate?

[✓ A.] Bluesnarfing
B. Theft of phone
C. Data exfiltration from mobile hotspot
D. Enable geofencing

Bluesnarfing - unauthorized access to info on wireless device through bluetooth

conductive metal boxes are a faraday cage that blocks bluetooth signals

lockboxes prevent theft but not main concern if conductive

Wireless hotspots are in public locations

a virtual

geofencing - creates a
fence using GPS, but
devices in cage won't
access GPS

26. Designing site to site VPN between offices in different cities. Use of certificates for mutual authentication. Want to ensure internal IP addresses are hidden.

[✓ A.] IPsec VPN using tunnel mode

B. IPsec VPN using transport mode

C. L2TP VPN

D. VLAN VPN

IPsec VPN provides mutual authentication

tunnel mode - encrypts payload and IP headers

transport mode - only encrypts payload

ling protocol

Layer 2 tunneling protocol

does not encrypt

VLAN VPN - provides network segmentation but does not act as VPN

27. Want to use HSM on server in network. What does this add to server?

A. Provide full drive encryption

B. Reduce risk of confidential info outside org

C. Provide webmail to clients

[✓ D.] Generate and store keys for servers

hardware security module - generate and store RSA keys

can be used to encrypt data sent to and from server

trusted platform module TPM provides full drive encryption

Data loss prevention DLP - reduce risk of sending confidential info outside org

SaaS provides webmail

28. Need to send email with sensitive info. Which best maintains confidentiality?

A. Digital signature

[✓ B.] Encryption

C. Data masking

D. Hashing

encryption provides confidentiality of any type of info

digital signature provides integrity, non-repudiation, and authentication

data masking modifies original data producing data that looks valid but not authentic

hashing provides integrity

24. Stores some data in cloud with its own resources. Another company also stores in cloud w/ own data

resources. Both decide to share data in both clouds for educational purposes.

[✓ A.] Community
B. Private
C. Public
D. XaaS

created a community cloud
both clouds separate were private, but shared resources were not

in this scenario, they are sharing only with each other, meaning it is not public - visible by everyone

Anything as a Service XaaS
Cloud services beyond IaaS, PaaS, and SaaS

30. Planning to implement a CYOD deployment model. Which are appropriate for policy?

A. SCADA access

[✓ B.] Storage segmentation

C. Database security

D. Embedded RTOS

Storage segmentation - create separate storage areas in mobile devices

can be used with choose your own device CYOD - users own their own devices

no other answer related to mobile

Supervisory control and data acquisition SCADA - controls industrial control system ICS such as nuclear plants or water treatment

SCADA should be isolated

Database security - use of permissions and encryption to protect data in database

Embedded systems use real-time OS RTOS when system specific must react within specific time

31. Plan to implement desktops via cloud. Each will include OS and core group of apps. cloud will manage desktops. Employees can access from anywhere and any device

A. IaaS
B. CASB
C. SaaS
[✓ D.] XaaS

anything as a service XaaS
would include desktops as a service

IaaS - vendor provides access to pc, but customer must install OS and apps

Cloud access security broker

CASB - software tool used to provide additional security for cloud resources but provides underlying cloud services

SaaS provides apps but not entire desktops

32. Want to improve security posture. Doesnt have any security staff.

A. SOAR
[✓ B.] MSSP
C. SaaS
D. XaaS

Managed security service provider MSSP - 3rd party vendor that provides security services for org

security orchestration, automation, and response SOAR - automates incident response for some events

requires security staff

SaaS and XaaS still need security staff

33. Allow employees to connect to internal network using personal device. Having problems:

keep devices updated

- do not keep
- no standardization of devices
- no adequate control over devices

Want to allow to keep using personal devices, which is best?

A. BYOD
B. COPE
[✓ C.] CYOD
D. IaaS

CYOD - includes a list of acceptable devices that employees can purchase and connect to network

IT can can then use mobile device management MDM system for standardized management

Bring your own device BYOD does not have standardization

Corporate owned personally enabled COPE policy - orgs own devices, not employees

34. Discover new systems on network during vulnerability scan. Systems weren't authorized because someone installed w/out going through standard process.

A. Hacktivist
B. Script kiddie
[✓ C.] Shadow IT
D. Authorized hacker

Shadow IT - any systems or apps installed on network without auth or approval

employees often add to bypass security controls

hacktivist - launches attacks as part of activist movement

Script kiddie - uses existing software or scripts to attack and often has little technical ability authorized hacker aka white hat - security professional working with law to protect org

35. Received phishing email with malicious attachment. Opened and installed malware that quickly spread to other systems on network. Exploited vulnerability that wasn't previously known by any trusted sources.

A. Backdoor

[✓ B.] Zero-day

C. Hoax

D. DDoS

Zero-day - not known by trusted sources like antivirus

hoax - not a specific attack, message spread about impending doom of virus security threat that

or sec
doesnt exist

DDoS comes from multiple sources

36. Completed antivirus scan and detected trojan. Removed trojan but worried attackers may still be able to access.

[✓ A.] Backdoor
B. Logic bomb
C. Rootkit
D. Botnet

trojans often create backdoors

Logic bombs and rootkits can create backdoors but trojans dont create logic bombs and rarely install rootkit

37. Some network appliances monitoring incoming data sending alerts about malicious files. These are PE32 files with tar.gz version and being downloaded users

extension users
to several systems.
opened email with infected
MHT file.

A. systems joined botnet
B. installed ransomware
[✓ C.] installed RAT
D. Shadow IT running in
network

users installed RAT when
they opened MHT file -
MHTML is a webpage
archive that stores HTML,
JS, CSS, images, etc.

after installing RAT, installed
portable executable PE32
files

systems may have joined botnet
but scenario doesn't
indicate

ransomware would encrypt
data

Shadow IT are unauth
systems in network

data.

38. Unable to access pc
see message that data has
been encrypted until pay
ransom.

A. Criminal syndicate
[✓ B.] Ransomware
C. Fileless virus
D. Rootkit

Criminal syndicate - launches criminal organized attack motivated by money

fileless virus - injects code into existing scripts and may install ransomware but not ransomware itself

rootkit - program or group of programs that provide root-level access to system but hides itself

39. SIEM sending alerts saying
malware has infected several
pcs. Examine border firewall
and NIDS logs, but cant
ffic entering

traffic

find malicious traffic from internet. All employees affected attended trade show in past 2 days

[✓ A.] Fileless virus via vCard

B. Malware on USB

C. Trojan from botnet

D. Worms from presentation media

vCard virtual contact file VCF - people usually share contact info w/ vCards but can contain malicious code

USBs not mentioned

malicious traffic from botnet comes from internet but IT didnt find any

Speakers at trade shows use presentation media but viewing presentation wont infect systems

saving

40. Receive email saying won lottery. Need to confirm identity w/ name, phone, address, bday. Will receive prize after.

A. Spear phishing
[✓ B.] Phishing
C. Smishing
D. Whaling

general phishing, not targeted (spear/whaling)
smishing from text, not email

41. Some protocols include sequence #'s and timestamps. Which does these thwart?

A. MAC flooding
[✓ B.] Replay
C. SYN flooding
D. Salting

and sequence

timestamps

#s act as counter measures against replay attacks

Media access control MAC flood attack - floods switch with different MAC addresses

SYN flood disrupt TCP handshake

Salting is not an attack

42. Reviewing logs for web server and see sus entries. suspect an attacker trying to write more data into web app memory than it can handle

A. Pointer/object dereference

B. Race condition exploit

C. DLL injection attack

[✓ D.] Buffer overflow attack

buffer overflow attack - write more data into app memory than it can handle

pointer/object dereference - programming error that can corrupt memory

programmers, not attackers cause this

race condition exploit - programming conflict where 2 or more apps or app models try to access or modify same resource at the same time

dynamic link library DLL injection attack injects DLL into memory and causes it to run

DLL - Microsoft windows module of functions or data other programs or DLLs can use

43. Org hosts web app selling digital products. customers can post comments. Attackers looking for ways

Attackers — to exploit. What is best way to test resilience of app?

[✓ A.] Fuzzing
B. Input validation
C. Error handling
D. Anti-malware

fuzzing - type of dynamic code analysis that tests site resilience
sends random data to app to see if it crashes site or expose data

input validation and error handling protect, but not test

same with anti-malware

44. Attacker launched successful XSS attacks on web app. Which are best to protect and prevent?

analysis

A. Dynamic code an

[✓ B.] Input validation

C. Code obfoscation

[✓ D.] WAF

E. Normalization

input validation and WAF are best

input validation - validate input before using

WAF - additional firewall that monitors, filters, and blocks HTTP traffic to web server

Dynamic code analysis is testing method

code obfoscation - makes code harder to read

normalization - organize tables and columns in database to reduce redundant data and improve overall database performance

45. User has account to post comments. Enters username and pword to login and Site displays username. changed username to JS code. other users experienced unexpected results when hovering over name.

[✓ A.] Cross site scripting

B. Input validation

C. Privilege escalation

D. Directory traversal

this is XSS

input validation is how you protect against it

privilege escalation - attempt to give attacker more rights or permissions

directory traversal attack. attacker navigates system's directory structure and reads files

46. Which best describes purpose of risk register?

A. Shows risk on plot or graph

[✓ B.] Listing of risks, risk owner, and mitigation measures

C. shows risks in color coded graph

D. Evaluates supply chain

risk register - lists risks and often includes risk, risk owner, mitigation measures, and risk score

risk matrix - plots risks in graph

heat map - plot risks onto color-coded graph or chart