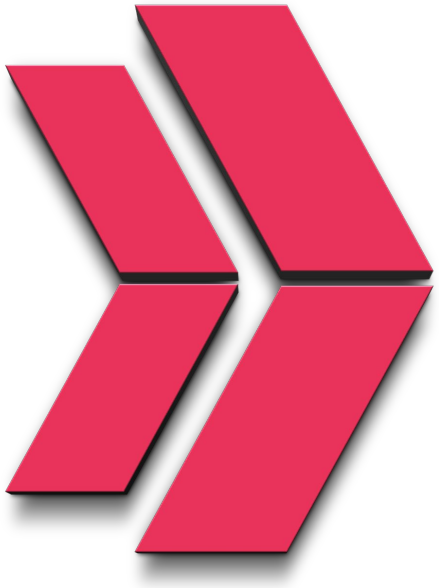


CLARUSWAY

WAY TO REINVENT YOURSELF

CompTIA (8A-8B-8C-8D) Explain Vulnerability Management

AGENDA

- 8A - Asset Management (10)
- 8B - Redundancy Strategies (11)
- 8C - Physical Security (4)
- 8D - Vulnerability Analysis and Remediation (7)
- TOTAL: 32

8A - Device and OS Vulnerabilities

8A - Device and OS Vulnerabilities

NO.1 Which of the following vulnerabilities is associated with installing software outside of a manufacturer's approved software repository?

A. Jailbreaking
B. Memory injection
C. Resource reuse
D. Side loading

8A - Device and OS Vulnerabilities

NO.1 Which of the following vulnerabilities is associated with installing software outside of a manufacturer's approved software repository?

A. Jailbreaking
B. Memory injection
C. Resource reuse
D. Side loading

8A - Device and OS Vulnerabilities

NO.2 A company is adding a clause to its AUP that states employees are not allowed to modify the operating system on mobile devices.
Which of the following vulnerabilities is the organization addressing?

A. Cross-site scripting
B. Buffer overflow
C. Jailbreaking
D. Side loading

8A - Device and OS Vulnerabilities

NO.2 A company is adding a clause to its AUP that states employees are not allowed to modify the operating system on mobile devices.
Which of the following vulnerabilities is the organization addressing?

A. Cross-site scripting
B. Buffer overflow
C. Jailbreaking
D. Side loading

8A - Device and OS Vulnerabilities

NO.3 A small business uses kiosks on the sales floor to display product information for customers. A security team discovers the kiosks use end-of-life operating systems. Which of the following is the security team most likely to document as a security implication of the current architecture?

A. Patch availability
B. Product software compatibility
C. Ease of recovery
D. Cost of replacement

8A - Device and OS Vulnerabilities

NO.3 A small business uses kiosks on the sales floor to display product information for customers. A security team discovers the kiosks use end-of-life operating systems. Which of the following is the security team most likely to document as a security implication of the current architecture?

A. Patch availability
B. Product software compatibility
C. Ease of recovery
D. Cost of replacement

8A - Device and OS Vulnerabilities

NO.4 While troubleshooting a firewall configuration, a technician determines that a "deny any" policy should be added to the bottom of the ACL. The technician updates the policy, but the new policy causes several company servers to become unreachable.
Which of the following actions would prevent this issue?

A. Documenting the new policy in a change request and submitting the request to change management
B. Testing the policy in a non-production environment before enabling the policy in the production network
C. Disabling any intrusion prevention signatures on the 'deny any' policy prior to enabling the new policy
D. Including an 'allow any1 policy above the 'deny any' policy

8A - Device and OS Vulnerabilities

NO.4 While troubleshooting a firewall configuration, a technician determines that a "deny any" policy should be added to the bottom of the ACL. The technician updates the policy, but the new policy causes several company servers to become unreachable.
Which of the following actions would prevent this issue?

A. Documenting the new policy in a change request and submitting the request to change management
B. Testing the policy in a non-production environment before enabling the policy in the production network
C. Disabling any intrusion prevention signatures on the 'deny any' policy prior to enabling the new policy
D. Including an 'allow any1 policy above the 'deny any' policy

8A - Device and OS Vulnerabilities

NO.5 One of a company's vendors sent an analyst a security bulletin that recommends a BIOS update.
Which of the following vulnerability types is being addressed by the patch?

A. Virtualization
B. Firmware
C. Application
D. Operating system

8A - Device and OS Vulnerabilities

NO.5 One of a company's vendors sent an analyst a security bulletin that recommends a BIOS update.
Which of the following vulnerability types is being addressed by the patch?

A. Virtualization
B. Firmware
C. Application
D. Operating system

8A - Device and OS Vulnerabilities

NO.6 Which of the following would be the best way to handle a critical business application that is running on a legacy server?

A. Segmentation
B. Isolation
C. Hardening
D. Decommissioning

8A - Device and OS Vulnerabilities

NO.6 Which of the following would be the best way to handle a critical business application that is running on a legacy server?

A. Segmentation
B. Isolation
C. Hardening
D. Decommissioning

8A - Device and OS Vulnerabilities

NO.7 Which of the following most impacts an administrator's ability to address CVEs discovered on a server?

A. Rescanning requirements
B. Patch availability
C. Organizational impact
D. Risk tolerance

8A - Device and OS Vulnerabilities

NO.7 Which of the following most impacts an administrator's ability to **address CVEs** discovered on a server?

A. Rescanning requirements
B. Patch availability
C. Organizational impact
D. Risk tolerance

8A - Device and OS Vulnerabilities

NO.8 A systems administrator notices that one of the systems critical for processing customer transactions is running an end-of-life operating system.

Which of the following techniques would increase enterprise security?
A. Installing HIDS on the system
B. Placing the system in an isolated VLAN
C. Decommissioning the system
D. Encrypting the system's hard drive

8A - Device and OS Vulnerabilities

NO.8 A systems administrator notices that one of the systems critical for processing customer transactions is **running an end-of-life operating system.**

Which of the following techniques would increase enterprise security?

A. Installing HIDS on the system

B. Placing the system in an isolated VLAN

C. Decommissioning the system

D. Encrypting the system's hard drive

8A - Device and OS Vulnerabilities

NO.9 A legacy device is being decommissioned and is no longer receiving updates or patches.

Which of the following describes this scenario?

A. End of business

B. End of testing

C. End of support

D. End of life

8A - Device and OS Vulnerabilities

NO.9 A legacy device is being decommissioned and is **no longer receiving updates or patches.**

Which of the following describes this scenario?

A. End of business

B. End of testing

C. End of support

D. End of life

8A - Device and OS Vulnerabilities

NO.10 A user would like to install software and features that are not available with a smartphone's default software.

Which of the following would allow the user to install unauthorized software and enable new features?

A. SOU

B. Cross-site scripting

C. Jailbreaking

D. Side loading

8A - Device and OS Vulnerabilities

NO.10 A user would like to install software and features that are **not available with a smartphone's default software.**

Which of the following would allow the user to install unauthorized software and enable new features?

A. SOU

B. Cross-site scripting

C. Jailbreaking

D. Side loading

8B - Application and Cloud Vulnerabilities

8B - Application and Cloud Vulnerabilities

NO.1 Which of the following involves an attempt to take advantage of database misconfigurations?

A. Buffer overflow
B. SQL injection
C. VM escape
D. Memory injection

8B - Application and Cloud Vulnerabilities

NO.1 Which of the following involves an attempt to take advantage of database misconfigurations?

A. Buffer overflow
B. SQL injection
C. VM escape
D. Memory injection

8B - Application and Cloud Vulnerabilities

NO.2 A company has decided to move its operations to the cloud. It wants to utilize technology that will prevent users from downloading company applications for personal use, restrict data that is uploaded, and have visibility into which applications are being used across the company.
Which of the following solutions will best meet these requirements?

A. An NGFW
B. A CASB
C. Application whitelisting
D. An NG-SWG

8B - Application and Cloud Vulnerabilities

NO.2 A company has decided to move its operations to the cloud. It wants to utilize technology that will prevent users from downloading company applications for personal use, restrict data that is uploaded, and have visibility into which applications are being used across the company.
Which of the following solutions will best meet these requirements?

A. An NGFW
B. A CASB
C. Application whitelisting
D. An NG-SWG

8B - Application and Cloud Vulnerabilities

NO.3 A technician is opening ports on a firewall for a new system being deployed and supported by a SaaS provider.
Which of the following is a risk in the new system?

A. Default credentials
B. Non-segmented network
C. Supply chain vendor
D. Vulnerable software

8B - Application and Cloud Vulnerabilities

NO.3 A technician is opening ports on a firewall for a new system being deployed and supported by a SaaS provider.
Which of the following is a risk in the new system?

A. Default credentials
B. Non-segmented network
C. Supply chain vendor
D. Vulnerable software

8B - Application and Cloud Vulnerabilities

NO.4 A security team is reviewing the findings in a report that was delivered after a third party performed a penetration test. One of the findings indicated that a web application form field is vulnerable to cross-site scripting.
Which of the following application security techniques should the security analyst recommend the developer implement to prevent this vulnerability?

A. Secure cookies
B. Version control
C. Input validation
D. Code signing

8B - Application and Cloud Vulnerabilities

NO.4 A security team is reviewing the findings in a report that was delivered after a third party performed a penetration test. One of the findings indicated that a web application form field is vulnerable to cross-site scripting.
Which of the following application security techniques should the security analyst recommend the developer implement to prevent this vulnerability?

A. Secure cookies
B. Version control
C. Input validation
D. Code signing

8B - Application and Cloud Vulnerabilities

NO.5 Which of the following enables the use of an input field to run commands that can view or manipulate data?

A. Cross-site scripting
B. Side loading
C. Buffer overflow
D. SQL injection

8B - Application and Cloud Vulnerabilities

NO.5 Which of the following enables the use of an input field to run commands that can view or manipulate data?

A. Cross-site scripting
B. Side loading
C. Buffer overflow
D. SQL injection

8B - Application and Cloud Vulnerabilities

NO.6 A security analyst is investigating an application server and discovers that software on the server is behaving abnormally. The software normally runs batch jobs locally and does not generate traffic, but the process is now generating outbound traffic over random high ports. Which of the following vulnerabilities has likely been exploited in this software?

A. Memory injection
B. Race condition
C. Side loading
D. SQL injection

8B - Application and Cloud Vulnerabilities

NO.6 A security analyst is investigating an application server and discovers that software on the server is behaving abnormally. The software normally runs batch jobs locally and does not generate traffic, but the process is now generating outbound traffic over random high ports. Which of the following vulnerabilities has likely been exploited in this software?

A. Memory injection
B. Race condition
C. Side loading
D. SQL injection

8B - Application and Cloud Vulnerabilities

NO.7 Which of the following vulnerabilities is exploited when an attacker overwrites a register with a malicious address?

A. VM escape
B. SQL injection
C. Buffer overflow
D. Race condition

8B - Application and Cloud Vulnerabilities

NO.7 Which of the following vulnerabilities is exploited when an attacker overwrites a register with a malicious address?

A. VM escape
B. SQL injection
C. Buffer overflow
D. Race condition

8B - Application and Cloud Vulnerabilities

NO.8 Which of the following risks can be mitigated by HTTP headers?

A. SQLi
B. XSS
C. DoS
D. SSL

8B - Application and Cloud Vulnerabilities

NO.8 Which of the following risks can be mitigated by **HTTP headers**?

A. SQLi
B. XSS
C. DoS
D. SSL

8B - Application and Cloud Vulnerabilities

NO.9 Which of the following examples would be best mitigated by input sanitization?

A. <script>alert ("Warning!") ,-</script>
B. nmap - 10.11.1.130
C. Email message: "Click this link to get your free gift card."
D. Browser message: "Your connection is not private."

8B - Application and Cloud Vulnerabilities

NO.9 Which of the following examples would be best mitigated by **input sanitization?**

A. <script>alert ("Warning!") ,-</script>
B. nmap - 10.11.1.130
C. Email message: "Click this link to get your free gift card."
D. Browser message: "Your connection is not private."

8B - Application and Cloud Vulnerabilities

NO.10 A security engineer is working to address the growing risks that shadow IT services are introducing to the organization. The organization has taken a cloud-first approach and does not have an on-premises IT infrastructure.

Which of the following would best secure the organization?

A. Upgrading to a next-generation firewall

B. Deploying an appropriate in-line CASB solution

C. Conducting user training on software policies

D. Configuring double key encryption in SaaS platforms

8B - Application and Cloud Vulnerabilities

NO.10 A security engineer is working to address the growing risks that **shadow IT services** are introducing to the organization. The organization has taken a cloud-first approach and does not have an on-premises IT infrastructure.

Which of the following would best secure the organization?

A. Upgrading to a next-generation firewall

B. Deploying an appropriate in-line CASB solution

C. Conducting user training on software policies

D. Configuring double key encryption in SaaS platforms

8B - Application and Cloud Vulnerabilities

NO.11 While investigating a recent security breach an analyst finds that an attacker gained access by SQL injection through a company website.

Which of the following should the analyst recommend to the website developers to prevent this from reoccurring?

A. Secure cookies

B. Input sanitization

C. Code signing

D. Blocklist

8B - Application and Cloud Vulnerabilities

NO.11 While investigating a recent security breach an analyst finds that an attacker gained access by **SQL injection** through a company website.

Which of the following should the analyst recommend to the website developers to prevent this from reoccurring?

A. Secure cookies

B. Input sanitization

C. Code signing

D. Blocklist

8C - Vulnerability Identification Methods

8C - Vulnerability Identification Methods

NO.1 Which of the following are the most likely vectors for the unauthorized or unintentional inclusion of vulnerable code in a software company's final software releases? (Choose two).

A. Certificate mismatch
B. Use of penetration-testing utilities
C. Weak passwords
D. Included third-party libraries
E. Vendors/supply chain
F. Outdated anti-malware software

8C - Vulnerability Identification Methods

NO.1 Which of the following are the most likely vectors for the unauthorized or unintentional inclusion of vulnerable code in a software company's final software releases? (Choose two).

A. Certificate mismatch
B. Use of penetration-testing utilities
C. Weak passwords
D. Included third-party libraries
E. Vendors/supply chain
F. Outdated anti-malware software

8C - Vulnerability Identification Methods

NO.2 A company is expanding its threat surface program and allowing individuals to security test the company's internet-facing application. The company will compensate researchers based on the vulnerabilities discovered.
Which of the following best describes the program the company is setting up?

A. Open-source intelligence
B. Bug bounty
C. Red team
D. Penetration testing

8C - Vulnerability Identification Methods

NO.2 A company is expanding its threat surface program and allowing individuals to security test the company's internet-facing application. The company will compensate researchers based on the vulnerabilities discovered.
Which of the following best describes the program the company is setting up?

A. Open-source intelligence
B. Bug bounty
C. Red team
D. Penetration testing

8C - Vulnerability Identification Methods

NO.3 A security analyst is reviewing the source code of an application in order to identify misconfigurations and vulnerabilities.

Which of the following kinds of analysis best describes this review?

A. Dynamic
B. Static
C. Gap
D. Impact

8C - Vulnerability Identification Methods

NO.3 A security analyst is **reviewing the source code** of an application in order to identify misconfigurations and vulnerabilities.

Which of the following kinds of analysis best describes this review?

A. Dynamic
B. Static
C. Gap
D. Impact

8C - Vulnerability Identification Methods

NO.4 A security audit of an organization revealed that most of the IT staff members have domain administrator credentials and do not change the passwords regularly.

Which of the following solutions should the security learner propose to resolve the findings in the most complete way?

A. Creating group policies to enforce password rotation on domain administrator credentials

B. Reviewing the domain administrator group, removing all unnecessary administrators, and rotating all passwords

C. Integrating the domain administrator's group with an IdP and requiring SSO with MFA for all access

D. Securing domain administrator credentials in a PAM vault and controlling access with role-based access control

8C - Vulnerability Identification Methods

NO.4 A security audit of an organization revealed that most of the IT staff members have **domain administrator credentials** and do **not change the passwords regularly.**

Which of the following solutions should the security learner propose to resolve the findings in the most complete way?

A. Creating group policies to enforce password rotation on domain administrator credentials

B. Reviewing the domain administrator group, removing all unnecessary administrators, and rotating all passwords

C. Integrating the domain administrator's group with an IdP and requiring SSO with MFA for all access

D. Securing domain administrator credentials in a PAM vault and controlling access with role-based access control

8D - Vulnerability Analysis and Remediation

8D - Vulnerability Analysis and Remediation

NO.1 Which of the following is used to quantitatively measure the criticality of a vulnerability?

A. CVE
B. CVSS
C. CIA
D. CERT

8D - Vulnerability Analysis and Remediation

NO.1 Which of the following is used to quantitatively measure the criticality of a vulnerability?

A. CVE
B. CVSS
C. CIA
D. CERT

8D - Vulnerability Analysis and Remediation

NO.2 A security practitioner completes a vulnerability assessment on a company's network and finds several vulnerabilities, which the operations team remediates.
Which of the following should be done next?

A. Conduct an audit.
B. Initiate a penetration test.
C. Rescan the network.
D. Submit a report.

8D - Vulnerability Analysis and Remediation

NO.2 A security practitioner completes a vulnerability assessment on a company's network and finds several vulnerabilities, which the operations team remediates.
Which of the following should be done next?

A. Conduct an audit.
B. Initiate a penetration test.
C. Rescan the network.
D. Submit a report.

8D - Vulnerability Analysis and Remediation

NO.3 An organization disabled unneeded services and placed a firewall in front of a business critical legacy system.
Which of the following best describes the actions taken by the organization?

A. Exception
B. Segmentation
C. Risk transfer
D. Compensating controls

8D - Vulnerability Analysis and Remediation

NO.3 An organization disabled unneeded services and placed a firewall in front of a business critical legacy system.
Which of the following best describes the actions taken by the organization?

A. Exception
B. Segmentation
C. Risk transfer
D. Compensating controls

8D - Vulnerability Analysis and Remediation

NO.4 After conducting a vulnerability scan, a systems administrator notices that one of the identified vulnerabilities is not present on the systems that were scanned.

Which of the following describes this example?

A. False positive
B. False negative
C. True positive
D. True negative

8D - Vulnerability Analysis and Remediation

NO.4 After conducting a vulnerability scan, a systems administrator notices that one of the identified **vulnerabilities is not present** on the systems that were scanned.

Which of the following describes this example?

A. False positive
B. False negative
C. True positive
D. True negative

8D - Vulnerability Analysis and Remediation

NO.5 A security analyst is investigating an alert that was produced by endpoint protection software. The analyst determines this event was a false positive triggered by an employee who attempted to download a file.

Which of the following is the most likely reason the download was blocked?

A. A misconfiguration in the endpoint protection software
B. A zero-day vulnerability in the file
C. A supply chain attack on the endpoint protection vendor
D. Incorrect file permissions

8D - Vulnerability Analysis and Remediation

NO.5 A security analyst is investigating an alert that was produced by endpoint protection software. The analyst determines this event was a false positive triggered by an **employee who attempted to download a file.**

Which of the following is the most likely reason the download was blocked?

A. A misconfiguration in the endpoint protection software
B. A zero-day vulnerability in the file
C. A supply chain attack on the endpoint protection vendor
D. Incorrect file permissions

8D - Vulnerability Analysis and Remediation

NO.6 Which of the following can a security director use to prioritize vulnerability patching within a company's IT environment?

A. SOAR
B. CVSS
C. SIEM
D. CVE

8D - Vulnerability Analysis and Remediation

NO.6 Which of the following can a security director use to **prioritize vulnerability patching** within a company's IT environment?

A. SOAR
B. CVSS
C. SIEM
D. CVE

8D - Vulnerability Analysis and Remediation

NO.7 Which of the following alert types is the most likely to be ignored over time?

A. True positive
B. True negative
C. False positive
D. False negative

8D - Vulnerability Analysis and Remediation

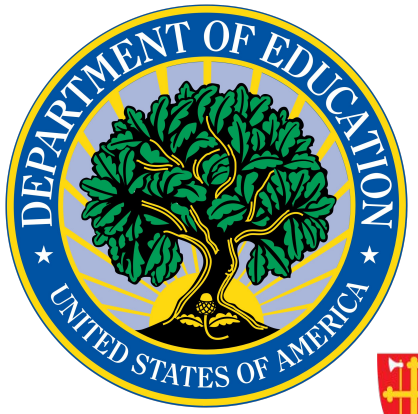
NO.7 Which of the following alert types is the most likely to be **ignored over time**?

A. True positive
B. True negative
C. False positive
D. False negative

THANKS!

Any questions?

Our Graduates are Hired By



Google

Deloitte.

AT&T

ally
do it right.

DEN NORSKE KIRKE
Kirkepartner

Robinhood

VIZNET

COMCAST

INSPARK

ING BANK

proValus

SOCRadar®
Extension to Your SOC Team!

AGILIS
TECHNOLOGIES

Humana
Wellness

EQUANS

BBS

BGA
SECURITY

gravity
IT RESOURCES

GetMoneyGlobal

proximus

northramp

ease
LEARNING