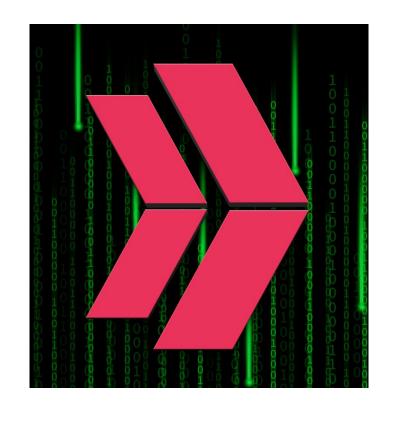


CLARUSWAY

WAY TO REINVENT YOURSELF



CompTIA (11A-11B)

AGENDA



- 11A Application Protocol Security Baselines (4)
- 11B Cloud and Web Application Security Concepts (4)
- ► TOTAL: 8







NO.1 A company's public-facing website, https://www.organization.com, has an IP address of 166.18.75.6. However, over the past hour the SOC has received reports of the site's homepage displaying incorrect information. A quick nslookup search shows https://www.organization.com is pointing to 151.191.122.115. Which of the following is occurring?

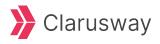
- (A). DoS attack
- (B). ARP poisoning
- (C). DNS spoofing
- (D). NXDOMAIN attack





NO.1 A company's public-facing website, https://www.organization.com, has an IP address of 166.18.75.6. However, over the past hour the SOC has received reports of the site's homepage displaying incorrect information. A quick nslookup search shows https://www.organization.com is pointing to 151.191.122.115. Which of the following is occurring?

- (A). DoS attack
- (B). ARP poisoning
- (C). DNS spoofing
- (D). NXDOMAIN attack





NO.2 After reviewing the following vulnerability scanning report:

Server:192.168.14.6

Service: Telnet

Port: 23 Protocol: TCP

Status: Open Severity: High

Vulnerability: Use of an insecure network protocol

A security analyst performs the following test:

nmap -p 23 192.168.14.6 --script telnet-encryption

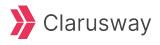
PORT STATE SERVICE REASON

23/tcp open telnet syn-ack

telnet encryption: Telnet server supports encryption

Which of the following would the security analyst conclude for this reported vulnerability?

- (A). It is a false positive
- (B). A rescan is required
- (C). It is considered noise
- (D). Compensating controls exist





NO.2 After reviewing the following vulnerability scanning report:

Server:192.168.14.6

Service: Telnet

Port: 23 Protocol: TCP

Status: Open Severity: High

Vulnerability: Use of an insecure network protocol

A security analyst performs the following test:

nmap -p 23 192.168.14.6 --script telnet-encryption

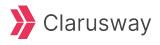
PORT STATE SERVICE REASON

23/tcp open telnet syn-ack

telnet encryption: Telnet server supports encryption

Which of the following would the security analyst conclude for this reported vulnerability?

- (A). It is a false positive
- (B). A rescan is required
- (C). It is considered noise
- (D). Compensating controls exist





NO.3 Which of the following would be used to detect an employee who is emailing a customer list to a personal account before leaving the company?

- A. DLP
- B. FIM
- C. IDS
- D. EDR



NO.3 Which of the following would be used to detect an <u>employee who is emailing a customer list to a personal account</u> before leaving the company?

A. DLP

B. FIM

C. IDS

D. EDR



NO.4 An administrator has identified and fingerprinted specific files that will generate an alert if an attempt is made to email these files outside of the organization.

Which of the following best describes the tool the administrator is using?

A. DLP

B. SNMP traps

C. SCAP

D. IPS



NO.4 An administrator has identified and fingerprinted specific files that will generate an alert if an attempt is made to **email these files outside of the organization**.

Which of the following best describes the tool the administrator is using?

A. DLP

B. SNMP traps

C. SCAP

D. IPS







NO.1 A company wants to verify that the software the company is deploying came from the vendor the company purchased the software from. Which of the following is the best way for the company to confirm this information?

- (A). Validate the code signature
- (B). Execute the code in a sandbox
- (C). Search the executable for ASCII strings
- (D). Generate a hash of the files



NO.1 A company wants to verify that the software the company is deploying came from the vendor the company purchased the software from. Which of the following is the best way for the company to confirm this information?

- (A). Validate the code signature
- (B). Execute the code in a sandbox
- (C). Search the executable for ASCII strings
- (D). Generate a hash of the files



NO.2 A software development manager wants to ensure the authenticity of the code created by the company. Which of the following options is the most appropriate?

- (A). Testing input validation on the user input fields
- (B). Performing code signing on company-developed software
- (C). Performing static code analysis on the software
- (D). Ensuring secure cookies are use



NO.2 A software development manager wants to ensure the authenticity of the code created by the company. Which of the following options is the most appropriate?

- (A). Testing input validation on the user input fields
- (B). Performing code signing on company-developed software
- (C). Performing static code analysis on the software
- (D). Ensuring secure cookies are use



NO.3 An organization recently updated its security policy to include the following statement: Regular expressions are included in source code to remove special characters such as \$, |, ;. &,`, and ? from variables set by forms in a web application. Which of the following best explains the security technique the organization adopted by making this addition to the policy?

- (A). Identify embedded keys
- (B). Code debugging
- (C). Input validation
- (D). Static code analysis





NO.3 An organization recently updated its security policy to include the following statement: Regular expressions are included in source code to remove special characters such as \$, |, ;. &,`, and ? from variables set by forms in a web application. Which of the following best explains the security technique the organization adopted by making this addition to the policy?

- (A). Identify embedded keys
- (B). Code debugging
- (C). Input validation
- (D). Static code analysis





NO.4 An organization wants to ensure the integrity of compiled binaries in the production environment.

Which of the following security measures would best support this objective?

- A. Input validation
- B. Code signing
- C. SQL injection
- **D.** Static analysis



NO.4 An organization wants to **ensure the integrity** of compiled binaries in the production environment.

Which of the following security measures would best support this objective?

- A. Input validation
- **B.** Code signing
- C. SQL injection
- **D.** Static analysis



THANKS!

Any questions?





Our Graduates are Hired By





Google Deloitte. AT&T ally













































