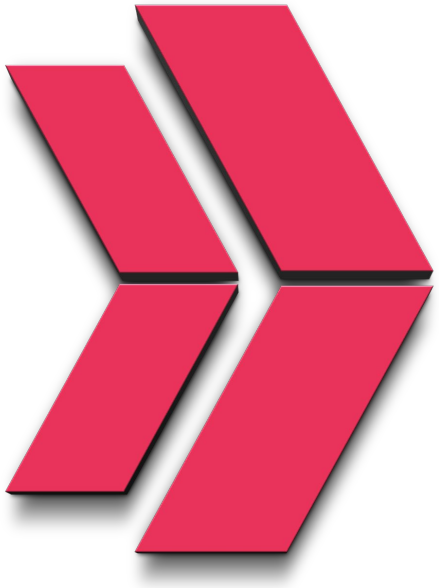


CLARUSWAY

WAY TO REINVENT YOURSELF

CompTIA (9A-9B)

AGENDA

- 9A - Network Security Baselines (3)
- 9B - Network Security Capability Enhancement (5)
- TOTAL: 8

9A - Network Security Baselines

9A - Network Security Baselines

NO.1 After a security incident, a systems administrator asks the company to buy a NAC platform. Which of the following attack surfaces is the systems administrator trying to protect?

(A). Bluetooth

(B). Wired

(C). NFC

(D). SCADA

9A - Network Security Baselines

NO.1 After a security incident, a systems administrator asks the company to buy a NAC platform. Which of the following attack surfaces is the systems administrator trying to protect?

(A). Bluetooth

(B). Wired

(C). NFC

(D). SCADA

9A - Network Security Baselines

NO.2 A security analyst needs to harden access to a network. One of the requirements is to authenticate users with smart cards. Which of the following should the analyst enable to best meet this requirement?

(A). CHAP

(B). PEAP

(C). MS-CHAPv2

(D). EAP-TLS

9A - Network Security Baselines

NO.2 A security analyst needs to harden access to a network. One of the requirements is to authenticate users with smart cards. Which of the following should the analyst enable to best meet this requirement?

(A). CHAP

(B). PEAP

(C). MS-CHAPv2

(D). EAP-TLS

9A - Network Security Baselines

NO.3 Local guidelines require that all information systems meet a minimum security baseline to be compliant. Which of the following can security administrators use to assess their system configurations against the baseline?

(A). SOAR playbook

(B). Security control matrix

(C). Risk management framework

(D). Benchmarks

9A - Network Security Baselines

NO.3 Local guidelines require that all information systems meet a minimum security baseline to be compliant. Which of the following can security administrators use to assess their system configurations against the baseline?

(A). SOAR playbook

(B). Security control matrix

(C). Risk management framework

(D). Benchmarks

9A - Network Security Baselines

NO.4 An administrator needs to perform server hardening before deployment.

Which of the following steps should the administrator take? (Select two).

A. Disable default accounts.
B. Add the server to the asset inventory.
C. Remove unnecessary services.
D. Document default passwords.
E. Send server logs to the SIEM.
F. Join the server to the corporate domain.

9A - Network Security Baselines

NO.4 An administrator needs to perform **server hardening before deployment.**

Which of the following steps should the administrator take? (Select two).

A. Disable default accounts.
B. Add the server to the asset inventory.
C. Remove unnecessary services.
D. Document default passwords.
E. Send server logs to the SIEM.
F. Join the server to the corporate domain.

9A - Network Security Baselines

NO.5 A security analyst is creating a base for the server team to follow when hardening new devices for deployment.

Which of the following best describes what the analyst is creating?
A. Change management procedure
B. Information security policy
C. Cybersecurity framework
D. Secure configuration guide

9A - Network Security Baselines

NO.5 A security analyst is **creating a base** for the server team to follow when hardening new devices for deployment.

Which of the following best describes what the analyst is creating?
A. Change management procedure
B. Information security policy
C. Cybersecurity framework
D. Secure configuration guide

9A - Network Security Baselines

NO.6 Since a recent upgrade to a WLAN infrastructure, several mobile users have been unable to access the internet from the lobby. The networking team performs a heat map survey of the building and finds several WAPs in the area. The WAPs are using similar frequencies with high power settings.

Which of the following installation considerations should the security team evaluate next?
A. Channel overlap
B. Encryption type
C. New WLAN deployment
D. WAP placement

9A - Network Security Baselines

NO.6 Since a recent upgrade to a WLAN infrastructure, several mobile users have been unable to access the internet from the lobby. The networking team performs a heat map survey of the building and finds several WAPs in the area. The WAPs are using similar frequencies with high power settings.

Which of the following installation considerations should the security team evaluate next?

A. Channel overlap
B. Encryption type
C. New WLAN deployment
D. WAP placement

9B - Network Security Capability Enhancement

9B - Network Security Capability Enhancement

NO.1 A company needs to provide administrative access to internal resources while minimizing the traffic allowed through the security boundary. Which of the following methods is most secure?

(A). Implementing a bastion host

(B). Deploying a perimeter network

(C). Installing a WAF

(D). Utilizing single sign-on

9B - Network Security Capability Enhancement

NO.1 A company needs to provide administrative access to internal resources while minimizing the traffic allowed through the security boundary. Which of the following methods is most secure?

(A). Implementing a bastion host

(B). Deploying a perimeter network

(C). Installing a WAF

(D). Utilizing single sign-on

9B - Network Security Capability Enhancement

NO.2 Users at a company are reporting they are unable to access the URL for a new retail website because it is flagged as gambling and is being blocked.

Which of the following changes would allow users to access the site?

(A). Creating a firewall rule to allow HTTPS traffic

(B). Configuring the IPS to allow shopping

(C). Tuning the DLP rule that detects credit card data

(D). Updating the categorization in the content filter

9B - Network Security Capability Enhancement

NO.2 Users at a company are reporting they are unable to access the URL for a new retail website because it is flagged as gambling and is being blocked.

Which of the following changes would allow users to access the site?

(A). Creating a firewall rule to allow HTTPS traffic

(B). Configuring the IPS to allow shopping

(C). Tuning the DLP rule that detects credit card data

(D). Updating the categorization in the content filter

9B - Network Security Capability Enhancement

NO.3 After an audit, an administrator discovers all users have access to confidential data on a file server. Which of the following should the administrator use to restrict access to the data quickly?

(A). Group Policy

(B). Content filtering

(C). Data loss prevention

(D). Access control lists

9B - Network Security Capability Enhancement

NO.3 After an audit, an administrator discovers all users have access to confidential data on a file server. Which of the following should the administrator use to restrict access to the data quickly?

(A). Group Policy

(B). Content filtering

(C). Data loss prevention

(D). Access control lists

9B - Network Security Capability Enhancement

NO.4 A company's web filter is configured to scan the URL for strings and deny access when matches are found. Which of the following search strings should an analyst employ to prohibit access to non-encrypted websites?

(A). encryption=off\

(B). http://

(C). www.*.com

(D). :443

9B - Network Security Capability Enhancement

NO.4 A company's web filter is configured to scan the URL for strings and deny access when matches are found. Which of the following search strings should an analyst employ to prohibit access to non-encrypted websites?

(A). encryption=off\

(B). http://

(C). www.*.com

(D). :443

9B - Network Security Capability Enhancement

NO.5 During a security incident, the security operations team identified sustained network traffic from a malicious IP address: 10.1.4.9. A security analyst is creating an inbound firewall rule to block the IP address from accessing the organization's network. Which of the following fulfills this request?

(A). access-list inbound deny ig source 0.0.0.0/0 destination 10.1.4.9/32

(B). access-list inbound deny ig source 10.1.4.9/32 destination 0.0.0.0/0

(C). access-list inbound permit ig source 10.1.4.9/32 destination 0.0.0.0/0

(D). access-list inbound permit ig source 0.0.0.0/0 destination 10.1.4.9/32

9B - Network Security Capability Enhancement

NO.5 During a security incident, the security operations team identified sustained network traffic from a malicious IP address: 10.1.4.9. A security analyst is creating an inbound firewall rule to block the IP address from accessing the organization's network. Which of the following fulfills this request?

(A). access-list inbound deny ig source 0.0.0.0/0 destination 10.1.4.9/32

(B). access-list inbound deny ig source 10.1.4.9/32 destination 0.0.0.0/0

(C). access-list inbound permit ig source 10.1.4.9/32 destination 0.0.0.0/0

(D). access-list inbound permit ig source 0.0.0.0/0 destination 10.1.4.9/32

9B - Network Security Capability Enhancement

NO.6 Which of the following is most likely to be deployed to obtain and analyze attacker activity and techniques?

A. Firewall
B. IDS
C. Honeypot
D. Layer 3 switch

9B - Network Security Capability Enhancement

NO.6 Which of the following is most likely to be deployed to **obtain and analyze attacker activity and techniques**?

A. Firewall
B. IDS
C. Honeypot
D. Layer 3 switch

9B - Network Security Capability Enhancement

NO.7 Which of the following is the first step to take when creating an anomaly detection process?

A. Selecting events
B. Building a baseline
C. Selecting logging options
D. Creating an event log

9B - Network Security Capability Enhancement

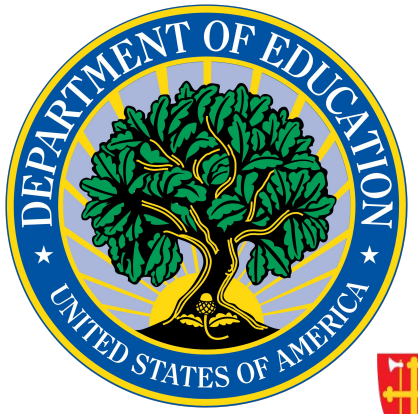
NO.7 Which of the following is the first step to take when **creating an anomaly detection process**?

A. Selecting events
B. Building a baseline
C. Selecting logging options
D. Creating an event log

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