DUMPSBOSS.COM

Certified Information Systems Security Professional

ISC CISSP

Version Demo

Total Demo Questions: 15

Total Premium Questions: 1382

Buy Premium PDF

https://dumpsboss.com

support@dumpsboss.com

Topic Break Down

Topic	No. of Questions
Topic 1, New Update	343
Topic 2, Jan 2023 Update	478
Topic 3, Security and Risk Management	28
Topic 4, Asset Security	48
Topic 5, Security Architecture and Engineering	67
Topic 6, Communication and Network Security	83
Topic 7, Identity and Access Management (IAM)	26
Topic 8, Security Assessment and Testing	37
Topic 9, Security Operations	46
Topic 10, Software Development Security	129
Topic 11, Mixed questions	97
Total	1382

QUESTION NO: 1

After a thorough analysis, it was discovered that a perpetrator compromised a network by gaining access to the network through a Secure Socket Layer (SSL) Virtual Private Network (VPN) gateway. The perpetrator guessed a username and brute forced the password to gain access. Which of the following BEST mitigates this issue?

A. Implement strong passwords authentication for VPN

B. Integrate the VPN with centralized credential stores

C. Implement an Internet Protocol Security (IPSec) client

D. Use two-factor authentication mechanisms

ANSWER: D

Explanation:

QUESTION NO: 2

Which of the following actions should be undertaken prior to deciding on a physical baseline Protection Profile (PP)?

A. Check the technical design.

B. Conduct a site survey.

C. Categorize assets.

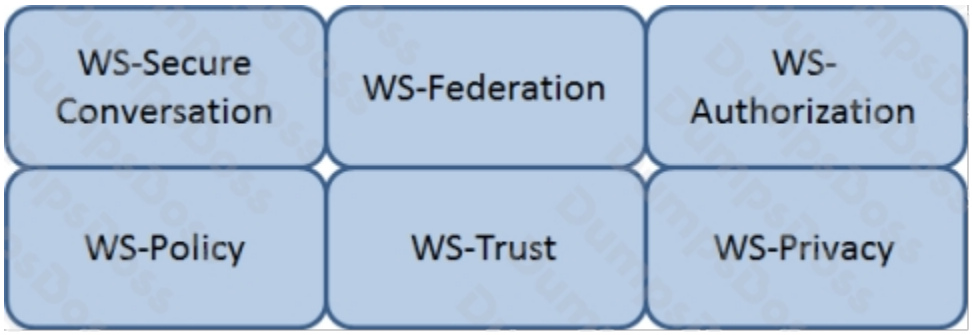
D. Choose a suitable location.

ANSWER: A

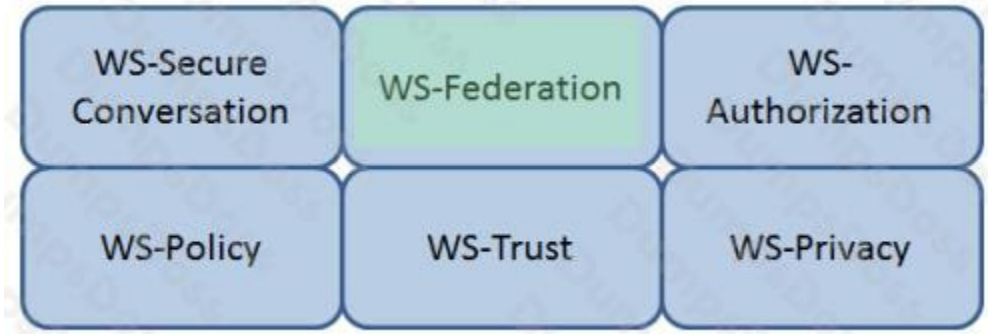
QUESTION NO: 3 - (HOTSPOT)

HOT SPOT

Which Web Services Security (WS-Security) specification maintains a single authenticated identity across multiple dissimilar environments? Click on the correct specification in the image below.



ANSWER:



Explanation:

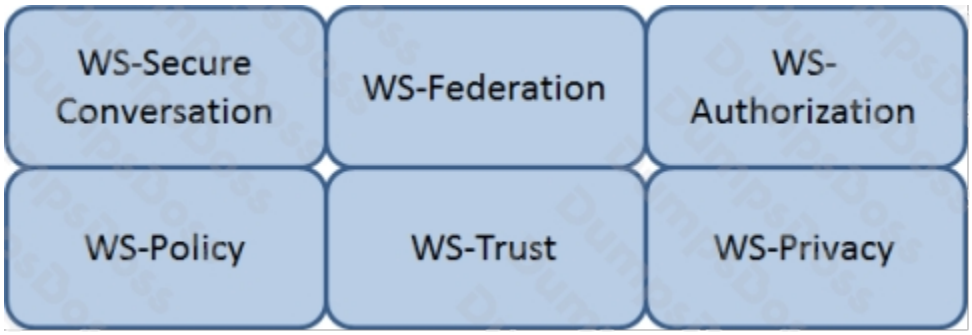
WS-Federation

Reference: Java Web Services: Up and Running" By Martin Kalin page 228

QUESTION NO: 4 - (HOTSPOT)

HOT SPOT

Which Web Services Security (WS-Security) specification negotiates how security tokens will be issued, renewed and validated? Click on the correct specification in the image below.



Answer:

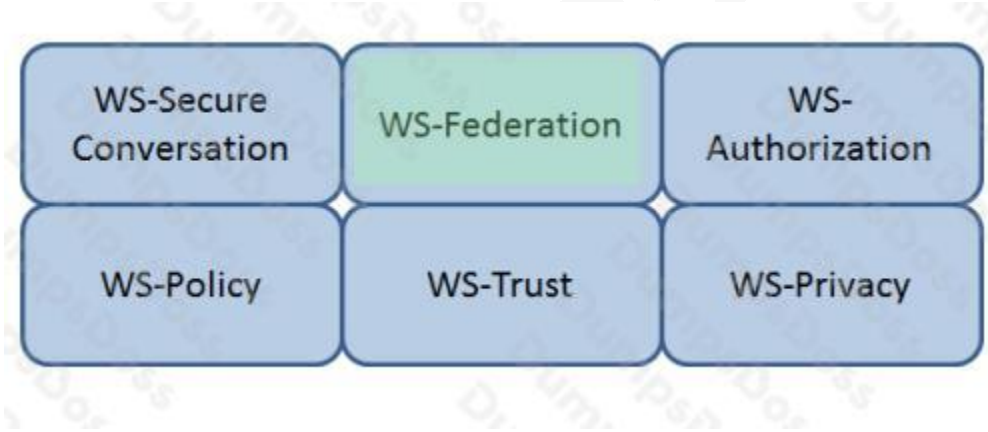
Explanation:

WS-Trust

The protocol used for issuing security tokens is based on WS-Trust. WS-Trust is a Web service specification that builds on WS-Security. It describes a protocol used for issuance, exchange, and validation of security tokens. WS-Trust provides a solution for interoperability by defining a protocol for issuing and exchanging security tokens, based on token format, namespace, or trust boundaries. Reference: https://msdn.microsoft.com/en-us/library/ff650503.aspx

---

ANSWER:



Explanation:

WS-Trust

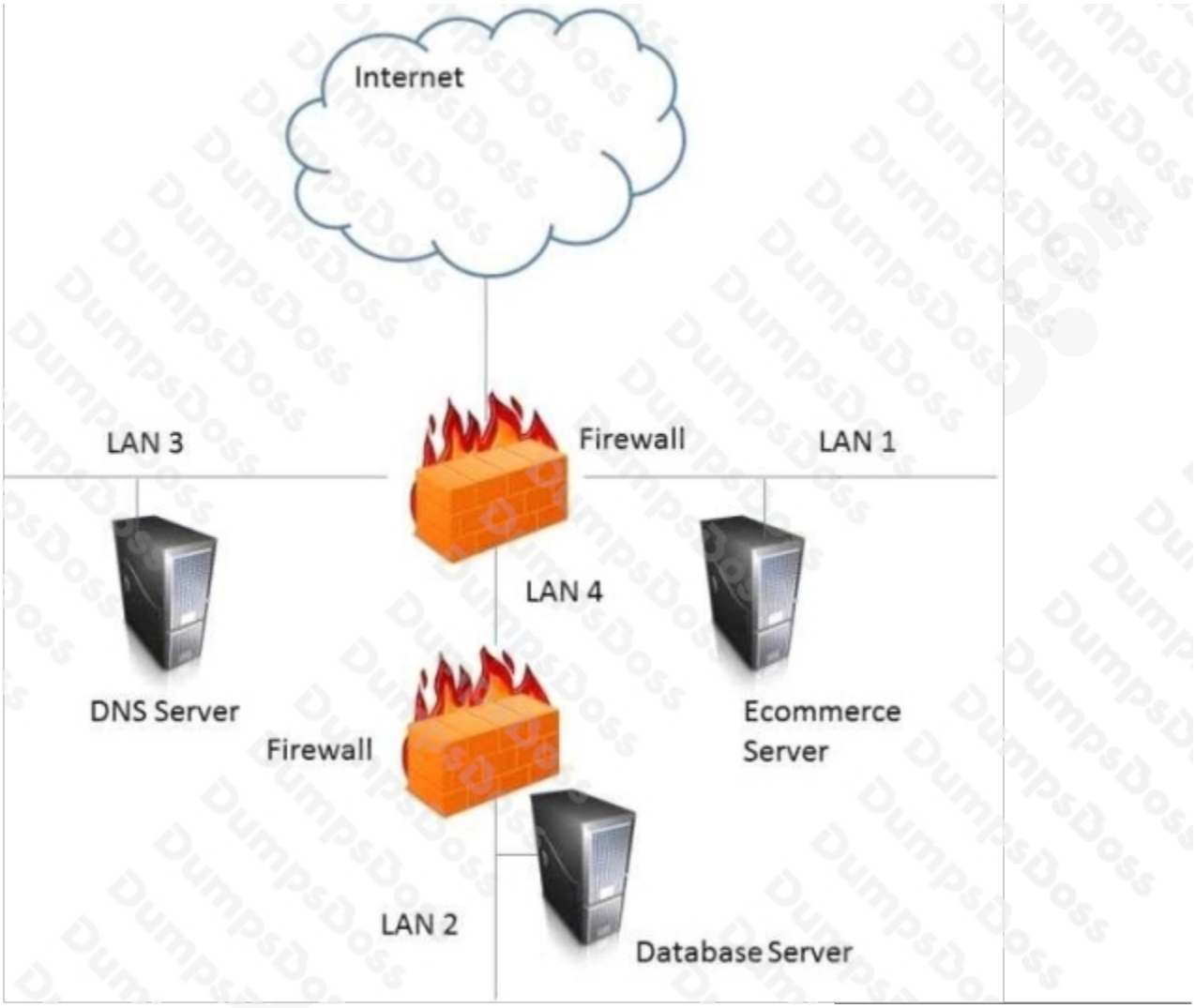
The protocol used for issuing security tokens is based on WS-Trust. WS-Trust is a Web service specification that builds on WS-Security. It describes a protocol used for issuance, exchange, and validation of security tokens. WS-Trust provides a solution for interoperability by defining a protocol for issuing and exchanging security tokens, based on token format, namespace, or trust boundaries. Reference: https://msdn.microsoft.com/en-us/library/ff650503.aspx

---

QUESTION NO: 5 - (HOTSPOT)

HOT SPOT

In the network design below, where is the MOST secure Local Area Network (LAN) segment to deploy a Wireless Access Point (WAP) that provides contractors access to the Internet and authorized enterprise services?

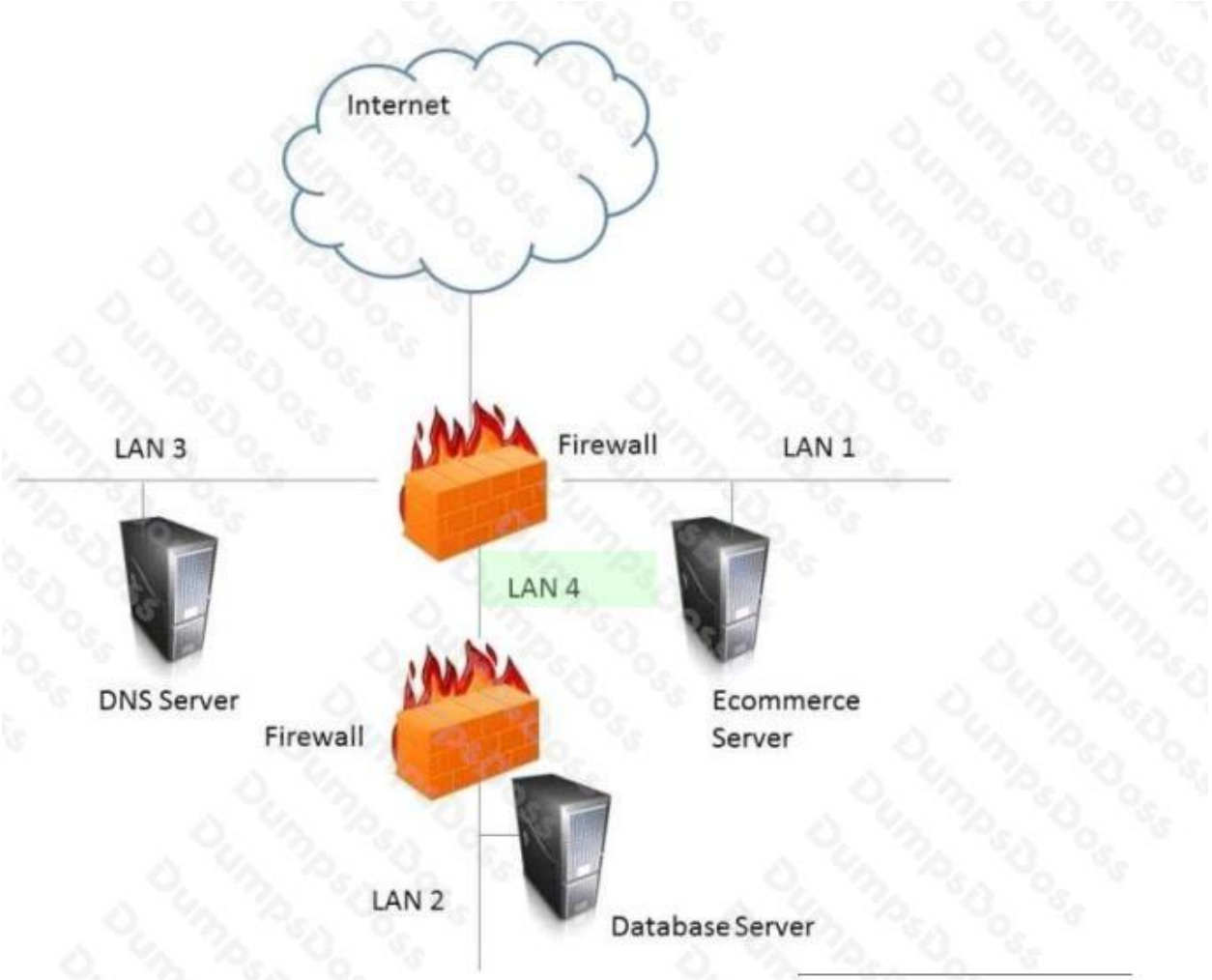


Answer:

Explanation:

LAN 4

ANSWER:



Explanation:

LAN 4

QUESTION NO: 6

How does Radio-Frequency Identification (RFID) assist with asset management?

A. It uses biometric information for system identification.

B. It uses two-factor authentication (2FA) for system identification.

C. It transmits unique Media Access Control (MAC) addresses wirelessly.

D. It transmits unique serial numbers wirelessly.

ANSWER: B

QUESTION NO: 7

In a High Availability (HA) environment, what is the PRIMARY goal of working with a virtual router address as the gateway to a network?

A. The second of two routers can periodically check in to make sure that the first router is operational.

B. The second of two routers can better absorb a Denial of Service (DoS) attack knowing the first router is present.

C. The first of two routers fails and is reinstalled, while the second handles the traffic flawlessly.

D. The first of two routers can better handle specific traffic, while the second handles the rest of the traffic seamlessly.

ANSWER: C

Explanation:

QUESTION NO: 8

Which of the following is the BEST type of authentication and encryption for a Secure Shell (SSH) implementation when network traffic traverses between a host and an infrastructure device?

A. Lightweight Directory Access Protocol (LDAP)

B. Public-key cryptography

C. Remote Authentication Dial-In User Service (RADIUS)

D. Private-key cryptography

ANSWER: B

Explanation:



GjsSJmaHZ_O9Iw&hl=en&sa=X&ved=2ahUKEwjDobCajqrpAhWMHRQKHW2FC4gQ6AEwAHoECBQQAQ#v=onepage&q=type%20of%20authentication%20and%20encryption%20for%20a%

20Secure%20Shell%20(SSH)%20implementation%20when%20network%20traffic%20traverses%20between%20a%20host%20and%20an%20infrastructure%20device&f=false

QUESTION NO: 9

When dealing with compliance with the Payment Card Industry-Data Security Standard (PCI-DSS), an organization that shares card holder information with a service provider MUST do which of the following?

A. Perform a service provider PCI-DSS assessment on a yearly basis

B. Validate the service provider's PCI-DSS compliance status on a regular basis

C. Validate that the service providers security policies are in alignment with those of the organization

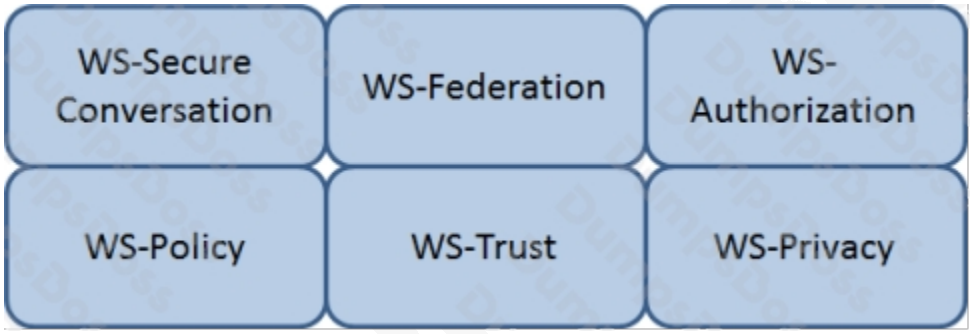
D. Ensure that the service provider updates and tests its Disaster Recovery Plan (DRP) on a yearly basis

ANSWER: B

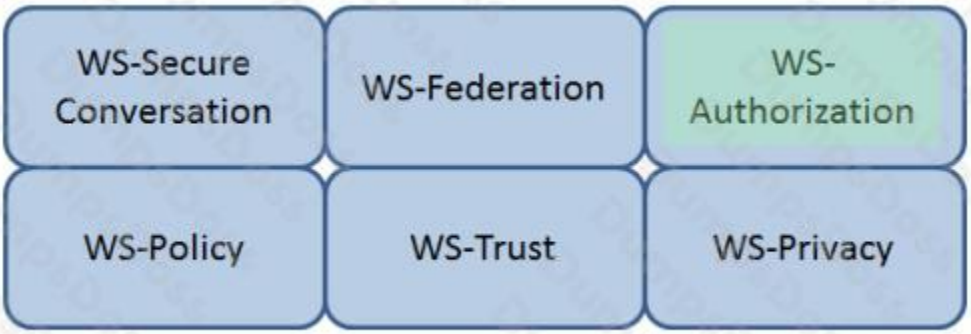
QUESTION NO: 10 - (HOTSPOT)

HOT SPOT

Which Web Services Security (WS-Security) specification handles the management of security tokens and the underlying policies for granting access? Click on the correct specification in the image below.



ANSWER:



Explanation:

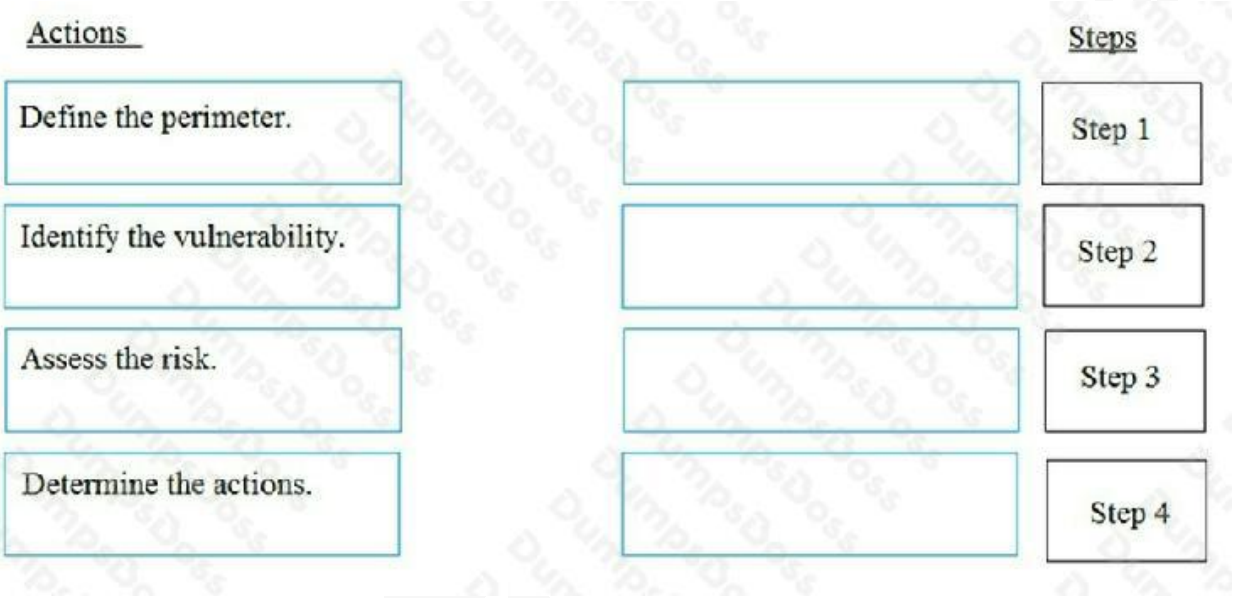
WS-Authorization

Reference: Java Web Services: Up and Running" By Martin Kalin page 228

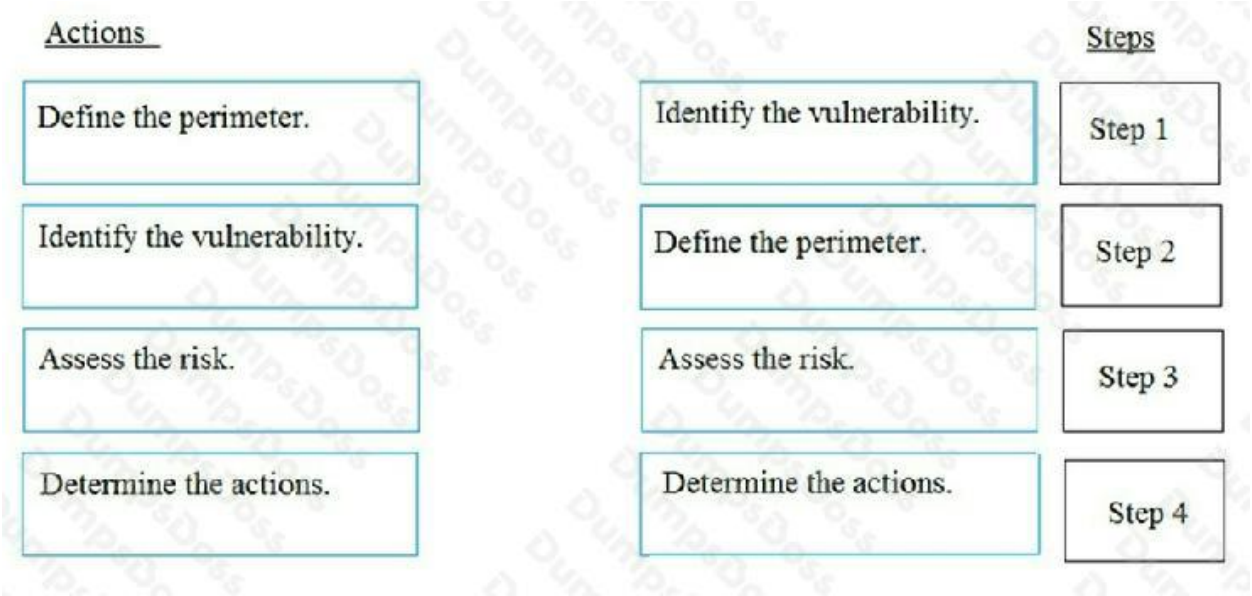
QUESTION NO: 11 - (DRAG DROP)

What is the correct order of steps in an information security assessment?

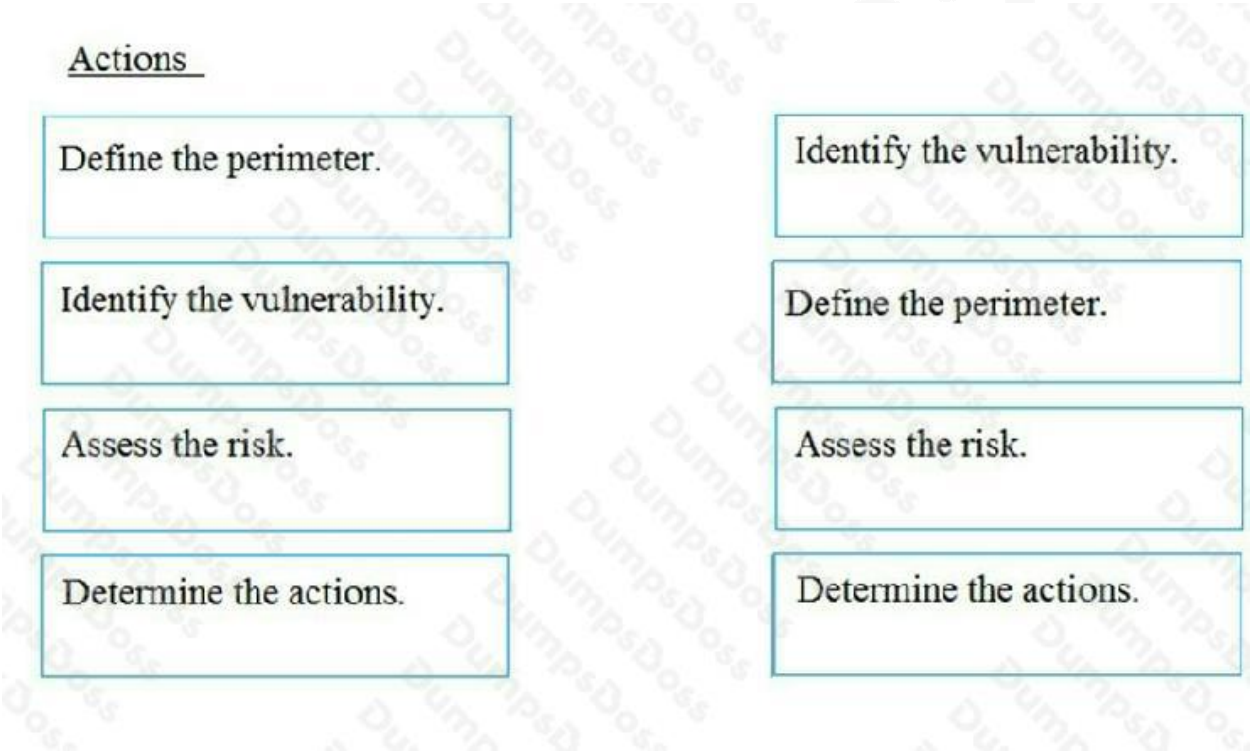
Place the information security assessment steps on the left next to the numbered boxes on the right in the correct order.



ANSWER:



Explanation:



QUESTION NO: 12 - (DRAG DROP)

DRAG DROP

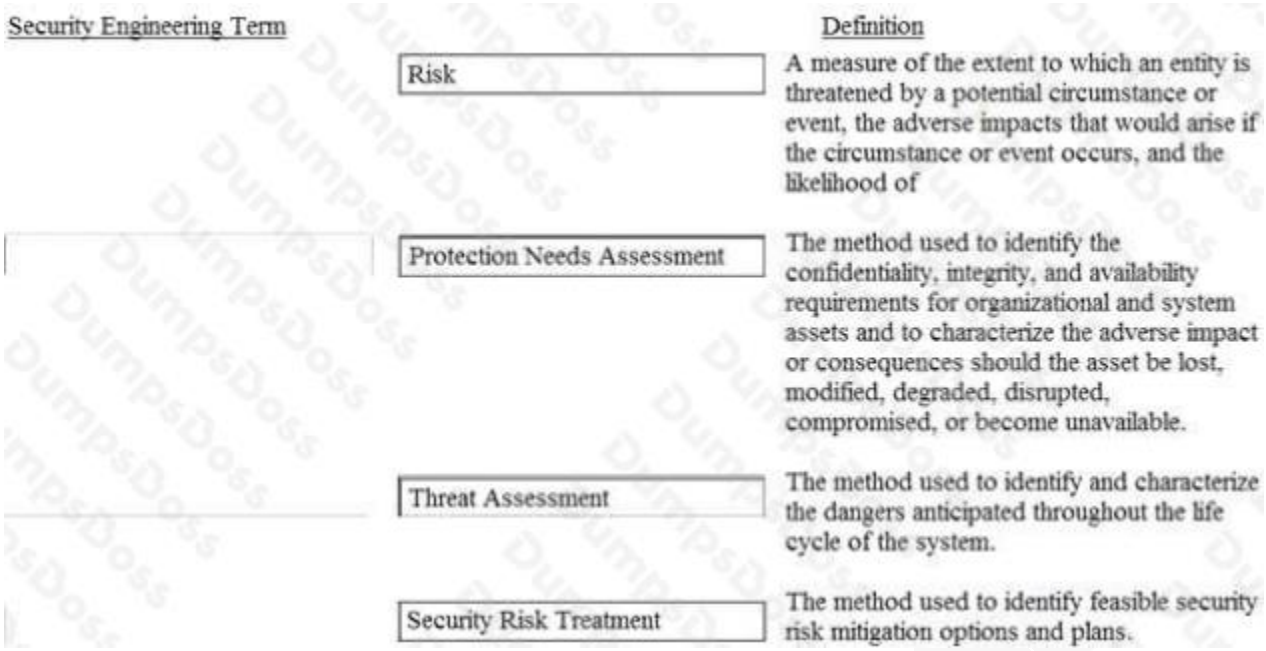
Drag the following Security Engineering terms on the left to the BEST definition on the right.

Security Engineering Term		Definition
Risk		A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of
Security Risk Treatment		The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.
Protection Needs Assessment		The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.
Threat Assessment		The method used to identify feasible security risk mitigation options and plans.

ANSWER:

Security Engineering Term		Definition
Risk	Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of
Security Risk Treatment	Protection Needs Assessment	The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.
Protection Needs Assessment	Threat Assessment	The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.
Threat Assessment	Security Risk Treatment	The method used to identify feasible security risk mitigation options and plans.

Explanation:



Risk - A measure of the extent to which an entity is threatened by a potential circumstance of event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of occurrence.

Protection Needs Assessment - The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should be asset be lost, modified, degraded, disrupted, compromised, or become unavailable.

Threat assessment - The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.

Security Risk Treatment - The method used to identify feasible security risk mitigation options and plans.

QUESTION NO: 13

The adoption of an enterprise-wide Business Continuity (BC) program requires which of the following?

A. Good communication throughout the organization

B. A completed Business Impact Analysis (BIA)

C. Formation of Disaster Recovery (DR) project team

D. Well-documented information asset classification

ANSWER: B

QUESTION NO: 14

Which of the following management process allows ONLY those services required for users to accomplish their tasks, change default user passwords, and set servers to retrieve antivirus updates?

A. Configuration

B. Identity

C. Compliance

D. Patch

ANSWER: A

QUESTION NO: 15

At which layer of the Open Systems Interconnect (OSI) model are the source and destination address for a datagram handled?

A. Transport Layer

B. Data-Link Layer

C. Network Layer

D. Application Layer

ANSWER: C

Explanation:

DUMPSBOSS.COM