CISSP-2018^{Q&As}

Certified Information Systems Security Professional 2018

Pass ISC CISSP-2018 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/cissp-2018.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by ISC Official Exam Center

Instant Download After Purchase

100% Money Back Guarantee

365 Days Free Update

800,000+ Satisfied Customers

QUESTION 1

DRAG DROP

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

Select and Place:

Security Engineering | | Definition

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.**

Threat Assessment | | 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 occurrence.**

Protection Needs | | The method used to identify and characterize the dangers anticipated **throughout the life cycle of the system.**

Risk | | The method used to identify feasible security **risk mitigation options and plans.**

Correct Answer:

Security Engineering

	Definition
Protection Needs	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.
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 occurrence.
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 2

DRAG DROP

A software security engineer is developing a black box-based test plan that will measure the system\\'s reaction to incorrect or illegal inputs or unexpected operational errors and situations. Match the functional testing techniques on the left with the correct input parameters on the right.

Select and Place:

Functional Testing Techniques		Input Parameter Selection
State-Based Analysis		Select one input that does not belong to any of the identified partitions.
Equivalence Class Analysis		Select inputs that are at the external limits of the domain of valid values.
Decision Table Analysis		Select invalid combinations of input values.
Boundary Value Analysis		Select unexpected inputs corresponding to each known condition.

Correct Answer:

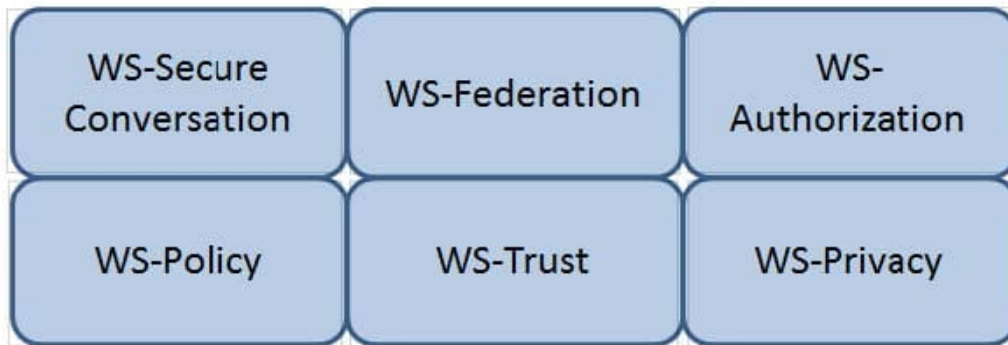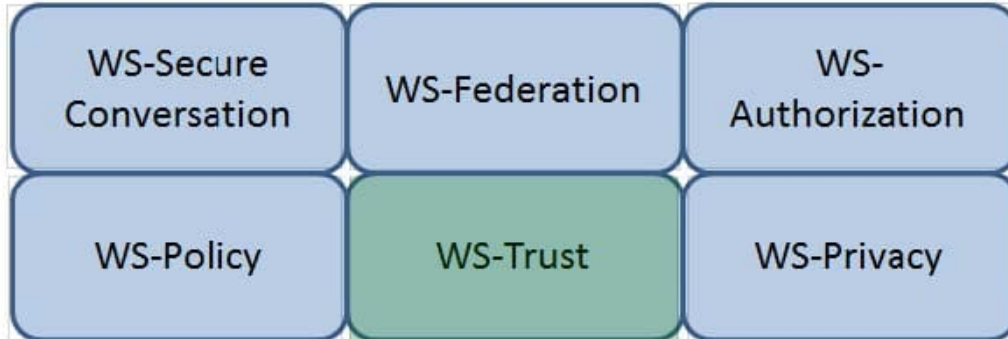| Functional Testing Techniques		Input Parameter Selection
	Equivalence Class Analysis	Select one input that does not belong to any of the identified partitions.
	Boundary Value Analysis	Select inputs that are at the external limits of the domain of valid values.
	Decision Table Analysis	Select invalid combinations of input values.
	State-Based Analysis	Select unexpected inputs corresponding to each known condition.

QUESTION 3

HOTSPOT

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.

Hot Area:

WS-Secure Conversation	WS-Federation	WS-Authorization
WS-Policy	WS-Trust	WS-Privacy

Correct Answer:

WS-Secure Conversation	WS-Federation	WS-Authorization
WS-Policy	WS-Trust	WS-Privacy

QUESTION 4

DRAG DROP

Match the name of access control model with its associated restriction.

Drag each access control model to its appropriate restriction access on the right.

Select and Place:

Access Control Model		Restrictions
Mandatory Access Control		End user cannot set controls
Discretionary Access Control(DAC)		Subject has total control over objects
Role Based Access Control (RBAC)		Dynamically assigns permissions to particular duties based on job function
Rule Based Access Control		Dynamically assigns roles to subjects bases on criteria assigned by a custodian

Correct Answer:

Access Control Model		Restrictions
	Mandatory Access Control	End user cannot set controls
	Discretionary Access Control (DAC)	Subject has total control over objects
	Role Based Access Control (RBAC)	Dynamically assigns permissions to particular duties based on job function
	Rule Based Access Control	Dynamically assigns roles to subjects bases on criteria assigned by a custodian

QUESTION 5

DRAG DROP

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

Select and Place:

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
	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.
	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.

Correct Answer:

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.

Latest CISSP-2018 Dumps   **CISSP-2018 VCE Dumps**   **CISSP-2018 Braindumps**