

CCNA Security IINS 640-553 Drag and Drop Questions (1-5)

Question 1

Match the descriptions on the left with the IKE phases on the right.

| | |
|--|-------------|
| Perform a Diffie-Hellman exchange | IKE Phase 1 |
| Establish IPsec SAs | |
| Negotiate IPsec security policies | IKE Phase 2 |
| Negotiate IKE policy sets and authenticate peers | |
| Perform an optional Diffie-Hellman exchange | |

Answer:

Match the descriptions on the left with the IKE phases on the right.

| | |
|--|-------------|
| Perform a Diffie-Hellman exchange | IKE Phase 1 |
| Establish IPsec SAs | |
| Negotiate IPsec security policies | IKE Phase 2 |
| Negotiate IKE policy sets and authenticate peers | |
| Perform an optional Diffie-Hellman exchange | |

Question 2

Match the cryptographic algorithms on the left with the type of algorithm on the right.

| | |
|------------------|------------|
| 3DES | Symmetric |
| RSA | |
| Diffie-Hellman | |
| AES | Asymmetric |
| IDEA | |
| Elliptical Curve | |

Answer:

Match the cryptographic algorithms on the left with the type of algorithm on the right.

| | |
|--|------------|
| | Symmetric |
| | |
| | |
| | Asymmetric |
| | |
| | |

Question 3

Drag the best practices for attack mitigation on the left to the list on the right. Not all choices are used.

| | |
|---|---------------------------------------|
| Store sensitive data on stand-alone devices | Best practices for attack mitigation: |
| Keep patches up to date | |
| Use passwords that cannot be broken | |
| Develop a static, tested security policy | |
| Inform users about social engineering | |
| Develop a dynamic security policy | |
| Log everything to a syslog server for forensic purposes | |
| Disable unnecessary services | |

Answer:

Drag the best practices for attack mitigation on the left to the list on the right. Not all choices are used.

Store sensitive data on stand-alone devices

Keep patches up to date

Use passwords that cannot be broken

Develop a static, tested security policy

Inform users about social engineering

Develop a dynamic security policy

Log everything to a syslog server for forensic purposes

Disable unnecessary services

Best practices for attack mitigation:

Keep patches up to date

Inform users about social engineering

Develop a dynamic security policy

Disable unnecessary services

Question 4 Drag the result on the left to the corresponding attack method on the right.

Identify operating systems

Determine live hosts

Determine potential vulnerabilities

Identify devices

Identify active services

Ping Sweep

Port Scan

Answer: Drag the result on the left to the corresponding attack method on the right.

Identify operating systems

Determine live hosts

Determine potential vulnerabilities

Identify devices

Identify active services

Ping Sweep

Determine live hosts

Identify devices

Port Scan

Question 5 Drag each AAA function on the left to the protocol that it corresponds to.

Has no option to authorize router commands

Encrypts the entire packet

Combines authentication and authorization functions

Uses TCP port 49

TACACS+

RADIUS

Answer: Drag each AAA function on the left to the protocol that it corresponds to.

Has no option to authorize router commands

Encrypts the entire packet

Combines authentication and authorization functions

Uses TCP port 49

TACACS+

Uses TCP port 49

Encrypts the entire packet

RADIUS

Combines authentication and authorization functions

Has no option to authorize router commands

All, there are 5 DD Questions on CCNA Security 640-553 Real Exam.