IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **SC0-402**

Title : Network Defense and Countermeasures (NDC)

Version : Demo

1.It has come to your attention that some host on the web has tried to do some reconnaissance on your network and send a VRFY command to try and steal user names. What type of attack was used against your network?

A. SMTP attack
B. Web browser attack
C. IMAP attack
D. IP Spoofing
E. Account scan
Answer: A

2.What technology is being employed to resist SYN floods by having each side of the connection attempt create its own sequence number (This sequence number contains a synopsis of the connection so that if/when the connection attempt is finalized the fist part of the attempt can be re-created from the sequence number)?

A. SYN cookie
B. SYN floodgate
C. SYN gate
D. SYN damn
E. SYN flood break
Answer: A

3.The main reason you have been hired at a company is to bring the network security of the organization up to current standards. A high priority is to have a full security audit of the network as soon as possible. You have chosen an Independent Audit and are describing it to your coworkers. Which of the following best describes an Independent Audit?

A. An independent audit is usually conducted by external or outside resources and may be a review or audit of detailed audit logs.
B. The independent audit is usually done by the current network administrators who ensure the security measures are up to
international standards.
C. The independent audit is typically done by an internal team who ensures the security measures are up to
international standards.
D. The independent audit is usually done by internal resources to examine the current daily and on-going activities within a network
system for compliance with an established security policy.
E. The independent audit is typically done by a contracted outside team of security experts who check for policy compliance.
Answer: A

4.The main reason you have been hired at a company is to bring the network security of the

organization up to current standards. A high priority is to have a full security audit of the network as soon as possible. You have chosen an Operational Audit and are describing it to your coworkers. Which of the following best describes an Operational audit?

A. This type of audit is typically done by a contracted external team of security experts who check for policy compliance.
B. This type of audit is usually done by internal resources to examine the current daily and on-going activities within a network
system for compliance with an established security policy.
C. This type of audit is typically done by an internal team who ensures the security measures are up to international standards.
D. This type of audit is usually done by the current network administrators who ensure the security measures are up to international
standards.
E. This type of audit is usually conducted by external resources and may be a review or audit of detailed audit logs.
Answer: B

5.Which of the following best describes the Insurance Model?

A. Before incurring the cost for insuring an inoperative asset, check for maintenance agreements that may include the cost of
insurance itself.
B. The insurance model is the transference of risk to an insurance company that covers the costs of replacing the critical assets within
your network. The drawbacks are increase in premiums after making a claim, high premiums anyway, down time while the
insurance company is processing the claim, and claim may not pay what replacement costs are today.
C. The insurance model makes use of preventive measures and regular service as well as updates such as
Service Packs, maintenance
updates, and patches. Preventive measures can also improve the chances of the insurance model working
better than if the system
had no preventive measures ever taken.
D. The insurance model makes use of the acknowledged skills and abilities of the existing personnel. Knowing that assets have very
specific dollar values assigned to them, the choice on how to manage the asset is based on the experience
of the personnel.
E. Assets will typically cost much more than the original capital outlay that it took to purchase it long ago. Insurance costs can be
very high and a decision to exercise this model should not be made in haste. There are also depreciation issues to deal with as well.

Answer: B

6.Which of the following best describes the Repair Model?

A. The model makes use of preventive measures and regular service as well as updates such as Service Packs, maintenance updates,
and patches. Preventive measures can also improve the chances of the repair model working better than if
the system had no
preventive measures ever taken.
B. The repair model is the transference of risk to an insurance company that covers the costs of replacing the critical assets within
your network. The drawbacks are increase in premiums after making a claim, high premiums anyway, down time while the
insurance company is processing the claim, and claim may not pay what replacement costs are today.
C. Assets will typically cost much more than the original capital outlay that it took to purchase it long ago. Repair costs can be very
high and a decision to exercise this model should not be made in haste. There are also depreciation issues
to deal with as well. In
any case, this model should be the last resort because of cost and may be the most time consuming.
D. The repair model makes use of the acknowledged skills and abilities of the existing personnel. Knowing that assets have very
specific dollar values assigned to them, the choice on how to manage the asset is based on the experience
of the personnel.
E. Before incurring the cost for repair of an inoperative asset, check for maintenance agreements that may
include the cost of repair
or the actual repair itself. Nevertheless, the repair model should focus on the restoration of the downed asset to its working status
within the network infrastructure. Keep in mind that after hardware costs, costs for the reloading or replacement of software can
be a large cost factor as well.
Answer: E

7.Which of the following best describes the Total Replacement Model?

A. The total replacement model makes use of the acknowledged skills and abilities of the existing personnel. Knowing that assets
have very specific dollar values assigned to them, the choice on how to manage the asset is based on the experience of the
personnel.
B. Before incurring the cost for replacing of an inoperative asset, check for maintenance agreements that

may include the cost of
repair or the actual repair itself. Nevertheless, the total replacement model should focus on the repairing of
the downed asset to its
working status within the network infrastructure. Keep in mind that after hardware costs, costs for the reloading or replacement of
software can be a large cost factor as well.
C. Assets will typically cost much more than the original capital outlay that it took to purchase it long ago. Replacement costs can be
very high and a decision to exercise this model should not be made in haste. There are also depreciation issues to deal with as well.
In any case, this model should be the last resort because of cost and may be the most time consuming.
D. The total replacement model is the transference of risk to an insurance company that covers the costs of
replacing the critical
assets within your network. The drawbacks are increase in premiums after making a claim, high premiums
anyway, down time
while the insurance company is processing the claim, and claim may not pay what replacement costs are today.
E. The total replacement model makes use of preventive measures and regular service as well as updates
such as Service Packs,
maintenance updates, and patches, before deciding to replace the asset. Preventive measures can also improve the chances of the
replacement model working better than if the system had no preventive measures ever taken.
Answer: C

8.Your company has decided to allow certain people to work from home. The work that they do, does not require that they be in the office for anything more than meetings. In addition, they already have high-speed DSL connections at their homes for personal use. You have been given the task of figuring out how to get your coworkers to connect to your company's network securely and reliably. What technology can you use to solve your problem most effectively?

A. Dedicated Leased Lines (ISDN or T1)
B. Dial-Up via PSTN lines.
C. VPN
D. IPChains
E. IDS
Answer: C

9.Your company has decided to allow certain people to work from home. The work that they do does not require that they be in the office for anything more than meetings and they already have

personal high-speed DSL connections at their homes. You have been given the task of figuring out how to get your coworkers to connect to your company's network securely and reliably. What technology can you use to solve your problem most effectively?

A. Dedicated Leased Lines (ISDN or T1)
B. Dial-Up via PSTN lines.
C. VPN
D. Firewall
E. IDS
Answer: C

10.You have been hired at a large company to manage network. Prior to your arrival, there was no one dedicated to security, so you are starting at the beginning. You hold a meeting and are discussing the main functions and features of network security. One of your assistants asks what the function of Integrity in network security is. Which of the following best describes Integrity?

A. The security must limit user privileges to minimize the risk of unauthorized access to sensitive information and areas of the
network that only authorized users should only be allowed to access.
B. Integrity verifies users to be who they say they are. In data communications, the integrity of the sender is necessary to verify that
the data came from the right source. The receiver is authenticated as well to verify that the data is going to
the right destination.
C. Data communications as well as emails need to be protected for privacy and Integrity. Integrity ensures the privacy of data on the
network system.
D. Integrity is a security principle that ensures the continuous accuracy of data and information stored within network systems. Data
must be kept from unauthorized modification, forgery, or any other form of corruption either from malicious threats or corruption
that is accidental in nature. Upon receiving the email or data communication, integrity must be verified to ensure that the message
has not been altered, modified, or added to or subtracted from in transit by unauthorized users.
E. Security must be established to prevent parties in a data transaction from denying their participation after the business transaction
has occurred. This establishes integrity for the transaction itself for all parties involved in the transaction.
Answer: D

11.You have been hired at a large company to manage network security. Prior to your arrival, there was no one dedicated to security, so you are starting at the beginning. You hold a meeting and are discussing the main functions and features of network security. One of your assistants asks what the function of Confidentiality in network security is. Which of the following best describes

Confidentiality?

A. Confidentiality verifies users to be who they say they are. In data communications, authenticating the sender is necessary to verify
that the data came from the right source. The receiver is authenticated as well to verify that the data is going to the right
destination.
B. Data communications as well as emails need to be protected in order to maintain appropriate levels of privacy and confidentiality.
Network security must provide a secure channel for the transmission of data and email that does not allow eavesdropping by
unauthorized users. Data confidentiality ensures the privacy of data on the network system.
C. The security must limit user privileges to minimize the risk of unauthorized access to sensitive information and areas of the
network that only authorized users should only be allowed to access.
D. Security must be established to prevent parties in a data transaction from denying their participation after the business transaction
has occurred. This establishes Confidentiality for the transaction itself for all parties involved in the transaction.
E. Confidentiality is a security principle that ensures the continuous accuracy of data and information stored within network systems.
Data must be kept from unauthorized modification, forgery, or any other form of corruption either from malicious threats or
corruption that is accidental in nature.
Answer: B

12.You have been hired at a large company to manage the network security issues. Prior to your arrival, there was no one dedicated to security, so you are starting at the beginning. You hold a meeting and are discussing the main functions and features of network security. One of your assistants asks what the function of Authentication in network security is. Which of the following best describes Authentication?

A. Data communications as well as emails need to be protected for privacy and Authentication. Authentication ensures the privacy of
data on the network system.
B. Authentication is a security principle that ensures the continuous accuracy of data and information stored within network systems.
Upon receiving the email or data communication, authentication must be verified to ensure that the message has not been altered,
modified, or added to or subtracted from in transit by unauthorized users.
C. The security must limit user privileges to minimize the risk of unauthorized access to sensitive information and areas of the
network that only authorized users should only be allowed to access.
D. Security must be established to prevent parties in a data transaction from denying their participation

after the business transaction
has occurred. This establishes authentication for the transaction itself for all parties involved in the transaction.
E. Authentication verifies users to be who they say they are. In data communications, authenticating the sender is necessary to verify
that the data came from the right source. The receiver is authenticated as well to verify that the data is going to the right
destination.
Answer: E

13.During a discussion of asset classification and protection with a coworker, you realize that your coworker does not know the basic concepts of asset protection. You are asked to describe the types of asset protection. Which of the following describes the concept of an infeasible protection of an asset?

A. The cost to protect the asset is greater than the cost of recovery of the asset
B. The cost to replace the asset is less than the cost of recovery of the asset
C. the cost to protect the asset is infeasible to determine
D. The cost to replace the asset is greater than the cost of recovery of the asset
E. The cost to protect the asset is less than the cost of recovery of the asset
Answer: A

14.During a discussion of asset classification and protection with a coworker, you realize that your coworker does not know the basic concepts of asset protection. You are asked to describe the types of asset protection. Which of the following describes the concept of feasible protection of an asset?

A. The cost to replace the asset is greater than the cost of recovery of the asset
B. The cost to replace the asset is less than the cost of protect the asset
C. The cost to protect the asset is greater than the cost of recovery of the asset.
D. The cost to replace the asset is less than the cost of recovery of the asset
E. The cost to protect the asset is less than the cost of recovery of the asset.
Answer: E

15.Signatures are generally divided into what three categories?

A. Corruptions
B. Exploits
C. Accesses
D. DoS attacks
E. Reconnaissance
Answer: BDE

16.You were recently hired as the security administrator of a small business. You are reviewing the current state of security in the network and find that the current logging system must be immediately modified. As the system is currently configured, auditing

has no practical value. Which of the following are the reasons that the current auditing has little value?

A. The logs go unchecked.
B. The logs are automatically deleted after three months.
C. The logs are deleted using FIFO and capped at 500Kb.
D. The only auditing is successful file access events.
E. The logs are deleted using FIFO and capped at 5000Kb.
Answer: AD

17.You are considering adding layers to your existing authentication system. Reading through some of the vendor literature on logon solutions, it frequently mentions two and three factor authentication. Your assistant asks you to describe the difference between the two. Select the options that correctly describe two-factor and three-factor authentication:

A. Two-factor authentication is the process providing something you have along with something you know.
B. Two-factor authentication is the process of providing two forms of authentication, such as a username and a password.
C. Two-factor authentication is the process of authenticating twice during the login sequence to verify user identity.
D. Three-factor authentication is the process of providing something you have along with something you know and something you are.
E. Three-factor authentication is the process of providing three forms of authentication, such as username,
password, and sitting at
the physical machine to login.
F. Three-factor authentication is the process of authenticating three times during the login sequence to verify user identity.
Answer: AD

18.You are the firewall administrator at your company and the network administrators have decided to implement a PPTP VPN solution, which of these ports would you need to allow through the firewall to allow these VPN sessions into your network?

A. 1723
B. 2317
C. 1273
D. 1372
E. 7132
Answer: A

19.You are the firewall administrator at your company and the network administrators have decided to implement a VPN solution that will use L2TP. Which port or ports would you

need to allow through the firewall to allow the L2TP traffic to reach the VPN server inside your network from a remote client?

A. TCP 1723
B. UDP 47
C. UDP 1701
D. TCP 443
E. UDP 500
Answer: C

20.You are the firewall administrator for your company and you have just learned that the Server administrators are gearing up support an L2TP based VPN solution. You are told to be sure that your firewall rule sets will not hinder the performance of the VPN. Which of the following ports will you have to allow through the firewall?
A. TCP 1701
B. UDP 1701
C. TCP 443
D. UDP 443
E. TCP1601
Answer: B