N10-006.exam.420q

Number: N10-006
Passing Score: 800
Time Limit: 120 min

N10-006

CompTIA Network+ Certification

Sections
1. Network security
2. Troubleshooting
3. Industry standards, practices, and network theory
4. Mix questions

Exam A

QUESTION 1
A network technician is assisting the company with developing a new business continuity plan.

Which of the following would be an appropriate suggestion to add to the plan?

A. Build redundant links between core devices
B. Physically secure all network equipment
C. Maintain up-to-date configuration backups
D. Perform reoccurring vulnerability scans

Correct Answer: A
Section: Network security
Explanation

Explanation/Reference:
Explanation:
The business continuity plan focuses on the tasks carried out by an organization to ensure that critical business functions continue to operate during and after a disaster.
By keeping redundant links between core devices critical business services can be kept running if one link is unavailable during a disaster.

QUESTION 2
Which of the following describes a smurf attack?

A. Attack on a target using spoofed ICMP packets to flood it
B. Intercepting traffic intended for a target and redirecting it to another
C. Spoofed VLAN tags used to bypass authentication
D. Forging tags to bypass QoS policies in order to steal bandwidth

Correct Answer: A
Section: Network security
Explanation

Explanation/Reference:
Explanation:
The Smurf Attack is a distributed denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP Broadcast address.
Most devices on a network will, by default, respond to this by sending a reply to the source IP address. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic. This can slow down the victim's computer to the point where it becomes impossible to work on.

QUESTION 3
A malicious user floods a switch with frames hoping to redirect traffic to the user's server.

Which of the following attacks is the user MOST likely using?

A. DNS poisoning
B. ARP poisoning
C. Reflection
D. SYN attack

Correct Answer: B
Section: Network security

Explanation

Explanation/Reference:
Explanation:
Address Resolution Protocol poisoning (ARP poisoning) is a form of attack in which an attacker changes the Media Access Control (MAC) address and attacks an Ethernet LAN by changing the target computer's ARP cache with a forged ARP request and reply packets. This modifies the layer -Ethernet MAC address into the hacker's known MAC address to monitor it. Because the ARP replies are forged, the target computer unintentionally sends the frames to the hacker's computer first instead of sending it to the original destination. As a result, both the user's data and privacy are compromised.

QUESTION 4
An attacker has connected to an unused VoIP phone port to gain unauthorized access to a network.

This is an example of which of the following attacks?

A. Smurf attack
B. VLAN hopping
C. Blue snarfing
D. Spear phishing

Correct Answer: B
Section: Network security
Explanation

Explanation/Reference:
Explanation:
The VoIP phone port can be used to attack a VLAN on the local network.
VLAN hopping is a computer security exploit, a method of attacking networked resources on a Virtual LAN (VLAN). The basic concept behind all VLAN hopping attacks is for an attacking host on a VLAN to gain access to traffic on other VLANs that would normally not be accessible.

QUESTION 5
Packet analysis reveals multiple GET and POST requests from an internal host to a URL without any response from the server.

Which of the following is the BEST explanation that describes this scenario?

A. Compromised system
B. Smurf attack
C. SQL injection attack
D. Man-in-the-middle

Correct Answer: A
Section: Network security
Explanation

Explanation/Reference:
Explanation:
As the extra unexplainable traffic comes from an internal host on your network we can assume that this host has been compromised.
If your system has been compromised, somebody is probably using your machine--possibly to scan and find other machines to compromise

QUESTION 6
A technician needs to ensure that new systems are protected from electronic snooping of Radio Frequency emanations.

Which of the following standards should be consulted?

A. DWDM
B. MIMO
C. TEMPEST
D. DOCSIS

Correct Answer: C
Section: Network security
Explanation

Explanation/Reference:
Explanation:
Tempest was the name of a government project to study the ability to understand the data over a network by listening to the emanations. Tempest rooms are designed to keep emanations contained in that room to increase security of data communications happening there.

QUESTION 7
A company has decided to update their usage policy to allow employees to surf the web unrestricted from their work computers.

Which of the following actions should the IT security team implement to help protect the network from attack as a result of this new policy?

A. Install host-based anti-malware software
B. Implement MAC filtering on all wireless access points
C. Add an implicit deny to the core router ACL
D. Block port 80 outbound on the company firewall
E. Require users to utilize two-factor authentication

Correct Answer: A
Section: Network security
Explanation

Explanation/Reference:
Explanation:
To protect the computers from employees installing malicious software they download on the internet, antimalware should be run on all systems.
After a single machine in a company is compromised and is running malicious software (malware), the attacker can then use that single computer to proceed further into the internal network using the compromised host as a pivot point. The malware may have been implemented by an outside attacker or by an inside disgruntled employee.

QUESTION 8
Which of the following would be the result of a user physically unplugging a VoIP phone and connecting it into another interface with switch port security enabled as the default setting?

A. The VoIP phone would request a new phone number from the unified communications server.
B. The VoIP phone would cause the switch interface, that the user plugged into, to shutdown.
C. The VoIP phone would be able to receive incoming calls but will not be able to make outgoing calls.
D. The VoIP phone would request a different configuration from the unified communications server.

Correct Answer: B
Section: Network security
Explanation

Explanation/Reference:

Explanation:
Without configuring any other specific parameters, the switchport security feature will only permit one MAC address to be learned per switchport (dynamically) and use the shutdown violation mode; this means that if a second MAC address is seen on the switchport the port will be shutdown and put into the err-disabled state.

QUESTION 9
A network technician has been tasked to configure a new network monitoring tool that will examine interface settings throughout various network devices.

Which of the following would need to be configured on each network device to provide that information in a secure manner?

A. S/MIME
B. SYSLOG
C. PGP
D. SNMPv3
E. RSH

Correct Answer: D
Section: Network security
Explanation

Explanation/Reference:
Explanation:
The network monitoring need to use a network management protocol. SNMP has become the de facto standard of network management protocols. The security weaknesses of SNMPv1 and SNMPv2c are addressed in SNMPv3.

QUESTION 10
A firewall ACL is configured as follows:

```
10. Deny Any Trust to Any DMZ eq to TCP port 22
11. Allow 10.200.0.0/16 to Any DMZ eq to Any
12. Allow 10.0.0.0/8 to Any DMZ eq to TCP ports 80, 443
13. Deny Any Trust to Any DMZ eq to Any
```

A technician notices that users in the 10.200.0.0/16 network are unable to SSH into servers in the DMZ. The company wants 10.200.0.0/16 to be able to use any protocol, but restrict the rest of the 10.0.0.0/8 subnet to web browsing only.

Reordering the ACL in which of the following manners would meet the company's objectives?

A. 11, 10, 12, 13
B. 12, 10, 11, 13
C. 13, 10, 12, 11
D. 13, 12, 11, 10

Correct Answer: A
Section: Network security
Explanation

Explanation/Reference:
Explanation:
ACL are processed in TOP DOWN process in routers or switches. This means that when a condition in the ACL is met, all processing is stopped.
We start by allowing any protocol on the 10.200.0.0/16 subnet:11. Allow 10.200.0.0/16 to AnyDMZ eq to Any
We then deny any traffic on TCP port 22:10. Deny Any Trust to Any DMZ eq to TCP port 22
We allow browsing (port 80 and 443) on the 10.0.0.0/8 subnet: Allow 10.0.0.0/8 to Any DMZ eq to TCP ports 80,

443
Finally, we deny all other traffic:13. Deny Any Trust to Any DMZ eq to Any

QUESTION 11
A technician is installing a surveillance system for a home network. The technician is unsure which ports need to be opened to allow remote access to the system.

Which of the following should the technician perform?

A. Disable the network based firewall
B. Implicit deny all traffic on network
C. Configure a VLAN on Layer 2 switch
D. Add the system to the DMZ

Correct Answer: D
Section: Network security
Explanation

Explanation/Reference:
Explanation:
By putting the system in the DMZ (demilitarized zone) we increase the security, as the system should be opened for remote access.
A DMZ is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data. A DMZ often contains servers that should be accessible from the public Internet.

QUESTION 12
The ability to make access decisions based on an examination of Windows registry settings, antivirus software, and AD membership status is an example of which of the following NAC features?

A. Quarantine network
B. Persistent agents
C. Posture assessment
D. Non-persistent agents

Correct Answer: C
Section: Network security
Explanation

Explanation/Reference:
Explanation:
Network Admission Control (NAC) can permit or deny access to a network based on characteristics of the device seeking admission, rather than just checking user credentials. For example, a client's OS, Windows Registry settings, AD membership status, and version of antivirus software could be checked against a set of requirements before allowing the client to access a network.
This process of checking a client's characteristics is called posture assessment.

QUESTION 13
Which of the following types of network would be set up in an office so that customers could access the Internet but not be given access to internal resources such as printers and servers?

A. Quarantine network
B. Core network
C. Guest network
D. Wireless network

Correct Answer: C

Section: Network security
Explanation

Explanation/Reference:
Explanation:
A wireless guest network could be set up so that it has limited access (no access to local resources) but does provide Internet access for guest users.

QUESTION 14
Which of the following is a security benefit gained from setting up a guest wireless network?

A. Optimized device bandwidth
B. Isolated corporate resources
C. Smaller ACL changes
D. Reduced password resets

Correct Answer: B
Section: Network security
Explanation

Explanation/Reference:
Explanation:
A wireless guest network could be set up so that it has limited access (no access to local resources) but does provide Internet access for guest users. The corporate resources would be inaccessible (isolated) from the guest network.

QUESTION 15
Ann, a network technician, was asked to remove a virus. Issues were found several levels deep within the directory structure. To ensure the virus has not infected the .mp4 files in the directory, she views one of the files and believes it contains illegal material.

Which of the following forensics actions should Ann perform?

A. Erase the files created by the virus
B. Stop and escalate to the proper authorities
C. Check the remaining directories for more .mp4 files
D. Copy the information to a network drive to preserve the evidence

Correct Answer: B
Section: Network security
Explanation

Explanation/Reference:
Explanation:
Computer forensics is about legal evidence found in computers and digital storage.
A plan should include first responders securing the area and then escalating to senior management and authorities when required by policy or law.

QUESTION 16
A network technician was tasked to respond to a compromised workstation. The technician documented the scene, took the machine offline, and left the PC under a cubicle overnight.

Which of the following steps of incident handling has been incorrectly performed?

A. Document the scene
B. Forensics report
C. Evidence collection

D. Chain of custody

Correct Answer: D
Section: Network security
Explanation

Explanation/Reference:
Explanation:
To verify the integrity of data since a security incident occurred, you need to be able to show a chain of custody. A chain of custody documents who has been in possession of the data (evidence) since a security breach occurred. A well-prepared organization will have process and procedures that are used when an incident occurs.
A plan should include first responders securing the area and then escalating to senior management and authorities when required by policy or law. The chain of custody also includes documentation of the scene, collection of evidence, and maintenance, e-discovery (which is the electronic aspect of identifying, collecting, and producing electronically stored information), transportation of data, forensics reporting, and a process to preserve all forms of evidence and data when litigation is expected. The preservation of the evidence, data, and details is referred to as legal hold.

QUESTION 17
A network technician is using a network monitoring system and notices that every device on a particular segment has lost connectivity.

Which of the following should the network technician do NEXT?

A. Establish a theory of probable cause.
B. Document actions and findings.
C. Determine next steps to solve the problem.
D. Determine if anything has changed.

Correct Answer: D
Section: Troubleshooting
Explanation

Explanation/Reference:
Explanation:
The technician has already identified the symptom: Loss of connectivity on a specific network segment. The next step in identifying the problem is to “Determine if anything has changed”.
Common troubleshooting steps and procedures:
1. Identify the problem.
- Information gathering.
- Identify symptoms.
- Question users.
- Determine if anything has changed.

1. Establish a theory of probable cause.
- Question the obvious.

1. Test the theory to determine cause:
- When the theory is confirmed, determine the next steps to resolve the problem.
- If theory is not confirmed, re-establish a new theory or escalate.

1. Establish a plan of action to resolve the problem and identify potential effects.
2. Implement the solution or escalate as necessary.
3. Verify full system functionality and if applicable implement preventive measures.
4. Document findings, actions, and outcomes.

QUESTION 18
A user calls the help desk and states that he was working on a spreadsheet and was unable to print it. However, his colleagues are able to print their documents to the same shared printer.

Which of the following should be the FIRST question the helpdesk asks?

A. Does the printer have toner?
B. Are there any errors on the printer display?
C. Is the user able to access any network resources?
D. Is the printer powered up?

Correct Answer: C
Section: Troubleshooting
Explanation

Explanation/Reference:
Explanation:
The user has already provided you with the information relevant to the first step in the 7-step troubleshooting process. The next step is to "Question the obvious." The user has stated: "…his colleagues are able to print their documents to the same shared printer." The obvious question in this instance is whether the user can access any network resources.
1. Identify the problem.
- Information gathering.
- Identify symptoms.
- Question users.
- Determine if anything has changed.

1. Establish a theory of probable cause.
- Question the obvious.

1. Test the theory to determine cause:
- When the theory is confirmed, determine the next steps to resolve the problem.
- If theory is not confirmed, re-establish a new theory or escalate.

1. Establish a plan of action to resolve the problem and identify potential effects.
2. Implement the solution or escalate as necessary.
3. Verify full system functionality and if applicable implement preventive measures.
4. Document findings, actions, and outcomes.

QUESTION 19
A network technician has detected duplicate IP addresses on the network. After testing the behavior of rogue DHCP servers, the technician believes that the issue is related to an unauthorized home router.

Which of the following should the technician do NEXT in the troubleshooting methodology?

A. Document the findings and action taken.
B. Establish a plan to locate the rogue DHCP server.
C. Remove the rogue DHCP server from the network.
D. Identify the root cause of the problem.

Correct Answer: B
Section: Troubleshooting
Explanation

Explanation/Reference:
Explanation:
By testing the behavior of rogue DHCP servers and determining that the issue is related to an unauthorized home router, the technician has completed the third step in the 7-step troubleshooting process. The next step is to establish a plan of action to resolve the problem and identify potential effects. Establishing a plan to locate the rogue DHCP server meets the requirements of this step.
1. Identify the problem.
- Information gathering.
- Identify symptoms.
- Question users.
- Determine if anything has changed.

1. Establish a theory of probable cause.

- Question the obvious.

1. Test the theory to determine cause:

- When the theory is confirmed, determine the next steps to resolve the problem.
- If theory is not confirmed, re-establish a new theory or escalate.

1. Establish a plan of action to resolve the problem and identify potential effects.
2. Implement the solution or escalate as necessary.
3. Verify full system functionality and if applicable implement preventive measures.
4. Document findings, actions, and outcomes.

QUESTION 20
A technician is troubleshooting a client's connection to a wireless network. The client is asked to run a "getinfo" command to list information about the existing condition.

```
myClient$ wificard --getinfo
agrCtlRSSI:-72
agrExtRSSI:0
state:running
op mode: station
lastTxRate:178
MaxRate:300
802.11 auth:open
link auth:wpa2-psk
BSSID:0F:33:AE:F1:02:0A
SSID:CafeWireless
Channel:149,1
```

Given this output, which of the following has the technician learned about the wireless network? (Select TWO).

A. The WAP is using RC4 encryption
B. The WAP is using 802.11a
C. The WAP is using AES encryption
D. The WAP issuing the 2.4GHz channel
E. The WAP is using the 5GHz channel
F. The WAP is using 802.11g

Correct Answer: CE
Section: Troubleshooting
Explanation

Explanation/Reference:
Explanation:
WPA2 makes use of the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) encryption protocol, which is an AES based protocol.
The output shows that the wireless network operates on channel 149, which is a channel in the 5GHz band.

QUESTION 21
An administrator only has telnet access to a remote workstation.

Which of the following utilities will identify if the workstation uses DHCP?

A. tracert
B. ping
C. dig
D. ipconfig
E. netstat

Correct Answer: D
Section: Troubleshooting