Cisco

640-554
Implementing Cisco IOS Network Security

Product Version

Question: 1

Which two features are supported by Cisco IronPort Security Gateway? (Choose two.)

A. Spam protection
B. Outbreak intelligence
C. HTTP and HTTPS scanning
D. Email encryption
E. DDoS protection

Answer: A, D

Explanation:
http://www.cisco.com/en/US/pHYPERLINK "http://www.cisco.com/en/US/prod/collateral/vpndevc/ps10128/ps10154/data-sheet-c78-729751.html#_blank"rod/collateral/vpndevc/ps10128/ps10154/data-sheet-c78-729751.html
Product Overview
Over the past 20 years, email has evolved from a tool used primarily by technical and research professionals to become the backbone of corporate communications. Each day, more than 100 billion corporate email messages are exchanged. As the level of use rises, security becomes a greater priority. Mass spam campaigns are no longer the only concern. Today, spam and malware are just part of a complex picture that includes inbound threats and outbound risks.
Cisco® Email Security solutions defend mission-critical email systems with appliance, virtual, cloud, and hybrid solutions. The industry leader in email security solutions, Cisco delivers:
Fast, comprehensive email protection that can block spam and threats before they even hit your network
Flexible cloud, virtual, and physical deployment options to meet your ever-changing business needs
Outbound message control through on-device data-loss prevention (DLP), email encryption, and optional integration with the RSA enterprise DLP solution
One of the lowest total cost of ownership (TCO) email security solutions available

Question: 2

Which two characteristics represent a blended threat? (Choose two.)

A. man-in-the-middle attack
B. trojan horse attack
C. pharming attack
D. denial of service attack
E. day zero attack

Answer: B, E

Explanation:

http://www.cisco.com/web/IN/about/netwHYPERLINK "http://www.cisco.com/web/IN/about/network/threat_defense.html#_blank"ork/threat_defense.html
Rogue developers create such threats by using worms, viruses, or application-embedded attacks. Botnets can be used to seed an attack, for example, rogue developers can use worms or application-embedded attacks, that is an attack that is hidden within application traffic such as web traffic or peer-to-peer shared files, to deposit "Trojans". This combination of attack techniques - a virus or worm used to deposit a Trojan, for example-is relatively new and is known as a blended attack. A blended attack can also occur in phases: an initial attack of a virus with a Trojan that might open up an unsecured port on a computer, disable an access control list (ACL), or disarm antivirus software, with the goal of a more devastating attack to follow soon after. Host Firewall on servers and desktops/laptops, day zero protection & intelligent behavioral based protection from application vulnerability and related flaws (within or inserted by virus, worms or Trojans) provided great level of confidence on what is happening within an organization on a normal day and when there is a attack situation, which segment and what has gone wrong and gives flexibility and control to stop such situations by having linkages of such devices with monitoring, log-analysis and event co-relation system.

Question: 3

Which two options represent a threat to the physical installation of an enterprise network? (Choose two.)

A. surveillance camera
B. security guards
C. electrical power
D. computer room access
E. change control

Answer: C, D

Explanation:
http://www.cisco.com/E-Learning/bulk/public/celc/CRS/media/targets/1_3_1.swf

Question: 4

Which option represents a step that should be taken when a security policy is developed?

A. Perform penetration testing.
B. Determine device risk scores.
C. Implement a security monitoring system.
D. Perform quantitative risk analysis.

Answer: D

Question: 5

Which type of security control is defense in depth?

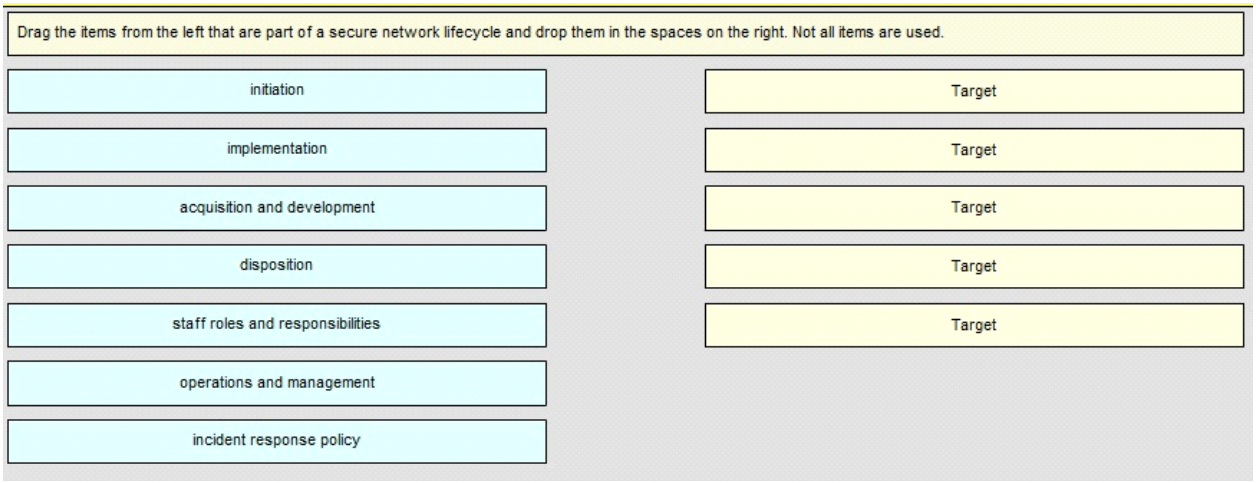
A. threat mitigation
B. risk analysis
C. botnet mitigation
D. overt and covert channels

Answer: A

Explanation:
http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/chap1.html
SAFE Design Blueprint
The Cisco SAFE uses the infrastructure-wide intelligence and collaboration capabilities provided by Cisco products to control and mitigate well-known and zero-day attacks. Under the Cisco SAFE design blueprints, intrusion protection systems, firewalls, network admission control, endpoint protection software, and monitoring and analysis systems work together to identify and dynamically respond to attacks. As part of threat control and containment, the designs have the ability to identify the source of a threat, visualize its attack path, and to suggest, and even dynamically enforce, response actions. Possible response actions include the isolation of compromised systems, rate limiting, packet filtering, and more.
Control is improved through the actions of harden, isolate, and enforce. Following are some of the objectives of the Cisco SAFE design blueprints:
•Adaptive response to real-time threats—Source threats are dynamically identified and may be blocked in realtime.
•Consistent policy enforcement coverage—Mitigation and containment actions may be enforced at different places in the network for defense in-depth.
•Minimize effects of attack—Response actions may be dynamically triggered as soon as an attack is detected, minimizing damage.
•Common policy and security management—A common policy and security management platform simplifies control and administration, and reduces operational expense.

Question: 6

DRAG DROP



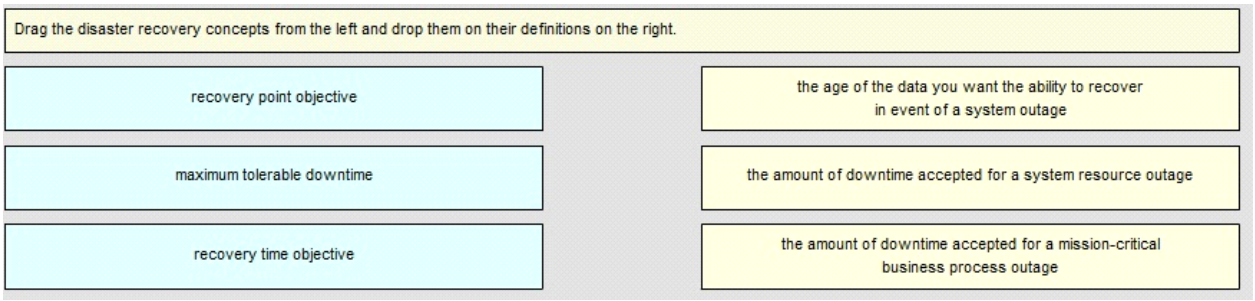
Answer:

1. Initiation
2. Acquisition and development
3. Implementation
4. Operations and maintenance
5. Disposition

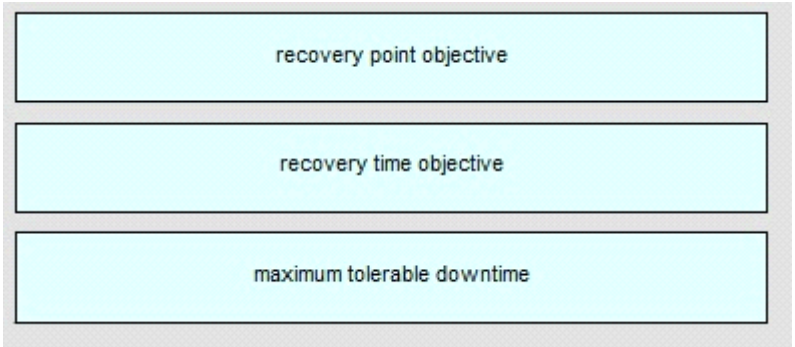
Explanation:
Secure Network Life Cycle
By framing security within the context of IT governance, compliance, and risk management, and by building it with a sound security architecture at its core, the result is usually a less expensive and more effective process. Including security early in the information process within the system design life cycle (SDLC) usually results in less-expensive and more-effective security when compared to adding it to an operational system.
A general SDLC includes five phases:
1. Initiation
2. Acquisition and development
3. Implementation
4. Operations and maintenance
5. Disposition
Each of these five phases includes a minimum set of security steps that you need to follow to effectively incorporate security into a system during its development. An organization either uses the general SDLC or develops a tailored SDLC that meets its specific needs. In either case, the National Institute of Standards and Technology (NIST) recommends that organizations incorporate the associated IT security steps of this general SDLC into their development process.

Question: 7

DRAG DROP



Answer:



Question: 8

Which four methods are used by hackers? (Choose four.)

A. footprint analysis attack
B. privilege escalation attack
C. buffer Unicode attack
D. front door attacks
E. social engineering attack
F. Trojan horse attack

Answer: A, B, E, F

Explanation:
https://learningnetwork.cisco.com/servlet/JiveServlet/download/15823-1-57665/CCNA%20Security%20(640-554)%20Portable%20Command%20Guide_ch01.pdf
Thinking Like a Hacker
The following seven steps may be taken to compromise targets and applications:
Step 1 Perform footprint analysis
Hackers generally try to build a complete profile of a target company's security posture using a broad range of easily available tools and techniques. They can discover organizational domain names, network blocks, IP addresses of systems, ports, services that are used, and more.
Step 2 Enumerate applications and operating systems
Special readily available tools are used to discover additional target information. Ping sweeps use Internet Control Message Protocol (ICMP) to discover devices on a network. Port scans discover TCP/UDP port status.
Other tools include Netcat, Microsoft EPDump and Remote Procedure Call (RPC) Dump, GetMAC, and software development kits (SDKs).
Step 3 Manipulate users to gain access
Social engineering techniques may be used to manipulate target employees to acquire passwords. They may call or email them and try to convince them to reveal passwords without raising any concern or suspicion.
Step 4 Escalate privileges
To escalate their privileges, a hacker may attempt to use Trojan horse programs and get target users to unknowingly copy malicious code to their corporate system.
Step 5 Gather additional passwords and secrets
With escalated privileges, hackers may use tools such as the pwdump and LSADump applications to gather passwords from machines running Windows.
Step 6 Install back doors
Hacker may attempt to enter through the "front door," or they may use "back doors" into the system. The backdoor method means bypassing normal authentication while attempting to remain undetected. A common backdoor point is a listening port that provides remote access to the system.
Step 7 Leverage the compromised system
After hackers gain administrative access, they attempt to hack other systems.

Question: 9

Which characteristic is the foundation of Cisco Self-Defending Network technology?

A. secure connectivity
B. threat control and containment
C. policy management

D. secure network platform

Answer: D

Explanation:
http://www.cisco.com/en/US/solutions/ns170/networking_solutions_products_genericcontent0900aecd8051HYPERLINK "http://www.cisco.com/en/US/solutions/ns170/networking_solutions_products_genericcontent0900aecd8051f378.html#_blank"f378.html
Create a Stronger Defense Against Threats
Each day, you reinvent how you conduct business by adopting Internet-based business models. But Internet connectivity without appropriate security can compromise the gains you hope to make. In today's connected environment, outbreaks spread globally in a matter of minutes, which means your security systems must react instantly.
Maintaining security using tactical, point solutions introduces complexity and inconsistency, but integrating security throughout the network protects the information that resides on it.
Three components are critical to effective information security:
• A secure network platform with integrated security to which you can easily add advanced security technologies and services
• Threat control services focused on antivirus protection and policy enforcement that continuously monitor network activity and prevent or mitigate problems
• Secure communication services that maintain the privacy and confidentiality of sensitive data, voice, video, and wireless communications while cost-effectively extending the reach of your network

Question: 10

In a brute-force attack, what percentage of the keyspace must an attacker generally search through until he or she finds the key that decrypts the data?

A. Roughly 50 percent
B. Roughly 66 percent
C. Roughly 75 percent
D. Roughly 10 percent

Answer: A

Question: 11

Which three items are Cisco best-practice recommendations for securing a network? (Choose three.)

A. Routinely apply patches to operating systems and applications.
B. Disable unneeded services and ports on hosts.
C. Deploy HIPS software on all end-user workstations.
D. Require strong passwords, and enable password expiration.

Answer: A, B, D

Question: 12

What Cisco Security Agent Interceptor is in charge of intercepting all read/write requests to the rc files in UNIX?

A. Configuration interceptor
B. Network interceptor
C. File system interceptor
D. Execution space interceptor

Answer: A

Explanation
Configuration interceptor: Read/write requests to the Registry in Windows or to rc configuration files on UNIX are intercepted. This interception occurs because modification of the operating system configuration can have serious consequences. Therefore, Cisco Security Agent tightly controls read/write requests to the Registry.

Question: 13

Information about a managed device's resources and activity is defined by a series of objects. What defines the structure of these management objects?

A. MIB
B. FIB
C. LDAP
D. CEF

Answer: A

Explanation
Management Information Base (MIB) is the database of configuration variables that resides on the networking device.

Question: 14

Which statement is true about vishing?

A. Influencing users to forward a call to a toll number (for example, a long distance or international number)
B. Influencing users to provide personal information over a web page
C. Using an inside facilitator to intentionally forward a call to a toll number (for example, a long distance or international number)
D. Influencing users to provide personal information over the phone

Answer: D

Explanation:
Vishing (voice phishing) uses telephony to glean information, such as account details, directly from users. Because many users tend to trust the security of a telephone versus the security of the web, some users are more likely to provide confidential information over the telephone. User education is the most effective method to combat vishing attacks.

Question: 15

Which item is the great majority of software vulnerabilities that have been discovered?

A. Stack vulnerabilities
B. Heap overflows
C. Software overflows
D. Buffer overflows

Answer: D

Thank You for Trying Our Product

For More Information – Visit link below:

http://www.examsboost.com/

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer

WE ACCEPT

PayPal