[Updated Constantly]

HERE

CCNA Security v2.0 Chapter 1 Exam Answers

How to find: Press “Ctrl + F” in the browser and fill in whatever wording is in the question to find that question/answer.

NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.

1. **What method can be used to mitigate ping sweeps?**
   - using encrypted or hashed authentication protocols
   - installing antivirus software on hosts
   - deploying antisniffer software on all network devices
   - **blocking ICMP echo and echo-replies at the network edge***

   A computer can have a worm installed through an email attachment, an executable program file, or a Trojan Horse. The worm attack not only affects one computer, but replicates to other computers. What the worm leaves behind is the payload–the code that results in some action.

2. **What are the three major components of a worm attack? (Choose three.)**
   - a penetration mechanism
   - an infecting vulnerability
   - **a payload***
   - **an enabling vulnerability***
   - a probing mechanism
   - **a propagation mechanism***
3. **Which statement accurately characterizes the evolution of threats to network security?**
   - **Internal threats can cause even greater damage than external threats.***
   - Threats have become less sophisticated while the technical knowledge needed by an attacker has grown.
   - Early Internet users often engaged in activities that would harm other users.
   - Internet architects planned for network security from the beginning.

   Internal threats can be intentional or accidental and cause greater damage than external threats because the internal user has direct access to the internal corporate network and corporate data.

4. **What causes a buffer overflow?**

- launching a security countermeasure to mitigate a Trojan horse
- sending repeated connections such as Telnet to a particular device, thus denying other data sources.
- downloading and installing too many software updates at one time
- **attempting to write more data to a memory location than that location can hold***
- sending too much information to two or more interfaces of the same device, thereby causing dropped packets

By sending too much data to a specific area of memory, adjacent memory locations are overwritten, which causes a security issue because the program in the overwritten memory location is affected.

5. **What commonly motivates cybercriminals to attack networks as compared to hactivists or state-sponsored hackers?**
   - status among peers
   - fame seeking
   - **financial gain***
   - political reasons

   Cybercriminals are commonly motivated by money. Hackers are known to hack for status. Cyberterrorists are motivated to commit cybercrimes for religious or political reasons.

6. **Which two network security solutions can be used to mitigate DoS attacks? (Choose two.)**
   - virus scanning
   - **intrusion protection systems***
   - applying user authentication
   - **antispoofing technologies***
   - data encryption

   Antivirus software is used to protect a system against viruses. Encryption helps with reconnaissance and man-in-the-middle attacks. The most important components that are used to deal with DoS attacks are firewalls and IPSes.

7. **Which two statements characterize DoS attacks? (Choose two.)**
   - **Examples include smurf attacks and ping of death attacks.***
   - **They attempt to compromise the availability of a network, host, or application***
   - They are difficult to conduct and are initiated only by very skilled attackers.
   - They are commonly launched with a tool called L0phtCrack.
   - They always precede access attacks.

DoS attacks can be launched using free software downloaded from the Internet. The software is designed to consume resources in order to disrupt network operations for legitimate network users and network devices. The L0phtCrack or LC5 application is used to perform a brute-force attack to obtain a Windows server password.

8. **An attacker is using a laptop as a rogue access point to capture all network traffic from a targeted user. Which type of attack is this?**
   - trust exploitation
   - buffer overflow
   - **man in the middle***
   - port redirection

   An access attack tries to gain access to a resource using a hijacked account or other means. The five types of access attacks include the following:
   password – a dictionary is used for repeated login attempts
   trust exploitation – uses granted privileges to access unauthorized material
   port redirection – uses a compromised internal host to pass traffic through a firewall
   man-in-the-middle – an unauthorized device positioned between two legitimate devices in order to redirect or capture traffic
   buffer overflow – too much data sent to a memory location that already contains data

9. **What functional area of the Cisco Network Foundation Protection framework is responsible for device-generated packets required for network operation, such as ARP message exchanges and routing advertisements?**
   - data plane
   - **control plane***
   - management plane
   - forwarding plane

   There are three functional areas of the Cisco Network Foundation Protection (NFP) framework:
   Control plane: Responsible for routing functions. Consists of the traffic generated by network devices to operate the network.
   Management plane: Responsible for managing network devices.
   Data (Forwarding) plane: Responsible for forwarding user data.

10. **What are the three components of information security ensured by cryptography? (Choose three.)**
    - threat prevention

- authorization
- **confidentiality***
- countermeasures
- **integrity***
- **availability***

There are three components of information security that are ensured by cryptography:
Confidentiality, which uses encryption algorithms to encrypt and hide data
Integrity, which uses hashing algorithms to ensure that data arrives at the destination unaltered
Availability, which ensures that data is accessible

11. **What is the primary method for mitigating malware?**
    - using encrypted or hashed authentication protocols
    - **installing antivirus software on all hosts***
    - blocking ICMP echo and echo-replies at the network edge
    - deploying intrusion prevention systems throughout the network

Antivirus software installed on hosts is the most effective mitigation method to prevent the spread of malware. Automatic updates to antivirus software ensure that hosts are protected from the most current forms of malware

12. **What is an objective of a state-sponsored attack?**
    - to gain financial prosperity
    - to sell operation system vulnerabilities to other hackers
    - to gain attention
    - **to right a perceived wrong***
    - Spy on citizens, disrupt foreign government

State-sponsored attacks are government-funded and guided operations motivated by objectives of the government.

13. **What role does the Security Intelligence Operations (SIO) play in the Cisco SecureX architecture?**
    - **identifying and stopping malicious traffic***
    - authenticating users
    - enforcing policy
    - identifying applications

Security Intelligence Operations (SIO) are able to distinguish legitimate traffic from malicious traffic. SIO uses a monitoring database for the sole purpose of identifying and stopping malicious traffic.

14. **What worm mitigation phase involves actively disinfecting infected systems?**
    - **Treatment***
    - containment
    - inoculation
    - quarantine
15. **How is a smurf attack conducted?**
    - by sending a large number of packets to overflow the allocated buffer memory of the target device
    - **by sending a large number of ICMP requests to directed broadcast addresses from a spoofed source address on the same network***
    - by sending a large number of TCP SYN packets to a target device from a spoofed source address
    - by sending an echo request in an IP packet larger than the maximum packet size of 65,535 bytes
16. **What is a characteristic of a Trojan horse as it relates to network security?**
    - **Malware is contained in a seemingly legitimate executable program.***
    - Extreme quantities of data are sent to a particular network device interface.
    - An electronic dictionary is used to obtain a password to be used to infiltrate a key network device.
    - Too much information is destined for a particular memory block causing additional memory areas to be affected.

A Trojan horse carries out malicious operations under the guise of a legitimate program. Denial of service attacks send extreme quantities of data to a particular host or network device interface. Password attacks use electronic dictionaries in an attempt to learn passwords. Buffer overflow attacks exploit memory buffers by sending too much information to a host to render the system inoperable.

17. **What is the first step in the risk management process specified by the ISO/IEC?**
    - Create a security policy.
    - **Conduct a risk assessment.***
    - Inventory and classify IT assets.
    - Create a security governance model.

There are 12 network security domains in the security framework specified by the ISO/IEC. The first task in this framework is to conduct a risk assessment.This assessment will enable an organization to quantify risks and threats.

18. **What is the significant characteristic of worm malware?**
    - **A worm can execute independently of the host system.***
    - A worm must be triggered by an event on the host system.
    - Worm malware disguises itself as legitimate software
    - Once installed on a host system, a worm does not replicate itself.

Worm malware can execute and copy itself without being triggered by a host program. It is a significant network and Internet security threat.

19. **Which condition describes the potential threat created by Instant On in a data center?**
    - when the primary firewall in the data center crashes
    - when an attacker hijacks a VM hypervisor and then launches attacks against other devices in the data center
    - when the primary IPS appliance is malfunctioning
    - **when a VM that may have outdated security policies is brought online after a long period of inactivity.***

The phrase Instant On describes a potential threat to a VM when it is brought online after it has not been used for a period of time. Because it is offline for a while, it may have outdated security policies that deviate from the baseline security and can introduce security vulnerabilities.

20. **What are the three core components of the Cisco Secure Data Center solution? (Choose three.)**
    - mesh network
    - **secure segmentation***
    - **visibility***
    - **threat defense***
    - servers
    - infrastructure

Secure segmentation is used when managing and organizing data in a data center. Threat defense includes a firewall and intrusion prevention system (IPS). Data center visibility is designed to simplify operations and compliance reporting by providing consistent security policy enforcement.

21. **A disgruntled employee is using Wireshark to discover administrative Telnet usernames and passwords. What type of network attack does this describe?**
    - trust exploitation
    - denial of service
    - **reconnaissance***
    - port redirection

    Wireshark is a free download that allows network packet inspection. Someone using this tool for malicious intent would be performing a reconnaissance attack. Through the capture of network packets, weak security network connectivity protocols such as Telnet can be caught, inspected, and then analyzed for detailed network information, including passwords.

22. **What is the role of an IPS?**
    - connecting global threat information to Cisco network security devices
    - authenticating and validating traffic
    - **detecting and blocking of attacks in real time***
    - filtering of nefarious websites

    An intrusion prevention system (IPS) provides real-time detection and blocking of attacks.

23. **Which two statements describe access attacks? (Choose two.)**
    - Trust exploitation attacks often involve the use of a laptop to act as a rogue access point to capture and copy all network traffic in a public location, such as a wireless hotspot.
    - To detect listening services, port scanning attacks scan a range of TCP or UDP port numbers on a host
    - **Buffer overflow attacks write data beyond the hallocated buffer memory to overwrite valid data or to exploit systems to execute malicious code.***
    - **Password attacks can be implemented by the use os brute-force attack methods, Trojan horse, or packet sniffers.***
    - Port redirection attacks use a network adapter card in promiscuous mode to capture all network packets that are sent across a LAN.

    An access attack tries to gain access to a resource using a hijacked account or other means. The five types of access attacks include the following:
    password – a dictionary is used for repeated login attempts
    trust exploitation – uses granted privileges to access unauthorized material
    port redirection – uses a compromised internal host to pass traffic through a firewall
    man-in-the-middle – an unauthorized device positioned between two legitimate devices in order to redirect or capture traffic
    buffer overflow – too much data sent to a memory location that already contains data

24. **What is a ping sweep?**

- a scanning technique that examines a range of TCP or UDP port numbers on a host to detect listening services.
- a software application that enables the capture of all network packets that are sent across a LAN.
- a query and response protocol that identifies information about a domain, including the addresses that are assigned to that domain
- **a network scanning technique that indicates the live hosts in a range of IP addresses.**

A ping sweep is a tool that is used during a reconnaissance attack. Other tools that might be used during this type of attack include a ping sweep, port scan, or Internet information query. A reconnaissance attack is used to gather information about a particular network, usually in preparation for another type of network attack.

25. **Fill in the blank.**

As a dedicated network security tool, an intrusion **Prevention** system can provide detection and blocking of attacks in real time.