CCNA Cyber Ops (Version 1.1) – Chapter 6 Exam Answers Full

itexamanswers.net/ccna-cyber-ops-chapter-6-exam-answers-full.html

May 13, 2019

How to find: Press **"Ctrl + F"** in the browser and fill in whatever wording is in the question to find that question/answer. If the question is not here, find it in **Questions Bank**.

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 type of attack uses zombies?

- Trojan horse
- SEO poisoning
- Spear phishing
- **DDoS ***

D. The hacker infects multiple machines (zombies), creating a botnet. Zombies launch the distributed denial-of-service (DDoS) attack.

2. What is the best description of Trojan horse malware?

- It is the most easily detected form of malware.
- **It appears as useful software but hides malicious code. ***
- It is malware that can only be distributed over the Internet.
- It is software that causes annoying but not fatal computer problems.

B. The best description of Trojan horse malware, and what distinguishes it from viruses and worms, is that it appears as useful software but hides malicious code. Trojan horse malware may cause annoying computer problems, but can also cause fatal problems. Some Trojan horses may be distributed over the Internet, but they can also be distributed by USB memory sticks and other means. Specifically targeted Trojan horse malware can be some of the most difficult malware to detect.

3. What is the purpose of a rootkit?

- To masquerade as a legitimate program
- To deliver advertisements without user consent
- To replicate itself independently of any other programs

- **To gain privileged access to a device while concealing itself ***

Explanation: Most rootkits take advantage of software vulnerabilities to gain access to resources that normally shouldn’t be accessible (privilege escalation) and modify system files.

4. When describing malware, what is a difference between a virus and a worm?

- A virus focuses on gaining privileged access to a device, whereas a worm does not.
- **A virus replicates itself by attaching to another file, whereas a worm can replicate itself independently. ***
- A virus can be used to launch a DoS attack (but not a DDoS), but a worm can be used to launch both DoS and DDoS attacks.
- A virus can be used to deliver advertisements without user consent, whereas a worm cannot.

B. Malware can be classified as follows:
Virus (self-replicates by attaching to another program or file)
Worm (replicates independently of another program)
Trojan horse (masquerades as a legitimate file or program)
Rootkit (gains privileged access to a machine while concealing itself)
Spyware (collects information from a target system)
Adware (delivers advertisements with or without consent)
Bot (waits for commands from the hacker)
Ransomware (holds a computer system or data captive until payment isreceived)

5. What is an example of “hacktivism”?

- Criminals use the Internet to attempt to steal money from a banking company.
- A country tries to steal defense secrets from another country by infiltrating government networks.
- A teenager breaks into the web server of a local newspaper and posts a picture of a favorite cartoon character.
- **A group of environmentalists launch a denial-of-service attack against an oil company that is responsible for a large oil spill. ***

D. Hacktivism is a term used to describe cyberattacks carried out by people who are considered political or ideological extremists. Hacktivists attack people or organizations that they believe are enemies to the hacktivist agenda.

6. What is the purpose of a reconnaissance attack on a computer network?

- To steal data from the network servers
- To prevent users from accessing network resources
- To redirect data traffic so that it can be monitored

- **To gather information about the target network and system** *

Preventing users from accessing network resources is a denial of service attack. Being able to steal data from the network servers may be the objective after a reconnaissance attack gathers information about the target network and system. Redirecting data traffic so it can be monitored is a man-in-the middle attack.

7. Which tool is used to provide a list of open ports on network devices?

- **Nmap** *
- Ping
- Whois
- Tracert

A. The Nmap tool is a port scanner that is used to determine which ports are open on a particular network device. A port scanner is used before launching an attack.

8. Which type of attack allows an attacker to use a brute-force approach?

- Packet sniffing
- Social engineering
- Denial of service
- **Password cracking** *

D. Common ways used to crack Wi-Fi passwords include social engineering, brute-force attacks, and network sniffing.

9. Which term is used to describe the act of sending an email message in an attempt to divulge sensitive information from someone?

- **Phishing** *
- DoS attack
- Hacktivisim
- Script kiddie

A. Phishing uses deception to convince people to divulge information. Hactivism is hacking done for a specific cause such as political or social reasons. A script kiddie is an inexperienced hacker who uses free scripts, software, and tools. A denial-of-service (DoS) attack causes one or more services to be inaccessible or not work.

10. What is the significant characteristic of worm malware?

- **A worm can execute independently of the host system.** *
- Worm malware disguises itself as legitimate software.
- A worm must be triggered by an event on the host system.

- Once installed on a host system, a worm does not replicate itself.

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

11. A network administrator detects unknown sessions involving port 21 on the network. What could be causing this security breach?

- **An FTP Trojan horse is executing. ***
- A reconnaissance attack is occurring.
- A denial-of-service attack is occurring.
- Cisco Security Agent is testing the network.

A. Network security personnel must be familiar with port numbers in order to identify the service being attacked. Well-known port number 21 is used to initiate an FTP connection to an FTP server. Well-known port 20 is then used to transfer data between the two devices. If the device connecting to the FTP server is unknown and launching an attack, the type of attack might be an FTP Trojan horse.

12. Which example illustrates how malware might be concealed?

- A botnet of zombies carry personal information back to the hacker.
- An attack is launched against the public website of an online retailer with the objective of blocking its response to visitors.
- A hacker uses techniques to improve the ranking of a website so that users are redirected to a malicious site.
- **An email is sent to the employees of an organization with an attachment that looks like an antivirus update, but the attachment actually consists of spyware. ***

D. An email attachment that appears as valid software but actually contains spyware shows how malware might be concealed. An attack to block access to a website is a DoS attack. A hacker uses search engine optimization (SEO) poisoning to improve the ranking of a website so that users are directed to a malicious site that hosts malware or uses social engineering methods to obtain information. A botnet of zombie computers is used to launch a DDoS attack.

13. Which type of security threat can be described as software that attaches itself to another program to execute a specific unwanted function?

- Worm
- **Virus ***
- Proxy Trojan horse
- Denial-of-service Trojan horse

B. Viruses can be malicious and destructive or simply change something about the computer, such as words or images, and not necessarily cause thecomputer to malfunction. Viruses can be spread through shared media such as CDs or memory sticks, but can also be delivered via the Internet and email.

14. What type of malware has the primary objective of spreading across the network?

- virus
- **worm**
- Trojan horse
- botnet

The main purpose of a worm is to self-replicate and propagate across the network. A virus is a type of malicious software that needs a user to spread. A trojan horse is not self-replicating and disguises itself as a legitimate application when it is not. A botnet is a series of zombie computers working together to wage a network attack.

15. Why would a rootkit be used by a hacker?

- **to gain access to a device without being detected**
- to do reconnaissance
- to reverse engineer binary files
- to try to guess a password

Hackers use rootkits to avoid detection as well as hide any software installed by the hacker.

16. Which type of hacker is motivated to protest against political and social issues?

- cybercriminal
- script kiddie
- vulnerability broker
- **hacktivist**

Hackers are categorized by motivating factors. Hacktivists are motivated by protesting political and social issues.

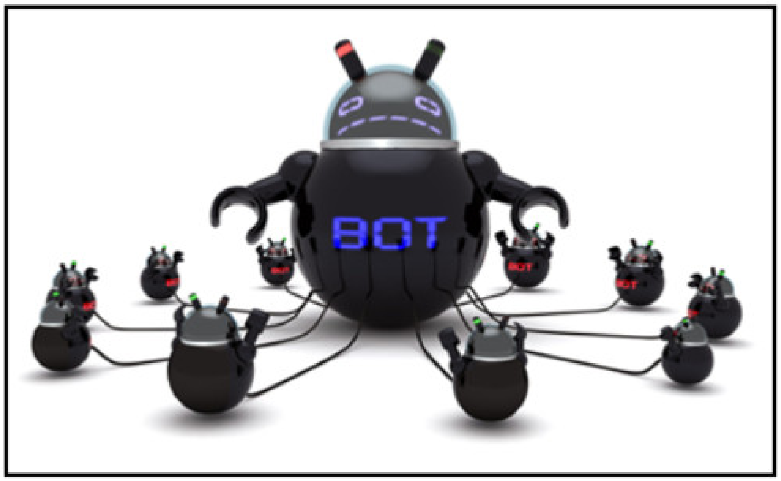
17. What is a characteristic of a Trojan horse as it relates to network security?

- 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.

- **Malware is contained in a seemingly legitimate executable program.**

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.

18. What is a botnet?



- a group of web servers that provide load balancing and fault tolerance
- an online video game intended for multiple players
- a network that allows users to bring their own technology
- **a network of infected computers that are controlled as a group**

One method of executing a DDoS attack involves using a botnet. A botnet builds or purchases a botnet of zombie hosts, which is a group of infected devices. The zombies continue to create more zombies which carry out the DDoS attack.

19. Which type of Trojan horse security breach uses the computer of the victim as the source device to launch other attacks?

- DoS
- FTP
- data-sending
- **proxy**

The attacker uses a proxy Trojan horse attack to penetrate one device and then use that device to launch attacks on other devices. The DoS Trojan horse slows or halts network traffic. The FTP trojan horse enables unauthorized file transfer services when port 21 has been compromised. A data-sending Trojan horse transmits data back to the hacker that could include passwords.

20. What is the primary goal of a DoS attack?

- **to prevent the target server from being able to handle additional requests**
- to scan the data on the target server
- to facilitate access to external networks
- to obtain all addresses in the address book within the server

A denial of service (DoS) attack attempts to overwhelm a system or process by sending large amounts of data or requests to the target. The goal is to keep the system so overwhelmed handling false requests that it is unable to respond to legitimate ones.

21. What is a main purpose of launching an access attack on network systems?

- to prevent other users from accessing the system
- to scan for accessible networks
- to gather information about the network
- **to retrieve data**

Gathering information about a network and scanning for access is a reconnaissance attack. Preventing other users from accessing a system is a denial of service attack.

22. What causes a buffer overflow?

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

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.

23. A company pays a significant sum of money to hackers in order to regain control of an email and data server. Which type of security attack was used by the hackers?

- DoS
- spyware
- Trojan horse
- **ransomware**

Ransomware involves the hackers preventing user access to the infected and controlled system until the user pays a specified amount.

24. What is the term used to describe an email that is targeting a specific person employed at a financial institution?

- spam
- spyware
- vishing
- target phishing
- **spear phishing**

Spear phishing is a phishing attack customized to reach a specific person or target.

25. Which access attack method involves a software program that attempts to discover a system password by the use of an electronic dictionary?

- packet sniffer attack
- denial of service attack
- buffer overflow attack
- **brute-force attack**
- port redirection attack
- IP spoofing attack

An access attack tries to affect services that affect entry into accounts, databases, and other sensitive information. Access attacks commonly involve a dictionary ths is used to guess a specific user password. A brute-force access attack would try to access an account via repeated attempts.

26. In what way are zombies used in security attacks?

- **They are infected machines that carry out a DDoS attack.**
- They are maliciously formed code segments used to replace legitimate applications.
- They target specific individuals to gain corporate or personal information.
- They probe a group of machines for open ports to learn which services are running

Zombies are infected computers that make up a botnet. The zombies are used to deploy a distributed denial of service (DDoS) attack.

27. What are two evasion methods used by hackers? (Choose two.)

- scanning
- **encryption**
- access attack
- phishing

- **resource exhaustion**

The following methods are used by hackers to avoid detection:Encryption and tunneling – hide or scramble the malware content
Resource exhaustion – keep the host device too busy to detect the invasion
Traffic fragmentation – split the malware into multiple packets
Protocol-level misinterpretation – sneak by the firewall
Pivot – use a compromised network device to attempt access to another device
Rootkit – allow the hacker to avoid detection as well as hide software installed by the hacker

28. What are two purposes of launching a reconnaissance attack on a network? (Choose two.)

- to retrieve and modify data
- **to scan for accessibility**
- to escalate access privileges
- to prevent other users from accessing the system
- **to gather information about the network and devices**

Gathering information about a network and scanning for access is a reconnaissance attack. Preventing other users from accessing a system is a denial of service attack. Attempting to retrieve and modify data, and attempting to escalate access privileges are types of access attacks.

29. What are three techniques used in social engineering attacks? (Choose three.)

- **vishing**
- **phishing**
- **pretexting**
- buffer overflow
- man-in-the-middle
- sending junk email

Phishing is an attempt to get a user to divulge information. Vishing is a type of phishing that uses voice and the phone system. With pretexting, the hacker lies to the user in an attempt to obtain information.

30. 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?

- port redirection
- trust exploitation
- buffer overflow

- **man in the middle**

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

31. A user is curious about how someone might know a computer has been infected with malware. What are two common malware behaviors? (Choose two.)

- The computer emits a hissing sound every time the pencil sharpener is used.
- **The computer freezes and requires reboots.**
- No sound emits when an audio CD is played.
- **The computer gets increasingly slower to respond.**
- The computer beeps once during the boot process.

Common symptoms of computers infected with malware:Appearance of files, applications, or desktop icons
Security tools such as antivirus software or firewalls turned off or changed
System crashes
Emails spontaneously sent to others
Modified or missing files
Slow system or browser response
Unfamiliar processes or services running
Unknown TCP or UDP ports open
Connections made to unknown remote devices

32. Which type of security attack would attempt a buffer overflow?

- ransomware
- reconnaissance
- **DoS**
- scareware

Denial of service (DoS) attacks attempt to disrupt service on the network by either sending a particular device an overwhelming amount of data so no other devices can access the attacked device or by sending malformed packets.

33. What is a significant characteristic of virus malware?

- Virus malware is only distributed over the Internet.
- Once installed on a host system, a virus will automatically propagate itself to other systems.
- **A virus is triggered by an event on the host system.**
- A virus can execute independently of the host system

A virus is malicious code that is attached to a legitimate program or executable file, and requires specific activation, which may include user actions or a time-based event. When activated, a virus can infect the files it has not yet infected, but does not automatically propagate itself to other systems. Self-propagation is a feature of worms. In addition to being distributed over the Internet, viruses are also spread by USB memory sticks, CDs, and DVDs.

34. A senior citizen receives a warning on the computer that states that the operating system registry is corrupt and to click a particular link to repair it. Which type of malware is being used to try to create the perception of a computer threat to the user?

- DoS
- **scareware**
- phishing
- adware

Scareware is a type of malware that attempts to shock or induce anxiety by creating a perception of a threat. Phishing tries to get the user to divulge some information. A DoS attack tries to disrupt service on a network. Adware usually appears in pop-ups trying to get the user to buy something or to visit a website.

35. What is the motivation of a white hat attacker?

- fine tuning network devices to improve their performance and efficiency
- taking advantage of any vulnerability for illegal personal gain
- studying operating systems of various platforms to develop a new system
- **discovering weaknesses of networks and systems to improve the security level of these systems**

White hat attackers break into networks or computer systems in order to discover weaknesses for the purpose of improving the security of these systems. These break-ins are done with permission from the owner or the organization. Any results are reported back to the owner or the organization.

36. What is a ping sweep?

- **a network scanning technique that indicates the live hosts in a range of IP addresses.**

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

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.

37. What is the term used when a malicious party sends a fraudulent email disguised as being from a legitimate, trusted source?

- Trojan
- vishing
- **phishing**
- backdoor

Phishing is used by malicious parties who create fraudulent messages that attempt to trick a user into either sharing sensitive information or installing malware.

38. What are the three major components of a worm attack? (Choose three.)

- **an enabling vulnerability**
- **a propagation mechanism**
- **a payload**
- a probing mechanism
- a penetration mechanism
- an infecting vulnerability

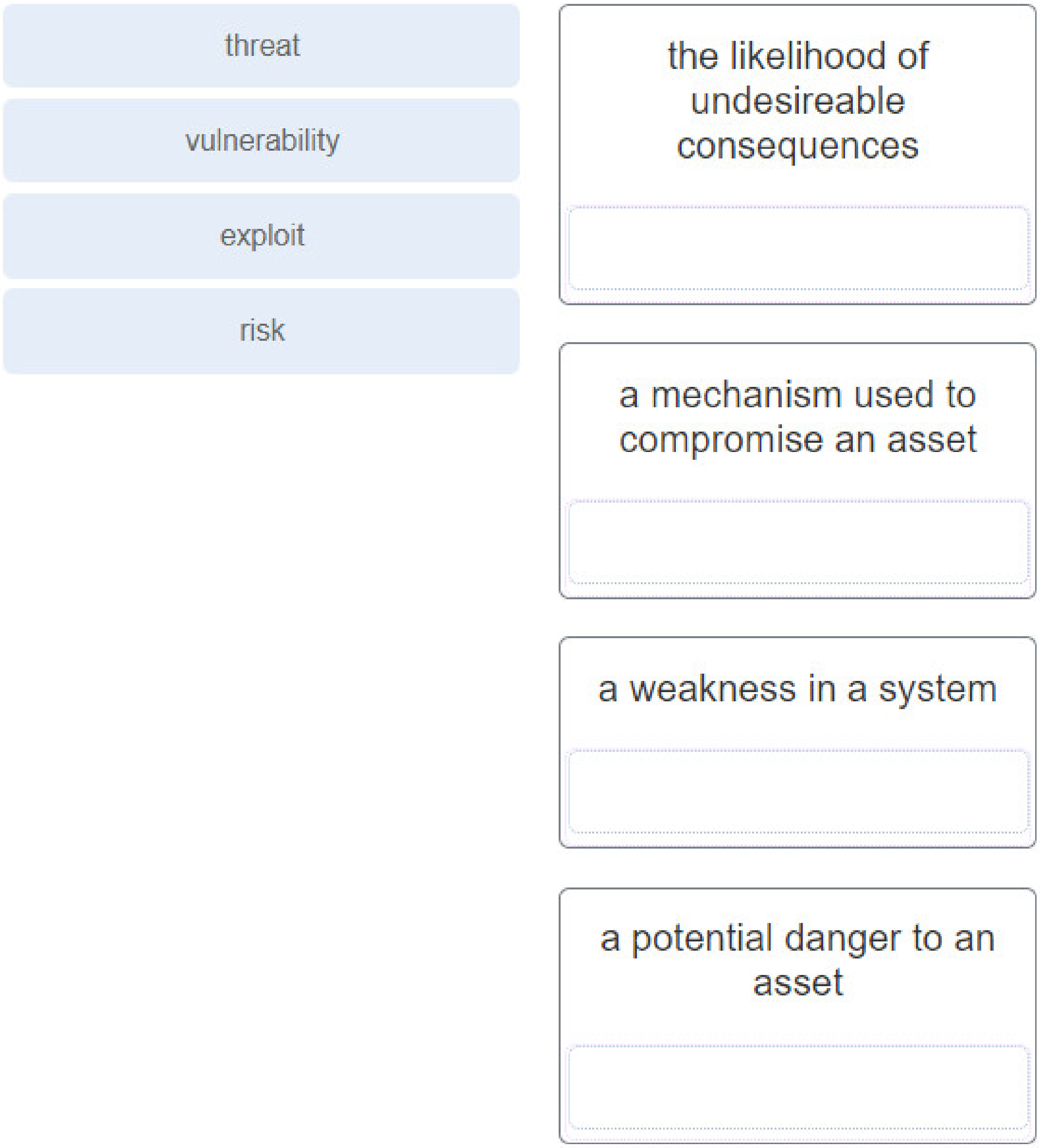
A computer can have a worm installed through an email attachment, an executable program file, or a Trojan Horse. The worm attack not only affects one computer, but replicates to other computers. What the worm leaves behind is the payload–the code that results in some action.

39. Which security threat installs on a computer without the knowledge of the user and then monitors computer activity?

- **spyware**
- viruses
- worms
- adware

Spyware normally installs on a system without end-user knowledge and monitors activity on a computer, which can then be sent to the source of spyware. Viruses infect systems and execute malicious code. Worms self-replicate and propagate across networks from a singular host, consuming a lot of bandwidth. Adware is normally distributed through downloaded software and results in the exhibition of several pop-up windows on the system.

40. Match the security concept to the description.



threat

vulnerability

exploit

risk

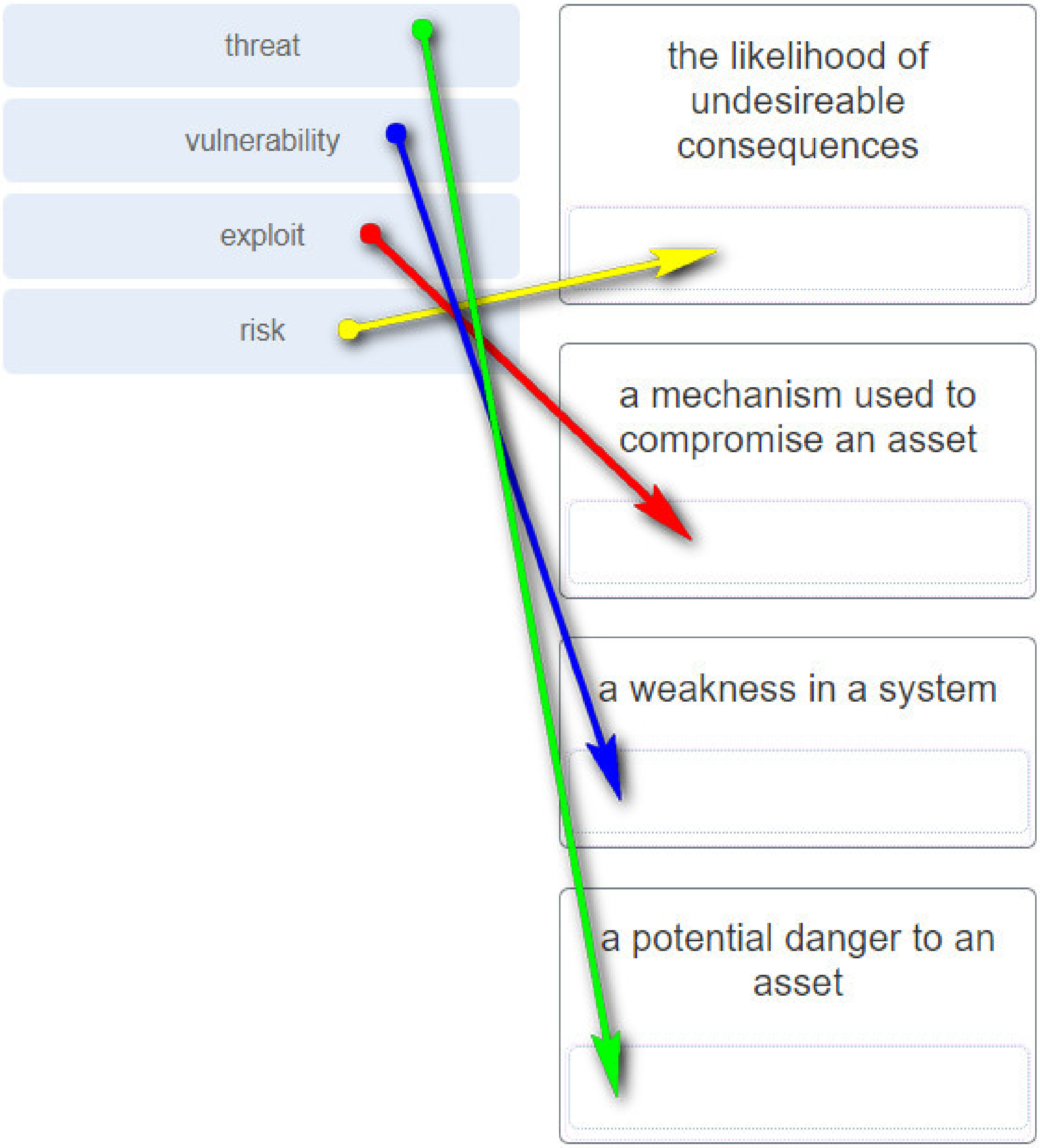
the likelihood of undesireable consequences

a mechanism used to compromise an asset

a weakness in a system

a potential danger to an asset

Answer



threat

vulnerability

exploit

risk

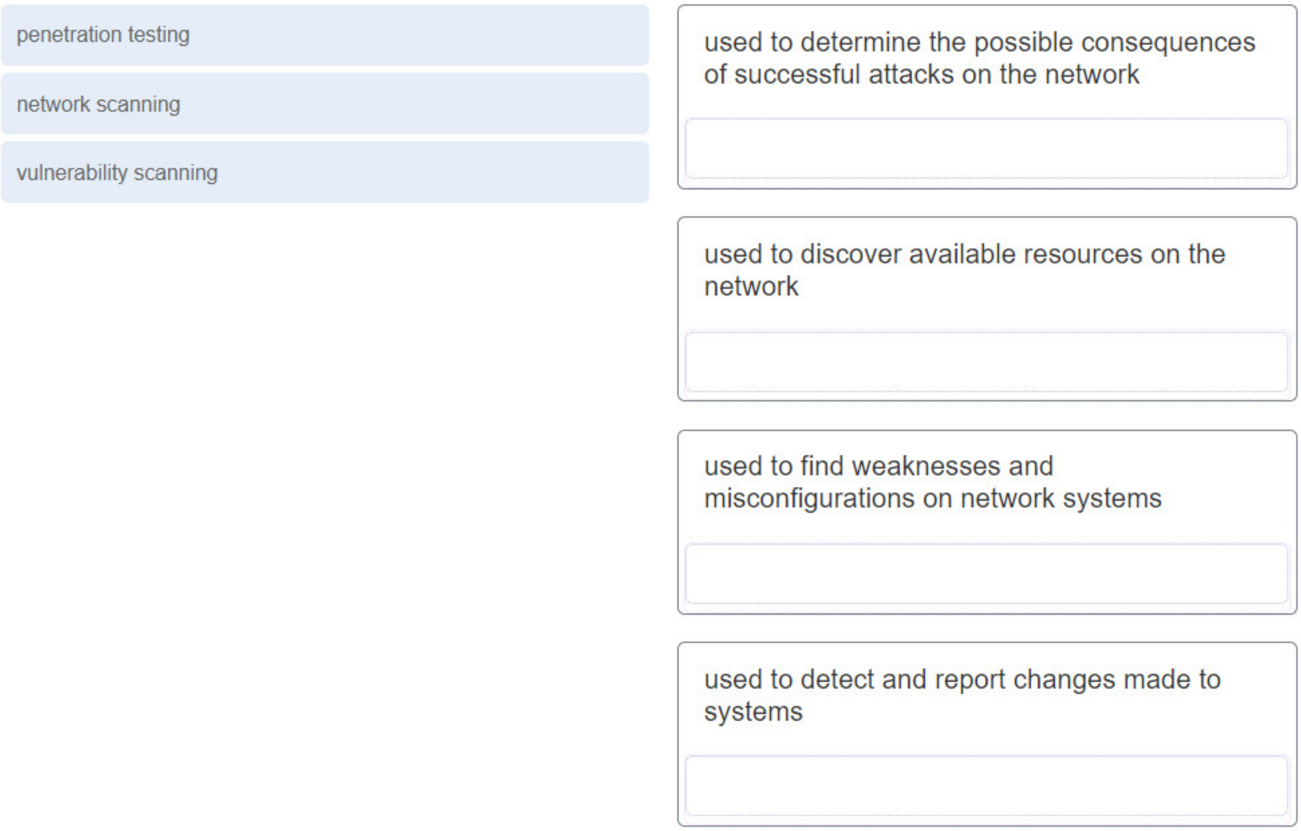
the likelihood of undesireable consequences

a mechanism used to compromise an asset

a weakness in a system

a potential danger to an asset

41. Match the network security testing technique with how it is used to test network security. (Not all options are used.)



penetration testing

network scanning

vulnerability scanning

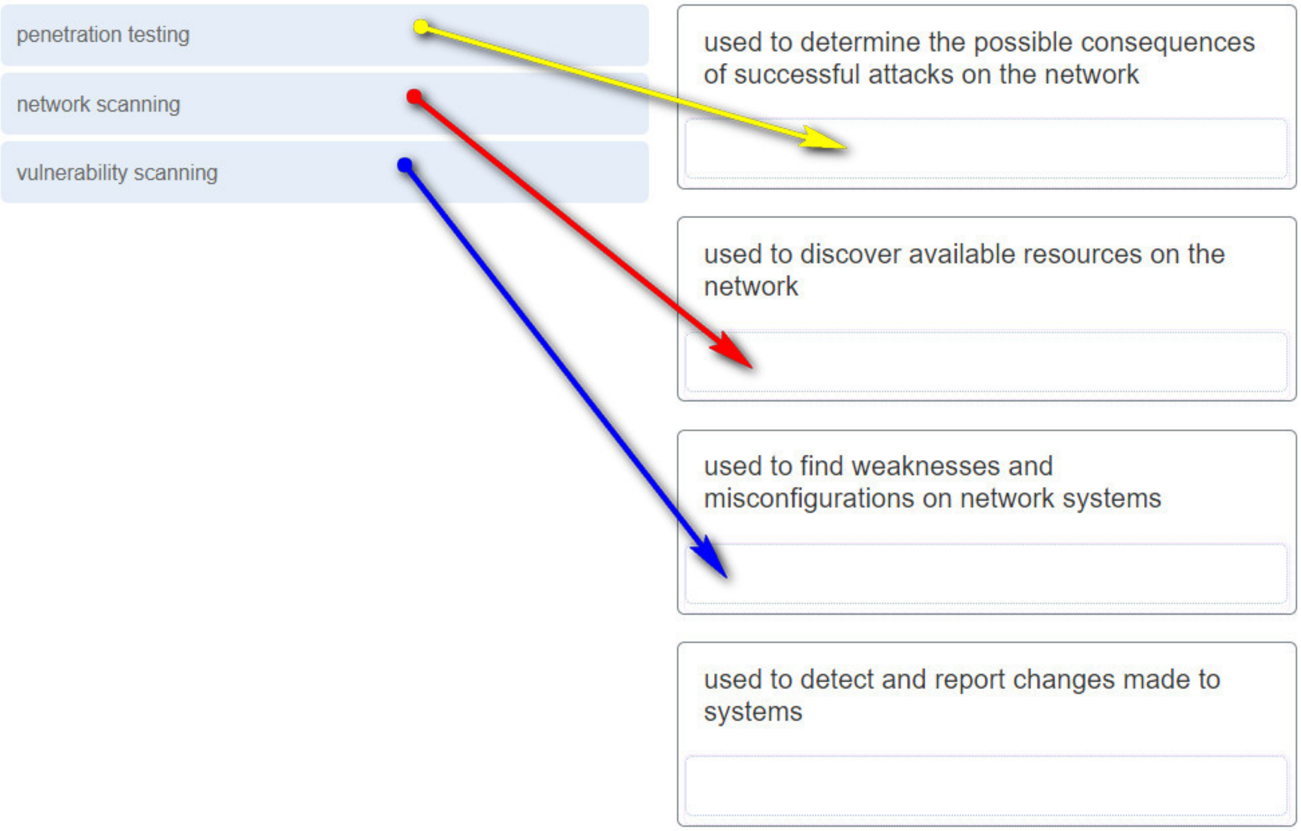
used to determine the possible consequences of successful attacks on the network

used to discover available resources on the network

used to find weaknesses and misconfigurations on network systems

used to detect and report changes made to systems

Answer



penetration testing

network scanning

vulnerability scanning

used to determine the possible consequences of successful attacks on the network

used to discover available resources on the network

used to find weaknesses and misconfigurations on network systems

used to detect and report changes made to systems

Explanation: Network scanning tools are used to probe network devices, servers and hosts for open TCP or UDP ports. Vulnerability scanning tools are used to discover security weaknesses in a network or computer system. Penetration testing tools are used to determine the possible outcome of a successful attack on a network or computer system.

Download PDF File below:

[sociallocker id="54558″]

CCNA Cybersecurity Operations (Version 1.1) - CyberOps Chapter 6 Exam Answers.pdf 371.22 KB 1527 downloads

…

Download

[/sociallocker]