CCNA 3 v7 Modules 3 – 5: Network Security Exam Answers

itexamanswers.net/ccna-3-v7-modules-3-5-network-security-exam-answers.html

December 22, 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.

Enterprise Networking, Security, and Automation (Version 7.00) – Modules 3 – 5: Network Security Exam

1. The IT department is reporting that a company web server is receiving an abnormally high number of web page requests from different locations simultaneously. Which type of security attack is occurring?

- adware
- **DDoS**
- phishing
- social engineering
- spyware

2. What causes a buffer overflow?

- launching a security countermeasure to mitigate a Trojan horse
- 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
- sending repeated connections such as Telnet to a particular device, thus denying other data sources

3. Which objective of secure communications is achieved by encrypting data?

- authentication
- availability

- **confidentiality**
- integrity

Explanation: When data is encrypted, it is scrambled to keep the data private and confidential so that only authorized recipients can read the message. A hash function is another way of providing confidentiality.

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

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

5. What commonly motivates cybercriminals to attack networks as compared to hactivists or state-sponsored hackers?

- **financial gain**
- fame seeking
- status among peers
- political reasons

Explanation: 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 type of hacker is motivated to protest against political and social issues?

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

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

7. What is a ping sweep?

- a query and response protocol that identifies information about a domain, including the addresses that are assigned to that domain.
- 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 network scanning technique that indicates the live hosts in a range of IP addresses.**

Explanation: 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.

8. In what type of attack is a cybercriminal attempting to prevent legitimate users from accessing network services?

- address spoofing
- MITM
- session hijacking
- **DoS**

Explanation: In a DoS or denial-of-service attack, the goal of the attacker is to prevent legitimate users from accessing network services.

9. Which requirement of secure communications is ensured by the implementation of MD5 or SHA hash generating algorithms?

- nonrepudiation
- authentication
- **integrity**
- confidentiality

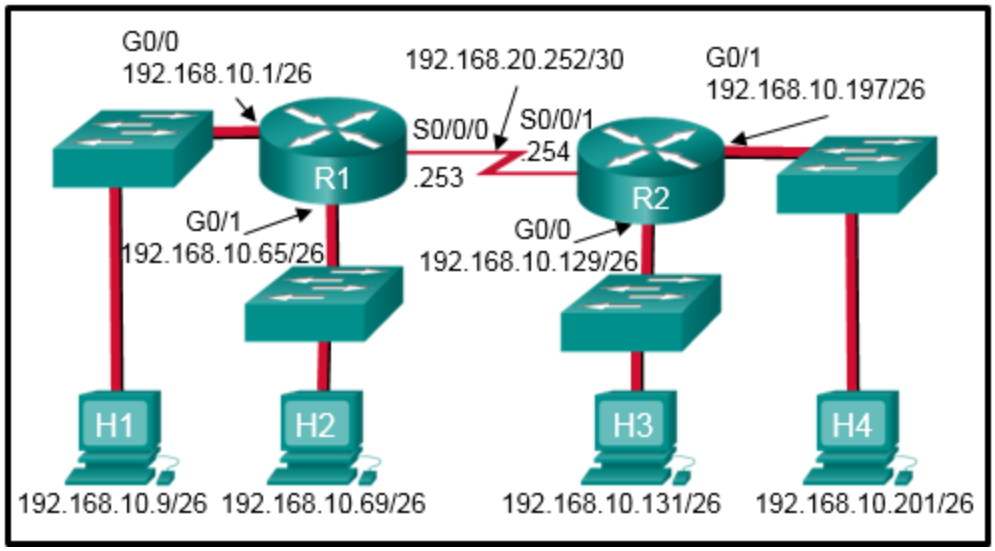
Explanation: Integrity is ensured by implementing either MD5 or SHA hash generating algorithms. Many modern networks ensure authentication with protocols, such as HMAC. Data confidentiality is ensured through symmetric encryption algorithms, including DES, 3DES, and AES. Data confidentiality can also be ensured using asymmetric algorithms, including RSA and PKI.

10. If an asymmetric algorithm uses a public key to encrypt data, what is used to decrypt it?

- a digital certificate
- a different public key
- **a private key**
- DH

Explanation: When an asymmetric algorithm is used, public and private keys are used for the encryption. Either key can be used for encryption, but the complementary matched key must be used for the decryption. For example if the public key is used for encryption, then the private key must be used for the decryption.

11. Refer to the exhibit. Which two ACLs would permit only the two LAN networks attached to R1 to access the network that connects to R2 G0/1 interface? (Choose two.)



- **access-list 1 permit 192.168.10.0 0.0.0.127**
- access-list 2 permit host 192.168.10.9
  access-list 2 permit host 192.168.10.69
- **access-list 5 permit 192.168.10.0 0.0.0.63**
  access-list 5 permit 192.168.10.64 0.0.0.63
- access-list 3 permit 192.168.10.128 0.0.0.63
- access-list 4 permit 192.168.10.0 0.0.0.255

Explanation: The **permit 192.168.10.0 0.0.0.127** command ignores bit positions 1 through 7, which means that addresses 192.168.10.0 through 192.168.10.127 are allowed through. The two ACEs of **permit 192.168.10.0 0.0.0.63** and **permit 192.168.10.64 0.0.0.63** allow the same address range through the router.

12. Which two packet filters could a network administrator use on an IPv4 extended ACL? (Choose two.)

- **destination UDP port number**
- computer type
- destination MAC address
- **ICMP message type**
- source TCP hello address

Explanation: Extended access lists commonly filter on source and destination IPv4 addresses and TCP or UDP port numbers. Additional filtering can be provided for protocol types.

13. What type of ACL offers greater flexibility and control over network access?

- numbered standard
- named standard
- **extended**
- flexible

Explanation: The two types of ACLs are standard and extended. Both types can be named or numbered, but extended ACLs offer greater flexibility.

14. What is the quickest way to remove a single ACE from a named ACL?

- **Use the no keyword and the sequence number of the ACE to be removed.**
- Copy the ACL into a text editor, remove the ACE, then copy the ACL back into the router.
- Create a new ACL with a different number and apply the new ACL to the router interface.
- Use the no access-list command to remove the entire ACL, then recreate it without the ACE.

Explanation: Named ACL ACEs can be removed using the **no** command followed by the sequence number.

15. Refer to the exhibit. A network administrator is configuring a standard IPv4 ACL. What is the effect after the command no access-list 10 is entered?

```
R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# access-list 10 permit host 192.168.25.16
R1(config)# access-list 10 deny 192.168.25.0 0.0.0.255
R1(config)# interface fastEthernet 0/1
R1(config-if)# ip access-group 10 in
R1(config-if)# end
R1#

R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# no access-list 10
R1(config)# end
R1#
```

- ACL 10 is removed from both the running configuration and the interface Fa0/1.
- **ACL 10 is removed from the running configuration.**

- ACL 10 is disabled on Fa0/1.
- ACL 10 will be disabled and removed after R1 restarts.

Explanation: The R1(config)# **no access-list** <*access-list number*> command removes the ACL from the running-config immediately. However, to disable an ACL on an interface, the command R1(config-if)# **no ip access-group** should be entered.

16. Refer to the exhibit. A network administrator has configured ACL 9 as shown. Users on the 172.31.1.0 /24 network cannot forward traffic through router CiscoVille. What is the most likely cause of the traffic failure?

```
CiscoVille#
CiscoVille# configure terminal
CiscoVille(config)# access-list 9 permit 172.29.0.0 0.0.0.255
CiscoVille(config)# access-list 9 permit 172.30.0.0 0.0.0.255
CiscoVille(config)# access-list 9 deny 172.31.0.0 0.0.255.255
CiscoVille(config)# access-list 9 permit 172.31.1.0 0.0.0.255
CiscoVille(config)# access-list 9 deny 192.168.1.0 0.0.0.255
CiscoVille(config)# access-list 9 permit any
CiscoVille(config)# interface fastethernet0/1
CiscoVille(config-if)# ip access-group 9 in
CiscoVille(config-if)# end
```

- The established keyword is not specified.
- **The sequence of the ACEs is incorrect.**
- The port number for the traffic has not been identified with the eq keyword.
- The permit statement specifies an incorrect wildcard mask.

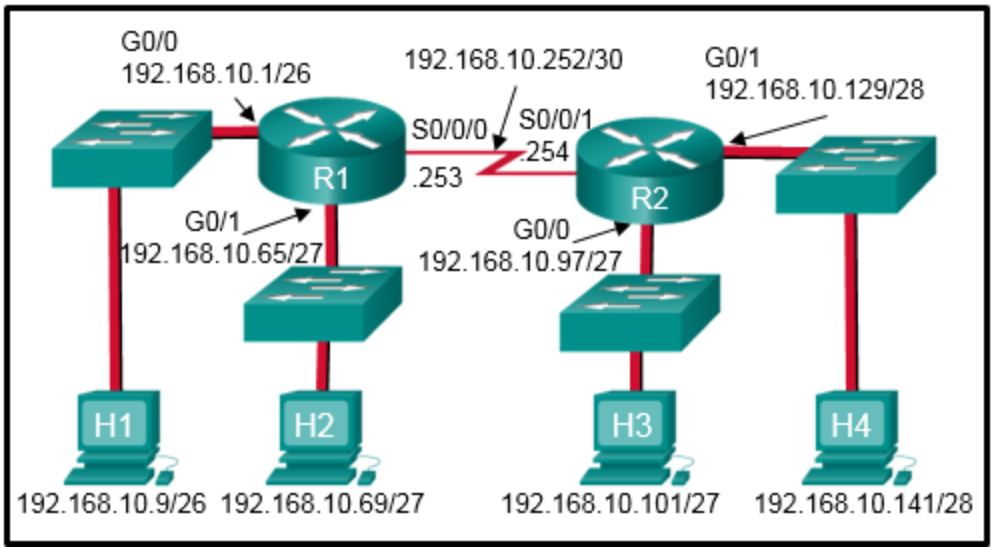
Explanation: When verifying an ACL, the statements are always listed in a sequential order. Even though there is an explicit permit for the traffic that is sourced from network 172.31.1.0 /24, it is being denied due to the previously implemented ACE of **CiscoVille(config)# access-list 9 deny 172.31.0.0 0.0.255.255**. The sequence of the ACEs must be modified to permit the specific traffic that is sourced from network 172.31.1.0 /24 and then to deny 172.31.0.0 /16.

17. A network administrator needs to configure a standard ACL so that only the workstation of the administrator with the IP address 192.168.15.23 can access the virtual terminal of the main router. Which two configuration commands can achieve the task? (Choose two.)

- **Router1(config)# access-list 10 permit 192.168.15.23 0.0.0.0**
- Router1(config)# access-list 10 permit 192.168.15.23 0.0.0.255
- Router1(config)# access-list 10 permit 192.168.15.23 255.255.255.255
- **Router1(config)# access-list 10 permit host 192.168.15.23**
- Router1(config)# access-list 10 permit 192.168.15.23 255.255.255.0

Explanation: To permit or deny one specific IP address, either the wildcard mask **0.0.0.0** (used after the IP address) or the wildcard mask keyword **host** (used before the IP address) can be used.

18. Refer to the exhibit. Which command would be used in a standard ACL to allow only devices on the network attached to R2 G0/0 interface to access the networks attached to R1?



- access-list 1 permit 192.168.10.128 0.0.0.63
- access-list 1 permit 192.168.10.0 0.0.0.255
- **access-list 1 permit 192.168.10.96 0.0.0.31**
- access-list 1 permit 192.168.10.0 0.0.0.63

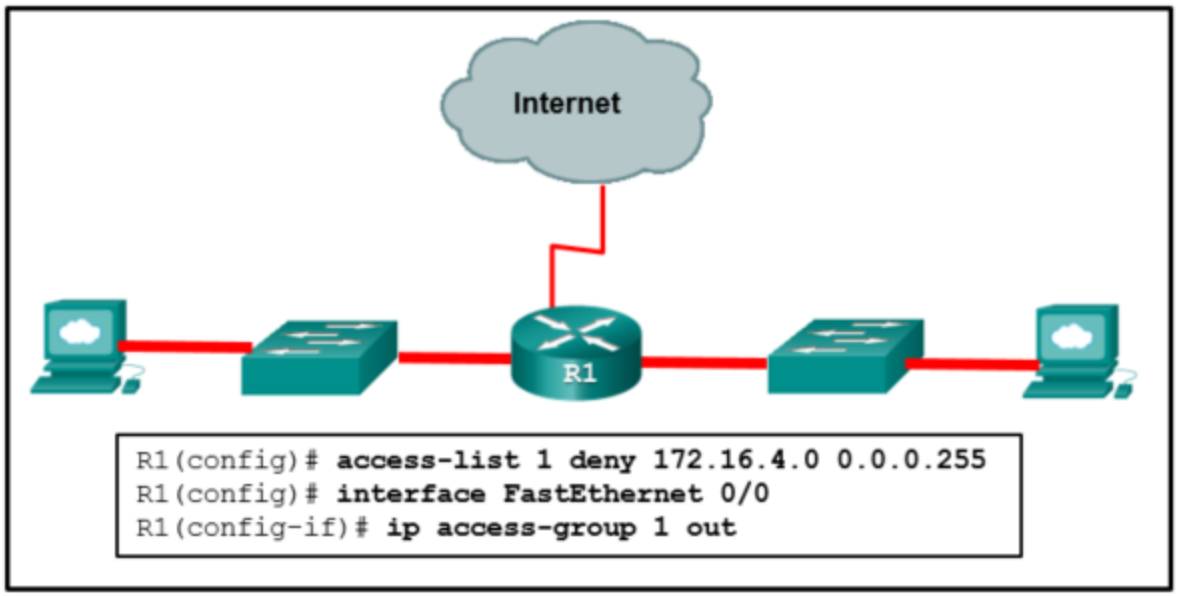
Explanation: Standard access lists only filter on the source IP address. In the design, the packets would be coming from the 192.168.10.96/27 network (the R2 G0/0 network). The correct ACL is **access-list 1 permit 192.168.10.96 0.0.0.31**.

19. A network administrator is writing a standard ACL that will deny any traffic from the 172.16.0.0/16 network, but permit all other traffic. Which two commands should be used? (Choose two.)

- Router(config)# access-list 95 deny 172.16.0.0 255.255.0.0
- **Router(config)# access-list 95 permit any**
- Router(config)# access-list 95 host 172.16.0.0
- **Router(config)# access-list 95 deny 172.16.0.0 0.0.255.255**
- Router(config)# access-list 95 172.16.0.0 255.255.255.255
- Router(config)# access-list 95 deny any

Explanation: To deny traffic from the 172.16.0.0/16 network, the **access-list 95 deny 172.16.0.0 0.0.255.255** command is used. To permit all other traffic, the **access-list 95 permit any** statement is added.

20. Refer to the exhibit. An ACL was configured on R1 with the intention of denying traffic from subnet 172.16.4.0/24 into subnet 172.16.3.0/24. All other traffic into subnet 172.16.3.0/24 should be permitted. This standard ACL was then applied outbound on interface Fa0/0. Which conclusion can be drawn from this configuration?



- The ACL should be applied outbound on all interfaces of R1.
- The ACL should be applied to the FastEthernet 0/0 interface of R1 inbound to accomplish the requirements.
- **All traffic will be blocked, not just traffic from the 172.16.4.0/24 subnet.**
- Only traffic from the 172.16.4.0/24 subnet is blocked, and all other traffic is allowed.
- An extended ACL must be used in this situation.

Explanation: Because of the implicit deny at the end of all ACLs, the **access-list 1 permit any** command must be included to ensure that only traffic from the 172.16.4.0/24 subnet is blocked and that all other traffic is allowed.

21. Refer to the exhibit. A network administrator needs to add an ACE to the TRAFFIC-CONTROL ACL that will deny IP traffic from the subnet 172.23.16.0/20. Which ACE will meet this requirement?

```
Router1# show access-lists
standard IP access list TRAFFIC-CONTROL
    10 permit 172.23.0.0, wildcard bits 0.0.255.255
    20 deny any
```

- 30 deny 172.23.16.0 0.0.15.255
- 15 deny 172.23.16.0 0.0.15.255
- **5 deny 172.23.16.0 0.0.15.255**
- 5 deny 172.23.16.0 0.0.255.255

Explanation: The only filtering criteria specified for a standard access list is the source IPv4 address. The wild card mask is written to identify what parts of the address to match, with a 0 bit, and what parts of the address should be ignored, which a 1 bit. The router will parse the ACE entries from lowest sequence number to highest. If an ACE must be added to an existing access list, the sequence number should be specified so that the ACE is in the correct place during the ACL evaluation process.

22. Refer to the exhibit. A network administrator configures an ACL on the router. Which statement describes the result of the configuration?

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# access-list 120 permit tcp host 192.168.25.18 host 172.16.45.16 eq 22
Router(config)# line vty 0 4
Router(config-line)# password admin-in
Router(config-line)# login local
Router(config-line)# access-class 120 in
Router(config-line)# end
Router#
```

- An SSH connection is allowed from a workstation with IP 172.16.45.16 to a device with IP 192.168.25.18.
- **An SSH connection is allowed from a workstation with IP 192.168.25.18 to a device with IP 172.16.45.16.**
- A Telnet connection is allowed from a workstation with IP 192.168.25.18 to a device with IP 172.16.45.16.
- A Telnet connection is allowed from a workstation with IP 172.16.45.16 to a device with IP 192.168.25.18.

Explanation: In an extended ACL, the first address is the source IP address and the second one is the destination IP address. TCP port number 22 is a well-known port number reserved for SSH connections. Telnet connections use TCP port number 23.

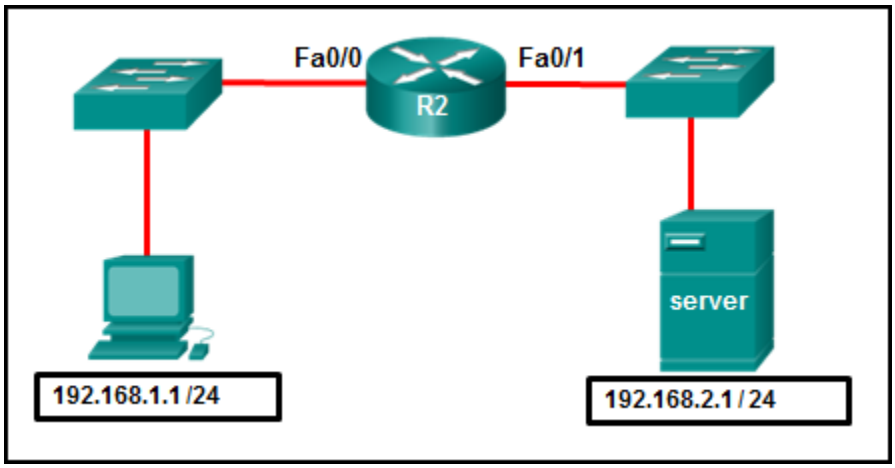
23. Refer to the exhibit. What can be determined from this output?

```
R1# show access-list MyACL
Extended IP access list MyACL
10 permit tcp host 10.35.80.22 host 10.23.77.101 eq telnet
20 permit tcp host 10.35.80.25 host 10.23.77.101 eq 16100 (149407 matches)
30 permit tcp host 10.35.80.25 host 10.23.77.101 eq 17600 (80592 matches)
40 permit tcp host 10.35.80.27 host 10.23.77.101 eq 10701 (26008 matches)
```

- The ACL is missing the deny ip any any ACE.
- The ACL is only monitoring traffic destined for 10.23.77.101 from three specific hosts.
- Because there are no matches for line 10, the ACL is not working.
- **The router has not had any Telnet packets from 10.35.80.22 that are destined for 10.23.77.101.**

Explanation: ACL entry 10 in MyACL matches any Telnet packets between host 10.35.80.22 and 10.23.77.101. No matches have occurred on this ACE as evidenced by the lack of a "(xxx matches)" ACE. The deny ip any any ACE is not required because there is an implicit deny ACE added to every access control list. When no matches exist for an ACL, it only means that no traffic has matched the conditions that exist for that particular line. The ACL is monitoring traffic that matches three specific hosts going to very specific destination devices. All other traffic is not permitted by the implicit deny ip any any ACE.

24. Refer to the exhibit. A network administrator wants to permit only host 192.168.1.1 /24 to be able to access the server 192.168.2.1 /24. Which three commands will achieve this using best ACL placement practices? (Choose three.)



- R2(config)# interface fastethernet 0/1
- R2(config-if)# ip access-group 101 out
- R2(config)# access-list 101 permit ip 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
- **R2(config-if)# ip access-group 101 in**
- R2(config)# access-list 101 permit ip any any
- **R2(config)# interface fastethernet 0/0**

- **R2(config)# access-list 101 permit ip host 192.168.1.1 host 192.168.2.1**

Explanation: An extended ACL is placed as close to the source of the traffic as possible. In this case.it is placed in an inbound direction on interface fa0/0 on R2 for traffic entering the router from host with the IP address192.168.1.1 bound for the server with the IP address192.168.2.1.

25. Consider the following access list.

access-list 100 permit ip host 192.168.10.1 any
access-list 100 deny icmp 192.168.10.0 0.0.0.255 any echo
access-list 100 permit ip any any

Which two actions are taken if the access list is placed inbound on a router Gigabit Ethernet port that has the IP address 192.168.10.254 assigned? (Choose two.)

- Only Layer 3 connections are allowed to be made from the router to any other network device.
- Devices on the 192.168.10.0/24 network are not allowed to reply to any ping requests.
- Devices on the 192.168.10.0/24 network can sucessfully ping devices on the 192.168.11.0 network.
- **A Telnet or SSH session is allowed from any device on the 192.168.10.0 into the router with this access list assigned.**
- **Devices on the 192.168.10.0/24 network are allowed to reply to any ping requests.**
- Only the network device assigned the IP address 192.168.10.1 is allowed to access the router.

Explanation: The first ACE allows the 192.168.10.1 device to do any TCP/IP-based transactions with any other destination. The second ACE stops devices on the 192.168.10.0/24 network from issuing any pings to any other location. Everything else is permitted by the third ACE. Therefore, a Telnet/SSH session or ping reply is allowed from a device on the 192.168.10.0/24 network.

26. Refer to the exhibit. The named ACL "Managers" already exists on the router. What will happen when the network administrator issues the commands that are shown in the exhibit?

```
Router(config)# ip access-list extended Managers
Router(config-ext-nacl)# deny tcp 192.168.1.0 0.0.0.255 any eq telnet
Router(config-ext-nacl)# deny tcp 192.168.1.0 0.0.0.255 any eq www
Router(config-ext-nacl)# deny tcp 192.168.1.0 0.0.0.255 any eq ftp
```

- **The commands are added at the end of the existing Managers ACL.**

- The commands overwrite the existing Managers ACL.
- The commands are added at the beginning of the existing Managers ACL.
- The network administrator receives an error that states that the ACL already exists.

27. In which TCP attack is the cybercriminal attempting to overwhelm a target host with half-open TCP connections?

- port scan attack
- **SYN flood attack**
- session hijacking attack
- reset attack

Explanation: In a TCP SYN flood attack, the attacker sends to the target host a continuous flood of TCP SYN session requests with a spoofed source IP address. The target host responds with a TCP-SYN-ACK to each of the SYN session requests and waits for a TCP ACK that will never arrive. Eventually the target is overwhelmed with half-open TCP connections.

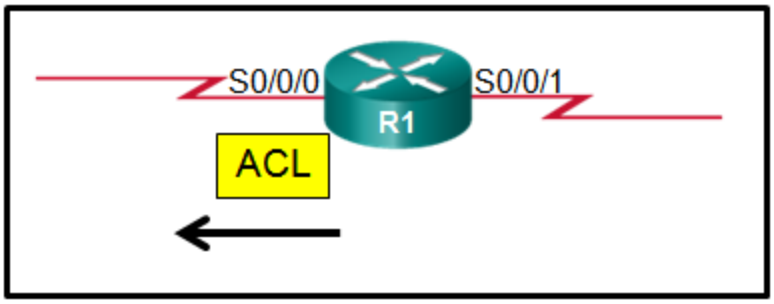
28. Which protocol is attacked when a cybercriminal provides an invalid gateway in order to create a man-in-the-middle attack?

- **DHCP**
- DNS
- ICMP
- HTTP or HTTPS

Explanation: A cybercriminal could set up a rogue DHCP server that provides one or more of the following:

- Wrong default gateway that is used to create a man-in-the-middle attack and allow the attacker to intercept data
- Wrong DNS server that results in the user being sent to a malicious website
- Invalid default gateway IP address that results in a denial of service attack on the DHCP client

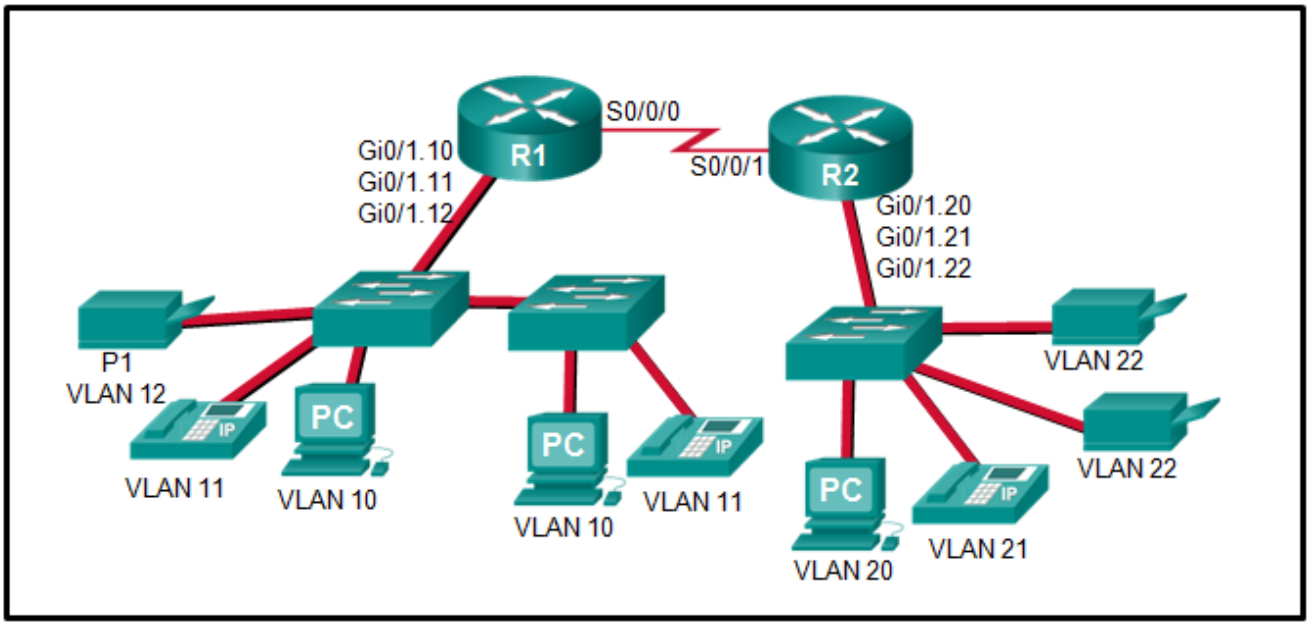
29. Refer to the exhibit. An administrator has configured a standard ACL on R1 and applied it to interface serial 0/0/0 in the outbound direction. What happens to traffic leaving interface serial 0/0/0 that does not match the configured ACL statements?



- **The traffic is dropped.**
- The source IP address is checked and, if a match is not found, traffic is routed out interface serial 0/0/1.
- The resulting action is determined by the destination IP address.
- The resulting action is determined by the destination IP address and port number.

Explanation: Any traffic that does not match one of the statements in an ACL has the implicit deny applied to it, which means the traffic is dropped.

30. Refer to the exhibit. The Gigabit interfaces on both routers have been configured with subinterface numbers that match the VLAN numbers connected to them. PCs on VLAN 10 should be able to print to the P1 printer on VLAN 12. PCs on VLAN 20 should print to the printers on VLAN 22. What interface and in what direction should you place a standard ACL that allows printing to P1 from data VLAN 10, but stops the PCs on VLAN 20 from using the P1 printer? (Choose two.)



- inbound
- R2 S0/0/1
- **R1 Gi0/1.12**

- **outbound**
- R1 S0/0/0
- R2 Gi0/1.20

Explanation: A standard access list is commonly placed as close to the destination network as possible because access control expressions in a standard ACL do not include information about the destination network.
The destination in this example is printer VLAN 12 which has router R1 Gigabit subinterface 0/1/.12 as its gateway. A sample standard ACL that only allows printing from data VLAN 10 (192.168.10.0/24), for example, and no other VLAN would be as follows:

```
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)# access-list 1 deny any
R1(config)# interface gigabitethernet 0/1.12
R1(config-if)# ip access-group 1 out
```

31. Which statement describes a characteristic of standard IPv4 ACLs?

- They are configured in the interface configuration mode.
- They can be configured to filter traffic based on both source IP addresses and source ports.
- They can be created with a number but not with a name.
- **They filter traffic based on source IP addresses only.**

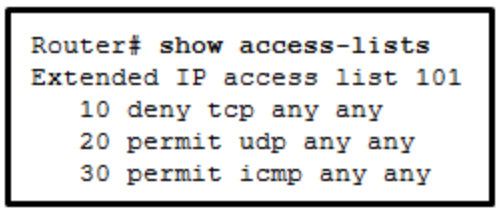
Explanation: A standard IPv4 ACL can filter traffic based on source IP addresses only. Unlike an extended ACL, it cannot filter traffic based on Layer 4 ports. However, both standard and extended ACLs can be identified with either a number or a name, and both are configured in global configuration mode.

32. What is considered a best practice when configuring ACLs on vty lines?

- **Place identical restrictions on all vty lines.**
- Remove the vty password since the ACL restricts access to trusted users.
- Apply the ip access-group command inbound.
- Use only extended access lists.

33.

Refer to the exhibit. An administrator first configured an extended ACL as shown by the output of the show access-lists command. The administrator then edited this access-list by issuing the commands below.



```
Router(config)# ip access-list extended 101
Router(config-ext-nacl)# no 20
Router(config-ext-nacl)# 5 permit tcp any any eq 22
Router(config-ext-nacl)# 20 deny udp any any
```

Which two conclusions can be drawn from this new configuration? (Choose two.)

- TFTP packets will be permitted.
- **Ping packets will be permitted.**
- Telnet packets will be permitted.
- **SSH packets will be permitted.**
- All TCP and UDP packets will be denied.

Explanation: After the editing, the final configuration is as follows:
Router# **show access-lists**
Extended IP access list 101
5 permit tcp any any eq ssh
10 deny tcp any any
20 deny udp any any
30 permit icmp any any
So, only SSH packets and ICMP packets will be permitted.

34. Which set of access control entries would allow all users on the 192.168.10.0/24 network to access a web server that is located at 172.17.80.1, but would not allow them to use Telnet?

- access-list 103 deny tcp host 192.168.10.0 any eq 23
  access-list 103 permit tcp host 192.168.10.1 eq 80
- access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80
  access-list 103 deny tcp 192.168.10.0 0.0.0.255 any eq 23
- access-list 103 permit 192.168.10.0 0.0.0.255 host 172.17.80.1
  access-list 103 deny tcp 192.168.10.0 0.0.0.255 any eq telnet
- **access-list 103 permit tcp 192.168.10.0 0.0.0.255 host 172.17.80.1 eq 80**
  access-list 103 deny tcp 192.168.10.0 0.0.0.255 any eq 23

Explanation: For an extended ACL to meet these requirements the following need to be included in the access control entries:

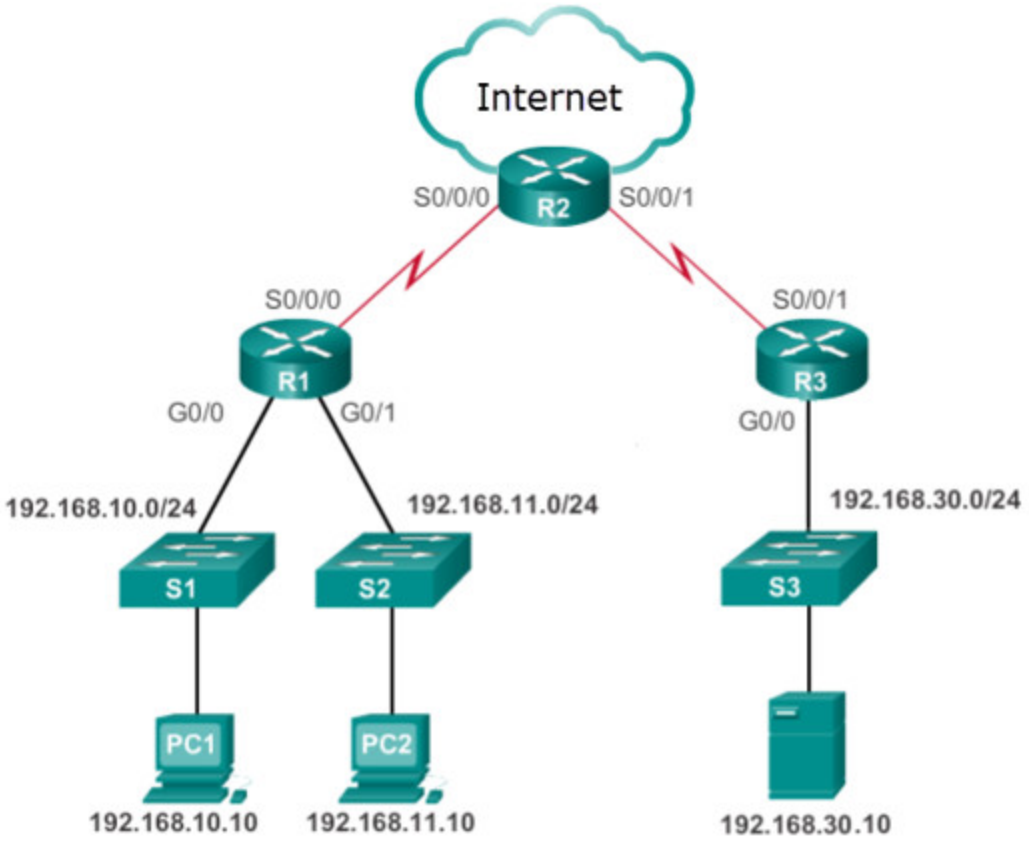
- identification number in the range 100-199 or 2000-2699
- permit or deny parameter
- protocol
- source address and wildcard
- destination address and wildcard

- port number or name

35. What is the term used to describe a mechanism that takes advantage of a vulnerability?

- mitigation
- **exploit**
- vulnerability
- threat

36. Refer to the exhibit. The network administrator has an IP address of 192.168.11.10 and needs access to manage R1. What is the best ACL type and placement to use in this situation?



- extended ACL outbound on R2 WAN interface towards the internet
- **standard ACL inbound on R1 vty lines**
- extended ACLs inbound on R1 G0/0 and G0/1
- extended ACL outbound on R2 S0/0/1

Explanation: Standard ACLs permit or deny packets based only on the source IPv4 address. Because all traffic types are permitted or denied, standard ACLs should be located as close to the destination as possible.

Extended ACLs permit or deny packets based on the source IPv4 address and destination IPv4 address, protocol type, source and destination TCP or UDP ports and more. Because the filtering of extended ACLs is so specific, extended ACLs should be located as close as possible to the source of the traffic to be filtered. Undesirable traffic is denied close to the source network without crossing the network infrastructure.

37. A technician is tasked with using ACLs to secure a router. When would the technician use the any configuration option or command?

- to add a text entry for documentation purposes
- to generate and send an informational message whenever the ACE is matched
- **to identify any IP address**
- to identify one specific IP address

38. Which statement accurately characterizes the evolution of threats to network security?

- Internet architects planned for network security from the beginning.
- Early Internet users often engaged in activities that would harm other users.
- **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.

Explanation: 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.

39. A user receives a phone call from a person who claims to represent IT services and then asks that user for confirmation of username and password for auditing purposes. Which security threat does this phone call represent?

- spam
- **social engineering**
- DDoS
- anonymous keylogging

Explanation: Social engineering attempts to gain the confidence of an employee and convince that person to divulge confidential and sensitive information, such as usernames and passwords. DDoS attacks, spam, and keylogging are all examples of software based security threats, not social engineering.

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

- 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.

- They are maliciously formed code segments used to replace legitimate applications.
- **They are infected machines that carry out a DDoS attack.**

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

41. Which attack involves threat actors positioning themselves between a source and destination with the intent of transparently monitoring, capturing, and controlling the communication?

- **man-in-the-middle attack**
- SYN flood attack
- DoS attack
- ICMP attack

Explanation: The man-in-the-middle attack is a common IP-related attack where threat actors position themselves between a source and destination to transparently monitor, capture, and control the communication.

42. Which two keywords can be used in an access control list to replace a wildcard mask or address and wildcard mask pair? (Choose two.)

- **host**
- most
- gt
- some
- **any**
- all

Explanation: The **host** keyword is used when using a specific device IP address in an ACL. For example, the **deny host 192.168.5.5** command is the same is the **deny 192.168.5.5 0.0.0.0** command. The **any** keyword is used to allow any mask through that meets the criteria. For example, the **permit any** command is the same as **permit 0.0.0.0 255.255.255.255** command.

43. Which statement describes a difference between the operation of inbound and outbound ACLs?

- **Inbound ACLs are processed before the packets are routed while outbound ACLs are processed after the routing is completed.**
- In contrast to outbound ALCs, inbound ACLs can be used to filter packets with multiple criteria.
- On a network interface, more than one inbound ACL can be configured but only one outbound ACL can be configured.

- Inbound ACLs can be used in both routers and switches but outbound ACLs can be used only on routers.

Explanation: With an inbound ACL, incoming packets are processed before they are routed. With an outbound ACL, packets are first routed to the outbound interface, then they are processed. Thus processing inbound is more efficient from the router perspective. The structure, filtering methods, and limitations (on an interface, only one inbound and one outbound ACL can be configured) are the same for both types of ACLs.

44. What effect would the Router1(config-ext-nacl)# permit tcp 172.16.4.0 0.0.0.255 any eq www command have when implemented inbound on the f0/0 interface?

- All TCP traffic is permitted, and all other traffic is denied.
- **Traffic originating from 172.16.4.0/24 is permitted to all TCP port 80 destinations.**
- All traffic from 172.16.4.0/24 is permitted anywhere on any port.
- The command is rejected by the router because it is incomplete.

45. Which ACE will permit a packet that originates from any network and is destined for a web server at 192.168.1.1?

- **access-list 101 permit tcp any host 192.168.1.1 eq 80**
- access-list 101 permit tcp host 192.168.1.1 eq 80 any
- access-list 101 permit tcp host 192.168.1.1 any eq 80
- access-list 101 permit tcp any eq 80 host 192.168.1.1

46. Refer to the exhibit. A new network policy requires an ACL denying FTP and Telnet access to a Corp file server from all interns. The address of the file server is 172.16.1.15 and all interns are assigned addresses in the 172.18.200.0/24 network. After implementing the ACL, no one in the Corp network can access any of the servers. What is the problem?

```
Corp# show running-config

interface GigabitEthernet0/1
description Server Farm
ip address 172.16.1.1 255.255.255.0
ip access-group FileServerAccess out
!
<output omitted>
!
ip access-list extended FileServerAccess
deny tcp 172.18.200.0 0.0.0.255 host 172.16.1.15 eq ftp
deny tcp 172.18.200.0 0.0.0.255 host 172.16.1.15 eq ftp-data
deny tcp 172.18.200.0 0.0.0.255 host 172.16.1.15 eq telnet
!
```

CCNA 3 v7 Modules 3 – 5: Network Security Exam Answers 46

- Inbound ACLs must be routed before they are processed.
- **The ACL is implicitly denying access to all the servers.**
- Named ACLs require the use of port numbers.
- The ACL is applied to the interface using the wrong direction.

Explanation: Both named and numbered ACLs have an implicit deny ACE at the end of the list. This implicit deny blocks all traffic.

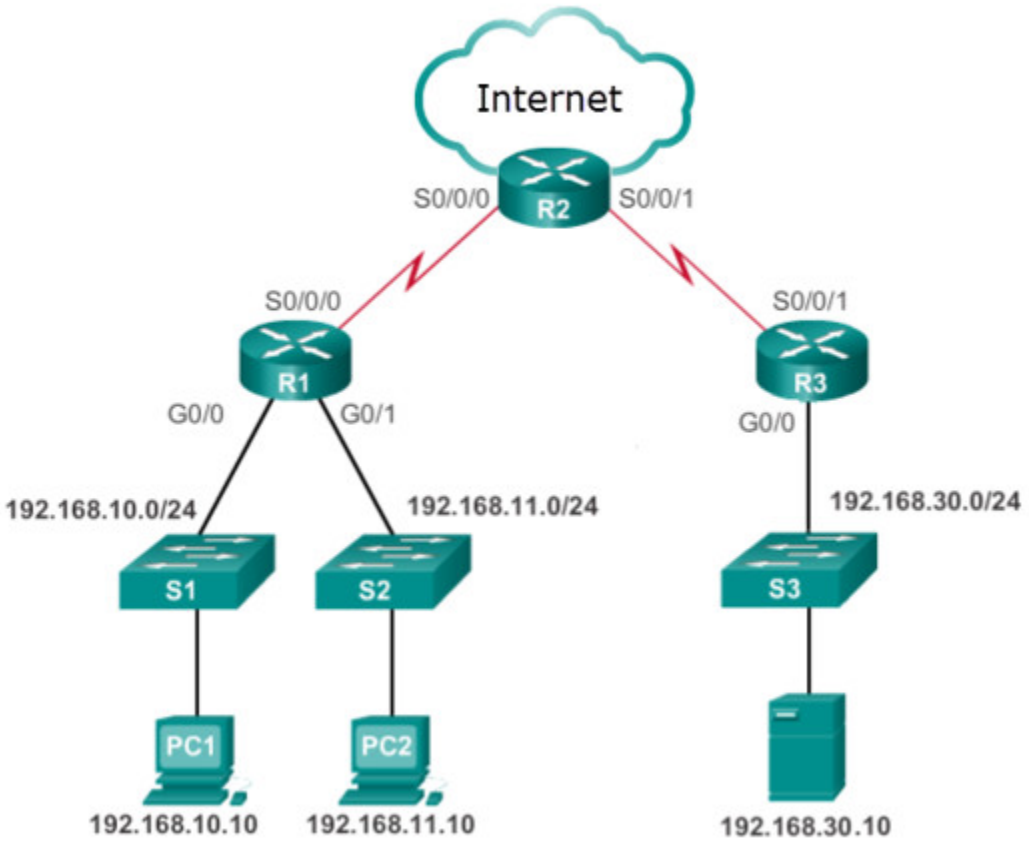
47. A technician is tasked with using ACLs to secure a router. When would the technician use the access-class 20 in configuration option or command?

- **to secure administrative access to the router**
- to remove an ACL from an interface
- to remove a configured ACL
- to apply a standard ACL to an interface

48. What is the term used to describe the same pre-shared key or secret key, known by both the sender and receiver to encrypt and decrypt data?

- **symmetric encryption algorithm**
- data integrity
- exploit
- risk

49. Refer to the exhibit. Internet privileges for an employee have been revoked because of abuse but the employee still needs access to company resources. What is the best ACL type and placement to use in this situation?

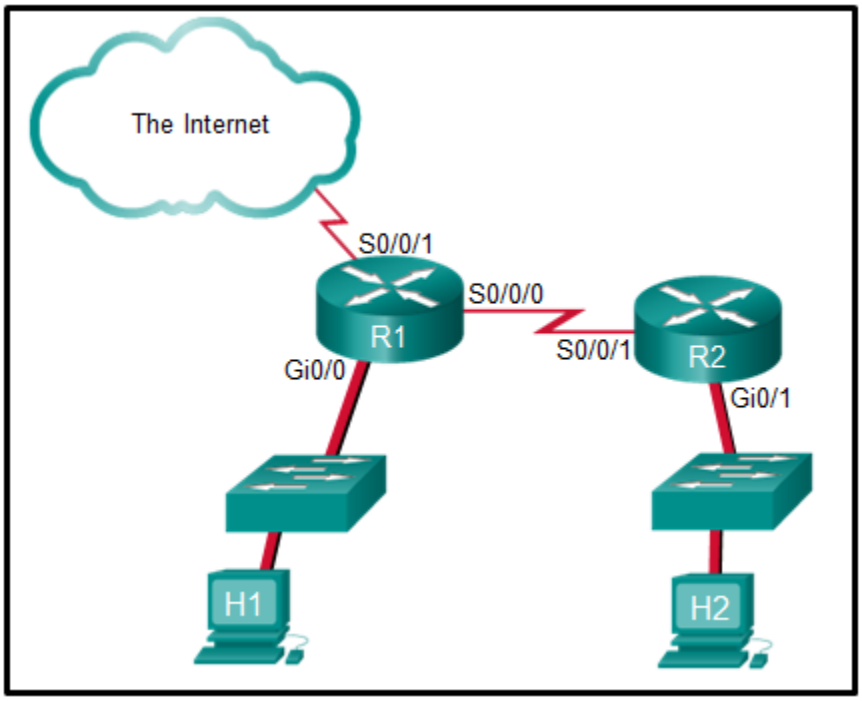


CCNA 3 v7 Modules 3 – 5: Network Security Exam Answers 49

- standard ACL inbound on R2 WAN interface connecting to the internet
- **standard ACL outbound on R2 WAN interface towards the internet**
- standard ACL inbound on R1 G0/0
- standard ACL outbound on R1 G0/0

Explanation: – Standard ACLs permit or deny packets based only on the source IPv4 address. Because all traffic types are permitted or denied, standard ACLs should be located as close to the destination as possible.
– Extended ACLs permit or deny packets based on the source IPv4 address and destination IPv4 address, protocol type, source and destination TCP or UDP ports and more. Because the filtering of extended ACLs is so specific, extended ACLs should be located as close as possible to the source of the traffic to be filtered. Undesirable traffic is denied close to the source network without crossing the network infrastructure.

50. Refer to the exhibit. The student on the H1 computer continues to launch an extended ping with expanded packets at the student on the H2 computer. The school network administrator wants to stop this behavior, but still allow both students access to web-based computer assignments. What would be the best plan for the network administrator?



CCNA 3 v7 Modules 3 – 5: Network Security Exam Answers 42

- Apply an inbound standard ACL on R1 Gi0/0.
- Apply an inbound extended ACL on R2 Gi0/1.
- Apply an outbound extended ACL on R1 S0/0/1.
- **Apply an inbound extended ACL on R1 Gi0/0.**
- Apply an outbound standard ACL on R2 S0/0/1.

Explanation: This access list must be an extended ACL in order to filter on specific source and destination host addresses. Commonly, the best place for an extended ACL is closest to the source, which is H1. Traffic from H1 travels into the switch, then out of the switch into the R1 Gi0/0 interface. This Gi0/0 interface would be the best location for this type of extended ACL. The ACL would be applied on the inbound interface since the packets from H1 would be coming into the R1 router.

51. A technician is tasked with using ACLs to secure a router. When would the technician use the 'ip access-group 101 in' configuration option or command?

- **to apply an extended ACL to an interface**
- to secure management traffic into the router
- to secure administrative access to the router
- to display all restricted traffic

52. In which type of attack is falsified information used to redirect users to malicious Internet sites?

- DNS amplification and reflection

- ARP cache poisoning
- **DNS cache poisoning**
- domain generation

Explanation: In a DNS cache poisoning attack, falsified information is used to redirect users from legitimate to malicious internet sites.

53. What is a feature of an IPS?

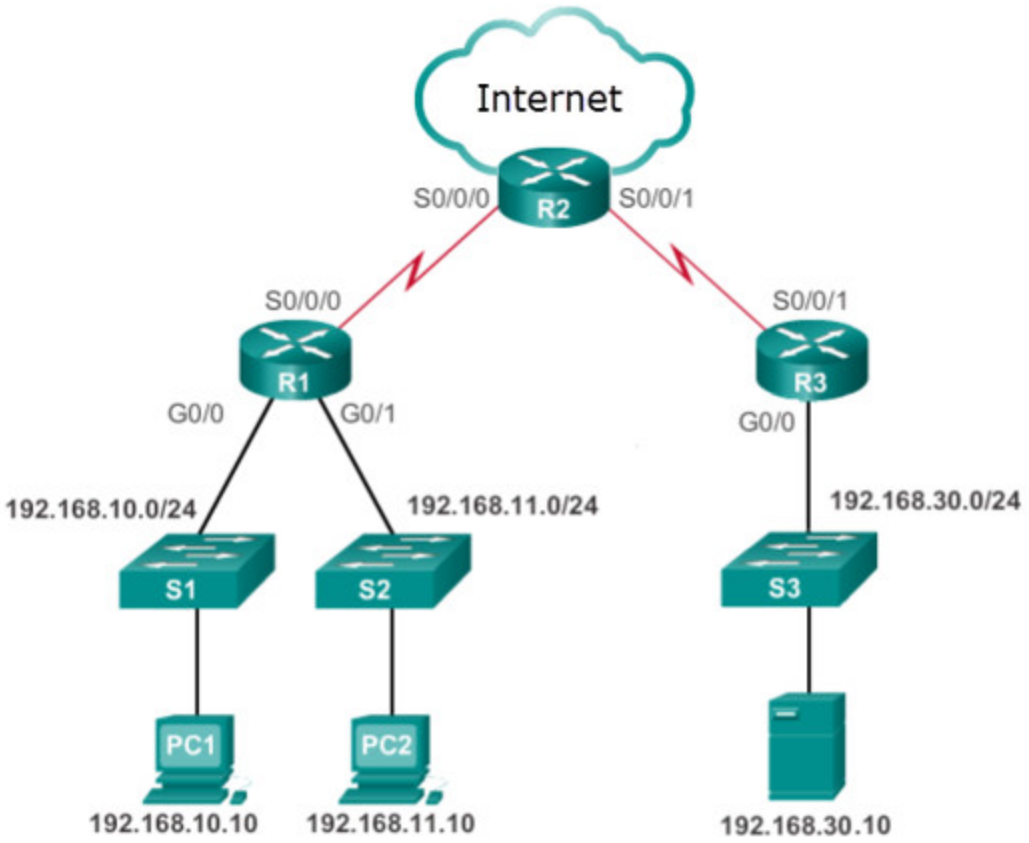
- **It can stop malicious packets.**
- It is deployed in offline mode.
- It has no impact on latency.
- It is primarily focused on identifying possible incidents.

Explanation: An advantage of an intrusion prevention systems (IPS) is that it can identify and stop malicious packets. However, because an IPS is deployed inline, it can add latency to the network.

54. What is the term used to describe a potential danger to a company's assets, data, or network functionality?

- vulnerability
- **threat**
- asset
- exploit

55. Refer to the exhibit. Network 192.168.30.0/24 contains all of the company servers. Policy dictates that traffic from the servers to both networks 192.168.10.0 and 192.168.11.0 be limited to replies for original requests. What is the best ACL type and placement to use in this situation?



- extended ACL inbound on R3 G0/0
- extended ACL inbound on R1 G0/0
- standard ACL inbound on R1 G0/1
- standard ACL inbound on R1 vty lines

Explanation: Standard ACLs permit or deny packets based only on the source IPv4 address. Because all traffic types are permitted or denied, standard ACLs should be located as close to the destination as possible.

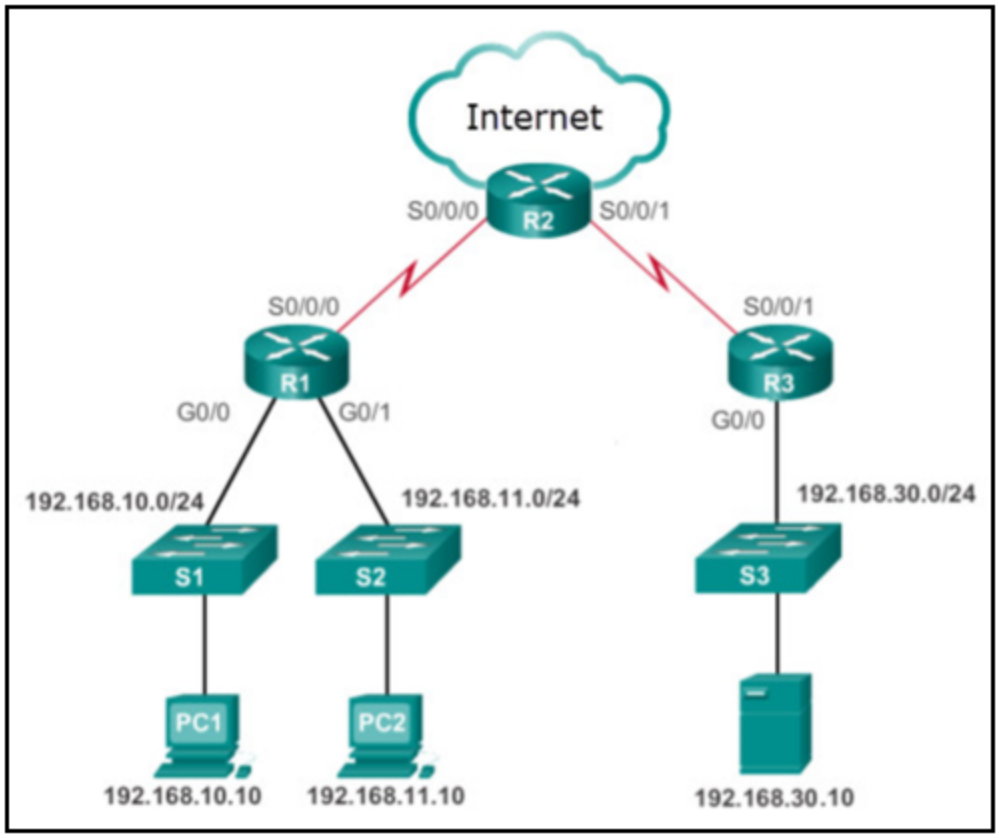
Extended ACLs permit or deny packets based on the source IPv4 address and destination IPv4 address, protocol type, source and destination TCP or UDP ports and more. Because the filtering of extended ACLs is so specific, extended ACLs should be located as close as possible to the source of the traffic to be filtered. Undesirable traffic is denied close to the source network without crossing the network infrastructure.

56. What does the CLI prompt change to after entering the command ip access-list standard aaa from global configuration mode?

- Router(config-line)#
- **Router(config-std-nacl)#**
- Router(config)#
- Router(config-router)#

- Router(config-if)#

57. Refer to the exhibit. Many employees are wasting company time accessing social media on their work computers. The company wants to stop this access. What is the best ACL type and placement to use in this situation?



- extended ACL outbound on R2 WAN interface towards the internet
- standard ACL outbound on R2 WAN interface towards the internet
- standard ACL outbound on R2 S0/0/0
- **extended ACLs inbound on R1 G0/0 and G0/1**

58. A technician is tasked with using ACLs to secure a router. When would the technician use the 40 deny host 192.168.23.8 configuration option or command?

- to remove all ACLs from the router
- **to create an entry in a numbered ACL**
- to apply an ACL to all router interfaces
- to secure administrative access to the router

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

- It is malware that can only be distributed over the Internet.
- **It appears as useful software but hides malicious code.**

- It is software that causes annoying but not fatal computer problems.
- It is the most easily detected form of malware.

60. What wild card mask will match networks 172.16.0.0 through 172.19.0.0?

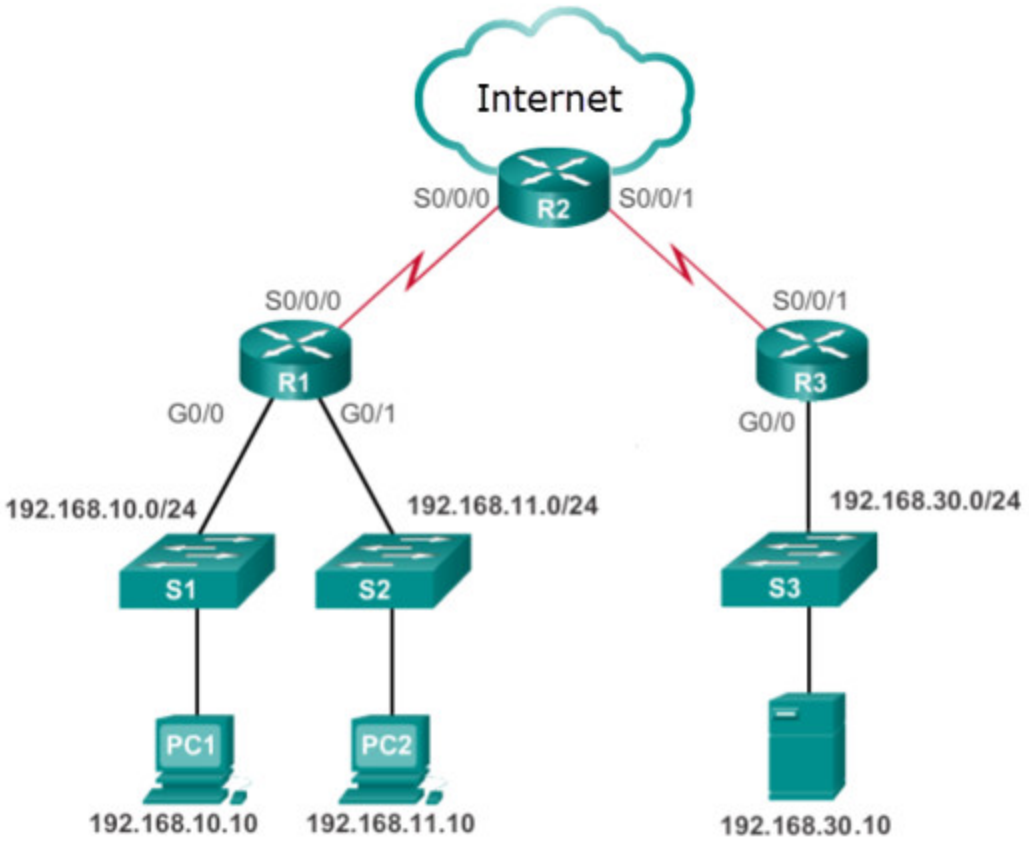
- 0.0.3.255
- 0.252.255.255
- **0.3.255.255**
- 0.0.255.255

Explanation: The subnets 172.16.0.0 through 172.19.0.0 all share the same 14 high level bits. A wildcard mask in binary that matches 14 high order bits is 00000000.00000011.11111111.11111111. In dotted decimal this wild card mask is 0.3.255.255.

60. What is the term used to describe gray hat hackers who publicly protest organizations or governments by posting articles, videos, leaking sensitive information, and performing network attacks?

- white hat hackers
- grey hat hackers
- **hacktivists**
- state-sponsored hacker

61. Refer to the exhibit. The company has provided IP phones to employees on the 192.168.10.0/24 network and the voice traffic will need priority over data traffic. What is the best ACL type and placement to use in this situation?



- **extended ACL inbound on R1 G0/0**
- extended ACL outbound on R2 WAN interface towards the internet
- extended ACL outbound on R2 S0/0/1
- extended ACLs inbound on R1 G0/0 and G0/1

Explanation: Standard ACLs permit or deny packets based only on the source IPv4 address. Because all traffic types are permitted or denied, standard ACLs should be located as close to the destination as possible.

Extended ACLs permit or deny packets based on the source IPv4 address and destination IPv4 address, protocol type, source and destination TCP or UDP ports and more. Because the filtering of extended ACLs is so specific, extended ACLs should be located as close as possible to the source of the traffic to be filtered. Undesirable traffic is denied close to the source network without crossing the network infrastructure.

62. A technician is tasked with using ACLs to secure a router. When would the technician use the no ip access-list 101 configuration option or command?

- to apply an ACL to all router interfaces
- to secure administrative access to the router
- to remove all ACLs from the router
- **to remove a configured ACL**

63. What is the term used to describe unethical criminals who compromise computer and network security for personal gain, or for malicious reasons?

- hacktivists
- vulnerability broker
- **black hat hackers**
- script kiddies

64. What is the term used to describe a guarantee that the message is not a forgery and does actually come from whom it states?

- **origin authentication**
- mitigation
- exploit
- data non-repudiation

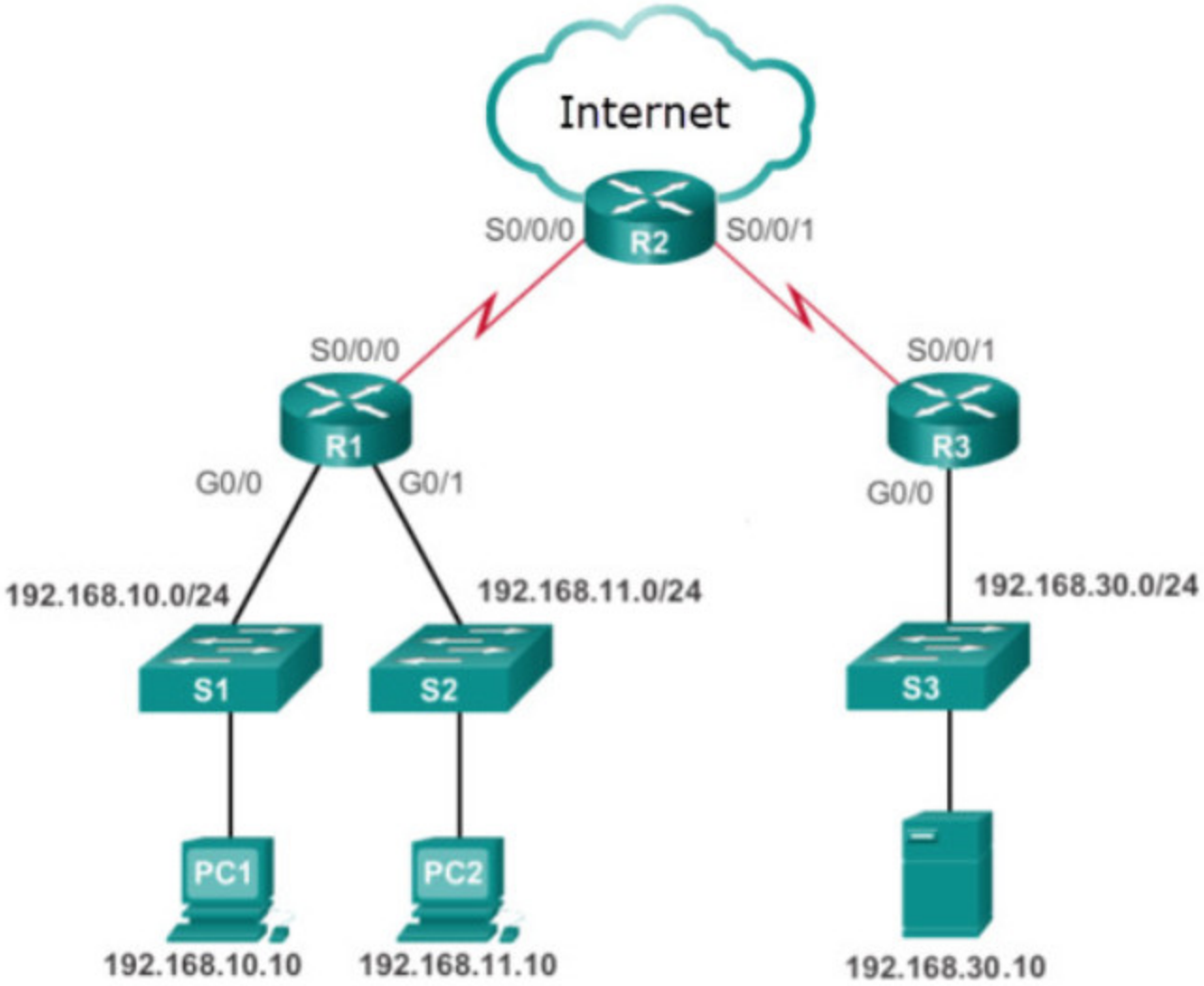
65. A technician is tasked with using ACLs to secure a router. When would the technician use the ip access-group 101 in configuration option or command?

- to secure administrative access to the router
- **to apply an extended ACL to an interface**
- to display all restricted traffic
- to secure management traffic into the router

66. A technician is tasked with using ACLs to secure a router. When would the technician use the remark configuration option or command?

- to generate and send an informational message whenever the ACE is matched
- **to add a text entry for documentation purposes**
- to identify one specific IP address
- to restrict specific traffic access through an interface

67. Refer to the exhibit. The company CEO demands that one ACL be created to permit email traffic to the internet and deny FTP access. What is the best ACL type and placement to use in this situation?



- **extended ACL outbound on R2 WAN interface towards the internet**
- standard ACL outbound on R2 S0/0/0
- extended ACL inbound on R2 S0/0/0
- standard ACL inbound on R2 WAN interface connecting to the internet

68. A technician is tasked with using ACLs to secure a router. When would the technician use the established configuration option or command?

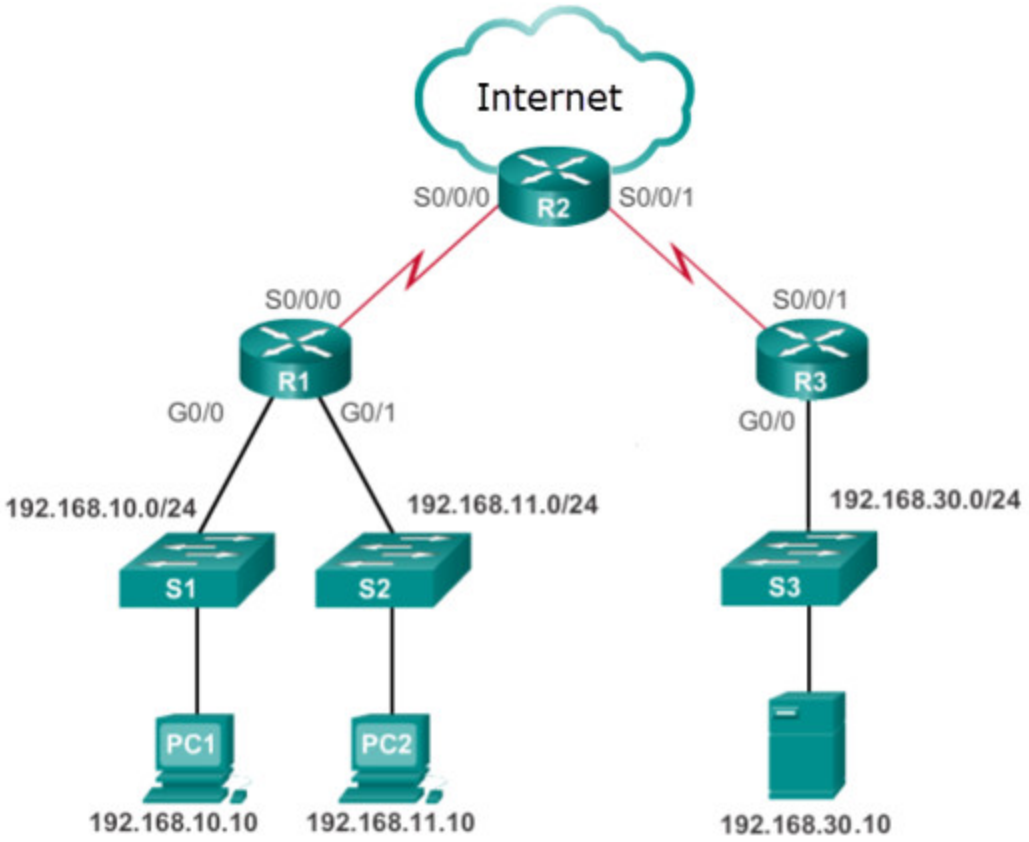
- to add a text entry for documentation purposes
- to display all restricted traffic
- to allow specified traffic through an interface
- to allow returning reply traffic to enter the internal network

69. A technician is tasked with using ACLs to secure a router. When would the technician use the deny configuration option or command?

- to identify one specific IP address
- to display all restricted traffic

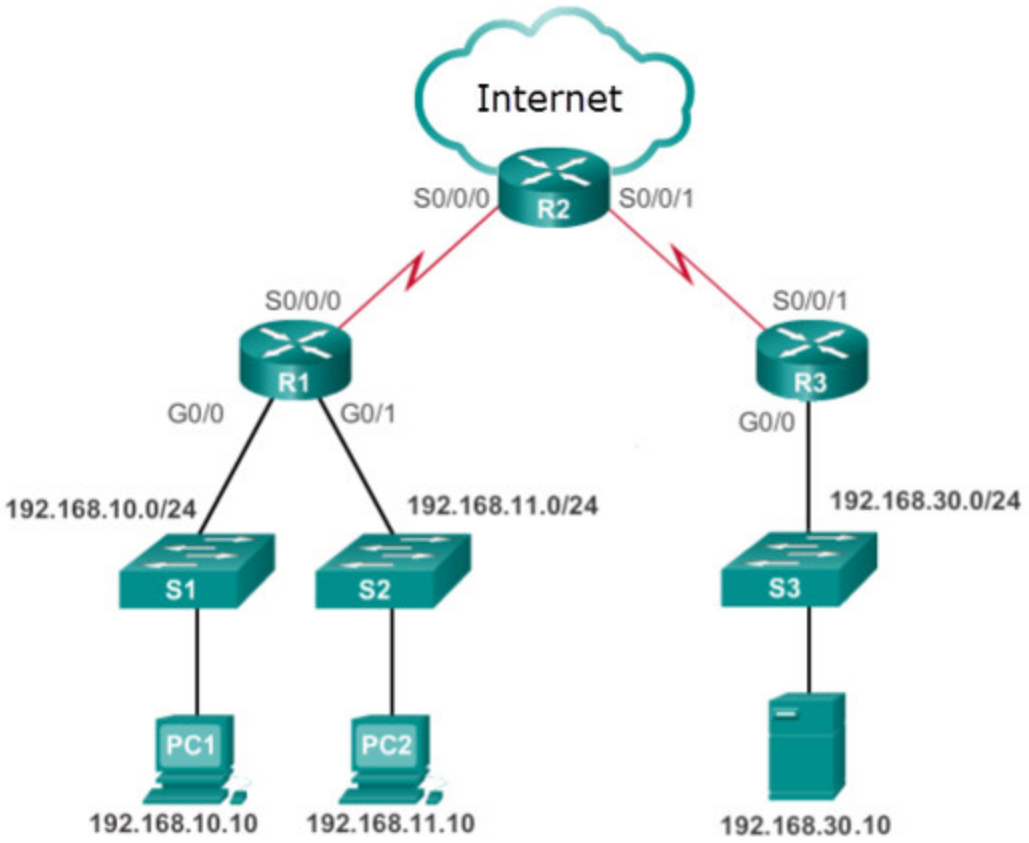
- **to restrict specific traffic access through an interface**
- to generate and send an informational message whenever the ACE is matched

70. Refer to the exhibit. Only authorized remote users are allowed remote access to the company server 192.168.30.10. What is the best ACL type and placement to use in this situation?



- extended ACLs inbound on R1 G0/0 and G0/1
- extended ACL outbound on R2 WAN interface towards the internet
- extended ACL inbound on R2 S0/0/0
- **extended ACL inbound on R2 WAN interface connected to the internet**

71. Refer to the exhibit. Employees on 192.168.11.0/24 work on critically sensitive information and are not allowed access off their network. What is the best ACL type and placement to use in this situation?



- standard ACL inbound on R1 vty lines
- extended ACL inbound on R1 G0/0
- **standard ACL inbound on R1 G0/1**
- extended ACL inbound on R3 S0/0/1

72. A technician is tasked with using ACLs to secure a router. When would the technician use the `host` configuration option or command?

- to add a text entry for documentation purposes
- to generate and send an informational message whenever the ACE is matched
- to identify any IP address
- **to identify one specific IP address**

73. What commonly motivates cybercriminals to attack networks as compared to hacktivists or state-sponsored hackers?

- **financial gain**
- political reasons
- fame seeking
- status among peers

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

Enterprise Networking, Security, and Automation (Version 7.00) – Network Security Exam PDF File