CompTIA CySA 1st edition Ciampa Test Bank

SKU: 9780357375464-TEST-BANK

Name:_____ Class:_____ Date:_____

Module 01: Applying Environmental Reconnaissance

Multiple Choice

1. Kendra has a very limited budget, but has three critical servers that she needs to secure against data breaches within her company's infrastructure. She knows that she won't be able to protect the entire network, but she has started searching for a solution to secure the most critical assets. Which of the following options would she most likely choose?

a. UTM appliance
b. NIPS
c. Proxy server
d. HIPS

ANSWER: d

FEEDBACK:

a. Incorrect. A unified threat management, or UTM, appliance is used to perform antivirus, spam filtering, and IDS/IPS functions within a single networked device. As such, it would be useful for an entire network or network segment, not just a few servers.
b. Incorrect.A network intrusion prevention system would meet all of the requirements listed in the scenario, except that it is network-based.
c. Incorrect.A proxy server can perform certain types of traffic filtering, but it is used at a network or network segment level and thus does not meet the requirements of the scenario.
d. Correct. A host intrusion prevention system is installed on individual hosts to detect an intrusion, log the event, alert administrators, and attempt to stop the intrusion. It is the only host-based solution described in the answer choices.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 6/17/2020 6:02 AM
DATE MODIFIED: 6/17/2020 6:05 AM

2. Talia has just been hired as the first security employee at an organization. Until this point, security has been everyone's responsibility, but she knows that the IT staff have different skill sets and may not be aware of certain weaknesses within various platforms. Which of the following tools might Talia use to help her determine the state of the existing infrastructure?

a. NIDS
b. Vulnerability scanner
c. OS fingerprinting
d. syslog

ANSWER: b

FEEDBACK:

a. Incorrect. A network intrusion detection system is a good tool to use, but before making any changes to the infrastructure, it would be a better idea to get an overall status update and determine where the weakest points are. From there, Talia could determine the best solutions for resolving any outstanding issues, prioritize which systems are most critical, and work within a budget to implement the changes.
b. Correct. A vulnerability scanner is a generic term for a range of products that look for different vulnerabilities, or weaknesses, within networks or systems. A comprehensive scan of the network and systems would be a good starting point before suggesting or implementing any new technologies or changes.
c. Incorrect. OS fingerprinting is a type of network scan that determines which operating

Copyright Cengage Learning. Powered by Cognero.

CompTIA CySA 1st edition Ciampa Test Bank

system(s) are running. This scan should be incorporated as a part of comprehensive vulnerability scanning.

d. Incorrect. Syslog is a universal standard for system messages, and Talia would be well served to review the log files on various devices. However, manual log analysis could be a very time-consuming process across an unknown number of servers or systems. The right vulnerability scanner can be configured to scan an entire network or network segment and detect any vulnerabilities that might exist.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 6/17/2020 6:06 AM
DATE MODIFIED: 6/17/2020 6:07 AM

3. Malik has received a call from an employee about suspicious activity on her computer. He's not sure if it's being controlled remotely or if any other remote network connections are contributing to this issue. Which of the following tools might he initially use as part of his investigation?

a. netstat
b. ping
c. traceroute
d. nslookup

ANSWER: a
FEEDBACK:

a. Correct. The netstat command can be used to show current network connections on a computer. From there, Malik can look up information on the IP addresses to determine where the traffic is coming from.

b. Incorrect. The ping command might be used with the results of the netstat command, but until Malik has a list of active network connections, he won't have a target or destination IP address to ping.

c. Incorrect. The traceroute command might be used with the results of the netstat command, but until Malik has a list of active network connections, he won't have a target or destination IP address to use.

d. Incorrect. The nslookup command is used to look up DNS records. It would not be useful to determine a list of active network connections with remote networks.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 6/17/2020 6:07 AM
DATE MODIFIED: 6/17/2020 6:09 AM

4. Tobias has just installed Linux on a virtual machine in his company's data center. However, he isn't sure whether the image he installed from automatically has an SMTP server running. Which of the following tools might he use to verify whether an SMTP server package is running?

a. nmap
b. nslookup
c. Vulnerability scanner
d. NIDS

Copyright Cengage Learning. Powered by Cognero.

CompTIA CySA 1st edition Ciampa Test Bank

Module 01: Applying Environmental Reconnaissance

ANSWER: a

FEEDBACK:

a. Correct. The nmap program can perform a port scan on a host or multiple hosts by using the FQDN, IP address, or IP address range. The port scan should return information about the logical ports that are responding to network requests.

b. Incorrect. The nslookup tool is used to look up DNS information. Even if DNS entries for mail are set to forward to the new server, that still doesn't confirm whether an active SMTP service or package is running.

c. Incorrect. A vulnerability scanner is looking for weaknesses or vulnerabilities within a network or on a host. While an SMTP server may be misconfigured or might be set as an open SMTP relay, simply having an SMTP server is not necessarily a vulnerability by itself.

d. Incorrect. A network intrusion detection system is meant to analyze traffic on a network and determine when an intrusion or data breach has occurred. It does not scan the network or hosts and report on services running on these systems.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 6/17/2020 6:09 AM
DATE MODIFIED: 6/17/2020 6:47 AM

5. Kevin must manually review the events that occur on a number of network devices to determine whether systems are running normally. He discovers that systems are available that can act as a centralized repository and perform much of the analysis for him. Which of the following might be used to collect events in a centralized location for analysis?

a. netstat
b. syslog
c. Phishing
d. DNS harvesting

ANSWER: b

FEEDBACK:

a. Incorrect. The netstat program can be used to show a variety of network statistics for a system. However, it is not used for log and event collection into a centralized repository for analysis.

b. Correct. Syslog is a universal standard for system messages. Events from a number of systems can be combined into a single repository for analysis and correlation.

c. Incorrect. Phishing is a form of social engineering and is not used for log collection and analysis.

d. Incorrect. DNS harvesting is a reconnaissance method in which DNS servers are queried to discover the systems and servers that exist within an organization.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 6/17/2020 6:11 AM
DATE MODIFIED: 6/17/2020 6:13 AM

6. Cheyenne is concerned about a recent news story that global data breaches are on the rise. She believes that she has installed the latest detection software on all of the servers she is responsible for, but she knows that security requires a

Copyright Cengage Learning. Powered by Cognero.

CompTIA CySA 1st edition Ciampa Test Bank

layered approach. Which of the following might she also decide to implement?

a. Proxy server
b. Spam filter
c. HIPS
d. NIPS

ANSWER: d

FEEDBACK:

a. Incorrect. A proxy server can provide caching and filtering services, but it doesn't detect and stop data breaches.
b. Incorrect. A spam filter examines emails as they arrive to determine whether they are legitimate. Illegitimate emails are flagged and prevented from being delivered to the user's inbox.
c. Incorrect. A host intrusion prevention system protects individual hosts on the network by detecting intrusions and stopping the traffic. However, the host layer is already covered with the detection software mentioned in the scenario.
d. Correct. A network intrusion prevention system provides protection from data breaches at the network level. A NIPS looks at traffic before it gets to the hosts rather than examining it once the data arrives.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 6/17/2020 6:13 AM
DATE MODIFIED: 6/17/2020 6:15 AM

7. Vince wants to configure a firewall on the perimeter of his organization's network to block all unsolicited incoming traffic. However, he still needs servers behind the firewall to be able to access the Internet for patching purposes. Which of the following types of firewalls might he decide to install?

a. Stateless firewall
b. Web application firewall
c. Stateful firewall
d. Portless firewall

ANSWER: c

FEEDBACK:

a. Incorrect. A stateless firewall doesn't care whether there is an existing connection before forwarding traffic. Thus, the return traffic would not be allowed.
b. Incorrect. A web application firewall may be stateful or stateless. This scenario would more specifically require a stateful firewall to be installed.
c. Correct. A stateful firewall determines if there is an existing connection before deciding whether to forward traffic. In this scenario, the server could reach out to the Internet for information, which would be allowed to come back because of the connection the server established.
d. Incorrect. There is no such thing as a portless firewall.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 6/17/2020 6:15 AM

Copyright Cengage Learning. Powered by Cognero.

CompTIA CySA 1st edition Ciampa Test Bank

Module 01: Applying Environmental Reconnaissance

DATE MODIFIED: 6/17/2020 6:16 AM

8. Peter has just been hired as a network engineer and has recently been examining the company's core router configuration. He notices that the current configuration would allow an incoming packet from the Internet to have a source IP address within the 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16 address space. Which of the following should Peter do?

a. Create a rule on the switches that connect to the router to discard any traffic with those addresses in the source IP field.
b. Modify the ACL on the router to prevent the traffic from transferring to the internal network from the Internet for those addresses.
c. Replace the router with a stateless firewall.
d. Nothing. The router configuration is correct.

ANSWER: b

FEEDBACK:

a. Incorrect. Most switches do not examine Layer 3 headers of traffic, and thus could not discard or block the offending traffic.
b. Correct. The access control list on the router can work like a firewall, allowing or disallowing certain types of traffic based upon source or destination IP addresses. Anytime traffic is coming in from the Internet, it should have a public IP address as the source IP address.
c. Incorrect. Routers can perform certain functions that firewalls perform, but firewalls do not perform routing functions, regardless of whether they are stateful or stateless.
d. Incorrect. Peter should ensure that incoming traffic from the Internet is discarded or blocked if it contains a source IP address that is reserved as a private address, as defined by RFC 1918.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 6/17/2020 6:17 AM
DATE MODIFIED: 6/17/2020 6:18 AM

9. Terry and Alex have been hired as consultants to determine the security posture of an organization. They have written a custom tool that will crawl social media networks and other popular sites looking for certain pieces of valuable information they can use as part of an attack. Which of the following is this tool most likely used for?

a. DNS harvesting
b. MAC address harvesting
c. Email harvesting
d. IP address harvesting

ANSWER: c

FEEDBACK:

a. Incorrect. DNS harvesting would be performed by querying the DNS servers used by the company, not social media networks.
b. Incorrect. MAC addresses are not typically shared on social media networks.
c. Correct. Email harvesting is the process of collecting as many valid email addresses as possible by scraping data from social media and other websites where the information is freely posted.
d. Incorrect. IP addresses are not typically shared on social media networks.

Copyright Cengage Learning. Powered by Cognero.

CompTIA CySA 1st edition Ciampa Test Bank

Module 01: Applying Environmental Reconnaissance

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 6/17/2020 6:18 AM
DATE MODIFIED: 6/17/2020 6:19 AM

10. Louise has been asked to provide a report to management that contains a list of insecure traffic types coming into the company's network from the Internet. Which of the following tools might she use to collect this information?

a. Packet analyzer
b. nmap
c. netstat
d. nslookup

ANSWER: a
FEEDBACK:

a. Correct. A packet analyzer, such as Wireshark, can be used to capture and log traffic moving across a network for further analysis and aggregation. In this case, a filter can be applied to look for any HTTP, FTP, Telnet, or other packets where insecure protocols are in use.
b. Incorrect. The nmap command can be used for such things as port scanning, but it does not capture and analyze traffic. A packet analyzer can even show the packets being sent and received by nmap, but it does not use the nmap command itself.
c. Incorrect. The netstat command is used on hosts to show various types of network statistics, such as open and active connections. It is not used at a network level to determine which types of traffic are coming into the network.
d. Incorrect. The nslookup command is used to query records from a nameserver. It is not used to analyze traffic on a network.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 6/17/2020 6:20 AM
DATE MODIFIED: 6/17/2020 6:21 AM

11. Marco has been hired as a penetration tester by a large organization. He has managed to exploit a vulnerability in the perimeter firewall. Which of the following tools might help him discover what other resources exist within the organization's network?

a. nslookup
b. Untidy
c. traceroute
d. netstat

ANSWER: a
FEEDBACK:

a. Correct. The nslookup command is available across a variety of platforms to query DNS servers for records that contain name-to-IP address mappings.
b. Incorrect. Untidy is an XML fuzzing tool. It is not used for discovery of other network resources.
c. Incorrect. The traceroute command is used to determine the path between the source and destination. It is not used to query DNS servers that contain the records of name-to-IP

Copyright Cengage Learning. Powered by Cognero.

CompTIA CySA 1st edition Ciampa Test Bank

address mappings.

d. Incorrect.If Marco has exploited a system beyond the perimeter firewall, the netstat command could be used. At this point, there is not enough information to determine whether he can send packets within the network or has managed to exploit one of the network servers.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 6/17/2020 6:22 AM
DATE MODIFIED: 6/17/2020 6:23 AM

12. Which of the following tools most likely generated the following output?

1 216.182.226.94 (216.182.226.94) 12.594 ms 216.182.226.146 (216.182.226.146) 15.121 ms 216.182.226.134 (216.182.226.134) 21.772 ms
2 100.66.8.14 (100.66.8.14) 21.115 ms 100.66.32.216 (100.66.32.216) 5.539 ms 100.66.8.248 (100.66.8.248) 20.062 ms
3 100.66.34.250 (100.66.34.250) 11.830 ms 100.66.11.164 (100.66.11.164) 15.988 ms 100.66.11.204 (100.66.11.204) 17.247 ms
4 100.66.7.189 (100.66.7.189) 16.971 ms 100.66.7.149 (100.66.7.149) 22.494 ms 100.66.6.81 (100.66.6.81) 16.582 ms
5 100.66.5.191 (100.66.5.191) 12.744 ms 100.66.5.41 (100.66.5.41) 16.752 ms 100.66.5.23 (100.66.5.23) 21.620 ms
6 100.65.15.193 (100.65.15.193) 0.876 ms 100.65.13.97 (100.65.13.97) 0.322 ms 100.66.5.71 (100.66.5.71) 15.611 ms
7 52.93.28.253 (52.93.28.253) 0.357 ms 52.93.28.243 (52.93.28.243) 0.497 ms 52.93.29.3 (52.93.29.3) 0.500 ms
8 100.100.2.32 (100.100.2.32) 3.957 ms 100.100.2.40 (100.100.2.40) 0.398 ms 100.100.2.32 (100.100.2.32) 0.664 ms
9 99.82.181.25 (99.82.181.25) 0.977 ms 100.100.2.44 (100.100.2.44) 0.705 ms 99.82.181.25 (99.82.181.25) 0.802 ms
10 * * *
11 * 216.239.58.30 (216.239.58.30) 0.718 ms 108.170.228.150 (108.170.228.150) 1.135 ms
12 74.125.37.221 (74.125.37.221) 1.445 ms 108.170.246.49 (108.170.246.49) 1.304 ms 108.170.246.66 (108.170.246.66) 1.546 ms
13 iad30s24-in-f14.1e100.net (172.217.164.142) 0.899 ms 216.239.63.235 (216.239.63.235) 2.164 ms 2.005 ms

a. ping
b. traceroute
c. netstat
d. nmap

ANSWER: b

FEEDBACK:

a. Incorrect. The ping command is used to send an ICMP echo request to a destination, which should respondwith an ICMP echo reply to determine the round-trip time. In this scenario, 13 hosts are shown—the result of a traceroute command from a Linux server.

b. Correct. The traceroute command is used on Linux, UNIX, Mac, Cisco, and other devices to show the hops, or routers, that a network transmission is sent across. In this scenario, a traceroute was performed from a virtual machine residing on Amazon Web Services to google.com.

c. Incorrect. The netstat command can provide various types of network statistics, but it is not used to display the route that traffic takes from source to destination.

d. Incorrect. The nmap command is used to display ports and services that are responding on a host. In this output, there are no port numbers displayed.

POINTS: 1

Copyright Cengage Learning. Powered by Cognero.

CompTIA CySA 1st edition Ciampa Test Bank

Module 01: Applying Environmental Reconnaissance

QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 6/17/2020 6:23 AM
DATE MODIFIED: 6/17/2020 6:25 AM

13. Rudyard has heard rumors that an employee has set up an FTP server at his house. The server issaid to be running on port 80, as ports 20 and 21 are blocked on the company's firewall. He knows that the firewall doesn't perform any sort of packet inspection to ensure that only HTTP traffic is being transmitted. Which of the following tools might he use in conjunction with port mirroring on the switch to monitor the user's traffic and search for signs of FTP traffic being sent on port 80?

a. Peach Fuzzer
b. Check Point
c. Metasploit
d. Wireshark

ANSWER: d

FEEDBACK:

a. Incorrect. Peach Fuzzer is a type of fuzzing tool. Fuzzing tools send a variety of data to an application so that the replies, or results, of the request can be analyzed for vulnerabilities or disclosure of confidential information.
b. Incorrect. Check Point is a manufacturer of firewalls.
c. Incorrect. Metasploit is an exploitation framework. While it does have remote packet capture capabilities, Wireshark is the better answer here.
d. Correct. Wireshark is a packet sniffer that can capture the packets being transmitted across a network. Rudyard could set up port mirroring on a switch to copy all traffic from the user's switch port to a system running Wireshark so that the traffic can be analyzed for improper usage.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 6/17/2020 6:26 AM
DATE MODIFIED: 6/17/2020 6:31 AM

14. Tito has logged into a Linux server that has just had a secondary NIC installed. Which of the following commands would he use as part of the next steps to connect the server to an out-of-band management network?

a. top
b. ipconfig
c. ifconfig
d. niconfig

ANSWER: c

FEEDBACK:

a. Incorrect. The top command is used to display running processes on Linux. It is not used to display interface configuration and status.
b. Incorrect. The ipconfig command is used in Windows to show the current IP addresses assigned to network interfaces.
c. Correct. The ifconfig command is used in Linux to display or change the interface configuration. On some newer distributions of Linux, the ifconfig command has been replaced by the ip command, though the older ifconfig command can still be installed

Copyright Cengage Learning. Powered by Cognero.

CompTIA CySA 1st edition Ciampa Test Bank

via the net-tools package.

d. Incorrect. Niconfig is not a command in the Linux operating system.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 6/17/2020 6:31 AM
DATE MODIFIED: 6/17/2020 6:34 AM

15. Jorge is reviewing the firewall logs and sees 28 echo requests leaving the network and ICMP echo replies coming back over the course of a five-minute period. Which of the following is most likely the cause of this traffic?

a. Users are streaming multimedia from a popular video-sharing website.

b. This is standard voice-over-IP traffic and is no cause for concern.

c. These are authentication requests for single sign-on using federation with large websites.

d. Someone has run multiple ping tests from the network to an outside address.

ANSWER: d

FEEDBACK:

a. Incorrect. ICMP is commonly used by ping and tracert/traceroute to determine round-trip times. It is not a multimedia streaming protocol such as RTMP.

b. Incorrect. A number of protocols can be used in VoIP connections, but ICMP is not used for that purpose.

c. Incorrect. ICMP is not used for authentication.

d. Correct. With both ping and tracert/traceroute, an ICMP echo request is sent to a particular host address. Assuming that ICMP isn't blocked at the firewall, the host will respond with an ICMP echo reply.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 6/17/2020 6:34 AM
DATE MODIFIED: 6/17/2020 6:36 AM

Copyright Cengage Learning. Powered by Cognero.

CompTIA CySA 1st edition Ciampa Test Bank