Exam Report: 2.5.4 Practice Questions

Date: 1/13/2020 1:11:02 pm
Time Spent: 2:24

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 100%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

▼ **Question 1:** Correct

Which of the following accurately describes what a protocol analyzer is used for? (Select two.)

□ A device that measures the amount of data that can be transferred through a network or processed by a device.

➡ ☑ A device that does **not** allow you to capture, modify, and retransmit frames (to perform an attack).

□ A device that can simulate a large number of client connections to a website, test file downloads for an FTP site, or simulate large volumes of email.

➡ ☑ A passive device that is used to copy frames and allow you to view frame contents.

□ A device that allows you to capture, modify, and retransmit frames (to perform an attack).

Explanation

A protocol analyzer is a passive device that copies frames and allows you to view frame contents, but does not allow you to capture, modify, and retransmit frames (activities that are used to perform an attack).

A load tester simulates a load on a server or service. For example, the load tester might simulate a large number of client connections to a website, test file downloads for an FTP site, or simulate large volumes of email. A throughput tester measures the amount of data that can be transferred through a network or processed by a device.

References

LabSim for Security Pro, Section 2.5.
[All Questions SecPro2017_v6.exm NET_MON_02]

▼ **Question 2:** Correct

You want to examine the data on your network to find out if any of the following are happening:

- Users are connecting to unauthorized websites
- Cleartext passwords are allowed by protocols or services
- Unencrypted traffic that contains sensitive data is on the network

Which of the following tools would you use?

➡ ● Protocol analyzer

○ Load tester

○ Throughput tester

○ System logging

Explanation

A protocol analyzer is a special type of packet sniffer that captures transmitted frames. A protocol analyzer is a passive device that copies frames and allows you to view frame contents, but does not allow you to capture, modify, and retransmit frames (activities that are used to perform an attack). A protocol analyzer can be used to check network traffic for many issues, including:

- Identifying users that are connecting to unauthorized websites
- Discovering cleartext passwords allowed by protocols or services
- Identifying unencrypted traffic that includes sensitive data

References

LabSim for Security Pro, Section 2.5.
[All Questions SecPro2017_v6.exm NET_MON_05]

▼ **Question 3:** Correct

Which of the following tools would you use to simulate a large number of client connections to a website, test file downloads for an FTP site, or simulate large volumes of email?

○ Protocol analyzer

○ Packet sniffer

○ Throughput tester

➡ ● Load tester

Explanation

A load tester simulates a load on a server or service. For example, the load tester might simulate a large number of client connections to a website, test file downloads for an FTP site, or simulate large volumes of email. Use a load tester to make sure that a system has sufficient capacity for expected loads. Load testers can even estimate failure points, where the load is more than the system can handle.

References

LabSim for Security Pro, Section 2.5.
[All Questions SecPro2017_v6.exm NET_MON_03]

▼ **Question 4:** Correct

Which of the following tools would you use to validate the bandwidth on your network and identify when the bandwidth is significantly below what it should be?

○ Packet sniffer

➡ ● Throughput tester

○ Load tester

○ Protocol analyzer

Explanation

A throughput tester measures the amount of data that can be transferred through a network or processed by a device (such as the amount of data that can be retrieved from a disk in a specific period of time). On a network, a throughput tester sends a specific amount of data through the network and measures the time it takes to transfer that data, creating a measurement of the actual bandwidth. Use a throughput tester to validate the bandwidth on your network and identify when the bandwidth is significantly below what it should be. A throughput tester can help you identify when a network is slow, but will not give you sufficient information to identify why it is slow.

References

LabSim for Security Pro, Section 2.5.
[All Questions SecPro2017_v6.exm NET_MON_04]

▼ **Question 5:** Correct

You are running a packet sniffer on your workstation so you can identify the types of traffic on your

network. You expect to see all the traffic on the network, but the packet sniffer only seems to be capturing frames that are addressed to the network interface on your workstation.
Which of the following must you configure in order to see all of the network traffic?

○ Configure the network interface to use protocol analysis mode

○ Configure the network interface to enable logging

○ Configure the network interface to use port mirroring mode

➡ ● Configure the network interface to use promiscuous mode

Explanation

Configure the network interface to use promiscuous mode. By default, a NIC will only accept frames addressed to itself. To enable the packet sniffer to capture frames sent to other devices, configure the NIC in promiscuous mode (sometimes called p-mode). In p-mode, the NIC will process every frame it sees.

References

LabSim for Security Pro, Section 2.5.
[All Questions SecPro2017_v6.exm NET_MON_01]