Exam Report: 6.10.4 Practice Questions

Date: 1/22/2020 9:02:27 am
Time Spent: 6:37

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 88%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

You want to identify traffic that is generated and sent through the network by a specific application running on a device.

Which tool should you use?

- Protocol analyzer
- Certifier
- Multimeter
- Toner probe
- TDR

Explanation

Use a protocol analyzer (also called a packet sniffer) to examine network traffic. You can capture or filter packets from a specific device or packets that use a specific protocol.

Use a time domain reflector (TDR) to measure the length of a cable or to identify the location of a fault in the cable. A *toner probe* is two devices used together to trace the end of a wire from a known endpoint into the termination point in the wiring closet. A cable *certifier* is a multi-function tool that verifies that a cable or an installation meets the requirements for a specific architecture implementation. A *multimeter* is a device that tests various electrical properties, such as voltage, amps, and ohms.

References

LabSim for Security Pro, Section 6.10.
[All Questions SecPro2017_v6.exm PROT_ANLYZ_01]

Question 2: Correct

You want to know which protocols are being used on your network. You'd like to monitor network traffic and sort traffic by protocol.

Which tool should you use?

- IPS
- Throughput tester
- IDS
- Port scanner
- Packet sniffer

Explanation

A *packet sniffer* is special software that captures (records) frames that are transmitted on the network. Use a packet sniffer to:

- Identify the types of traffic on a network.
- View the exchange of packets between communicating devices. For example, you can capture frames related to DNS and view the exact exchange of packets for a specific name resolution request.
- Analyze packets sent to and from a specific device.
- View packet contents.

Use a port scanner to identify protocol ports that are opened in a firewall or active on a device. A port scanner checks individual systems, while a packet sniffer watches traffic on the network. 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 disk in a specific period of time).

An intrusion detection system (IDS) is a special network device that can detect attacks and suspicious activity. A *passive* IDS monitors, logs, and detects security breaches, but takes no action to stop or prevent the attack. An *active* IDS (also called an *intrusion protection system* or IPS) performs the functions of an IDS, but can also react when security breaches occur.

References

LabSim for Security Pro, Section 6.10.
[All Questions SecPro2017_v6.exm PROT_ANLYZ_02]

Question 3: Correct

You want to use a tool to see packets on a network, including the source and destination of each packet. Which tool should you use?

- Nessus
- Wireshark
- OVAL
- Nmap

Explanation

A *protocol analyzer*, also called a *packet sniffer*, is special software that captures (records) frames that are transmitted on the network. A protocol analyzer is a passive device. It 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). Wireshark is a popular protocol analyzer.

Nmap is a tool that performs ping scans (finding devices on the network) as well as port scans (looking for open ports on the network).

Nessus is a vulnerability scanning tool. While a protocol analyzer looks at packets on the network, a vulnerability scanner looks for weaknesses in systems, including open ports, running services, and missing patches. The Open Vulnerability and Assessment Language (OVAL) is an international standard for testing, analyzing, and reporting a system's security vulnerabilities.

References

LabSim for Security Pro, Section 6.10.
[All Questions SecPro2017_v6.exm PROT_ANLYZ_03]

Question 4: Correct

You have a small network of devices connected using a switch. You want to capture the traffic that is sent from Host A to Host B.

On Host C, you install a packet sniffer that captures network traffic. After running the packet sniffer, you cannot find any captured packets between Host A and Host B.

What should you do?

- Configure the default gateway address on hosts A and B with the IP address of Host C
- Connect hosts A and B together on the same switch port through a hub

Configure port mirroring

Manually set the MAC address of Host C to the MAC address of Host A

Explanation

You need to configure port mirroring on the switch. In a network that uses a switch, network traffic is sent through the switch to only the destination device. In this scenario, Host C will only receive broadcast traffic and traffic addressed to its own MAC address. With port mirroring, all frames sent to all other switch ports will be forwarded on the mirrored port.

Alternatively, you could put Host C on the same switch port as either Host A or Host B using a hub. All devices connected to the hub will be able to see the traffic sent to all other devices connected to the hub.

Changing the MAC address on Host C would cause a conflict with duplicate addresses being used. Setting the default gateway would not affect the path of packets on the LAN. The default gateway is only used for traffic that goes outside of the current subnet.

References

LabSim for Security Pro, Section 6.10.
[All Questions SecPro2017_v6.exm PROT_ANLYZ_04]

Question 5: Correct

You are concerned about attacks directed against the firewall on your network. You would like to examine the content of individual frames sent to the firewall.

Which tool should you use?

Packet sniffer

System log

Load tester

Event log

Throughput tester

Explanation

A *packet sniffer* is special software that captures frames transmitted on the network. Use a packet sniffer to:

- View packet contents.
- Identify the types of traffic on a network.
- View the exchange of packets between communicating devices. For example, you can capture frames related to DNS and view the exact exchange of packets for a specific name resolution request.
- Analyze packets sent to and from a specific device.

A *load tester* simulates a load on a server or service. 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 disk in a specific period of time). System and event logs record what has happened on a device, but do not record individual frames or packets.

References

LabSim for Security Pro, Section 6.10.
[All Questions SecPro2017_v6.exm PROT_ANLYZ_05]

Question 6: Correct

You decide to use a packet sniffer to identify the type of traffic sent to a router. You run the packet sniffing software on a device, which is connected to the same hub that is connected to the router.

When you run the software, you only see frames addressed to the workstation, not to other devices.

Which feature should you configure?

Mirroring

Promiscuous mode

Bonding

Spanning tree

Explanation

By default, a NIC only accepts frames addressed to that NIC. 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.

When devices are connected to a switch, the switch only forwards frames to the destination port. To see frames addressed to any device on any port, use port mirroring. In this scenario, the workstation and the router are connected with a hub, so the hub already sends all packets for all devices to all ports.

Bonding logically groups two or more network adapters to be used at the same time for a single logical network connection. Spanning tree runs on a switch and ensures that there is only one active path between switches, allowing backup redundant paths.

References

LabSim for Security Pro, Section 6.10.
[All Questions SecPro2017_v6.exm PROT_ANLYZ_06]

Question 7: Incorrect

You decide to use a packet sniffer to identify the type of traffic sent to a router. You run the packet sniffing software on a device that is connected to a hub with three other computers. The hub is connected to the same switch that is connected to the router.

When you run the software, you see frames addressed to the four workstations, but not to the router.

Which feature should you configure?

Mirroring

~~Promiscuous mode~~

Bonding

Spanning tree

Explanation

A switch will only forward packets to the switch port that holds a destination device. This means that when your packet sniffer is connected to a switch port, it will not see traffic sent to other switch ports. To configure the switch to send all frames to the packet sniffing device, configure *port mirroring* on the switch. With port mirroring, all frames sent to all other switch ports will be forwarded on the mirrored port.

Promiscuous mode configures a network adapter to process every frame it sees, not just the frames addressed to that network adapter. In this scenario, you know that the packet sniffer is running in promiscuous mode because it can already see frames sent to other devices.

Bonding logically groups two or more network adapters to be used at the same time for a single logical network connection. Spanning tree runs on a switch and ensures that there is only one active path between switches, allowing for backup redundant paths.

References

LabSim for Security Pro, Section 6.10.
[All Questions SecPro2017_v6.exm PROT_ANLYZ_07]

Question 8: Correct

You have recently reconfigured FTP to require encryption of both passwords and data transfers. You would like to check network traffic to verify that all FTP passwords and data are encrypted.

Which tool should you use?

Systems monitor

- Protocol analyzer
- Vulnerability scanner
- Performance monitor

Explanation

Use a protocol analyzer to examine network traffic. With the protocol analyzer, you can examine the contents of each packet. Plaintext communications can be read using the protocol analyzer, while encrypted packets cannot.

Use a performance monitor or system monitor tool to gather statistics about system and network performance and loads. Use a vulnerability scanner to check systems for vulnerabilities. A vulnerability scanner might reveal that FTP is configured to accept clear text communications, but it does not examine the actual packets sent on the network.

References

LabSim for Security Pro, Section 6.10.
[All Questions SecPro2017_v6.exm PROT_ANLYZ_08]