Exam Report: 15.6.8 Practice Questions

Date: 12/6/2019 5:35:07 pm
Time Spent: 9:11

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 33%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

You are concerned about attacks directed at 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
- Load tester
- System log
- Throughput tester
- Event log

Explanation

A packet sniffer is special software that captures (records) frames that are 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 a 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 Network Pro, Section 15.6.
[netpro18v5_all_questions_en.exm NP09_4-4 #MCS1]

Question 2: Incorrect

You have a website that customers use to view product information and place orders. You would like to identify the maximum number of simultaneous sessions that this server can maintain before performance is negatively impacted.

Which tool should you use?

- System log
- Load tester
- ~~Throughput tester~~
- Baseline

- Packet sniffer

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, and even to estimate a failure point where the load is more than the system can handle.

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). A packet sniffer is special software that captures (records) frames that are transmitted on the network.

A baseline is a snapshot of past performance statistics of the network or devices. A system log identifies events or actions performed on a device.

References

LabSim for Network Pro, Section 15.6.
[netpro18v5_all_questions_en.exm NP09_4-4 #MCS2]

Question 3: 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 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 other devices.

Which feature should you configure?

- Promiscuous mode
- ~~Mirroring~~
- Bonding
- Spanning tree

Explanation

By default, a NIC only accepts 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 processes every frame it sees.

When devices are connected to a switch, the switch will only forward 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 redundant paths.

References

LabSim for Network Pro, Section 15.6.
[netpro18v5_all_questions_en.exm NP09_4-4 #MCS4]

Question 4: 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
- Spanning tree
- Promiscuous mode
- ~~Bonding~~

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. Port mirroring makes it so 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 redundant paths.

References

LabSim for Network Pro, Section 15.6.
[netpro18v5_all_questions_en.exm NP09_4-4 #MCS5]

Question 5: Incorrect

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

Which tool should you use?

- IPS
- ~~Port scanner~~
- IDS
- Throughput tester
- 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 Network Pro, Section 15.6.
[netpro18v5_all_questions_en.exm NP09_5-2 #MCS1]

Question 6: Correct

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

Which tool should you use?

- Protocol analyzer
- TDR

- Certifier
- Multimeter
- Toner probe

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 use a specific protocol.

Use a time domain reflector (TDR) to measure the length of a cable or 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 or validates 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 Network Pro, Section 15.6.
[netpro18v5_all_questions_en.exm NP09_5-3 MCS10]

Question 7: Incorrect

You have heard about a Trojan horse program where the compromised system sends personal information to a remote attacker on a specific TCP port. You want to be able to easily tell whether any of your systems are sending data to the attacker.

Which log should you monitor?

- Security
- ~~Application~~
- Firewall
- System

Explanation

A firewall log identifies traffic that has been allowed or denied through a firewall. You can identify traffic types used by computers on your network by looking at the outgoing ports. For example, you can identify servers that are running a specific service, or you can see computers that are communicating using ports that might indicate malicious software.

A system log records operating system, system, and hardware events. A security log records information related to logons, such as incorrect passwords being used, and the use of user rights. An application log records actions performed by an application. For each of these logs, the Trojan horse program will likely be written in a way that little or no logging will be recorded by the program, so examining these logs will not give you much information about the program on a system.

References

LabSim for Network Pro, Section 15.6.
[netpro18v5_all_questions_en.exm SP08_4-6 2]

Question 8: Incorrect

You have a small network of devices connected together 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?

- Manually set the MAC address of Host C to the MAC address of Host A.
- ~~Connect hosts A and B together on the same switch port through a hub.~~
- Run the packet sniffer application on Host B.
-

Configure the default gateway address on hosts A and B with the IP address of Host C.

Explanation

You need to run the packet sniffing software on either Host A or Host B. Network traffic is sent through a switch to only the destination device. In this scenario, Host C will only receive broadcast traffic and traffic addressed to its own MAC address.

Alternatively, you could put Host C on the same switch port as either Host A or Host B using a hub. When connected with 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 Network Pro, Section 15.6.
[netpro18v5_all_questions_en.exm NP05_1-6 #347]

Question 9: Incorrect

Each of the following are tools used to check the health of a network.

Which of these is typically used for managing and sending messages from one computer system to another?

- ~~Packet sniffer~~
- syslog
- Protocol analyzer
- Load tester

Explanation

The syslog standard is used for managing and sending log messages from one computer system to another. It can analyze messages and notify administrators of problems or performance.

A packet sniffer is special software that captures (records) frames that are transmitted on the network. A protocol analyzer is a special type of packet sniffer that captures transmitted frames. A load tester simulates a load on a server or service.

References

LabSim for Network Pro, Section 15.6.
[netpro18v5_all_questions_en.exm *NP15_MONITORING_02]

Question 10: Incorrect

Which of the following are reasons to use a protocol analyzer? (Select two.)

- [ ] Identify users that are connecting to unauthorized websites.
- [x] ~~Simulate a large number of client connections to a website.~~
- [ ] Find devices that might be using legacy protocols, such as IPX/SPX or NetBIOS.
- [ ] Identify when a network is slow.
- [x] ~~Measure the amount of data that can be transferred through a network.~~

Explanation

A protocol analyzer is a device that copies frames and allows you to view frame contents. Use a protocol analyzer to:

- Find devices that might be using restricted protocols (such as ICMP) or legacy protocols (such as IPX/SPX or NetBIOS).
- Identify frames that might cause errors.
- Examine the data contained within a packet (for example, to identify users that are connecting to unauthorized websites).

• Troubleshoot communication problems or investigate the source of heavy network traffic.

Use a throughput tester to measure the amount of data that can be transmitted on a network, which can help you identify when a network is slow. A load tester can be used to simulate a large number of client connections to a website.

References

LabSim for Network Pro, Section 15.6.
[netpro18v5_all_questions_en.exm *NP15_MONITORING_01]

Question 11: Correct

You have a WAN link that connects two sites. The WAN link is supposed to provide 1.5 Mbps of bandwidth. You want to perform a test to see the actual bandwidth of the link.

Which tool should you use?

- (selected) Throughput tester
- Load tester
- Baseline
- Packet sniffer

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 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, arriving at a measure 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 baseline would tell you the average amount of data sent on the WAN link, but would not tell you the actual capacity or bandwidth for that link.

A load tester simulates a load on a server or service. A packet sniffer is special software that captures (records) frames that are transmitted on the network.

References

LabSim for Network Pro, Section 15.6.
[netpro18v5_all_questions_en.exm NP09_4-4 #MCS3]

Question 12: Incorrect

You have installed a new application on a network device. During testing, it appears as if the software is causing other services running on the device to stop responding.

Which tool should you consult to identify the problem?

- Throughput tester
- Load tester
- (selected) Application log
- (selected) ~~Packet sniffer~~

Explanation

Logs contain a record of events that have happened on a system. Logging capabilities are built into operating systems, services, and applications. Log entries are generated in response to configuration changes, changes in system state, or network condition variations.

A packet sniffer is special software that captures (records) frames that are transmitted on the network. 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).

References

LabSim for Network Pro, Section 15.6.
[netpro18v5_all_questions_en.exm NP09_4-4 #MCS6]

Question 13: Correct

You manage a firewall that connects your private network to the internet. You would like to see a record of every packet that has been rejected by the firewall in the past month.

Which tool should you use?

- Throughput tester
- Event log
- Packet sniffer
- Load tester

Explanation

Use the event logs to see a record of past events. Logging capabilities are built into operating systems, services, and applications. Log entries are generated in response to configuration changes or actions taken by the system. Depending on the device, there might be multiple logs with different names, so the exact log you consult might vary depending on the device.

A packet sniffer is special software that captures (records) frames that are transmitted on the network. A packet sniffer would tell you the frames and packets sent to the device, but would not identify the actions the firewall took in response to those packets.

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).

References

LabSim for Network Pro, Section 15.6.
[netpro18v5_all_questions_en.exm NP09_4-4 #MCS7]

Question 14: Incorrect

You suspect that your web server has been the target of a denial-of-service attack. You would like to view information about the number of connections to the server over the past three days.

Which log would you most likely examine?

- Performance
- ~~Security~~
- Firewall
- System

Explanation

A performance log records information about the use of system resources. For example, the performance log records processor, memory, disk, and network utilization. In addition, the performance log can record information related to the performance of a specific service, such as the number of connections to a web server. You might also find this information in an application log for the service.

A security log records information related to logons, such as incorrect passwords being used, and the use of user rights. A system log records operating system, system, and hardware events. A firewall log identifies traffic that has been allowed or denied through a firewall.

References

LabSim for Network Pro, Section 15.6.
[netpro18v5_all_questions_en.exm SP08_4-6 6]

Question 15: Correct

Which of the following functions can a port scanner provide?

- Automatically close open ports on the network.

- Testing virus definition design for false positives.
- Determining which ports are open on a network.
- Auditing IPsec encryption algorithm configuration.

Explanation

Port scanners can determine which TCP/UDP ports are open on a network . Many port scanners provide additional information, including the host operating system and version of any detected servers. Hackers use port scanners to gather valuable information about a target. System administrators should use the same tools for proactive penetration testing and to ensure compliance with all corporate security policies.

References

LabSim for Network Pro, Section 15.6.
[netpro18v5_all_questions_en.exm SP02_1-7 84]