Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 4/12/2022 9:13:50 pm • Time spent: 02:45

Score: 80% Passing Score: 80%

Question 1: ✔ Correct

You are using a protocol analyzer to capture network traffic. You want to only capture the frames coming from a specific IP address.

Which of the following can you use to simplify this process?

- Display filters
- Switch
- NIC
- Capture filters

EXPLANATION

A capture filter records only the frames identified by the filter. Frames that don't match the filter criteria are not captured.

A switch connects multiple computers together in a network. It is not used to capture specific frames.

A network interface card (NIC) is used to transmit and receive frames addressed to it. It is not used to capture specific frames.

A display filter shows only the frames that match the filter criteria. Frames that don't match the filter criteria are still captured, but are not shown.

REFERENCES

11.5.2 Protocol Analyzer Facts

q_prot_analyzers_filter_secp7.question.fex

Question 2: ✔ Correct

Which of the following processes identifies an operating system based on its response to different types of network traffic?

- Port scanning
- Fingerprinting
- Firewalking
- Social engineering

EXPLANATION

A hacker can use an analyzer to perform system fingerprinting. System fingerprinting identifies which operating system the system is running based on how it responds to different types of network traffic.

Port scanning pings every port on an external interface or attempts a connection in order to discover which ports are open and active, and which ones are not.

Firewalking uses the **traceroute** command to discover which services can pass through a firewall or router.

Social engineering exploits human nature to obtain information. A hacker often impersonates someone of authority and requests data.

REFERENCES

11.5.2 Protocol Analyzer Facts

q_prot_analyzers_finger_secp7.question.fex

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 that is connected to a hub with three other computers. The hub is connected to a 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 on the switch?

- Bonding
- Spanning Tree Protocol
- Port mirroring
- ~~Promiscuous mode~~

EXPLANATION

A switch only forwards packets to the switch port that holds a destination device. This means that when your packet sniffer is connected to a switch port, it does 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 are 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 together to be used at the same time for a single logical network connection.

Spanning Tree Protocol (STP) runs on a switch and ensures that there is only one active path between switches, allowing for backup-redundant paths.

REFERENCES

11.5.2 Protocol Analyzer Facts

q_prot_analyzers_mirroring_secp7.question.fex

Question 4: ✔ 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 promiscuous mode.
- Configure the network interface to enable logging.
- Configure the network interface to use port mirroring mode.
- Configure the network interface to use protocol analysis mode.

EXPLANATION

Configure the network interface to use promiscuous mode. 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.

REFERENCES

11.5.1 Protocol Analyzers

11.5.2 Protocol Analyzer Facts

11.5.3 Analyzing Network Traffic

q_prot_analyzers_output_01_secp7.question.fex

Question 5: ✔ Correct

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

- [ ] A device that allows you to capture, modify, and retransmit frames (to perform an attack).
- [x] A device that does NOT allow you to capture, modify, and retransmit frames (to perform an attack).
- [x] A passive device that is used to copy frames and allow you to view frame contents.
- [ ] 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 emails.
- [ ] A device that measures the amount of data that can be transferred through a network or processed by a device.

EXPLANATION

A protocol analyzer is a passive device that copies frames and allows you to view frame contents. However, it 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, a 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 emails. A throughput tester measures the amount of data that can be transferred through a network or processed by a device.

REFERENCES

11.5.1 Protocol Analyzers

11.5.2 Protocol Analyzer Facts

11.5.3 Analyzing Network Traffic

q_prot_analyzers_output_02_secp7.question.fex

Question 6: ✔ Correct

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

Which tool should you use?

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

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 architectural implementation. A multimeter is a device that tests various electrical properties, such as voltage, amps, and ohms.

REFERENCES

11.5.1 Protocol Analyzers

11.5.2 Protocol Analyzer Facts

11.5.3 Analyzing Network Traffic

q_prot_analyzers_output_03_secp7.question.fex

Question 7: ✔ 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?

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

EXPLANATION

A packet sniffer is special software that captures (records) frames that are transmitted on a 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 the domain name system (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 a disk in a specific period of time).

An IDS is a special network device that can detect attacks and suspicious activity. A passive IDS monitors, logs, and detects security breaches, but it 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 it can also react when security breaches occur.

REFERENCES

11.5.1 Protocol Analyzers

11.5.2 Protocol Analyzer Facts

11.5.3 Analyzing Network Traffic

q_prot_analyzers_sniffer_01_secp7.question.fex

Question 8: ✔ 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
- Throughput tester
- Event log
- System log
- Load 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 the domain name system 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. They do not record individual frames or packets.

REFERENCES

11.5.1 Protocol Analyzers

11.5.2 Protocol Analyzer Facts

11.5.3 Analyzing Network Traffic

q_prot_analyzers_sniffer_02_secp7.question.fex

Question 9: ✕ Incorrect

Which of the following roles would be MOST likely to use a protocol analyzer to identify frames that might cause errors?

- ~~Network administrator~~
- Malicious hacker
- Security operations team
- Standard user

EXPLANATION

The network SecOps team can use a protocol analyzer during a vulnerability assessment. The protocol analyzer can help the SecOps team to:

- Identify frames that might cause errors. For example, the network administrator can:
  - Determine which flags are set in a TCP handshake.
  - Detect any malformed or fragmented packets. This would indicate that someone is trying to get around the firewall.
- Discover passwords and other sensitive data being sent in cleartext.
- Find any open network ports that should not be open.

A network administrator can use a protocol analyzer to assist in the management of the network and employee usage. However, a network administrator would not be the most likely to use a protocol analyzer to identify frames that might cause errors.

A malicious hacker could use a protocol analyzer to identify frames that might cause errors, but they most likely would not use it for that purpose.

A standard user should not be using a protocol analyzer on a network for any reason.

REFERENCES

11.5.2 Protocol Analyzer Facts

q_prot_analyzers_soar_secp7.question.fex

Question 10: ✔ 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?

- Wireshark
- OVAL
- Nessus
- **nmap**

EXPLANATION

A protocol analyzer, also called a packet sniffer, is special software that captures (records) frames that are transmitted on a network. A protocol analyzer is a passive device. It copies frames and allows you to view frame contents, but it does not allow you to capture, modify, and retransmit frames (activities that are used to perform an attack). Wireshark is a popular protocol analyzer.

The **nmap** command 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.

Open Vulnerability and Assessment Language (OVAL) is an international standard for testing, analyzing, and reporting a system's security vulnerabilities.

REFERENCES

11.5.2 Protocol Analyzer Facts

q_prot_analyzers_wireshark_secp7.question.fex