Assessment Results **Item Feedback Report**

CCNA Cybersecurity Operations (Version 1.1) - CyberOps Chapter 7 Exam

Below is the feedback on items for which you did not receive full credit. Some interactive items may not display your response.

Subscore: Security.Security Fundamentals.Monitoring

1 What are two monitoring tools that capture network traffic and forward it to network monitoring devices? (Choose two.)

Correct Response	Your Response
	☑ SIEM
	☑ Wireshark
✓	□ SPAN
	□ SNMP
✓	□ network tap

A network tap is used to capture traffic for monitoring the network. The tap is typically a passive splitting device implemented inline on the network and forwards all traffic including physical layer errors to an analysis device. SPAN is a port mirroring technology supported on Cisco switches that enables the switch to copy frames and forward them to an analysis device.

This item references content from the following areas:

CCNA Cybersecurity Operations

- 7.1.1 Introduction to Network Monitoring

2 What network monitoring technology enables a switch to copy and forward traffic sent and received on multiple interfaces out another interface toward a network analysis device?

Correct Response	Your Response
	○ SNMP
	○ NetFlow
	● network tap
✓	○ port mirroring

When enabled on a switch, port mirroring copies frames sent and recieved by the switch and forwards them to another port, which has a analysis device attached.

This item references content from the following areas:

CCNA Cybersecurity Operations

- 7.1.1 Introduction to Network Monitoring

4 Which technology is an open source SIEM system?

Correct Response	Your Response
✓	○ ELK

○ StealWatch

○ Splunk

◉ Wireshark

There are many SIEM systems available to network administrators. The ELK suite is an open source option.

This item references content from the following areas:

CCNA Cybersecurity Operations

- 7.1.2 Introduction to Network Monitoring Tools

6 Which SIEM function is associated with speeding up detection of security threats by examining logs and events from different systems?

Correct Response	Your Response
	○ forensic analysis
	○ retention
	◉ aggregation
✓	○ correlation

The correlation function of SIEM speeds the detection and reaction to security threats by examining logs and events from different systems.

This item references content from the following areas:

CCNA Cybersecurity Operations

- 7.1.2 Introduction to Network Monitoring Tools

7 Which capability is provided by the aggregation function in SIEM?

Correct Response	Your Response
✓	○ reducing the volume of event data by consolidating duplicate event records
	◉ searching logs and event records of multiple sources for more complete forensic analysis
	○ presenting correlated and aggregated event data in real-time monitoring
	○ increasing speed of detection and reaction to security threats by examining logs from many systems and applications

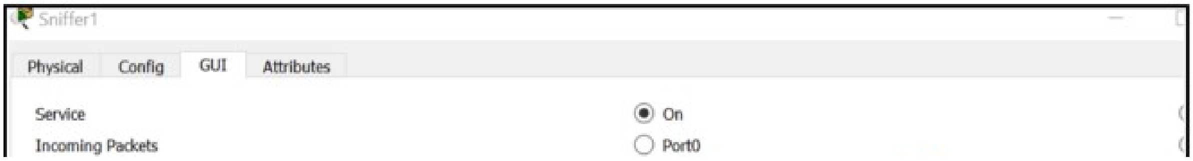
The aggregation function of SIEM reduces the volume of event data by consolidating duplicate event records.

This item references content from the following areas:

CCNA Cybersecurity Operations

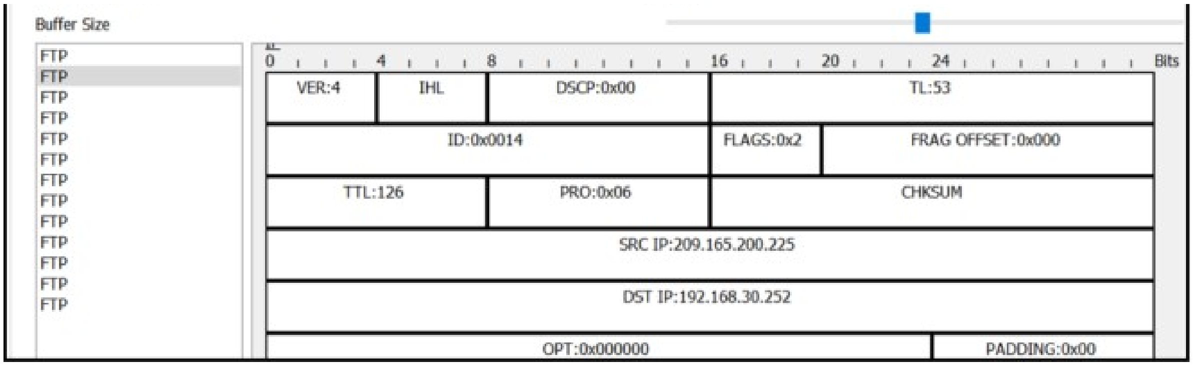
- 7.1.2 Introduction to Network Monitoring Tools

8



Service ● On

Incoming Packets ○ Port0



Buffer Size

FTP
FTP
FTP
FTP
FTP
FTP
FTP
FTP
FTP
FTP
FTP
FTP
FTP

VER:4	IHL	DSCP:0x00	TL:53
ID:0x0014		FLAGS:0x2	FRAG OFFSET:0x000
TTL:126	PRO:0x06	CHKSUM	
SRC IP:209.165.200.225			
DST IP:192.168.30.252			
OPT:0x000000			PADDING:0x00

Refer to the exhibit. A junior network administrator is inspecting the traffic flow of a particular server in order to make security recommendations to the departmental supervisor. Which recommendation should be made?

Correct Response **Your Response**

● The person accessing the server should never access it from a device using a private IP address.

○ The person accessing the server should use the private IP address of the server.

○ The total length (TL) field indicates an unsecure Layer 4 protocol is being used.

✓ ○ A more secure protocol should be used.

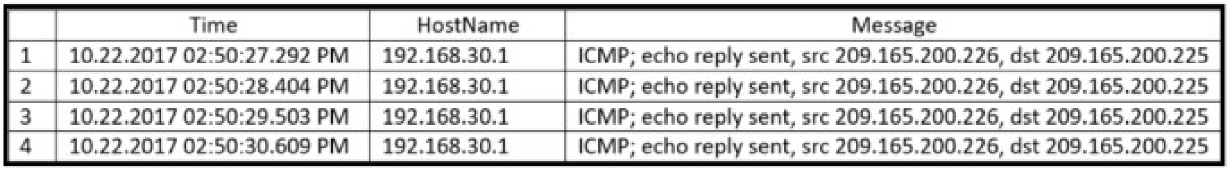
FTP is an unsecure network protocol. Anyone capturing packets can obtain the username and password from the capture. A more secure protocol such as SFTP should be used.

This item references content from the following areas:

CCNA Cybersecurity Operations

- 7.1.2 Introduction to Network Monitoring Tools

9



	Time	HostName	Message
1	10.22.2017 02:50:27.292 PM	192.168.30.1	ICMP; echo reply sent, src 209.165.200.226, dst 209.165.200.225
2	10.22.2017 02:50:28.404 PM	192.168.30.1	ICMP; echo reply sent, src 209.165.200.226, dst 209.165.200.225
3	10.22.2017 02:50:29.503 PM	192.168.30.1	ICMP; echo reply sent, src 209.165.200.226, dst 209.165.200.225
4	10.22.2017 02:50:30.609 PM	192.168.30.1	ICMP; echo reply sent, src 209.165.200.226, dst 209.165.200.225

Refer to the exhibit. What protocol would be used by the syslog server service to create this type of output for security purposes?

Correct Response **Your Response**

✓ ○ SNMP

○ AAA

● ICMP

○ NTP

The Simple Network Management Protocol is used by network devices to send and log messages to a syslog server in order to monitor traffic and network device events.

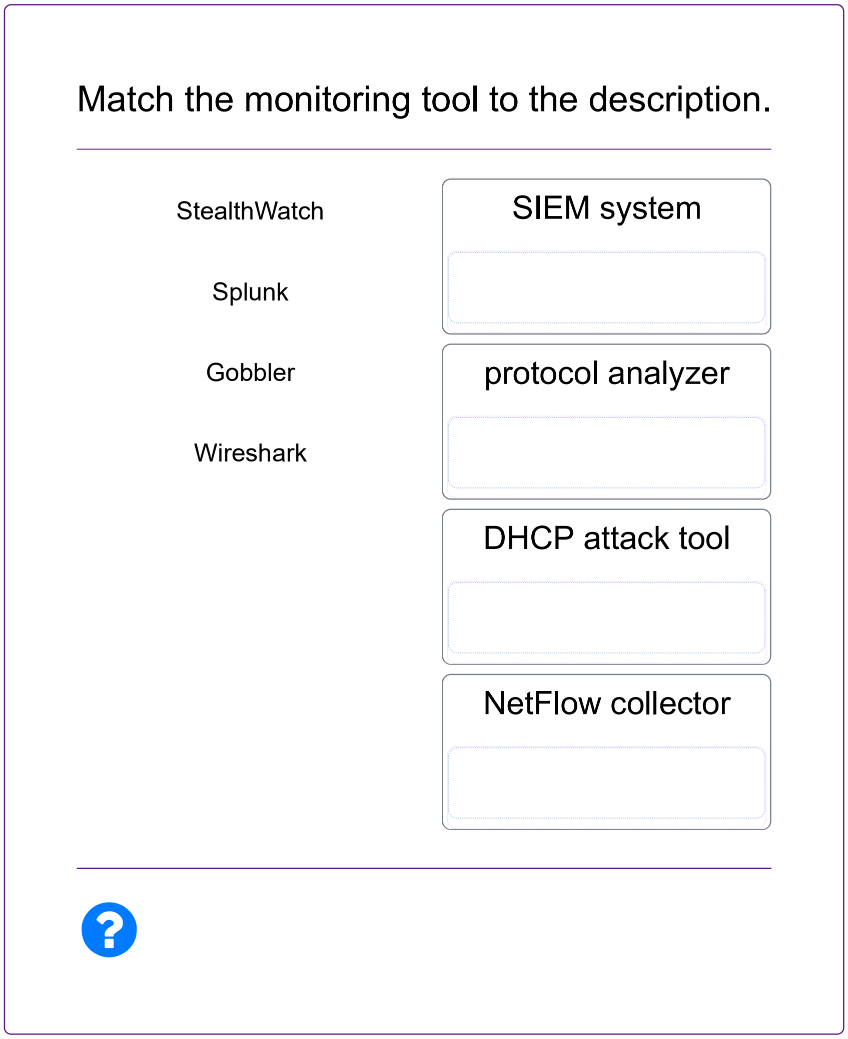
This item references content from the following areas:

CCNA Cybersecurity Operations

- 7.1.2 Introduction to Network Monitoring Tools

24

Question as presented:



Match the monitoring tool to the description.

StealthWatch

Splunk

Gobbler

Wireshark

SIEM system

protocol analyzer

DHCP attack tool

NetFlow collector

This item references content from the following areas:

CCNA Cybersecurity Operations

- 7.1.2 Introduction to Network Monitoring Tools

Your response:

Match the monitoring tool to the description.

StealthWatch

Splunk

Gobbler

Wireshark

SIEM system	✗ StealthWatch
protocol analyzer	✗ Splunk
DHCP attack tool	✓ Gobbler
NetFlow collector	✗ Wireshark

?