Net-Protect-4 : Managing Information Using SIEM

Due Nov 15, 2021 at 11:59pm **Points** 100 **Questions** 7
Available Nov 8, 2021 at 7am - Nov 18, 2021 at 11:59pm **Time Limit** None

Instructions

MODULE 12

Net-Protect 4: Managing Information Using SIEM

This assignment has been paired with the discussion on Security Information and Event Management. As you will find during the discussion, SIEM can be very complex to setup and manage. The goal of this assignment is to give you a "high-level" understanding of what SIEM is all about and the mechanics used to setup this type of system in your test environment. This exercise will only scratch the surface of what SIEM is all about and the capabilities that are built into these types of systems. For this assignment, you will perform the following task:

1. Read the **lab document (https://usflearn.instructure.com/courses/1598910/files/125663634/download?wrap=1) (https://usflearn.instructure.com/courses/1598910/files/125663634/download?download_frd=1)** very carefully
2. Download the **Graylog OVA (https://usflearn.instructure.com/courses/1598910/files/116260998/download?wrap=1) (https://usflearn.instructure.com/courses/1598910/files/116260998/download?download_frd=1)** and install it by performing the following:
    1. Open the OVA image using VMware
    2. Make sure you configure the SIEM image via VMware settings to use your LAN (VMnet1)
    3. Start the Firewall and make sure DHCP is running
    4. Start the Graylog SIEM image
    5. Log into the Graylog image
    6. Determine what IP address was assigned
3. Configure the Firewall to use a remote syslog (which will be the Graylog system)
4. Perform firewall operations (log in and out of the UI for example)
5. Log into the Graylog system using the Web GUI
6. Search and filter on opnsense events
7. Capture your results and take the quiz

NOTE:

If you do not receive the generated events in Greylog as expected,

make sure your Graylog and OPNsense firewall times are in sync,

.i.e. they are in the same timezone and reflect the same relative time

and you wait a few minutes for the event to roll-up to the server. Also, try to perform a query with a start date one day before the event occurred

and stop date one day past the event you are trying to query.

This quiz is no longer available as the course has been concluded.

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	179 minutes	90 out of 100

Score for this quiz: **90** out of 100
Submitted Nov 15, 2021 at 11:12pm
This attempt took 179 minutes.

Question 1

10 / 10 pts

SIEM stands for?

Correct!

Security Information and Event Management

Correct Answers

Security Information and Event Management

security information event management

Correct, it is Security Information and Event Management (SIEM)

Question 2

10 / 10 pts

In the lab assignment, we integrated OPNsense with Graylog using what system facility?

Correct!

syslog

Correct Answers

syslog

rsyslog

standard linux logging

remote syslog

Correct, it was syslog or rsyslog (remote syslog)

Question 3

10 / 10 pts

The network protocol that was used to communicate between the OPNsense firewall and Graylog was?

Correct!

UDP

Correct Answers

UDP

User Datagram Protocol

Correct, it was UDP

Question 4

20 / 20 pts

The standard port used in this assignment that allowed OPNsense to communicate with Graylog for SIEM was?

Correct!

514

Correct Answers

514

UDP 514

UDP port 514

Correct, it is port 514

Question 5

20 / 20 pts

Which RFCs defined the message format that is required for performing remote logging from OPNsense to Graylog?

5424 3164

Answer 1:

Correct! 5424

Correct Answer RFC 5424

Correct Answer RFC5424

Correct Answer RFC 3164

Correct Answer RFC3164

Correct Answer 3164

Answer 2:

Correct! 3164

Correct Answer RFC 5424

Correct Answer RFC5424

Correct Answer 5424

Correct Answer RFC 3164

Correct Answer RFC3164

Correct, it is RFC 5424 and RFC 3164

Question 6

20 / 20 pts

In this assignment, the OPNsense firewall was configured to use Graylog SIEM by using what tool?

○ The console

○ Putty

○ Remote file copy

Correct! ● The web interface

Correct, the web interface was used to configure SIEM for OPNsense

Unanswered

Question 7

0 / 10 pts

Submit a snapshot of your result from using Graylog to capture OPNsense login operations by filter out all but opnsense traffic.

Quiz Score: **90** out of 100