## Final Exam

 Bookmark this page

Final Exam Instructions

1. Time allowed: 1 hour
2. Attempts per question:
   * One attempt - For True/False questions
   * Two attempts - For any question other than True/False
3. Clicking the "**Submit**" button when it appears under each Question, means your submission is **FINAL**.  You will **NOT** be able to resubmit your answer for that question ever again
4. Check your grades in the course at any time by clicking on the "**Progress**" tab

**IMPORTANT: Do not let the time run out and expect the system to grade you automatically. You must explicitly submit your answers, otherwise they would be marked as incomplete.**

### Question 1

1/1 point (graded)

Hackers usually used the computer virus for \_\_\_\_\_\_\_\_\_\_ purpose.

To log, monitor each and every user's stroke

To gain access the sensitive information like user's Id and Passwords

To corrupt the user's data stored in the computer system

All of the above

correct

Submit

You have used 2 of 2 attemptsSome problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

### Question 2

1/1 point (graded)

When using IBM Security QRadar SIEM , which option defines the functions a user can access ?

user roles

individual users

network objects

authorized services

correct

Submit

You have used 2 of 2 attemptsSome problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

### Question 3

1/1 point (graded)

An Administrator needs to configure authentication types for an IBM Security QRadar SIEM system. What are two available authentication types?

Telnet and SSH

IBM X-force and Google Account

RADIUS and IBM Passport Advantage

System Authentication and Microsoft Active Directory

correct

Submit

You have used 2 of 2 attemptsSome problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

### Question 4

1/1 point (graded)

The term "TCP/IP" stands for \_\_\_\_\_\_\_\_\_

Transmission Contribution protocol/ internet protocol

Transmission Control Protocol/ internet protocol

Transaction Control protocol/ internet protocol

Transmission Control Protocol/ internet protocol

correct

Submit

You have used 2 of 2 attemptsSome problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

### Question 5

1/1 point (graded)

A Deployment Professional working with IBM Security QRadar SIEM is asked to optimize the Quick Filter searching performance of the deployment. The Deployment Professional is considering enabling payload indexing but wants to check the requirements. Which two performance metrics need to be checked before enabling this option ? (Choose two)

a. Console is using less than 50% of storage

b. EP and FP are using less than 70% of storage

c. Console is using less than 75% of EPS license

d. EP, FP, and Console are utilizing less than 70% of CPUE

e. EP and FP are using less than 70% of the EPS license and FPI rating

correct

Submit

You have used 2 of 2 attemptsSome problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

### Question 6

0/1 point (graded)

A Deployment Professional is investigating a rule that is not generating offenses even though the log source has been added and is sending logs to a QRadar All-in-One appliance. The rule is based on a custom property that is present in the event payload. What could be one of the causes of this problem ?

The custom property must be indexed.

The regular expression used is incorrect.

The event's content is incompatible with regular expressions.

The rule is defined as a 'Local' rule but should be set to 'Global'.

incorrect

Submit

You have used 2 of 2 attemptsSome problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

### Question 7

1/1 point (graded)

How would an Administrator working with IBM Security QRadar SIEM go about tuning an existing Asset Reconciliation Exclusion rule?

Duplicate the rule.

Run the Tuning Wizard.

Duplicate the Reference Set.

Disable the threshold parameter while modifying the Rule

correct

Submit

You have used 2 of 2 attemptsSome problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

### Question 8

1/1 point (graded)

What is the term for "machine-driven execution of actions on security tools and IT systems, as part of a response to an incident"?

Automation

Orchestration

Collaboration

response

correct

Submit

You have used 2 of 2 attemptsSome problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

### Question 9

1/1 point (graded)

Which of the following statements is correct about the firewall ?

It is a device installed at the boundary of a company to prevent unauthorized physical access.

It is a device installed at the boundary of an incorporate to protect it against the unauthorized access.

It is a kind of wall built to prevent files form damaging the corporate.

None of the above.

correct

Submit

You have used 2 of 2 attemptsSome problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

### Question 10

1/1 point (graded)

Which of the following is considered as the unsolicited commercial email ?

Virus

Malware

Spam

All of the above

correct

Submit

You have used 2 of 2 attemptsSome problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

### Question 11

1/1 point (graded)

Which is a type of software designed to help the user's computer detect viruses and avoid them.

Malware

Adware

Antivirus

Both B and C

correct

Submit

You have used 2 of 2 attemptsSome problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

### Question 12

1/1 point (graded)

Which one of the following is a type of antivirus program ?

Quick heal

Mcafee

Kaspersky

All of the above

correct

Submit

You have used 2 of 2 attemptsSome problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

### Question 13

1/1 point (graded)

Which of the following refers to stealing one's idea or invention of others and use it for their own benefits ?

Piracy

Plagiarism

Intellectual property rights

All of the above

correct

Submit

You have used 2 of 2 attemptsSome problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

### Question 14

1/1 point (graded)

What is the best practice in the firewall domain environment ?

Create two domain trusted and untrusted domain

Create strong policy in firewall to support different types of users

Create a Demilitarized zone

Create two DMZ zones with one untrusted domain

correct

Submit

You have used 2 of 2 attemptsSome problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

### Question 15

1/1 point (graded)

Read the following statement carefully and find out whether it is correct about the hacking or not? It can be possible that in some cases, hacking a computer or network can be legal.

No, in any situation, hacking cannot be legal

It may be possible that in some cases, it can be referred to as a legal task

correct

Submit

You have used 2 of 2 attemptsSome problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

### Question 16

1/1 point (graded)

How do viruses avoid basic pattern match of antivirus ?

They are encrypted

They act with special permissions

They modify themselves

None of the mentioned

correct

Submit

You have used 2 of 2 attemptsSome problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

### Question 17

1/1 point (graded)

Which of the following refers to the violation of the principle if a computer is no more accessible ?

Access control

Confidentiality

Availability

All of the above

correct

Submit

You have used 2 of 2 attemptsSome problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

### Question 18

1/1 point (graded)

Which of the following can be considered as the elements of cyber security ?

Application Security

Operational Security

Network Security

All of the above

correct

Submit

You have used 2 of 2 attemptsSome problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

### Question 19

1/1 point (graded)

What is are two safe computing practices ?

Not to open software from unknown vendors

Open and execute programs in admin level/root

Open and execute programs in presence of antivirus

None of the mentioned

correct

Submit

You have used 2 of 2 attemptsSome problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

### Question 20

1/1 point (graded)

How does an antivirus of today identify viruses ?

Previously known patterns

It can detect unknown patterns

It can take high priority to increase scanning speed

None of the mentioned

correct

Submit

You have used 2 of 2 attemptsSome problems have options such as save, reset, hints, or show answer. These options follow the Submit button.

### Question 21

1/1 point (graded)

Which of the following are famous and common cyber-attacks used by hackers to infiltrate the user's system ?

DDos and Derive-by Downloads

Malware and Malvertising

Phishing and Password attacks

All of the above