Incident and Intrusion Response Quiz

**Question 1 (1 point)**

An event is any observable occurrence in a system or network.

Adverse events are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.

A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Which of the following describes an event?

|  |  |
| --- | --- |
|  | An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money. |
|  | A user provides or exposes sensitive information to others through peer-to-peer file sharing services. |
|  | A user connecting to a file share |
|  | An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash. |

**Question 2 (1 point)**

 Signs of an incident fall into one of two categories: precursors and indicators. A precursor is a sign that an incident may occur in the future. An indicator is a sign that an incident may have occurred or may be occurring now.

Which of the following is an example of an indicator?

|  |  |
| --- | --- |
|  | Web server log entries that show the usage of a vulnerability scanner |
|  | A threat from a group stating that the group will attack the organization. |
|  | An announcement of a new exploit that targets a vulnerability of the organization’s mail server |
|  | A network intrusion detection sensor alerts when a buffer overflow attempt occurs against a database server. |

**Question 3 (1 point)**

The incident response life cycle consists of 4 major phases. Which of the following is the correct order for these phases?

|  |  |
| --- | --- |
|  | Detection and Analysis, Preparation,  Containment Eradication and Recovery, Post-incident Activity |
|  | Preparation, Containment Eradication and Recovery, Detection and Analysis, Post-incident Activity |
|  | Preparation, Detection and Analysis, Post-incident Activity, Containment Eradication and Recovery |
|  | Preparation, Detection and Analysis, Containment Eradication and Recovery, Post-incident Activity |

**Question 4 (1 point)**

 An event is any observable occurrence in a system or network.

Adverse events are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.

A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Which of the following describes an incident?

|  |  |
| --- | --- |
|  | A server receiving a request for a web page. |
|  | A a user sending email. |
|  | A firewall blocking a connection attempt. |
|  | Users are tricked into opening a “quarterly report” sent via email that is actually malware; running the tool has infected their computers and established connections with an external host. |

**Question 5 (1 point)**

Signs of an incident fall into one of two categories: precursors and indicators. A precursor is a sign that an incident may occur in the future. An indicator is a sign that an incident may have occurred or may be occurring now.

Which of the following is an example of a precursor?

|  |  |
| --- | --- |
|  | A threat from a group stating that the group will attack the organization. |
|  | Antivirus software alerts when it detects that a host is infected with malware. |
|  | A host records an auditing configuration change in its log |
|  | A network intrusion detection sensor alerts when a buffer overflow attempt occurs against a database server. |

**Question 6 (1 point)**

 Which of the following are common sources of indicators and precursors?

|  |  |
| --- | --- |
|  | IDPs and IDSs |
|  | SIEMs |
|  | Logs and CVEs |
|  | All of the above |
|  | None of the above |

**Question 7 (1 point)**

Which of the following departments, among others in an organization, should be represented in the incident response team?

|  |  |
| --- | --- |
|  | Management |
|  | Legal Department |
|  | Human Resources |
|  | All of the above |
|  | None of the above |

**Question 8 (1 point)**

Signs of an incident fall into one of two categories: precursors and indicators. A precursor is a sign that an incident may occur in the future. An indicator is a sign that an incident may have occurred or may be occurring now.

True or False: While indicators are relatively rare, precursors are all too common.

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 9 (1 point)**

In \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ structure,  a single incident response team handles incidents throughout the organization. In \_\_\_\_\_\_\_\_\_\_\_ structure, the organization has multiple incident response teams, each responsible for a particular logical or physical segment of the organization.

|  |  |
| --- | --- |
|  | Central incident response team, external incident team |
|  | Central incident response team, distributed incident response team |
|  | Distributed incident response team, coordinating team |
|  | Distributed incident response team, central incident response team |

**Question 10 (1 point)**

True or False. Incidents should not be handled on a first-come, first-served basis as a result of resource limitations.

|  |  |
| --- | --- |
|  | True |
|  | False |