**Quiz 11**

**Question 1 (1 point)**

\_\_\_\_\_\_\_\_\_\_\_  perform packet sniffing and analyze network traffic to identify and stop suspicious activity, whereas \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  attempts to stop attacks by identifying unusual network traffic flow.

|  |  |
| --- | --- |
|  | Network behavior analysis system, Network IPS |
|  | Network IPS, Network behavior analysis system |

**Question 2 (1 point)**

To reduce the impact of malicious plug-ins being downloaded in a browser, users can use one brand of browser for corporate applications and another brand of browser for all other website access. What is this technique referred to?

|  |  |
| --- | --- |
|  | Sandboxing |
|  | Eradication |
|  | Browser separation |
|  | Virtualization |

**Question 3 (1 point)**

Most application whitelisting technologies can be run in two modes: audit and enforcement.

In \_\_\_\_\_\_\_\_\_\_ mode, the technology generally prohibits all applications that are not in the whitelist from being executed. In \_\_\_\_\_\_\_\_ mode, the technology logs all instances of non-whitelisted applications being run on the host, but does not act to stop them.

|  |  |
| --- | --- |
|  | enforcement, audit |
|  | audit, enforcement |

**Question 4 (1 point)**

A \_\_\_\_\_\_\_\_\_\_\_ is a malicious program that listens for commands on a certain TCP or UDP port. It allows an attacker to perform a certain set of actions on a host, such as acquiring passwords or executing arbitrary command

|  |  |
| --- | --- |
|  | Web browser plugin |
|  | Backdoor |
|  | Keystroke logger |
|  | Email generator |

**Question 5 (1 point)**

A \_\_\_\_\_\_\_\_\_\_ is a device deployed between networks to restrict which types of traffic can pass from one network to another. A \_\_\_\_\_\_\_\_\_\_\_ is a piece of software running on a single host that can restrict incoming and outgoing network activity for that host only

|  |  |
| --- | --- |
|  | host-based firewall, network firewall |
|  | network firewall, host-based firewall |

**Question 6 (1 point)**

 \_\_\_\_\_\_\_\_\_\_\_\_  involves the use of separate applications or operating systems from each other through, such as having one OS instance for corporate applications and another OS instance for all other activity.

|  |  |
| --- | --- |
|  | Virtualization |
|  | Browser separation |
|  | OS Spoofing |
|  | Sandboxing |

**Question 7 (1 point)**

 A \_\_\_\_\_\_\_\_\_ self-replicates by inserting copies of itself into host programs or data files, while a \_\_\_\_\_\_\_\_\_\_\_\_\_ is a self-replicating, self-contained program that usually executes itself without user intervention.

|  |  |
| --- | --- |
|  | Logic bomb, worm |
|  | Virus, logic bomb |
|  | Virus, worm |
|  | Worm, virus |

**Question 8 (1 point)**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  is a security model where applications are run within a controlled environment that restricts what operations the applications can perform and isolates them from other applications.

|  |  |
| --- | --- |
|  | Content filtering |
|  | Sandboxing |
|  | Malware protection |
|  | IPS |

**Question 9 (1 point)**

A \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  refers to an instance in which a security tool incorrectly classifies benign content as malicious, whereas \_\_\_\_\_\_\_\_\_\_\_ refers to an instance in which a security tool intended to detect a particular threat fails to do so.

|  |  |
| --- | --- |
|  | True positive, true negative |
|  | False negative, false positive |
|  | True positive, false negative |
|  | False positive, false negative |

**Question 10 (1 point)**

 Which of the following describe common malware prevention–related policy considerations?

|  |  |
| --- | --- |
|  | Requiring that email file attachments be scanned before they are opened |
|  | Restricting or prohibiting the use of unnecessary software |
|  | Restricting the use of removable media |
|  | Prohibiting the sending or receipt of certain types of files (e.g., .exe files) via email |
|  | All of the above |