**Self Test**

The following Self Test questions will help you measure your understanding of the material presented in this chapter. Read all the choices carefully, as there may be more than one correct answer. Choose all correct answers for each question.

**Endpoint Security Introduction**

|  |  |  |
| --- | --- | --- |
| **1.** | What is the most common type of attack?   1. Buffer overflow 2. Trojan horse 3. Operating system 4. Application | [*     D. The most common type of attack is an application attack.  *     A , B , and C are not the most common types of attacks.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=356288139&rowid=995#answer.N27) |
| **2.** | What security feature should you implement to reduce the effectiveness of a worm attack once a device in your network has become infected?   1. Security patches 2. Network IPS 3. Connection limits 4. Antivirus and antispyware | [*     C. Connection limits should be implemented to reduce the effectiveness of a worm attack once a device in your network has become infected-appropriate traffic levels should be defined for your little-used protocols (common with worms), like ICMP and UDP.  *     A , B , and D are used to prevent worm attacks.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=356288139&rowid=995#answer.N83) |
| **3.** | Match the item to the description.  Items: (1) virus; (2) worm; and (3) Trojan horse. Descriptions: (a) a self-contained program that executes arbitrary code and installs itself in memory on infected machines; (b) stand-alone programs that pretend to be something useful or valid, but perform something the user would find undesirable; and (c) malicious software that attaches to a program (vector) and executes a function that a user would find undesirable or unwanted. | [*     (1)-(c) ; (2)-(a) ; and (3)-(b)](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=356288139&rowid=995#answer.N140) |

**Answers**

|  |  |
| --- | --- |
| **1.** | *  **D.** The most common type of attack is an application attack. *  **A**, **B**, and **C** are not the most common types of attacks. |
| **2.** | *  **C.** Connection limits should be implemented to reduce the effectiveness of a worm attack once a device in your network has become infected—appropriate traffic levels should be defined for your little-used protocols (common with worms), like ICMP and UDP. *  **A**, **B**, and **D** are used to prevent worm attacks. |
| **3.** | *  **(1)—(c)**; **(2)—(a)**; and **(3)—(b)** |

**Cisco Endpoint Security Products**

|  |  |  |
| --- | --- | --- |
| **4.** | What IronPort C-series component collects e-mail statistics to detect and prevent spam attacks?   1. SendBase 2. Dynamic Vectoring and Streaming engine 3. NAC 4. CSA | [*     A. SendBase collects e-mail statistics to detect and prevent spam attacks.  *     B is the IronPort S-series product that deals with web-based attacks. C implements posture validation. D is Cisco's HIPS product.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=356288139&rowid=995#answer.N177) |
| **5.** | What protocol is used between a CSA agent and the CSA MC console?   1. SSH 2. SNMP 3. SSL 4. IPSec | [*     C. SSL (HTTPS) is used between a CSA agent and the CSA MC console.  *     A , B , and D are not used between the agent and console.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=356288139&rowid=995#answer.N233) |
| **6.** | What CSA interceptor is used to protect against buffer overflow attacks?   1. File system 2. Network 3. Configuration 4. Execution space | [*     D. The execution space interceptor is used to protect against buffer overflow attacks.  *     A is used to protect access to files. B is used to protect access to network interfaces. C is used to protect access to registry and rc files.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=356288139&rowid=995#answer.N294) |

**Answers**

|  |  |
| --- | --- |
| **4.** | *  **A.** SendBase collects e-mail statistics to detect and prevent spam attacks. *  **B** is the IronPort S-series product that deals with web-based attacks. **C** implements posture validation. **D** is Cisco's HIPS product. |
| **5.** | *  **C.** SSL (HTTPS) is used between a CSA agent and the CSA MC console. *  **A**, **B**, and **D** are not used between the agent and console. |
| **6.** | *  **D.** The execution space interceptor is used to protect against buffer overflow attacks. *  **A** is used to protect access to files. **B** is used to protect access to network interfaces. **C** is used to protect access to registry and rc files. |

**Storage Area Networks**

|  |  |  |
| --- | --- | --- |
| **7.** | In SANS, what is used as an identifier for a particular disk drive, virtual partition, or volume when using SCSI?   1. LUN 2. WWN 3. Zone 4. VSAN | [*     A. A LUN is used as an identifier for a particular disk drive, virtual partition, or volume when using SCSI.  *     B consists of 64-bit addresses used in Fibre Channel networks that uniquely identify each SAN element. C is used with FCIP to control access to devices and elements in SANs. D functions similar to VLANs in Ethernet, where fabric events are isolated per VSAN.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=356288139&rowid=995#answer.N360) |
| **8.** | FCAP, used with FCIP, supports all the following forms of authentication except which one?   1. DH-CHAP 2. PKI 3. Token cards 4. CHAP | [*     C. FCAP doesn't support token cards.  *     A , B , and D are supported by FCAP.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=356288139&rowid=995#answer.N416) |

### Answers

|  |  |
| --- | --- |
| **7.** | *  **A.** A LUN is used as an identifier for a particular disk drive, virtual partition, or volume when using SCSI. *  **B** consists of 64-bit addresses used in Fibre Channel networks that uniquely identify each SAN element. **C** is used with FCIP to control access to devices and elements in SANs. **D** functions similar to VLANs in Ethernet, where fabric events are isolated per VSAN. |
| **8.** | *  **C.** FCAP doesn't support token cards. *  **A**, **B**, and **D** are supported by FCAP. |

**Voice over IP**

|  |  |  |
| --- | --- | --- |
| **9.** | What VoIP component provides call admission control (CAC), address translation (mapping phone numbers to IP addresses of those phones), and management of bandwidth?   1. Gateway 2. Gatekeeper 3. Application server 4. Multipoint control unit | [*     B. A gatekeeper provides call admission control, address translation, and management of bandwidth.  *     A connects together VoIP and non-VoIP networks. C provides services like unified messaging and faxing services. D connects multiple locations together for voice conferencing.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=356288139&rowid=995#answer.N482) |
| **10.** | What voice attack is similar to phishing?   1. Vishing 2. SPIT 3. Spam 4. Eavesdropping | [*     A. Vishing is a voice version of phishing, where an attacker tries to learn phone account information from a user over a phone.  *     B and C are where hundreds or thousands of voice calls are made, playing some type of advertisement or message to the user. D is where an attacker intercepts and examines RTP connections, recording the voice conversations of people.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=356288139&rowid=995#answer.N538) |

**Answers**

|  |  |
| --- | --- |
| **9.** | *  **B.** A gatekeeper provides call admission control, address translation, and management of bandwidth. *  **A** connects together VoIP and non-VoIP networks. **C** provides services like unified messaging and faxing services. **D** connects multiple locations together for voice conferencing. |
| **10.** | *  **A.** Vishing is a voice version of phishing, where an attacker tries to learn phone account information from a user over a phone. *  **B** and **C** are where hundreds or thousands of voice calls are made, playing some type of advertisement or message to the user. **D** is where an attacker intercepts and examines RTP connections, recording the voice conversations of people. |