**Security Threats**

|  |  |  |
| --- | --- | --- |
| **1.** | In what type of threat do technically skilled people, including perpetrators of major fraud, industry competitors, organized crime figures, and government intelligence agencies, attempt to gain access to your network?   1. Unstructured 2. External 3. Structured 4. DDoS | [*     C. A structured threat is where technically skilled people attempt to gain access to your network; they may intend major fraud or be industry competitors, organized crime figures, or government intelligence agencies.  *     A is incorrect because these are non-technically skilled people, commonly called script kiddies. B is incorrect because this classifies the location of the attack. D is incorrect because this could be an unstructured or structured attack.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=406246456&rowid=203#answer.N27) |
| **2.** | What security vulnerability category would include using a password of "cisco"?   1. Policies 2. Technology 3. Administration and configuration 4. Access | [*     C. Administration and configuration weaknesses would include the kinds of passwords you use.  *     A is incorrect because it includes both business and security policies. B is incorrect because it includes protocols, operating systems, and applications. D is incorrect because it is not a security vulnerability category.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=406246456&rowid=203#answer.N83) |

**Answers**

|  |  |
| --- | --- |
| **1.** | *  **C.** A structured threat is where technically skilled people attempt to gain access to your network; they may intend major fraud or be industry competitors, organized crime figures, or government intelligence agencies. *  **A** is incorrect because these are non—technically skilled people, commonly called script kiddies. **B** is incorrect because this classifies the location of the attack. **D** is incorrect because this could be an unstructured or structured attack. |
| **2.** | *  **C.** Administration and configuration weaknesses would include the kinds of passwords you use. *  **A** is incorrect because it includes both business and security policies. **B** is incorrect because it includes protocols, operating systems, and applications. **D**is incorrect because it is not a security vulnerability category. |

**Attack Categories**

|  |  |  |
| --- | --- | --- |
| **3.** | What type of attack is used to learn information about your network?   1. Footprint analysis 2. Access 3. DoS 4. Session | [*     A. A reconnaissance attack, commonly called footprint analysis, is used to learn information about your network.  *     B is incorrect because access attacks are attacks used to gain illegal or unauthorized access to your organization's resources. C is incorrect because this attack is used to reduce the level of operation of a resource. D is incorrect because this is a type of access attack.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=406246456&rowid=203#answer.N149) |
| **4.** | What is the most effective type of network reconnaissance attack?   1. DNS 2. Phishing 3. Packet sniffing 4. Social engineering | [*     D. Social engineering is the most effective type of network reconnaissance attack.  *    Since social engineering is the most effective reconnaissance attack, answers A , B , and C are incorrect.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=406246456&rowid=203#answer.N205) |
| **5.** | What type of attack redirects traffic from one web site to another, where the attack either changes the hosts file on a user's PC or exploits a vulnerability on a DNS server to send back a spoofed DNS reply?   1. Phishing 2. Pharming 3. Emanations capturing 4. Dumpster driving | [*     B. A pharming attack redirects traffic from one web site to another, which is a fake server pretending to be the real thing.  *     A is incorrect because this attack uses masquerading to learn information, like user accounts, passwords, or credit card information, from a user via HTML e-mails that look like they come from a legitimate source. C is incorrect because this attack captures electrical signals that leak from copper wiring or CRT monitors. D is incorrect because in this attack, the attacker goes through the trash bins to find employee directories, handbooks, and sensitive information that he can use to learn more information about your network.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=406246456&rowid=203#answer.N266) |
| **6.** | What type of attack conceals data inside another object, like an image or a sound file?   1. Steganography 2. Overt channel 3. Covert channel 4. ICMP tunneling | [*     A. A steganography attack conceals data inside another object.  *     B and D are incorrect because these kinds of attacks hide data by tunneling traffic in another protocol, for example using IM file sharing across HTTP, or tunneling data using ICMP or SSH. C is incorrect because in this process, the attacker encodes the reconnaissance information as another set of events.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=406246456&rowid=203#answer.N323) |
| **7.** | In a brute-force password attack, about what percentage of passwords have to be guessed by a password cracking program before the password is cracked?   1. 25 2. 50 3. 75 4. 100 | [*     B. In a brute-force password attack, about 50 percent of passwords have to be guessed by a password cracking program before it is cracked.  *    Therefore answers A , C , and D are incorrect.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=406246456&rowid=203#answer.N384) |
| **8.** | What is the most common type of application access attack?   1. Social engineering 2. Trojan horse 3. E-mail attachment 4. Buffer overflow | [*     D. The most common type of application access attack is a buffer overflow, which targets vulnerabilities found in software because of poor programming practices.  *     A is incorrect because this is a reconnaissance attack. B is incorrect because this is a DoS attack. C is an access attack, but it is not the most common.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=406246456&rowid=203#answer.N441) |
| **9.** | What would be used to mitigate TCP SYN flood attacks?   1. TCP setup controls 2. Java and ActiveX filtering 3. RFC 2827 filtering 4. uRPF | [*     A. TCP setup controls, on products like Guard and ASA and PIX security appliances, are used to mitigate TCP SYN flood attacks.  *     B is incorrect because these are used to prevent application attacks against web services. C and D are used to prevent spoofing attacks and can't necessarily be used to prevent TCP SYN flood attacks unless these mechanisms are implemented at the source or destination, which involves the spoofed addresses.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=406246456&rowid=203#answer.N498) |
| **10.** | Which of the following is not used in a Smurf attack?   1. uRPF 2. ICMP 3. Directed broadcast addresses 4. Reflectors | [*     A. uRPF is used to help mitigate Smurf attacks and is not part of the attack itself.  *     B , C , and D are part of a Smurf attack and therefore are incorrect answers.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=406246456&rowid=203#answer.N555) |

**Answers**

|  |  |
| --- | --- |
| **3.** | *  **A.** A reconnaissance attack, commonly called footprint analysis, is used to learn information about your network. *  **B** is incorrect because access attacks are attacks used to gain illegal or unauthorized access to your organization's resources. **C** is incorrect because this attack is used to reduce the level of operation of a resource. **D** is incorrect because this is a type of access attack. |
| **4.** | *  **D.** Social engineering is the most effective type of network reconnaissance attack. *  Since social engineering is the most effective reconnaissance attack, answers **A**, **B**, and **C** are incorrect. |
| **5.** | *  **B.** A pharming attack redirects traffic from one web site to another, which is a fake server pretending to be the real thing. *  **A** is incorrect because this attack uses masquerading to learn information, like user accounts, passwords, or credit card information, from a user via HTML e-mails that look like they come from a legitimate source. **C** is incorrect because this attack captures electrical signals that leak from copper wiring or CRT monitors. **D** is incorrect because in this attack, the attacker goes through the trash bins to find employee directories, handbooks, and sensitive information that he can use to learn more information about your network. |
| **6.** | *  **A.** A steganography attack conceals data inside another object. *  **B** and **D** are incorrect because these kinds of attacks hide data by tunneling traffic in another protocol, for example using IM file sharing across HTTP, or tunneling data using ICMP or SSH. **C** is incorrect because in this process, the attacker encodes the reconnaissance information as another set of events. |
| **7.** | *  **B.** In a brute-force password attack, about 50 percent of passwords have to be guessed by a password cracking program before it is cracked. *  Therefore answers **A**, **C**, and **D** are incorrect. |
| **8.** | *  **D.** The most common type of application access attack is a buffer overflow, which targets vulnerabilities found in software because of poor programming practices. *  **A** is incorrect because this is a reconnaissance attack. **B** is incorrect because this is a DoS attack. **C** is an access attack, but it is not the most common. |
| **9.** | *  **A.** TCP setup controls, on products like Guard and ASA and PIX security appliances, are used to mitigate TCP SYN flood attacks. *  **B** is incorrect because these are used to prevent application attacks against web services. **C** and **D** are used to prevent spoofing attacks and can't necessarily be used to prevent TCP SYN flood attacks unless these mechanisms are implemented at the source or destination, which involves the spoofed addresses. |
| **10.** | *  **A.** uRPF is used to help mitigate Smurf attacks and is not part of the attack itself. *  **B**, **C**, and **D** are part of a Smurf attack and therefore are incorrect answers. |