**Review Questions**

|  |  |  |
| --- | --- | --- |
| **1.** | Which is a method to prevent denial-of-service attacks?   1. Static routing 2. Traffic filtering 3. Firewall rules 4. Personal firewall | [Traffic filtering is a method to prevent DoS attacks. Static routing will not prevent DoS attacks as it does not perform any traffic filtering or blocking. Firewall rules and personal firewalls will not stop traffic associated with a DoS attack but will help detect an attack.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=470654524&rowid=285&noteMenuToggle=0&leftMenuState=1#answer.N14) |
| **2.** | What is a zombie?   1. A compromised system used to launch a DDoS attack 2. The hacker's computer 3. The victim of a DDoS attack 4. A compromised system that is the target of a DDoS attack | [A zombie is a compromised system used to launch a DDoS attack.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=470654524&rowid=285&noteMenuToggle=0&leftMenuState=1#answer.N39) |
| **3.** | The Trinoo tool uses what protocol to perform a DoS attack?   1. TCP 2. IP 3. UDP 4. HTTP | [Trinoo uses UDP to flood the target system with data.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=470654524&rowid=285&noteMenuToggle=0&leftMenuState=1#answer.N64) |
| **4.** | What is the first phase of a DDoS attack?   1. Intrusion 2. Attack 3. DoS 4. Finding a target system | [The intrusion phase compromises and recruits zombie systems to use in the coordinated attack phase.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=470654524&rowid=285&noteMenuToggle=0&leftMenuState=1#answer.N89) |
| **5.** | Which tool can run eight different types of DoS attacks?   1. Ping of Death 2. Trinoo 3. Targa 4. TFN2K | [Targa is able to send eight different types of DoS attacks.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=470654524&rowid=285&noteMenuToggle=0&leftMenuState=1#answer.N114) |
| **6.** | What is a smurf attack?   1. Sending a large amount of ICMP traffic with a spoofed source address 2. Sending a large amount of TCP traffic with a spoofed source address 3. Sending a large number of TCP connection requests with a spoofed source address 4. Sending a large number of TCP connection requests | [A smurf attack sends a large number of ICMP request frames with a spoofed address of the victim system.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=470654524&rowid=285&noteMenuToggle=0&leftMenuState=1#answer.N139) |
| **7.** | What is a LAND attack? (Choose all that apply.)   1. Sending oversized ICMP packets 2. Sending packets to a victim with a source address set to the victim's IP address 3. Sending packets to a victim with a destination address set to the victim's IP address 4. Sending a packet with the same source and destination address | [A LAND attack sends packets to a system with that system as the source address, causing the system to try to reply to itself.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=470654524&rowid=285&noteMenuToggle=0&leftMenuState=1#answer.N164) |
| **8.** | What is the Ping of Death?   1. Sending packets that, when reassembled, are too large for the system to understand 2. Sending very large packets that cause a buffer overflow 3. Sending packets very quickly to fill up the receiving buffer 4. Sending a TCP packet with the fragment offset out of bounds | [The Ping of Death attack sends packets that, when reassembled, are too large and cause the system to crash or lock up.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=470654524&rowid=285&noteMenuToggle=0&leftMenuState=1#answer.N189) |
| **9.** | How does a denial-of-service attack work? (Choose all that apply.)   1. Cracks passwords, causing the system to crash 2. Imitates a valid user 3. Prevents a legitimate user from using a system or service 4. Attempts to break the authentication method | [A DoS attack works by preventing legitimate users from accessing the system.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=470654524&rowid=285&noteMenuToggle=0&leftMenuState=1#answer.N214) |
| **10.** | What is the goal of a DoS attack?   1. To capture files from a remote system 2. To incapacitate a system or network 3. To exploit a weakness in the TCP/IP stack 4. To execute a Trojan using the hidden shares | [The goal of a DoS attack is to overload a system and cause it to stop responding.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=470654524&rowid=285&noteMenuToggle=0&leftMenuState=1#answer.N239) |
| **11.** | Which of the following tools is only for Sun Solaris systems?   1. Juggernaut 2. T-Sight 3. IP Watcher 4. TTYWatcher | [TTYWatcher is used to perform session hijacking on Sun Solaris systems.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=470654524&rowid=285&noteMenuToggle=0&leftMenuState=1#answer.N264) |
| **12.** | What is a sequence number?   1. A number that indicates where a packet falls in the data stream 2. A way of sending information from the sending to the receiving station 3. A number that the hacker randomly chooses in order to hijack a session 4. A number used in reconstructing a UDP session | [A sequence number indicates where the packet is located in the data stream so the receiving station can reassemble the data.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=470654524&rowid=285&noteMenuToggle=0&leftMenuState=1#answer.N289) |
| **13.** | What type of information can be obtained during a session-hijacking attack? (Choose all that apply.)   1. Passwords 2. Credit card numbers 3. Confidential data 4. Authentication information | [Passwords, credit card numbers, and other confidential data can be gathered in a session-hijacking attack. Authentication information isn't accessible because session hijacking occurs after the user has authenticated.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=470654524&rowid=285&noteMenuToggle=0&leftMenuState=1#answer.N314) |
| **14.** | Which of the following is essential information to a hacker performing a session-hijacking attack?   1. Session ID 2. Session number 3. Sequence number 4. Source IP address | [In order to perform a session-hijacking attack, the hacker must know the sequence number to use in the next packet so the server will accept the packet.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=470654524&rowid=285&noteMenuToggle=0&leftMenuState=1#answer.N339) |
| **15.** | Which of the following is a session-hijacking tool that runs on Linux operating systems?   1. Juggernaut 2. Hunt 3. TTYWatcher 4. TCP Reset Utility | [Juggernaut runs on Linux operating systems.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=470654524&rowid=285&noteMenuToggle=0&leftMenuState=1#answer.N364) |
| **16.** | Which of the following is the best countermeasure to session hijacking?   1. Port filtering firewall 2. Encryption 3. Session monitoring 4. Strong passwords | [Encryption makes any information the hacker gathers during a session-hijacking attempt unreadable.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=470654524&rowid=285&noteMenuToggle=0&leftMenuState=1#answer.N389) |
| **17.** | Which of the following best describes sniffing?   1. Gathering packets to locate IP addresses in order to initiate a session-hijacking attack 2. Analyzing packets in order to locate the sequence number to start a session hijack 3. Monitoring TCP sessions in order to initiate a session-hijacking attack 4. Locating a host susceptible to a session-hijack attack | [Sniffing is usually used to locate the sequence number, which is necessary for a session hijack.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=470654524&rowid=285&noteMenuToggle=0&leftMenuState=1#answer.N414) |
| **18.** | What is session hijacking?   1. Monitoring UDP sessions 2. Monitoring TCP sessions 3. Taking over UDP sessions 4. Taking over TCP sessions | [The most common form of session hijacking is the process of taking over a TCP session.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=470654524&rowid=285&noteMenuToggle=0&leftMenuState=1#answer.N439) |
| **19.** | What types of packets are sent to the victim of a session-hijacking attack to cause them to close their end of the connection?   1. FIN and ACK 2. SYN or ACK 3. SYN and ACK 4. FIN or RST | [FIN (finish) and RST (reset) packets are sent to the victim to desynchronize their connection and cause them to close the existing connection.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=470654524&rowid=285&noteMenuToggle=0&leftMenuState=1#answer.N464) |
| **20.** | What is an ISN?   1. Initiation session number 2. Initial sequence number 3. Initial session number 4. Indication sequence number | [ISN is the initial sequence number that is sent by the host and is the starting point for the sequence numbers used in later packets.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=470654524&rowid=285&noteMenuToggle=0&leftMenuState=1#answer.N489) |

**Answers**

|  |  |
| --- | --- |
| **1.** | Traffic filtering is a method to prevent DoS attacks. Static routing will not prevent DoS attacks as it does not perform any traffic filtering or blocking. Firewall rules and personal firewalls will not stop traffic associated with a DoS attack but will help detect an attack. |
| **2.** | A zombie is a compromised system used to launch a DDoS attack. |
| **3.** | Trinoo uses UDP to flood the target system with data. |
| **4.** | The intrusion phase compromises and recruits zombie systems to use in the coordinated attack phase. |
| **5.** | Targa is able to send eight different types of DoS attacks. |
| **6.** | A smurf attack sends a large number of ICMP request frames with a spoofed address of the victim system. |
| **7.** | A LAND attack sends packets to a system with that system as the source address, causing the system to try to reply to itself. |
| **8.** | The Ping of Death attack sends packets that, when reassembled, are too large and cause the system to crash or lock up. |
| **9.** | A DoS attack works by preventing legitimate users from accessing the system. |
| **10.** | The goal of a DoS attack is to overload a system and cause it to stop responding. |
| **11.** | TTYWatcher is used to perform session hijacking on Sun Solaris systems. |
| **12.** | A sequence number indicates where the packet is located in the data stream so the receiving station can reassemble the data. |
| **13.** | Passwords, credit card numbers, and other confidential data can be gathered in a session-hijacking attack. Authentication information isn't accessible because session hijacking occurs after the user has authenticated. |
| **14.** | In order to perform a session-hijacking attack, the hacker must know the sequence number to use in the next packet so the server will accept the packet. |
| **15.** | Juggernaut runs on Linux operating systems. |
| **16.** | Encryption makes any information the hacker gathers during a session-hijacking attempt unreadable. |
| **17.** | Sniffing is usually used to locate the sequence number, which is necessary for a session hijack. |
| **18.** | The most common form of session hijacking is the process of taking over a TCP session. |
| **19.** | FIN (finish) and RST (reset) packets are sent to the victim to desynchronize their connection and cause them to close the existing connection. |
| **20.** | ISN is the initial sequence number that is sent by the host and is the starting point for the sequence numbers used in later packets. |