**Review Questions**

|  |  |  |
| --- | --- | --- |
| **1.** | What is a system that performs attack recognition and alerting for a network?   1. HIDS 2. NIDS 3. Anomaly detection HIDS 4. Signature-based NIDS | [An NIDS performs attack recognition for an entire network.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=324446311&rowid=407&noteMenuToggle=0&leftMenuState=1#answer.N14) |
| **2.** | Which of the following tools bypasses a firewall by sending one byte at a time in the IP header?   1. Honeyd 2. Nessus 3. Covert\_TCP 4. 007 Shell 5. TCP to IP Hide | [Covert_TCP passes through a firewall by sending one byte at a time of a file in the IP header.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=324446311&rowid=407&noteMenuToggle=0&leftMenuState=1#answer.N39) |
| **3.** | Which of the following is a honeypot-detection tool?   1. Honeyd 2. Specter 3. KFSensor 4. Sobek | [Sobek is a honeypot-detection tool.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=324446311&rowid=407&noteMenuToggle=0&leftMenuState=1#answer.N67) |
| **4.** | Which of the following is a system designed to attract and identify hackers?   1. Honeypot 2. Firewall 3. Honeytrap 4. IDS | [A honeypot is a system designed to attract and identify hackers.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=324446311&rowid=407&noteMenuToggle=0&leftMenuState=1#answer.N92) |
| **5.** | Which of the following is a tool used to modify an attack script to bypass an IDS's signature detection?   1. ADMmutate 2. Script Mutate 3. Snort 4. Specter | [ADMmutate is a tool used to modify an attack script to bypass an IDS's signature detection.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=324446311&rowid=407&noteMenuToggle=0&leftMenuState=1#answer.N117) |
| **6.** | What is a reverse WWW shell?   1. A web server making a reverse connection to a firewall 2. A web client making a connection to a hacker through the firewall 3. A web server connecting to a web client through the firewall 4. A hacker connecting to a web server through a firewall | [A reverse WWW shell occurs when a compromised web client makes a connection back to a hacker's computer and is able to pass through a firewall.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=324446311&rowid=407&noteMenuToggle=0&leftMenuState=1#answer.N142) |
| **7.** | A reverse WWW shell connects to which port on a hacker's system?   1. 80 2. 443 3. 23 4. 21 | [The hacker's system, which is acting as a web server, uses port 80.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=324446311&rowid=407&noteMenuToggle=0&leftMenuState=1#answer.N167) |
| **8.** | What is the command used to install and run Snort?   1. snort –l c:\snort\log –c C:\snort\etc\snort.conf –A console 2. snort –c C:\snort\etc\snort.conf –A console 3. snort –c C:\snort\etc\snort.conf console 4. snort –l c:\snort\log –c –A | [Use the command snort  l c:\snort\log  c C:\snort\etc\snort.conf  A console to install and run the Snort program.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=324446311&rowid=407&noteMenuToggle=0&leftMenuState=1#answer.N192) |
| **9.** | What type of program is Snort?   1. NIDS 2. Sniffer, HIDS, and traffic-logging tool 3. Sniffer and HIDS 4. NIDS and sniffer | [Snort is a sniffer, HIDS, and traffic-logging tool.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=324446311&rowid=407&noteMenuToggle=0&leftMenuState=1#answer.N229) |
| **10.** | What are the ways in which an IDS is able to detect intrusion attempts? (Choose all that apply.)   1. Signature detection 2. Anomaly detection 3. Traffic identification 4. Protocol analysis | [Signature analysis and anomaly detection are the ways an IDS detects instruction attempts.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=324446311&rowid=407&noteMenuToggle=0&leftMenuState=1#answer.N254) |
| **11.** | You are viewing a snort output report and see an entry with the following address information: 168.175.44.80:34913 -> 142.155.44.28:443. What type of server is the destination address?   1. HTTP 2. FTP 3. SSL 4. HTTPS | [The destination port 443 indicates the traffic destination is an HTTPS server.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=324446311&rowid=407&noteMenuToggle=0&leftMenuState=1#answer.N279) |
| **12.** | What is the snort.conf file variable for the local IP subnet?   1. INTERNAL\_NET 2. DESTINATION\_NETWORK 3. SOURCE\_NET 4. HOME\_NET | [The HOME_NET variable is used in a snort.conf file to identify the local network.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=324446311&rowid=407&noteMenuToggle=0&leftMenuState=1#answer.N308) |
| **13.** | How is the rule location identified in the snort.conf file?   1. RULE\_PATH 2. RULE\_DIR 3. RULES 4. RULE\_NET | [The rule location is identified by the RULE_PATH variable in a snort.conf file.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=324446311&rowid=407&noteMenuToggle=0&leftMenuState=1#answer.N353) |
| **14.** | Which field is *not* located in the rule header in a Snort rule?   1. Rule Action 2. Protocol 3. Source Address 4. HOME\_NET | [Rule Action, Protocol, Source Address, and Destination Address are all included in a Snort rule header. HOME_NET is the variable to define the Internal Network in the snort.conf file.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=324446311&rowid=407&noteMenuToggle=0&leftMenuState=1#answer.N398) |
| **15.** | Which Snort rule option would associate a high priority to an alert?   1. class:attempted-admin 2. classtype:High 3. classtype:attempted-admin 4. class:admin | [This Snort option associates a high priority to this alert by giving it an attack class of attempted-admin .](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=324446311&rowid=407&noteMenuToggle=0&leftMenuState=1#answer.N436) |
| **16.** | What are the two components needed when installing Snort?   1. Snort rules 2. Snort signatures 3. Snort Engine 4. Snort processor | [Snort rules and the Snort Engine need to be installed separately during installation of Snort.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=324446311&rowid=407&noteMenuToggle=0&leftMenuState=1#answer.N476) |
| **17.** | What is an attack signature in an IDS?   1. A pattern of packets that indicates an attack 2. The first packet that indicates the start of an attack 3. The TCP header that indicates an attack 4. The confirmation that an attack has occurred | [An attack signature is a pattern used to identify either a single packet or a series of packets that, when combined, execute an attack.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=324446311&rowid=407&noteMenuToggle=0&leftMenuState=1#answer.N501) |
| **18.** | What is a method used to defeat an IDS signature match?   1. Anomaly detection 2. Tunneling 3. Packet smashing 4. Buffer overflows | [Tunneling is a method used to defeat an IDS signature match.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=324446311&rowid=407&noteMenuToggle=0&leftMenuState=1#answer.N529) |
| **19.** | You are reviewing a Snort output report with the following content:  10/17-20:28:15.014784 0:10:5A:1:D:5B -> 0:2:B3:87:84:25 type:0x800 len:0x3C  192.168.1.4:1244 -> 192.168.1.67:443 TCP TTL:128 TOS:0x0 ID:39235  IpLen:20 DgmLen:40 DF  \*\*\*A\*\*\*\* Seq: 0xA18BBE Ack: 0x69749F36 Win: 0x2238 TcpLen: 20  0x0000: 00 02 B3 87 84 25 00 10 5A 01 0D 5B 08 00 45 00 .....%..Z..[..E.  0x0010: 00 28 99 43 40 00 80 06 DD F4 C0 A8 01 04 C0 A8 .(.C@...........  0x0020: 01 43 04 DC 01 BB 00 A1 8B BE 69 74 9F 36 50 10 .C........it.6P.  0x0030: 22 38 6E 63 00 00 00 00 00 00 00 00 "8nc........  What TCP flags are set in the packet?   1. ACK 2. SYN 3. FIN 4. RST | [***A**** indicates the ACK flag is set.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=324446311&rowid=407&noteMenuToggle=0&leftMenuState=1#answer.N554) |
| **20.** | A Snort file has been retrieved with the following output:  10/17-20:28:15.080091 0:2:B3:87:84:25 -> 0:10:5A:1:D:5B type:0x800 len:0x13B  192.168.1.67:443 -> 192.168.1.4:1244 TCP TTL:64 TOS:0x0 ID:6664  IpLen:20 DgmLen:301 DF  \*\*\*AP\*\*\* Seq: 0x6974A4F2 Ack: 0xA18F51 Win: 0x1E51 TcpLen: 20  0x0000: 00 10 5A 01 0D 5B 00 02 B3 87 84 25 08 00 45 00 ..Z..[.....%..E.  0x0010: 01 2D 1A 08 40 00 40 06 9C 2B C0 A8 01 43 C0 A8 .-..@.@..+...C..  0x0020: 01 04 01 BB 04 DC 69 74 A4 F2 00 A1 8F 51 50 18 ......it.....QP.  0x0030: 1E 51 5B AF 00 00 17 03 01 01 00 9D 6D 31 27 DB .Q[.........m1'.  0x0040: 5C 57 B7 39 48 C5 FE 3C 92 77 65 E4 95 49 F4 C5 \W.9H..<.we..I..  0x0050: 5B 98 CB A2 A5 F9 DF C1 F1 6D A2 1A 22 04 E4 DB [........m.."...  0x0060: 4A 1F 18 A9 F8 11 54 57 E6 AF 9A 6C 55 43 8D 37 J.....TW...lUC.7  0x0070: 76 E9 DB 61 2C 62 63 3C 7D E0 F4 08 E0 44 96 03 v..a,bc<}....D..  0x0080: 72 72 16 0C 87 B9 BC FF 08 52 C1 41 22 59 D7 B9 rr.......R.A"Y..  0x0090: 8E 4B 77 DE B8 11 AE AF B2 CB 8D 01 92 E8 26 4A .Kw...........&J  0x00A0: 8C 24 00 8E C3 07 36 7F 84 9F 08 AF 2B 83 F8 13 .$....6.....+...  0x00B0: 1F 61 93 A8 2E 9D 5E 11 A1 DE CF 5E CF 1A 69 1B .a....^....^..i.  0x00C0: 24 F9 A8 B1 CF C7 6C 08 69 ED BF 75 0A 46 C6 63 $.....l.i..u.F.c  0x00D0: CF D2 29 5B 2D 25 C1 44 0E 3F 4C 40 8D 30 75 74 ..)[-%.D.?L@.0ut  0x00E0: A4 C3 06 90 45 65 AC 73 0C C8 CD 4E 0E 22 DD C3 ....Ee.s...N."..  0x00F0: 37 48 FD 8B E6 77 02 9C 76 84 3F E9 7C 0E 9F 28 7H...w..v.?.|..(  0x0100: 06 C1 07 B8 88 4D 22 F2 D0 EF EA B4 37 40 F4 6D .....M".....7@.m  0x0110: F8 79 47 25 85 AC 12 BB 92 94 0E 66 D9 2C 88 53 .yG%.......f.,.S  0x0120: F7 25 D7 DE 44 BF FF F2 54 4F 5B EF AB 6E E1 A0 .%..D...TO[..n..  0x0130: 38 BB DD 36 BF 5B 26 65 58 F8 8A 8..6.[&eX..  What is the web client's port number?   1. 443 2. 1244 3. 64 4. 080091 | [The destination address is 192.168.1.4:1244 and 1244 indicates the client port number. The source port of 443 indicates an HTTPS server.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=324446311&rowid=407&noteMenuToggle=0&leftMenuState=1#answer.N587) |

**Answers**

|  |  |
| --- | --- |
| **1.** | An NIDS performs attack recognition for an entire network. |
| **2.** | Covert\_TCP passes through a firewall by sending one byte at a time of a file in the IP header. |
| **3.** | Sobek is a honeypot-detection tool. |
| **4.** | A honeypot is a system designed to attract and identify hackers. |
| **5.** | ADMmutate is a tool used to modify an attack script to bypass an IDS's signature detection. |
| **6.** | A reverse WWW shell occurs when a compromised web client makes a connection back to a hacker's computer and is able to pass through a firewall. |
| **7.** | The hacker's system, which is acting as a web server, uses port 80. |
| **8.** | Use the command snort –l c:\snort\log –c C:\snort\etc\snort.conf –A console to install and run the Snort program. |
| **9.** | Snort is a sniffer, HIDS, and traffic-logging tool. |
| **10.** | Signature analysis and anomaly detection are the ways an IDS detects instruction attempts. |
| **11.** | The destination port 443 indicates the traffic destination is an HTTPS server. |
| **12.** | The HOME\_NET variable is used in a snort.conf file to identify the local network. |
| **13.** | The rule location is identified by the RULE\_PATH variable in a snort.conf file. |
| **14.** | Rule Action, Protocol, Source Address, and Destination Address are all included in a Snort rule header. HOME\_NET is the variable to define the Internal Network in thesnort.conf file. |
| **15.** | This Snort option associates a high priority to this alert by giving it an *attack class* of attempted-admin. |
| **16.** | Snort rules and the Snort Engine need to be installed separately during installation of Snort. |
| **17.** | An attack *signature* is a pattern used to identify either a single packet or a series of packets that, when combined, execute an attack. |
| **18.** | Tunneling is a method used to defeat an IDS signature match. |
| **19.** | \*\*\*A\*\*\*\* indicates the ACK flag is set. |
| **20.** | The destination address is 192.168.1.4:1244 and 1244 indicates the client port number. The source port of 443 indicates an HTTPS server. |