Security+ Practice Questions Exam Cram 2 (Exam SYO-101)

International Standard Book Number: 0789731517

Warning and Disclaimer

When reviewing corrections, always check the print number of your book. Corrections are made to printed books with each subsequent printing. To determine the print number of your book, view the copyright page. The print number is the right-most number on the line below the "First Printing" line. For example, the following indicates that this is the 1st printing of this title and it was printed in May 2003.

First Printing: May 2003

06 05 04 03 4 3 2 1

First Printing Corrections

Pg	Error	Correction
1	General Security Concepts, Question 1 There are many security concepts that have turned into well-known acronyms. Which of the following refer to the security acronym, CIA? a. Central Intelligence Agency b. Confidentiality, integrity, and availability c. Confidence, intelligence, and accountability d. Confidentiality, integrity, and authentication	Should be There are many security concepts that have turned into well-known acronyms. Which of the following refer**s** to the **network** security acronym, CIA? a. Central Intelligence Agency b. Confidentiality, integrity, and availability c. Confidence, intelligence, and accountability d. Confidentiality, integrity, and authentication
1	Objective 1.1, Question 2 Which of the following are reasonable ~~examples~~ of denying access to network resources? (Select all that apply.) a. Domain names b. Computer IP addresses c. Computer names d. ~~Brute force~~	Should be Which of the following are reasonable **methods** of denying access to network resources? (Select all that apply.) a. Domain names b. Computer IP addresses c. Computer names d. **Dictionary names**
4	Question 12 There are several models that relate to network security. Which of the following is generally not associated with Mandatory Access Control (MAC)? a. The Biba Model b. The Bell La-Padula Model c. The Clark Wilson Model d. Sensitivity ~~labels~~	Should be There are several models that relate to network security. Which of the following is generally not associated with Mandatory Access Control (MAC)? a. The Biba Model b. The Bell La-Padula Model c. The Clark Wilson Model d. Sensitivity **Model**

5	Question 3 Which of the following statements ~~is~~ true about Discretionary Access Control methods? (Select all that apply.) a. They are more flexible than Mandatory Access Control. b. They are concerned with the flow of information. c. They use security labels. d. They are widely used in commercial environments	Should be Which of the following statements **are** true about Discretionary Access Control methods? (Select all that apply.) a. They are more flexible than Mandatory Access Control. b. They are concerned with the flow of information. c. They use security labels. d. They are widely used in commercial environments
10	Question 2 Are system clocks important in a Kerberos system? a. Yes, Kerberos must use a remote time Server, which all hosts use. b. Yes, clocks must be synchronized between all hosts on the network to create reliable timestamps in granting tickets. c. Yes, without Kerberos, system clocks would not function properly. d. No, Kerberos uses operating system-based authentication, not ~~system clocks~~	Should be Are system clocks important in a Kerberos system? a. Yes, Kerberos must use a remote time Server, which all hosts use. b. Yes, clocks must be synchronized between all hosts on the network to create reliable timestamps in granting tickets. c. Yes, without Kerberos, system clocks would not function properly. d. No, Kerberos uses operating system-based authentication, not **system-clock based.**
23	Question 12 ~~Which of the following is another name for ICMP storms?~~ ~~a. UDP flooding~~ ~~b. TCP flooding~~ ~~c. Data link layer storms~~ ~~d. Broadcast storms~~	Should be **One method of DoS is an ICMP storm. What does ICMP stand for?** a. **Internet Control Mail Protocol** b. **Internal Control Message Protocol** c. **Internal Control Mail Protocol** d. **Internet Control Message Protocol**

23	Question 13 Broadcast storms ~~are also known as~~ ~~a. ICMP storms~~ ~~b. TCP flooding~~ ~~c. UDP broadcasting~~ ~~d. SYN attack~~	Should be Broadcast storms **can be prevented by which of the following?** **a. Spanning Tree Protocol** **b. Antivirus software** **c. Bridges rather than switches** **d. Hubs rather than bridges**
30	Question 1 What type of attack uses an application to capture and manipulate your network packets? ~~a. DDOS~~ ~~b. Server Spoofing~~ ~~c. Spoofing~~ d. Man in the Middle	Should be What type of attack uses an application to capture and manipulate your network packets? **a. DDoS** **b. Network Sniffing** **c. Server Spamming** d. Man in the Middle
35	Question 1 Which specific method does L0pht Crack utility use to attempt to gain user authentication information? ~~(Select the best answer.)~~ a. Strong Key b. Replay c. Brute Strength d. Dictionary	Should be Which specific method does L0pht Crack utility use to attempt to gain user authentication information? a. Strong Key **attack** b. Replay **attack** c. Brute Strength **attack** d. Dictionary **attack**

38	Question 5 Your network is being exploited by more traffic than expected. What kind of attack may be occurring? a. ~~Ping of Broadcasts~~ b. Violent Death c. Overflow of Logic d. Buffer Overflow	Should be Your network is being exploited by more traffic than expected. What kind of attack may be occurring? a. **Network Broadcast Ping** b. Violent Death c. Overflow of Logic d. Buffer Overflow
38	Question 8 What occurs when a string of data is sent to a buffer that is larger than the buffer was designed to ~~handle.~~ a. Brute Force attack b. Buffer Overflow c. Man in the Middle attack d. Blue Screen of Death	Should be What occurs when a string of data is sent to a buffer that is larger than the buffer was designed to **handle?** a. Brute Force attack b. Buffer Overflow c. Man in the Middle attack d. Blue Screen of Death
44	Objective 1.1.1, Answer 2 a, c, and d. MAC places sensitivity labels on both subjects and objects.	Should be a, c, and d. MAC places sensitivity labels on both subjects and objects. **Folders are objects and all the rest are subjects.**
48	Objective 1.2.3, Answer 5 d. Third parties generally ~~issue~~ a Certificate Authority.	Should be d. Third parties generally **function as** a Certificate Authority **(CA).**
52	Answer 12 d. ~~Broadcast storm is another name for ICMP storm.~~	Should be d. **ICMP stands for Internet Control Message Protocol.**
52	Answer 13 a. ~~ICMP storms and broadcast storms are similar terms.~~	Should be a. **Broadcast storm can be prevented by the Spanning Tree Protocol.**
55	Objective 1.4.11, Answer 1 c. Sniffing is used to capture sensitive pieces of information, ~~such~~ user passwords, as they pass through the network.	Should be c. Sniffing is used to capture sensitive pieces of information, **like** user passwords, as they pass through the network.

56	Objective 1.4.12, Answer 1 c. ~~Attacks on software vulnerabilities is the best explanation of Software Exploitation~~	Should be c. **Software Exploitations are attacks on software vulnerabilities.**
59	Objective 2.1.1, Question 1 The IEEE 802.1x is a standard for remote access. Which of the following items would the 802.1x standard be concerned with? (Select all that apply.) a. Authentication for remote access to a centralized LAN b. Simple Network Management Protocol (SNMP) c. RADIUS server d. ~~Extensive~~ Authentication Protocol (EAP)	Should be The IEEE 802.1x is a standard for remote access. Which of the following items would the 802.1x standard be concerned with? (Select all that apply.) a. Authentication for remote access to a centralized LAN b. Simple Network Management Protocol (SNMP) c. RADIUS server d. **Extensible** Authentication Protocol (EAP)
60	Question 4 You want to have a secure connection. You decide on establishing a VPN. Which of the following can be used to accomplish your goal? ~~(Select all that apply.)~~ a. X.509 b. TLS c. S/MIME d. L2TP	Should be You want to have a secure connection. You decide on establishing a VPN. Which of the following can be used to accomplish your goal? a. X.509 b. TLS c. S/MIME d. L2TP
63	Objective 2.1.5, Question 4 Which of the following Virtual Private Network (VPN) protocols uses Transmission Control Protocol (TCP) port ~~1721~~? a. L2F b. L2TP c. PPTP d. MPPE	Should be Which of the following Virtual Private Network (VPN) protocols uses Transmission Control Protocol (TCP) port **1701**? a. L2F b. L2TP c. PPTP d. MPPE
69	Question 4 What does S/MIME stand for? a. Secure Multipurpose Internet Mail ~~Expansion~~ b. Separate Messages in My Email c. Secure Multi Interface Message Extensions d. Separate Mail Internet Extensions	Should be What does S/MIME stand for? a. Secure Multipurpose Internet Mail **Extensions** b. Separate Messages in My Email c. Secure Multi Interface Message Extensions d. Separate Mail Internet Extensions

74	Question 2 Your boss wants to establish growth through use of secure Web commerce. You create a great Web site with all kinds of pictures and special links to equipment that your company sells. Which of the following should you use for security? a. ~~Secure Sockets Layer (SSL)~~ b. ~~Secure Shell (SSH)~~ c. Layer Two Tunneling Protocol (L2TP) d. IP Security (IPSec)	Should be Your boss wants to establish growth through use of secure Web commerce. You create a great Web site with all kinds of pictures and special links to equipment that your company sells. Which of the following should you use for security? a. **Secure Shell (SSH)** b. **Secure Sockets Layer (SSL)** c. Layer Two Tunneling Protocol (L2TP) d. IP Security (IPSec)
84	Objective 2.5.2, Question 2 Which of the following applies to anonymous accounts on FTP servers? a. Crackers can use these accounts to overwrite files b. Anonymous FTP accounts are still very popular c. In order to increase security, anonymous FTP logins should be allowed d. There is no serious security concern when using anonymous FTP accounts	Should be Which of the following **apply** to anonymous accounts on FTP servers? **(Select all that apply.)** a. Crackers can use these accounts to overwrite files b. Anonymous FTP accounts are still very popular c. In order to increase security, anonymous FTP logins should be allowed d. There is no serious security concern when using anonymous FTP accounts
87	Question 4 Which of the following items ~~are~~ not required when employing 802.11b Wireless networks? a. A modem b. A wireless NIC c. A station d. An access point	Should be Which of the following items **is** not required when employing 802.11b Wireless networks? a. A modem b. A wireless NIC c. A station d. An access point
95	Objective 2.1.3, Answer 2 a. Remote Access Dial-In User Service (RADIUS) is a remote authentication method that provides a central server for all remote network access, but provides less security than TACACS.	Should be a. Remote Access Dial-In User Service (RADIUS) is a remote authentication method that provides a central server for all remote network access, but provides less security than TACACS**+**.
96	Objective 2.1.5, Answer 4 b. L2TP uses Transmission Control Protocol (TCP) port ~~1721~~. Notice that there is only one "P" in L2TP.	Should be b. L2TP uses Transmission Control Protocol (TCP) port **1701.** Notice that there is only one "P" in L2TP.

98	Objective 2.2.1, Answer 4 a. S/MIME stands for Secure Multipurpose Internet Mail ~~Expansions~~	Should be a. S/MIME stands for Secure Multipurpose Internet Mail **Extensions**
101	Objective 2.3.4.3, Answer 1 d. A buffer attack could be the cause of this situation.	Should be d. A buffer **overflow** attack could be the cause of this situation.
107	Objective 3.1.1, Question 1 Your company receives Internet access through a network or gateway server. Which of the following devices is best suited to protect resources and subnet your LAN directly on the network server? a. DSL Modem b. ~~A multi-homed firewall~~ c. VLAN d. ~~A brouter that acts both as a bridge and a router~~	Should be Your company receives Internet access through a network or gateway server. Which of the following devices is best suited to protect resources and subnet your LAN directly on the network server? a. DSL Modem b. **Firewall** c. VLAN d. **Brouter**
143	Objective 3.2, Answer 2 c. You use a crossover cable directly between two ~~like components, like between two~~ computers.	Should be c. You use a crossover cable directly between two computers.
148	Objective 3.5.2.2.1, Answer 2 a. FTP = ports 20 (data) and 21 (session), Telnet = port 23, SMTP = port 25, Wins replication = port 42, DNS = 53, bootp = 67, IIS Gopher = 70, HTTP = 80, ~~pop3~~ = 110, NNTP = 119, RPC = port 135, NetBIOS over IP = 139, SNMP = 161, and SSL = ~~44 3.~~	Should be a. FTP = ports 20 (data) and 21 (session), Telnet = port 23, SMTP = port 25, Wins replication = port 42, DNS = 53, bootp = 67, IIS Gopher = 70, HTTP = 80, **POP3** = 110, NNTP = 119, RPC = port 135, NetBIOS over IP = 139, SNMP = 161, and SSL = **443**.

189	Objective 5.1.3.1, Question 1 Your company headquarters works with highly sensitive data and the president now insists on using wireless cell technology for his private office, which happens to overlook the park. Which ~~one~~ of the following security measures would you recommend to increase your network ~~security.~~ a. Consider placing wireless antennae near windows for greater connectivity ~~b. Consider shielding the outer walls for greater security~~ ~~c. Consider shielding walls and ceilings for greater security~~ d. Consider removing windows for total isolation	Should be Your company headquarters works with highly sensitive data and the president now insists on using wireless cell technology for his private office, which happens to overlook the park. **Which** of the following security measures would you recommend to increase your network **security?** a. Consider placing wireless antennae near windows for greater connectivity **b. Consider shielding walls and ceilings for greater security** **c. Consider shielding the outer walls for greater security** d. Consider removing windows for total isolation
208	Objective 5.7.2, Question 1 Which of the following Risk Analysis Formulas is a useful tool that is based upon these three concepts: Single Loss Expectancy, Annualized Rate of Occurrence and Annual Loss Expectancy? a. SLE + ARO = ALE b. SLE x ARO = ALE c. ALE - ARO = SLE d. ~~ALE - ARO = SLE~~	Should be Which of the following Risk Analysis Formulas is a useful tool that is based upon these three concepts: Single Loss Expectancy, Annualized Rate of Occurrence and Annual Loss Expectancy? a. SLE + ARO = ALE b. SLE x ARO = ALE c. ALE - ARO = SLE d. **ALE x ARO = SLE**
209	Objective 5.7.3, Question 2 Which of the following threats will most likely produce a Risk that affects Confidentiality, Integrity and Availability? a. Fraud b. ~~Natural disaster~~ c. ~~Physical theft~~ d. Terrorism	Should be Which of the following threats will most likely produce a Risk that affects Confidentiality, Integrity and Availability? a. Fraud b. **Physical theft** c. **Natural disaster** d. Terrorism
227	c. An Incident Response Policy provides employees the guidelines in cases of a physical disaster, network disaster or security ~~attack?~~	c. An Incident Response Policy provides employees the guidelines in cases of a physical disaster, network disaster or security **attack.**

New Questions

New	1.4.1	**Which of the following statements are characteristics of a Denial of Service (DoS) attack? (Select two correct answers.)** **a. Results in theft of information** **b. Does not result in theft of information** **c. Results in inability to use a system** **d. Does not result in inability to use a system**
New	1.5.1-1	**Which of the following best describes a computer virus? (Select three.)** **a. Infects other programs** **b. Spreads to other programs** **c. Uses malicious code** **d. Forces users to open the attachment**
New	1.5.1-2	**Which of the following describes a virus? (Select all that apply.)** **a. Exists to damage computer systems** **b. Has no productive purpose** **c. Uses a piece of malicious code** **d. Replicates itself**
New	1.5.1-3	**When comparing malicious code, which of the following propagates when the host is running after copying itself into the host program?** **a. Back Door attacks** **b. Worms like Code Red II** **c. Viruses like Melissa** **d. Trojan horses like ILOVEYOU**
New	1.5.2-1	**Which of the following are applicable to Trojan horses? (Select all that apply.)** **a. Makes use of an application that appears to perform a useful function** **b. Hides malicious code silently** **c. May trick the user unknowingly** **d. May use Social Engineering techniques**

New	1.5.2-2	**Which of the following do not replicate or attach to other files?** **a. Worms** **b. Viruses** **c. Trojan horses** **d. Logic bombs**
New	1.5.3-1	**Your company just fired the previous system administrator. After one week, you notice that files start deleting from the DNS server. What could be the cause?** **a. Logic bomb** **b. Worm** **c. Trojan horse** **d. Virus**
New	1.5.4-1	**Which of the following could be considered a computer parasite?** **a. Logic bomb** **b. Worm** **c. Trojan horse** **d. Virus**
New	1.5.4-2	**What are Sadmind, Adore, and Morris examples of?** **a. Logic bombs** **b. Worms** **c. Trojan horses** **d. Viruses**
New	1.6-1	**Someone just played a bad hoax on you, tricking you to send an e-mail to all your loved ones, and then asking if you if they could help repair your troubled computer. What type of attack does this represent?** **a. Logic bomb** **b. Worm** **c. Virus** **d. Social Engineering**

New	1.7-1	**Which mode allows computers on an Ethernet network to be configured to monitor or read and record all network traffic?** **a. Silent mode** **b. Listening mode** **c. Scanning mode** **d. Promiscuous mode**
New	1.7-2	**Which of the following can be set for auditing as either successful or unsuccessful events? (Select all that apply.)** **a. Specific files, including system files** **b. Select folders** **c. Network print devices** **d. Specific files, including hidden files**
New	1.7-3	**What do Nmap, Security Analyzer, and Nessus have in common?** **a. They are network auditing tools** **b. They are network topology tools** **c. They are network hardware tools** **d. They are network software tools**
New	1.4.1	**b and c.**
New	1.5.1-1	**a, b, and c**
New	1.5.1-2	**a, b, c, and d**
New	1.5.1-3	**c**
New	1.5.2-1	**a, b, c, and d**
New	1.5.2-2	**c**
New	1.5.3-1	**a**
New	1.5.4-1	**b**
New	1.5.4-2	**b**
New	1.6-1	**d**
New	1.7-1	**d**
New	1.7-2	**a, b, c, and d**
New	1.7-3	**a**
New	1.4.1	**b and c. Characteristics of a DoS attack results in an inability to use a system, but does not primarily result in theft of information.**

New	1.5.1-1	**a, b, and c. A virus uses malicious code to infect other programs and spreads to other programs. A virus is a program that can infect other programs by modifying them to include a version of itself.**
New	1.5.1-2	**a, b, c, and d. A virus uses malicious code to infect other programs and spread to other programs. A virus is a program that can infect other programs by modifying them to include a version of itself. It exists to damage computer systems and has no productive purpose.**
New	1.5.1-3	**c. Viruses, like the Melissa virus, propagates when the host is running after copying itself into the host program.**
New	1.5.2-1	**a, b, c, and d. A Trojan horse generally uses Social Engineering techniques to trick the user unknowingly. The Trojan horse makes use of an application that appears to perform a useful function by quietly hiding malicious code.**
New	1.5.2-2	**c. A Trojan horse does not replicate or attach to other files as do viruses. Some are used as back-door access tools for product-data gathering.**
New	1.5.3-1	**a. Programs like viruses, Trojan horses, worms, and logic bombs are malicious code that when activated cause Denial of Service or destruction, or modification of the information on computers. Logic bombs are triggered events.**
New	1.5.4-1	**b. A worm is a type of malicious code that behaves like a tapeworm or parasite in your computer.**
New	1.5.4-2	**b. These, along with many others, are examples of worms.**
New	1.6-1	**d. Anytime a user is tricked into doing something, Social Engineering is the cause. Crackers that take advantage of human behaviors may be only playing a mean joke initially.**
New	1.7-1	**d. Promiscuous mode allows computers on an Ethernet network to be configured to monitor or read and record all network traffic.**

New	1.7-2	**a, b, c, and d. Given adequate resources, auditing can be established on nearly any chosen file, folder, or network device.**
New	1.7-3	**a. Nmap, Security Analyzer, and Nessus are network auditing tools to scan the network to identify security weaknesses.**
New	4.2.1	**Which of the following OSI layers provides Confidentiality? (Select all that apply.)** **a. Network layer 3** **b. Transport layer 4** **c. Session layer 5** **d. Presentation layer 6**
New	4.2.1	**a, b, and d.**
New	4.2.1	**a, b and d. Layers 3, 5 and 6 offer confidentiality.**
New	5.3.2	**Which of the following offers High Availability and Disaster Recovery, but has a single point of vulnerability?** **a. Server clustering** **b. Tape Backup** **c. RAID 0** **d. Full Backup**
New	5.3.2	**a.**
New	5.3.2	**a. Server clustering offers High Availability and Disaster Recovery, but has a single point of vulnerability.**

Second Printing Corrections

Pg	**Error**	Correction
220	Objective 5.7.3; answer 2: B	**C**

230	Objective 5.7.3; answer 2: 2. **b.** Of the items listed, physical theft will most likely affect confidentiality, integrity, and availability.	 2. **c.** Of the items listed, physical theft will most likely affect confidentiality, integrity, and availability.

Third Printing Corrections

55	c. Sniffing is used to capture sensitive pieces of information, ~~such as~~ user passwords, as they pass through the network.	c. Sniffing is used to capture sensitive pieces of information, **like** user passwords, as they pass through the network.
148	a. FTP = ports 20 (data) and 21 (session), Telnet = port 23, SMTP = port 25, Wins replication = port 42, DNS = 53, bootp = 67, IIS Gopher = 70, HTTP = 80, pop3 = 110, NNTP = 119, RPC = port 135, NetBIOS over IP = 139, SNMP = 161, and SSL = ~~44s3~~.	a. FTP = ports 20 (data) and 21 (session), Telnet = port 23, SMTP = port 25, Wins replication = port 42, DNS = 53, bootp = 67, IIS Gopher = 70, HTTP = 80, POP3 = 110, NNTP = 119, RPC = port 135, NetBIOS over IP = 139, SNMP = 161, and SSL = **443**.
173	Objective 4.2, answer 4: 4. ~~d.~~	 4. **a.**
178	Objective 4.2, answer 4: 4. ~~d.~~ When dealing with network security, C.I.A. is an acronym that implies Confidentiality, Integrity, and Availability.	 4. **a.** When dealing with network security, C.I.A. is an acronym that implies Confidentiality, Integrity, and Availability.

189	Objective 5.1.3.1: Wireless Cells Answers a. Consider placing wireless antennae near windows for greater connectivity ~~b. Consider shielding the outer walls for greater security~~ ~~c. Consider shielding walls and ceilings for greater security~~ d. Consider removing windows for total isolation	 a. Consider placing wireless antennae near windows for greater connectivity **b. Consider shielding the walls and ceilings for greater security** **c. Consider placing wireless antennae near outer walls for greater connectivity security** d. Consider removing windows for total isolation

New 1.4.1-21	*NB: add corresponding quick answer and detailed answers in margin.	21. Which of the following statements are characteristics of a Denial of Service (DoS) attack? (Select two correct answers.) a. Results in theft of information b. Does not result in theft of information c. Results in inability to use a system d. Does not result in inability to use a system
New 1.5.1-1	Which of the following best describes a computer virus? (Select ~~three~~.) a. ~~A virus~~ infects other programs b. ~~A virus~~ spreads to other programs c. ~~A virus~~ uses malicious code d. ~~A virus~~ forces users to open the attachment	Which of the following best describes a computer virus? (Select **three**.) a. Infects other programs b. Spreads to other programs c. Uses malicious code d. Forces users to open the attachment

New 1.5.1-2	Which of the following describes a virus? (Select all that apply.) a. ~~A virus~~ exists to damage computer systems b. ~~A virus~~ has no productive purpose c. ~~A virus~~ uses a piece of malicious code d. ~~A virus~~ replicates itself	Which of the following describes a virus? (Select all that apply.) a. Exists to damage computer systems b. Has no productive purpose c. Uses a piece of malicious code d. Replicates itself
New 1.5.1-3	Which of the following types of malicious code propagates by copying itself into the host program when the host is running?	**When comparing malicious code, which of the following propagates when the host is running after copying itself into the host program?** **a. Back Door attacks** **b. Worms like Code Red II** **c. Viruses like Melissa** **d. Trojan horses like ILOVEYOU**
New 1.5.2-2	What type of malicious code does not replicate or attach to other files? a. Worm b. Virus c. Trojan horse d. Logic bomb	**Which of the following do** not replicate or attach to other files? a. Worm**s** b. Virus**es** c. Trojan horse**s** d. Logic bomb**s**

New 1.7-2	Which of the following can be set for auditing as either successful or unsuccessful events? (Select all that apply.) a. System files b. Select folders c. Network print devices d. Hidden files	Which of the following can be set for auditing as either successful or unsuccessful events? (Select all that apply.) a. **Specific files, including** system files b. Select folders c. Network print devices d. **Specific files, including** hidden files
New 1.4.1-21		b and c.
New 1.5.1-1	a, b, and c. A virus uses malicious code to infect other programs by modifying ~~those programs~~ to include a version of itself.	a, b, and c. A virus uses malicious code to infect other programs and spreads to other programs. **A virus is a program that can infect other programs** by modifying **them** to include a version of itself.
New 1.5.1-2	a, b, c, and d. A virus uses malicious code to infect other programs by modifying ~~those programs~~ to include a version of itself. It exists to damage computer systems and has no productive purpose.	a, b, c, and d. A virus uses malicious code to infect other programs and spreads to other programs. **A virus is a program that can infect other programs** by modifying **them** to include a version of itself. It exists to damage computer systems and has no productive purpose.
New 1.5.1-3	Viruses, like the Melissa virus, propagate ~~by copying themselves into the host program when the host is running.~~	c. Viruses, like the Melissa virus, propagate **when the host is running after copying itself into the host program.**
New 1.5.2-2	c. A Trojan horse does not replicate or attach to other files as viruses do. Some are used as back-door access tools for product-data gathering.	c. A Trojan horse does not replicate or attach to other files as **do viruses**. Some are used as back-door access tools for product-data gathering.
New 1.5.3-1	a. Programs like viruses, Trojan horses, worms, and logic bombs are malicious code that when activated cause Denial of Service or destruction, or modification of the information on computers. Logic bombs are triggered ~~by~~ events.	a. Programs like viruses, Trojan horses, worms, and logic bombs are malicious code that when activated cause Denial of Service or destruction, or modification of the information on computers. Logic bombs are triggered events.
New 1.5.4-2	~~Sadmind, Adore, and Morris,~~ along with many others, are examples of worms.	b. **These** along with many others, are examples of worms.

New 1.6-1	d. ~~Whenever~~ a user is tricked into doing something, Social Engineering is the cause. Crackers that take advantage of human behaviors may be only playing a mean joke initially.	d**. Anytime** a user is tricked into doing something, Social Engineering is the cause. Crackers that take advantage of human behaviors may be only playing a mean joke initially.
New 1.7-3	a. Nmap, Security Analyzer, and Nessus are network auditing tools to scan the network to identify security weaknesses ~~by scanning the network~~.	a. Nmap, Security Analyzer, and Nessus are network auditing tools to scan the network to identify security weaknesses.

This errata sheet is intended to provide updated technical information. Spelling and grammar misprints are updated during the reprint process, but are not listed on this errata sheet.