Mis chapter 8

A21) _____ refers to policies, procedures, and technical measures used to prevent unauthorized access, alternation, theft, or physical damage to information systems.

A) " Security"

B) " Controls"

C) " Benchmarking"

D) " Algorithms"

D22) _____ refers to all of the methods, policies, and organizational procedures that ensure the safety of the organization's assets, the accuracy and reliability of its accounting records, and operational adherence to management standards.

A) " Legacy systems"

B) " SSID standards"

C) " Vulnerabilities"

D) " Controls"

C23) Which of the following is not one of the challenges in securing wireless networks?

A) broadcasted SSIDs

B) scannability of radio frequency bands

C) SQL injection attacks

D) geographic range of wireless signals

C24) Electronic data are more susceptible to destruction, fraud, error, and misuse because information systems concentrate data in computer files that

A) are usually bound up in legacy systems that are difficult to access and

difficult to correct in case of error.

B) are not secure because the technology to secure them did not exist at the time the files were created.

C) have the potential to be accessed by large numbers of people and by groups outside of the organization.

D) are frequently available on the Internet.

A25) All of the following are methods of ensuring software quality except for

A) systems analysis.

B) walkthroughs.

C) software testing.

D) internal corporate back-end system.

B26) Sniffing is a security challenge that is most likely to occur in which of the following points of a corporate network?

A) client computer

B) communications lines

C) corporate servers

D) internal corporate back-end system

B27) Inputting data into a poorly programmed Web form in order to disrupt a company's systems and networks is called

A) a Trojan horse.

B) an SQL injection attack.

C) key logging.

D) a DDoS attack.

A28) The Internet poses specific security problems because

A) it was designed to be easily accessible.

B) Internet data is not run over secure lines.

C) Internet standards are universal.

D) it changes so rapidly.

C29) Which of the following statements about the Internet security is not true?

A) The use of P2P networks can expose a corporate computer to outsiders.

B) A corporate network without access to the Internet is more secure than one provides access.

C) VoIP is more secure than the switched voice network.

D) Instant messaging can provide hackers access to an otherwise secure network.

A30) An independent computer program that copies itself from one computer to another over a network is called a

A) worm.

B) Trojan horse.

C) bug.

D) pest.

D31) A salesperson clicks repeatedly on the online ads of a competitor's in order to drive the competitor's advertising costs up. This is an example of

A) phishing.

B) pharming.

C) spoofing.

D) click fraud.

A32) In 2004, ICQ users were enticed by a sales message from a supposed anti-virus vendor. On the vendor's site, a small program called Mitglieder was downloaded to the user's machine. The program enabled outsiders to infiltrate the user's machine. What type of malware is this an example of?

A) Trojan horse

B) virus

C) worm

D) spyware

B33) Redirecting a Web link to a different address is a form of

A) snooping.

B) spoofing.

C) sniffing.

D) war driving.

D34) A keylogger is a type of

A) worm.

B) Trojan horse.

C) virus.

D) spyware.

C35) Hackers create a botnet by

A) infecting Web search bots with malware.

B) using Web search bots to infect other computers.

C) causing other people's computers to become " zombie" PCs following a

master computer.

D) infecting corporate servers with " zombie" Trojan horses that allow undetected access through a back door.

A36) Using numerous computers to inundate and overwhelm the network from numerous launch points is called a(n) _____ attack.

A) DDoS

B) DoS

C) SQL injection

D) phishing

C37) Which of the following is not an example of a computer used as a target of crime?

A) knowingly accessing a protected computer to commit fraud

B) accessing a computer system without authority

C) illegally accessing stored electronic communication

D) threatening to cause damage to a protected computer

D) Which of the following is not an example of a computer used as an instrument of crime?

A) theft of trade secrets

B) intentionally attempting to intercept electronic communication

C) unauthorized copying of software

D) breaching the confidentiality of protected computerized data

A39) Approximately how many new threats from malware were detected by Internet security firms in 2012?

A) 400 thousand

B) 4 million

C) 40 million

D) 400 million

B40) An example of phishing is

A) setting up bogus Wi-Fi hot spots.

B) setting up a fake medical Web site that asks users for confidential information.

C) pretending to be a utility company's employee in order to garner information from that company about their security system.

D) sending bulk e-mail that asks for financial aid under a false pretext.

D41) Evil twins are

A) Trojan horses that appears to the user to be a legitimate commercial software application.

B) e-mail messages that mimic the e-mail messages of a legitimate business.

C) fraudulent Web sites that mimic a legitimate business's Web site.

D) bogus wireless network access points that look legitimate to users.

A42) Pharming involves

A) redirecting users to a fraudulent Web site even when the user has typed in the correct address in the Web browser.

B) pretending to be a legitimate business's representative in order to garner information about a security system.

C) setting up fake Web sites to ask users for confidential information.

D) using e-mails for threats or harassment.

B43) You have been hired as a security consultant for a law firm. Which of the following constitutes the greatest source of security threats to the firm?

A) wireless network

B) employees

C) authentication procedures

D) lack of data encryption

B44) Tricking employees to reveal their passwords by pretending to be a legitimate member of a company is called

A) sniffing.

B) social engineering.

C) phishing.

D) pharming.

B45) How do software vendors correct flaws in their software after it has been distributed?

A) issue bug fixes

B) issue patches

C) re-release software

D) issue updated versions

D46) The HIPAA Act

A) requires financial institutions to ensure the security of customer data.

B) specifies best practices in information systems security and control.

C) imposes responsibility on companies and management to safeguard the accuracy of financial information.

D) outlines medical security and privacy rules.

A47) The Gramm-Leach-Bliley Act

A) requires financial institutions to ensure the security of customer data.

B) specifies best practices in information systems security and control.

C) imposes responsibility on companies and management to safeguard the accuracy of financial information.

D) outlines medical security and privacy rules.

C48) The Sarbanes-Oxley Act

A) requires financial institutions to ensure the security of customer data.

B) specifies best practices in information systems security and control.

C) imposes responsibility on companies and management to safeguard the accuracy of financial information.

D) outlines medical security and privacy rules.

D49) The most common type of electronic evidence is

A) voice-mail.

B) spreadsheets.

C) instant messages.

D) e-mail.

B50) Electronic evidence on computer storage media that is not visible to the average user is called _____ data.

A) defragmented

B) ambient

C) forensic

D) fragmented

A51) Application controls

A) can be classified as input controls, processing controls, and output controls.

B) govern the design, security, and use of computer programs and the security of data files in general throughout the organization.

C) apply to all computerized applications and consist of a combination of hardware, software, and manual procedures that create an overall control environment.

D) include software controls, computer operations controls, and implementation controls.

C52) _____ controls ensure that valuable business data files on either disk or tape are not subject to unauthorized access, change, or destruction while they are in use or in storage.

A) Software

B) Administrative

C) Data security

D) Implementation

C53) Analysis of an information system that rates the likelihood of a security incident occurring and its cost is included in a(n)

A) security policy.

B) AUP.

C) risk assessment.

D) business impact analysis.

A54) A(n) _____ system is used to identify and authorize different categories of system users and specify which portions of the organization's systems each user can access.

A) identity management

B) AUP

C) authentication

D) firewall

D55) Which of the following is not one of the main firewall screening techniques?

A) application proxy filtering

B) static packet filtering

C) NAT

D) secure socket filtering

B56) Rigorous password systems

A) are one of the most effective security tools.

B) may hinder employee productivity.

C) are costly to implement.

D) are often disregarded by employees.

C57) An authentication token is a(n)

A) device the size of a credit card that contains access permission data.

B) type of smart card.

C) gadget that displays passcodes.

D) electronic marker attached to a digital authorization file.

C58) Which of the following is not a trait used for identification in biometric systems?

A) retinal image

B) voice

C) hair color

D) face

A59) A firewall allows the organization to

A) prevent unauthorized communication both into and out of the network.

B) monitor network hot spots for signs of intruders.

C) prevent known spyware and malware from entering the system.

D) all of the above.

A60) In which technique are network communications analyzed to see whether packets are part of an ongoing dialogue between a sender and a receiver?

A) stateful inspection

B) intrusion detection system

C) application proxy filtering

D) packet filtering

B61) Which of the following is the greatest threat that employees pose to an organization's information systems?

A) forgetting passwords

B) lack of knowledge

C) entering faulty data

D) introducing software errors

D62) Currently, the protocols used for secure information transfer over the Internet are

A) TCP/IP and SSL.

B) S-HTTP and CA.

C) HTTP and TCP/IP.

D) SSL, TLS, and S-HTTP.

D63) Most antivirus software is effective against

A) only those viruses active on the Internet and through e-mail.

B) any virus.

C) any virus except those in wireless communications applications.

D) only those viruses already known when the software is written.

B64) In which method of encryption is a single encryption key sent to the receiver so both sender and receiver share the same key?

A) SSL

B) symmetric key encryption

C) public key encryption

D) private key encryption

A65) A digital certificate system

A) uses third-party CAs to validate a user's identity.

B) uses digital signatures to validate a user's identity.

C) uses tokens to validate a user's identity.

D) is used primarily by individuals for personal correspondence.

B66) Downtime refers to periods of time in which a

A) computer system is malfunctioning.

B) computer system is not operational.

C) company or organization is not operational.

D) computer is not online

C67) For 100% availability, online transaction processing requires

A) high-capacity storage.

B) a multi-tier server network.

C) fault-tolerant computer systems.

D) dedicated phone lines.

B68) In controlling network traffic to minimize slow-downs, a technology called _____ is used to examine data files and sort low-priority data from high-priority data.

A) high availability computing

B) deep-packet inspection

C) application proxy filtering

D) stateful inspection

B69) The development and use of methods to make computer systems resume their activities more quickly after mishaps is called

A) high availability computing.

B) recovery oriented computing.

C) fault tolerant computing.

D) disaster recovery planning.

C70) Smaller firms may outsource some or many security functions to

A) ISPs.

B) MISs.

C) MSSPs.

D) CAs.

ONMIS CHAPTER 8 SPECIFICALLY FOR YOUFOR ONLY$13. 90/PAGEOrder NowTags:

- Web Search