Name: _____
Date: _____
Results: _____

Practice Test

"It's time to begin, isn't it?"

Question 1
This is a class of programs that searches your hard drive and floppy disks for any known or potential viruses.

A. Intrusion detection
B. Security identifier
C. Firewall
D. Antivirus software

Question 2
What governs the type of traffic that is and is not allowed through a firewall?
A. Rule base
B. Gateway
C. Access control list
D. Partition

Question 3
What protocol ensures privacy between communicating applications and their users on the Internet?
A. F-Secure
B. Privacy Control Protocol
C. Secure Shell Authentication
D. Transport Layer Security

Question 4
This standard being developed by IBM, Microsoft, Novell and others will allow different manufacturers' biometrics software to interact.
A. IDEA
B. Twofish
C. BioAPI
D. MetricStat

Question 5
This two-level scheme for authenticating network users functions as part of the Web's Hypertext Transfer Protocol.

A. SSL
B. CRAM
C. LUHN formula
D. DES

Question 6
What is the term for an attempt to determine the valid e-mail addresses associated with an e-mail server so that they can be added to a spam database?
A. E-mail harvest
B. Directory harvest attack
C. Spambot attack
D. E-mail validator

Question 7
This is a common type of denial-of-service attack that involves sending more traffic to a network address than the temporary data storage area is intended to hold, thereby shutting down the service and possibly corrupting or overwriting valid data.
A. War dialing
B. Buffer overflow
C. Smurf attack
D. Bucket brigade

Question 8
This is a computer system on the Internet that is expressively set up to attract and trap intruders.
A. Exploit
B. Demilitarized zone
C. Pitfall site
D. Honeypot

Question 9
WEP is a security protocol, specified in 802.11b, that is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN. What does WEP stand for?
A. Wired Equivalent Privacy
B. Wireless Equivalent Protocol
C. Wireless Equivalent Privacy
D. Wired Encryption Protocol

Question 10
What is the name given to a program used to detect unsolicited and unwanted e-mail and prevents those messages from getting to a user's inbox?
A. Anti-spammer
B. Email guard
C. Virus filter
D. Spam filter

Question 11
HTTPS is a Web protocol developed by Netscape and built into its browser that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. What does HTTPS stand for?

A. Hypertext Transfer Protocol over Secure Socket Layer
B. Hypertext Transfer Protocol Security
C. Hypertext Transfer Protocol over Sublayer
D. Hypertext Transfer Protocol Systematics

Question 12
What was SSL used for?

A. Encrypt data as it travels over a network
B. Encrypt passwords for storage in a database
C. Encrypt files located on a Web server
D. Encrypt digital certificates used to authenticate a Web site

Question 13
How does spyware differ from other forms of malware, such as worms and viruses?

A. The delivery mechanism is unaware it contains spyware
B. Spyware installs without the user's knowledge
C. Not all spyware is malicious
D. Spyware replicates itself

Question 14
On average, how long does it take for an unprotected networked computer to be compromised once it is connected to the internet?

A. 1 week
B. 20 minutes
C. 10 hours
D. 1 hour

Question 15
What type of attack relies on the trusting nature of employees and the art of deception?

A. Social Engineering
B. Truth Mirroring
C. Brute force
D. Social Dishonesty

Question 16
The National Security Alliance in 2004 estimated what percentage of home PCs are infected with spyware?

A. 20%
B. 40%
C. 60%
D. 80%

Question 17
What can a firewall protect against?

A. Viruses
B. Unauthenticated interactive logins from the outside world
C. Social Engineering
D. Connecting to and from the outside world

Question 18
This document states in writing how a company plans to protect the company's physical and IT assets.

A. Data encryption standard
B. Security policy
C. Public key certificate
D. Access control list

Question 19
What is "phishing"?

A. Spoofed e-mails and fraudulent websites designed to fool recipients into divulging personal financial data
B. A type of computer virus designed to look benevolent
C. Storing passwords and account data in one setting
D. Data mining on social network sites such as Facebook with the intent of identity theft.

Question 20
According to the FBI and the Computer Security Institute, most information security breaches occur due to what?

A. External hackers
B. Poor programming
C. Internal employees
D. Bad firewall settings

Question 21
Typo-squatting is?

A. A typo in operating system code that gives malware easy entry
B. A malicious website using a similar URL similar to legitimate website
C. The use of spyware to assist in keystroke logging
D. Intentionally misspelling words in posts on social websites in order to mark suspicious activity

Question 22
This piece of code is inserted into a software system and will set off a malicious function when certain conditions are met.

A. Provisional script
B. Logic bomb
C. Conditional malware
D. Virus

Question 23
Released November 2, 1988, this small, 99-line program brought large pieces of the Internet to a standstill, prompting DARPA to sponsor the establishment of CERT/CC.

A. Ghostball
B. OneHalf
C. Jerusalem virus
D. Morris worm

Question 24
These hackers are often employed by security companies to work as security auditors and perform penetration testing.

A. Script kiddies
B. Black hats
C. White hats
D. Grey hats

Question 25
Which port is used for RADIUS authentication?

A. 543
B. 1701
C. 1723
D. 1812

Question 26
Which of the following is true regarding the WTLS protocol?

A. It is a derivate of the SSH protocol
B. It is optimized for use with high-speed broadband connections
C. It is used to provide data encryption for WAP connections
D. It is used in 802.11x networks to provide authentication services

Question 27
What is the term used to describe the type of FTP access in which the user does not have permission to list the content of directories but can access the contents if the path and name are known?

A. Blind FTP
B. Anonymous FTP
C. Secure FTP
D. Passive FTP

Question 28
Users in a network are able to assign permission to their own shared resources. Which of the following access control models is being used?

A. DAC
B. RBAC
C. MAC

D. DBAC

Question 29
Which of the following should NOT be used with username/password authentication?
A. Strong passwords
B. Cognitive passwords
C. Biometrics
D. Smart cards

Question 30
Which of the following access control models allows classification and labeling of objects?
A. DAC
B. RBAC
C. MAC
D. DBAC

Question 31
Users in a company use a smart card and fingerprint scan to authenticate to the network. Which of the following authentication methods is being used?
A. Biometrics
B. Mutual authentication
C. Multi-factor authentication
D. Certificates

Question 32
Which of the following Rainbow Series is incorrectly paired?
A. Amber Book (1988) – Configuration Management in Trusted Systems
B. Red Book (1987) – Trusted Network Interpretation
C. Orange Book (1987) – A Guide to Understanding Audit in Trusted Systems
D. Yellow Book (1991) – Trusted Recovery in Trusted Systems

Question 33
Which of the following attacks is NOT aimed at fragmentation vulnerabilities of the IP stack?
A. Smurf attack
B. Teardrop attack
C. Bonk attack
D. Boink attack

Question 34
Which of the following protocols does NOT support RC4 ciphering?
A. SSL
B. WEP
C. AES
D. HTTPS

Question 35

What are typical elements of authentication as part of physical access controls?

A. ID badges
B. Username/password
C. Biometrics
D. Kerberos

Question 36

Which of the following is NOT an application layer security protocol?

A. SET
B. SSH
C. S-HTTP
D. IPSec

Question 37

What fire suppression method should be used to extinguish an electrical fire in one of the racks in the server room?

A. Water
B. Dry powder
C. Soda acid
D. Gas

Question 38

What port does the Domain Name Service (DNS) use by default?

A. 27
B. 46
C. 53
D. 80

Question 39

A set of instructions normally implemented on a computer system as a procedure to manipulate data is called a(n)?

A. Algorithm
B. Procedure
C. Process
D. Program

Question 40

Which of the following is a legal term that refers to the effort a company makes to ensure that security policies and procedures are operational?

A. Due care
B. Due diligence
C. Monitoring
D. Auditing

Question 41

Which type of virus is able to alter its own code to avoid being detected by anti-virus software?

A. Stealth
B. Boot sector
C. Polymorphic
D. Hoax

Question 42
Which of the following is not an asymmetric system?
A. SSL
B. DES
C. RSA
D. PGP

Question 43
Which of the following procedures protocols is often used in combination with L2TP to add an additional layer of security?
A. PPTP
B. PPP
C. MS-CHAP
D. IPSec

Question 44
Separating of duties is valuable in deterring?
A. Malicious software
B. External intruders
C. Fraud
D. DoS

Question 45
Which port is used by HTTPS?
A. 23
B. 43
C. 143
D. 443

Question 46
What is the name of the process during which an attacker gathers information about a target company's intranet, remote access, extranet, and Internet connections?
A. Fingerprinting
B. Scanning
C. Footprinting
D. Sniffing

Question 47
Which of the following is used for exchanging secret keys over an insecure public network?
A. Diffie-Hellman
B. RSA

C. IDEA
D. PGP

Question 48
Which of the following security principles is used when users are assigned only those rights necessary for them to perform their work?
A. Role-based access
B. Least privilege
C. Separation of duties
D. Due care

Question 49
What allows for all activities on a network or system to be traced to the user who performed them?
A. Accountability
B. Authentication
C. Authorization
D. Identification

Question 50
Which of the following manages peer authentication and key exchange for an IPSec connection?
A. IKE
B. ISAKMP
C. Oakley
D. Policy agent

Question 51
The 64 bit block cipher with 16 iterations giving a 56 bit key is called?
A. MARS
B. RC6
C. Serpent
D. Data Encryption Standard

Question 52
What principle requires that for a particular set of transactions, no one individual is solely responsible or allowed to execute the complete set?
A. Separation of duties
B. Balance of power
C. Sharing of power
D. Delegation of duties

Question 53
What does the AAA Protocol stand for?
A. Authentication, Authorization, and Auditing
B. Auditing, Authorization, and Accounting
C. Authentication, Authorization, and Accounting

D. Alerts, Audits, and Accounts

Question 54
What port is used by the File Transfer Protocol?
A. 21
B. 22
C. 23
D. 53

Question 55
In what RAID level is data written identically to two drives, therefore producing a mirrored set?
A. RAID 0
B. RAID 1
C. RAID 5
D. RAID 6

Question 56
What does PKI stand for?
A. Personal Key Interface
B. Public Key Infrastructure
C. Public Keylogging Interceptor
D. Personal Keylogging Indicator

Question 57
When the sender and the recipient can transmit data to each other over an unsecured or monitored link by encrypting messages without worrying that their communications are being monitored, it is called:
A. Authentication
B. Confidentiality
C. Integrity
D. Nonrepudiation

Question 58
Which one of the following is a primary mechanism for a malicious code to enter a desktop?
A. E-mail messages
B. E-mail attachments
C. Worms
D. Trojan horses

Question 59
Networks that allow access to some database materials and e-mail are called:
A. Campus networks
B. Trusted networks
C. Semi-trusted networks
D. Untrusted networks

Question 60
Which one of the following is a message signed with a sender's private key that can be verified by anyone who has access to the sender's public key, thereby proving that the sender had access to the private key (and therefore is likely to be the person associated with the public key used), and the part of the message that has not been tampered with.

A. Linked keys
B. Public Key Encryption
C. CryptoSystems
D. Digital Signature

Question 61
Which of the following is a duplicate of some or all of a main database's data stored on a separate computer from the main database?

A. Database backup
B. Data warehouse
C. DFS
D. Disk mirror

Question 62
A prolonged increase in voltage power is called a:

A. Spike
B. Fault
C. Critical Increase
D. Surge

Question 63
When it comes to magnetic media sanitization, what difference can be made between clearing and purging information?

A. Clearing renders information unrecoverable against a laboratory attack and purging renders information unrecoverable to a keyboard attack.
B. Clearing completely erases the media whereas purging only removes file headers, allowing the recovery of files.
C. Clearing renders information unrecoverable by a keyboard attack and purging renders information unrecoverable against laboratory attack.
D. They both involve rewriting the media.

Question 64
PGP is a data encryption and decryption computer program provides cryptographic privacy and authentication for data communication. What does PGP stand for?

A. Pretty Good Privacy
B. Privacy Guaranteed Program
C. Personal Guaranteed Privacy
D. Programmed Good Privacy

Question 65

What is the central part of a computer or communications system hardware, firmware, and software that implements the basic security procedures for controlling access to system resources?

A. Security kernel
B. Access base
C. Security perimeter
D. Reference base

Question 66
Which of the following is NOT a property of a reference monitor?

A. The reference validation mechanism must always be invoked
B. The reference validation mechanism must be tamperproof
C. The reference validation mechanism must be small enough to be subject to analysis and tests
D. The reference validation mechanism must be hardware

Question 67
Which of the following is a channel not intended for information transfer at all, such as the service program's effect on system load?

A. Trap door
B. Back door
C. Gateway
D. Covert channel

Question 68
Which two Internet protocols are currently used to send and retrieve e-mail?

A. SMTP and AES
B. POP3 and AES
C. SMTP and POP3
D. FTP and POP3

Question 69
Which of the following is a physical device that an authorized user of computer services is given to ease authentication?

A. KeyLock
B. Security token
C. IPSec
D. Defense ring

Question 70
Locks, fences, cameras, and security guards are example of what?

A. Physical security
B. Social Engineering
C. Spoofing
D. Access Deterrence

Question 71
Which of the following access control measures prevents piggybacking from occurring?

A. Mantrap
B. Firewall
C. Anti-virus software
D. Honeypot

Question 72
Which computer security model is designed for the goal of achieving confidentiality?

A. Brewer and Nash model
B. Biba model
C. Clark-Wilson model
D. Bell-LaPadula model

Question 73
What does RAID 10 do?

A. Block-level striping with dedicated parity
B. Block-level striping with distributed parity
C. Mirroring and striping
D. Block-level striping without parity or mirroring

Question 74
In cryptography, who is directly responsible for issuing digital certificates?

A. PKI
B. IPSec
C. CA
D. Kerberos

Question 75
Which of the following is NOT an example of biometric authentication?

A. Keyboard dynamics
B. Keylogging
C. Iris scan
D. Signature dynamics

Question 76
Which of the following is a true smart card that can not only store data, but also process data?

A. IC Microprocessor card
B. IC Memory card
C. Magnetic strip card
D. DataCard

Question 77
The Brewer and Nash model seeks to ensure which of the following?

A. Integrity

B. Authentication
C. Confidentiality
D. Lack of conflict of interest

Question 78
Which DoS attack involves the attacker sending an ICMP Echo request packet with a size larger than 65,535 bytes?
A. UDP Flood Attacks
B. Ping of Death Attacks
C. Man in the Middle Attacks
D. Spoofing

Question 79
What is a computer network attack that seeks to maximize the severity of damage and speed of contagion by combining methods?
A. Combination strike
B. Combined attack force
C. Unique threat
D. Blended threat

Question 80
Which of the following backup sites is a duplicate of the original site of the organization, with full computer systems as well as near-complete backups of user data?
A. Cold sites
B. Warm sites
C. Hot sites
D. Parallel sites

Question 81
Spim is best defined as:
A. An encrypting protocol
B. A type of security token
C. Spam sent over Instant Messaging
D. A type of proxy program

Question 82
What is the official name given to the Orange Book?
A. Trusted Computer System Evaluation Criteria
B. Password Management Guideline
C. Guidance for Applying TPSEC in Specific
D. Assessing Controlled Access Protection

Question 83
A digital signature is an example of which of the following?
A. Public key cryptography
B. Biometrics

C. Physical security
D. SSL

Question 84
Which of the following is responsible for designing a security system or major components of a security system?
A. Security engineer
B. Security architect
C. Security analyst
D. Security administrator

Question 85
What specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects?
A. ACL
B. DES
C. AES
D. SMTP

Question 86
Which of the following may act as a firewall by responding to input packets (connection requests, for example) in the manner of an application, while blocking other packets?
A. Security tokens
B. Keys
C. Antivirus software
D. Proxy servers

Question 87
A sandbox is:
A. A trap to help fight unauthorized computer access
B. A type of virus that is programed to remain idle until certain conditions are met
C. A security mechanism for separating running programs
D. An unofficial name given to a census program that determines the number of computers connected to the Internet at a given time

Question 88
Passwords are generated, based on a dictionary for example, and the password checker tries the password until it succeeds. What kind of attack is being described?
A. Password aging
B. Phishing
C. Brute-force
D. Pharming

Question 89

Released in November 1993, this Rainbow Series book states as one of its goals as the "generation of assurance evidence to show that all channels are handled according to the policy in force". What is the color of this book?

A. Light pink
B. Blue
C. Yellow
D. Green

Question 90

Which of the following IDS is a dedicated hardware appliance monitors all traffic in a network or coming thru an entry-point such as an Internet connection?

A. Host-based
B. Network-based
C. Private-based
D. Detection-based

Question 91

Which of the following is a text file that a website stores on the local computer to maintain information about a visitor's session?

A. Virus
B. Adware
C. Worm
D. Cookie

Question 92

Which of the following is NOT something that can be achieved via a Trojan horse?

1. Blue screen of death
2. Keystroke logging
3. Data theft
4. Integrity

Question 93

TCP/IP is:

A. The set of communications protocols used for the Internet and similar networks
B. An encryption/decryption program
C. A biometric system in use by companies such as Microsoft
D. A protocol used for transmitting e-mails across the Internet.

Question 94

What protocol uses port 110?

A. IMAP
B. POP3
C. NNTP
D. SMTP

Question 95
Which of the following authentication protocols utilizes the MD4 hashing algorithm?

A. EAP
B. MS-CHAP
C. Kerberos
D. PAP

Question 96
Which of the following is achieved when a message is digitally signed?

A. Authorization
B. Confidentiality
C. Access Control
D. Integrity

Question 97
A cold site is:

1. The least expensive type of backup site for an organization to operate
2. A website that has not been updated for at least a year, indicating a likely false site
3. A computer hardware that has been infected
4. A physical security measure designed to locate bugs on an infiltrator

Question 98
The difference between AES and DES is:

1. AES has been made obsolete by DES
2. DES relies on a 56-bit key size while AES can operate up to a 256-bit key size
3. DES uses the Rijndael cipher while AES does not
4. AES and DES are different names for the same encryption standard

Question 99
A collection of Internet-connected programs communicating with other similar programs in order to perform tasks is called a:

1. Botnet
2. CellNet
3. Phishnet
4. TechNet

Question 100
Which of the following adds an additional layer of security to an organization's LAN with a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network?

1. Antivirus software
2. Access control
3. DMZ
4. IDEA