Question: 1.
DES - Data Encryption standard has a 128 bit key and is very difficult to break.

A. True  
B. False

Answer: B

Question: 2.
What is the main difference between computer abuse and computer crime?

A. Amount of damage  
B. Intentions of the perpetrator  
C. Method of compromise  
D. Abuse = company insider; crime = company outsider

Answer: B

Question: 3.
A standardized list of the most common security weaknesses and exploits is the __________.

A. SANS Top 10  
B. CSI/FBI Computer Crime Study  
C. CVE - Common Vulnerabilities and Exposures  
D. CERT Top 10

Answer: C

Question: 4.
A salami attack refers to what type of activity?

A. Embedding or hiding data inside of a legitimate communication - a picture, etc.  
B. Hijacking a session and stealing passwords  
C. Committing computer crimes in such small doses that they almost go unnoticed  
D. Setting a program to attack a website at 11:59 am on New Year's Eve

Answer: C

Question: 5.
Multi-partite viruses perform which functions?

A. Infect multiple partitions  
B. Infect multiple boot sectors  
C. Infect numerous workstations  
D. Combine both boot and file virus behavior

Answer: D

Question: 6.
What security principle is based on the division of job responsibilities - designed to prevent fraud?

A. Mandatory Access Control  
B. Separation of Duties  
C. Information Systems Auditing  
D. Concept of Least Privilege
Question: 7.
_____ is the authoritative entity which lists port assignments

A. IANA
B. ISSA
C. Network Solutions
D. Register.com
E. InterNIC

Answer: A

Question: 8.
Cable modems are less secure than DSL connections because cable modems are shared with other subscribers?

A. True
B. False

Answer: B

Question: 9.
____________ is a file system that was poorly designed and has numerous security flaws.

A. NTS
B. RPC
C. TCP
D. NFS
E. None of the above

Answer: D

Question: 10.
Trend Analysis involves analyzing historical __________ files in order to look for patterns of abuse or misuse.

Answer: Log files

Question: 11.
HTTP, FTP, SMTP reside at which layer of the OSI model?

A. Layer 1 - Physical
B. Layer 3 - Network
C. Layer 4 - Transport
D. Layer 7 - Application
E. Layer 2 - Data Link

Answer: D

Question: 12.
Layer 4 in the DoD model overlaps with which layer(s) of the OSI model?

A. Layer 7 - Application Layer
B. Layers 2, 3, & 4 - Data Link, Network, and Transport Layers  
C. Layer 3 - Network Layer  
D. Layers 5, 6, & 7 - Session, Presentation, and Application Layers  

Answer: D  

Question: 13.  
A Security Reference Monitor relates to which DoD security standard?  

A. LC3  
B. C2  
C. D1  
D. L2TP  
E. None of the items listed  

Answer: B  

Question: 14.  
The ability to identify and audit a user and his / her actions is known as _____________.  

A. Journaling  
B. Auditing  
C. Accessibility  
D. Accountability  
E. Forensics  

Answer: D  

Question: 15.  
There are 5 classes of IP addresses available, but only 3 classes are in common use today, identify the three: (Choose three)  

A. Class A: 1-126  
B. Class B: 128-191  
C. Class C: 192-223  
D. Class D: 224-255  
E. Class E: 0.0.0.0 - 127.0.0.1  

Answer: A, B, C  

Question: 16.  
The ultimate goal of a computer forensics specialist is to _______________.  

A. Testify in court as an expert witness  
B. Preserve electronic evidence and protect it from any alteration  
C. Protect the company's reputation  
D. Investigate the computer crime  

Answer: B  

Question: 17.  
One method that can reduce exposure to malicious code is to run applications as generic accounts with little or no privileges.  

A. True
B. False

**Answer: A**

**Question: 18.**
___________ is a major component of an overall risk management program.

**Answer: Risk assessment**

**Question: 19.**
An attempt to break an encryption algorithm is called ____________.

**Answer: Cryptanalysis**

**Question: 20.**
The act of intercepting the first message in a public key exchange and substituting a bogus key for the original key is an example of which style of attack?

A. Spoofing  
B. Hijacking  
C. Man In The Middle  
D. Social Engineering  
E. Distributed Denial of Service (DDoS)

**Answer: C**

**Question: 21.**
If Big Texas telephone company suddenly started billing you for caller ID and call forwarding without your permission, this practice is referred to as ________________.

**Answer: Cramming**

**Question: 22.**
When an employee leaves the company, their network access account should be __________?

**Answer: Disable**

**Question: 23.**
Passwords should be changed every ________ days at a minimum.  
90 days is the recommended minimum, but some resources will tell you that 30-60 days is ideal.

**Answer: 90**

**Question: 24.**
IKE - Internet Key Exchange is often used in conjunction with what security standard?

A. SSL  
B. OPSEC  
C. IPSEC  
D. Kerberos  
E. All of the above

**Answer: C**

**Question: 25.**
Wiretapping is an example of a passive network attack?

A. True  
B. False  

**Answer: A**

**Question: 26.**
What are some of the major differences of Qualitative vs. Quantitative methods of performing risk analysis? (Choose all that apply)

A. Quantitative analysis uses numeric values  
B. Qualitative analysis uses numeric values  
C. Quantitative analysis is more time consuming  
D. Qualitative analysis is more time consuming  
E. Quantitative analysis is based on Annualized Loss Expectancy (ALE) formulas  
F. Qualitative analysis is based on Annualized Loss Expectancy (ALE) formulas  

**Answer: A, C, E**

**Question: 27.**
Which of the concepts best describes Availability in relation to computer resources?

A. Users can gain access to any resource upon request (assuming they have proper permissions)  
B. Users can make authorized changes to data  
C. Users can be assured that the data content has not been altered  
D. None of the concepts describes Availability properly  

**Answer: A**

**Question: 28.**
Which form of media is handled at the Physical Layer (Layer 1) of the OSI Reference Model?

A. MAC  
B. L2TP  
C. SSL  
D. HTTP  
E. Ethernet  

**Answer: E**

**Question: 29.**
Instructions or code that executes on an end user's machine from a web browser is known as ______ code.

A. Active X  
B. JavaScript  
C. Malware  
D. Windows Scripting  
E. Mobile  

**Answer: E**

**Question: 30.**
Is the person who is attempting to log on really who they say they are? What form of access control does this question stem from?

A. Authorization  
B. Authentication  
C. Kerberos  
D. Mandatory Access Control

Answer: B

Question: 31.
Information Security policies should be ________________? (Choose all that apply)

A. Written down  
B. Clearly Communicated to all system users  
C. Audited and revised periodically  
D. None of the choices listed are correct

Answer: A, B, C

Question: 32.
Which layer of the OSI model handles encryption?

A. Presentation Layer - L6  
B. Application Layer - L7  
C. Session Layer - L5  
D. Data Link Layer - L2

Answer: A

Question: 33.
EDI (Electronic Data Interchange) differs from e-Commerce in that ________________.

A. EDI involves only computer to computer transactions  
B. E-Commerce involves only computer to computer transactions  
C. EDI allows companies to take credit cards directly to consumers via the web  
D. None of the items listed accurately reflect the differences between EDI and e-Commerce

Answer: A

Question: 34.
A type of virus that resides in a Word or Excel document is called a ___________ virus?

Answer: Macro

Question: 35.
Vulnerability x Threat = RISK is an example of the ________________.

A. Disaster Recovery Equation  
B. Threat Assessment  
C. Risk Equation  
D. Calculation of Annual Loss Expectancy

Answer: C
Question: 36.
Only law enforcement personnel are qualified to do computer forensic investigations.

A. True
B. False

Answer: B

Question: 37.
Countermeasures have three main objectives, what are they? (Choose all that apply)

A. Prevent
B. Recover
C. Detect
D. Trace
E. Retaliate

Answer: A, B, C

Question: 38.
___________________ is responsible for creating security policies and for communicating those policies to system users.

Answer: ISO

Question: 39.
An intrusion detection system is an example of what type of countermeasure?

A. Preventative
B. Corrective
C. Subjective
D. Detective
E. Postulative

Answer: D

Question: 40.
So far, no one has been able to crack the IDEA algorithm with Brute Force.

A. True
B. False

Answer: A

Question: 41.
___________________ relates to the concept of protecting data from unauthorized users.

Answer: Confidentiality

Question: 42.
Which auditing practice relates to the controlling of hardware, software, firmware, and documentation to insure it has not been improperly modified?

A. System Control
B. Configuration Control
C. Consequence Assessment
D. Certification / Accreditation

Answer: B

**Question: 43.**
MD5 is a ___________ algorithm

A. One way hash
B. 3DES
C. 192 bit
D. PKI

Answer: A

**Question: 44.**
Which of the following is an example of One-Time Password technology? (Choose all that apply)

A. S/Key
B. OPIE
C. LC3
D. MD5

Answer: A, B

**Question: 45.**
How often should virus definition downloads and system virus scans be completed?

A. Daily
B. Monthly
C. Weekly
D. Yearly

Answer: C

**Question: 46.**
S/MIME was developed for the protection of what communication mechanism(s)?

A. Telephones
B. Email
C. Wireless devices
D. Firewalls

Answer: B

**Question: 47.**
Unclassified, Private, Confidential, Secret, Top Secret, and Internal Use Only are levels of ___________

A. Security Classification
B. Data Classification
C. Object Classification
D. Change Control Classification

Answer: B
Question: 48.
Contracting with an insurance company to cover losses due to information security breaches is known as risk __________.

A. Avoidance  
B. Reduction  
C. Assignment  
D. Acceptance

Answer: C

Question: 49.
_______________ is a Unix security scanning tool developed at Texas A&M university.

A. COPS  
B. SATAN  
C. TIGER  
D. AGGIE  
E. SNIFFER

Answer: C

Question: 50.
Security incidents fall into a number of categories such as accidental, deliberate, and __________.

Answer: Environmental

Question: 51.
Decentralized access control allows ______________________.

A. File owners to determine access rights  
B. Help Desk personnel to determine access rights  
C. IT personnel to determine access rights  
D. Security Officers to determine access rights  
E. Security Officers to delegate authority to other users

Answer: A

Question: 52.
Intentionally embedding secret data into a picture or some form of media is known as Steganography or data __________.

Answer: Data Hiding

Question: 53.
From a security standpoint, the product development life cycle consists of which of the following?

A. Code Review  
B. Certification  
C. Accreditation  
D. Functional Design Review  
E. System Test Review  
F. All of the items listed
Question: 54.
Only key members of the staff need to be educated in disaster recovery procedures.

A. True
B. False

Answer: B

Question: 55.
A virus is considered to be "in the _____ " if it has been reported as replicating and causing harm to computers.

A. Zoo
B. Wild
C. Cage
D. Jungle
E. Fire

Answer: B

Question: 56.
_______ is used in mission critical systems and applications to lock down information based on sensitivity levels (Confidential, Top Secret, etc).

A. MAC - Mandatory Access Control
B. DAC - Discretionary Access Control
C. SAC - Strategic Access Control
D. LAC - Limited Access Control

Answer: A

Question: 57.
_______ viruses change the code order of the strain each time they replicate to another machine.

A. Malicious
B. Zenomorphic
C. Worm
D. Super
E. Polymorphic

Answer: E

Question: 58.
Which major vendor adopted TACACS into its product line as a form of AAA architecture?

A. Microsoft
B. Dell
C. Sun
D. Cisco
E. All of the above
Question: 59.
Name three types of firewalls __________, _______________, and _________________
(Choose three)
A. Packet Filtering
B. Application Proxy
C. Stateful Inspection
D. Microsoft Proxy
E. SonicWall
F. Raptor Firewall
Answer: A, B, C

Question: 60.
This free (for personal use) program is used to encrypt and decrypt emails.
A. SHA-1
B. MD5
C. DES
D. PGP
E. 3DES
F. None of the above
Answer: D

Question: 61.
__________ attacks capitalize on programming errors and can allow the originator to gain additional privileges on a machine.
A. SYN Flood
B. Buffer Overflow
C. Denial of Service
D. Coordinated
E. Distributed Denial of Service
Answer: B

Question: 62.
A good password policy uses which of the following guidelines? (Choose all that apply)
A. Passwords should contain some form of your name or userid
B. Passwords should always use words that can be found in a dictionary
C. Passwords should be audited on a regular basis
D. Passwords should never be shared or written down
Answer: C, D

Question: 63.
What is the main goal of a risk management program?
A. To develop a disaster recovery plan
B. To help managers find the correct cost balance between risks and countermeasures
C. To evaluate appropriate risk mitigation scenarios
D. To calculate ALE formulas
E. None of the above

Answer: B

Question: 64.
The ___________ is the most dangerous part of a virus program.

A. Code
B. Payload
C. Strain
D. Trojan
E. None of the above

Answer: B

Question: 65.
A one way hash converts a string of random length into a _______________ encrypted string.

A. 192 bit
B. fixed length
C. random length
D. 56 bit
E. SHA
F. MD5

Answer: B

Question: 66.
Although it is considered a low tech attack ___ _________ is still a very effective way of gaining unauthorized access to network systems.

A. Sniffing
B. Eavesdropping
C. Social Engineering
D. Shoulder Surfing
E. None of the items are correct

Answer: C

Question: 67.
Diffie Hellman, RSA, and ___________ are all examples of Public Key cryptography?

A. SSL - Secure Sockets Layer
B. DSS - Digital Signature Standard
C. Blowfish
D. AES - Advanced Encryption Standard

Answer: B

Question: 68.
__________, generally considered "need to know" access is given based on permissions granted to the user.

A. MAC - Mandatory Access Control
B. DAC - Discretionary Access Control  
C. SAC - Strategic Access Control  
D. LAC - Limited Access Control  

**Answer:** B

**Question: 69.**  
What are the main goals of an information security program? (Choose all that apply)

A. Complete Security  
B. Confidentiality  
C. Availability  
D. Integrity of data  
E. Ease of Use  

**Answer:** B, C, D

**Question: 70.**  
The ability to adjust access control to the exact amount of permission necessary is called ______________.

A. Detection  
B. Granularity  
C. Separation of Duties  
D. Concept of Least Privilege  

**Answer:** B

**Question: 71.**  
Which one of these formulas is used in Quantitative risk analysis?

A. SLO - Single Loss Occurrence  
B. ARE - Annual Rate of Exposure  
C. SLE - Single Loss Expectancy  
D. ALO - Annual Loss Occurrence  

**Answer:** C

**Question: 72.**  
Integrity = ______________

A. Data being delivered from the source to the intended receiver without being altered  
B. Protection of data from unauthorized users  
C. Data being kept correct and current  
D. Ability to access data when requested  
E. All answers are correct  

**Answer:** A

**Question: 73.**  
A true network security audit does include an audit for modems?

A. True  
B. False
Answer: A

Question: 74.
What is the main difference between a logic bomb and a stealth virus? (Choose all that apply)

A. Stealth viruses supply AV engines with false information to avoid detection
B. Stealth viruses live in memory while logic bombs are written to disk
C. Stealth viruses "wake up" at a pre-specified time in the code, then execute payload
D. Logic Bombs supply AV engines with false information to avoid detection

Answer: A, B

Question: 75.
What is the minimum recommended length of a security policy?

A. 200 pages
B. 5 pages
C. 1 page
D. There is no minimum length - the policy length should support the business needs

Answer: D

Question: 76.
There are ______ available service ports

A. 65535
B. 65536
C. 1024
D. 1-1024
E. Unlimited

Answer: B

Question: 77.
Each of the following is a valid step in handling incidents except ____________

A. Contain
B. Prosecute
C. Recover
D. Review
E. Identify
F. Prepare

Answer: B

Question: 78.
A __________ is an electronically generated record that ties a user's ID to their public key.

Answer: Certificate

Question: 79.
Which of the following is NOT an encryption algorithm?

A. DES
B. 3DES
C. SSL
D. MD5
E. SHA-1

Answer: C

Question: 80.
Which range defines "well known ports?"

A. 0-1024
B. 0-1023
C. 1-1024
D. 1024-49151

Answer: B

Question: 81.
What does RADIUS stand for?

A. Remote Access Dialup User Systems
B. Remote Access Dial-in User Service
C. Revoke Access Deny User Service
D. Roaming Access Dial-in User System

Answer: B

Question: 82.
In the past, many companies had been hesitant to report computer crimes.

A. True
B. False

Answer: A

Question: 83.
If you the text listed below at the beginning or end of an email message, what would it be an indication of?
mQGiBDfJY1ERBADd1IBX8WlbSHj2uDt6YbMVI4Da3O1yG0exQnEwU3sKQARzspNB
zB2BF+ngFiy1+RsfDjfbpwz6vLHo6zQZkT2v/KOfDu1e4/LqiuOLpd/6rOrmH/Mvk

A. A virus
B. A worm
C. A PGP Signed message
D. A software error

Answer: C

Question: 84.
Although they are accused of being one in the same, hackers and crackers are two distinctly different groups with different goals pertaining to computers.

A. True
B. False
Question: 85.
Select three ways to deal with risk.

A. Acceptance  
B. Avoid / Eliminate  
C. Transfer  
D. Mitigate  
E. Deny

Answer: A, C, D

Question: 86.
Digital Certificates use which protocol?

A. X.400  
B. X.500  
C. X.509  
D. X.511  
E. X.525  
F. None of the above

Answer: C

Question: 87.
X.500 protocol relates to which technology?

A. L2TP  
B. LDAP  
C. L2F  
D. PPTP

Answer: B

Question: 88.
Public keys are used for ___________ messages and private keys are used for ___________ messages.

Answer: encrypting, decrypting

Question: 89.
In a Public Key Infrastructure (PKI), what is the role of a directory server?

A. To issue certificates to users  
B. To make user certificates available to others  
C. Authorizes CA servers to issue certificates to users  
D. Is the root authority for the PKI

Answer: B

Question: 90.
RSA has all of the following characteristics except?

A. Can produce a digital signature
B. Relies on large prime number factoring  
C. Uses third party key distribution centers  
D. Is based on a symmetric algorithm

Answer: D

Question: 91.  
What distinguishes a hacker / cracker from a phreak?

A. Hackers and crackers specifically target telephone networks  
B. Phreaks specifically target data networks  
C. Phreaks specifically target telephone networks  
D. Phreaks cause harm, hackers and crackers do not

Answer: C

Question: 92.  
Identifying specific attempts to penetrate systems is the function of the _______________.

A. Firewall  
B. Router  
C. Intrusion Detection System  
D. Vulnerability Scanner  
E. CERT - Computer Emergency Response Team

Answer: C

Question: 93.  
A boot sector virus goes to work when what event takes place?

A. Reboot or system startup  
B. File is deleted  
C. File is saved  
D. March 16th

Answer: A

Question: 94.  
Which of the following organizations can be a valid Certificate Authority (CA)?

A. Verisign  
B. Microsoft  
C. Netscape  
D. Dell  
E. All of the entities listed could be valid Certificate Authorities

Answer: E

Question: 95.  
It is difficult to prosecute a computer criminal if warning banners are not deployed?

A. True  
B. False

Answer: A
Question: 96.
What is the following paragraph an example of?

<<ATTN: This system is for the use of authorized persons only. If you use this system without authority, or if you abuse your authority, then you are subject to having all of your activities on this system monitored and recorded by system personnel. >>

A. Audit Trail Banner  
B. Warning Banner  
C. Welcome Banner  
D. Access Control Banner

Answer: B

Question: 97.
EICAR is an example of a ____________ used to test AV products without introducing a live virus into the network.

Answer: Test virus

Question: 98.
___________ is the most famous Unix password cracking tool.

A. SNIFF  
B. ROOT  
C. NMAP  
D. CRACK  
E. JOLT

Answer: D

Question: 99.
PGP & PEM are programs that allow users to send encrypted messages to each other. What form of encryption do these programs use?

A. DES  
B. 3DES  
C. RSA  
D. 3RSA  
E. Blowfish  
F. All of the above

Answer: C

Question: 100.
Which of the following are NT Audit events? (Choose all that apply)

A. Logon and Logoff  
B. Use of User Rights  
C. Security Policy Change  
D. Registry Tracking  
E. All of choices are correct

Answer: A, B, C
Question: 101.
The most secure method for storing backup tapes is?

A. In a locked desk drawer
B. In the same building, but on a different floor
C. In a cool dry climate
D. Off site in a climate controlled area
E. In a fire proof safe inside the data center (for faster retrieval)
F. None of the above

Answer: D

Question: 102.
__________ is a tool used by network administrators to capture packets from a network.

Answer: Sniffer

Question: 103.
The IDEA algorithm (used in PGP) is _______ bits long.

A. 56
B. 158
C. 128
D. 168

Answer: C

Question: 104.
Which organization(s) are responsible for the timely distribution of information security intelligence data?

A. CERT
B. SANS
C. CERIAS
D. COAST
E. All of the organizations listed

Answer: E

Question: 105.
A password audit consists of checking for ____________?

A. Minimum password length
B. Password aging
C. Password Strength
D. Blank Passwords
E. All of the items listed

Answer: E

Question: 106.
Accounting, __________, and ____________ are the AAAs of information security.

Answer: Authentication, Authorization
Question: 107.
What term describes the amount of risk that remains after the countermeasures have been deployed and the vulnerabilities classified?

A. Terminal risk
B. Infinite risk
C. Imminent risk
D. Residual risk

Answer: D

Question: 108.
Risk assessment deals with constant monitoring?

A. True
B. False

Answer: B

Question: 109.
Countermeasures address security concerns in which of the following categories?

A. Physical
B. Operations
C. Computer
D. Communication
E. Information
F. All of the listed categories

Answer: E

Question: 110.
Which of these virus incidents did not occur in 1999? (Choose all that apply)

A. I Love You
B. Chernobyl
C. Melissa
D. Michelangelo
E. Anna Kournikova
F. None of the above - they all happened in 1999

Answer: A, E

Question: 111.
Companies can now be sued for privacy violations just as easily as they can be sued for security compromises.

A. True
B. False

Answer: A

Question: 112.
Passfilt.dll enforces which of the following? (Choose all that apply)
A. 8 character minimum password length
B. 90 day password change
C. Each password must have a combination of upper case, lower case, numbers and special characters
D. 6 character minimum password length

**Answer: C, D**

**Question: 113.**
_________ is a form of Denial of Service attack which interrupts the TCP three way handshake and leaves half open connections.

A. DNS Recursion
B. NMAP
C. Land Attack
D. SYN Flooding
E. Port Scanning

**Answer: D**

**Question: 114.**
The following actions have been noted as providing motivation to virus writers? (Choose all that apply)

A. Fame
B. Fortune
C. Boredom
D. Stupidity

**Answer: A, C**

**Question: 115.**
The ____________ protocol sends passwords in clear text, while ____________ encrypts passwords. Both protocols are used by PPP (Point to Point Protocol) to transport IP traffic.

**Answer: PAP, CHAP**

**Question: 116.**
Which of the following are used in Biometrics?

A. Retinal Scanning
B. Fingerprint
C. Face Recognition
D. Voice Recognition
E. All of the above
F. None of the above

**Answer: E**

**Question: 117.**
Smart cards are a secure alternative to which weak security mechanism?

A. Biometrics
B. Public Key Encryption
C. Passwords
D. Tokens

Answer: C

Question: 118.
What type of software can be used to prevent, detect (and possibly correct) malicious activities on a system?

A. Personal Firewall
B. IDS - host based
C. Antivirus
D. All methods listed

Answer: D

Question: 119.
Information security policies are a _______________.

A. Necessary evil
B. Waste of time
C. Business enabler
D. Inconvenience for the end user
E. All of the answers are correct

Answer: C

Question: 120.
Macintosh computers are not at risk for receiving viruses.

A. True
B. False

Answer: B

Question: 121.
Unlike viruses and worm, __________ are bogus messages that spread via email forwarding.

Answer: Hoaxes

Question: 122.
There are 6 types of security control practices. __________ controls are management policies, procedures, and guidelines that usually effect the entire system. These types of controls deal with system auditing and usability.

A. Preventive
B. Detective
C. Corrective
D. Directive
E. Recovery
F. Combination

Answer: D

Question: 123.
Name two types of Intrusion Detection Systems ________ and ________.

**Answer: host based, network based**

**Explanation:**
Intrusion Detection Systems are like a burglar alarm for your computer network... they detect unauthorized access attempts. They are the first line of defence for your computer systems. There are basically two main types of IDS being used today: Network based (a packet monitor), and Host based (looking for instance at system logs for evidence of malicious or suspicious application activity in real time).

**Question: 124.**
Today, privacy violations are almost as serious as security violations?

A. True  
B. False  

**Answer: A**

**Question: 125.**
________ is a protocol developed by Visa and MasterCard to protect electronic transactions.

A. SSL  
B. SHA-1  
C. HMAC  
D. SET  
E. ETP  

**Answer: D**

**Question: 126.**
Which of the following are Unix / Linux based security tools?

A. Tiger  
B. TCP Wrappers  
C. TripWire  
D. LogCheck  
E. SATAN  
F. All of the tools listed can work on the Unix platforms  

**Answer: F**

**Question: 127.**
Layer 4 of the OSI model corresponds to which layer of the DoD model?

A. Layer 4 - Application  
B. Layer 3 - Host to Host  
C. Layer 2 - Internet  
D. Layer 1 - Network  
E. Layer 6 - Presentation  

**Answer: B**

**Question: 128.**
When gathering digital evidence it is very important to do the following: (Choose all that apply)
A. Shut down the compromised system to avoid further attacks
B. Reboot the victim system offline
C. Document the chain of evidence by taking good notes
D. Perform a bit-level back up of the data before analysis

Answer: C, D

Question: 129.
A security policy is a rigid set of rules that must be followed explicitly in order to be effective.

A. True
B. False

Answer: B

Question: 130.
BIND should be disabled on the which of the following?

A. All DNS servers to avoid recursive lookups
B. All non DNS servers
C. Firewalls
D. Routers

Answer: B

Question: 131.
IPSEC resides at which layer of the OSI model?

A. Layer 6 - Presentation
B. Layer 3 - Network
C. Layer 4 - Transport
D. Layer 5 - Session
E. Layer 2 - Data Link
F. Layer 1 - Physical

Answer: B

Question: 132.
DES, 3DES, Blowfish, and AES are all examples of what type of cryptography?

A. Public Key
B. Message Digest
C. Hash Algorithm
D. Secret Key

Answer: D

Question: 133.
Your ATM card is a form of two-factor authentication for what reason?

A. It combines something you are with something you know
B. It combines something you have with something you know
C. It combines something you control with something you know
D. It combines something you are with something you have
Answer: B

Question: 134.
Attackers have been known to search through company trash bins in order to collect potentially useful information. This method of attack is known as _________________.

Answer: Dumpster diving

Question: 135.
BIA - Business Impact Analysis deals strictly with financial assessment of a loss in relation to business operations?

A. True
B. False

Answer: B

Question: 136.
Of the protocols list, which one is connection oriented?

A. IP
B. UDP
C. DNS
D. TCP
E. All protocols listed are connection oriented

Answer: D

Question: 137.
The Internet service that converts www.soundbodyworks.com to 216.230.195.151 is known as:

A. SMTP
B. DNS
C. HTTP
D. FTP
E. GOPHER

Answer: B

Question: 138.
Corporate networks are safer if an end user connects through a VPN connection?

A. True
B. False

Answer: B

Question: 139.
A __________ is a program that can be useful in preventing cookies and Java applets from accessing a system.

Answer: Desktop Firewall

Question: 140.
___________ programs decrease the number of security incidents, educate users about procedures, and can potentially reduce losses.

A. New hire orientation
B. HR Briefings
C. Security Awareness
D. Employee Termination

Answer: C

Question: 141.
What reference model describes computer communication services and protocols in a layered approach?

A. IETF - Internet Engineering Task Force
B. ISO - International Standards Organization
C. IANA - Internet Assigned Numbers Authority
D. OSI - Open System Interconnection

Answer: D

Question: 142.
Government categories of data classification include which of the following? (Choose all that apply)

A. Confidentiality
B. Secret
C. Top Secret
D. Confidential
E. Need to Know
F. Availability

Answer: B, C, D

Question: 143.
In the DoD accreditation process a __________ is the formal entity which ensures that information systems meet a certain criteria for secure operation. Once approved these machines are certified to operate with a set of listed safeguards.

A. DISA - Defense Information Systems Agency
B. ISC2 - International Information Systems Security Certification Consortium
C. DAA - Designated Approving Authority
D. ISACA - The Information Systems Audit and Control Association

Answer: C

Question: 144.
TCPWrappers is an example of which type of security tool?

A. Network Based IDS
B. Host Based IDS
C. Personal Firewall
D. All of the above
E. None of the above
Answer: B

**Question: 145.**
Trin00 is an example of what type of attack?

A. Man in the Middle
B. Spamming
C. Spoofing
D. Distributed Denial of Service
E. Brute Force

Answer: D

**Question: 146.**
Inference attacks involve ___________________________.

A. Gathering pieces of secret information to predict or guess an outcome
B. Deciphering encrypted communications
C. Spoofing a connection to intercept plain text transmissions
D. Collecting unclassified pieces of information to predict or guess an outcome

Answer: D

**Question: 147.**
Of the following, which is NOT a risk assessment system?

A. Aggregated Countermeasures Effectiveness (ACE) Model
B. Information Security Protection Assessment Model (ISPAM)
C. Dollar-based OPSEC Risk Analysis (DORA)
D. Analysis of Networked Systems Security Risks (ANSSR)

Answer: B

**Question: 148.**
Heuristic scanning in antivirus software is designed to catch 100% of all known and unknown virus technologies.

A. True
B. False

Answer: B

**Question: 149.**
The main difference between MD5 and SHA is what?

A. Security - MD5 can be forged and SHA cannot
B. SHA has 160 bit signature and MD5 has a 128 bit signature
C. MD5 has 160 bit signature and SHA has a 128 bit signature
D. Security - SHA can be forged and MD5 cannot

Answer: B

**Question: 150.**
The most important component of antivirus software is the _____________?
A. Desktop  
B. Definitions  
C. Engine  
D. Heuristics  
E. Console  

**Answer:** C

**Question: 151.** The two categories of threats are natural and ___________.  

**Answer:** Human

**Question: 152.** Sending an ICMP packet greater than 64Kb is an example of what type of attack?  

A. Buffer Overflow  
B. Ping of Death  
C. Syn Flooding  
D. TearDrop  
E. Land Attack  

**Answer:** B

**Question: 153.** Which of the following steps are involved in a basic risk assessment?  

A. Determine what data and systems need to be protected  
B. Evaluate who are the potential threats  
C. Investigate potential legal, financial, and regulatory issues  
D. Determine the chances of a disaster or risk related event occurring  
E. All of the items listed  
F. None of the items listed  

**Answer:** E

**Question: 154.** NIPC stands for _______________ ___________ and is a government organization designed to help protect our nation's vital information resources.  

**Answer:** National Infrastructure Protection Center

**Question: 155.** SATAN is a _____________ based tool and COPS is a ______________ based tool  

**Answer:** Network, Host based

**Explanation:**  
Security Administrators Tool for Analyzing Networks (SATAN) is a UNIX-specific program that tests network connectivity; a well-known tool for both hackers and security analysts. Computer Oracle and Password System (COPS). Examines a system for a number of predetermined weaknesses, then alerts the system administrator. Originally written as a shell script or a C program. For use on UNIX systems.
Echo, chargen, finger, and bootp are all examples of?

A. Security weaknesses
B. Possibly unnecessary services
C. Service ports
D. Router commands
E. Hacker tools

**Answer: B**

**Question: 157.**
The ___________ protocol converts IP addresses (logical) to MAC Addresses (physical)

A. IPSEC
B. ARP
C. DARP
D. DNS
E. None of the above

**Answer: B**

**Question: 158.**
What are the two most critical aspects of risk analysis? (Choose two)

A. Identifying vulnerabilities
B. Identifying threats
C. Identifying resources
D. Identifying assets

**Answer: B, D**

**Question: 159.**
A program that intentionally leaves a security hole or covert method of access is referred to as a ___________.

A. Logic bomb
B. Back door
C. Trojan horse
D. Honey pot

**Answer: B**

**Question: 160.**
In order for events to be written to the NT security events log, the ___________ function has to be enabled first.

**Answer: Auditing**

**Question: 161.**
Which of the following is NOT an administrative control?

A. Locks, CCTV, alarm systems
B. Security Awareness Program
C. Information Security Policy
D. Disabling a user account upon termination
Answer: A

Question: 162.
Symmetric = private key = secret
________ = public key = shared

Answer: Asymmetric

Question: 163.
What is a big difference between Java Applets and Active X controls?

A. Active X controls can run on any platform
B. Java Applets only run in Windows
C. Java Applets have access to the full Windows OS
D. Active X controls have access to the full Windows OS

Answer: D

Question: 164.
Which method of password cracking takes the most time and effort?

A. Guessing
B. Brute Force
C. Hybrid
D. Shoulder Surfing
E. Dictionary attack

Answer: B

Question: 165.
Words appearing in the English dictionary are not considered to be good passwords, but words appearing in the French, Spanish, Italian, and Japanese dictionaries are not considered a risk.

A. True
B. False

Answer: B

Question: 166.
Accreditation grants permission to operate a system freely since all risk has been eliminated.

A. True
B. False

Answer: B

Question: 167.
Which of the following is not an element of a business continuity plan?

A. Public Relations
B. Costs
C. Facilities
D. Prosecution
E. Human Resources
Question: 168.
AH - Authentication Header is used in what industry standard protocol?
A. SSL - Secure Sockets Layer
B. ESP - Encapsulating Security payload
C. ISAKMP - Internet Security Association and Key Management Protocol
D. IKE - Internet Key Exchange
E. IPSEC - Internet Protocol Security

Answer: E

Question: 169.
___________________ is ultimately responsible for security and privacy violations.
A. Person committing the violation
B. Security Officer
C. CIO / CEO
D. OS Software

Answer: C

Question: 170.
___________________ is a vendor neutral authorization and authentication protocol used by Windows 2000.

Answer: Kerberos

Question: 171.
When compiling a risk assessment report, which of the following items should be included? (Choose all that apply)
A. Vulnerability levels
B. Method of attack used
C. Names of frequent security violators
D. Data sensitivity levels
E. ALE calculations

Answer: A, D, E

Question: 172.
According to the annual CSI/FBI Computer Crime report, which group commits the most computer crimes?
A. Foreign governments
B. Teenage Hackers
C. Company Insiders
D. Company Competitors
E. All of these groups create equal numbers of computer crimes

Answer: C

Question: 173.
The SubSeven Trojan has been known to exploit which service ports?

A. 137, 139  
B. 6711, 6712, 6776, 27374  
C. 31337, 31338  
D. 65000, 65001, 65002

**Answer: B**

**Question: 174.**
The NT Event Viewer holds which of the following types of logs?

A. System  
B. Application  
C. Security  
D. All three of the types listed

**Answer: D**

**Question: 175.**
________ attacks generally prevent valid authorized users from gaining access to system resources.

**Answer: Denial of Service**

**Question: 176.**
When a security violation occurs, what important information should be logged? (Choose all that apply)

A. User ID  
B. Timestamp  
C. User's first and last name  
D. Computer / Terminal ID  
E. All of the items listed

**Answer: A, B, D**

**Question: 177.**
A __________ is a means, method, or program to neutralize a threat or vulnerability.

A. Risk Assessment  
B. Vulnerability Scan  
C. Countermeasure  
D. Firewall

**Answer: C**

**Question: 178.**
If a sender is unable to deny having sent an electronic transmission, this concept is known as __________

A. PKI  
B. Verification  
C. Non-Repudiation  
D. Irrevocable Trust
Question: 179.
The CERT (Computer Emergency Response Team) was created in response to what famous security problem?

A. The ILOVEYOU virus
B. CodeRed
C. Kevin Mitnik
D. The Morris worm
E. SATAN

Answer: D

Question: 180.
The NT password cracking program L0pht is capable of pulling passwords from the registry?

A. True
B. False

Answer: A

Question: 181.
The difference between fraud and embezzlement is ________________.

A. Fraud = money or goods; embezzlement = money only
B. Fraud = removing hardware / software; embezzlement = removing data only
C. Fraud = misdemeanor; embezzlement = felony
D. There is no difference, fraud and embezzlement are the same
E. Embezzlement is about publicity; fraud is about personal gain

Answer: A

Question: 182.
In order to use L0pht, the ___________ must be exported from Windows NT.

A. SAMBA
B. LDAP
C. Kernel
D. SAM
E. PDC

Answer: D

Question: 183.
The standard of ___________ states that a certain level of integrity and information protection levels will be maintained.

A. Due Diligence
B. Due Process
C. Due Care
D. BSO 1799
Question: 184.
What happens if this registry value is set to 1?
HKLM\System\CurrentControlSet\Control\Lsa\CrashonAuditFail

A. System will crash
B. System will continue operations as normal
C. No such registry key exists
D. System will perform a shutdown if maximum log size is reached
E. System will overwrite logs

Answer: D

Question: 185.
A _______ refers to hidden code or instructions added to an application or operating system. This code will not execute until appropriate / predetermined conditions are met.

Answer: mail bomb

Question: 186.
Tripwire is a ________________-

A. Log analyzer
B. Port Scanner
C. Digital Certificate Company
D. Polymorphic virus
E. File Integrity Checker

Answer: E

Question: 187.
Some Unix systems use a very simple cipher called ________.

A. ROT13
B. SOT14
C. DES
D. Block
E. Stream

Answer: A

Question: 188.
When packets are captured and converted to hexadecimal, _______ represents the ICMP protocol in the IP header.

A. 17
B. 25
C. 16
D. 01
E. 06
F. All of the above

Answer: D
Question: 189.
L2TP is considered to be a less secure protocol than PPTP.

A. True
B. False

Answer: B

Question: 190.
_____________ is the process of capturing network packets, breaking them apart, and examining the contents.

Answer: Sniffing

Question: 191.
Which of the following is NOT an encryption method used by VPNs (Virtual Private Networks)?

A. IPSEC - IP Security
B. L2F - Layer 2 Forwarding
C. L2TP - Layer 2 Tunneling Protocol
D. SSH - Secure Shell
E. PPTP - Point to Point Tunneling Protocol
F. All of the above are encryption methods used by VPNs

Answer: F

Question: 192.
_____________ is a high speed data routing technology also known as X.25.

Answer: Packet Switching

Question: 193.
Define the acronym RBAC

A. Role Based Access Center
B. Rule Based Access Center
C. Role Based Access Control
D. Rule Based Access Control

Answer: C

Question: 194.
A ___________ is a signal sent from a receiving machine to another host asking it to slow down the rate at which it is sending information.

Answer: Source Quench

Question: 195.
A ___________ is a program that poses as a useful or legitimate program, but turns out to be malicious code.

A. Worm
B. Trojan Horse
C. Logic Bomb
D. Polymorphic Virus
Question: 196.
Select the major difference(s) between block and stream ciphers. (Choose all that apply)

A. Block = bit by bit; stream = encrypted in equal sections
B. Stream = bit by bit; block = encrypted in equal sections
C. Block = hardware driven; stream = software driven
D. Stream = hardware driven; block = software driven
E. Block = slower encryption; stream = fast encryption

Answer: B, D, E

Question: 197.
__________ states that users should only be given enough access to accomplish their jobs.

A. Separation of Duties
B. Due Diligence
C. Concept of Least Privilege
D. All of the listed items are correct

Answer: C

Question: 198.
SATAN stands for ____________________________________________

A. System Administrator Tool for Analyzing Networks
B. Storage Administration Tool for Analyzing Networks
C. Simple Administration Tool for Analyzing Networks
D. System Administrator Tool for Analyzing Networks
E. SANS Administrator Tool for Analyzing Networks

Answer: D

Question: 199.
PGP allows which of the following to be encrypted?

A. Files
B. Email
C. Network connections
D. Disk volumes
E. PGP will encrypt all of the listed items

Answer: E

Question: 200.
A chronologically sorted record of all the activities on a system is known as an ____________

A. IDS system
B. Packet sniffer
C. Application log
D. Audit log
E. Audit trail
Question: 201.
Much like the layers of an onion, ______________ is a comprehensive set of security solutions layered to provide the best protection.

A. Security policy
B. Risk Assessment
C. Defense in Depth
D. Vulnerability Assessment
E. Firewall Penetration Testing

Answer: C

Question: 202.
Threat assessment has four major components, name them. (Choose four)

A. Type
B. Mechanism
C. Impact
D. Probability
E. ALE - Annual Loss Expectancy

Answer: A, B, C, D

Question: 203
A system's ability to identify a particular individual, track their actions, and monitor their behavior is known as:

A. Authorization
B. Auditing
C. Accountability
D. Monitoring
E. Logging

Answer: C

Accountability is used to monitor, track, and determine the actions of an individual

Question: 204
To meet SSCP certification requirements a candidate must _______ and ___________.<br>(Choose two)

A. Subscribe to the SSCP code of ethics
B. Subscribe to the IETF code of ethics
C. Have 2 years work experience  
D. Have 1 year work experience  
E. Obtain a recommendation from a SSCP in good standing  

**Answer: A, D**  
Besides successful completion of the SSCP exam, candidates must subscribe to the SSCP code of ethics and have one year work experience in one or more of the 7 SSCP domains.  

**Question: 205**  
________ is the act of a user professing an identity to a system.  

A. Validation  
B. Authentication  
C. Identification  
D. Confirmation  

**Answer: C**  
Identification is used to establish user accountability. Many times identification takes the form of a logon ID.  

**Question: 206**  
_______ and ________ are the primary controls of most access control systems.<br>(Choose two)  

A. Tickets  
B. Biometrics  
C. Authorization  
D. Identification  
E. Authentication  

**Answer: D, E**  
Identifying a user and authenticating them into the system form the foundations of most access control systems.  

**Question: 207**  
Authentication is based on which of the following:<br>(Choose three)  

A. Something you are  
B. Something you input  
C. Something you know  
D. Something you compute  
E. Something you have  

**Answer: A, C, E**  
The three types of authentication include something you know, something you have, and something you are.  

**Question: 208**  
________ _________ refers to the act of requiring more than one type of authentication to be used and is considered more secure than any single type of authentication<br>(Choose two)  

A. One  
B. Two  
C. Three  
D. Factor
E. Exponent
F. Method

**Answer: B, D**
Two-factor is considered more secure than any single authentication type.

**Question: 209**
What system allows a user to provide one ID and password per work session and then is automatically logged-on to all the required applications?

A. Tickets  
B. SSO  
C. Challenge Response  
D. Token-based authentication  
E. Biometrics

**Answer: B**
Single Sign-On (SSO) overcomes the problems of having to log on multiple times to access different network resources.

**Question: 210**
Name three SSO types? (Choose three)

A. KryptoKnight  
B. Kerberos  
C. Clipper  
D. SESAME  
E. DES

**Answer: A, B, D**
Single Sign-On (SSO) options include: KryptoKnight, Kerberos, and SESAME.

**Question: 211**
Kerberos uses asymmetric encryption. (True / False)

A. True  
B. False

**Answer: B**
Kerberos authenticates clients to other entities on a network of which a client requires services by using a system of symmetric key cryptography.

**Question: 212**
Why are clipping levels used?

A. Reduce the amount of data to be evaluated  
B. Limit the number of alphanumeric characters in a password  
C. Limit errors in RADIUS systems  
D. To only set thresholds for file and object access

**Answer: A**
Clipping is used to reduce the amount to be evaluated.

**Question: 213**
Which three things must be considered for the design, planning, and implementation of access control mechanisms? (Choose three)

A. Exposures  
B. Objectives  
C. Risks  
D. Vulnerabilities  
E. Threats  

**Answer: C, D, E**

Threats, vulnerabilities, and risks are the three items that must be considered when designing access control mechanisms. Threats are possible violations, vulnerabilities are shortcomings in the system, and risks are measured by the likelihood that any particular threat may be carried out.

**Question: 214**
The Crossover Error Rate (CER) is a good measure of performance for:

A. Biometrics  
B. Tokens  
C. Kerberos  
D. A fingerprint scan  
E. Discretionary access control  

**Answer: A**
The CER is one of the three main performance measurements used in biometrics.

**Question: 215**
What are the three performance measurements used in biometrics? (Choose three)

A. Crossover error rate  
B. False rejection rate  
C. Positive error rate  
D. False acceptance rate  
E. Negative error rate  

**Answer: A, B, D**
The Crossover error rate, false reject rate, and the false acceptance rate are the three main performance measurements used in biometrics.

**Question: 216**
As telnet is widely know to be insecure, one time passwords (OPIE) offer a great alternative. After a user logs on remotely, OPIE will issue a challenge. What two elements will thi challenge contain? (Choose two)

A. CHAP  
B. A hashed value  
C. A random value  
D. A seed number  
E. A sequence number  

**Answer: D, E**

OPIE is based on S/Key, supports MD5, and features a challenge that contains the following two elements: A seed value, which is a fixed number for each account, and a sequence number, which begins at 499 and decrements each time a user logs in.
Question: 217
Overloading or congesting a system's resources so that it is unable to provide required services is referred to as:

A. Swamping
B. Denial of Service
C. Bandwidth displacement
D. A passive attack
E. ICMP redirect

Answer: B
A denial-of-service attack is aimed at depriving an organization of its resources. They are typically intentional attacks targeted against a specific system or network.

Question: 218
Spoofing is a sophisticated technique of authenticating one computer to another by forging IP packets from a trusted source address (True / False)

A. True
B. False

Answer: A
Spoofing can be achieved by exploiting trust and authentication.

Question: 219
Password crackers fall into two broad categories. What are they? (Choose two)
A. Brute force
B. Passive
C. Active
D. Random
E. Dictionary

Answer: A, E
Password crackers are programs that circumvent password security by revealing passwords that have previously been encrypted. These systems work by using dictionary attacks or brute force.

Question: 220
Sandra has used Ethereal, a packet sniffer, to listen in on network transmissions. She has captured several passwords. What type of attack has been performed on her network?

A. An active attack
B. A man-the-middle attack
C. A session hijacking
D. A privilege escalation attack
E. An illicit server attack

Answer: B
The type of attack described above is a man-in-the-middle attack.

Question: 221
Which of the following DoS attacks use ICMP? (Choose two)
A. SYN attack
B. Smurf attack

Answer: B, C
Smurf attack and ICMP redirect use ICMP.
C. Ping of death
D. UDP flood
E. NMAP

Answer: B, C
The ping-of-death attack sends an ICMP packet so large that some systems crash before they can process all of the information. The Smurf attack also manipulates ICMP. The other answers are incorrect. NMAP is a port scanning and banner grabbing tool.

Question: 222
The term "principle of least privilege" is best as:
A. A separation of command, program and interface functions
B. Active monitoring with network base intrusion detection systems and host based intrusion detection systems
C. The process of granting each user the lowest clearance and access needed to accomplish their task
D. Implementation of mandatory access control

Answer: C
The principle of least privilege is used in part to limit the damage resulting from accidents, errors, or unauthorized use of system resources.

Question: 223
What security control provides a method to insure that a transaction did or did not occur?
A. Identification
B. Accountability
C. Nonrepudiation
D. Verification
E. Access control

Answer: C
Nonrepudiation serves to validate whether or not a claimed event or action occurred in order to resolve disputes about the validity of the event. Nonrepudiation is vital in electronic commerce because it protects both the seller and the consumer from fraudulent behavior by the other party.

Question: 224
The most common source of attack against companies comes from:
A. Insiders
B. Hackers
C. Crackers
D. Script kiddies
E. Spies

Answer: A
Insiders are the most dangerous and often overlooked group of attackers.

Question: 225
________, __________, and __________ are required to successfully complete a crime. (Choose three)
A. Root kit
B. Motive
C. Buffer Overflow  
D. Means  
E. Opportunity  
F. Advantage  

**Answer: B, D, E**  
Means, motive, and opportunity are the three items needed to commit a crime.

**Question: 226**  
Insiders have a clear advantage in committing computer crime. Which two of the following do they possess? (Choose two)

A. Advantage  
B. Motive  
C. Outside connections  
D. Means  
E. Opportunity  
F. Tools  

**Answer: D, E**  
Insiders possess the means and opportunity to commit a computer crime. All that is lacking is a motive.

**Question: 227**  
Which of the following is considered the MOST secure?

A. Confidential  
B. Public  
C. Private  
D. Sensitive  

**Answer: D**  
The order of classification from highest to lowest is: Sensitive, Confidential, Private, and Public. Review NIST Special Publication 800-26 for more details about information classifications.

**Question: 228**  
Which of the following are valid modes of operation? (Choose all that apply)

A. Multilevel mode  
B. Restricted mode  
C. Dedicated mode  
D. Allowed mode  
E. Access Mode  

**Answer: A, C**  
The four modes of operation include: dedicated mode, system-high mode, compartmented mode, and multilevel mode.

**Question: 229**  
Masquerading is synonymous with _______.

A. Spoofing  
B. DNS poisoning  
C. ARP poisoning  
D. Password cracking
Answer: A
Masquerading or spoofing can come in many forms from social engineering to forging addresses in IP packets.

Question: 230
Which of the following is considered the LEAST secure?

A. Confidential
B. Public
C. Private
D. Sensitive

Answer: B
The order of classification from highest to lowest is: Sensitive, Confidential, Private, and Public. Review NIST Special Publication 800-26 for more details about information classifications.

Question: 231
The principle of least privilege is effective in helping prevent security breaches, however, prevention works best when applied with _______ and _______. Together, these three complete a security triad. (Choose two)

A. Footprinting
B. Scanning
C. Attack
D. Detection
E. Response

Answer: D, E
Prevention, detection, and response form the basis of an effective security stance. Least privilege helps provides prevention. Detection is needed because program bugs or human errors have the potential to cause security breaches. Security policy must be monitored for violations to determine an adequate response.

Question: 232
What are the three components of the AIC triad? (Choose three)

A. Accountability
B. Intelligence
C. Integrity
D. Confinement
E. Confidentiality
F. Availability

Answer: C, E, F
The AIC triad is: availability, integrity, and confidentiality. This is a key concept of security.

Question: 233
What security control provides a method to insure that a transaction did or did not occur?

A. Identification
B. Accountability
C. Nonrepudiation
D. Verification
E. Access control
Answer: C
Nonrepudiation serves to validate whether or not a claimed event or action occurred in order to resolve disputes about the validity of the event. Nonrepudiation is vital in electronic commerce because it protects both the seller and the consumer from fraudulent behavior by the other party.

Question: 234
The most common source of attack against companies comes from:

A. Insiders
B. Hackers
C. Crackers
D. Script kiddies
E. Spies

Answer: A
Insiders are the most dangerous and often overlooked group of attackers.

Question: 235
___, ___, and ________ are required to successfully complete a crime. (Choose three)

A. Root kit
B. Motive
C. Buffer Overflow
D. Means
E. Opportunity
F. Advantage

Answer: B, D, E
Means, motive, and opportunity are the three items needed to commit a crime.

Question: 236
Insiders have a clear advantage in committing computer crime. Which two of the following do they possess? (Choose two)

A. Advantage
B. Motive
C. Outside connections
D. Means
E. Opportunity
F. Tools

Answer: D, E
Insiders possess the means and opportunity to commit a computer crime. All that is lacking is a motive.

Question: 237
Which of the following is considered the MOST secure?

A. Confidential
B. Public
C. Private
D. Sensitive
Answer: D
The order of classification from highest to lowest is: Sensitive, Confidential, Private, and Public. Review NIST Special Publication 800-26 for more details about information classifications.

Question: 238
Which of the following are valid modes of operation? (Choose all that apply)

A. Multilevel mode
B. Restricted mode
C. Dedicated mode
D. Allowed mode
E. Access Mode

Answer: A, C
The four modes of operation include: dedicated mode, system-high mode, compartmented mode, and multilevel mode.

Question: 239
Masquerading is synonymous with ________.

A. Spoofing
B. DNS poisoning
C. ARP poisoning
D. Password cracking

Answer: A
Masquerading or spoofing can come in many forms from social engineering to forging addresses in IP packets.

Question: 240
Which of the following is considered the LEAST secure?

A. Confidential
B. Public
C. Private
D. Sensitive

Answer: B
The order of classification from highest to lowest is: Sensitive, Confidential, Private, and Public. Review NIST Special Publication 800-26 for more details about information classifications.

Question: 241
The change control process:

A. Should allow for quick changes without the burden on paperwork or formal committee review
B. Every incorporated required change does not need to be traceable to an approved change request
C. Should be a well defined in that it provides stakeholders with a formal mechanism for proposing changes in requirements
D. The change control process should not let you track the status of all proposed changes E. Should allow for design or implementation work to be performed without approval

Answer: C
While the change control process is not intended to be an obstacle or roadblock to making changes, it should provide stakeholders a formal mechanism for proposing and controlling change.

**Question: 242**
Which of the following criteria is used to determine the proper classification of a data object? (Choose three)

A. Sensitivity  
B. Value  
C. Useful life  
D. Storage cost  
E. Age

**Answer: B, C, E**
The criterion used to value information includes: personal association, useful life, value, and age.

**Question: 243**
Volatile memory is referred to as ROM.

A. Yes  
B. No

**Answer: B**
Volatile memory is Random Access Memory (RAM)

**Question: 244**
Define the term tuple.

A. A record in a relational database  
B. An unordered set of values  
C. An ordered set of rules placed in an ACL  
D. A method of joining HIDS and NIDS together  
E. Values placed in a flat database such as Excel

**Answer: A**
In programming languages or in relational databases, tuples are used as records. These records represent a string of values or attributes passed from one program (database) to another.

**Question: 245**
While there are many different models for IT system life cycle most contain five unique phases. Which of the following would be the first phase?

A. Development  
B. Initiation  
C. Disposal  
D. Operation / Maintenance  
E. Implementation

**Answer: B**
The order of implementation is: initiation, development, implementation, operation/maintenance, and disposal.

**Question: 246**
Risk can be totally eliminated through planning, control, procedures, and insurance. (True / False)

A. True
B. False

**Answer: B**

Whereas risk can be reduced to an acceptable level, it can NEVER be totally eliminated.

**Question: 247**

While there are many different models for IT system life cycle, most contain five unique phases. Which of the following would be the last phase?

A. Development
B. Initiation
C. Disposal
D. Operation / Maintenance
E. Implementation

**Answer: C**

The order of implementation is: initiation, development, implementation, operation/maintenance, and disposal.

**Question: 248**

Total risk is defined as:

A. Threats * Vulnerability * Asset Control Gap = Total Risk
B. Threats * Vulnerability * Asset Replacement Cost = Total Risk
C. Threats * Estimated Downtime * Asset Value = Total Risk
D. Total Risk = Asset Value * Exposure
E. Threats * Vulnerability * Asset Value = Total Risk

**Answer: E**

**Question: 249**

The amount of risk remaining after security controls have been applied is referred to as:

A. Remaining risk
B. Residual risk
C. Acceptable risk
D. Outstanding risk
E. Enduring risk

**Answer: B**

Residual risk is the amount of risk remaining after security controls have been applied.

**Question: 250**

Penetration testing involves three steps. Identify the three steps below: (Choose three)

A. War Driving
B. Network reconnaissance
C. Network Penetration
D. System Control
E. Denial of system services
F. Network scanning
Answer: B, C, D
Penetration tests are intrusive and should always have the written approval of management. The steps include: reconnaissance, penetration, and control.

Question: 251
Penetration testing involves three steps. At which step should an approve penetration test stop?

A. War Driving  
B. Network reconnaissance  
C. Network Penetration  
D. System Control  
E. Denial of system services  
F. Network scanning

Answer: C
The three steps in a penetration test include: reconnaissance, penetration, and control. An approved test is typically concluded at the point of penetration. Control of the network is usually not carried out. Penetration tests are intrusive and should always have the written approval of management.

Answer: B
The Trusted Computer Security Evaluation Criteria book (TCSEC) is also referred to as the Orange book.

Question: 253
The Trusted Computer Security Evaluation Criteria book (TCSEC) defines two types of assurance. What are they? (Choose two)

A. Life cycle assurance  
B. Quality assurance  
C. System architecture assurance  
D. OS hardening methods and assurance  
E. Operational assurance

Answer: A, E
Life cycle assurance ensures that a trusted computer base (TCB) is designed and developed with controlled standards that act to enforce protection at each stage in the system's life cycle. Operational assurance are concerned with the basic features and architecture of a system.

Question: 254
A _________ is an information path that is not normally used for communication within a computer system. It is not protected by the any of the systems security mechanisms.

A. Trojaned program
B. Backdoor
C. Covert channel
D. Hijacked session
E. Back-path

**Answer: C**

Covert channels can be used as a secret way to convey information to another person or program or for other illicit means.