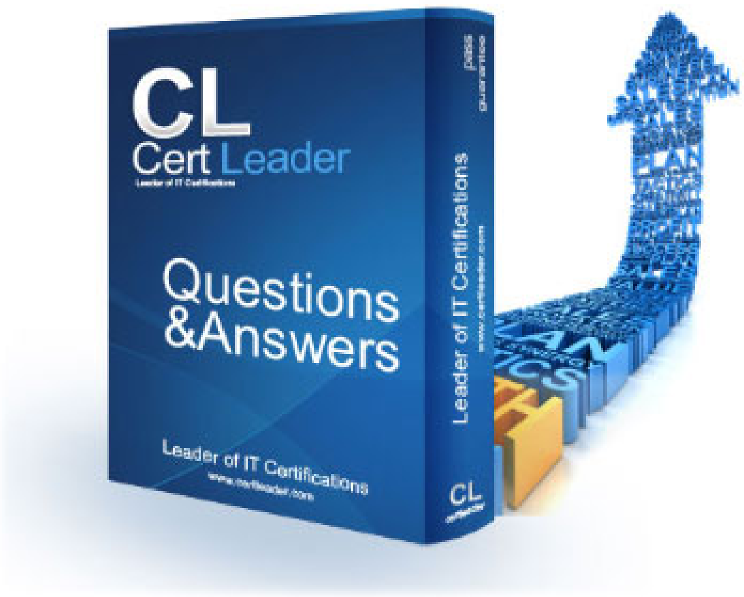
SY0-101 Dumps

SECURITY+ CERTIFICATION EXAM

https://www.certleader.com/SY0-101-dumps.html



NEW QUESTION 1
Which of the following protects the confidentiality of data by making the data unreadable to those who don't have the correct key?

A. Hashing
B. Digital signatures
C. Encryption
D. Non-repudiation

Answer: C

NEW QUESTION 2
On the topic of the DAC (Discretionary Access Control) model, choose the statement(s) which are TRUE.

A. All files that do not have a specified owner cannot be modified.
B. The system administrator is an owner of all objects.
C. The operating system is an owner of all objects.
D. All objects have an owner, and this owner has full control over that specific object.

Answer: D

NEW QUESTION 3
Communication is important to maintaining security because communication keeps:

A. the network bandwidth usage under control
B. the user community informed of threats
C. law enforcement informed of what is being done
D. the IT security budget justified

Answer: B

NEW QUESTION 4
Which access control system allows the system administrator to establish access permissions to network resources?

A. MAC
B. DAC
C. RBAC
D. None of the above.

Answer: A

NEW QUESTION 5
A programming mechanism used to allow administrative access while bypassing the usual access control methods is known as a:

A. logic bomb
B. software exploit
C. Trojan horse
D. back door

Answer: D

NEW QUESTION 6
Which of the following methods of password guessing typically requires the longest attack time?

A. Rainbow
B. Birthday
C. Dictionary
D. Brute force

Answer: D

NEW QUESTION 7
To aid in preventing the execution of malicious code in email clients, which of the following should be done by the email administrator?

A. Spam and anti-virus filters should be used
B. Regular updates should be performed
C. Preview screens should be disabled
D. Email client features should be disabled

Answer: A

NEW QUESTION 8
Which of the following access decisions are based on a Mandatory Access Control (MAC) environment?

A. Access control lists
B. Ownership
C. Group membership
D. Sensitivity labels

Answer: D

NEW QUESTION 9
Which of the following types of attacks is BEST described as an attacker capturing part of a communication and later sending that communication segment to the server while pretending to be the client?

A. TCP/IP hijacking
B. Replay
C. Back door
D. Man in the middle

Answer: B

NEW QUESTION 10
Message authentication codes are used to provide which service?

A. Integrity
B. Fault recover
C. Key recovery
D. Acknowledgement

Answer: A

NEW QUESTION 10
A user downloads and installs a new screen saver and the program starts to rename and delete random files. Which of the following would be the BEST description of this program?

A. Worm
B. Virus
C. Trojan horse
D. Logic bomb

Answer: C

NEW QUESTION 11
When should a technician perform penetration testing?

A. When the technician suspects that weak passwords exist on the network
B. When the technician is trying to guess passwords on a network
C. When the technician has permission from the owner of the network
D. When the technician is war driving and trying to gain access

Answer: C

NEW QUESTION 16
Which of the following access control models uses subject and object labels?

A. Mandatory Access Control (MAC)
B. Role Based Access Control (RBAC)
C. Rule Based Access Control (RBAC)
D. Discretionary Access Control (DAC)

Answer: A

NEW QUESTION 19
A security specialist for a large distributed network with numerous divisions is selecting an access control model. Employees in the human resource division need access to personnel information but not production data and operations employees need access to production data only. Which of the following access control models would be MOST appropriate?

A. Discretionary Access Control (DAC)
B. Rule Based Access Control (RBAC)
C. Mandatory Access Control (MAC)
D. Role Based Access Control (RBAC)

Answer: D

NEW QUESTION 23
A task-based control model is an example of which of the following?

A. Role Based Access Control (RBAC)

B. Discretionary Access Control (DAC)
C. Rule Based Access Control (RBAC)
D. Mandatory Access Control (MAC)

Answer: A

NEW QUESTION 24
An important component of a good data retention policy is:

A. backup software licensing
B. offsite storage
C. magnetic media sorting
D. server drive redundancy

Answer: B

NEW QUESTION 28
Choose the mechanism that is NOT a valid access control mechanism.

A. DAC (Discretionary Access Control) list.
B. SAC (Subjective Access Control) list.
C. MAC (Mandatory Access Control) list.
D. RBAC (Role Based Access Control) list.

Answer: B

NEW QUESTION 31
What does the DAC access control model use to identify the users who have permissions to a resource?

A. Predefined access privileges.
B. The role or responsibilities users have in the organization
C. Access Control Lists
D. None of the above.

Answer: C

NEW QUESTION 32
Non-essential services are often appealing to attackers because non-essential services: (Select TWO)

A. consume less bandwidth
B. are not visible to an IDS
C. provide root level access
D. decrease the surface area for the attack
E. are not typically configured correctly or secured
F. sustain attacks that go unnoticed

Answer: EF

NEW QUESTION 36
Which access control model uses Access Control Lists to identify the users who have permissions to a resource?

A. MAC
B. RBAC
C. DAC
D. None of the above.

Answer: C

NEW QUESTION 40
The DAC (Discretionary Access Control) model has an inherent flaw. Choose the option that describes this flaw.

A. The DAC (Discretionary Access Control) model uses only the identity of the user or specific process to control access to a resourc
B. This creates a security loophole for Trojan horse attacks.
C. The DAC (Discretionary Access Control) model uses certificates to control access to resource
D. This creates an opportunity for attackers to use your certificates.
E. The DAC (Discretionary Access Control) model does not use the identity of a user to control access to resource
F. This allows anyone to use an account to access resources.
G. The DAC (Discretionary Access Control) model does not have any known security flaws.

Answer: A

NEW QUESTION 43
The IPSec Security Association is managed by

A. ESP

B. ISAKMP
C. IEEE
D. AH

Answer: B

NEW QUESTION 47
Which of the following are types of certificate-based authentication? (Select TWO)

A. Many-to-one mapping
B. One-to-one mapping
C. One-to-many mapping
D. Many-to-many mapping

Answer: AB

NEW QUESTION 52
The ability to logon to multiple systems with the same credentials is typically known as:

A. decentralized management
B. single sign-on
C. Role Based Access Control (RBAC)
D. centralized management

Answer: B

NEW QUESTION 56
CGI scripts are susceptible to which of the following types of attacks?

A. Buffer overflows
B. SQL injection
C. Cross site scripting
D. DNS spoofing

Answer: C

NEW QUESTION 61
The risks of social engineering can be decreased by implementing: (Select TWO)

A. security awareness training
B. risk assessment policies
C. operating system patching instructions
D. vulnerability testing techniques
E. identity verification methods

Answer: AE

NEW QUESTION 65
The MOST common Certificate Server port required for secure web page access is port:

A. 25
B. 80
C. 443
D. 446

Answer: C

NEW QUESTION 70
Most key fob based identification systems use which of the following types of authentication mechanisms? (Select TWO).

A. Kerberos
B. Biometrics
C. Username/password
D. Certificates
E. Token

Answer: CE

NEW QUESTION 73
Which of the following protocols are not recommended due to them supplying passwords and information over the network?

A. Network News Transfer Protocol (NNTP)
B. SNMP (Simple Network Management Protocol).
C. Domain Name Service (DNS)
D. Internet Control Message Protocol (ICMP)

Answer: B

NEW QUESTION 77
A VPN typically provides a remote access link from one host to another over:

A. an intranet
B. a modem
C. a network interface card
D. the Internet

Answer: D

NEW QUESTION 81
Which of the following are nonessential protocols and services?

A. Network News Transfer Protocol (NNTP)
B. TFTP (Trivial File Transfer Protocol).
C. Domain Name Service (DNS)
D. Internet Control Message Protocol (ICMP)

Answer: B

NEW QUESTION 84
Which of the following steps is MOST often overlooked during the auditing process?

A. Reviewing event logs regularly
B. Enabling auditing on the system
C. Auditing every system event
D. Deciding what events to audit

Answer: A

NEW QUESTION 89
Disguising oneself as a reputable hardware manufacturer's field technician who is picking up a server for repair would be described as:

A. a phishing attack
B. a Trojan horse
C. a man-in-the-middle attack
D. social engineering

Answer: D

NEW QUESTION 94
Kerberos uses which of the following ports by default?

A. 23
B. 88
C. 139
D. 443

Answer: B

NEW QUESTION 95
Which of the following programming techniques should be used to prevent buffer overflow attacks?

A. Input validation
B. Nested loops
C. Signed applets
D. Automatic updates

Answer: A

NEW QUESTION 98
IPSec uses which of the following protocols to provide traffic security? (Select TWO).

A. SSH
B. AH
C. PPTP
D. SSL
E. L2TP
F. Encapsulating Security Protocol (ESP)

Answer: BF

NEW QUESTION 101
You work as the security administrator at Exambible.com. You must implement an authentication protocol that uses only encrypted passwords during the authentication process.
Choose the authentication protocol that accomplishes this.

A. PPTP (Point-to-Point Tunneling Protocol)
B. SMTP (Simple Mail Transfer Protocol)
C. Kerberos
D. CHAP (Challenge Handshake Authentication Protocol)

Answer: D

NEW QUESTION 105
Which of the following would be the MOST important reason to apply updates?

A. Software is a licensed product and the license will expire if not updated
B. Software is a supported product and vendors won't support the product if the latest version is not installed.
C. Software is a productivity facilitator and as new functionality is available the functionality must be enabled.
D. Software is inherently insecure and as new vulnerabilities are found the vulnerabilities must be fixed.

Answer: D

NEW QUESTION 106
A Windows file server is an example of which of the following types of models?

A. Discretionary Access Control (DAC)
B. Rule Based Access Control (RBAC)
C. Mandatory Access Control (MAC)
D. Role Based Access Control (RBAC)

Answer: A

NEW QUESTION 107
Which of the following methods of authentication makes use of hand scanners, fingerprints, retinal scanners or DNA structure to identify the user?

A. Smart Cards
B. Multi-Factor
C. Kerberos
D. Biometrics

Answer: D

NEW QUESTION 111
Which of the following would be needed to ensure that a user who has received an email cannot claim that the email was not received?

A. Anti-aliasing
B. Data integrity
C. Asymmetric cryptography
D. Non-repudiation

Answer: D

NEW QUESTION 115
A security specialist is called to an onsite vacant office where an employee has found an unauthorized wireless access device connected to an RJ-45 jack linked to the corporate LAN. Which of the following actions should the administrator take FIRST?

A. Install a sniffer.
B. Call the police.
C. Disconnect the network cable.
D. Turn off the power.

Answer: C

NEW QUESTION 118
An IDS sensor on a network is not capturing all the network data traffic. This may be happening because the sensor is connected to the network with a:

A. switch
B. hub
C. bridge
D. router

Answer: A

NEW QUESTION 123
Which of the following types of firewalls provides inspection at layer 7 of the OSI model?

A. Application-proxy
B. Network address translation (NAT)
C. Packet filters
D. Stateful inspection

Answer: A

NEW QUESTION 127
Which password management system best provides for a system with a large number of users?

A. Self service password reset management systems
B. Locally saved passwords management systems
C. multiple access methods management systems
D. synchronized passwords management systems

Answer: A

NEW QUESTION 128
A newly hired security specialist is asked to evaluate a company's network security. The security specialist discovers that users have installed personal software; the network OS has default settings and no patches have been installed and passwords are not required to be changed regularly. Which of the following would be the FIRST step to take?

A. Install software patches.
B. Disable non-essential services.
C. Enforce the security policy.
D. Password management

Answer: C

NEW QUESTION 133
WEP uses which of the following stream ciphers?

A. RC2
B. RC4
C. IKE
D. 3DES

Answer: B

NEW QUESTION 136
Turnstiles, double entry doors and security guards are all prevention measures for which of the following types of social engineering?

A. Piggybacking
B. Looking over a co-workers should'er to retrieve information
C. Looking through a co-worker's trash to retrieve information
D. Impersonation

Answer: A

NEW QUESTION 141
Which of the following is a solution that you can implement to protect against an intercepted password?

A. Implement a VPN (Virtual Private Network).
B. Implement PPTP (Point-to-Point Tunneling Protocol).
C. Implement a one time password.
D. Implement complex password requirements.

Answer: C

NEW QUESTION 144
The employees at a company are using instant messaging on company networked computers. The MOST important security issue to address when using instant messaging is that instant messaging:

A. communications are a drain on bandwidth
B. communications are open and unprotected
C. has no common protocol
D. uses weak encryption

Answer: B

NEW QUESTION 145
Which of the following describes an attacker encouraging a person to perform an action in order to be successful?

A. Man-in-the-middle
B. Social engineering

C. Back door
D. Password guessing

Answer: B

NEW QUESTION 146
The purpose of the SSID in a wireless network is to:

A. define the encryption protocols used.
B. secure the WAP
C. identify the network
D. protect the client

Answer: C

NEW QUESTION 149
A digital signature is used for:

A. storage and recovery.
B. integrity and non-repudiation.
C. access control and trusts.
D. confidentiality and encryption.

Answer: B

NEW QUESTION 153
Which of the following types of IDS uses known patterns to detect malicious activity?

A. Anomaly based
B. Detection based
C. Keyword based
D. Signature based

Answer: D

NEW QUESTION 158
Which of the following trust models would allow each user to create and sign certificates for the people they know?

A. Single certificate authority (CA)
B. Web-of-trust
C. Hierarchical
D. Browser trust-list

Answer: B

NEW QUESTION 162
A security specialist is reviewing writable FTP directories and observes several files that violate the company's security policy. In addition to checking the FTP server, the specialist should:

A. review logs for other compromises and report the situation to authorities.
B. reboot the affected server, review logs for other compromises and notify the human resources department.
C. review logs for other compromises, delete the files that violate security policy and report the situation to authorities.
D. contain the affected system, review logs for other compromises and report the situation.

Answer: D

NEW QUESTION 166
Which of the following daemons is MOST likely to be the cause if an unauthorized user obtains a copy of a Linux systems /etc/passwd file?

A. SSH with version 0.9.8a is installed and configured for remote administration.
B. Sendmail is configured to allow the administrator's web access.
C. SSL has enabled the Apache service with no virtual hosts configured
D. FTP configures to allow anonymous user access.

Answer: D

NEW QUESTION 167
Which of the following connectivity is required for a web server that is hosting an SSL based web site?

A. Port 443 inbound
B. Port 443 outbound
C. Port 80 inbound
D. Port 80 outbound

Answer: A

NEW QUESTION 168
Which of the following describes the process by which a single user name and password can be entered to access multiple computer applications?

A. Single sign-on
B. Encryption protocol
C. Access control lists
D. Constrained user interfaces

Answer: A

NEW QUESTION 172
Which of the following describes the validation of a message's origin?

A. Integrity
B. Confidentiality
C. Non-repudiation
D. Asymmetric encryption

Answer: C

NEW QUESTION 176
PKI provides non-repudiation by providing third-party assurance of certificate:

A. destruction
B. expiration
C. revocation
D. validation

Answer: D

NEW QUESTION 178
Malicious port scanning is a method of attack to determine which of the following?

A. Computer name
B. The fingerprint of the operating system
C. The physical cabling topology of a network
D. User IDs and passwords

Answer: B

NEW QUESTION 181
Using software on an individual computer to generate a key pair is an example of which of the following approaches to PKI architecture?

A. Decentralized
B. Centralized
C. Hub and spoke
D. Distributed key

Answer: A

NEW QUESTION 182
Which of the following could cause communication errors with an IPSec VPN tunnel because of changes made to the IP header?

A. SOCKS
B. NAT
C. DNS
D. Private addressing

Answer: B

NEW QUESTION 186
Users are reporting that when attempting to access the company web page on the Internet, the user is rerouted to a protest webpage. This is MOSTUsers are reporting that when attempting to access the company? web page on the Internet, the user is rerouted to a protest webpage. This is MOST likely:

A. a replay attack.
B. DNS Poisoning
C. a social engineering attack
D. a DDoS attack

Answer: B

NEW QUESTION 189

When setting password rules, which of the following would lower the level of security of a network?

A. Passwords must be greater than six characters and contain at least one non-alpha.
B. All passwords are set to expire at regular intervals and users are required to choose new passwords that have not been used before.
C. Complex passwords that users can not remotely change are randomly generated by the administrator and given to users
D. After a set number of failed attempts the server will lock out any user account forcing the user to call the administrator to re-enable the account.

Answer: C

NEW QUESTION 190
Which of the following access control models refers to assigning sensitivity labels to the user and the data?

A. Rule Based Access Control (RBAC)
B. Mandatory Access Control (MAC)
C. Discretionary Access Control (DAC)
D. Role Based Access Control (RBAC)

Answer: B

NEW QUESTION 195
Fiber optic cable is considered safer than CAT5 because fiber optic cable: (Select TWO).

A. is not susceptible to interference.
B. is hard to tap in to.
C. is made of glass rather than copper.
D. can be run for a longer distance
E. is more difficult to install

Answer: AB

NEW QUESTION 199
Pretty good privacy (PGP) uses a PKI Trust Model where no certificate authority (CA) is subordinate to another. The model with no single trusted root is known as:

A. peer-to-peer.
B. downlevel.
C. hierarchical
D. hybrid

Answer: A

NEW QUESTION 204
Which of the following types of servers should be placed on a private network?

A. Remote Access Server (RAS)
B. File and print server
C. Email server
D. Web server

Answer: B

NEW QUESTION 205
Non-repudiation is enforced by which of the following?

A. Secret keys
B. Digital signatures
C. PKI
D. Cipher block chaining

Answer: B

NEW QUESTION 209
Which of the following sequence of steps should be contained in a computer incident response policy?

A. Preparation; controlling; detection and analysis; containment, eradication and recovery
B. Preparation; detection and analysis; containment, eradication and recovery; post- incident activity
C. Planning; initiation; execution; controlling; closing
D. Planning; detection and analysis; execution; containment, eradication and recovery

Answer: B

NEW QUESTION 211
Open FTP file shares on servers can facilitate which of the following types of attacks?

A. Memory starvation
B. Disk storage consumption

C. CPU starvation
D. Smurf

Answer: B

NEW QUESTION 213
Which of the following is a protocol analyzer?

A. John the Ripper
B. WireShark
C. Cain & Abel
D. Nessus

Answer: B

NEW QUESTION 217
Which of the following VPN implementations consists of taking IPv6 security features and porting them to IPv4?

A. SSL
B. IPSec
C. L2TP
D. PPTP

Answer: B

NEW QUESTION 222
The MOST common exploits of Internet-exposed network services are due to:

A. illicit servers
B. Trojan horse programs
C. active content (e.
D. Java Applets)
E. buffer overflows

Answer: D

NEW QUESTION 225
Nmap has been run against a server and more open ports than expected have been discovered. Which of the following would be the FIRST step to take?

A. All ports should be closed and observed to see whether a process tries to reopen the port.
B. Nmap should be run again and observed to see whether different results are obtained.
C. All ports should be left open and traffic monitored for malicious activity
D. The process using the ports should be examined.

Answer: D

NEW QUESTION 226
Social engineering attacks would be MOST effective in which of the following environments? (Select TWO).

A. A locked, windowless building
B. A military facility with computer equipment containing biometrics.
C. A public building that has shared office space.
D. A company with a dedicated information technology (IT) security staff.
E. A company with a help desk whose personnel have minimal training.

Answer: CE

NEW QUESTION 227
Which of the following would be the MOST effective backup site for disaster recovery?

A. Cold site
B. Warm site
C. Hot site
D. Reciprocal agreement

Answer: C

NEW QUESTION 229
Default passwords in hardware and software should be changed:

A. if a threat becomes known.
B. once each month
C. when the hardware or software is turned on.
D. when the vendor requires it

Answer: C

NEW QUESTION 233
The process of documenting who applied a patch to a specific firewall at a specific time and what the patch is supposed to accomplish is known as:

A. user awareness.
B. change control management
C. logs and inventories
D. asset identification

Answer: B

NEW QUESTION 234
Which of the following would be an example of a hardware device where keys can be stored? (Select TWO).

A. PCI card
B. Smart card
C. PCMCIA card
D. Network interface card (NIC)

Answer: BC

NEW QUESTION 236
MITRE and CERT are:

A. virus and malware cataloging organizations.
B. anti-virus software companies.
C. virus propagation monitoring utilities.
D. spyware and virus distributing software

Answer: A

NEW QUESTION 237
Which of the following protocols suites are responsible for IP addressing?

A. ARP
B. IP
C. IGMP
D. ICMP

Answer: B

NEW QUESTION 242
One of the below options are correct regarding the DDoS (Distributed Denial of Service) attack?

A. Listening or overhearing parts of a conversation
B. Placing a computer system between the sender and receiver to capture information
C. Use of multiple computers to attack a single organization
D. Prevention access to resources by users authorized to use those resources

Answer: C

NEW QUESTION 246
Choose the correct combination of VPN (Virtual Private Network) tunneling protocols.

A. IPSec (Internet Protocol Security), L2TP (Layer Two Tunneling Protocol), and SSL (Secure Sockets Layer)
B. IPSec (Internet Protocol Security), L2TP (Layer Two Tunneling Protocol), and PPP (Point-to-Point Protocol)
C. PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer Two Tunneling Protocol), and SSL (Secure Sockets Layer)
D. PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer Two Tunneling Protocol), and IPSec (Internet Protocol Security)

Answer: D

NEW QUESTION 251
Choose the attack or malicious code that cannot be prevented or deterred solely through using technical measures.

A. Dictionary attacks.
B. Man in the middle attacks.
C. DoS (Denial of Service) attacks.
D. Social engineering.

Answer: D

NEW QUESTION 253
To which of the following viruses does the characteristic when the virus may attempt to infect your boot sector, infect all of your executable files, and destroy your

applications files
form part of?

A. Multipartite Virus
B. Armored Virus
C. Companion Virus
D. Phage Virus

Answer: A

NEW QUESTION 258
From the list of protocols, which two are VPN (Virtual Private Network) tunneling protocols? Choose two protocols.

A. PPP (Point-to-Point Protocol).
B. SLIP (Serial Line Internet Protocol).
C. L2TP (Layer Two Tunneling Protocol).
D. SMTP (Simple Mail Transfer Protocol).
E. PPTP (Point-to-Point Tunneling Protocol).

Answer: CE

NEW QUESTION 260
Choose the concept that represents the scenario where a string of data sent to a buffer is larger than the buffer is capable of handling.

A. Brute Force attack
B. Buffer overflows
C. Man in the middle attack
D. Blue Screen of Death attack
E. SYN flood attack
F. Spoofing attack

Answer: B

NEW QUESTION 262
Which of the below options would you consider as a program that constantly observes data traveling over a network?

A. Smurfer
B. Sniffer
C. Fragmenter
D. Spoofer

Answer: B

NEW QUESTION 266
Choose the network mapping tool (scanner) which uses ICMP (Internet Control Message Protocol).

A. A port scanner.
B. A map scanner.
C. A ping scanner.
D. A share scanner.

Answer: C

NEW QUESTION 267
From the options, which is a tunneling protocol that can only work on IP networks because it requires IP connectivity?

A. IPX protocol
B. L2TP protocol
C. PPTP protocol
D. SSH

Answer: C

NEW QUESTION 268
Which of the following attacks are being referred to if someone is accessing your e-mail server and sending inflammatory information to others?

A. Trojan Horse.
B. Phage Virus.
C. Repudiation Attack.
D. Polymorphic Virus.

Answer: C

NEW QUESTION 270
From the listing of attacks, choose the attack which misuses the TCP (Transmission Control Protocol) three-way handshake process, in an attempt to overload

network servers, so that authorized users are denied access to network resources?

A. Man in the middle attack
B. Smurf attack
C. Teardrop attack
D. SYN (Synchronize) attack

Answer: D

NEW QUESTION 271
Which of the following would be MOST useful in determining which internal user was the source of an attack that compromised another computer in its network?

A. The firewall's logs
B. The attacking computer's audit logs
C. The target computer's audit logs.
D. The domain controller's logs.

Answer: C

NEW QUESTION 273
Which of the following protocols is used to transmit data between a web browser and a web server?

A. SSH
B. HTTP
C. SFTP
D. IMAP4

Answer: B

NEW QUESTION 277
Which of the following options is the correct sequence for the TCP Three-Way Handshake?

A. Host A, SYN, SYN/ACK, ACK, Host B
B. Host A, ACK, SYN/ACK, Host B, SYN
C. Host A, SYN/ACK, ACK, SYN, Host B
D. Host A, ACK, SYN/ACK, SYN, Host B

Answer: A

NEW QUESTION 282
An Auditing system is necessary to prevent attacks on what part of the system?

A. The files.
B. The operating system.
C. The systems memory
D. None of the above

Answer: A

NEW QUESTION 284
Which of the following options best describe how a social engineering attack occurs?

A. You are attacked and robbed of the necessary information
B. You are e-mailed by your "manager" and he is out of town and forgot his password and you send him the necessary information
C. A family member told your "best friend" the password
D. A colleague spies on you in a quest to get your password and acquires it by reading as you type.

Answer: B

NEW QUESTION 289
One of the below is a description for a password cracker, which one is it?

A. A program that can locate and read a password file.
B. A program that provides software registration passwords or keys.
C. A program that performs comparative analysis.
D. A program that obtains privileged access to the system.

Answer: C

NEW QUESTION 292
A computer system containing personal identification information is being implemented by a company's sales department. The sales department has requested that the system become operational before a security review can be completed. Which of the following can be used to explain the reasons a security review must be completed?

A. Vulnerability assessment

B. Risk assessment
C. Corporate security policy
D. Need to know policy

Answer: C

NEW QUESTION 297
401.Which of the following are MOST likely to be analyzed by Internet filter appliances/servers? (Select THREE).401.Which of the following are MOST likely to be analyzed by Internet filter appliances/servers? (Select THREE).

A. Certificates
B. Keys
C. TLSs
D. URLs
E. Content
F. CRLs

Answer: ADE

NEW QUESTION 301
Which of the following has largely replaced SLIP?

A. SLIP (Serial Line Internet Protocol)
B. PPP (Point-to-Point Protocol)
C. VPN
D. RADIUS (Remote Authentication Dial-In User Service)

Answer: B

NEW QUESTION 305
Choose the malicious code which can distribute itself without using having to attach to a host file.

A. A virus.
B. A Trojan horse.
C. A logic bomb.
D. A worm.

Answer: D

NEW QUESTION 308
Which of the following assessment tools would be MOST appropriate for determining if a password was being sent across the network in clear text?

A. Protocol analyzer
B. Port scanner
C. Password cracker
D. Vulnerability scanner

Answer: A

NEW QUESTION 313
For a SSL (Secure Sockets Layer) connection to be automatically established between a web client and server, a specific element has to exist. Which is it?

A. Shared password.
B. Certificate signed by a trusted root CA (Certificate Authority).
C. Address on the same subnet.
D. Common operating system.

Answer: B

NEW QUESTION 316
You work as the security administrator at Exambible.com. You want to implement a solution which will provide a WLAN (Wireless Local Area Network) with the security typically associated with a wired LAN (Local Area Network):
Which solution should you implement?

A. WEP (Wired Equivalent Privacy)
B. ISSE (Information Systems Security Engineering)
C. ISDN (Integrated Services Digital Network)
D. VPN (Virtual Private Network)

Answer: A

NEW QUESTION 318
Which of the following definitions fit correctly to IPSec?

A. It supports encapsulation in a single point-to-point environment

B. It was created by Cisco as a method of creating tunnels primarily for dial-up connections
C. It is primarily a point-to-point protocol
D. It is not a tunneling protocol, but it is used in conjunction with tunneling protocols.

Answer: D

NEW QUESTION 322
Which of the following freeware forensic tools is used to capture packet traffic from a network?

A. NESSUS
B. dd
C. tcpdump
D. nmap

Answer: C

NEW QUESTION 326
Which of the following web vulnerabilities is being referred to when it receives more data than it is programmed to accept?

A. Buffer Overflows.
B. Cookies.
C. CGI.
D. SMTP Relay

Answer: A

NEW QUESTION 328
Which of the following statements are true regarding File Sharing?

A. FTP is a protocol, a client, and a server.
B. Security was based on the honor system.
C. As discussed earlier, SSH is a program that allows connections to be secured by encrypting the session between the client and the server.
D. When files are stored on a workstation, the connection is referred to as a peer-to-peer connection.

Answer: D

NEW QUESTION 329
Which of the following Directory Services does the statement that it stores information on all system resources, users, and any other relevant information about systems attached to a NetWare server refer to?

A. LDAP
B. Active Directory
C. X.500
D. eDirectory

Answer: D

NEW QUESTION 330
Which of the following type of fire suppression tools would cause the MOST damage to electrical equipment?

A. Water
B. Carbon Dioxide
C. Halon
D. Foam

Answer: A

NEW QUESTION 331
SSL (Secure Socket Layer) establishes a stateful connection negotiated by a process performed between client and server. Identify the protocol (steps) that allow for the following:
1. Client and server authentication.
2. MAC (Mandatory Access Control) and encryption algorithm negotiation.
3. Selection of cryptographic keys.

A. SSL (Secure Sockets Layer) alert protocol.
B. SSL (Secure Sockets Layer) change cipher spec protocol.
C. SSL (Secure Sockets Layer) record protocol.
D. SSL (Secure Sockets Layer) handshake protocol.

Answer: D

NEW QUESTION 332
Which of the following definitions BEST suit JavaScript?

A. It is a programming language that allows access to system resources of the system running the script

B. The client browser must have the ability to run Java applets in a virtual machine on the client
C. It can also include a digital signature to verify authenticity
D. It allows customized controls, icons, and other features to increase the usability of web enabled systems

Answer: A

NEW QUESTION 337
On the topic of comparing viruses and hoaxes, which statement is TRUE? Choose the best TRUE statement.

A. Hoaxes can create as much damage as a real virus.
B. Hoaxes are harmless pranks and should be ignored.
C. Hoaxes can help educate users about a virus.
D. Hoaxes carry a malicious payload and can be destructive.

Answer: A

NEW QUESTION 342
Which of the following trust models would allow each user to create and sign certificates for the people they know?

A. Single certificate authority (CA)
B. Web-of-trust
C. Hierarchical
D. Browser trust-list

Answer: B

NEW QUESTION 345
Which scenario or element would typically cause a CGI (Common Gateway Interface) security issue?

A. The HTTP (Hypertext Transfer Protocol) protocol.
B. The compiler or interpreter which runs the CGI script.
C. The web browser.
D. The external data provided by the user.

Answer: D

NEW QUESTION 349
Choose the ports that are used to access the FTP (File Transfer Protocol) protocol.

A. Ports 80 and 443.
B. Ports 20 and 21.
C. Ports 21 and 23.
D. Ports 20 and 80.

Answer: B

NEW QUESTION 351
Which of the following definitions BEST suit Buffer Overflow?

A. It receives more data than it is programmed to accept.
B. It is used to provide a persistent, customized web experience for each visit.
C. It's an older form of scripting that was used extensively in early web systems
D. It has a feature designed into many e-mail servers that allows them to forward e-mail to other e-mail servers

Answer: A

NEW QUESTION 356
Choose the primary disadvantage of using a third party mail relay.

A. Spammers can utilize the third party mail relay.
B. A third party mail relay limits access to specific users.
C. A third party mail relay restricts the types of e-mail that maybe sent.
D. A third party mail relay restricts spammers from gaining access.

Answer: A

NEW QUESTION 361
You work as the security administrator at Exambible.com. You want to implement a solution which will provide the following for handled devices in your wireless network:
1. Data privacy
2. Data integrity
3. Authentication
Which solution should you implement?

A. WEP (Wired Equivalent Privacy)

B. WAP (Wireless Application Protocol)
C. WSET (Wireless Secure Electronic Transaction)
D. WTLS (Wireless Transport Layer Security)

Answer: D

NEW QUESTION 364
One of the following options details the main advantage of why you should choose to use SSL (Secure Sockets Layer) over using HTTPS (Hypertext Transfer Protocol over Secure Sockets Layer). Which is it?

A. SSL provides full application security for HTTP whereas HTTPS does not.
B. SSL supports additional Application layer protocols, for instance FTP (File Transfer Protocol) and NNTP (Network News Transport Protocol), whereas HTTPS does not.
C. SSL and HTTPS are transparent to the application.
D. SSL supports user authentication whereas HTTPS does not.

Answer: B

NEW QUESTION 369
You work as the security administrator at Exambible.com. The Exambible.com network must be configured to allow LDAP (Lightweight Directory Access Protocol) traffic.
Which ports must you open on the firewall to allow LDAP traffic?

A. Open ports 389 and 636
B. Open ports 389 and 139
C. Open ports 636 and 137
D. Open ports 137 and 139

Answer: A

NEW QUESTION 371
Choose the scheme or system used by PGP (Pretty Good Privacy) to encrypt data.

A. Asymmetric scheme
B. Symmetric scheme
C. Symmetric key distribution system
D. Asymmetric key distribution system

Answer: A

NEW QUESTION 373
Which of the following definitions fit correctly to L2TP?

A. It supports encapsulation in a single point-to-point environment
B. It was created by Cisco as a method of creating tunnels primarily for dial-up connections
C. It is primarily a point-to-point protocol
D. It is a tunneling protocol originally designed for UNIX systems.

Answer: C

NEW QUESTION 378
Which of the following CANNOT be performed by a proxy server?

A. Network Address Translation.
B. Web page caching.
C. Packet filtering.
D. Data encryption.

Answer: D

NEW QUESTION 379
Which of the following should be scanned for viruses?

A. Plain text documents.
B. Microsoft Word documents.
C. Executable files.
D. All of the above.

Answer: C

NEW QUESTION 380
Which of the following characteristics form part of an IEEE (Institute of Electrical and Electronics Engineers) connection?

A. A low-power transmitter
B. A wireless device

C. An access point
D. All of the above

Answer: D

NEW QUESTION 382
WTLS (Wireless Transport Layer Security) provides security services between network devices or mechanisms. Which is it? Choose all that apply.

A. Web server.
B. Mobile device.
C. Wireless client.
D. Wireless network interface card.
E. WAP (Wireless Application Protocol) gateway

Answer: BE

NEW QUESTION 387
Which of the following networking devices is MOST often used to eliminate the capturing of data packets not destined for the host machine?

A. Switch
B. Router
C. Hub
D. Concentrator

Answer: A

NEW QUESTION 390
Documentation describing a group's expected minimum behavior is known as:

A. the need to know.
B. acceptable usage.
C. the separation of duties.
D. a code of ethics.

Answer: D

NEW QUESTION 395
From the options, choose the disadvantage of implementing an IDS (Intrusion Detection System).

A. False positives.
B. Decrease in throughput.
C. Compatibility.
D. Administration

Answer: A

NEW QUESTION 397
Which of the following coorectly specifies where user accounts and passwords are stored in a decentralized privilege management environment?

A. User accounts and passwords are stored on a central authentication server.
B. User accounts and passwords are stored on each individual server.
C. User accounts and passwords are stored on no more than two servers.
D. User accounts and passwords are stored on a server configured for decentralized management.

Answer: B

NEW QUESTION 400
When should you remove all systems that were affected by an attack, for immediate evidence collection and system recovery purposes?

A. When an attack is in progress.
B. When an attack is over.
C. When an attack is being performed and also when it is over.

Answer: B

NEW QUESTION 404
Which of the following standards does S/MIME use to perform public key exchange and authentication?

A. RC2
B. X.509
C. 3DES
D. RSA

Answer: B

NEW QUESTION 406
Which of the following is a suitable hashing algorithm for a secure environment?

A. MD5 because it produces 160-bits message digests
B. RC4 because it produces 160-bits message digests
C. MD5 because it produces fewer numbers of collisions.
D. SHA-1 because it produces 160-bits message digests.

Answer: A

NEW QUESTION 408
From the options, which details a specific advantage of implementing a single sign-on technology?

A. Users must log on twice at all times.
B. You can configure system wide permissions.
C. Multiple applications can be installed.
D. Multiple directories can be browsed.

Answer: D

NEW QUESTION 410
Which of the following BEST describes the sequence of steps in the auditing process?

A. Enable auditing and set auditing to record all events.
B. Set auditing on the object and respond as alerts are generated.
C. Enable auditing, set auditing on the object and respond as alerts are generated.
D. Enable auditing, set auditing on objects and review event logs.

Answer: D

NEW QUESTION 415
You work as the security administrator at Exambible.com. Exambible.com has headquarters in London and a branch office in Paris. You must ensure that a secure connection is established between the London headquarters and the Paris branch office over the public network.
You deploy IPSec (Internet Protocol Security) to achieve this goal. You must still configure the IPSec mode for the router at each location.
Which IPSec mode should you configure?

A. Secure moe
B. Tunnel mode
C. Transport mode
D. Data link mode

Answer: B

NEW QUESTION 416
You work as the security administrator at Exambible.com. One morning you discover that a user named Mia Hamm has used her user account to log on to a network server. Mia has then executed a program and been able to perform operations which only a network administrator or security administrator should be able to. What type of attack has occurred?

A. Trojan horse.
B. Privilege escalation attack.
C. Subseven back door.
D. Security policy removal.

Answer: B

NEW QUESTION 419
You work as the security administrator at Exambible.com. You have become aware of a hacker accessing confidential company data from over the network.
Which of the following actions should you perform? Choose all correct answers.

A. Prevent members of the organization from entering the server room.
B. Prevent members of the incident response team from entering the server room.
C. Shut down the server to prevent the hacker from accessing more data.
D. Detach the network cable from the server to prevent the hacker from accessing more data

Answer: AD

NEW QUESTION 421
Which of the following is a popular network IDS system?

A. Tripwire
B. Snort
C. SWATCH
D. None of the above

Answer: B

NEW QUESTION 426
Which of the following intrusion detection technologies work by monitoring the file structure of a system to determine whether any system files were deleted or modified by an attacker?

A. Network IDS
B. Host-based IDS
C. System integrity verifier (SIV)
D. Log file monitor (LFM)

Answer: C

NEW QUESTION 429
Which if the following technologies would you use if you need to implement a system that simulates a network of vulnerable devices, so that this network can be targeted by attackers?

A. A IDS
B. A circuit-level firewall
C. A honeypot
D. A system integrity verifier

Answer: C

NEW QUESTION 432
A compromise of which device could result in a VLAN being compromised?

A. Router
B. Switch
C. NAT server
D. None of the above

Answer: B

NEW QUESTION 435
Automatic collection of evidence involves the collection of evidence using a number of tools. Choose the option that is FALSE?

A. Intrusion detection systems (IDSs).
B. Monitoring tools.
C. Specialized tools that collect evidence from hard drives, system cache, CPU caches, RAM and virtual memory.
D. Network data analysis tools.

Answer: C

NEW QUESTION 437
From the options, which explains the general standpoint behind a DMZ (Demilitarized Zone)?

A. All systems on the DMZ can be compromised because the DMZ can be accessed from the Internet.
B. No systems on the DMZ can be compromised because the DMZ cannot be accessed from the Internet.
C. Only those systems on the DMZ that can be accessed from the Internet can be compromised.
D. No systems on the DMZ can be compromised because the DMZ is completely secure and cannot be accessed from the Internet.

Answer: A

NEW QUESTION 441
Which of the following types of network cabling has a center conductor, an outer conductor
, and an outer sheath; where the center conductor is used to carry data from point to point?

A. Coaxial cable.
B. STP (Shielded Twisted Pair) cable.
C. UTP (Unshielded Twisted Pair) cable.
D. Fiber-optic cable.

Answer: A

NEW QUESTION 444
You work as the security administrator at Exambible.com. You must ensure that internal access to other parts of the network is controlled and restricted. The solution which you implement to restrict network access must be hardware based. You also want to use the least amount of administrative effort to accomplish your task.
How will you accomplish the task?

A. Deploy firewalls between your subnets.
B. Deploy a VLAN (Virtual Local Area Network) Deploy.
C. Deploy a proxy server Deploy.
D. Deploy a VPN (Virtual Private Network).

Answer: B

NEW QUESTION 449
Which concept correctly specifies the location where a system administrator would deploy a web server if that web server should be separated from other network servers?

A. A honey pot
B. A hybrid subnet
C. A DMZ (Demilitarized Zone)
D. A VLAN (Virtual Local Area Network)

Answer: C

NEW QUESTION 451
Which of the following types of network cabling has no shielding?

A. Coaxial cable.
B. Unshielded Twisted Pair.
C. Shielded Twisted Pair.
D. Fiber optic cable.

Answer: B

NEW QUESTION 454
When evidence is used in court, a number of factors must be TRUE for the actual data. Choose the option that is FALSE.

A. The data must be legally usable or admissible in court, and must represent a complete copy.
B. The data must have been modified while it was being collected, documented, and maintained or stored; so that is current.
C. The data must have been secured from when evidence gathering commenced, to the point at which it is in court.
D. The data must have been collected through a reliable procedure.

Answer: B

NEW QUESTION 458
Which of the following personnel security policies detail processes for terminating employment of employees, and should specify that the appropriate personnel be informed so that the necessary accounts can be disabled and systems be backed up?

A. Acceptable use policies
B. Ethics policies
C. Need to Know policies
D. Termination policies

Answer: D

NEW QUESTION 461
A program allows a user to execute code with a higher level of security than the user should have access to. Which of the following is this an example of?

A. Privilege escalation
B. Default accounts
C. Weak passwords
D. DoS

Answer: A

NEW QUESTION 465
Of the intrusion detection capabilities listed below, which is FALSE for a network based IDS system?

A. A network based IDS system can monitor and report on all network traffic, based on where it is located.
B. A network based IDS system can see packet header information, which is invisible to host-based IDS systems.
C. A network based IDS system can detect dial-in intrusions and attempts to physically access the server.
D. A network based IDS system can detect attacks in progress, attack patterns within the network and malicious activities.

Answer: C

NEW QUESTION 467
Which of the following should be considered when subnetting is performed? (Select TWO).

A. The number of networks
B. The number of domains
C. The number of workgroups
D. The number of hosts
E. The number of hops

Answer: AD

NEW QUESTION 471
Which of the following is the MOST efficient way to force a large number of users to change their passwords on logon?

A. Force the change by security group.
B. Force the change with remote logon.
C. Force the change with registry editor.
D. Force the change with group policy

Answer: D

NEW QUESTION 472
You work as the security administrator at Exambible.com. You want to reduce the current vulnerability from dumpster diving.
How will you accomplish the task?

A. Employ additional security staff
B. Destroy all paper and other media that are no longer required.
C. Install expensive surveillance equipment.
D. Remove the contents of the trash can on a regular basis.

Answer: B

NEW QUESTION 474
A host-based IDS system can perform a number of monitoring and intrusion detection activities which a network IDS cannot. Choose the one that does not apply?

A. Can monitor system activity on the workstation
B. Can monitor workstation activity.
C. Can see information within encrypted tunnels.
D. Can monitor program installations.
E. Can monitor user logon/logoff events.

Answer: C

NEW QUESTION 478
Which IDS response type(s) only collects information on the attack and reports it?

A. Active response method
B. Passive response method
C. Both of these response methods

Answer: B

NEW QUESTION 483
Choose the terminology used to refer to the situation when authorized access is perceived as an intrusion or network attack.

A. False negative
B. False intrusion
C. False positive
D. False alarm

Answer: B

NEW QUESTION 484
Which type of policies must clearly define which type of data is allowed and which type of data is not allowed to move over the firewall?

A. Privacy policy
B. Firewall policy
C. Violations reporting policy
D. Network maintenance policy

Answer: B

NEW QUESTION 486
What is the BEST process of removing PII data from a disk drive before reuse?

A. Destruction
B. Sanitization
C. Reformatting
D. Degaussing

Answer: B

NEW QUESTION 490
Which ports need to be open to allow a user to login remotely onto a workstation?

A. 53
B. 636
C. 3389
D. 8080

Answer: C

NEW QUESTION 495
With reference to locating honeypots, which of the following locations is the most dangerous placement strategy because an administrator has little control over it?

A. Inside the DMZ
B. Outside all firewalls.
C. Inside the private network
D. All of the above.

Answer: B

NEW QUESTION 499
Which of the following will allow a credit card information theft? (chose TWO)

A. Worm
B. Phishing
C. SPIM
D. Virus
E. Adwar

Answer: BE

NEW QUESTION 504
Choose the option that best defines what a security patch is?

A. It is a major, crucial update for an operating system or product for which it is intended, and consists of a collection of patches released to date since the operating system or product was shipped.
B. It is a fully tested hotfix, which addresses a new vulnerability, is mandatory for all users, and should be deployed as soon as possible.
C. It is a crucial update that should be deployed on each operating system installation as soon as possible.
D. It is a not fully tested software fix which addresses a specific issue(s) being experienced by certain customers.

Answer: B

NEW QUESTION 505
A technician wants to be able to add new users to a few key groups by default, which of the following will allow this?

A. Auto-population
B. Inheritance
C. Default pairing
D. Template

Answer: B

NEW QUESTION 510
Which of the following activities is MOST closely associated with DLL injection?

A. Penetration testing
B. Network mapping
C. Vulnerability assessment
D. SQL servers

Answer: A

NEW QUESTION 514
Privileges are used for which of the following purposes?

A. To allow or deny specific actions to users or groups
B. To allow or deny signature updates to group applications
C. To allow or deny network traffic from host based systems
D. To allow or deny network traffic from server based systems

Answer: A

NEW QUESTION 515
……