QUESTION 468
The company has implemented a backup plan. James is working as a network administrator for the company and is taking full backups of the data every time a backup is initiated. Alex who is a senior security manager talks to him about using a differential backup instead and asks him to implement this once a full backup of the data is completed. What is/are the reason(s) Alex is suggesting that James use a differential backup? (Select all that apply)

A. Less storage space is required
B. Father restoration
C. Slower than a full backup
D. Faster than a full backup
E. Less expensive than full backup

Answer: AD

QUESTION 469
The agency Jacob works for stores and transmits vast amounts of sensitive government data that cannot be compromised. Jacob has implemented Encapsulating Security Payload (ESP) to encrypt IP traffic. Jacob wants to encrypt the IP traffic by inserting the ESP header in the IP datagram before the transport layer protocol header. What mode of ESP does Jacob need to use to encrypt the IP traffic?

A. He should use ESP in transport mode.
B. Jacob should utilize ESP in tunnel mode.
C. Jacob should use ESP in pass-through mode.
D. He should use ESP in gateway mode

Answer: B

QUESTION 470
Kyle, a front office executive, suspects that a Trojan has infected his computer. What should be his first course of action to deal with the incident?

A. Contain the damage
B. Disconnect the five infected devices from the network
C. Inform the IRT about the incident and wait for their response
D. Inform everybody in the organization about the attack

Answer: C

QUESTION 471
Katie has implemented the RAID level that split data into blocks and evenly write the data to multiple hard drives but does not provide data redundancy. This type of RAID level requires a minimum of_____in order to setup.

A. Four drives
B. Three drives
C. Two drives
D. Six drives

Answer: C

QUESTION 472
Henry needs to design a backup strategy for the organization with no service level downtime. Which backup method will he select?

A. Normal backup
B. Warm backup
C. Hot backup
D. Cold backup

Answer: C

QUESTION 473
James wants to implement certain control measures to prevent denial-of-service attacks against the organization. Which of the following control measures can help James?

A. Strong passwords
B. Reduce the sessions time-out duration for the connection attempts
C. A honeypot in DMZ
D. Provide network-based anti-virus

Answer: B

QUESTION 474
An US-based organization decided to implement a RAID storage technology for their data backup plan. John wants to setup a RAID level that require a minimum of six drives but will meet high fault tolerance and with a high speed for the data read and write operations. What RAID level is John considering to meet this requirement?

A. RAID level 1
B. RAID level 10
C. RAID level 5
D. RAID level 50

Answer: D

QUESTION 475
An attacker uses different types of password cracking techniques to crack the password and gain unauthorized access to a system. An attacker uses a file containing a list of commonly used passwords. They then upload this file into the cracking application that runs against the user accounts. Which of the following password cracking techniques is the attacker trying?

A. Bruteforce
B. Rainbow table
C. Hybrid
D. Dictionary

Answer: D

QUESTION 476
A company wants to implement a data backup method which allows them to encrypt the data ensuring its security as well as access at any time and from any location. What is the appropriate backup method that should be implemented?

A. Onsite backup
B. Hot site backup
C. Offsite backup
D. Cloud backup

Answer: D

QUESTION 477
If there is a fire incident caused by an electrical appliance short-circuit, which fire suppressant should be used to control it?

A. Water
B. Wet chemical
C. Dry chemical
D. Raw chemical

Answer: C

QUESTION 478
Kyle is an IT technician managing 25 workstations and 4 servers. The servers run applications and mostly store confidential data. Kyle must backup the server's data daily to ensure nothing is lost. The power in the company's office is not always reliable, Kyle needs to make sure the servers do not go down or are without power for too long. Kyle decides to purchase an Uninterruptible Power Supply (UPS) that has a pair of inverters and converters to charge the battery and provides power when needed. What type of UPS has Kyle purchased?

A. Kyle purchased a Ferro resonant Standby UPS.
B. Kyle purchased a Line-Interactive UPS
C. He has bought a Standby UPS
D. He purchased a True Online UPS.

Answer: C

QUESTION 479
Ross manages 30 employees and only 25 computers in the organization. The network the company uses is a peer-to-peer. Ross configures access control measures allowing the employees to set their own control measures for their files and folders. Which access control did Ross implement?

A. Discretionary access control
B. Mandatory access control
C. Non-discretionary access control
D. Role-based access control

Answer: A

QUESTION 480
Paul is a network security technician working on a contract for a laptop manufacturing company in Chicago. He has focused primarily on securing network devices, firewalls, and traffic traversing in and out of the network. He just finished setting up a server a gateway between the internal private network and the outside public network. This server will act as a proxy, limited amount of services, and will filter packets. What is this type of server called?

A. Bastion host
B. Edge transport server

C. SOCKS hsot
D. Session layer firewall

Answer: A

QUESTION 481
Larry is responsible for the company's network consisting of 300 workstations and 25 servers. After using a hosted email service for a year, the company wants to control the email internally. Larry likes this idea because it will give him more control over the email. Larry wants to purchase a server for email but does not want the server to be on the internal network due to the potential to cause security risks. He decides to place the server outside of the company's internal firewall. There is another firewall connected directly to the Internet that will protect traffic from accessing the email server. The server will be placed between the two firewalls. What logical area is Larry putting the new email server into?

A. He is going to place the server in a Demilitarized Zone (DMZ)
B. He will put the email server in an IPsec zone.
C. Larry is going to put the email server in a hot-server zone.
D. For security reasons, Larry is going to place the email server in the company's Logical Buffer Zone (LBZ).

Answer: A

QUESTION 482
Cindy is the network security administrator for her company. She just got back from a security conference in Las Vegas where they talked about all kinds of old and new security threats; many of which she did not know of. She is worried about the current security state of her company's network so she decides to start scanning the network from an external IP address. To see how some of the hosts on her network react, she sends out SYN packets to an IP range. A number of IPs responds with a SYN/ACK response. Before the connection is established, she sends RST packets to those hosts to stop the session. She has done this to see how her intrusion detection system will log the traffic. What type of scan is Cindy attempting here?

A. The type of scan she is usinq is called a NULL scan.
B. Cindy is using a half-open scan to find live hosts on her network.
C. Cindy is attempting to find live hosts on her company's network by using a XMAS scan.
D. She is utilizing a RST scan to find live hosts that are listening on her network.

Answer: B

QUESTION 483
A newly joined network administrator wants to assess the organization against possible risk. He notices the organization doesn't have a_____identified which helps measure how risky an activity is.

A. Risk Severity
B. Risk Matrix
C. Key Risk Indicator
D. Risk levels

Answer: C

QUESTION 484
A VPN Concentrator acts as a bidirectional tunnel endpoint among host machines. What are the other f unction(s) of the device? (Select all that apply)

A. Provides access memory, achieving high efficiency
B. Assigns user addresses
C. Enables input/output (I/O) operations

D. Manages security keys

Answer: BCD

QUESTION 485
James is working as a Network Administrator in a reputed company situated in California. He is monitoring his network traffic with the help of Wireshark. He wants to check and analyze the traffic against a PING sweep attack. Which of the following Wireshark filters will he use?

A. lcmp.type==0 and icmp.type==16
B. lcmp.type==8 or icmp.type==16
C. lcmp.type==8 and icmp.type==0
D. lcmp.type==8 or icmp.type==0

Answer: D

QUESTION 486
Harry has successfully completed the vulnerability scanning process and found serious vulnerabilities exist in the organization's network. Identify the vulnerability management phases through which he will proceed to ensure all the detected vulnerabilities are addressed and eradicated. (Select all that apply)

A. Mitigation
B. Assessment
C. Verification
D. Remediation

Answer: ACD

QUESTION 487
George was conducting a recovery drill test as a part of his network operation. Recovery drill tests are conducted on the_____.

A. Archived data
B. Deleted data
C. Data in transit
D. Backup data

Answer: D

QUESTION 488
During a security awareness program, management was explaining the various reasons which create threats to network security. Which could be a possible threat to network security?

A. Configuring automatic OS updates
B. Having a web server in the internal network
C. Implementing VPN
D. Patch management

Answer: B

QUESTION 489
Identify the network topology where each computer acts as a repeater and the data passes from one computer to the other in a single direction until it reaches the destination.

A. Ring

B. Mesh
C. Bus
D. Star

Answer: A

QUESTION 490
John, the network administrator and he wants to enable the NetFlow feature in Cisco routers to collect and monitor the IP network traffic passing through the router.
Which command will John use to enable NetFlow on an interface?

A. Router(Config-if) # IP route - cache flow
B. Router# Netmon enable
C. Router IP route
D. Router# netflow enable

Answer: A

QUESTION 491
Michael decides to view the----------to track employee actions on the organization's network.

A. Firewall policy
B. Firewall log
C. Firewall settings
D. Firewall rule set

Answer: B

QUESTION 492
Kyle is an IT consultant working on a contract for a large energy company in Houston. Kyle was hired on to do contract work three weeks ago so the company could prepare for an external IT security audit. With suggestions from upper management, Kyle has installed a network-based IDS system. This system checks for abnormal behavior and patterns found in network traffic that appear to be dissimilar from the traffic normally recorded by the IDS. What type of detection is this network-based IDS system using?

A. This network-based IDS system is using anomaly detection.
B. This network-based IDS system is using dissimilarity algorithms.
C. This system is using misuse detection.
D. This network-based IDS is utilizing definition-based detection.

Answer: A

QUESTION 493
Mark is monitoring the network traffic on his organization's network. He wants to detect a TCP and UDP ping sweep on his network. Which type of filter will be used to detect this on the network?

A. Tcp.srcport==7 and udp.srcport==7
B. Tcp.srcport==7 and udp.dstport==7
C. Tcp.dstport==7 and udp.srcport==7
D. Tcp.dstport==7 and udp.dstport==7

Answer: D

QUESTION 494
Ivan needs to pick an encryption method that is scalable even though it might be slower. He has settled on a method

that works where one key is public and the other is private. What encryption method did Ivan settle on?

A. Ivan settled on the private encryption method.
B. Ivan settled on the symmetric encryption method.
C. Ivan settled on the asymmetric encryption method
D. Ivan settled on the hashing encryption method

Answer: C

QUESTION 495
Identify the password cracking attempt involving precomputed hash values stored as plaintext and using these to crack the password.

A. Bruteforce
B. Rainbow table
C. Dictionary
D. Hybrid

Answer: B

QUESTION 496
Justine has been tasked by her supervisor to ensure that the company's physical security is on the same level as their logical security measures. She installs video cameras at all entrances and exits and installs badge access points for all doors. The last item she wants to install is a method to prevent unauthorized people piggybacking employees. What should she install to prevent piggybacking?

A. She should install a mantrap
B. Justine needs to install a biometrics station at each entrance
C. Justine will need to install a revolving security door
D. She should install a Thompson Trapdoor.

Answer: A

QUESTION 497
Tom works as a network administrator in a multinational organization having branches across North America and Europe. Tom wants to implement a storage technology that can provide centralized data storage and provide free data backup on the server. He should be able to perform data backup and recovery more efficiently with the selected technology. Which of the following storage technologies best suits Tom's requirements?

A. DAS
B. PAS
C. RAID
D. NAS

Answer: D

QUESTION 498
Identify the spread spectrum technique that multiplies the original data signal with a pseudo random noise spreading code.

A. FHSS
B. DSSS
C. OFDM
D. ISM

Answer: B