Exam : 312-38

Title : Certified Network Defender (CND)

Version : V10.02

1.Timothy works as a network administrator in a multinational organization. He decides to implement a dedicated network for sharing storage resources. He uses a_______as it seperates the storage units from the servers and the user network.

A. SAN

B. SCSA

C. NAS

D. SAS

Answer: A

2.Management wants to bring their organization into compliance with the ISO standard for information security risk management.

Which ISO standard will management decide to implement?

A. ISO/IEC 27004

B. ISO/IEC 27002

C. ISO/IEC 27006

D. ISO/IEC 27005

Answer: D

3.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

4.Which of the following is a best practice for wireless network security?

A. Enabling the remote router login

B. Do not changing the default SSID

C. Do not placing packet filter between the AP and the corporate intranet

D. Using SSID cloaking

Answer: D

5.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

6.Alex is administrating the firewall in the organization's network.

What command will he use to check all the remote addresses and ports in numerical form?

A. Netstat -o

B. Netstat -a

C. Netstat -ao

D. Netstat -an

Answer: D

7.Blake is working on the company's updated disaster and business continuity plan. The last section of the plan covers computer and data incidence response.

Blake is outlining the level of severity for each type of incident in the plan. Unsuccessful scans and probes are at what severity level?

A. Extreme severity level

B. Low severity level

C. Mid severity level

D. High severity level

Answer: B

8.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

9.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

10.Fred is a network technician working for Johnson Services, a temporary employment agency in Boston. Johnson Services has three remote offices in New England and the headquarters in Boston where Fred works.

The company relies on a number of customized applications to perform daily tasks and unfortunately these applications require users to be local administrators. Because of this, Fred's supervisor wants to implement tighter security measures in other areas to compensate for the inherent risks in making those users local admins. Fred's boss wants a solution that will be placed on all computers throughout the company and monitored by Fred. This solution will gather information on all network traffic to and from the local computers without actually affecting the traffic.

What type of solution does Fred's boss want to implement?

A. Fred's boss wants a NIDS implementation.

B. Fred's boss wants Fred to monitor a NIPS system.

C. Fred's boss wants to implement a HIPS solution.

D. Fred's boss wants to implement a HIDS solution.

Answer: D

11.Heather has been tasked with setting up and implementing VPN tunnels to remote offices. She will most likely be implementing IPsec VPN tunnels to connect the offices.

At what layer of the OSI model does an IPsec tunnel function on?

A. They work on the session layer.

B. They function on either the application or the physical layer.

C. They function on the data link layer

D. They work on the network layer

Answer: D

12.Alex is administrating the firewall in the organization's network.

What command will he use to check the ports applications open?

A. Netstat -an

B. Netstat -o

C. Netstat -a

D. Netstat -ao

Answer: A

13.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

14.Management decides to implement a risk management system to reduce and maintain the organization's risk at an acceptable level.

Which of the following is the correct order in the risk management phase?

A. Risk Identification, Risk Assessment, Risk Treatment, Risk Monitoring & Review

B. Risk Treatment, Risk Monitoring & Review, Risk Identification, Risk Assessment

C. Risk Assessment, Risk Treatment, Risk Monitoring & Review, Risk Identification

D. Risk Identification. Risk Assessment. Risk Monitoring & Review, Risk Treatment

Answer: A

15.John wants to implement a firewall service that works at the session layer of the OSI model. The firewall must also have the ability to hide the private network information.

Which type of firewall service is John thinking of implementing?

A. Application level gateway

B. Stateful Multilayer Inspection

C. Circuit level gateway

D. Packet Filtering

Answer: C

16.Frank is a network technician working for a medium-sized law firm in Memphis. Frank and two other IT employees take care of all the technical needs for the firm. The firm's partners have asked that a secure wireless network be implemented in the office so employees can move about freely without being tied to a network cable. While Frank and his colleagues are familiar with wired Ethernet technologies, 802.3, they are not familiar with how to setup wireless in a business environment.

What IEEE standard should Frank and the other IT employees follow to become familiar with wireless?

A. The IEEE standard covering wireless is 802.9 and they should follow this.

B. 802.7 covers wireless standards and should be followed

C. They should follow the 802.11 standard

D. Frank and the other IT employees should follow the 802.1 standard.

Answer: C

17.If a network is at risk from unskilled individuals, what type of threat is this?

A. External Threats

B. Structured Threats

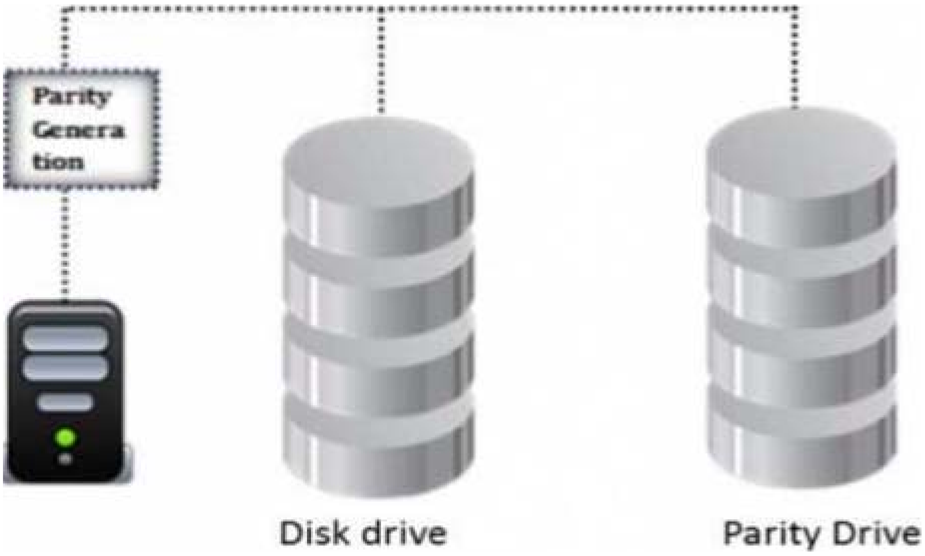
C. Unstructured Threats

D. Internal Threats

Answer: C

18.CORRECT TEXT

Identify the minimum number of drives required to setup RAID level 5.



A. Multiple

B. 3

C. 4

D. 2

Answer: B

19.Daniel is monitoring network traffic with the help of a network monitoring tool to detect any abnormalities.

What type of network security approach is Daniel adopting?

A. Preventative

B. Reactive

C. Retrospective

D. Defense-in-depth

Answer: B

20.James was inspecting ARP packets in his organization's network traffic with the help of Wireshark. He is checking the volume of traffic containing ARP requests as well as the source IP address from which they are originating.

Which type of attack is James analyzing?

A. ARP Sweep

B. ARP misconfiguration

C. ARP spoofinq

D. ARP Poisioning

Answer: A

21.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

22.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: B,C,D

23.Daniel is giving training on designing and implementing a security policy in the organization. He is explaining the hierarchy of the security policy which demonstrates how policies are drafted, designed and implemented.

What is the correct hierarchy for a security policy implementation?

A. Laws, Policies, Regulations, Procedures and Standards

B. Regulations, Policies, Laws, Standards and Procedures

C. Laws, Regulations, Policies, Standards and Procedures

D. Procedures, Policies, Laws, Standards and Regulations

Answer: C

24.Management asked Adam to implement a system allowing employees to use the same credentials to access multiple applications. Adam should implement the------------------------- authentication technique to satisfy the management request.

A. Two-factor Authentication

B. Smart Card Authentication

C. Single-sign-on

D. Biometric

Answer: C

25.------------is a group of broadband wireless communications standards for Metropolitan Area Networks (MANs)

A. 802.15

B. 802.16

C. 802.15.4

D. 802.12

Answer: B

26.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

27.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

28.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

29.The bank where you work has 600 windows computers and 400 Red Hat computers which primarily serve as bank teller consoles. You have created a plan and deployed all the patches to the Windows computers and you are now working on updating the Red Hat computers.
What command should you run on the network to update the Red Hat computers, download the security package, force the package installation, and update all currently installed packages?
A. You should run the up2date -d -f -u command
B. You should run the up2data -u command
C. You should run the WSUS -d -f -u command.
D. You should type the sysupdate -d command
Answer: A

30.Which IEEE standard does wireless network use?
A. 802.11
B. 802.18
C. 802.9
D. 802.10
Answer: A

31.Smith is an IT technician that has been appointed to his company's network vulnerability assessment team. He is the only IT employee on the team. The other team members include employees from Accounting, Management, Shipping, and Marketing. Smith and the team members are having their first meeting to discuss how they will proceed.
What is the first step they should do to create the network vulnerability assessment plan?
A. Their first step is to analyze the data they have currently gathered from the company or interviews.
B. Their first step is to make a hypothesis of what their final findings will be.
C. Their first step is to create an initial Executive report to show the management team.
D. Their first step is the acquisition of required documents, reviewing of security policies and compliance.
Answer: D

32.Assume that you are a network administrator and the company has asked you to draft an Acceptable Use Policy (AUP) for employees.
Under which category of an information security policy does AUP fall into?
A. System Specific Security Policy (SSSP)
B. Incident Response Policy (IRP)

C. Enterprise Information Security Policy (EISP)

D. Issue Specific Security Policy (ISSP)

Answer: A

33.Management wants to calculate the risk factor for their organization. Kevin, a network administrator in the organization knows how to calculate the risk factor. Certain parameters are required before calculating risk factor.

What are they? (Select all that apply) Risk factor =............X..............X..........

A. Vulnerability

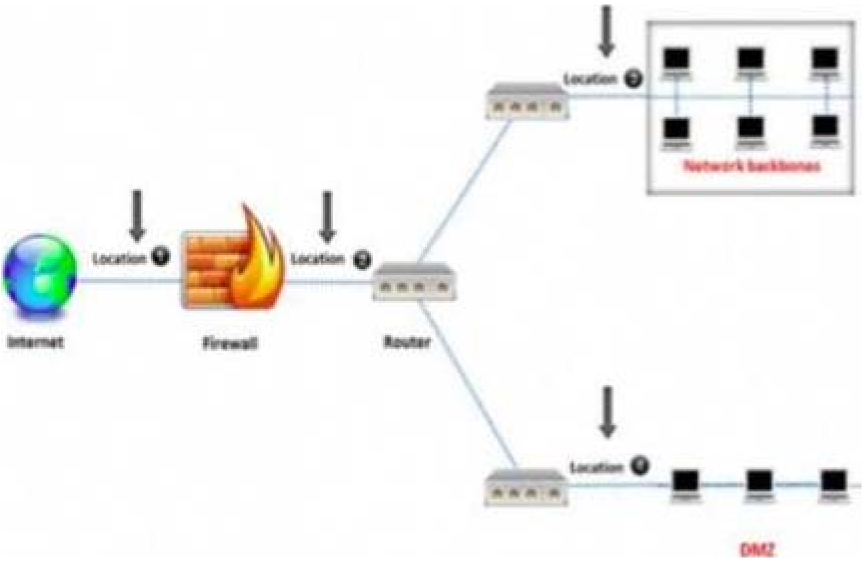
B. Impact

C. Attack

D. Threat

Answer: A,B,D

34.An administrator wants to monitor and inspect large amounts of traffic and detect unauthorized attempts from inside the organization, with the help of an IDS.



They are not able to recognize the exact location to deploy the IDS sensor. Can you help him spot the location where the IDS sensor should be placed?

A. Location 2

B. Location 3

C. Location 4

D. Location 1

Answer: A

35.Liza was told by her network administrator that they will be implementing IPsec VPN tunnels to connect the branch locations to the main office.

What layer of the OSI model do IPsec tunnels function on?

A. The data link layer

B. The session layer

C. The network layer

D. The application and physical layers
Answer: C

36.You are responsible for network functions and logical security throughout the corporation.
Your company has over 250 servers running Windows Server 2012, 5000 workstations running Windows 10, and 200 mobile users working from laptops on Windows 8. Last week 10 of your company's laptops were stolen from a salesman, while at a conference in Barcelona. These laptops contained proprietary company information. While doing a damage assessment, a news story leaks about a blog post containing information about the stolen laptops and the sensitive information.
What built-in Windows feature could you have implemented to protect the sensitive information on these laptops?
A. You should have used 3DES.
B. You should have implemented the Distributed File System (DFS).
C. If you would have implemented Pretty Good Privacy (PGP).
D. You could have implemented the Encrypted File System (EFS)
Answer: D

37.The network admin decides to assign a class B IP address to a host in the network. Identify which of the following addresses fall within a class B IP address range.
A. 255.255.255.0
B. 18.12.4.1
C. 172.168.12.4
D. 169.254.254.254
Answer: C

38.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

39.Consider a scenario consisting of a tree network. The root Node N is connected to two man nodes N1 and N2. N1 is connected to N11 and N12. N2 is connected to N21 and N22.
What will happen if any one of the main nodes fail?
A. Failure of the main node affects all other child nodes at the same level irrespective of the main node.
B. Does not cause any disturbance to the child nodes or its tranmission
C. Failure of the main node will affect all related child nodes connected to the main node
D. Affects the root node only

Answer: C

40.As a network administrator, you have implemented WPA2 encryption in your corporate wireless network. The WPA2's _________integrity check mechanism provides security against a replay attack
A. CRC-32
B. CRC-MAC
C. CBC-MAC
D. CBC-32
Answer: C

41.An organization needs to adhere to the______________rules for safeguarding and protecting the electronically stored health information of employees.
A. HI PA A
B. PCI DSS
C. ISEC
D. SOX
Answer: A

42.The risk assessment team in Southern California has estimated that the probability of an incident that has potential to impact almost 80% of the bank's business is very high.
How should this risk be categorized in the risk matrix?
A. High
B. Medium
C. Extreme
D. Low
Answer: C

43.Geon Solutions INC., had only 10 employees when it started. But as business grew, the organization had to increase the amount of staff. The network administrator is finding it difficult to accommodate an increasing number of employees in the existing network topology. So the organization is planning to implement a new topology where it will be easy to accommodate an increasing number of employees. Which network topology will help the administrator solve the problem of needing to add new employees and expand?
A. Bus
B. Star
C. Ring
D. Mesh
Answer: B

44.As a network administrator, you have implemented WPA2 encryption in your corporate wireless network. The WPA2's_________integrity check mechanism provides security against a replay attack
A. CBC-32
B. CRC-MAC
C. CRC-32

D. CBC-MAC

Answer: D

45.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

46.Assume that you are working as a network administrator in the head office of a bank. One day a bank employee informed you that she is unable to log in to her system. At the same time, you get a call from another network administrator informing you that there is a problem connecting to the main server.

How will you prioritize these two incidents?

A. Based on approval from management

B. Based on a first come first served basis

C. Based on a potential technical effect of the incident

D. Based on the type of response needed for the incident

Answer: C

47.Steven's company has recently grown from 5 employees to over 50. Every workstation has a public IP address and navigated to the Internet with little to no protection. Steven wants to use a firewall. He also wants IP addresses to be private addresses, to prevent public Internet devices direct access to them.

What should Steven implement on the firewall to ensure this happens?

A. Steven should use a Demilitarized Zone (DMZ)

B. Steven should use Open Shortest Path First (OSPF)

C. Steven should use IPsec

D. Steven should enabled Network Address Translation(NAT)

Answer: D

48.James is a network administrator working at a student loan company in Minnesota. This company processes over 20,000 student loans a year from colleges all over the state. Most communication between the company schools, and lenders is carried out through emails. Much of the email communication used at his company contains sensitive information such as social security numbers. For this reason, James wants to utilize email encryption. Since a server-based PKI is not an option for him, he is looking for a low/no cost solution to encrypt emails.

What should James use?

A. James could use PGP as a free option for encrypting the company's emails.

B. James should utilize the free OTP software package.

C. James can use MD5 algorithm to encrypt all the emails

D. James can enforce mandatory HTTPS in the email clients to encrypt emails

Answer: A

49.The network administrator wants to strengthen physical security in the organization. Specifically, to implement a solution stopping people from entering certain restricted zones without proper credentials. Which of following physical security measures should the administrator use?
A. Bollards
B. Fence
C. Video surveillance
D. Mantrap
Answer: B

50.Which of the following network monitoring techniques requires extra monitoring software or hardware?
A. Non-router based
B. Switch based
C. Hub based
D. Router based
Answer: A

51.John wants to implement a packet filtering firewall in his organization's network.
What TCP/IP layer does a packet filtering firewall work on?
A. Application layer
B. Network Interface layer
C. TCP layer
D. IP layer
Answer: D

52.What is the name of the authority that verifies the certificate authority in digital certificates?
A. Directory management system
B. Certificate authority
C. Registration authority
D. Certificate Management system
Answer: D

53.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: A,D

54.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

55.Sean has built a site-to-site VPN architecture between the head office and the branch office of his company. When users in the branch office and head office try to communicate with each other, the traffic is encapsulated. As the traffic passes though the gateway, it is encapsulated again. The header and payload both are encapsulated. This second encapsulation occurs only in the __________implementation of a VPN.
A. Full Mesh Mode
B. Point-to-Point Mode
C. Transport Mode
D. Tunnel Mode
Answer: D

56.What command is used to terminate certain processes in an Ubuntu system?
A. #grep Kill [Target Process}
B. #kill-9[PID]
C. #ps ax Kill
D. # netstat Kill [Target Process]
Answer: C

57.You are an IT security consultant working on a contract for a large manufacturing company to audit their entire network. After performing all the tests and building your report, you present a number of recommendations to the company and what they should implement to become more secure. One recommendation is to install a network-based device that notifies IT employees whenever malicious or questionable traffic is found. From your talks with the company, you know that they do not want a device that actually drops traffic completely, they only want notification.
What type of device are you suggesting?
A. The best solution to cover the needs of this company would be a HIDS device.
B. A NIDS device would work best for the company
C. You are suggesting a NIPS device
D. A HIPS device would best suite this company
Answer: B

58.An enterprise recently moved to a new office and the new neighborhood is a little risky. The CEO wants to monitor the physical perimeter and the entrance doors 24 hours.
What is the best option to do this job?

A. Install a CCTV with cameras pointing to the entrance doors and the street
B. Use fences in the entrance doors
C. Use lights in all the entrance doors and along the company's perimeter
D. Use an IDS in the entrance doors and install some of them near the corners
Answer: A

59.Dan and Alex are business partners working together. Their Business-Partner Policy states that they should encrypt their emails before sending to each other.
How will they ensure the authenticity of their emails?
A. Dan will use his public key to encrypt his mails while Alex will use Dan's digital signature to verify the authenticity of the mails.
B. Dan will use his private key to encrypt his mails while Alex will use his digital signature to verify the authenticity of the mails.
C. Dan will use his digital signature to sign his mails while Alex will use his private key to verify the authenticity of the mails.
D. Dan will use his digital signature to sign his mails while Alex will use Dan's public key to verify the authencity of the mails.
Answer: D

60.Which of the following VPN topologies establishes a persistent connection between an organization's main office and its branch offices using a third-party network or the Internet?
A. Star
B. Point-to-Point
C. Full Mesh
D. Hub-and-Spoke
Answer: D

61.Blake is working on the company's updated disaster and business continuity plan. The last section of the plan covers computer and data incidence response.
Blake is outlining the level of severity for each type of incident in the plan. Unsuccessful scans and probes are at what severity level?
A. High severity level
B. Extreme severity level
C. Mid severity level
D. Low severity level
Answer: D

62.A local bank wants to protect their card holder data. The bank should comply with the________standard to ensure the security of card holder data.
A. HIPAA
B. ISEC
C. PCI DSS
D. SOAX
Answer: C

63.Management asked their network administrator to suggest an appropriate backup medium for their backup plan that best suits their organization's need.
Which of the following factors will the administrator consider when deciding on the appropriate backup medium?
A. Capability
B. Accountability
C. Extensibility
D. Reliability
Answer: A,C,D

64.Which OSI layer does a Network Interface Card (NIC) work on?
A. Physical layer
B. Presentation layer
C. Network layer
D. Session layer
Answer: A

65.The IR team and the network administrator have successfully handled a malware incident on the network. The team is now preparing countermeasure guideline to avoid a future occurrence of the malware incident.
Which of the following countermeasure(s) should be added to deal with future malware incidents? (Select all that apply)
A. Complying with the company's security policies
B. Implementing strong authentication schemes
C. Implementing a strong password policy
D. Install antivirus software
Answer: D

66.Frank installed Wireshark at all ingress points in the network. Looking at the logs he notices an odd packet source. The odd source has an address of 1080:0:FF:0:8:800:200C:4171 and is using port 21. What does this
source address signify?
A. This address means that the source is using an IPv6 address and is spoofed and signifies an IPv4 address of 127.0.0.1.
B. This source address is IPv6 and translates as 13.1.68.3
C. This source address signifies that the originator is using 802dot1x to try and penetrate into Frank's network
D. This means that the source is using IPv4
Answer: D

67.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: A,C,D

68.Which VPN QoS model guarantees the traffic from one customer edge (CE) to another?
A. Pipe Model
B. AAA model
C. Hub-and-Spoke VPN model
D. Hose mode
Answer: A

69.Harry has sued the company claiming they made his personal information public on a social networking site in the United States. The company denies the allegations and consulted a/an ______for legal advice to defend them against this allegation.
A. PR Specialist
B. Attorney
C. Incident Handler
D. Evidence Manager
Answer: B

70.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

71.Which of the following Event Correlation Approach checks and compares all the fields systematically and intentionally for positive and negative correlation with each other to determine the correlation across one or multiple fields?
A. Automated Field Correlation
B. Field-Based Approach
C. Rule-Based Approach
D. Graph-Based Approach
Answer: A

72.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

73.Identify the correct statements regarding a DMZ zone:
A. It is a file integrity monitoring mechanism
B. It is a Neutral zone between a trusted network and an untrusted network
C. It serves as a proxy
D. It includes sensitive internal servers such as database servers
Answer: B

74.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

75.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

76.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

77.A network administrator is monitoring the network traffic with Wireshark.
Which of the following filters will she use to view the packets moving without setting a flag to detect TCP Null Scan attempts?
A. TCRflags==0x000
B. Tcp.flags==0X029
C. Tcp.dstport==7

D. Tcp.flags==0x003
Answer: A

78.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

79.Rick has implemented several firewalls and IDS systems across his enterprise network.
What should he do to effectively correlate all incidents that pass through these security controls?
A. Use firewalls in Network Address Transition (NAT) mode
B. Implement IPsec
C. Implement Simple Network Management Protocol (SNMP)
D. Use Network Time Protocol (NTP)
Answer: D

80.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

81.You are monitoring your network traffic with the Wireshark utility and noticed that your network is experiencing a large amount of traffic from a certain region. You suspect a DoS incident on the network.
What will be your first reaction as a first responder?
A. Avoid Fear, Uncertainty and Doubt
B. Communicate the incident
C. Make an initial assessment

D. Disable Virus Protection

Answer: A

82.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

83.Brendan wants to implement a hardware based RAID system in his network. He is thinking of choosing a suitable RAM type for the architectural setup in the system. The type he is interested in provides access times of up to 20 ns.

Which type of RAM will he select for his RAID system?

A. NVRAM

B. SDRAM

C. NAND flash memory

D. SRAM

Answer: D

84.Simon had all his systems administrators implement hardware and software firewalls to ensure network security. They implemented IDS/IPS systems throughout the network to check for and stop any unauthorized traffic that may attempt to enter. Although Simon and his administrators believed they were secure, a hacker group was able to get into the network and modify files hosted on the company's website. After searching through the firewall and server logs, no one could find how the attackers were able to get in. He decides that the entire network needs to be monitored for critical and essential file changes. This monitoring tool alerts administrators when a critical file is altered.

What tool could Simon and his administrators implement to accomplish this?

A. Snort is the best tool for their situation

B. They can implement Wireshark

C. They could use Tripwire

D. They need to use Nessus

Answer: C

85.David is working in a mid-sized IT company. Management asks him to suggest a framework that can be used effectively to align the IT goals to the business goals of the company. David suggests the______framework, as it provides a set of controls over IT and consolidates them to form a framework.

A. RMIS

B. ITIL

C. ISO 27007

D. COBIT

Answer: D

86.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

87.Which of the following acts as a verifier for the certificate authority?
A. Certificate Management system
B. Certificate authority
C. Directory management system
D. Registration authority
Answer: D

88.Jason has set a firewall policy that allows only a specific list of network services and deny everything else. This strategy is known as a____________.
A. Default allow
B. Default deny
C. Default restrict
D. Default access
Answer: B

89.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

90.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

91.Sam wants to implement a network-based IDS in the network. Sam finds out the one IDS solution which works is based on patterns matching.
Which type of network-based IDS is Sam implementing?
A. Behavior-based IDS
B. Anomaly-based IDS
C. Stateful protocol analysis
D. Signature-based IDS
Answer: D

92.According to the company's security policy, all access to any network resources must use Windows Active Directory Authentication. A Linux server was recently installed to run virtual servers and it is not using Windows Authentication.
What needs to happen to force this server to use Windows Authentication?
A. Edit the ADLIN file.
B. Edit the shadow file.
C. Remove the /var/bin/localauth.conf file.
D. Edit the PAM file to enforce Windows Authentication
Answer: D

93.Which of the information below can be gained through network sniffing? (Select all that apply)
A. Telnet Passwords
B. Syslog traffic
C. DNS traffic
D. Programming errors
Answer: A,B,C

94.Nancy is working as a network administrator for a small company. Management wants to implement a RAID storage for their organization. They want to use the appropriate RAID level for their backup plan that will satisfy the following requirements: 1. It has a parity check to store all the information about the data in multiple drives 2. Help reconstruct the data during downtime. 3. Process the data at a good speed. 4. Should not be expensive. The management team asks Nancy to research and suggest the appropriate RAID level that best suits their requirements.
What RAID level will she suggest?
A. RAID 0
B. RAID 10
C. RAID 3
D. RAID 1
Answer: C

95.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

96.Malone is finishing up his incident handling plan for IT before giving it to his boss for review. He is outlining the incident response methodology and the steps that are involved.
What is the last step he should list?
A. Containment
B. Assign eradication
C. A follow-up
D. Recovery
Answer: C

97.Will is working as a Network Administrator. Management wants to maintain a backup of all the company data as soon as it starts operations. They decided to use a RAID backup storage technology for their data backup plan. To implement the RAID data backup storage, Will sets up a pair of RAID disks so that all the data written to one disk is copied automatically to the other disk as well. This maintains an additional copy of the data.
Which RAID level is used here?
A. RAID 3
B. RAID 1
C. RAID 5
D. RAID 0
Answer: B

98.Which phase of vulnerability management deals with the actions taken for correcting the discovered vulnerability?
A. Mitigation
B. Assessment
C. Remediation
D. Verification
Answer: C

99.Malone is finishing up his incident handling plan for IT before giving it to his boss for review. He is outlining the incident response methodology and the steps that are involved.
What is the last step he should list?
A. Assign eradication.
B. Recovery
C. Containment
D. A follow-up.
Answer: D

100.Chris is a senior network administrator. Chris wants to measure the Key Risk Indicator (KRI) to assess the organization.

Why is Chris calculating the KRI for his organization? It helps Chris to:

A. Identifies adverse events

B. Facilitates backward

C. Facilitates post Incident management

D. Notifies when risk has reached threshold levels

Answer: A,D

101.John is a network administrator and is monitoring his network traffic with the help of Wireshark. He suspects that someone from outside is making a TCP OS fingerprinting attempt on his organization's network.

Which of the following Wireshark filter(s) will he use to locate the TCP OS fingerprinting attempt?

A. Tcp.flags==0x2b

B. Tcp.flags=0x00

C. Tcp.options.mss_val<1460

D. Tcp.options.wscale_val==20

Answer: A,B,C

102.The--------------protocol works in the network layer and is responsible for handling the error codes during the delivery of packets. This protocol is also responsible for providing communication in the TCP/IP stack.

A. RARP

B. ICMP

C. DHCP

D. ARP

Answer: B

103.Stephanie is currently setting up email security so all company data is secured when passed through email. Stephanie first sets up encryption to make sure that a specific user's email is protected. Next, she needs to ensure that the incoming and the outgoing mail has not been modified or altered using digital signatures.

What is Stephanie working on?

A. Usability

B. Data Integrity

C. Availability

D. Confidentiality

Answer: B

104.-----------is a group of broadband wireless communications standards for Metropolitan Area Networks (MANs)

A. 802.15.4

B. 802.15

C. 802.12

D. 802.16

Answer: D

105.John has implemented________in the network to restrict the limit of public IP addresses in his organization and to enhance the firewall filtering technique.

A. DMZ

B. Proxies

C. VPN

D. NAT

Answer: D

106.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

107.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

108.Eric is receiving complaints from employees that their systems are very slow and experiencing odd issues including restarting automatically and frequent system hangs. Upon investigating, he is convinced the systems are infected with a virus that forces systems to shut down automatically after period of time. What type of security incident are the employees a victim of?

A. Scans and probes

B. Malicious Code

C. Denial of service

D. Distributed denial of service

Answer: B

109.Stephanie is currently setting up email security so all company data is secured when passed through email. Stephanie first sets up encryption to make sure that a specific user's email is protected. Next, she needs to ensure that the incoming and the outgoing mail has not been modified or altered using digital signatures.

What is Stephanie working on?
A. Confidentiality
B. Availability
C. Data Integrity
D. Usability
Answer: C

110.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

111.John wants to implement a firewall service that works at the session layer of the OSI model. The firewall must also have the ability to hide the private network information.
Which type of firewall service is John thinking of
implementing?
A. Application level gateway
B. Circuit level gateway
C. Stateful Multilayer Inspection
D. Packet Filtering
Answer: B

112.Bryson is the IT manager and sole IT employee working for a federal agency in California. The agency was just given a grant and was able to hire on 30 more employees for a new extended project. Because of this, Bryson has hired on two more IT employees to train up and work. Both of his new hires are straight out of college and do not have any practical IT experience. Bryson has spent the last two weeks teaching the new employees the basics of computers, networking, troubleshooting techniques etc. To see how these two new hires are doing, he asks them at what layer of the OSI model do Network Interface Cards (NIC) work on.
What should the new employees answer?
A. NICs work on the Session layer of the OSI model.
B. The new employees should say that NICs perform on the Network layer.
C. They should tell Bryson that NICs perform on the Physical layer
D. They should answer with the Presentation layer.
Answer: C

113.Malone is finishing up his incident handling plan for IT before giving it to his boss for review. He is outlining the incident response methodology and the steps that are involved.
Which step should Malone list as the last step in the incident response methodology?
A. Malone should list a follow-up as the last step in the methodology

B. Recovery would be the correct choice for the last step in the incident response methodology
C. He should assign eradication to the last step.
D. Containment should be listed on Malone's plan for incident response.
Answer: B

114.John has successfully remediated the vulnerability of an internal application that could have caused a threat to the network. He is scanning the application for the existence of a remediated vulnerability, this process is called a________and it has to adhere to the_________
A. Verification, Security Policies
B. Mitigation, Security policies
C. Vulnerability scanning, Risk Analysis
D. Risk analysis, Risk matrix
Answer: A

115.Lyle is the IT director for a medium-sized food service supply company in Nebraska. Lyle's company employs over 300 workers, half of which use computers. He recently came back from a security training seminar on logical security. He now wants to ensure his company is as secure as possible. Lyle has many network nodes and workstation nodes across the network. He does not have much time for implementing a network-wide solution. He is primarily concerned about preventing any external attacks on the network by using a solution that can drop packets if they are found to be malicious. Lyle also wants this solution to be easy to implement and be network-wide.
What type of solution would be best for Lyle?
A. A NEPT implementation would be the best choice.
B. To better serve the security needs of his company, Lyle should use a HIDS system.
C. Lyle would be best suited if he chose a NIPS implementation
D. He should choose a HIPS solution, as this is best suited to his needs.
Answer: C

116.Kelly is taking backups of the organization's data. Currently, he is taking backups of only those files which are created or modified after the last backup.
What type of backup is Kelly using?
A. Full backup
B. Incremental backup
C. Differential Backup
D. Normal Backup
Answer: B

117.A company has the right to monitor the activities of their employees on different information systems according to the _______policy.
A. Information system
B. User access control
C. Internet usage
D. Confidential data
Answer: B

118.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

119.A network is setup using an IP address range of 0.0.0.0 to 127.255.255.255. The network has a default subnet mask of 255.0.0.0.
What IP address class is the network range a part of?
A. Class C
B. Class A
C. Class B
D. Class D
Answer: B

120.Sam, a network administrator is using Wireshark to monitor the network traffic of the organization. He wants to detect TCP packets with no flag set to check for a specific attack attempt.
Which filter will he use to view the traffic?
A. Tcp.flags==0x000
B. Tcp.flags==0000x
C. Tcp.flags==000x0
D. Tcp.flags==x0000
Answer: A