- **Vendor:** EC-Council
- **Exam Code:** 312-38
- **Exam Name:** EC-Council Certified Network Defender Certification Exam
- **New Updated Questions from Braindump2go (Updated in October/2021)**

QUESTION 437
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

QUESTION 438
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

QUESTION 439
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: ABD

QUESTION 440
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

QUESTION 441
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

QUESTION 442
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

QUESTION 443
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

QUESTION 444
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

QUESTION 445
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

QUESTION 446
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

QUESTION 447
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

QUESTION 448
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

QUESTION 449
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

QUESTION 450
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

QUESTION 451
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

QUESTION 452
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

QUESTION 453
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

QUESTION 454
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

QUESTION 455
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

QUESTION 456
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

QUESTION 457
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

QUESTION 458
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

QUESTION 459
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

QUESTION 460
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: ABC

QUESTION 461
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

QUESTION 462
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

QUESTION 463
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

QUESTION 464
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

QUESTION 465
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

QUESTION 466
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

QUESTION 467
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