

EC-Council

Exam Questions 312-38

EC-Council Network Security Administrator (ENSA)



NEW QUESTION 1

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

NEW QUESTION 2

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

NEW QUESTION 3

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

NEW QUESTION 4

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

NEW QUESTION 5

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

NEW QUESTION 6

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

NEW QUESTION 7

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

NEW QUESTION 8

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

NEW QUESTION 9

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

NEW QUESTION 10

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. Faster restoration
- C. Slower than a full backup
- D. Faster than a full backup
- E. Less expensive than full backup

Answer: AD

NEW QUESTION 10

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

NEW QUESTION 15

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. `icmp.type==0 and icmp.type==16`
- B. `icmp.type==8 or icmp.type==16`
- C. `icmp.type==8 and icmp.type==0`
- D. `icmp.type==8 or icmp.type==0`

Answer: D

NEW QUESTION 18

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

NEW QUESTION 20

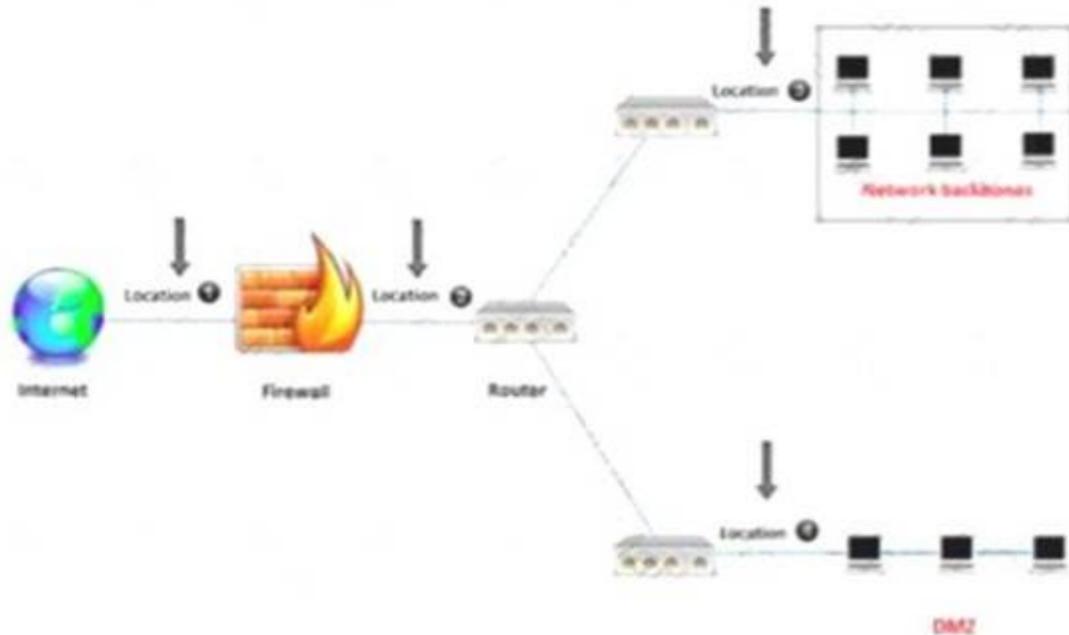
An US-based organization decided to implement a RAID storage technology for their data backup plan. John wants to setup a RAID level that require a minimum of six drives but will meet high fault tolerance and with a high speed for the data read and write operations. What RAID level is John considering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

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

Answer: D

NEW QUESTION 23

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

NEW QUESTION 25

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

NEW QUESTION 30

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

NEW QUESTION 31

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

NEW QUESTION 35

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

NEW QUESTION 38

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

NEW QUESTION 39

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

NEW QUESTION 41

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

NEW QUESTION 42

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

NEW QUESTION 44

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

NEW QUESTION 48

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

NEW QUESTION 53

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

NEW QUESTION 56

Consider a scenario consisting of a tree network. The root Node N is connected to two main 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 transmission
- 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

NEW QUESTION 57

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 authenticity of the mails.

Answer: D

NEW QUESTION 62

A VPN Concentrator acts as a bidirectional tunnel endpoint among host machines. What are the other function(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

NEW QUESTION 63

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

NEW QUESTION 64

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

NEW QUESTION 68

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

NEW QUESTION 71

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

NEW QUESTION 75

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

NEW QUESTION 79

Which IEEE standard does wireless network use?

- A. 802.11
- B. 802.18
- C. 802.9
- D. 802.10

Answer: A

NEW QUESTION 84

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

NEW QUESTION 88

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

NEW QUESTION 90

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: ACD

NEW QUESTION 92

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

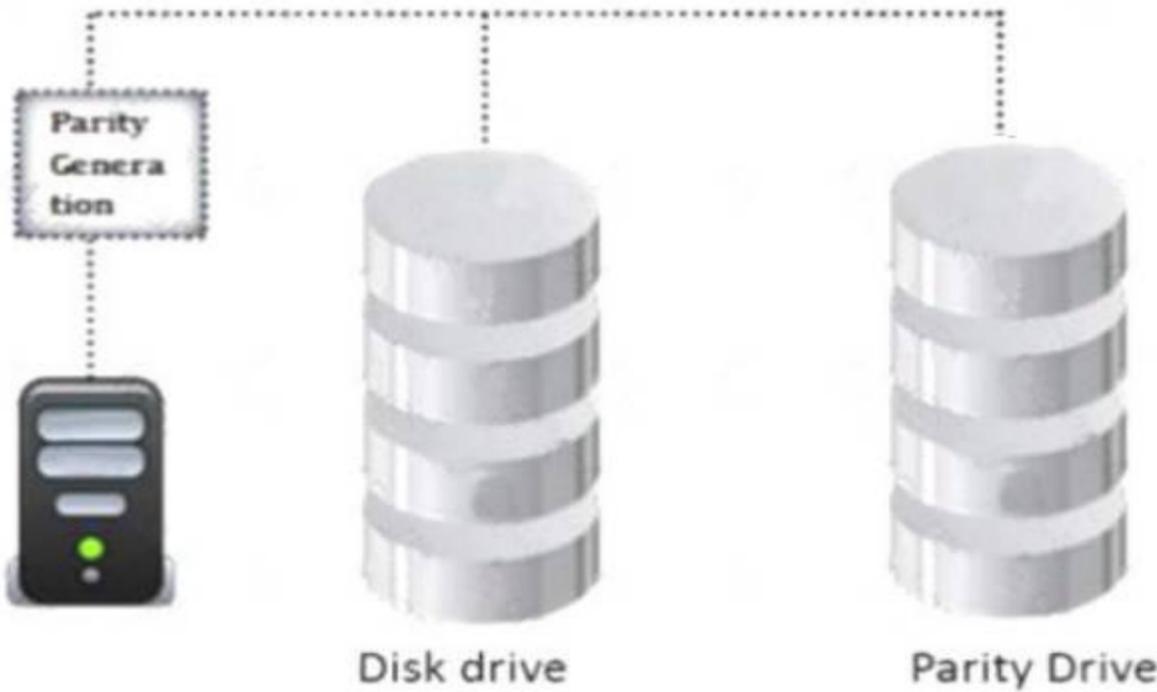
- A. Firewall policy
- B. Firewall log

- C. Firewall settings
- D. Firewall rule set

Answer: B

NEW QUESTION 94

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



- A. Multiple
- B. 3
- C. 4
- D. 2

Answer: B

NEW QUESTION 99

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

NEW QUESTION 104

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 Identificatio
- E. Risk Assessmen
- F. Risk Monitoring & Review, Risk Treatment

Answer: A

NEW QUESTION 107

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

NEW QUESTION 110

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

NEW QUESTION 111

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

NEW QUESTION 115

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

NEW QUESTION 117

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

NEW QUESTION 120

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

NEW QUESTION 122

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

NEW QUESTION 126

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

NEW QUESTION 127

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

NEW QUESTION 128

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

NEW QUESTION 130

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

NEW QUESTION 132

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

312-38 Practice Exam Features:

- * 312-38 Questions and Answers Updated Frequently
- * 312-38 Practice Questions Verified by Expert Senior Certified Staff
- * 312-38 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * 312-38 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 312-38 Practice Test Here](#)