



Paloalto-Networks

Exam Questions PCCET

Palo Alto Networks Certified Cybersecurity Entry-level Technician

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

Which model would a customer choose if they want full control over the operating system(s) running on their cloud computing platform?

- A. SaaS
- B. DaaS
- C. PaaS
- D. IaaS

Answer: D

NEW QUESTION 2

Match the Identity and Access Management (IAM) security control with the appropriate definition.

IAM security		Ensuring least-privileged access to cloud resources and infrastructure
Machine Identity		Discovering threats by identifying activity that deviates from a normal baseline
User Entity Behavior Analytics		Securing and managing the relationships between users and cloud resources
Access Management		Decoupling workload identity from IP addresses

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

IAM security	IAM security	Ensuring least-privileged access to cloud resources and infrastructure
Machine Identity	User Entity Behavior Analytics	Discovering threats by identifying activity that deviates from a normal baseline
User Entity Behavior Analytics	Access Management	Securing and managing the relationships between users and cloud resources
Access Management	Machine Identity	Decoupling workload identity from IP addresses

NEW QUESTION 3

Which of the following is a service that allows you to control permissions assigned to users in order for them to access and utilize cloud resources?

- A. User-ID
- B. Lightweight Directory Access Protocol (LDAP)
- C. User and Entity Behavior Analytics (UEBA)
- D. Identity and Access Management (IAM)

Answer: D

Explanation:

Identity and access management (IAM) is a software service or framework that allows organizations to define user or group identities within software environments, then associate permissions with them. The identities and permissions are usually spelled out in a text file, which is referred to as an IAM policy.

NEW QUESTION 4

The customer is responsible only for which type of security when using a SaaS application?

- A. physical

- B. platform
- C. data
- D. infrastructure

Answer: C

NEW QUESTION 5

What is the key to “taking down” a botnet?

- A. prevent bots from communicating with the C2
- B. install openvas software on endpoints
- C. use LDAP as a directory service
- D. block Docker engine software on endpoints

Answer: A

NEW QUESTION 6

Under which category does an application that is approved by the IT department, such as Office 365, fall?

- A. unsanctioned
- B. prohibited
- C. tolerated
- D. sanctioned

Answer: D

NEW QUESTION 7

Which product from Palo Alto Networks enables organizations to prevent successful cyberattacks as well as simplify and strengthen security processes?

- A. Expedition
- B. AutoFocus
- C. MineMeld
- D. Cortex XDR

Answer: D

Explanation:

From a business perspective, XDR platforms enable organizations to prevent successful cyberattacks as well as simplify and strengthen security processes.

NEW QUESTION 8

Which endpoint product from Palo Alto Networks can help with SOC visibility?

- A. STIX
- B. Cortex XDR
- C. WildFire
- D. AutoFocus

Answer: B

Explanation:

XDR solutions bring a proactive approach to threat detection and response. It delivers visibility across all data, including endpoint, network, and cloud data, while applying analytics and automation to address today’s increasingly sophisticated threats. With XDR, cybersecurity teams can:

Identify hidden, stealthy, and sophisticated threats proactively and quickly Track threats across any source or location within the organization Increase the productivity of the people operating the technology

Get more out of their security investments Conclude investigations more efficiently

NEW QUESTION 9

Which Palo Alto Networks product provides playbooks with 300+ multivendor integrations that help solve any security use case?

- A. Cortex XSOAR
- B. Prisma Cloud
- C. AutoFocus
- D. Cortex XDR

Answer: A

Explanation:

SOAR tools ingest aggregated alerts from detection sources (such as SIEMs, network security tools, and mailboxes) before executing automatable, process-driven playbooks to enrich and respond to these alerts.

<https://www.paloaltonetworks.com/cortex/security-operations-automation>

NEW QUESTION 10

What is used to orchestrate, coordinate, and control clusters of containers?

- A. Kubernetes

- B. Prisma Saas
- C. Docker
- D. CN-Series

Answer: A

Explanation:

As containers grew in popularity and used diversified orchestrators such as Kubernetes (and its derivatives, such as OpenShift), Mesos, and Docker Swarm, it became increasingly important to deploy and operate containers at scale.
<https://www.dynatrace.com/news/blog/kubernetes-vs-docker/>

NEW QUESTION 10

Which three services are part of Prisma SaaS? (Choose three.)

- A. Data Loss Prevention
- B. DevOps
- C. Denial of Service
- D. Data Exposure Control
- E. Threat Prevention

Answer: ADE

NEW QUESTION 14

What is a characteristic of the National Institute Standards and Technology (NIST) defined cloud computing model?

- A. requires the use of only one cloud service provider
- B. enables on-demand network services
- C. requires the use of two or more cloud service providers
- D. defines any network service

Answer: B

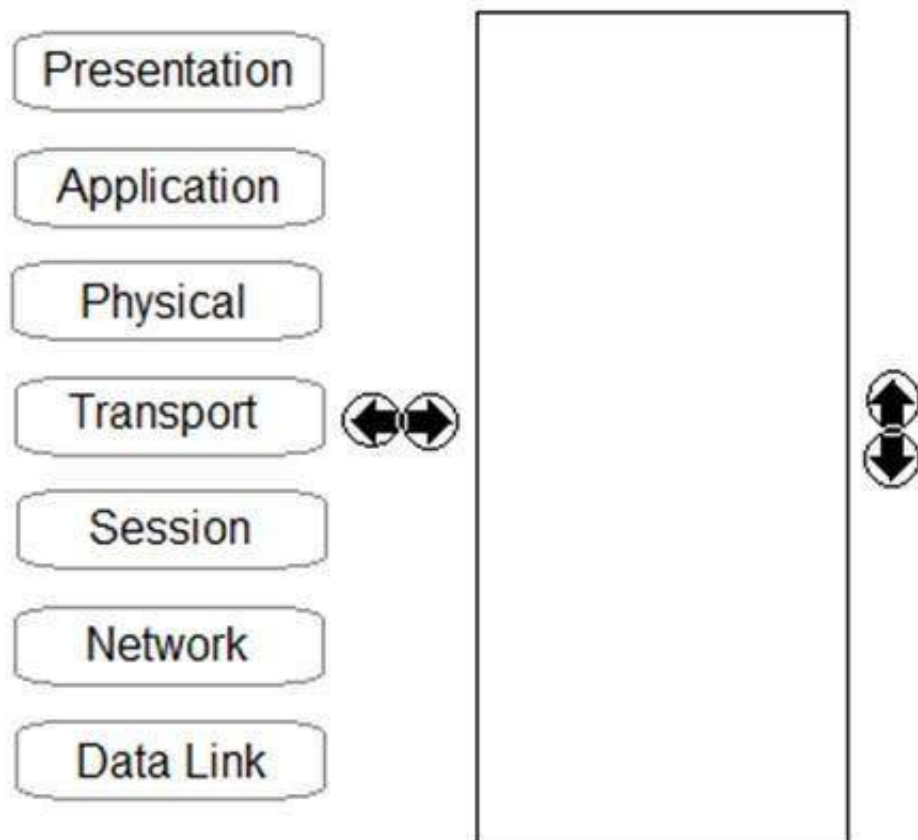
Explanation:

Cloud computing is not a location but rather a pool of resources that can be rapidly provisioned in an automated, on-demand manner.

NEW QUESTION 17

Order the OSI model with Layer7 at the top and Layer1 at the bottom.

Unordered Options Ordered Options

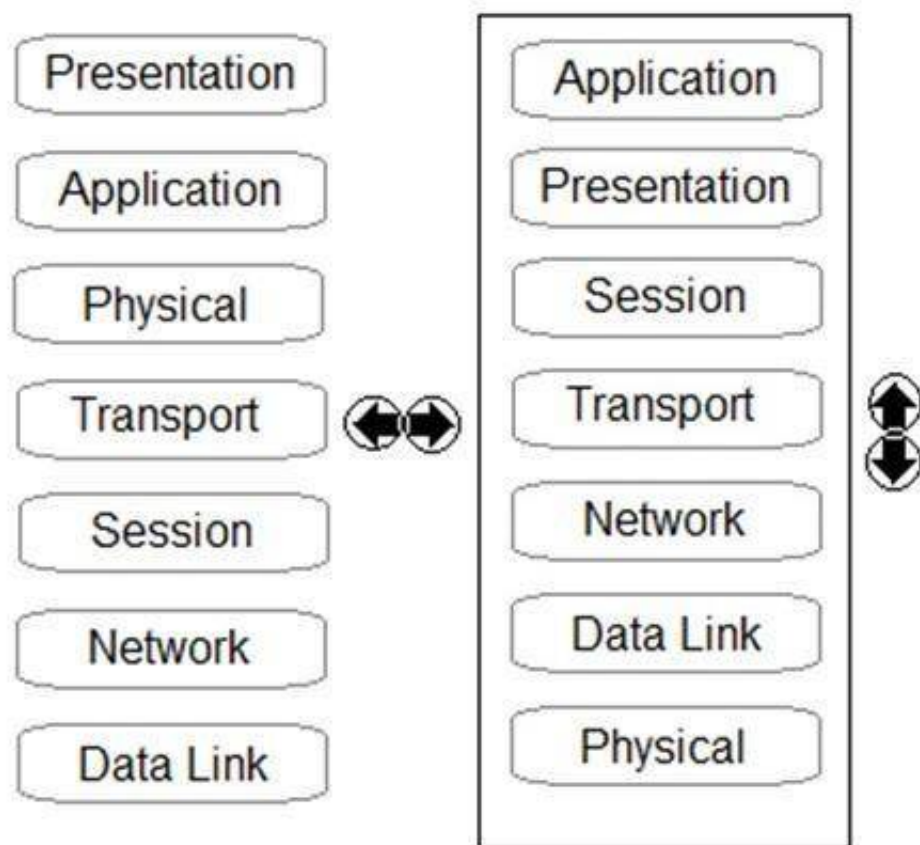


- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Unordered Options Ordered Options



NEW QUESTION 19

Which network device breaks networks into separate broadcast domains?

- A. Hub
- B. Layer 2 switch
- C. Router
- D. Wireless access point

Answer: C

Explanation:

A layer 2 switch will break up collision domains but not broadcast domains. To break up broadcast domains you need a Layer 3 switch with vlan capabilities.

NEW QUESTION 23

During the OSI layer 3 step of the encapsulation process, what is the Protocol Data Unit (PDU) called when the IP stack adds source (sender) and destination (receiver) IP addresses?

- A. Frame
- B. Segment
- C. Packet
- D. Data

Answer: C

Explanation:

The IP stack adds source (sender) and destination (receiver) IP addresses to the TCP segment (which now is called an IP packet) and notifies the server operating system that it has an outgoing message ready to be sent across the network.

NEW QUESTION 28

Which Palo Alto subscription service identifies unknown malware, zero-day exploits, and advanced persistent threats (APTs) through static and dynamic analysis in a scalable, virtual environment?

- A. DNS Security
- B. URL Filtering
- C. WildFire
- D. Threat Prevention

Answer: C

Explanation:

"The WildFire cloud-based malware analysis environment is a cyber threat prevention service that identifies unknown malware, zero-day exploits, and advanced persistent threats (APTs) through static and dynamic analysis in a scalable, virtual environment. WildFire automatically disseminates updated protections in near-real time to immediately prevent threats from spreading; this occurs without manual intervention"

NEW QUESTION 29

Which term describes data packets that move in and out of the virtualized environment from the host network or a corresponding traditional data center?

- A. North-South traffic

- B. Intrazone traffic
- C. East-West traffic
- D. Interzone traffic

Answer: A

NEW QUESTION 30

How does adopting a serverless model impact application development?

- A. costs more to develop application code because it uses more compute resources
- B. slows down the deployment of application code, but it improves the quality of code development
- C. reduces the operational overhead necessary to deploy application code
- D. prevents developers from focusing on just the application code because you need to provision the underlying infrastructure to run the code

Answer: C

Explanation:

List three advantages of serverless computing over

CaaS: - Reduce costs - Increase agility - Reduce operational overhead

NEW QUESTION 35

In addition to integrating the network and endpoint components, what other component does Cortex integrate to speed up IoC investigations?

- A. Computer
- B. Switch
- C. Infrastructure
- D. Cloud

Answer: D

Explanation:

Cortex XDR breaks the silos of traditional detection and response by natively integrating network, endpoint, and cloud data to stop sophisticated attacks

NEW QUESTION 38

Which option describes the “selective network security virtualization” phase of incrementally transforming data centers?

- A. during the selective network security virtualization phase, all intra-host communication paths are strictly controlled
- B. during the selective network security virtualization phase, all intra-host traffic is forwarded to a Web proxy server
- C. during the selective network security virtualization phase, all intra-host traffic is encapsulated and encrypted using the IPSEC protocol
- D. during the selective network security virtualization phase, all intra-host traffic is load balanced

Answer: A

Explanation:

Selective network security virtualization: Intra-host communications and live migrations are architected at this phase. All intra-host communication paths are strictly controlled to ensure that traffic between VMs at different trust levels is intermediated either by an on-box, virtual security appliance or by an off-box, physical security appliance.

NEW QUESTION 40

Which product from Palo Alto Networks extends the Security Operating Platform with the global threat intelligence and attack context needed to accelerate analysis, forensics, and hunting workflows?

- A. Global Protect
- B. WildFire
- C. AutoFocus
- D. STIX

Answer: C

Explanation:

page 173 "AutoFocus makes over a billion samples and sessions, including billions of artifacts, immediately actionable for security analysis and response efforts. AutoFocus extends the product portfolio with the global threat intelligence and attack context needed to accelerate analysis, forensics, and hunting workflows. Together, the platform and AutoFocus move security teams away from legacy manual approaches that rely on aggregating a growing number of detectionbased alerts and post-event mitigation, to preventing sophisticated attacks and enabling proactive hunting activities."

NEW QUESTION 41

Which method is used to exploit vulnerabilities, services, and applications?

- A. encryption
- B. port scanning
- C. DNS tunneling
- D. port evasion

Answer: D

Explanation:

Attack communication traffic is usually hidden with various techniques and tools, including:

Encryption with SSL, SSH (Secure Shell), or some other custom or proprietary encryption Circumvention via proxies, remote access tools, or tunneling. In some instances, use of cellular networks enables complete circumvention of the target network for attack C2 traffic. Port evasion using network anonymizers or port hopping to traverse over any available open ports
Fast Flux (or Dynamic DNS) to proxy through multiple infected endpoints or multiple, ever-changing C2 servers to reroute traffic and make determination of the true destination or attack source difficult
DNS tunneling is used for C2 communications and data infiltration

NEW QUESTION 45

Which type of malware replicates itself to spread rapidly through a computer network?

- A. ransomware
- B. Trojan horse
- C. virus
- D. worm

Answer: D

Explanation:

A worm replicates through the network while a virus replicates, not necessarily to spread through the network.

NEW QUESTION 47

Which classification of IDS/IPS uses a database of known vulnerabilities and attack profiles to identify intrusion attempts?

- A. Statistical-based
- B. Knowledge-based
- C. Behavior-based
- D. Anomaly-based

Answer: B

Explanation:

A knowledge-based system uses a database of known vulnerabilities and attack profiles to identify intrusion attempts. These types of systems have lower false-alarm rates than behavior-based systems but must be continually updated with new attack signatures to be effective.

A behavior-based system uses a baseline of normal network activity to identify unusual patterns or levels of network activity that may be indicative of an intrusion attempt. These types of systems are more adaptive than knowledge-based systems and therefore may be more effective in detecting previously unknown vulnerabilities and attacks, but they have a much higher false-positive rate than knowledge-based systems.

NEW QUESTION 51

Which type of malware takes advantage of a vulnerability on an endpoint or server?

- A. technique
- B. patch
- C. vulnerability
- D. exploit

Answer: A

NEW QUESTION 53

Which element of the security operations process is concerned with using external functions to help achieve goals?

- A. interfaces
- B. business
- C. technology
- D. people

Answer: A

Explanation:

The six pillars include:

- * 1. Business (goals and outcomes)
- * 2. People (who will perform the work)
- * 3. Interfaces (external functions to help achieve goals)
- * 4. Visibility (information needed to accomplish goals)
- * 5. Technology (capabilities needed to provide visibility and enable people)
- * 6. Processes (tactical steps required to execute on goals)

NEW QUESTION 54

Which three layers of the OSI model correspond to the Application Layer (L4) of the TCP/IP model?

- A. Session, Transport, Network
- B. Application, Presentation, and Session
- C. Physical, Data Link, Network
- D. Data Link, Session, Transport

Answer: B

Explanation:

Application (Layer 4 or L4): This layer loosely corresponds to Layers 5 through 7 of the OSI model. Transport (Layer 3 or L3): This layer corresponds to Layer 4 of the OSI model.

Internet (Layer 2 or L2): This layer corresponds to Layer 3 of the OSI model.

Network Access (Layer 1 or L1): This layer corresponds to Layers 1 and 2 of the OSI model

NEW QUESTION 58

Which analysis detonates previously unknown submissions in a custom-built, evasion-resistant virtual environment to determine real-world effects and behavior?

- A. Dynamic
- B. Pre-exploit protection
- C. Bare-metal
- D. Static

Answer: A

Explanation:

The WildFire cloud-based malware analysis environment is a cyber threat prevention service that identifies unknown malware, zero-day exploits, and advanced persistent threats (APTs) through static and dynamic analysis in a scalable, virtual environment.

NEW QUESTION 61

Which type of Wi-Fi attack depends on the victim initiating the connection?

- A. Evil twin
- B. Jasager
- C. Parager
- D. Mirai

Answer: A

Explanation:

Perhaps the easiest way for an attacker to find a victim to exploit is to set up a wireless access point that serves as a bridge to a real network. An attacker can inevitably bait a few victims with “free Wi-Fi access.” The main problem with this approach is that it requires a potential victim to stumble on the access point and connect. The attacker can’t easily target a specific victim, because the attack depends on the victim initiating the connection.

<https://www.paloaltonetworks.com/blog/2013/11/wireless-man-middle/>

NEW QUESTION 63

Which characteristic of serverless computing enables developers to quickly deploy application code?

- A. Uploading cloud service autoscaling services to deploy more virtual machines to run their application code based on user demand
- B. Uploading the application code itself, without having to provision a full container image or any OS virtual machine components
- C. Using cloud service spot pricing to reduce the cost of using virtual machines to run their application code
- D. Using Container as a Service (CaaS) to deploy application containers to run their code.

Answer: B

Explanation:

"In serverless apps, the developer uploads only the app package itself, without a full container image or any OS components. The platform dynamically packages it into an image, runs the image in a container, and (if needed) instantiates the underlying host OS and VM and the hardware required to run them."

NEW QUESTION 68

When signature-based antivirus software detects malware, what three things does it do to provide protection? (Choose three.)

- A. decrypt the infected file using base64
- B. alert system administrators
- C. quarantine the infected file
- D. delete the infected file
- E. remove the infected file's extension

Answer: CDE

NEW QUESTION 70

Why is it important to protect East-West traffic within a private cloud?

- A. All traffic contains threats, so enterprises must protect against threats across the entire network
- B. East-West traffic contains more session-oriented traffic than other traffic
- C. East-West traffic contains more threats than other traffic
- D. East-West traffic uses IPv6 which is less secure than IPv4

Answer: A

NEW QUESTION 72

Which network firewall operates up to Layer 4 (Transport layer) of the OSI model and maintains information about the communication sessions which have been established between hosts on trusted and untrusted networks?

- A. Group policy
- B. Stateless

- C. Stateful
- D. Static packet-filter

Answer: C

Explanation:

Stateful packet inspection firewalls Second-generation stateful packet inspection (also known as dynamic packet filtering) firewalls have the following characteristics:
They operate up to Layer 4 (Transport layer) of the OSI model and maintain state information about the communication sessions that have been established between hosts on the trusted and untrusted networks.
They inspect individual packet headers to determine source and destination IP address, protocol (TCP, UDP, and ICMP), and port number (during session establishment only) to determine whether the session should be allowed, blocked, or dropped based on configured firewall rules.
After a permitted connection is established between two hosts, the firewall creates and deletes firewall rules for individual connections as needed, thus effectively creating a tunnel that allows traffic to flow between the two hosts without further inspection of individual packets during the session.
This type of firewall is very fast, but it is port-based and it is highly dependent on the trustworthiness of the two hosts because individual packets aren't inspected after the connection is established.

NEW QUESTION 76

Match the DNS record type to its function within DNS.

Answer Area

CNAME	MX		Maps domain of subdomain to another hostname
SOA	NS		Specifies an authoritative name server for a given host
			Specifies the hostname or hostnames of email servers for a domain
			Specifies authoritative information about DNS Zone such as Primary name server

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The basic DNS record types are as follows:
A (IPv4) or AAAA (IPv6) (Address): Maps a domain or subdomain to an IP address or multiple IP addresses
CNAME (Canonical Name): Maps a domain or subdomain to another hostname
MX (Mail Exchanger): Specifies the hostname or hostnames of email servers for a domain PTR (Pointer): Points to a CNAME; commonly used for reverse DNS lookups that map an IP address to a host in a domain or subdomain
SOA (Start of Authority): Specifies authoritative information about a DNS zone such as primary name server, email address of the domain administrator, and domain serial number
NS (Name Server): The NS record specifies an authoritative name server for a given host. TXT (Text): Stores text-based information

NEW QUESTION 78

Match the Palo Alto Networks WildFire analysis verdict with its definition.

Answer Area

Benign		malicious in intent and can pose a security threat
Grayware		does not pose a direct security threat
Malware		does not exhibit a malicious behavior

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Benign: Safe and does not exhibit malicious behavior

Grayware: No security risk but might display obtrusive behavior (for example, adware, spyware, and browser helper objects)

Malware: Malicious in nature and intent and can pose a security threat (for example, viruses, worms, trojans, root kits, botnets, and remote-access toolkits)

Phishing: Malicious attempt to trick the recipient into revealing sensitive data

NEW QUESTION 81

What does SIEM stand for?

- A. Security Infosec and Event Management
- B. Security Information and Event Management
- C. Standard Installation and Event Media
- D. Secure Infrastructure and Event Monitoring

Answer: B

Explanation:

Originally designed as a tool to assist organizations with compliance and industry-specific regulations, security information and event management (SIEM) is a technology that has been around for almost two decades

NEW QUESTION 83

A user is provided access over the internet to an application running on a cloud infrastructure. The servers, databases, and code of that application are hosted and maintained by the vendor.

Which NIST cloud service model is this?

- A. IaaS
- B. SaaS
- C. PaaS
- D. CaaS

Answer: B

Explanation:

SaaS - User responsible for only the data, vendor responsible for rest

NEW QUESTION 84

Which network analysis tool can be used to record packet captures?

- A. Smart IP Scanner
- B. Wireshark
- C. Angry IP Scanner
- D. Netman

Answer: B

NEW QUESTION 88

Which IPsec feature allows device traffic to go directly to the Internet?

- A. Split tunneling
- B. Diffie-Hellman groups
- C. d.Authentication Header (AH)
- D. IKE Security Association

Answer: A

Explanation:

"Or split tunneling can be configured to allow internet traffic from the device to go directly to the internet, while other specific types of traffic route through the IPsec tunnel, for acceptable protection with much less performance degradation."

NEW QUESTION 92

Which Palo Alto Networks subscription service complements App-ID by enabling you to configure the next- generation firewall to identify and control access to websites and to protect your organization from websites hosting malware and phishing pages?

- A. Threat Prevention
- B. DNS Security
- C. WildFire
- D. URL Filtering

Answer: D

Explanation:

The URL Filtering service complements App-ID by enabling you to configure the next-generation firewall to identify and control access to websites and to protect your organization from websites that host malware and phishing pages.

NEW QUESTION 97

Anthem server breaches disclosed Personally Identifiable Information (PII) from a number of its servers. The infiltration by hackers was attributed to which type of vulnerability?

- A. an intranet-accessed contractor's system that was compromised
- B. exploitation of an unpatched security vulnerability
- C. access by using a third-party vendor's password
- D. a phishing scheme that captured a database administrator's password

Answer: D

NEW QUESTION 102

Which option is a Prisma Access security service?

- A. Compute Security
- B. Firewall as a Service (FWaaS)
- C. Virtual Private Networks (VPNs)
- D. Software-defined wide-area networks (SD-WANs)

Answer: B

Explanation:

Prisma Access provides firewall as a service (FWaaS) that protects branch offices from threats while also providing the security services expected from a next-generation firewall. The full spectrum of FWaaS includes threat prevention, URL filtering, sandboxing, and more.

NEW QUESTION 107

Which activities do local organization security policies cover for a SaaS application?

- A. how the data is backed up in one or more locations
- B. how the application can be used
- C. how the application processes the data
- D. how the application can transit the Internet

Answer: B

NEW QUESTION 109

Which aspect of a SaaS application requires compliance with local organizational security policies?

- A. Types of physical storage media used
- B. Data-at-rest encryption standards
- C. Acceptable use of the SaaS application
- D. Vulnerability scanning and management

Answer: C

NEW QUESTION 113

.....

Relate Links

100% Pass Your PCCET Exam with Exambible Prep Materials

<https://www.exambible.com/PCCET-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>