**QUESTION 583**
Which of the following refers to the data that is stored or processed by RAM, CPUs, or databases?

A. Data in Backup
B. Data at Rest
C. Data in Transit
D. Data is Use

**Answer:** B

**QUESTION 584**
Which of the following data security technology can ensure information protection by obscuring specific areas of information?

A. Data retention
B. Data encryption
C. Data hashing
D. Data masking

**Answer:** D

**QUESTION 585**
How can one identify the baseline for normal traffic?

A. When the SYN flag appears at the beginning and the FIN flag appears at the end of the connection
B. When the RST flag appears at the beginning and the ACK flag appears at the end of the connection
C. When the ACK flag appears at the beginning and the RST flag appears at the end of the connection
D. When the FIN flag appears at the beginning and the SYN flag appears at the end of the connection

**Answer:** D

**QUESTION 586**
How is an “attack” represented?

A. Motive (goal) + method
B. Motive (goal) + method + vulnerability
C. Asset + Threat + Vulnerability
D. Asset + Threat

**Answer:** A

**QUESTION 587**
Kelly is taking backups of the organization's data. Currently, she is taking backups of only those files that are created or modified after the last backup. What type of backup is Kelly using?

A. Full backup
B. Incremental backup
C. Normal backup
D. Differential backup

**Answer:** D

**QUESTION 588**
Sam wants to implement a network-based IDS and finalizes an IDS solution that works based on pattern matching. Which type of network-based IDS is Sam implementing?

A. Behavior-based IDS
B. Anomaly-based IDS
C. Signature-based IDS
D. Stateful protocol analysis

**Answer:** C

**QUESTION 589**
Which of the following refers to a potential occurrence of an undesired event that can eventually damage and interrupt the operational and functional activities of an organization?

A. Attack
B. Risk
C. Threat
D. Vulnerability

**Answer:** C

**QUESTION 590**
Byron, a new network administrator at FBI, would like to ensure that Windows PCs there are up-to-date and have less internal security flaws. What can he do?

A. Centrally assign Windows PC group policies
B. Dedicate a partition on HDD and format the disk using NTFS
C. Download and install latest patches and enable Windows Automatic Updates
D. Install antivirus software and turn off unnecessary services

**Answer:** D

**QUESTION 591**
Which of the following entities is responsible for cloud security?

A. Cloud consumer

B. Cloud provider
C. Both cloud consumer and provider
D. Cloud broker

**Answer:** C

**QUESTION 592**
The _____ mechanism works on the basis of a client-server model.

A. Push-based
B. Host-based
C. Pull-based
D. Network-based

**Answer:** C

**QUESTION 593**
Peter works as a network administrator at an IT company. He wants to avoid exploitation of the cloud, particularly Azure services. Which of the following is a group of PowerShell scripts designed to help the network administrator understand how attacks happen and help them protect the cloud?

A. POSH-Sysmon
B. MicroBurst
C. SecurityPolicyDsc
D. Sysmon

**Answer:** B

**QUESTION 594**
Docker provides Platform-as-a-Service (PaaS) through _____ and delivers containerized software packages.

A. Server-level virtualization
B. Network-level virtualization
C. OS-level virtualization
D. Storage-level virtualization

**Answer:** C

**QUESTION 595**
Mark is monitoring the network traffic on his organization's network. He wants to detect TCP and UDP ping sweeps on his network. Which type of filter will be used to detect this?

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

**Answer:** C

**QUESTION 596**
John has implemented _____ in the network to restrict the number of public IP addresses in his organization and to enhance the firewall filtering technique.

A. VPN
B. Proxies

C. DMZ
D. NAT

**Answer:** D

**QUESTION 597**
Which of the following statements holds true in terms of virtual machines?

A. Hardware-level virtualization takes place in VMs
B. OS-level virtualization takes place in VMs
C. All VMs share the host OS
D. VMs are light weight than containers

**Answer:** A

**QUESTION 598**
Leslie, the network administrator of Livewire Technologies, has been recommending multilayer inspection firewalls to deploy the company's infrastructure. What layers of the TCP/IP model can it protect?

A. IP, application, and network interface
B. Network interface, TCP, and IP
C. Application, TCP, and IP
D. Application, IP, and network interface

**Answer:** D

**QUESTION 599**
Which command list all ports available on a server?

A. sudo apt nst -tunlp
B. sudo netstat -tunlp
C. sudo apt netstate -ls tunlp
D. sudo ntstat -ls tunlp

**Answer:** B

**QUESTION 600**
Which BC/DR activity works on the assumption that the most critical processes are brought back from a remote location first, followed by the less critical functions?

A. Recovery
B. Restoration
C. Response
D. Resumption

**Answer:** A

**QUESTION 601**
Richard has been working as a Linux system administrator at an MNC. He wants to maintain a productive and secure environment by improving the performance of the systems through Linux patch management. Richard is using Ubuntu and wants to patch the Linux systems manually. Which among the following command installs updates (new ones) for Debian-based Linux OSes?

A. sudo apt-get upgrade
B. sudo apt-get dist-update

C. sudo apt-get dist-upgrade
D. sudo apt-get update

**Answer:** C

**QUESTION 602**
Which of the following connects the SDN controller and SDN networking devices and relays information from network services to network devices such as switches and routers?

A. Southbound API
B. Eastbound API
C. Westbound API
D. Northbound API

**Answer:** A

**QUESTION 603**
Henry, head of network security at Gentech, has discovered a general report template that someone has reserved only for the CEO. Since the file has to be editable, viewable, and deletable by everyone, what permission value should he set?

A. 700
B. 777
C. 755
D. 600

**Answer:** B

**QUESTION 604**
Which of the following provides a set of voluntary recommended cyber security features to include in network-capable IoT devices?

A. FGMA
B. GLBA
C. GCMA
D. NIST

**Answer:** D

**QUESTION 605**
Which type of wireless network threats an attacker stakes out the area from a nearby location with a high gain amplifier drowning out the legitimate access point?

A. Rogue access point attack
B. Jamming signal attack
C. Ad Hoc Connection attack
D. Unauthorized association

**Answer:** B

**QUESTION 606**
Which of the following type of UPS is used to supply power above 10kVA and provides an ideal electric output presentation, and its constant wear on the power components reduces the dependability?

A. Line Interactive

B. Double conversion on-line
C. Stand by Ferro
D. Stand by On-line hybrid

**Answer:** B

**QUESTION 607**
John has planned to update all Linux workstations in his network. The organization is using various Linux distributions including Red hat, Fedora and Debian. Which of following commands will he use to update each respective Linux distribution?

| | | | |
|---|---|---|---|
| 1. | Autoupdate | i. | Slackware based |
| 2. | Swaret | ii. | RPM-based |
| 3. | apt-get | iii. | Red Hat based |
| 4. | up2date | iv. | Debian based |
| | | v. | Fedora based |

A. 1-ii, 2-i,3-iv,4-iii
B. 1-v,2-iii,3-i,4-iv
C. 1-iv,2-v,3-iv,4-iii
D. 1-iii,2-iv,3-ii,4-v

**Answer:** A

**QUESTION 608**
Andrew would like to configure IPsec in a manner that provides confidentiality for the content of packets. What component of IPsec provides this capability?

A. IKE
B. ESP
C. AH
D. ISAKMP

**Answer:** B

**QUESTION 609**
Which characteristic of an antenna refers to how directional an antennas radiation pattern is?

A. Radiation pattern
B. Polarization
C. Directivity
D. Typical gain

**Answer:** A

**QUESTION 610**
Which field is not included in the TCP header?

A. Acknowledgment number
B. Sequence number
C. Source port
D. Source IP address

**Answer:** D