QUESTION 531
A company wants to implement a data backup method that allows them to encrypt the data ensuring its security as well as access it at any time and from any location. What is the appropriate backup method that should be implemented?

A. Cloud backup
B. Offsite backup
C. Hot site backup
D. Onsite backup

Answer: A

QUESTION 532
Which of the following helps in viewing account activity and events for supported services made by AWS?

A. AWS CloudFormation
B. AWS Certificate Manager
C. AWS CloudHSM
D. AWS CloudTrial

Answer: D

QUESTION 533
John is working as a network defender at a well-reputed multinational company. He wanted to implement security that can help him identify any future attacks that can be targeted toward his organization and take appropriate security measures and actions beforehand to defend against them. Which one of the following security defense techniques should be implement?

A. Reactive security approach
B. Retrospective security approach
C. Proactive security approach
D. Preventive security approach

Answer: C

QUESTION 534
Which type of firewall consists of three interfaces and allows further subdivision of the systems based on specific security objectives of the organization?

A. Screened subnet
B. Bastion host

C. Unscreened subnet
D. Multi-homed firewall

Answer: D

QUESTION 535
Which of the following is true regarding any attack surface?

A. Decrease in vulnerabilities decreases the attack surface
B. Increase in vulnerabilities decreases the attack surface
C. Decrease in risk exposures increases the attack surface
D. Decrease in vulnerabilities increases the attack surface

Answer: A

QUESTION 536
Which type of attack is used to hack an IoT device and direct large amounts of network traffic toward a web server, resulting in overloading the server with connections and preventing any new connections?

A. XSS
B. DDoS
C. XCRF
D. Sniffing

Answer: B

QUESTION 537
How is a "risk" represented?

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

Answer: C

QUESTION 538
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. Evidence Manager
B. Incident Handler
C. Attorney
D. PR Specialist

Answer: C

QUESTION 539
An employee of a medical service company clicked a malicious link in an email sent by an attacker. Suddenly, employees of the company are not able to access billing information or client record as it is encrypted. The attacker asked the company to pay money for gaining access to their dat

A. Which type of malware attack is described above?
B. Logic bomb

C. Rootkits
D. Trojan
E. Ransomware

Answer: D

QUESTION 540
Which of the following defines the extent to which an interruption affects normal business operations and the amount of revenue lost due to that interruption?

A. RPO
B. RFO
C. RSP
D. RTO

Answer: D

QUESTION 541
Which command is used to change the permissions of a file or directory?

A. rmdir
B. systemctl
C. kill
D. chmod

Answer: D

QUESTION 542
John, a network administrator, is configuring Amazon EC2 cloud service for his organization. Identify the type of cloud service modules his organization adopted.

A. Software-as-a-Service (SaaS)
B. Infrastructure-as-a-Service (IaaS)
C. Platform-as-a-Service (PaaS)
D. Storage-as-a-Service (SaaS)

Answer: B

QUESTION 543
Identify the type of event that is recorded when an application driver loads successfully in Windows.

A. Success Audit
B. Error
C. Warning
D. Information

Answer: D

QUESTION 544
Based on which of the following registry key, the Windows Event log audit configurations are recorded?

A. HKEY_LOCAL_MACHINE\SYSTEM\Services\EventLog\ < ErrDev >
B. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\EventLog\ < EntAppsvc >
C. HKEY_LOCAL_MACHINE\CurrentControlSet\Services\EventLog\< ESENT >
D. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\ < Event Log >

Answer: D

QUESTION 545
Which of the following is an example of MAC model?

A. Chinese Waterfall model
B. Clark-Beason integrity model
C. Access control matrix model
D. Bell-LaPadula model

Answer: A

QUESTION 546
How can a WAF validate traffic before it reaches a web application?

A. It uses a role-based filtering technique
B. It uses an access-based filtering technique
C. It uses a sandboxing filtering technique
D. It uses a rule-based filtering technique

Answer: D

QUESTION 547
Jason has set a firewall policy that allows only a specific list of network services and denies everything else. This strategy is known as a _____.

A. Default allow
B. Default access
C. Default accept
D. Default deny

Answer: D

QUESTION 548
Which of the following things need to be identified during attack surface visualization?

A. Attacker's tools, techniques, and procedures
B. Authentication, authorization, and auditing in networks
C. Regulatory frameworks, standards and, procedures for organizations
D. Assets, topologies, and policies of the organization

Answer: A

QUESTION 549
John is a senior network security administrator working at a multinational company. He wants to block specific syscalls from being used by container binaries. Which Linux kernel feature restricts actions within the container?

A. Cgroups
B. LSMs
C. Seccomp
D. Userns

Answer: C

QUESTION 550
Which of the following is not part of the recommended first response steps for network defenders?

A. Restrict yourself from doing the investigation
B. Extract relevant data from the suspected devices as early as possible
C. Disable virus protection
D. Do not change the state of the suspected device

Answer: D

QUESTION 551
Which among the following tools can help in identifying IoEs to evaluate human attack surface?

A. securiCAD
B. Amass
C. Skybox
D. SET

Answer: A

QUESTION 552
In _____ method, event logs are arranged in the form of a circular buffer.

A. Non-wrapping method
B. LIFO method
C. Wrapping method
D. FIFO method

Answer: D

QUESTION 553
Which of the following indicators refers to potential risk exposures that attackers can use to breach the security of an organization?

A. Indicators of attack
B. Key risk indicators
C. Indicators of exposure
D. Indicators of compromise

Answer: C

QUESTION 554
Which of the following can be used to disallow a system/user from accessing all applications except a specific folder on a system?

A. Hash rule
B. Path rule
C. Internet zone rule
D. Certificate rule

Answer: A

QUESTION 555
Which of the following helps prevent executing untrusted or untested programs or code from untrusted or unverified third-parties?

A. Application sandboxing
B. Deployment of WAFS
C. Application whitelisting
D. Application blacklisting

Answer: A

QUESTION 556
Who is an IR custodian?

A. An individual responsible for conveying company details after an incident
B. An individual who receives the initial IR alerts and leads the IR team in all the IR activities
C. An individual who makes a decision on the classifications and the severity of the incident identified
D. An individual responsible for the remediation and resolution of the incident that occurred

Answer: B

QUESTION 557
Which of the following attack surface increase when you keep USB ports enabled on your laptop unnecessarily?

A. Human attack surface
B. Network attack surface
C. Physical attack surface
D. Software attack surface

Answer: C

QUESTION 558
Which among the following filter is used to detect a SYN/FIN attack?

A. tcp.flags==0x002
B. tcp.flags==0x004
C. tcp.flags==0x003
D. tcp.flags==0x001

Answer: D

QUESTION 559
In _____ mechanism, the system or application sends log records either on the local disk or over the network.

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

Answer: C

QUESTION 560
Choose the correct order of steps to analyze the attack surface.

A. Identify the indicators of exposure->visualize the attack surface->simulate the attack->reduce the attack surface
B. Visualize the attack surface->simulate the attack->identify the indicators of exposure->reduce the

attack surface

C. Identify the indicators of exposure->simulate the attack->visualize the attack surface->reduce the attack surface
D. Visualize the attack surface->identify the indicators of exposure->simulate the attack->reduce the attack surface

Answer: D

QUESTION 561
To provide optimum security while enabling safe/necessary services, blocking known dangerous services, and making employees accountable for their online activity, what Internet Access policy would Brian, the network administrator, have to choose?

A. Prudent policy
B. Paranoid policy
C. Promiscuous policy
D. Permissive policy

Answer: A

QUESTION 562
Emmanuel works as a Windows system administrator at an MNC. He uses PowerShell to enforce the script execution policy. He wants to allow the execution of the scripts that are signed by a trusted publisher. Which of the following script execution policy setting this?

A. AllSigned
B. Restricted
C. RemoteSigned
D. Unrestricted

Answer: A

QUESTION 563
Fargo, head of network defense at Globadyne Tech, has discovered an undesirable process in several Linux systems, which causes machines to hang every 1 hour. Fargo would like to eliminate it; what command should he execute?

A. # update-rc.d -f [service name] remove
B. # service [service name] stop
C. # ps ax | grep [Target Process]
D. # kill -9 [PID]

Answer: D

QUESTION 564
Elden is working as a network administrator at an IT company. His organization opted for a virtualization technique in which the guest OS is aware of the virtual environment in which it is running and communicates with the host machines for requesting resources. Identify the virtualization technique implemented by Elden's organization.

A. Hybrid virtualization
B. Hardware-assisted virtualization
C. Full virtualization
D. Para virtualization

Answer: B

QUESTION 565
Albert works as a Windows system administrator at an MNC. He uses PowerShell logging to identify any suspicious scripting activity across the network. He wants to record pipeline execution details as PowerShell executes, including variable initialization and command invocations. Which PowerShell logging component records pipeline execution details as PowerShell executes?

A. Module logging
B. Script block logging
C. Event logging
D. Transcript logging

Answer: A

QUESTION 566
Sophie has been working as a Windows network administrator at an MNC over the past 7 years. She wants to check whether SMB1 is enabled or disabled. Which of the following command allows Sophie to do so?

A. Get-WindowsOptionalFeatures -Online -FeatureNames SMB1Protocol
B. Get-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
C. Get-WindowsOptionalFeature -Online -FeatureNames SMB1Protocol
D. Get-WindowsOptionalFeatures -Online -FeatureName SMB1Protocol

Answer: B

QUESTION 567
How is an "attack" represented?

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

Answer: A

QUESTION 568
Identify the virtualization level that creates a massive pool of storage areas for different virtual machines running on the hardware.

A. Fabric virtualization
B. Storage device virtualization
C. Server virtualization
D. File system virtualization

Answer: B

QUESTION 569
Steven is a Linux system administrator at an IT company. He wants to disable unnecessary services in the system, which can be exploited by the attackers. Which among the following is the correct syntax for disabling a service?

A. $ sudo system-ctl disable [service]
B. $ sudo systemctl disable [service]
C. $ sudo system.ctl disable [service]
D. $ sudo system ctl disable [service]

Answer: B

QUESTION 570
Simran is a network administrator at a start-up called Revolution. To ensure that neither party in the company can deny getting email notifications or any other communication, she mandates authentication before a connection establishment or message transfer occurs. What fundamental attribute of network defense is she enforcing?

A. Integrity
B. Non-repudiation
C. Confidentiality
D. Authentication

Answer: B