CND EXAM ANSWERS

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?
Script block logging
Based on which of the following registry keys, the Windows Event log audit configurations are recorded?

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\ < Event Log >

Which of the following is an example of MAC model?

Bell-LaPadula model

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

Assets, topologies, and policies of the organization

Oliver is a Linux security administrator at an MNC. An employee named Alice has resigned from his organization and Oliver wants to disable this user in Ubuntu. Which of the following commands can be used to accomplish this?

usermod -L alice

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

Physical attack surface

Which firewall technology can filter application-specific commands such as GET and POST requests?

Application proxy

Which phase of incident response process involves collection of incident evidence and sending them to forensic department for further investigation?

Incident recording and assignment

Which form of access control is trust centric?

Application whitelisting

Which firewall technology can be implemented in all (application, session, transport, network, and presentation) layers of the OSI model?

Circuit-level gateway

which among the following is used by anti-malware systems and threat intelligence platforms to spot and stop malicious activities at an initial stage?

Indicators of compromise

Which of the following entities is responsible for cloud security?

Both cloud consumer and provider

Who offers formal experienced testimony in court?

Expert witness

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

NIST

Maximus Tech is a multinational company that uses Cisco ASA Firewalls for their systems. Jason is the one of the members of the team that checks the logs at Maximus Tech. As a part of his job, he is going through the logs and he came across a firewall log that looks like this:
May 06 2018 21:27:27 asa 1: % ASA -5 – 11008: User ‘enable_15’ executed the ‘configure term’ command
Based on the security level mentioned in the log, what did Jason understand about the description of this message?

Normal but significant message

Clement is the CEO of an IT firm. He wants to implement a policy allowing employees with a preapproved set of devices from which the employees choose devices (laptops, smartphones, and tablets) to access company data as per the organization's access privileges. Which among the following policies does Clement want to enforce?

CYOD policy

Ivan needs to pick an encryption method that is scalable even though it might be slower. He has settled on a method that works where one key is public and the other is private. What encryption method did Ivan settle on?

Ivan settled on the asymmetric encryption method.

Hacktivists are threat actors, who can be described as ________________.

People having political or social agenda

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

AWS CloudTrail

Which category of suspicious traffic signatures includes SYN flood attempts?

Denial of Service

In ______method, windows event logs are arranged in the form of a circular buffer.

Wrapping method

An attacker uses different types of password cracking techniques to crack the password and gain unauthorized access to a system. The attacker uses a file containing a list of commonly used passwords. They then upload this file into the cracking application that runs against the user accounts.

The attacker is trying:

Dictionary

The option that provides enhanced password protection, secured IoT connections, and encompasses stronger encryption techniques is:

WPA3

The clues, artifacts, or evidence that indicate a potential intrusion or malicious activity in an organization's infrastructure are referred to as:

Indicators of compromise

John is thinking of implementing:

Circuit level gateway

Rosa can find the security related logs at:

/private/var/log

The modulation technique used in local area wireless networks (LAWNs) is:

OFDM

The security model that enables strict identity verification for every user or device attempting to access the network resources is:

I only (Zero-trust network model)

James should use:

James could use PGP as a free option for encrypting the company's emails.

The type of training that can create awareness among employees regarding compliance issues is:

Security policy training

The scan attempt that can penetrate through a router and a firewall that filter incoming packets with particular flags set and is not supported by Windows is:

TCP null scan attempt

A multilayer inspection firewall can protect the following layers of the TCP/IP model:

Application, TCP, and IP

In the _______ mechanism, the system or application sends log records either on the local disk or over the network:

Push-based

The ability of an organization to respond under emergency in order to minimize the damage to its brand name, business operation, and profit represents:

Crisis management

The person responsible for executing the policies and plans required for supporting the information technology and computer systems of an organization is the:

Chief Information Officer (CIO)

The risk management phase that helps in establishing context and quantifying risks is:

Risk assessment

The indicators discovered through an attacker's intent, their end goal or purpose, and a series of actions that they must take before being able to successfully launch an attack are:

Indicators of attack

Michelle should implement:

MCM

The person who oversees all the incident response activities in an organization and is responsible for all actions of the IR team and IR function is the:

IR officer

According to standard IoT security practice, IoT Gateway should be connected to a:

Secure router

The firewall technology that provides the best of both packet filtering and application-based filtering and is used in Cisco Adaptive Security Appliances is:

Stateful multilayer inspection

The RAID level system that provides very good data performance but does not offer fault tolerance and data redundancy is:

RAID level 0

The CEO of Max Rager can prevent the message from being altered in transit by using:

Hashing; hash code

The virtualization technique implemented by Elden's organization is:

Para virtualization

In terms of virtual machines, the following statement holds true:

OS-level virtualization takes place in VMs

Unsuccessful scans and probes are at the:

Low severity level

For better bandwidth management, deep packet inspection, and stateful inspection, a network administrator can use:

Next-generation firewall

The company should consult a/an _______ for legal advice to defend them against the allegation:

Attorney

A WAF validates traffic before it reaches a web application by using:

It uses a rule-based filtering technique

A firewall that consists of three interfaces and allows further subdivision of the systems based on specific security objectives of the organization is:

Multi-homed firewall

The permission value Henry should set for the file is:

777

Ross implemented:

Discretionary access control

The database encryption feature that secures sensitive data in MS SQL Server is:

Always Encrypted

WPA encryption in a wireless network uses:

CCMP, AES-based encryption protocol and a/an 64-bit MIC integrity check

Sophie can check whether SMB1 is enabled or disabled using the command:

Get-WindowsOptionalFeature -Online -FeatureName SMB1Protocol

The tool that can help in identifying IoEs to evaluate the human attack surface is:

securiCAD

The type of antenna based on the principle of a satellite dish and can pick up Wi-Fi signals from a distance of ten miles or more is:

Parabolic Grid antenna

The local bank should comply with the following standard to ensure the security of cardholder data:

PCI DSS

In business continuity management, the process that enables an organization to analyze, identify, and rectify hazards and prevent future recurrence is:

Incident management

The data destruction technique that protects the sensitivity of information against a laboratory attack is:

Purging

The Windows in-built feature that provides filesystem-level encryption, except in the Home version of Windows, is:

EFS

Regarding any attack surface, the following statement is true:

Decrease in vulnerabilities decreases the attack surface

Professional hackers with an aim of attacking systems for profit are represented by:

Organized hackers

The RAID level that Katie has implemented requires a minimum of:

Two drives

A drawback of traditional perimeter security is:

Traditional firewalls are static in nature

Implementing access control mechanisms, such as a firewall, to protect the network is an example of which network defense approach?

Preventive approach

The encryption algorithm used by WPA3 encryption is:

AES-GCMP 256

John has been working as a network administrator at an IT company. He wants to prevent misuse of accounts by unauthorized users. He wants to ensure that no accounts have empty passwords. Which of the following commands does John use to list all the accounts with an empty password?

```
awk -F: '($2 == "") {print}' /etc/shadow
```

How is the chip-level security of an IoT device achieved?

Encrypting JTAG interface

Which among the following is used to limit the number of cmdlets or administrative privileges of administrator, user, or service accounts?

Just Enough Administration (JEA)

Identify the method involved in purging technique of data destruction.

Degaussing

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?

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.

Disaster Recovery is a

Business-centric strategy.

Which of the following technologies can be used to leverage zero-trust model security?

Software-defined perimeter (SDP)

John is the Vice-President of a BPO. He wants to implement a policy allowing employees to use and manage devices purchased by the organization but restrict the use of the device for business use only. Which among the following policies does John want to implement?

COPE policy

John is working as a network defender at a well-reputed multinational company. He wants 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 he implement?

Proactive security approach

Docker provides Platform-as-a-Service (PaaS) through ___________ and delivers containerized software packages

OS-level virtualization

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?

$ sudo systemctl disable [service]

Which type of risk treatment process includes not allowing the use of laptops in an organization to ensure its security?

Risk avoidance

What should an administrator do while installing a sniffer on a system to listen to all data transmitted over the network?

Set the system's NIC to promiscuous mode

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?

AllSigned

How is a "risk" represented?

Asset + threat + vulnerability

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

Data masking

How is application whitelisting different from application blacklisting?

It rejects all applications other than the allowed applications

How can an administrator detect a TCP null scan attempt on a UNIX server by using Wireshark?

By applying the filter tcp.flags==0x000

Which of the following statement holds true in terms of containers?

Process-level isolation happens; a container in hence less secure

Which of following are benefits of using IoT devices in IoT-enabled environments? I. IoT device can be connected anytime II. IoT device can be connected at any place III. IoT devices connected to anything

I , II, and III

What defines the maximum time period an organization is willing to lose data during a major IT outage event?

RPO

Which of the following characteristics represents a normal TCP packet?

FIN ACK and ACK are used in terminating the connection

In MacOS, how can the user implement disk encryption?

By enabling FileVault feature

Which of the following filters can be applied to detect an ICMP ping sweep attempt using Wireshark?

icmp.type==8

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

Information

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?

tcp.dstport==7 and udp.dstport==7

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?

sudo apt-get upgrade

Identify the correct order for a successful black hat operation.

Reconnaissance, Scanning, Gaining Access, Maintaining Access, and Covering Tracks

Who is responsible for conveying company details after an incident?

PR specialist

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?

Seccomp

Which of the following filters can be used to detect UDP scan attempts using Wireshark?

icmp.type==3 and icmp.code==3

Nancy is working as a network defender 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) 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; and 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?

RAID 5