techniques would BEST meet the requirement?

A. Asymmetric
B. Symmetric
C. Homeomorphic
D. Ephemeral

**Correct Answer:** C
**Explanation:**
"In a nutshell, homomorphic encryption is a method of encryption that allows any data to remain encrypted while it's being processed and manipulated. It enables you or a third party (such as a cloud provider) to apply functions on encrypted data without needing to reveal the values of the data."

https://www.thesslstore.com/blog/what-is-homomorphic-encryption/
https://en.wikipedia.org/wiki/Homomorphic_encryption

**QUESTION 385**
A client sent several inquiries to a project manager about the delinquent delivery status of some critical reports. The project manager claimed the reports were previously sent via email, but then quickly generated and backdated the reports before submitting them as plain text within the body of a new email message thread. Which of the following actions MOST likely supports an investigation for fraudulent submission?

A. Establish chain of custody.
B. Inspect the file metadata.
C. Reference the data retention policy.
D. Review the email event logs

**Correct Answer:** B

**QUESTION 386**
A security analyst is investigating multiple hosts that are communicating to external IP addresses during the hours of 2:00 a.m - 4:00 am. The malware has evaded detection by traditional antivirus software. Which of the following types of malware is MOST likely infecting the hosts?

A. RAT
B. Ransomware
C. Logic bomb
D. A worm

**Correct Answer:** C

**QUESTION 387**
An external forensics investigator has been hired to investigate a data breach at a large enterprise with numerous assets. It is known that the breach started in the DMZ and moved to the sensitive information, generating multiple logs as the attacker traversed through the network. Which of the following will BEST assist with this investigation?

A. Perform a vulnerability scan to identity the weak spots.
B. Use a packet analyzer to Investigate the NetFlow traffic.
C. Check the SIEM to review the correlated logs.
D. Require access to the routers to view current sessions.

**Correct Answer:** C

**QUESTION 388**
An information security officer at a credit card transaction company is conducting a framework-mapping exercise with the internal controls. The company recently established a new office in Europe. To which of the following frameworks should the security officer map the existing controls? (Select TWO).

A. ISO
B. PCI DSS
C. SOC
D. GDPR
E. CSA
F. NIST

**Correct Answer:** BD

**QUESTION 389**
A security analyst has been reading about a newly discovered cyber attack from a known threat actor. Which of the following would BEST support the analyst's review of the tactics, techniques, and protocols the threat actor was observed using in previous campaigns?

A. Security research publications
B. The MITRE ATT&CK framework
C. The Diamond Model of Intrusion Analysis
D. The Cyber Kill Chain

**Correct Answer:** B

**QUESTION 390**
A security analyst is responding to an alert from the SIEM. The alert states that malware was discovered on a host and was not automatically deleted. Which of the following would be BEST for the analyst to perform?

A. Add a deny-all rule to that host in the network ACL
B. Implement a network-wide scan for other instances of the malware.
C. Quarantine the host from other parts of the network
D. Revoke the client's network access certificates

**Correct Answer:** C
**Explanation:**
What is Malware?
Malware, short for "malicious software," refers to any intrusive software developed by cybercriminals (often called "hackers") to steal data and damage or destroy computers and computer systems. Examples of common malware include viruses, worms, Trojan viruses, spyware, adware, and ransomware. Recent malware attacks have exfiltrated data in mass amounts.

How do I protect my network against malware?
Typically, businesses focus on preventative tools to stop breaches. By securing the perimeter, businesses assume they are safe. Some advanced malware, however, will eventually make their way into your network. As a result, it is crucial to deploy technologies that continually monitor and

detect malware that has evaded perimeter defenses. Sufficient advanced malware protection requires multiple layers of safeguards along with high-level network visibility and intelligence.

How do I detect and respond to malware?
Malware will inevitably penetrate your network. You must have defenses that provide significant visibility and breach detection. In order to remove malware, you must be able to identify malicious actors quickly. This requires constant network scanning. Once the threat is identified, you must remove the malware from your network. Today's antivirus products are not enough to protect against advanced cyber threats. Learn how to update your antivirus strategy.

**QUESTION 391**
The Chief Information Security Officer warns lo prevent exfiltration of sensitive information from employee cell phones when using public USB power charging stations. Which of the following would be the BEST solution to Implement?

A. DLP
B. USB data blocker
C. USB OTG
D. Disabling USB ports

**Correct Answer:** A

**QUESTION 392**
Certain users are reporting their accounts are being used to send unauthorized emails and conduct suspicious activities. After further investigation, a security analyst notices the following:

- All users share workstations throughout the day.
- Endpoint protection was disabled on several workstations throughout the network.
- Travel times on logins from the affected users are impossible.
- Sensitive data is being uploaded to external sites.
- All user account passwords were forced to be reset and the issue continued.

Which of the following attacks is being used to compromise the user accounts?

A. Brute-force
B. Keylogger
C. Dictionary
D. Rainbow

**Correct Answer:** B

**QUESTION 393**
Which of the following would be the BEST resource for a software developer who is looking to improve secure coding practices for web applications?

A. OWASP
B. Vulnerability scan results
C. NIST CSF
D. Third-party libraries

**Correct Answer:** A

**QUESTION 394**
Law enforcement officials sent a company a notification that states electronically stored information and paper documents cannot be destroyed. Which of the following explains this process?

A. Data breach notification
B. Accountability
C. Legal hold
D. Chain of custody

**Correct Answer:** C

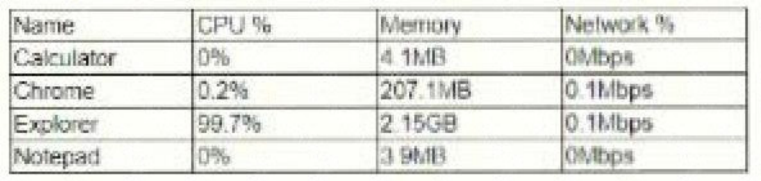
**QUESTION 395**
After gaining access to a dual-homed (i.e.. wired and wireless) multifunction device by exploiting a vulnerability in the device's firmware, a penetration tester then gains shell access on another networked asset. This technique is an example of:

A. privilege escalation
B. footprinting
C. persistence
D. pivoting.

**Correct Answer:** A

**QUESTION 396**
A user reports trouble using a corporate laptop. The laptop freezes and responds slowly when writing documents and the mouse pointer occasional disappears.

The task list shows the following results



| Name | CPU % | Memory | Network % |
|---|---|---|---|
| Calculator | 0% | 4 1MB | 0Mbps |
| Chrome | 0.2% | 207.1MB | 0.1Mbps |
| Explorer | 99.7% | 2 15GB | 0.1Mbps |
| Notepad | 0% | 3 9MB | 0Mbps |

Which of the following is MOST likely the issue?

A. RAT
B. PUP
C. Spyware
D. Keylogger

**Correct Answer:** A

**QUESTION 397**
A cloud service provider has created an environment where customers can connect existing local networks to the cloud lor additional computing resources and block internal HR applications from reaching the cloud. Which of the following cloud models is being used?

A. Public
B. Community

C. Hybrid
D. Private

**Correct Answer:** C

**QUESTION 398**
Which of the following control types is focused primarily on reducing risk before an incident occurs?

A. Preventive
B. Deterrent
C. Corrective
D. Detective

**Correct Answer:** A

**QUESTION 399**
A new security engineer has started hardening systems. One of the hardening techniques the engineer is using involves disabling remote logins to the NAS. Users are now reporting the inability to use SCP to transfer files to the NAS, even though the data is still viewable from the users PCs. Which of the following is the MOST likely cause of this issue?

A. TFTP was disabled on the local hosts
B. SSH was turned off instead of modifying the configuration file
C. Remote login was disabled in the networkd.config instead of using the sshd.conf
D. Network services are no longer running on the NAS

**Correct Answer:** C

**QUESTION 400**
A penetration tester gains access to the network by exploiting a vulnerability on a public-facing web server. Which of the following techniques will the tester most likely perform NEXT?

A. Gather more information about the target through passive reconnaissance
B. Establish rules of engagement before proceeding
C. Create a user account to maintain persistence
D. Move laterally throughout the network to search for sensitive information

**Correct Answer:** C

**QUESTION 401**
A security engineer obtained the following output from a threat intelligence source that recently performed an attack on the company's server: