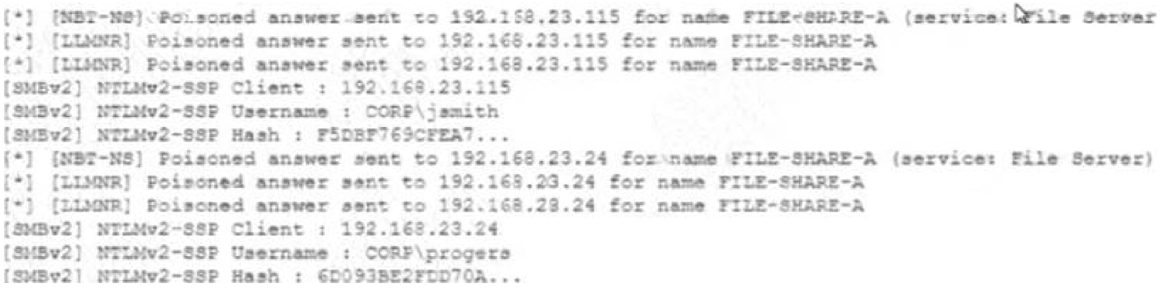
A new on-premises application server was recently installed on the network. Remote access to the server was enabled for vendor support on required ports, but recent security reports show large amounts of data are being sent to various unauthorized networks through those ports. Which of the following configuration changes must be implemented to resolve this security issue while still allowing remote vendor access?

A. Apply a firewall application server rule.
B. Whitelist the application server.
C. Sandbox the application server.
D. Enable port security.
E. Block the unauthorized networks.

Correct Answer: B

QUESTION 49
While conducting a network infrastructure review, a security analyst discovers a laptop that is plugged into a core switch and hidden behind a desk.

The analyst sees the following on the laptop's screen:



```
[*] [NBT-NS] Poisoned answer sent to 192.168.23.115 for name FILE-SHARE-A (service: File Server
[*] [LLMNR] Poisoned answer sent to 192.168.23.115 for name FILE-SHARE-A
[*] [LLMNR] Poisoned answer sent to 192.168.23.115 for name FILE-SHARE-A
[SMBv2] NTLMv2-SSP Client : 192.168.23.115
[SMBv2] NTLMv2-SSP Username : CORP\jsmith
[SMBv2] NTLMv2-SSP Hash : F5DBF769CFEA7...
[*] [NBT-NS] Poisoned answer sent to 192.168.23.24 for name FILE-SHARE-A (service: File Server)
[*] [LLMNR] Poisoned answer sent to 192.168.23.24 for name FILE-SHARE-A
[*] [LLMNR] Poisoned answer sent to 192.168.23.24 for name FILE-SHARE-A
[SMBv2] NTLMv2-SSP Client : 192.168.23.24
[SMBv2] NTLMv2-SSP Username : CORP\progers
[SMBv2] NTLMv2-SSP Hash : 6D093BE2FDD70A...
```

Which of the following is the BEST action for the security analyst to take?

A. Initiate a scan of devices on the network to find password-cracking tools.
B. Disconnect the laptop and ask the users jsmith and progers to log out.
C. Force all users in the domain to change their passwords at the next login.
D. Take the FILE-SHARE-A server offline and scan it for viruses.

Correct Answer: D

QUESTION 50
Which of the following BEST articulates the benefit of leveraging SCAP in an organization's cybersecurity analysis toolset?

A. It automatically performs remedial configuration changes to enterprise security services
B. It enables standard checklist and vulnerability analysis expressions for automation
C. It establishes a continuous integration environment for software development operations
D. It provides validation of suspected system vulnerabilities through workflow orchestration

Correct Answer: B

QUESTION 51
A development team uses open-source software and follows an Agile methodology with two-week sprints. Last month, the security team filed a bug for an insecure version of a common library. The DevOps team updated the library on the server, and then the security team rescanned the server to verify it was no longer vulnerable. This month, the security team found the same vulnerability on the server. Which of the following should be done to correct the cause of the vulnerability?

A. Deploy a WAF in front of the application.
B. Implement a software repository management tool.
C. Install a HIPS on the server.
D. Instruct the developers to use input validation in the code.

Correct Answer: B

QUESTION 52
Which of the following roles is ultimately responsible for determining the classification levels assigned to specific data sets?

A. Data custodian
B. Data owner
C. Data processor
D. Senior management

Correct Answer: B

QUESTION 53
A security architect is reviewing the options for performing input validation on incoming web form submissions. Which of the following should the architect as the MOST secure and manageable option?

A. Client-side whitelisting
B. Server-side whitelisting
C. Server-side blacklisting
D. Client-side blacklisting

Correct Answer: B

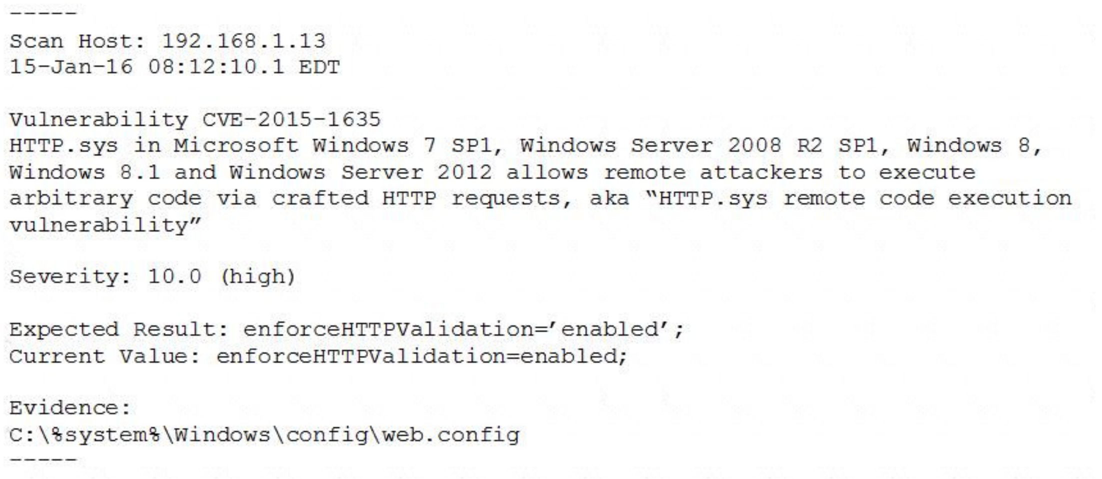
QUESTION 54
A product manager is working with an analyst to design a new application that will perform as a data analytics platform and will be accessible via a web browser. The product manager suggests using a PaaS provider to host the application. Which of the following is a security concern when using a PaaS solution?

A. The use of infrastructure-as-code capabilities leads to an increased attack surface.
B. Patching the underlying application server becomes the responsibility of the client.
C. The application is unable to use encryption at the database level.
D. Insecure application programming interfaces can lead to data compromise.

Correct Answer: D

QUESTION 55

A system's authority to operate (ATO) is set to expire in four days. Because of other activities and limited staffing, the organization has neglected to start reauthentication activities until now. The cybersecurity group just performed a vulnerability scan with the partial set of results shown below:



```
-----
Scan Host: 192.168.1.13
15-Jan-16 08:12:10.1 EDT

Vulnerability CVE-2015-1635
HTTP.sys in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8,
Windows 8.1 and Windows Server 2012 allows remote attackers to execute
arbitrary code via crafted HTTP requests, aka “HTTP.sys remote code execution
vulnerability”

Severity: 10.0 (high)

Expected Result: enforceHTTPValidation=’enabled’;
Current Value: enforceHTTPValidation=enabled;

Evidence:
C:\%system%\Windows\config\web.config
-----
```

Based on the scenario and the output from the vulnerability scan, which of the following should the security team do with this finding?

A. Remediate by going to the web config file, searching for the enforce HTTP validation setting, and manually updating to the correct setting.
B. Accept this risk for now because this is a "high" severity, but testing will require more than the four days available, and the system ATO needs to be competed.
C. Ignore it. This is false positive, and the organization needs to focus its efforts on other findings.
D. Ensure HTTP validation is enabled by rebooting the server.

Correct Answer: A

QUESTION 56

Which of the following technologies can be used to house the entropy keys for disk encryption on desktops and laptops?

A. Self-encrypting drive
B. Bus encryption
C. TPM
D. HSM

Correct Answer: A

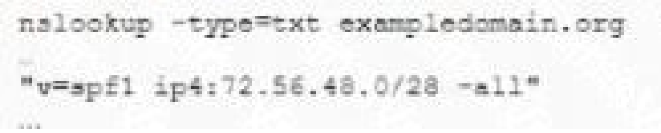
QUESTION 57

Which of the following technologies can be used to store digital certificates and is typically used in high-security implementations where integrity is paramount?

A. HSM
B. eFuse
C. UEFI
D. Self-encrypting drive

Correct Answer: A

QUESTION 58
The help desk noticed a security analyst that emails from a new email server are not being sent out. The new email server was recently added to the existing ones. The analyst runs the following command on the new server.



```
nslookup -type=txt exampledomain.org
...
"v=spf1 ip4:72.56.48.0/28 -all"
...
```

Given the output, which of the following should the security analyst check NEXT?

A. The DNS name of the new email server
B. The version of SPF that is being used
C. The IP address of the new email server
D. The DMARC policy

Correct Answer: A

QUESTION 59
A security analyst reviews the latest reports from the company's vulnerability scanner and discovers the following:

21213 HTTP TRACE / TRACK Methods Allowed The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.
64912 Apache 4.2.x < 4.2.24 XSS Vulnerabilities The web server responded with a popup <script>alert ('123') ; </script> when this was entered in the "txtDescription" field of \providestatus.php
53523 Apache 4.2.x < 4.2.24 mod_status Vulnerabilities The 'mod_status' module contains a race condition that can be triggered by a specially crafted packet to cause denial of service.
73825 SSL Weak Block Size Cipher Suites Supported The use of a block cipher with 32-bit blocks enable man-in-the-middle attackers with sufficient resources to exploit this vulnerability.

Which of the following changes should the analyst recommend FIRST?

A. Configuring SSL ciphers to use different encryption blocks
B. Programming changes to encode output
C. Updating the 'mod_status' module
D. Disabling HTTP connection debugging commands

Correct Answer: C

QUESTION 60
A malicious artifact was collected during an incident response procedure. A security analyst is unable to run it in a sandbox to understand its features and method of operation. Which of the following procedures is the BEST approach to perform a further analysis of the malware's capabilities?

A. Reverse engineering
B. Dynamic analysis
C. Strings extraction
D. Static analysis

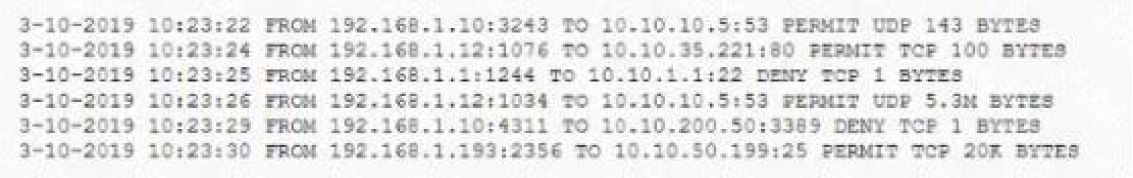
Correct Answer: D

QUESTION 61
Which of the following BEST describes the primary role ol a risk assessment as it relates to compliance with risk-based frameworks?

A. It demonstrates the organization's mitigation of risks associated with internal threats.
B. It serves as the basis for control selection.
C. It prescribes technical control requirements.
D. It is an input to the business impact assessment.

Correct Answer: A

QUESTION 62
After a breach involving the exfiltration of a large amount of sensitive data a security analyst is reviewing the following firewall logs to determine how the breach occurred:



```
3-10-2019 10:23:22 FROM 192.168.1.10:3243 TO 10.10.10.5:53 PERMIT UDP 143 BYTES
3-10-2019 10:23:24 FROM 192.168.1.12:1076 TO 10.10.35.221:80 PERMIT TCP 100 BYTES
3-10-2019 10:23:25 FROM 192.168.1.1:1244 TO 10.10.1.1:22 DENY TCP 1 BYTES
3-10-2019 10:23:26 FROM 192.168.1.12:1034 TO 10.10.10.5:53 PERMIT UDP 5.3M BYTES
3-10-2019 10:23:29 FROM 192.168.1.10:4311 TO 10.10.200.50:3389 DENY TCP 1 BYTES
3-10-2019 10:23:30 FROM 192.168.1.193:2356 TO 10.10.50.199:25 PERMIT TCP 20K BYTES
```

Which of the following IP addresses does the analyst need to investigate further?

A. 192.168.1.1
B. 192.168.1.10
C. 192.168.1.12
D. 192.168.1.193

Correct Answer: C

QUESTION 63
A user receives a potentially malicious email that contains spelling errors and a PDF document. A