DUMPSBOSS.

CompTIA CySA+ Certification Exam (CS0-002)

CompTIA CS0-002

Version Demo

Total Demo Questions: 15

Total Premium Questions: 275

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

Which of me following are reasons why consumer IoT devices should be avoided in an enterprise environment? (Select TWO)

A. Message queuing telemetry transport does not support encryption.

B. The devices may have weak or known passwords.

C. The devices may cause a dramatic Increase in wireless network traffic.

D. The devices may utilize unsecure network protocols.

E. Multiple devices may interface with the functions of other IoT devices.

F. The devices are not compatible with TLS 12.

ANSWER: B D

Explanation:

Consumer IoT devices are devices that connect to the internet and provide various functions or services for personal or home use, such as smart speakers, cameras, thermostats, etc. Consumer IoT devices should be avoided in an enterprise environment because they may pose security risks or challenges for the organization's network and data. Some of the reasons why consumer IoT devices should be avoided are:

Reference: Why Consumer IoT Devices Should Be Avoided In Enterprise Environments | Security Boulevard

QUESTION NO: 2

An online gaming company was impacted by a ransomware attack. An employee opened an attachment that was received via an SMS attack on a company-issue firewall. Which following actions would help during the forensic analysis of the mobile device? (Select TWO).

A. Resetting the phone to factory settings

B. Rebooting the phone and installing the latest security updates

C. Documenting the respective chain of custody

D. Uninstalling any potentially unwanted programs

E. Performing a memory dump of the mobile device for analysis

F. Unlocking the device by blowing the eFuse

ANSWER: C E

Explanation:

Documenting the respective chain of custody and performing a memory dump of the mobile device for analysis would help during the forensic analysis of the mobile device. The chain of custody is a record of who handled the evidence, when, where, how, and why. The chain of custody helps to preserve the integrity and admissibility of the evidence by preventing tampering, alteration, or loss1. A memory dump is a process of capturing and storing the contents of the device's memory (RAM) for analysis. A memory dump can help to recover volatile data that may be lost when the device is powered off or rebooted, such as running processes, network connections, encryption keys, or malware traces2.

QUESTION NO: 3

Which of the following are considered PII by themselves? (Select TWO).

A. Government ID

B. Job title

C. Employment start date

D. Birth certificate

E. Employer address

F. Mother's maiden name

ANSWER: A D

Explanation:

PII (Personally Identifiable Information) is any information that can be used to identify, contact, or locate a specific individual, either by itself or when combined with other information1. PII by itself is information that can uniquely identify an individual without any additional information. Examples of PII by itself are:

Other examples of PII by itself are biometric data, DNA profile, fingerprints, etc. Examples of information that are not PII by themselves are:

Other examples of information that are not PII by themselves are gender, race, ethnicity, age, etc.

Reference: 1: https://www.techopedia.com/definition/23889/personally-identifiable-information-pii

QUESTION NO: 4

Which of the following BEST explains the function of trusted firmware updates as they relate to hardware assurance?

A. Trusted firmware updates provide organizations with development, compilation, remote access, and customization for embedded devices.

B. Trusted firmware updates provide organizations with security specifications, open-source libraries, and custom toots for embedded devices.

C. Trusted firmware updates provide organizations with remote code execution, distribution, maintenance, and extended warranties for embedded devices

D. Trusted firmware updates provide organizations with secure code signing, distribution, installation. and attestation for embedded devices.

ANSWER: D

Explanation:

The CySA+ exam outline calls out “trusted firmware updates,” but trusted firmware itself is more commonly described as part of trusted execution environments (TEEs). Trusted firmware is signed by a chip vendor or other trusted party, and then used to access keys to help control access to hardware. TEEs like those used by ARM processors leverage these technologies to protect the hardware by preventing unsigned code from using privileged features."

Trusted firmware updates provide organizations with secure code signing, distribution, installation, and attestation for embedded devices. Embedded devices are devices that have a dedicated function and are part of a larger system or network, such as routers, cameras, sensors, etc. Embedded devices often run on firmware, which is a type of software that controls the device’s hardware and functionality. Firmware updates are essential for improving the performance, security, and reliability of embedded devices. However, firmware updates also pose risks of introducing vulnerabilities or malware into the devices if they are not properly secured. Trusted firmware updates are firmware updates that use cryptographic techniques to ensure the integrity, authenticity, and confidentiality of the firmware code and data. Trusted firmware updates typically involve four steps1:

Trusted firmware updates provide organizations with several benefits for hardware assurance, such as2:

Trusted firmware updates do not provide organizations with development, compilation, remote access, or customization for embedded devices (A), as these are software engineering tasks that are not directly related to firmware security. Trusted firmware updates do not provide organizations with security specifications, open-source libraries, or custom tools for embedded devices (B), as these are software resources that are not directly related to firmware security. Trusted firmware updates do not provide organizations with remote code execution, distribution, maintenance, or extended warranties for embedded devices ©, as these are software features or services that are not directly related to firmware security.

References: 1: https://www.techopedia.com/definition/24771/technical-controls 2: https://www.techopedia.com/definition/25888/security-development-lifecycle-sdl

QUESTION NO: 5

The Chief information Officer of a large cloud software vendor reports that many employees are falling victim to phishing emails because they appear to come from other employees. Which of the following would BEST prevent this issue

A. Induce digital signatures on messages originating within the company.

B. Require users authenticate to the SMTP server

C. Implement DKIM to perform authentication that will prevent this Issue.

D. Set up an email analysis solution that looks for known malicious links within the email.

ANSWER: C

Explanation:

DKIM, or DomainKeys Identified Mail, is an email authentication method that uses a digital signature to let the receiver of an email know that the message was sent and authorized by the owner of a domain1 DKIM helps prevent phishing emails that spoof or impersonate other domains by verifying the identity and integrity of the sender. DKIM works by adding a DKIM signature header to each outgoing email message, which contains a hash value of selected parts of the message and the domain name of the sender. The sender’s domain also publishes a public key in its DNS records, which can be used by the receiver to decrypt the DKIM signature and compare it with its own hash value of the message. If they match, it means that the message was not altered in transit and that it came from the claimed domain.

Reference: 1 What Is DKIM? - How It Works, Definition & More | Proofpoint US

QUESTION NO: 6

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.

ANSWER: D

Explanation:

Insecure application programming interfaces (APIs) can lead to data compromise when using a PaaS solution. APIs are interfaces that allow applications to communicate with each other and with the underlying platform. APIs can expose sensitive data or functionality to unauthorized or malicious users if they are not properly designed, implemented, or secured. Insecure APIs can result in data breaches, denial of service, unauthorized access, or code injection .

Reference: https://spot.io/resources/cloud-security/paas-security-threats-solutions-and-best-practices/

QUESTION NO: 7

A digital forensics investigator works from duplicate images to preserve the integrity of the original evidence. Which of the following types of media are most volatile and should be preserved? (Select two).

A. Memory cache

B. Registry file

C. SSD storage

D. Temporary filesystems

E. Packet decoding

F. Swap volume

ANSWER: A F

Explanation:

Memory cache and swap volume are types of media that are most volatile and should be preserved during a digital forensics investigation. Volatile media are those that store data temporarily and lose their contents when the power is turned off or interrupted. Memory cache is a small and fast memory that stores frequently used data or instructions for faster access by

the processor. Swap volume is a part of the hard disk that is used as an extension of the memory when the memory is full or low .

Reference: https://www.techopedia.com/definition/10339/memory-dump

QUESTION NO: 8

During a company's most recent incident, a vulnerability in custom software was exploited on an externally facing server by an APT. The lessons-learned report noted the following:

• The development team used a new software language that was not supported by the security team's automated assessment tools.

• During the deployment, the security assessment team was unfamiliar with the new language and struggled to evaluate the software during advanced testing. Therefore, the vulnerability was not detected.

• The current IPS did not have effective signatures and policies in place to detect and prevent runtime attacks on the new application.

To allow this new technology to be deployed securely going forward, which of the following will BEST address these findings? (Choose two.)

A. Train the security assessment team to evaluate the new language and verify that best practices for secure coding have been followed

B. Work with the automated assessment-tool vendor to add support for the new language so these vulnerabilities are discovered automatically

C. Contact the human resources department to hire new security team members who are already familiar with the new language

D. Run the software on isolated systems so when they are compromised, the attacker cannot pivot to adjacent systems

E. Instruct only the development team to document the remediation steps for this vulnerability

F. Outsource development and hosting of the applications in the new language to a third-party vendor so the risk is transferred to that provider

ANSWER: A B

Explanation:

The solution will address the findings that the development team used a new software language that was not supported by the security team's automated assessment tools and the security assessment team was unfamiliar with the new language and struggled to evaluate the software during advanced testing. The training of the security assessment team and working with the automated assessment-tool vendor to add support for the new language will ensure that future deployments of the new technology are secure and the vulnerabilities are detected and prevented.

QUESTION NO: 9

A software developer is correcting the error-handling capabilities of an application following the initial coding of the fix. Which of the following would the software developer MOST likely performed to validate the code poor to pushing it to production?

A. Web-application vulnerability scan

B. Static analysis

C. Packet inspection

D. Penetration test

ANSWER: B

Explanation:

Static analysis is a method of analyzing software code without executing it, by using tools or techniques that check for syntax errors, logic errors, vulnerabilities, coding standards, and other quality issues. Static analysis can help software developers to correct the error-handling capabilities of an application before pushing it to production, as it can detect potential errors and bugs at an early stage of development. A web-application vulnerability scan (A) is a method of testing web applications for security flaws by simulating attacks and analyzing responses. It can be useful for finding vulnerabilities in web applications, but not for validating the error-handling capabilities of an application. A packet inspection © is a method of monitoring network traffic by examining the data packets that are sent and received over a network. It can be useful for detecting malicious or unauthorized activity on a network, but not for validating the error-handling capabilities of an application. A penetration test (D) is a method of evaluating the security of a system or network by simulating real-world attacks and exploiting vulnerabilities. It can be useful for assessing the overall security posture of a system or network, but not for validating the error-handling capabilities of an application.

References: : https://www.techopedia.com/definition/14436/static-analysis : https://www.techopedia.com/definition/4160/web-application-security-scanner-was : https://www.techopedia.com/definition/4010/packet-inspection : https://www.techopedia.com/definition/13493/penetration-testing

QUESTION NO: 10

A manufacturing company uses a third-party service provider for Tier 1 security support. One of the requirements is that the provider must only source talent from its own country due to geopolitical and national security interests. Which of the following can the manufacturing company implement to ensure the third-party service provider meets this requirement?

A. Implement a secure supply chain program with governance.

B. Implement blacklisting lor IP addresses from outside the county.

C. Implement strong authentication controls for at contractors.

D. Implement user behavior analytics tor key staff members.

ANSWER: A

Explanation:

A secure supply chain program is a set of processes and practices that aim to protect the supply chain from various risks, such as cyberattacks, data breaches, fraud, theft, sabotage, or natural disasters1. A secure supply chain program can help to ensure the integrity, availability, and confidentiality of the products, services, data, and systems involved in the supply chain. A secure supply chain program with governance means that there are clear roles, responsibilities, policies, procedures, and controls for managing the security of the supply chain. This can help to monitor and enforce the compliance of the third-party service provider with the requirement to source talent from its own country. A secure supply chain program with governance can also help to identify and mitigate any potential threats or vulnerabilities in the supply chain. Implementing blacklisting for IP addresses from outside the country (B) may not be sufficient or effective, as IP addresses

can be spoofed or bypassed by attackers. Implementing strong authentication controls for all contractors © may not be relevant or adequate, as authentication controls do not prevent the sourcing of talent from other countries. Implementing user behavior analytics for key staff members (D) may not be applicable or useful, as user behavior analytics do not verify the origin or location of the talent.

Reference: 1: https://www.ibm.com/blog/what-is-supply-chain-security/

QUESTION NO: 11

A user reports a malware alert to the help desk. A technician verities the alert, determines the workstation is classified as a low-severity device, and uses network controls to block access. The technician then assigns the ticket to a security analyst who will complete the eradication and recovery processes. Which of the following should the security analyst do next?

A. Document the procedures and walk through the incident training guide.

B. Reverse engineer the malware to determine its purpose and risk to the organization.

C. Sanitize the workstation and verify countermeasures are restored.

D. Isolate the workstation and issue a new computer to the user.

ANSWER: C

Explanation:

Sanitizing the workstation and verifying countermeasures are restored are part of the eradication and recovery processes that the security analyst should perform next. Eradication is the process of removing malware or other threats from the affected systems, while recovery is the process of restoring normal operations and functionality to the affected systems. Sanitizing the workstation can involve deleting or wiping any malicious files or programs, while verifying countermeasures are restored can involve checking and updating any security controls or settings that may have been compromised .

Reference: https://www.cynet.com/incident-response/incident-response-sans-the-6-steps-in-depth/

QUESTION NO: 12

A company's domain has been spooled in numerous phishing campaigns. An analyst needs to determine the company is a victim of domain spoofing, despite having a DMARC record that should tell mailbox providers to ignore any email that fails DMARC upon review of the record, the analyst finds the following:

```
v=DMARC1; p=none; fo=0; rua=mailto:security@company.com; ruf=mailto:security@company.com; adkim=r; rf=afrf; ri=86400;
```

Which of the following BEST explains the reason why the company's requirements are not being processed correctly by mailbox providers?

A. The DMARC record's DKIM alignment tag Is incorrectly configured.

B. The DMARC record's policy tag is incorrectly configured.

C. The DMARC record does not have an SPF alignment tag.

D. The DMARC record's version tag is set to DMARC1 instead of the current version, which is DMARC3.

ANSWER: B

Explanation:

The DMARC record's policy tag is incorrectly configured and explains why the company's requirements are not being processed correctly by mailbox providers. The policy tag (p) specifies how mailbox providers should handle messages from the domain that fail DMARC checks. The possible values for the policy tag are none, quarantine, or reject1. None means that no action is taken on failed messages and only reports are sent. Quarantine means that failed messages are treated as suspicious and may be filtered or marked as spam. Reject means that failed messages are rejected and not delivered. In this case, the company's DMARC record has a policy tag value of none, which means that mailbox providers will not ignore any email that fails DMARC as required by the company. Instead, mailbox providers will deliver all messages from the domain regardless of their DMARC status and only send reports to the company. To fix this issue, the company should change its policy tag value to reject, which means that mailbox providers will reject and ignore any email that fails DMARC as required by the company. The DMARC record's DKIM alignment tag (A) is not incorrectly configured and does not explain why the company's requirements are not being processed correctly by mailbox providers. The DKIM alignment tag (adkim) specifies how strictly mailbox providers should match DKIM identifiers with From domain identifiers2. The possible values for DKIM alignment tag are s or r. S means strict alignment, which means that DKIM identifiers must exactly match From domain identifiers. R means relaxed alignment, which means that DKIM identifiers must match From domain identifiers at an organizational level (e.g., subdomain.example.com and example.com are considered aligned). In this case, the company's DMARC record has a DKIM alignment tag value of r, which means that mailbox providers will use relaxed alignment for DKIM verification.

QUESTION NO: 13

Which of the following APT adversary archetypes represent non-nation-state threat actors? (Select TWO)

A. Kitten

B. Panda

C. Tiger

D. Jackal

E. Bear

F. Spider

ANSWER: A D

Explanation:

Kitten and Jackal are two APT (Advanced Persistent Threat) adversary archetypes that represent non-nation-state threat actors. APT adversary archetypes are categories of threat actors that share common characteristics, such as motivation, objectives, capabilities, or tactics. APT adversary archetypes can help security analysts understand and prioritize the threats they face2. Kitten is a term used to describe Iranian-based threat actors that are typically not backed by the Iranian government. They are motivated by ideological or religious beliefs and target political or regional adversaries3. Jackal is a term used to describe cybercriminal groups that operate as mercenaries or proxies for other threat actors. They are motivated by financial gain and target various sectors and regions.

QUESTION NO: 14

A security manager has asked an analyst to provide feedback on the results of a penetration test. After reviewing the results, the manager requests

information regarding the possible exploitation of vulnerabilities. Which of the following information data points would be MOST useful for the analyst

to provide to the security manager, who would then communicate the risk factors to the senior management team? (Select TWO).

A. Probability

B. Adversary capability

C. Attack vector

D. Impact

E. Classification

F. Indicators of compromise

ANSWER: B D

Explanation:

According to the CompTIA CySA+ (CS0-002) best practices, the most useful information data points to provide to the security manager for communicating the risk factors to senior management are the impact and adversary capability. The impact refers to the potential consequences of a successful attack or exploitation of a vulnerability, such as data loss or system compromise. The adversary capability refers to the ability of an attacker to exploit a vulnerability, including their technical expertise and resources. Together, these data points help to provide a complete picture of the risk associated with a vulnerability, and allow senior management to make informed decisions regarding risk mitigation and remediation. The other data points, such as probability, attack vector, classification, and indicators of compromise, can also be valuable, but the impact and adversary capability are considered the most critical for prioritizing risk mitigation efforts.

QUESTION NO: 15 - (HOTSPOT)

A security analyst performs various types of vulnerability scans. Review the vulnerability scan results to determine the type of scan that was executed and if a false positive occurred for each device.

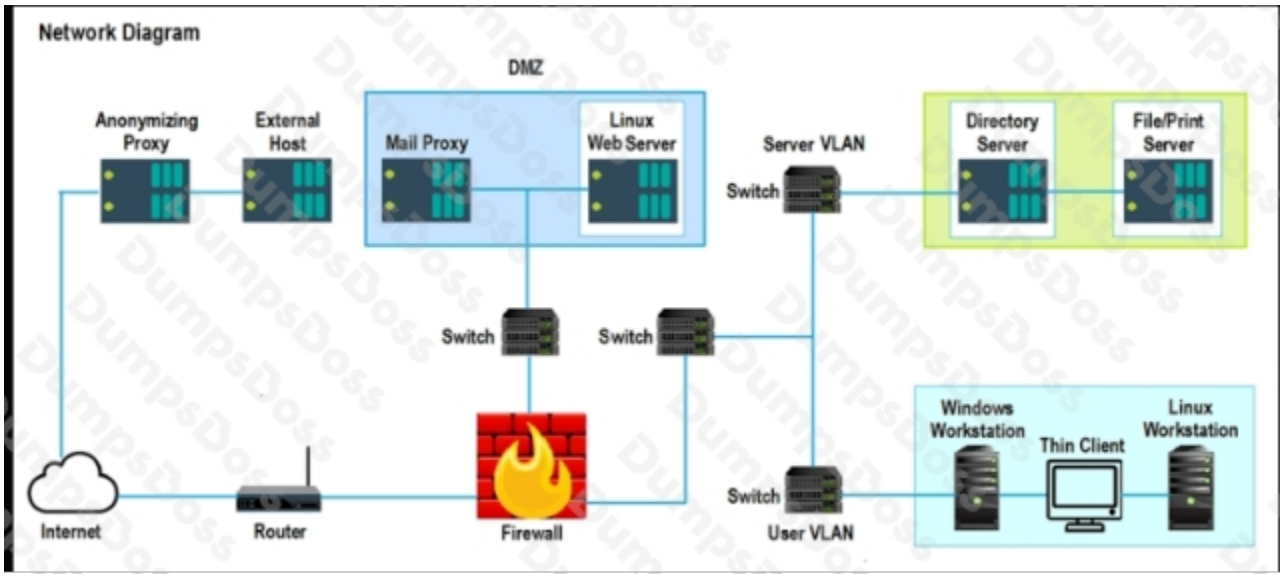
Instructions:

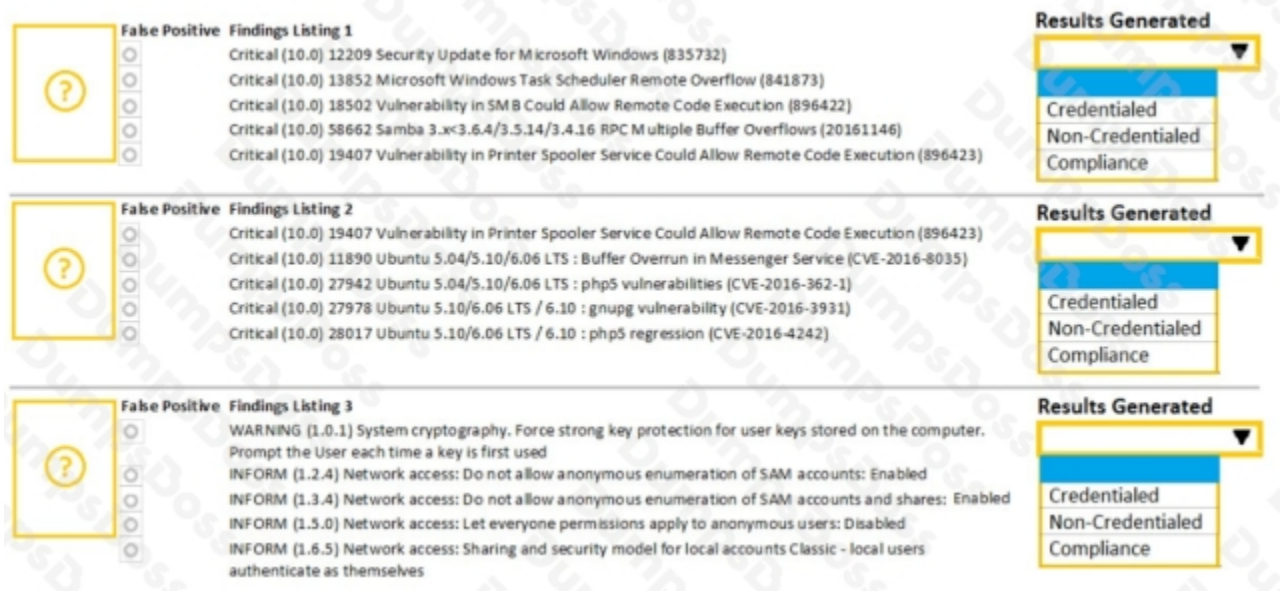
Select the Results Generated drop-down option to determine if the results were generated from a credentialed scan, non-credentialed scan, or a compliance scan.

For ONLY the credentialed and non-credentialed scans, evaluate the results for false positives and check the findings that display false positives. NOTE: If you would like to uncheck an option that is currently selected, click on the option a second time.

Lastly, based on the vulnerability scan results, identify the type of Server by dragging the Server to the results.

The Linux Web Server, File-Print Server and Directory Server are draggable.If at any time you would like to bring back the initial state of the simulation, please select the Reset All button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.


Network Diagram
DMZ
Anonymizing Proxy
External Host
Mail Proxy
Linux Web Server
Server VLAN
Switch
Directory Server
File/Print Server
Switch
Switch
Windows Workstation
Thin Client
Linux Workstation
Internet
Router
Firewall
Switch
User VLAN


False Positive
Findings Listing 1
Critical (10.0) 12209 Security Update for Microsoft Windows (835732)
Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow (841873)
Critical (10.0) 18502 Vulnerability in SMB Could Allow Remote Code Execution (896422)
Critical (10.0) 58662 Samba 3.x<3.6.4/3.5.14/3.4.16 RPC Multiple Buffer Overflows (20161146)
Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)
Results Generated
Credentialed
Non-Credentialed
Compliance
False Positive
Findings Listing 2
Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)
Critical (10.0) 11890 Ubuntu 5.04/5.10/6.06 LTS : Buffer Overrun in Messenger Service (CVE-2016-8035)
Critical (10.0) 27942 Ubuntu 5.04/5.10/6.06 LTS : php5 vulnerabilities (CVE-2016-362-1)
Critical (10.0) 27978 Ubuntu 5.10/6.06 LTS / 6.10 : gnupg vulnerability (CVE-2016-3931)
Critical (10.0) 28017 Ubuntu 5.10/6.06 LTS / 6.10 : php5 regression (CVE-2016-4242)
Results Generated
Credentialed
Non-Credentialed
Compliance
False Positive
Findings Listing 3
WARNING (1.0.1) System cryptography. Force strong key protection for user keys stored on the computer. Prompt the User each time a key is first used
INFORM (1.2.4) Network access: Do not allow anonymous enumeration of SAM accounts: Enabled
INFORM (1.3.4) Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled
INFORM (1.5.0) Network access: Let everyone permissions apply to anonymous users: Disabled
INFORM (1.6.5) Network access: Sharing and security model for local accounts Classic - local users authenticate as themselves
Results Generated
Credentialed
Non-Credentialed
Compliance

ANSWER:


False Positive
Findings Listing 1
Critical (10.0) 12209 Security Update for Microsoft Windows (835732)
Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow (841873)
Critical (10.0) 18502 Vulnerability in SMB Could Allow Remote Code Execution (896422)
Critical (10.0) 58662 Samba 3.x < 3.6.4 / 3.5.14 / 3.4.16 RPC Multiple Buffer Overflows (20161146)
Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)
Results Generated
Credentialed
False Positive
Findings Listing 2
Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)
Critical (9.3) 08955 Ubuntu 5.04 / 5.10 / 6.06 LTS : Buffer overrun in enscript before 1.6.4 (CVE-2008-4306)
Critical (10.0) 27942 Ubuntu 5.04 / 5.10 / 6.06 LTS : php5 vulnerabilities (CVE-2016-362-1)
Critical (10.0) 27978 Ubuntu 5.10 / 6.06 LTS / 6.10 : gnupg vulnerability (CVE-2016-3931)
Critical (10.0) 28017 Ubuntu 5.10 / 6.06 LTS / 6.10 : php5 regression (CVE-2016-4242)
Results Generated
Non-Credentialed
False Positive
Findings Listing 3
WARNING (1.0.1) System cryptography: Force strong key protection for user keys stored on the computer: Prompt the User each time a key is first used
INFORM (1.2.4) Network access: Do not allow anonymous enumeration of SAM accounts: Enabled
INFORM (1.3.4) Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled
INFORM (1.5.0) Network access: Let Everyone permissions apply to anonymous users: Disabled
INFORM (1.6.5) Network access: Sharing and security model for local accounts: Classic - local users authenticate as themselves
Results Generated
Compliance