IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **RC0-C02**

Title : CompTIA Advanced Security Practitioner (CASP) Recertification Exam for Continuing Education

Version : DEMO

1.An administrator wants to enable policy based flexible mandatory access controls on an open source OS to prevent abnormal application modifications or executions. Which of the following would BEST accomplish this?
A. Access control lists
B. SELinux
C. IPtables firewall
D. HIPS
Answer: B
Explanation:
The most common open source operating system is LINUX.
Security-Enhanced Linux (SELinux) was created by the United States National Security Agency (NSA) and is a Linux kernel security module that provides a mechanism for supporting access control security policies, including United States Department of Defense-style mandatory access controls (MAC).
NSA Security-enhanced Linux is a set of patches to the Linux kernel and some utilities to incorporate a strong, flexible mandatory access control (MAC) architecture into the major subsystems of the kernel. It provides an enhanced mechanism to enforce the separation of information based on confidentiality and integrity requirements, which allows threats of tampering and bypassing of application security mechanisms to be addressed and enables the confinement of damage that can be caused by malicious or flawed applications.
Incorrect Answers:
A: An access control list (ACL) is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects. ACLs do not enable policy based flexible mandatory access controls to prevent abnormal application modifications or executions.
C: A firewall is used to control data leaving a network or entering a network based on source and destination IP address and port numbers. IP Tables is a Linux firewall. However, it does not enable policy based flexible mandatory access controls to prevent abnormal application modifications or executions.
D: Host-based intrusion prevention system (HIPS) is an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host. It does not enable policy based flexible mandatory access controls to prevent abnormal application modifications or executions.
References:
https://en.wikipedia.org/wiki/Security-Enhanced_Linux

2.Company ABC's SAN is nearing capacity, and will cause costly downtimes if servers run out disk space. Which of the following is a more cost effective alternative to buying a new SAN?
A. Enable multipath to increase availability
B. Enable deduplication on the storage pools
C. Implement snapshots to reduce virtual disk size
D. Implement replication to offsite datacenter
Answer: B
Explanation:
Storage-based data deduplication reduces the amount of storage needed for a given set of files. It is most effective in applications where many copies of very similar or even identical data are stored on a single disk.

It is common for multiple copies of files to exist on a SAN. By eliminating (deduplicating) repeated copies of the files, we can reduce the disk space used on the existing SAN. This solution is a cost effective alternative to buying a new SAN.
Incorrect Answers:
A: Multipathing enables multiple links to transfer the data to and from the SAN. This improves performance and link redundancy. However, it has no effect on the amount of data on the SAN.
C: Snapshots would not reduce the amount of data stored on the SAN.
D: Replicating the data on the SAN to an offsite datacenter will not reduce the amount of data stored on the SAN. It would just create another copy of the data on the SAN in the offsite datacenter.
References:
https://en.wikipedia.org/wiki/Data_deduplication

3.A systems administrator establishes a CIFS share on a UNIX device to share data to Windows systems. The security authentication on the Windows domain is set to the highest level. Windows users are stating that they cannot authenticate to the UNIX share. Which of the following settings on the UNIX server would correct this problem?
A. Refuse LM and only accept NTLMv2
B. Accept only LM
C. Refuse NTLMv2 and accept LM
D. Accept only NTLM
Answer: A
Explanation:
In a Windows network, NT LAN Manager (NTLM) is a suite of Microsoft security protocols that provides authentication, integrity, and confidentiality to users. NTLM is the successor to the authentication protocol in Microsoft LAN Manager (LANMAN or LM), an older Microsoft product, and attempts to provide backwards compatibility with LANMAN. NTLM version 2 (NTLMv2), which was introduced in Windows NT 4.0 SP4 (and natively supported in Windows 2000), enhances NTLM security by hardening the protocol against many spoofing attacks, and adding the ability for a server to authenticate to the client.
This question states that the security authentication on the Windows domain is set to the highest level. This will be NTLMv2. Therefore, the answer to the question is to allow NTLMv2 which will enable the Windows users to connect to the UNIX server. To improve security, we should disable the old and insecure LM protocol as it is not used by the Windows computers.
Incorrect Answers:
B: The question states that the security authentication on the Windows domain is set to the highest level. This will be NTLMv2, not LM.
C: The question states that the security authentication on the Windows domain is set to the highest level. This will be NTLMv2, not LM so we need to allow NTLMv2.
D: The question states that the security authentication on the Windows domain is set to the highest level. This will be NTLMv2, not NTLM (version1).
References:
https://en.wikipedia.org/wiki/NT_LAN_Manager

4.A security architect is designing a new infrastructure using both type 1 and type 2 virtual machines. In addition to the normal complement of security controls (e.g. antivirus, host hardening, HIPS/NIDS) the

security architect needs to implement a mechanism to securely store cryptographic keys used to sign code and code modules on the VMs. Which of the following will meet this goal without requiring any hardware pass-through implementations?
A. vTPM
B. HSM
C. TPM
D. INE
Answer: A
Explanation:
A Trusted Platform Module (TPM) is a microchip designed to provide basic security-related functions, primarily involving encryption keys. The TPM is usually installed on the motherboard of a computer, and it communicates with the remainder of the system by using a hardware bus.
A vTPM is a virtual Trusted Platform Module.
IBM extended the current TPM Vl.2 command set with virtual TPM management commands that allow us to create and delete instances of TPMs. Each created instance of a TPM holds an association with a virtual machine (VM) throughout its lifetime on the platform.
Incorrect Answers:
B: A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys for strong authentication and provides crypto processing. These modules traditionally come in the form of a plug-in card or an external device that attaches directly to a computer or network server. This solution would require hardware pass-through.
C: A Trusted Platform Module (TPM) is a microchip designed to provide basic security-related functions, primarily involving encryption keys. The TPM is usually installed on the motherboard of a computer, and it communicates with the remainder of the system by using a hardware bus. Virtual machines cannot access a hardware TPM.
D: INE (intelligent network element) is not used for storing cryptographic keys.
References:
https://en.wikipedia.org/wiki/Hardware_security_module
http://researcher.watson.ibm.com/researcher/view_group.php?id=2850

5.A user has a laptop configured with multiple operating system installations. The operating systems are all installed on a single SSD, but each has its own partition and logical volume. Which of the following is the BEST way to ensure confidentiality of individual operating system data?
A. Encryption of each individual partition
B. Encryption of the SSD at the file level
C. FDE of each logical volume on the SSD
D. FDE of the entire SSD as a single disk
Answer: A
Explanation:
In this question, we have multiple operating system installations on a single disk. Some operating systems store their boot loader in the MBR of the disk. However, some operating systems install their boot loader outside the MBR especially when multiple operating systems are installed. We need to encrypt as much data as possible but we cannot encrypt the boot loaders. This would prevent the operating systems from loading.

Therefore, the solution is to encrypt each individual partition separately.
Incorrect Answers:
B: The question is asking for the BEST way to ensure confidentiality of individual operating system data. Individual file encryption could work but if files are ever added to the operating systems (for updates etc.), you would have to manually encrypt the new files as well. A better solution would be to encrypt the entire partition. That way any new files added to the operating system would be automatically encrypted.
C: You cannot perform full disk encryption on an individual volume. Full disk encryption encrypts the entire disk.
D: FDE of the entire SSD as a single disk would encrypt the boot loaders which would prevent the operating systems from booting.