Unsure defects

|  |  |  |
| --- | --- | --- |
| Describe the defect | In /etc folder, when ls -Z passwd command is used to view the security label, + appears. This means that /etc/passwd file has an extended Access Control list.  -rw-rw-r--+ root root system\_u:object\_r:passwd\_file\_t:s0 passwd | For marker’s use only |

|  |  |  |
| --- | --- | --- |
| Describe the defect | In the /root folder’s .bash\_history file, ‘setfacl -m u:reg:rw /etc/passwd’ command has been run. This is to give reg(a user) permission to read and write the passwd file, however passwd file should have read write permission for root, and readable by group and others. Since reg is not the root, reg must not be given access. | For marker’s use only |
| How would you correct the problem? | Change file permissions to -rw-r - - r- -. |  |

|  |  |  |
| --- | --- | --- |
| Describe the defect | In the /var/log folder, messages file has read and write permissions for user and group and read permissions for others. However, messages should have read and write permissions for root user only, since it contains sensitive system information which can be misused. | For marker’s use only |
| How would you correct the problem? | Change file permissions to rw--------. |  |

|  |  |  |
| --- | --- | --- |
| Describe the defect | In the /etc directory, ssh folder should have drwx (read, write and execute) for the user, and must not be accessible by group or others. However, in cwk2a image directory permissions are drwxr-xr-x, which means it is readable and executable for group and others. | For marker’s use only |
| How would you correct the problem? | Change file permissions to drwx------. |  |

|  |  |  |
| --- | --- | --- |
| Describe the defect | In the /etc/ssh folder all private ssh\_keys (ssh\_host\_ecdsa\_key, ssh\_host\_ed25519\_key, ssh\_host\_rsa\_key) have file permissions of read and write by user and read by group, whereas only user should have read and write permission, since it contains private key. Private key can be used to decrypt messages that were encrypted with the user’s public key, hence unintended users will be able to view information/data. | For marker’s use only |
| How would you correct the problem? | Change file permissions to -rw-------. |  |

|  |  |  |
| --- | --- | --- |
| Describe the defect | In the /mnt/disk/regstorage/tmp1/etc shadow file has permissions world readable and writeable by user. However, since the shadow file contains hashes, it should only be read and write for user and no permissions for group and others. Also, in the file (for root and tc) MD5 is used, which is insecure. | For marker’s use only |
| How would you correct the problem? | Change file permissions to rw- - - - - - and use SHA 256 or 512 for encryption. |  |

|  |  |  |
| --- | --- | --- |
| Describe the defect | In /home/reg/projecttc when extract.sh file is run (using ./extract.sh) opt command, which installs application software packages, is run with tcemirror, bootsync.sh, shutdown.sh, bootlocal.sh. Bootsync.sh, bootlocal.sh and shutdown.sh modify the behaviour from the base system. They block the boot process until they are finished. Hence are a defect in Linux. | For marker’s use only |
| How would you correct the problem? | Restricting users to run opt with specific arguments such as bootlocal.sh, shutdown.sh and bootsync.sh. |  |

5 more