Afeefah Manzoor

Lab 2 Report:

5. HIPAA requires physical safeguards- which includes implementing policies and procedures to limit the physical access to electronic information and facilities where they are located while allowing the properly authorized access. HIPAA does not need to comply with STIG requirements from DISA.

7. The main vulnerabilities found on a workstation are USB devices, Peer-to-Peer file sharing, antivirus problems, outdated Microsoft service packs, missing security agents, unauthorized remote-control software, media files, unnecessary modems, unauthorized or unsecured synchronization software, and wireless connectivity.

13. Public instant messaging clients are not installed on the work station and neither are Peer-to-Perr clients or utilities.

18. Display shut down button is used to close your machine in a orderly manner.

Clear system pagefile is to make sure that no sensitive data is left on your machine.

Removeable media devices can pose some threat, like stolen data or malware being introduced, but are a removeable storage device.

Halt on audit failure automatically shuts down the system immediately if it is enabled and if the security audit cannot be logged for any reason.

Security configuration tools are security measures that are used or implemented when installing and building computers and network devices to reduce cyber vulnerabilities.

23. To mitigate risks of losing data system recovery backups are used to incrementally backup new data which takes less time and the user will not lose a ton of data in case of an incident. Caching logon credentials will keep a log of who logs on incase an incident happens. Password uniqueness makes it harder for someone to guess the user’s password.

26 CVE are a dictionary that provides definition for publicly disclosed cyber security vulnerabilities.