Lab 6 Assessment Worksheet

Auditing the Workstation Domain for Compliance

Course Name and Number: ITN262

Student Name: Afeefah Manzoor

Instructor Name: KK

Lab Due Date: 9/6/20

1. What are some risks, threats, and vulnerabilities commonly found in the Workstation Domain that must be mitigated through a layered security strategy?

Things that can be mitigated are trojan horses, worms, and viruses.

1. File-sharing utilities and client-to-client communication applications can provide the capability to share files with other users (for instance, peer-to-peer networking or sharing.) what risks and/or vulnerabilities are introduced with these applications?

Peer-to-peer can result in causing trojan horse attacks, worms and viruses, as well as introducing other big risks like prosecution of pirating software.

1. Explain how confidentiality can be achieved in the Workstation Domain with security controls and security countermeasures.

Confidentiality can be achieved with virus scanning software and password protecting computers-including not giving out the user’s password, other personal information and updating the workstation regularly.

1. Explain how data integrity can be achieved in the Workstation Domain with security controls and security countermeasures.

In the Access Control List the user can add security controls and countermeasures to make sure only authorized people can access and change data.

1. Explain how availability can be achieved in the Workstation Domain with security controls and security countermeasures.

Having security controls in place to protect and to have countermeasures to keep it running or get into back up quickly in case something is to go wrong can achieve availability.

1. Although users of desktop applications might not create mission-critical data, all of their data represents a resource that, if lost, can result in a permanent loss of information or productivity. Explain what countermeasures and best practices should be implemented to avoid this potential disaster.

To prevent loss the best way its to have daily backups on the machine and cloud storage..

1. What is the purpose for Microsoft Windows Security Configuration and Analysis snap-in? Explain.

It loads a security template and then compares the user’s system to it an d highlights possibilities for problems and can apply those changes to meet the requirements.

1. How would you go about updating the Windows Security Options Files? Explain how this option can help mitigate risk in the Workstation Domain.

By using the secedit.exe program; it will inform the admin what security measures/standers are in a good position and what measures are needed to be replaced and updated

1. What does the Microsoft® Windows executable GPResult.exe do and what general information does it provide? Explain how this application helps mitigate the risks, threats, and vulnerabilities commonly found in the Workstation Domain.

GPResult.exe shows Resultant Set of Policy for the users/computers and can be used to understand what the policy is in place. It can also troubleshoot the problems.

1. What is the risk involved in caching logon credentials on a Microsoft® Windows system?

If hackers get into the system, the hacker can steal information and use it for their own benefit.

1. What is the current URL for the location of the DISA Military STIGs on Microsoft® Windows 7 operating systems?

Events/~/media/Files/DISA/News/Conference/CIF/Briefing/IA\_STIG\_SCAP\_and\_Data\_Metrics.pdf

1. Within the Windows 7 Security Technical Implementation Guide (STIG), what are the three Vulnerability Severity Code Definitions defined?

* CAT I- vulnerability will result directly in loss of CIA
* CAT II- vulnerability has potential to lose CIA
* CAT III- vulnerability degrades measures that protect CIA

1. DumpSec is a tool used by system administrators performing information assurance on a Microsoft® Windows 7 workstation. What is the purpose of this tool?

DumpSec dumps the permissions and audit settings for printers, registry, file systems, and share in a concise and readable format so hole in the security system are apparent.

1. From the Windows 7 Security Technical Implementation Guide (STIG), where can Windows 7 File & Registry Settings be reviewed and audited on a Windows 7 workstation?

Object access

1. As per DoD and information assurance procedures, who must be notified if any exceptions to DoD STIGs standards for workstation configurations are to be implemented?

Digital Advertising Alliance