Fundamentals of Information Technology Security
CSEC 1110
Lab 02

- Contact your instructor with your questions about the assignments.
- The student must insure all the answers are free from any malware.
- The student must ensure all answers are legal as defined by the class syllabus.
- All parts of your answers must be neat and easy to read.
- Paragraphs are at least four properly constructed English sentences.
- Embedding documents within documents does not work with the D2L Bright Space assignments.
- Plagiarism will not be tolerated.
- Unless noted, all lab sections must be done as unprivileged login.
- Labeling answers is highly recommended.

2. Lab 02: Controlling Files

2.1. Upload each answer to the D2L Bright Space Assignment section 2.1 before the due date found in the csec1110a.pdf document. Submit a Portable Document Format (PDF) or word processing file containing the following. Use the Center for Internet Security (CIS) recommendation.

2.1.1. Provide all your “Account Policies” settings for your Windows virtual machine.
2.1.2. Provide all your “Local Policies” settings for your Windows virtual machine.
2.1.3. Provide all your “Security Options” settings for your Windows virtual machine.
2.1.4. Provide all your “Event Log” settings for your Windows virtual machine.
2.1.5. Provide all your “Restricted Groups” settings for your Windows virtual machine.
2.1.6. Provide all your “System Services” settings for your Windows virtual machine.
2.1.7. Provide all your “Registry” settings for your Windows virtual machine.
2.1.8. Provide all your “File System” settings for your Windows virtual machine.
2.1.9. Provide all your “Wire Network Policies” settings for your Windows virtual machine.
2.1.10. Provide all your “Windows Defender with Advance Security” settings for your Windows virtual machine.
2.1.11. Provide all your “Network List Manager Policies” settings for your Windows virtual machine.
2.1.12. Provide all your “Wireless Network Polices” settings for your Windows virtual machine.
2.1.13. Provide all your “Public Key Policies” settings for your Windows virtual machine.
2.1.14. Provide all your “Software Restriction Policies” settings for your Windows virtual machine.
2.1.15. Provide all your “Network Access Protection NAP Client Configuration” settings for your Windows virtual machine.
2.1.16. Provide all your “IP Security Policies” settings for your Windows virtual machine.
2.1.17. Provide all your “Advance Audit Policy Configuration” settings for your Windows virtual machine.
2.1.18. Provide all your “Administrative Templates” settings for your Windows virtual machine.
2.1.19. Provide all your “Start Menu and Taskbar” settings for your Windows virtual machine.
2.1.20. Provide all your “Administrative Templates” settings for your Windows virtual machine.
2.1.21. List five settings that need to be modified immediately. Explain why each setting needs modification.
2.1.22. Identify if an AI type program was used to complete this lab section. If an AI program is used, identify the AI system used.

2.2. Upload each answer to the D2L Bright Space Assignment section 2.2 before the due date found in the csec1110a.pdf document. Submit a Portable Document Format (PDF) or word processing file containing the following. Put your answer in a single document.

2.2.1. Provide all the hypervisor settings for a router/firewall system installation.
2.2.2. Provide all the router/firewall system installation option configuration settings for a virtual machine.
2.2.3. Show your virtual router/firewall system is current with updates.
2.2.4. Show the IPv4 and IPv6 address ranges for the external and internal networks.
2.2.5. Show the all the firewall rules for the external and internal networks.
2.2.6. Show the NAT/PAT rules for the router/firewall.
2.2.7. Show the DHCPv4 and DHCPv6 configuration for the internal network.
2.2.8. Identify if an AI type program was used to complete this lab section. If an AI program is used, identify the AI system used.

2.3. Upload each answer to the D2L Bright Space Assignment section 2.3 before the due date found in the csec1110a.pdf document. Submit a Portable Document Format (PDF) or word processing file containing the following. Put your answer in a single document.

2.3.1. Show the state of updates for the router/firewall. Explain why the system is not current with updates.

2.3.2. Show the additional installed packages for the router/firewall.
2.3.3. Provide at least two IPv4 DHCP log entries including mac address and lease ending day/time.
2.3.4. Provide at least two IPv6 DHCP log entries including mac address and lease ending day/time.
2.3.5. Provide a list of at least 50 states of pfTop.
2.3.6. Identify if an AI type program was used to complete this lab section. If an AI program is used, identify the AI system used.

2.4. Upload each answer to the D2L Bright Space Assignment section 2.4 before the due date found in the csec1110a.pdf document. Submit a Portable Document Format (PDF) or word processing file containing the following. Put your answer in a single document.
2.4.1. This section is based on the SANS Top 6 Essential Log Reports found on the D2L site. Provide the complete text or XML log entry from a system you control showing “Authentication and Authorization Report” issue for a Windows system. Windows systems will report event id 4624 or equivalent.
2.4.2. In at least one sentence, explain how the log entry fits with the requested log report category.
2.4.3. This section is based on the SANS Top 6 Essential Log Reports found on the D2L site. Provide the complete text or XML log entry from a system you control showing “Authentication and Authorization Report” issue for a Linux system.
2.4.4. In at least one sentence, explain how the log entry fits with the requested log report category.
2.4.5. Identify if an AI type program was used to complete this lab section. If an AI program is used, identify the AI system used.