

Linux 2  
CPTR 2234  
Lab 06

- Contact your instructor with your questions about the assignments.
- The student must insure all the answers are free from any malware.
- The student must insure 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.
- Submit your answers in the appropriate file type.
- Embedding documents within documents does not work with the D2L Bright Space assignments.
- Plagiarism will not be tolerated.

### Lab 06: Linux Server

- 6.1. each section answer to the D2L Bright Space Assignment section 6.1 before the due date found in the 2234a.pdf document. Use the **script** command or a **putty log file (printable output only)**. Your answers must appear in your answer in the same order as the lab. The file must be human readable text only and must show your login name and all entered commands. Submit a Windows or UNIX text file with the appropriate Windows extension.
  - 6.1.1. Configure auditd to export the host01 audit files to host02.
  - 6.1.2. Provide the host01 auditd configuration file with export statements.
  - 6.1.3. Provide the host02 auditd configuration file with export statements.
  - 6.1.4. Provide host01 firewall settings
  - 6.1.5. Provide host02 firewall settings.
  - 6.1.6. Provide evidence of successful log file export.
  - 6.1.7. Identify if an AI program was used in this lab section. If used, identify the AI program.
- 6.2. Upload each section answer to the D2L Bright Space Assignment section 6.2 before the due date found in the 2234a.pdf document. Use the **script** command or a **putty log file (printable output only)**. Your answers must appear in your answer in the same order as the lab. The file must be human readable text only and must show your login name and all entered commands. Submit a Windows or UNIX text file with the appropriate Windows extension.
  - 6.2.1. Provide evidence of successfully installing and starting the AppArmor service. The Debian host is recommended for this lab section.
  - 6.2.2. Provide the URL of two different AppArmor profiles.
  - 6.2.3. Provide evidence of installing each AppArmor profile on your system.
  - 6.2.4. Provide evidence each AppArmor profile is working.
  - 6.2.5. Identify if an AI program was used in this lab section. If used, identify the AI program.
- 6.3. Upload each section answer to the D2L Bright Space Assignment section 6.3 before the due date found in the 2234a.pdf document. Use the **script** command or a **putty log file (printable output only)**. Your answers must appear in your answer in the same order as the lab. The file must be human readable text only and must show your login name and all entered commands. Submit a Windows or UNIX text file with the appropriate Windows extension.
  - 6.3.1. Identify a current Linux vulnerability.
  - 6.3.2. Provide an AppArmor profile that will detect the vulnerability or exploitation of vulnerability.
  - 6.3.3. Provide evidence the AppArmor profile is working as expected.
    - 6.3.3.1. Create a script.
      - 6.3.3.1.1. The script will have remarks identifying the author, creation date, outside help credit, and script purpose.
      - 6.3.3.1.2. The script will report the records of the AppArmor Profile log entry.
      - 6.3.3.1.3. The script will report the date and time of the vulnerability search.
      - 6.3.3.1.4. Provide the script source code.
      - 6.3.3.1.5. Provide documentation of running the script at least four times.
  - 6.3.4. Identify if an AI program was used in this lab section. If used, identify the AI program.
- 6.4. Upload each section answer to the D2L Bright Space Assignment section 6.4 before the due date found in the 2234a.pdf document. Use the **script** command or a **putty log file (printable output only)**. Your answers must appear in your answer in the same order as the lab. The file must be human readable text only and must show your login name and all entered commands. Submit a Windows or UNIX text file with the appropriate Windows extension.
  - 6.4.1. Provide a list of all the steps you performed to setup the logrotate on host01.
  - 6.4.2. Provide a copy of all the configuration files you changed to setup the logrotate on host01.

- 6.4.3. Provide the URL for a best practices for logrotate setup and explain why you selected this document.
- 6.4.4. Identify in the configuration files the information from your best practices document.
- 6.4.5. Provide the documentation of successful logrotate operation.
- 6.4.6. Identify if an AI program was used in this lab section. If used, identify the AI program.