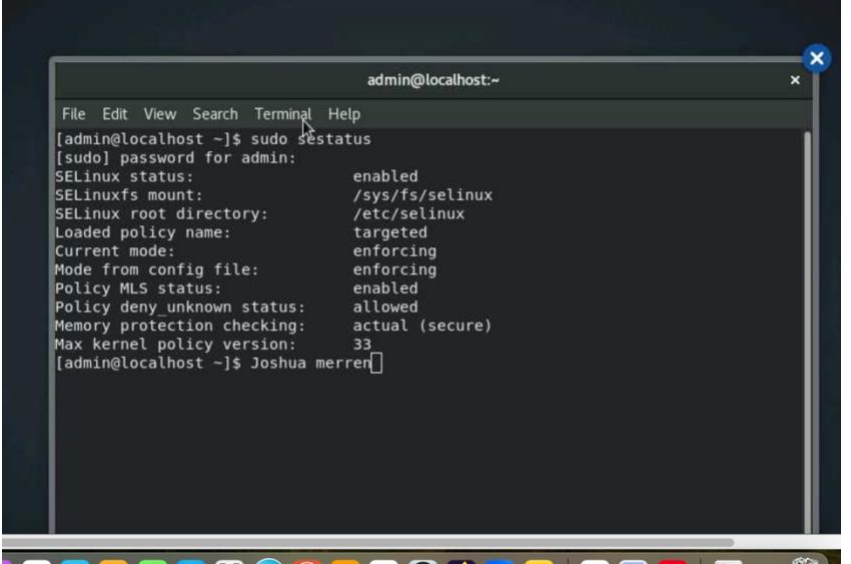
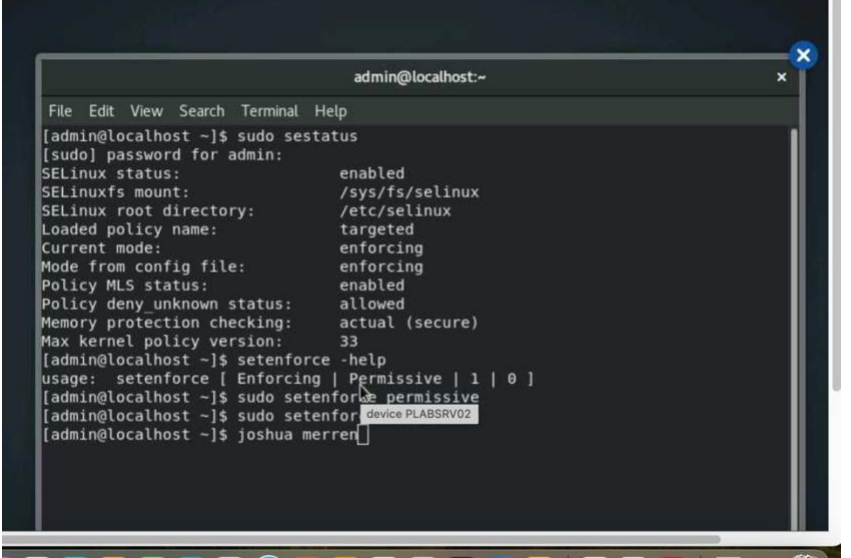


CYB 300 Module One Practice Lab Worksheet

Complete this worksheet by replacing the bracketed phrases in the Response column with the relevant information. For all screenshots, include your name in the command line.

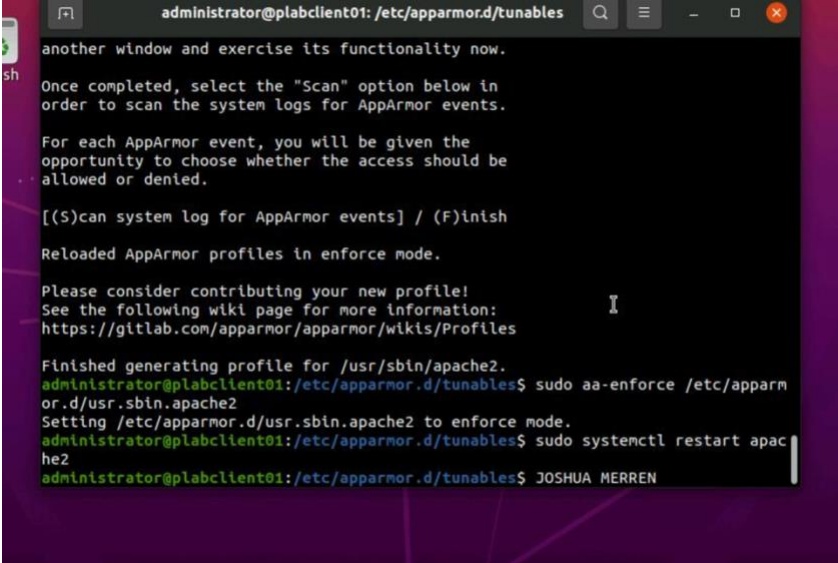
Lab: Securing Linux Devices

Exercise 1: Secure an Alma Device

Prompt	Response
Task 1: Take a screenshot of Step 3 showing the sudo sestatus command. Add your name in the command line.	 <pre> admin@localhost:~\$ sudo sestatus [sudo] password for admin: SELinux status: enabled SELinuxfs mount: /sys/fs/selinux SELinux root directory: /etc/selinux Loaded policy name: targeted Current mode: enforcing Mode from config file: enforcing Policy MLS status: enabled Policy deny_unknown status: allowed Memory protection checking: actual (secure) Max kernel policy version: 33 admin@localhost ~]\$ Joshua merren </pre>
Task 1: Take a screenshot of Step 5 showing sudo setenforce permissive. Include your name in the command line.	 <pre> admin@localhost:~\$ sudo sestatus [sudo] password for admin: SELinux status: enabled SELinuxfs mount: /sys/fs/selinux SELinux root directory: /etc/selinux Loaded policy name: targeted Current mode: enforcing Mode from config file: enforcing Policy MLS status: enabled Policy deny_unknown status: allowed Memory protection checking: actual (secure) Max kernel policy version: 33 admin@localhost ~]\$ setenforce -help usage: setenforce [Enforcing Permissive 1 0] admin@localhost ~]\$ sudo setenforce permissive admin@localhost ~]\$ sudo setenfor device PLABSRV02 admin@localhost ~]\$ joshua merren </pre>

Prompt	Response
Task 3: Take a screenshot of Step 5 showing the context label of the website folder changed. Include your name in the command line.	 <pre> admin@localhost:/ File Edit View Search Terminal Help drwxrwxrwt. 15 root root system_u:object_r:tmp_t:s0 4096 Jul 4 20:00 t mp drwxr-xr-x. 13 root root system_u:object_r:usr_t:s0 158 Mar 31 2022 u sr drwxr-xr-x. 22 root root system_u:object_r:var_t:s0 4096 Mar 22 2023 v ar drwxr-xr-x. 4 root root unconfined_u:object_r:default_t:s0 33 Jul 4 20:04 w ebsite [admin@localhost /]\$ sudo chcon -Rv -- chcon: missing operand Try 'chcon --help' for more information. [admin@localhost /]\$ sudo chcn -Rv --type=httpd_sys_content_t /website sudo: chcn: command not found [admin@localhost /]\$ sudo chcon -Rv --type=httpd_sys_content_t /website changing security context of '/website/cgi-bin' changing security context of '/website/html' changing security context of '/website' [admin@localhost /]\$ ls -lZ /website total 0 drwxr-xr-x. 2 root root unconfined_u:object_r:httpd_sys_content_t:s0 6 Jul 4 20 :04 cgi-bin drwxr-xr-x. 2 root root unconfined_u:object_r:httpd_sys_content_t:s0 6 Jul 4 20 :04 html [admin@localhost /]\$ joshua merren </pre>
Why is it important to show the status and context label of the website folder?	It is essential to show the status and context label of the website folder because it verifies that the correct security settings are in place. This ensures that SELinux is enforcing the appropriate policies to protect the folder. By confirming these settings, we can protect the folder from unauthorized access and potential security threats.
Task 3: Take a screenshot of Step 9 showing Port 50080 being added to the SELinux.	 <pre> File Edit View Search Terminal Help zented_port_t tcp 1229 zented_port_t udp 1229 zookeeper_client port_t tcp 2181 zookeeper_election port_t tcp 3888 zookeeper_leader port_t tcp 2888 zope port_t tcp 8021 [admin@localhost /]\$ suo semanage port -l grep http bash: suo: command not found... [admin@localhost /]\$ sudo semanage port -l grep http http_cache_port_t tcp 8080, 8118, 8123, 10001-10010 http_cache_port_t udp 3130 http_port_t tcp 80, 81, 443, 488, 8008, 8009, 8443, 9000 pegasus_http port_t tcp 5988 pegasus_https port_t tcp 5989 [admin@localhost /]\$ sudo semanage port -a -t http_port_t -p tcp 50080 [admin@localhost /]\$ sudo semanage port -l grep http [admin@localhost /]\$ sudo semanage port -l grep http http_cache_port_t tcp 8080, 8118, 8123, 10001-10010 http_cache_port_t udp 3130 http_port_t tcp 50080, 80, 81, 443, 488, 8008, 8009, 844 3, 9000 pegasus_http port_t tcp 5988 pegasus_https port_t tcp 5989 [admin@localhost /]\$ JOSHUA MERREN </pre>
What is the significance of showing the port addition?	Showing the port addition is significant because it confirms that the system is configured to allow network traffic on the newly added port. This is crucial for the proper functioning of services that use non-standard ports. It also helps maintain security by ensuring only designated ports are open, reducing the risk of unauthorized access.

Exercise 2: Secure an Ubuntu Device

Prompt	Response
<p>Task 3: Take a screenshot of Step 7 showing the apparmor has been enabled to protect the apache server.</p>	 <p>The screenshot shows a terminal window titled 'administrator@plabclient01: /etc/apparmor.d/tunables'. The text in the terminal includes instructions to scan system logs for AppArmor events, reload profiles, and generate a profile for /usr/sbin/apache2. The user then runs the command 'sudo aa-enforce /etc/apparmor.d/usr.sbin.apache2' and 'sudo systemctl restart apache2'. The terminal output shows the profile being generated and the system being restarted. The user's name 'JOSHUA MERREN' is visible at the bottom of the terminal window.</p>
<p>What is the importance of apparmor when it comes to protecting the apache server?</p>	<p>apparmor is essential for protecting the Apache server because it enforces strict security policies that limit what the server can do. Ensuring that the damage is contained even if the server is compromised reduces the risk of exploitation. By confining the server's operations, apparmor helps maintain the overall security and stability of the system.</p>