Securing Linux Devices

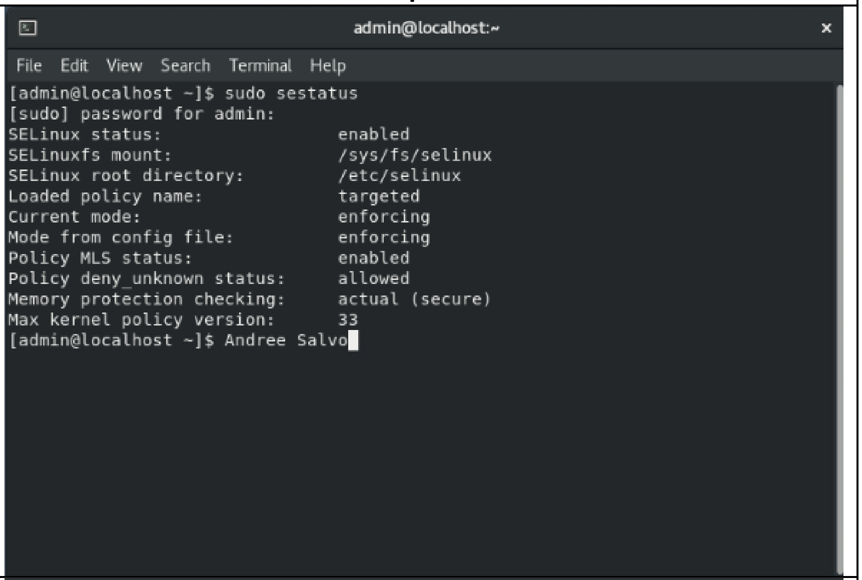
Andree Salvo
Southern New Hampshire University
CYB 300-14668
Instructor: Jason Keltner

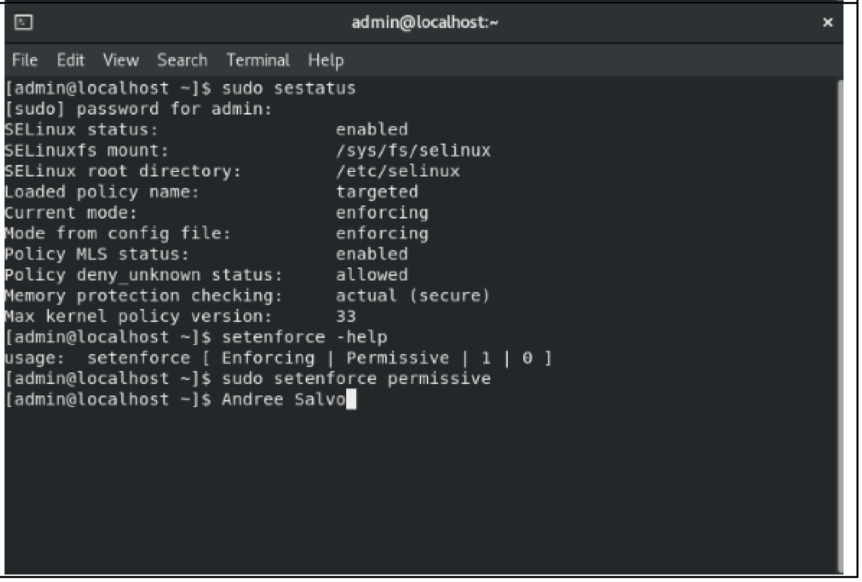
CYB 300 Module One Lab Worksheet

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.

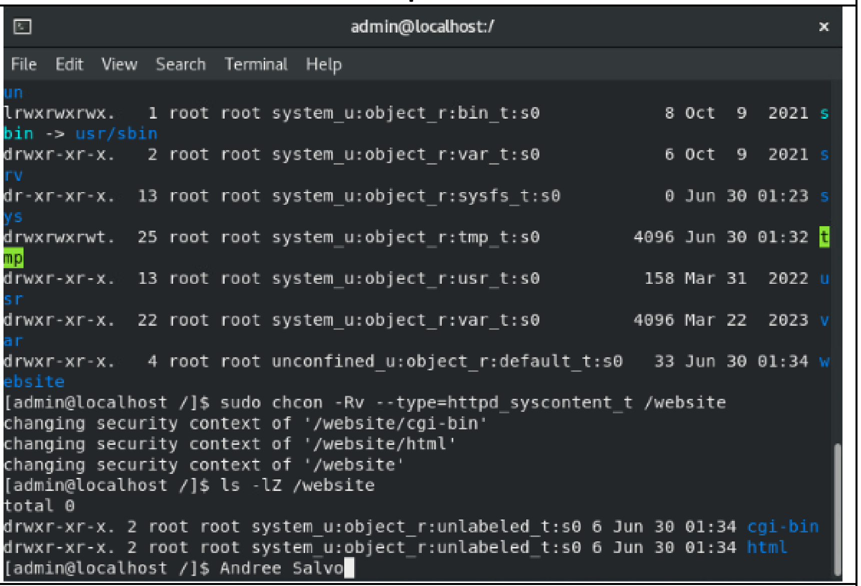
Lab: Securing Linux Devices
Exercise 1: Secure an Alma Device

Prompt	Response

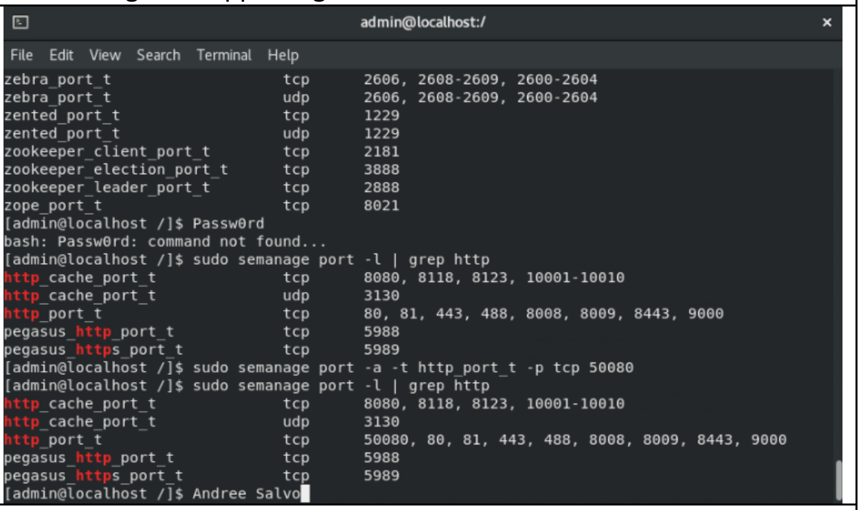
Task 1: Take a screenshot of **Step 3** showing the sudo sestatus command. Add your name in the command line.	
	`[admin@localhost ~]$ sudo sestatus`
	`[sudo] password for admin:`
	`SELinux status:                 enabled`
	`SELinuxfs mount:                /sys/fs/selinux`
	`SELinux root directory:         /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 ~]$ Andree Salvo`

Task 1: Take a screenshot of **Step 5** showing sudo setenforce permissive. Include your name in the command line.	
	`[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 ~]$ Andree Salvo`

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.	
	`un`
	`lrwxrwxrwx.   1 root root system_u:object_r:bin_t:s0           8 Oct  9  2021 s`
	`bin -> usr/sbin`
	`drwxr-xr-x.   2 root root system_u:object_r:var_t:s0           6 Oct  9  2021 s`
	`rv`
	`dr-xr-xr-x.  13 root root system_u:object_r:sysfs_t:s0         0 Jun 30 01:23 s`
	`ys`
	`drwxrwxrwt.  25 root root system_u:object_r:tmp_t:s0        4096 Jun 30 01:32 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 Jun 30 01:34 w`
	`ebsite`
	`[admin@localhost /]$ sudo chcon -Rv --type=httpd_syscontent_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 system_u:object_r:unlabeled_t:s0 6 Jun 30 01:34 cgi-bin`
	`drwxr-xr-x. 2 root root system_u:object_r:unlabeled_t:s0 6 Jun 30 01:34 html`
	`[admin@localhost /]$ Andree Salvo`

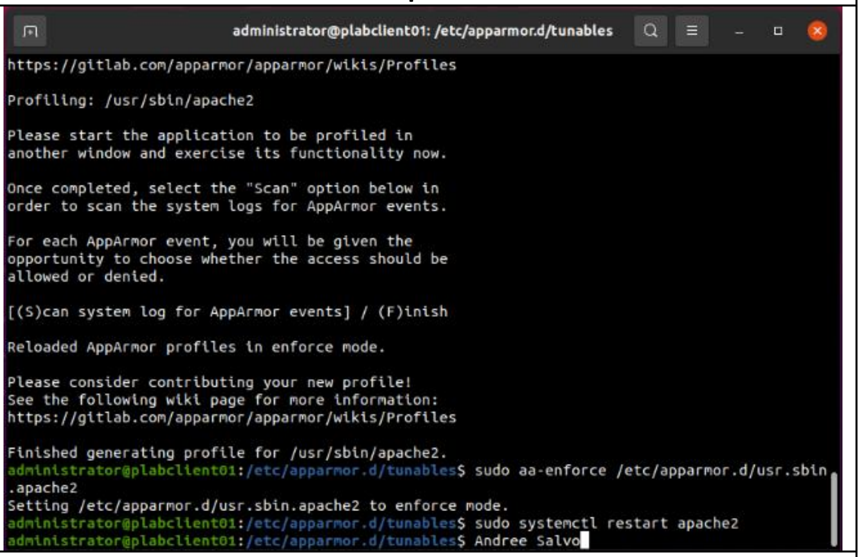
Why is it important to show the status and context label of the website folder?	Showing the status and context label is key because it reveals the folder's security, name, user roles, and access levels—helping prevent mislabeling and supporting better access control.

Task 3: Take a screenshot of **Step 9** showing Port 50080 being added to the SELinux.	
	`zebra_port_t                   tcp      2606, 2608-2609, 2600-2604`
	`zebra_port_t                   udp      2606, 2608-2609, 2600-2604`
	`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 /]$ Passw0rd`
	`bash: Passw0rd: 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`
	`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, 8443, 9000`
	`pegasus_http_port_t            tcp      5988`
	`pegasus_https_port_t           tcp      5989`
	`[admin@localhost /]$ Andree Salvo`

What is the significance of showing the port addition?	Showing the port addition matters because it clarifies how the server is being accessed, makes troubleshooting much easier, supports secure setups, and keeps things very organized.

Exercise 2: Secure an Ubuntu Device

<table>
<tr><th>Prompt</th><th>Response</th></tr>
<tr><td>Task 3: Take a screenshot of <b>Step 7</b> showing the apparmor has been enabled to protect the apache server.</td><td>



```
https://gitlab.com/apparmor/apparmor/wikis/Profiles

Profiling: /usr/sbin/apache2

Please start the application to be profiled in
another window and exercise its functionality now.

Once completed, select the "Scan" option below in
order to scan the system logs for AppArmor events.

For each AppArmor event, you will be given the
opportunity to choose whether the access should be
allowed or denied.

[(S)can system log for AppArmor events] / (F)inish

Reloaded AppArmor profiles in enforce mode.

Please consider contributing your new profile!
See the following wiki page for more information:
https://gitlab.com/apparmor/apparmor/wikis/Profiles

Finished generating profile for /usr/sbin/apache2.
administrator@plabclient01:/etc/apparmor.d/tunables$ sudo aa-enforce /etc/apparmor.d/usr.sbin
.apache2
Setting /etc/apparmor.d/usr.sbin.apache2 to enforce mode.
administrator@plabclient01:/etc/apparmor.d/tunables$ sudo systemctl restart apache2
administrator@plabclient01:/etc/apparmor.d/tunables$ Andree Salvo
```

</td></tr>
<tr><td>What is the importance of apparmor when it comes to protecting the apache server?</td><td>Apparmor protects the Apache server by restricting access to all but the most essential parts of the system. If an attacker finds a way to exploit a bug in Apache or one of its modules, Apparmor will limit the potential damage from that attack.</td></tr>
</table>