### **Bonus: Check for Policy and File Violations**

1. Command to verify auditd is active:

Solution:

~$ sudo systemctl status auditd

1. Command to set number of retained logs and maximum log file size:

Solution:

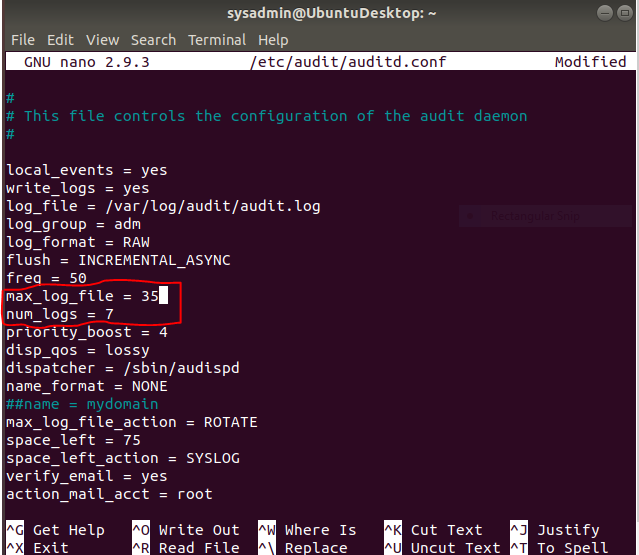
~$ sudo nano /etc/audit/auditd.conf

* + Add the edits made to the configuration file below:

num\_logs = 7

max\_log\_file = 35

1. [Your solution edits here]



1. Command using auditd to set rules for /etc/shadow, /etc/passwd and /var/log/auth.log:

Solution:

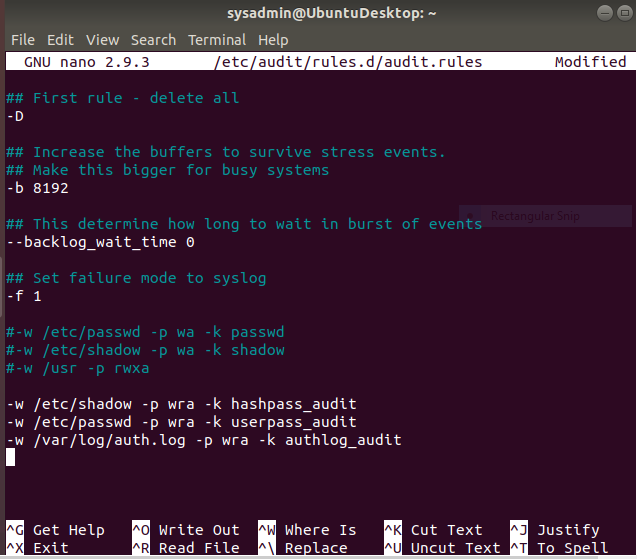
~$ sudo nano /etc/audit/rules.d/audit.rules

* + Add the edits made to the rules file below:

-w /etc/shadow -p wra -k hashpass\_audit

-w /etc/passwd -p wra -k userpass\_audit

-w /var/log/auth.log -p wra -k authlog\_audit

1. [Your solution edits here]  
   
2. Command to restart auditd:

Solution:

~$ sudo service auditd restart

1. Command to list all auditd rules:

Solution:

~$ sudo auditctl -l

Command to produce an audit report:

Solution:

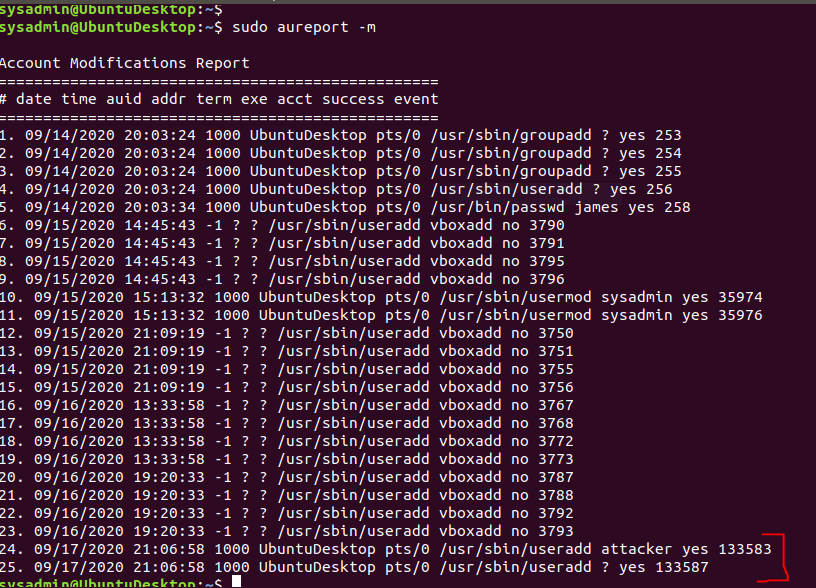
~$ sudo aureport -au

1. Create a user with sudo useradd attacker and produce an audit report that lists account modifications:

Solution:

~$ sudo useradd attacker

~$ sudo aureport -m



1. Command to use auditd to watch /var/log/cron:

Solution:

~$ sudo auditctl -w /var/log/cron/

~$ sudo systemctl restart auditd

1. Command to verify auditd rules:

Solution:

~$ sudo auditctl -l