

Forum:[Hack Forums](#)

Thread: [One Line Kernel Audit](#)

Clumsy - November 9, 2024, 3:19 pm

The following command installs configures and starts the auditd service which is used for system auditing. It sets up various rules to monitor critical activities such as kernel module operations, system calls, file changes, and user modifications. After setting the audit rules, it searches the audit logs for specific activities and then checks the status of the auditd service to ensure it's running.

```
sudo apt update && sudo apt install -y auditd && sudo systemctl enable auditd && sudo systemctl start auditd && sudo auditctl -w /sbin/insmod -p x -k kernel-modules && sudo auditctl -w /sbin/rmmod -p x -k kernel-modules && sudo auditctl -w /sbin/modprobe -p x -k kernel-modules && sudo auditctl -a always,exit -F arch=b64 -S execve -k syscall-exec && sudo auditctl -a always,exit -F arch=b32 -S execve -k syscall-exec && sudo auditctl -w /etc -p wa -k config-changes && sudo auditctl -w /bin -p wa -k bin-exec && sudo auditctl -w /sbin -p wa -k/sbin-exec && sudo auditctl -w /usr -p wa -k usr-changes && sudo auditctl -w /usr/sbin/useradd -p x -k user-modifications && sudo auditctl -w /usr/sbin/userdel -p x -k user-modifications && sudo auditctl -w /usr/sbin/usermod -p x -k user-modifications && sudo auditctl -w /usr/bin/sudo -p x -k sudo-exec && sudo auditctl -w /bin/su -p x -k su-exec && sudo auditctl -w /var/log/boot.log -p wa -k boot-logs && sudo auditctl -w /var/log/shutdown.log -p wa -k shutdown-logs && sudo auditctl -a always,exit -F arch=b64 -S all -k syscalls-all && sudo auditctl -a always,exit -F arch=b32 -S all -k syscalls-all && sudo ausearch -m avc -i && sudo ausearch -k kernel-modules && sudo ausearch -k syscall-exec && sudo ausearch -k config-changes && sudo ausearch -k bin-exec && sudo ausearch -k/sbin-exec && sudo ausearch -k usr-changes && sudo ausearch -k user-modifications && sudo ausearch -k sudo-exec && sudo ausearch -k su-exec && sudo ausearch -k boot-logs && sudo ausearch -k shutdown-logs && sudo ausearch -k syscalls-all && sudo systemctl status auditd
```

Install and Enable auditd

Updates package lists and installs auditd

Enables auditd to start on boot and starts it immediately

Set Audit Rules

Uses auditctl to monitor specific files and commands such as kernel module operations, system calls, and user modifications

Search Audit Logs

Uses ausearch to search the logs for specific events

Check Service Status

Displays the status of the auditd service

This setup enables auditing of system activity, helping to monitor potential security issues or system changes.