**Project Support: System Auditing Analysis**

**In this final project, you will be exploring the system auditing techniques, and you will get familiar with provenance analysis.**

**Before delving into specific tasks and details, you should first get familiar with Linux *auditd*.**

***Auditd.* The *auditd* subsystem is an access monitoring and accounting for Linux developed and maintained by RedHat. It was designed to integrate with the kernel and watch for interesting system calls. You can refer to the official documents:**

<https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/security_hardening/auditing-the-system_security-hardening>

**To help you quickly get familiar with *auditd*, please refer to the provided video tutorial:** <https://www.youtube.com/watch?v=x2u_prS2HmM&t=55s>

***Auditbeat.* Auditbeat is actually a wrapper of Linux *auditd*, providing a more convenient interface and nested log format. Please refer to the following link to know more details:** <https://www.elastic.co/guide/en/beats/auditbeat/current/index.html>

**Environment Setup**

**For the final project, we will provide you an Ubuntu 20.04 VM with installed Linux *auditd* and the Auditbeat wrapper. Also, we will provide handcrafted malicious programs to simulate a demo cyber-attack.**

**Download the VM. You can download the VM from the following link:**

<https://drive.google.com/file/d/1WL6gVtE3KNCzqjSG3pnv7m3wHsLlg2rJ>

**Logging in the VM.** Both the user account and the password of the VM are student.

**Get Started**

**After logging into the VM, please first run the following command:**

**bash -c “$(curl -fsSL https://raw.githubusercontent.com/Icegrave0391/patch/main/patch.sh)”**

**Then, please refer to /home/student/proj\_tools to see the full instructions (e.g., the description of the demo cyber-attack) and the provided tools (e.g., the script for running the demo cyber-attack, the scripts to record and collect system audit logs).**

**Open Questions**

**In order to profile the system behaviors via system auditing and analyze the audit logs, there are several open questions:**

1. **How to (effectively) parse and analyze the system-wide audit logs?**
2. **How to delineate the dependencies among system events based on those audit logs?**
3. Do you encounter any problems/difficulties while analysing those logs, or what impedes you from investigating the attack behaviours?