CYB102 Project 2

(🔗 Instructions Page)

👤 Student Name: Didier Joseph Desmangles
✉️ Student Email: djdesmangles@gmail.com

Reflection (Required)

> 🤔 **Reflection Question #1:** If I had to **explain "what Audit does" in 3 emojis,** they would be… (Feel free to put other comments about your experience in this unit here, too!)
>
> "HIDS" reminds me a lot of a sophisticated surveillance camera system 📹. The cameras don't prevent an attacker from getting in. Still, it can give an alert (motion detection) and provide a lot of information to help defend the area (like face recognition), as well as logs (video playback).
> 📹 **Camera** to **Protect** 🔎 **Magnifier** to **Monitor** 📜 **Paper** to **Log**

> 🧠**Reflection Question #2:** How does Audit track changes made to specific files?
>
> - Audit is a service (auditd) that requires a set of rules defined by the administrator, specifying which files or directories to monitor, along with the possible actions on these objects, (**r**ead, **w**rite, e**x**ecute, **a**ttribute).
> - Based on the rules, Audit will monitor file access and modification events, and provide a detailed log of any events.
> - These rules are inside the file /etc/audit/rules.d/audit.rules. (on ubuntu)
>
> - Lets define a rule as an example:
>   We will edit audit.rules with a text editor and add :
>   ```
>   -w /home/codepath/project2-main/protected_files/cloudia.txt -p w -k unit2_prj_changes
>   ```
>   "-w": watch this file or directory
>   "-p": what to track (rwxa)
>   "-k": create a key for easy identification in the log file
>
>   After saving and closing "audit.rules". We restart auditd
>   ```
>   sudo systemctl restart auditd
>   ```
>   We can check the service status:
>   ```
>   sudo systemctl status auditd
>   ```
>   We make sure the rules are correctly loaded
>   ```
>   auditctl -R /etc/audit/rules.d/audit.rules
>   ```
>   We can list the rules
>   ```
>   auditctl -l
>   ```

All monitored actions will be recorded. Now we need to access the log to assess a situation.

```
sudo ausearch -ts today -k unit2_lab_changes -i > changes.txt
```

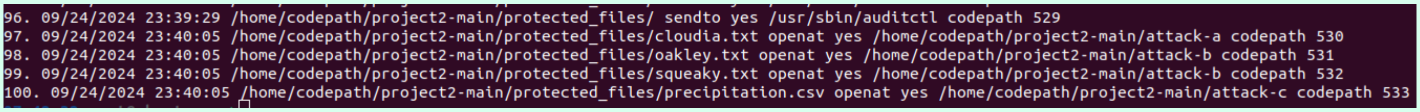
ausearch is the command to access the log
“-ts” : time start: we search in today events
“-k” : we use the key we defined “unit2_prj_changes”
“-i” : convert raw numerical values to “human-readable” form.
“> changes.txt” : I redirect the output to a text file that I can use later.

We can also use to display informations about a specific file:

```
sudo ausearch -f /home/codepath/project2-main/protected_files/cloudia.txt -i
```

We can also use the command aureport in combination with ausearch to show directly the effects of the attack:

```
sudo ausearch --start yesterday --end now -k unit2_prj_changes | aureport -f -i
```



```
96. 09/24/2024 23:39:29 /home/codepath/project2-main/protected_files/ sendto yes /usr/sbin/auditctl codepath 529
97. 09/24/2024 23:40:05 /home/codepath/project2-main/protected_files/cloudia.txt openat yes /home/codepath/project2-main/attack-a codepath 530
98. 09/24/2024 23:40:05 /home/codepath/project2-main/protected_files/oakley.txt openat yes /home/codepath/project2-main/attack-b codepath 531
99. 09/24/2024 23:40:05 /home/codepath/project2-main/protected_files/squeaky.txt openat yes /home/codepath/project2-main/attack-b codepath 532
100. 09/24/2024 23:40:05 /home/codepath/project2-main/protected_files/precipitation.csv openat yes /home/codepath/project2-main/attack-c codepath 533
```

📢 **Shoutouts:** Share appreciation for anyone who helped you out with this project or made your day a little better!

ALL TEAM 17 !!! Special shoudout to Isael MELENDEZ

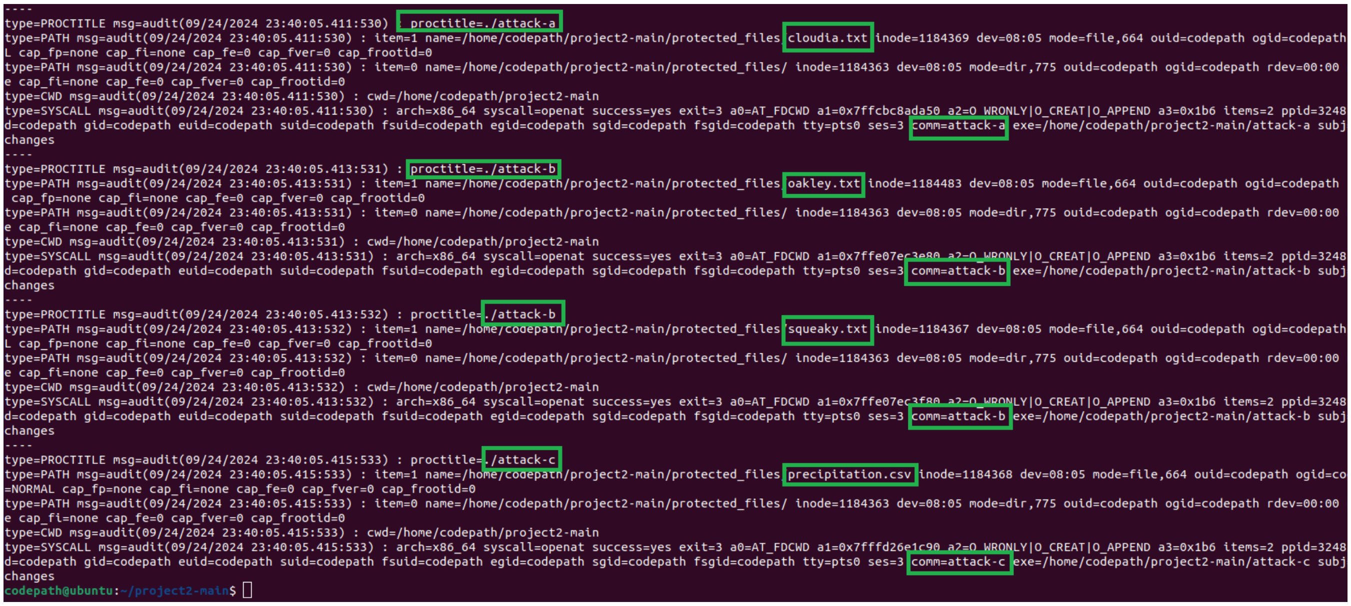
Required Challenges (Required)

Item #1: The names of the affected files:

/home/codepath/project2-main/protected_files/cloudia.txt
/home/codepath/project2-main/protected_files/oakley.txt
/home/codepath/project2-main/protected_files/squeaky.txt
/home/codepath/project2-main/protected_files/precipitation.csv

Item #2: The (file, attack) pairings of which attack changed which file:

cloudia.txt, attack-a
oakley.txt, attack-b
squeaky.txt, attack-b
precipitation.csv, attack-c



```
----
type=PROCTITLE msg=audit(09/24/2024 23:40:05.411:530) : proctitle=./attack-a
type=PATH msg=audit(09/24/2024 23:40:05.411:530) : item=1 name=/home/codepath/project2-main/protected_files/cloudia.txt inode=1184369 dev=08:05 mode=file,664 ouid=codepath ogid=codepath
L cap_fp=none cap_fi=none cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(09/24/2024 23:40:05.411:530) : item=0 name=/home/codepath/project2-main/protected_files/ inode=1184363 dev=08:05 mode=dir,775 ouid=codepath ogid=codepath rdev=00:00
e cap_fi=none cap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(09/24/2024 23:40:05.411:530) : cwd=/home/codepath/project2-main
type=SYSCALL msg=audit(09/24/2024 23:40:05.411:530) : arch=x86_64 syscall=openat success=yes exit=3 a0=AT_FDCWD a1=0x7ffcbc8ada50 a2=O_WRONLY|O_CREAT|O_APPEND a3=0x1b6 items=2 ppid=3248
d=codepath gid=codepath euid=codepath suid=codepath fsuid=codepath egid=codepath sgid=codepath fsgid=codepath tty=pts0 ses=3 comm=attack-a exe=/home/codepath/project2-main/attack-a subj
changes
----
type=PROCTITLE msg=audit(09/24/2024 23:40:05.413:531) : proctitle=./attack-b
type=PATH msg=audit(09/24/2024 23:40:05.413:531) : item=1 name=/home/codepath/project2-main/protected_files/oakley.txt inode=1184483 dev=08:05 mode=file,664 ouid=codepath ogid=codepath
 cap_fp=none cap_fi=none cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(09/24/2024 23:40:05.413:531) : item=0 name=/home/codepath/project2-main/protected_files/ inode=1184363 dev=08:05 mode=dir,775 ouid=codepath ogid=codepath rdev=00:00
e cap_fi=none cap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(09/24/2024 23:40:05.413:531) : cwd=/home/codepath/project2-main
type=SYSCALL msg=audit(09/24/2024 23:40:05.413:531) : arch=x86_64 syscall=openat success=yes exit=3 a0=AT_FDCWD a1=0x7ffe07ec3e80 a2=O_WRONLY|O_CREAT|O_APPEND a3=0x1b6 items=2 ppid=3248
d=codepath gid=codepath euid=codepath suid=codepath fsuid=codepath egid=codepath sgid=codepath fsgid=codepath tty=pts0 ses=3 comm=attack-b exe=/home/codepath/project2-main/attack-b subj
changes
----
type=PROCTITLE msg=audit(09/24/2024 23:40:05.413:532) : proctitle=./attack-b
type=PATH msg=audit(09/24/2024 23:40:05.413:532) : item=1 name=/home/codepath/project2-main/protected_files/squeaky.txt inode=1184367 dev=08:05 mode=file,664 ouid=codepath ogid=codepath
L cap_fp=none cap_fi=none cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(09/24/2024 23:40:05.413:532) : item=0 name=/home/codepath/project2-main/protected_files/ inode=1184363 dev=08:05 mode=dir,775 ouid=codepath ogid=codepath rdev=00:00
e cap_fi=none cap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(09/24/2024 23:40:05.413:532) : cwd=/home/codepath/project2-main
type=SYSCALL msg=audit(09/24/2024 23:40:05.413:532) : arch=x86_64 syscall=openat success=yes exit=3 a0=AT_FDCWD a1=0x7ffe07ec3f80 a2=O_WRONLY|O_CREAT|O_APPEND a3=0x1b6 items=2 ppid=3248
d=codepath gid=codepath euid=codepath suid=codepath fsuid=codepath egid=codepath sgid=codepath fsgid=codepath tty=pts0 ses=3 comm=attack-b exe=/home/codepath/project2-main/attack-b subj
changes
----
type=PROCTITLE msg=audit(09/24/2024 23:40:05.415:533) : proctitle=./attack-c
type=PATH msg=audit(09/24/2024 23:40:05.415:533) : item=1 name=/home/codepath/project2-main/protected_files/precipitation.csv inode=1184368 dev=08:05 mode=file,664 ouid=codepath ogid=co
=NORMAL cap_fp=none cap_fi=none cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(09/24/2024 23:40:05.415:533) : item=0 name=/home/codepath/project2-main/protected_files/ inode=1184363 dev=08:05 mode=dir,775 ouid=codepath ogid=codepath rdev=00:00
e cap_fi=none cap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(09/24/2024 23:40:05.415:533) : cwd=/home/codepath/project2-main
type=SYSCALL msg=audit(09/24/2024 23:40:05.415:533) : arch=x86_64 syscall=openat success=yes exit=3 a0=AT_FDCWD a1=0x7fffd26e1c90 a2=O_WRONLY|O_CREAT|O_APPEND a3=0x1b6 items=2 ppid=3248
d=codepath gid=codepath euid=codepath suid=codepath fsuid=codepath egid=codepath sgid=codepath fsgid=codepath tty=pts0 ses=3 comm=attack-c exe=/home/codepath/project2-main/attack-c subj
changes
codepath@ubuntu:~/project2-main$ 
```

Submission Checklist

👉*Check off each of the features you have completed.* ***You will only be graded on the features you check off.***

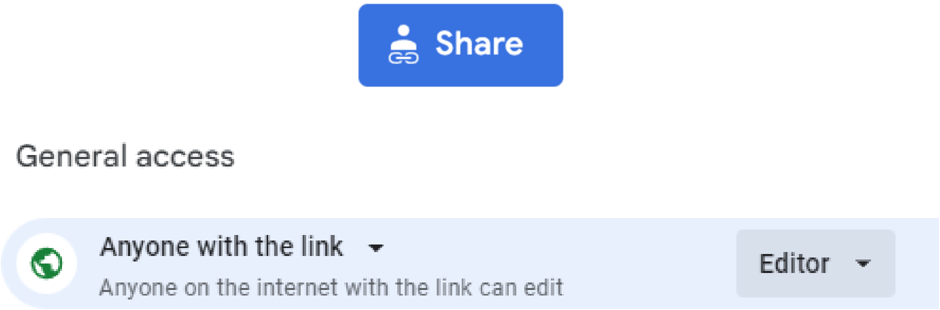
Required Challenges

- ~~Item #1~~
- ~~Item #2~~

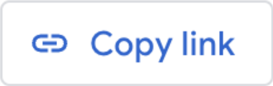
💡Tip: You can see specific grading information, including points breakdown, by going to 🔗 the grading page on the course portal.

Submit your work!

Step 1: **Click** the Share button at the top of your screen double check that anyone with the link can edit.



Step 2: **Copy** the link to this document.



Step 3: **Submit** the link on the portal.