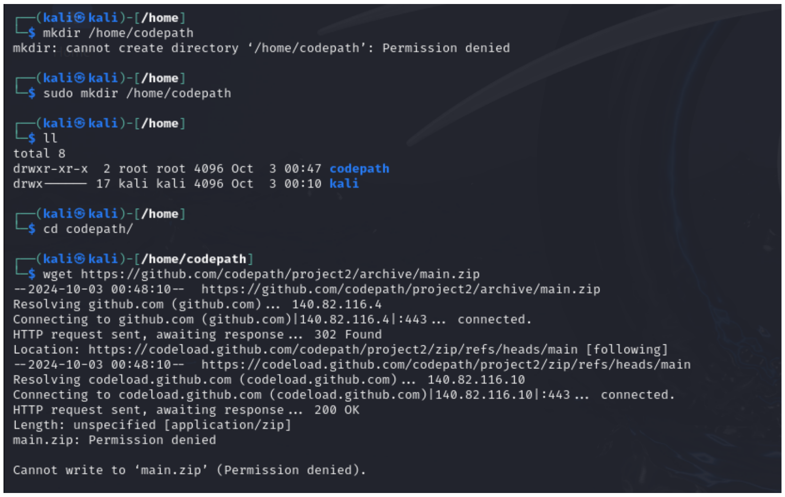
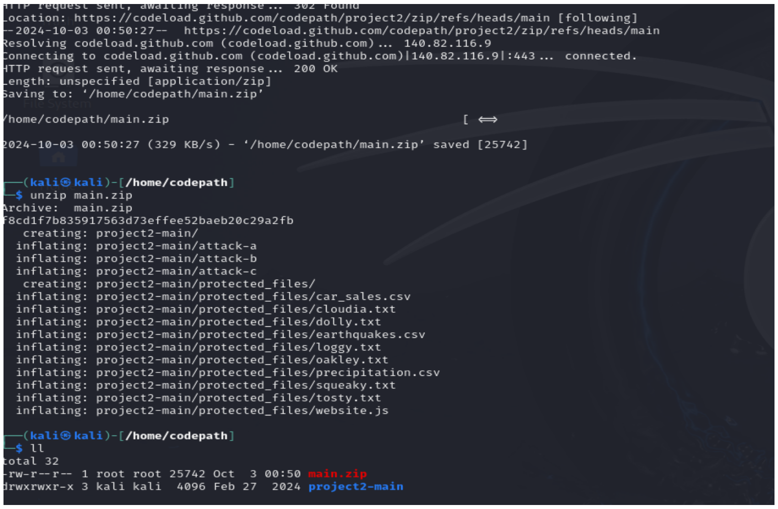
Step 1 : Create a codepath directory :
Download the Starter Repo to your VM (make sure you are in the ~ directory so filepaths are consistent) with the command wget https://github.com/codepath/project2/archive/main.zip.

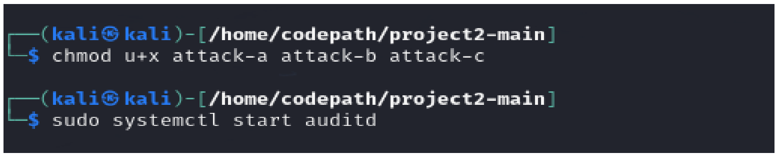


```
┌──(kali㉿kali)-[/home]
└─$ mkdir /home/codepath
mkdir: cannot create directory '/home/codepath': Permission denied

┌──(kali㉿kali)-[/home]
└─$ sudo mkdir /home/codepath

┌──(kali㉿kali)-[/home]
└─$ ll
total 8
drwxr-xr-x  2 root root 4096 Oct  3 00:47 codepath
drwx────── 17 kali kali 4096 Oct  3 00:10 kali

┌──(kali㉿kali)-[/home]
└─$ cd codepath/

┌──(kali㉿kali)-[/home/codepath]
└─$ wget https://github.com/codepath/project2/archive/main.zip
--2024-10-03 00:48:10--  https://github.com/codepath/project2/archive/main.zip
Resolving github.com (github.com)... 140.82.116.4
Connecting to github.com (github.com)|140.82.116.4|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/codepath/project2/zip/refs/heads/main [following]
--2024-10-03 00:48:10--  https://codeload.github.com/codepath/project2/zip/refs/heads/main
Resolving codeload.github.com (codeload.github.com)... 140.82.116.10
Connecting to codeload.github.com (codeload.github.com)|140.82.116.10|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/zip]
main.zip: Permission denied

Cannot write to 'main.zip' (Permission denied).
```



```
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/codepath/project2/zip/refs/heads/main [following]
--2024-10-03 00:50:27--  https://codeload.github.com/codepath/project2/zip/refs/heads/main
Resolving codeload.github.com (codeload.github.com)... 140.82.116.9
Connecting to codeload.github.com (codeload.github.com)|140.82.116.9|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/zip]
Saving to: '/home/codepath/main.zip'

/home/codepath/main.zip                              [ <=>

2024-10-03 00:50:27 (329 KB/s) - '/home/codepath/main.zip' saved [25742]


┌──(kali㉿kali)-[/home/codepath]
└─$ unzip main.zip
Archive:  main.zip
f8cd1f7b835917563d73effee52baeb20c29a2fb
   creating: project2-main/
  inflating: project2-main/attack-a
  inflating: project2-main/attack-b
  inflating: project2-main/attack-c
   creating: project2-main/protected_files/
  inflating: project2-main/protected_files/car_sales.csv
  inflating: project2-main/protected_files/cloudia.txt
  inflating: project2-main/protected_files/dolly.txt
  inflating: project2-main/protected_files/earthquakes.csv
  inflating: project2-main/protected_files/loggy.txt
  inflating: project2-main/protected_files/oakley.txt
  inflating: project2-main/protected_files/precipitation.csv
  inflating: project2-main/protected_files/squeaky.txt
  inflating: project2-main/protected_files/tosty.txt
  inflating: project2-main/protected_files/website.js

┌──(kali㉿kali)-[/home/codepath]
└─$ ll
total 32
-rw-r--r-- 1 root root 25742 Oct  3 00:50 main.zip
drwxrwxr-x 3 kali kali  4096 Feb 27  2024 project2-main
```

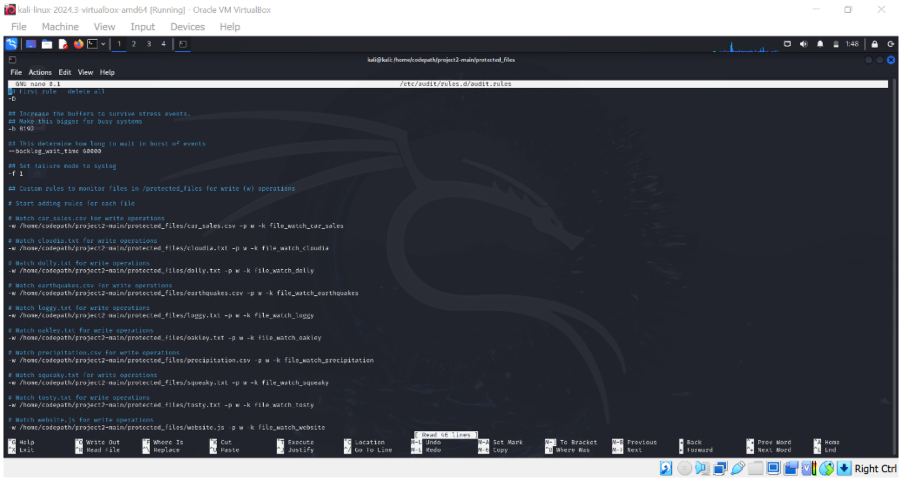
Step 2 : **Set Permissions for Attack Scripts**



```
┌──(kali㉿kali)-[/home/codepath/project2-main]
└─$ chmod u+x attack-a attack-b attack-c

┌──(kali㉿kali)-[/home/codepath/project2-main]
└─$ sudo systemctl start auditd
```

Step 3 :

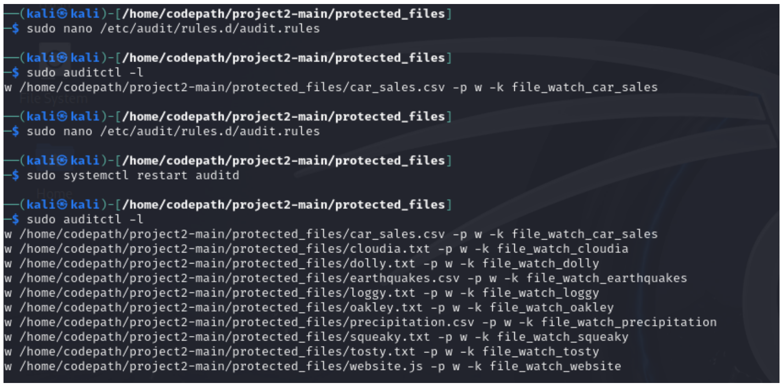
Configure Audit Rules to Monitor File Changes



kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: /home/codepath/project2-main/protected_files
File Actions Edit View Help
Right Ctrl

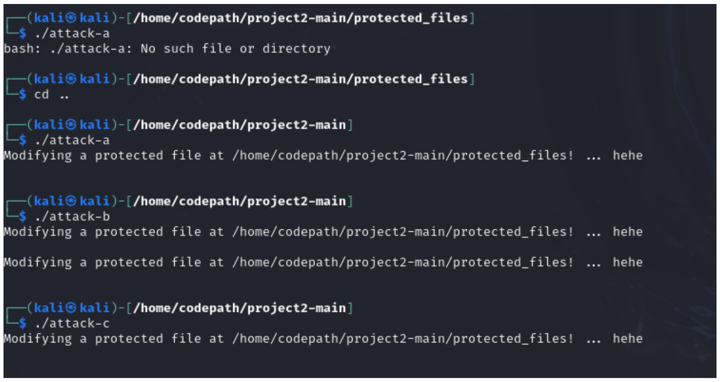
```
  GNU nano 8.1                                   /etc/audit/rules.d/audit.rules
## First rule - delete all
-D

## Increase the buffers to survive stress events.
## Make this bigger for busy systems
-b 8192

## This determine how long to wait in burst of events
--backlog_wait_time 60000

## Set failure mode to syslog
-f 1

## Custom rules to monitor files in /protected_files for write (w) operations

# Start adding rules for each file

# Watch car_sales.csv for write operations
-w /home/codepath/project2-main/protected_files/car_sales.csv -p w -k file_watch_car_sales

# Watch cloudia.txt for write operations
-w /home/codepath/project2-main/protected_files/cloudia.txt -p w -k file_watch_cloudia

# Watch dolly.txt for write operations
-w /home/codepath/project2-main/protected_files/dolly.txt -p w -k file_watch_dolly

# Watch earthquakes.csv for write operations
-w /home/codepath/project2-main/protected_files/earthquakes.csv -p w -k file_watch_earthquakes

# Watch loggy.txt for write operations
-w /home/codepath/project2-main/protected_files/loggy.txt -p w -k file_watch_loggy

# Watch oakley.txt for write operations
-w /home/codepath/project2-main/protected_files/oakley.txt -p w -k file_watch_oakley

# Watch precipitation.csv for write operations
-w /home/codepath/project2-main/protected_files/precipitation.csv -p w -k file_watch_precipitation

# Watch squeaky.txt for write operations
-w /home/codepath/project2-main/protected_files/squeaky.txt -p w -k file_watch_squeaky

# Watch tosty.txt for write operations
-w /home/codepath/project2-main/protected_files/tosty.txt -p w -k file_watch_tosty

# Watch website.js for write operations
-w /home/codepath/project2-main/protected_files/website.js -p w -k file_watch_website
                                   [ Read 46 lines ]
^G Help      ^O Write Out  ^F Where Is   ^K Cut    ^T Execute  ^C Location    M-U Undo  M-A Set Mark  M-] To Bracket  M-Q Previous  ^B Back     ^◀ Prev Word  ^A Home
^X Exit      ^R Read File  ^\ Replace    ^U Paste  ^J Justify  ^/ Go To Line  M-E Redo  M-6 Copy      ^Q Where Was    M-W Next      ^F Forward  ^▶ Next Word  ^E End
```

Restart Audit :



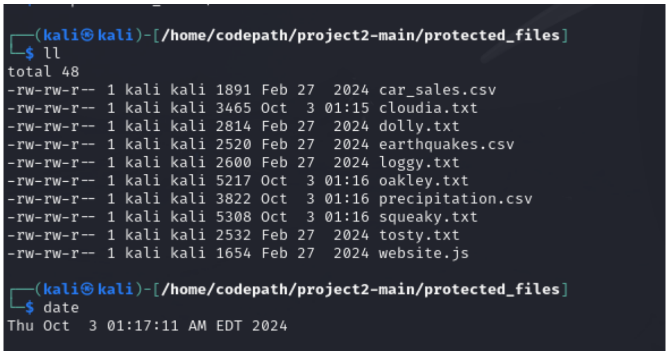
```
┌──(kali㉿kali)-[/home/codepath/project2-main/protected_files]
└─$ sudo nano /etc/audit/rules.d/audit.rules

┌──(kali㉿kali)-[/home/codepath/project2-main/protected_files]
└─$ sudo auditctl -l
w /home/codepath/project2-main/protected_files/car_sales.csv -p w -k file_watch_car_sales

┌──(kali㉿kali)-[/home/codepath/project2-main/protected_files]
└─$ sudo nano /etc/audit/rules.d/audit.rules

┌──(kali㉿kali)-[/home/codepath/project2-main/protected_files]
└─$ sudo systemctl restart auditd

┌──(kali㉿kali)-[/home/codepath/project2-main/protected_files]
└─$ sudo auditctl -l
w /home/codepath/project2-main/protected_files/car_sales.csv -p w -k file_watch_car_sales
w /home/codepath/project2-main/protected_files/cloudia.txt -p w -k file_watch_cloudia
w /home/codepath/project2-main/protected_files/dolly.txt -p w -k file_watch_dolly
w /home/codepath/project2-main/protected_files/earthquakes.csv -p w -k file_watch_earthquakes
w /home/codepath/project2-main/protected_files/loggy.txt -p w -k file_watch_loggy
w /home/codepath/project2-main/protected_files/oakley.txt -p w -k file_watch_oakley
w /home/codepath/project2-main/protected_files/precipitation.csv -p w -k file_watch_precipitation
w /home/codepath/project2-main/protected_files/squeaky.txt -p w -k file_watch_squeaky
w /home/codepath/project2-main/protected_files/tosty.txt -p w -k file_watch_tosty
w /home/codepath/project2-main/protected_files/website.js -p w -k file_watch_website
```

Step 4 : Run the Attack Scripts

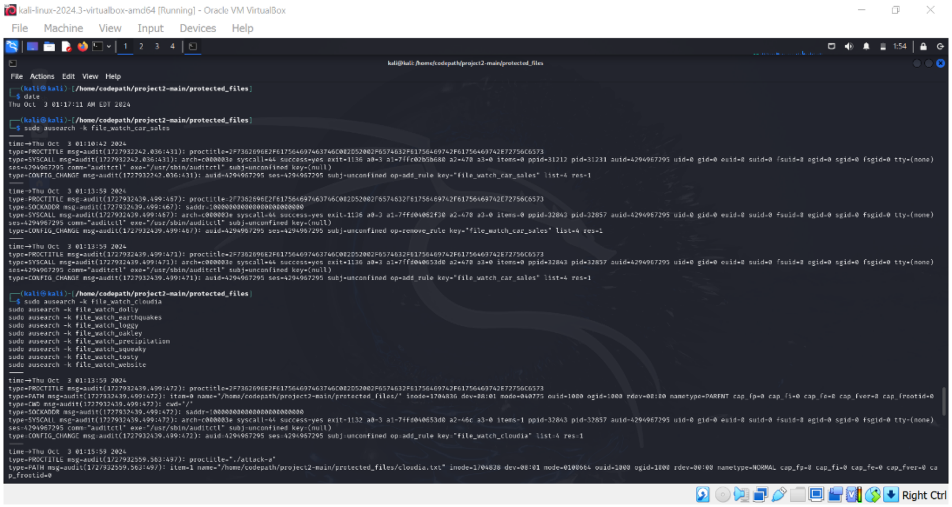


```
┌──(kali㉿kali)-[/home/codepath/project2-main/protected_files]
└─$ ./attack-a
bash: ./attack-a: No such file or directory

┌──(kali㉿kali)-[/home/codepath/project2-main/protected_files]
└─$ cd ..

┌──(kali㉿kali)-[/home/codepath/project2-main]
└─$ ./attack-a
Modifying a protected file at /home/codepath/project2-main/protected_files! ... hehe


┌──(kali㉿kali)-[/home/codepath/project2-main]
└─$ ./attack-b
Modifying a protected file at /home/codepath/project2-main/protected_files! ... hehe

Modifying a protected file at /home/codepath/project2-main/protected_files! ... hehe


┌──(kali㉿kali)-[/home/codepath/project2-main]
└─$ ./attack-c
Modifying a protected file at /home/codepath/project2-main/protected_files! ... hehe
```

Step 5 : Analyze Audit Logs to Identify Changes



```
┌──(kali㉿kali)-[/home/codepath/project2-main/protected_files]
└─$ ll
total 48
-rw-rw-r-- 1 kali kali 1891 Feb 27  2024 car_sales.csv
-rw-rw-r-- 1 kali kali 3465 Oct  3 01:15 cloudia.txt
-rw-rw-r-- 1 kali kali 2814 Feb 27  2024 dolly.txt
-rw-rw-r-- 1 kali kali 2520 Feb 27  2024 earthquakes.csv
-rw-rw-r-- 1 kali kali 2600 Feb 27  2024 loggy.txt
-rw-rw-r-- 1 kali kali 5217 Oct  3 01:16 oakley.txt
-rw-rw-r-- 1 kali kali 3822 Oct  3 01:16 precipitation.csv
-rw-rw-r-- 1 kali kali 5308 Oct  3 01:16 squeaky.txt
-rw-rw-r-- 1 kali kali 2532 Feb 27  2024 tosty.txt
-rw-rw-r-- 1 kali kali 1654 Feb 27  2024 website.js

┌──(kali㉿kali)-[/home/codepath/project2-main/protected_files]
└─$ date
Thu Oct  3 01:17:11 AM EDT 2024
```


kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
1
2
3
4
1:54
kali@kali: /home/codepath/project2-main/protected_files
File
Actions
Edit
View
Help
Right Ctrl

```
┌──(kali㉿kali)-[/home/codepath/project2-main/protected_files]
└─$ date
Thu Oct  3 01:17:11 AM EDT 2024

┌──(kali㉿kali)-[/home/codepath/project2-main/protected_files]
└─$ sudo ausearch -k file_watch_car_sales
----
time->Thu Oct  3 01:10:42 2024
type=PROCTITLE msg=audit(1727932242.036:431): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469742E72756C6573
type=SYSCALL msg=audit(1727932242.036:431): arch=c000003e syscall=44 success=yes exit=1136 a0=3 a1=7ffc02b5b680 a2=478 a3=0 items=0 ppid=31212 pid=31231 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none)
ses=4294967295 comm="auditctl" exe="/usr/sbin/auditctl" subj=unconfined key=(null)
type=CONFIG_CHANGE msg=audit(1727932242.036:431): auid=4294967295 ses=4294967295 subj=unconfined op=add_rule key="file_watch_car_sales" list=4 res=1
----
time->Thu Oct  3 01:13:59 2024
type=PROCTITLE msg=audit(1727932439.499:467): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469742E72756C6573
type=SOCKADDR msg=audit(1727932439.499:467): saddr=100000000000000000000000
type=SYSCALL msg=audit(1727932439.499:467): arch=c000003e syscall=44 success=yes exit=1136 a0=3 a1=7ffd04062f30 a2=478 a3=0 items=0 ppid=32843 pid=32857 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none)
ses=4294967295 comm="auditctl" exe="/usr/sbin/auditctl" subj=unconfined key=(null)
type=CONFIG_CHANGE msg=audit(1727932439.499:467): auid=4294967295 ses=4294967295 subj=unconfined op=remove_rule key="file_watch_car_sales" list=4 res=1
----
time->Thu Oct  3 01:13:59 2024
type=PROCTITLE msg=audit(1727932439.499:471): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469742E72756C6573
type=SYSCALL msg=audit(1727932439.499:471): arch=c000003e syscall=44 success=yes exit=1136 a0=3 a1=7ffd040653d0 a2=478 a3=0 items=0 ppid=32843 pid=32857 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none)
ses=4294967295 comm="auditctl" exe="/usr/sbin/auditctl" subj=unconfined key=(null)
type=CONFIG_CHANGE msg=audit(1727932439.499:471): auid=4294967295 ses=4294967295 subj=unconfined op=add_rule key="file_watch_car_sales" list=4 res=1

┌──(kali㉿kali)-[/home/codepath/project2-main/protected_files]
└─$ sudo ausearch -k file_watch_cloudia
sudo ausearch -k file_watch_dolly
sudo ausearch -k file_watch_earthquakes
sudo ausearch -k file_watch_loggy
sudo ausearch -k file_watch_oakley
sudo ausearch -k file_watch_precipitation
sudo ausearch -k file_watch_squeaky
sudo ausearch -k file_watch_tosty
sudo ausearch -k file_watch_website
----
time->Thu Oct  3 01:13:59 2024
type=PROCTITLE msg=audit(1727932439.499:472): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469742E72756C6573
type=PATH msg=audit(1727932439.499:472): item=0 name="/home/codepath/project2-main/protected_files/" inode=1704836 dev=08:01 mode=040775 ouid=1000 ogid=1000 rdev=00:00 nametype=PARENT cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(1727932439.499:472): cwd="/"
type=SOCKADDR msg=audit(1727932439.499:472): saddr=100000000000000000000000
type=SYSCALL msg=audit(1727932439.499:472): arch=c000003e syscall=44 success=yes exit=1132 a0=3 a1=7ffd040653d0 a2=46c a3=0 items=1 ppid=32843 pid=32857 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none)
ses=4294967295 comm="auditctl" exe="/usr/sbin/auditctl" subj=unconfined key=(null)
type=CONFIG_CHANGE msg=audit(1727932439.499:472): auid=4294967295 ses=4294967295 subj=unconfined op=add_rule key="file_watch_cloudia" list=4 res=1
----
time->Thu Oct  3 01:15:59 2024
type=PROCTITLE msg=audit(1727932559.563:497): proctitle="./attack-a"
type=PATH msg=audit(1727932559.563:497): item=1 name="/home/codepath/project2-main/protected_files/cloudia.txt" inode=1704838 dev=08:01 mode=0100664 ouid=1000 ogid=1000 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 ca
p_frootid=0
```