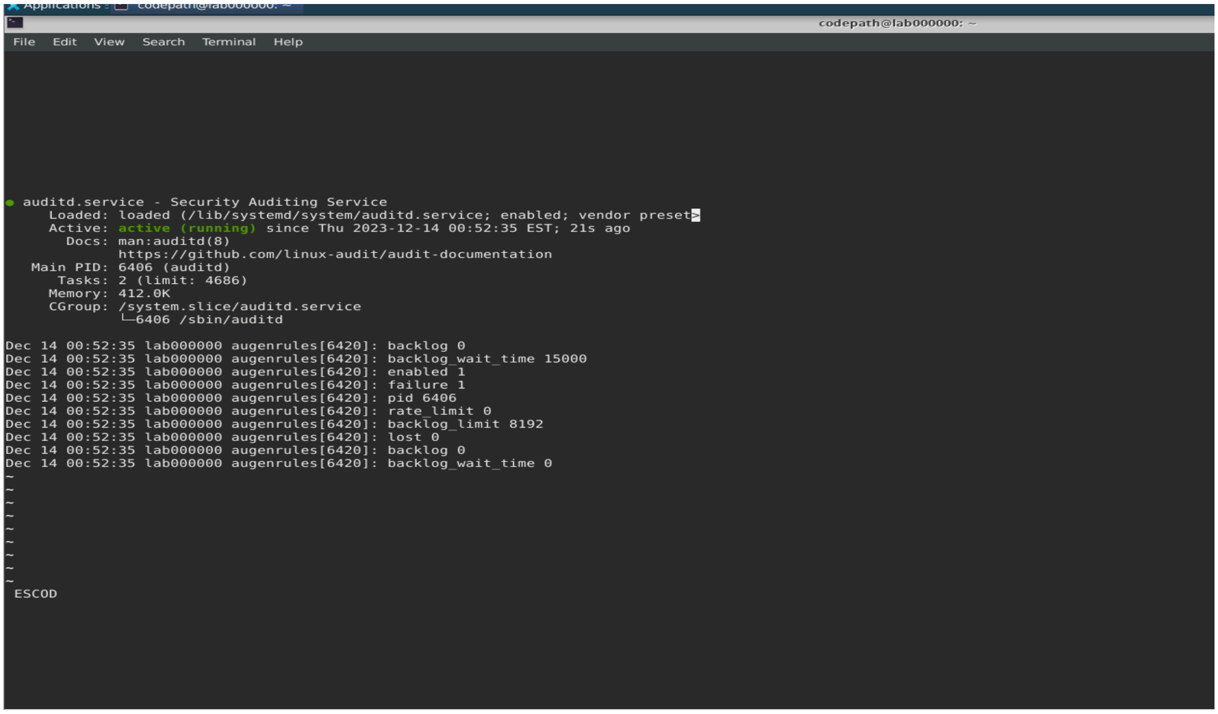
MILOT JEUNE
Project 2

HIDS(Host Intrusion Detection System) AUDITS

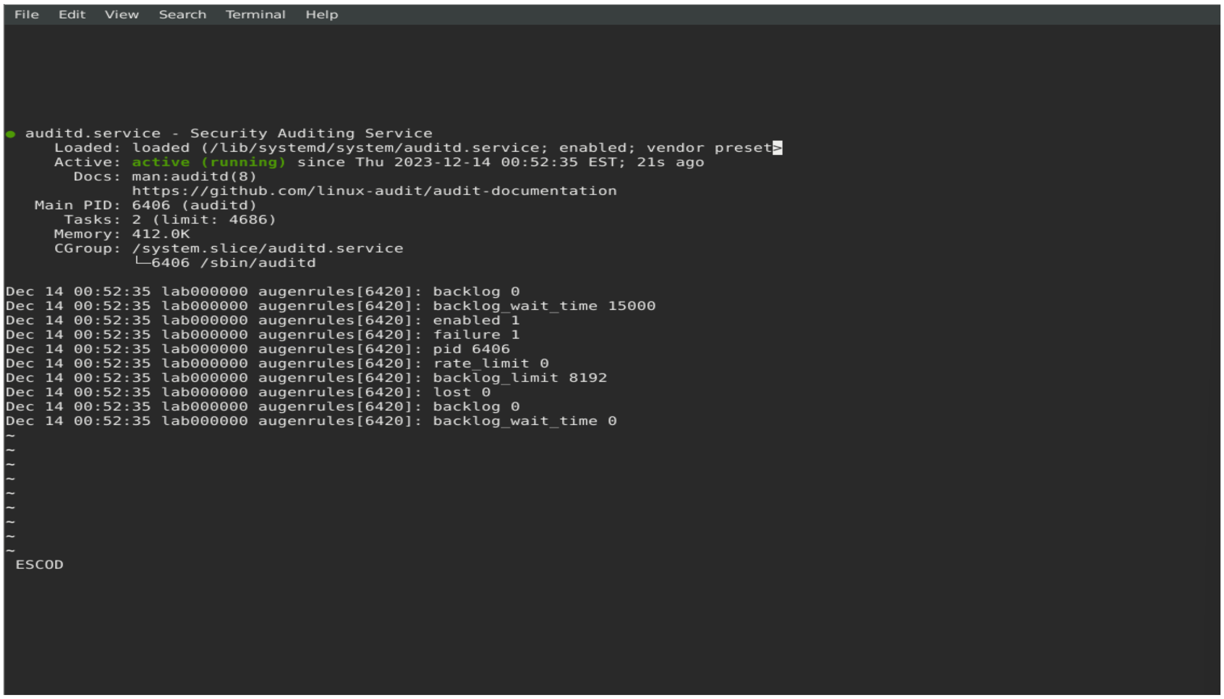
Summary

In a past project, I implemented a HIDS (Host Intrusion Detection System) known as HIDS Audit on a host device. The objective was to monitor the device for suspicious activities without the necessity of creating a predefined ruleset for detection. Utilizing the Linux Auditing System located in /var/log, I successfully configured the HIDS to provide a detailed log of security events, enabling effective file monitoring and enhancing overall security measures

To kick off the process, I started by ensuring that all our packages were up to date with the command sudo apt-get update. Following that, in Step 0, we proceeded to install Audit by executing sudo apt-get install auditd. I was then prompted a output verifying that Audit was up and running as intended, laying the groundwork for subsequent security measures.

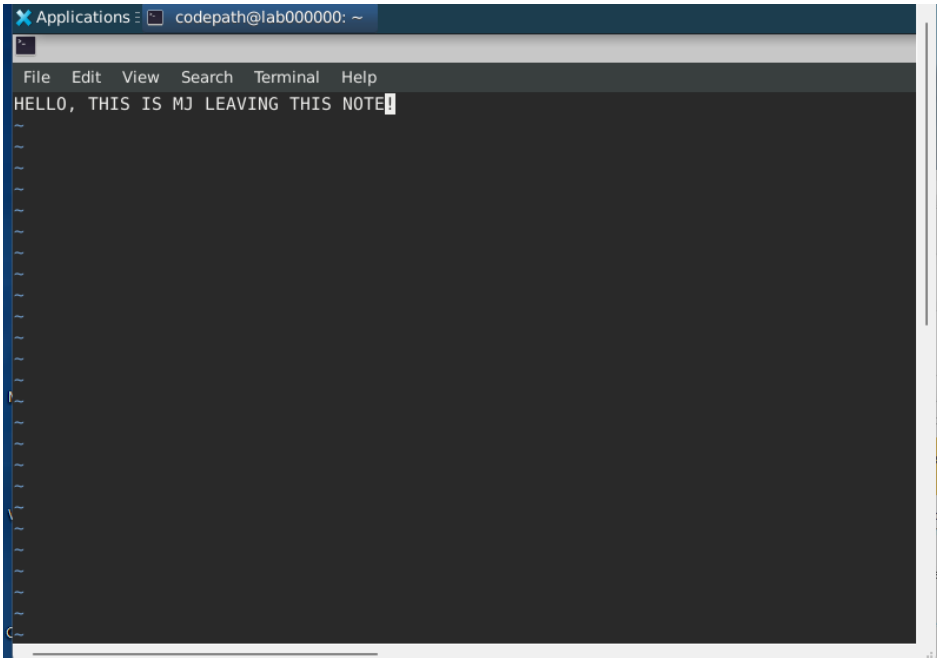


```
● auditd.service - Security Auditing Service
     Loaded: loaded (/lib/systemd/system/auditd.service; enabled; vendor preset>
     Active: active (running) since Thu 2023-12-14 00:52:35 EST; 21s ago
       Docs: man:auditd(8)
             https://github.com/linux-audit/audit-documentation
   Main PID: 6406 (auditd)
      Tasks: 2 (limit: 4686)
     Memory: 412.0K
     CGroup: /system.slice/auditd.service
             └─6406 /sbin/auditd

Dec 14 00:52:35 lab000000 augenrules[6420]: backlog 0
Dec 14 00:52:35 lab000000 augenrules[6420]: backlog_wait_time 15000
Dec 14 00:52:35 lab000000 augenrules[6420]: enabled 1
Dec 14 00:52:35 lab000000 augenrules[6420]: failure 1
Dec 14 00:52:35 lab000000 augenrules[6420]: pid 6406
Dec 14 00:52:35 lab000000 augenrules[6420]: rate_limit 0
Dec 14 00:52:35 lab000000 augenrules[6420]: backlog_limit 8192
Dec 14 00:52:35 lab000000 augenrules[6420]: lost 0
Dec 14 00:52:35 lab000000 augenrules[6420]: backlog 0
Dec 14 00:52:35 lab000000 augenrules[6420]: backlog_wait_time 0
~
~
~
~
~
~
~
~
~
 ESCOD
```



```
● auditd.service - Security Auditing Service
     Loaded: loaded (/lib/systemd/system/auditd.service; enabled; vendor preset>
     Active: active (running) since Thu 2023-12-14 00:52:35 EST; 21s ago
       Docs: man:auditd(8)
             https://github.com/linux-audit/audit-documentation
   Main PID: 6406 (auditd)
      Tasks: 2 (limit: 4686)
     Memory: 412.0K
     CGroup: /system.slice/auditd.service
             └─6406 /sbin/auditd

Dec 14 00:52:35 lab000000 augenrules[6420]: backlog 0
Dec 14 00:52:35 lab000000 augenrules[6420]: backlog_wait_time 15000
Dec 14 00:52:35 lab000000 augenrules[6420]: enabled 1
Dec 14 00:52:35 lab000000 augenrules[6420]: failure 1
Dec 14 00:52:35 lab000000 augenrules[6420]: pid 6406
Dec 14 00:52:35 lab000000 augenrules[6420]: rate_limit 0
Dec 14 00:52:35 lab000000 augenrules[6420]: backlog_limit 8192
Dec 14 00:52:35 lab000000 augenrules[6420]: lost 0
Dec 14 00:52:35 lab000000 augenrules[6420]: backlog 0
Dec 14 00:52:35 lab000000 augenrules[6420]: backlog_wait_time 0
~
~
~
~
~
~
~
~
~
 ESCOD
```

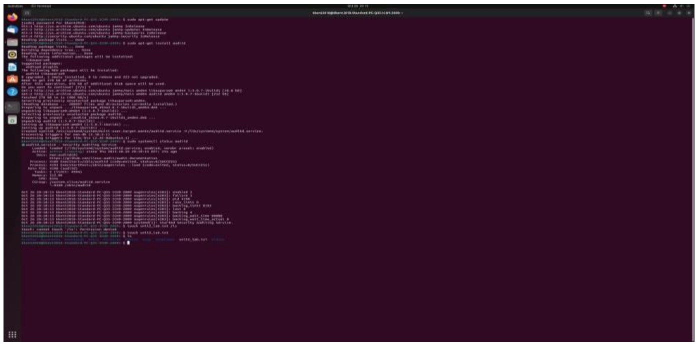
Vim, a built-in Linux text editor, proved essential in our course. It has two modes: command and insert. We switched to insert mode ('i') to edit files and seamlessly transitioned back to command mode ('Esc'). In insert mode, similar to other editors, we typed a message like "HELLO, THIS IS MJ LEAVING THIS NOTE!"



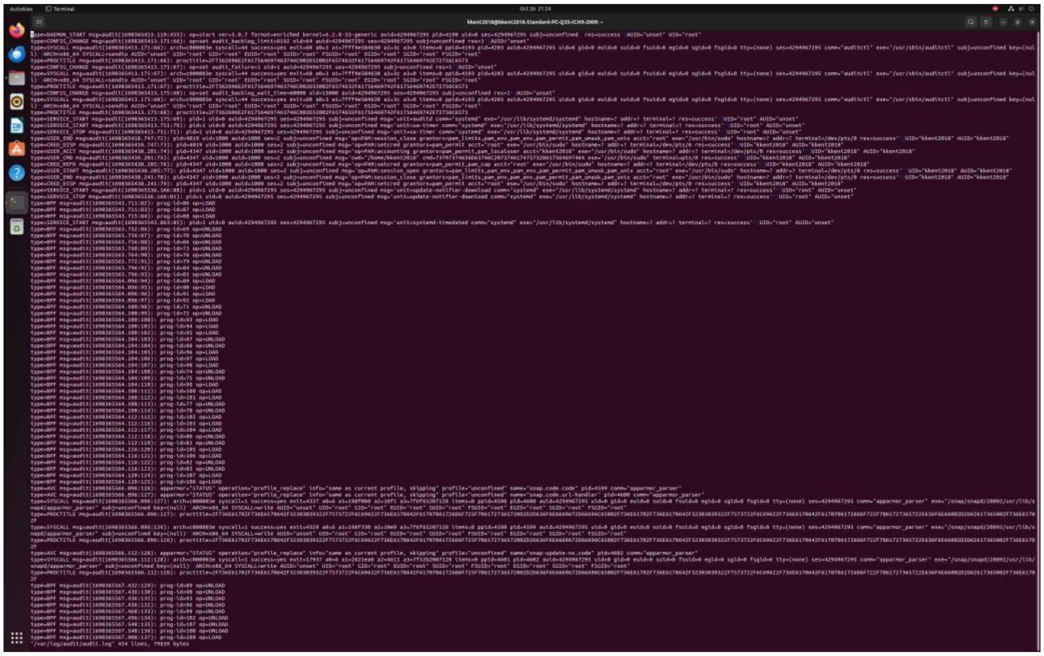
```
HELLO, THIS IS MJ LEAVING THIS NOTE!
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
```

Step 2

To initiate file monitoring, we first generated a new file named unit2_lab.txt in the ~ directory using the command touch unit2_lab.txt. A quick verification via ls confirmed the file's existence in the current directory, setting the stage for subsequent content additions.



Displaying event logs



```
type=DAEMON_START msg=audit(1698365413.119:455): op=start ver=3.0.7 format=enriched kernel=6.2.0-33-generic auid=4294967295 pid=4190 uid=0 ses=4294967295 subj=unconfined  res=success  AUID="unset" UID="root"
type=CONFIG_CHANGE msg=audit(1698365413.171:66): op=set audit_backlog_limit=8192 old=64 auid=4294967295 ses=4294967295 subj=unconfined res=1  AUID="unset"
type=SYSCALL msg=audit(1698365413.171:66): arch=c000003e syscall=44 success=yes exit=60 a0=3 a1=7fff4e584630 a2=3c a3=0 items=0 ppid=4193 pid=4203 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=(nul
l)  ARCH=x86_64 SYSCALL=sendto AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=PROCTITLE msg=audit(1698365413.171:66): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469742E72756C6573
type=CONFIG_CHANGE msg=audit(1698365413.171:67): op=set audit_failure=1 old=1 auid=4294967295 ses=4294967295 subj=unconfined res=1  AUID="unset"
type=SYSCALL msg=audit(1698365413.171:67): arch=c000003e syscall=44 success=yes exit=60 a0=3 a1=7fff4e584630 a2=3c a3=0 items=0 ppid=4193 pid=4203 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=(nul
l)  ARCH=x86_64 SYSCALL=sendto AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=PROCTITLE msg=audit(1698365413.171:67): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469742E72756C6573
type=CONFIG_CHANGE msg=audit(1698365413.175:68): op=set audit_backlog_wait_time=60000 old=15000 auid=4294967295 ses=4294967295 subj=unconfined res=1  AUID="unset"
type=SYSCALL msg=audit(1698365413.175:68): arch=c000003e syscall=44 success=yes exit=60 a0=3 a1=7fff4e584630 a2=3c a3=0 items=0 ppid=4193 pid=4203 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=(nul
l)  ARCH=x86_64 SYSCALL=sendto AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=PROCTITLE msg=audit(1698365413.175:68): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469742E72756C6573
type=SERVICE_START msg=audit(1698365413.175:69): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=unconfined msg='unit=auditd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'  UID="root" AUID="unset"
type=SERVICE_START msg=audit(1698365413.751:70): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=unconfined msg='unit=ua-timer comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'  UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1698365413.751:71): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=unconfined msg='unit=ua-timer comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'  UID="root" AUID="unset"
type=USER_END msg=audit(1698365418.747:72): pid=4019 uid=1000 auid=1000 ses=2 subj=unconfined msg='op=PAM:session_close grantors=pam_limits,pam_env,pam_env,pam_permit,pam_umask,pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'  UID="kkent2018" AUID="kkent2018"
type=CRED_DISP msg=audit(1698365418.747:73): pid=4019 uid=1000 auid=1000 ses=2 subj=unconfined msg='op=PAM:setcred grantors=pam_permit acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'  UID="kkent2018" AUID="kkent2018"
type=USER_ACCT msg=audit(1698365430.201:74): pid=4347 uid=1000 auid=1000 ses=2 subj=unconfined msg='op=PAM:accounting grantors=pam_permit,pam_localuser acct="kkent2018" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'  UID="kkent2018" AUID="kkent2018"
type=USER_CMD msg=audit(1698365430.201:75): pid=4347 uid=1000 auid=1000 ses=2 subj=unconfined msg='cwd="/home/kkent2018" cmd=73797374656D63746C2073746174757320617564697464 exe="/usr/bin/sudo" terminal=pts/0 res=success'  UID="kkent2018" AUID="kkent2018"
type=CRED_REFR msg=audit(1698365430.205:76): pid=4347 uid=1000 auid=1000 ses=2 subj=unconfined msg='op=PAM:setcred grantors=pam_permit,pam_cap acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'  UID="kkent2018" AUID="kkent2018"
type=USER_START msg=audit(1698365430.205:77): pid=4347 uid=1000 auid=1000 ses=2 subj=unconfined msg='op=PAM:session_open grantors=pam_limits,pam_env,pam_env,pam_permit,pam_umask,pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'  UID="kkent2018" AUID="kkent2018"
type=USER_END msg=audit(1698365430.241:78): pid=4347 uid=1000 auid=1000 ses=2 subj=unconfined msg='op=PAM:session_close grantors=pam_limits,pam_env,pam_env,pam_permit,pam_umask,pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'  UID="kkent2018" AUID="kkent2018"
type=CRED_DISP msg=audit(1698365430.241:79): pid=4347 uid=1000 auid=1000 ses=2 subj=unconfined msg='op=PAM:setcred grantors=pam_permit acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'  UID="kkent2018" AUID="kkent2018"
type=SERVICE_START msg=audit(1698365536.166:80): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=unconfined msg='unit=update-notifier-download comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'  UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1698365536.166:81): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=unconfined msg='unit=update-notifier-download comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'  UID="root" AUID="unset"
type=BPF msg=audit(1698365543.711:82): prog-id=86 op=LOAD
type=BPF msg=audit(1698365543.711:83): prog-id=87 op=LOAD
type=BPF msg=audit(1698365543.715:84): prog-id=88 op=LOAD
type=SERVICE_START msg=audit(1698365543.863:85): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=unconfined msg='unit=systemd-timedated comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'  UID="root" AUID="unset"
type=BPF msg=audit(1698365563.752:86): prog-id=69 op=UNLOAD
type=BPF msg=audit(1698365563.756:87): prog-id=70 op=UNLOAD
type=BPF msg=audit(1698365563.756:88): prog-id=66 op=UNLOAD
type=BPF msg=audit(1698365563.760:89): prog-id=73 op=UNLOAD
type=BPF msg=audit(1698365563.764:90): prog-id=76 op=UNLOAD
type=BPF msg=audit(1698365563.772:91): prog-id=79 op=UNLOAD
type=BPF msg=audit(1698365563.796:92): prog-id=84 op=UNLOAD
type=BPF msg=audit(1698365563.796:93): prog-id=85 op=UNLOAD
type=BPF msg=audit(1698365564.096:94): prog-id=89 op=LOAD
type=BPF msg=audit(1698365564.096:95): prog-id=90 op=LOAD
type=BPF msg=audit(1698365564.096:96): prog-id=91 op=LOAD
type=BPF msg=audit(1698365564.096:97): prog-id=92 op=LOAD
type=BPF msg=audit(1698365564.100:98): prog-id=71 op=UNLOAD
type=BPF msg=audit(1698365564.100:99): prog-id=72 op=UNLOAD
type=BPF msg=audit(1698365564.100:100): prog-id=93 op=LOAD
type=BPF msg=audit(1698365564.100:101): prog-id=94 op=LOAD
type=BPF msg=audit(1698365564.100:102): prog-id=95 op=LOAD
type=BPF msg=audit(1698365564.104:103): prog-id=87 op=UNLOAD
type=BPF msg=audit(1698365564.104:104): prog-id=88 op=UNLOAD
type=BPF msg=audit(1698365564.104:105): prog-id=96 op=LOAD
type=BPF msg=audit(1698365564.104:106): prog-id=97 op=LOAD
type=BPF msg=audit(1698365564.104:107): prog-id=98 op=LOAD
type=BPF msg=audit(1698365564.104:108): prog-id=74 op=UNLOAD
type=BPF msg=audit(1698365564.104:109): prog-id=75 op=UNLOAD
type=BPF msg=audit(1698365564.104:110): prog-id=99 op=LOAD
type=BPF msg=audit(1698365564.108:111): prog-id=100 op=LOAD
type=BPF msg=audit(1698365564.108:112): prog-id=101 op=LOAD
type=BPF msg=audit(1698365564.108:113): prog-id=77 op=UNLOAD
type=BPF msg=audit(1698365564.108:114): prog-id=78 op=UNLOAD
type=BPF msg=audit(1698365564.112:115): prog-id=102 op=LOAD
type=BPF msg=audit(1698365564.112:116): prog-id=103 op=LOAD
type=BPF msg=audit(1698365564.112:117): prog-id=104 op=LOAD
type=BPF msg=audit(1698365564.112:118): prog-id=80 op=UNLOAD
type=BPF msg=audit(1698365564.112:119): prog-id=81 op=UNLOAD
type=BPF msg=audit(1698365564.116:120): prog-id=105 op=LOAD
type=BPF msg=audit(1698365564.116:121): prog-id=106 op=LOAD
type=BPF msg=audit(1698365564.116:122): prog-id=82 op=UNLOAD
type=BPF msg=audit(1698365564.116:123): prog-id=83 op=UNLOAD
type=BPF msg=audit(1698365564.120:124): prog-id=107 op=LOAD
type=BPF msg=audit(1698365564.120:125): prog-id=108 op=LOAD
type=AVC msg=audit(1698365566.096:126): apparmor="STATUS" operation="profile_replace" info="same as current profile, skipping" profile="unconfined" name="snap.code.code" pid=4599 comm="apparmor_parser"
type=AVC msg=audit(1698365566.096:127): apparmor="STATUS" operation="profile_replace" info="same as current profile, skipping" profile="unconfined" name="snap.code.url-handler" pid=4600 comm="apparmor_parser"
type=SYSCALL msg=audit(1698365566.096:127): arch=c000003e syscall=1 success=yes exit=4337 a0=6 a1=198f0b0 a2=10f1 a3=7f6f65207120 items=0 ppid=4598 pid=4600 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="apparmor_parser" exe="/snap/snapd/20092/usr/lib/s
napd/apparmor_parser" subj=unconfined key=(null)  ARCH=x86_64 SYSCALL=write AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=PROCTITLE msg=audit(1698365566.096:127): proctitle=2F736E61702F736E6170642F32303039322F7573722F6C69622F736E6170642F61707061726D6F725F706172736572002D2D636F6E6669672D66696C65002F736E61702F736E6170642F32303039322F7573722F6C69622F736E6170642F61707061726D6F722F7061727365722E636F6E66002D2D62617365002F736E6170
2F
type=SYSCALL msg=audit(1698365566.096:126): arch=c000003e syscall=1 success=yes exit=4329 a0=6 a1=198f330 a2=10e9 a3=7f6f65207120 items=0 ppid=4598 pid=4599 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="apparmor_parser" exe="/snap/snapd/20092/usr/lib/s
napd/apparmor_parser" subj=unconfined key=(null)  ARCH=x86_64 SYSCALL=write AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=PROCTITLE msg=audit(1698365566.096:126): proctitle=2F736E61702F736E6170642F32303039322F7573722F6C69622F736E6170642F61707061726D6F725F706172736572002D2D636F6E6669672D66696C65002F736E61702F736E6170642F32303039322F7573722F6C69622F736E6170642F61707061726D6F722F7061727365722E636F6E66002D2D62617365002F736E6170
2F
type=AVC msg=audit(1698365566.112:128): apparmor="STATUS" operation="profile_replace" info="same as current profile, skipping" profile="unconfined" name="snap-update-ns.code" pid=4602 comm="apparmor_parser"
type=SYSCALL msg=audit(1698365566.112:128): arch=c000003e syscall=1 success=yes exit=17937 a0=6 a1=2621ea0 a2=4611 a3=7f52b2007120 items=0 ppid=4601 pid=4602 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="apparmor_parser" exe="/snap/snapd/20092/usr/lib/
snapd/apparmor_parser" subj=unconfined key=(null)  ARCH=x86_64 SYSCALL=write AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=PROCTITLE msg=audit(1698365566.112:128): proctitle=2F736E61702F736E6170642F32303039322F7573722F6C69622F736E6170642F61707061726D6F725F706172736572002D2D636F6E6669672D66696C65002F736E61702F736E6170642F32303039322F7573722F6C69622F736E6170642F61707061726D6F722F7061727365722E636F6E66002D2D62617365002F736E6170
2F
type=BPF msg=audit(1698365567.432:129): prog-id=89 op=UNLOAD
type=BPF msg=audit(1698365567.436:130): prog-id=90 op=UNLOAD
type=BPF msg=audit(1698365567.436:131): prog-id=93 op=UNLOAD
type=BPF msg=audit(1698365567.436:132): prog-id=96 op=UNLOAD
type=BPF msg=audit(1698365567.460:133): prog-id=99 op=UNLOAD
type=BPF msg=audit(1698365567.496:134): prog-id=102 op=UNLOAD
type=BPF msg=audit(1698365567.548:135): prog-id=107 op=UNLOAD
type=BPF msg=audit(1698365567.548:136): prog-id=108 op=UNLOAD
type=BPF msg=audit(1698365567.908:137): prog-id=109 op=LOAD
"/var/log/audit/audit.log" 454 lines, 79839 bytes
```

POST Incident / Takeaways

Reflecting on the HIDS Audit project, I learned crucial lessons about proactive host intrusion detection. Keeping system packages updated with sudo apt-get update ensured a secure foundation. Installing Audit with sudo apt-get install auditd and verifying its operation set the stage for dynamic file monitoring without predefined rulesets.

Vim's role in editing configuration files emphasized the importance of clear documentation, and creating and confirming the existence of unit2_lab.txt showcased the HIDS's effectiveness in detecting changes.

In future projects, I'll apply these insights, prioritizing proactive security and regular system updates to maintain a resilient defense against evolving threats.