MANAGEMENT AND ANALYSIS OF SECURITY LOGS VIA A SIEM FOR A WEB SERVER

BOUTAINA MOSSADEQ
&
MERYEM DARDOURI

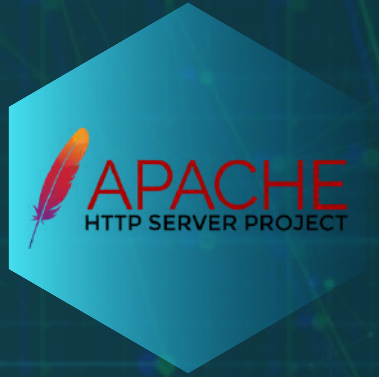
INTRODUCTION

Web servers are critical components of modern IT infrastructure, but they are also prime targets for cyberattacks. Common threats include SQL injections, brute force attacks, and unauthorized access attempts. To mitigate these risks, it's essential to monitor server activity and respond to threats in real time. This is where a SIEM (Security Information and Event Management) solution comes into play. In this project, I implemented a SIEM using the ELK stack to secure an Apache web server and analyze its logs.

OBJECTIVES

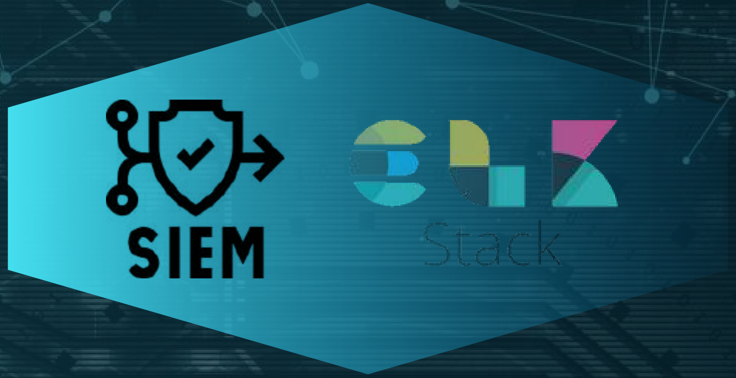
1. INSTALL AND CONFIGURE A SECURE APACHE WEB SERVER USING **SELINUX**.
2. DEPLOY THE ELK STACK—**ELASTICSEARCH**, **LOGSTASH**, AND **KIBANA**—FOR CENTRALIZED LOG MANAGEMENT.
3. CONFIGURE **FILEBEAT** TO COLLECT **APACHE** LOGS AND SEND THEM TO **LOGSTASH**.
4. ANALYZE LOGS IN **KIBANA** TO DETECT SUSPICIOUS ACTIVITIES.
5. SET UP **ALERTS** FOR POTENTIAL SECURITY INCIDENTS.
6. DEVELOP A PROCESS FOR INCIDENT RESPONSE.

KEY CONCEPTS



1. APACHE

a powerful, open-source web server widely used for hosting websites and serving web content over HTTP/HTTPS.



2. SIEM

A SIEM solution collects and analyzes logs from multiple sources to detect security threats. It provides real-time alerts and helps with incident response.

ELK STACK

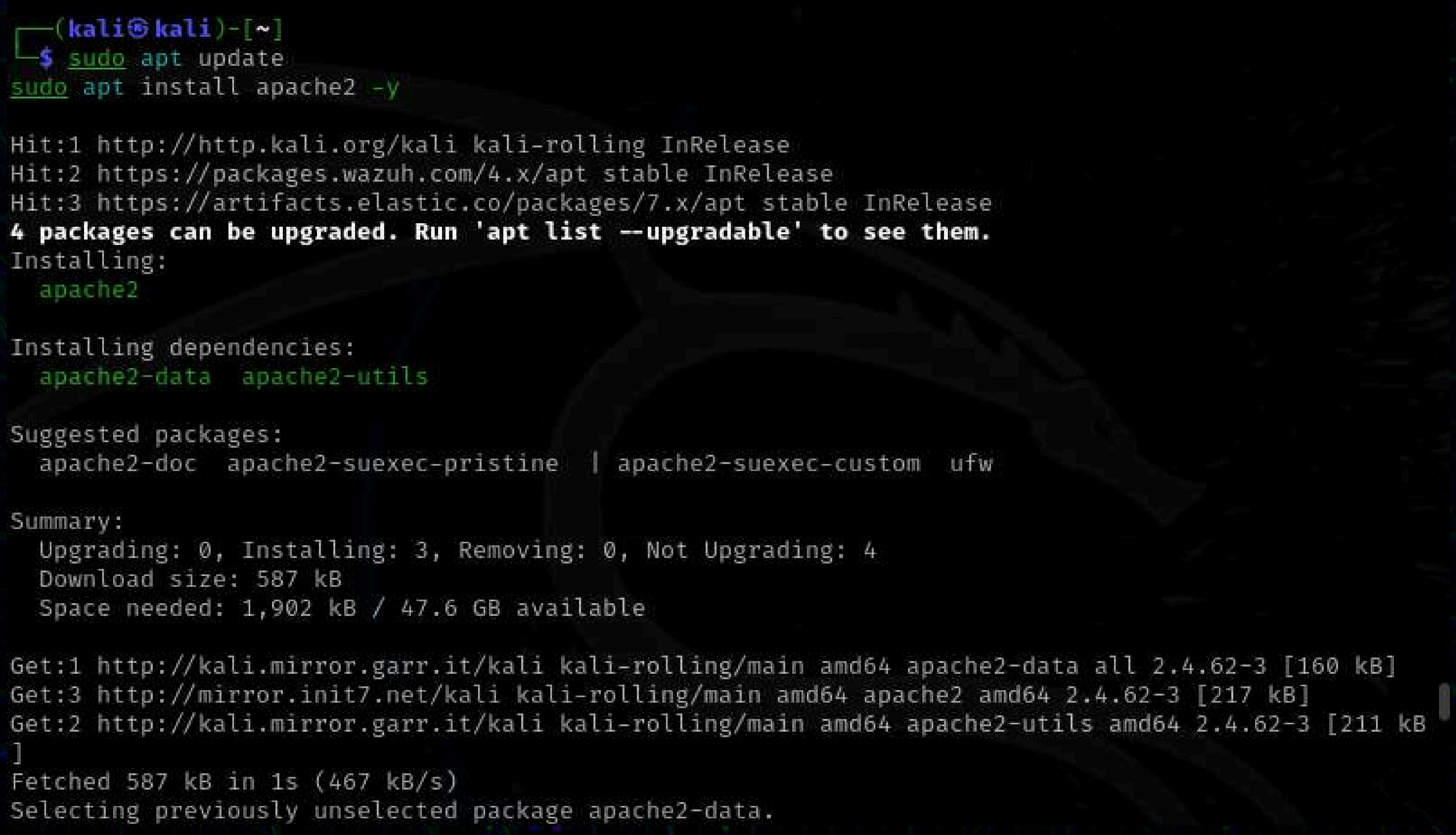
Elasticsearch: Stores and indexes log data.
Logstash: Processes and enriches logs before sending them to Elasticsearch.
Kibana: Visualizes logs and provides interactive dashboards.

3. SELINUX

This is a Linux security module that enforces strict access controls. It operates in three modes: Enforcing, Permissive, and Disabled

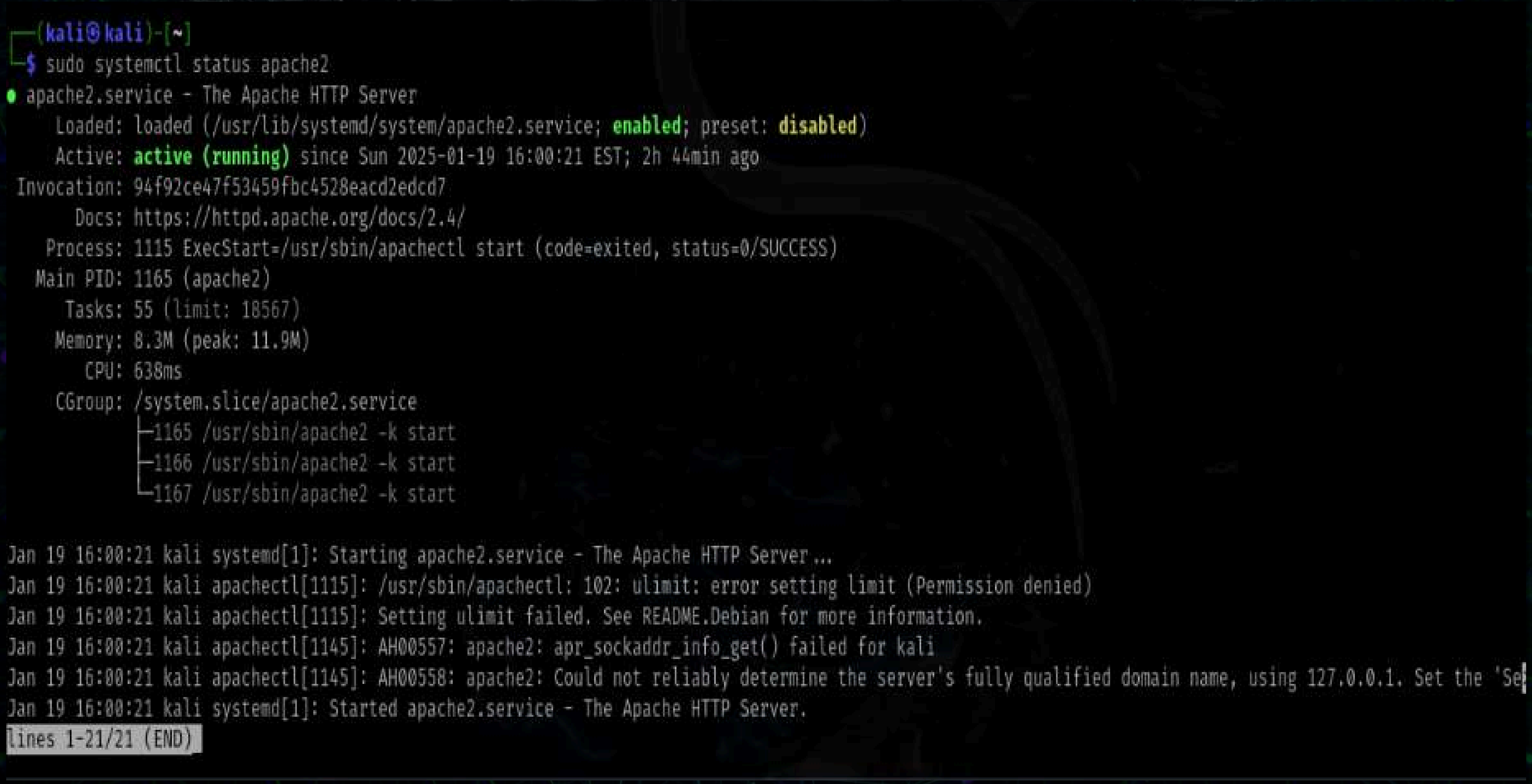
INSTALLATION AND CONFIGURATION

1. APACHE WEB SERVER



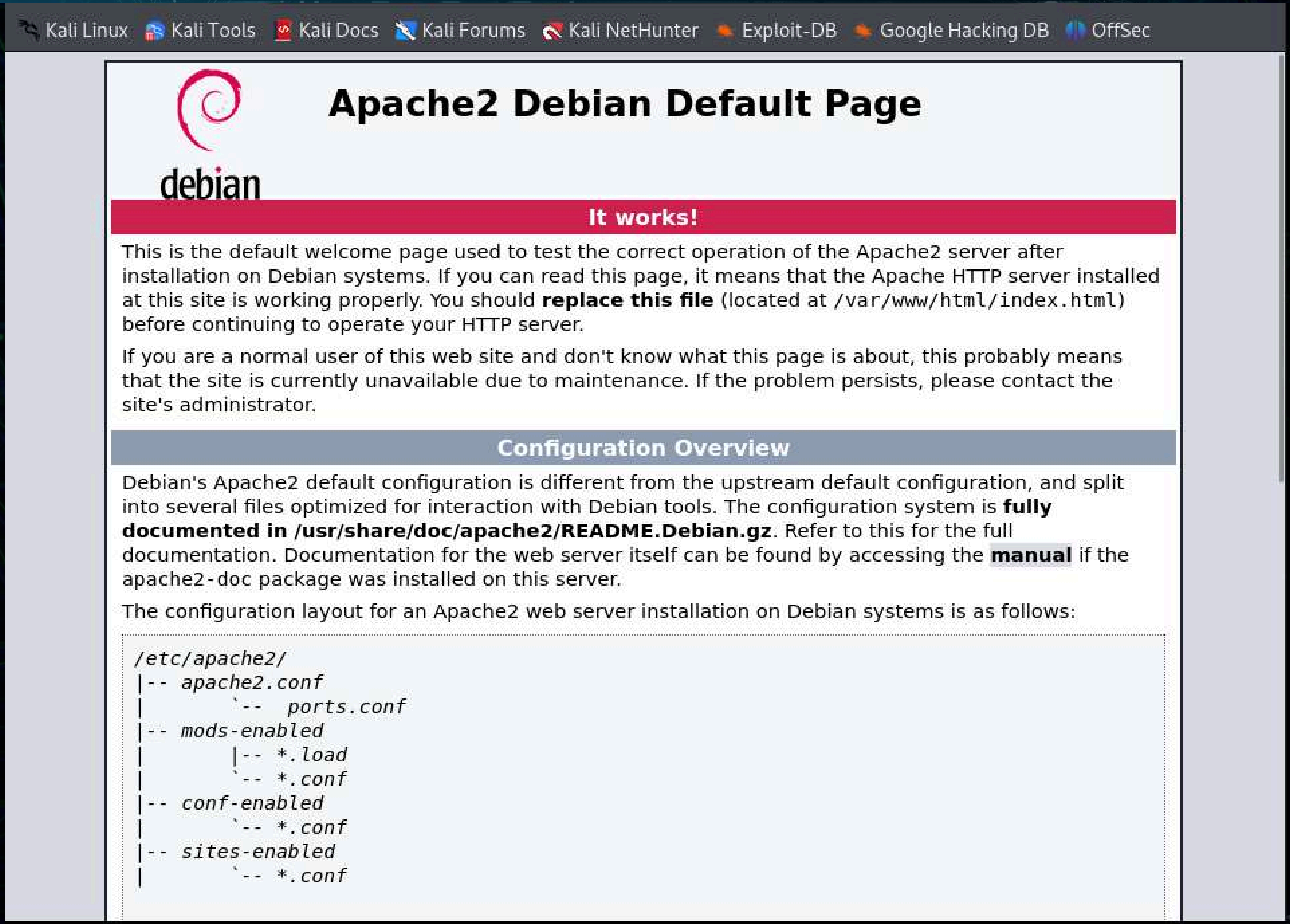
```
┌──(kali㉿kali)-[~]
└─$ sudo apt update
sudo apt install apache2 -y

Hit:1 http://http.kali.org/kali kali-rolling InRelease
Hit:2 https://packages.wazuh.com/4.x/apt stable InRelease
Hit:3 https://artifacts.elastic.co/packages/7.x/apt stable InRelease
4 packages can be upgraded. Run 'apt list --upgradable' to see them.
Installing:
  apache2

Installing dependencies:
  apache2-data  apache2-utils

Suggested packages:
  apache2-doc  apache2-suexec-pristine  | apache2-suexec-custom  ufw

Summary:
  Upgrading: 0, Installing: 3, Removing: 0, Not Upgrading: 4
  Download size: 587 kB
  Space needed: 1,902 kB / 47.6 GB available

Get:1 http://kali.mirror.garr.it/kali kali-rolling/main amd64 apache2-data all 2.4.62-3 [160 kB]
Get:3 http://mirror.init7.net/kali kali-rolling/main amd64 apache2 amd64 2.4.62-3 [217 kB]
Get:2 http://kali.mirror.garr.it/kali kali-rolling/main amd64 apache2-utils amd64 2.4.62-3 [211 kB
]
Fetched 587 kB in 1s (467 kB/s)
Selecting previously unselected package apache2-data.
```

INSTALLATION AND CONFIGURATION



```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: disabled)
     Active: active (running) since Sun 2025-01-19 16:00:21 EST; 2h 44min ago
 Invocation: 94f92ce47f53459fbc4528eacd2edcd7
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 1115 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 1165 (apache2)
      Tasks: 55 (limit: 18567)
     Memory: 8.3M (peak: 11.9M)
        CPU: 638ms
     CGroup: /system.slice/apache2.service
             ├─1165 /usr/sbin/apache2 -k start
             ├─1166 /usr/sbin/apache2 -k start
             └─1167 /usr/sbin/apache2 -k start

Jan 19 16:00:21 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Jan 19 16:00:21 kali apachectl[1115]: /usr/sbin/apachectl: 102: ulimit: error setting limit (Permission denied)
Jan 19 16:00:21 kali apachectl[1115]: Setting ulimit failed. See README.Debian for more information.
Jan 19 16:00:21 kali apachectl[1145]: AH00557: apache2: apr_sockaddr_info_get() failed for kali
Jan 19 16:00:21 kali apachectl[1145]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.0.1. Set the 'Se
Jan 19 16:00:21 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-21/21 (END)
```

INSTALLATION AND CONFIGURATION



Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

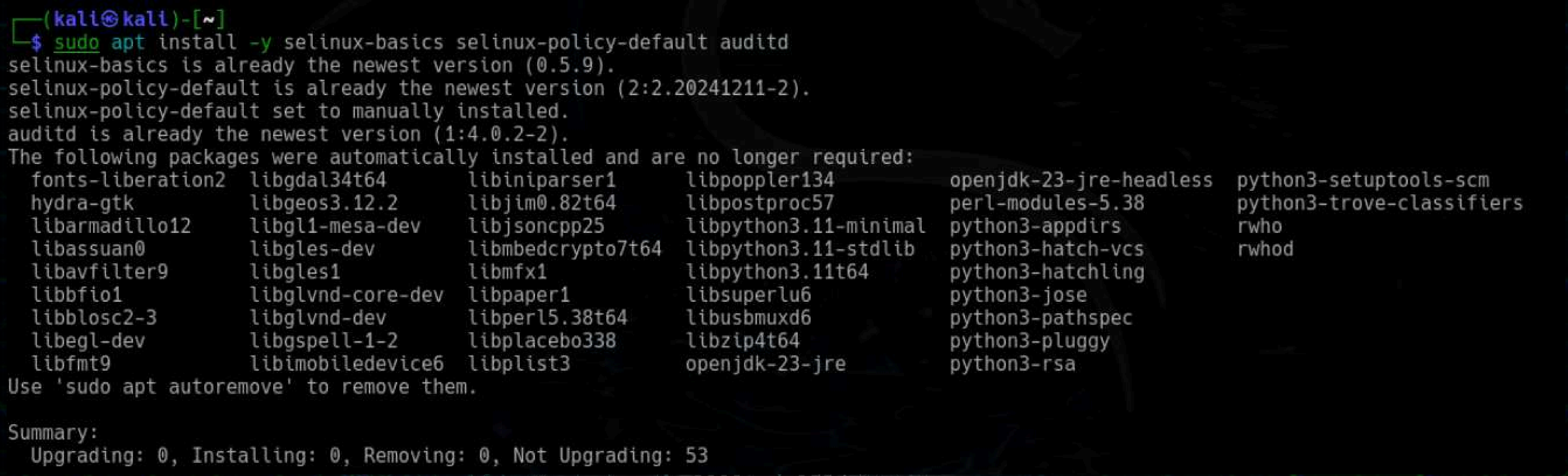
Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

INSTALLATION AND CONFIGURATION

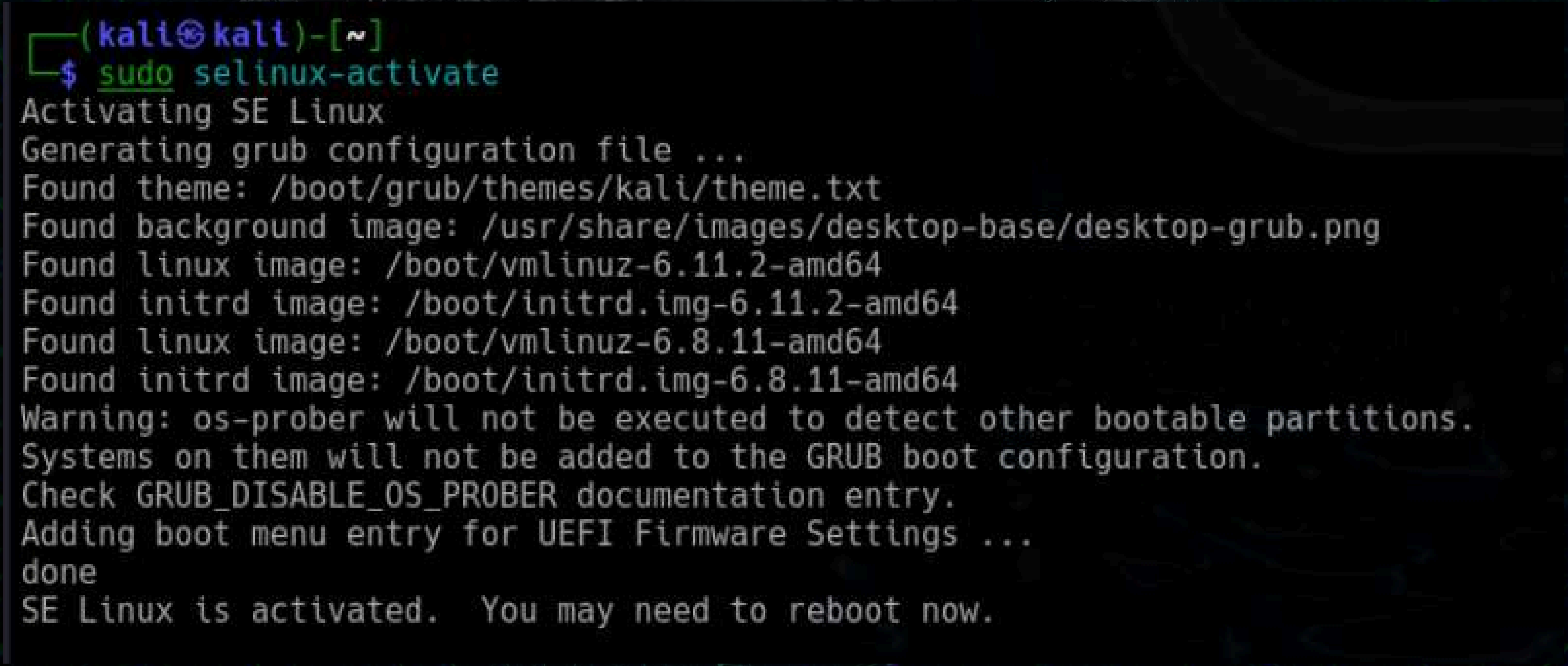
2. SELINUX



```
┌──(kali㉿kali)-[~]
└─$ sudo apt install -y selinux-basics selinux-policy-default auditd
selinux-basics is already the newest version (0.5.9).
selinux-policy-default is already the newest version (2:2.20241211-2).
selinux-policy-default set to manually installed.
auditd is already the newest version (1:4.0.2-2).
The following packages were automatically installed and are no longer required:
  fonts-liberation2  libgdal34t64       libiniparser1      libpoppler134          openjdk-23-jre-headless  python3-setuptools-scm
  hydra-gtk          libgeos3.12.2      libjim0.82t64      libpostproc57          perl-modules-5.38        python3-trove-classifiers
  libarmadillo12     libgl1-mesa-dev    libjsoncpp25       libpython3.11-minimal  python3-appdirs          rwho
  libassuan0         libgles-dev        libmbedcrypto7t64  libpython3.11-stdlib   python3-hatch-vcs        rwhod
  libavfilter9       libgles1           libmfx1            libpython3.11t64       python3-hatchling
  libbfio1           libglvnd-core-dev  libpaper1          libsuperlu6            python3-jose
  libblosc2-3        libglvnd-dev       libperl5.38t64     libusbmuxd6            python3-pathspec
  libegl-dev         libgspell-1-2      libplacebo338      libzip4t64             python3-pluggy
  libfmt9            libimobiledevice6  libplist3          openjdk-23-jre         python3-rsa
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 53
```

INSTALLATION AND CONFIGURATION

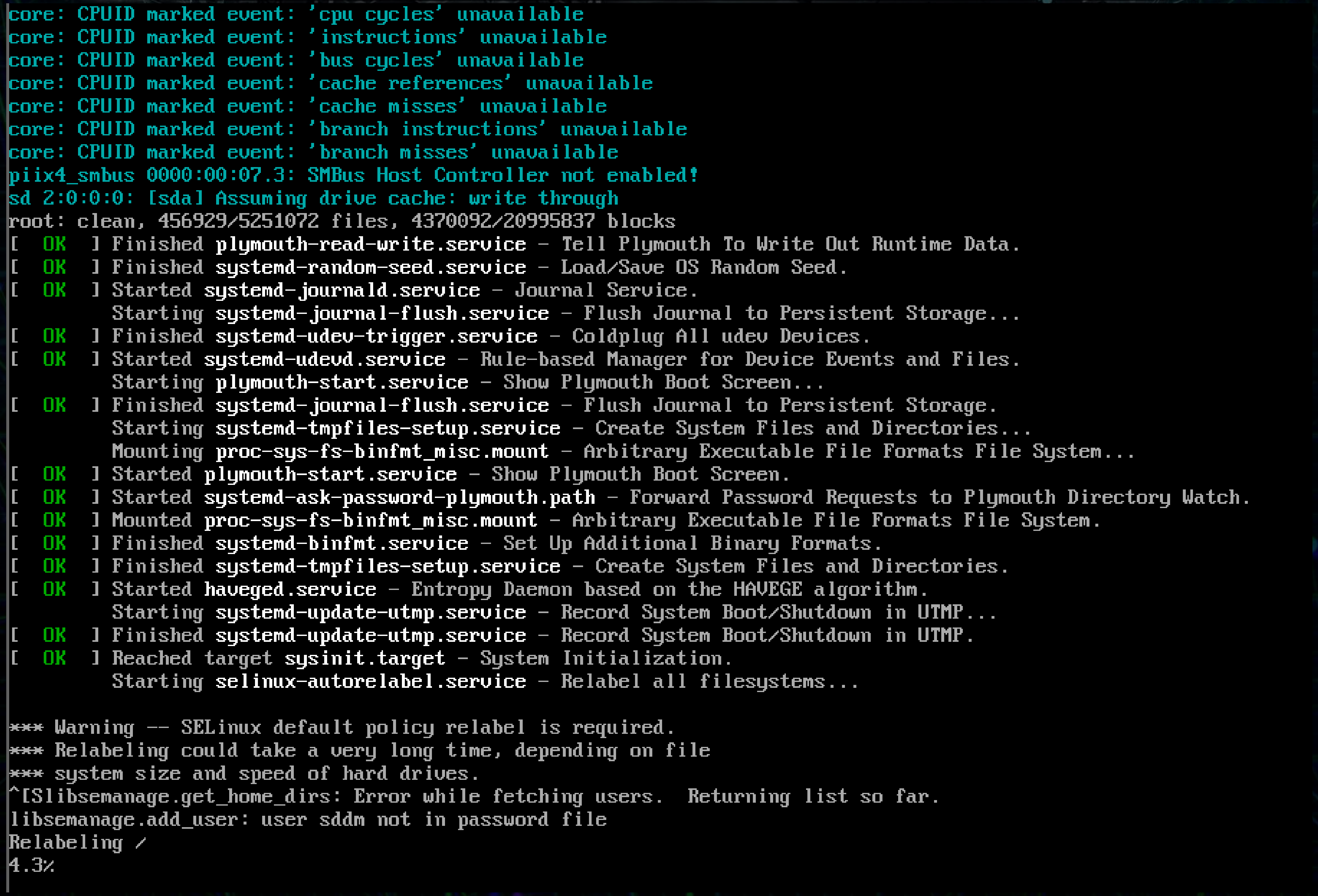
2. SELINUX(



```
┌──(kali㉿kali)-[~]
└─$ sudo selinux-activate
Activating SE Linux
Generating grub configuration file ...
Found theme: /boot/grub/themes/kali/theme.txt
Found background image: /usr/share/images/desktop-base/desktop-grub.png
Found linux image: /boot/vmlinuz-6.11.2-amd64
Found initrd image: /boot/initrd.img-6.11.2-amd64
Found linux image: /boot/vmlinuz-6.8.11-amd64
Found initrd image: /boot/initrd.img-6.8.11-amd64
Warning: os-prober will not be executed to detect other bootable partitions.
Systems on them will not be added to the GRUB boot configuration.
Check GRUB_DISABLE_OS_PROBER documentation entry.
Adding boot menu entry for UEFI Firmware Settings ...
done
SE Linux is activated.  You may need to reboot now.
```

INSTALLATION AND CONFIGURATION

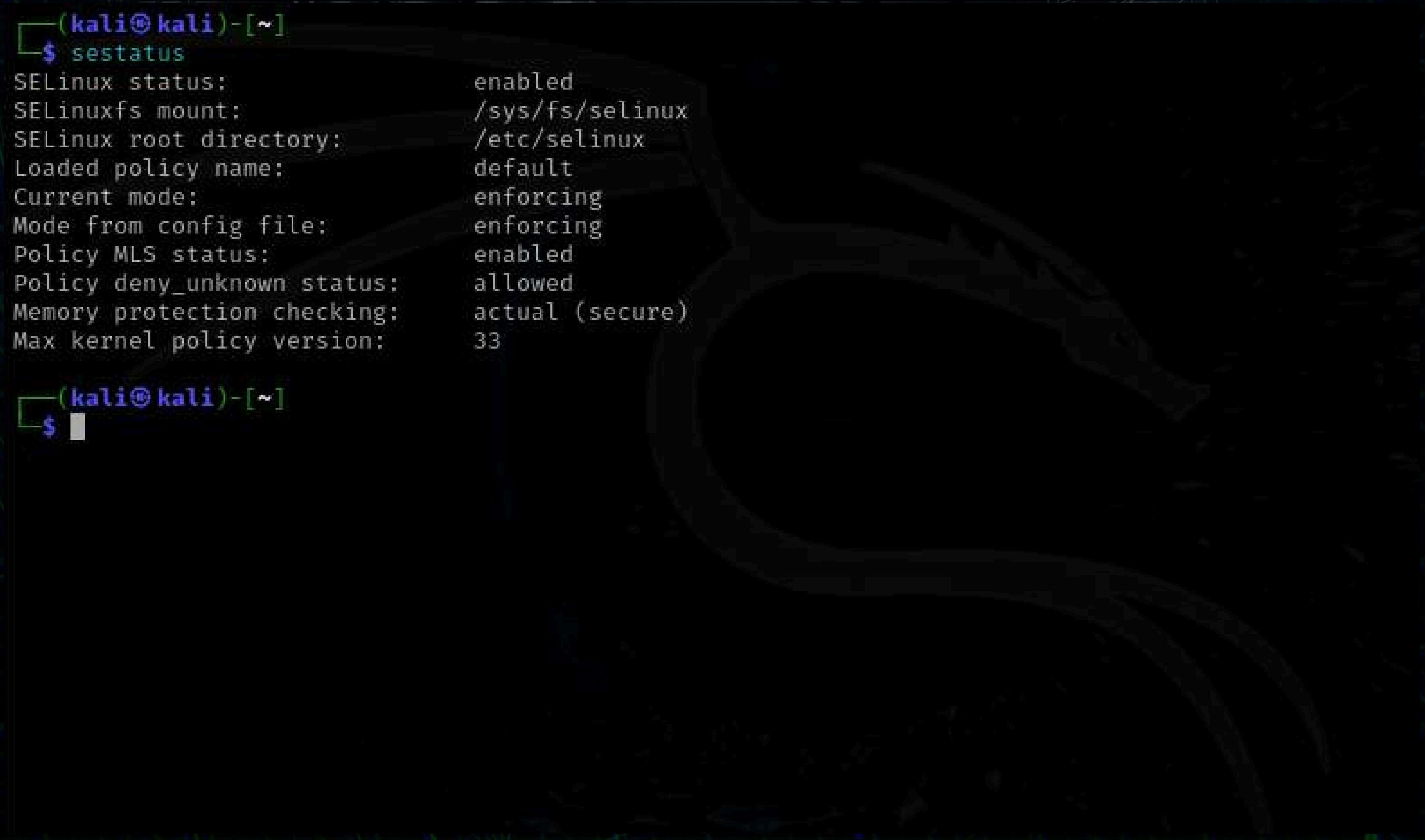
REBOOT



```
core: CPUID marked event: 'cpu cycles' unavailable
core: CPUID marked event: 'instructions' unavailable
core: CPUID marked event: 'bus cycles' unavailable
core: CPUID marked event: 'cache references' unavailable
core: CPUID marked event: 'cache misses' unavailable
core: CPUID marked event: 'branch instructions' unavailable
core: CPUID marked event: 'branch misses' unavailable
piix4_smbus 0000:00:07.3: SMBus Host Controller not enabled!
sd 2:0:0:0: [sda] Assuming drive cache: write through
root: clean, 456929/5251072 files, 4370092/20995837 blocks
[  OK  ] Finished plymouth-read-write.service - Tell Plymouth To Write Out Runtime Data.
[  OK  ] Finished systemd-random-seed.service - Load/Save OS Random Seed.
[  OK  ] Started systemd-journald.service - Journal Service.
         Starting systemd-journal-flush.service - Flush Journal to Persistent Storage...
[  OK  ] Finished systemd-udev-trigger.service - Coldplug All udev Devices.
[  OK  ] Started systemd-udevd.service - Rule-based Manager for Device Events and Files.
         Starting plymouth-start.service - Show Plymouth Boot Screen...
[  OK  ] Finished systemd-journal-flush.service - Flush Journal to Persistent Storage.
         Starting systemd-tmpfiles-setup.service - Create System Files and Directories...
         Mounting proc-sys-fs-binfmt_misc.mount - Arbitrary Executable File Formats File System...
[  OK  ] Started plymouth-start.service - Show Plymouth Boot Screen.
[  OK  ] Started systemd-ask-password-plymouth.path - Forward Password Requests to Plymouth Directory Watch.
[  OK  ] Mounted proc-sys-fs-binfmt_misc.mount - Arbitrary Executable File Formats File System.
[  OK  ] Finished systemd-binfmt.service - Set Up Additional Binary Formats.
[  OK  ] Finished systemd-tmpfiles-setup.service - Create System Files and Directories.
[  OK  ] Started haveged.service - Entropy Daemon based on the HAVEGE algorithm.
         Starting systemd-update-utmp.service - Record System Boot/Shutdown in UTMP...
[  OK  ] Finished systemd-update-utmp.service - Record System Boot/Shutdown in UTMP.
[  OK  ] Reached target sysinit.target - System Initialization.
         Starting selinux-autorelabel.service - Relabel all filesystems...

*** Warning -- SELinux default policy relabel is required.
*** Relabeling could take a very long time, depending on file
*** system size and speed of hard drives.
^[Slibsemanage.get_home_dirs: Error while fetching users.  Returning list so far.
libsemanage.add_user: user sddm not in password file
Relabeling /
4.3%
```

INSTALLATION AND CONFIGURATION

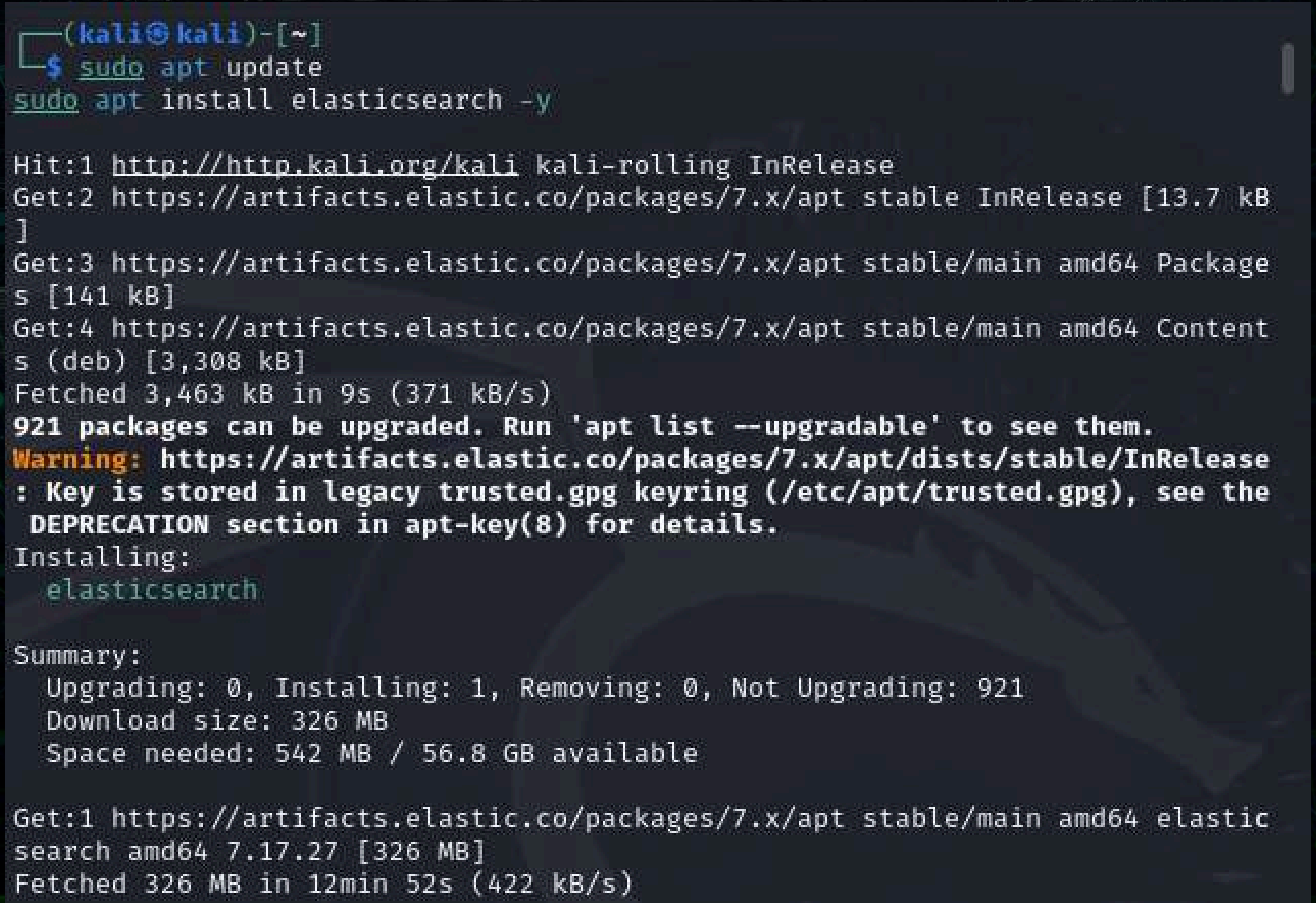
2. SELINUX



```
┌──(kali㉿kali)-[~]
└─$ sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             default
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33

┌──(kali㉿kali)-[~]
└─$ 
```

INSTALLATION AND CONFIGURATION

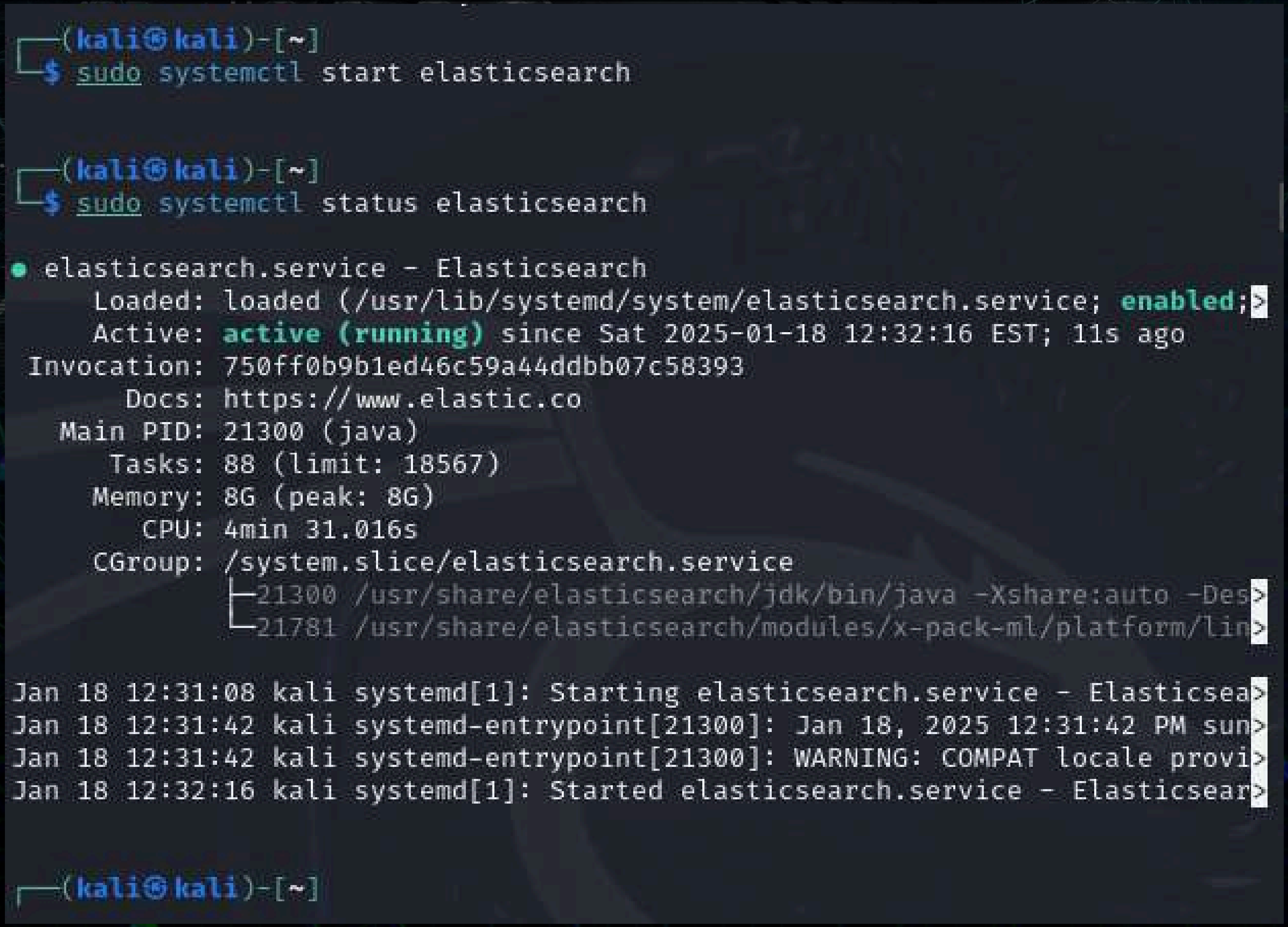
3. ELASTICSEARCH



```
┌──(kali㉿kali)-[~]
└─$ sudo apt update
sudo apt install elasticsearch -y

Hit:1 http://http.kali.org/kali kali-rolling InRelease
Get:2 https://artifacts.elastic.co/packages/7.x/apt stable InRelease [13.7 kB
]
Get:3 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 Package
s [141 kB]
Get:4 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 Content
s (deb) [3,308 kB]
Fetched 3,463 kB in 9s (371 kB/s)
921 packages can be upgraded. Run 'apt list --upgradable' to see them.
Warning: https://artifacts.elastic.co/packages/7.x/apt/dists/stable/InRelease
: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the
 DEPRECATION section in apt-key(8) for details.
Installing:
  elasticsearch

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 921
  Download size: 326 MB
  Space needed: 542 MB / 56.8 GB available

Get:1 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 elastic
search amd64 7.17.27 [326 MB]
Fetched 326 MB in 12min 52s (422 kB/s)
```

INSTALLATION AND CONFIGURATION

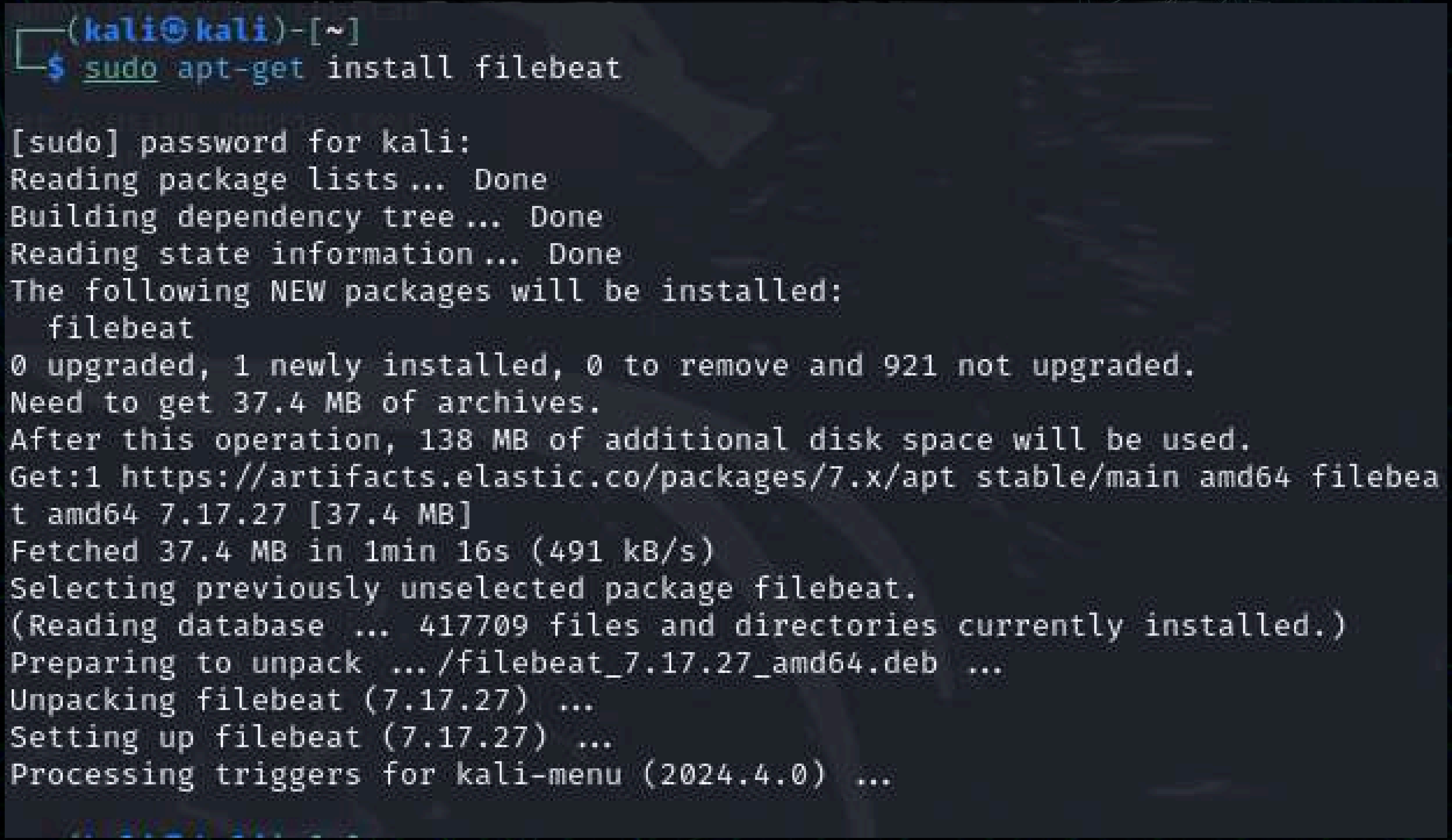
3. ELASTICSEARCH (ACTIVE)



```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl start elasticsearch


┌──(kali㉿kali)-[~]
└─$ sudo systemctl status elasticsearch

● elasticsearch.service - Elasticsearch
     Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled;>
     Active: active (running) since Sat 2025-01-18 12:32:16 EST; 11s ago
 Invocation: 750ff0b9b1ed46c59a44ddbb07c58393
       Docs: https://www.elastic.co
   Main PID: 21300 (java)
      Tasks: 88 (limit: 18567)
     Memory: 8G (peak: 8G)
        CPU: 4min 31.016s
     CGroup: /system.slice/elasticsearch.service
             ├─21300 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des>
             └─21781 /usr/share/elasticsearch/modules/x-pack-ml/platform/lin>

Jan 18 12:31:08 kali systemd[1]: Starting elasticsearch.service - Elasticsea>
Jan 18 12:31:42 kali systemd-entrypoint[21300]: Jan 18, 2025 12:31:42 PM sun>
Jan 18 12:31:42 kali systemd-entrypoint[21300]: WARNING: COMPAT locale provi>
Jan 18 12:32:16 kali systemd[1]: Started elasticsearch.service - Elasticsear>


┌──(kali㉿kali)-[~]
```

INSTALLATION AND CONFIGURATION

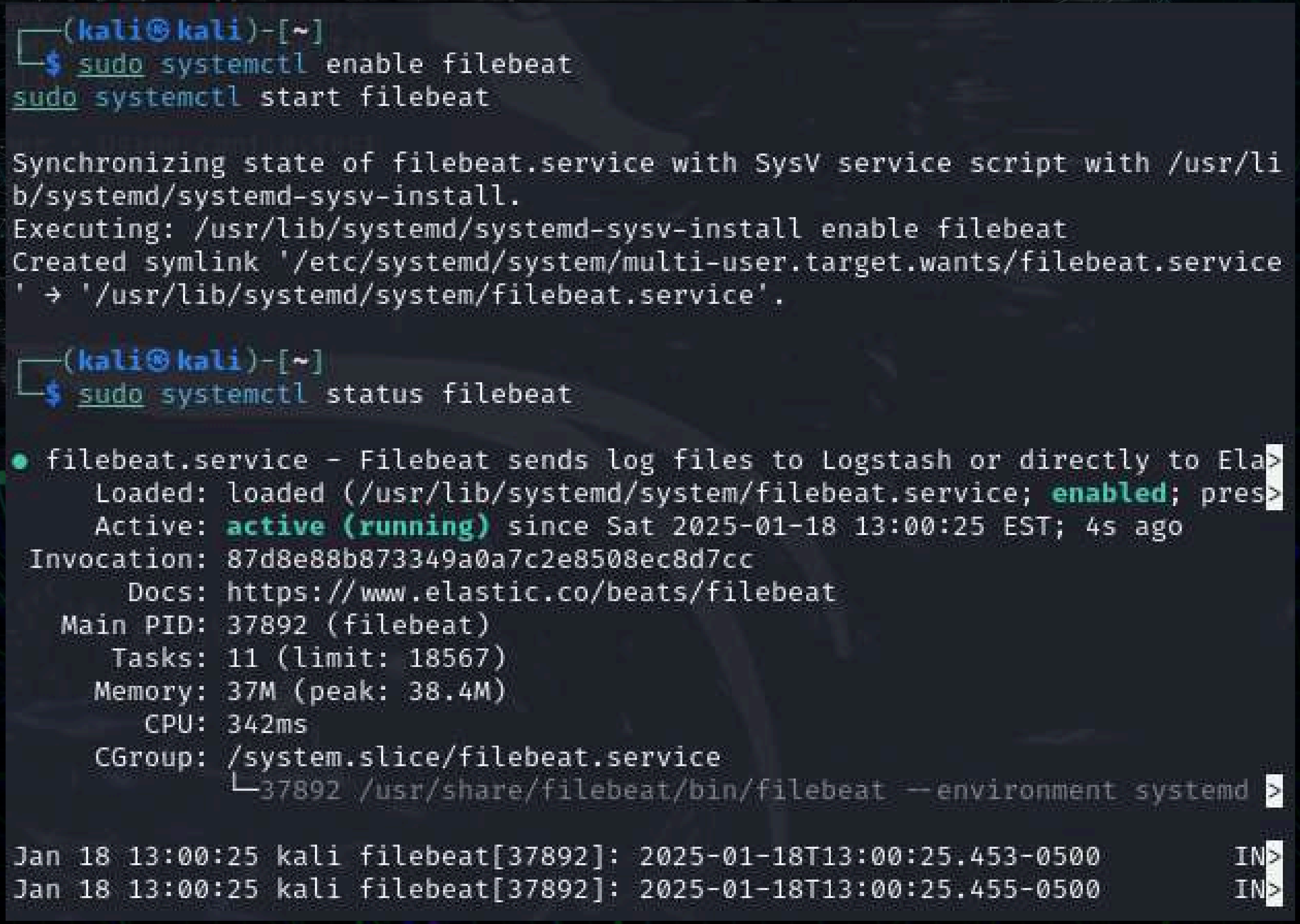
4 FILEBEAT



```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install filebeat

[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  filebeat
0 upgraded, 1 newly installed, 0 to remove and 921 not upgraded.
Need to get 37.4 MB of archives.
After this operation, 138 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 filebea
t amd64 7.17.27 [37.4 MB]
Fetched 37.4 MB in 1min 16s (491 kB/s)
Selecting previously unselected package filebeat.
(Reading database ... 417709 files and directories currently installed.)
Preparing to unpack .../filebeat_7.17.27_amd64.deb ...
Unpacking filebeat (7.17.27) ...
Setting up filebeat (7.17.27) ...
Processing triggers for kali-menu (2024.4.0) ...
```

INSTALLATION AND CONFIGURATION

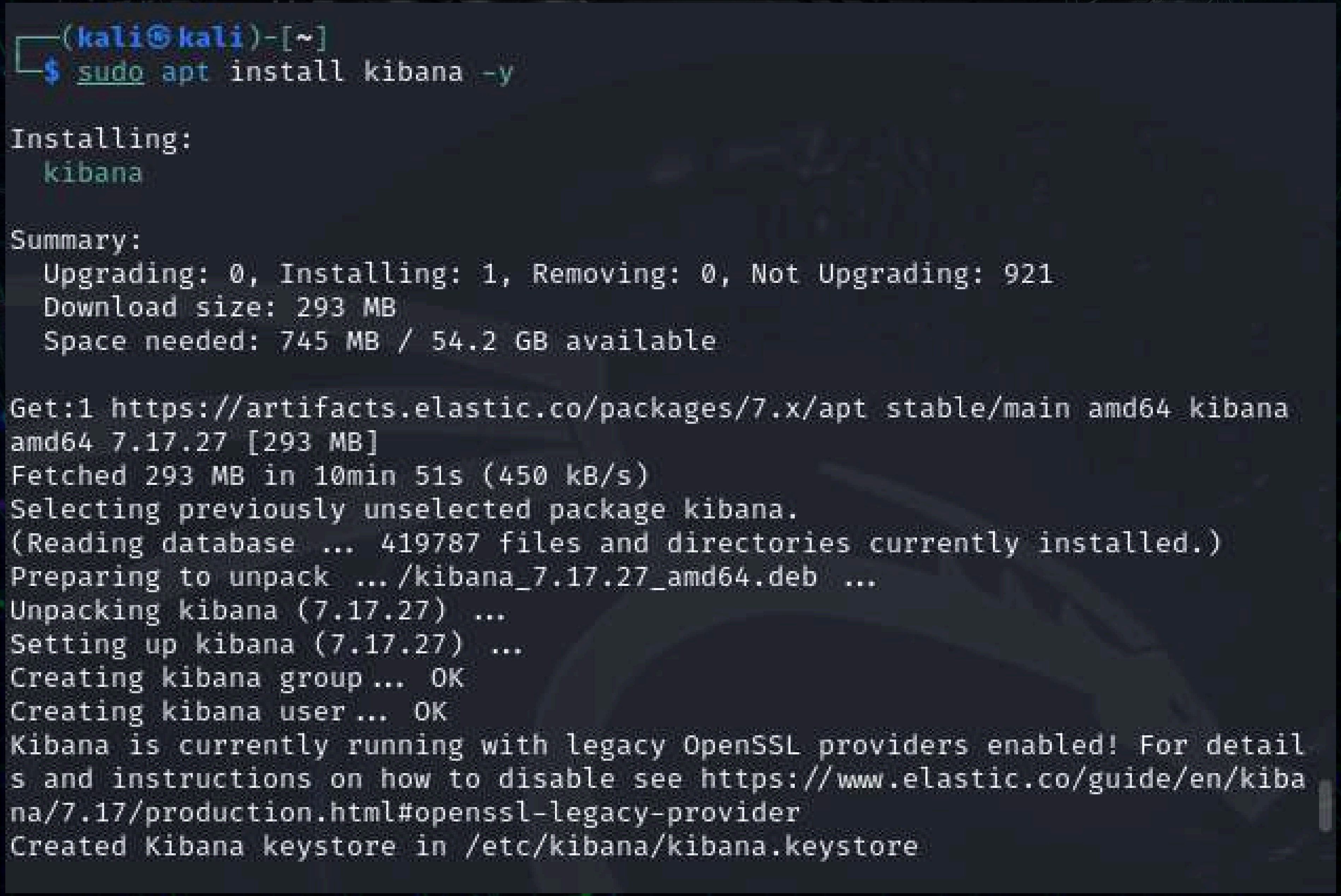
4 FILEBEAT(ACTIVE)



```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl enable filebeat
sudo systemctl start filebeat

Synchronizing state of filebeat.service with SysV service script with /usr/li
b/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable filebeat
Created symlink '/etc/systemd/system/multi-user.target.wants/filebeat.service
' → '/usr/lib/systemd/system/filebeat.service'.

┌──(kali㉿kali)-[~]
└─$ sudo systemctl status filebeat

● filebeat.service - Filebeat sends log files to Logstash or directly to Ela>
     Loaded: loaded (/usr/lib/systemd/system/filebeat.service; enabled; pres>
     Active: active (running) since Sat 2025-01-18 13:00:25 EST; 4s ago
 Invocation: 87d8e88b873349a0a7c2e8508ec8d7cc
       Docs: https://www.elastic.co/beats/filebeat
   Main PID: 37892 (filebeat)
      Tasks: 11 (limit: 18567)
     Memory: 37M (peak: 38.4M)
        CPU: 342ms
     CGroup: /system.slice/filebeat.service
             └─37892 /usr/share/filebeat/bin/filebeat --environment systemd >

Jan 18 13:00:25 kali filebeat[37892]: 2025-01-18T13:00:25.453-0500       IN>
Jan 18 13:00:25 kali filebeat[37892]: 2025-01-18T13:00:25.455-0500       IN>
```

INSTALLATION AND CONFIGURATION

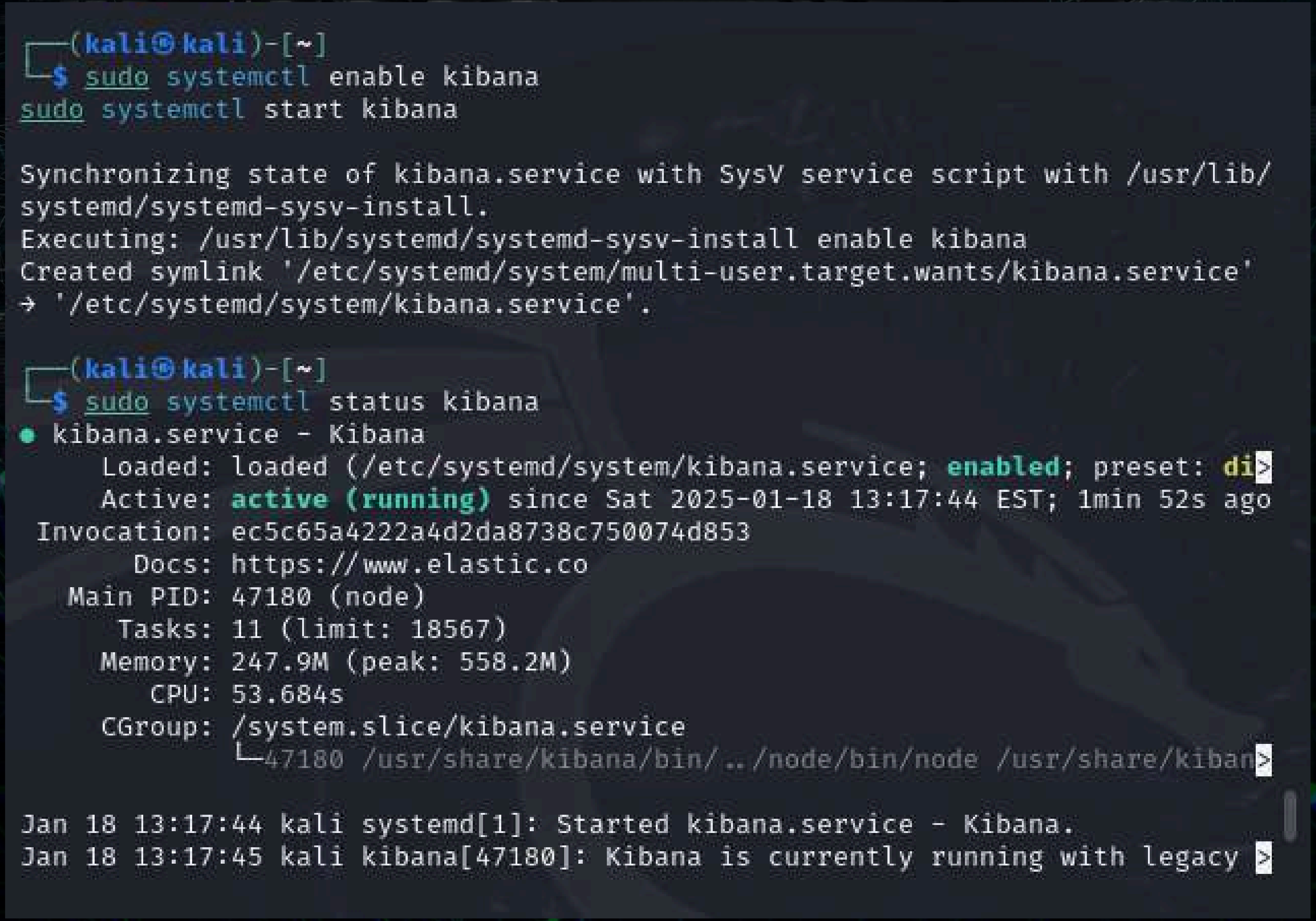
5 KIBANA



```
┌──(kali㉿kali)-[~]
└─$ sudo apt install kibana -y

Installing:
  kibana

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 921
  Download size: 293 MB
  Space needed: 745 MB / 54.2 GB available

Get:1 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 kibana
amd64 7.17.27 [293 MB]
Fetched 293 MB in 10min 51s (450 kB/s)
Selecting previously unselected package kibana.
(Reading database ... 419787 files and directories currently installed.)
Preparing to unpack .../kibana_7.17.27_amd64.deb ...
Unpacking kibana (7.17.27) ...
Setting up kibana (7.17.27) ...
Creating kibana group... OK
Creating kibana user... OK
Kibana is currently running with legacy OpenSSL providers enabled! For detail
s and instructions on how to disable see https://www.elastic.co/guide/en/kiba
na/7.17/production.html#openssl-legacy-provider
Created Kibana keystore in /etc/kibana/kibana.keystore
```

INSTALLATION AND CONFIGURATION

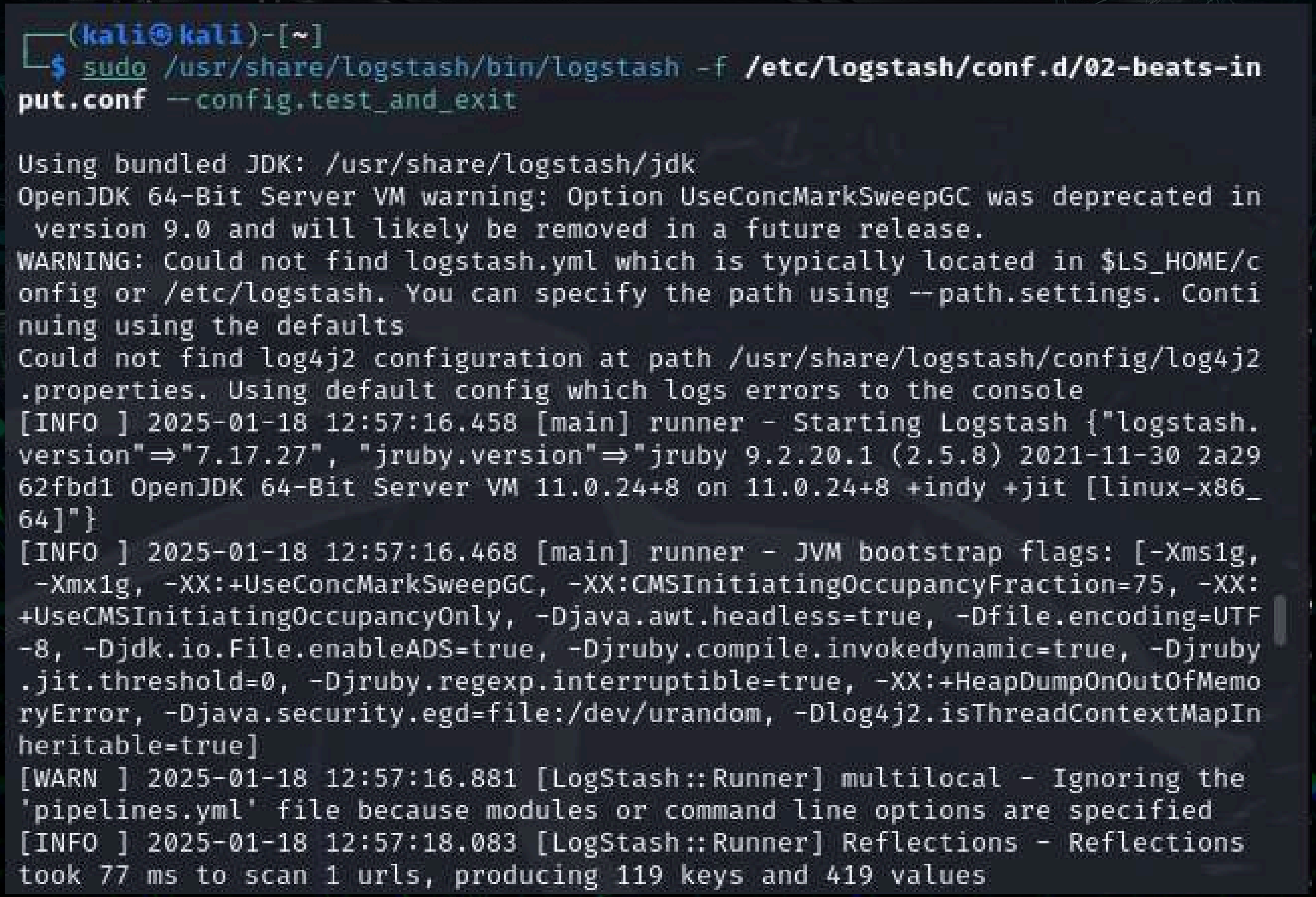
5 KIBANA (ACTIVE)



```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl enable kibana
sudo systemctl start kibana

Synchronizing state of kibana.service with SysV service script with /usr/lib/
systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable kibana
Created symlink '/etc/systemd/system/multi-user.target.wants/kibana.service'
→ '/etc/systemd/system/kibana.service'.

┌──(kali㉿kali)-[~]
└─$ sudo systemctl status kibana
● kibana.service - Kibana
     Loaded: loaded (/etc/systemd/system/kibana.service; enabled; preset: di>
     Active: active (running) since Sat 2025-01-18 13:17:44 EST; 1min 52s ago
 Invocation: ec5c65a4222a4d2da8738c750074d853
       Docs: https://www.elastic.co
   Main PID: 47180 (node)
      Tasks: 11 (limit: 18567)
     Memory: 247.9M (peak: 558.2M)
        CPU: 53.684s
     CGroup: /system.slice/kibana.service
             └─47180 /usr/share/kibana/bin/../node/bin/node /usr/share/kiban>

Jan 18 13:17:44 kali systemd[1]: Started kibana.service - Kibana.
Jan 18 13:17:45 kali kibana[47180]: Kibana is currently running with legacy >
```

INSTALLATION AND CONFIGURATION

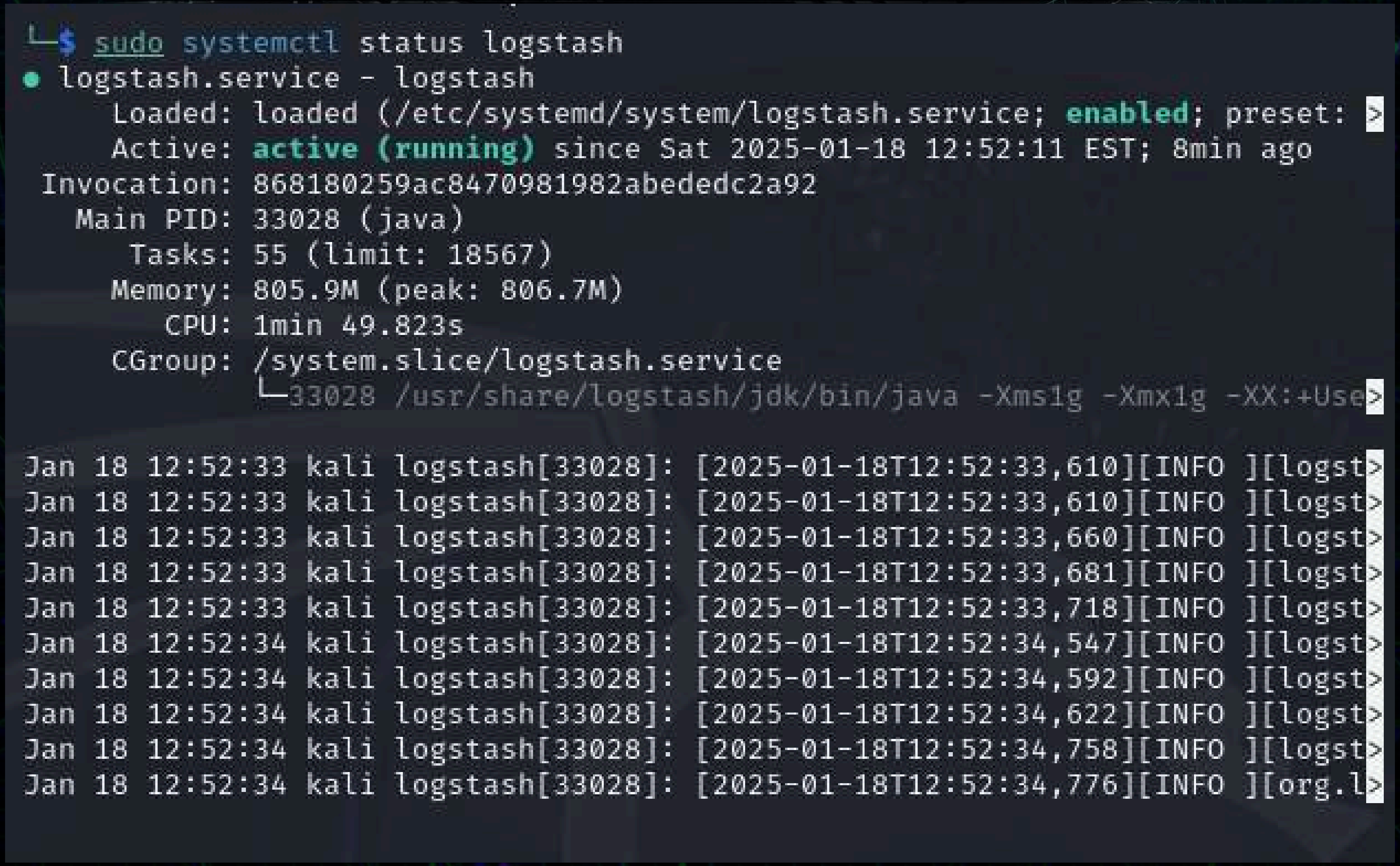
6 LOGSTASH



```
┌──(kali㉿kali)-[~]
└─$ sudo /usr/share/logstash/bin/logstash -f /etc/logstash/conf.d/02-beats-in
put.conf --config.test_and_exit

Using bundled JDK: /usr/share/logstash/jdk
OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in
 version 9.0 and will likely be removed in a future release.
WARNING: Could not find logstash.yml which is typically located in $LS_HOME/c
onfig or /etc/logstash. You can specify the path using --path.settings. Conti
nuing using the defaults
Could not find log4j2 configuration at path /usr/share/logstash/config/log4j2
.properties. Using default config which logs errors to the console
[INFO ] 2025-01-18 12:57:16.458 [main] runner - Starting Logstash {"logstash.
version"⇒"7.17.27", "jruby.version"⇒"jruby 9.2.20.1 (2.5.8) 2021-11-30 2a29
62fbd1 OpenJDK 64-Bit Server VM 11.0.24+8 on 11.0.24+8 +indy +jit [linux-x86_
64]"}
[INFO ] 2025-01-18 12:57:16.468 [main] runner - JVM bootstrap flags: [-Xms1g,
 -Xmx1g, -XX:+UseConcMarkSweepGC, -XX:CMSInitiatingOccupancyFraction=75, -XX:
+UseCMSInitiatingOccupancyOnly, -Djava.awt.headless=true, -Dfile.encoding=UTF
-8, -Djdk.io.File.enableADS=true, -Djruby.compile.invokedynamic=true, -Djruby
.jit.threshold=0, -Djruby.regexp.interruptible=true, -XX:+HeapDumpOnOutOfMemo
ryError, -Djava.security.egd=file:/dev/urandom, -Dlog4j2.isThreadContextMapIn
heritable=true]
[WARN ] 2025-01-18 12:57:16.881 [LogStash::Runner] multilocal - Ignoring the
'pipelines.yml' file because modules or command line options are specified
[INFO ] 2025-01-18 12:57:18.083 [LogStash::Runner] Reflections - Reflections
took 77 ms to scan 1 urls, producing 119 keys and 419 values
```

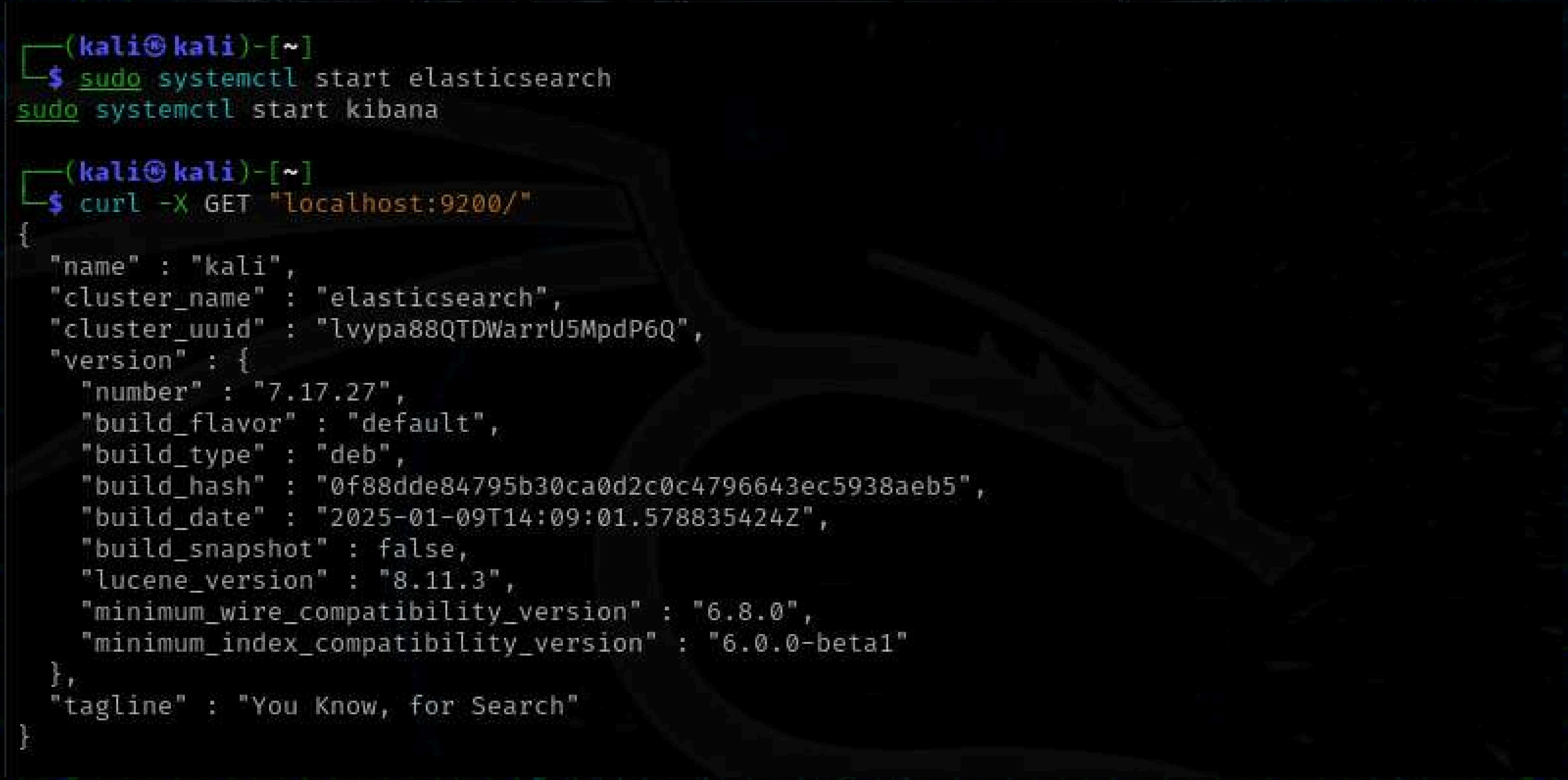
INSTALLATION AND CONFIGURATION

6 LOGSTASH (ACTIVE)



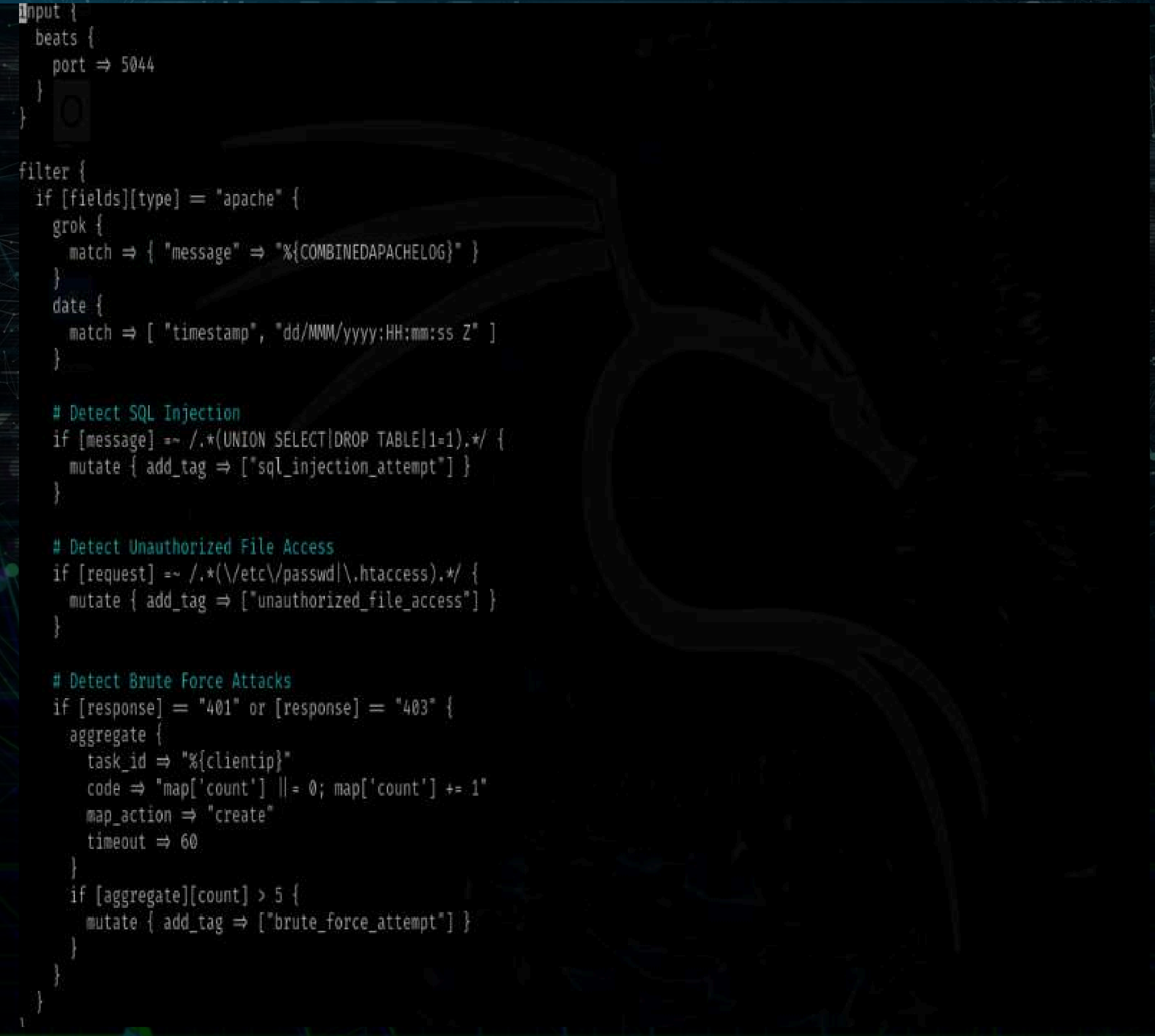
```
└─$ sudo systemctl status logstash
● logstash.service - logstash
     Loaded: loaded (/etc/systemd/system/logstash.service; enabled; preset: >
     Active: active (running) since Sat 2025-01-18 12:52:11 EST; 8min ago
 Invocation: 868180259ac8470981982abededc2a92
   Main PID: 33028 (java)
      Tasks: 55 (limit: 18567)
     Memory: 805.9M (peak: 806.7M)
        CPU: 1min 49.823s
     CGroup: /system.slice/logstash.service
             └─33028 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+Use>

Jan 18 12:52:33 kali logstash[33028]: [2025-01-18T12:52:33,610][INFO ][logst>
Jan 18 12:52:33 kali logstash[33028]: [2025-01-18T12:52:33,610][INFO ][logst>
Jan 18 12:52:33 kali logstash[33028]: [2025-01-18T12:52:33,660][INFO ][logst>
Jan 18 12:52:33 kali logstash[33028]: [2025-01-18T12:52:33,681][INFO ][logst>
Jan 18 12:52:33 kali logstash[33028]: [2025-01-18T12:52:33,718][INFO ][logst>
Jan 18 12:52:34 kali logstash[33028]: [2025-01-18T12:52:34,547][INFO ][logst>
Jan 18 12:52:34 kali logstash[33028]: [2025-01-18T12:52:34,592][INFO ][logst>
Jan 18 12:52:34 kali logstash[33028]: [2025-01-18T12:52:34,622][INFO ][logst>
Jan 18 12:52:34 kali logstash[33028]: [2025-01-18T12:52:34,758][INFO ][logst>
Jan 18 12:52:34 kali logstash[33028]: [2025-01-18T12:52:34,776][INFO ][org.l>
```

LOG ANALYSIS WITH ELK STACK



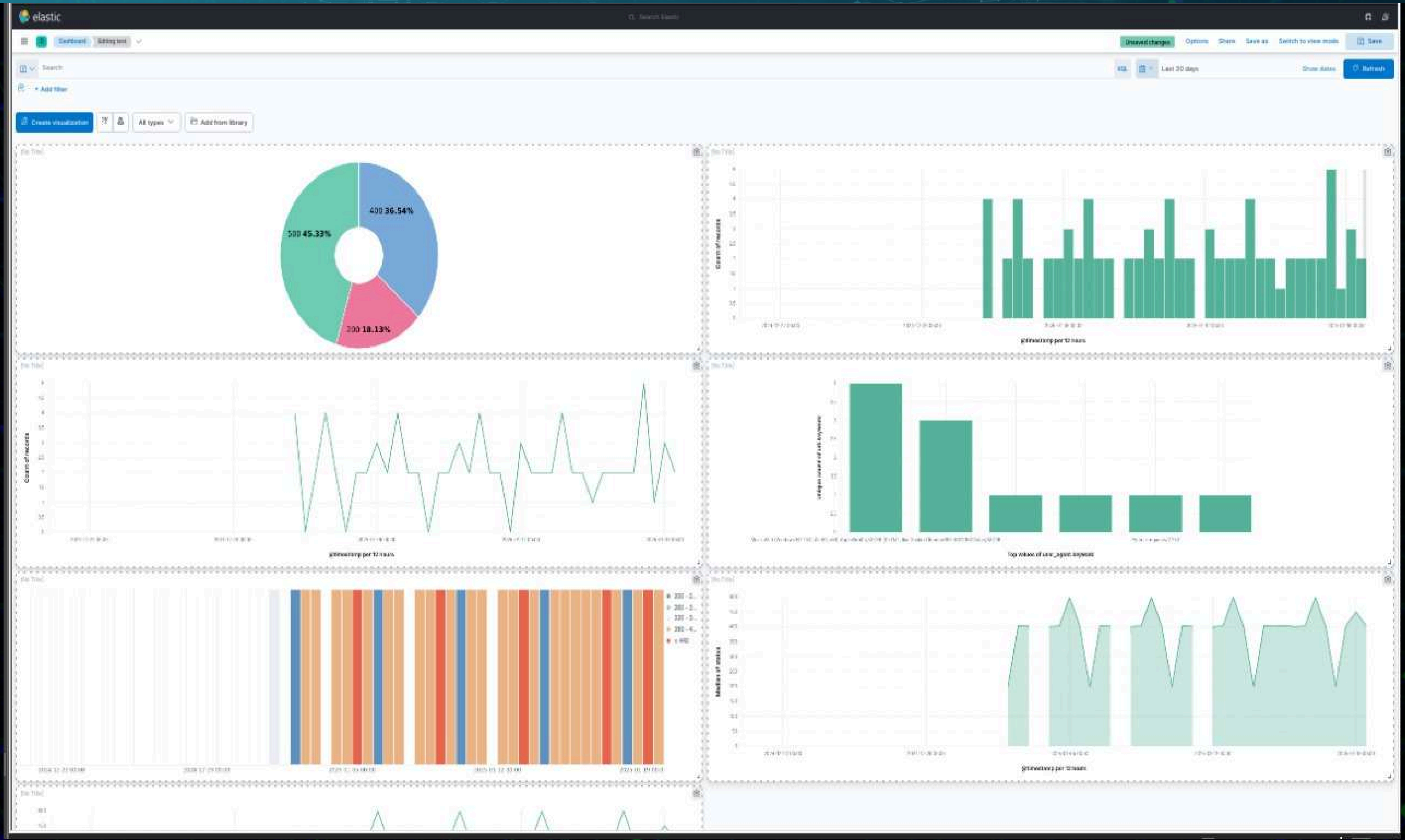
```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl start elasticsearch
sudo systemctl start kibana

┌──(kali㉿kali)-[~]
└─$ curl -X GET "localhost:9200/"
{
  "name" : "kali",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "lvypa88QTDWarrU5MpdP6Q",
  "version" : {
    "number" : "7.17.27",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "0f88dde84795b30ca0d2c0c4796643ec5938aeb5",
    "build_date" : "2025-01-09T14:09:01.578835424Z",
    "build_snapshot" : false,
    "lucene_version" : "8.11.3",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

LOG ANALYSIS WITH ELK STACK

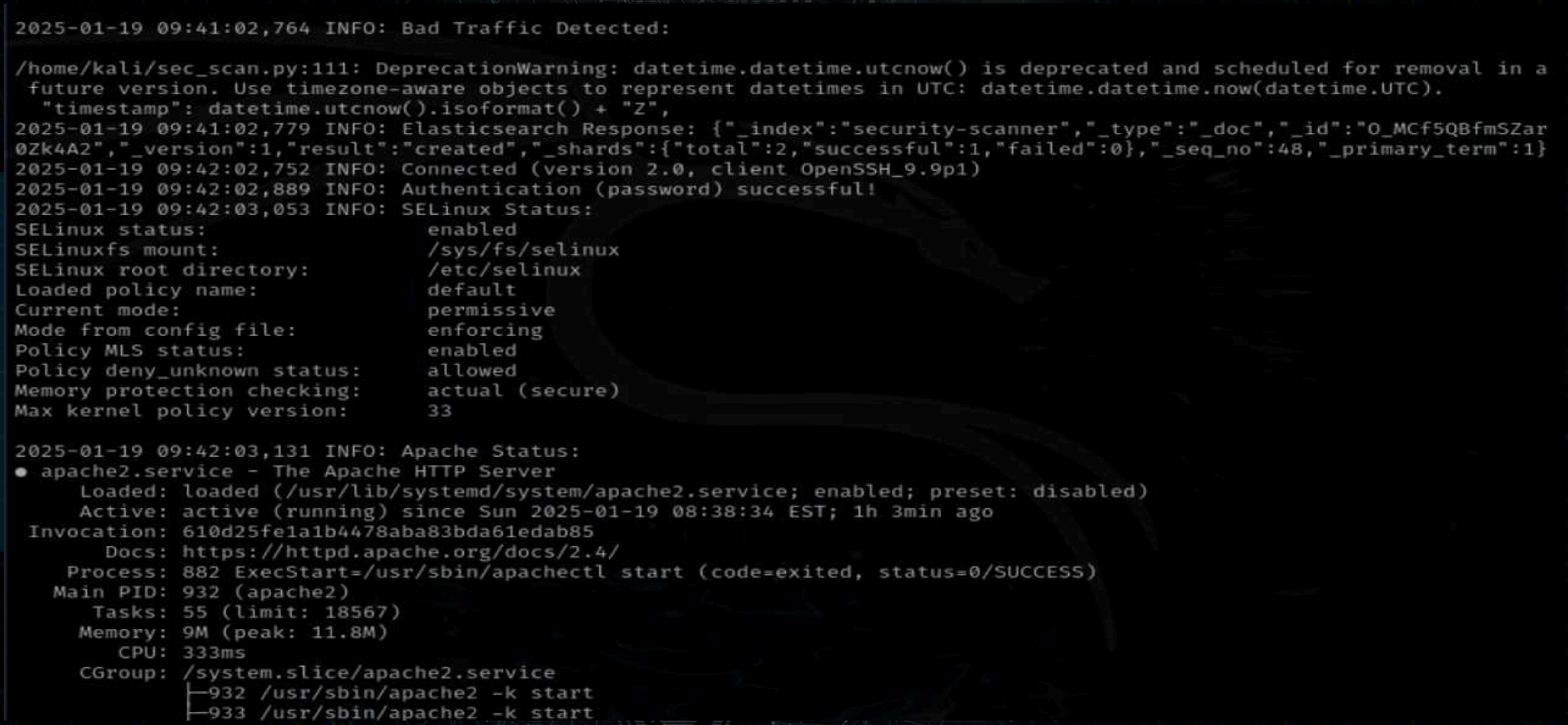


```
input {
  beats {
    port ⇒ 5044
  }
}

filter {
  if [fields][type] == "apache" {
    grok {
      match ⇒ { "message" ⇒ "%{COMBINEDAPACHELOG}" }
    }
    date {
      match ⇒ [ "timestamp", "dd/MMM/yyyy:HH:mm:ss Z" ]
    }

    # Detect SQL Injection
    if [message] =~ /.*(UNION SELECT|DROP TABLE|1=1).*/ {
      mutate { add_tag ⇒ ["sql_injection_attempt"] }
    }

    # Detect Unauthorized File Access
    if [request] =~ /.*(\/etc\/passwd|\.htaccess).*/ {
      mutate { add_tag ⇒ ["unauthorized_file_access"] }
    }

    # Detect Brute Force Attacks
    if [response] == "401" or [response] == "403" {
      aggregate {
        task_id ⇒ "%{clientip}"
        code ⇒ "map['count'] ||= 0; map['count'] += 1"
        map_action ⇒ "create"
        timeout ⇒ 60
      }
      if [aggregate][count] > 5 {
        mutate { add_tag ⇒ ["brute_force_attempt"] }
      }
    }
  }
}
```

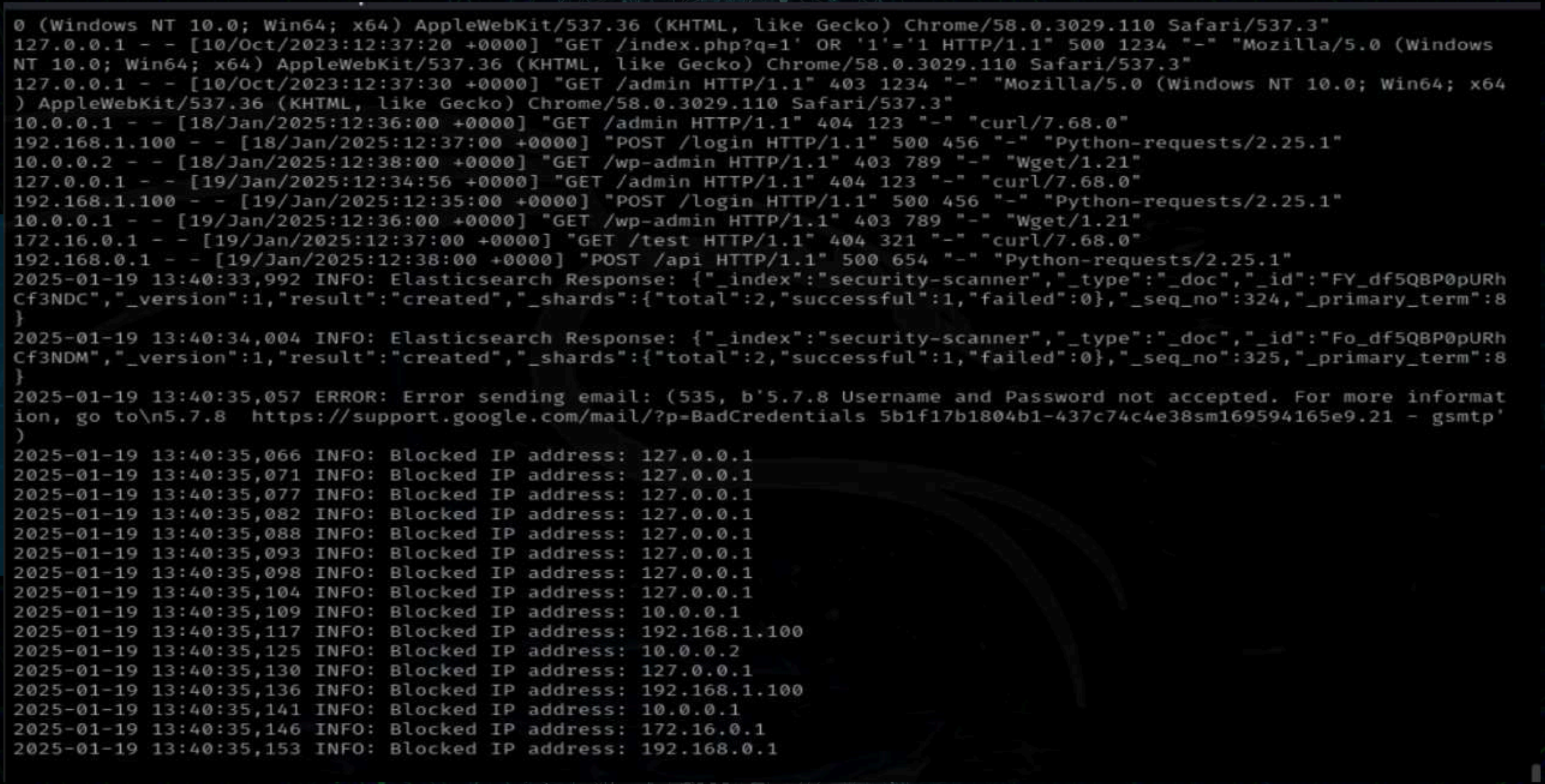
VISUALIZATION IN KIBANA



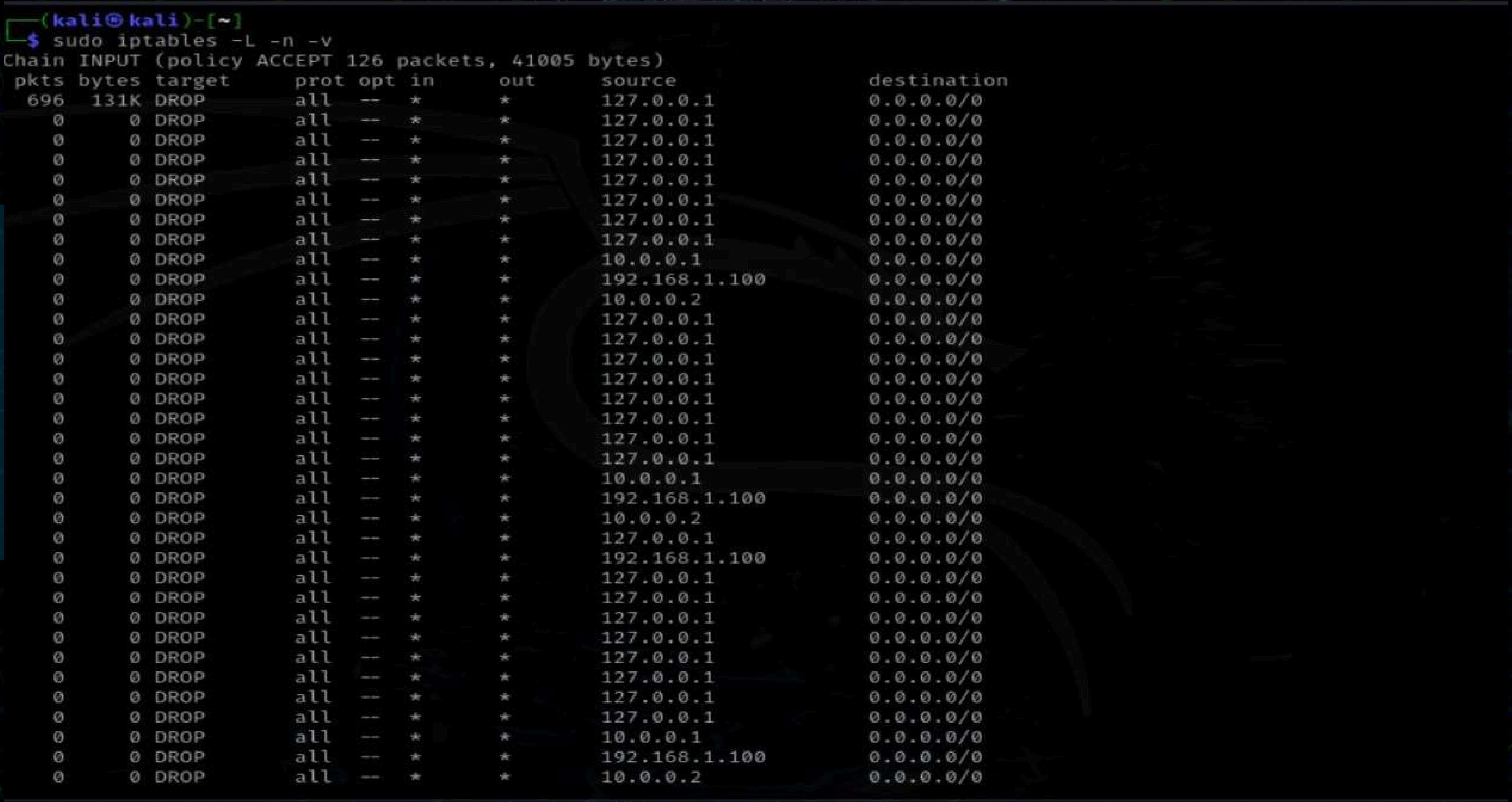
ALERTS / INCIDENT RESPONSE



```
2025-01-19 09:41:02,764 INFO: Bad Traffic Detected:

/home/kali/sec_scan.py:111: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a
 future version. Use timezone-aware objects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  "timestamp": datetime.utcnow().isoformat() + "Z",
2025-01-19 09:41:02,779 INFO: Elasticsearch Response: {"_index":"security-scanner","_type":"_doc","_id":"O_MCf5QBfmSZar
0Zk4A2","_version":1,"result":"created","_shards":{"total":2,"successful":1,"failed":0},"_seq_no":48,"_primary_term":1}
2025-01-19 09:42:02,752 INFO: Connected (version 2.0, client OpenSSH_9.9p1)
2025-01-19 09:42:02,889 INFO: Authentication (password) successful!
2025-01-19 09:42:03,053 INFO: SELinux Status:
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             default
Current mode:                   permissive
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33

2025-01-19 09:42:03,131 INFO: Apache Status:
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: disabled)
     Active: active (running) since Sun 2025-01-19 08:38:34 EST; 1h 3min ago
 Invocation: 610d25fe1a1b4478aba83bda61edab85
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 882 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 932 (apache2)
      Tasks: 55 (limit: 18567)
     Memory: 9M (peak: 11.8M)
        CPU: 333ms
     CGroup: /system.slice/apache2.service
             ├─932 /usr/sbin/apache2 -k start
             ├─933 /usr/sbin/apache2 -k start
```



```
0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.3"
127.0.0.1 - - [10/Oct/2023:12:37:20 +0000] "GET /index.php?q=1' OR '1'='1 HTTP/1.1" 500 1234 "-" "Mozilla/5.0 (Windows
NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.3"
127.0.0.1 - - [10/Oct/2023:12:37:30 +0000] "GET /admin HTTP/1.1" 403 1234 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64
) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.3"
10.0.0.1 - - [18/Jan/2025:12:36:00 +0000] "GET /admin HTTP/1.1" 404 123 "-" "curl/7.68.0"
192.168.1.100 - - [18/Jan/2025:12:37:00 +0000] "POST /login HTTP/1.1" 500 456 "-" "Python-requests/2.25.1"
10.0.0.2 - - [18/Jan/2025:12:38:00 +0000] "GET /wp-admin HTTP/1.1" 403 789 "-" "Wget/1.21"
127.0.0.1 - - [19/Jan/2025:12:34:56 +0000] "GET /admin HTTP/1.1" 404 123 "-" "curl/7.68.0"
192.168.1.100 - - [19/Jan/2025:12:35:00 +0000] "POST /login HTTP/1.1" 500 456 "-" "Python-requests/2.25.1"
10.0.0.1 - - [19/Jan/2025:12:36:00 +0000] "GET /wp-admin HTTP/1.1" 403 789 "-" "Wget/1.21"
172.16.0.1 - - [19/Jan/2025:12:37:00 +0000] "GET /test HTTP/1.1" 404 321 "-" "curl/7.68.0"
192.168.0.1 - - [19/Jan/2025:12:38:00 +0000] "POST /api HTTP/1.1" 500 654 "-" "Python-requests/2.25.1"
2025-01-19 13:40:33,992 INFO: Elasticsearch Response: {"_index":"security-scanner","_type":"_doc","_id":"FY_df5QBP0pURh
Cf3NDC","_version":1,"result":"created","_shards":{"total":2,"successful":1,"failed":0},"_seq_no":324,"_primary_term":8
}
2025-01-19 13:40:34,004 INFO: Elasticsearch Response: {"_index":"security-scanner","_type":"_doc","_id":"Fo_df5QBP0pURh
Cf3NDM","_version":1,"result":"created","_shards":{"total":2,"successful":1,"failed":0},"_seq_no":325,"_primary_term":8
}
2025-01-19 13:40:35,057 ERROR: Error sending email: (535, b'5.7.8 Username and Password not accepted. For more informat
ion, go to\n5.7.8  https://support.google.com/mail/?p=BadCredentials 5b1f17b1804b1-437c74c4e38sm169594165e9.21 - gsmtp'
)
2025-01-19 13:40:35,066 INFO: Blocked IP address: 127.0.0.1
2025-01-19 13:40:35,071 INFO: Blocked IP address: 127.0.0.1
2025-01-19 13:40:35,077 INFO: Blocked IP address: 127.0.0.1
2025-01-19 13:40:35,082 INFO: Blocked IP address: 127.0.0.1
2025-01-19 13:40:35,088 INFO: Blocked IP address: 127.0.0.1
2025-01-19 13:40:35,093 INFO: Blocked IP address: 127.0.0.1
2025-01-19 13:40:35,098 INFO: Blocked IP address: 127.0.0.1
2025-01-19 13:40:35,104 INFO: Blocked IP address: 127.0.0.1
2025-01-19 13:40:35,109 INFO: Blocked IP address: 10.0.0.1
2025-01-19 13:40:35,117 INFO: Blocked IP address: 192.168.1.100
2025-01-19 13:40:35,125 INFO: Blocked IP address: 10.0.0.2
2025-01-19 13:40:35,130 INFO: Blocked IP address: 127.0.0.1
2025-01-19 13:40:35,136 INFO: Blocked IP address: 192.168.1.100
2025-01-19 13:40:35,141 INFO: Blocked IP address: 10.0.0.1
2025-01-19 13:40:35,146 INFO: Blocked IP address: 172.16.0.1
2025-01-19 13:40:35,153 INFO: Blocked IP address: 192.168.0.1
```



```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -L -n -v
Chain INPUT (policy ACCEPT 126 packets, 41005 bytes)
 pkts bytes target     prot opt in     out     source               destination
  696  131K DROP       all  --  *       *       127.0.0.1            0.0.0.0/0
    0     0 DROP       all  --  *       *       127.0.0.1            0.0.0.0/0
    0     0 DROP       all  --  *       *       127.0.0.1            0.0.0.0/0
    0     0 DROP       all  --  *       *       127.0.0.1            0.0.0.0/0
    0     0 DROP       all  --  *       *       127.0.0.1            0.0.0.0/0
    0     0 DROP       all  --  *       *       127.0.0.1            0.0.0.0/0
    0     0 DROP       all  --  *       *       127.0.0.1            0.0.0.0/0
    0     0 DROP       all  --  *       *       127.0.0.1            0.0.0.0/0
    0     0 DROP       all  --  *       *       10.0.0.1             0.0.0.0/0
    0     0 DROP       all  --  *       *       192.168.1.100        0.0.0.0/0
    0     0 DROP       all  --  *       *       10.0.0.2             0.0.0.0/0
    0     0 DROP       all  --  *       *       127.0.0.1            0.0.0.0/0
    0     0 DROP       all  --  *       *       127.0.0.1            0.0.0.0/0
    0     0 DROP       all  --  *       *       127.0.0.1            0.0.0.0/0
    0     0 DROP       all  --  *       *       127.0.0.1            0.0.0.0/0
    0     0 DROP       all  --  *       *       127.0.0.1            0.0.0.0/0
    0     0 DROP       all  --  *       *       127.0.0.1            0.0.0.0/0
    0     0 DROP       all  --  *       *       127.0.0.1            0.0.0.0/0
    0     0 DROP       all  --  *       *       127.0.0.1            0.0.0.0/0
    0     0 DROP       all  --  *       *       10.0.0.1             0.0.0.0/0
    0     0 DROP       all  --  *       *       192.168.1.100        0.0.0.0/0
    0     0 DROP       all  --  *       *       10.0.0.2             0.0.0.0/0
    0     0 DROP       all  --  *       *       127.0.0.1            0.0.0.0/0
    0     0 DROP       all  --  *       *       192.168.1.100        0.0.0.0/0
    0     0 DROP       all  --  *       *       127.0.0.1            0.0.0.0/0
    0     0 DROP       all  --  *       *       127.0.0.1            0.0.0.0/0
    0     0 DROP       all  --  *       *       127.0.0.1            0.0.0.0/0
    0     0 DROP       all  --  *       *       127.0.0.1            0.0.0.0/0
    0     0 DROP       all  --  *       *       127.0.0.1            0.0.0.0/0
    0     0 DROP       all  --  *       *       127.0.0.1            0.0.0.0/0
    0     0 DROP       all  --  *       *       127.0.0.1            0.0.0.0/0
    0     0 DROP       all  --  *       *       127.0.0.1            0.0.0.0/0
    0     0 DROP       all  --  *       *       10.0.0.1             0.0.0.0/0
    0     0 DROP       all  --  *       *       192.168.1.100        0.0.0.0/0
    0     0 DROP       all  --  *       *       10.0.0.2             0.0.0.0/0
```

OBSTACLES AND SOLUTIONS

Apache Server Not Working

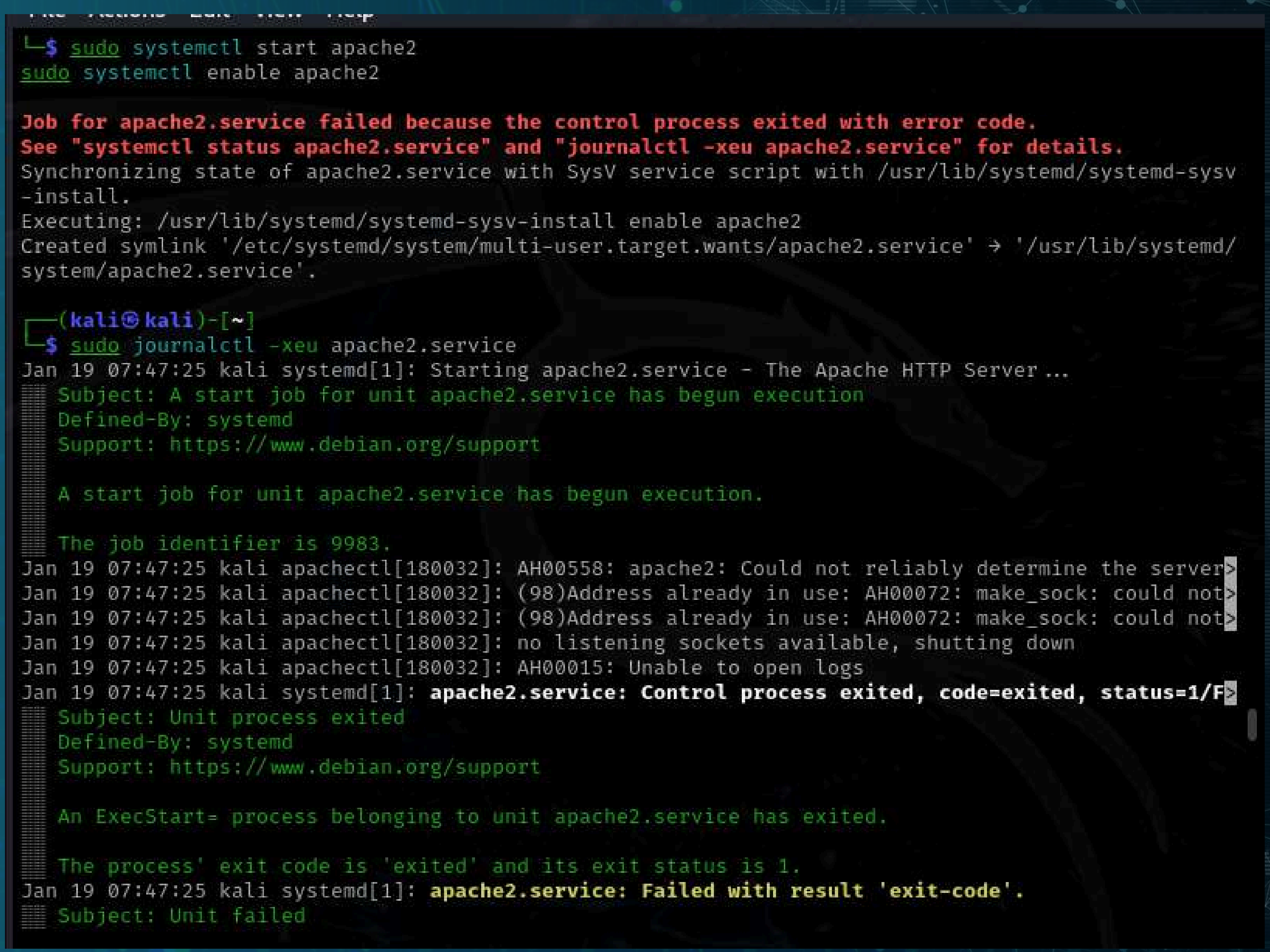
- The Apache server failed to start due to port conflicts.

Firefox ,elasticsearch Not Working Due to SELinux Policies

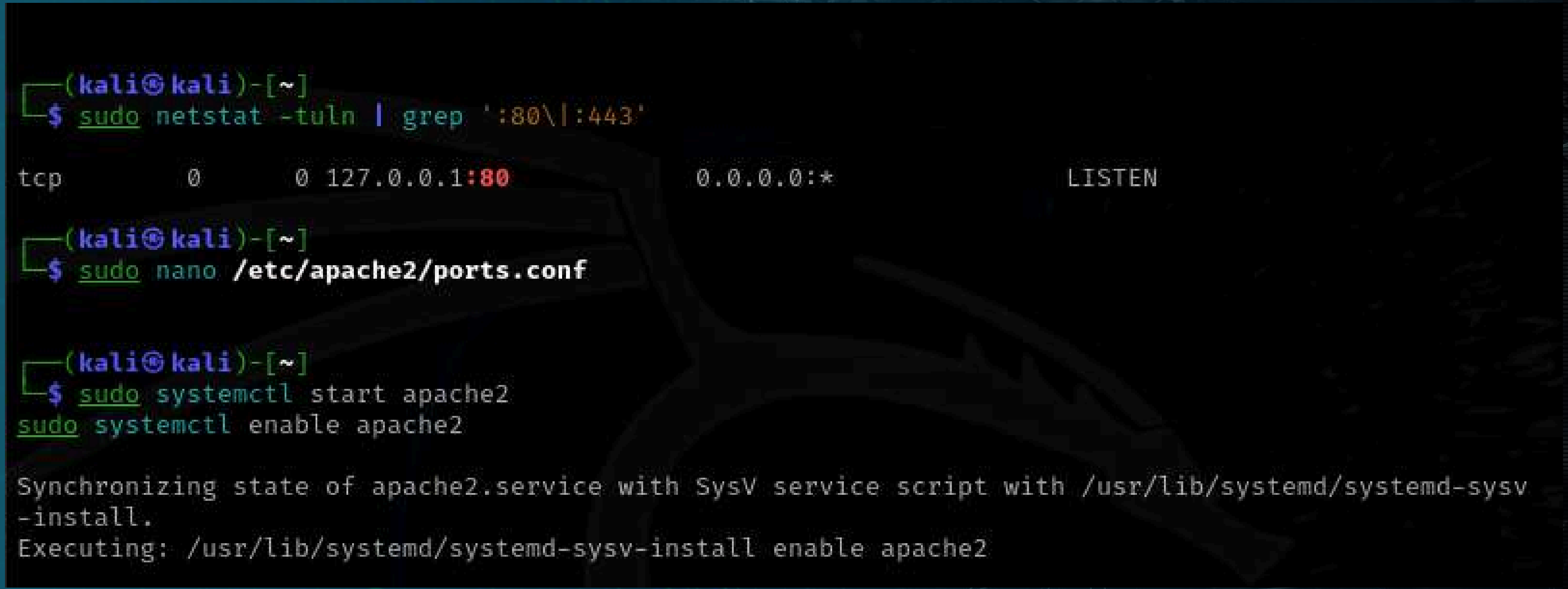
- Firefox was unable to access certain resources because of strict SELinux policies.

Alerts and Response in Kibana Not Functioning

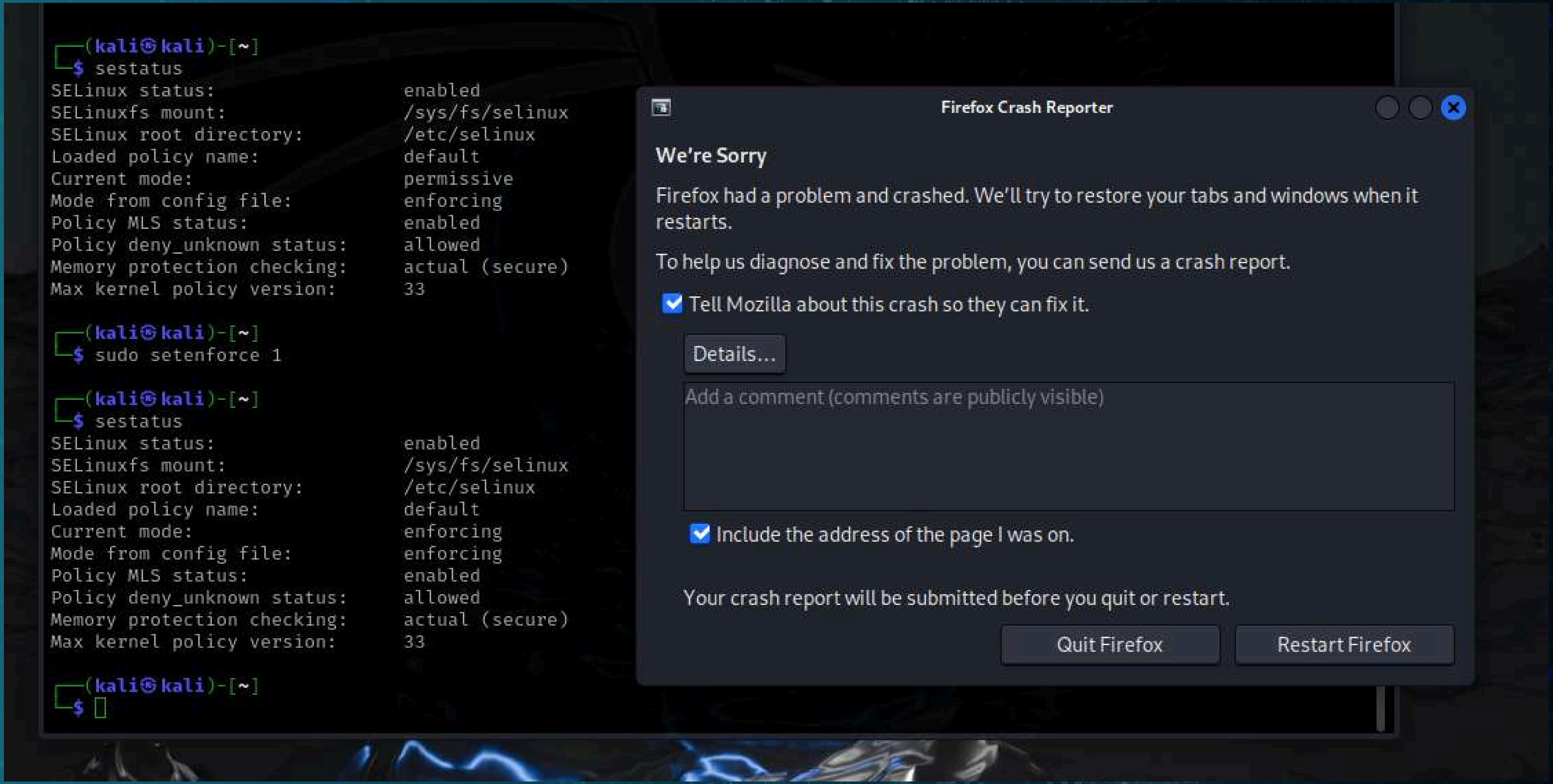
- Faced difficulties setting up alerts and automated responses in Kibana.



```
File  Actions  Edit  View  Help
└─$ sudo systemctl start apache2
sudo systemctl enable apache2

Job for apache2.service failed because the control process exited with error code.
See "systemctl status apache2.service" and "journalctl -xeu apache2.service" for details.
Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-sysv
-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2
Created symlink '/etc/systemd/system/multi-user.target.wants/apache2.service' → '/usr/lib/systemd/
system/apache2.service'.

┌──(kali㉿kali)-[~]
└─$ sudo journalctl -xeu apache2.service
Jan 19 07:47:25 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
░░ Subject: A start job for unit apache2.service has begun execution
░░ Defined-By: systemd
░░ Support: https://www.debian.org/support
░░
░░ A start job for unit apache2.service has begun execution.
░░
░░ The job identifier is 9983.
Jan 19 07:47:25 kali apachectl[180032]: AH00558: apache2: Could not reliably determine the server>
Jan 19 07:47:25 kali apachectl[180032]: (98)Address already in use: AH00072: make_sock: could not>
Jan 19 07:47:25 kali apachectl[180032]: (98)Address already in use: AH00072: make_sock: could not>
Jan 19 07:47:25 kali apachectl[180032]: no listening sockets available, shutting down
Jan 19 07:47:25 kali apachectl[180032]: AH00015: Unable to open logs
Jan 19 07:47:25 kali systemd[1]: apache2.service: Control process exited, code=exited, status=1/F>
░░ Subject: Unit process exited
░░ Defined-By: systemd
░░ Support: https://www.debian.org/support
░░
░░ An ExecStart= process belonging to unit apache2.service has exited.
░░
░░ The process' exit code is 'exited' and its exit status is 1.
Jan 19 07:47:25 kali systemd[1]: apache2.service: Failed with result 'exit-code'.
░░ Subject: Unit failed
```



```
┌──(kali㉿kali)-[~]
└─$ sudo netstat -tuln | grep ':80\|:443'
tcp        0      0 127.0.0.1:80            0.0.0.0:*               LISTEN

┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/apache2/ports.conf


┌──(kali㉿kali)-[~]
└─$ sudo systemctl start apache2
sudo systemctl enable apache2

Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-sysv
-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2
```



```
┌──(kali㉿kali)-[~]
└─$ sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             default
Current mode:                   permissive
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33

┌──(kali㉿kali)-[~]
└─$ sudo setenforce 1

┌──(kali㉿kali)-[~]
└─$ sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             default
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33

┌──(kali㉿kali)-[~]
└─$ 
```

Firefox Crash Reporter

We're Sorry

Firefox had a problem and crashed. We'll try to restore your tabs and windows when it restarts.

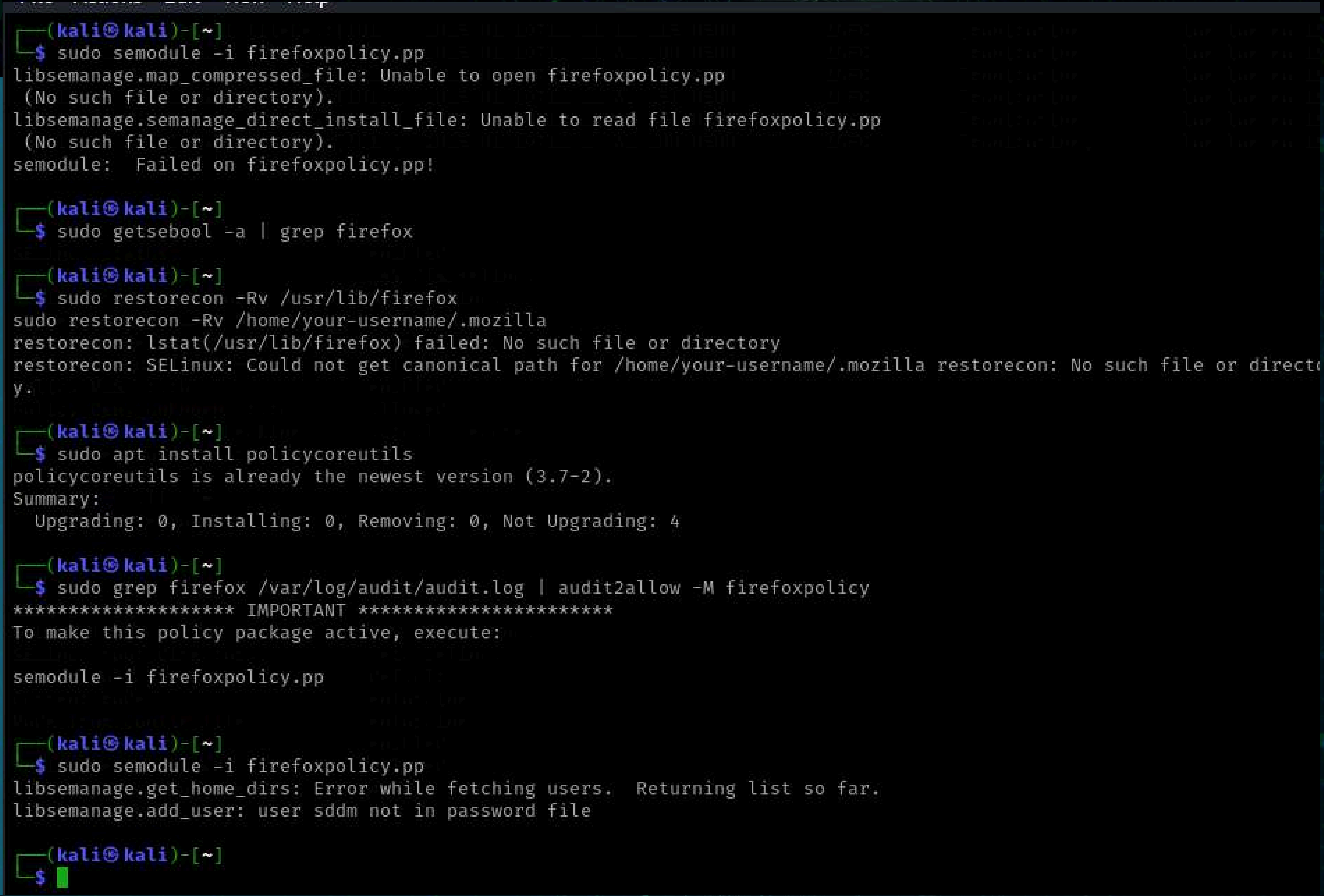
To help us diagnose and fix the problem, you can send us a crash report.

☑ Tell Mozilla about this crash so they can fix it.

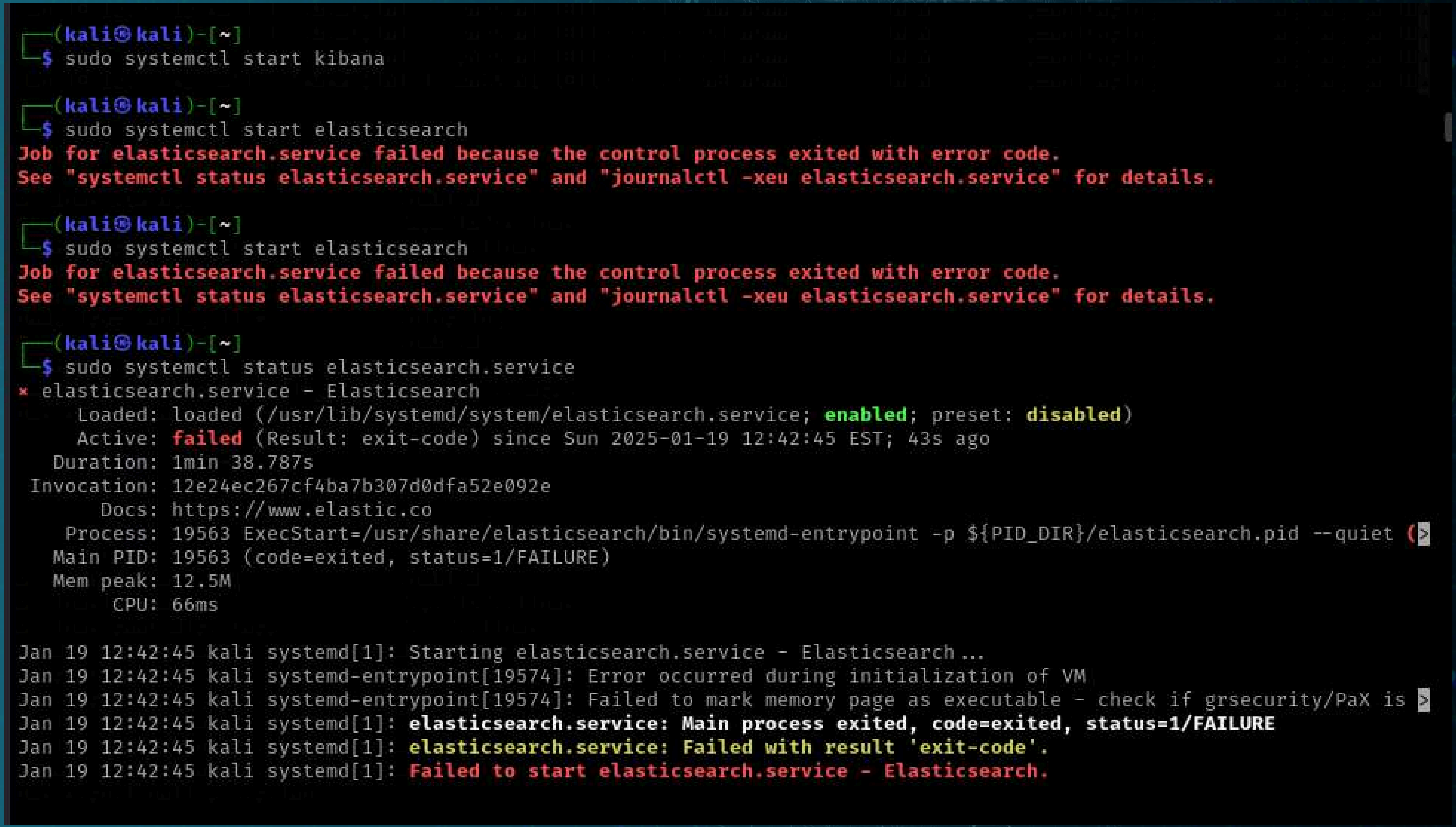
Add a comment (comments are publicly visible)

☑ Include the address of the page I was on.

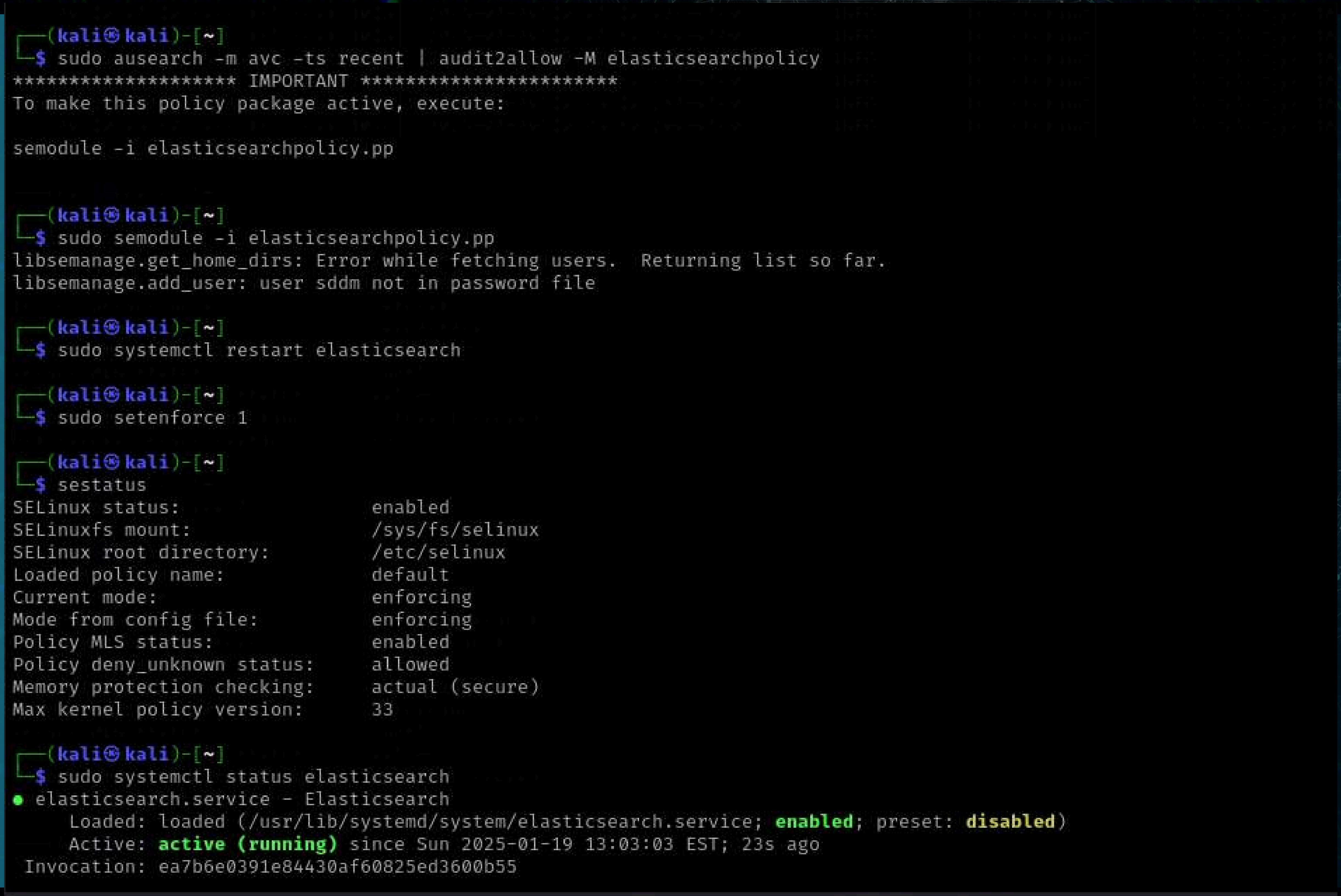
Your crash report will be submitted before you quit or restart.



```
┌──(kali㉿kali)-[~]
└─$ sudo semodule -i firefoxpolicy.pp
libsemanage.map_compressed_file: Unable to open firefoxpolicy.pp
 (No such file or directory).
libsemanage.semanage_direct_install_file: Unable to read file firefoxpolicy.pp
 (No such file or directory).
semodule:  Failed on firefoxpolicy.pp!

┌──(kali㉿kali)-[~]
└─$ sudo getsebool -a | grep firefox

┌──(kali㉿kali)-[~]
└─$ sudo restorecon -Rv /usr/lib/firefox
sudo restorecon -Rv /home/your-username/.mozilla
restorecon: lstat(/usr/lib/firefox) failed: No such file or directory
restorecon: SELinux: Could not get canonical path for /home/your-username/.mozilla restorecon: No such file or directo
y.

┌──(kali㉿kali)-[~]
└─$ sudo apt install policycoreutils
policycoreutils is already the newest version (3.7-2).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 4

┌──(kali㉿kali)-[~]
└─$ sudo grep firefox /var/log/audit/audit.log | audit2allow -M firefoxpolicy
******************** IMPORTANT ***********************
To make this policy package active, execute:

semodule -i firefoxpolicy.pp

┌──(kali㉿kali)-[~]
└─$ sudo semodule -i firefoxpolicy.pp
libsemanage.get_home_dirs: Error while fetching users.  Returning list so far.
libsemanage.add_user: user sddm not in password file

┌──(kali㉿kali)-[~]
└─$ 
```



```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl start kibana

┌──(kali㉿kali)-[~]
└─$ sudo systemctl start elasticsearch
Job for elasticsearch.service failed because the control process exited with error code.
See "systemctl status elasticsearch.service" and "journalctl -xeu elasticsearch.service" for details.

┌──(kali㉿kali)-[~]
└─$ sudo systemctl start elasticsearch
Job for elasticsearch.service failed because the control process exited with error code.
See "systemctl status elasticsearch.service" and "journalctl -xeu elasticsearch.service" for details.

┌──(kali㉿kali)-[~]
└─$ sudo systemctl status elasticsearch.service
× elasticsearch.service - Elasticsearch
     Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; preset: disabled)
     Active: failed (Result: exit-code) since Sun 2025-01-19 12:42:45 EST; 43s ago
   Duration: 1min 38.787s
 Invocation: 12e24ec267cf4ba7b307d0dfa52e092e
       Docs: https://www.elastic.co
    Process: 19563 ExecStart=/usr/share/elasticsearch/bin/systemd-entrypoint -p ${PID_DIR}/elasticsearch.pid --quiet (>
   Main PID: 19563 (code=exited, status=1/FAILURE)
   Mem peak: 12.5M
        CPU: 66ms

Jan 19 12:42:45 kali systemd[1]: Starting elasticsearch.service - Elasticsearch...
Jan 19 12:42:45 kali systemd-entrypoint[19574]: Error occurred during initialization of VM
Jan 19 12:42:45 kali systemd-entrypoint[19574]: Failed to mark memory page as executable - check if grsecurity/PaX is >
Jan 19 12:42:45 kali systemd[1]: elasticsearch.service: Main process exited, code=exited, status=1/FAILURE
Jan 19 12:42:45 kali systemd[1]: elasticsearch.service: Failed with result 'exit-code'.
Jan 19 12:42:45 kali systemd[1]: Failed to start elasticsearch.service - Elasticsearch.
```



```
┌──(kali㉿kali)-[~]
└─$ sudo ausearch -m avc -ts recent | audit2allow -M elasticsearchpolicy
******************** IMPORTANT ***********************
To make this policy package active, execute:

semodule -i elasticsearchpolicy.pp


┌──(kali㉿kali)-[~]
└─$ sudo semodule -i elasticsearchpolicy.pp
libsemanage.get_home_dirs: Error while fetching users.  Returning list so far.
libsemanage.add_user: user sddm not in password file

┌──(kali㉿kali)-[~]
└─$ sudo systemctl restart elasticsearch

┌──(kali㉿kali)-[~]
└─$ sudo setenforce 1

┌──(kali㉿kali)-[~]
└─$ sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             default
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33

┌──(kali㉿kali)-[~]
└─$ sudo systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; preset: disabled)
     Active: active (running) since Sun 2025-01-19 13:03:03 EST; 23s ago
 Invocation: ea7b6e0391e84430af60825ed3600b55
```

FUTURE IMPROVEMENTS

Integration with Other Tools:

integrating with Suricata for network intrusion detection or Wazuh for endpoint security.

Advanced Analytics

Using machine learning models to automatically detect anomalies in log data

CONCLUSION

This project demonstrated the importance of centralized log management and real-time security monitoring for web servers. By leveraging the ELK stack and SELinux, WE was able to detect and respond to security incidents effectively. Despite encountering obstacles such as Apache port conflicts, SELinux policy restrictions, and Kibana alert limitations, WE implemented practical solutions, including a custom Python script. This project not only enhanced out understanding of cybersecurity but also provided a scalable and adaptable solution for future improvements.

THANK YOU FOR YOUR ATTENTION !!!

←

DONE