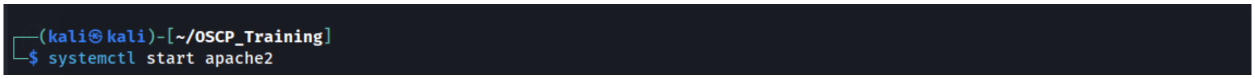
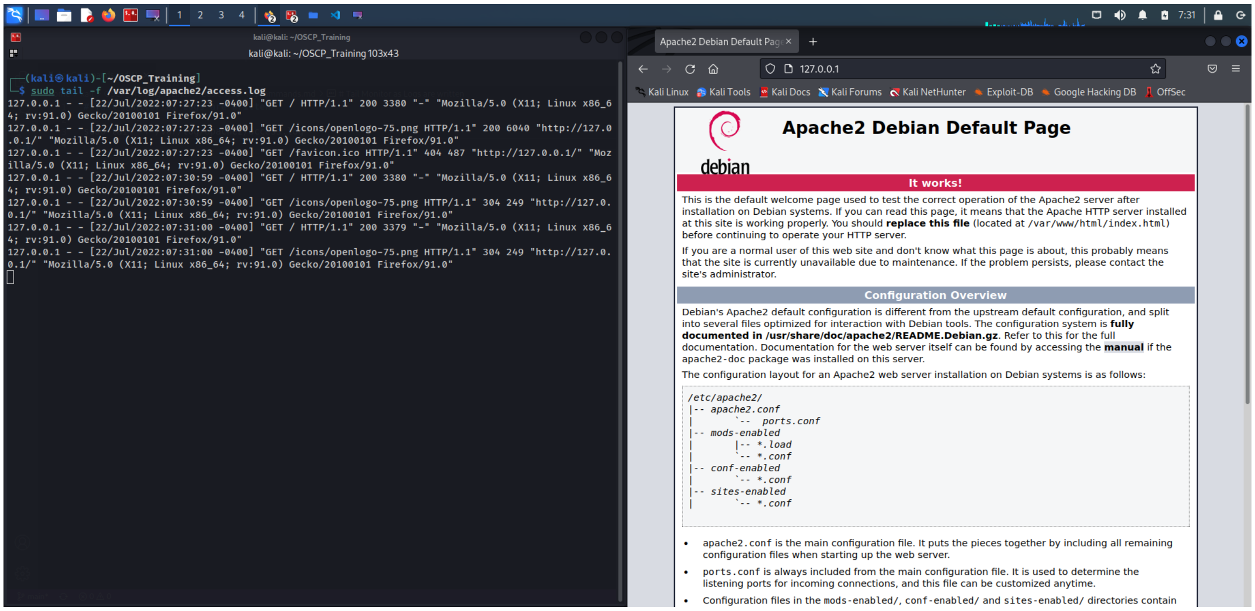
OSCP-OS-562990

3.7.3. Practice - File and Command Monitoring

1. Start your apache2 web service and access it locally while monitoring its access.log file in real-time.



```
┌──(kali㉿kali)-[~/OSCP_Training]
└─$ systemctl start apache2
```



```
┌──(kali㉿kali)-[~/OSCP_Training]
└─$ sudo tail -f /var/log/apache2/access.log
127.0.0.1 - - [22/Jul/2022:07:27:23 -0400] "GET / HTTP/1.1" 200 3380 "-" "Mozilla/5.0 (X11; Linux x86_6
4; rv:91.0) Gecko/20100101 Firefox/91.0"
127.0.0.1 - - [22/Jul/2022:07:27:23 -0400] "GET /icons/openlogo-75.png HTTP/1.1" 200 6040 "http://127.0
.0.1/" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
127.0.0.1 - - [22/Jul/2022:07:27:23 -0400] "GET /favicon.ico HTTP/1.1" 404 487 "http://127.0.0.1/" "Moz
illa/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
127.0.0.1 - - [22/Jul/2022:07:30:59 -0400] "GET / HTTP/1.1" 200 3380 "-" "Mozilla/5.0 (X11; Linux x86_6
4; rv:91.0) Gecko/20100101 Firefox/91.0"
127.0.0.1 - - [22/Jul/2022:07:30:59 -0400] "GET /icons/openlogo-75.png HTTP/1.1" 304 249 "http://127.0.
0.1/" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
127.0.0.1 - - [22/Jul/2022:07:31:00 -0400] "GET / HTTP/1.1" 200 3379 "-" "Mozilla/5.0 (X11; Linux x86_6
4; rv:91.0) Gecko/20100101 Firefox/91.0"
127.0.0.1 - - [22/Jul/2022:07:31:00 -0400] "GET /icons/openlogo-75.png HTTP/1.1" 304 249 "http://127.0.
0.1/" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
```

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

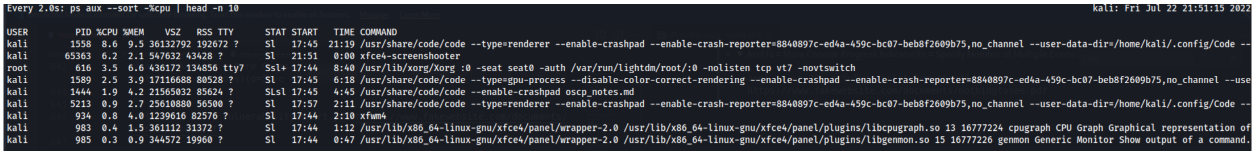
Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. 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
```

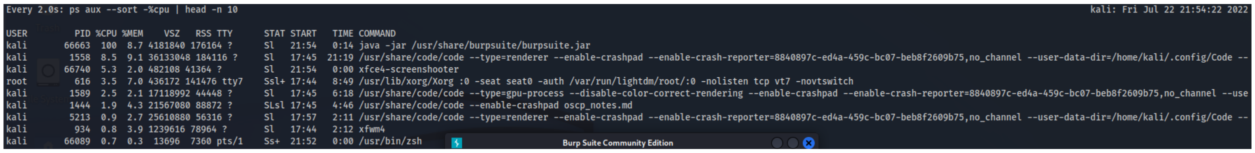
- apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain

2. Use a combination of watch and ps to monitor the most CPU-intensive processes on your Kali machine in a terminal window; launch different applications to see how the list changes in real time.



```
Every 2.0s: ps aux --sort -%cpu | head -n 10                                                                  kali: Fri Jul 22 21:51:15 2022

USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
kali        1558  8.6  9.5 36132792 192672 ?     Sl   17:45  21:19 /usr/share/code/code --type=renderer --enable-crashpad --enable-crash-reporter=8840897c-ed4a-459c-bc07-beb8f2609b75,no_channel --user-data-dir=/home/kali/.config/Code --
kali       65363  6.2  2.1 547632 43428 ?        Sl   21:51   0:00 xfce4-screenshooter
root         616  3.5  6.6 436172 134856 tty7    Ssl+ 17:44   8:40 /usr/lib/xorg/Xorg :0 -seat seat0 -auth /var/run/lightdm/root/:0 -nolisten tcp vt7 -novtswitch
kali        1589  2.5  3.9 17116688 80528 ?      Sl   17:45   6:18 /usr/share/code/code --type=gpu-process --disable-color-correct-rendering --enable-crashpad --enable-crash-reporter=8840897c-ed4a-459c-bc07-beb8f2609b75,no_channel --use
kali        1444  1.9  4.2 21565032 85624 ?      SLsl 17:45   4:45 /usr/share/code/code --enable-crashpad oscp_notes.md
kali        5213  0.9  2.7 25610880 56500 ?      Sl   17:57   2:11 /usr/share/code/code --type=renderer --enable-crashpad --enable-crash-reporter=8840897c-ed4a-459c-bc07-beb8f2609b75,no_channel --user-data-dir=/home/kali/.config/Code --
kali         934  0.8  4.0 1239616 82576 ?       Sl   17:44   2:10 xfwm4
kali         983  0.4  1.5 361112 31372 ?        Sl   17:44   1:12 /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libcpugraph.so 13 16777224 cpugraph CPU Graph Graphical representation of
kali         985  0.3  0.9 344572 19960 ?        Sl   17:44   0:47 /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libgenmon.so 15 16777226 genmon Generic Monitor Show output of a command.
```



```
Every 2.0s: ps aux --sort -%cpu | head -n 10                                                                  kali: Fri Jul 22 21:54:22 2022

USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
kali       66663  100  8.7 4181840 176164 ?      Sl   21:54   0:14 java -jar /usr/share/burpsuite/burpsuite.jar
kali        1558  8.5  9.1 36133048 184116 ?     Sl   17:45  21:19 /usr/share/code/code --type=renderer --enable-crashpad --enable-crash-reporter=8840897c-ed4a-459c-bc07-beb8f2609b75,no_channel --user-data-dir=/home/kali/.config/Code --
kali       66740  5.3  2.0 482108 41364 ?        Sl   21:54   0:00 xfce4-screenshooter
root         616  3.5  7.0 436172 141476 tty7    Ssl+ 17:44   8:49 /usr/lib/xorg/Xorg :0 -seat seat0 -auth /var/run/lightdm/root/:0 -nolisten tcp vt7 -novtswitch
kali        1589  2.5  2.1 17118992 44448 ?      Sl   17:45   6:18 /usr/share/code/code --type=gpu-process --disable-color-correct-rendering --enable-crashpad --enable-crash-reporter=8840897c-ed4a-459c-bc07-beb8f2609b75,no_channel --use
kali        1444  1.9  4.3 21567080 88872 ?      SLsl 17:45   4:46 /usr/share/code/code --enable-crashpad oscp_notes.md
kali        5213  0.9  2.7 25610880 56316 ?      Sl   17:57   2:11 /usr/share/code/code --type=renderer --enable-crashpad --enable-crash-reporter=8840897c-ed4a-459c-bc07-beb8f2609b75,no_channel --user-data-dir=/home/kali/.config/Code --
kali         934  0.8  3.9 1239616 78964 ?       Sl   17:44   2:12 xfwm4
kali       66089  0.7  0.3  13696  7360 pts/1    Ss+  21:52   0:00 /usr/bin/zsh
```