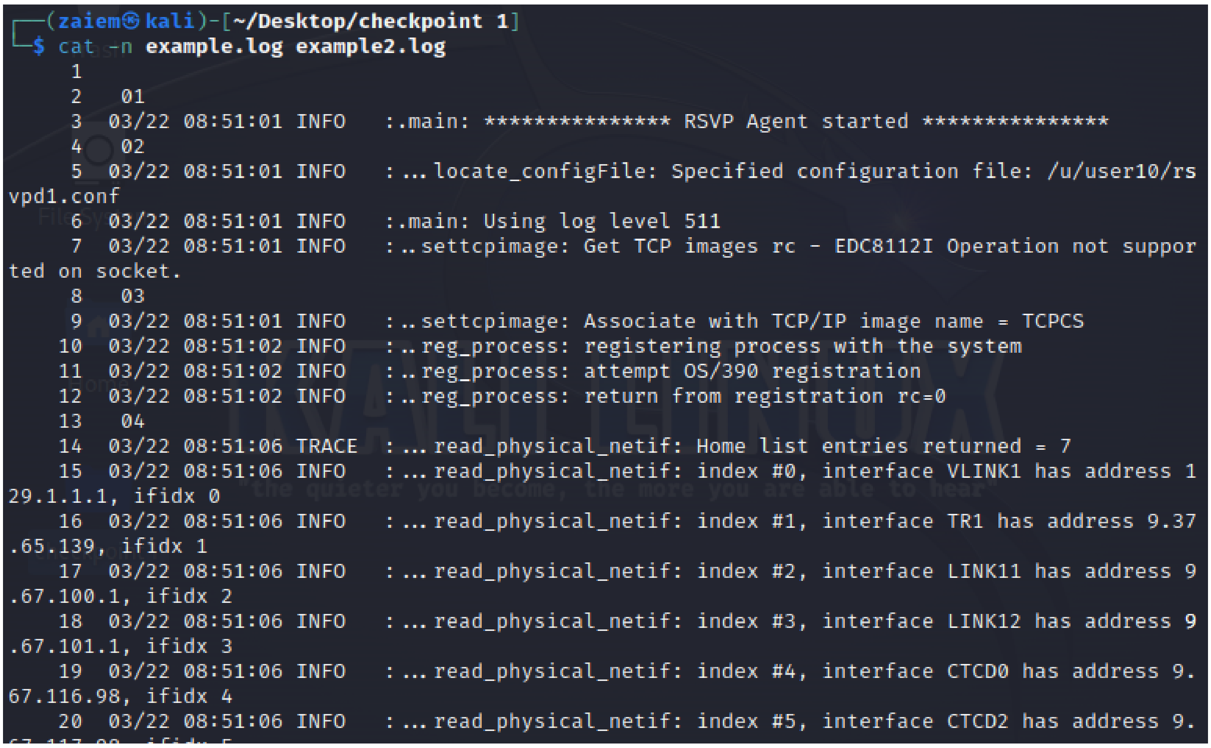
<u>Intro to CyberSecurity Checkpoint</u>

Step 1: Open Terminal

Step 2: View Content of Files

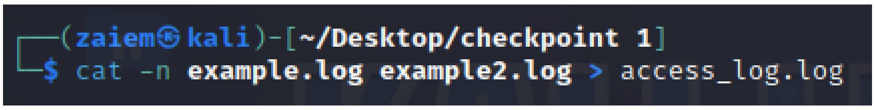
cat -n example.log example2.log: This command displays the contents of `example.log` and `example2.log` with line numbers.



```
┌──(zaiem㉿kali)-[~/Desktop/checkpoint 1]
└─$ cat -n example.log example2.log
     1
     2   01
     3  03/22 08:51:01 INFO   :.main: *************** RSVP Agent started ***************
     4   02
     5  03/22 08:51:01 INFO   :...locate_configFile: Specified configuration file: /u/user10/rs
vpd1.conf
     6  03/22 08:51:01 INFO   :.main: Using log level 511
     7  03/22 08:51:01 INFO   :..settcpimage: Get TCP images rc - EDC8112I Operation not suppor
ted on socket.
     8   03
     9  03/22 08:51:01 INFO   :..settcpimage: Associate with TCP/IP image name = TCPCS
    10  03/22 08:51:02 INFO   :..reg_process: registering process with the system
    11  03/22 08:51:02 INFO   :..reg_process: attempt OS/390 registration
    12  03/22 08:51:02 INFO   :..reg_process: return from registration rc=0
    13   04
    14  03/22 08:51:06 TRACE  :...read_physical_netif: Home list entries returned = 7
    15  03/22 08:51:06 INFO   :...read_physical_netif: index #0, interface VLINK1 has address 1
29.1.1.1, ifidx 0
    16  03/22 08:51:06 INFO   :...read_physical_netif: index #1, interface TR1 has address 9.37
.65.139, ifidx 1
    17  03/22 08:51:06 INFO   :...read_physical_netif: index #2, interface LINK11 has address 9
.67.100.1, ifidx 2
    18  03/22 08:51:06 INFO   :...read_physical_netif: index #3, interface LINK12 has address 9
.67.101.1, ifidx 3
    19  03/22 08:51:06 INFO   :...read_physical_netif: index #4, interface CTCD0 has address 9.
67.116.98, ifidx 4
    20  03/22 08:51:06 INFO   :...read_physical_netif: index #5, interface CTCD2 has address 9.
```

Step 3: Redirect Output to a File

cat -n example.log example2.log > access_log.log: This command saves the content of `example.log` and `example2.log` with line numbers into a file named `access_log.log`.

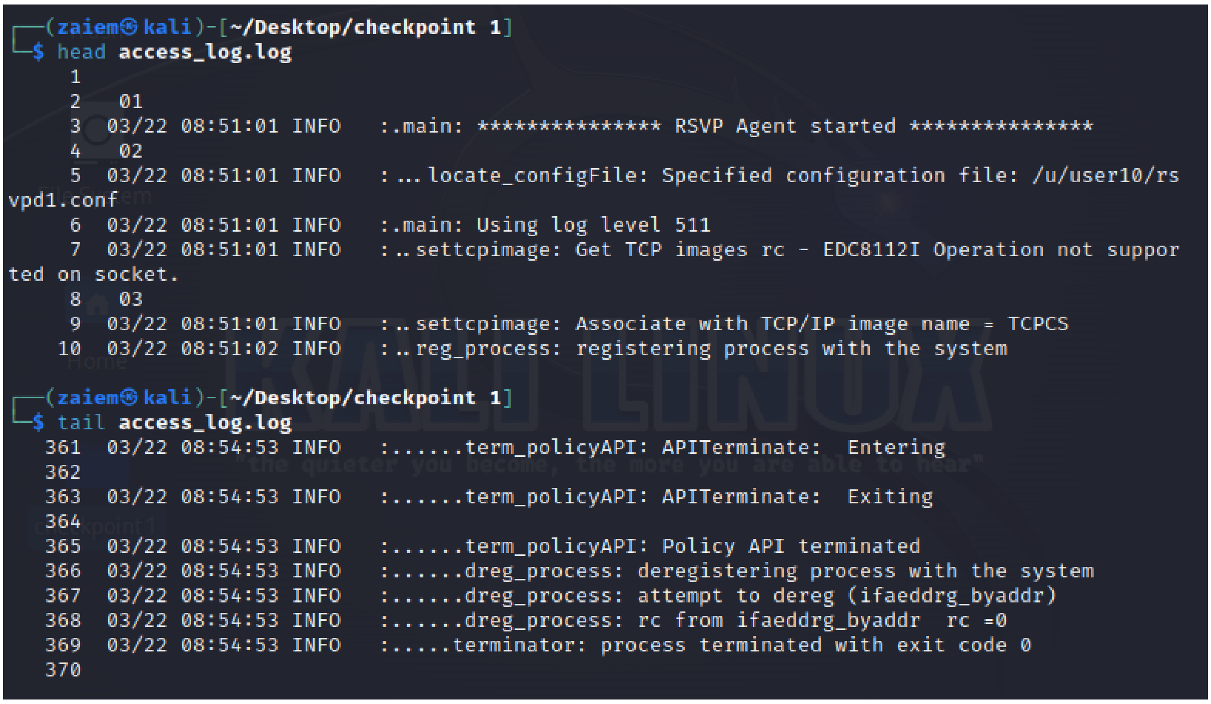


```
┌──(zaiem㉿kali)-[~/Desktop/checkpoint 1]
└─$ cat -n example.log example2.log > access_log.log
```

Step 4: Display First and last 10 Lines

head access_log.log: This will show the first 10 lines of access_log.log.

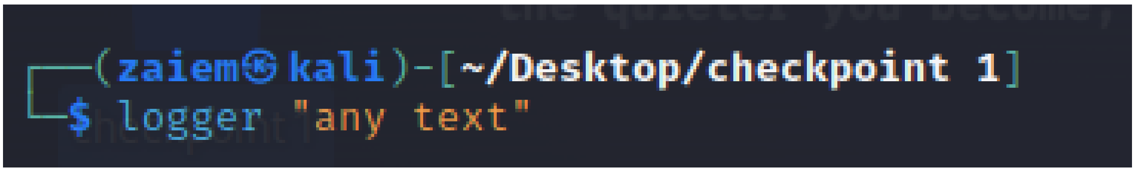
tail access_log.log: This will show the last 10 lines of `access_log.log`.



```
┌──(zaiem㉿kali)-[~/Desktop/checkpoint 1]
└─$ head access_log.log
     1
     2    01
     3  03/22 08:51:01 INFO   :.main: *************** RSVP Agent started ***************
     4    02
     5  03/22 08:51:01 INFO   :...locate_configFile: Specified configuration file: /u/user10/rs
vpd1.conf
     6  03/22 08:51:01 INFO   :.main: Using log level 511
     7  03/22 08:51:01 INFO   :..settcpimage: Get TCP images rc - EDC8112I Operation not suppor
ted on socket.
     8    03
     9  03/22 08:51:01 INFO   :..settcpimage: Associate with TCP/IP image name = TCPCS
    10  03/22 08:51:02 INFO   :..reg_process: registering process with the system

┌──(zaiem㉿kali)-[~/Desktop/checkpoint 1]
└─$ tail access_log.log
   361  03/22 08:54:53 INFO   :......term_policyAPI: APITerminate:  Entering
   362
   363  03/22 08:54:53 INFO   :......term_policyAPI: APITerminate:  Exiting
   364
   365  03/22 08:54:53 INFO   :......term_policyAPI: Policy API terminated
   366  03/22 08:54:53 INFO   :......dreg_process: deregistering process with the system
   367  03/22 08:54:53 INFO   :......dreg_process: attempt to dereg (ifaeddrg_byaddr)
   368  03/22 08:54:53 INFO   :......dreg_process: rc from ifaeddrg_byaddr  rc =0
   369  03/22 08:54:53 INFO   :.....terminator: process terminated with exit code 0
   370
```

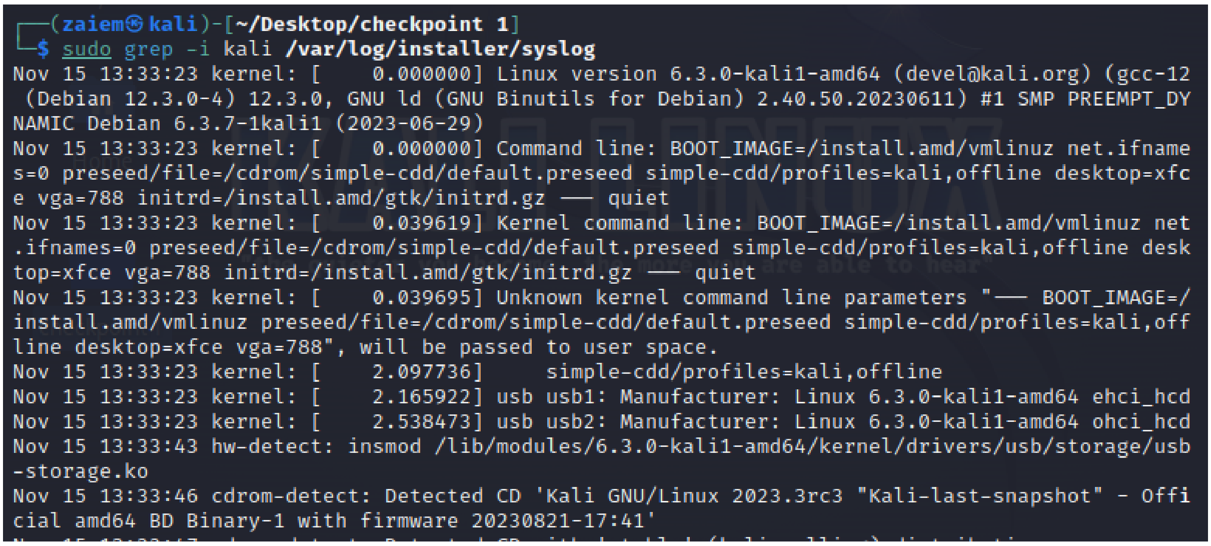
Step 6: Add Information to Syslog



```
┌──(zaiem㉿kali)-[~/Desktop/checkpoint 1]
└─$ logger "any text"
```

Step 7: Filter Syslog Output

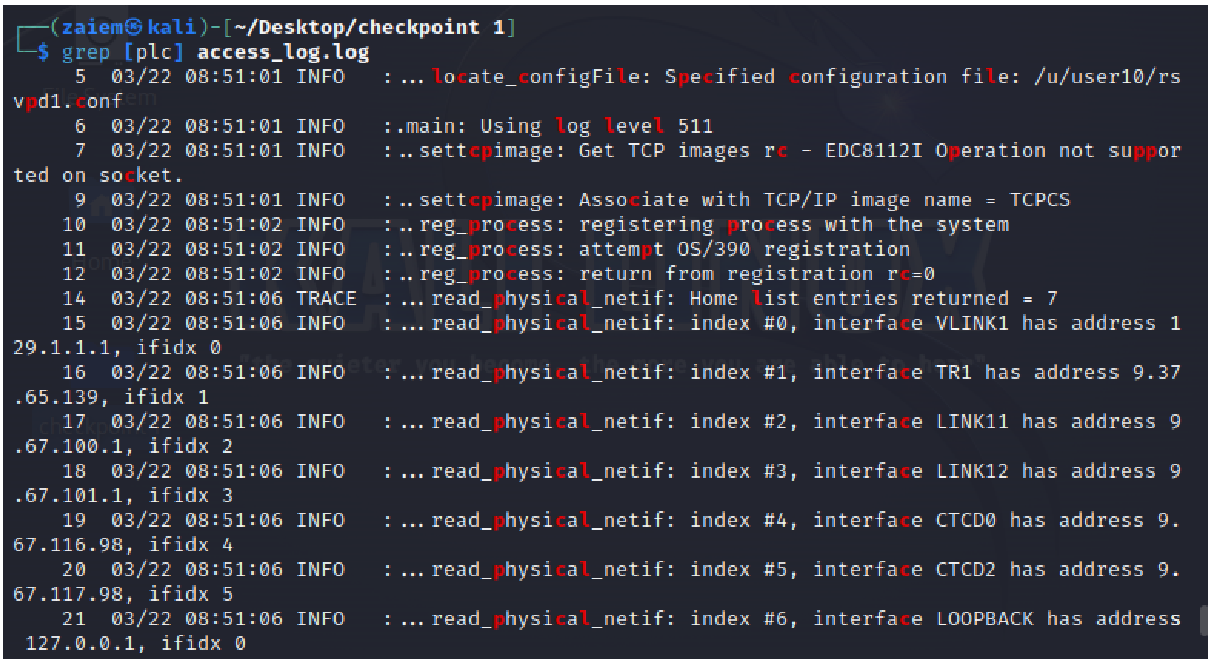
grep -i kali /var/log/syslog: This command filters and displays lines containing the keyword "kali" from the syslog.



```
┌──(zaiem㉿kali)-[~/Desktop/checkpoint 1]
└─$ sudo grep -i kali /var/log/installer/syslog
Nov 15 13:33:23 kernel: [    0.000000] Linux version 6.3.0-kali1-amd64 (devel@kali.org) (gcc-12
 (Debian 12.3.0-4) 12.3.0, GNU ld (GNU Binutils for Debian) 2.40.50.20230611) #1 SMP PREEMPT_DY
NAMIC Debian 6.3.7-1kali1 (2023-06-29)
Nov 15 13:33:23 kernel: [    0.000000] Command line: BOOT_IMAGE=/install.amd/vmlinuz net.ifname
s=0 preseed/file=/cdrom/simple-cdd/default.preseed simple-cdd/profiles=kali,offline desktop=xfc
e vga=788 initrd=/install.amd/gtk/initrd.gz --- quiet
Nov 15 13:33:23 kernel: [    0.039619] Kernel command line: BOOT_IMAGE=/install.amd/vmlinuz net
.ifnames=0 preseed/file=/cdrom/simple-cdd/default.preseed simple-cdd/profiles=kali,offline desk
top=xfce vga=788 initrd=/install.amd/gtk/initrd.gz --- quiet
Nov 15 13:33:23 kernel: [    0.039695] Unknown kernel command line parameters "--- BOOT_IMAGE=/
install.amd/vmlinuz preseed/file=/cdrom/simple-cdd/default.preseed simple-cdd/profiles=kali,off
line desktop=xfce vga=788", will be passed to user space.
Nov 15 13:33:23 kernel: [    2.097736]     simple-cdd/profiles=kali,offline
Nov 15 13:33:23 kernel: [    2.165922] usb usb1: Manufacturer: Linux 6.3.0-kali1-amd64 ehci_hcd
Nov 15 13:33:23 kernel: [    2.538473] usb usb2: Manufacturer: Linux 6.3.0-kali1-amd64 ohci_hcd
Nov 15 13:33:43 hw-detect: insmod /lib/modules/6.3.0-kali1-amd64/kernel/drivers/usb/storage/usb
-storage.ko
Nov 15 13:33:46 cdrom-detect: Detected CD 'Kali GNU/Linux 2023.3rc3 "Kali-last-snapshot" - Offi
cial amd64 BD Binary-1 with firmware 20230821-17:41'
```

Step 8: Filter Log File for Specific Words

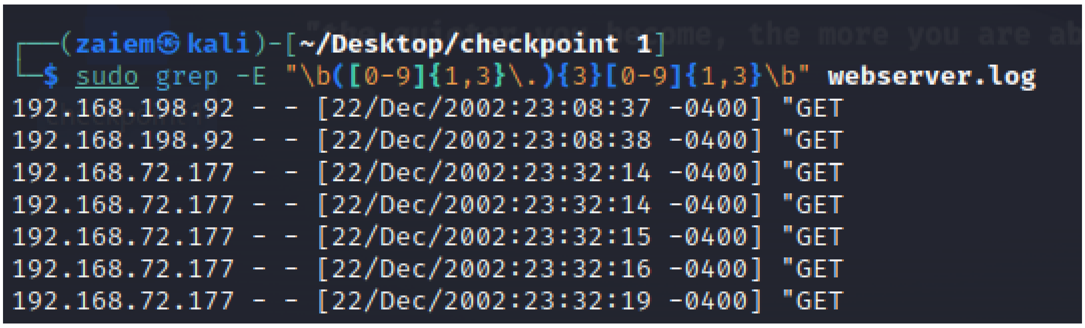
grep [plc] access_log.log: This command filters and displays lines containing 'p', 'l', or 'c' from the `access_log.log` file.



```
┌──(zaiem㉿kali)-[~/Desktop/checkpoint 1]
└─$ grep [plc] access_log.log
     5  03/22 08:51:01 INFO   :...locate_configFile: Specified configuration file: /u/user10/rs
vpd1.conf
     6  03/22 08:51:01 INFO   :.main: Using log level 511
     7  03/22 08:51:01 INFO   :..settcpimage: Get TCP images rc - EDC8112I Operation not suppor
ted on socket.
     9  03/22 08:51:01 INFO   :..settcpimage: Associate with TCP/IP image name = TCPCS
    10  03/22 08:51:02 INFO   :..reg_process: registering process with the system
    11  03/22 08:51:02 INFO   :..reg_process: attempt OS/390 registration
    12  03/22 08:51:02 INFO   :..reg_process: return from registration rc=0
    14  03/22 08:51:06 TRACE  :...read_physical_netif: Home list entries returned = 7
    15  03/22 08:51:06 INFO   :...read_physical_netif: index #0, interface VLINK1 has address 1
29.1.1.1, ifidx 0
    16  03/22 08:51:06 INFO   :...read_physical_netif: index #1, interface TR1 has address 9.37
.65.139, ifidx 1
    17  03/22 08:51:06 INFO   :...read_physical_netif: index #2, interface LINK11 has address 9
.67.100.1, ifidx 2
    18  03/22 08:51:06 INFO   :...read_physical_netif: index #3, interface LINK12 has address 9
.67.101.1, ifidx 3
    19  03/22 08:51:06 INFO   :...read_physical_netif: index #4, interface CTCD0 has address 9.
67.116.98, ifidx 4
    20  03/22 08:51:06 INFO   :...read_physical_netif: index #5, interface CTCD2 has address 9.
67.117.98, ifidx 5
    21  03/22 08:51:06 INFO   :...read_physical_netif: index #6, interface LOOPBACK has address
 127.0.0.1, ifidx 0
```

Step 9: Filter Log File for IP Addresses

grep -E "[^^][0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}" webserver.log: This command filters and displays lines containing IP addresses from the `webserver.log` file.



```
┌──(zaiem㉿kali)-[~/Desktop/checkpoint 1]
└─$ sudo grep -E "\b([0-9]{1,3}\.){3}[0-9]{1,3}\b" webserver.log
192.168.198.92 - - [22/Dec/2002:23:08:37 -0400] "GET
192.168.198.92 - - [22/Dec/2002:23:08:38 -0400] "GET
192.168.72.177 - - [22/Dec/2002:23:32:14 -0400] "GET
192.168.72.177 - - [22/Dec/2002:23:32:14 -0400] "GET
192.168.72.177 - - [22/Dec/2002:23:32:15 -0400] "GET
192.168.72.177 - - [22/Dec/2002:23:32:16 -0400] "GET
192.168.72.177 - - [22/Dec/2002:23:32:19 -0400] "GET
```