

Ex.No.9 Use Process Explorer to identify suspicious processes

AIM:

To identify and remove suspicious processes from the system using Linux command-line tools.

PROCEDURE:

Process Explorer helps monitor and analyze running processes on Windows to detect suspicious or malicious activity. It provides detailed information like CPU/memory usage, digital signatures, file paths, and network activity, allowing identification and safe termination of suspicious processes.

```
--(kali@kali)-[~]
-$ ps aux | head -10

SER          PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
oot           1  0.0  0.3  23724 14316 ?        Ss   00:55   0:01 /sbin/init splash
oot           2  0.0  0.0      0     0 ?        S    00:55   0:00 [kthreadd]
oot           3  0.0  0.0      0     0 ?        S    00:55   0:00 [pool_workqueue_release]
oot           4  0.0  0.0      0     0 ?        I<   00:55   0:00 [kworker/R-kvfree_rcu_reclaim]
oot           5  0.0  0.0      0     0 ?        I<   00:55   0:00 [kworker/R-rcu_gp]
oot           6  0.0  0.0      0     0 ?        I<   00:55   0:00 [kworker/R-sync_wq]
oot           7  0.0  0.0      0     0 ?        I<   00:55   0:00 [kworker/R-slub_flushwq]
oot           8  0.0  0.0      0     0 ?        I<   00:55   0:00 [kworker/R-netns]
oot          12  0.0  0.0      0     0 ?        I    00:55   0:00 [kworker/u12:0-ipv6_addrconf]

--(kali@kali)-[~]
-$ ps aux | grep kali

ali          1033  0.0  0.3  22852 13000 ?        Ss   00:55   0:00 /usr/lib/systemd/systemd --user
ali          1035  0.0  0.0  25048  3800 ?        S    00:55   0:00 (sd-pam)
ali          1055  0.0  0.1  9308  6120 ?        Ss   00:55   0:00 /usr/bin/dbus-daemon --session --address=systemd
--nofork --nopidfile --systemd-activation --syslog-only
ali          1056  0.0  0.3 110864 14228 ?        S<sl 00:55   0:00 /usr/bin/pipewire
ali          1057  0.0  0.1  84744  5288 ?        Ssl  00:55   0:00 /usr/bin/pipewire -c filter-chain.conf
ali          1059  0.0  0.8 613192 34012 ?        S<sl 00:55   0:00 /usr/bin/wireplumber
ali          1060  0.0  0.2  99704  8872 ?        S<sl 00:55   0:00 /usr/bin/pipewire-pulse
ali          1061  0.0  0.2 183144 10024 ?        SLsl 00:55   0:00 /usr/bin/gnome-keyring-daemon --foreground --com
onents=pkcs11,secrets --control-directory=/run/user/1000/keyring
ali          1062  0.0  0.0   7224  3480 ?        Ss   00:55   0:00 /usr/bin/mpiris-proxy
ali          1078  0.0  0.8 347984 34076 ?        Ssl  00:55   0:03 xfce4-session
ali          1168  0.0  0.0  17128  1924 ?        S    00:55   0:00 /usr/bin/VBoxClient --clipboard
ali          1170  0.0  1.8 221564 74256 ?        Sl   00:55   0:02 /usr/bin/VBoxClient --clipboard
ali          1183  0.0  0.0  17128  1924 ?        S    00:55   0:00 /usr/bin/VBoxClient --seamless
ali          1184  0.1  0.0 215416 3172 ?        Sl   00:55   0:11 /usr/bin/VBoxClient --seamless
ali          1191  0.0  0.0  17128  1752 ?        S    00:55   0:00 /usr/bin/VBoxClient --draganddrop
ali          1192  0.6  0.0 215932 2872 ?        Sl   00:55   0:38 /usr/bin/VBoxClient --draganddrop
ali          1216  0.0  0.1 381164 7408 ?        Ssl  00:55   0:00 /usr/libexec/at-spi-bus-launcher
ali          1223  0.0  0.1   8724  4976 ?        S    00:55   0:00 /usr/bin/dbus-daemon --config-file=/usr/share/de
aults/at-spi2/accessibility.conf --nofork --print-address 11
ali          1234  0.0  0.1 168876 7376 ?        Sl   00:55   0:04 /usr/libexec/at-spi2-registrd --use-gnome-sessi
n
ali          1241  0.0  0.0  10676  1736 ?        Ss   00:55   0:00 /usr/bin/ssh-agent -s
ali          1250  0.0  0.0  155452 3600 ?        Ssl  00:55   0:00 /usr/bin/gpg-agent --supervised
ali          1253  0.7  3.2 1035396 125784 ?        Sl   00:55   0:45 xfwm4
ali          1258  0.0  0.0  17128  1828 ?        S    00:55   0:00 /usr/bin/VBoxClient --vmsvga
ali          1259  0.0  0.0 215520 3472 ?        Sl   00:55   0:04 /usr/bin/VBoxClient --vmsvga
ali          1268  0.0  0.2 312636 7968 ?        Ssl  00:55   0:00 /usr/libexec/gvfsd
ali          1274  0.0  0.1 398368 6988 ?        Sl   00:55   0:00 /usr/libexec/gvfsd-fuse /run/user/1000/gvfs -f
ali          1292  0.0  0.7 277312 29132 ?        Sl   00:55   0:05 xfsettingsd
ali          1297  0.0  0.1 165228 5832 ?        Ssl  00:55   0:00 /usr/libexec/dconf-service
```

```

(kali@kali)-[~]
$ ps -p 1387 -o pid,user,cmd,lstart
PID USER      CMD                                STARTED
1387 kali      xcape -e Super_L Control_L Thu Oct 23 00:55:41 2025

(kali@kali)-[~]
$ readlink -f /proc/1387/exe
/usr/bin/xcape

```

```

(kali@kali)-[~]
$ sudo lsof -nP -p 1387 -i

sof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
Output information may be incomplete.
sof: WARNING: can't stat() fuse.portal file system /run/user/1000/doc
Output information may be incomplete.
COMMAND  PID USER  FD  TYPE             DEVICE SIZE/OFF      NODE NAME
Container 711 root   9u  IPv4             6068     0t0      TCP 127.0.0.1:45261 (LISTEN)
xcape    1387 kali   cwd  DIR              8,1      4096        2 /
xcape    1387 kali  rtd  DIR              8,1      4096        2 /
xcape    1387 kali  txt  REG             8,1     22624 1227710 /usr/bin/xcape
xcape    1387 kali  mem  REG             8,1     26728 2364354 /usr/lib/x86_64-linux-gnu/libXdmcp.so.6.0.0
xcape    1387 kali  mem  REG             8,1     14472 2364434 /usr/lib/x86_64-linux-gnu/libXau.so.6.0.0
xcape    1387 kali  mem  REG             8,1     170936 2362761 /usr/lib/x86_64-linux-gnu/libxcb.so.1.1.0
xcape    1387 kali  mem  REG             8,1      81568 2363528 /usr/lib/x86_64-linux-gnu/libXext.so.6.4.0
xcape    1387 kali  mem  REG             8,1    2003408 2364879 /usr/lib/x86_64-linux-gnu/libc.so.6
xcape    1387 kali  mem  REG             8,1    1342984 2363369 /usr/lib/x86_64-linux-gnu/libX11.so.6.4.0
xcape    1387 kali  mem  REG             8,1      26976 2365485 /usr/lib/x86_64-linux-gnu/libXtst.so.6.1.0
xcape    1387 kali  mem  REG             8,1    225600 2364657 /usr/lib/x86_64-linux-gnu/ld-linux-x86-64.so.2
xcape    1387 kali   0u  CHR              1,3         0t0        4 /dev/null
xcape    1387 kali   1u  CHR              1,3         0t0        4 /dev/null
xcape    1387 kali   2u  CHR              1,3         0t0        4 /dev/null
xcape    1387 kali   3u  unix 0x00000000d1437205 0t0 10617 type=STREAM (CONNECTED)
xcape    1387 kali   4u  unix 0x00000000bd163197 0t0 10619 type=STREAM (CONNECTED)
deconnec 1393 kali  18u  IPv6            12364     0t0      UDP *:1716
deconnec 1393 kali  19u  IPv6            12365     0t0      TCP *:1716 (LISTEN)
deconnec 1393 kali  20u  IPv4            12366     0t0      UDP *:5353
deconnec 1393 kali  21u  IPv6            12367     0t0      UDP *:5353
deconnec 1393 kali  22u  IPv4            12369     0t0      UDP *:43532
deconnec 1393 kali  23u  IPv6            12370     0t0      UDP *:58549
deconnec 1393 kali  24u  IPv6            12371     0t0      UDP *:50364
deconnec 1393 kali  25u  IPv4            12372     0t0      UDP *:52133

(kali@kali)-[~]
$ ls -l /proc/1387/fd

total 0
-rwx----- 1 kali kali 64 Oct 23 02:29 0 -> /dev/null
-rwx----- 1 kali kali 64 Oct 23 02:29 1 -> /dev/null
-rwx----- 1 kali kali 64 Oct 23 02:29 2 -> /dev/null
-rwx----- 1 kali kali 64 Oct 23 02:29 3 -> 'socket:[10617]'
-rwx----- 1 kali kali 64 Oct 23 02:29 4 -> 'socket:[10619]'

```

```
(kali㉿kali)-[~]  
$ sudo kill 1387  
  
(kali㉿kali)-[~]  
$ sudo rm -f $(readlink -f /proc/1387/exe)
```

```
(kali㉿kali)-[~]  
$ sudo apt install clamav -y  
sudo clamscan -r / --bell -i  
  
Installing:  
clamav  
  
Installing dependencies:  
clamav-base clamav-freshclam libclamav12 libmspack0t64  
  
Suggested packages:  
libclamunrar clamav-doc libclamunrar11  
  
Summary:  
Upgrading: 0, Installing: 5, Removing: 0, Not Upgrading: 1348  
Download size: 15.2 MB  
Space needed: 68.3 MB / 57.1 GB available  
  
Get:1 http://http.kali.org/kali kali-rolling/main amd64 clamav-base all 1.4.3+dfsg-1 [100 kB]  
Get:2 http://http.kali.org/kali kali-rolling/main amd64 libmspack0t64 amd64 0.11-1.1+b1 [53.0 kB]  
Get:3 http://http.kali.org/kali kali-rolling/main amd64 libclamav12 amd64 1.4.3+dfsg-1+b1 [7,765 kB]  
Get:4 http://http.kali.org/kali kali-rolling/main amd64 clamav-freshclam amd64 1.4.3+dfsg-1+b1 [161 kB]  
Get:5 http://http.kali.org/kali kali-rolling/main amd64 clamav amd64 1.4.3+dfsg-1+b1 [7,077 kB]  
Fetched 15.2 MB in 16s (954 kB/s)  
Preconfiguring packages ...  
Selecting previously unselected package clamav-base.  
(Reading database ... 431156 files and directories currently installed.)  
Preparing to unpack .../clamav-base_1.4.3+dfsg-1_all.deb ...  
Unpacking clamav-base (1.4.3+dfsg-1) ...  
Selecting previously unselected package libmspack0t64:amd64.  
Preparing to unpack .../libmspack0t64_0.11-1.1+b1_amd64.deb ...  
Unpacking libmspack0t64:amd64 (0.11-1.1+b1) ...  
Selecting previously unselected package libclamav12:amd64.  
Preparing to unpack .../libclamav12_1.4.3+dfsg-1+b1_amd64.deb ...  
Unpacking libclamav12:amd64 (1.4.3+dfsg-1+b1) ...  
Selecting previously unselected package clamav-freshclam.  
Preparing to unpack .../clamav-freshclam_1.4.3+dfsg-1+b1_amd64.deb ...  
Unpacking clamav-freshclam (1.4.3+dfsg-1+b1) ...  
Selecting previously unselected package clamav.  
Preparing to unpack .../clamav_1.4.3+dfsg-1+b1_amd64.deb ...  
Unpacking clamav (1.4.3+dfsg-1+b1) ...  
Setting up libmspack0t64:amd64 (0.11-1.1+b1) ...  
Setting up libclamav12:amd64 (1.4.3+dfsg-1+b1) ...  
Setting up clamav-base (1.4.3+dfsg-1) ...  
add: 'clamav': no such user  
Setting up clamav-freshclam (1.4.3+dfsg-1+b1) ...  
update-rc.d: We have no instructions for the clamav-freshclam init script.  
update-rc.d: It looks like a non-network service, we enable it.
```



```

update-rc.d: We have no instructions for the clamav-freshclam init script.
update-rc.d: It looks like a non-network service, we enable it.
Setting up clamav (1.4.3+dfsg-1+b1) ...
Processing triggers for libc-bin (2.41-6) ...
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.2.7) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
LibClamAV Error: cli_loaddbdir: No supported database files found in /var/lib/clamav
ERROR: Can't open file or directory

----- SCAN SUMMARY -----
Known viruses: 0
Engine version: 1.4.3
Scanned directories: 0
Scanned files: 0
Infected files: 0
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 0.005 sec (0 m 0 s)
Start Date: 2025:10:23 02:45:13
End Date: 2025:10:23 02:45:13

```

RESULT:

```

----- SCAN SUMMARY -----
Known viruses: 0
Engine version: 1.4.3
Scanned directories: 0
Scanned files: 0
Infected files: 0
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 0.005 sec (0 m 0 s)
Start Date: 2025:10:23 02:45:13
End Date: 2025:10:23 02:45:13

```

```

-(kali@kali)-[~]
$ ps -p 1387 -o pid,user,cmd,%cpu,%mem,etime

  PID USER      CMD                                %CPU %MEM    ELAPSED
  1387 kali      xcapse -e Super_L Control_L      0.0  0.0    01:46:39

```

