

The first thing I did was to export all the objects, but nothing. Then, I looked through the strings :

```
strings -n 7 mule.pcapng > file.txt
```

And at some point, I found this list of processes :

	USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND
root	1	0.0	0.0	24876	14384	?	Ss	10:08	0:06	/sbin/init	splash
root	2	0.0	0.0	0	0	?	S	10:08	0:00	[kthreadd]	
root	3	0.0	0.0	0	0	?	S	10:08	0:00	[pool_workqueue_release]	
root	4	0.0	0.0	0	0	?	I<	10:08	0:00	[kworker/R-rcu_gp]	
root	5	0.0	0.0	0	0	?	I<	10:08	0:00	[kworker/R-sync_wq]	
.											
.											
.											

And it was huge! The first thing I reminded of was Q3 : Ce comanda a fost executata pe serverul de C2, pentru a exfiltra date? (Points: 48) **Formatul raspunsului este: xx.** It was **ps**, the command used to list the processes on Linux.

Now, we have to look after the malware. I filtered the strings because I wanted to see all the processes from **darius**, the used found in the packets :

```
strings file.txt | grep darius > darius.txt
```

For the malware, it was pretty hard to find. I got an idea : I searched for the malware file thanks to the title of the challenge. After multiple failed tries, I used :

```
strings darius.txt | grep lue
```

And the output was :

darius	177717	0.0	0.0	2684	1384	pts/2	S+	12:55	0:00	./mblue-lockerV1
darius	177717	0.0	0.0	2684	1384	pts/2	S+	12:55	0:00	./mblue-lockerV1
darius	177717	0.0	0.0	2684	1384	pts/2	S+	12:55	0:00	./mblue-lockerV1
darius	177717	0.0	0.0	2684	1384	pts/2	S+	12:55	0:00	./mblue-lockerV1
.										
.										
.										

In the title, you can get hits about the challenge

Q1. Sa se identifice numele malware-ului care ruleaza pe statia compromisa. (Points: 100)Formatul raspunsului este de forma: cuvant-cuvant. : **mblue-lockerV1**

For the rest second question, I searched **mblue-lockerV1** with Wireshark and I found the IP and the Port :

Packet bytes		String		mblue-lockerV1		
Options:		Narrow & Wide		<input checked="" type="checkbox"/> Case sensitive	<input checked="" type="checkbox"/> Backwards	<input checked="" type="checkbox"/> Multiple occurrences
Time	Source	Destination	Protocol	Length Info		
532	66.254954676	192.168.1.229	86.124.78.162	WireGu...	140	Transport Data, receiver=0x7B1D
533	66.825657812	10.0.212.4	3.68.63.139	TLSv1.2	124	Application Data
534	66.825835024	192.168.1.229	86.124.78.162	WireGu...	188	Transport Data, receiver=0x7B1D
535	66.907826983	86.124.78.162	192.168.1.229	WireGu...	140	Transport Data, receiver=0x7369
536	66.907912303	3.68.63.139	10.0.212.4	TCP	68	443 → 39806 [ACK] Seq=1644 Ack=
537	67.645794244	127.0.0.1	127.0.0.1	TCP	68	[TCP Keep-Alive] 34656 → 9001 [
538	67.645815190	127.0.0.1	127.0.0.1	TCP	68	[TCP ZeroWindow] 9001 → 34656 [
539	68.307317504	127.0.0.1	127.0.0.1	TCP	68	[TCP Window Update] 9001 → 3465
540	68.307383947	127.0.0.1	127.0.0.1	TCP	47492	34656 → 9001 [ACK] Seq=161922 A
541	68.307395328	127.0.0.1	127.0.0.1	TCP	47492	[TCP Window Full] 34656 → 9001
542	68.327899871	127.0.0.1	127.0.0.1	TCP	47492	[TCP Window Full] [TCP Retransm
543	68.335129985	127.0.0.1	127.0.0.1	TCP	80	9001 → 34656 [ACK] Seq=27 Ack=2
544	68.335201581	127.0.0.1	127.0.0.1	TCP	47492	34656 → 9001 [ACK] Seq=256770 A
545	68.335211953	127.0.0.1	127.0.0.1	TCP	47492	[TCP Window Full] 34656 → 9001
546	68.335228283	127.0.0.1	127.0.0.1	TCP	68	9001 → 34656 [ACK] Seq=27 Ack=3
547	68.335320392	127.0.0.1	127.0.0.1	TCP	65551	34656 → 9001 [ACK] Seq=351618 A
548	68.335338550	127.0.0.1	127.0.0.1	TCP	65551	34656 → 9001 [PSH, ACK] Seq=417
549	68.335354990	127.0.0.1	127.0.0.1	TCP	65551	34656 → 9001 [ACK] Seq=482584 A
550	68.335370767	127.0.0.1	127.0.0.1	TCP	65551	34656 → 9001 [PSH, ACK] Seq=548
551	68.335377492	127.0.0.1	127.0.0.1	TCP	68	9001 → 34656 [ACK] Seq=27 Ack=4
552	68.335434723	127.0.0.1	127.0.0.1	TCP	68	9001 → 34656 [ACK] Seq=27 Ack=4
553	68.335510117	127.0.0.1	127.0.0.1	TCP	68	9001 → 34656 [ACK] Seq=27 Ack=5
554	68.335515290	127.0.0.1	127.0.0.1	TCP	68	9001 → 34656 [ACK] Seq=27 Ack=6
555	68.335531080	127.0.0.1	127.0.0.1	TCP	65551	34656 → 9001 [ACK] Seq=613550 A
556	68.335549605	127.0.0.1	127.0.0.1	TCP	65551	34656 → 9001 [PSH, ACK] Seq=679
557	68.335562202	127.0.0.1	127.0.0.1	TCP	41985	34656 → 9001 [PSH, ACK] Seq=744
558	68.335578993	127.0.0.1	127.0.0.1	TCP	65551	34656 → 9001 [ACK] Seq=786433 A
559	68.335589647	127.0.0.1	127.0.0.1	TCP	32889	34656 → 9001 [PSH, ACK] Seq=851

Q2. Identifică IP si port pentru serverul de C2. (Points: 60) Formatul raspunsului este:

IP:PORT : 127.0.0.1:9001