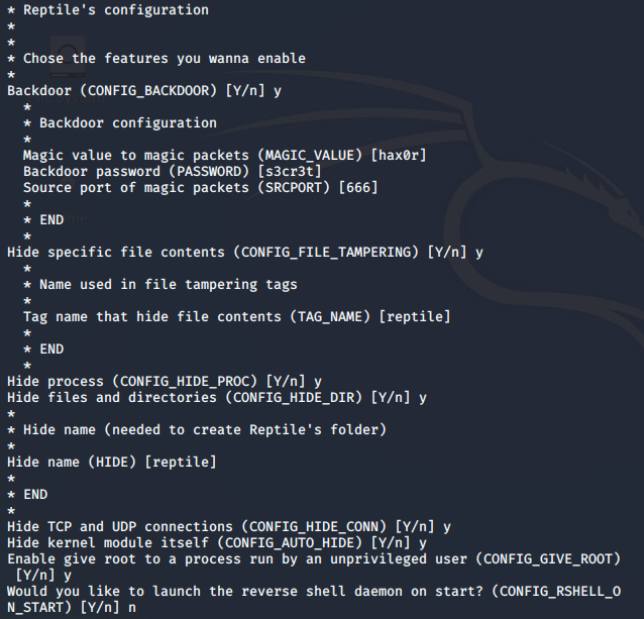
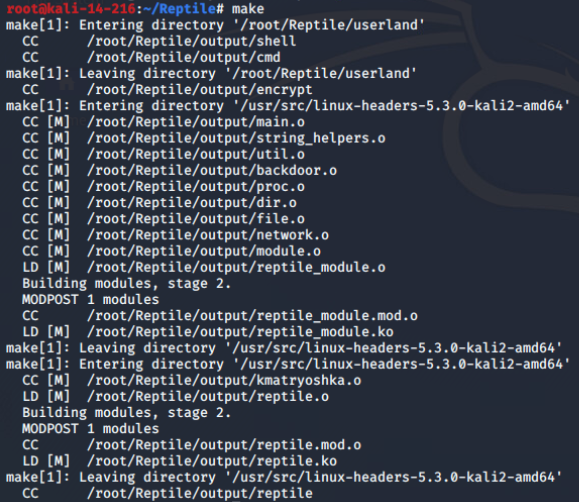
**ATT&CK: Persistence-1).rootkit**

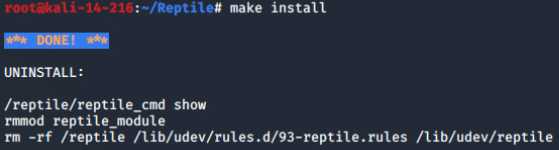
**LKM Linux rootkit:Reptile https://github.com/f0rb1dd3n/Reptile**

目标机器:

apt install build-essential libncurses-dev linux-headers-$(uname -r) && make config







Reptile's Backdoor

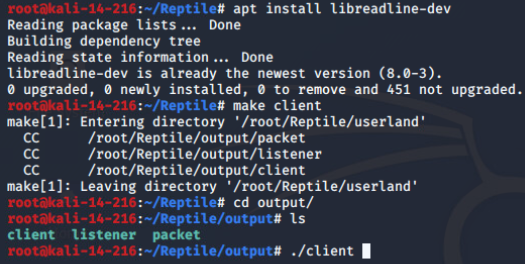
The backdoor is a reverse shell triggered by a magic packet sent via TCP, UDP or ICMP protocol. It will call a binary in userland which will connect, trigger Reptile's hidding commands and provide you a reverse shell with some nice features like:

File uploader and downloader

Possibility to set a delay to connect back in a period of time (in seconds)

Full TTY shell (like ssh)

控制端:





There are another two binaries: listener and packet. The client binary will handle listener and packet but you can use them separately if you want

shell

The shell is easy to use, when you got a connection just type help to see the commands.

It already hide its process and connection.

Its connection is encrypted

There is a file uploader and file downloader inside.

You can set a delay to receive a reverse connection every time you want.

If you run shell you will get a full TTY/PTY shell like ssh.



