Running a Rootkit and Generating Memory Dump

I downloaded the rootkit vlany to my Ubuntu VM from:

https://github.com/mempodippy/vlany

This is a rootkit targeting Linux operating systems.

It has the following features (taken from its github site)

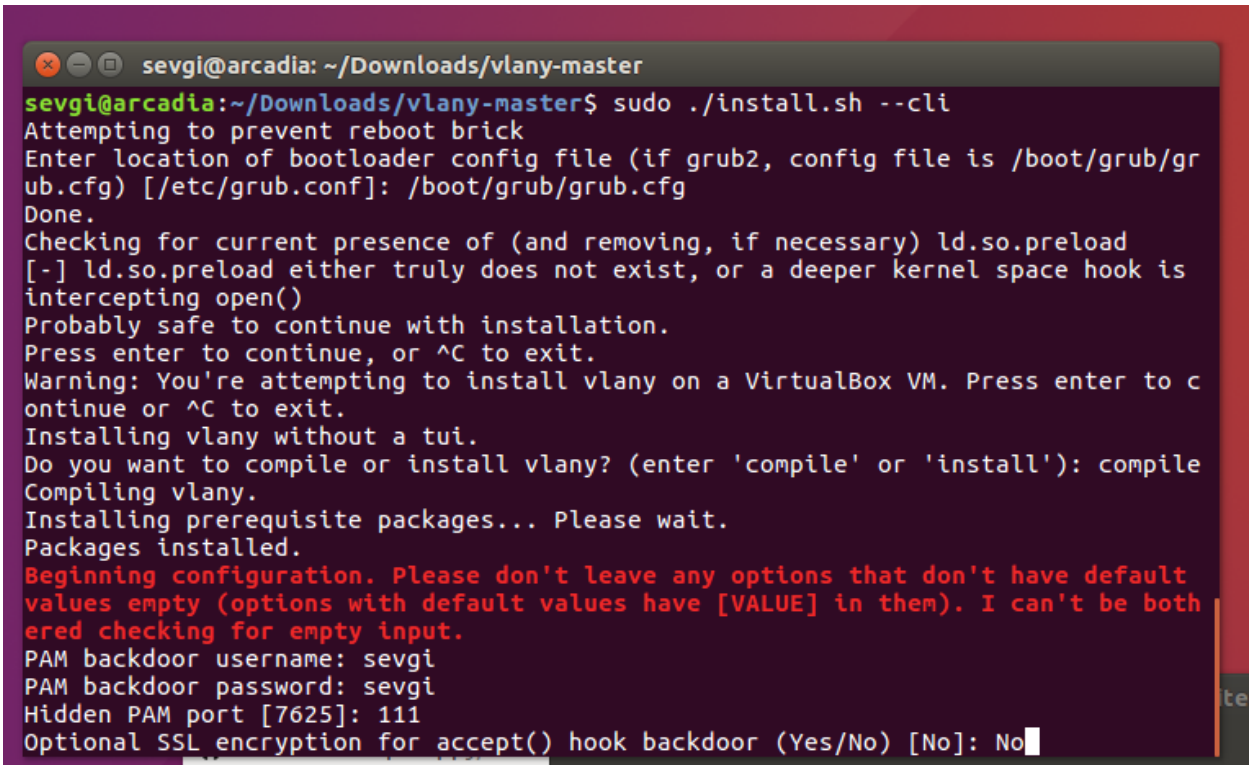
- Process hiding
- User hiding
- Network hiding
- LXC container
- Anti-Debug
- Anti-Forensics
- Persistent (re)installation & Anti-Detection
- Dynamic linker modifications
- Backdoors
    - accept() backdoor (derived from Jynx2)
    - PAM backdoor
        - PAM auth logger
    - snodew reverse shell backdoor
- vlany-exclusive commands

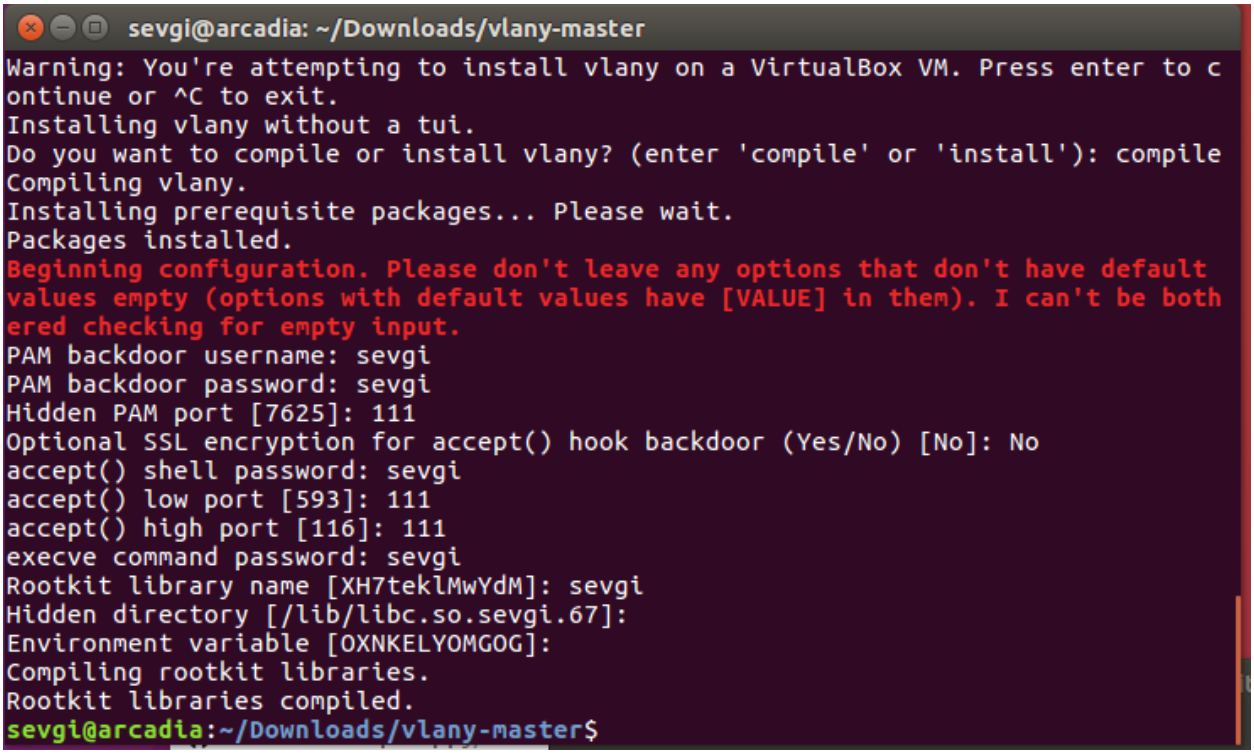
Running the rootkit:

I first unzip the document and run the rootkit with the command:

sudo ./install.sh –cli

Then as seen from the screenshots create a username and password. Then create hidden PAM ports.


sevgi@arcadia: ~/Downloads/vlany-master
sevgi@arcadia:~/Downloads/vlany-master$ sudo ./install.sh --cli
Attempting to prevent reboot brick
Enter location of bootloader config file (if grub2, config file is /boot/grub/gr
ub.cfg) [/etc/grub.conf]: /boot/grub/grub.cfg
Done.
Checking for current presence of (and removing, if necessary) ld.so.preload
[-] ld.so.preload either truly does not exist, or a deeper kernel space hook is
intercepting open()
Probably safe to continue with installation.
Press enter to continue, or ^C to exit.
Warning: You're attempting to install vlany on a VirtualBox VM. Press enter to c
ontinue or ^C to exit.
Installing vlany without a tui.
Do you want to compile or install vlany? (enter 'compile' or 'install'): compile
Compiling vlany.
Installing prerequisite packages... Please wait.
Packages installed.
Beginning configuration. Please don't leave any options that don't have default
values empty (options with default values have [VALUE] in them). I can't be both
ered checking for empty input.
PAM backdoor username: sevgi
PAM backdoor password: sevgi
Hidden PAM port [7625]: 111
Optional SSL encryption for accept() hook backdoor (Yes/No) [No]: No


sevgi@arcadia: ~/Downloads/vlany-master
Warning: You're attempting to install vlany on a VirtualBox VM. Press enter to c
ontinue or ^C to exit.
Installing vlany without a tui.
Do you want to compile or install vlany? (enter 'compile' or 'install'): compile
Compiling vlany.
Installing prerequisite packages... Please wait.
Packages installed.
Beginning configuration. Please don't leave any options that don't have default
values empty (options with default values have [VALUE] in them). I can't be both
ered checking for empty input.
PAM backdoor username: sevgi
PAM backdoor password: sevgi
Hidden PAM port [7625]: 111
Optional SSL encryption for accept() hook backdoor (Yes/No) [No]: No
accept() shell password: sevgi
accept() low port [593]: 111
accept() high port [116]: 111
execve command password: sevgi
Rootkit library name [XH7teklMwYdM]: sevgi
Hidden directory [/lib/libc.so.sevgi.67]:
Environment variable [OXNKELYOMGOG]:
Compiling rootkit libraries.
Rootkit libraries compiled.
sevgi@arcadia:~/Downloads/vlany-master$

Generating Memory Dump:

To get the memory dump I used the program LiME – Linux Memory Extractor.

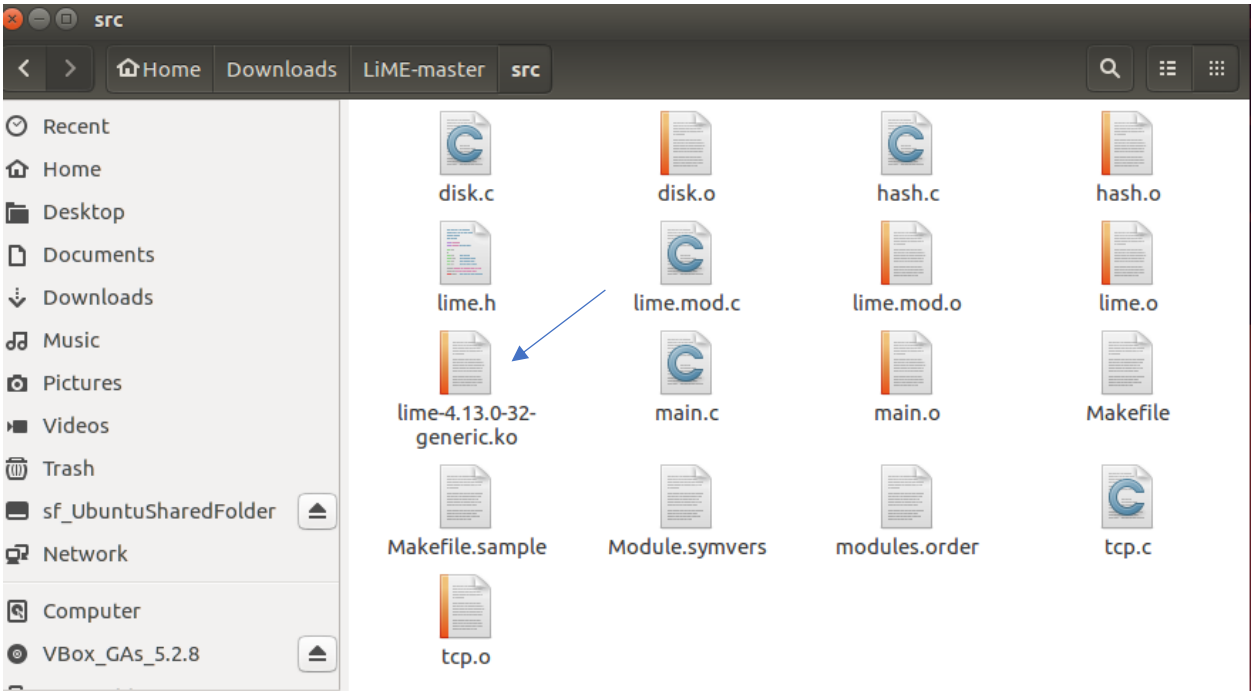
I downloaded the program from:

https://github.com/504ensicsLabs/LiME

I extracted the file and move my current directory to Donloads/Lime-master/src to run the make command.

```
sevgi@arcadia:~$ cd Downloads/LiME-master/src make
sevgi@arcadia:~/Downloads/LiME-master/src$ make
make -C /lib/modules/4.13.0-32-generic/build M="/home/sevgi/Downloads/LiME-maste
r/src" modules
make[1]: Entering directory '/usr/src/linux-headers-4.13.0-32-generic'
  CC [M]  /home/sevgi/Downloads/LiME-master/src/tcp.o
  CC [M]  /home/sevgi/Downloads/LiME-master/src/disk.o
  CC [M]  /home/sevgi/Downloads/LiME-master/src/main.o
  CC [M]  /home/sevgi/Downloads/LiME-master/src/hash.o
  LD [M]  /home/sevgi/Downloads/LiME-master/src/lime.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC      /home/sevgi/Downloads/LiME-master/src/lime.mod.o
  LD [M]  /home/sevgi/Downloads/LiME-master/src/lime.ko
make[1]: Leaving directory '/usr/src/linux-headers-4.13.0-32-generic'
strip --strip-unneeded lime.ko
mv lime.ko lime-4.13.0-32-generic.ko
```

The make command created .ko file under the same directory.



To get the .vmem file I executed the following command:

```
sevgi@arcadia:~/Downloads/LiME-master/src$ sudo insmod lime-4.13.0-32-generic.ko
 "path=/media/myDump.vmem format=lime"
sevgi@arcadia:~/Downloads/LiME-master/src$
```