Comandos VPS:

```
labsec@labsec:~$ history
    1  su -
    2  su -l
    3  su -
    4  exit
    5  su -
    6  exit
    7  su -
    8  clear
    9  ls
   10  clear
   11  exit
   12  clear
   13  ls
   14  clear
   15  ls
   16  clear
   17  exit
   18  clear
   19  sudo su
   20  su -
   21  clear
   22  ls
   23  clear
   24  ls
   25  clear
   26  ls
   27  cd /
   28  ls
   29  cd var/
   30  cls
   31  clear
   32  ls
   33  clear
   34  ls
   35  cd www/
   36  ls
   37  clear
   38  cd html/
   39  ls
   40  clear
   41  cd /etc/host
   42  cat /etc/host
   43  cd /etc/
   44  ks
   45  ls
```

```
46  clear
47  cd apache2/
48  ls
49  cat apache2.conf
50  clear
51  exit
52  clear
53  su -
54  exit
55  clear
56  su -
57  clear
58  ls
59  cd scapy/
60  ls
61  vi setup.py
62  cd ..
63  su -
64  clear
65  cls
66  clear
67  cd /etc/ansible/
68  clear
69  vi /etc/ansible/
70  vi /etc/ansible/hosts
71  clear
72  ls
73  clear
74  ls
75  clear
76  ls
77  clear
78  ls
79  clear
80  ls
81  clear
82  ls
83  cd /
84  ls
85  cd ~
86  ls
87  cd scapy/
88  ls
89  cd ..
90  ls
91  clear
92  su
93  labsec
```

```
  94  clear
  95  su -
  96  cd /etc/ansible/
  97  ls
  98  clear
  99  systemctl status ssh
 100  clear
 101  ls
 102  clear
 103  ansible-playbook playbook_improve_labsec.yml
 104  clear
 105  ls
 106  clear
 107  systecmtl status ansible
 108  clear
 109  ansible-playbook playbook_improve_labsec.yml
 110  nano hosts
 111  clear
 112  ansible-playbook playbook_improve_labsec.yml
 113  ls
 114  sudo ansible-playbook playbook_improve_labsec.yml
 115  history | grep NOPASS
 116  sudo su
 117  clear
 118  su -
 119  clear
 120  ansible-playbook playbook_improve_labsec.yml
 121  sudo ansible-playbook playbook_improve_labsec.yml
 122  clear
 123  ls
 124  sudo chown -R labsec:labsec /etc/ansible/
 125  sudo ansible-playbook playbook_improve_labsec.yml
 126  ansible-playbook playbook_improve_labsec.yml
 127  hosts
 128  cat hosts
 129  clear
 130  ls
 131  clear
 132  init 0
 133  clear
 134  ls
 135  clear
 136  history
 137  clear
 138  history
labsec@labsec:~$ sudo su
root@labsec:/home/labsec# history
   1  ifconfig
```

```
    2  apt update
    3  apt install net-tools
    4  ifconfig .
    5  ifconfig
    6  dhclient
    7  ifconfig
    8  ifconfig
    9  dhclient
   10  dhclient ennp0s3
   11  dhclient ennpos3
   12  dhclient ennp0s3
   13  dhclient enp0s3
   14  ifconfig
   15  init 6
   16  apt update -y
   17  apt upgrade -y
   18  apt install nmap -y
   19  apt install build-essential manpages-dev -y
   20  apt install net-tools -y
   21  apt install vim -y
   22  apt install hping3 -y
   23  # Analisador de pacotes de rede
   24  apt install tcpdump -y
   25  # Trace das rotas de um pacote
   26  apt install traceroute -y
   27  apt install tor torbrowser-launcher  -y
   28  apt install tor torbrowser
   29  apt install tor
   30  apt install proxychains -y
   31  apt install -y git
   32  # Software registry NPM
   33  apt install npm
   34  apt -y install ansible-core
   35  mkdir /etc/ansible
   36  apt -y install apache2
   37  apt -y install sudo
   38  cd ~labsec
   39  cd -
   40  ls
   41  cd -
   42  curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/c
onfig/templates/metasploit-framework-wrappers/msfupdate.erb > msfinstall
   43  apt install curl -y
   44  curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/c
onfig/templates/metasploit-framework-wrappers/msfupdate.erb > msfinstall
   45  ls
   46  chmod +x msfinstall
   47  ./msfinstall
```

```
  48  msfconsole
  49  apt -y  remove docker docker-engine docker.io containerd runc
  50  apt -y install   ca-certificates         curl     gnupg
  51  mkdir -m 0755 -p /etc/apt/keyrings
  52  curl -fsSL https://download.docker.com/linux/debian/gpg |  gpg --dearmor
-o /etc/apt/keyrings/docker.gpg
  53  echo   "deb [arch="$(dpkg --print-architecture)" signed-by=/etc/apt/keyri
ngs/docker.gpg] https://download.docker.com/linux/debian \
  54    "$(. /etc/os-release && echo "$VERSION_CODENAME")" stable" |    tee /et
c/apt/sources.list.d/docker.list > /dev/null
  55  apt update
  56  apt install -y docker-ce docker-ce-cli containerd.io docker-buildx-plugin
docker-compose-plugin
  57   docker run hello-world
  58  docker ls
  59  docker image ls
  60  docker image rm hello-world:latest
  61  docker image ls
  62  docker image rm hello
  63  docker image ls
  64  docker image rm d2
  65  docker image ls
  66  docker image rm d2c94e258dcb
  67  docker container ls
  68  docker container prune
  69  docker image rm d2c94e258dcb
  70  docker image ls
  71  apt install python3-pip -y
  72  pip3 install scapy -y
  73  pip3 install scapy
  74  pip3 install scapy
  75  pip install scapy
  76  apt install scapy -y
  77  python
  78  python3.11
  79  pip3 install docker-compose
  80  apt install docker-compose
  81  apt install --user docker-compose
  82  docker pull quay.io/keycloak/keycloak
  83  docker image ls
  84  git clone https://github.com/anders94/blockchain-demo.git
  85  apt install python3.11-venv -y
  86  apt install unzip
  87  curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscl
iv2.zip"
  88  unzip awscliv2.zip
  89  ./aws/install
  90  aws --version
```

```
   91  apt-get update && sudo apt-get install -y gnupg software-properties-commo
n
   92  wget -O- https://apt.releases.hashicorp.com/gpg | gpg --dearmor | tee /us
r/share/keyrings/hashicorp-archive-keyring.gpg
   93  exit
   94  ifconfig
   95  ping 8.8.8.8
   96  ifconfig
   97  ls
   98  cd ~labsec
   99  ls
  100  ls
  101  sed -i "s\ res.render('index')\ res.render('hash')\g"  blockchain-demo/ro
utes/index.js
  102  cd blockchain-demo/
  103  ls
  104  ls
  105  cd ..
  106  apt-get install -y tftpd telnetd rsh-server
  107  apt-get install -y tftpd-hpa telnetd rsh-server
  108  apt install unattended-upgrades apt-listchanges bsd-mailx
  109  apt install selinux-basics selinux-policy-default -y
  110  ls
  111  curl https://github.com/sqlmapproject/sqlmap/tarball/master
  112  ls
  113  git clone https://github.com/sqlmapproject/sqlmap/tarball/master
  114  ls
  115  git clone --depth 1 https://github.com/sqlmapproject/sqlmap.git sqlmap-de
v
  116  ls
  117  cd sqlmap-dev/
  118  ls
  119  cd ..
  120  ls
  121  python3
  122  pip install scapy
  123  pip install https://github.com/secdev/scapy/archive/refs/heads/master.zip
  124  pip3 install https://github.com/secdev/scapy/archive/refs/heads/master.zi
p
  125  pipx install https://github.com/secdev/scapy/archive/refs/heads/master.zi
p
  126   git clone https://github.com/secdev/scapy.git
  127   cd scapy
  128  pip install .
  129  ls
  130  pip3 install .
  131  pip3 install . --break-system-packages.
  132  init 6
```

```
133  cd ~labasec
134  cd labsec
135  cd /home/labsec/
136  ls
137  cd basicHttpServer/
138  ls
139  python3 clientHttp.py
140  vi clientHttp.py
141  vi clientHttp.py
142  python3 clientHttp.py
143  vi clientHttp.py
144  python3 clientHttp.py
145  vi clientHttp.py
146  cat clientHttp.py
147  ls
148  vi .env
149  python3 clientHttp.py
150  vi clientHttp.py
151  python3 clientHttp.py
152  vi clientHttp.py
153  python3 clientHttp.py
154  vi clientHttp.py
155  python3 clientHttp.py
156  vi clientHttp.py
157  python3 clientHttp.py
158  vi clientHttp.py
159  python3 clientHttp.py
160  cat clientHttp.py
161  vi clientHttp.py
162  python3 clientHttp.py
163  vi serverHttp.py
164  python3 clientHttp.py
165  exit
166  scapy
167  ext
168  exit
169  python3
170  pip install scapy
171  scapy
172  ls
173  cd ~labsec
174  ls
175  mkdir basicHttpServer
176  cd basicHttpServer/
177  ls
178  vi http.py
179  vi http.py
180  python3 http.py
```

```
181  vi http.py
182  python3 http.py
183  vi http.py
184  python3 http.py
185  vi http.py
186  python3 http.py
187  vi http.py
188  ls
189  mv http.py httpServer.py
190  ls
191  vi clientHttp.py
192  mv httpServer.py serverHttp.py
193  ls
194  vi clientHttp.py
195  python3 serverHttp.py
196  vi clientHttp.py
197  python3 serverHttp.py
198  vi serverHttp.py
199  python3 serverHttp.py
200  python3 serverHttp.py
201  ls
202  cd ..
203  ls
204  mv basicHttpServer/ basicTCPConn
205  ls
206  cd /home/labsec/basicTCPConn/
207  vi .env
208  ls
209  mv clientHttp.py clientTCP.py
210  mv serverHttp.py serverTCP.py
211  vi .env
212  cat .env
213  iptables -L
214  iptables -L -t nat
215  ls
216  cd ..
217  ls
218  rm awscliv2.zip
219  ls
220  ls
221  cd aws/
222  ls
223  cd ..
224  aws --version
225  rm aws/ -rf
226  aws --version
227  ls
228  ls
```

```
229  init 0
230  ifconfig
231  clear
232  ls
233  clear
234  ls
235  init 0
236  clear
237  su labsec
238  ifconfig
239  dhclient
240  ifconfig
241  clear
242  ifconfig
243  exit
244  init 0
245  ifconfig
246  ifconfig
247  dhclient
248  ifconfig
249  clear
250  ls
251  sudo apt-get update && apt-get upgrade
252  clear
253  cls
254  clear
255  ls
256  cd ~
257  ls
258  cd /
259  ls
260  exit
261  ls -al
262  ls -a
263  clear
264  ls
265  ls -a
266  ls -al
267  ls
268  chmod 760 leo.py
269  ls
270  ls -al
271  rm leo.py
272  clear
273  nano LucasZoser.txt
274  clear
275  chmod 760 LucasZoser.txt
276  ls -al
```

```
277  [200~ apt install -y selinux-basics selinux-policy-default
278  apt install -y selinux-basics selinux-policy-default
279  sestatus
280  selinux-activate
281  sestatus
282  clear
283  sestatus
284  cls
285  vi /etc/selinux/config
286  getenforce
287  clear
288  cd /etc/ansible
289  cd /etc/ansible/
290  cls
291  clear
292  mkdir /etc/ansible
293  ls
294  cd /etc/ansible/
295  cls
296  clear
297  ls
298  vi /etc/ansible/hosts
299  pwd
300  ls
301  vi /etc/ansible/hosts
302  cat hosts
303  exit
304  clear
305  ifconfig
306  ls
307  clear
308  ifconfig
309  dhclient
310  ifconfig
311  dhclient
312  ifconfig
313  clear
314  exit
315  init 0
316  init0
317  clear
318  vi leo.txt
319  cat leo.txt
320  nano leo.txt
321  mv leo.txt leo.py
322  clear
323  python3 leo.py
324  ls
```

```
325  nano leo.py
326  clear
327  python3 leo.py
328  clear
329  clear
330  python3 leo.py
331  nano leo.py
332  clear
333  python3 leo.py
334  clear
335  python3 leo.py
336  cls
337  clear
338  nano leo.py
339  clear
340  python3 leo.py
341  clear
342  history | grep leo
343  clear
344  ls
345  clear
346  vi leo.py
347  clear
348  python3 leo.py
349  vi leo.py
350  clear
351  python3 leo.py
352  clear
353  clear
354  nano leo.py
355  python3 leo.py
356  clear
357  nano leo.py
358  clear
359  dpkg --list
360  clear
361  telnet gmail.com 25
362  telnet gmail.com 587
363  clear
364  telnet box.zoser.me 25
365  clear
366  ls
367  clear
368  telnet localhost 25
369  clear
370  telnet localhost 25
371  clear
372  clear
```

```
373  hostname
374   apt-get --purge remove -y tftpd-hpa telnetd rsh-server
375  apt-get update && apt-get upgrade
376  clear
377  clear
378  ls
379  sl
380  clear
381  echo "labsec ALL=(ALL) NOPASSWD=ALL" > /etc/sudoers.d/labsec
382  chmod 440 /etc/sudoers.d/labsec
383  ls -al /etc/sudoers.d/labsec
384  sestatus
385  chage -l labsec
386  vi /etc/login.defs
387  nao /etc/login.defs
388  nano /etc/login.defs
389  chage -M 60 -m 7 -W 7 labsec
390  chage -M 90 -m 7 -W 7 labsec
391  CLEAR
392  clear
393  cat /etc/login.defs
394  clear
395  sudo nano /etc/login.defs
396  CLEAR
397  clear
398  cat /etc/login.defsclea
399  clear
400  ls
401  clear
402  cd /etc/ansible/
403  ls
404  cd hos
405  cat hosts
406  clear
407  ls
408  cd ..
409  ls
410  clear
411  cd ansible/
412  clear
413  nano playbook_improve_labsec.yaml
414  nano playbook_hardening.yml
415  ls
416  mv playbook_improve_labsec.yaml playbook_improve_labsec.yml
417  ls
418  clear
419  ls
420  clear
```

```
421  ls
422  clear
423  ls
424  nano hosts
425  ls
426  nano hosts
427  ls
428  clear
429  ls
430  clear
431  clear
432  chown -R labsec.labsec /etc/ansible/
433  chown -R labsec:labsec /etc/ansible/
434  exit
435  history | grep NOPASS
436  echo "labsec ALL=(ALL) NOPASSWD:ALL" > /etc/sudoers.d/labsec
437  clear
438  exit
439  clear
440  ls
441  ifconfig
442  dhclient
443  ifconfig
444  dhclient
445  claer
446  clear
447  ifconfig
448  exit
449  clear
450  cd /
451  ls
452  clear
453  cat ~/.ssh/known_hosts
454  ssh-keygen -t rsa
455  ssh-keygen -t rsa -b 2048
456  clear
457  ls
458  clear
459  cd /home/labsec/.ssh/
460  clear
461  ls
462  ls -al
463  clear
464  ls
465  clear
466  clear
467  exit
468  clear
```

```
469  cat /root/.ssh/id_rsa.pub
470  clear
471  ssh-keygen -t rsa -b 2048
472  clear
473  cat /root/.ssh/id_rsa.pub
474  clear
475  exit
476  clear
477  ifconfig
478  dhclient
479  ifconfig
480  clear
481  exit
482  clear
483  ls
484  init 0
485  history
```