

SSH Tunneling

Sometimes it can be that a target network is in another subnet and you are not able to access it because you are only connected to the one machine.

Example of TryHackMe Internal.

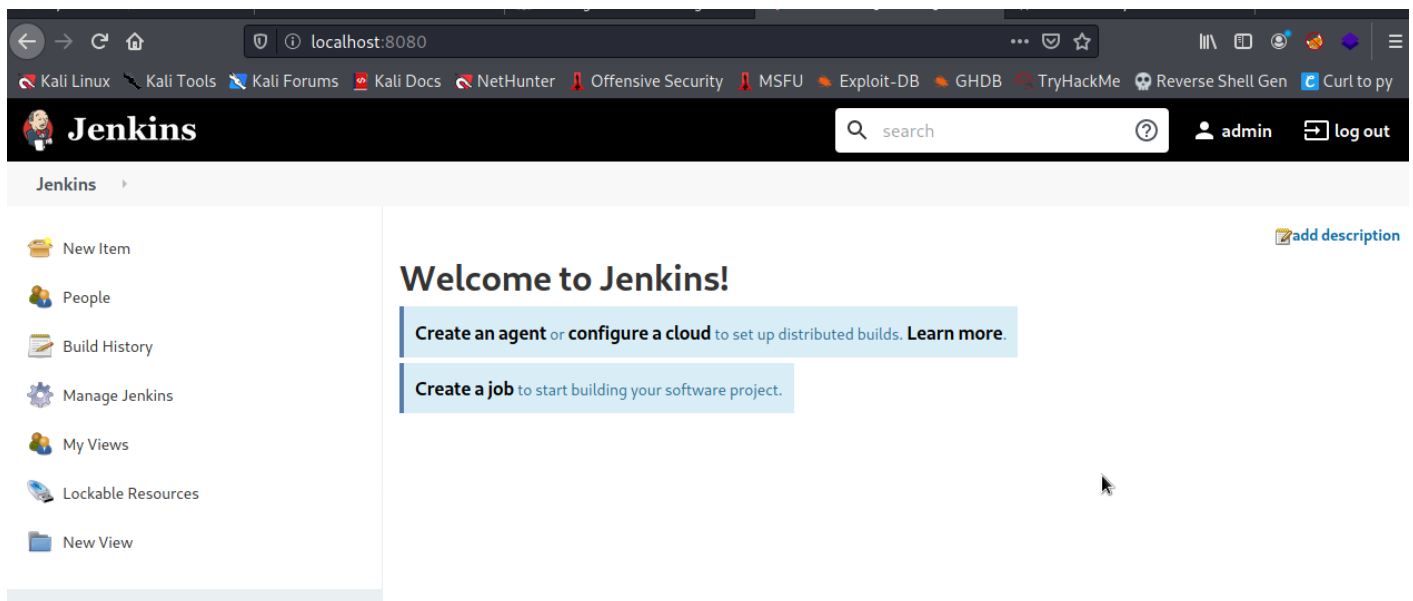
```
aubreanna@internal:~$ ls
jenkins.txt  snap  user.txt
aubreanna@internal:~$ cat jenkins.txt
Internal Jenkins service is running on 172.17.0.2:8080
```

There we see that Jenkins is running in a container on IP 172.17.0.2:8080
But as we are in the THM Network we won't be able to access the Jenkins server.

With SSH Tunneling we can "move" the content which is running on 172.17.0.2:8080 to our localhost:8080

```
ssh -L 8080:172.17.0.2:8080 username@10.10.10.10
```

As soon we done that we are able to see Jenkins on our localhost.



Revision #3

Created 9 July 2022 13:22:15 by Togoboi

Updated 10 July 2022 08:23:01 by Togoboi