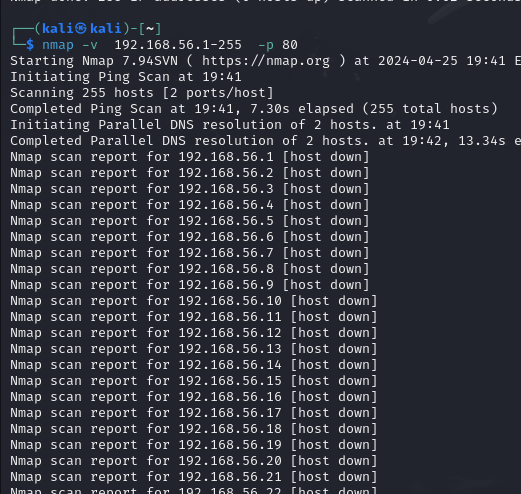
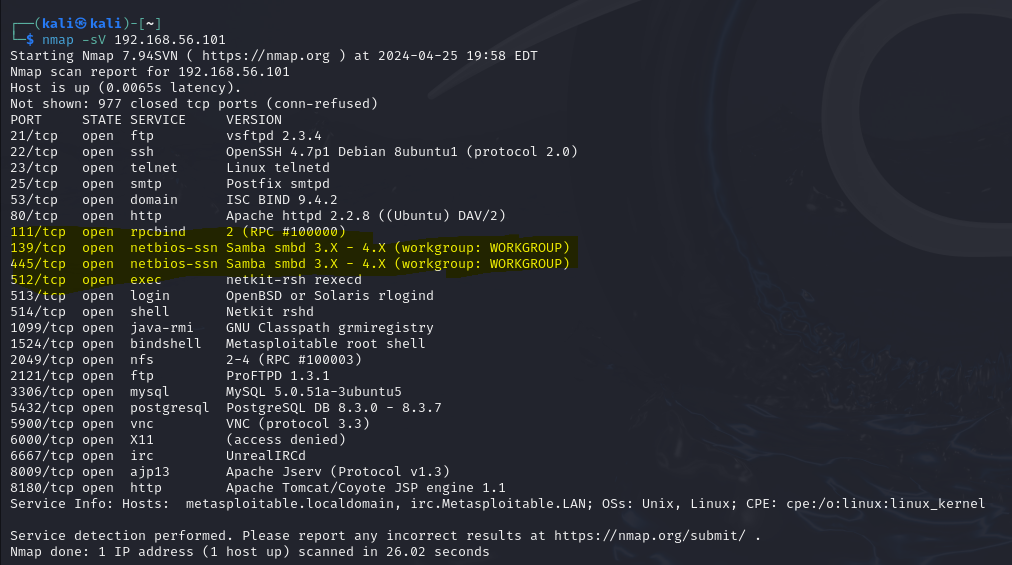
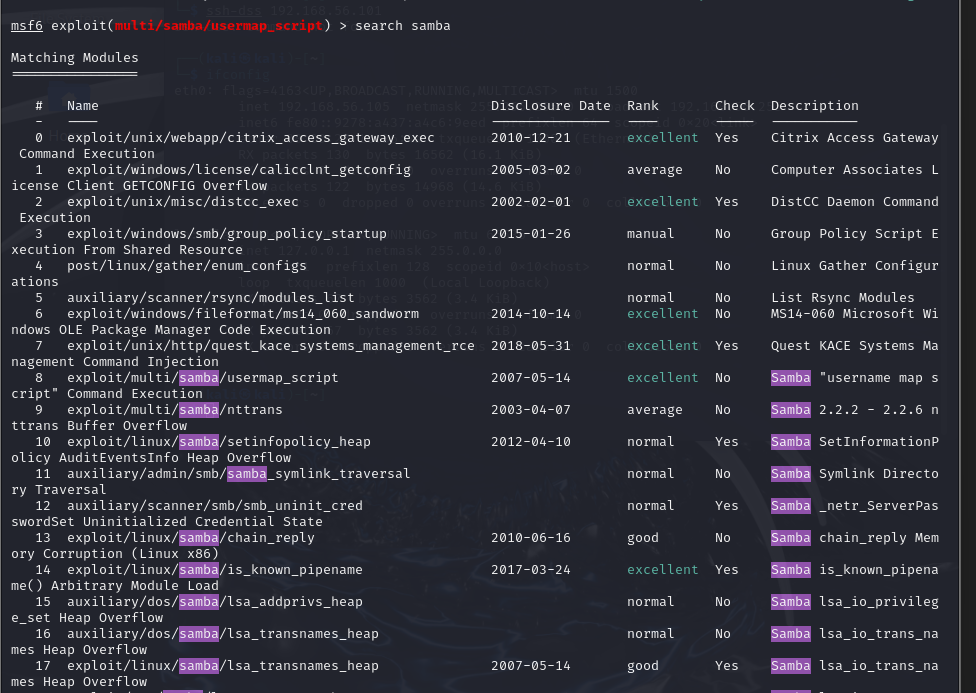
Discovering the different hosts on the same network using nmap:



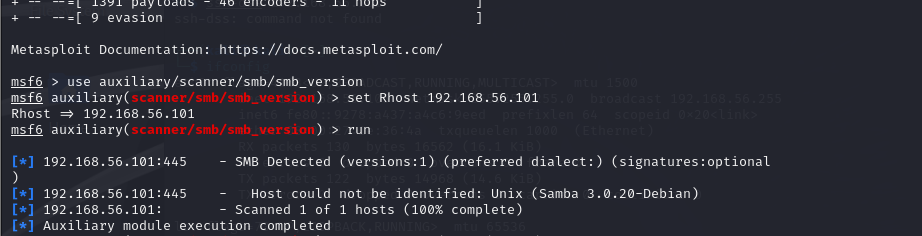
Finding services using nmap:



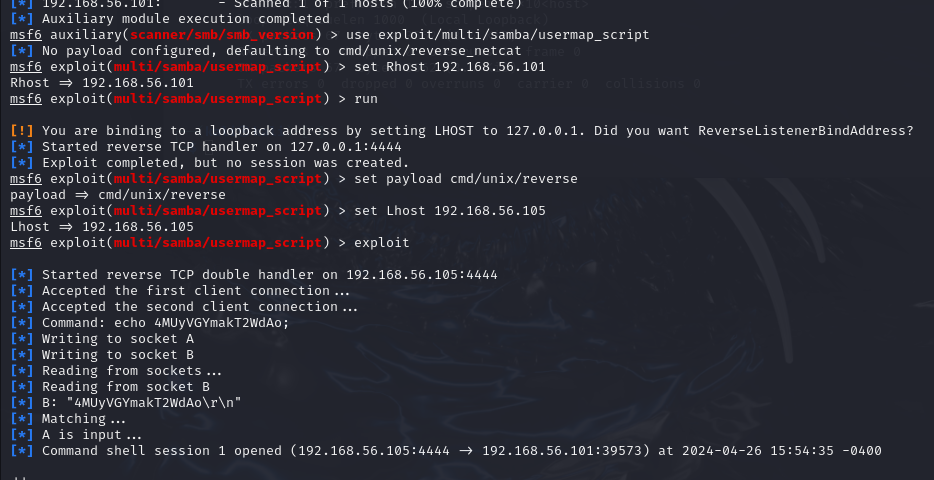
Using Metasploit to exploit and get access to metasploitable2:



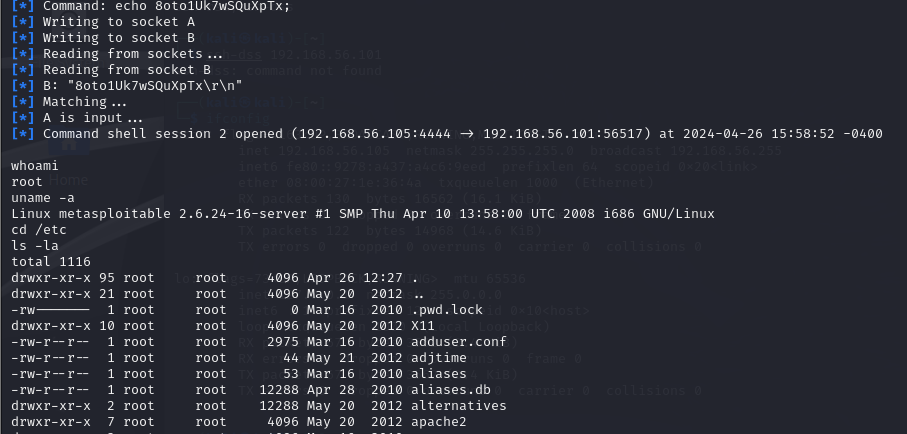
Used scanner module to get know the version of samba on metaspolit



After that used usermap\_script module with reverse command shell has a payload and run the exploit

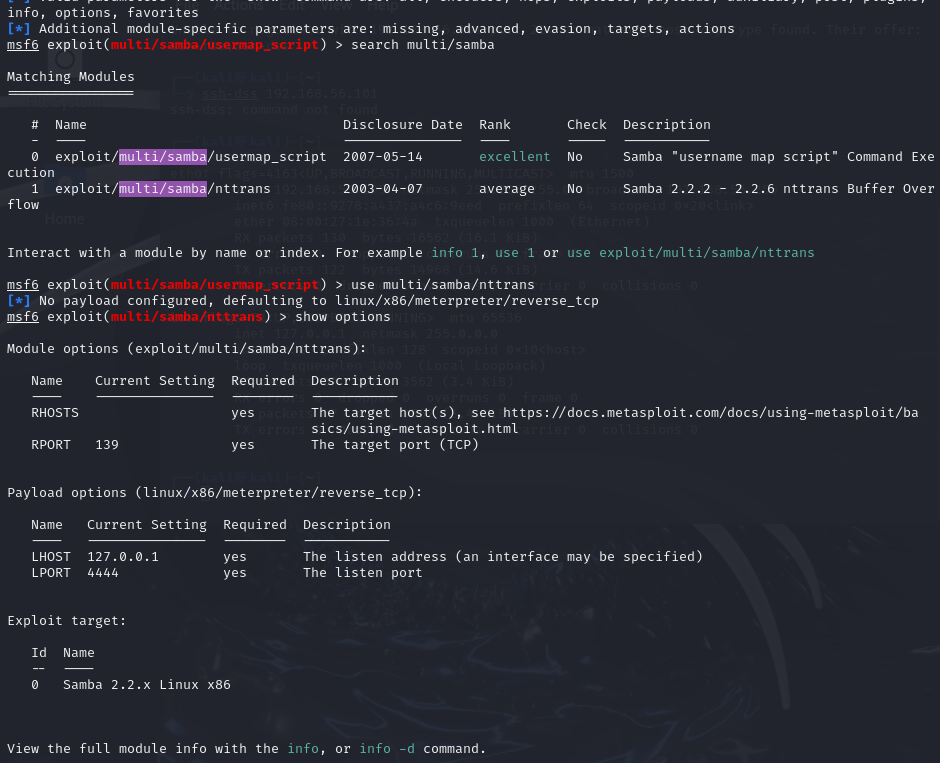


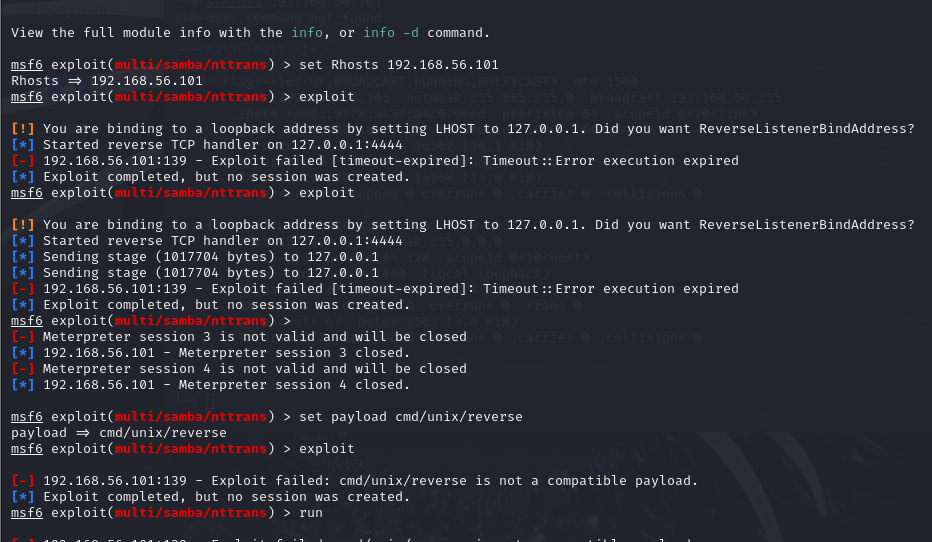
Has you can see we got the root access from it and has access to all the files in it.



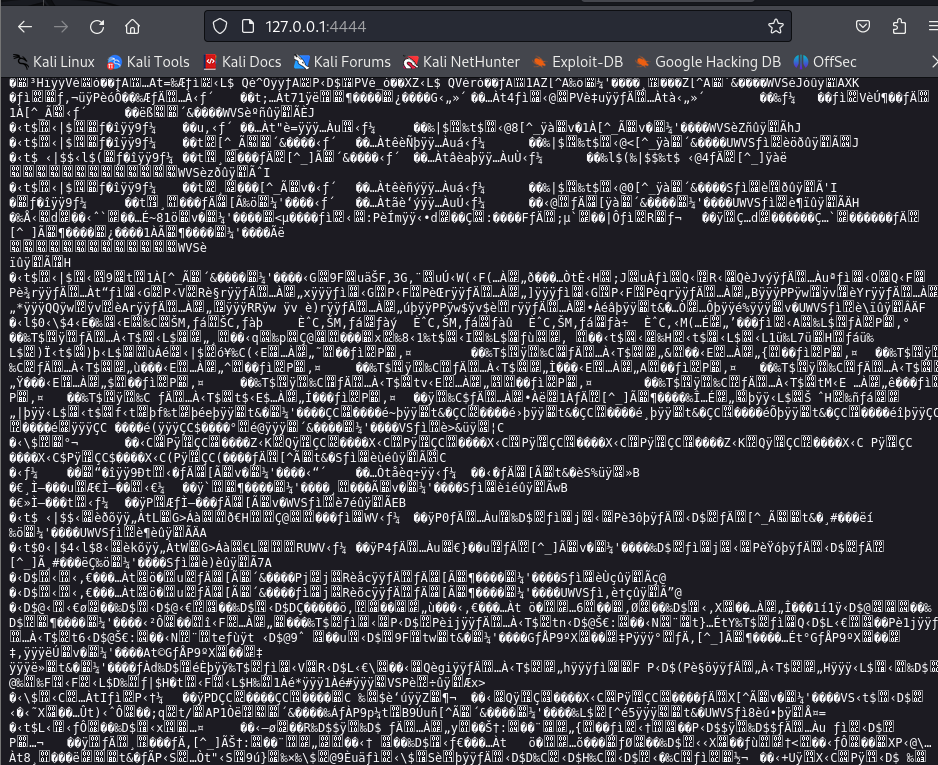
Successfully got the access.

Trail -2: Tried using nttrans module for the attack

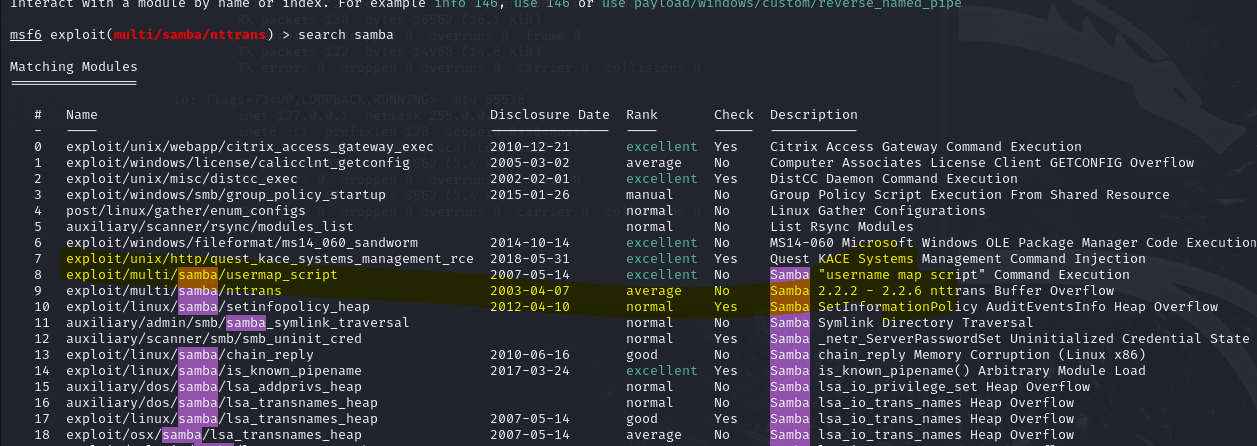




Got the below results but couldn’t get session created and access



Found the reason why attack 2 didn’t work: nttrans vulnerability only works on samba version from 2.2.2 to 2.2.4, but we have version 3.x on our metasploitable2 machice, you can see the version in the first screenshot of metasploit scanner attack.

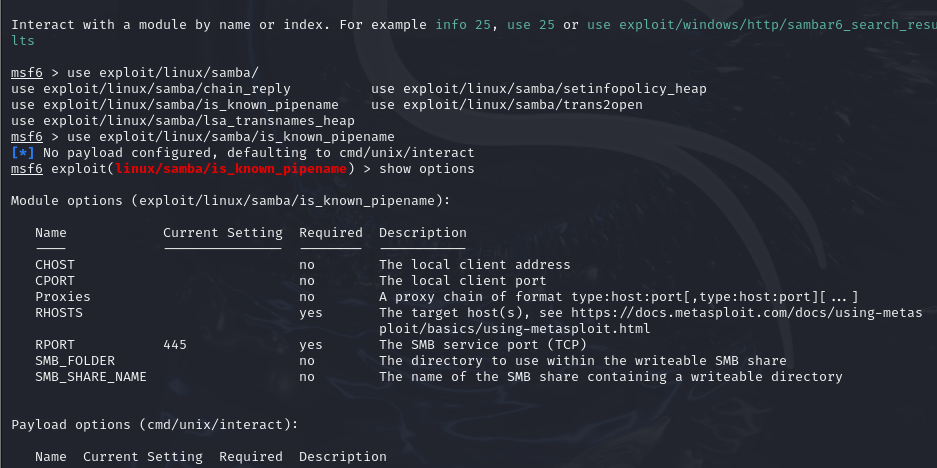


Trail 3:

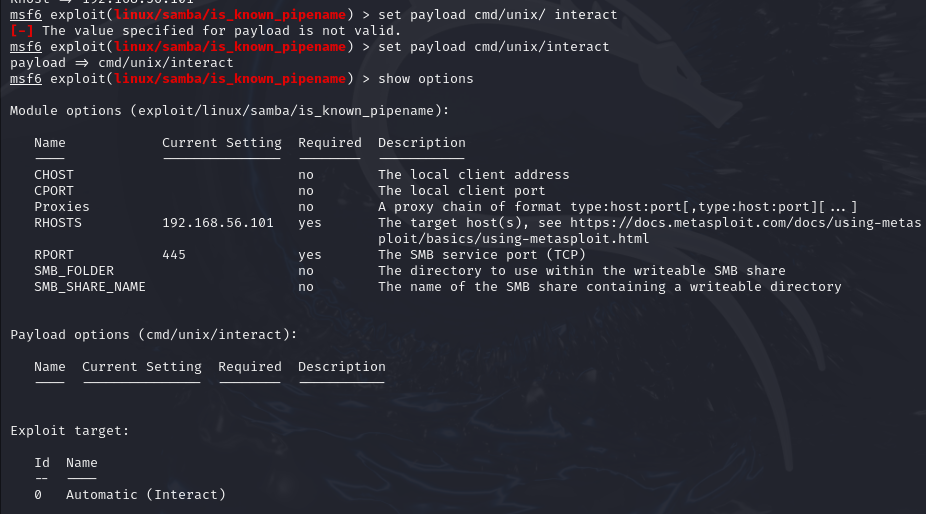
Used Linux/samba/chain\_reply module:  
After setting the attack, in first instance it tried different return address, but couldn’t get the session created.

Tried the attack second time, same thing tried different return address, Not sure what happened. The system got into loop and the terminal closed.

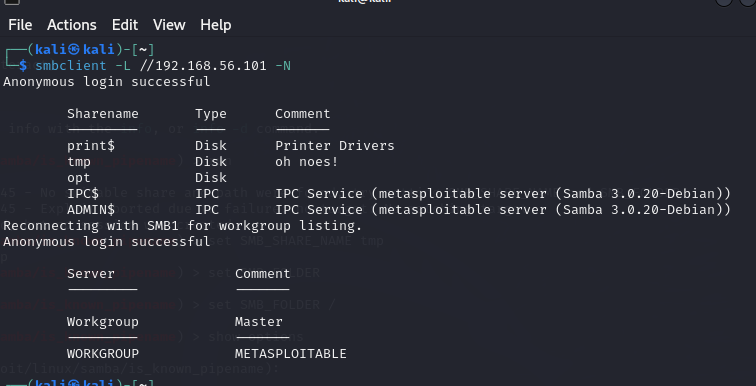
Trail 4: using is\_known\_pipename module



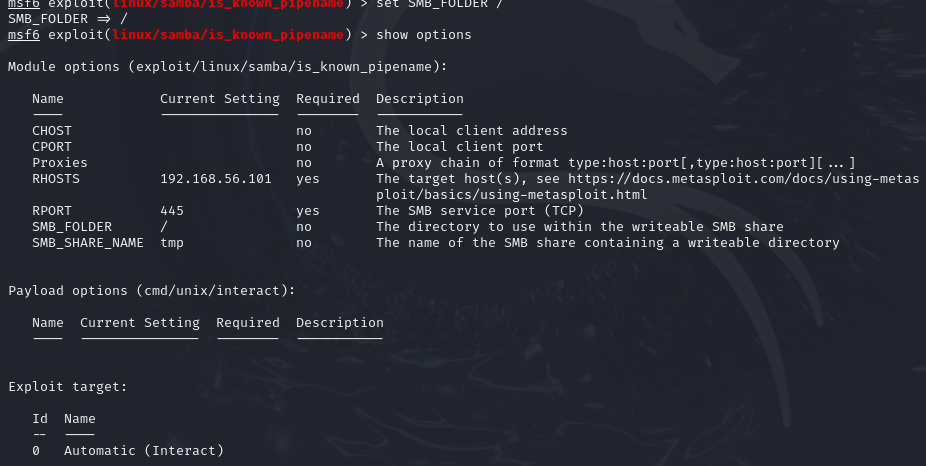
Set the rhost and payload.



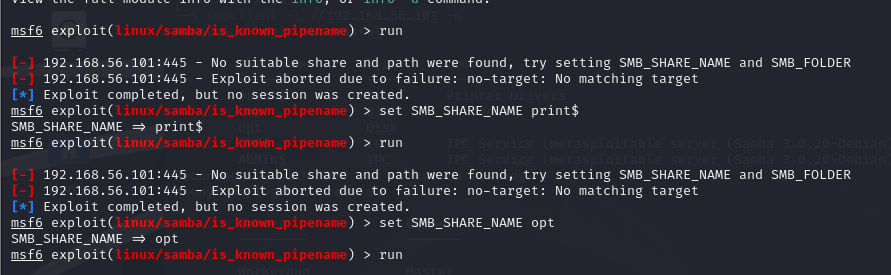
Tried to get more details on samba using smbclient command



Chare the share name and folder and tried the attack again.



Got the same result for it as well.



Reference:

<https://www.cvedetails.com/vulnerability-list/vendor_id-102/product_id-171/version_id-406020/Samba-Samba-3.0.20.html?page=1&order=1&trc=59&sha=3dd7d9a16c462a20692bc7785df9ac6cb16aa402>

<https://www.infosecmatter.com/metasploit-module-library/?mm=auxiliary/scanner/smb/smb_version>