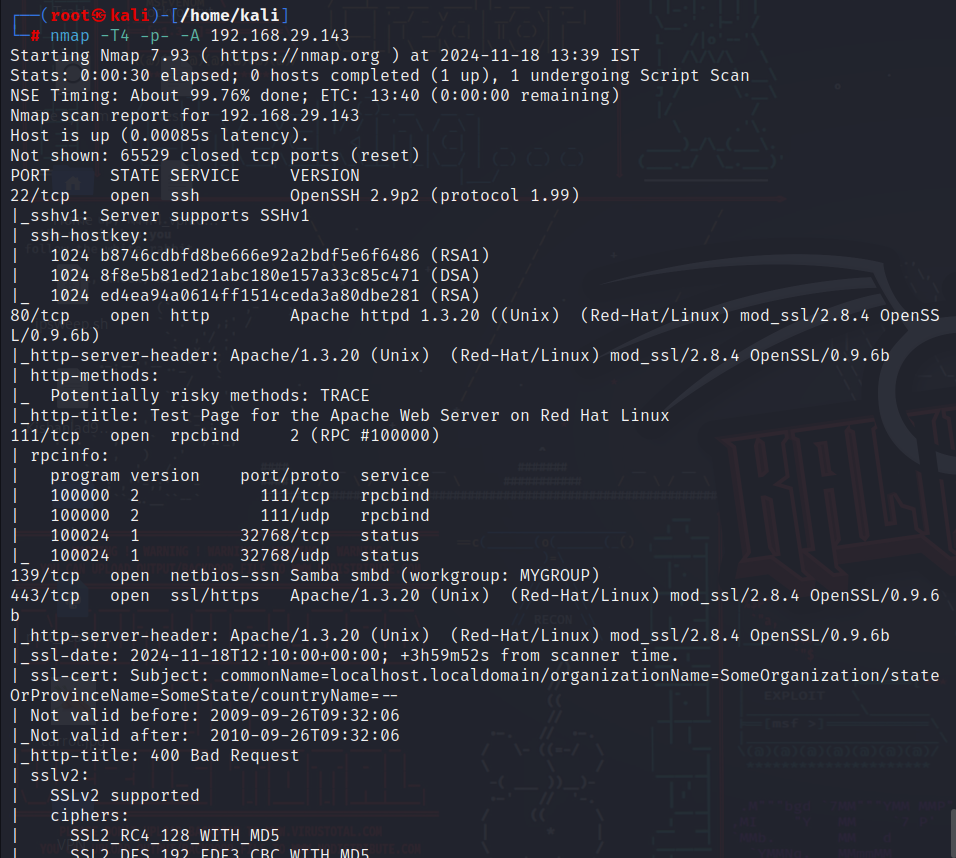
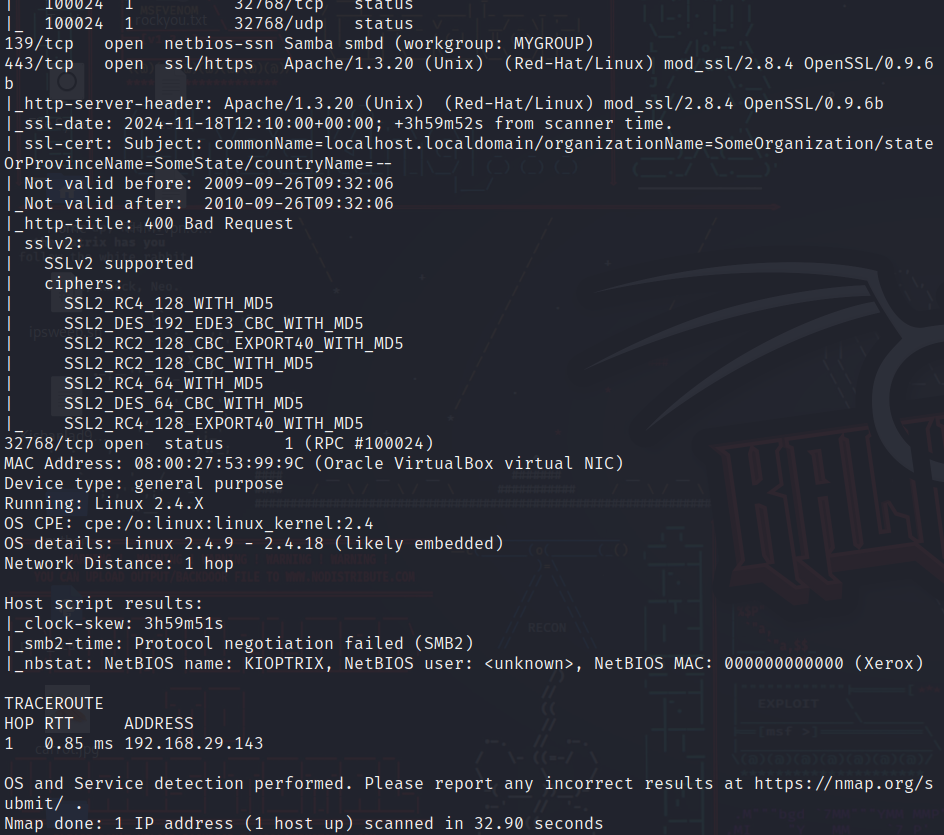
**Pentest on Kioptrix vulnhub machine**

* Just add .ova file in VMware or virtual box.
* Cred will be,  
  Username: **john**  
  Password: **TwoCows2**
* In these machine we can't use ip addr, ipconfig or ifconfig command. So If we want to know our IP then just ping 8.8.8.8. In its result we get our ip in from portion.

1. **Scanning with NMAP :**

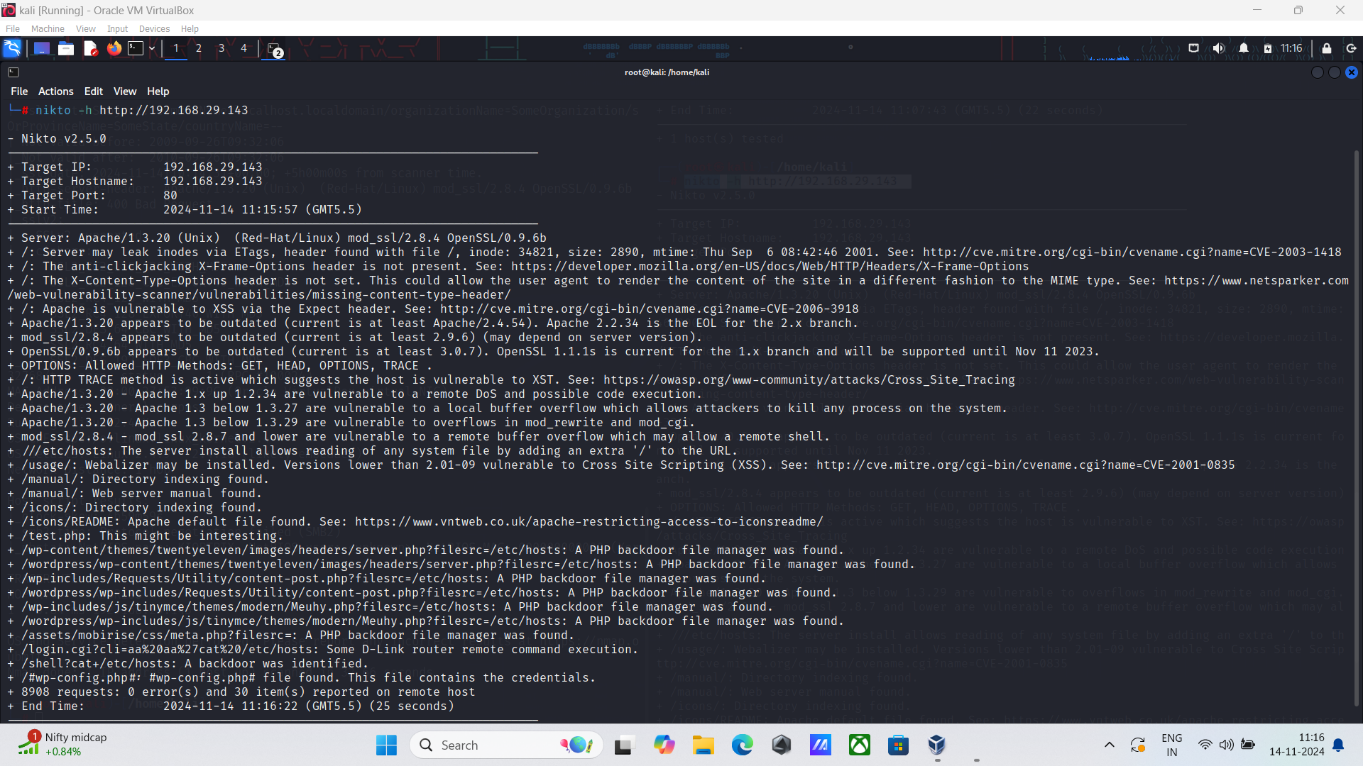
* Nmap is used to get list of open ports and services.
* It will follow 3-way handshake proccess for discovering open port and services. -> syn, syn/ack, ack
* Here, for syn:- "Hii, is this port is open", for syn/ack(response):- "Yes port is open", for ack(if port is open): - "lets make active connection".
* If we follow this stratergy(syn, syn/ack, ack) then it will make connection in last handshake and we can be detected.
* Insted of this we have to do "syn, syn/ack, rst"
* Here, for syn:- "Hii, is this port is open", for syn/ack(response):- "Yes port is open", for rst(reset): - "Kidding, not making connection bye"
* If we use these(syn, syn/ack,rst) stratergy then it is good for us.
* In nmap -A switch is for all(OS detection, version detection, default script scanning,tracert).
* 



* This is the result of nmap scanning.

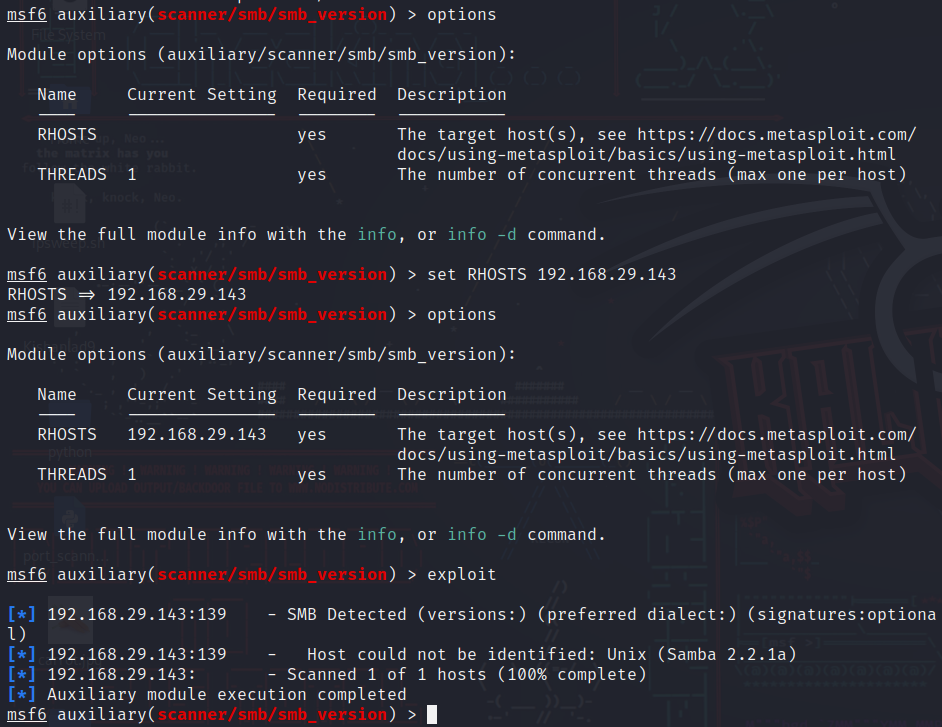
1. **Scanning with Nikto:**

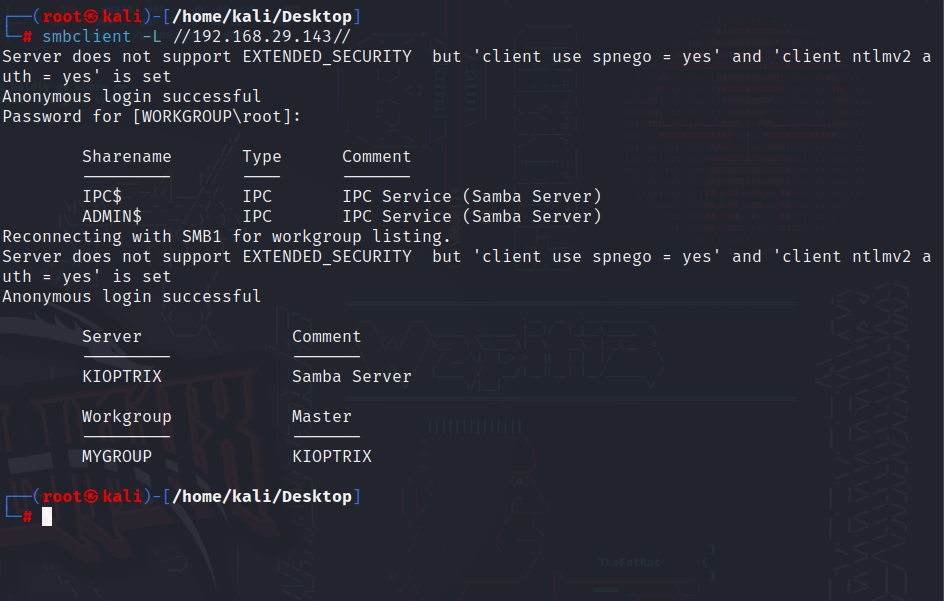
* It is used for scanning web server.
* With the use of it we can retrieve server version, OS, Vulnerability, directory etc.
* Look the result thoroughly and you will get all the required info.



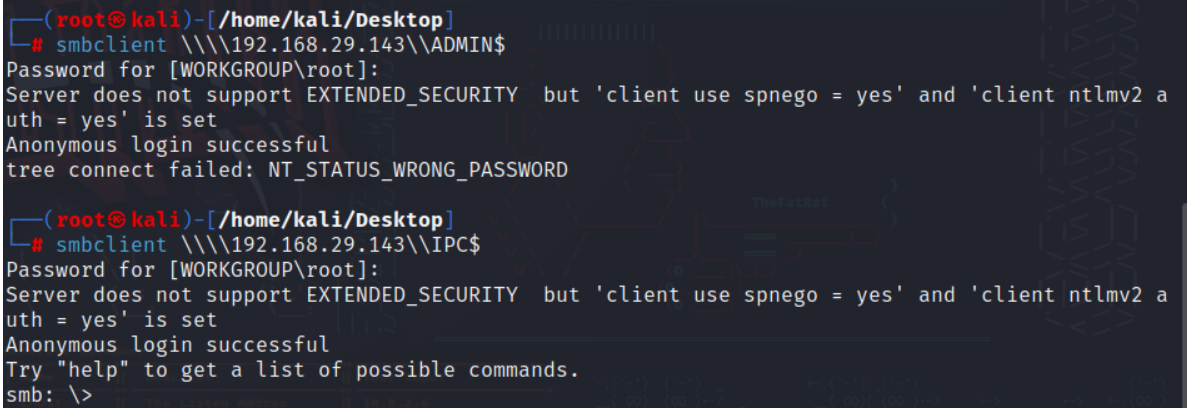
Here we got info "mod\_ssl/2.8.4 - mod\_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell".

1. **Enumerating SMB:**

* We can use Metasploit for identify the SMB version of machine.
* for that just write "search smb\_version" in Metasploit. In the result we get some kind of module for it.  
  EX: auxiliary/scanner/smb/smb\_version
* Here second part "scanner" is stands for action to perform. It can be dos(Denial of service), scanner, fuzzer etc.
* after using this module we have to set RHOSTS and then exploit.
* 
* Now we get the correct version (samba 2.2.1a) in the exploit result. Now we have to connect to the machine. We would use smbclient tool for it.

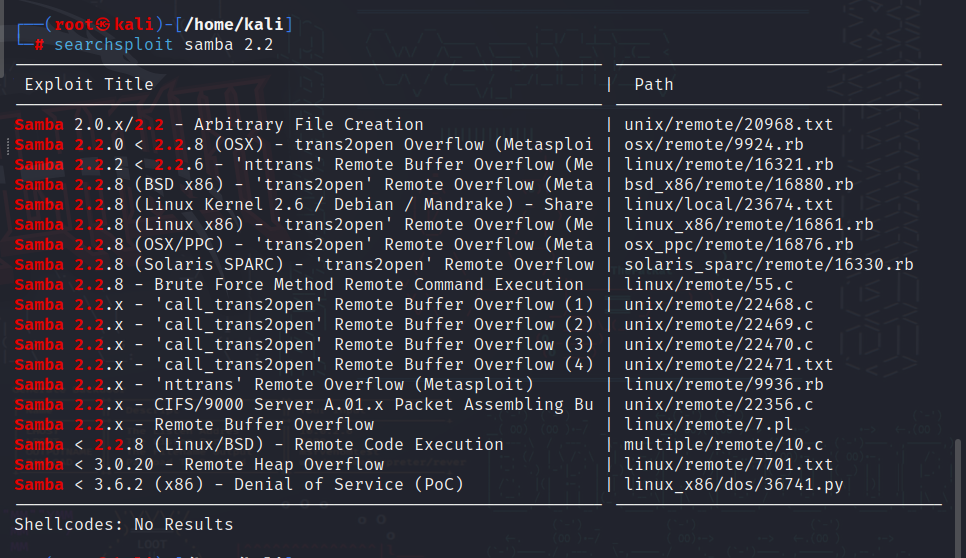


* Now we are going to connect with specific workgroup.

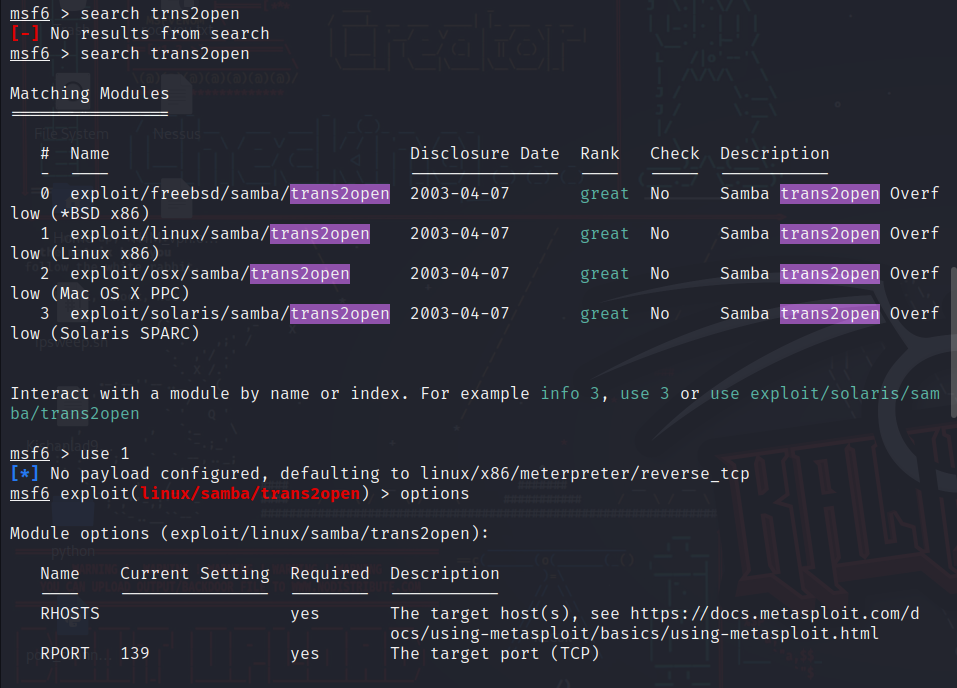


Here due to anonymous login we are connect it successfully.

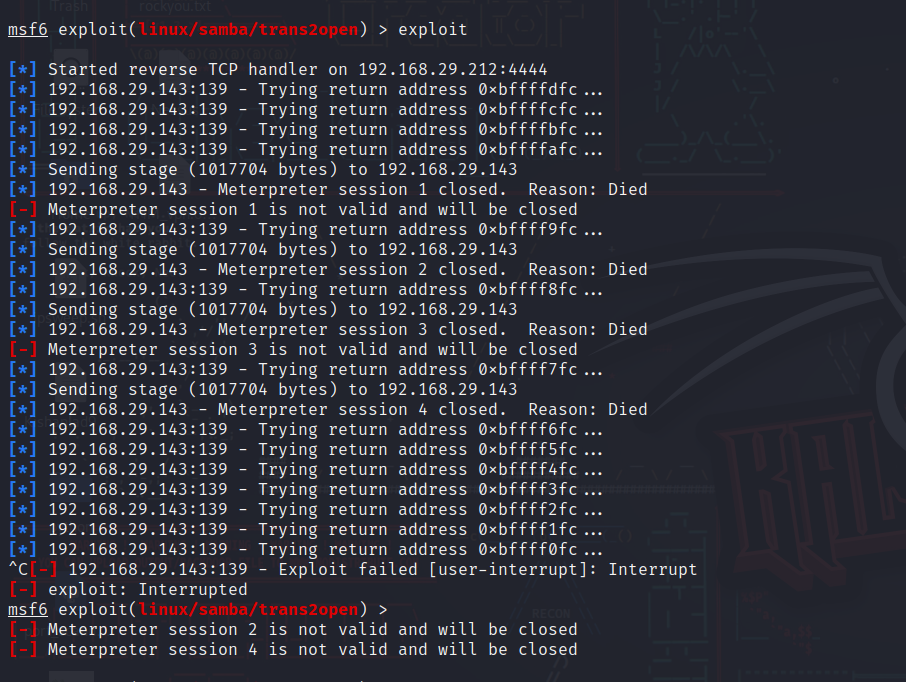
1. **Try to get shell of machine**:



* Now we have to check trans2open in Metasploit exploit.



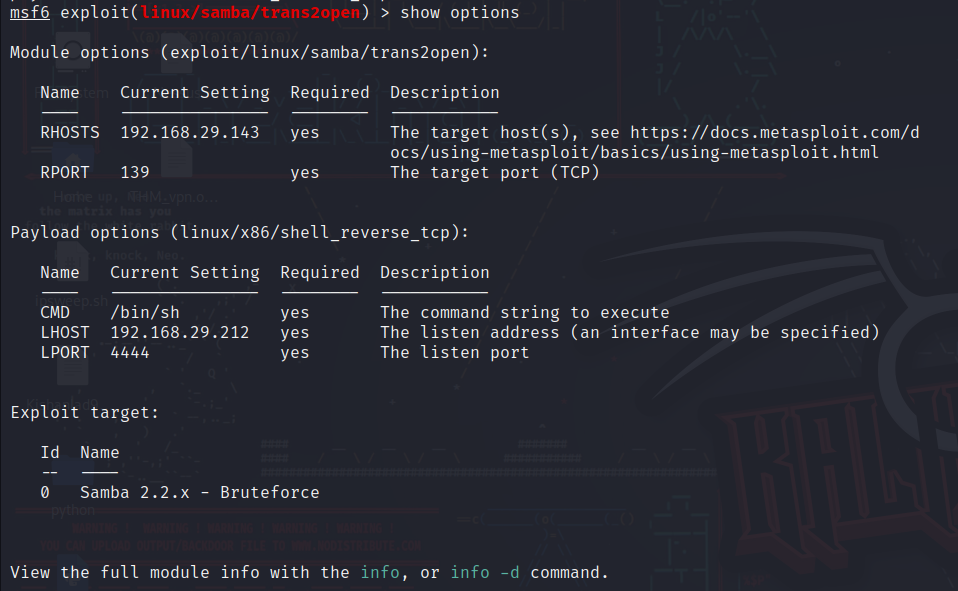
* Select the linux exploit with the use of “**use 1**”
* Here we use stage payload(linux/samba/trans2open). Now use appropriate module (As we use linux so choose linux).
* After that set RHOSTS value and type “**exploit”**



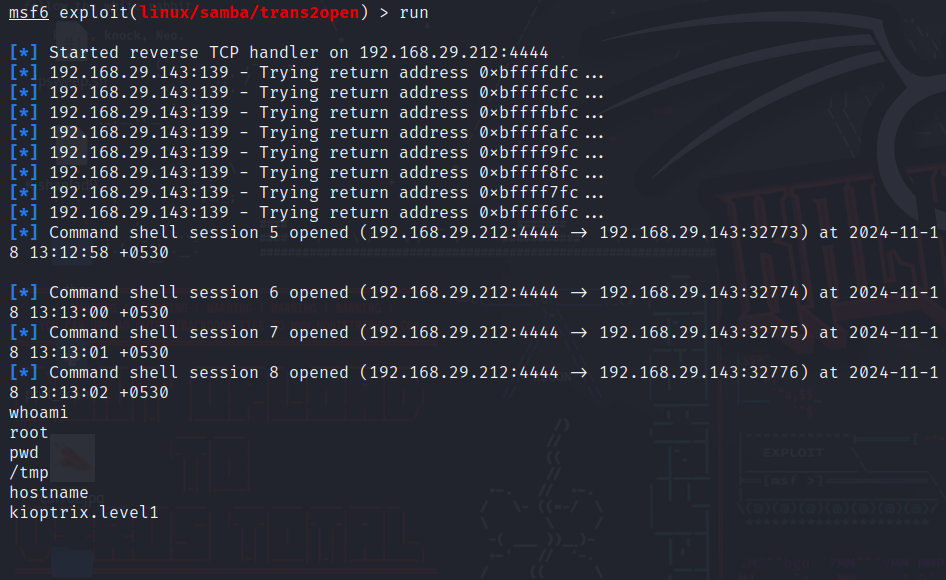
* With stage payload session is dying so try with non-stage payload.



* Checking options in selected payload.



* Now run the command “**exploit**” or “**run**”.



* Now we got shell of the machine. Here we can perform various commands which is shown above.