WEEK 16 DAY4: PROJECT

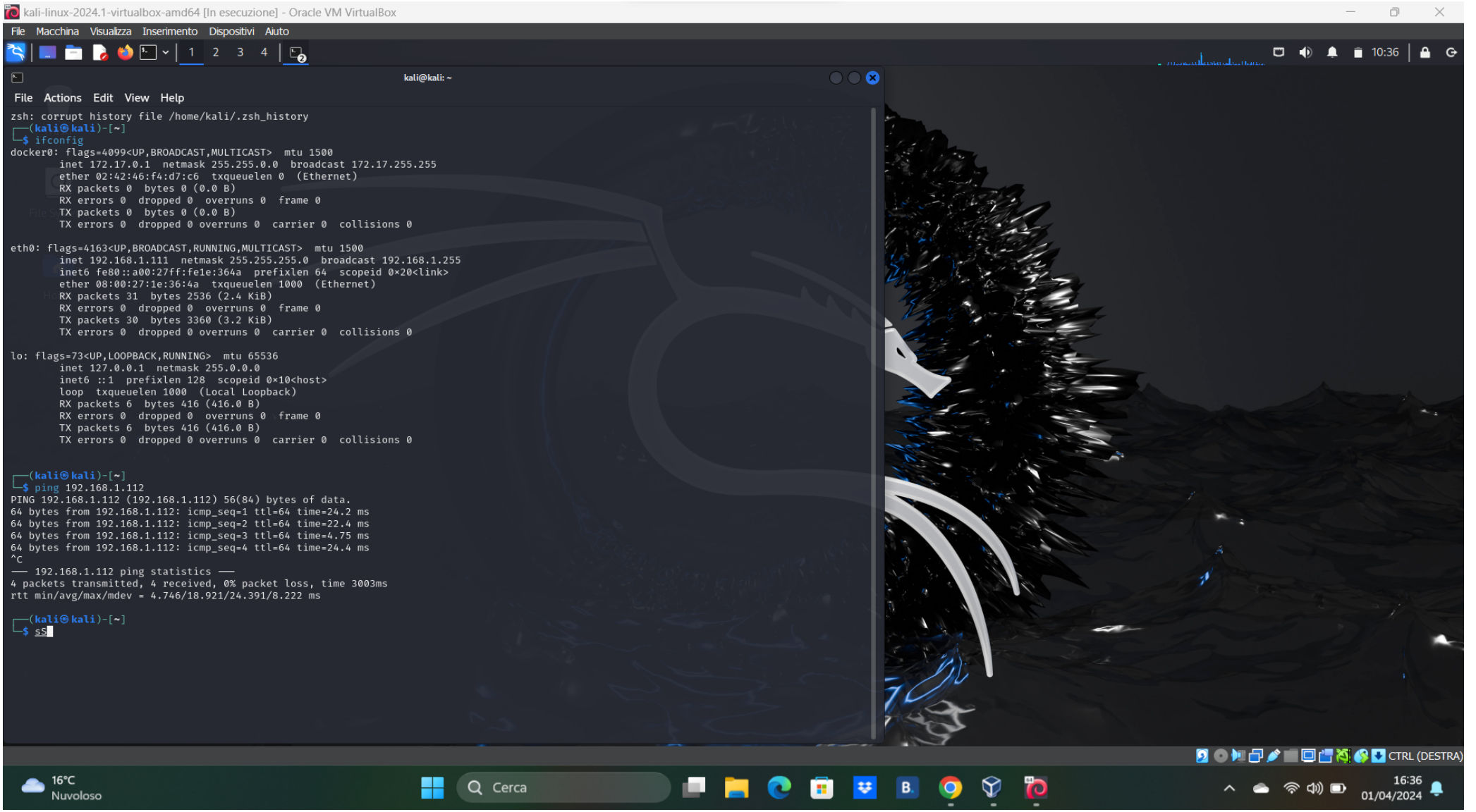
Traccia:

La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 – Java RMI. Si richiede allo studente, ripercorrendo gli step visti nelle lezioni teoriche, di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota.

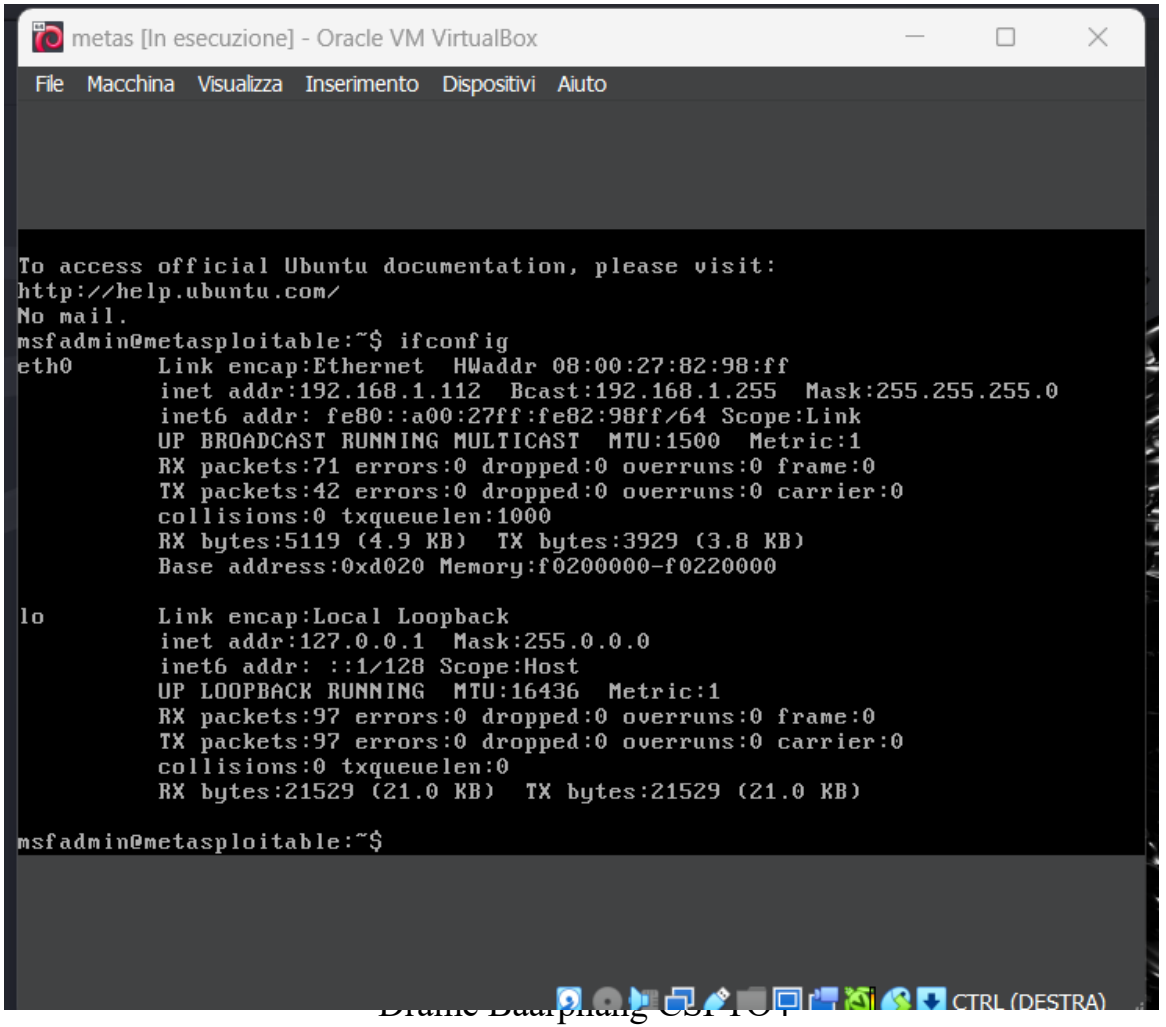
I requisiti dell'esercizio sono:

- La macchina attaccante (KALI) deve avere il seguente indirizzo IP: **192.168.11.111**
- La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP: **192.168.11.112**
- Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota: 1) configurazione di rete; 2) informazioni sulla tabella di routing della macchina vittima 3) altro...

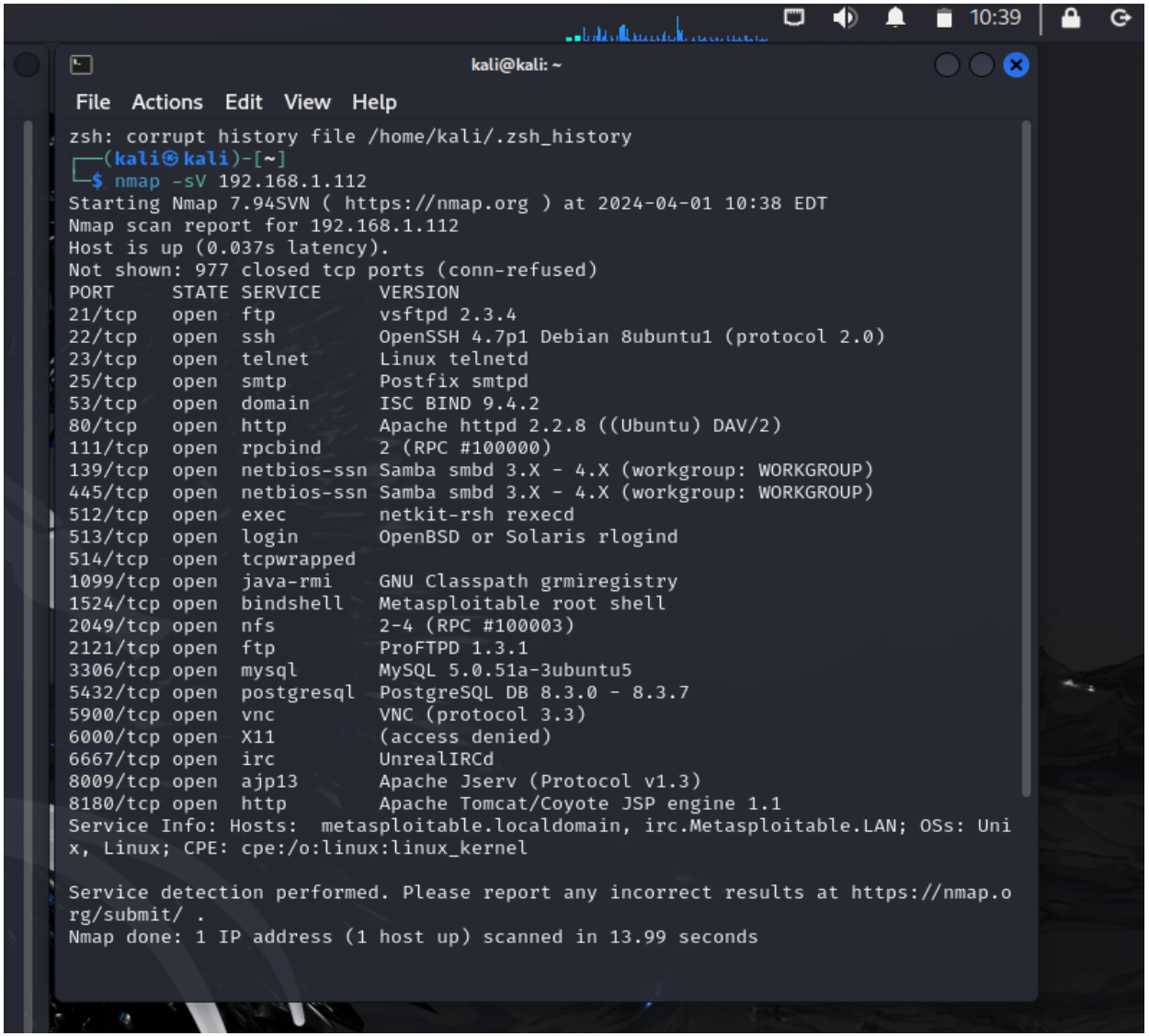
SETTING KALI LINUX IP ADDRESS AT 192.168.1.111



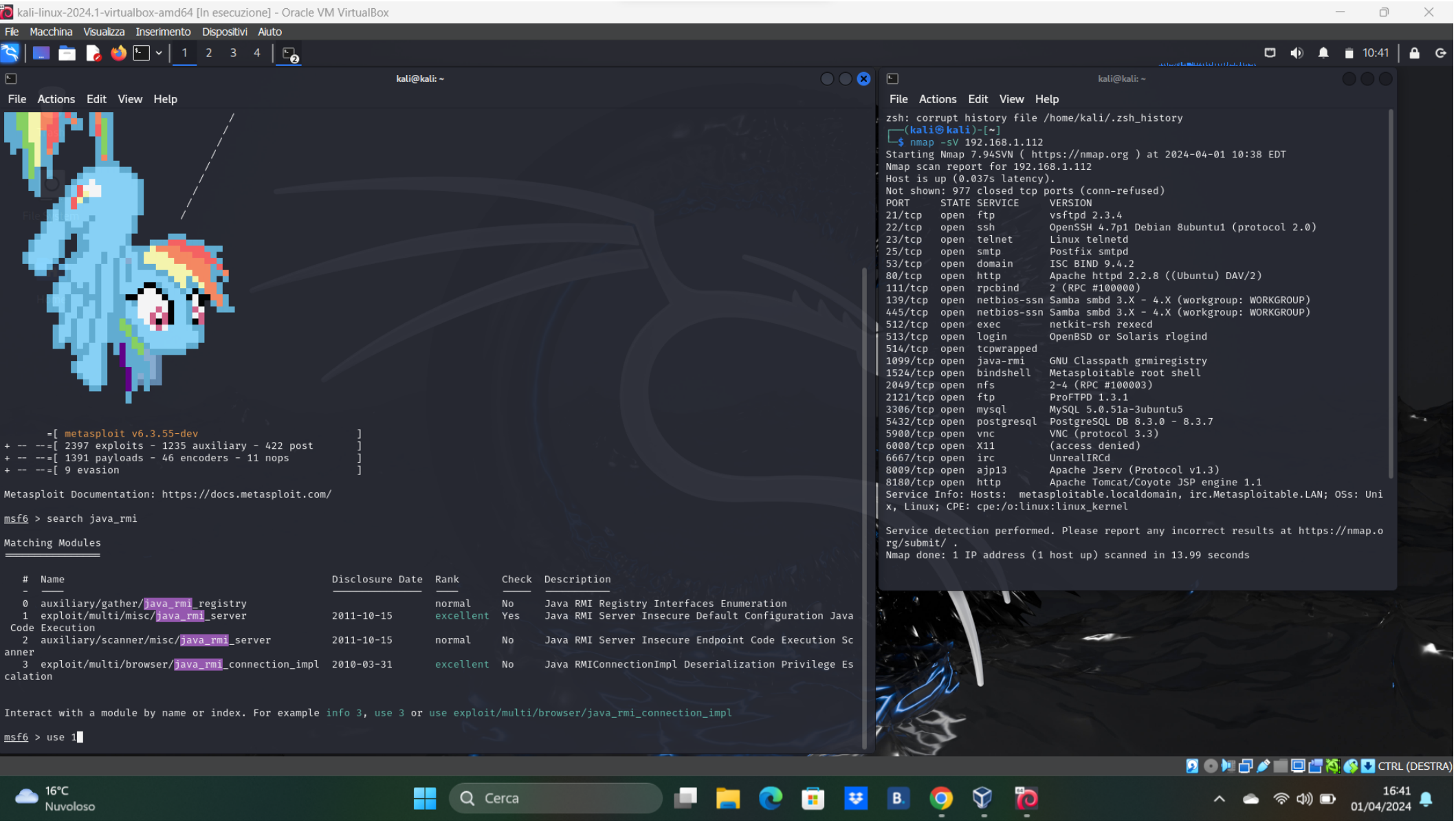
SETTING METASPLOITABLE2 IP ADDRESS AT 192.168.1.112



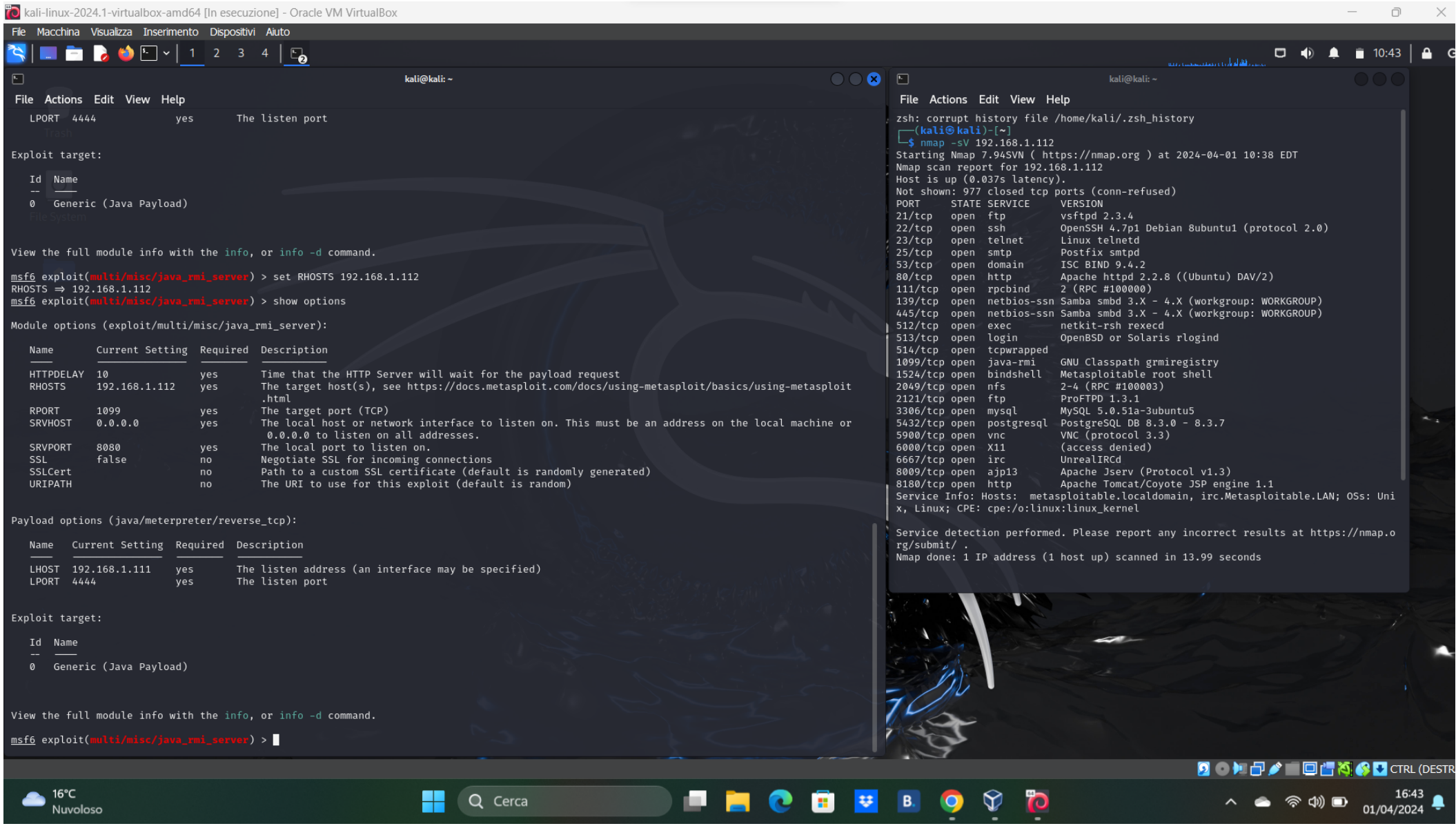
THE NEXT STEP IS TO CHECK THE TARGET IP ADDRESS WITH AN NMAP SCAN TO FIND EVERY VULNERABLE PORT;



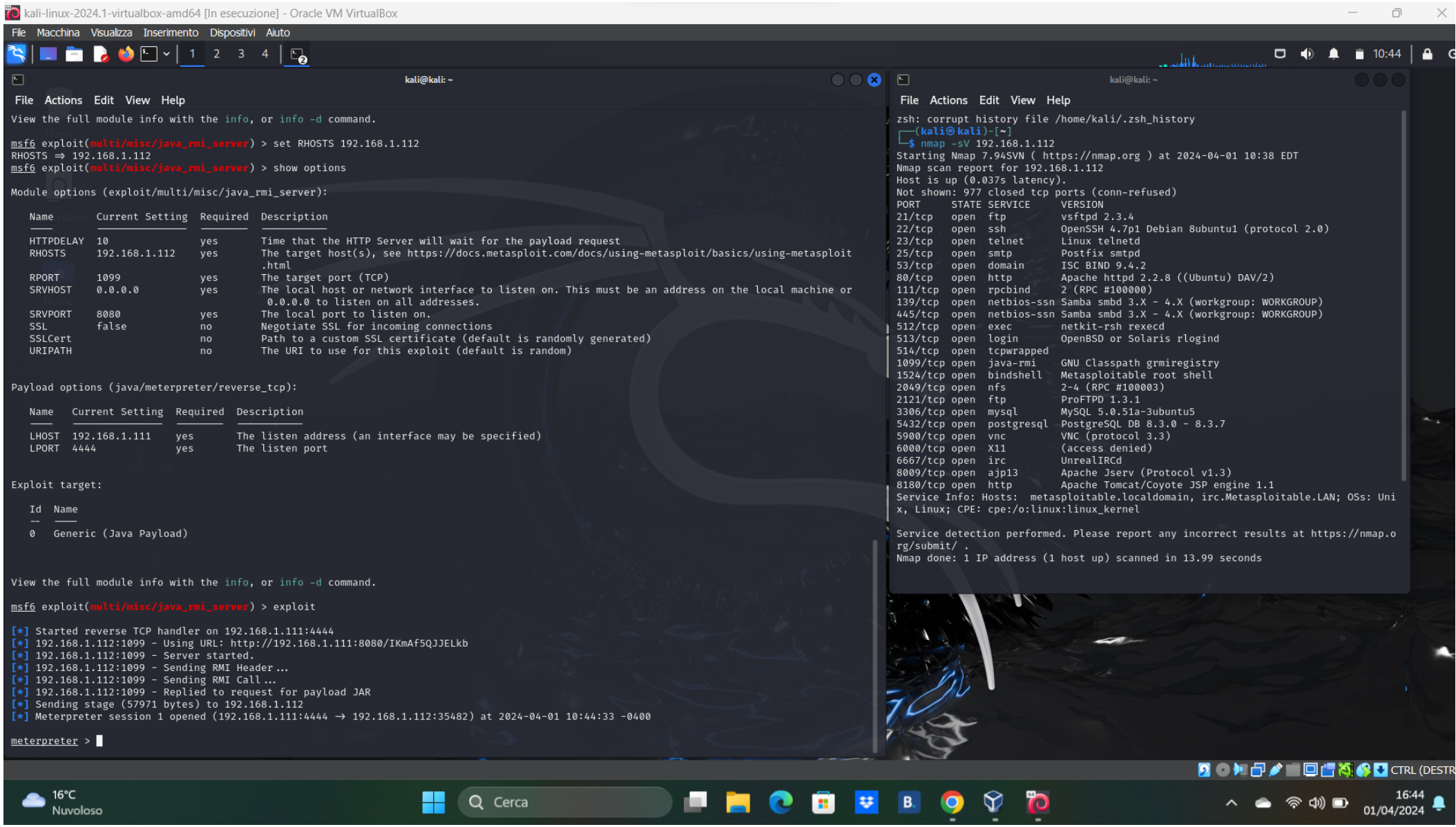
AFTER THE SCAN, WE WILL FOCUS ON PORT 1099; FROM OUR TERMINAL ON KALI LET'S START 'MSFCONSOLE' AND CHECK IF WE CAN FIND ANY MODULE OR AUXILIARY TO EXPLOIT THE VULNERABILITY.



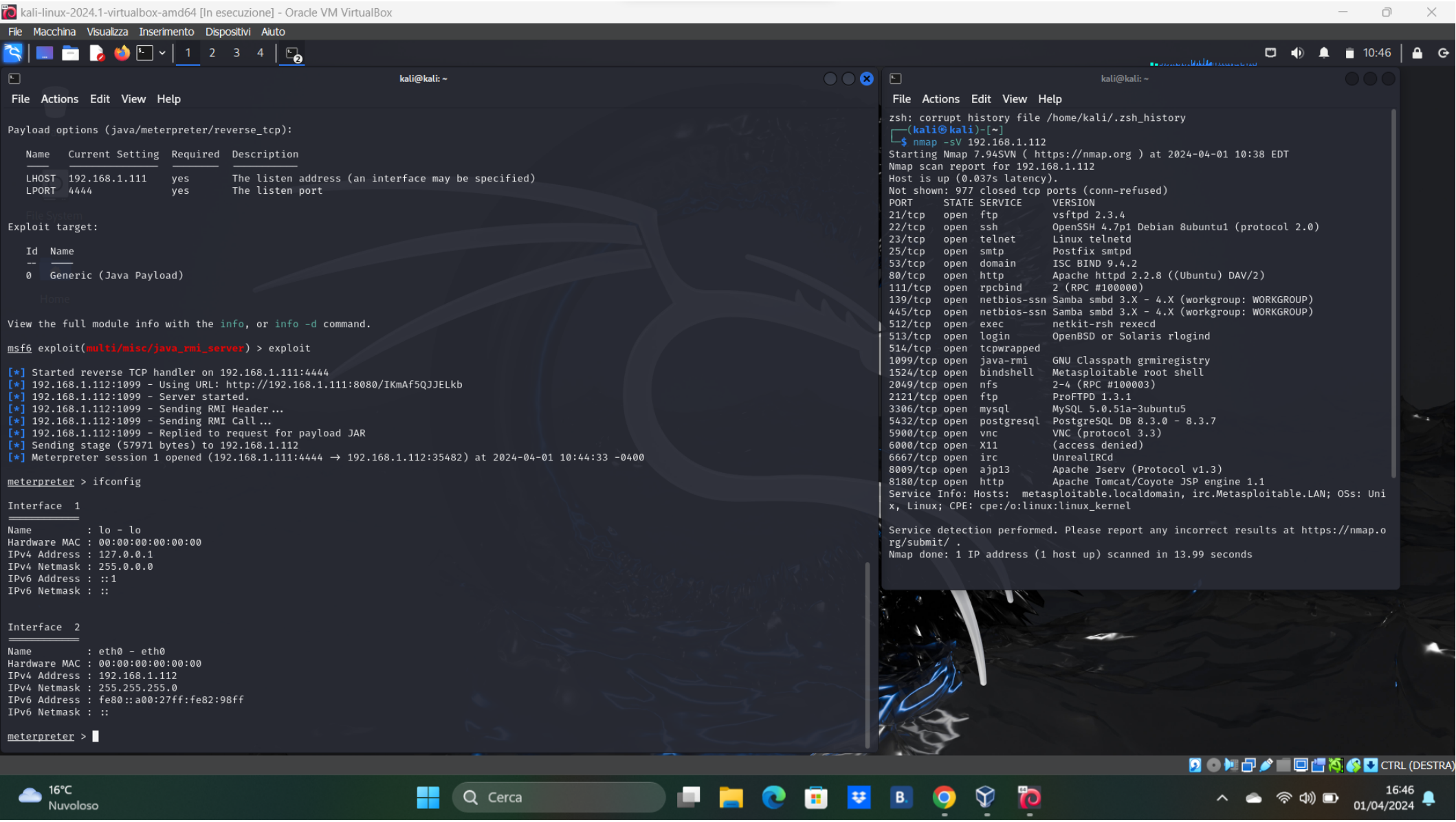
'EXPLOIT 1' SEEMS TO BE THE ONE FOR US, LET'S USE IT AND SEE HOW TO PROPERLY SET.



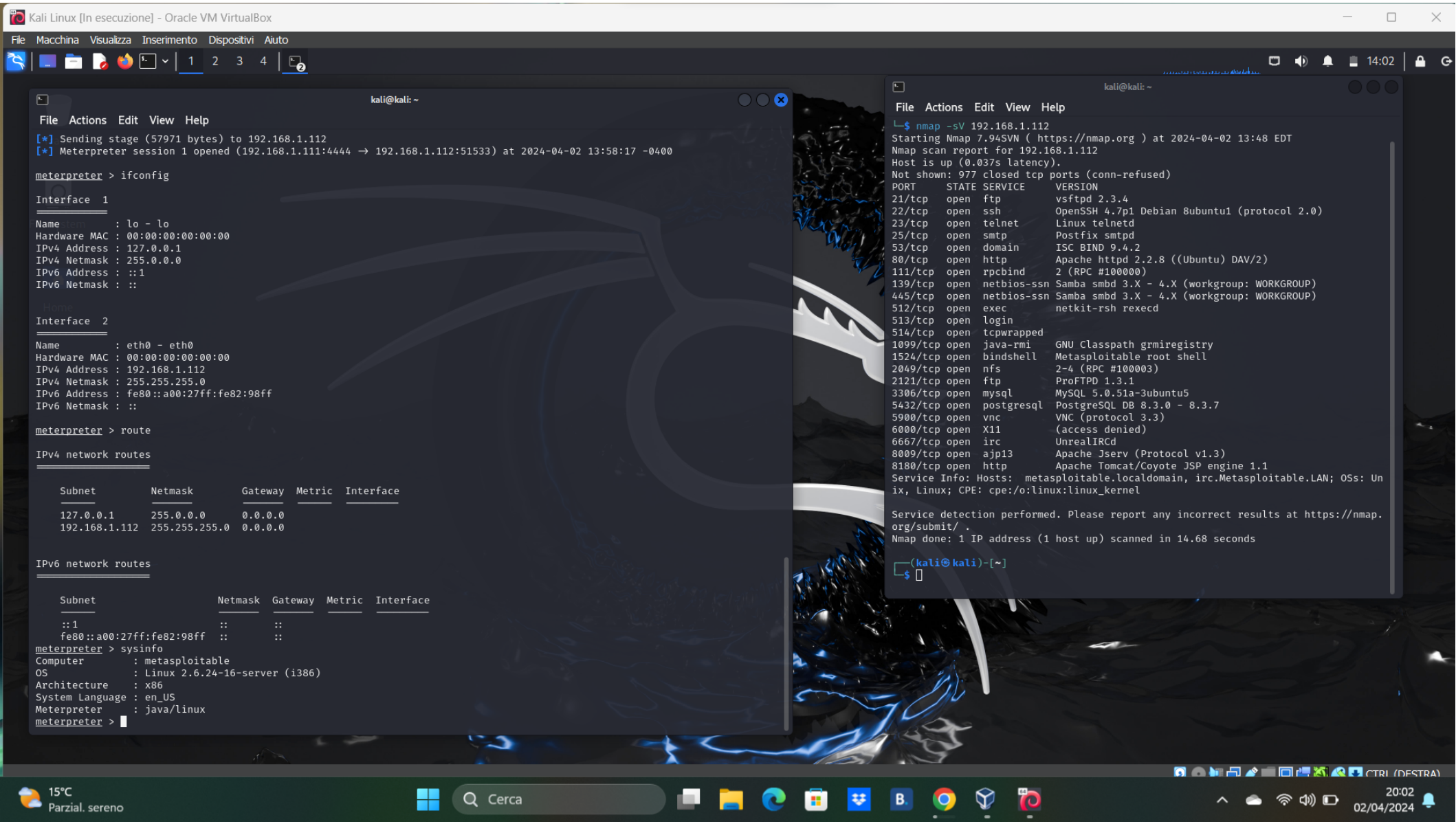
AFTER SETTING THE REQUIRED RHOSTS, WE CAN LAUNCH THE EXPLOIT.



MSFCONSOLE TELLS US THAT THE SESSION HAS BEEN CREATED, WE CAN CHEK IF THIS IS TRUE BY TYPING AN 'IFCONFIG' FROM METERPRETER; IF WE REALLY ARE INSIDE THE TARGET MACHINE METASPLOITABLE2 WE SHOULD SEE ITS SETTINGS



WE HAVE CORRECLTY EXPLOITED THE JAVA RMI 1099 PORT. LET'S CHECK THE ROUTING INFO AND SYSTEM INFO OF OUR TARGET FROM OUR TERMINAL IN KALI LINUX , ALWAYS THROUGH METERPRETER!



THANK YOU FOR THE KIND ATTENTION,
DRAME BAARPHANG