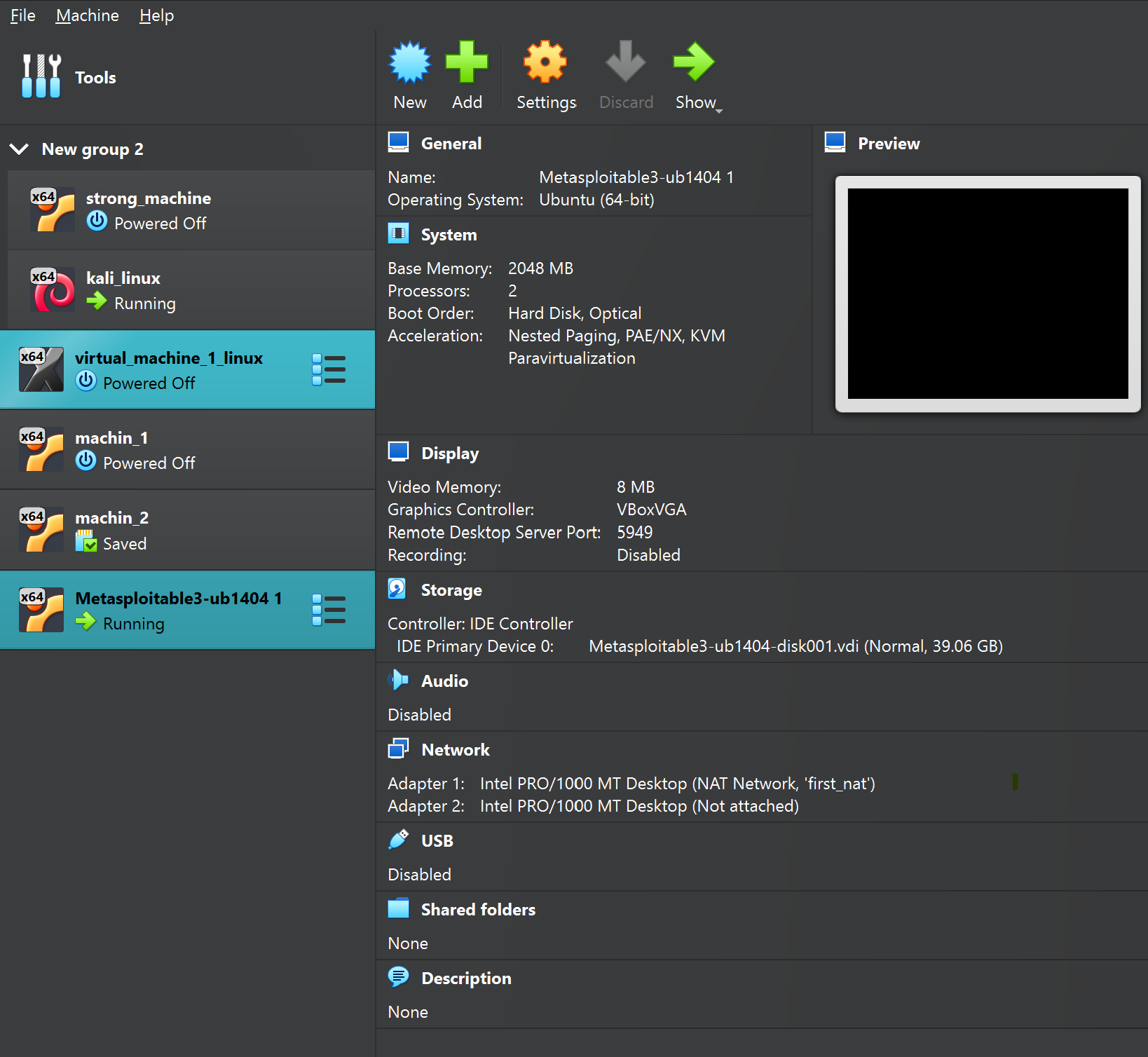
**ICS 344**

**COMPUTER INFORMATION DEPARTMENT**

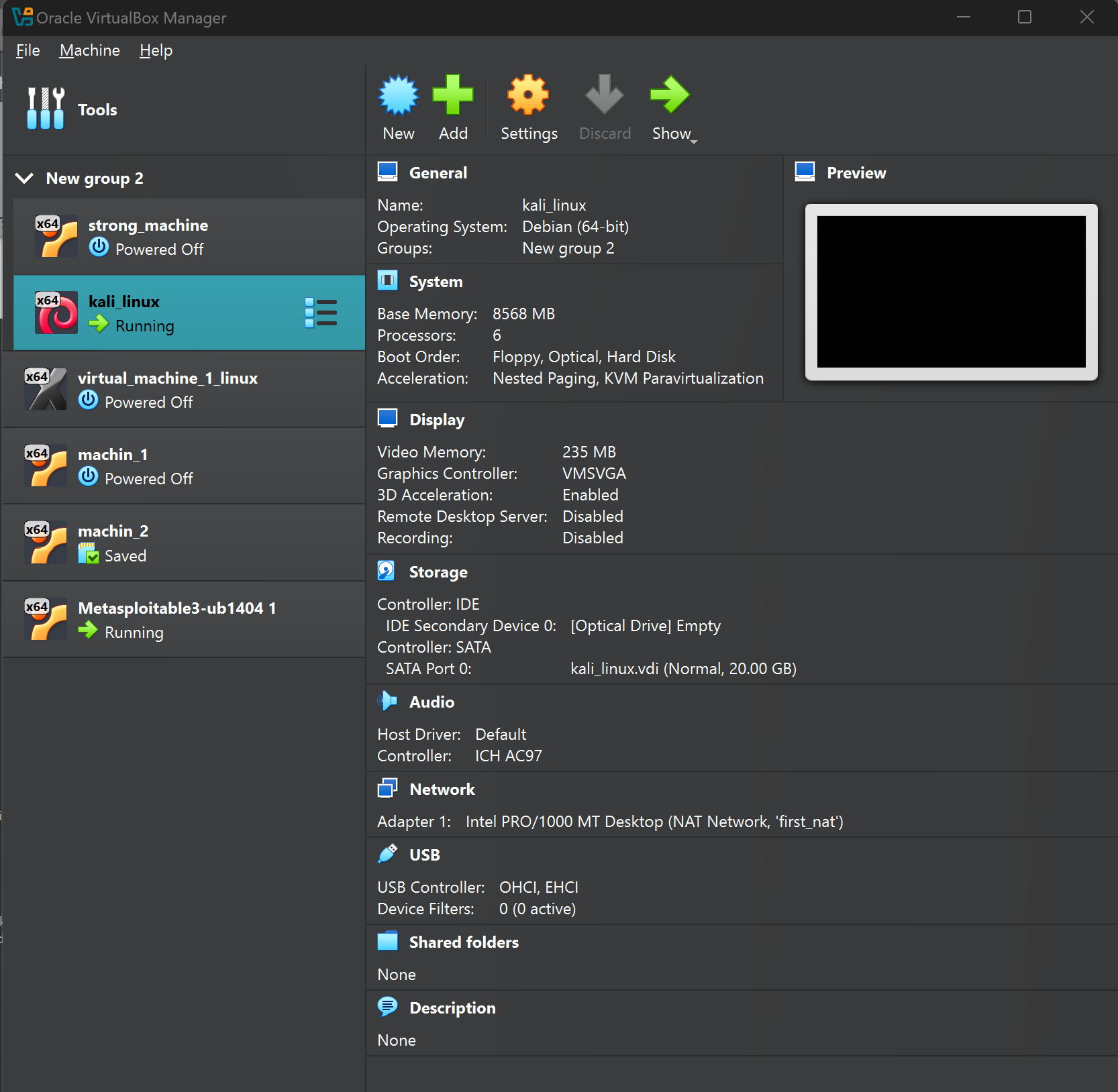
**Phase 1**

**Saad ahmed**

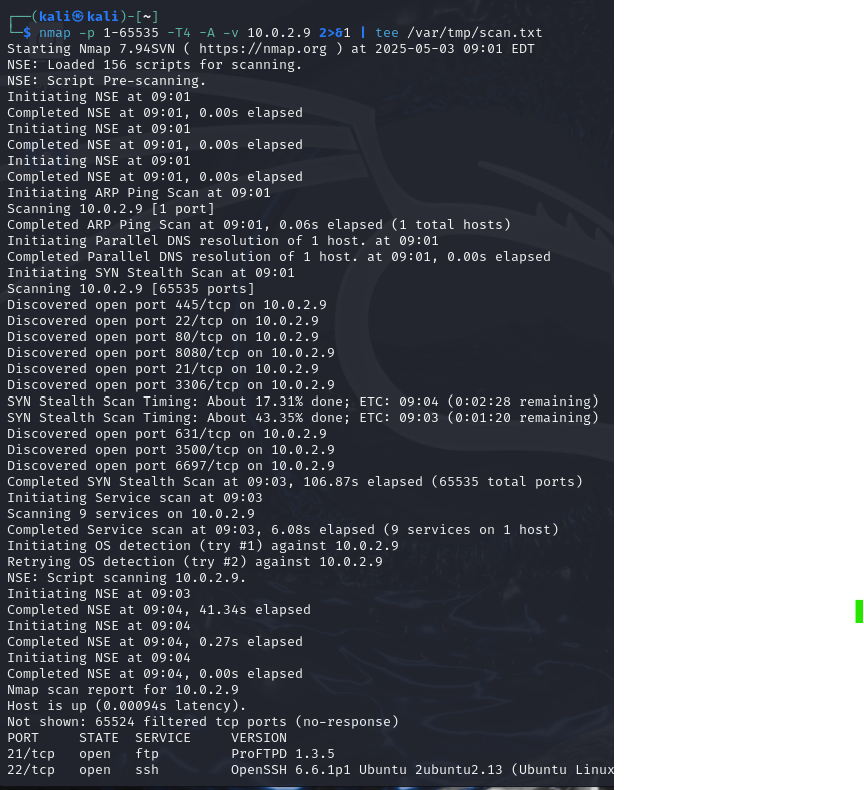
**Vm of Metasploittable**



**VM of kali linx :**



**RUNING NMAP TO SEE ALL PORTS AND DEVICES ON NETWORK**



**WE FOUND OUT THAT OPENSHELL USES AN OLD VERSION THUS THERE MIGHT BE A VULNRABILITY**

A screenshot of a computer

AI-generated content may be incorrect.

**SO WE EXPLIOT IT USING METASPOLT , AND AFTER THESE COMMANDS WE**

**HAVE ESTABLISHED A CONNECTION WITH THE VICTIM VM**

**THE PROOF OF CONCEPT IS ‘WHOAMI” -> VAGRANT**

A screenshot of a computer program

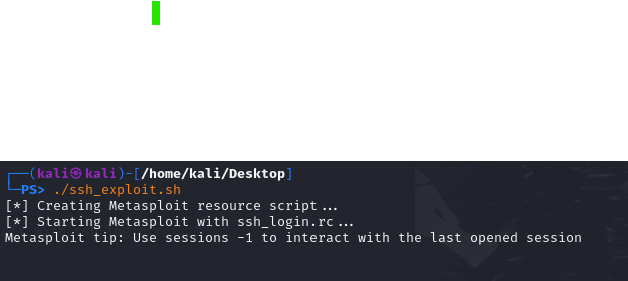
AI-generated content may be incorrect.

**WE THEN COPY ALL THE COMMANDS WE USED PREVIOUSLY TO MAKE A SCRIPT FILE**

**THAT IS EXCUTED BY SHELL**

A screenshot of a computer

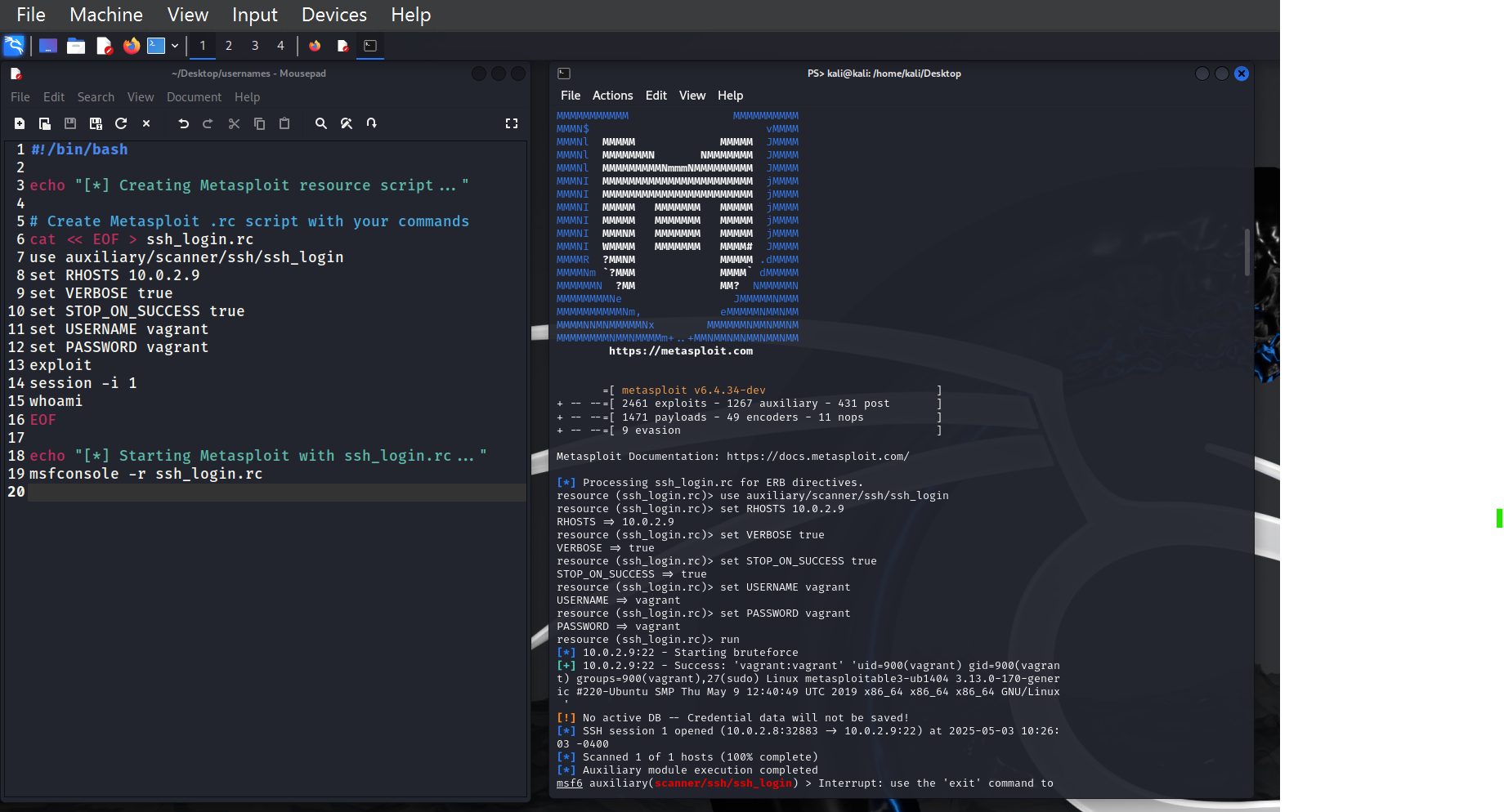
AI-generated content may be incorrect.



**Here we execute the script file**

A screenshot of a computer screen

AI-generated content may be incorrect.

**This is the result , same as previous , when we execute the script – this is a continuation picture of the previous picture , cause its long.** f