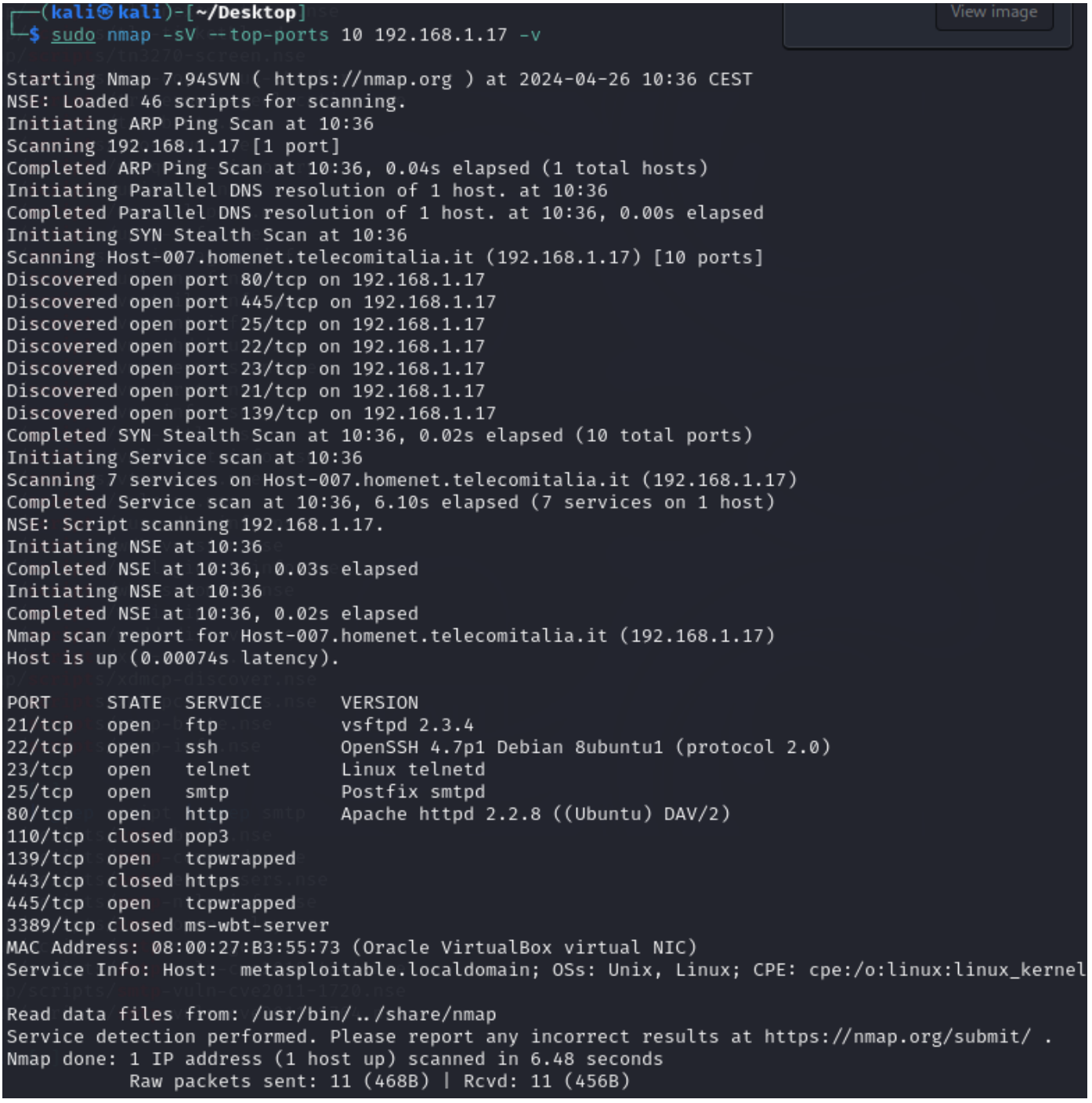
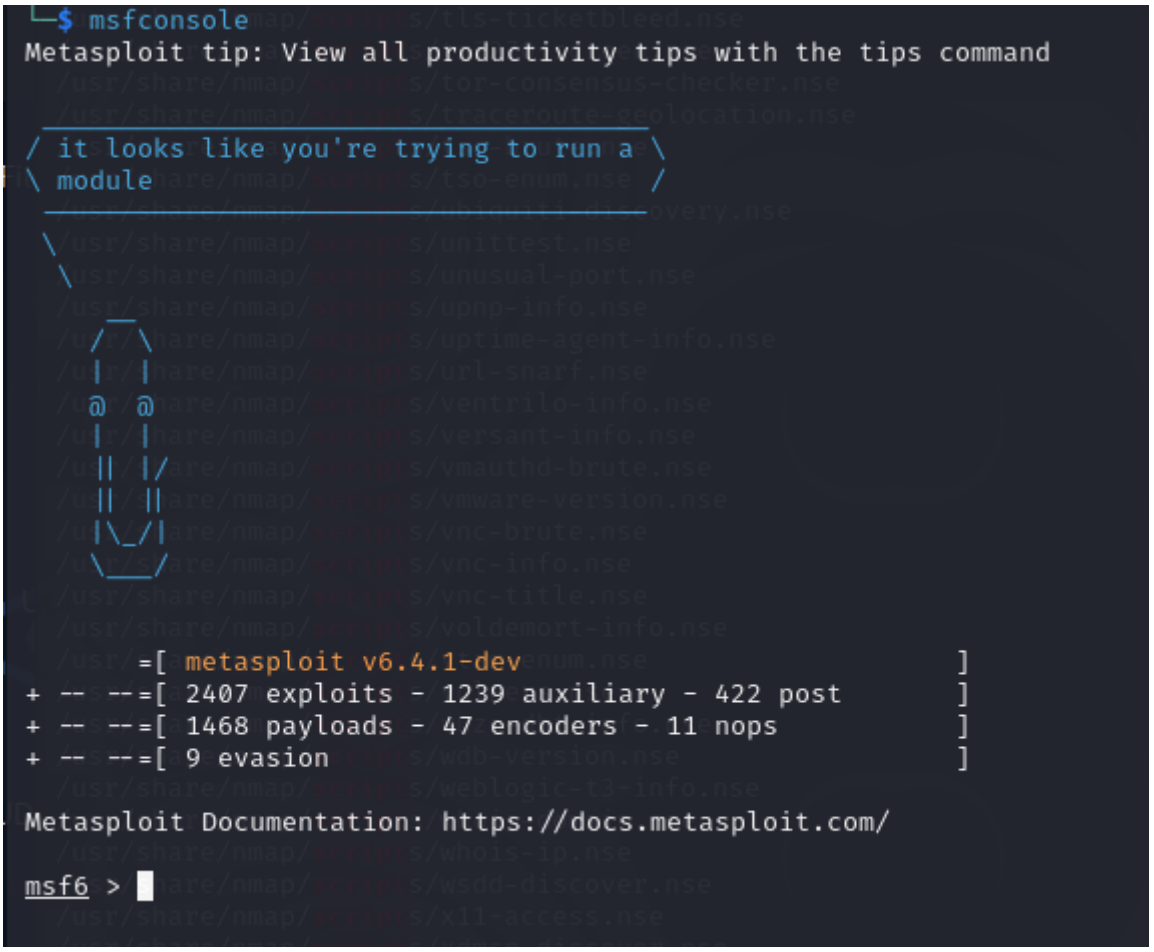
W10D4

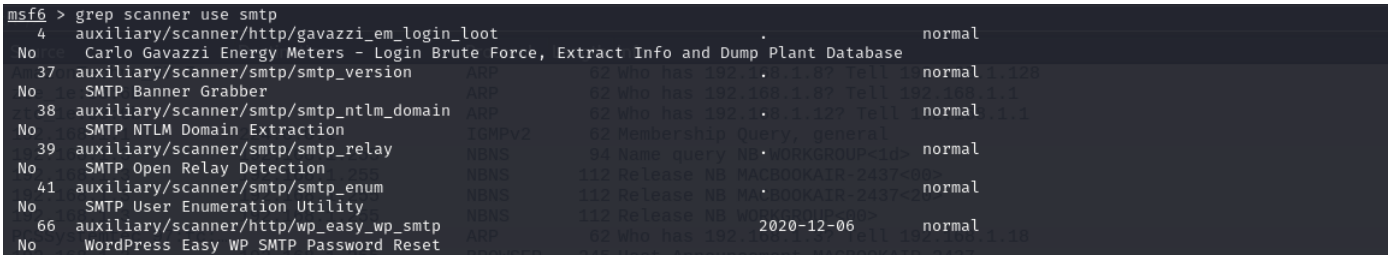
con nmap controllo le porte aperte di metasploitable 2



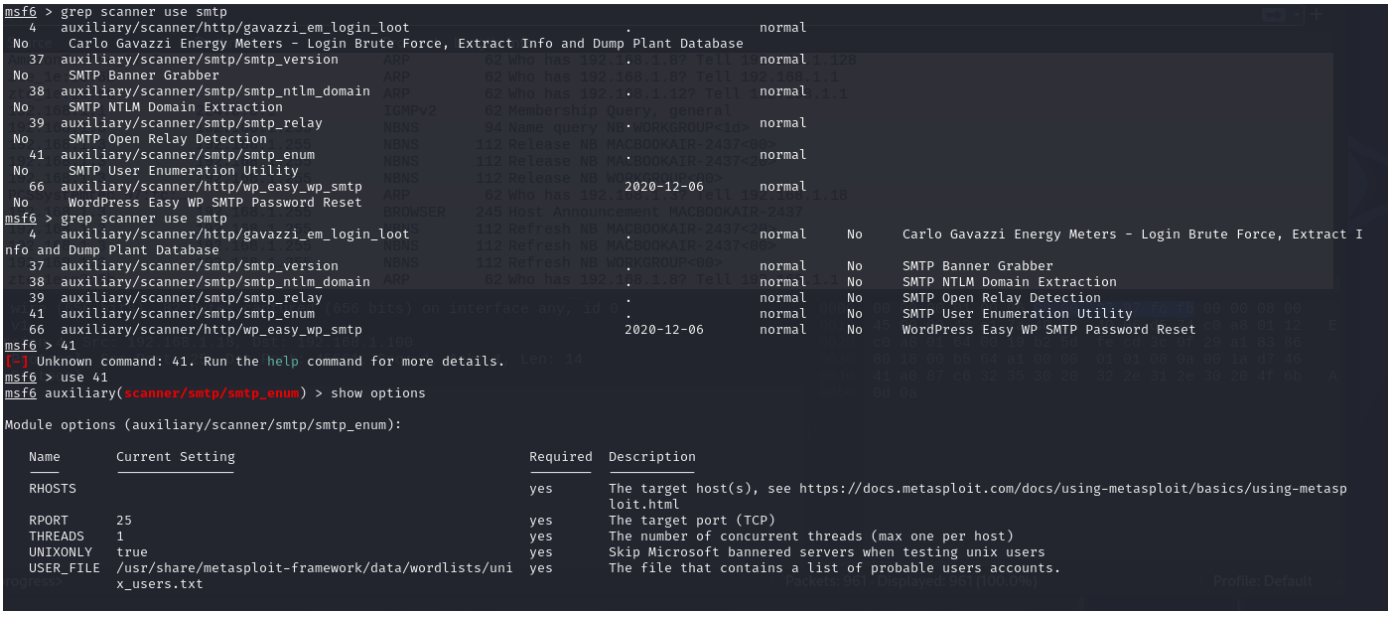
faccio partire metasploit con il comando **msfconsole**



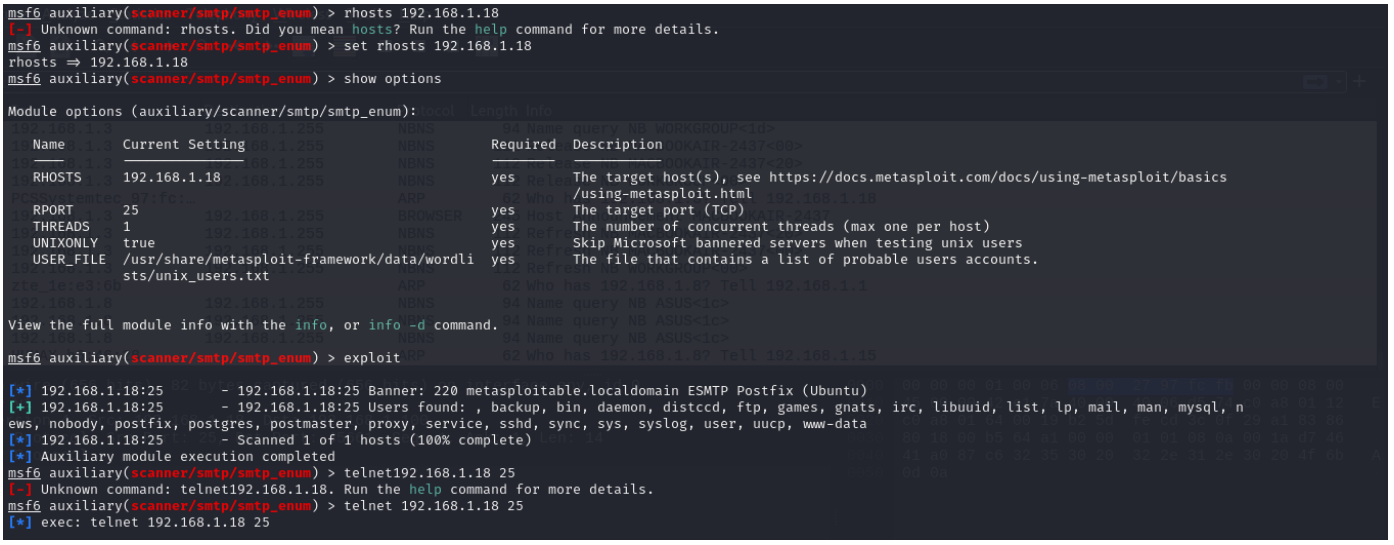
con il comando **grep scanner use** smtp mi filtra gli exploit riguardanti il protocollo smtp



scelgo lo script che la enumerazione smtp con il comando use 41



set rhost seguito dall'ip di metaesploitable e poi lancio lo script exploit, il quale mi restituirà gli user presenti sulla macchina attaccata, trovati grazie al file unix_users.txt



faccio **banner grabbing** con telnet con il comando VRFY