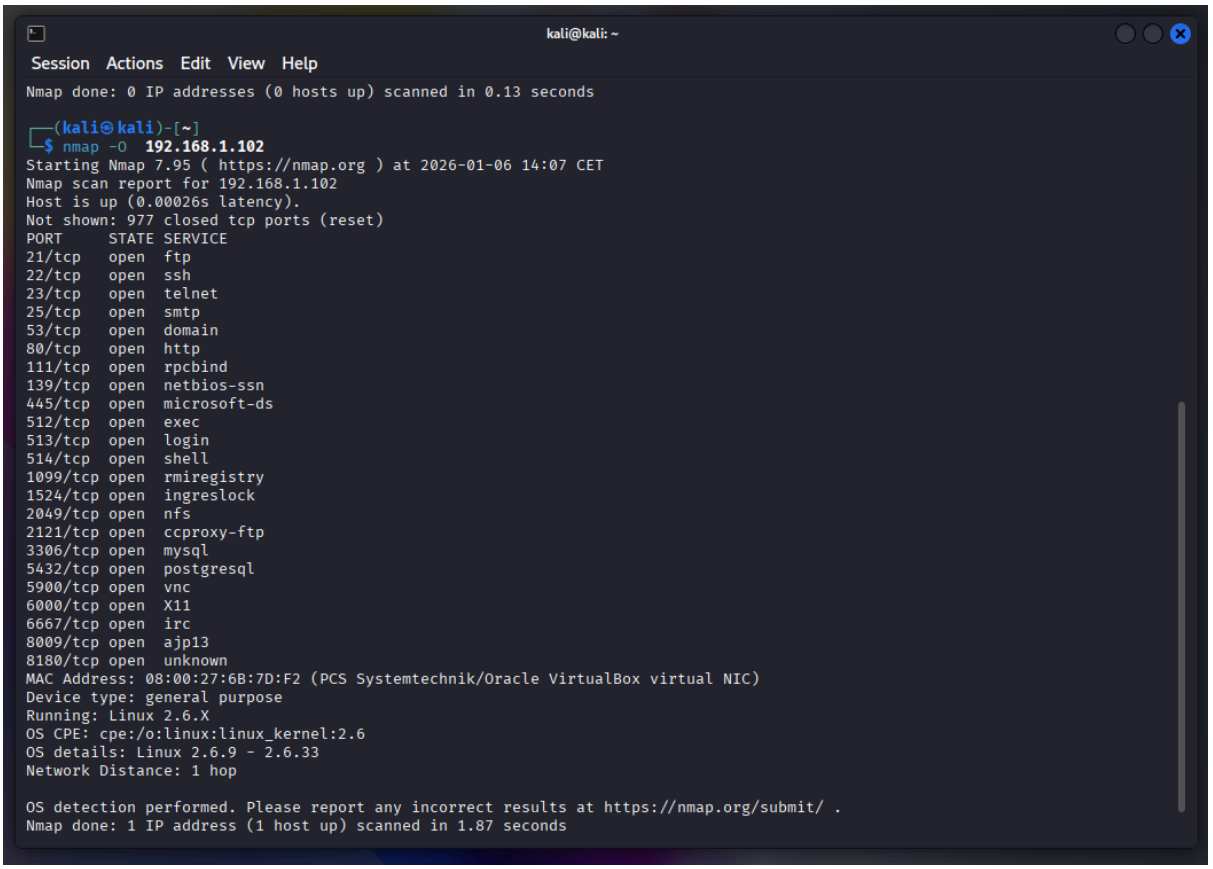
# Report per scansione NMap su Target Metasploitable

## Obbiettivo :

Si decide di raccogliere informazioni su un **target Metasploitable** di **Ip 192.168.1.102**

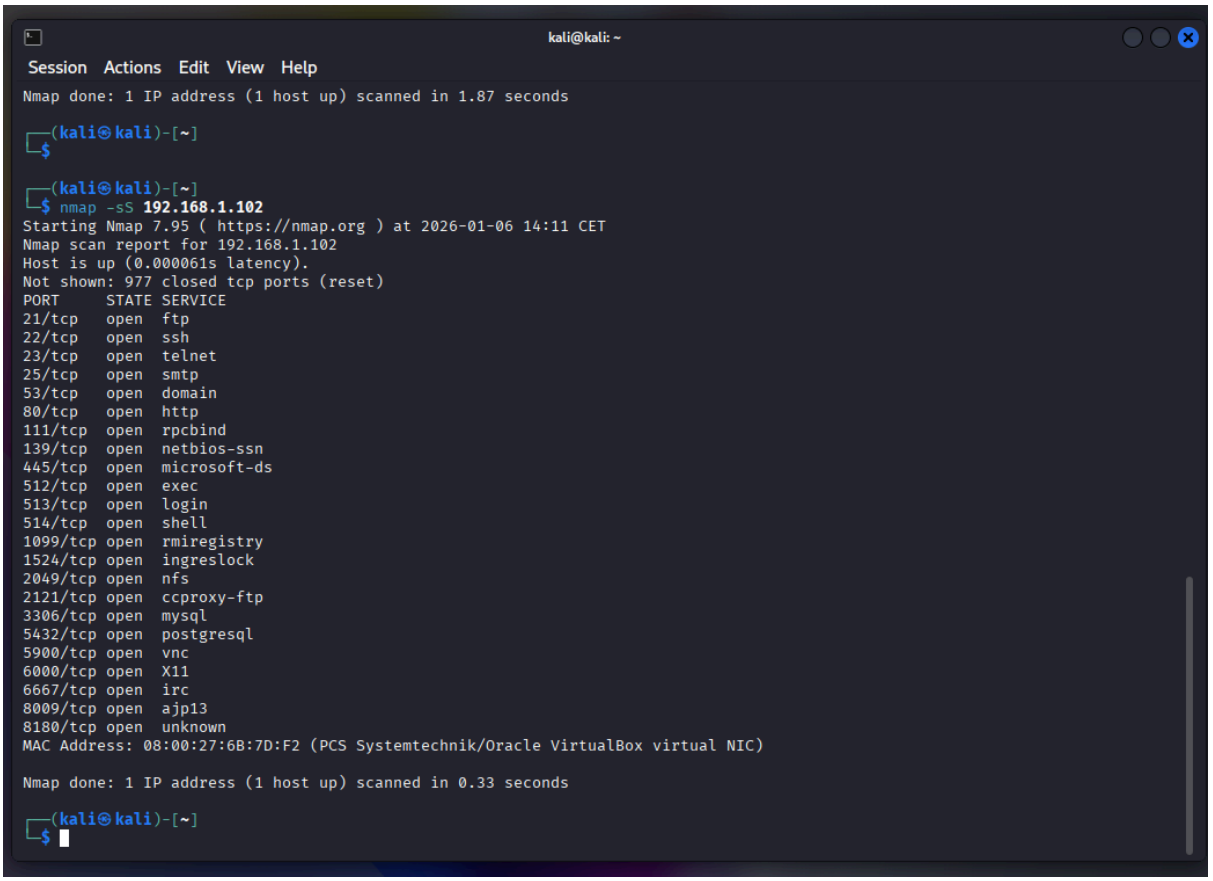
- Os FingerPrint : determina il sistema operativo chè e in esecuzione sul target :
    - Comando : nmap -O 192.168.1.102



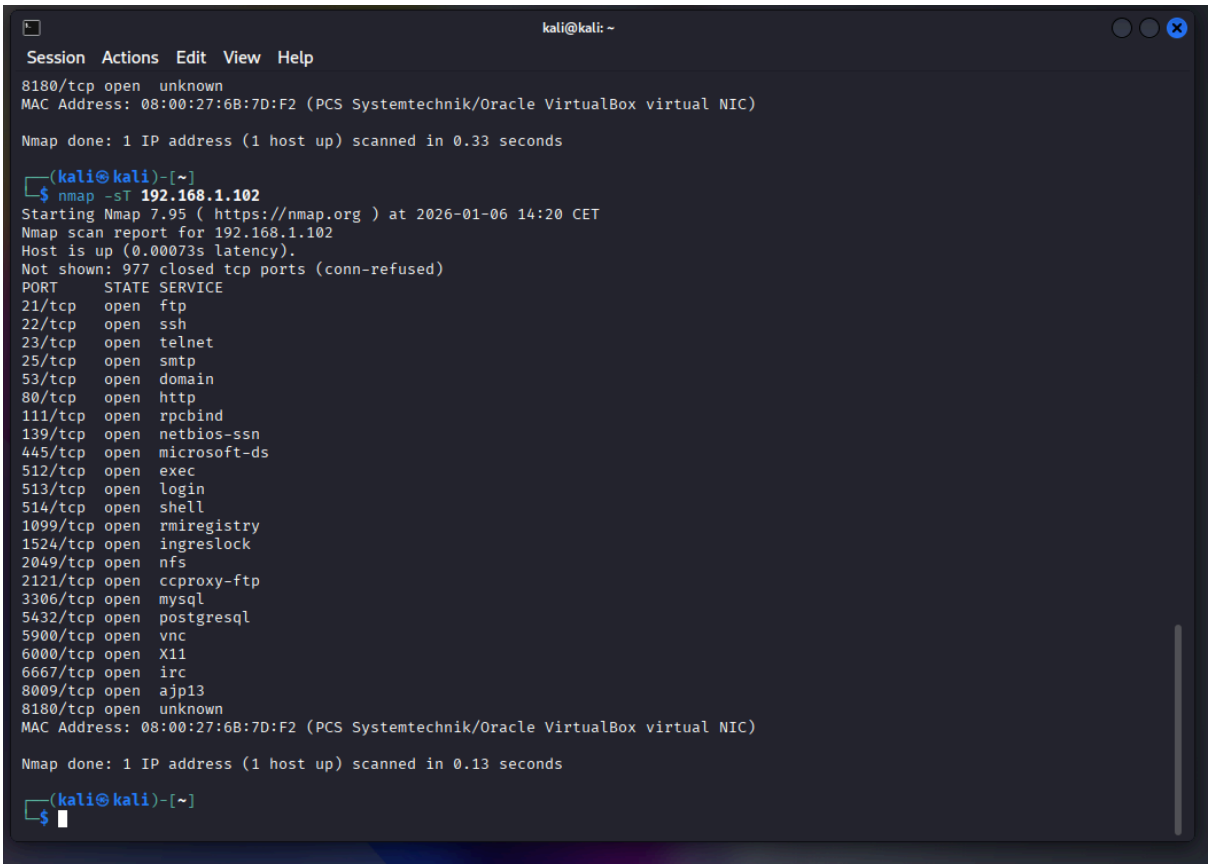

Come si può vedsere il **sistema operativo** della Meta è :

Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33

- **Syn Scan :**
  - Comando : nmap -sS 192.168.1.102



- **Tcp Connect :**
    - Comando : nmap -sT 192.168.1.102



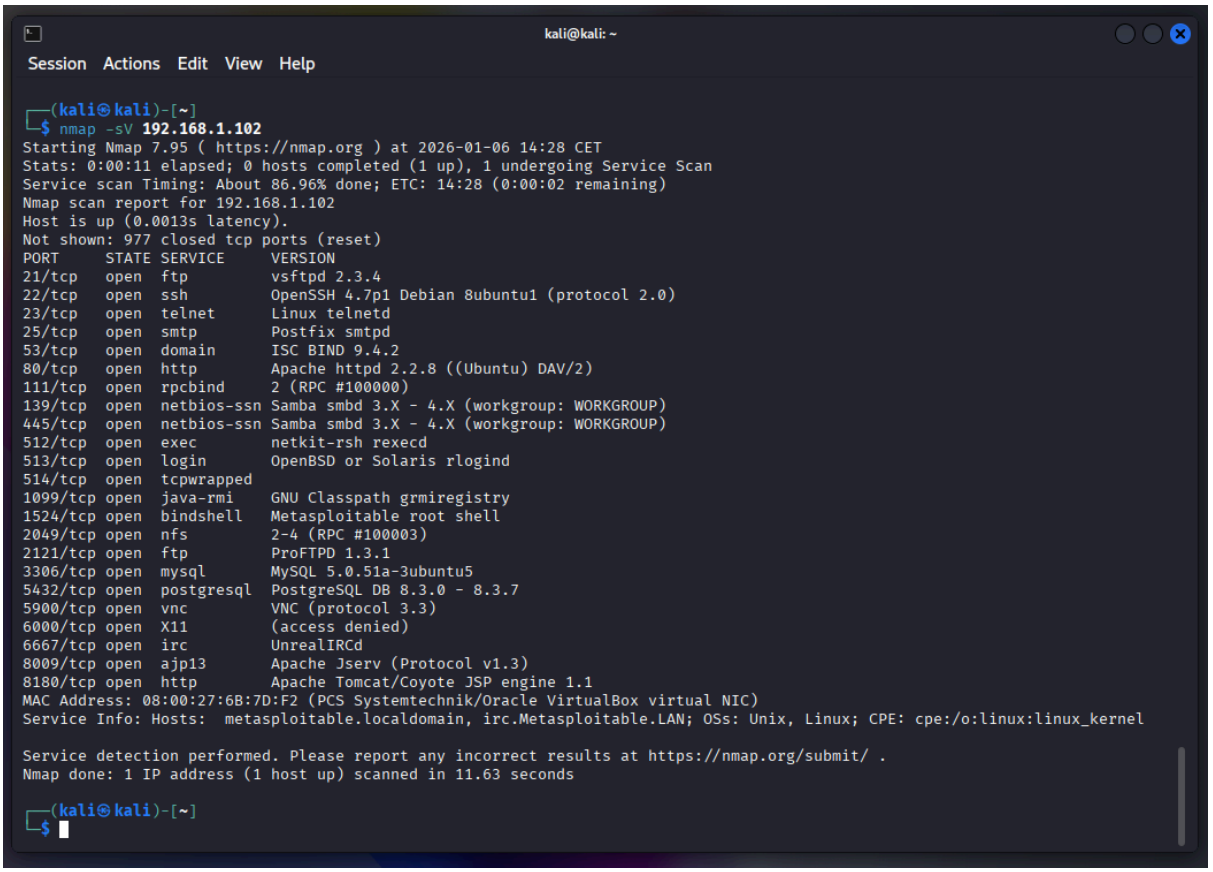

Differenza tra i due :

**Nessuna differenza** nella porte trovate aperte. L'unica differenza consiste nel metodo utilizzato per controllare la porta.

SYN Scan : reset

TCP Connect Scan : Conn-refused

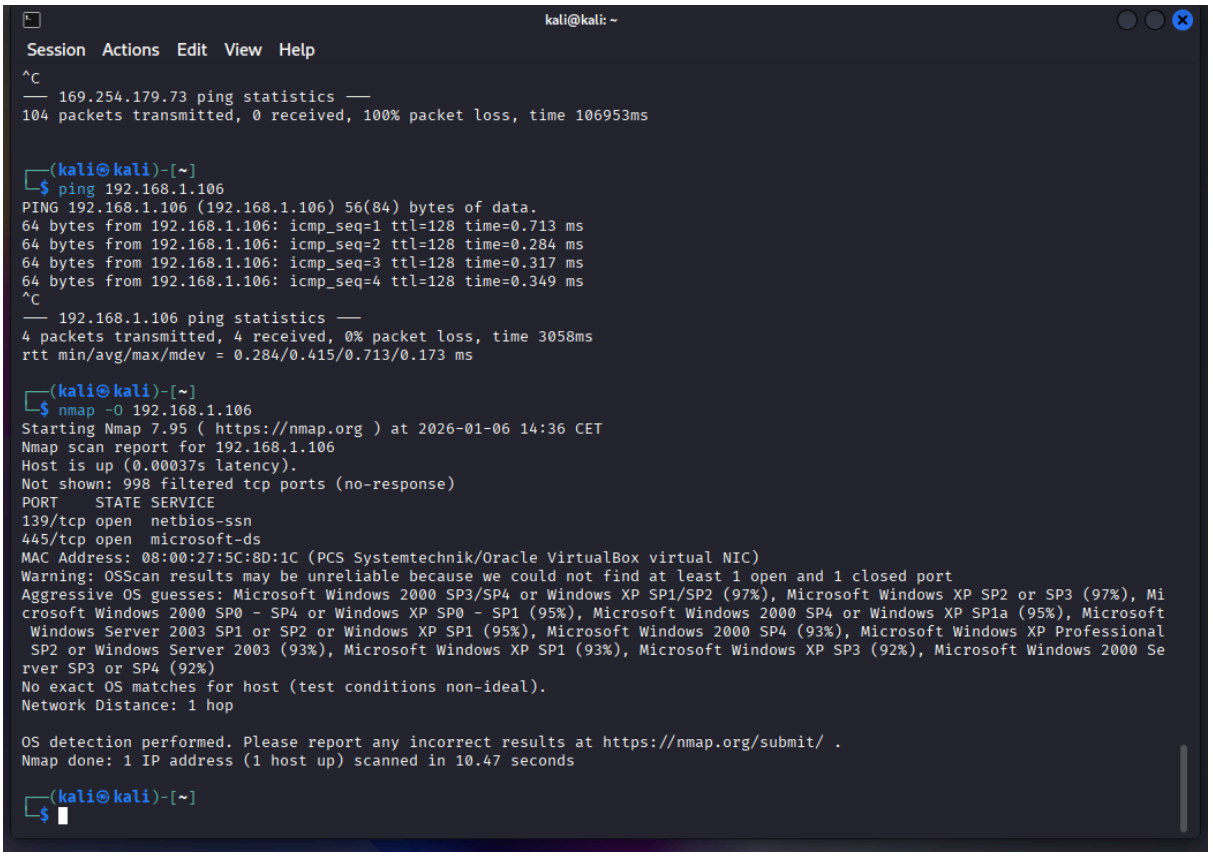
- **Version Detected**
  - Comando : nmap -sV 192.168.1.102

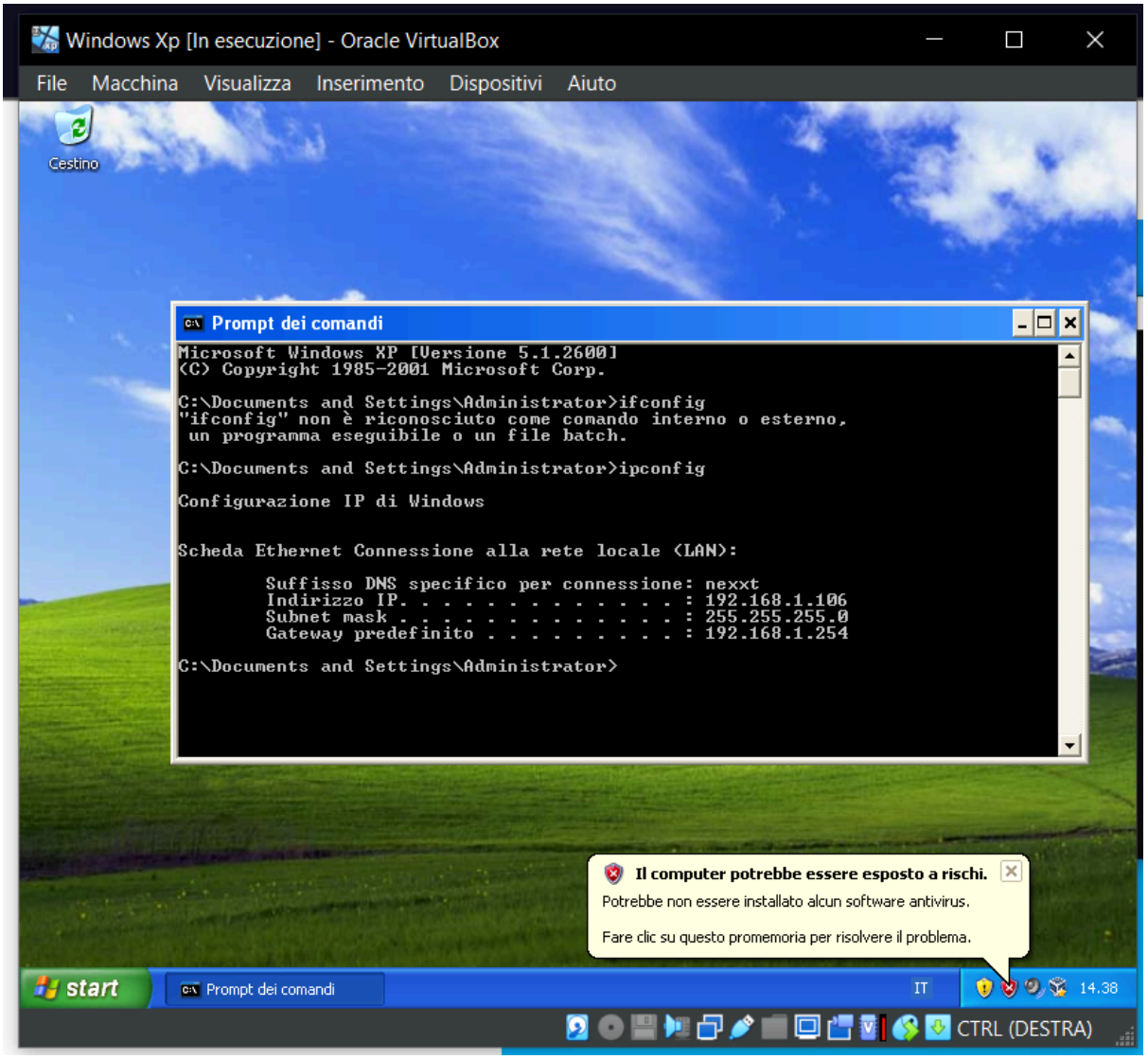


# Obbiettivo :

Si decide di raccogliere informazioni su un **target Windows XP** di **Ip 192.168.1.106**

- Os FingerPrint : determina il sistema operativo chè e in esecuzione sul target :
    - Comando : nmap -O 192.168.1.106






Indirizzo ip, Subnet Mask e Gateway predefonito della macchina Windows Xp