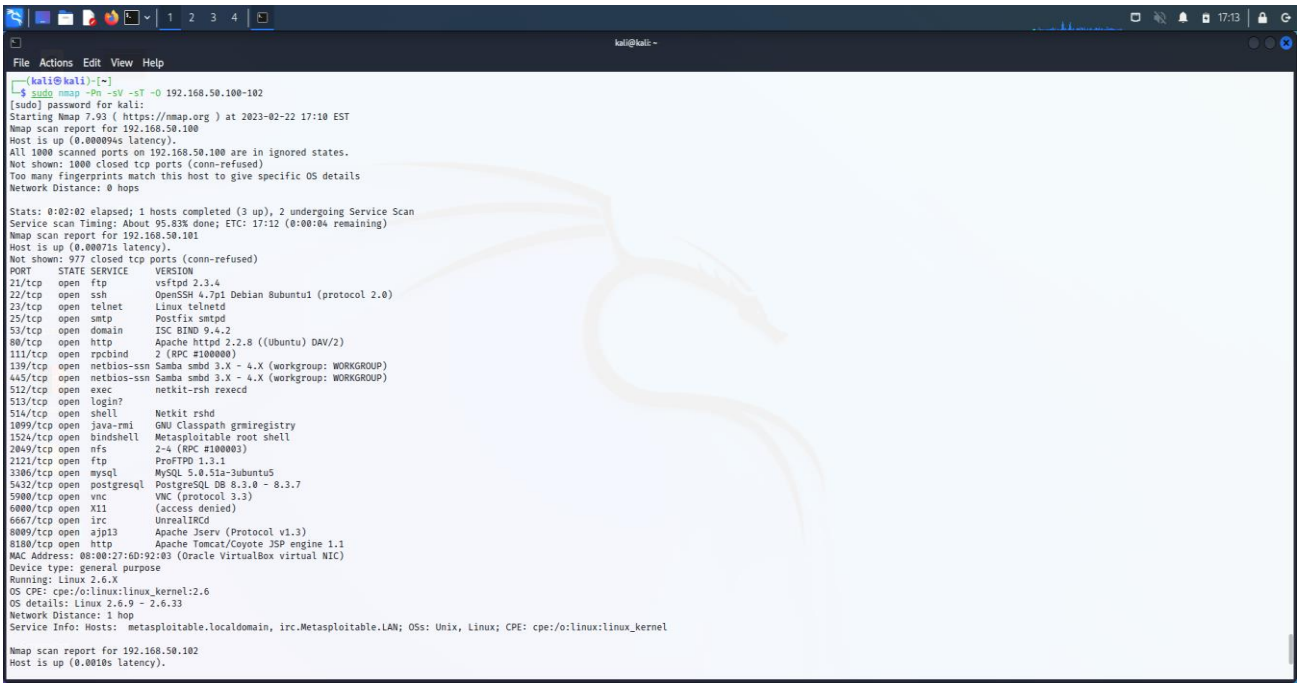
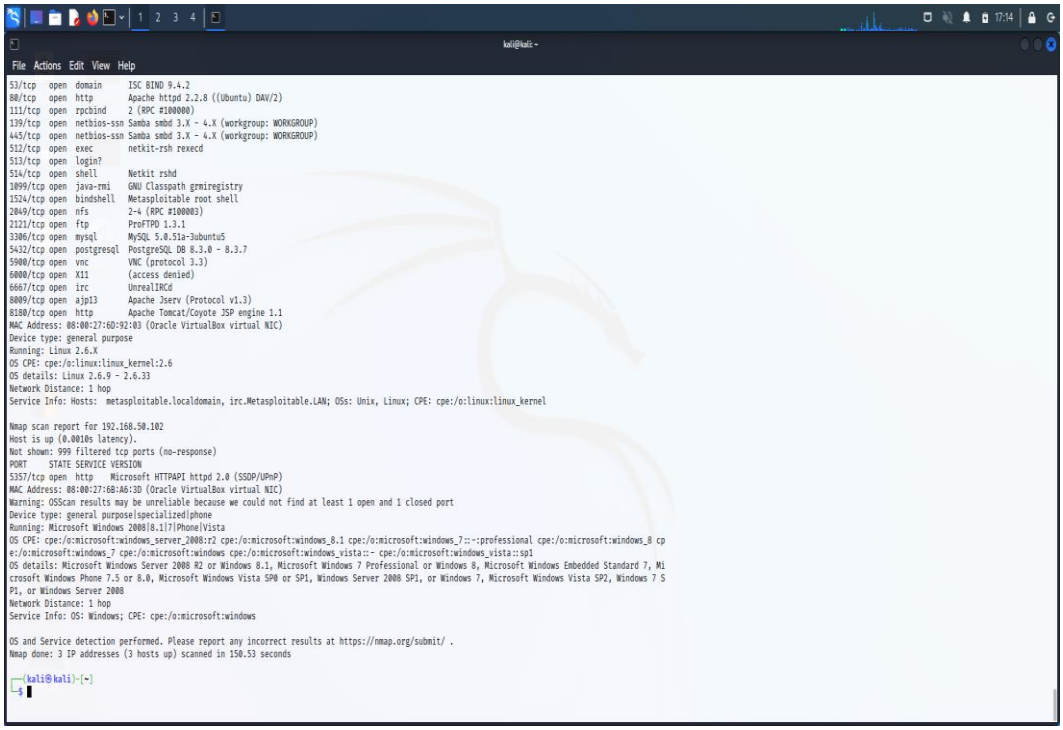
REPORT:

1) Effettuato un host discovery con il comando **fping 192.168.50.0/24** e trova 3 host attivi (ovvero le 3 macchine virtuali di KALI, META, WINDOW 7). A seguire con il comando nmap -sn 192.168.50.* trova solo 2 host attivi (KALI E META).
2) Per scansionare le porte di Windows 7 qualsiasi cmando di nmap mi dice che **host seems down**, mentre per Kali mi dice che lo stato delle porte è **ignored.**
3) Per poter scansionare anche le porte di windows ed eseguire un O.S fingerprint l'unico modo trovato è stato di inserire il comando -Pn, e tramite l'esecuzione seguente siamo riusciti a recuperare più informazioni possibili tramite un unico comando, eccetto per kali che continua a fornire come output che lo stato delle porte è "ignored":





Con il comando: **sudo nmap -Pn -sV -sT -O** riusciamo a trarre molte informazioni necessarie:

- Ip_address: 192.168.50.102 (windows 7) – 192.168.50.101 (metasplotable) – 192.168.50.100 (kali linux)
- Rileviamo le porte attive e i relativi servizi. Notiamo che su meta vi sono diverse porte attive, mentre su Windows ne ha trovata solo una (5357-open-http service)
- O.S: su meta abbiamo info abbastanza precise, con Linux 2.6 e service info indicate come metasploitable, mentre in windows essendoci una sola porta trovata i dettagli sul O.S non sono molto attendibili. Grazie al comando -sV abbiamo catturato il banner del servizio della porta trovata e deduciamo che il S.O è windows
- Su kali stesso invece abbiamo pochissime informazioni.