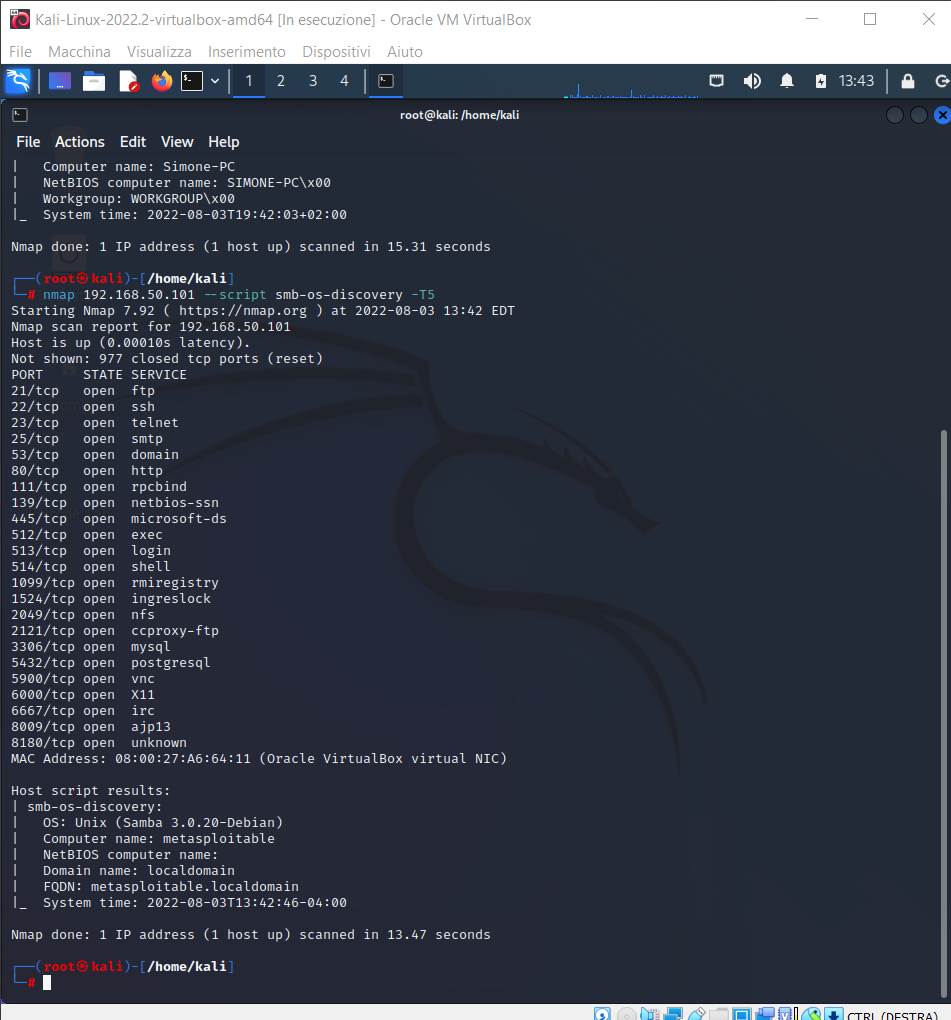
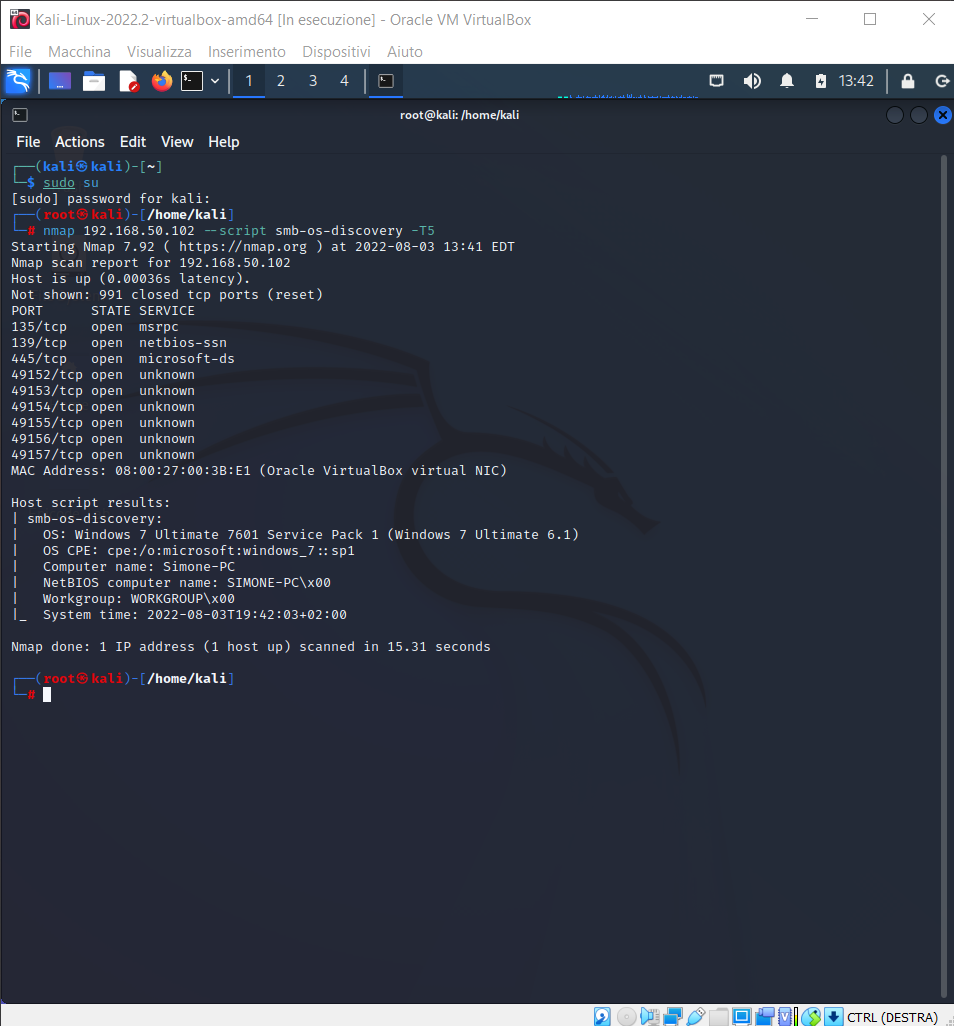
Report

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Target | IP | S.O. | Porte aperte | Versione servizi in ascolto |
| Metaspoitable | 192.168.50.101 | Unix (Samba 3.0.20-Debian) | 21,22,23,25,53,88,111,139,445,  512,513,514,1099,1524,2049,2121,  3306,5432,5900,6000,6667,8009,8180 | Vedere foto |
| Windows7 | 192.168.50.102 | Windows 7 Ultimate 7601 Service Pack 1 | 135,139,445,49152,49153,49154,49155,  49156,49157 | Vedere foto |

In questo report ho utilizzato i comandi di nmap v 7.92 per effettuare le scansioni e scoprire il Sistema Operativo, le porte aperte con i relativi servizi e versioni.

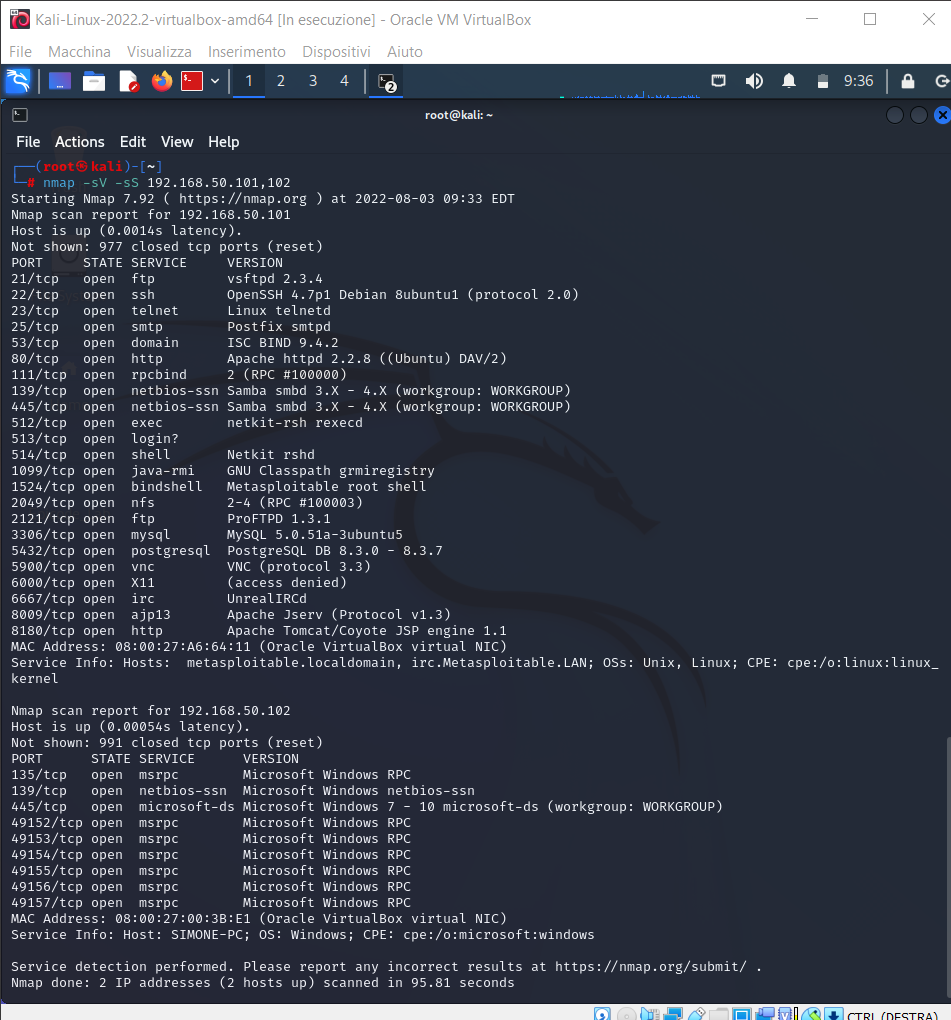
Script smb-os-discovery





Con questo comando possiamo vedere diverse informazioni tra cui il Sistema Operativo e le varie porte aperte. Windows 7 blocca questo comando grazie al firewall perciò ho dovuto attivare una regola per permettere la scansione.

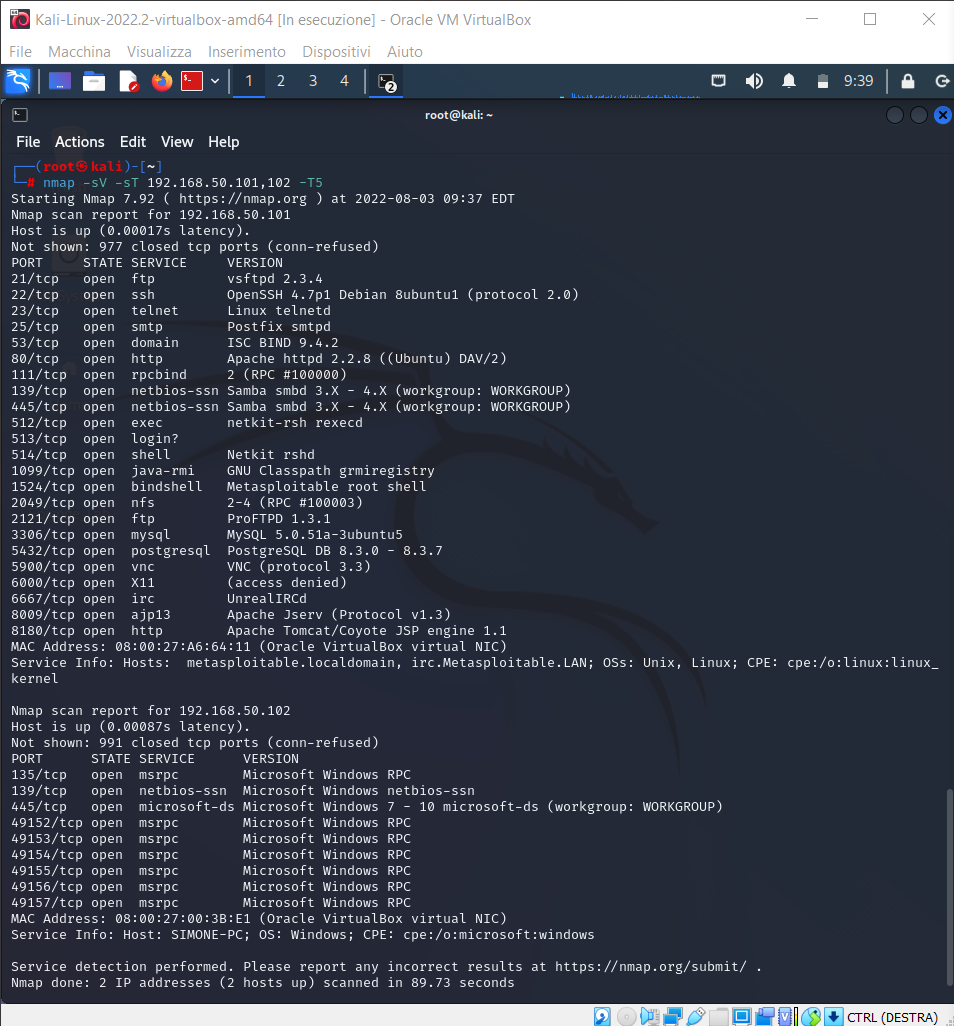
Scansione Syn Scan



Ho effettuato varie combinazioni con nmap per cercare la soluzione migliore, questa in foto è la Syn Scan di entrambe le macchine con l’aggiunta della specificazione dei servizi.

Questa scansione è meno aggressiva perché non termina la 3w hand shake e quindi genera meno rumore e quindi meno scopribile.

Scansione TCP



La seconda immagine riguarda la scansione TCP che non sembra mostrare alcune differenze con quella Syn Scan, anzi quella TCP ha impiegato anche meno tempo nonostante fosse più aggressiva, però genera più rumore e quindi più scopribile.