

SCANSIONI CON NMAP

SCANSIONE TCP:

Tramite il comando -sT si avvia una scansione TCP. Nello screenshot seguente si possono vedere le porte con relativo stato e servizio con accanto,

21/tcp(porta): ftp (servizio) = File Transfer Protocol, basato su architettura client/server, ed è un protocllo utilizzato per trasferire file tra computer su internet.

22/tcp: ssh= Secure Shell, protocollo che consente di stabilire una sessione remota con un altro host di una rete

25/tcp: smtp= Simple Mail Transfer Protocol, protocollo standard per la trasmissione di email.

53/tcp: domain = associa il nome di un dominio ad un indirizzio IP

80/tcp: http = HyperText Transfer Protocol, protocollo utilizzato per la trasmissione di informazioni sul web.

139/tcp netbios-ssn = Network Basic Input/Output System, solitamente riferito ad un’API per comunicazione sulla rete locale.

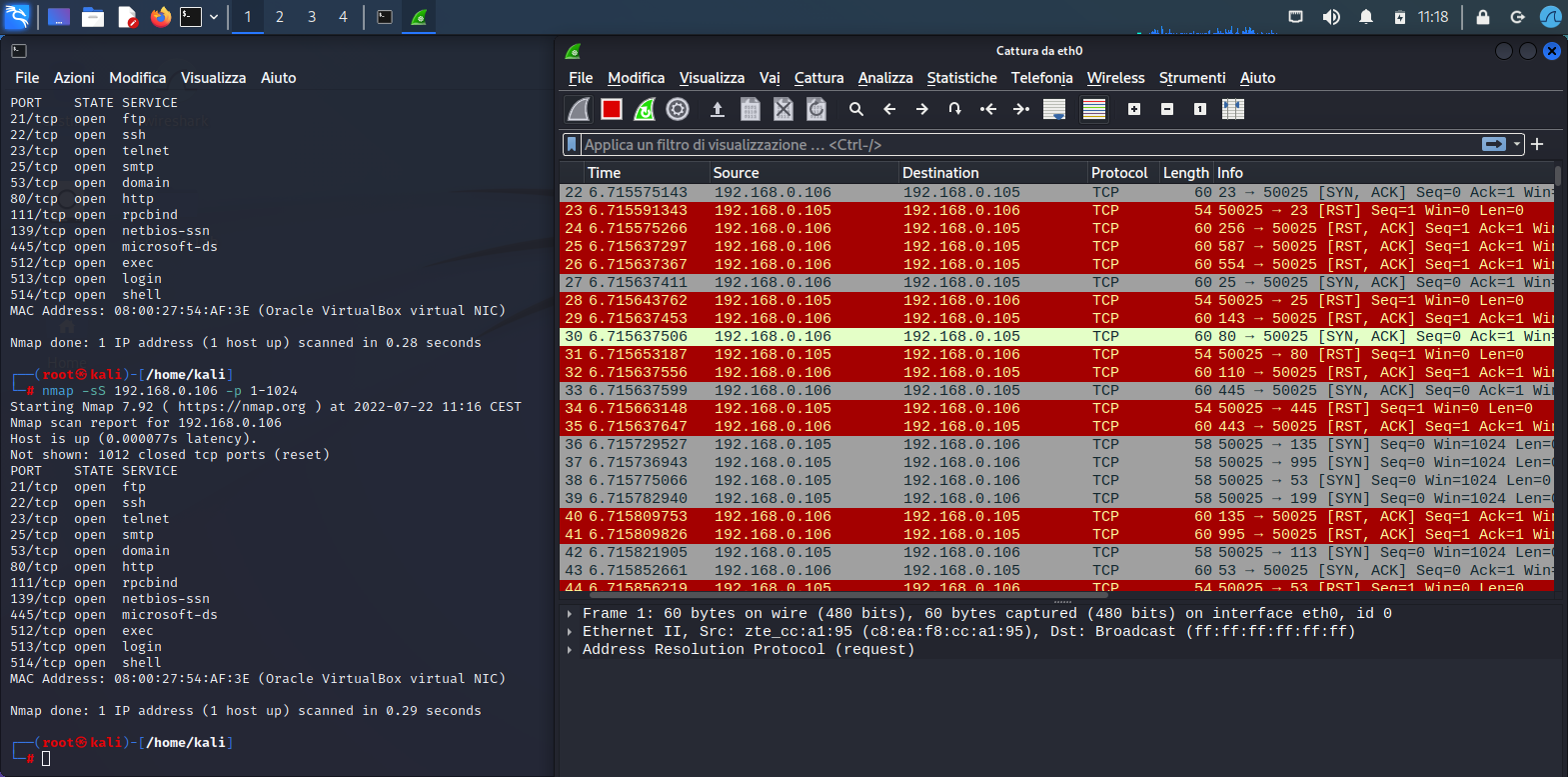
445/tcp Microsoft-ds, servizio che viene utilizzato per le risorse condivise smb(sever message block)

512/tcp exec= qui troviamo il servizio exec(Remote Execution Control) che viene utilizzato per eseguire un programma su un server remoto

513/tcp login= servizio login che veniva utilizzato per l’amministrazione da remoto, ma è stato rimpiazzato dal servizio SSH

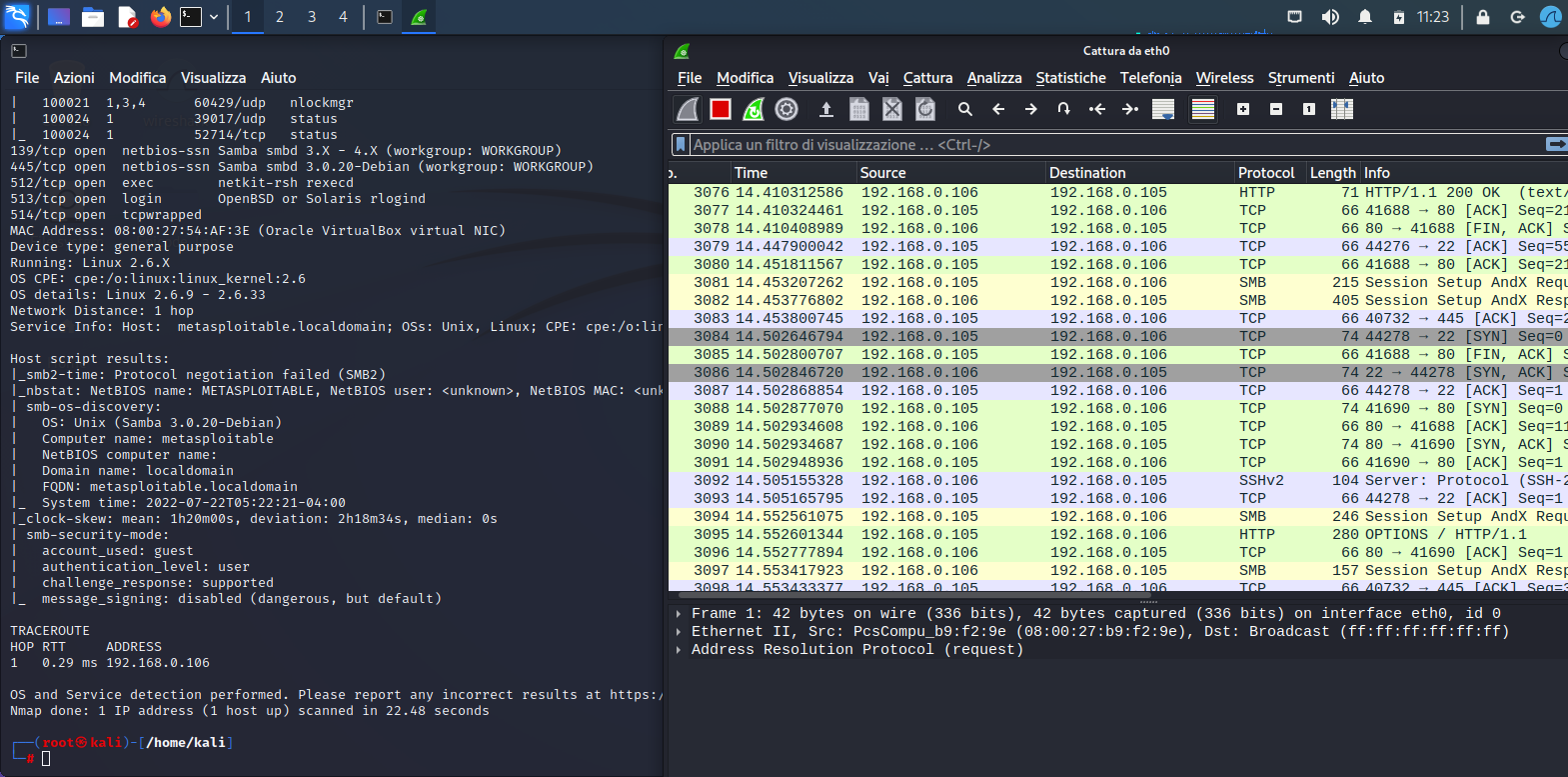
514/tcp shell= servizio per lo spoofing degli indirizzi IP.

Su wireshark possiamo anche vedere la cattura dei pacchetti tcp in rosso, in cui significa che negano la connessione per evitare di fare rumore dato che lo scan -sT è invasiva e completa il 3 way handshake, facendo molto rumore.



SCANSIONE SYN (-sS)

La scansione SYN è meno invasiva, Nmap non completa il 3 way handshake, ma chiude la comunicazoine inviando un pacchetto RST(reset). Tuttavia, recupera informazioni sullo stato della porta generando meno meno rumore e cosi definita come ‘’stealth scan’’



SCAN -A

Abilita la detenzione del sistema operativo, rivela la versione, scanning dello script e il traceroot. Uno scan molto dettagliato quanto molto aggressivo e Pericoloso, perché fa molto più rumore del TCP fornendo ogni singolo dettaglio.