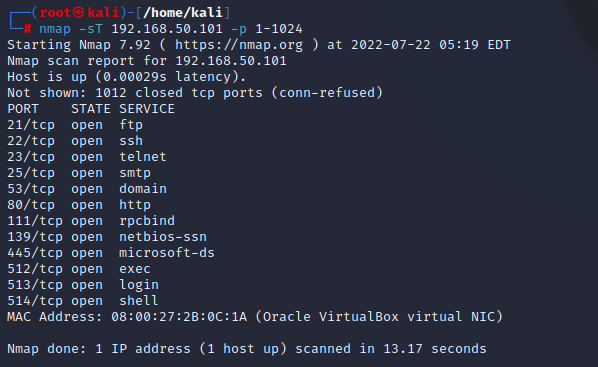
**SCANSIONI CON NMAP** (Fonte scan: Kali ; Target scan: Metasploitable)

Scansione TCP:



Tramite il parametro “-sT” stiamo facendo una scansione TCP. Nell’immagine si possono osservare le porte, con il relativo stato (le porte in questo caso sono tutte aperte) e servizio; i servizi delle porte sono:

21/tcp (porta) : ftp (servizio) → File Transfer Protocol, basato sull’architettura client/server, è un protocollo 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.

23/tcp : telnet → Terminal Network, protocollo di rete che tramite la shell fornisce all’utente sessioni di login remoto.

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 indirizzo IP.

80/tcp : htttp → HyperText Transfer Protocol, protocollo utilizzato per la trasmissione d’informazioni sul Web.

111/tcp : rpcbind → si occupa di convertire i numeri dei programmi RPC in indirizzi universali.

139/tcp : netbios-ssn → Network Basic Input/Output System, solitamente è riferito ad un’API per comunicazioni sulla rete locale.

445/tcp : microsoft-ds → servizio utilizzato per le risorse condivise in forma SMB, Service Message Block.

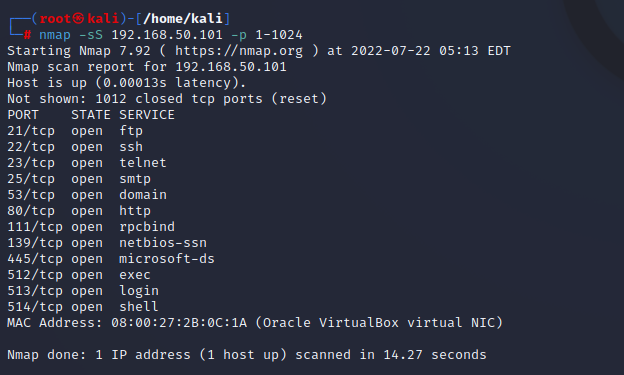
512/tcp : exec → Remote Execution Protocol, protocollo utilizzato per eseguire un programma su un server remoto.

513/tcp : login → utilizzato in passato per stabilire una sessione da remoto, ormai è sostituito dal protocollo SSH.

514/tcp : shell → utilizzato per lo spoofing degli indirizzi IP.

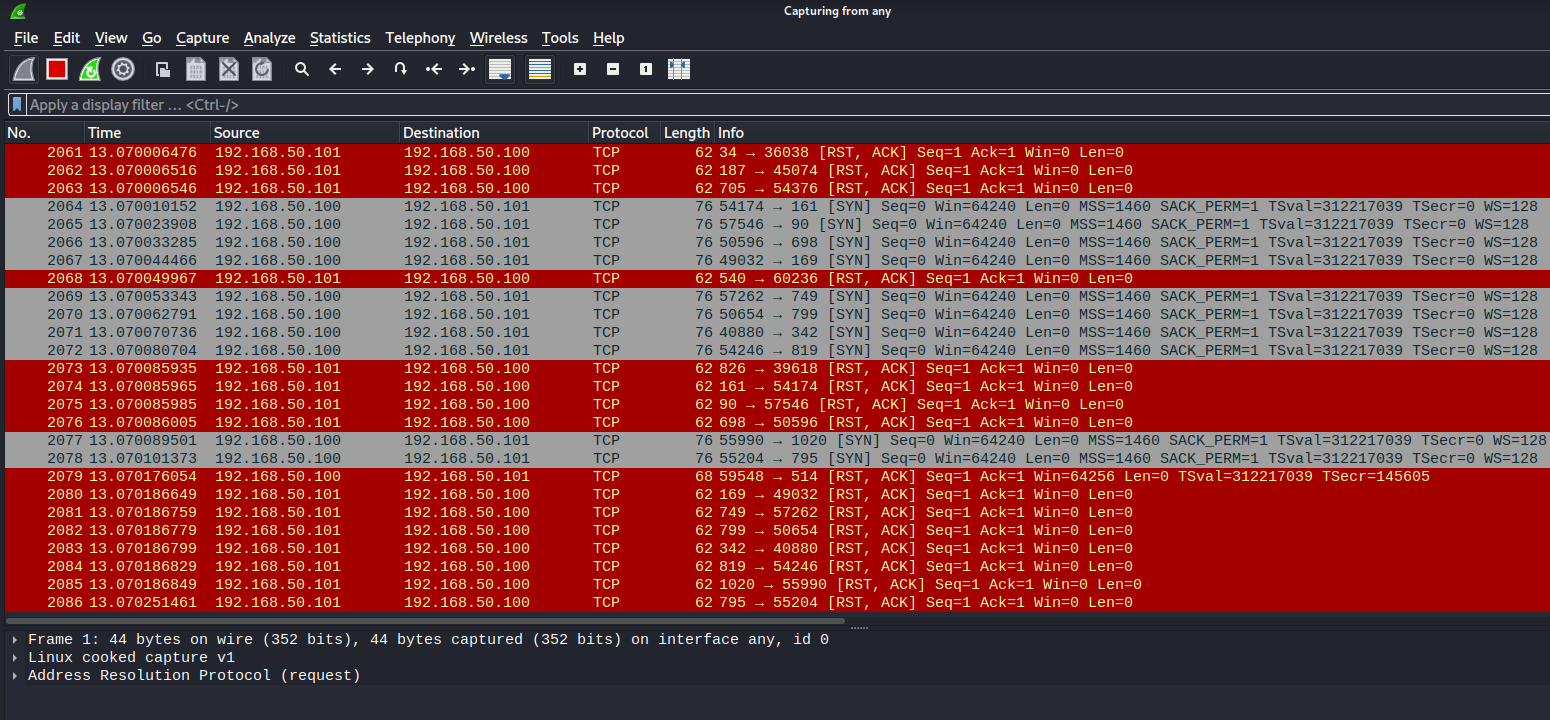
Mac Address: 08:00:27:2B:0C:1A (indirizzo fisico di metasploitable).

Scansione SYN:

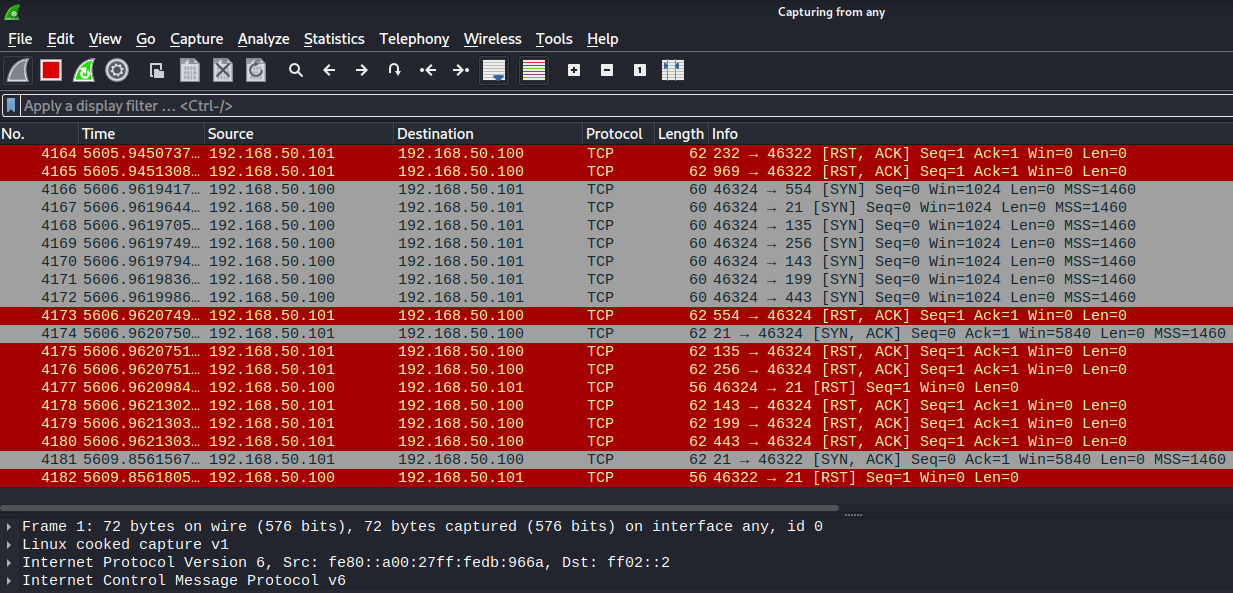


Tramite il parametro “-sS” stiamo facendo una scansione SYN. Nell’immagine si può osservare che le porte, gli stati ed i servizi sono i medesimi di quelli della scansione TCP.

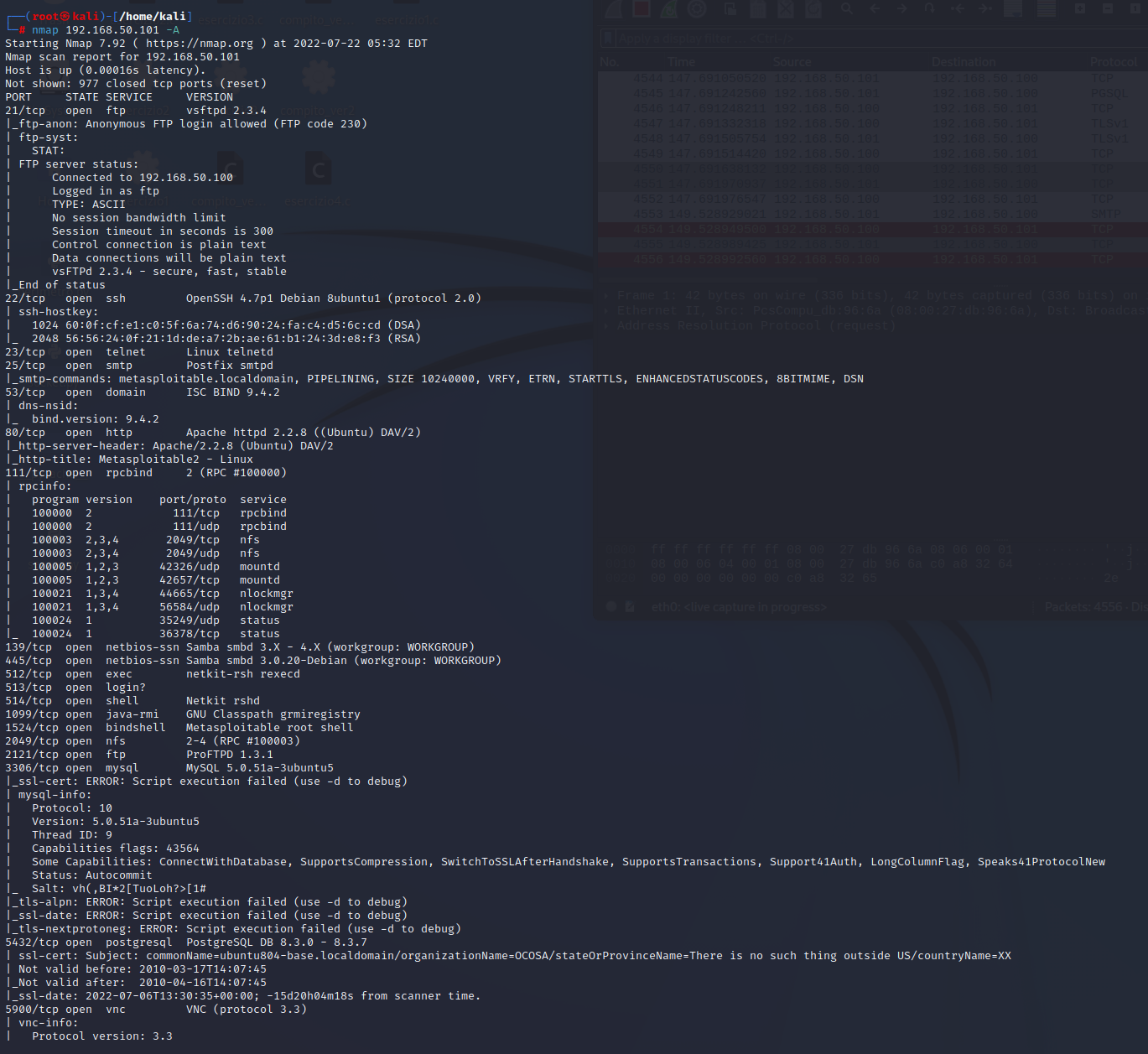
Scansione TCP in Wireshark:

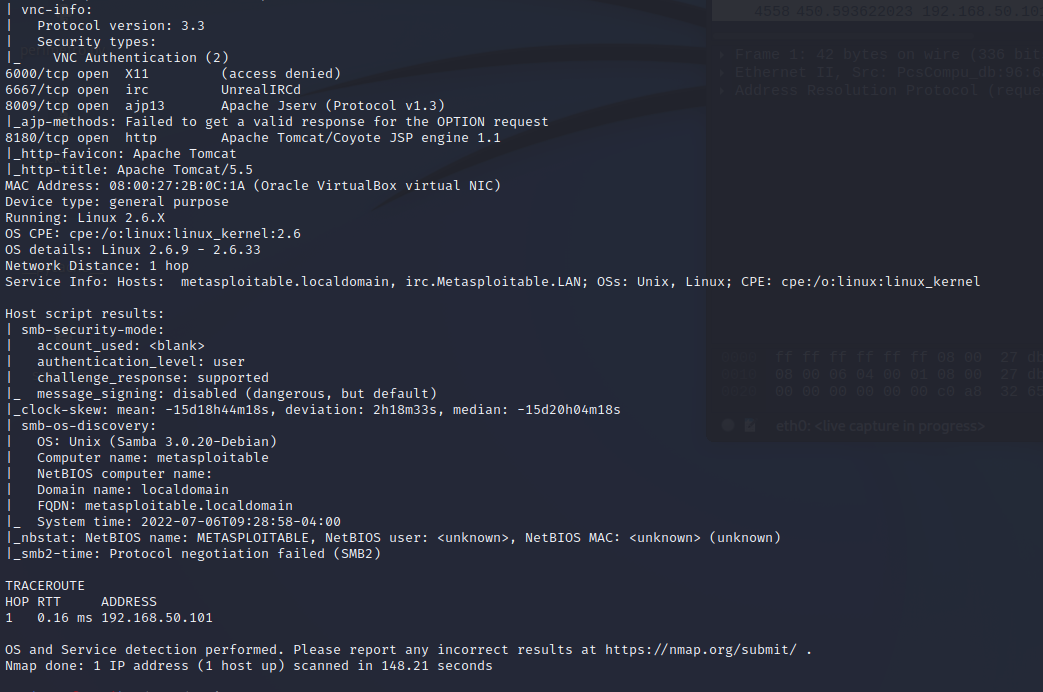


In Wireshark si può osservare il processo compiuto da Nmap, completando tutti i passaggi della 3-Way Handshake e stabilendo un vero e proprio canale. Nella scansione TCP si può notare come la risposta ACK faccia sì che la connessione venga chiusa, importante perché è quello che differenzia questa scansione dalle altre.

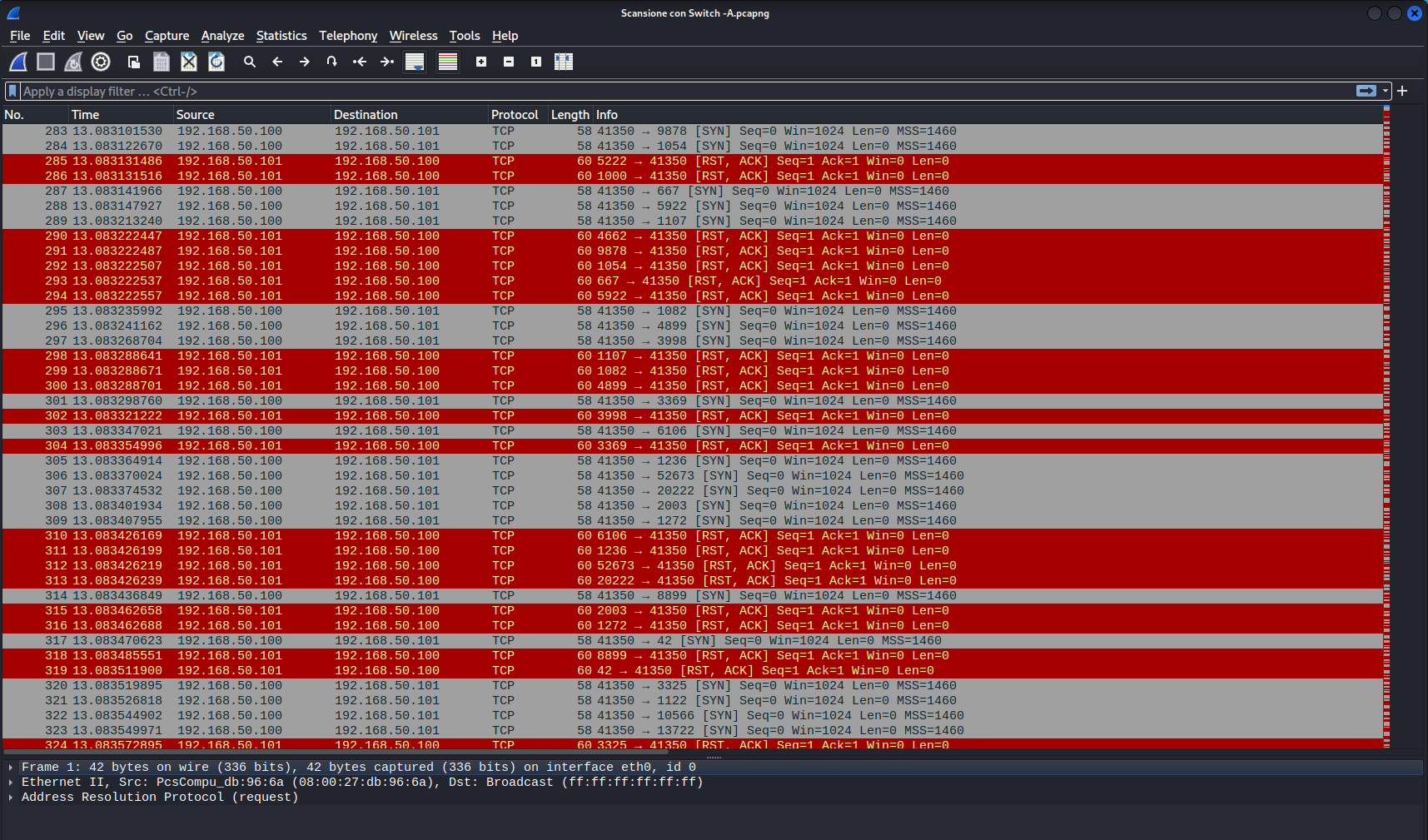
Scansione SYN in Wireshark:

In questo caso in wireshark si può vedere come la scansione SYN, a differenza della scansione TCP, non termini l’ultima fase della 3-Way Handshake; invece invia un pacchetto RST (reset) per chiudere la conversazione.

Scansione con Switch -A: 



La scansione di Nmap tramite -A, oltre ad identificare le porte, identifica il sistema operativo, la versione, fa lo scanning dello script e la traceroute.

Scansione con Switch -A in Wireshark: 

Differenze principali:

La differenza tra le tre scansioni è che nella scansione TCP, concludendo la 3-Way Handshake, genera “rumore” all’interno della rete perciò è più facile identificare questa tipologia di scansione piuttosto che la scansione SYN; dunque diversamente dalla scansione TCP, quella SYN permette di generare meno “rumore” grazie all’invio del pacchetto SYN. Infine la scansione con -A è la più aggressiva tra tutte, oltre ad essere quella più completa.