REPORT:

-Lo scanner è stato fatto da: Nmap 7.94SVN scan initiated Thu Jul 11 18:30:34 2024
-Il comando utilizato : nmap -sS -p 1-1024 -oG scan-sS.txt 192.168.50.101
-Il Hos che invia il pacchetto(source): 192.168.32.100
-Il host che riceve il pacchetto in stato attivo: Host: 192.168.50.101 () Status: Up
-Pkorte aperte e protocolli: Host: 192.168.50.101 () Ports: 53/open/tcp//domain///, 80/open/tcp//http///

-Chi, quando e hos a quale è stato fatto lo scan: Nmap done at Thu Jul 11 18:30:39 2024 -- 1 IP address (1 host up) scanned in 4.98 seconds.

Nel iimagini di wiresharek possiamo vedere informazioni piu dittagiata,

-sS (TCP SYN scan)
-sT (TCP connect scan)

-sS (TCP SYN scan) Il SYN scan è l'opzione di default ed è la più usata per buone ragioni. Può essere effettuato velocemente: effettua la scansione su migliaia di porte al secondo su una rete veloce non limitata da firewall restrittivi. Il SYN scan è relativamente nascosto e poco invasivo, poiché non completa mai le connessioni TCP. Funziona inoltre con ogni stack TCP compatibile e non dipende dai comportamenti particolari che possono avere pi piattaforme specifiche come fanno gli altri tipi di scan di Nmap quali FIN/NULL/Xmas, Maimon e Idle scan. Inoltre permette una differenziazione chiara ed affidabile tra le porte appartenenti agli stati open, closed e filtered.