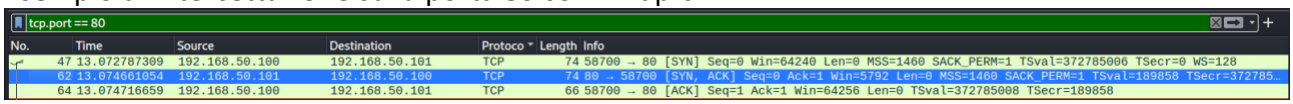
REPORT NMAP

FRANCESCO PERSICHETTI

Scansione nmap -sT

PORTA	FONTE	TARGET	TIPO DI SCAN	SERVIZIO
21	192.168.50.100	192.168.50.101	Nmap -sT	ftp
22	192.168.50.100	192.168.50.101	Nmap -sT	Ssh
23	192.168.50.100	192.168.50.101	Nmap -sT	telnet
25	192.168.50.100	192.168.50.101	Nmap -sT	Smtp
53	192.168.50.100	192.168.50.101	Nmap -sT	Domain
80	192.168.50.100	192.168.50.101	Nmap -sT	http
111	192.168.50.100	192.168.50.101	Nmap -sT	Rpcbind
139	192.168.50.100	192.168.50.101	Nmap -sT	Netbios-ssn
445	192.168.50.100	192.168.50.101	Nmap -sT	Microsoft-ds
512	192.168.50.100	192.168.50.101	Nmap -sT	Exec
513	192.168.50.100	192.168.50.101	Nmap -sT	Login
514	192.168.50.100	192.168.50.101	Nmap -sT	shell

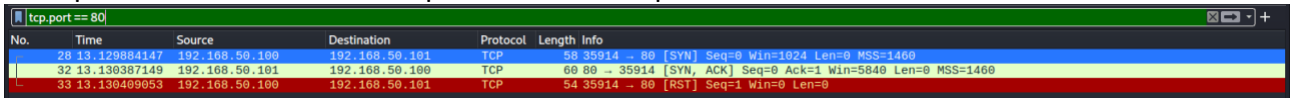
Esempio di intercettazione sulla porta 80 con nmap-sT



Scansione nmap -sS

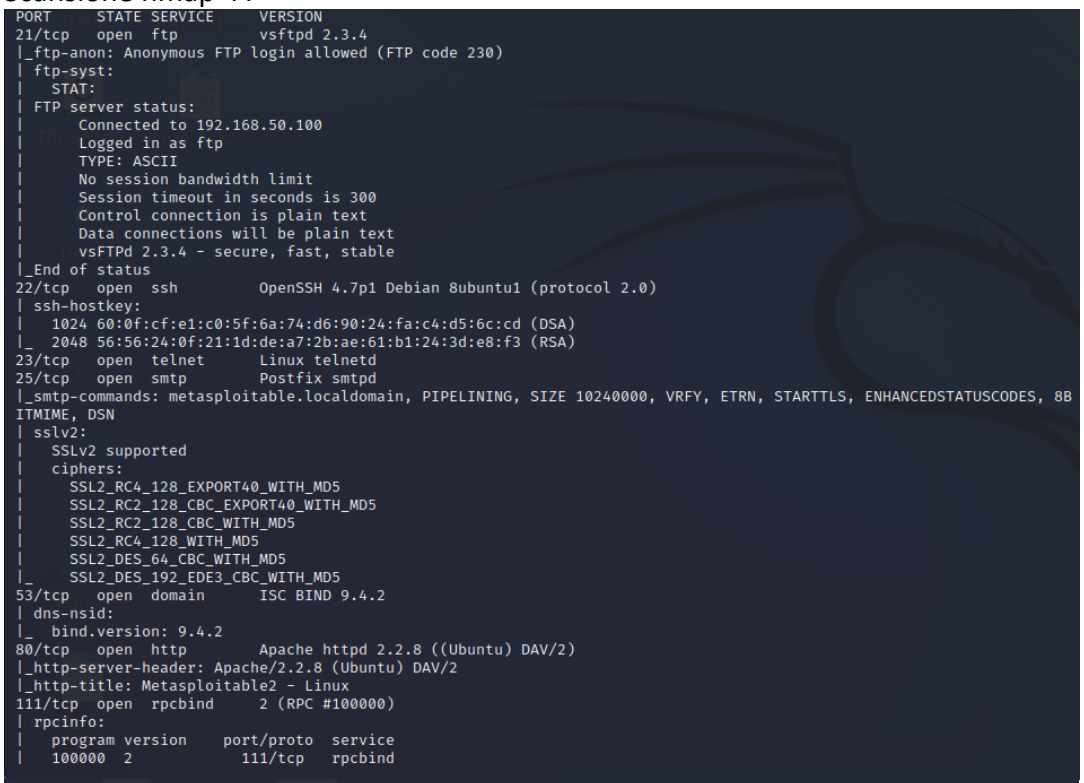
PORTA	FONTE	TARGET	TIPO DI SCAN	SERVIZIO
21	192.168.50.100	192.168.50.101	Nmap -sS	ftp
22	192.168.50.100	192.168.50.101	Nmap -sS	Ssh
23	192.168.50.100	192.168.50.101	Nmap -sS	telnet
25	192.168.50.100	192.168.50.101	Nmap -sS	Smtp
53	192.168.50.100	192.168.50.101	Nmap -sS	Domain
80	192.168.50.100	192.168.50.101	Nmap -sS	http
111	192.168.50.100	192.168.50.101	Nmap -sS	Rpcbind
139	192.168.50.100	192.168.50.101	Nmap -sS	Netbios-ssn
445	192.168.50.100	192.168.50.101	Nmap -sS	Microsoft-ds
512	192.168.50.100	192.168.50.101	Nmap -sS	Exec
513	192.168.50.100	192.168.50.101	Nmap -sS	Login
514	192.168.50.100	192.168.50.101	Nmap -sS	shell

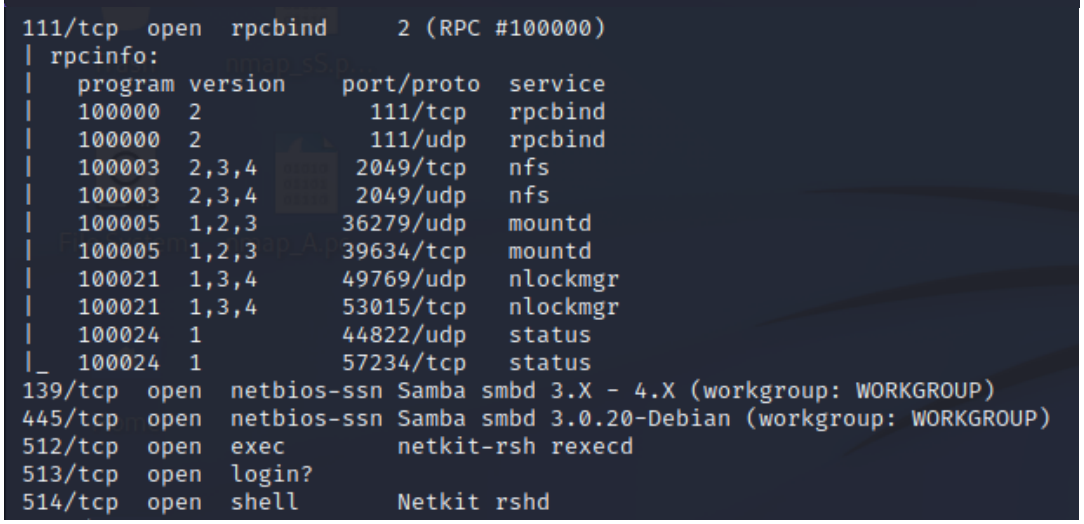
Esempio di intercettazione sulla porta 80 con nmap-sS



La differenza principale che si può notare dalle due scansioni è che con “nmap -sT” (che è più invasiva) la scansione completa la 3-way-handshake creando così la connessione. Mentre nella scansione “nmap -sS” (meno invasiva) non completa la connessione e chiude la comunicazione con un pacchetto di reset (RST)

Scansione nmap -A





A differenza delle altre scansioni, la scansione “nmap-A” fa una scansione più ampia prendendo molte altre informazioni come, per esempio, la versione del servizio. Rispetto alle altre due però è molto più lungo come procedimento proprio perché intercetta molte più cose.