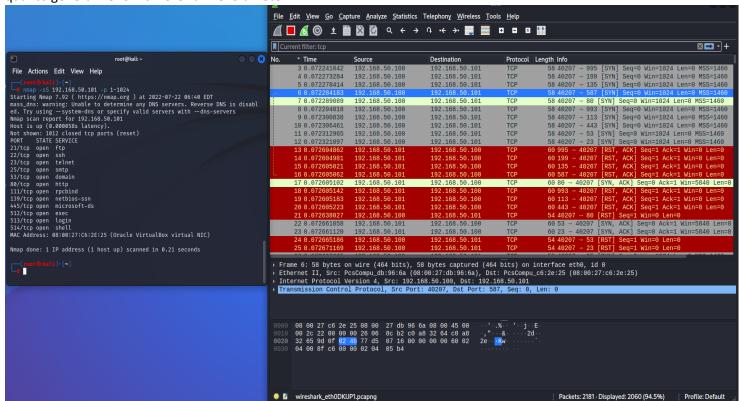
Progetto della settimana su nmap

La differenza principale tra le due scansioni è che il metodo SYN ci mostra solo se le porte sono aperte senza creare rumore e dunque di difficile rintracciamento, invece la scansione TCP essendo completa cioè che esegue il 3 way handshake crea piu rumore ma crea anche un canale di comunicazione.

Nel primo scan che andremo a fare useremo il metodo

-sS: questo metodo è meno invasivo rispetto ad sT. Con questo metodo Nmap non completa il 3-way-handshake, ma chiude la comunicazione inviando un pacchetto RST(reset). Tuttavia , riesce a recuperare informazioni sullo stato della porta. Utile in quanto genera meno "rumore" a livello di rete.



A sinistra dopo aver scritto il comando nmap, osserviamo le porte e il loro stato(in questo caso sono tutte aperte).

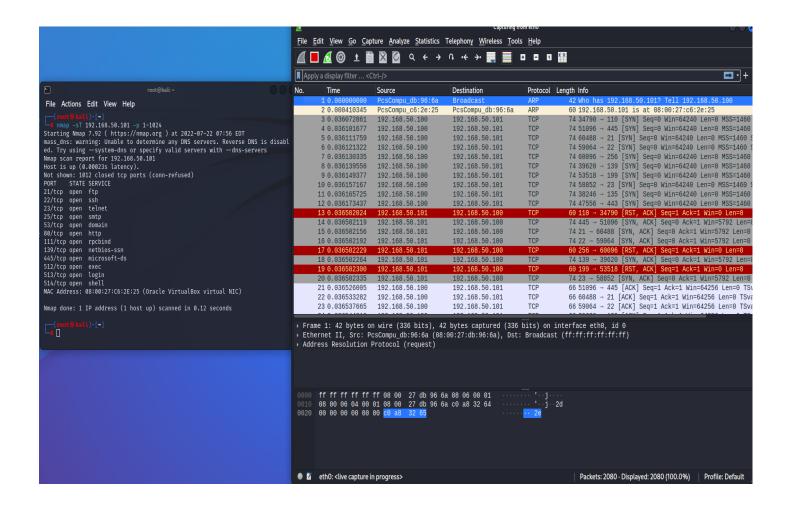
Una breve descrizione dei servizi:

- **ftp**: la sigla sta per "file transfer protocol". Indica il protocollo che si usa per trasferire i file verso un server e viceversa ,uno dei protocolli più usati sono HTTP e HTTPS che usiamo per richiamare i siti web.
- Ssh: è l'acronimo di Secure Socket Shell, definizione usata per indicare un protocollo che fornisce agli amministratori di rete un modo sicuro per accedere a un computer remoto.
- **Telnet**: è un protocollo di rete, utilizzato tramite interfaccia a riga di comando per fornire all'utente sessioni di login remoto.
- **Smtp**: "protocollo semplice di trasferimento di posta". L'SMTP è specificamente responsabile dell'invio e dell'inoltro di e-mail da un mittente a un destinatario.
- Domain: associa il nome di un dominio ad un indirizzo IP.
- http: è un linguaggio di testo che consente la comunicazione tra client e server attraverso internet.
- Netbioss-ssn: è l'acronimo di Network basic input output system ed è utilizzato in Windows per la condivisione di file e stampanti.
- Exect: sostituisce l'intero contenuto corrente del processo con un nuovo programma.
- Login: è la procedura di identificazione che permette di essere riconosciuti da un'applicazione.

1

• Shell: La shell è l'interprete dei comandi di un sistema operativo.

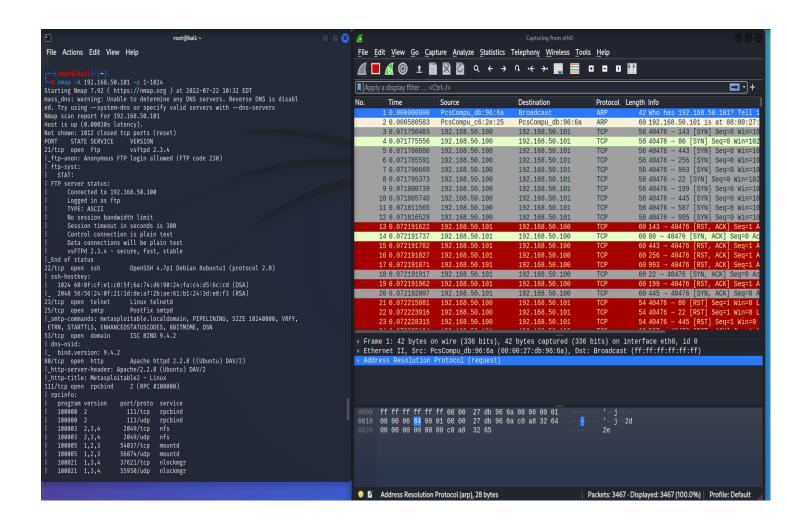
-sT: il seguente scan che facciamo è il metodo piu invasivo perché completa il passaggio 3way handshake, cioè controlla se una port e aperta o meno e recupera informazioni sul servizio in ascolto stabilendo un canale.



Anche in questo caso osserviamo che quasi tutte le porte sono aperte.

Osserviamo che alla riga 20 ci è data la risposta SYN/ACK che sta a dire che sta a dire che la porta è aperta.

In questo terzo caso invece utilizzando lo scan –A osserviamo che è molto più aggressivo e invasiva rispetto agli altri due perché stabilisce una connessione completa e identifica la versione del servizio attivo su quella determinata porta, scannerizza lo script, il sitema OS e la sua versione in uso



```
root@kali: ~
   File Actions Edit View Help
          100000 2
100000 2,3,4
100003 2,3,4
100005 1,2,3
100005 1,2,3
100021 1,3,4
100021 1,3,4
100024 1
100024 1
7tcp open netb
                                                     111/udp
2049/tcp
2049/udp
54037/tcp
56874/udp
37621/tcp
                                                                                nfs
nfs
                                                                                 mountd
                                                                                mountd
nlockmgr
513/tcp open login?
514/tcp open shell Netkit rshd
MAC Address: 08:00:27:C6:2E:25 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
 OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
 Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
  Host script results:
   Host script results:
| smb-os-discovery:
| OS: Unix (Samba 3.0.20-Debian)
| Computer name: metasploitable
| NetBIOS computer name:
| Domain name: localdomain
| FQDN: metasploitable.localdomain
| FQDN: time: 2022-07-22T10:33:31-04:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 2h00m03s, deviation: 2h49m43s, median: 2s
| smb-security-mode:
| account_used: guest
         account_used: guest
authentication_level: user
  | challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC:
<unknown> (unknown)
 HOP RTT ADDRESS
1 0.30 ms 192.168.50.101
                          ADDRESS
 OS and Service detection performed. Please report any incorrect results at ht tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 75.28 seconds
```