PRATICA S5-L3: Tecniche di scansione con Nmap

1. Si richiede allo studente di effettuare le seguenti scansioni sul **target Metasploitable**:

   -OS fingerprint Syn
   -Scan TCP connect - trovate differenze tra i risultati della scansioni TCP connect e SYN?
   -Version detection

   E le seguenti sul **target Windows 7**:
   OS fingerprint .

   Modificate le impostazioni di rete delle macchine virtuali per fare in modo che i due target siano sulla stessa rete.
2. A valle delle scansioni, per entrambi gli IP, è prevista la produzione di un **report** contenente le seguenti info (dove disponibili):

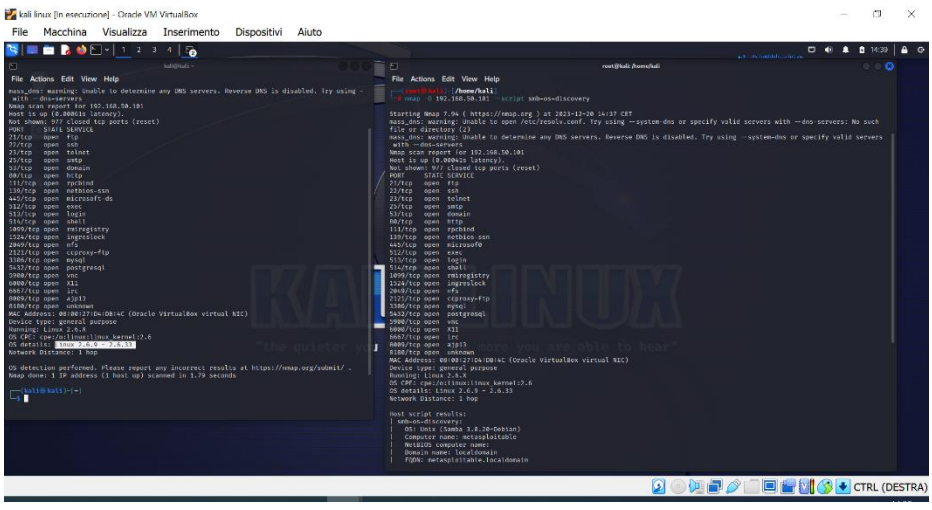
   -IP
   -Sistema Operativo
   -Porte Aperte
   -Servizi in ascolto con versione

3. Quesito extra (al completamento dei quesiti sopra):

   Quale potrebbe essere una valida ragione per spiegare il risultato ottenuto dalla scansione sulla macchina Windows 7? Che tipo di soluzione potreste proporre per continuare le scansioni?

1) Scansioni Nmap sul target **Metaspoitable** (da Kali)

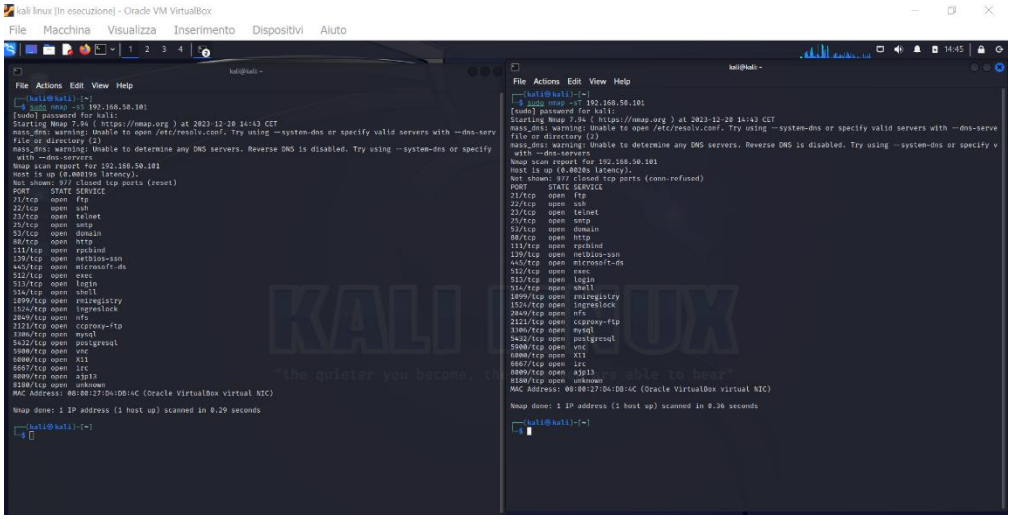
- ***Os fingerprinting***: processo di identificazione del sistema operativo su una rete.
  Il 1° comando (sudo nmap 192.168.50.101) e il 2°comando (sudo nmap -O 192.168.50.101) scansionando Meta, restituiscono entrambi:
  l'IP 192.168.50.101
  Sistema operativo: Linux 2.6.X fornendo il range 2.6.9 – 2.6.33
  La differenza sta nel fatto che con il secondo comando si ottengono più informazioni sull'OS (trai quali il tipo de sistema informativo Unix (Samba 3.0.20-Debian)



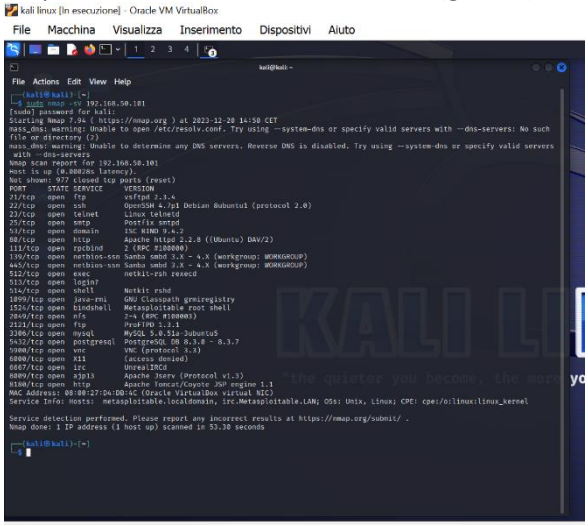
[Port scanning= processo per capire quali porte (TCP e UDP) sono aperte su un host al fine di rilevare i servizi in ascolto - varie tecniche offerte di scansione]

- ***Syn scan:*** anche detta Stealth scan (scansione furtiva) in quanto metodo di scansione *meno invasivo* rispetto ad sT. Infatti, Nmap, una volta ricevuto il pacchetto SYN/ACK dalla macchina target, *non conclude il 3-way-handshake*, ma appurato che la porta è aperta chiude la comunicazione, di fatto evitando overload dato dalla creazione del canale. In sostanza, non si stabilisce una connessione completa con il demone target e viene *inviato solo il pacchetto iniziale SYN* e si *chiude* la comunicazione inviando *un pacchetto RST (**Reset**, come da grafico)*.

- ***Scan TCP connect:*** è il metodo di scansione *più invasivo*, in quanto, per controllare se una porta è aperta o meno e recuperare informazioni sul servizio in ascolto, nmap *completa* tutti i passaggi del *3-way-handshake*, stabilendo di fatto un canale comunicativo**.** In sostanza, stabilisce una connessione con il demone del servizio in ascolto, completando il three-way-handshake.



- ***Version Detection:*** è a tutti gli effetti una *scansione TCP connect* con l'aggiunta di specifici test per la rilevazione dei servizi in ascolto su una porta. Così come la scansione TCP connect, è piuttosto facile da rilevare in quanto genera molto traffico di rete. Durante una scansione version detection, nmap esegue prima una TCP connect e poi recupera *informazioni circa il servizio in ascolto* dal banner del demone, in particolare la versione dei servizi (grafico).

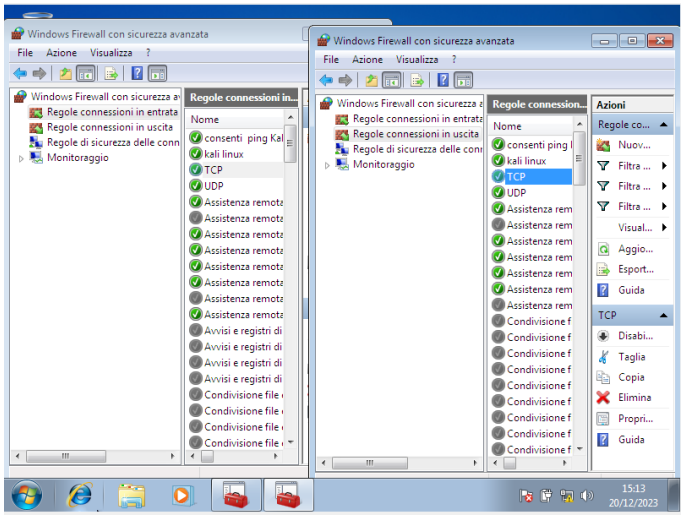


1) Scansioni Nmap sul target **Windows 7**

Il tentativo di Fingerprinting per identificare il sistema operativo si Windows non è riuscito.

3) **Ragione risultato della scansione su Windows e soluzioni per continuare scansioni:**

La ragione dei risultati della scansione su Windows 7 è dipeso dalla presenza del ***firewall*** che blocca la connessione tramite TCP e UDP necessarie per la comunicazione con la macchina Kali, e di conseguenza con il Port scanning.
La soluzione consiste nel creare ***nuove regole nel policy set***, sia in ***entrata*** che in ***uscita***, che consentano la connessione tramite protocolli ***TCP*** e ***UDP***, come in grafico.



2) **Report** sui due indirizzi IP, Meta e Windows, dove possibile:

- Metasploitable

  IP: 192.168.50.101
  Os: Linux 2.6.X; Unix (Samba 3.0.20-Debian)
  Porte aperte: 21-23, 25, 53, 80, 111, 139, 445, 512-514, 1099, 1524, 2049, 2121, 3306, 5432, 5900, 6000, 6667, 8009.

Servizi in Ascolto: ftp, ssh, telnet, smtp, domain, http, rpcbind, netbios-ssn, microsof0, exec, login, shell, rmiregistry, ingreslock, nfs, ccproxy-ftp, mysql, postgresql, vnc, X11, irc, ajp13,

- Windows 7: impossibile acquisire informazioni su sistemi operativi, porte e servizi.