

## 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):

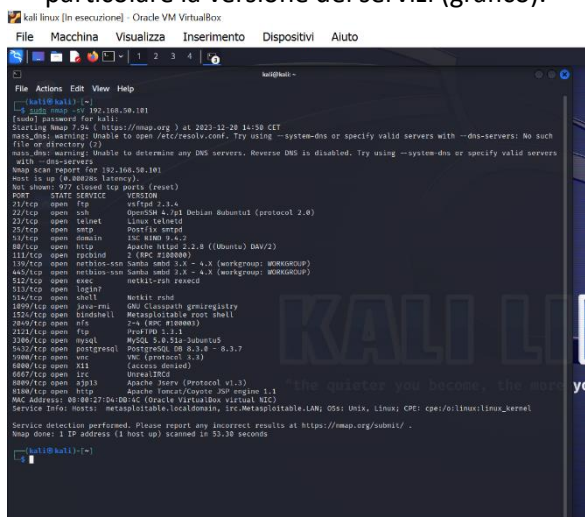
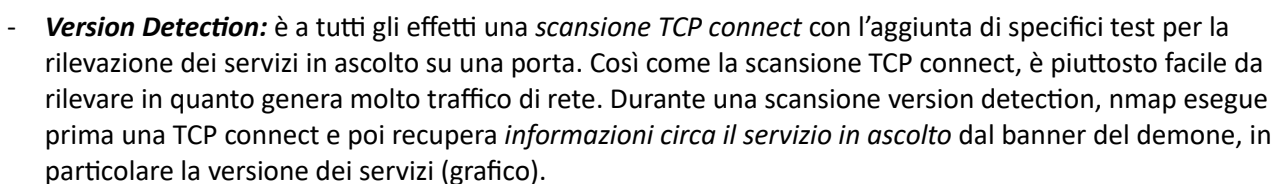
Quale potrebbe essere una valida ragione per spiegare il risultato ottenuto dalla scansione sulla macchina Windows 7? Che tipo di soluzione potreste proporre per continuare le scansioni?

### 1) Scansioni Nmap sul target **Metasploitable** (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 (tra i quali il tipo di sistema informativo Unix (Samba 3.0.20-Debian))

```
root@kali:~/metasploit# nmap -O 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 14:37 CET
nmap: Warning: Unable to open /etc/hosts.conf, try using --system-dns or specify valid servers with --dns-servers: No such file or directory (2)
nmap: Warning: Unable to determine any DNS servers, Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.101
Host is up (0.0000s latency).
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  dns
80/tcp    open  http
111/tcp   open  rpcbind
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
143/tcp   open  imap
312/tcp   open  tcpwrapped
313/tcp   open  tcpwrapped
514/tcp   open  shell
543/tcp   open  msrpc
554/tcp   open  msrpc
562/tcp   open  msrpc
563/tcp   open  msrpc
564/tcp   open  msrpc
565/tcp   open  msrpc
566/tcp   open  msrpc
567/tcp   open  msrpc
568/tcp   open  msrpc
569/tcp   open  msrpc
570/tcp   open  msrpc
571/tcp   open  msrpc
572/tcp   open  msrpc
573/tcp   open  msrpc
574/tcp   open  msrpc
575/tcp   open  msrpc
576/tcp   open  msrpc
577/tcp   open  msrpc
578/tcp   open  msrpc
579/tcp   open  msrpc
580/tcp   open  msrpc
581/tcp   open  msrpc
582/tcp   open  msrpc
583/tcp   open  msrpc
584/tcp   open  msrpc
585/tcp   open  msrpc
586/tcp   open  msrpc
587/tcp   open  msrpc
588/tcp   open  msrpc
589/tcp   open  msrpc
590/tcp   open  msrpc
591/tcp   open  msrpc
592/tcp   open  msrpc
593/tcp   open  msrpc
594/tcp   open  msrpc
595/tcp   open  msrpc
596/tcp   open  msrpc
597/tcp   open  msrpc
598/tcp   open  msrpc
599/tcp   open  msrpc
600/tcp   open  msrpc
601/tcp   open  msrpc
602/tcp   open  msrpc
603/tcp   open  msrpc
604/tcp   open  msrpc
605/tcp   open  msrpc
606/tcp   open  msrpc
607/tcp   open  msrpc
608/tcp   open  msrpc
609/tcp   open  msrpc
610/tcp   open  msrpc
611/tcp   open  msrpc
612/tcp   open  msrpc
613/tcp   open  msrpc
614/tcp   open  msrpc
615/tcp   open  msrpc
616/tcp   open  msrpc
617/tcp   open  msrpc
618/tcp   open  msrpc
619/tcp   open  msrpc
620/tcp   open  msrpc
621/tcp   open  msrpc
622/tcp   open  msrpc
623/tcp   open  msrpc
624/tcp   open  msrpc
625/tcp   open  msrpc
626/tcp   open  msrpc
627/tcp   open  msrpc
628/tcp   open  msrpc
629/tcp   open  msrpc
630/tcp   open  msrpc
631/tcp   open  msrpc
632/tcp   open  msrpc
633/tcp   open  msrpc
634/tcp   open  msrpc
635/tcp   open  msrpc
636/tcp   open  msrpc
637/tcp   open  msrpc
638/tcp   open  msrpc
639/tcp   open  msrpc
640/tcp   open  msrpc
641/tcp   open  msrpc
642/tcp   open  msrpc
643/tcp   open  msrpc
644/tcp   open  msrpc
645/tcp   open  msrpc
646/tcp   open  msrpc
647/tcp   open  msrpc
648/tcp   open  msrpc
649/tcp   open  msrpc
650/tcp   open  msrpc
651/tcp   open  msrpc
652/tcp   open  msrpc
653/tcp   open  msrpc
654/tcp   open  msrpc
655/tcp   open  msrpc
656/tcp   open  msrpc
657/tcp   open  msrpc
658/tcp   open  msrpc
659/tcp   open  msrpc
660/tcp   open  msrpc
661/tcp   open  msrpc
662/tcp   open  msrpc
663/tcp   open  msrpc
664/tcp   open  msrpc
665/tcp   open  msrpc
666/tcp   open  msrpc
667/tcp   open  msrpc
668/tcp   open  msrpc
669/tcp   open  msrpc
670/tcp   open  msrpc
671/tcp   open  msrpc
672/tcp   open  msrpc
673/tcp   open  msrpc
674/tcp   open  msrpc
675/tcp   open  msrpc
676/tcp   open  msrpc
677/tcp   open  msrpc
678/tcp   open  msrpc
679/tcp   open  msrpc
680/tcp   open  msrpc
681/tcp   open  msrpc
682/tcp   open  msrpc
683/tcp   open  msrpc
684/tcp   open  msrpc
685/tcp   open  msrpc
686/tcp   open  msrpc
687/tcp   open  msrpc
688/tcp   open  msrpc
689/tcp   open  msrpc
690/tcp   open  msrpc
691/tcp   open  msrpc
692/tcp   open  msrpc
693/tcp   open  msrpc
694/tcp   open  msrpc
695/tcp   open  msrpc
696/tcp   open  msrpc
697/tcp   open  msrpc
698/tcp   open  msrpc
699/tcp   open  msrpc
700/tcp   open  msrpc
701/tcp   open  msrpc
702/tcp   open  msrpc
703/tcp   open  msrpc
704/tcp   open  msrpc
705/tcp   open  msrpc
706/tcp   open  msrpc
707/tcp   open  msrpc
708/tcp   open  msrpc
709/tcp   open  msrpc
710/tcp   open  msrpc
711/tcp   open  msrpc
712/tcp   open  msrpc
713/tcp   open  msrpc
714/tcp   open  msrpc
715/tcp   open  msrpc
716/tcp   open  msrpc
717/tcp   open  msrpc
718/tcp   open  msrpc
719/tcp   open  msrpc
720/tcp   open  msrpc
721/tcp   open  msrpc
722/tcp   open  msrpc
723/tcp   open  msrpc
724/tcp   open  msrpc
725/tcp   open  msrpc
726/tcp   open  msrpc
727/tcp   open  msrpc
728/tcp   open  msrpc
729/tcp   open  msrpc
730/tcp   open  msrpc
731/tcp   open  msrpc
732/tcp   open  msrpc
733/tcp   open  msrpc
734/tcp   open  msrpc
735/tcp   open  msrpc
736/tcp   open  msrpc
737/tcp   open  msrpc
738/tcp   open  msrpc
739/tcp   open  msrpc
740/tcp   open  msrpc
741/tcp   open  msrpc
742/tcp   open  msrpc
743/tcp   open  msrpc
744/tcp   open  msrpc
745/tcp   open  msrpc
746/tcp   open  msrpc
747/tcp   open  msrpc
748/tcp   open  msrpc
749/tcp   open  msrpc
750/tcp   open  msrpc
751/tcp   open  msrpc
752/tcp   open  msrpc
753/tcp   open  msrpc
754/tcp   open  msrpc
755/tcp   open  msrpc
756/tcp   open  msrpc
757/tcp   open  msrpc
758/tcp   open  msrpc
759/tcp   open  msrpc
760/tcp   open  msrpc
761/tcp   open  msrpc
762/tcp   open  msrpc
763/tcp   open  msrpc
764/tcp   open  msrpc
765/tcp   open  msrpc
766/tcp   open  msrpc
767/tcp   open  msrpc
768/tcp   open  msrpc
769/tcp   open  msrpc
770/tcp   open  msrpc
771/tcp   open  msrpc
772/tcp   open  msrpc
773/tcp   open  msrpc
774/tcp   open  msrpc
775/tcp   open  msrpc
776/tcp   open  msrpc
777/tcp   open  msrpc
778/tcp   open  msrpc
779/tcp   open  msrpc
780/tcp   open  msrpc
781/tcp   open  msrpc
782/tcp   open  msrpc
783/tcp   open  msrpc
784/tcp   open  msrpc
785/tcp   open  msrpc
786/tcp   open  msrpc
787/tcp   open  msrpc
788/tcp   open  msrpc
789/tcp   open  msrpc
790/tcp   open  msrpc
791/tcp   open  msrpc
792/tcp   open  msrpc
793/tcp   open  msrpc
794/tcp   open  msrpc
795/tcp   open  msrpc
796/tcp   open  msrpc
797/tcp   open  msrpc
798/tcp   open  msrpc
799/tcp   open  msrpc
800/tcp   open  msrpc
801/tcp   open  msrpc
802/tcp   open  msrpc
803/tcp   open  msrpc
804/tcp   open  msrpc
805/tcp   open  msrpc
806/tcp   open  msrpc
807/tcp   open  msrpc
808/tcp   open  msrpc
809/tcp   open  msrpc
810/tcp   open  msrpc
811/tcp   open  msrpc
812/tcp   open  msrpc
813/tcp   open  msrpc
814/tcp   open  msrpc
815/tcp   open  msrpc
816/tcp   open  msrpc
817/tcp   open  msrpc
818/tcp   open  msrpc
819/tcp   open  msrpc
820/tcp   open  msrpc
821/tcp   open  msrpc
822/tcp   open  msrpc
823/tcp   open  msrpc
824/tcp   open  msrpc
825/tcp   open  msrpc
826/tcp   open  msrpc
827/tcp   open  msrpc
828/tcp   open  msrpc
829/tcp   open  msrpc
830/tcp   open  msrpc
831/tcp   open  msrpc
832/tcp   open  msrpc
833/tcp   open  msrpc
834/tcp   open  msrpc
835/tcp   open  msrpc
836/tcp   open  msrpc
837/tcp   open  msrpc
838/tcp   open  msrpc
839/tcp   open  msrpc
840/tcp   open  msrpc
841/tcp   open  msrpc
842/tcp   open  msrpc
843/tcp   open  msrpc
844/tcp   open  msrpc
845/tcp   open  msrpc
846/tcp   open  msrpc
847/tcp   open  msrpc
848/tcp   open  msrpc
849/tcp   open  msrpc
850/tcp   open  msrpc
851/tcp   open  msrpc
852/tcp   open  msrpc
853/tcp   open  msrpc
854/tcp   open  msrpc
855/tcp   open  msrpc
856/tcp   open  msrpc
857/tcp   open  msrpc
858/tcp   open  msrpc
859/tcp   open  msrpc
860/tcp   open  msrpc
861/tcp   open  msrpc
862/tcp   open  msrpc
863/tcp   open  msrpc
864/tcp   open  msrpc
865/tcp   open  msrpc
866/tcp   open  msrpc
867/tcp   open  msrpc
868/tcp   open  msrpc
869/tcp   open  msrpc
870/tcp   open  msrpc
871/tcp   open  msrpc
872/tcp   open  msrpc
873/tcp   open  msrpc
874/tcp   open  msrpc
875/tcp   open  msrpc
876/tcp   open  msrpc
877/tcp   open  msrpc
878/tcp   open  msrpc
879/tcp   open  msrpc
880/tcp   open  msrpc
881/tcp   open  msrpc
882/tcp   open  msrpc
883/tcp   open  msrpc
884/tcp   open  msrpc
885/tcp   open  msrpc
886/tcp   open  msrpc
887/tcp   open  msrpc
888/tcp   open  msrpc
889/tcp   open  msrpc
890/tcp   open  msrpc
891/tcp   open  msrpc
892/tcp   open  msrpc
893/tcp   open  msrpc
894/tcp   open  msrpc
895/tcp   open  msrpc
896/tcp   open  msrpc
897/tcp   open  msrpc
898/tcp   open  msrpc
899/tcp   open  msrpc
900/tcp   open  msrpc
901/tcp   open  msrpc
902/tcp   open  msrpc
903/tcp   open  msrpc
904/tcp   open  msrpc
905/tcp   open  msrpc
906/tcp   open  msrpc
907/tcp   open  msrpc
908/tcp   open  msrpc
909/tcp   open  msrpc
910/tcp   open  msrpc
911/tcp   open  msrpc
912/tcp   open  msrpc
913/tcp   open  msrpc
914/tcp   open  msrpc
915/tcp   open  msrpc
916/tcp   open  msrpc
917/tcp   open  msrpc
918/tcp   open  msrpc
919/tcp   open  msrpc
920/tcp   open  msrpc
921/tcp   open  msrpc
922/tcp   open  msrpc
923/tcp   open  msrpc
924/tcp   open  msrpc
925/tcp   open  msrpc
926/tcp   open  msrpc
927/tcp   open  msrpc
928/tcp   open  msrpc
929/tcp   open  msrpc
930/tcp   open  msrpc
931/tcp   open  msrpc
932/tcp   open  msrpc
933/tcp   open  msrpc
934/tcp   open  msrpc
935/tcp   open  msrpc
936/tcp   open  msrpc
937/tcp   open  msrpc
938/tcp   open  msrpc
939/tcp   open  msrpc
940/tcp   open  msrpc
941/tcp   open  msrpc
942/tcp   open  msrpc
943/tcp   open  msrpc
944/tcp   open  msrpc
945/tcp   open  msrpc
946/tcp   open  msrpc
947/tcp   open  msrpc
948/tcp   open  msrpc
949/tcp   open  msrpc
950/tcp   open  msrpc
951/tcp   open  msrpc
952/tcp   open  msrpc
953/tcp   open  msrpc
954/tcp   open  msrpc
955/tcp   open  msrpc
956/tcp   open  msrpc
957/tcp   open  msrpc
958/tcp   open  msrpc
959/tcp   open  msrpc
960/tcp   open  msrpc
961/tcp   open  msrpc
962/tcp   open  msrpc
963/tcp   open  msrpc
964/tcp   open  msrpc
965/tcp   open  msrpc
966/tcp   open  msrpc
967/tcp   open  msrpc
968/tcp   open  msrpc
969/tcp   open  msrpc
970/tcp   open  msrpc
971/tcp   open  msrpc
972/tcp   open  msrpc
973/tcp   open  msrpc
974/tcp   open  msrpc
975/tcp   open  msrpc
976/tcp   open  msrpc
977/tcp   open  msrpc
978/tcp   open  msrpc
979/tcp   open  msrpc
980/tcp   open  msrpc
981/tcp   open  msrpc
982/tcp   open  msrpc
983/tcp   open  msrpc
984/tcp   open  msrpc
985/tcp   open  msrpc
986/tcp   open  msrpc
987/tcp   open  msrpc
988/tcp   open  msrpc
989/tcp   open  msrpc
990/tcp   open  msrpc
991/tcp   open  msrpc
992/tcp   open  msrpc
993/tcp   open  msrpc
994/tcp   open  msrpc
995/tcp   open  msrpc
996/tcp   open  msrpc
997/tcp   open  msrpc
998/tcp   open  msrpc
999/tcp   open  msrpc
1000/tcp  open  msrpc
```

- **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.



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

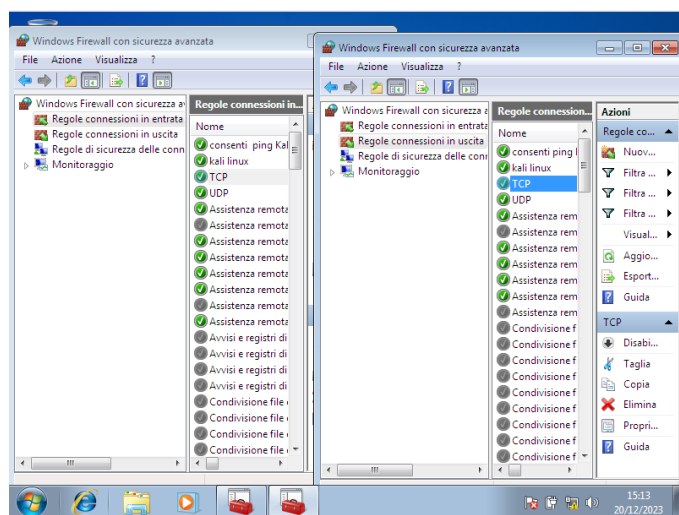
Il tentativo di Fingerprinting per identificare il sistema operativo su Windows non è riuscito.



## 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, microsoft, 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.