Report di nmap del 22/07/2022

In questo report andrò ad analizzare le vulnerabilità rilevate dalla macchina virtuale Linux nei confronti della

macchina virtuale Metasploitable con il programma di port scanner più utilizzato, nmap.

La fonte delle scansioni che andrò ad analizzare è la macchina virtuale Kali Linux con indirizzo Ip statico

(192.168.50.100), mentre il target delle scansioni è la macchina virtuale Metasploitable con indirizzo Ip statico

(192.168.50.101). Le due macchine comunicano sulla stessa rete interna.

I tipi di scansione utilizzati sono la “Scansione SYN” (-sS), la “scansione TCP” (-sT) e la scansione con switch “-A” (-A).

SCANSIONE SYN

Inizialmente, la mia analisi parte da una scansione SYN (-sS) della rete della macchina Metasploitable in cui sono

state rilevate aperte le seguenti porte:

Numero di servizi rilevati→ 12

Immagine che contiene testo, monitor, screenshot, elettronico

Descrizione generata automaticamente

Partendo dall’inizio le porte rilevate sono:

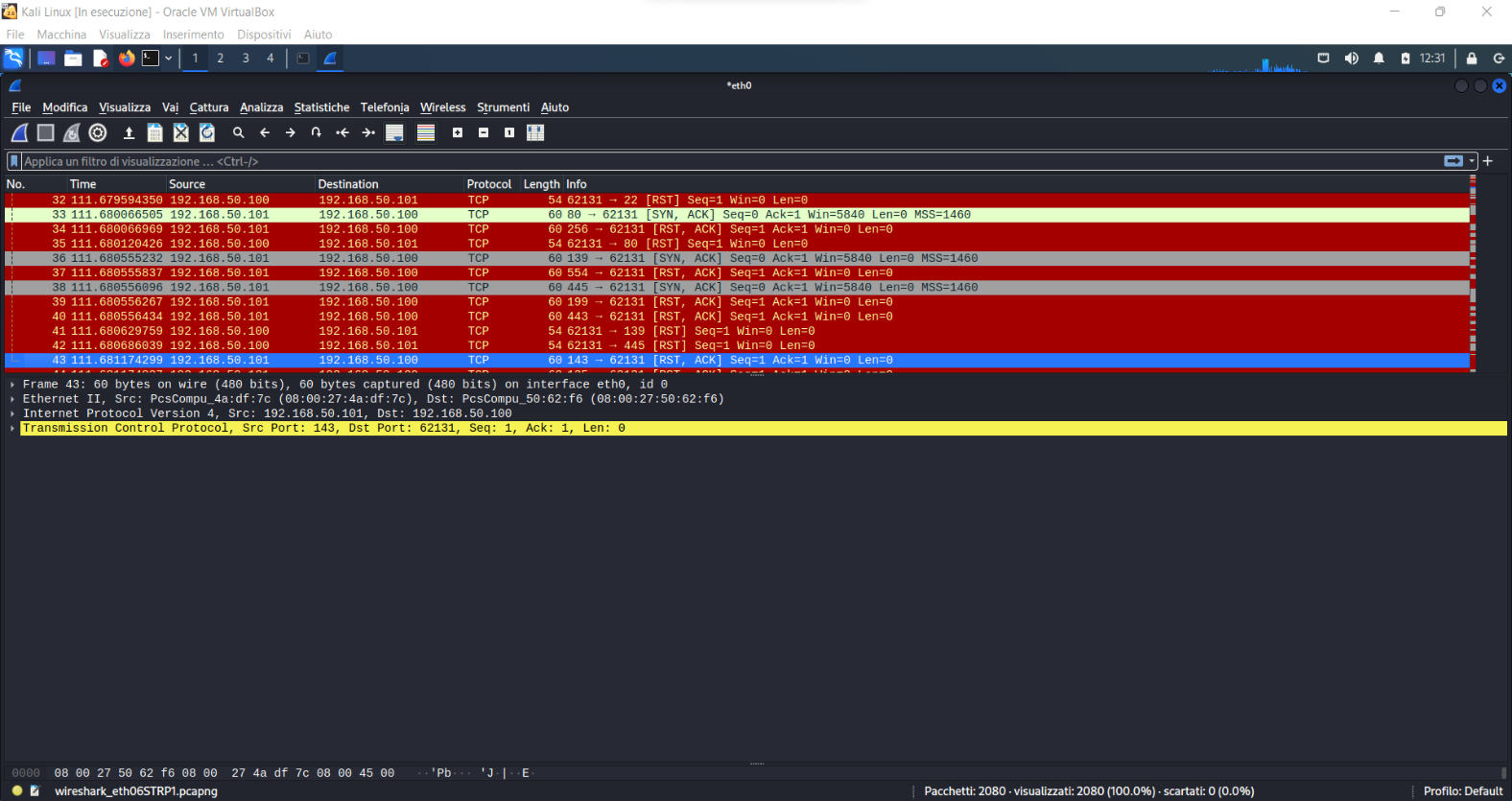
* **Porta 21/tcp** con stato “open”, service **ftp→** è una porta con il servizio di “file transfert protocol”, ovvero che viene utilizzata per il trasferimento dei file.
* **Porta 22/tcp** con stato “open”, service **ssh (Secure Shell)** → è una porta con protocollo di sicurezza che permette di stabilire una sessione remota cifrata, proprio per garantire la sicurezza.
* **Porta 23/tcp** con stato “open”. service **telnet** (**Terminal network)** → è un protocollo di rete utilizzato come supporto per le telecomunicazioni tra client e server.
* **Porta 25/tcp** con stato “open”, service **smtp (simple mail transfert protocol) →** è un protocollo che si utilizza per la trasmissione delle e-mail.
* **Porta 53/tcp** con stato “open”, service **domain (dominio)**→ è un servizio che trasforma gli indirizzi dei siti web in indirizzi IP.
* **Porta 80/tcp** con stato “open”, service **http (Hypertext transfert protocol) →** è uno dei servizi più conosciuti, utilizzato per il trasferimento delle pagine web in internet.
* **Porta 111/tcp** con stato “open”, service **rpcbind→** è un server che converte i numeri di programmi RPC (attivazione di un programma da un computer ad un altro) in indirizzi universali.
* **Porta 139/tcp** con stato “open”, service **netbios-ssn** (**Sistema di input/output della rete)** → è un servizio che esegue la mappatura dei nomi e degli indirizzi IP relativi a questi nomi.
* **Porta 445/tcp** con stato “open”, service **microsoft-ds→** servizio di Microsoft Domain Service.
* **Porta 512/tcp** con stato “open”, service **exec**→ funzione di sistema standard della libreria del linguaggio di programmazione “C”.
* **Porta 513/tcp** con stato “open”, service **login→** servizio di procedura dell’identificazione di un utente.
* **Porta 514/tcp** con stato “open”, service **shell**→ componente fondamentale per l’impartizione dei comandi e avvio dei programmi sulla macchina.

Parallelamente, avviando il programma Wireshark, programma di vulnerability scanner, ho catturato i pacchetti relativi a questa interazione tra le due macchine, rilevando varie anomalie dovute all’esecuzione del comando “nmap -sS 192.168.50.101 -p 1-1024”.

Il comando “**nmap -sS 192.168.50.101 -p 1-1024”** indica che nMap andrà a scansionare con la modalità **stealt** (ovvero meno invasiva) le porte dell’indirizzo Ip 192.168.50.101 della macchina Metasploitable con il range di porte considerato, dalla numero 1 alla numero 1024.

Questo comando è riconducibile alla scansione SYN sulle porte conosciute (“well-known”) ed è uno dei comandi meno invasivi eseguibili con Nmap.

Di seguito i pacchetti catturati con Wireshark al momento di esecuzione del comando riportato sopra:



All’interno di questa immagine possiamo notare quello che succede nel momento in cui Nmap scansiona le porte della macchina Metasploitable. All’interno della scansione SYN, è possibile intravedere come nMap non completa il “three-way-handshake”, ma invia un pacchetto “RST” (reset) per chiudere la comunicazione. Ciò significa che non va a stabilire una connessione ma recupera soltanto le informazioni delle porte, il loro stato e il servizio che svolgono all’interno della macchina.

Dalla riga **36 ,** ad esempio, possiamo notare che viene avviata la “stretta di mano a tre vie” che poi si che poi si completa nelle righe successive con un **RST**, ovvero reset. Questo sta ad indicare che la “three-way-handshake” non è stata completata.

SCANSIONE TCP

Lo stesso processo è stato da me ripetuto per rintracciare le porte “well-known” con il tipo di scansione TCP.

Con il programma di sniffing Wireshark in esecuzione, ho eseguito il comando “**nmap -sT 192.168.1.101 -p 1-1024”** allo scopo di avviare una scansione molto più invasiva della precedente.ù

Il comando “**nmap -sT 192.168.1.101 -p 1-1024”** indica che il programma andrà a scansionare le porte della macchina Metasploitable con indirizzo 192.168.1.101, nello specifico all’interno del range di porte considerato, dalla numero 1 alla numero 1024.

Le porte rilevate dalla scansione TCP sono le stesse rilevate dalla scansione SYN. Numero di servizi rilevati→12

Immagine che contiene testo

Descrizione generata automaticamente

Attraverso Wireshark, ho catturato i pacchetti avviati dalla scansione TCP:

Immagine che contiene testo, screenshot, schermo, appartamento

Descrizione generata automaticamente

Qui possiamo vedere come la “stretta di mano a tre vie” viene completata tra le due macchine. Da lì parte la comunicazione attraverso la rete interna. Per questo motivo abbiamo detto prima che questo tipo di scansione è molto invasiva e “rumorosa”, in quanto è facilmente rintracciabile dalla macchina attaccata.

DIFFERENZA TRA SCANSIONE SYN E SCANSIONE TCP

La differenza sostanziale che può essere rinvenuta tra la prima scansione SYN e la seconda scansione TCP è il modo in cui queste operano.

Nella prima scansione, nMap non stabilisce nessuna comunicazione ma rileva soltanto le porte aperte, ma soprattutto non conclude la “three-way-handshake”.

Nella seconda scansione, più invasiva, nMap va a stabilire una connessione completando la “three-way-handshake” creando proprio il canale di comunicazione tra le due macchine.

Inoltre, un’altra differenza sostanziale delle due scansioni è la “rumorosità”:

* la prima scansione (SYN) è abbastanza silenziosa, nel senso che non desta alcuna preoccupazione in quanto riceve solo lo stato delle porte.
* La seconda scansione (TCP) è definita “rumorosa” in quanto appunto va ad avviare una comunicazione facile da identificare all’interno del network.

SCANSIONE CON SWITCH “-A”

Nell’ultima situazione andremo ad utilizzare una scansione molto aggressiva e molto approfondita in quanto vengono riportate anche le versioni dei servizi scansionati, i tipi di porta e tutte le informazioni approfondite riguardanti le porte aperte rilevate.

Di seguito riporto la scansione effettuata sul terminale kali Linux con il comando “nmap -A 192.168.50.101 -p 1-1024”.

Il comando “**nmap -A 192.168.50.101 -p 1-1024”** sta ad indicare che la scansione “aggressive-mode” è stata effettuata sulla macchina Metasploitable con indirizzo Ip statico 192.168.50.101 con un range di porte compreso tra la numero 1 e la numero 1024.

Immagine che contiene testo

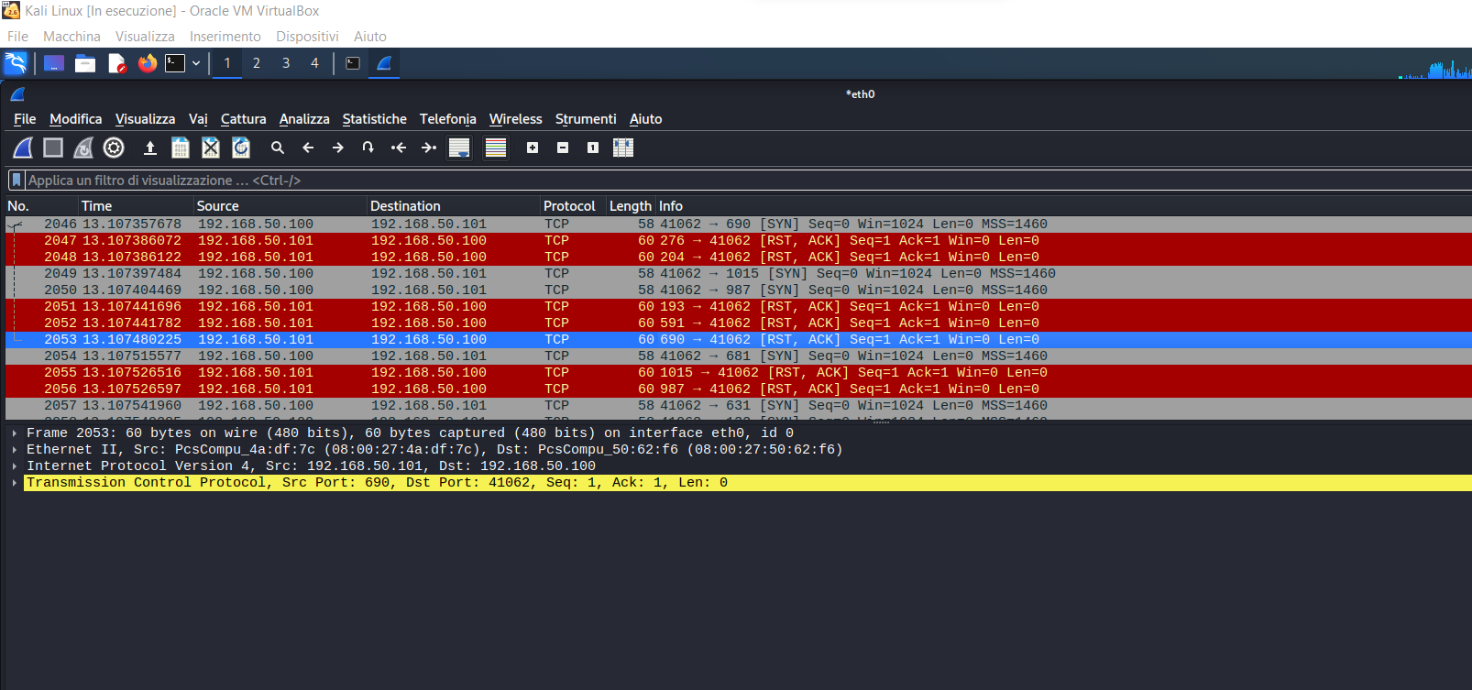
Descrizione generata automaticamente

Immagine che contiene testo

Descrizione generata automaticamente

All’interno di questa scansione con switch “-A” si possono notare anche altri tipi di informazioni, come le informazioni sul sistema operativo presente sulle due macchine, i MAC address, i nomi dei due computer, la scansione degli IP, il Traceroute (che ricava il percorso dei pacchetti informatici), il nome dei domini e addirittura quali sono gli account utilizzati all’interno dei sistemi operativi.

Attraverso Wireshark ho catturato i pacchetti rilevati dopo l’esecuzione del comando sopra riportato.



Anche qui si può notare come le varie porte non completano il processo di “**three-way-handshake”** ma troncano la comunicazione con l’altra macchina attraverso la funzione “**RST**” (reset), come si può notare, ad esempio dalla riga 2049 alla riga 2053.

Anche in questo caso non viene creata una comunicazione tra le due macchine, nonostante il livello di scansione risulti molto più approfondito della scansione SYN.