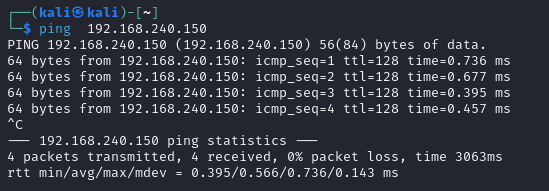
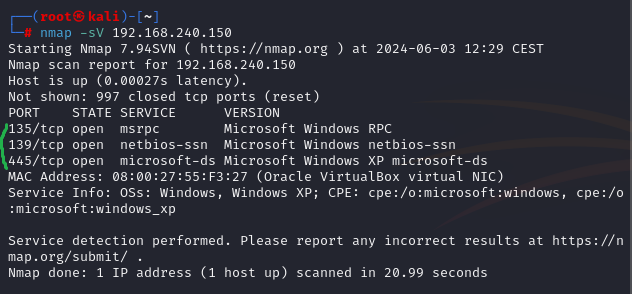
In data odierna la nostra azienda la “CORTANA” è stata contattata dall’azienda del Sig. Rossi per un vulnerability assessment per mettere in sicurezza il pc della propria azienda. Il primo step era quello di determinare l’impatto che aveva il firewall sulla macchina che utilizzava lui stesso. Pertanto abbiamo eseguito un controllo della macchina prima e dopo aver attivato il firewall per mettere in evidenza l’impatto che questo avrebbe avuto sulla sicurezza della macchina.

**FIREWALL DISATTIVATO**

Dalla macchina di Kali effettuiamo prima un ping per assicurarci che le macchine comunichino tra loro.



Dalla macchina di Kali effettuiamo prima una scansione dei servizi e delle relative versioni con il comando di nmap “-sV”.



Possiamo notare che nmap ha trovato 3 porte aperte con i rispettivi servizi e versioni.

Porta 135 (msrpc): Utilizzata per le chiamate di procedura remota di Microsoft (RPC). È una porta critica per le funzionalità di rete di Windows e può essere un vettore di attacco se non adeguatamente protetta.

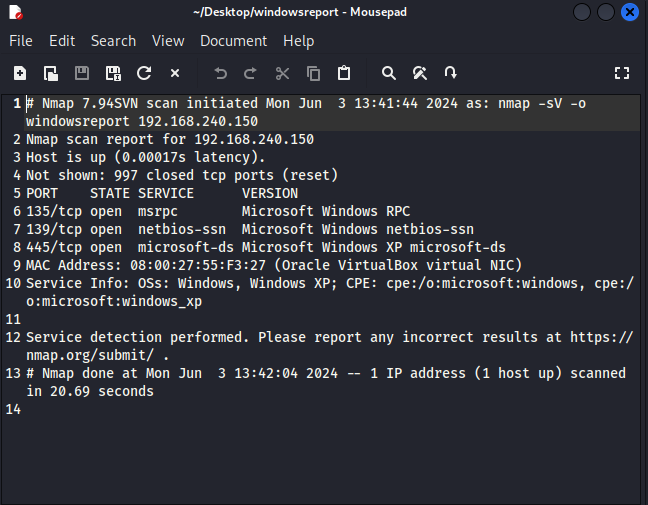
Porta 139 (netbios-ssn): Utilizzata dal servizio NetBIOS per sessioni di rete su TCP/IP. Tipicamente usata per condivisioni di file e stampanti.

Porta 445 (microsoft-ds): Utilizzata per la condivisione di file e stampanti tramite SMB (Server Message Block) su TCP/IP. Sostituisce la funzionalità del NetBIOS sulle reti più moderne.

Possiamo salvare direttamente i risultati ottenuti in un file di testo che chiameremo “windowsreport”; dopodichè ci spostiamo nella directory dove è contenuto il file di testo, apriamo il terminale (come root) e aggiungiamo alla scansione precedente il comando “-o” seguito dal nome del file di testo.

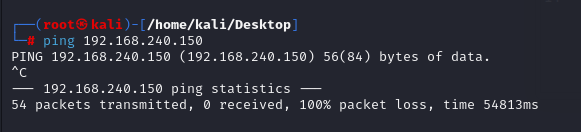


I risultati ci verranno restituiti direttamente all’interno del file di testo.



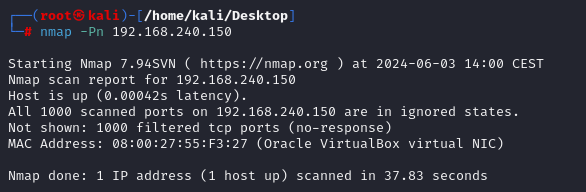
**FIREWALL ATTIVO**

Proviamo ad effettuare un ping tra le due macchine e possiamo già notare delle differenze rispetto a quando il firewall era disattivato.



La macchina sembra essere irraggiungibile tramite ping. Possiamo ipotizzare che il firewall stia bloccando le richieste ICMP (quindi anche i pacchetti inviati da noi tramite ping).

Proviamo dunque un comando meno invasivo per vedere se riceviamo risposta dalla macchina di windows XP: diamo in input il comando “nmap –PN” seguito dall’IP della macchina di metasploitable.



Anche questa volta non siamo riusciti ad ottenere molte informazioni sulla macchina; tuttavia, ci viene restituito il MAC Address della macchina di windows XP e scopriamo anche che il sistema operativo è in esecuzione all’interno di una macchina virtuale.

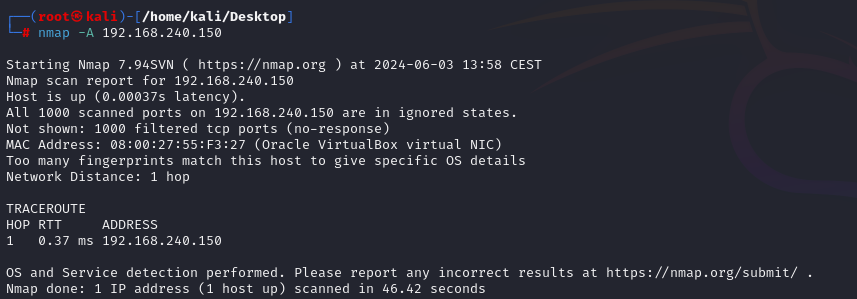
Proviamo con un metodo più invasivo. Il comando “nmap –A” è il metodo di scansione più completo. Questo comando unisce in un'unica soluzione le seguenti scansioni:

-OS fingerprint: Rilevamento del sistema operativo

-Version detection: analisi delle porte aperte, servizi attivi sulle porte e relative versioni (corrispondente al comando “nmap –sV”)

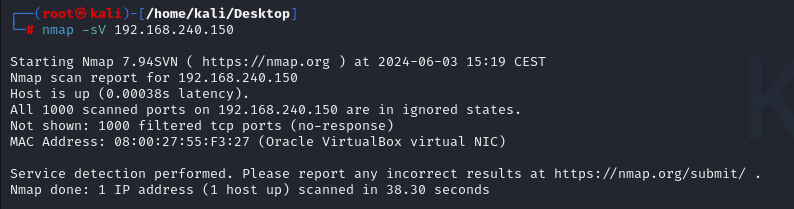
-Script scanning: Raccolta informazioni aggiuntive per identificare vulnerabilità (corrispondente al comando “nmap --script=default”)

-Traceroute: tenta di identificare il percorso preso dai pacchetti per raggiungere il target (corrispondente al comando “nmap –traceroute”)



Otteniamo qualche informazione aggiuntiva sulla macchina, ovvero il numero di HOP (cioè quanti dispositivi di rete sono stati attraversati dai pacchetti da noi inviati) e il RTT (Tempo di andata e ritorno, cioè il tempo di risposta della macchina al pacchetto inviato).

Effettuiamo nuovamente la scansione delle porte e versione dei servizi presenti su di esse e possiamo osservare come nessuna porta sia raggiungibile.



In conclusione, possiamo affermare che il firewall incrementa sensibilmente la sicurezza di una macchina, anche se questa presenta servizi obsoleti e quindi poco sicuri, rendendo più difficile per un attaccante sfruttarne le vulnerabilità.

Importo totale servizio= manodopera: 880 euro

Partecipanti del Team : STEFANO CESARONI E VALERIO ZAMPONE