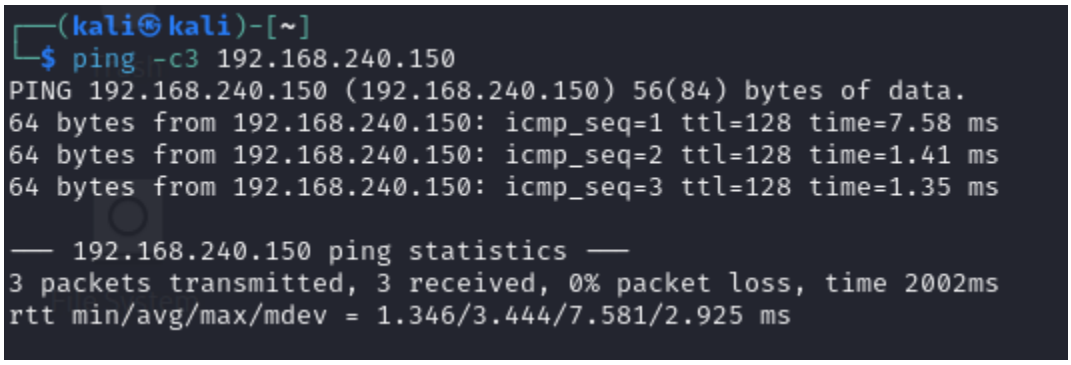
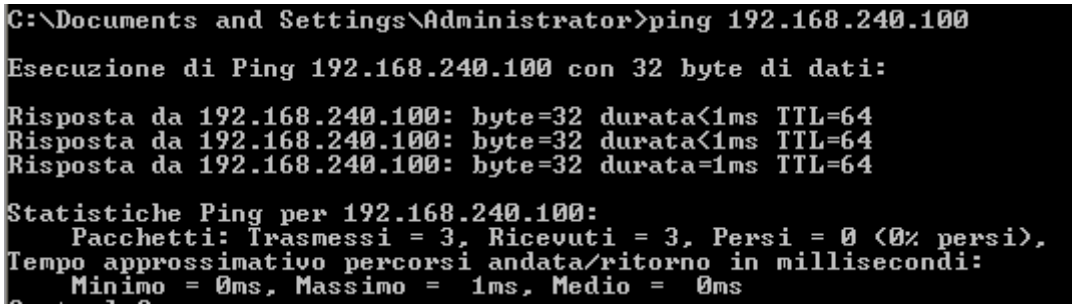
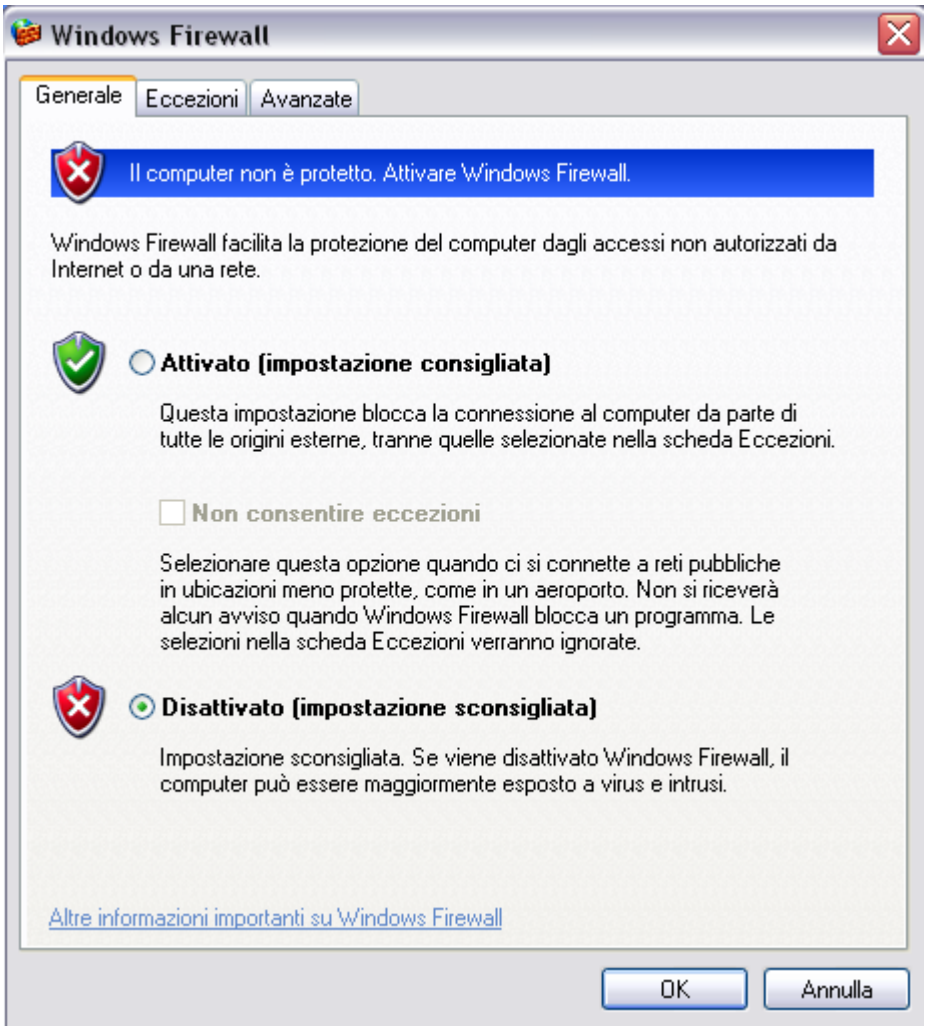
CONSEGNA U3 S9 L1

Prima di eseguire l'esercizio ho settato correttamente gli indirizzi IP sulle macchine Kali e XP. Poi ho eseguito il **ping** da entrambe per verificare che la connessione fosse attiva e funzionante.

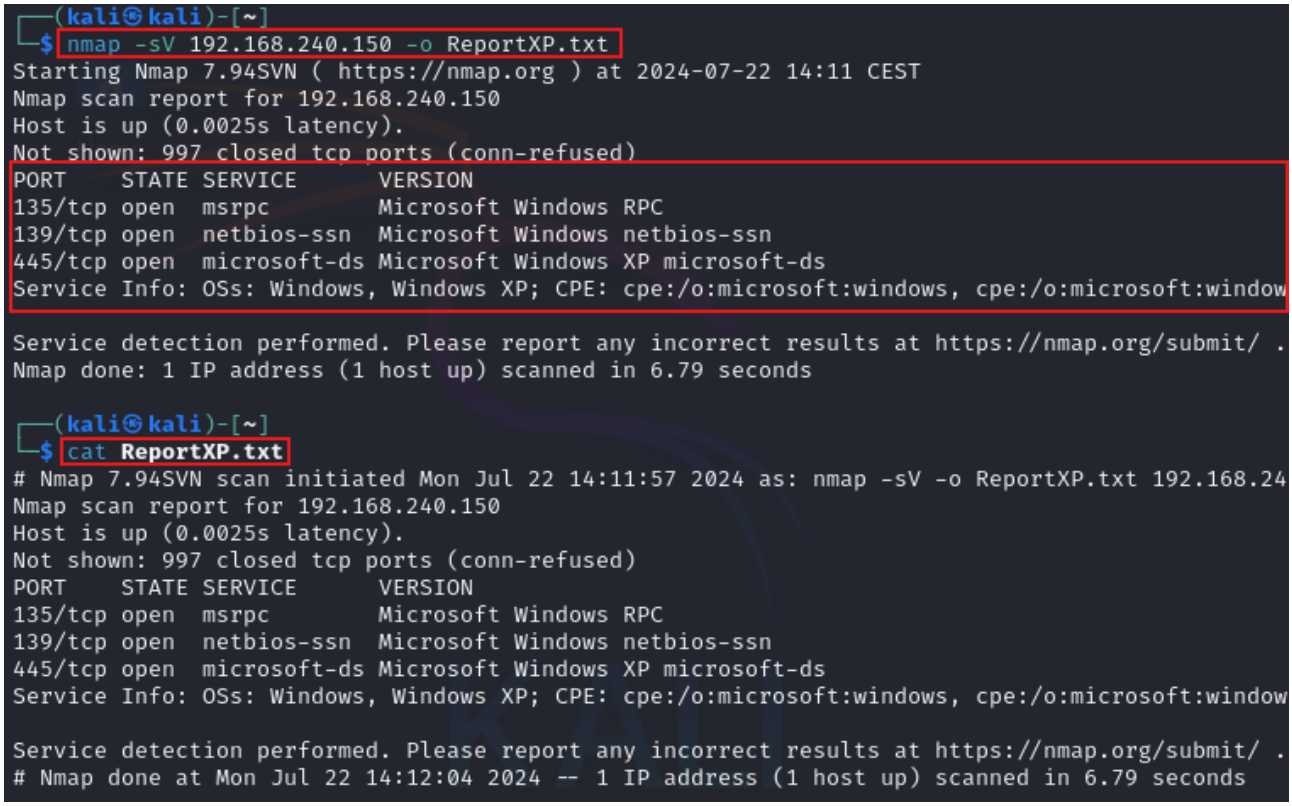




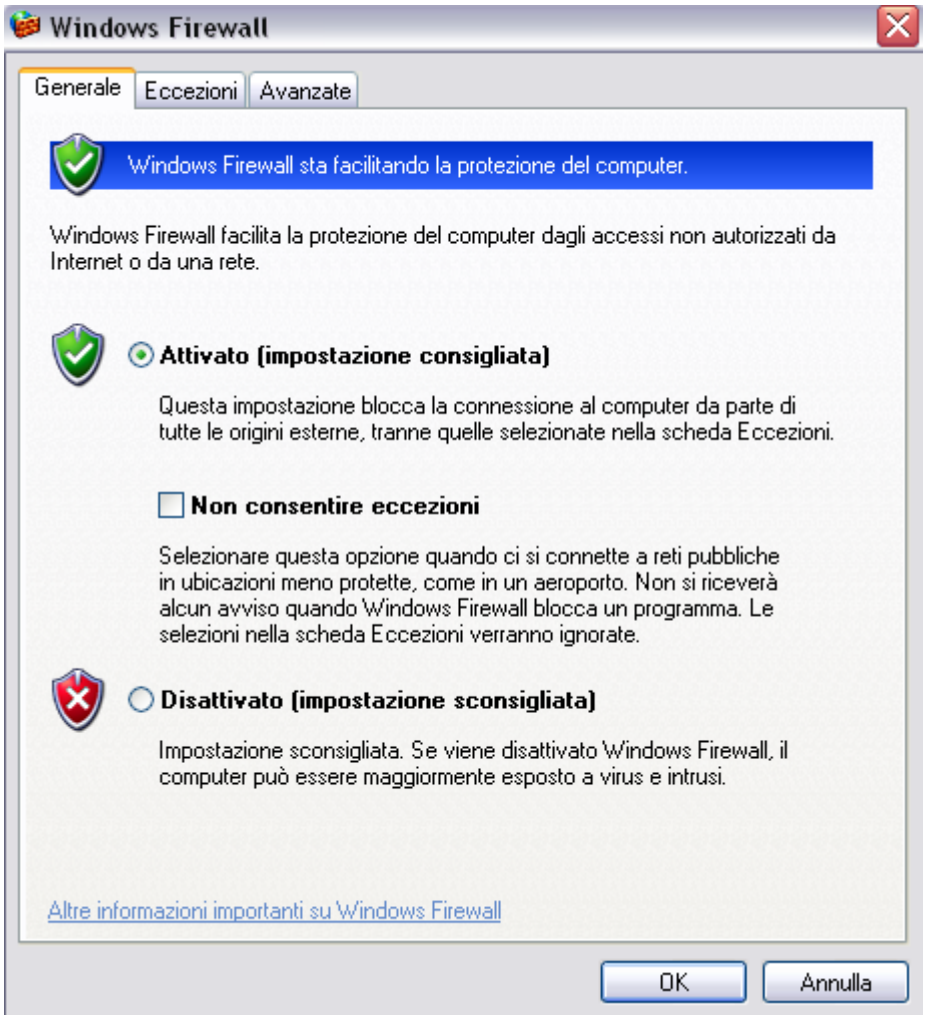
Poi sulla macchina Windows XP ho disattivato il firewall.



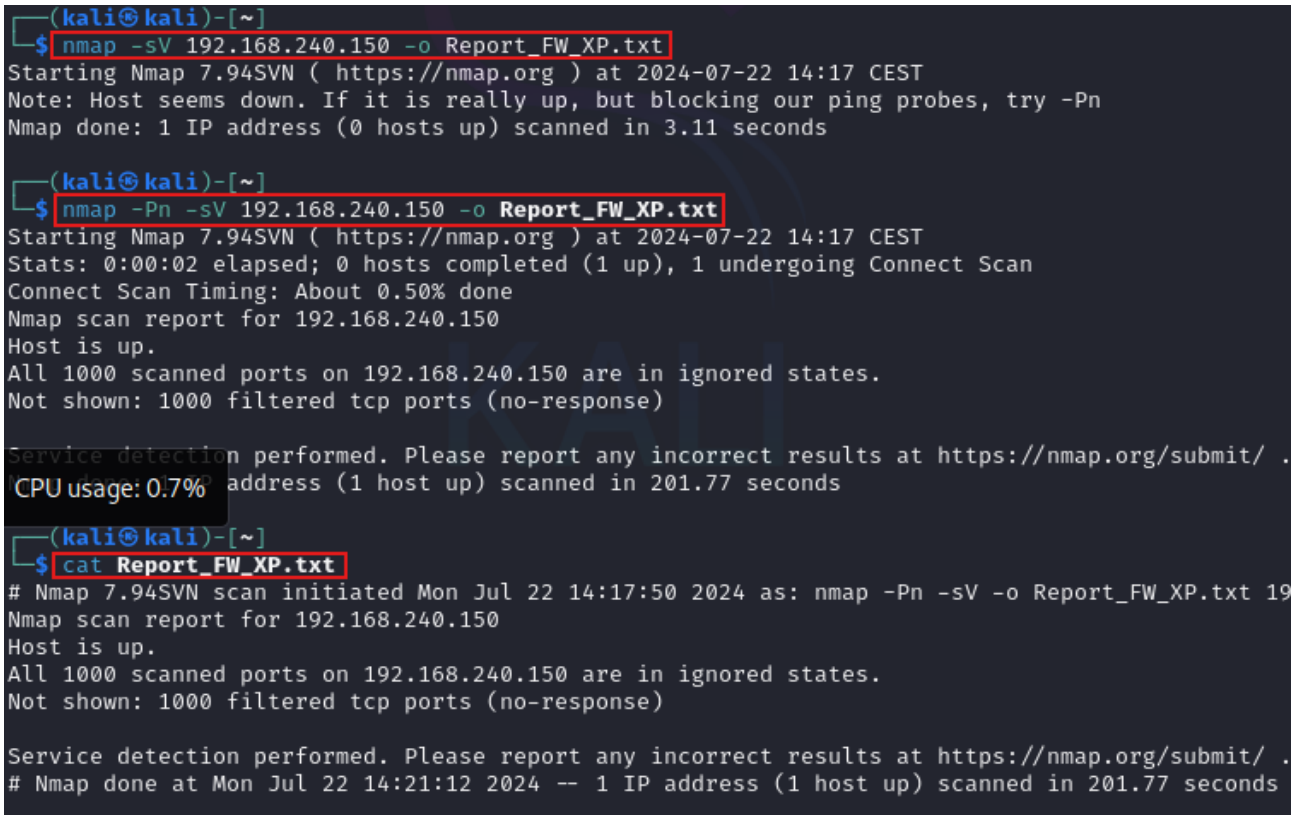
Avvio la scansione di **nmap** con lo switch **-sV** all'indirizzo di XP **192.168.240.150**. con lo switch **-o** dico a **nmap** di salvare l'output della scansione in un file di testo nominato **ReportXP.txt**. Si nota che ci sono diverse porte aperte e vari servizi attivi sulle stesse. Poi col comando **cat** visualizzo a schermo il file di report.



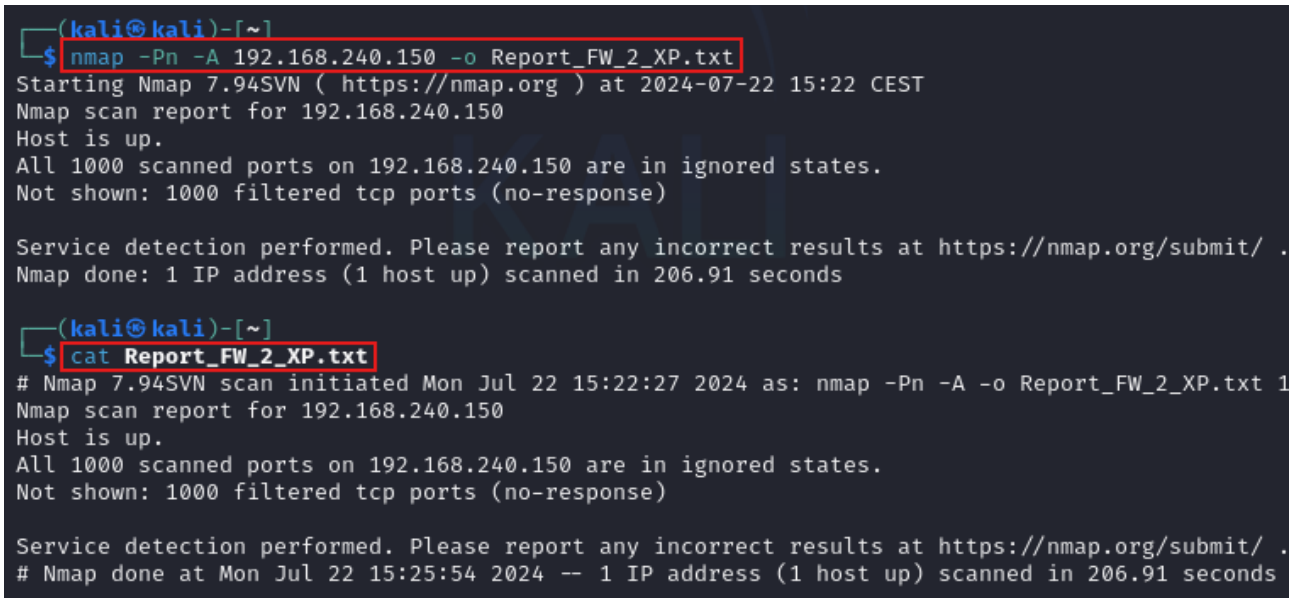
Adesso attivo il firewall di XP e ripeto la scansione.



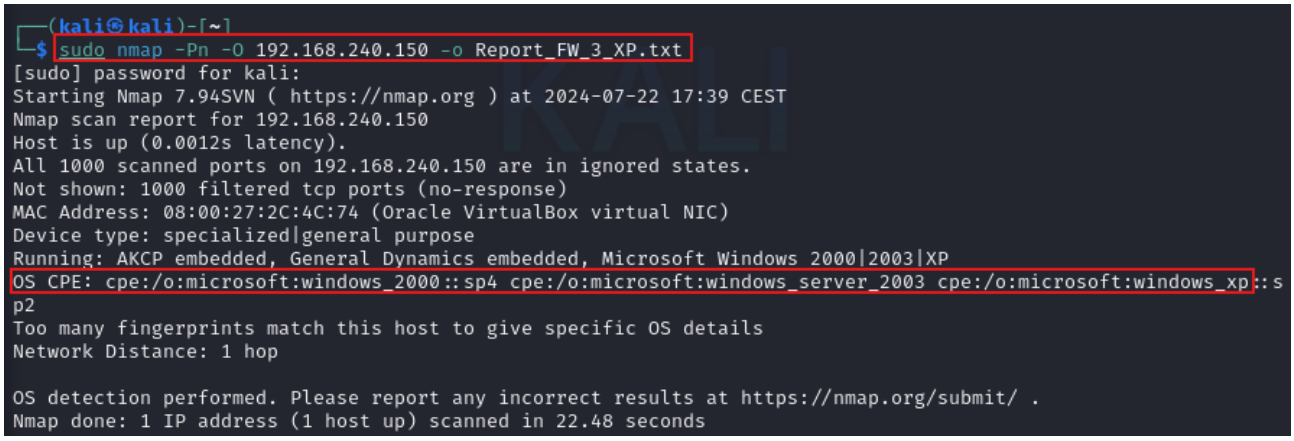
Effettuo nuovamente la scansione con **nmap** da Kali. In questa scansione con il firewall abilitato sulla macchina. Creo un nuovo file di report dove salvare le informazioni della scansione chiamato **Report_FW_XP.txt**. Tra l'altro **nmap** adesso necessita dello switch **-Pn** affinché la scansione vada a buon fine. Alla fine visualizzo a schermo il file di report.



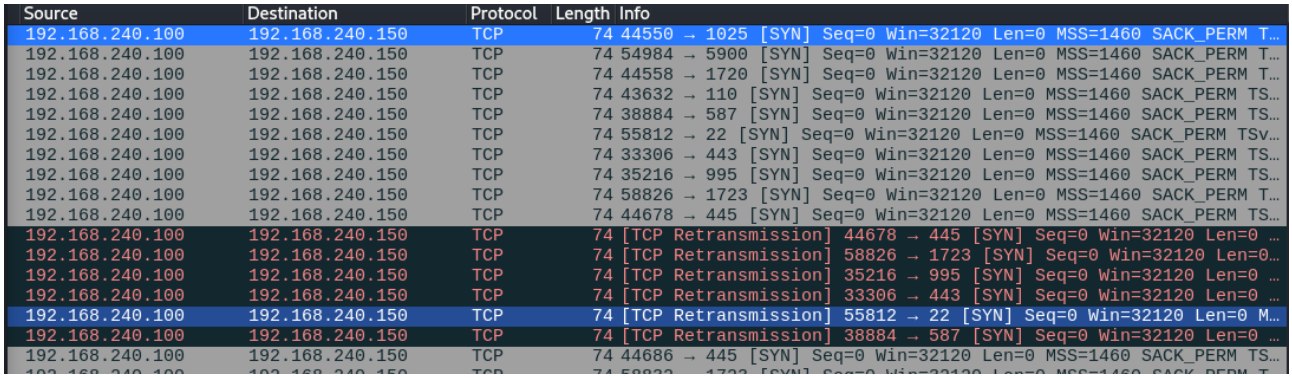
Provo poi ad effettuare un'altra scansione più completa con lo switch **-A** per vedere se cambia il risultato e salvo il risultato all'interno del file **Report_FW_2_XP.txt** che successivamente visualizzo sul terminale. Come nella scansione precedente non riesce a trovare nulla.



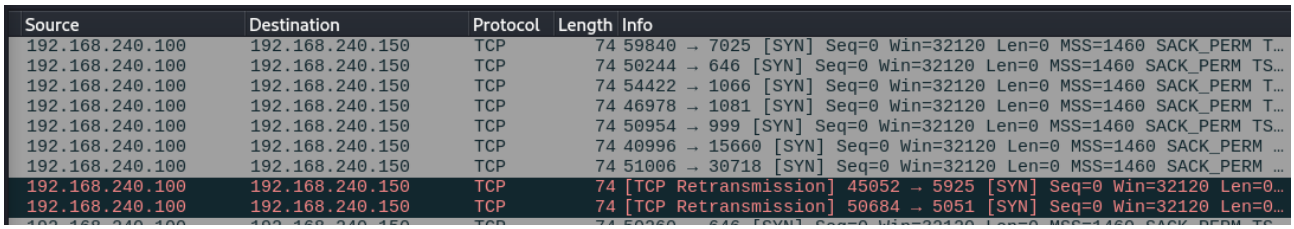
Provando ad effettuare la scansione con lo switch **-O** si riesce, anche a firewall attivo, ad ottenere informazioni sul sistema operativo della macchina target. (In questo caso Windows XP SP2)



Verifico con **wireshark** il traffico di rete, mi accorgo che con il firewall attivo sulla macchina Windows, molte delle trasmissioni avviate da **nmap** per la verifica dei servizi attivi sulle porte vengono rifiutate per motivi di sicurezza. (le righe evidenziate in rosso)



Source	Destination	Protocol	Length	Info
192.168.240.100	192.168.240.150	TCP	74	44550 → 1025 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM T…
192.168.240.100	192.168.240.150	TCP	74	54984 → 5900 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM T…
192.168.240.100	192.168.240.150	TCP	74	44558 → 1720 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM T…
192.168.240.100	192.168.240.150	TCP	74	43632 → 110 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS…
192.168.240.100	192.168.240.150	TCP	74	38884 → 587 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS…
192.168.240.100	192.168.240.150	TCP	74	55812 → 22 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSv…
192.168.240.100	192.168.240.150	TCP	74	33306 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS…
192.168.240.100	192.168.240.150	TCP	74	35216 → 995 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS…
192.168.240.100	192.168.240.150	TCP	74	58826 → 1723 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM T…
192.168.240.100	192.168.240.150	TCP	74	44678 → 445 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS…
192.168.240.100	192.168.240.150	TCP	74	[TCP Retransmission] 44678 → 445 [SYN] Seq=0 Win=32120 Len=0 …
192.168.240.100	192.168.240.150	TCP	74	[TCP Retransmission] 58826 → 1723 [SYN] Seq=0 Win=32120 Len=0…
192.168.240.100	192.168.240.150	TCP	74	[TCP Retransmission] 35216 → 995 [SYN] Seq=0 Win=32120 Len=0 …
192.168.240.100	192.168.240.150	TCP	74	[TCP Retransmission] 33306 → 443 [SYN] Seq=0 Win=32120 Len=0 …
192.168.240.100	192.168.240.150	TCP	74	[TCP Retransmission] 55812 → 22 [SYN] Seq=0 Win=32120 Len=0 M…
192.168.240.100	192.168.240.150	TCP	74	[TCP Retransmission] 38884 → 587 [SYN] Seq=0 Win=32120 Len=0 …
192.168.240.100	192.168.240.150	TCP	74	44686 → 445 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS…



Source	Destination	Protocol	Length	Info
192.168.240.100	192.168.240.150	TCP	74	59840 → 7025 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM T…
192.168.240.100	192.168.240.150	TCP	74	50244 → 646 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS…
192.168.240.100	192.168.240.150	TCP	74	54422 → 1066 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM T…
192.168.240.100	192.168.240.150	TCP	74	46978 → 1081 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM T…
192.168.240.100	192.168.240.150	TCP	74	50954 → 999 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS…
192.168.240.100	192.168.240.150	TCP	74	40996 → 15660 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM …
192.168.240.100	192.168.240.150	TCP	74	51006 → 30718 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM …
192.168.240.100	192.168.240.150	TCP	74	[TCP Retransmission] 45052 → 5925 [SYN] Seq=0 Win=32120 Len=0…
192.168.240.100	192.168.240.150	TCP	74	[TCP Retransmission] 50684 → 5051 [SYN] Seq=0 Win=32120 Len=0…

Conclusioni

Nonostante le porte con servizi attivi sulla rete, quando il firewall sulla macchina Windows è disattivato siano poche, comunque l'aver attivato il firewall protegge notevolmente di più la macchina da attacchi esterni. Inoltre, si da il caso che sulle macchine più obsolete, come per esempio Windows /, Vista, XP, quelle poche porte aperte possono permettere a qualche malintenzionato di sfruttare delle vulnerabilità che permettono di avere accesso e pieno controllo sulla macchina target.