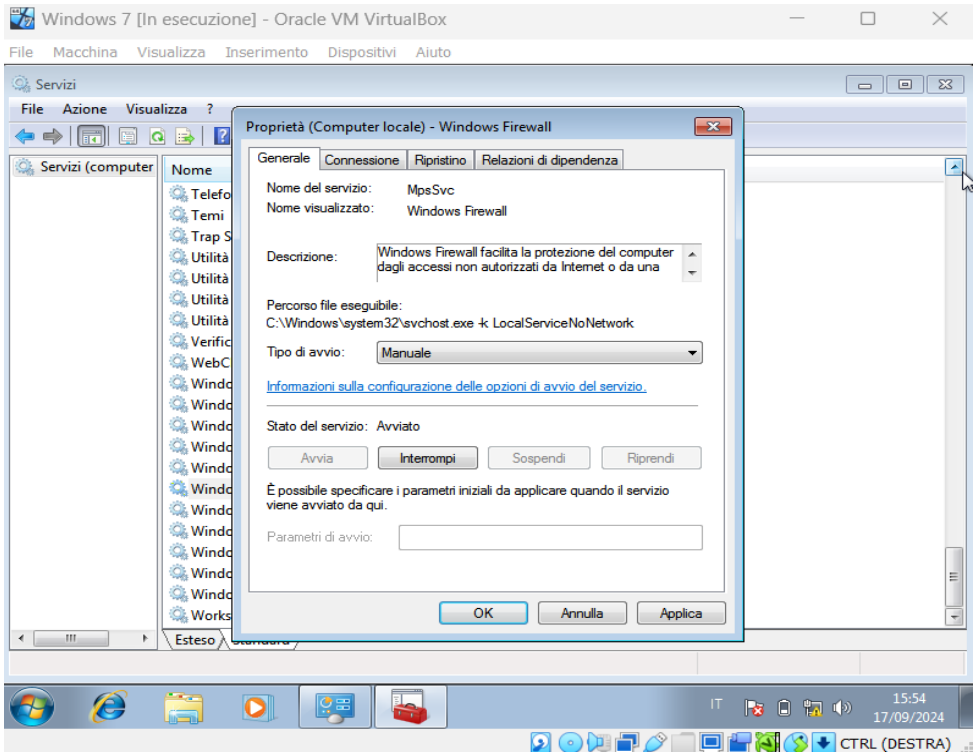
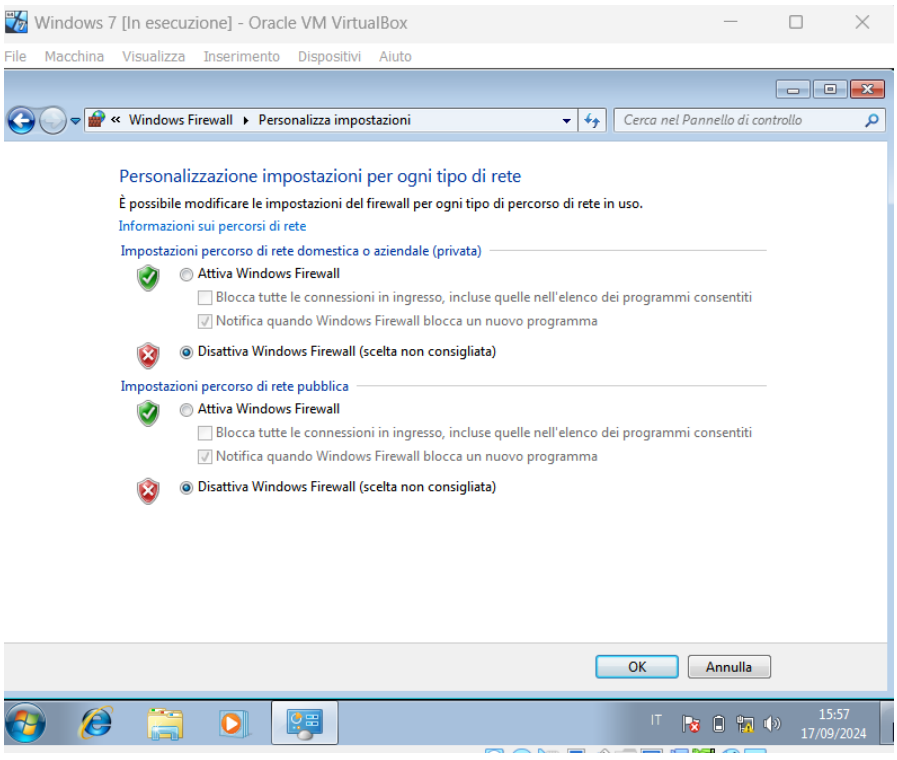
W18D1 – Firewall

Esercizio obbligatorio

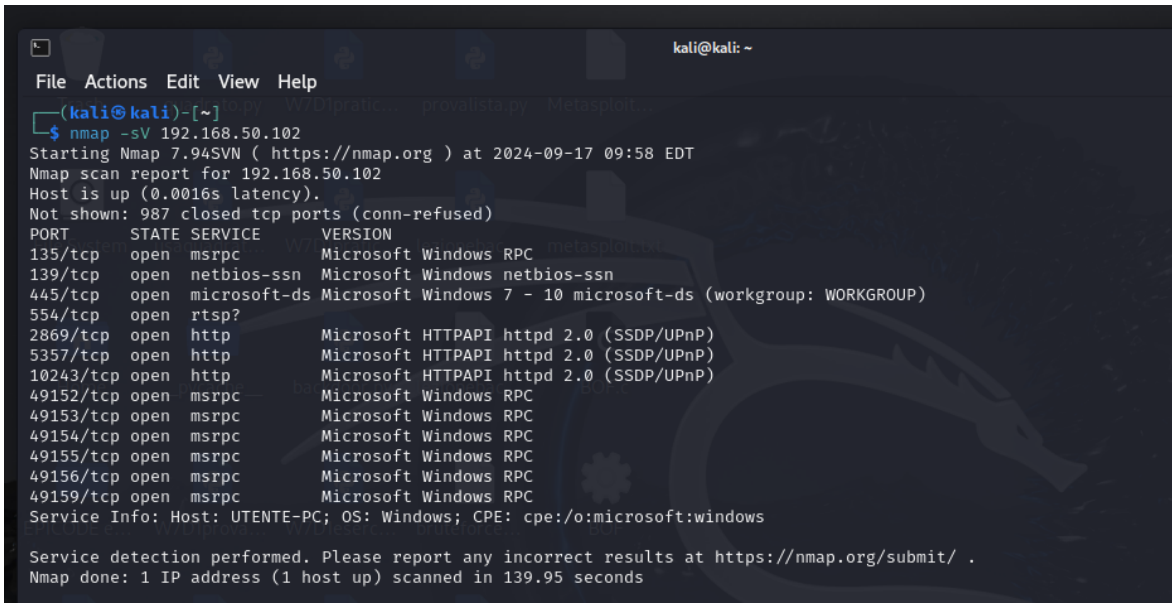
Nei "Servizi", ho impostato l'avvio del firewall su "manuale" per poter decidere ogni volta manualmente se avviare o meno il firewall.



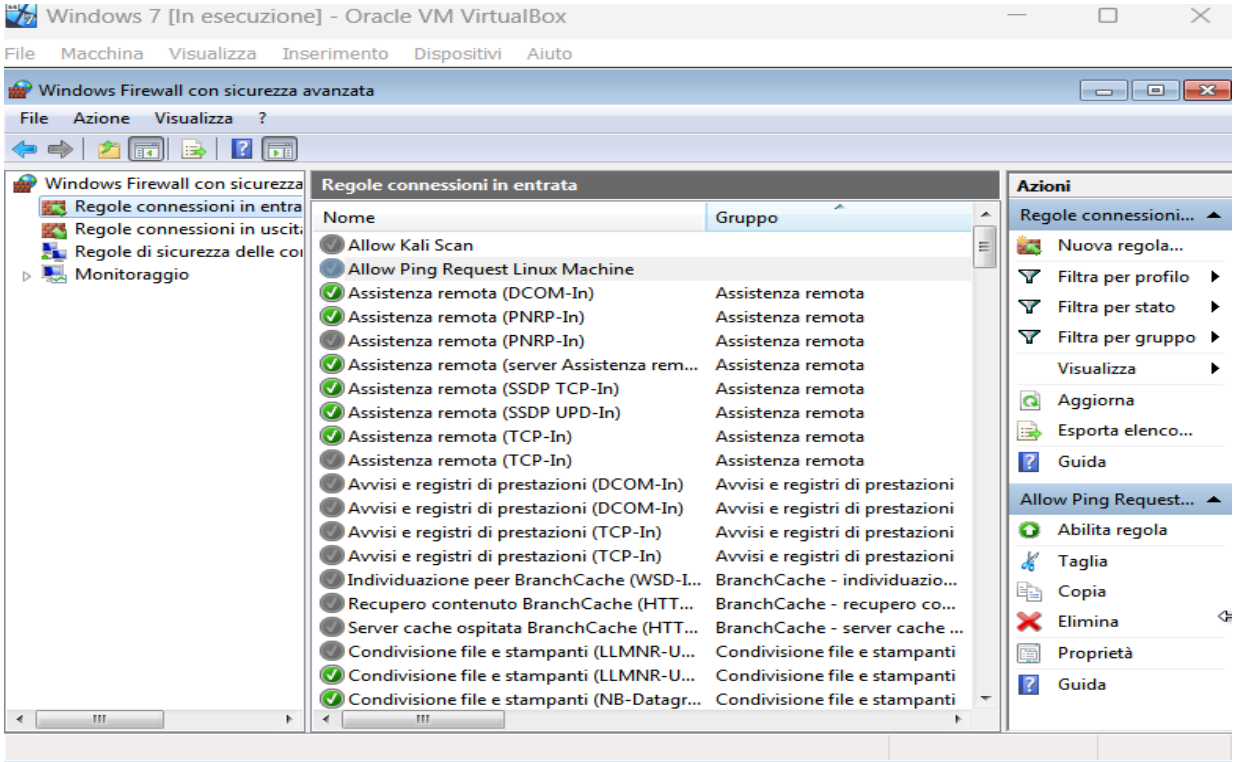
Dal pannello di controllo ho trovato le impostazioni del firewall e l'ho disattivato per eseguire la prima scansione con Nmap a firewall spento.



Ho quindi svolto la prima scansione della macchina target, ossia Windows 7 con IP 192.168.50.102, con Nmap ed ho impostato lo switch -sV per vedere le versioni dei servizi. Sono state trovate 13 porte attive.



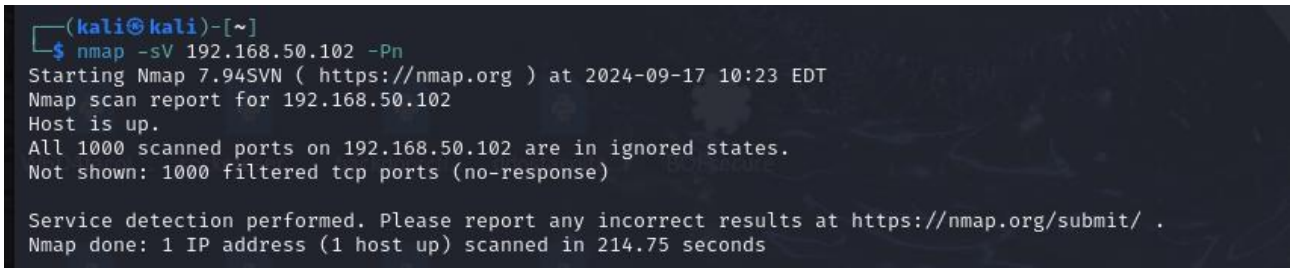
A questo punto sono tornata ad abilitare il firewall dal pannello di controllo, seguendo la stessa procedura fatta precedentemente per disattivarlo ed ho controllato le policy che avevo scritto in precedenza riguardo alle connessioni. Per simulare il funzionamento del firewall di base, senza le policy che avevo scritto, ho disabilitato le regole "Allow Kali Scan" ed "Allow Ping Request Linux Machine".



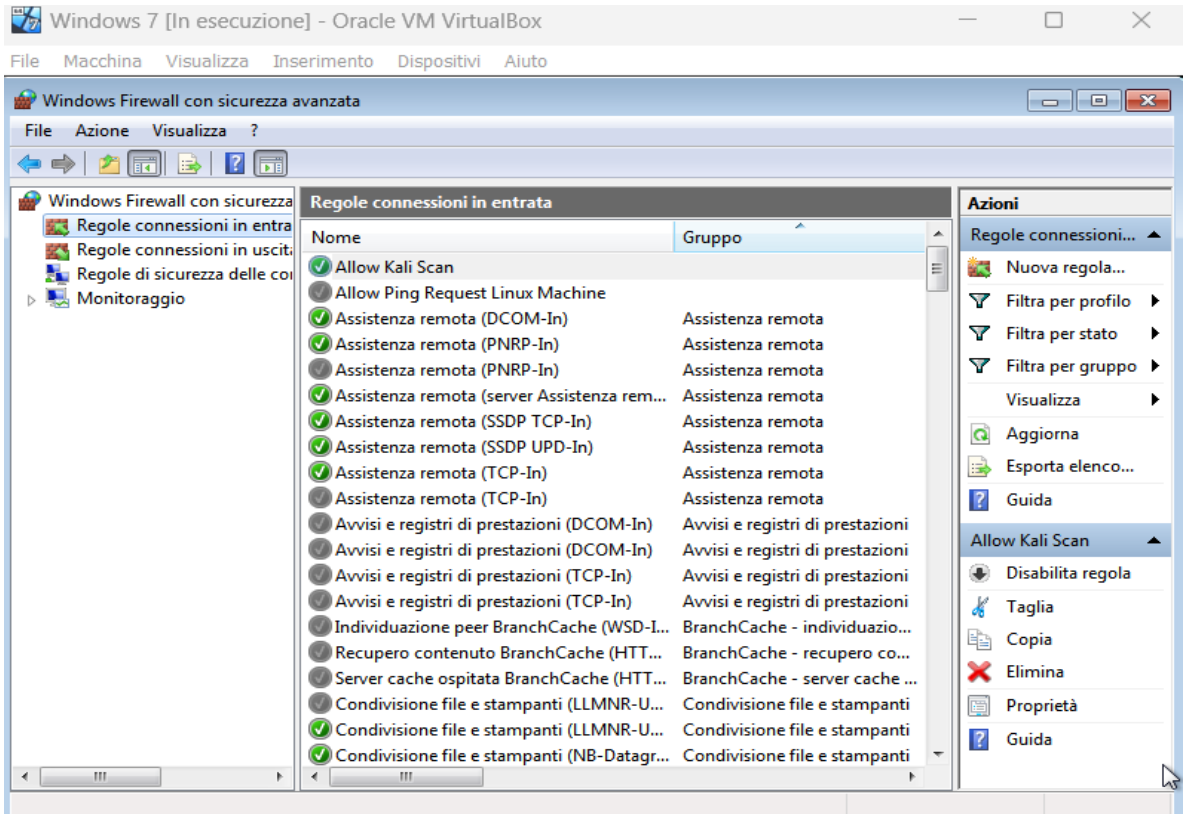
Ho quindi lanciato la scansione con Nmap e lo switch -sV ed è quindi evidente che il firewall funziona e sta bloccando il traffico in entrata con il protocollo del ping, ossia ICMP. La

macchina sembra spenta, proteggendola da un malintenzionato che cerca di scansionare l'host e il firewall blocca il ping, come spesso succede per evitare che una macchina venga trovata e scansionata.

Con lo switch -Pn ho disabilitato l'host discovery tramite ping per superare la barriera del ping e passare ad altro. Le porte risultano tutte filtrate, perché lo scanner non è riuscito a stabilire se siano aperte o chiuse e che servizio espongano e questa è opera del firewall, che scherma le porte in modo che risultino filtrate e che un possibile attaccante non riesca a studiare le porte aperte e i servizi per preparare un attacco. La differenza tra la prima e la terza scansione è evidente, perché nel primo caso era possibile fare una scansione dettagliata del target, mentre nel terzo caso l'utilizzo del firewall ha schermato le porte, bloccando le scansioni esterne che potrebbero essere alla base di un possibile attacco. Il firewall ha una funzione di protezione perché riduce la superficie di attacco e scherma porte e servizi vulnerabili.



Per completare l'esercizio ho abilitato di nuovo la regola "Allow Kali Scan" per consentire la scansione con Nmap da Kali, lasciando sempre disabilitata la policy che consente l'host discovery tramite ping.



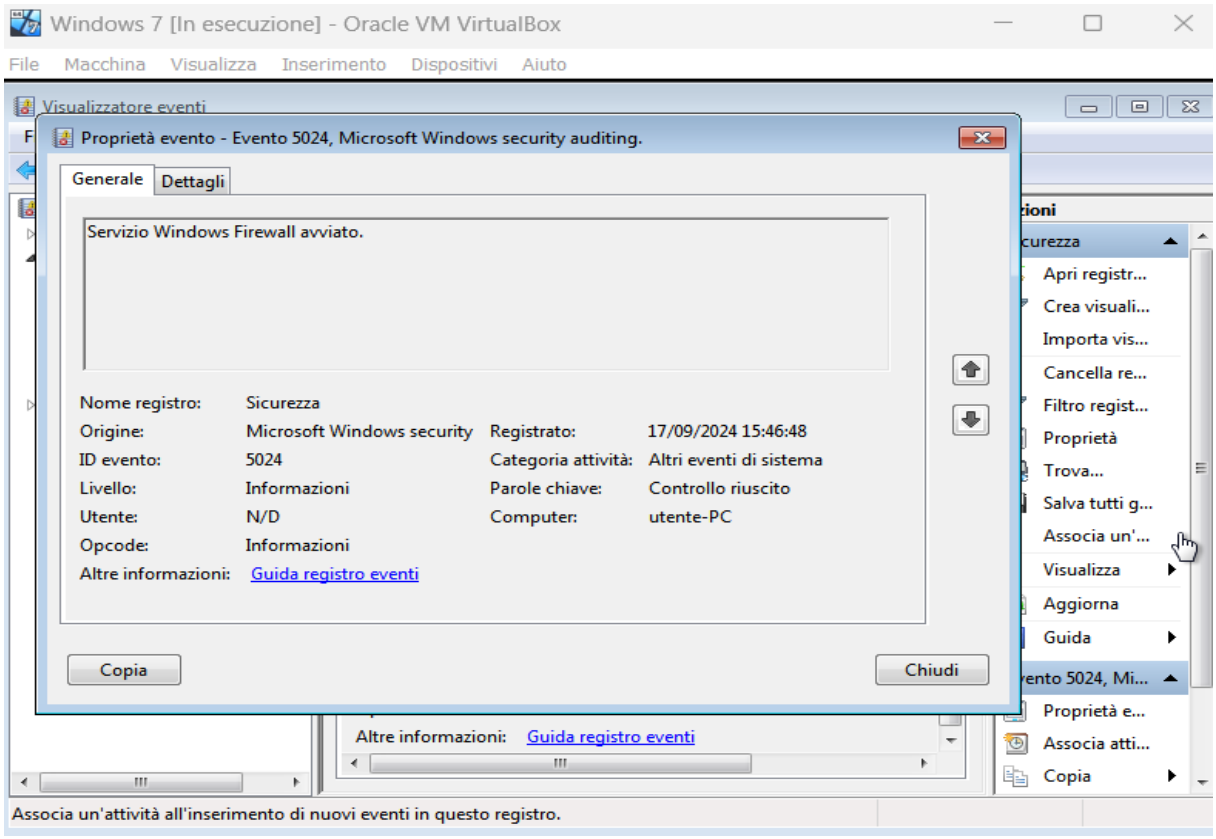
Ho rifatto la scansione con Nmap con gli switch -sV e -Pn attivati ed ho ottenuto lo stesso risultato della scansione di partenza, con il firewall disattivato. Le porte aperte sono sempre 13 e questo significa che il firewall, tramite le policy, è stato configurato per consentire la scansione all'host Kali sicuro, mostrando le porte ma evitando l'host discovery tramite ping. La configurazione del firewall e delle sue policy cambia completamente il risultato delle scansioni.

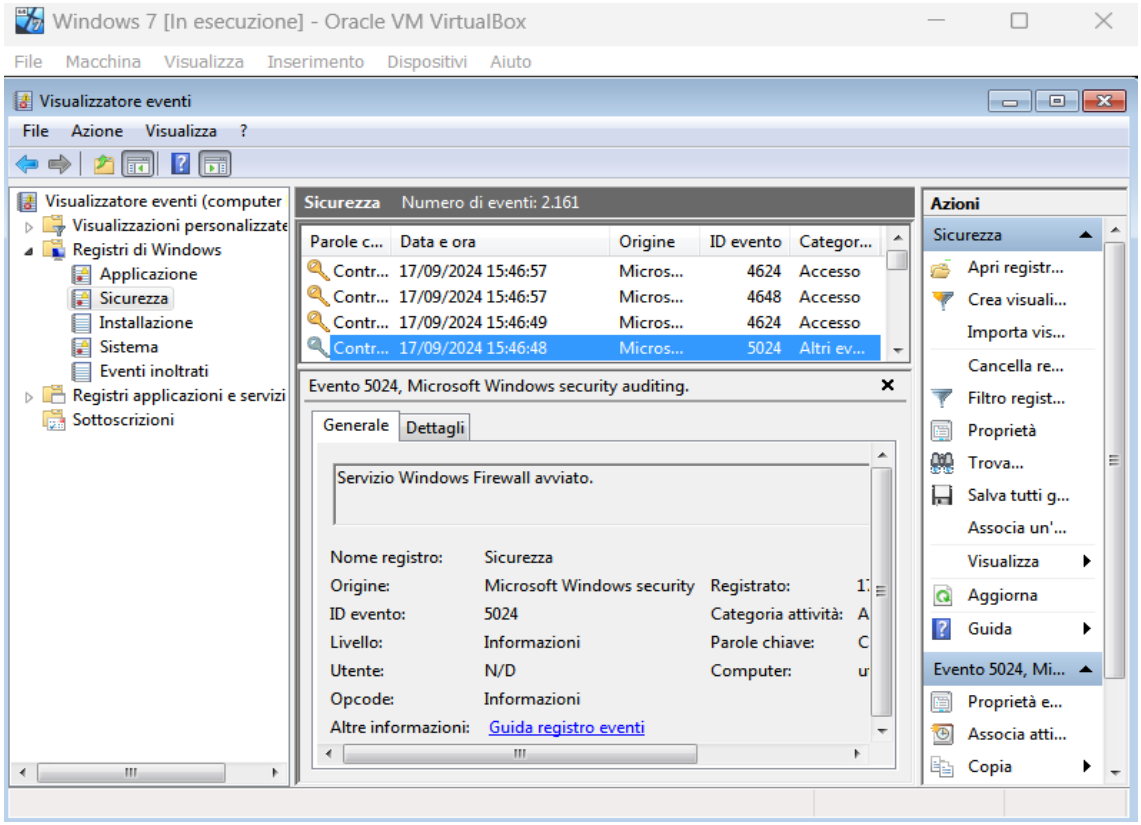
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.102 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-17 10:31 EDT
Nmap scan report for 192.168.50.102
Host is up (0.0050s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49159/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: UTENTE-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 143.04 seconds
```

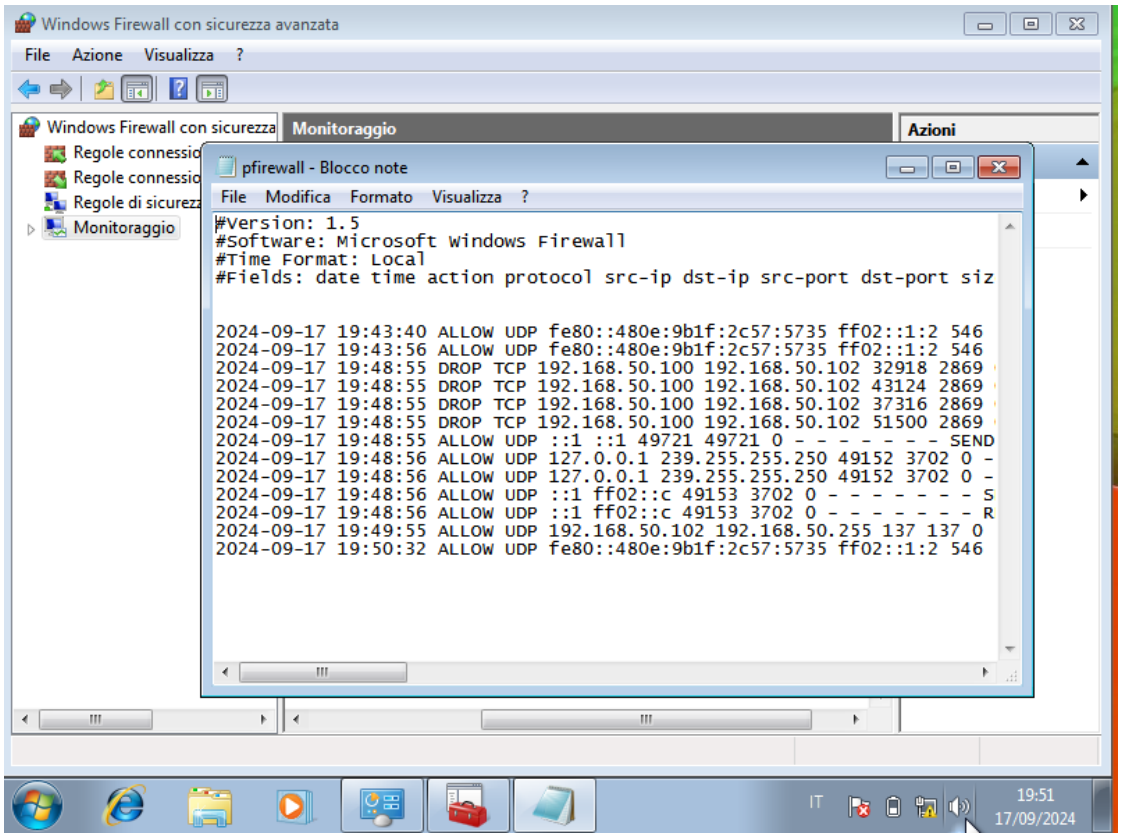
Esercizio facoltativo.

Per controllare le tracce di quanto avvenuto durante questo esercizio, ho monitorato i log di Windows. Sono andata nel Visualizzatore eventi, ho aperto i log di Windows ed ho monitorato gli eventi nel log "Sicurezza", che registra gli eventi riguardo alla sicurezza del dispositivo. Ho trovato traccia dell'attivazione del firewall, nell'evento con ID 5024, che riporta nel dettaglio la data e l'orario dell'attivazione, il computer e l'utente che ha effettuato questa modifica. Sono dati utili in caso di attacchi per recuperare informazioni forensi. L'unico log nel quale si trova traccia dell'attivazione del firewall è quello relativo alla Sicurezza e fornisce molte informazioni preziose non solo per ricostruire quando è stato attivato il firewall, ma anche altre informazioni riguardo alla sicurezza, come l'accesso degli account e la gestione dei privilegi.

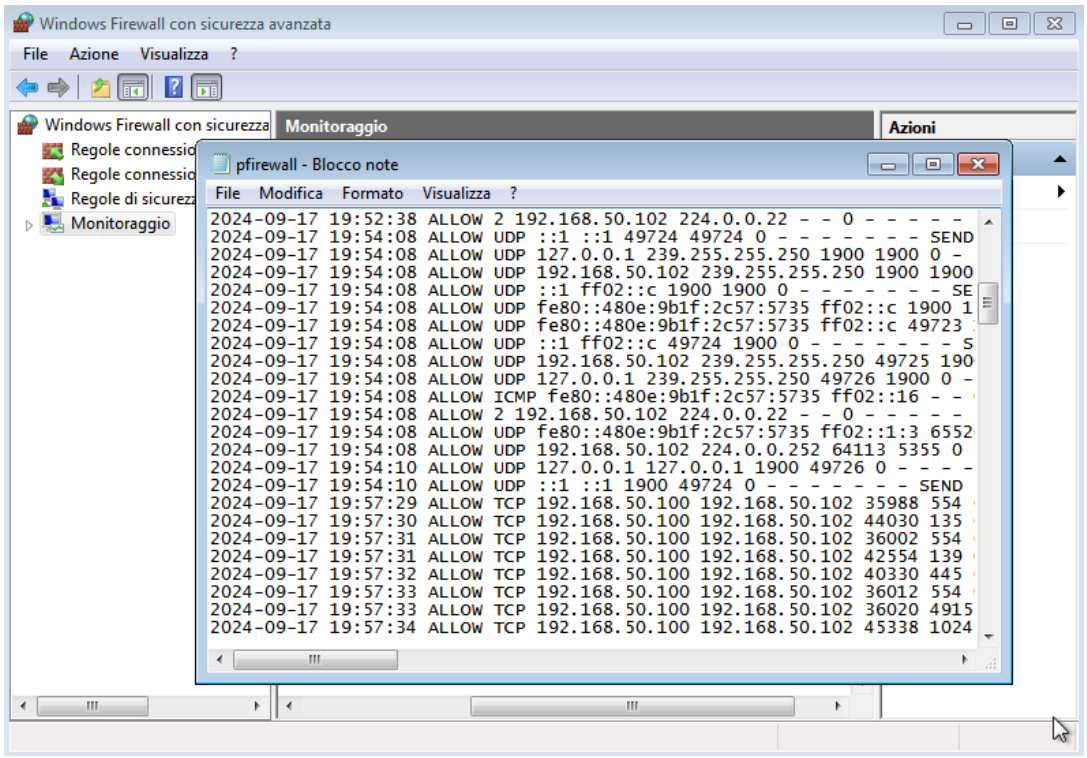


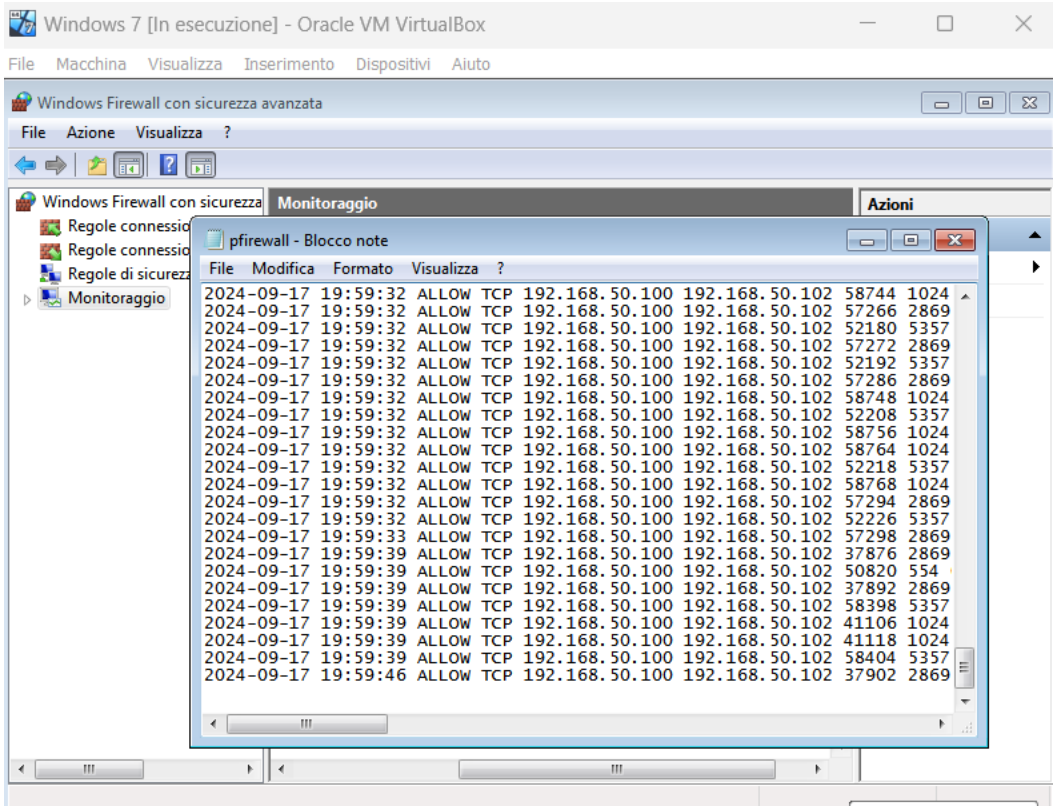


Ho controllato direttamente il log del firewall, che registra le connessioni che il firewall consente e le connessioni che invece vengono bloccate ed ho esaminato le differenze tra le varie scansioni. Quando il firewall è abilitato, la policy "Allow Kali Scan" è disabilitata e quindi le porte vengono filtrate per ragioni di sicurezza, si vede che le connessioni UDP vengono accettate, mentre le connessioni TCP vengono rifiutate. Le connessioni TCP sono molto più pericolose e quindi, per proteggere il computer, vengono abilitate solo le connessioni UDP. Per ogni connessione si vedono la data e l'ora, l'azione del firewall, il protocollo e dati come indirizzi MAC e IP. Le porte vengono quindi filtrate e nascoste ad eventuali utenti esterni malintenzionati, consentendo solo le connessioni UDP e non TCP.



Quando invece il firewall è attivo, abilito la policy "Allow Kali Scan" ed evito l'host discovery tramite ping, il firewall non deve nascondere le porte perché si basa sulla policy e considera l'indirizzo IP di Kali come sicuro. In questo modo, vengono mostrate tutte le porte senza schermarle. Questo si vede nel log del firewall, in cui si registra che il firewall consente sia le connessioni UDP sia le connessioni TCP. Le porte vengono quindi mostrate tutte, anche le porte TCP.




Windows 7 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Windows Firewall con sicurezza avanzata
File Azione Visualizza ?
Windows Firewall con sicurezza
Monitoraggio
Azioni
Regole connessio
Regole connessio
Regole di sicurez
Monitoraggio
pfirewall - Blocco note
File Modifica Formato Visualizza ?
2024-09-17 19:59:32 ALLOW TCP 192.168.50.100 192.168.50.102 58744 1024
2024-09-17 19:59:32 ALLOW TCP 192.168.50.100 192.168.50.102 57266 2869
2024-09-17 19:59:32 ALLOW TCP 192.168.50.100 192.168.50.102 52180 5357
2024-09-17 19:59:32 ALLOW TCP 192.168.50.100 192.168.50.102 57272 2869
2024-09-17 19:59:32 ALLOW TCP 192.168.50.100 192.168.50.102 52192 5357
2024-09-17 19:59:32 ALLOW TCP 192.168.50.100 192.168.50.102 57286 2869
2024-09-17 19:59:32 ALLOW TCP 192.168.50.100 192.168.50.102 58748 1024
2024-09-17 19:59:32 ALLOW TCP 192.168.50.100 192.168.50.102 52208 5357
2024-09-17 19:59:32 ALLOW TCP 192.168.50.100 192.168.50.102 58756 1024
2024-09-17 19:59:32 ALLOW TCP 192.168.50.100 192.168.50.102 58764 1024
2024-09-17 19:59:32 ALLOW TCP 192.168.50.100 192.168.50.102 52218 5357
2024-09-17 19:59:32 ALLOW TCP 192.168.50.100 192.168.50.102 58768 1024
2024-09-17 19:59:32 ALLOW TCP 192.168.50.100 192.168.50.102 57294 2869
2024-09-17 19:59:32 ALLOW TCP 192.168.50.100 192.168.50.102 52226 5357
2024-09-17 19:59:33 ALLOW TCP 192.168.50.100 192.168.50.102 57298 2869
2024-09-17 19:59:39 ALLOW TCP 192.168.50.100 192.168.50.102 37876 2869
2024-09-17 19:59:39 ALLOW TCP 192.168.50.100 192.168.50.102 50820 554
2024-09-17 19:59:39 ALLOW TCP 192.168.50.100 192.168.50.102 37892 2869
2024-09-17 19:59:39 ALLOW TCP 192.168.50.100 192.168.50.102 58398 5357
2024-09-17 19:59:39 ALLOW TCP 192.168.50.100 192.168.50.102 41106 1024
2024-09-17 19:59:39 ALLOW TCP 192.168.50.100 192.168.50.102 41118 1024
2024-09-17 19:59:39 ALLOW TCP 192.168.50.100 192.168.50.102 58404 5357
2024-09-17 19:59:46 ALLOW TCP 192.168.50.100 192.168.50.102 37902 2869