

10/11/2023

Ilaria Pedrelli

Configurazione Policy su Firewall e Packet Capture con Wireshark

Esercizio:

- Configurare policy per permettere il ping da macchine Linux a Macchina Windows 7 nel nostro laboratorio virtuale (windows firewall)
- Utilizzo dell'Utility InetSim per l'emulazione di servizi Internet
- Cattura di pacchetti con Wireshark

1. Utilizzo dell'Utility InetSim per l'emulazione di servizi Internet e Cattura di pacchetti con Wireshark

Per prima cosa, su laboratorio virtuale Kali Linux, configuro il software InetSim che mi permette di simulare una rete, per esempio, un web server.

Inizio la configurazione dal prompt di Kali, con **nano /etc/inetsim** poi mi sposto nella directory con **cd /etc/inetsim** all'interno della directory lancio il comando **ls** per vedere i file all'interno, nel mio caso trovo inetsim.conf e lo apro con il comando nano. Nel file vado a disattivare tutti i servizi con esclusione del servizio HTTPS. Commento quindi gli altri per disattivarli.

Modifico anche l'indirizzo IP LocalHost con l'indirizzo 127.0.0.1.

```
kali@kali: /etc/inetsim
File Actions Edit View Help

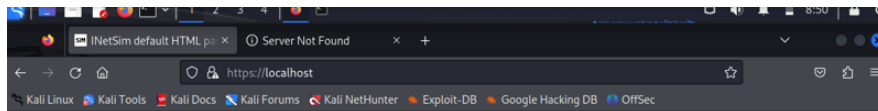
(kali@kali)-[/etc/inetsim]
$ nano inetsim.conf

(kali@kali)-[/etc/inetsim]
$ sudo nano /etc/inetsim/inetsim.conf
[sudo] password for kali:

(kali@kali)-[/etc/inetsim]
$ sudo inetsim
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory:      /var/log/inetsim/
Using data directory:     /var/lib/inetsim/
Using report directory:   /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
≡ INetSim main process started (PID 5003) ≡
Session ID:      5003
Listening on:    127.0.0.1
Real Date/Time:  2023-11-12 08:40:56
Fake Date/Time: 2023-11-12 08:40:56 (Delta: 0 seconds)
Forking services ...
  * https_443_tcp - started (PID 5005)
done.
Simulation running.
█
```

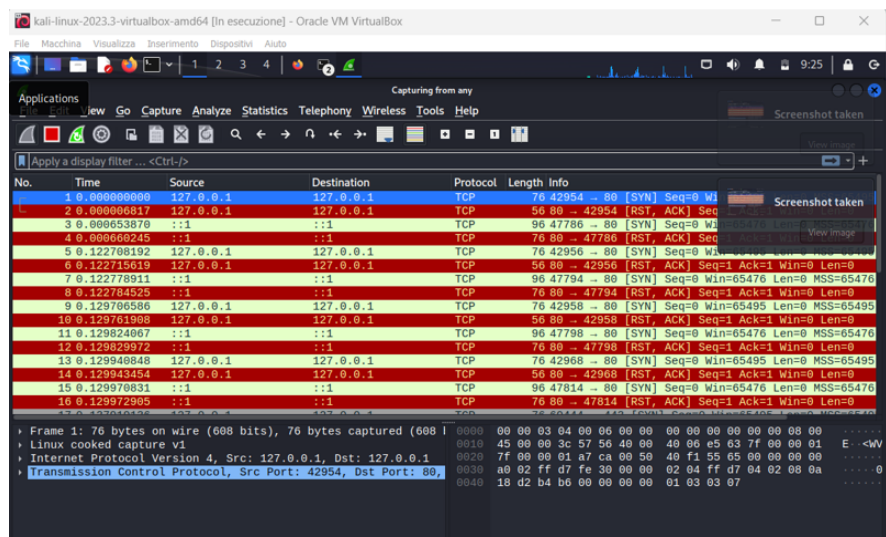
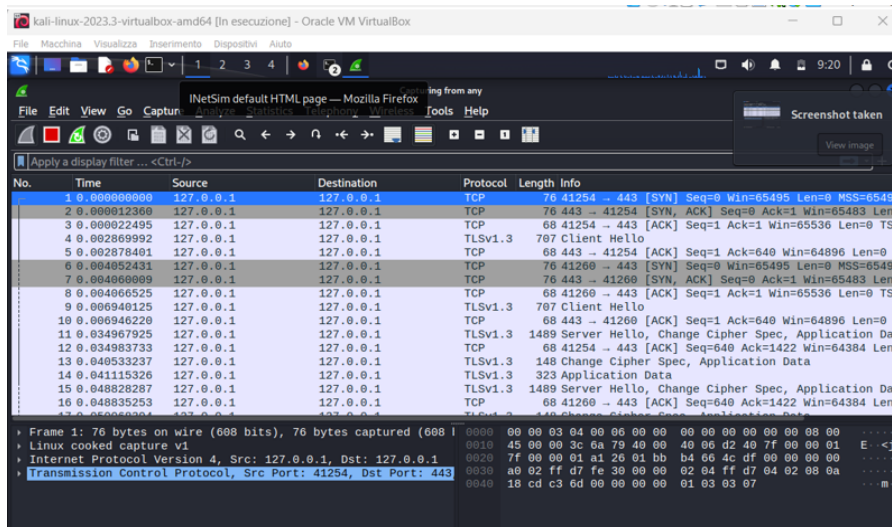
Successivamente testo la rete con l'indirizzo <https://localhost/> e mi restituisce una pagina fake HTML. Verifico, poi, il traffico del pacchetto su Wireshark. Posso notare che vengono intercettati pacchetti con richiesta GET su porta 443.

Su inetsim attivo anche il servizio HTTP per un'ulteriore prova e posso vedere che vengono intercettati i pacchetti con richiesta GET su porta 80.



This is the default HTML page for INetSim HTTP server fake mode.

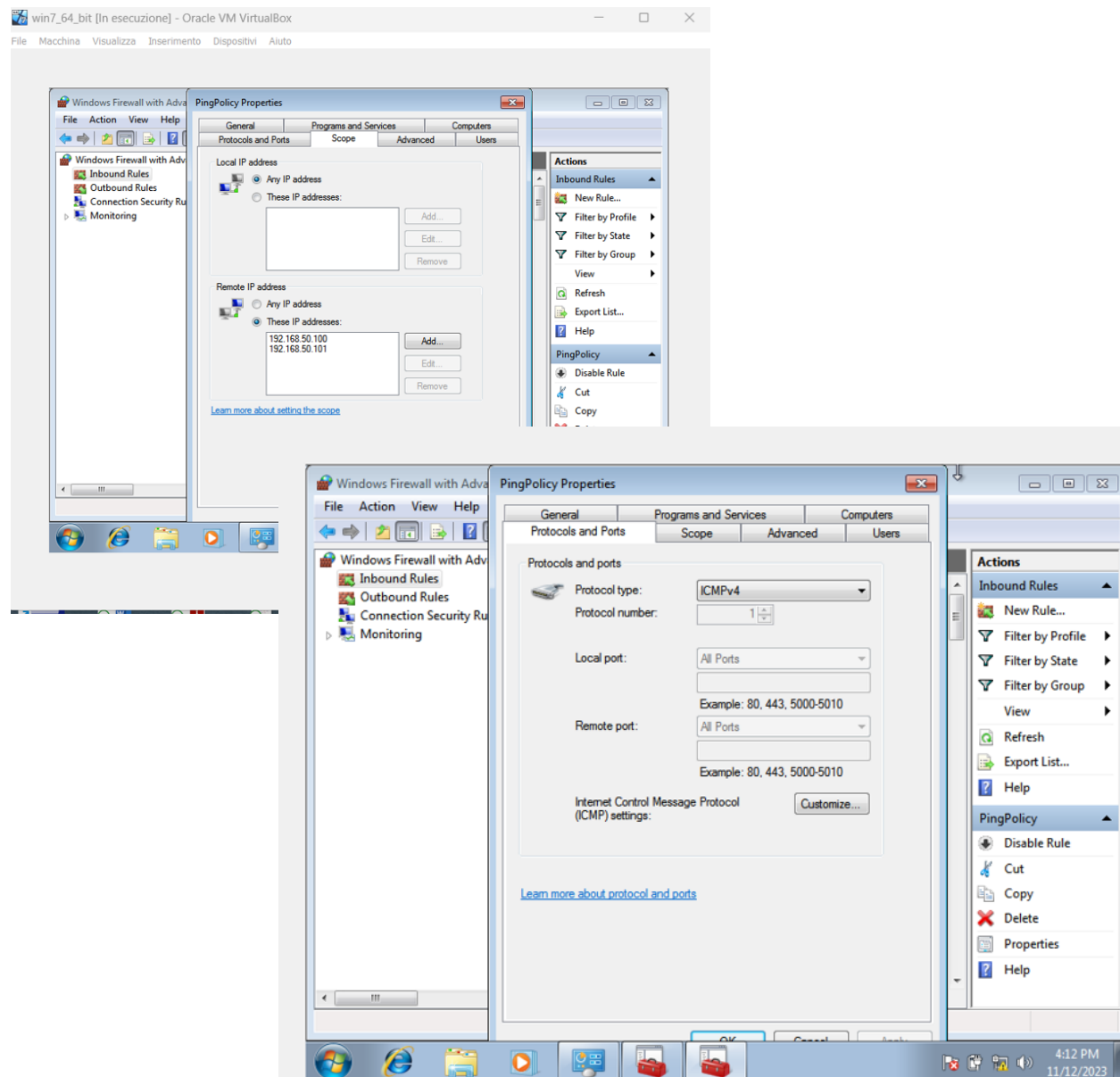
This file is an HTML document.



2. Configurare policy per permettere il ping da macchine Linux a Macchina Windows 7 nel nostro laboratorio virtuale (windows firewall)

Sul mio laboratorio virtuale avvio la macchina Window 7. Vado nelle configurazioni del Firewall e creo una nuova regola d'ingresso (INBOUND RULES). Imposto lo "scope": Local IP address (Win7) su any IP. Per remote IP address, imposto gli IP di Metasploitable e Kali.

In "protocols and ports" imposto il protocollo ICMPv4 per permettere il ping tra le macchine della nostra rete interna.



Verifico, infine, il ping dalla macchina Kali verso Win 7.

```
(kali㉿kali)-[~]  
$ ping 192.168.50.102  
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.  
64 bytes from 192.168.50.102: icmp_seq=1 ttl=128 time=1.23 ms  
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=0.554 ms  
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.723 ms  
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=0.729 ms  
64 bytes from 192.168.50.102: icmp_seq=5 ttl=128 time=0.594 ms  
64 bytes from 192.168.50.102: icmp_seq=6 ttl=128 time=0.715 ms  
64 bytes from 192.168.50.102: icmp_seq=7 ttl=128 time=0.561 ms  
64 bytes from 192.168.50.102: icmp_seq=8 ttl=128 time=0.721 ms  
64 bytes from 192.168.50.102: icmp_seq=9 ttl=128 time=0.670 ms  
^C  
— 192.168.50.102 ping statistics —  
9 packets transmitted, 9 received, 0% packet loss, time 8157ms  
rtt min/avg/max/mdev = 0.554/0.722/1.233/0.192 ms  
  
(kali㉿kali)-[~]  
$
```