M1-W3D4 - Pratica

DATA

Cybersecurity Analyst

Studente:

Andrea Scarmagnani

Docente:

Giuseppe Placanica

Esercizio:

L'esercizio di oggi mira a consolidare le conoscenze acquisite.

Vedremo due esercizi: I) la configurazione di una policy sul firewall windows; II) una packet capture con Wireshark.

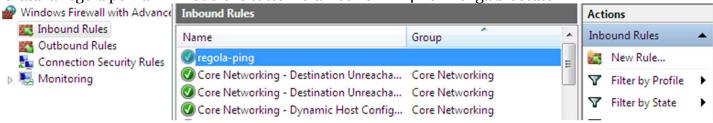
Vedremo anche come simulare alcuni servizi di rete con un tool pre-installato su Kali Linux (InetSim)

Esercizio:

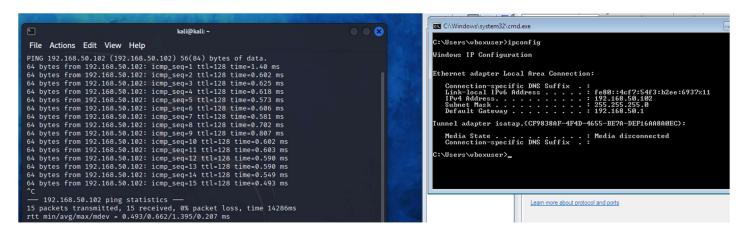
- Configurare policy per permettere il ping da macchine Linux a Macchina Windows 7 nel nostro laboratorio (Windows firewall);
- Utilizzo dell'utility InetSim per l'emulazione di servizi Internet;
- Cattura di pacchetti con Wireshark;

Configurare policy per permettere il ping da macchine Linux a Macchina Windows 7 nel nostro laboratorio (Windows firewall):

Crata la regola per far in modo che tutto il traffico ICMPv4 non venga bloccato



Qui sotto il ping eseguito dalla macchina Kali con destinazione macchina Win7

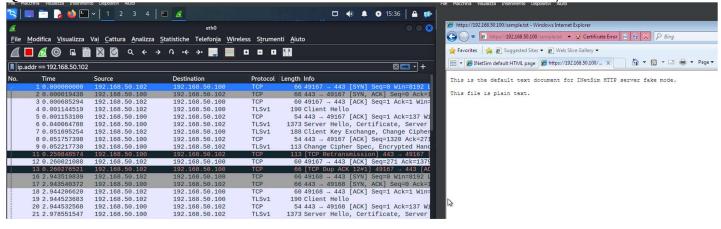


-Utilizzo dell'utility InetSim per l'emulazione di servizi Internet.

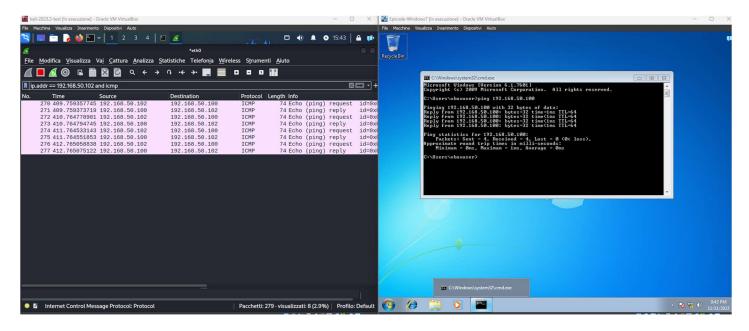
Qui sotto si vede il funzionamento e la corretta esecuzione di InetSim sulla macchina Kali all'indirizzo IP 192.168.50.100-

```
└$ inetsim
Sorry, this program must be started as root!
  -(kali⊛kali)-[~]
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 66212)
Session ID:
               66212
               192.168.50.100
Listening on:
Real Date/Time: 2023-11-11 15:32:41
Fake Date/Time: 2023-11-11 15:32:41 (Delta: 0 seconds)
 Forking services ...
  * http_80_tcp - started (PID 66214)
  * https_443_tcp - started (PID 66215)
done.
Simulation running.
```

Qui si vede come la macchina Kali ha catturato le richiese della macchina Win7.



Qui si vede come la macchina Kali ha catturato le richieste ICMP della macchina Win7 192.168.50.102.



Cybersecurity Analyst 2023