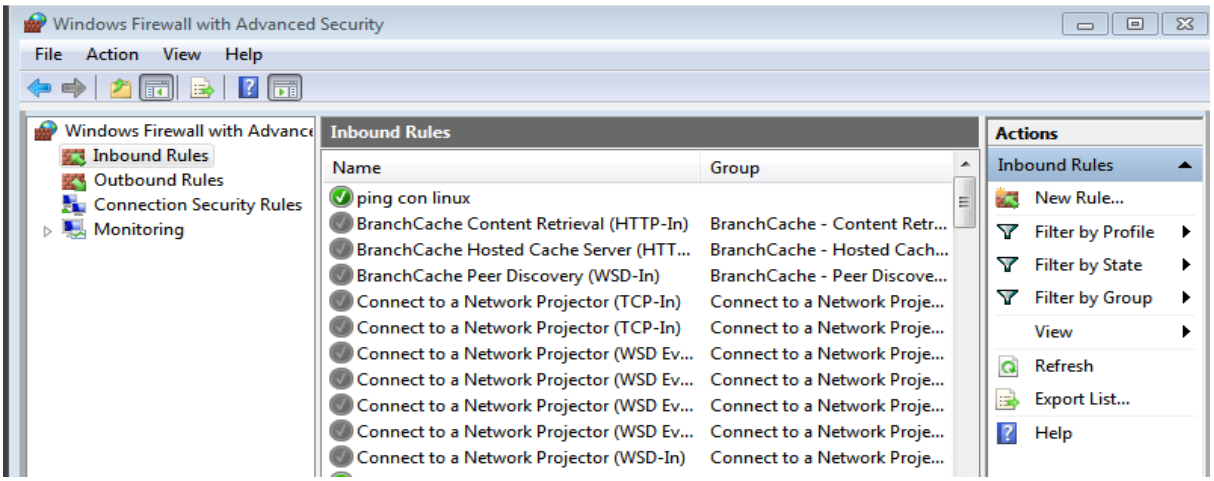
ESERCIZIO GIORNATA 6

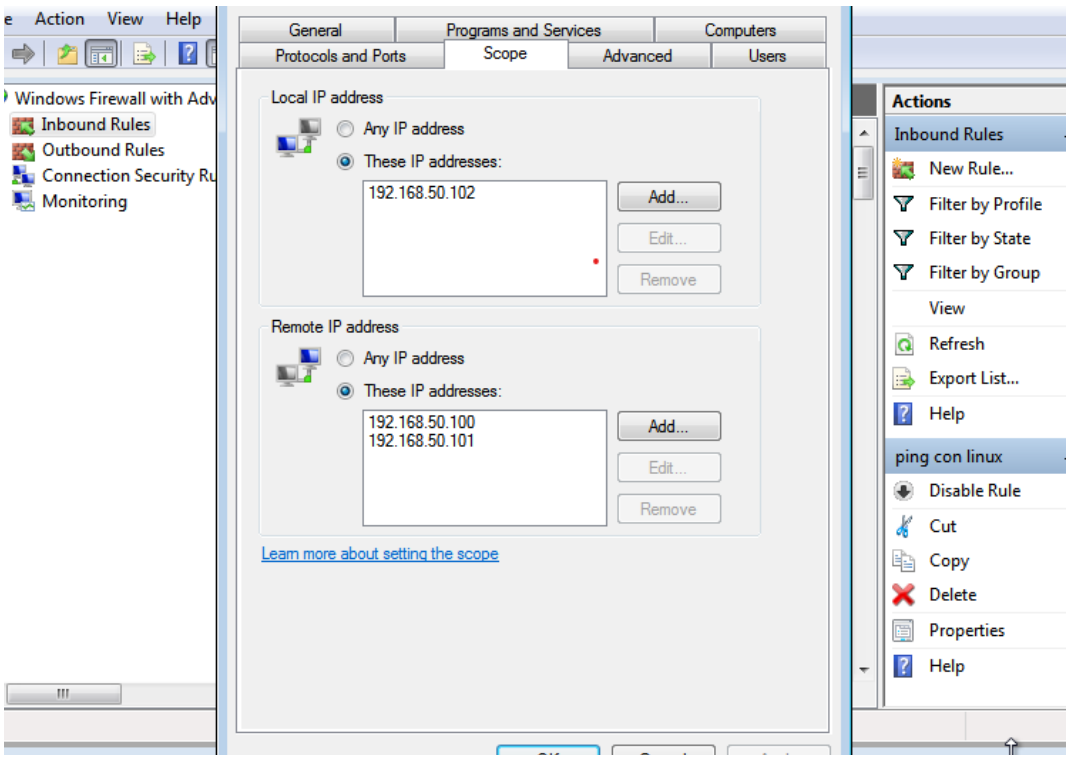
Oggi ci è stato chiesto di configurare una policy del software firewall e di fare una pocket capture usando Wireshark tramite l'utilizzo delle nostre macchine virtuali Kali e quella Win.7.

Configurazione Policy:

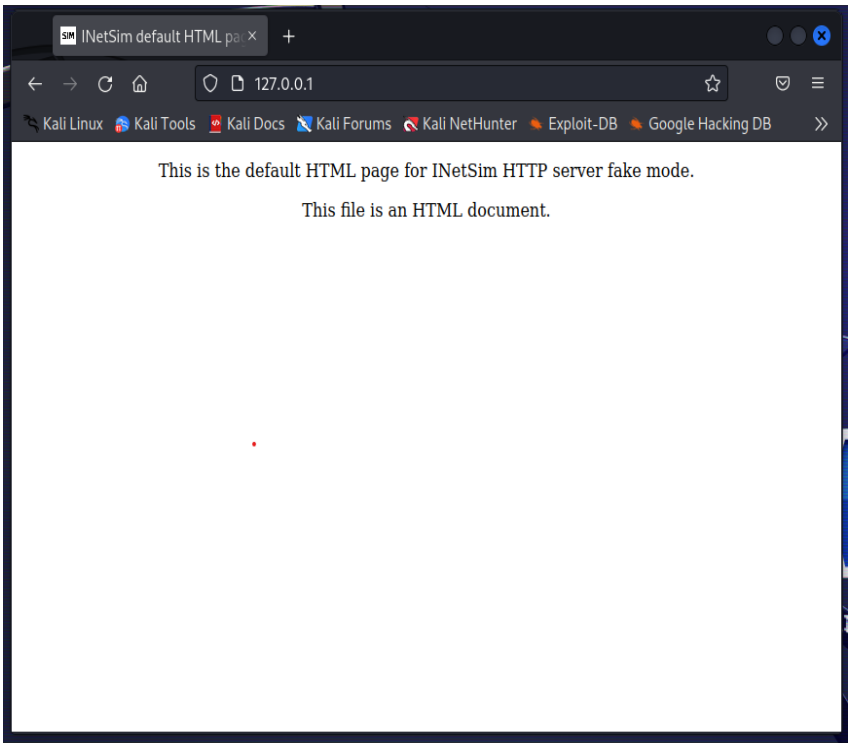


Accedendo alle sezione "Windows Firewall Advanced Security" e selezionando la voce "inbound rules" (come possiamo vedere in figura) sono andato a creare una nuova "regola" nella voce "Action". Dopo aver configurato alcune impostazioni, sono andato nella voce "scope" e ho impostato manualmente il Local IP, mettendo come IP quello assegnato alla macchina WIN.7, e come Remote IP quelli delle macchine linux.

Facendo ciò ho permesso nonostante la presenza del firewall il ping tra le varie macchine. Per controllare se l'operazione fosse andata a buon fine, mi sono spostato sulla macchina Linux Kali e avviando il tool Wireshark ho controllato fosse presente il traffico di informazioni tra le due macchine.


Action View Help
Windows Firewall with Adv
Inbound Rules
Outbound Rules
Connection Security Ru
Monitoring
General
Programs and Services
Computers
Protocols and Ports
Scope
Advanced
Users
Local IP address
Any IP address
These IP addresses:
192.168.50.102
Add...
Edit...
Remove
Remote IP address
Any IP address
These IP addresses:
192.168.50.100
192.168.50.101
Add...
Edit...
Remove
Learn more about setting the scope
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
ping con linux
Disable Rule
Cut
Copy
Delete
Properties
Help


File Actions Edit View Help
* daytime_13_tcp - started (PID 3176)
* quotd_17_tcp - started (PID 3182)
* syslog_514_udp - started (PID 3173)
* ftp_21_tcp - started (PID 3166)
* ftps_990_tcp - started (PID 3167)
* finger_79_tcp - started (PID 3171)
* chargen_19_tcp - started (PID 3184)
* smtp_25_tcp - started (PID 3162)
* irc_6667_tcp - started (PID 3169)
* https_443_tcp - started (PID 3161)
* echo_7_udp - started (PID 3179)
* ntp_123_udp - started (PID 3170)
* pop3s_995_tcp - started (PID 3165)
* pop3_110_tcp - started (PID 3164)
* chargen_19_udp - started (PID 3185)
* smtps_465_tcp - started (PID 3163)
* time_37_tcp - started (PID 3174)
* echo_7_tcp - started (PID 3178)
* dummy_1_udp - started (PID 3187)
* dummy_1_tcp - started (PID 3186)
* tftp_69_udp - started (PID 3168)
* daytime_13_udp - started (PID 3177)
* http_80_tcp - started (PID 3160)
* discard_9_udp - started (PID 3181)
done.
Simulation running.


INetSim default HTML pa
127.0.0.1
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
This is the default HTML page for INetSim HTTP server fake mode.
This file is an HTML document.

Emulazione servizi internet e uso di Wireshark:

Avviando la macchina linux kali, aprendo il terminale ho eseguito il comando “sudo inetsim” facendo ciò il comando stesso ha iniziato l’emulazione di alcuni protocolli. Fatto ciò sono andato su firefox e mettendo nella barra di ricerca l’IP 127.0.0.1 (controllato usando il comando ifconfig) si è avviata la simulazione di una pagina/documento HTML grazie all’utility inetsim. Infine aprendo wiresharck nella sezione “loopback” e ricaricando la pagina firefox sono comparsi i pacchetti (evidenziati in verde) come da consegna.