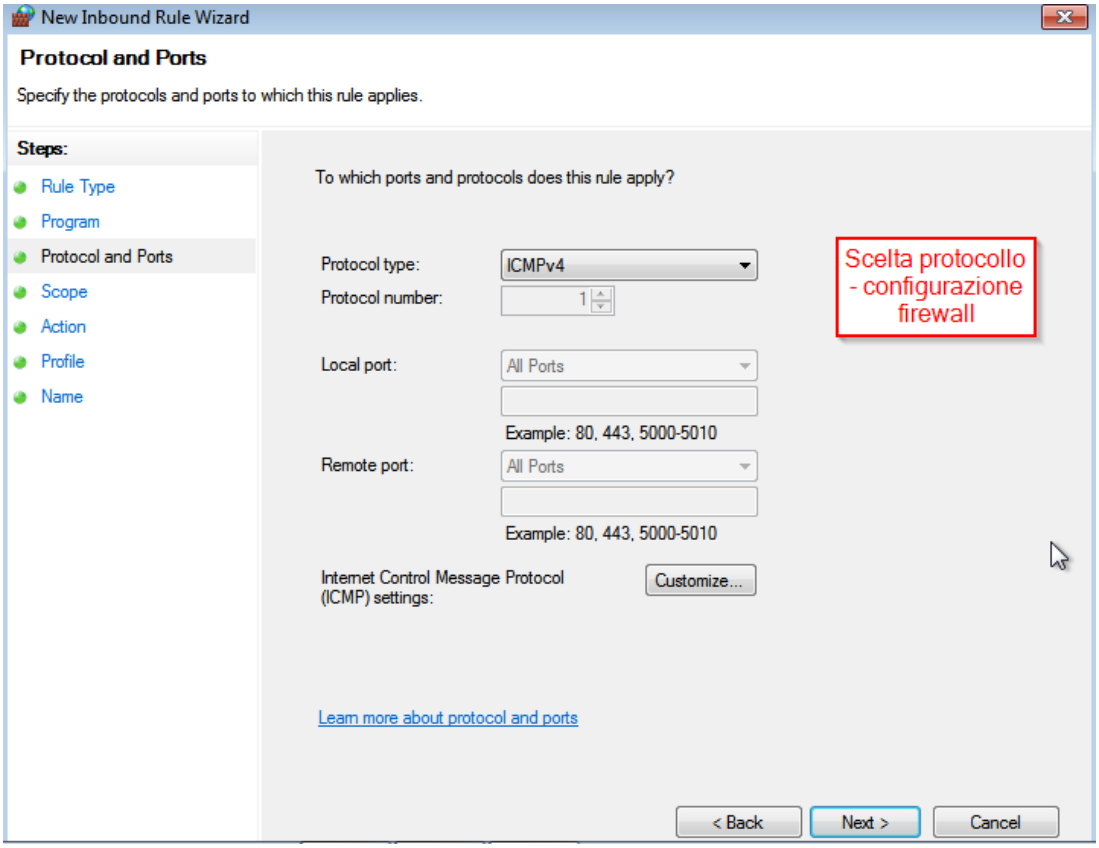
ESERCIZIO EPICODE W3D4

L'esercizio punta alla corretta configurazione di un' eccezione sul firewall Windows, assieme al packet capture su Wireshark. Le tracce mostrate sono le seguenti:

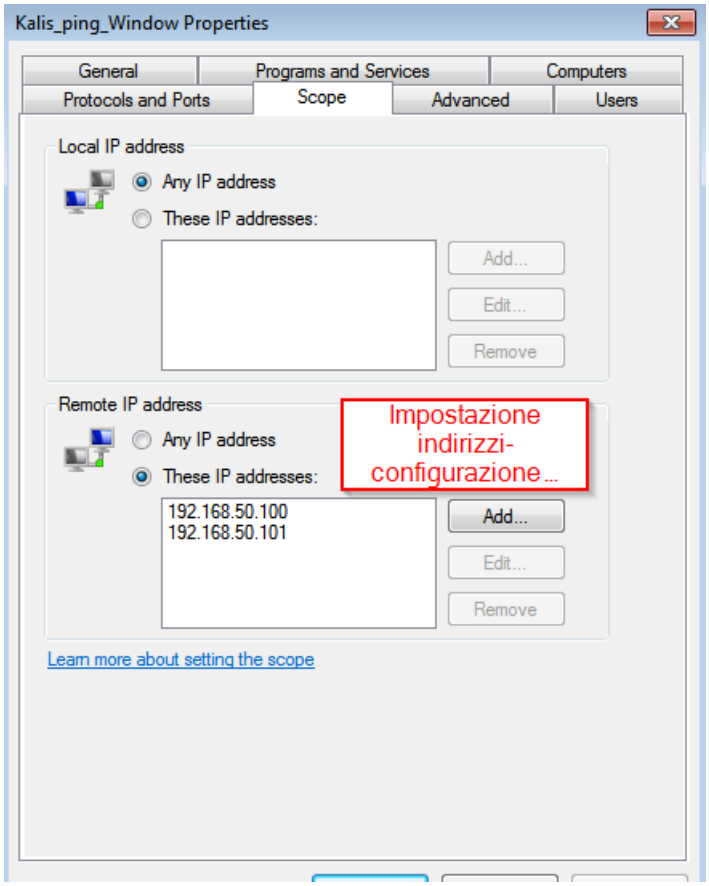
- Configurare policy per permettere il ping da macchine Linux a Macchina Windows 7 nel nostro laboratorio (Windows firewall).
- Utilizzo dell'utility InetSim per l'emulazione di servizi Internet.
- Cattura di pacchetti con Wireshark.

Configurazione eccezione firewall Windows

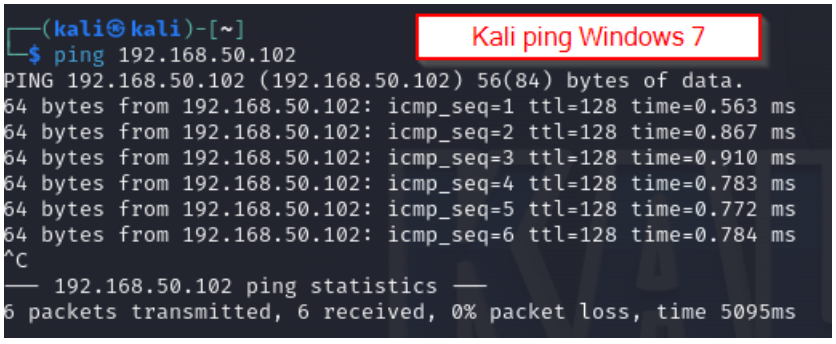
Prima di tutto, seguiamo quest'ordine per raggiungere la casella qua sottostante Windows Firewall->Advanced settings->New Rule->Custom. A quel punto entriamo in Protocols and Ports per specificare quale tipo di protocollo interesserà la regola. Scegliamo ICMP in modo da consentire lo scambio di ping tra macchine Linux e Windows 7.

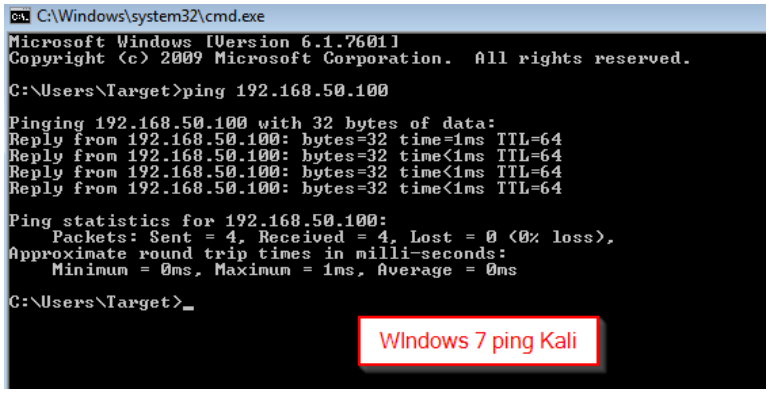


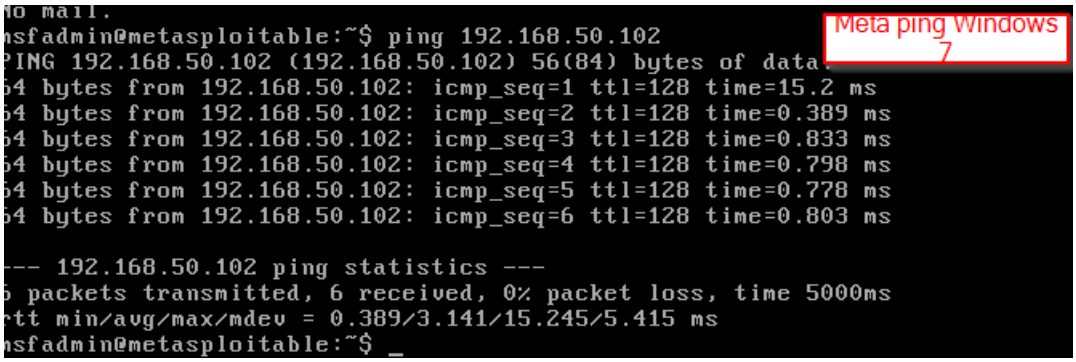
Dopo di che procediamo a cliccare la sezione Scope. Nella finestra andremo ad indicare quali sono gli IP address che invieranno i pacchetti ICMP a Windows. 192.168.50.100 per Kali e 192.168.50.101 per Metaploitable.

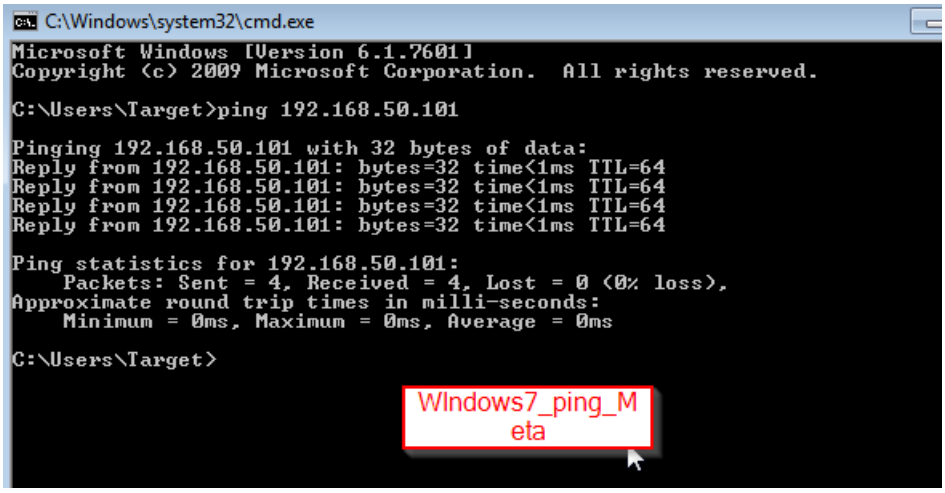


Dopo questi passaggi non ci resta che confermare il Ping tra le due parti. Andiamo ad aprire il Prompt dei comandi per testare la ricezione di Kali, Metasploitable e Windows 7.



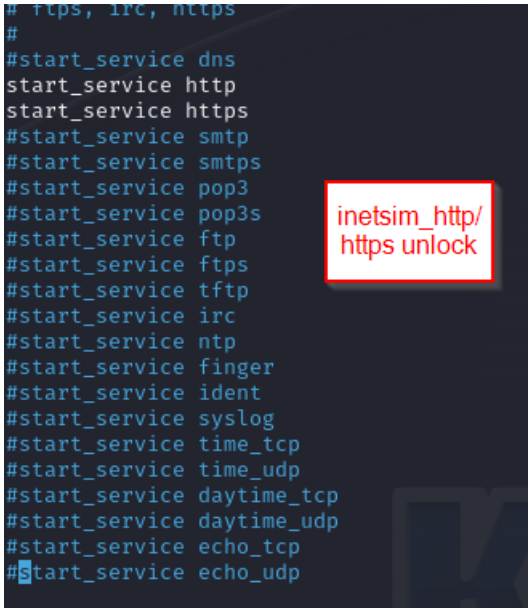




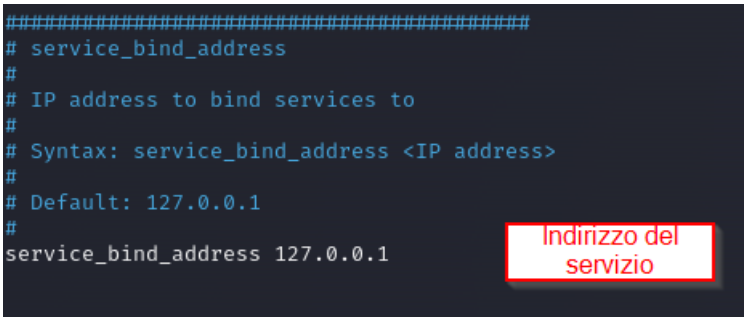


Configurazione e utilizzo inetsim

Per attivare il servizio inetsim iniziamo con l'entrare nella cartella giusta. Dentro il prompt di Kali Linux, inseriamo cd /etc/inetsim. Per essere sicuri di aver fatto centro, possiamo anche controllare il contenuto della cartella grazie al comando ls. A questo punto dovremmo riuscire a vedere il file di testo inetsim.conf. Per entrarci dentro con i diritti amministrativi usiamo il comando sudo nano inetsim.conf.

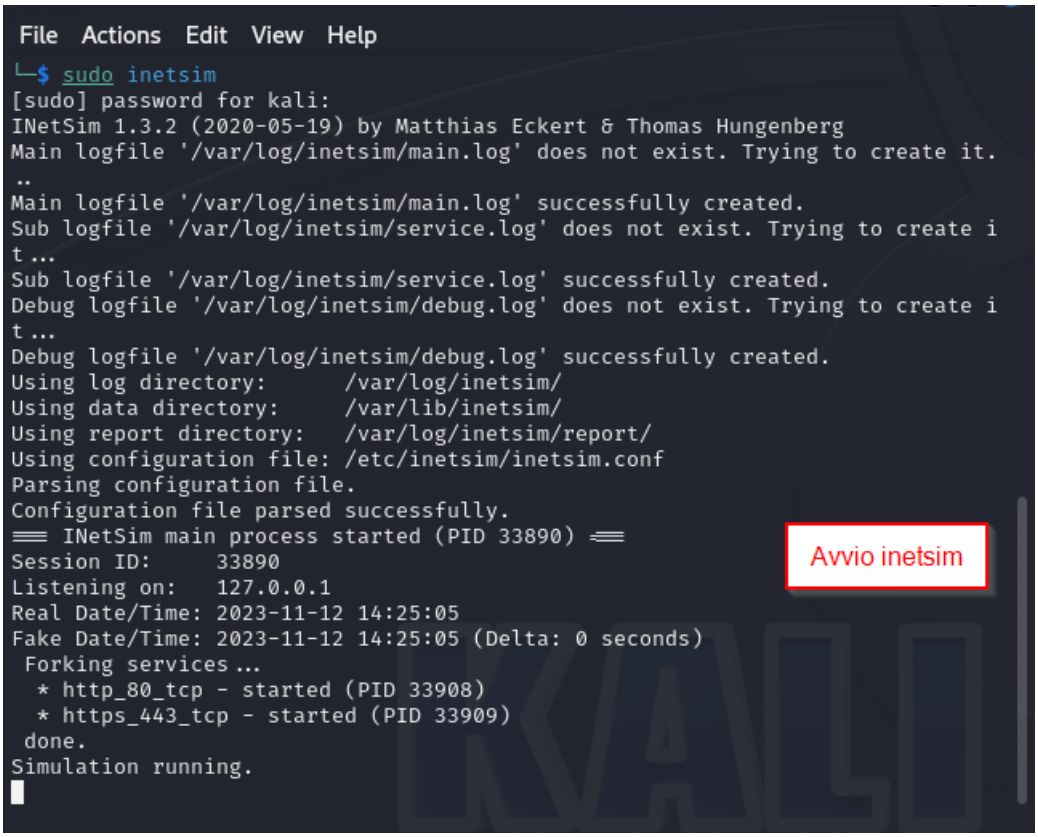


Scorriamo il contenuto del testo per attivare solo i servizi HTTP/HTTPS, il resto sarà coperto con il carattere griglia a fianco. Dopo questo non resta che modificare il bind_address IP, che scegliamo essere 127.0.0.1.



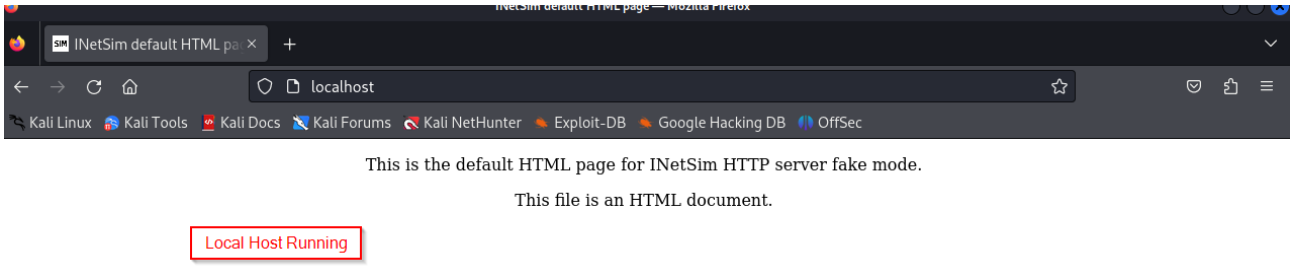

```
##############################################
# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
service_bind_address 127.0.0.1
```

Salviamo il contenuto con CTRL+Y per uscire dal servizio nano e torniamo alla finestra principale del prompt. Attiviamo ora il servizio sudo inetsim.



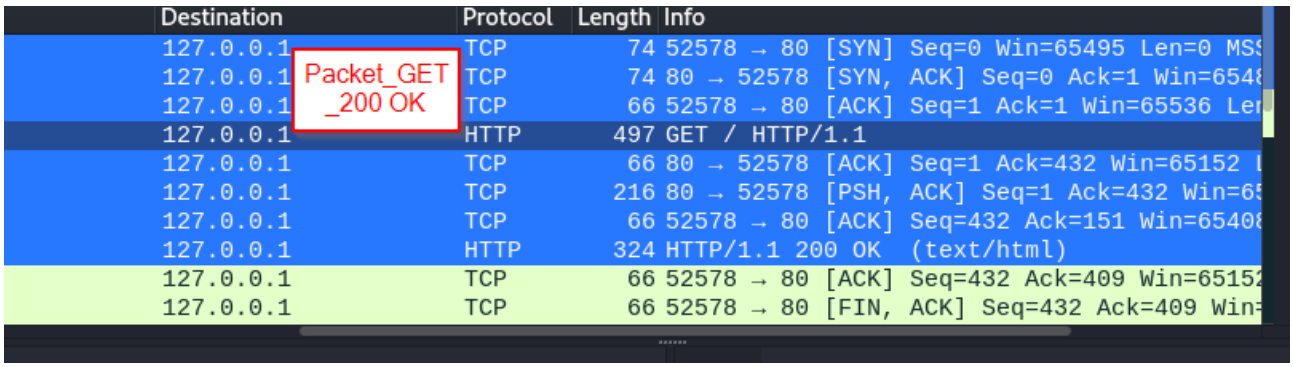

```
File  Actions  Edit  View  Help
└─$ sudo inetsim
[sudo] password for kali:
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Main logfile '/var/log/inetsim/main.log' does not exist. Trying to create it.
..
Main logfile '/var/log/inetsim/main.log' successfully created.
Sub logfile '/var/log/inetsim/service.log' does not exist. Trying to create i
t ...
Sub logfile '/var/log/inetsim/service.log' successfully created.
Debug logfile '/var/log/inetsim/debug.log' does not exist. Trying to create i
t ...
Debug logfile '/var/log/inetsim/debug.log' successfully created.
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 33890) ===
Session ID:     33890
Listening on:   127.0.0.1
Real Date/Time: 2023-11-12 14:25:05
Fake Date/Time: 2023-11-12 14:25:05 (Delta: 0 seconds)
 Forking services ...
  * http_80_tcp - started (PID 33908)
  * https_443_tcp - started (PID 33909)
 done.
Simulation running.
```

Ultima cosa da controllare, per essere sicuri che funziona, è l'inserimento sul browser dell'url http://localhost. Se la pagina si carica, allora la configurazione è riuscita bene.

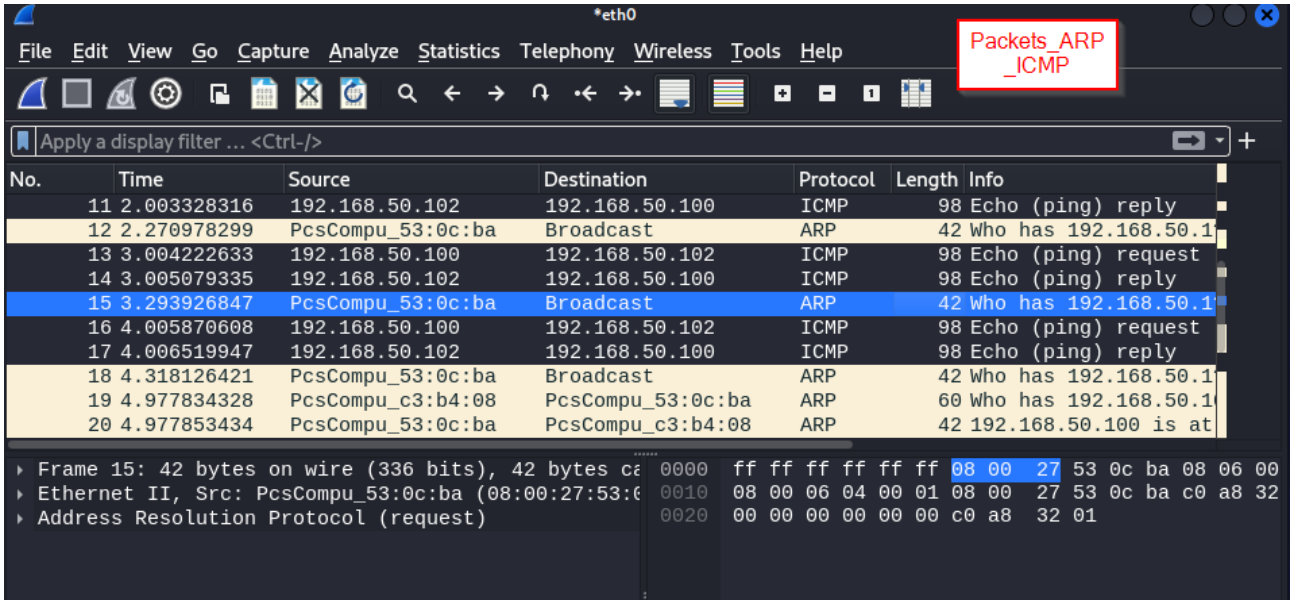


Cattura di Packets con Wireshark

La terza e ultima richiesta prevede invece la cattura di packets tramite Wireshark. Per prima cosa andremo a visualizzare il traffico generato dall'indirizzo localhost 127.0.0.1, presente nell'interfaccia loopback.



Una volta attivato il servizio inetsim e caricata la pagina web, sopra Wireshark appariranno le richieste GET assieme alla risposta del web server(200 OK). Sulla finestra compare anche il three-way-handshake. Ora che abbiamo raccolto i packet della pagina web, possiamo passare all'interfaccia eth0 per il catturare i messaggi ICMP tra le macchine.



Sull’interfaccia troviamo gli ICMP echo request e replay tra Kali e Windows. Da notare il fatto che prima di partire con i ping, Kali invia un ARP request per scoprire l’indirizzo IP della macchina destinataria, Windows 7.