

REPORT

CONFIGURAZIONE DI UNA POLICY, WIRESHARK, INETSIM

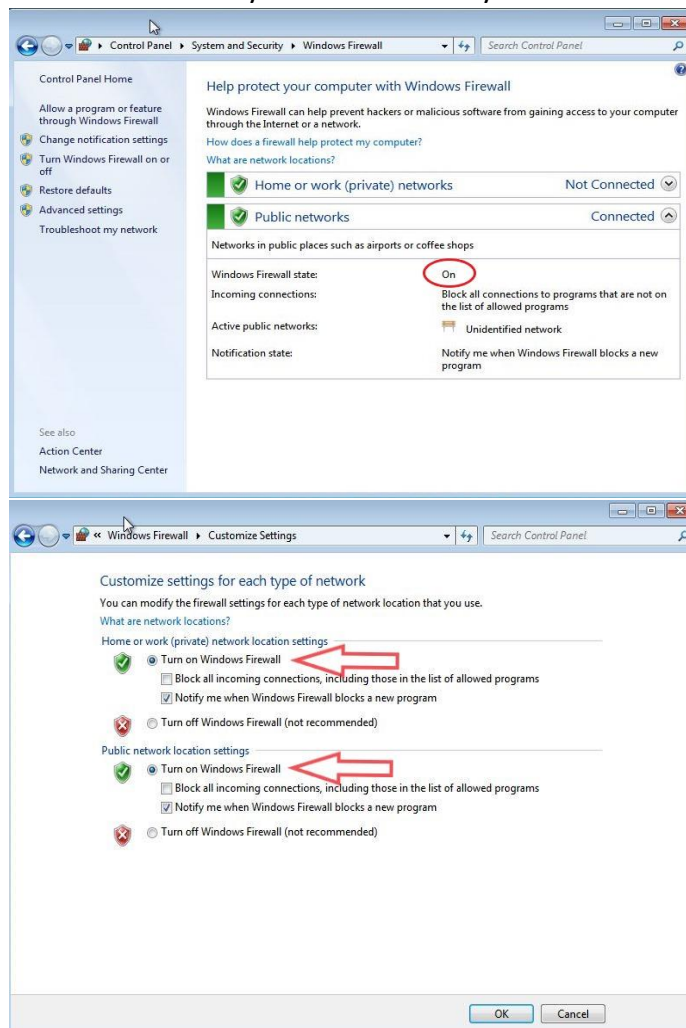
TASK

1. Configurazione policy per il ping da macchina Linux a Macchina Windows
2. Utilizzo dell'utility InetSim per l'emulazione di servizi Internet
3. Cattura di pacchetti con Wireshark

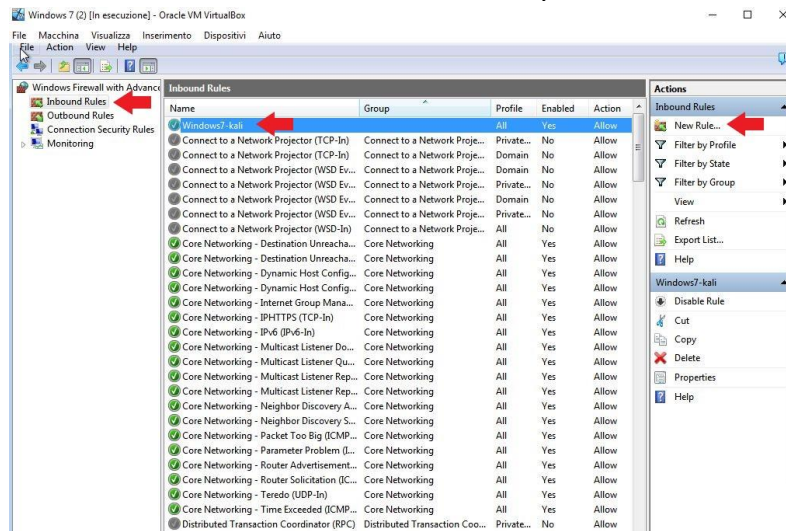
PREMESSA: Siamo in una rete Locale Interna pertanto è stato impostato a priori nella VirtualBox di Kali e di Windows un impostazione di rete Interna.

ANALISI E VALUTAZIONI

1. Iniziamo nel configurare Windows Firewall attivandolo dai seguenti passaggi:
Control Panel → System and Security → Windows Firewall → Change notification settings

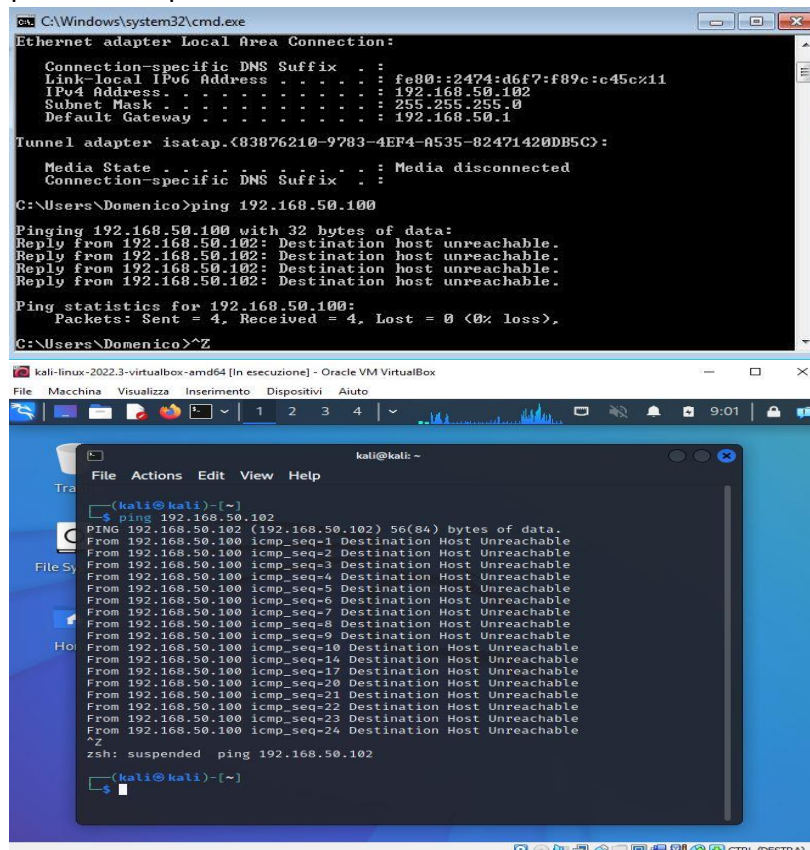


Successivamente andiamo a creare una nuova Regola per fare in modo che Kali Linux e Windows 7 possano pingarsi tra di loro, per farlo basterà andare su:
Windows Firewall with Advanced Security → Inbound Rules → New Rule

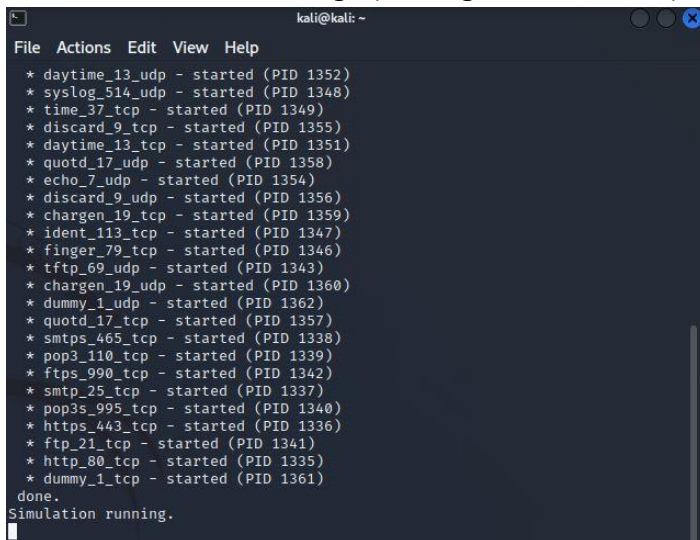


Per la creazione della nuova regola basterà proseguire cliccare su Custom Rule e successivamente impostare ICMPv4, dopo come indirizzi IP nella parte superiore quelli rispettivamente di Kali e di Windows in modo tale da permettere la comunicazione tra i due. Successivamente dato un nome alla nostra regola, nel nostro caso “Windows7-kali” sarà necessario controllare se la spunta alla sua sinistra sarà impostata con la spunta verde in modo tale da renderla attiva.

Successivamente andiamo ad applicare il ping tra le due parti e questo sarà il risultato sia per Kali che per Windows:

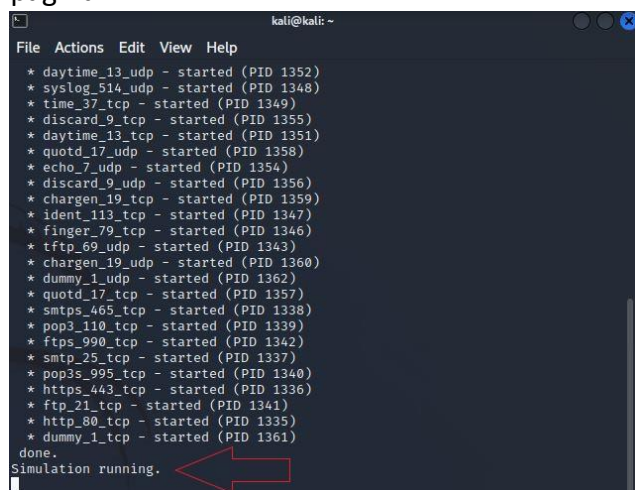


2. Il passaggio due invece riguarda l'utilizzo dell'utility InetSim per l'emulazione dei servizi internet. Per farlo ci basterà andare all'interno del prompt dei comandi di Kali e digitare il codice <<sudo intelsim>> questo ci darà modo di aprire la nostra utility con conferma della scritta "Simulation running" (vedi figura sottostante):

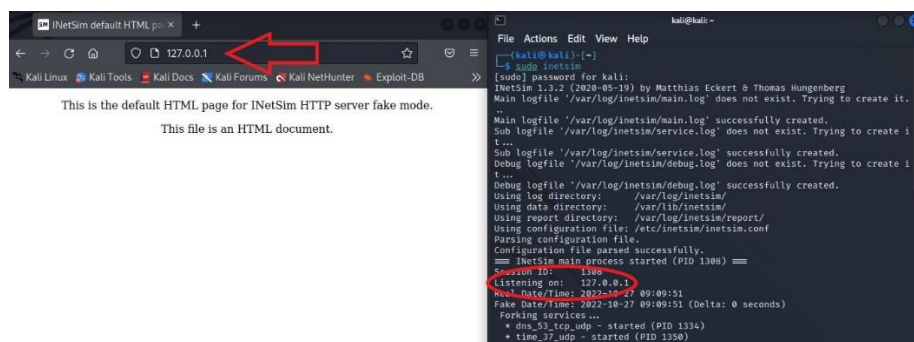


```
kali@kali: ~  
File Actions Edit View Help  
* daytime_13_udp - started (PID 1352)  
* syslog_514_udp - started (PID 1348)  
* time_37_tcp - started (PID 1349)  
* discard_9_tcp - started (PID 1355)  
* daytime_13_tcp - started (PID 1351)  
* quotd_17_udp - started (PID 1358)  
* echo_7_udp - started (PID 1354)  
* discard_9_udp - started (PID 1356)  
* chargen_19_tcp - started (PID 1359)  
* ident_113_tcp - started (PID 1347)  
* finger_79_tcp - started (PID 1346)  
* tftp_69_udp - started (PID 1343)  
* chargen_19_udp - started (PID 1360)  
* dummy_1_udp - started (PID 1362)  
* quotd_17_tcp - started (PID 1357)  
* smtps_465_tcp - started (PID 1338)  
* pop3_110_tcp - started (PID 1339)  
* ftps_990_tcp - started (PID 1342)  
* smtp_25_tcp - started (PID 1337)  
* pop3s_995_tcp - started (PID 1340)  
* https_443_tcp - started (PID 1336)  
* ftp_21_tcp - started (PID 1341)  
* http_80_tcp - started (PID 1335)  
* dummy_1_tcp - started (PID 1361)  
done.  
Simulation running.
```

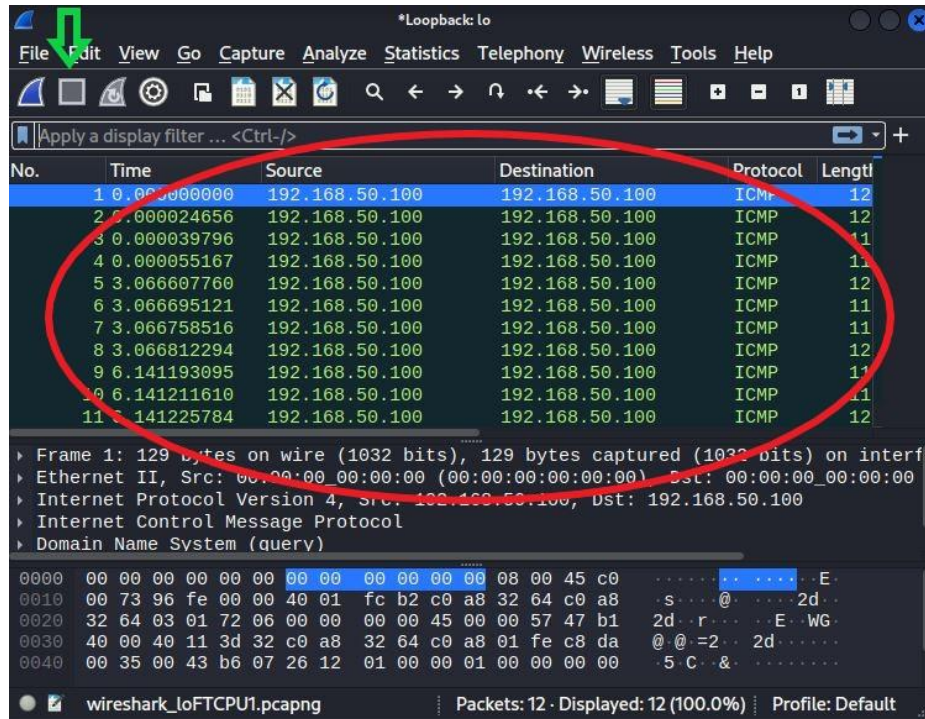
Se andiamo a notare nella parte superiore ci sarà un indirizzo IP relativamente nella sezione "Listening On" che ci permetterà di aprire una pagina internet come simulazione. Di fatti l'indirizzo in questione sarà "127.0.0.1" (vedi figura sottostante) il quale andandolo ad inserire nell'URL del browser (Firefox) ci permetterà di aprire la nostra "simulazione" di pagina HTML:



```
kali@kali: ~  
File Actions Edit View Help  
* daytime_13_udp - started (PID 1352)  
* syslog_514_udp - started (PID 1348)  
* time_37_tcp - started (PID 1349)  
* discard_9_tcp - started (PID 1355)  
* daytime_13_tcp - started (PID 1351)  
* quotd_17_udp - started (PID 1358)  
* echo_7_udp - started (PID 1354)  
* discard_9_udp - started (PID 1356)  
* chargen_19_tcp - started (PID 1359)  
* ident_113_tcp - started (PID 1347)  
* finger_79_tcp - started (PID 1346)  
* tftp_69_udp - started (PID 1343)  
* chargen_19_udp - started (PID 1360)  
* dummy_1_udp - started (PID 1362)  
* quotd_17_tcp - started (PID 1357)  
* smtps_465_tcp - started (PID 1338)  
* pop3_110_tcp - started (PID 1339)  
* ftps_990_tcp - started (PID 1342)  
* smtp_25_tcp - started (PID 1337)  
* pop3s_995_tcp - started (PID 1340)  
* https_443_tcp - started (PID 1336)  
* ftp_21_tcp - started (PID 1341)  
* http_80_tcp - started (PID 1335)  
* dummy_1_tcp - started (PID 1361)  
done.  
Simulation running.
```



3. Come ultimo passaggio non ci resta che andare ad aprire Wireshark per andare ad analizzare i pacchetti che vengono mostrati. Per farlo ci basterà aprire la nostra App e andare rispettivamente su "Loopback: lo" in quanto siamo in una rete Locale Interna (come impostato inizialmente) e ci verranno elencati tutti i pacchetti che sono in transizione in quell'istante, i quali saranno tutti di protocollo ICMP:



N.B. per bloccare il continuo flusso dei pacchetti basterà cliccare sull'icona quadrata in rosso come rappresentato dalla freccetta verde in figura soprastante.