


ESERCITAZIONE W3D4



W3D4 - Pratica PDF

Esercizio

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

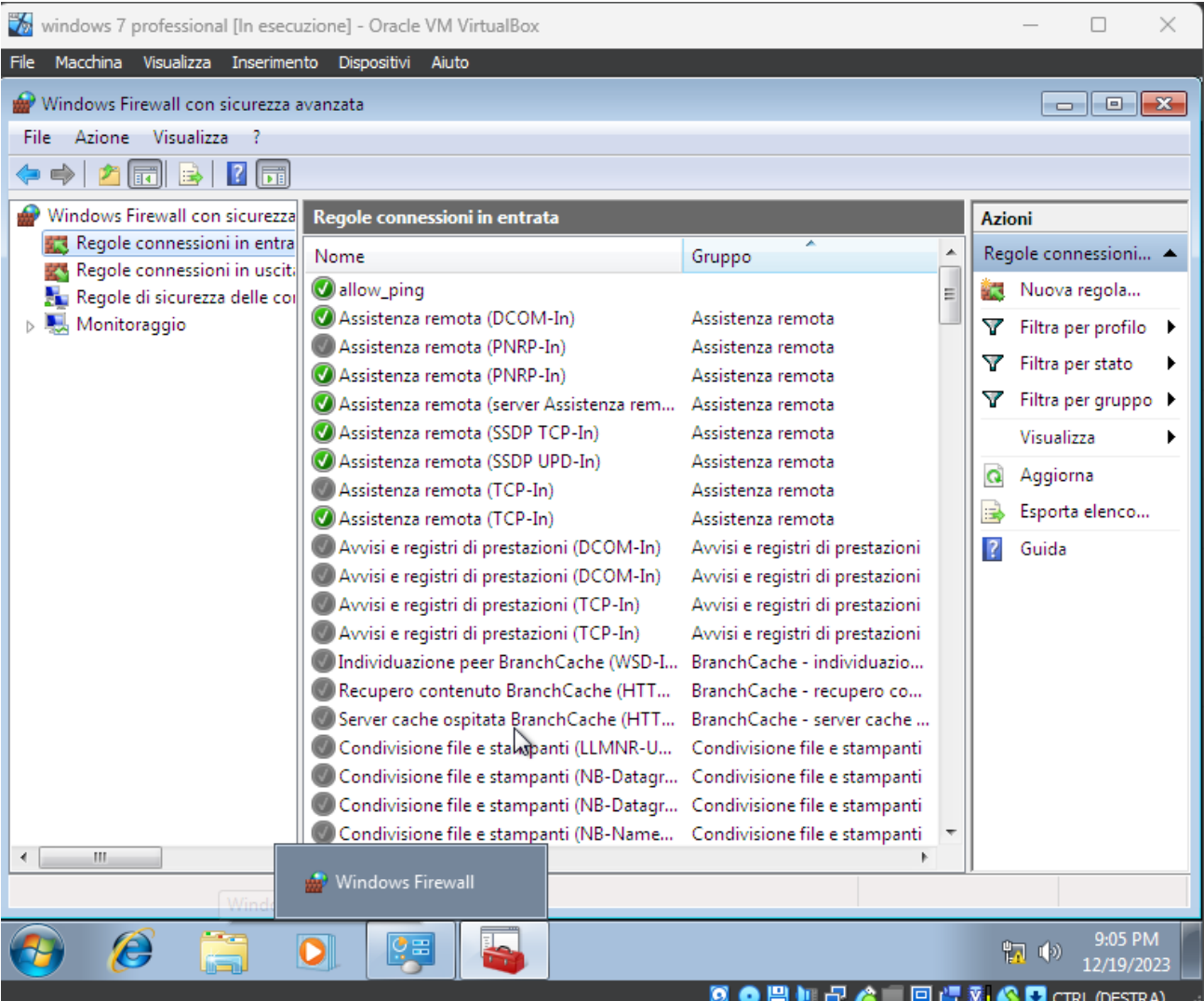
Vedremo due esercizi: I) la configurazione di una policy sul firewall windows; II) una packet capture con Wireshark.

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

Per prima cosa ho configurato una policy che permette il ping delle macchine kali e windows 7, chiamata "allow_ping".



Di seguito ho configurato INETSIM sulla porta http

File Actions Edit View Help

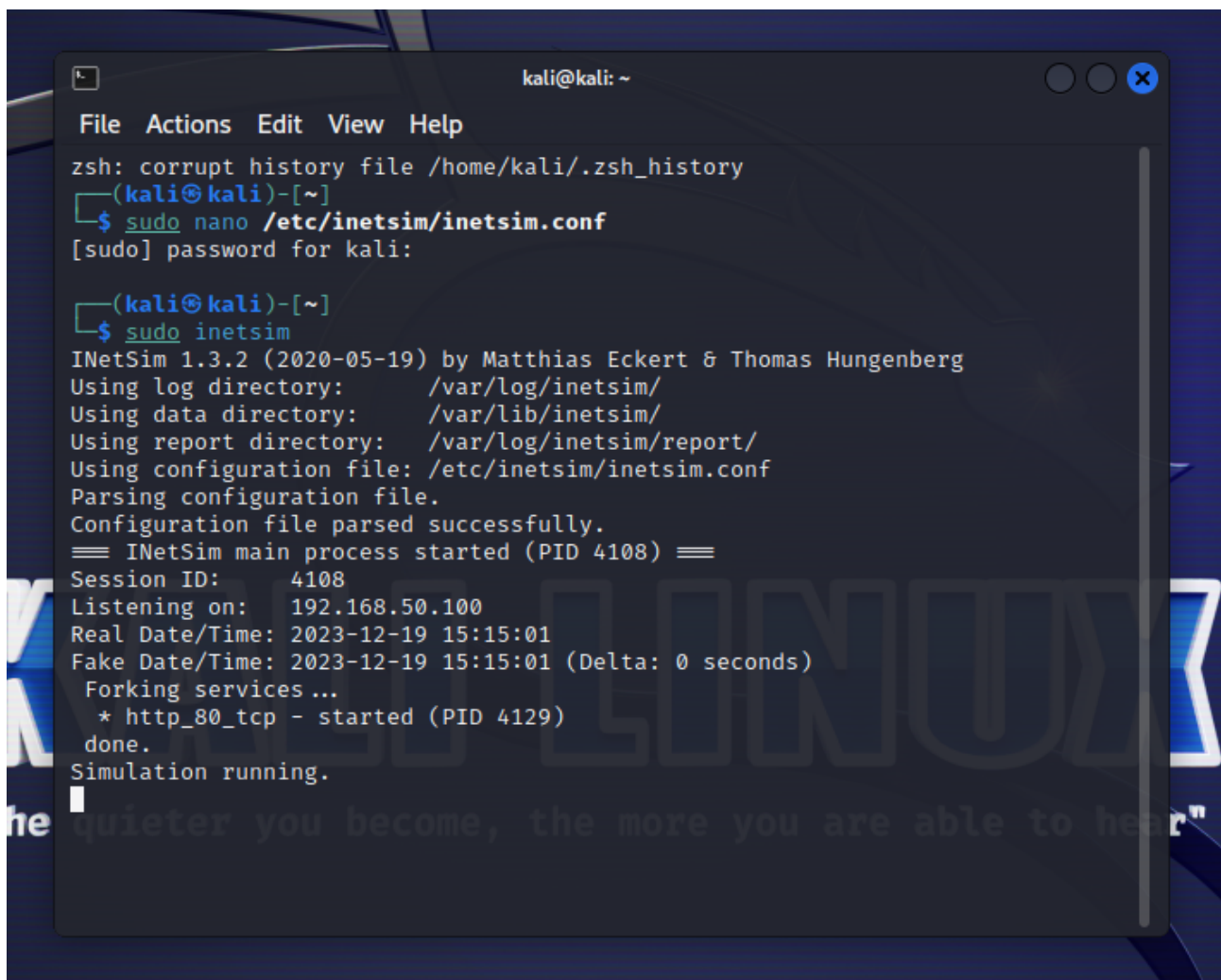
GNU nano 7.2 /etc/inetsim/inetsim.conf

```
# ident, syslog, dummy_tcp, dummy_udp, smtps, pop3s,  
# ftps, irc, https  
#  
# start_service dns  
start_service http  
#start_service https  
#start_service smtp  
#start_service smtps  
#start_service pop3  
##start_service pop3s  
#start_service ftp  
#start_service ftps  
#start_service tftp  
#start_service irc  
#start_service ntps  
#start_service finger  
#start_service ident  
#start_service syslog  
#start_service time_tcp  
#start_service time_udp  
#start_service daytime_tcp  
#start_service daytime_udp  
#start_service echo_tcp
```

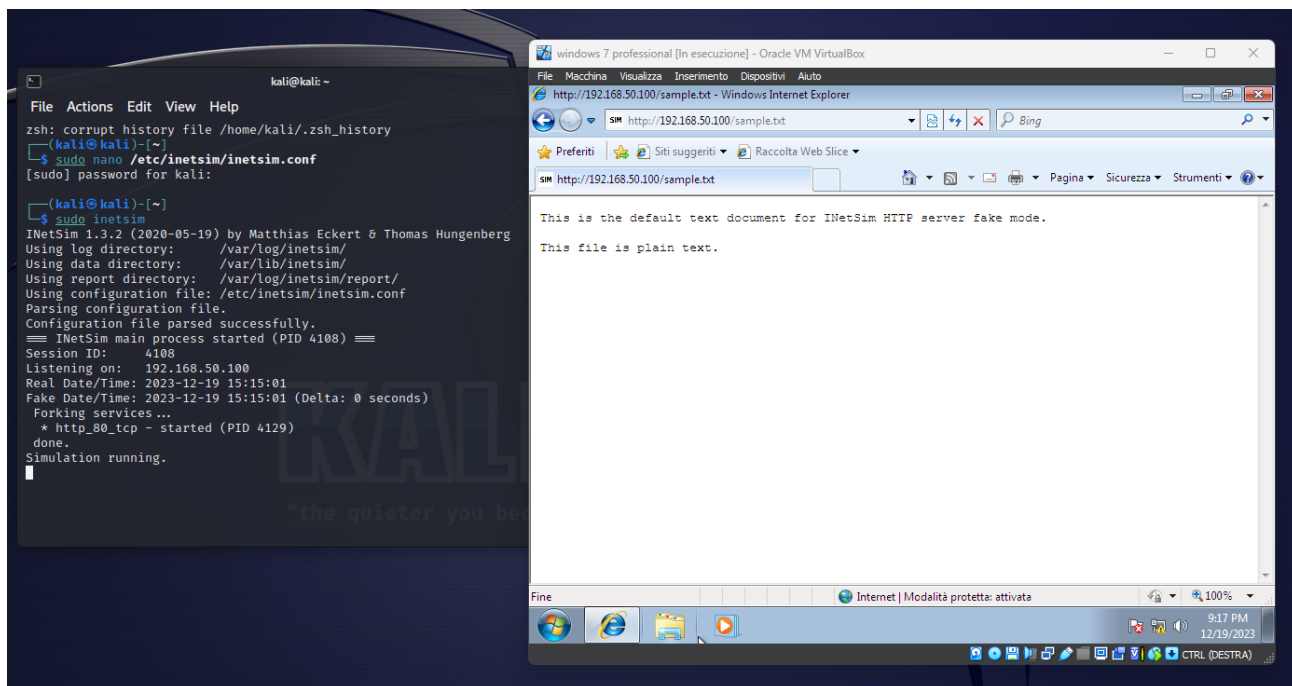
^G Help**^O** Write Out**^W** Where Is**^K** Cut**^T** Execute**^X** Exit**^R** Read File**^N** Replace**^U** Paste**^J** Justify

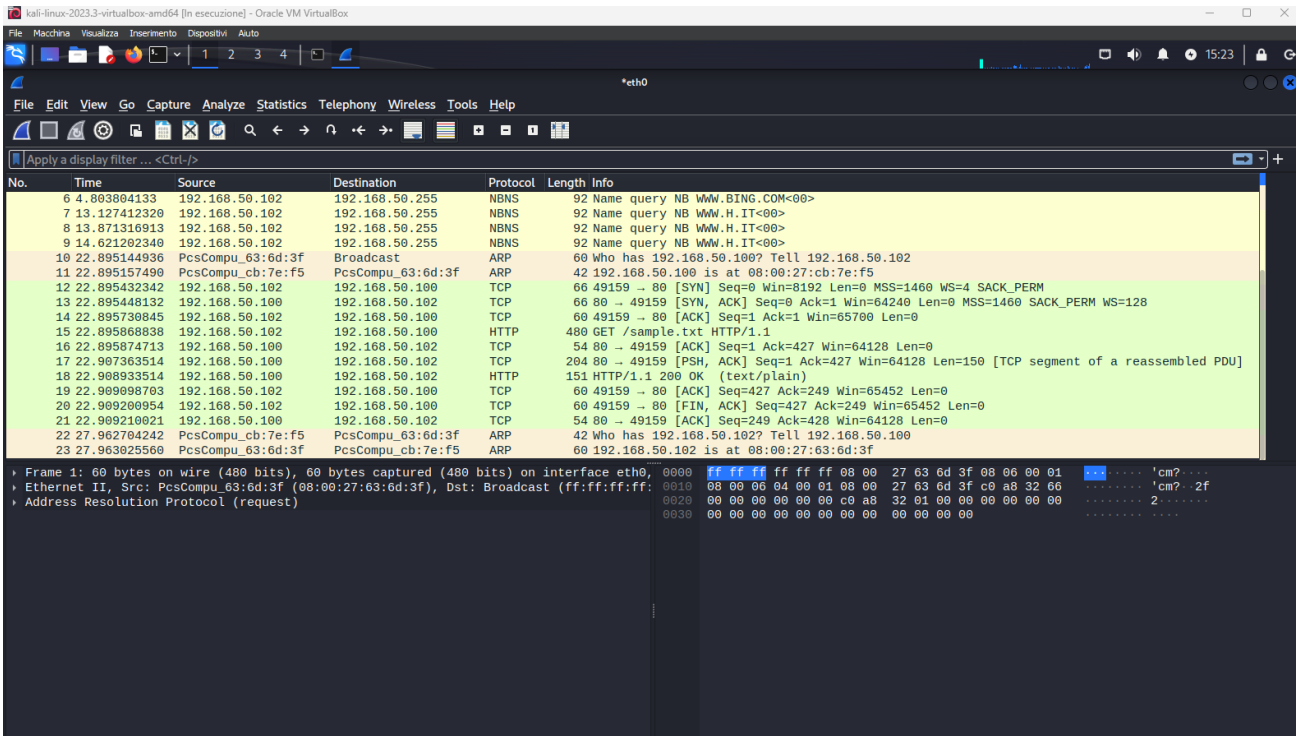
```
kali@kali: ~  
File Actions Edit View Help  
GNU nano 7.2 /etc/inetsim/inetsim.conf  
#start_service chargen_tcp  
#start_service chargen_udp  
#start_service dummy_tcp  
#start_service dummy_udp  
  
#####  
# service_bind_address  
#  
# IP address to bind services to  
#  
# Syntax: service_bind_address <IP address>  
#  
# Default: 127.0.0.1  
#  
service_bind_address 192.168.50.100  
  
#####  
# service_run_as_user  
#  
# User to run services  
#  
# Syntax: service_run_as_user <username>  
#####  
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute  
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify
```

Poi ho avviato INETSIM



In seguito ho aperto su windows 7 il "fake file" di inetsim e con wireshark ho visualizzato i pacchetti.





di seguito ho fatto la stessa procedura modificando la porta https, per analizzare la differenza dei pacchetti raccolti.

