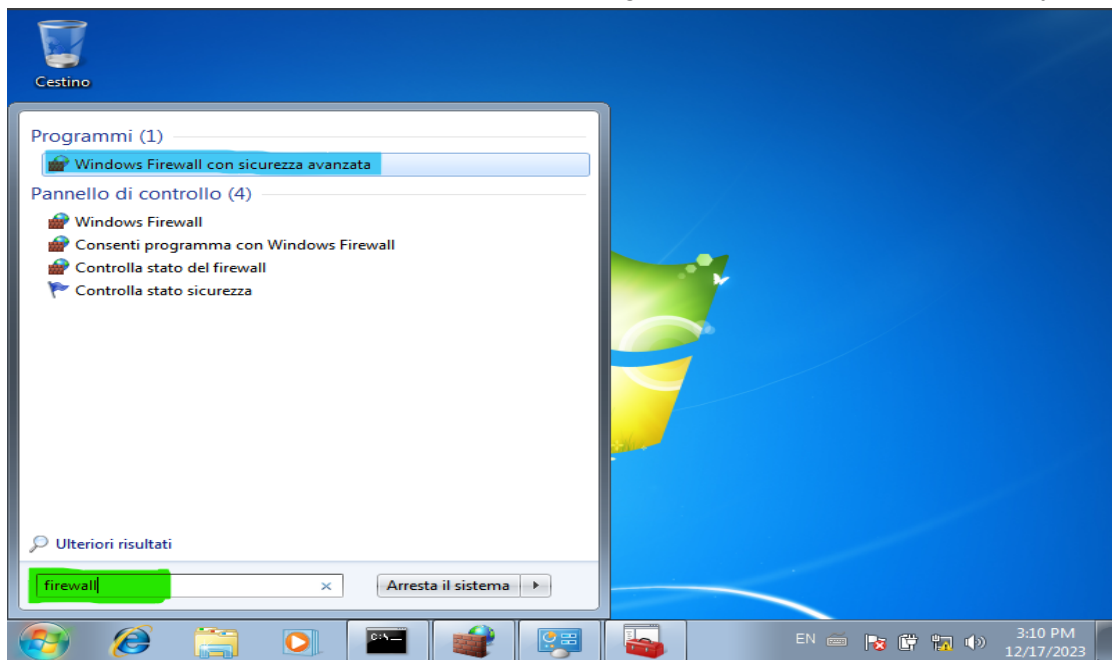
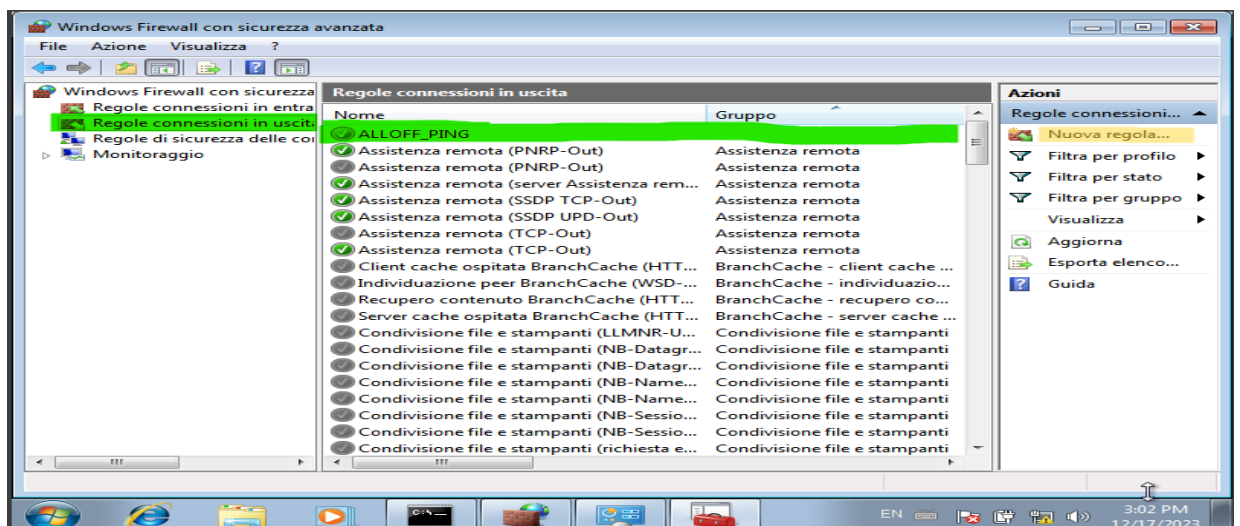


USANDO WIRESHARK PER LA PRIMA VOLTA

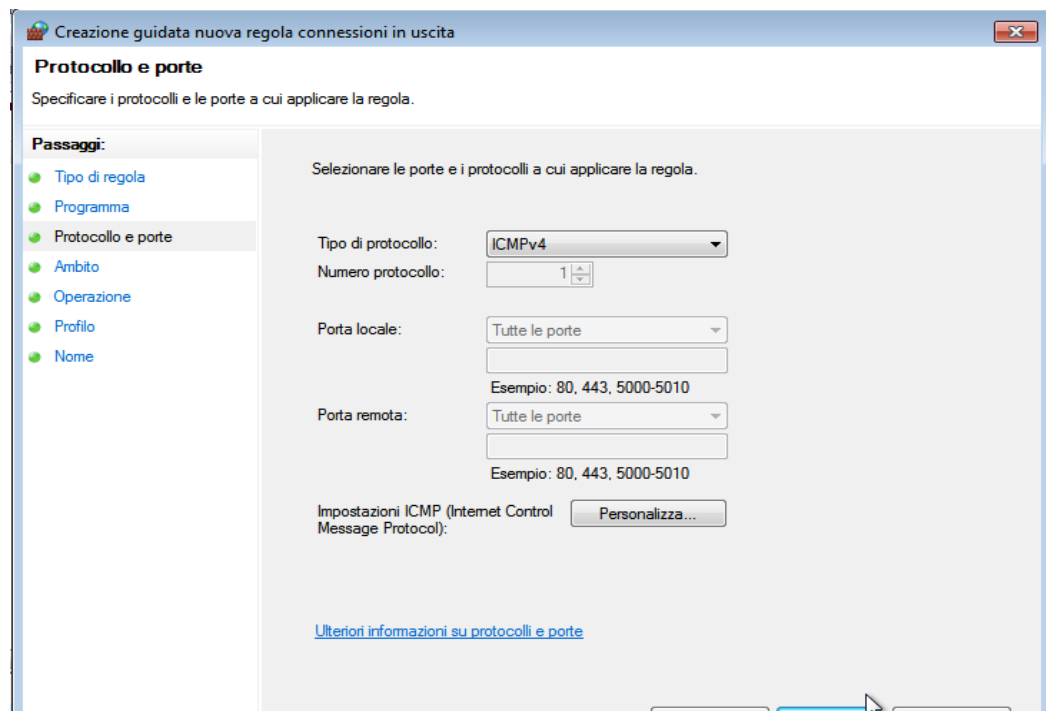
1. Come primo step, dobbiamo avviare le due macchine virtuali già prè-configurate in precedenza nelle altre lezioni.
2. Dentro alla macchina di windows 7, andiamo in cerca del firewall di windows, rapidamente raggiungibile usando il comando di ricerca. Come sottolineato in verde nell'immagine. Dopo aver fatto la ricerca, basta cliccare su **"Windows Firewall con sicurezza avanzata"**, questo aprirà subito la pagina da introdurre la nuova policy.



3. Dopo aver aperto la pagina dei firewall, andiamo su **"regola connessione in uscita"** e dopo aggiungiamo una nuova regola, andando su **"nuova regola"**



4. Dentro a “nuova regola”, su “**tipo di regola**” scegliamo personalizzata (custom) dopodiché clicchiamo su avanti fino a raggiungere la casella “**Protocollo e porte**” e sul menu a tendiamo di “**tipo di protocollo**” impostiamo su ICMPv4 e clicchiamo su avanti fino a raggiungere “**nome**”, diamo il nome “ALLOFF_PING” e una descrizione per sapere cosa fa il comando.



5. Dopo andiamo sulla macchina Kali, e dal cmd lanciamo il comando “**sudo nano /etc/inetsim/inetsim.conf**”, subito nella prima parte, lasciamo soltanto HTTPS attivo, mettendo un cancelletto davanti agli altri service, in modo da cancellarli.

```
File Actions Edit View Help
GNU nano 7.2
# 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 ntp
#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
#start_service echo_udp
#start_service discard_tcp
#start_service discard_udp
#start_service quotd_tcp
#start_service quotd_udp
#start_service chargen_tcp
#start_service chargen_udp
#start_service dummy_tcp
#start_service dummy_udp
```

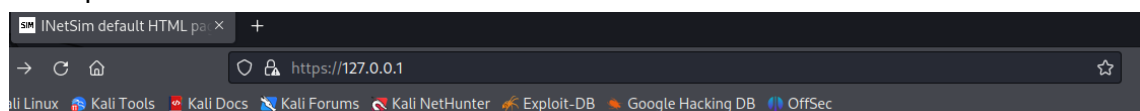
6. Andiamo giù e configuriamo l'IP che vogliamo, togliendo il cancelletto da davanti l'IP e dal Service. Io ho lasciato quello di Default come immagine.

```
#####
# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
Default: 127.0.0.1
#
service_bind_address 0.0.0.0
#####
```

7. Adesso avviamo Inetsim, con il comando “**sudo Inetsim**”

```
(kali@kali)-[~]
$ sudo inetsim
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 it...
Sub logfile '/var/log/inetsim/service.log' successfully created.
Debug logfile '/var/log/inetsim/debug.log' does not exist. Trying to create it...
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.
Warning: Unknown option 'Default:' in configuration file '/etc/inetsim/inetsim.conf' line 67
Configuration file parsed successfully.
== INetSim main process started (PID 34826) ==
Session ID: 34826
Listening on: 0.0.0.0
Real Date/Time: 2023-12-17 09:12:20
Fake Date/Time: 2023-12-17 09:12:20 (Delta: 0 seconds)
Forking services ...
* https_443_tcp - started (PID 34836)
done.
Simulation running.
```

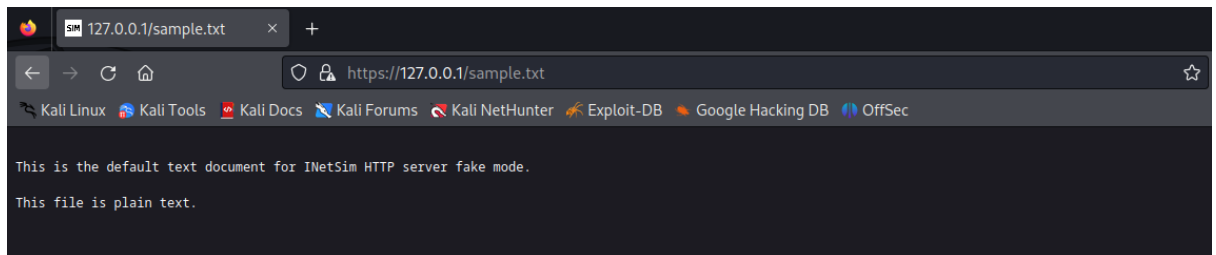
8. Da un browser di nostra preferenza su kali, andiamo in cerca della pagina web con l'IP impostato.



This is the default HTML page for INetSim HTTP server fake mode.

This file is an HTML document.

Dopo possiamo andare in cerca del “**sample.txt**” mettendo davanti alla pagina “/sample.txt”



9. Sempre su kali avviamo “**Wireshark**” e da windows 7 facciamo ping a kali e wireshark cattura il ping come in immagine.

```
C:\Users\Gust>ping 192.168.50.100

Esecuzione di Ping 192.168.50.100 con 32 byte di dati:
Risposta da 192.168.50.100: byte=32 durata=8ms TTL=64
Risposta da 192.168.50.100: byte=32 durata=3ms TTL=64
Risposta da 192.168.50.100: byte=32 durata=1ms TTL=64
Risposta da 192.168.50.100: byte=32 durata=1ms TTL=64

Statistiche Ping per 192.168.50.100:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 <0% persi>,
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 1ms, Massimo = 8ms, Medio = 3ms
```

