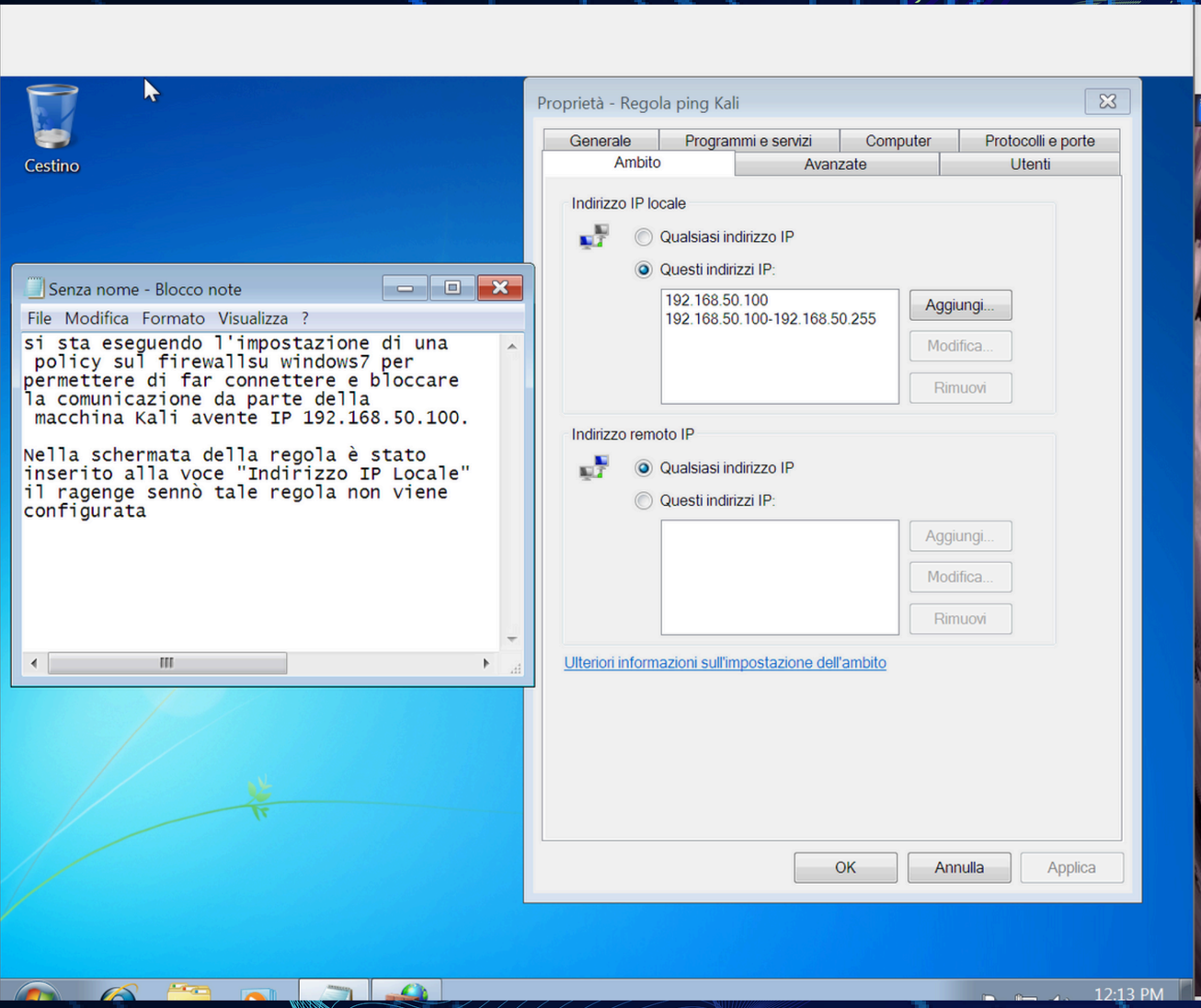
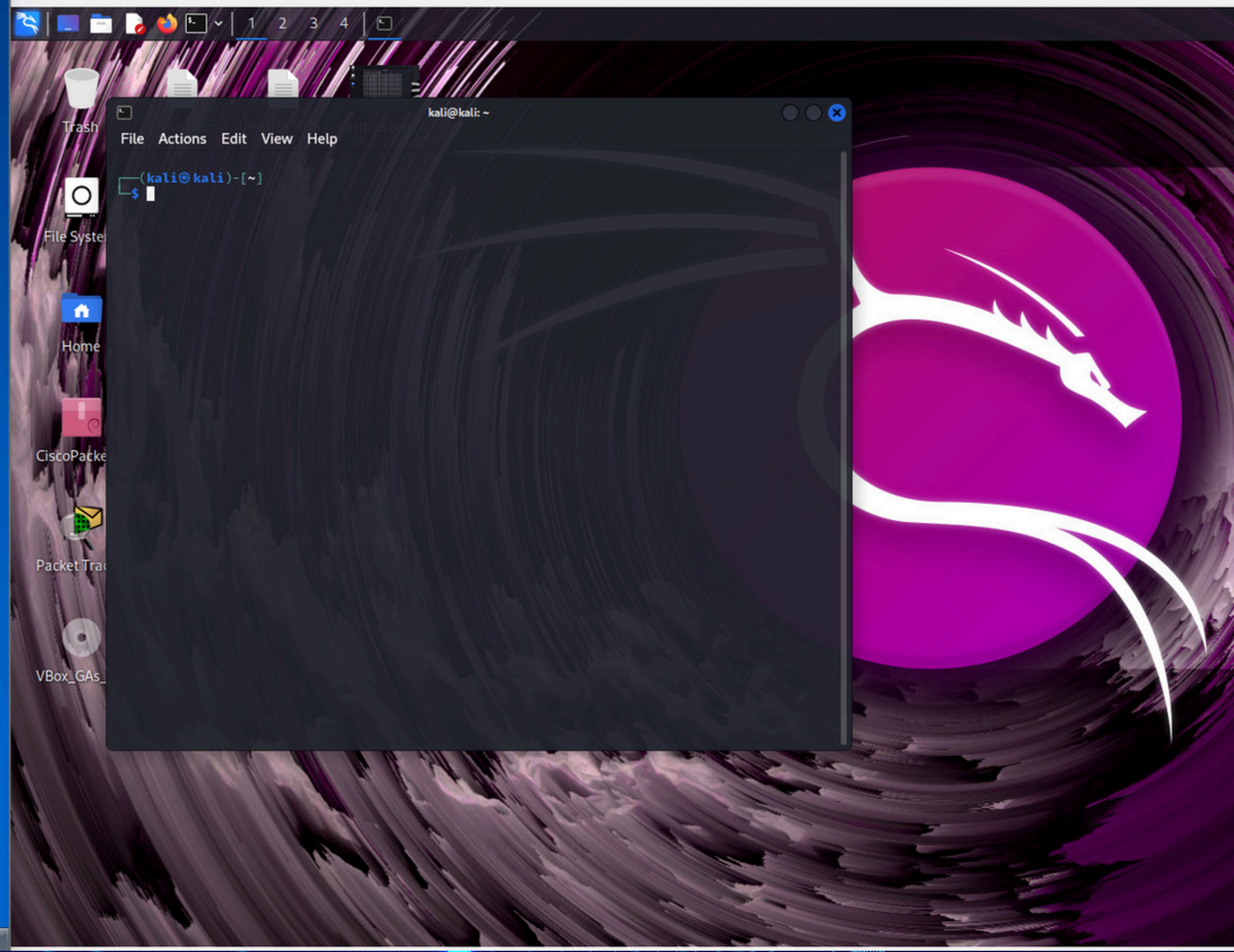
CONSEGNA DEL GIORNO W3D4

FIREWALL, INETSIM E WIREDSHARK

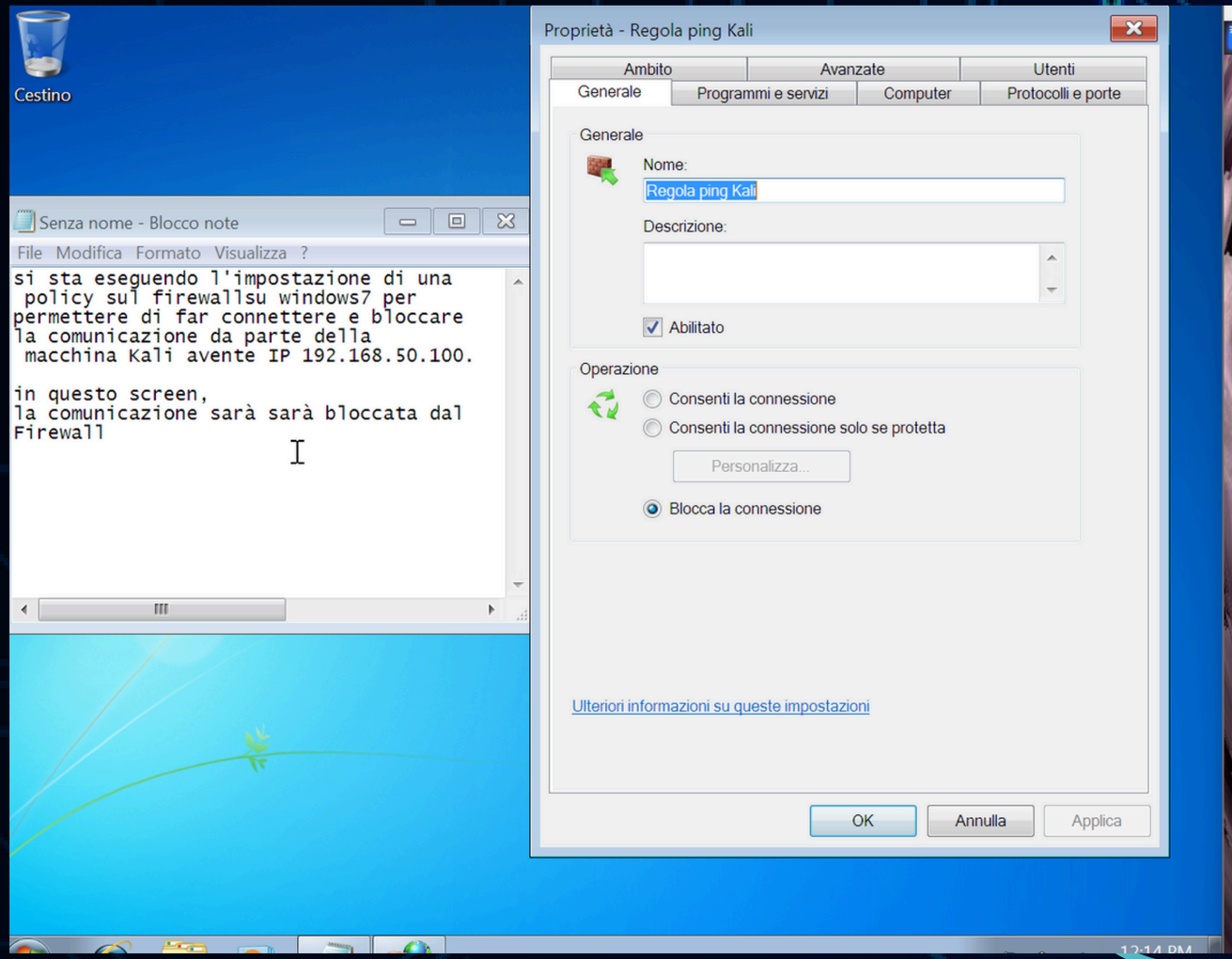
PROF è LA MIA PRIMA VOLTA CHE FACCIO SLIDE, PRESENTAZIONI E COSE DI QUESTO TIPO, MIGLIORERO'

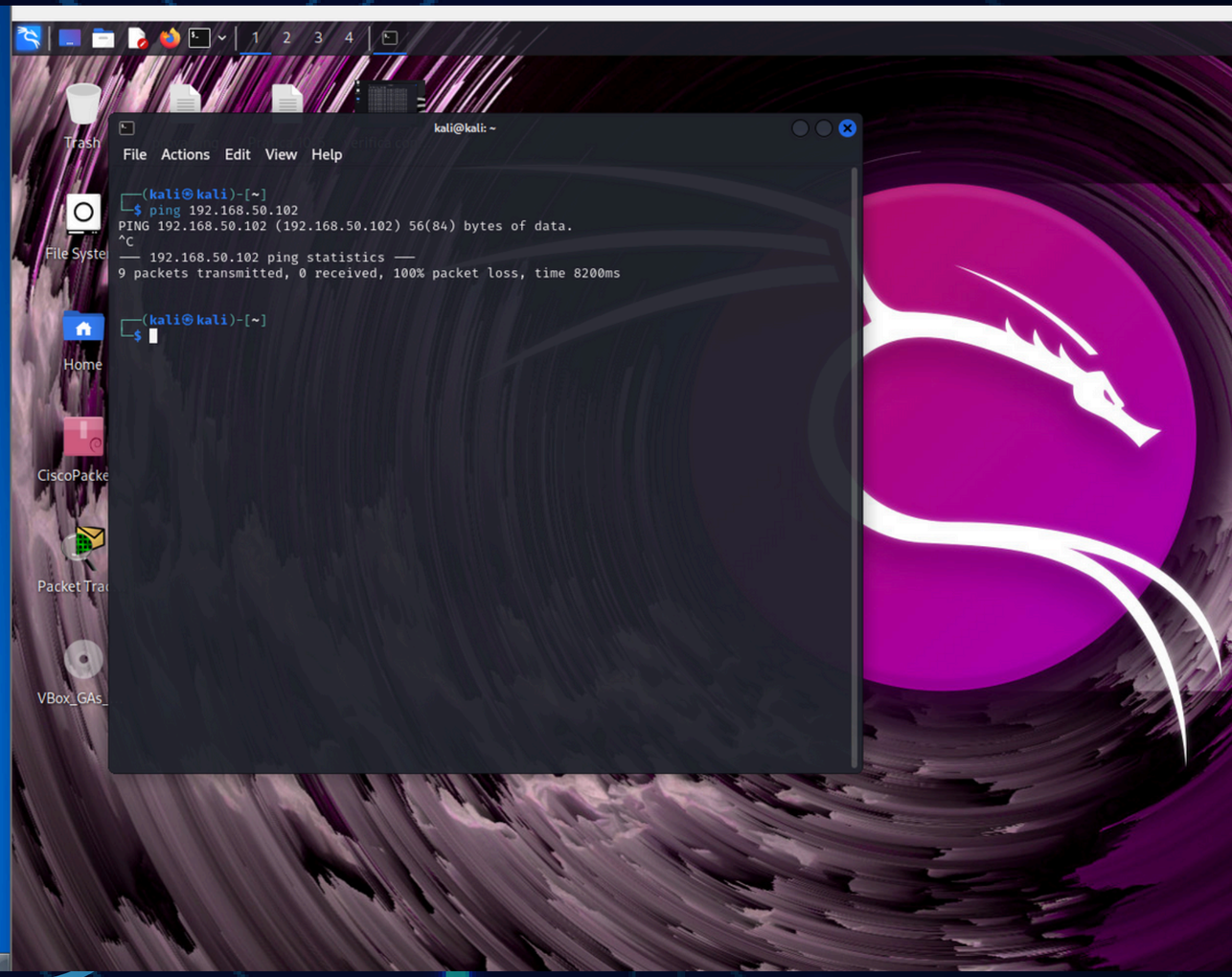
FIREWALL


Cestino
Senza nome - Blocco note
File Modifica Formato Visualizza ?
si sta eseguendo l'impostazione di una
policy sul firewallsu windows7 per
permettere di far connettere e bloccare
la comunicazione da parte della
macchina Kali avente IP 192.168.50.100.
Nella schermata della regola è stato
inserito alla voce "Indirizzo IP Locale"
il ragenge sennò tale regola non viene
configurata
Proprietà - Regola ping Kali
Generale
Programmi e servizi
Computer
Protocolli e porte
Ambito
Avanzate
Utenti
Indirizzo IP locale
Qualsiasi indirizzo IP
Questi indirizzi IP:
192.168.50.100
192.168.50.100-192.168.50.255
Aggiungi...
Modifica...
Rimuovi
Indirizzo remoto IP
Qualsiasi indirizzo IP
Questi indirizzi IP:
Aggiungi...
Modifica...
Rimuovi
Ulteriori informazioni sull'impostazione dell'ambito
OK
Annulla
Applica
12:13 PM

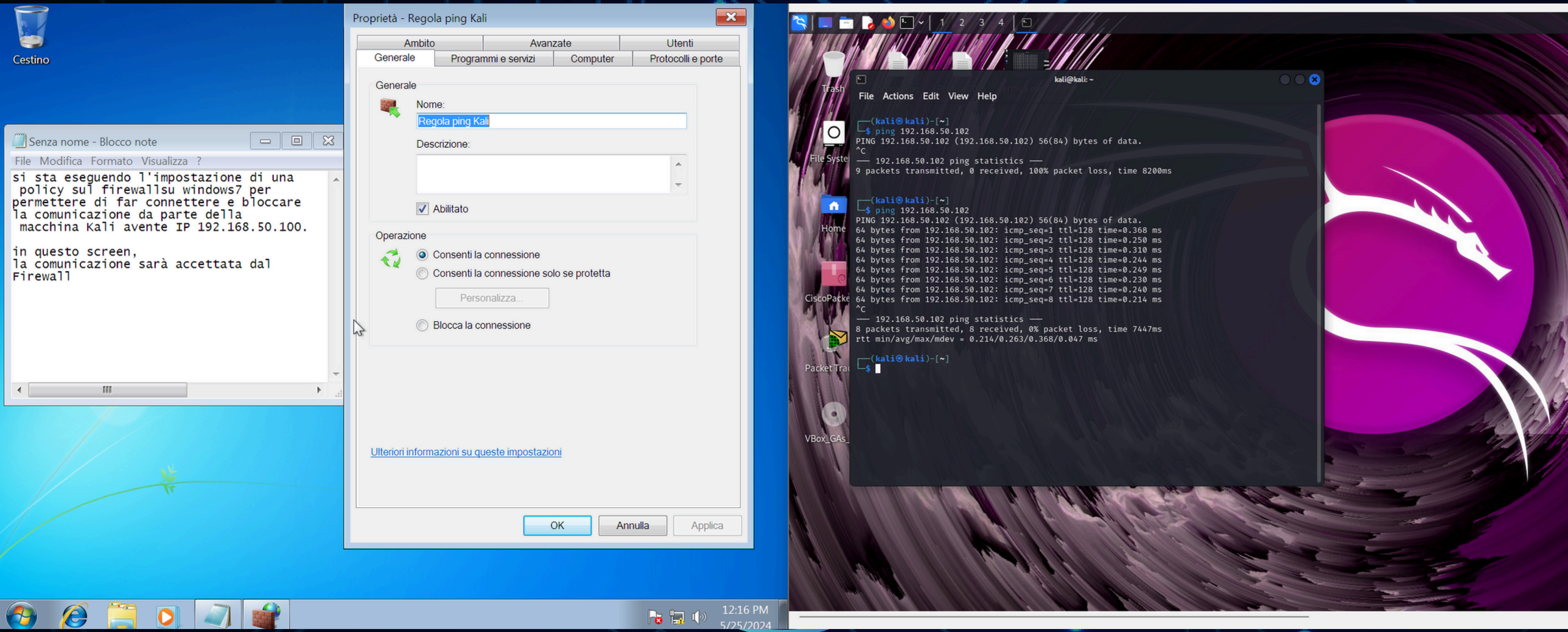

Trash
File Syste
Home
CiscoPacke
Packet Tra
VBox_GAs_
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$

FIREWALL

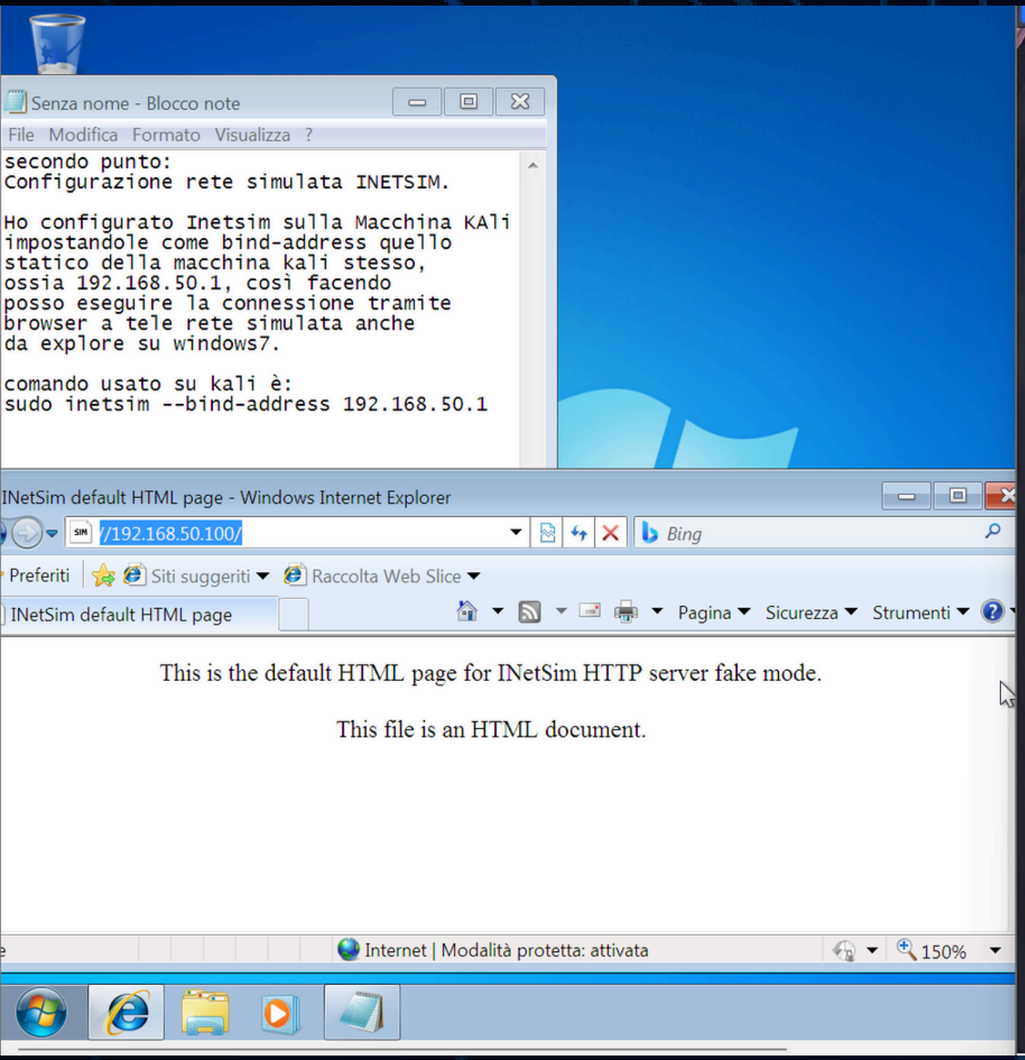

Cestino
Senza nome - Blocco note
File Modifica Formato Visualizza ?
si sta eseguendo l'impostazione di una
policy sul firewallsu windows7 per
permettere di far connettere e bloccare
la comunicazione da parte della
macchina Kali avente IP 192.168.50.100.
in questo screen,
la comunicazione sarà sarà bloccata dal
Firewall
Proprietà - Regola ping Kali
Ambito
Avanzate
Utenti
Generale
Programmi e servizi
Computer
Protocolli e porte
Generale
Nome:
Regola ping Kali
Descrizione:
Abilitato
Operazione
Consenti la connessione
Consenti la connessione solo se protetta
Personalizza...
Blocca la connessione
Ulteriori informazioni su queste impostazioni
OK
Annulla
Applica

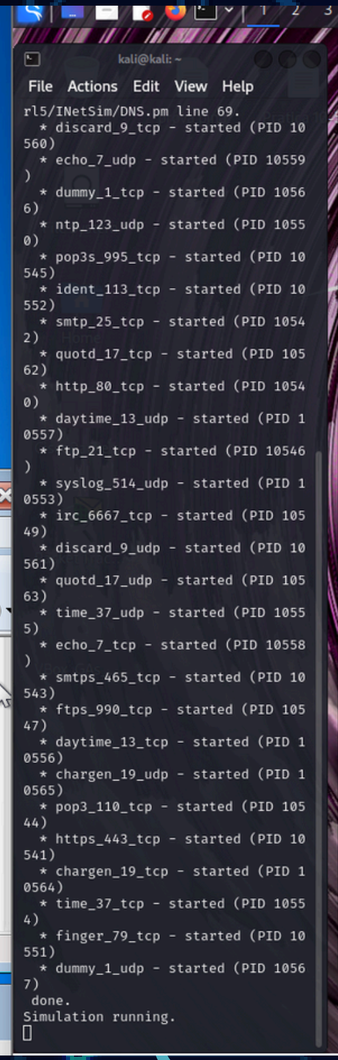

Trash
File Syste
Home
CiscoPacke
Packet Trac
VBox_GAs_
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ ping 192.168.50.102
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.
^C
— 192.168.50.102 ping statistics —
9 packets transmitted, 0 received, 100% packet loss, time 8200ms
(kali㉿kali)-[~]
$

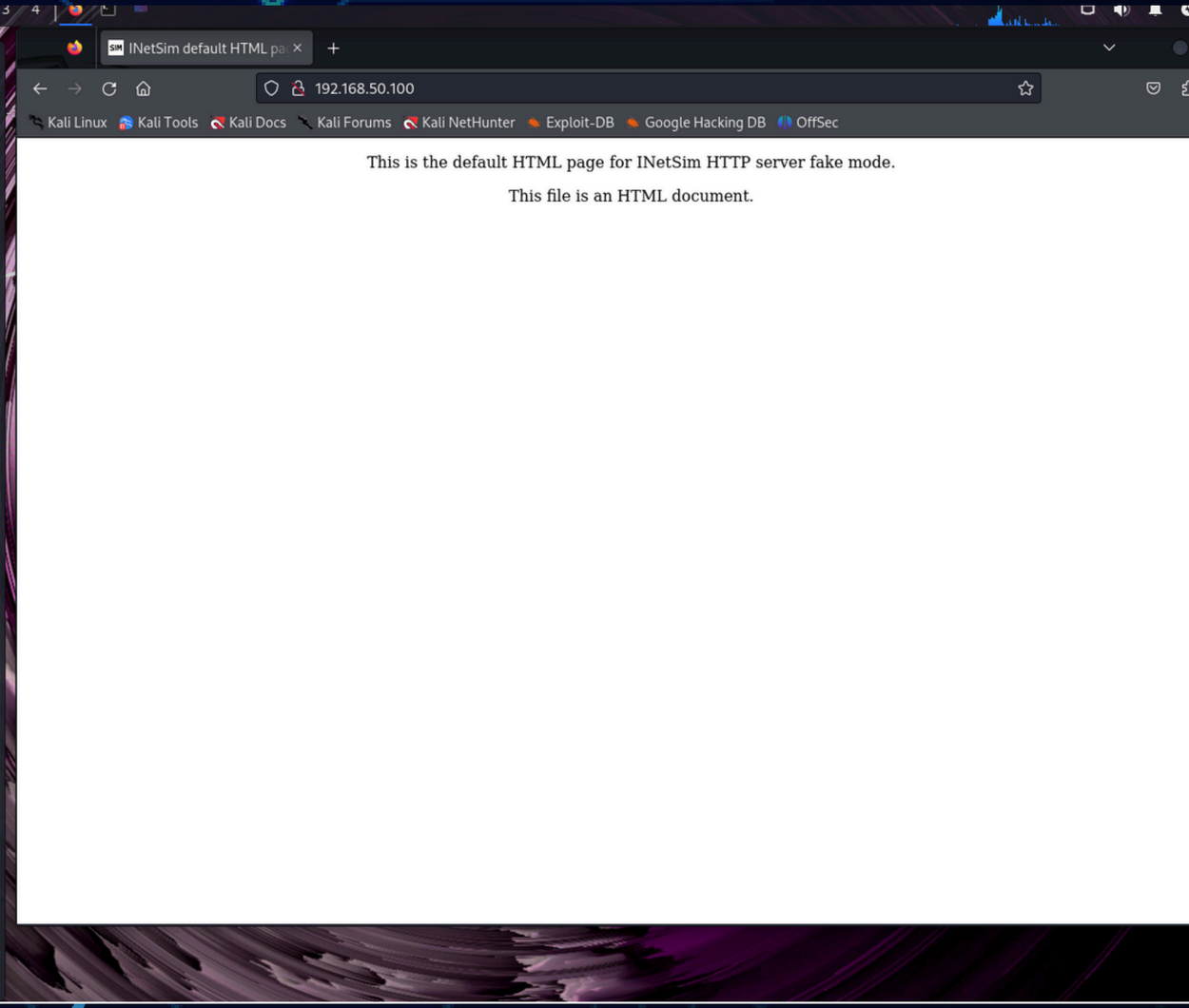
FIREWALL


Cestino
Senza nome - Blocco note
File Modifica Formato Visualizza ?
si sta eseguendo l'impostazione di una
policy sul firewallsu windows7 per
permettere di far connettere e bloccare
la comunicazione da parte della
macchina Kali avente IP 192.168.50.100.
in questo screen,
la comunicazione sarà accettata dal
Firewall
Proprietà - Regola ping Kali
Ambito
Avanzate
Utenti
Generale
Programmi e servizi
Computer
Protocolli e porte
Generale
Nome:
Regola ping Kali
Descrizione:
Abilitato
Operazione
Consenti la connessione
Consenti la connessione solo se protetta
Personalizza...
Blocca la connessione
Ulteriori informazioni su queste impostazioni
OK
Annulla
Applica
12:16 PM
5/25/2024
Trash
File Syste
Home
CiscoPacke
Packet Tra
VBox_GAs_
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ ping 192.168.50.102
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.
^C
— 192.168.50.102 ping statistics —
9 packets transmitted, 0 received, 100% packet loss, time 8200ms
(kali㉿kali)-[~]
$ ping 192.168.50.102
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.
64 bytes from 192.168.50.102: icmp_seq=1 ttl=128 time=0.368 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=0.250 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.310 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=0.244 ms
64 bytes from 192.168.50.102: icmp_seq=5 ttl=128 time=0.249 ms
64 bytes from 192.168.50.102: icmp_seq=6 ttl=128 time=0.230 ms
64 bytes from 192.168.50.102: icmp_seq=7 ttl=128 time=0.240 ms
64 bytes from 192.168.50.102: icmp_seq=8 ttl=128 time=0.214 ms
^C
— 192.168.50.102 ping statistics —
8 packets transmitted, 8 received, 0% packet loss, time 7447ms
rtt min/avg/max/mdev = 0.214/0.263/0.368/0.047 ms
(kali㉿kali)-[~]
$

INETSIM


Senza nome - Blocco note
File Modifica Formato Visualizza ?
secondo punto:
Configurazione rete simulata INETSIM.
Ho configurato Inetsim sulla Macchina KAli
impostandole come bind-address quello
statico della macchina kali stesso,
ossia 192.168.50.1, così facendo
posso eseguire la connessione tramite
browser a tele rete simulata anche
da explore su windows7.
comando usato su kali è:
sudo inetsim --bind-address 192.168.50.1
INetSim default HTML page - Windows Internet Explorer
http://192.168.50.100/
Bing
Preferiti
Siti suggeriti
Raccolta Web Slice
INetSim default HTML page
Pagina
Sicurezza
Strumenti
This is the default HTML page for INetSim HTTP server fake mode.
This file is an HTML document.
Internet | Modalità protetta: attivata
150%


kali@kali: ~
File Actions Edit View Help
rl5/INetSim/DNS.pm line 69.
* discard_9_tcp - started (PID 10560)
* echo_7_udp - started (PID 10559)
* dummy_1_tcp - started (PID 10566)
* ntp_123_udp - started (PID 10550)
* pop3s_995_tcp - started (PID 10545)
* ident_113_tcp - started (PID 10552)
* smtp_25_tcp - started (PID 10542)
* quotd_17_tcp - started (PID 10562)
* http_80_tcp - started (PID 10540)
* daytime_13_udp - started (PID 10557)
* ftp_21_tcp - started (PID 10546)
* syslog_514_udp - started (PID 10553)
* irc_6667_tcp - started (PID 10549)
* discard_9_udp - started (PID 10561)
* quotd_17_udp - started (PID 10563)
* time_37_udp - started (PID 10555)
* echo_7_tcp - started (PID 10558)
* smtps_465_tcp - started (PID 10543)
* ftps_990_tcp - started (PID 10547)
* daytime_13_tcp - started (PID 10556)
* chargen_19_udp - started (PID 10565)
* pop3_110_tcp - started (PID 10544)
* https_443_tcp - started (PID 10541)
* chargen_19_tcp - started (PID 10564)
* time_37_tcp - started (PID 10554)
* finger_79_tcp - started (PID 10551)
* dummy_1_udp - started (PID 10567)
done.
Simulation running.


INetSim default HTML pa
192.168.50.100
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
This is the default HTML page for INetSim HTTP server fake mode.
This file is an HTML document.

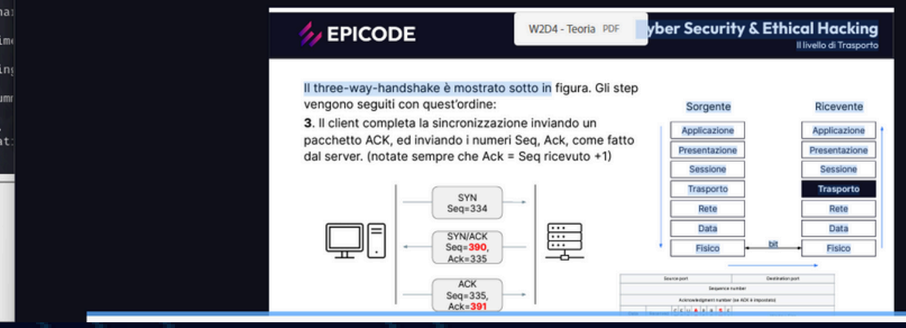
WIREDSHARK

terzo punto:
lettura comunicazioni con Wireshark.

WiredShark avviato con lettura "ANY".
avviata una connesisone tramite Browser da win7 verso la inetsim di kali,
nelle prime linee si evince la richiesta di comunicazione tra client e host,
nelle quale sta avvendendo il three-way-handshake(livello trasporto iso/osi).

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

This file is an HTML document.



GRAZIE