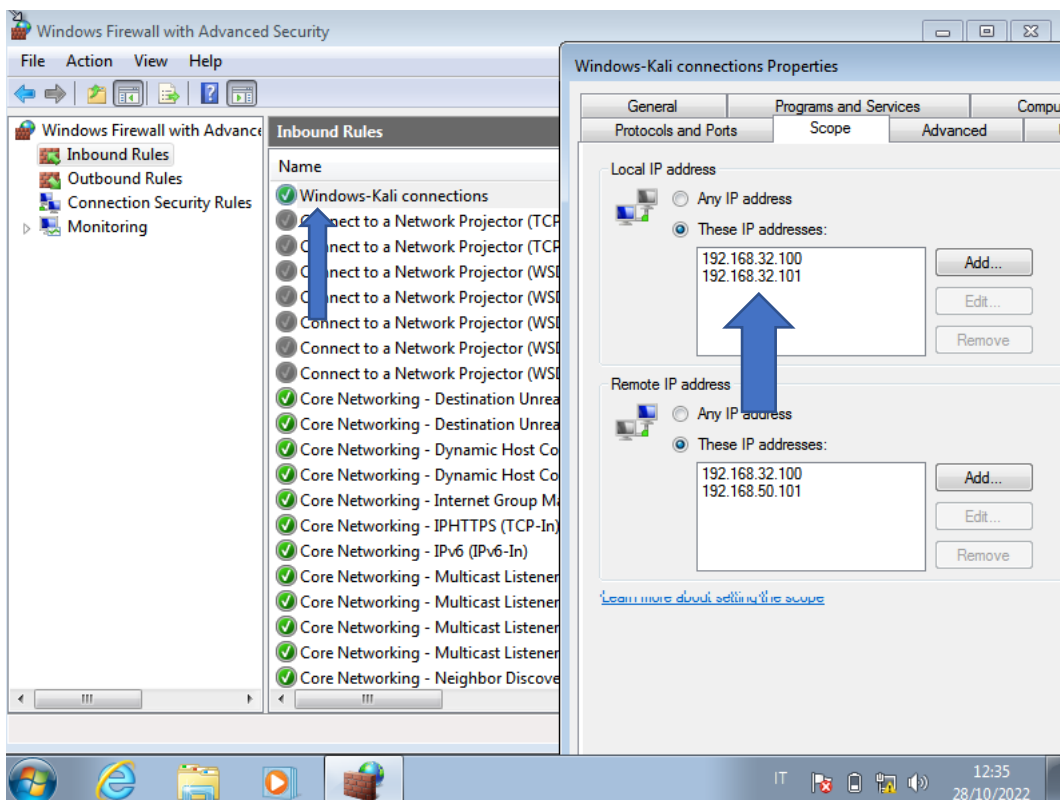


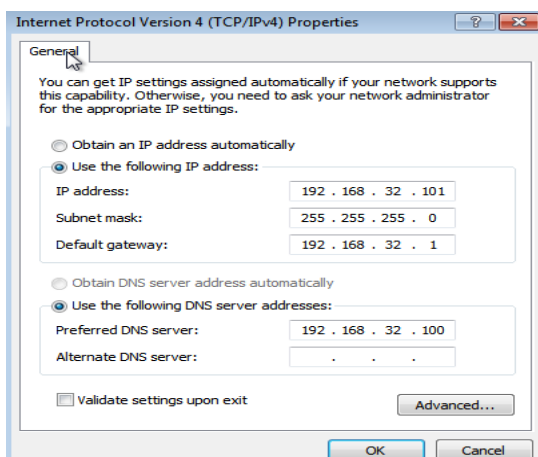
Controllo di pacchetti scambiati tra windows e kali con Wireshark

La richiesta di oggi era quella di far comunicare le virtual machine di kali e windows tramite un DNS creato tramite inetsim e poi registrare i pacchetti che transitavano sulla rete virtuale con Wireshark.

- 1) Come prima cosa andiamo a modificare l'ambiente di lavoro di Windows.
 - Come prima cosa dobbiamo modificare le policy precedentemente create
 - Andiamo nella sezione firewall, advanced e premiamo sulla policy da noi creata
 - Poi su scope è andiamo a modificare gli indirizzi IP



Procediamo poi con il cambiare indirizzo IP, default gateway, DNS server (questo sarà l'indirizzo IP di kali)



Per fare questo andiamo nella voce "Network and sharing center" poi "local area connection", properties.

2) Adesso modifichiamo l'ambiente di lavoro Linux e l'applicazione Inetsim.

- Come prima cosa modifichiamo l'indirizzo ip di kali eseguendo il comando `sudo nano /etc/network/interfaces/`
- Modifichiamo l'indirizzo IP con il nuovo è anche il gateway

```
GNU nano 6.3
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.32.100
gateway 192.168.32.1
```

Adesso dobbiamo modificare la configurazione di Inetsim

- Eseguiamo il comando `sudo nano /etc/inetsim/inetsim.conf`
- Aggiungiamo il comando `dns_default_ip 192.168.32.100` e anche `dns_default_domainname` con `epicode internal`

```
kali@kali: ~
File Actions Edit View Help
GNU nano 6.3 /etc/inetsim/inetsim.conf *
# Default IP address to return with DNS replies
#
# Syntax: dns_default_ip <IP address>
#
# Default: 127.0.0.1
#
#dns_default_ip 10.10.10.1
dns_default_ip 192.168.32.100

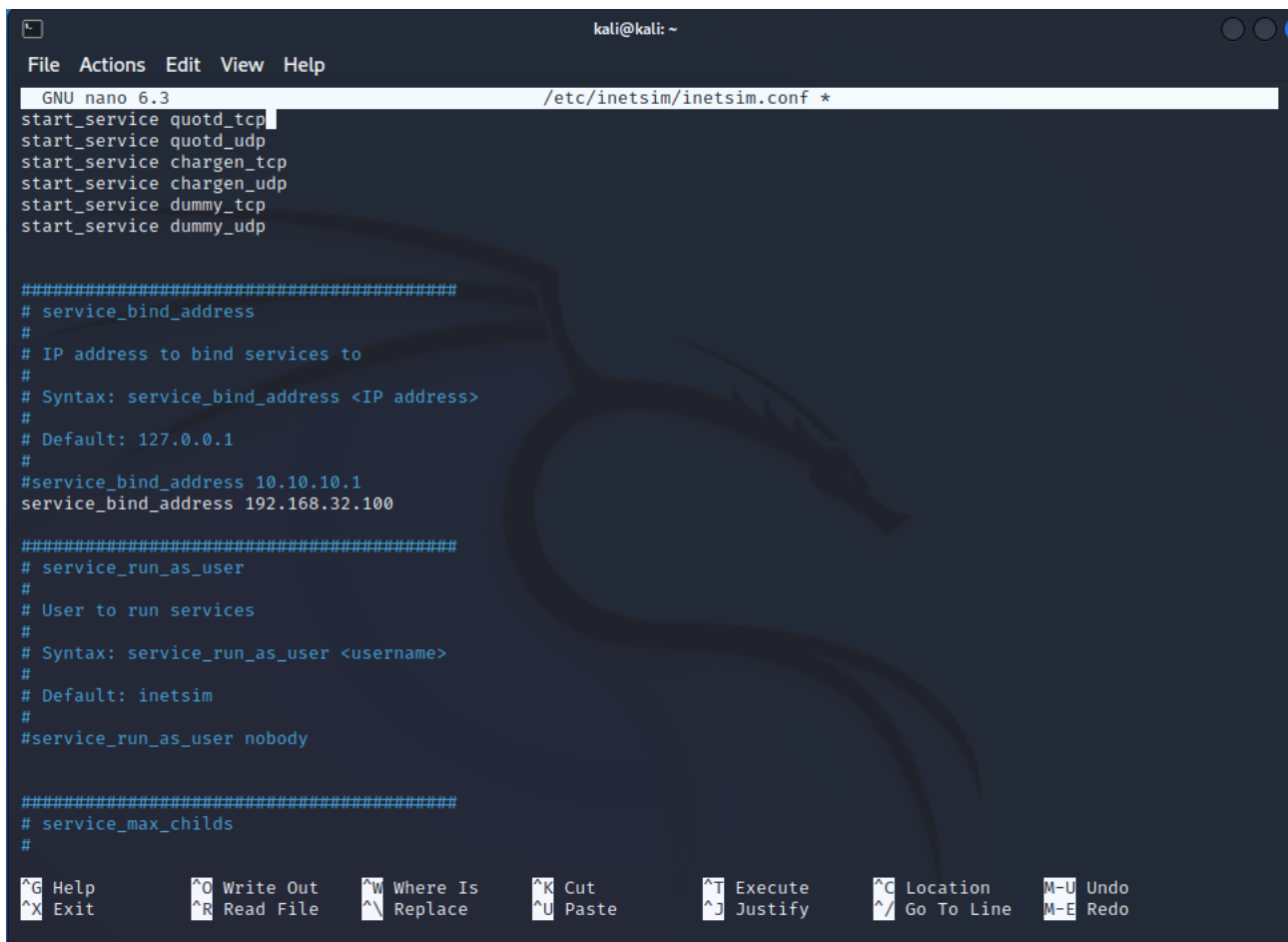
#####
# dns_default_hostname
#
# Default hostname to return with DNS replies
#
# Syntax: dns_default_hostname <hostname>
#
# Default: www
#
#dns_default_hostname somehost

#####
# dns_default_domainname
#
# Default domain name to return with DNS replies
#
# Syntax: dns_default_domainname <domain name>
#
# Default: inetsim.org
#
#dns_default_domainname some.domain
dns_default_domainname epicode.internal

#####
# dns_static

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line  M-E Redo
```

- Adesso aggiungiamo `service_bind_address` a cui assegniamo `192.168.32.100`



```

GNU nano 6.3 /etc/inetsim/inetsim.conf *
start_service quotd_tcp
start_service quotd_udp
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 10.10.10.1
service_bind_address 192.168.32.100

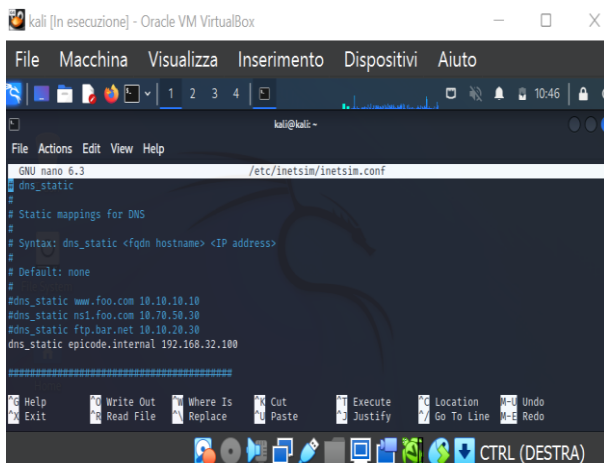
#####
# service_run_as_user
#
# User to run services
#
# Syntax: service_run_as_user <username>
#
# Default: inetsim
#
#service_run_as_user nobody

#####
# service_max_childs
#

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute   ^C Location   M-U Undo
^X Exit      ^R Read File  ^_ Replace    ^J Paste      ^_ Justify   ^_ Go To Line M-E Redo

```

Quindi continuiamo con la voce `dns_static` epicode.internal 192.168.32.100



```

GNU nano 6.3 /etc/inetsim/inetsim.conf
dns_static
#
# Static mappings for DNS
#
# Syntax: dns_static <fqdn hostname> <IP address>
#
# Default: none
#
#dns_static www.foo.com 10.10.10.10
#dns_static ns1.foo.com 10.70.50.30
#dns_static ftp.bar.net 10.10.20.30
dns_static epicode.internal 192.168.32.100

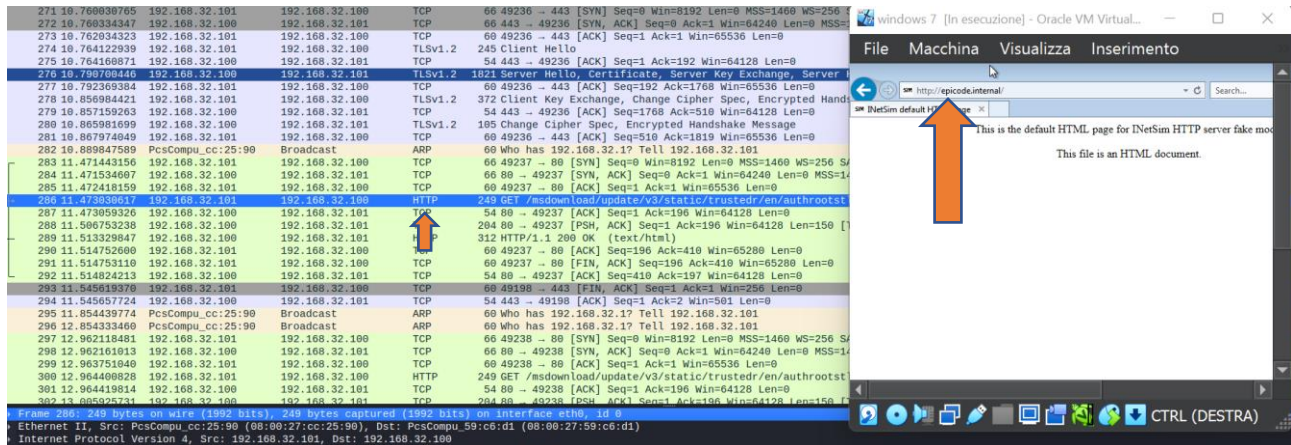
#####

```

Adesso avviamo Inetsim con il comando “`sudo inetsim`”

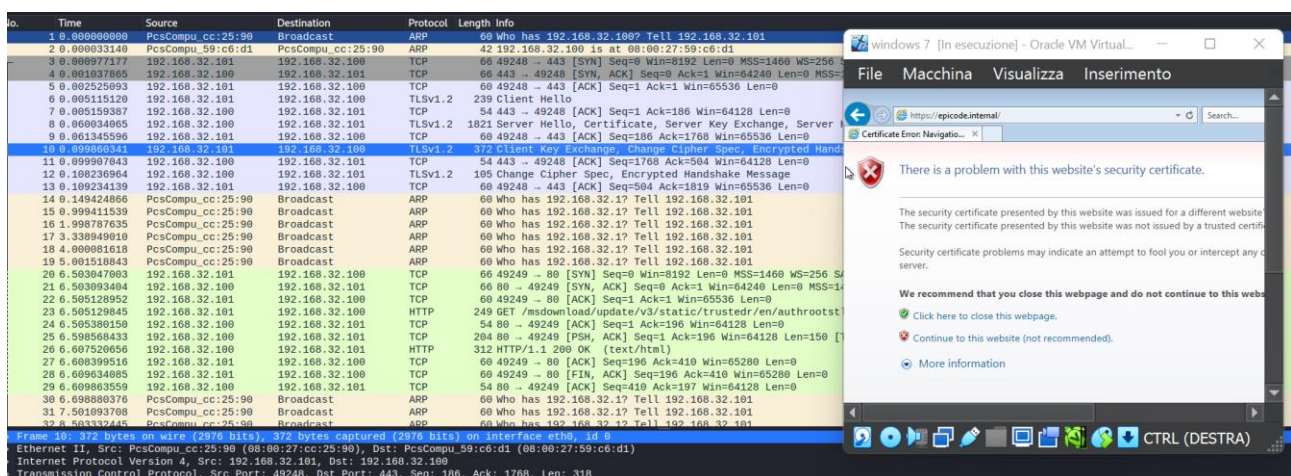
3) Registrazione dei pacchetti in transito con Wireshark

- Avviamo wireshark su kali come canale usiamo *any* avviamo la registrazione
- Apriamo internet explorer e digitiamo epicode.internal vedremo la pagina di default di inetsim
- Nella nostra schermata di wireshark invece vedremo vari pacchetti: TCP, ARP, HTTP



Come richiesto dalla traccia monitoriamo ora i pacchetti in transito sempre con epicode internal ma con il protocollo HTTPS

- Quindi nella barra di ricerca modificheremo l'URL aggiungendo una S



Come vediamo il pacchetto a differenza di quello http ci saranno dei pacchetti TLSv1.2 che come vediamo lavorano sulla porta 433.