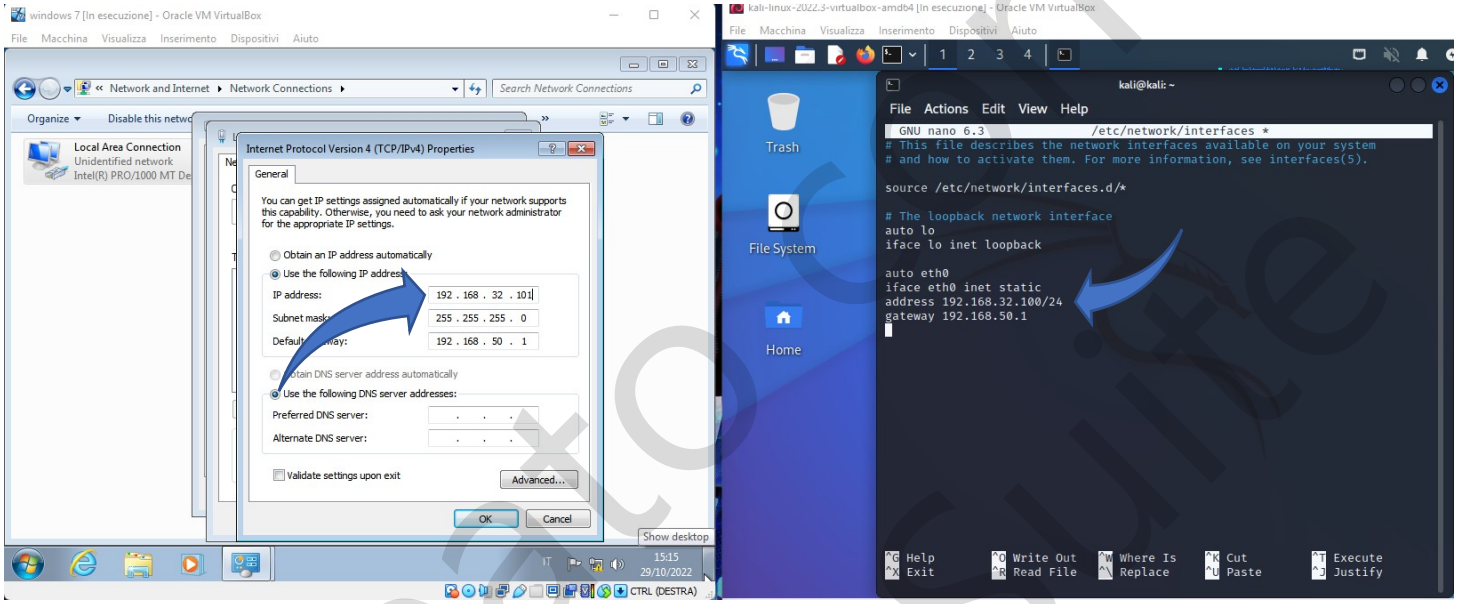
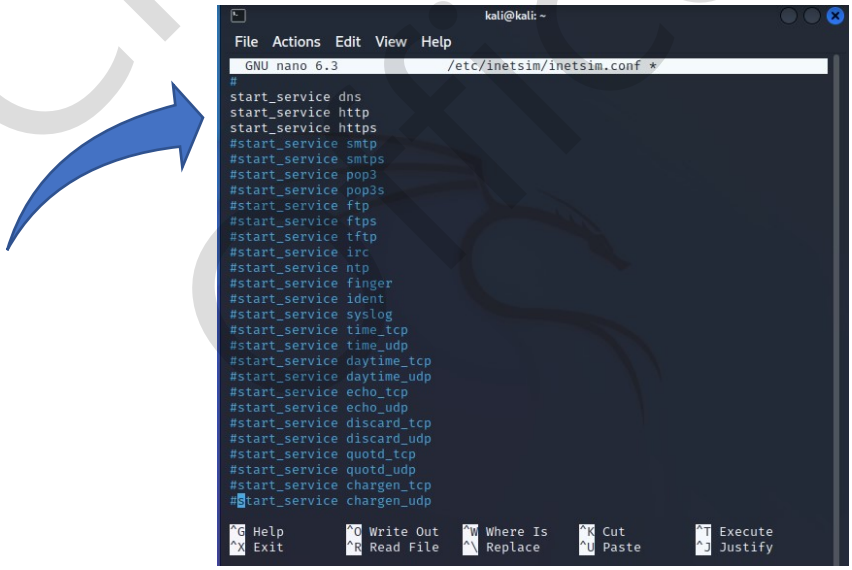
Claudio De Cicco

29/10/2022

Report del Venerdì



Come prima richiesta andiamo a modificare i nuovi IP di windows 7 e di linux. (rispettivamente 192.168.32.101 e 192.168.32.100)



Successivamente da linux andiamo ad aprire la configurazione di Inetsim in modo da lasciare attivi solo i servizi di cui abbiamo bisogno. Sempre nella configurazione andiamo ad assegnare al "dns bind address" l'ip di linux e al "dns static" , epicode.internal associandolo all'ip di linux (192.168.32.100)

```
#########################################
# 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
```

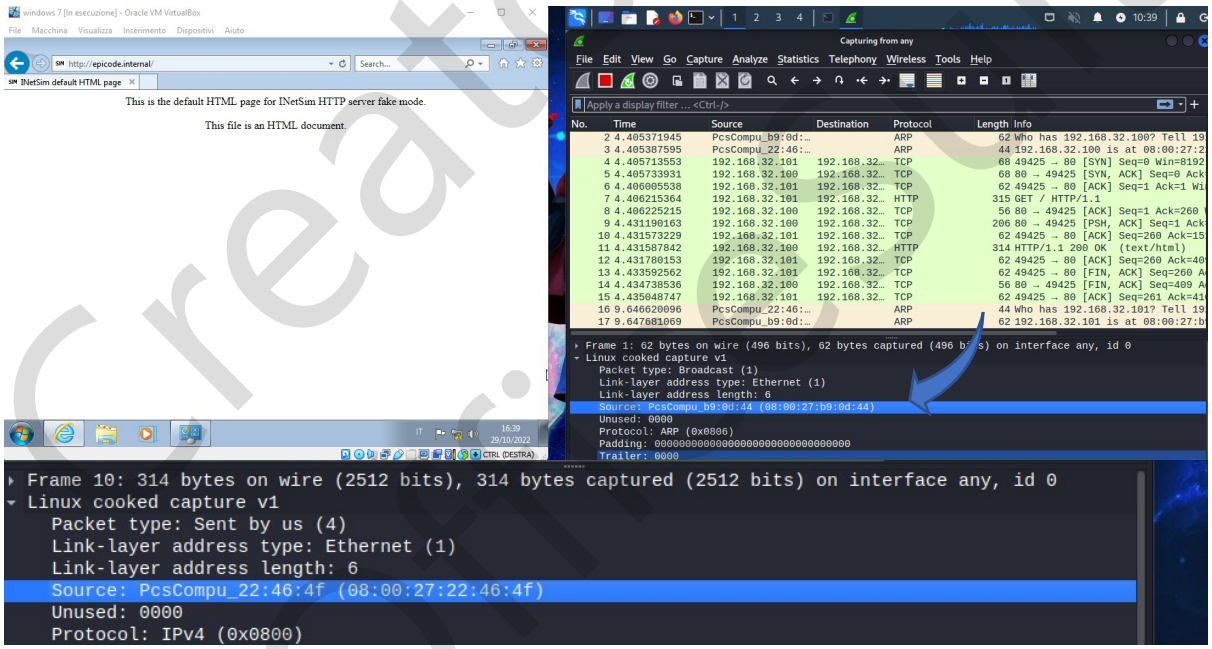
kali@kali: ~

File Actions Edit View Help

GNU nano 6.3 /etc/inetsim/inetsim.conf

```
########################################
# 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
```

Ora , dopo aver avviato la simulazione con inetsim , possiamo vedere come il sito venga raggiunto correttamente e come dal raporto di Wireshark si riesca a risalire ai MAC.



MAC linux 08:00:27:b9:0d:44

MAC Win 08:00:27:22:46:4f

Successivamente ho registrato anche la comunicazione sostituendo il server in HTTPS.

La differenza che possiamo notare è che ora abbiamo registrato una comunicazione che sfrutta il protocollo TLS che permette di crittografare lo scambio di dati conferendogli quindi maggiore sicurezza e privacy cosa che con server HTTP non avviene.