Simulazione rete complessa

29/09/23

Davide Diglio

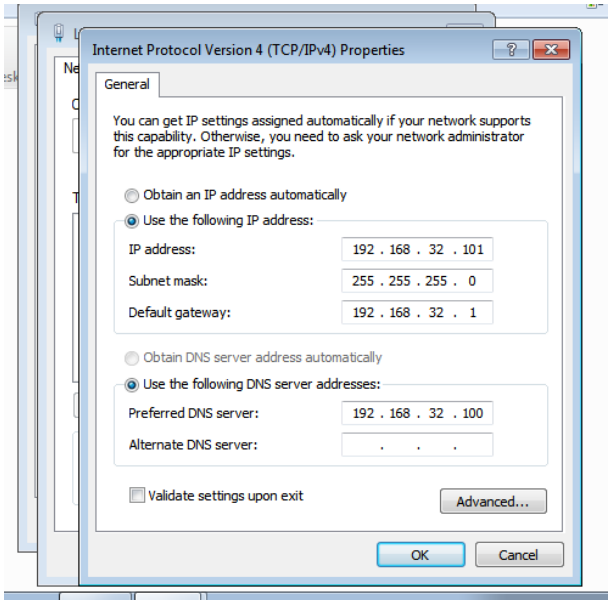
Obiettivi

1. Simulare un'architettura cliet server in cui l'indirizzo 192.186.32.101 richiede al l'indirizzo 192.168.32.100 un risorsa all'hostname epicode.internal tramite web browser.
2. Intercettare la comunicazione con Wireshark.

Svolgimento

In questo compito l'obiettivo era quello di intercettare la comunicazione tra i due indirizzi, evidenziando i Mac address ed il contenuto del HTTPS o HTTP.

Prima di intercettare la comunicazione si doveva impostare l'IP ai due client server (Kali con 192.168.32.100 e Windows 7 con 192.168.32.101).

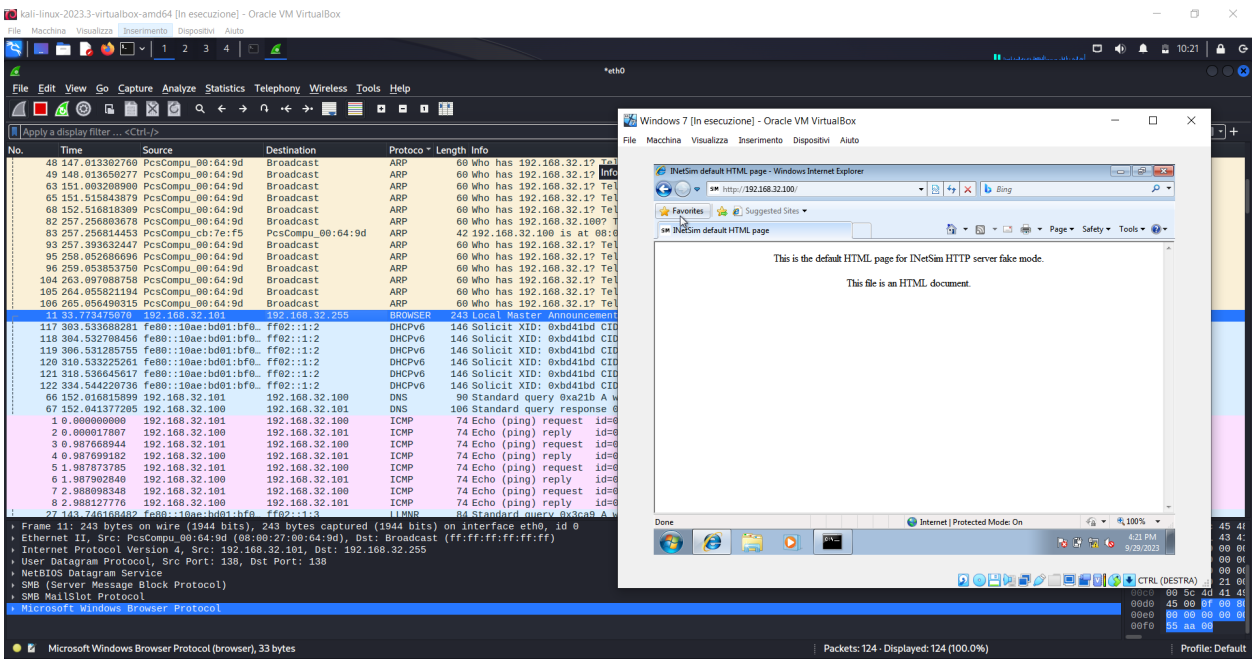


Dopodichè su Kali si doveva attivare il servizio DNS impostandolo; ad esempio:

```
##############################################
# dns_default_ip
#
# Default IP address to return with DNS replies
#
# Syntax: dns_default_ip <IP address>
#
# Default: 127.0.0.1
#
dns_default_ip 192.168.32.100
```

```
##############################################
# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
service_bind_address 192.168.32.100
```

dopo aver impostato tutto si inizia a intercettare la comunicazione con Wireshark cercando di evidenziare i Mac address e il contenuto della richiesta HTTPS.



Conclusione

Questa simulazione abbiamo visto come intercettare la comunicazione tramite Wiresahrk e come impostare un server DNS e attivare anche i server HTTP/HTTPS che sono dei protocolli di comunicazione tra client e un server web e la principale differenza è che HTTPS è più sicuro, perchè in forma criptata.