Esercitazione creazione rete tra due macchine

Prerequisiti:

Creare una rete tra due macchine così composta:

- kali linux con IP 192.168.32.100
- windows 7 con IP 192.168.32.101

La macchina kali dovrà fare sia da server HTTP e HTTPS che da server DNS. Dalla macchina windows dovremo accedere al sito "epicode.internal" e sniffare i pacchetti con wireshark su kali linux.

Metodologia:

Ho impostato l'ip della macchina kali lanciando il comando:

sudo nano /etc/network/interfaces

Su windows sono andato nelle impostazioni di rete ed ho modificato la sezione Internet Protocol Version 4 ed ho inserito due parametri:

- l'ip della macchina
- l'ip del server DNS (ip impostato su inetsim che crea il server DNS)

Una volta terminato questo passaggio si sono susseguite due fasi sulla macchina kali:

- test del servizio http
- test del servizio https

Per attivare i relativi servizi ho modificato il file di configurazione di inetsim lanciando questo comando:

sudo nano /etc/inetsim/inetsim.conf

all'interno del file ho attivato il servizio DNS e HTTP e ho impostato i parametri come segue:

service_bind_address 192.168.32.100

dns_default_ip 192.168.32.100

dns_static epicode.internal 192.168.32.100

Il primo parametro imposta l'indirizzo IP del server che di default corrisponde a quello di loopback o localhost.
Il secondo parametro imposta l'indirizzo IP del server DNS che in questo caso coincide
Mentre il terzo parametro crea l'associazione tra il dominio epicode.internal all'indirizzo ip del server.

Terminato questo passaggio ho testato se tutto funzionasse con dei ping da terminale e successivamente ho testato dal browser su windows. Nello stesso tempo ho lasciato in ascolto wireshark per sniffare i pacchetti e verificare che venissero scambiati.
Lo stesso procedimento è stato poi ripetuto per il protocollo HTTPS andando a cambiare il servizio attivo all'interno di inetsim.

Conclusioni:
Le principali differenze che ho potuto constatare si riscontrano nel pacchetto trasmesso. Attraverso l'utilizzo del protocollo HTTP il pacchetto è in chiaro ed è possibile vedere il contenuto del sito che la macchina windows 7 sta visitando. Al contrario con l'utilizzo del protocollo HTTPS possiamo osservare che il pacchetto viene cifrato grazie al protocollo TLS e non è possibile vederne il contenuto.

29/09/2023
Davide Lecci