Relazione progetto Networking Modulo 1

Il progetto sostanzialmente prevedeva l'impostazione degli indirizzi IP in modo tale da permettere la comunicazione da Windows 7 a Kali Linux tramite la connessione settata su internal. Mi sono servito del server DNS (Domain Name System) per assegnare al dominio 'epicode.internal' l'indirizzo IP di Kali, in modo tale che attraverso una regolare ricerca su internet partita da Windows 7, cercando il dominio richiesto, sarebbe avvenuta la connessione alla risorsa richiesta. Per settare il DNS in base alle necessità, ho usato il software 'inetsim', il quale permette di simulare i servizi internet più richiesti, ad esempio http, https e DNS. Tornando a Windows e settati gli indirizzi IP e quello di DNS, che sarebbe quello di kali e del dominio, ho creato una nuova regola del Firewall per permettere la connessione in uscita solo all'indirizzo IP assegnato al DNS. Tornando su Kali, ho attivato WireShark per iniziare a tracciare i pacchetti di dati scambiati. Ovviamente a questo punto, tramite Internet Explorer, ho inoltrato la richiesta http al dominio 'epicode.internal'. Il protocollo ARP è entrato subito in gioco per poter assegnare l'IP di Kali ad un indirizzo MAC, e una volta assegnato, tramite il protocollo TCP sono partiti i tre messaggi di connessione, Syn, Syn-Ack e Ack, appunto per stabilire la connessione sicura e inviare dati tramite i MAC address unici per ciascuna macchina. Utilizzando la richiesta https invece, la richiesta non va a buon fine, ed esce "There is a problem with the website's security certificate". Immagino sia intervenuto il certificato di sicurezza SSL (Secure Socket Layer) che di norma cifra il traffico per garantire la sicurezza e l'integrità dei dati. La differenza dunque è

chiara, la richiesta http garantisce meno protezione dei propri dati, mentre quella https alza più barriere protettive.