EPICODE

Esercizio S2 – L1

Immagine che contiene diagramma, schermata, cerchio, testo

Descrizione generata automaticamente

Si è creata una rete LAN con 1 router, 3 switch e un NAS (dispositivo di archiviazione intelligente). Questa struttura di rete è adatta ad un’azienda.

La rete è protetta da un firewall perimetrale dinamico che permette di proteggere la rete LAN dall’esterno senza dover inserire manualmente tutti i parametri da bloccare come in un firewall statico. Considerando la grandezza di internet è ormai una scelta obbligata. Ciò permette quindi una maggior sicurezza a discapito di un’accessibilità limitata in quanto è possibile ricevere pacchetti di dati solamente da chi è già stato destinatario di un pacchetto proveniente dall’interno della nostra rete LAN.

È necessario quindi creare una zona “demilitarizzata” (DMZ) per poter ricevere i pacchetti di dati dall’esterno liberamente. In questo caso è presente un server web (HTTP) e un server di posta elettronica (SMTP). Questa zona non protetta da firewall necessita di una difesa. Per questo si è implementato un WAF (Web Application Firewall) in grado di leggere i pacchetti e, confrontandoli con quelli a disposizione grazie ad un database, riconoscere potenziali pericoli.

Per una maggiore difesa della rete LAN, in caso di inefficacia del WAF a protezione della zona DMZ, si è aggiunto un IPS in grado di rilevare e bloccare attacchi informatici provenienti dall’esterno. Oltre al firewall perimetrale per difendere ulteriormente il NAS (essendo un dispositivo di archiviazione contiene spesso dati sensibili) si è aggiunto un IDS che è in grado di rilevare potenziali attacchi informatici. L’IDS, a differenza dell’IPS, non blocca automaticamente i potenziali attacchi, ma si limita a segnalarli. Così da poter intervenire solo quando realmente necessario senza dover subire problematiche in termini di accessibilità.