Sicurezza delle reti

Teoria dei Firewall

Minacce alla sicurezza di rete

- Non-strutturate
- Strutturate
- Esterne
- Interne

Minacce non-strutturate

- Portate avanti da persone non molto esperte
- Utilizzati tools reperibili liberamente in internet
- Motivazione di base di tipo intellettuale
- Script kiddies o kiddiots

Minacce strutturate

- Hacker motivati e skilled
- Grande conoscenza delle reti e comprensione degli strumenti di hacking
- Intenzioni a volte malevoli

Minacce esterne-interne

- Esterne: portate tramite collegamenti Internet o Dial-up
- Interne: portate da personale interno, che approfitta dei propri account e della propria presenza fisica all’interno della rete.

Primary network attacks

- Reconnaissance attacks
- Access attacks
- DOS attacks

Reconnaisance attacks

- Mappature dei sistemi, dispositivi, della rete, ottenuta in maniera non autorizzata
- Ping generalizzato per scoprire quali IP rispondono, poi ricerca dei servizi attivi su questi IP per scoprirne versioni ed eventuali vulnerabilità

Access attacks

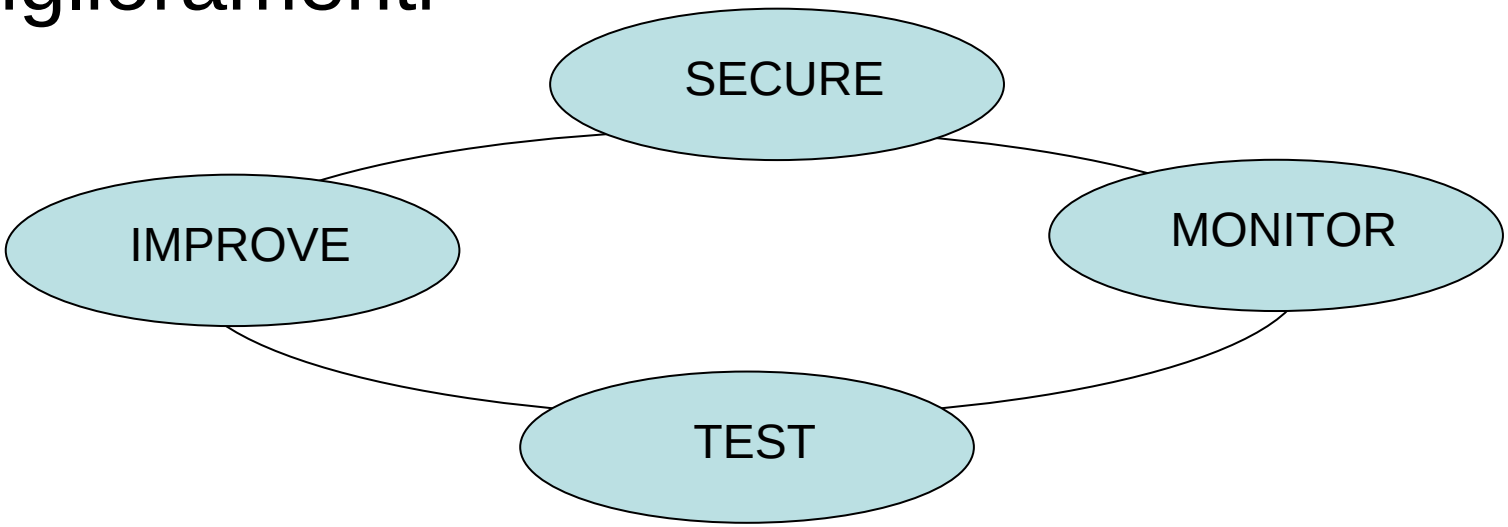
- Accesso ai dati e manipolazione degli stessi non autorizzato: es shared folder, stazioni di lavoro lasciate “aperte” e incustodite
- accesso ai sistemi: utilizzando script, social engineering
- Escalation dei privilegi: si ottengono privilegi superiori con cui installare sniffer, key-logger ecc ecc

DoS attacks

- Quando viene disabilitato un servizio, bloccato un network, crash del sistema
- Per lo più si utilizzano script o tools ad-hoc

Sicurezza in 4 passi

- Hardening dei sistemi
- Controllo dei sistemi
- Test
- Miglioramenti



Cos’è un Firewall?

- Sorta di porta blindata, muro di fuoco che protegge “l’interno” dall’”esterno”
- Come porta blindata non serve a nulla se le finestre non hanno inferriate o la chiave è a disposizione di tutti
- Non può essere il sostituto di una buona politica di sicurezza, infatti…

…è inutile un firewall se…

- Esistono altri accessi alla rete non protetti
- Le applicazioni utilizzate sono piene di vulnerabilità
- Gli utenti sono “disinvolti” nel comunicare le password e la struttura di rete
- Sono presenti reti WLAN non protette

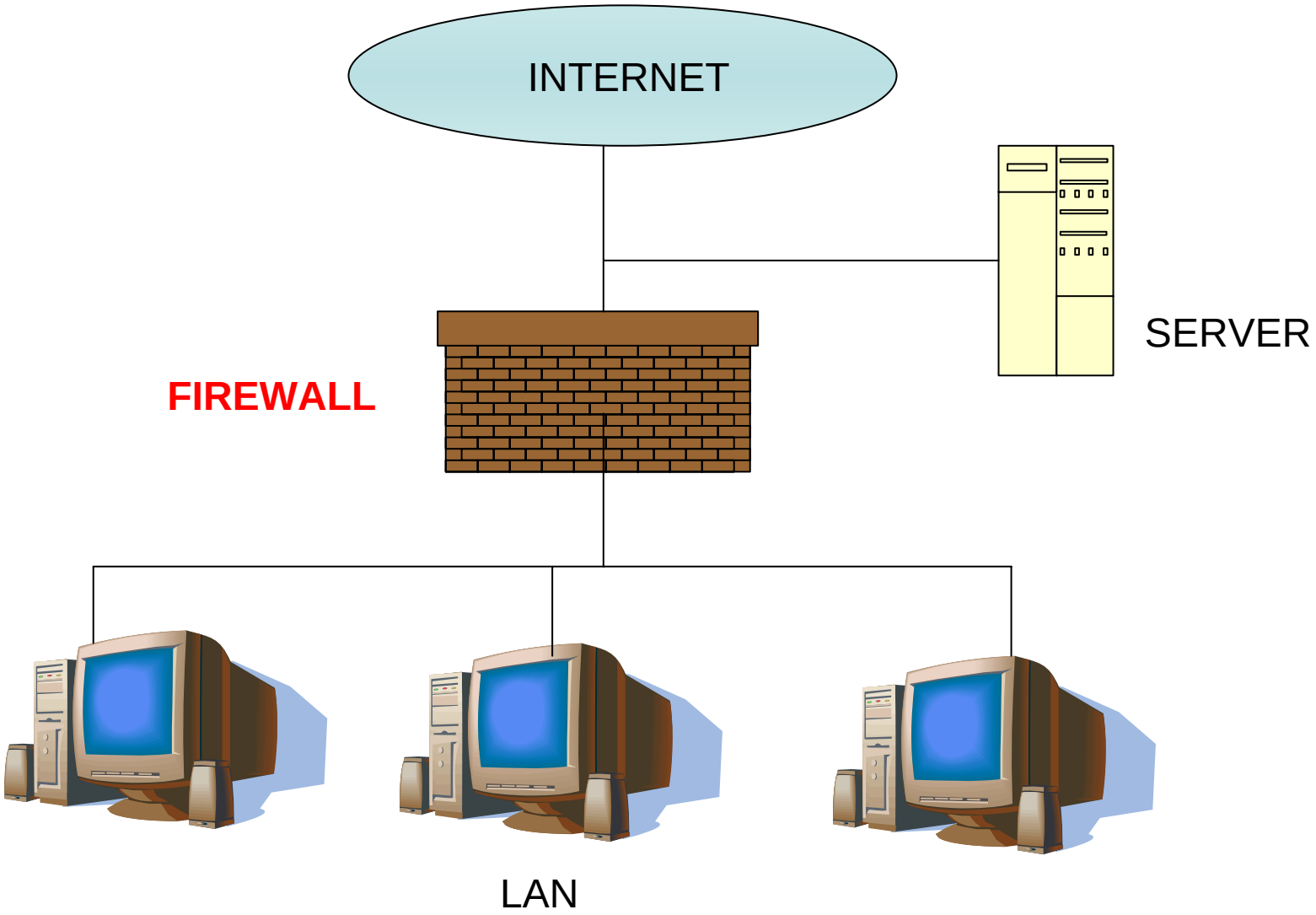
Cosa fa il Firewall?

- Suddivide la rete in “zone” ed è in grado di applicare regole che gestiscano il passaggio di dati tra queste zone, guardando indirizzi IP e servizi
- Di norma non è in grado di entrare nei pacchetti di dati e verificarne il contenuto (content filtering)

Tipologia dei Firewall

- Stateless: analizza ogni pacchetto come entità singola
- Stateful: analizza i pacchetti nel loro insieme, come “flusso di dati”

Posizionamento del Firewall (1)



Posizionamento del Firewall (2)