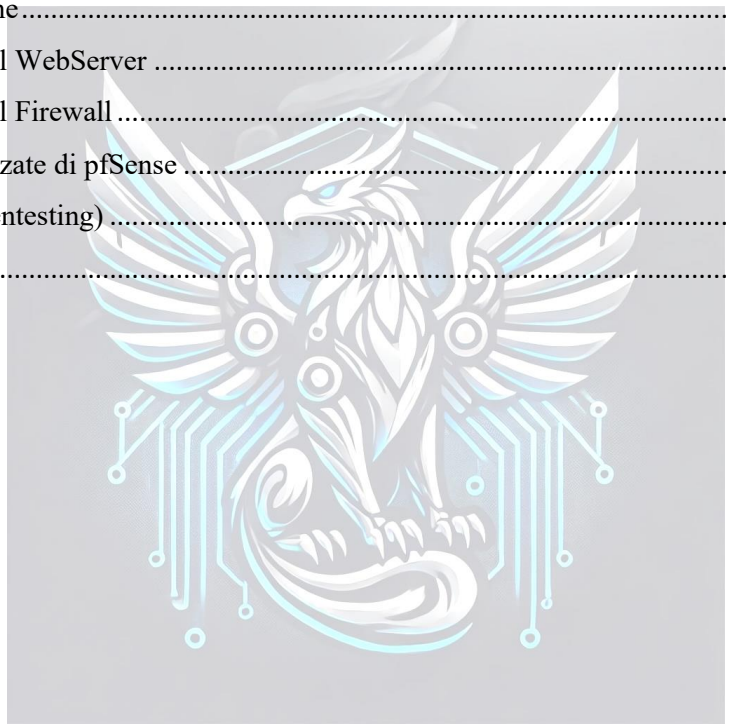
REPORT CONFIGURAZIONE FIREWALL, WEB SERVER E RETE INTERNA

Sommario



Report sulla Configurazione del Firewall, WebServer e Rete Interna

Introduzione

L'obiettivo del progetto era implementare una rete interna per l'azienda Theta, garantendo un alto livello di sicurezza, semplicità d'uso e scalabilità. Il mio ruolo specifico si è concentrato sulla progettazione, configurazione e collaudo della rete interna, con particolare attenzione all'implementazione di un WebServer intuitivo e sicuro, nonché alla configurazione di un firewall per proteggere la rete e ottimizzarne l'accesso.

Studio della Soluzione

Per rispondere alle esigenze di Theta, ho condotto uno studio approfondito sulle tecnologie disponibili, considerando costi, prestazioni e versatilità. La scelta del firewall è ricaduta su pfSense, un software open-source noto per il suo eccellente rapporto qualità-prezzo e la flessibilità. Questa piattaforma non solo consente configurazioni avanzate ma è installabile su una vasta gamma di dispositivi hardware, rendendola ideale per una soluzione aziendale scalabile.

Configurazione del WebServer

Il WebServer rappresenta un punto centrale della rete interna, essendo progettato per essere accessibile anche ai dipendenti meno esperti in tecnologia. Gli obiettivi principali erano:

- Facilità d'uso: la configurazione dell'interfaccia e delle risorse disponibili è stata progettata per risultare intuitiva e navigabile.
- Sicurezza: il server è stato posizionato su una rete separata e protetto tramite regole del firewall per prevenire accessi non autorizzati e attacchi da reti esterne.
- Accesso multi-rete: il server è accessibile da dipendenti che operano su diverse reti, ma sempre attraverso canali protetti da crittografia e autenticazione.

Per garantire questi requisiti, sono state adottate tecnologie standard come HTTPS per le comunicazioni e un'infrastruttura di autenticazione centralizzata, integrata con il firewall per un controllo granulare degli accessi.

Configurazione del Firewall

Il firewall pfSense è stato configurato per proteggere la rete interna e gestire in modo flessibile le comunicazioni tra i diversi segmenti aziendali. Le principali configurazioni implementate includono:

Regole di Firewall Personalizzate

1. Separazione delle Reti:

- Alcuni piani aziendali sono stati isolati completamente per motivi di sicurezza. Questo è stato realizzato mediante VLAN (Virtual LAN) e regole che bloccano qualsiasi traffico non esplicitamente autorizzato tra di esse.
- Per altri piani è stata implementata una comunicazione unilaterale, permettendo ai dispositivi di inviare dati a server centrali senza ricevere traffico in ingresso.

2. Filtri per il Web:

- Sono stati configurati filtri per bloccare l'accesso a siti web notoriamente pericolosi, tra cui piattaforme vulnerabili come DVWA (Damn Vulnerable Web Application), che potrebbero essere utilizzate per testare exploit
- Questi filtri riducono il rischio di errore umano da parte di dipendenti che potrebbero cliccare su link malevoli.

3. Regole di Accesso Basate su IP e Porte:

- L'accesso alle risorse è stato regolato con precisione, consentendo solo a specifici indirizzi IP di comunicare attraverso porte predefinite.

Funzionalità Avanzate di pfSense

- VPN (Virtual Private Network): Implementata per consentire connessioni sicure da remoto per i dipendenti che lavorano fuori sede.
- Intrusion Detection and Prevention System (IDS/IPS): Configurato per monitorare e bloccare tentativi di attacco o traffico sospetto.
- Load Balancing e Failover: Per garantire disponibilità continua della rete interna e del WebServer.

Test di Sicurezza (Pentesting)

In collaborazione con i miei colleghi Octavian Ceresau e Leonardo Nigro, è stato condotto un approfondito processo di pentesting per identificare eventuali vulnerabilità nella rete. Utilizzando software sviluppati da loro, sono stati simulati diversi scenari di attacco, analizzando i seguenti aspetti:

- Forza delle regole di firewall: Testando la capacità del firewall di bloccare tentativi di intrusione provenienti sia dall'interno che dall'esterno.
- Robustezza del WebServer: Simulazioni di attacchi DoS (Denial of Service) e tentativi di accesso non autorizzato per verificare la resilienza del sistema.
- Protezione da phishing e malware: Valutazione delle capacità di bloccare link malevoli.

I risultati di questi test hanno portato a ulteriori ottimizzazioni delle regole del firewall e alla definizione di policy più restrittive.

Conclusioni

La rete interna di Theta è stata progettata per essere robusta, sicura e intuitiva. L'implementazione del firewall pfSense e del WebServer ha garantito:

- Una protezione completa contro attacchi esterni e rischi interni.
- Accesso controllato e sicuro alle risorse aziendali.
- Semplicità d'uso per i dipendenti, con una configurazione che consente di lavorare in ambienti diversi senza compromessi sulla sicurezza.

Grazie alla collaborazione con il team il progetto ha raggiunto un livello di sicurezza tale da rendere la rete aziendale virtualmente inespugnabile, rispondendo pienamente alle esigenze di Theta. Per dettagli aggiuntivi sugli aspetti software, si rimanda al contributo dei colleghi Octavian Ceresau e Leonardo Nigro.