RANCANG BANGUN KOMUNIKASI INTERNAL BERBASIS *VOICE OVER INTERNET PROTOCOL (VOIP)* DENGAN PENGAMANAN *FAIL2BAN* TERHADAP SERANGAN *SESSION INITIATION PROTOCOL (SIP)*

(Studi Kasus: Gedung Teknik Informatika dan Gedung C)

Nama Mahasiswa : Danil Hanapi

NIM : 6103230032

Dosen Pembimbing : Wahyat, S.Kom., M.Kom.

ABSTRAK

Ketergantungan pada layanan seluler berbayar dan aplikasi pihak ketiga di lingkungan instansi sering kali menyebabkan inefisiensi biaya dan risiko keamanan data. Sebagai solusi, penelitian ini bertujuan membangun infrastruktur komunikasi *Voice over Internet Protocol* (*VoIP*) mandiri menggunakan *IP-PBX Asterisk* dengan aplikasi klien *custom* berbasis *Flutter*, serta mengamankannya dari serangan siber menggunakan *Intrusion Prevention System* (*IPS*) *Fail2Ban*. Metode pengembangan sistem menggunakan kerangka kerja *Network Development Life Cycle* (*NDLC*). Pengujian dilakukan melalui uji fungsionalitas lintas jaringan dan uji penetrasi keamanan terhadap serangan *SIP Brute Force*. Hasil pengujian fungsionalitas menunjukkan bahwa aplikasi klien berhasil mengeksekusi panggilan suara, panggilan video berbasis *WebRTC*, dan sinkronisasi pesan instan melalui antarmuka *REST API* tanpa kendala jeda (latensi) yang mengganggu. Pada pengujian keamanan menggunakan simulasi serangan *SIPVicious* (*svcrack*), sistem mencapai tingkat keberhasilan 100% dalam mendeteksi anomali autentikasi. *Fail2Ban* secara otomatis memblokir IP penyerang pada *firewall* (*Iptables*) di *port* 5060 dalam hitungan detik. Kesimpulannya, penelitian ini menghasilkan ekosistem komunikasi internal yang terbukti andal, dengan tolak ukur kelancaran operasional fitur komunikasi lintas jaringan dan tingkat keberhasilan 100% dalam menggagalkan eksploitasi akses ilegal secara otomatis.

Kata Kunci: VoIP, Asterisk, Fail2Ban, Flutter, Keamanan Jaringan.

DESIGN AND IMPLEMENTATION OF AN INTERNAL COMMUNICATION SYSTEM BASED ON VOICE OVER INTERNET PROTOCOL (VOIP) WITH FAIL2BAN SECURITY MECHANISM AGAINST SESSION INITIATION PROTOCOL (SIP) ATTACKS

(*Case Study*: Gedung Teknik Informatika dan Gedung C)

Student Name : Danil Hanapi

Student ID : 6103230032

Supervisor : Wahyat, S.Kom., M.Kom.

ABSTRACT

Reliance on paid cellular services and third-party applications in institutional environments often causes cost inefficiency and data security risks. As a solution, this study aims to build an independent Voice over Internet Protocol (VoIP) communication infrastructure using Asterisk IP-PBX with a custom Flutter-based client application, secured from cyber attacks using the Fail2Ban Intrusion Prevention System (IPS). The system development uses the Network Development Life Cycle (NDLC) framework. Evaluations were conducted through cross-network functionality testing and security penetration testing against SIP Brute Force attacks. Functionality test results show that the client application successfully executes voice calls, WebRTC-based video calls, and instant messaging synchronization via a REST API without disruptive latency. In security testing using SIPVicious (svcrack) simulation, the system achieved a 100% success rate in detecting authentication anomalies. Fail2Ban automatically blocked the attacker's IP at the firewall (Iptables) on port 5060 within seconds. In conclusion, this research produced an internal communication ecosystem with proven reliability, measured by the seamless operation of cross-network communication features and a 100% success rate in automatically thwarting illegal access exploitation.

Keywords: *VoIP, Asterisk, Fail2Ban, Flutter, Network Security.*

.

.