

## DAFTAR GAMBAR

---

Gambar 2. 1 Sistem Keamanan HIDS OSSIM.....	7
Gambar 3. 1 Topologi sistem Saat ini .....	10
Gambar 3. 2 Topologi sistem usulan.....	11
Gambar 4. 1 Proses instalasi awal.....	15
Gambar 4. 2 Pemilihan Bahasa .....	16
Gambar 4. 3 Pemilihan zona waktu .....	16
Gambar 4. 4 Pemilihan konfigurasi keyboard.....	17
Gambar 4. 5 Proses menentukan IP OSSIM.....	17
Gambar 4. 6 Proses pengisian password root .....	18
Gambar 4. 7 Pemilihan zona waktu .....	18
Gambar 4. 8 Proses instalasi selesai dan proses booting .....	19
Gambar 4. 9 Tampilan login root .....	19
Gambar 4. 10 Proses instalasi OSSEC Agent pada host windows .....	20
Gambar 4. 11 Proses instalasi OSSEC Agent .....	20
Gambar 4. 12 Centang secara default pada OSSEC Agent.....	21
Gambar 4. 13 Pemilihan lokasi file penginstalan.....	21
Gambar 4. 14 Proses instalasi OSSEC Agent .....	22
Gambar 4. 15 Instalasi OSSEC Agent selesai .....	22
Gambar 4. 16 Extract key pada OSSEC agent .....	22
Gambar 4. 17 Pengisian IP server dan key.....	23
Gambar 4. 18 OSSEC Agent berhasil berjalan untuk terhubung ke server OSSIM .....	23
Gambar 4. 19 Status IDS telah terhubung dengan host .....	24
Gambar 4. 20 Status IDS telah aktif pada host .....	24
Gambar 4. 21 Terdapat error pada saat konfigurasi.....	25
Gambar 4. 22 nmap scan .....	26
Gambar 4. 23 Dos Attack menggunakan hping3 .....	27
Gambar 4. 24 Kondisi traffic sebelum penyerangan .....	27
Gambar 4. 25 Kondisi traffic saat terjadi penyerangan .....	28
Gambar 4. 26 SSH Brute Force Attack .....	28
Gambar 4. 27 nmap scan .....	29
Gambar 4. 28 Tampilan alert setelah port scanning.....	30
Gambar 4. 29 DoS Attack menggunakan hping3 .....	30
Gambar 4. 30 Kondisi traffic sebelum penyerangan .....	31
Gambar 4. 31 Kondisi traffic setelah penyerangan.....	31
Gambar 4. 32 Alert DoS belum muncul setelah penyerangan .....	32
Gambar 4. 33 SSH Brute Force Attack .....	32
Gambar 4. 34 Alert login failed .....	32
Gambar 4. 35 Alert SSH failed.....	33
Gambar 4. 36 IP penyerang diblokir oleh active response .....	33

Gambar 4. 37 IP penyerang diblokir .....33