

## Daftar Gambar

Gambar 2.A ilustrasi Serangan DoS	4
Gambar 2.B database signature fortinet pada fortiguard	7
Gambar 2.C ilustrasi Serangan Traffik Pada firewall	8
Gambar 2.D Fixed Contoh lalu lintas Jaringan	12
Gambar 2.E Kerangka Pemikiran	13
Gambar 2.F Perbandingan Dos kepada 2 hardware	14
Gambar.3.A skema topologi yang sedang berjalan	18
Gambar 4.A memusatkan titik penelitian	22
Gambar 4.B utilitas dalam command Hping3	23
Gambar 4.C Skema testing tanpa firewall	24
Gambar 4.D hasil test tanpa firewall	24
Gambar 4.E Hasil tes tanpa firewall 2	25
Gambar 4.E Skema testing penyerangan pada firewall signature-based	26
Gambar 4.G informasi serangan pada firewall signature-based	27
Gambar 4.H informasi serangan pada database signature Fortinet	27
Gambar 4.I skema testing firewall behavior-based	28
Gambar 4.J tampilan dvwa diakses dari jaringan	29
Gambar 4.K Tampilan dashboard Fortiddos	30
Gambar 4.L Fortiddos mengganti password	31
Gambar 4.M Fortiddos mengatur hak user	31
Gambar 4.N Fortiddos menjadi super admin	32
Gambar 4.N Login Test	32
Gambar 4.O Fortiddos setting interfaces	33
Gambar 4.P Fortiddos setting DNS	33
Gambar 4.Q Fortiddos setting route gateway	34
Gambar 4.R fortiddos setting service protection policy	34
Gambar 4.S fortiddos setting protection profile	35
Gambar 4.T Fortiddos setting protection profile 2	35
Gambar 4.U fortiddos setting mode detection	36
Gambar 4.W Tampilan Hping3 pada pc penyerang	37
Gambar 4.X Informasi grafik adanya serangan	37
Gambar 4.Y informasi detail serangan	38
Gambar 4.Z skema testing jaringan hybrid	39
Gambar 4.AA tampilan command hping3	39
Gambar 4.AB Firewall signature informasi yang lebih detail	40
Gambar 4.AC informasi serangan pada fortinet signature	40