

DAFTAR ISI

BAB I PENDAHULUAN	15
1.1 Latar Belakang	15
1.2 Identifikasi Masalah	17
1.3 Tujuan Penelitian	17
1.4 Manfaat Penelitian	18
1.5 Lingkup Tugas Akhir	18
1.6 Sistematika Penulisan Tugas Akhir	18
BAB II LANDASAN TEORI	20
2.1 Network Development Life Cycle	20
2.2 IDPS	21
2.3 PfSense	22
2.4 Snort	22
2.5 Penetration Testing	23
2.6 Kali Linux	23
2.7 Indeks KAMI	24
BAB III METODE PENELITIAN	28
3.1 Waktu dan Tempat Penelitian	28
3.2 Metode Pengumpulan Data	28
3.3 Metodologi Pengembangan Sistem	29
3.4 Penelitian terdahulu	32
3.5 Analisis Sistem Berjalan	39
3.5.1 <i>Topology Physical</i>	39
3.5.2 <i>Topology Logical</i>	40
3.6 Analisis Masalah	42
3.7 Implementasi Usulan	43
3.7.1 <i>Topology Physical Usulan</i>	44
3.7.2 <i>Topology Logical Usulan</i>	45
3.8 Jadwal Perencanaan	46
BAB IV PEMBAHASAN	47
4.1 Pra Asesment Indeks KAMI	47
4.2 Implementation	50
4.2.1 <i>Analysis</i>	50
4.2.2 <i>Design</i>	51

4.2.3	Simulasi.....	52
4.2.4	Implementation	55
4.2.5	Monitoring	81
4.2.6	Management.....	83
4.3	Penetration Testing	83
4.3.1	UDP Flooding	84
4.3.2	SYN Flooding	86
4.3.3	MAC Flooding	87
4.3.4	ARP Poisoning.....	88
4.3.5	DNS Spoofing.....	90
4.3.6	DHCP Starvation.....	91
4.3.7	DHCP Rogue.....	92
4.3.8	SSH Brute Force	93
4.4	Pasca Installation Assesment Indeks KAMI.....	94
BAB V KESIMPULAN DAN SARAN		98
5.1	Kesimpulan	98
5.2	Saran.....	98
Daftar Pustaka.....		100
Lampiran		104

DAFTAR GAMBAR

Gambar 2-1. Network Development Life Cycle	21
Gambar 2-2. Tingkat Kematangan	26
Gambar 3-1. Topologi Physical Berjalan	39
Gambar 3-2. Topologi Logical Berjalan	40
Gambar 3-3. Topologi Physical Usulan	44
Gambar 3-4. Topologi Logical Usulan	45
Gambar 4-1. Penilaian Awal NA	47
Gambar 4-2. Penilaian Awal SA	48
Gambar 4-3. Grafik Penilaian Awal	49
Gambar 4-4. Topologi Berjalan	50
Gambar 4-5. Topologi Usulan	51
Gambar 4-6. Simulation Topology	52
Gambar 4-7. Hasil Simulasi	53
Gambar 4-8. Ip Address Yang Terblokir	53
Gambar 4-9. Attack Simulation Topology	54
Gambar 4-10. Hasil Uji Serang	54
Gambar 4-11. IP Address Yang Terblokir	55
Gambar 4-12. Cable Topology	56
Gambar 4-13. Kabel FO pada Switch Distribution	56
Gambar 4-14. Kabel FO Pada pfsense	57
Gambar 4-15. License Agreement	57
Gambar 4-16. Installation Option	58
Gambar 4-17. Layout Keyboard	58
Gambar 4-18. Partition Option	59
Gambar 4-19. Partition Configuration	59
Gambar 4-20. RAID Configuration	60
Gambar 4-21. Installation Harddisk Option	60
Gambar 4-22. Installation Warning	61
Gambar 4-23. Installation Process	61
Gambar 4-24. Configuration Option	62
Gambar 4-25. Reboot Option	62
Gambar 4-26. Main Menu	63
Gambar 4-27. IP Address Configuration	63
Gambar 4-28. Successful Installation	64
Gambar 4-29. pfSense Web Configurator	64
Gambar 4-30. Setup Agreement	65
Gambar 4-31. General Setup	65
Gambar 4-32. Time Server Setup	66
Gambar 4-33. WAN Setup	66
Gambar 4-34. LAN Setup	67
Gambar 4-35. Password Setup	67
Gambar 4-36. Reload Option	67
Gambar 4-37. Reload Process	68

Gambar 4-38. Completion Setup	68
Gambar 4-39. pfSense Dashboard.....	69
Gambar 4-40. Interface Configuration.....	69
Gambar 4-41. OPT1 Setup.....	70
Gambar 4-42. OPT1 Apply Configuration	70
Gambar 4-43. Bridge Setup.....	71
Gambar 4-44. Bridge Configuration	71
Gambar 4-45. Interface Assignment	71
Gambar 4-46. Enable Bridge Interface	72
Gambar 4-47. Bridge Rule	72
Gambar 4-48. Rule Option.....	73
Gambar 4-49. Bridge Rule Setup.....	73
Gambar 4-50. Snort Package	74
Gambar 4-51. Snort Installation Confirmation	74
Gambar 4-52. Snort Installation Process.....	75
Gambar 4-53. Snort Installation Completed	75
Gambar 4-54. Snort Interface.....	76
Gambar 4-55. Snort Enable Interface.....	76
Gambar 4-56. Snort Block Option	77
Gambar 4-57. Snort Subscriber Rule	77
Gambar 4-58. Snort Rule Option	78
Gambar 4-59. Snort Update Rule.....	78
Gambar 4-60. Snort Update Success.....	79
Gambar 4-61. Snort Interface List	79
Gambar 4-62. Snort Rule Categories	80
Gambar 4-63. Snort Categories List.....	80
Gambar 4-64. Snort Activation.....	81
Gambar 4-65. Snort Activated	81
Gambar 4-66. Snort Alert List	82
Gambar 4-67. Snort Block List.....	83
Gambar 4-68. Kali IP Address	84
Gambar 4-69. Kali UDP Flooding	84
Gambar 4-70. Kali Wireshark UDP Monitoring.....	85
Gambar 4-71. Snort UDP Alert.....	85
Gambar 4-72. Snort UDP Block	85
Gambar 4-73. Kali SYN Flooding	86
Gambar 4-74. Kali Wireshark SYN Monitoring.....	86
Gambar 4-75. Snort SYN Alert.....	87
Gambar 4-76. Snort SYN Block	87
Gambar 4-77. Kali MAC Flooding	87
Gambar 4-78. Kali MAC Flooding Process.....	88
Gambar 4-79. Snort MAC Flooding Alert	88
Gambar 4-80. Kali ARP Poisoning.....	89
Gambar 4-81. Kali Wireshark ARP Monitoring.....	89
Gambar 4-82. Snort ARP Spoofing Alert	90

Gambar 4-83. Kali DNS Spoofing.....	90
Gambar 4-84. Snort DNS Spoofing Alert.....	91
Gambar 4-85. Kali DHCP Starvation	91
Gambar 4-86. Snort DHCP Starvation Alert	92
Gambar 4-87. DHCP Rogue	92
Gambar 4-88. Snort DHCP Rogue Alert	93
Gambar 4-89. Kali SSH Brute Force	93
Gambar 4-90. Snort SSH Brute Force Alert	93
Gambar 4-91. Snort SSH Brute Force Block.....	94
Gambar 4-92. Penilaian Pasca Installation NA.....	94
Gambar 4-93. Penilaian Pasca Installation SA	95
Gambar 4-94. Grafik Penilaian Pasca Installation	96

DAFTAR TABEL

Tabel 2-1. Status Pengamanan	25
Tabel 2-2. Kategori Pengamanan	25
Tabel 2-3. Perubahan Indeks KAMI	26
Tabel 3-1. Penelitian Terdahulu	33
Tabel 3-2. IP Address Management	41
Tabel 3-3. Rincian Kegiatan	46
Tabel 4-1. Hasil Penilaian Awal NA	48
Tabel 4-2. Hasil Penilaian Awal SA	49
Tabel 4-3. Hasil Penilaian Pasca Installation NA	95
Tabel 4-4. Hasil Penilaian Pasca Installation SA	96