

DAFTAR ISI

HALAMAN SAMPUL.....	i
HALAMAN JUDUL	ii
HALAMAN PERSETUJUAN	iii
HALAMAN PENGESAHAN	iv
HALAMAN MOTTO	v
HALAMAN PERSEMBAHAN	vi
INTISARI	vii
KATA PENGANTAR.....	viii
DAFTAR ISI.....	x
DAFTAR GAMBAR	xii
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah.....	2
1.3 Ruang Lingkup	2
1.4 Tujuan Penelitian	3
BAB II TINJAUAN PUSTAKA DAN DASAR TEORI.....	4
2.1 Tinjauan Pustaka	4
2.2 Dasar Teori	4
2.2.1 Penyebab vulnerability	4
2.2.2 Buffer overflow	6
2.2.2.1 Stack Overflow	6
2.2.2.2 Heap Corruption.....	7
2.2.3 SEH	8
2.2.4 SafeSEH.....	8
2.2.5 Fuzzer	9

BAB III ANALISIS DAN PERANCANGAN SISTEM.....	12
3.1 Analisis sistem	12
3.1.1 Sistem Perangkat Keras (Hardware)	12
3.1.2 Sistem Perangkat Lunak (Software)	13
3.1.3 kebutuhan perangkat lunak pengujian	14
3.2 Perancangan Sistem	15
3.2.1 Perancangan Fuzzer.....	15
3.2.2 Perancangan Proses penetrasi.....	16
3.2.3 Flowchat sistem	16
BAB IV IMPLEMENTASI DAN PEMBAHASAN SISTEM	21
4.1 Implementasi Sistem	21
4.2 Pembahasan Sistem.....	21
4.2.1 Social Engineering.....	21
4.2.2 Nmap	23
4.2.3 Fuzzing	24
4.2.4 Mencari alamat "Batu loncatan"	28
4.2.5 Mencari offset untuk Overwrite SEH.....	31
4.2.6 Mengontrol proses CPU	35
4.2.7 Membuat shellcode.....	38
4.2.8 Aplikasi Winamp.....	43
4.2.8.1 Menganalisa vulnerability	43
4.2.8.2 Fuzzing	44
4.2.8.3 Pattern create.....	49
4.2.8.4 Pattern offset.....	53
4.2.8.5 JMP ESP	55
4.2.8.6 Ujicoba JMP ESP.....	60
4.2.8.7 Payload.....	62
BAB V KESIMPULAN DAN SARAN	70
5.1 Kesimpulan.....	70

5.2 Saran.....	70
DAFTAR PUSTAKA	72

DAFTAR GAMBAR

	Halaman
Gambar 3.1 Flowchat sistem direct return	18
Gambar 3.2 Flowchart sistem SEH dan SafeSEH	20
Gambar 4.1 Nmap	24
Gambar 4.2 Fuzzer 1	24
Gambar 4.3 Menu file pada olldb.....	25
Gambar 4.4 Menu attach yang ada di ollydbg.....	25
Gambar 4.5 Windows register aplikasi bigant server	26
Gambar 4.6 Mengirimkan fuzzer.....	26
Gambar 4.7 Register bigant saat di fuzzing	27
Gambar 4.8 SEH chain pada bigant.....	27
Gambar 4.9 Nilai register EIP	28
Gambar 4.10 Modul yang di gunakan aplikasi Bigant.....	29
Gambar 4.11 Menu Sequence of commands.....	30
Gambar 4.12 Window pencarian	30
Gambar 4.13 Alamat POP, POP, RETN pada vbajet32.dll.....	31
Gambar 4.14 Membuat string pattern	31
Gambar 4.15 Fuzzer yang telah di tambah string pattern.....	32
Gambar 4.16 Nilai register pada bigant telah tertimpa	33
Gambar 4.17 Nilai register EIP	33
Gambar 4.18 Hasil perhitungan pattern offset	34
Gambar 4.19 Memasukkan pattern offset ke fuzzer.....	34
Gambar 4.20 Fuzzer yang telah disisipi register EIP	35
Gambar 4.21 Tabel Seh chain dalam file vbajet32.dll	35
Gambar 4.22 Proses melempar ke perintah POP, POP, RETN	36
Gambar 4.23 Proses di kirim ke dalam stack.....	36
Gambar 4.24 Proses pemindahan ke alamat lain	37
Gambar 4.25 Data di dalam memory	37
Gambar 4.26 Web server metasploit di jalankan.....	38
Gambar 4.27 Daftar payload	38

Gambar 4.28 Daftar payload untuk windows	39
Gambar 4.29 Konfigurasi shellcode	39
Gambar 4.30 Hasil generate payload.....	40
Gambar 4.31 Menyisipkan payload pada fuzzer	41
Gambar 4.32 Melakukan Telnet pada aplikasi bigant server.....	42
Gambar 4.33 Tampilan Winamp beserta versinya	43
Gambar 4.34 Tampilan version history	43
Gambar 4.35 Fuzzer winamp.....	44
Gambar 4.36 Berhasil membuat file.txt	44
Gambar 4.37 file .txt yang siap di selipkan pada winamp.....	45
Gambar 4.38 kirim file .txt dan riplace .txt yg ada	45
Gambar 4.39 Tampilan menu attach pada ollydbg	46
Gambar 4.40 Register memory winamp tertimpa	47
Gambar 4.41 Membuat pattren create sebesar 2000 byte	50
Gambar 4.42 fuzzer yang di sisipi pattern create	51
Gambar 4.43 Register memory tertimpa dengan string pattern	52
Gambar 4.44 Menghitung pattern offset	53
Gambar 4.45 Mengubah register EIP menjadi DEEDBEEF	54
Gambar 4.46 Nilai register memory dari winamp	55
Gambar 4.47 Menu serch for command pada ollydbg	57
Gambar 4.48 Windows executable modules pada ollydbg.....	57
Gambar 4.49 Menu serch for comand pada ollydbg	59
Gambar 4.50 Window input command	60
Gambar 4.51 Ollydbg menemukan perintah JMP ESP.....	60
Gambar 4.52 Fuzzer yang di ubah menjadi JMP ESP.....	61
Gambar 4.53 Ollydbg mengarah ke dalam buffer(stack)	62
Gambar 4.54 Webserver metasploit sedang dijalankan	64
Gambar 4.55 Daftar payload pada metasploit.....	64
Gambar 4.56 Daftar payload untuk OS windows	65
Gambar 4.57 window konfigurasi payload shell blind_v26067..	66
Gambar 4.58 Hasil payload	67
Gambar 4.59 Fuzzer yang telah di sisipi payload.....	68

Gambar 4.60 Melakukan telnet pada aplikasi winamp..... 69