

## DAFTAR ISI

HALAMAN JUDUL .....	i
PERNYATAAN .....	ii
HALAMAN PENGESAHAN .....	iii
KATA PENGANTAR .....	iv
HALAMAN PERSEMBAHAN .....	vi
DAFTAR ISI .....	vii
DAFTAR GAMBAR .....	ix
DAFTAR TABEL.....	xv
INTISARI.....	xvi
 <b>BAB I PENDAHULUAN.....</b>	 <b>1</b>
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	3
1.3 Batasan Masalah.....	3
1.4 Keaslian Penelitian.....	4
1.5 Tujuan Penelitian.....	5
1.6 Manfaat Penelitian .....	5
1.7 Metode Penelitian.....	5
1.8 Sistematika Penulisan .....	9
 <b>BAB II TINJAUAN PUSTAKA .....</b>	 <b>11</b>
 <b>BAB III LANDASAN TEORI.....</b>	 <b>19</b>
3.1 Metode Banner Grabbing .....	19
3.2 Elemen-elemen keamanan sistem informasi.....	22
3.3 Tahapan hacking .....	23
3.4 Vulnerability Development .....	25
3.4.1 Terminologi dan penjelasan umum register general purpose register dan register EIP .....	27
3.4.2 Fuzzer .....	30
3.4.3 Structure Exception Handling (SEH).....	33
3.4.4 SafeSEH .....	35
3.4.5 JMP ESP.....	37
3.4.6 ASLR atau Address Space Layout Randomization.....	38
3.4.7 Metasploit Framework tool.....	41
 <b>BAB IV ANALISIS DAN RANCANGAN PROGRAM.....</b>	 <b>42</b>
4.1 Tahapan Penetration Testing .....	42
4.2 Fasilitas Pendukung .....	43
4.3 Sumber data.....	43
4.4 Rancangan Penelitian .....	47
4.5 Penggunaan Fuzzer .....	53

4.6	Rancangan Maintaining Access .....	54
4.7	Rancangan Covering Tracks .....	55
4.8	Rancangan untuk pengamanan.....	55
4.9	Diagram Penelitian.....	47
<b>BAB V</b>	<b>IMPLEMENTASI .....</b>	<b>57</b>
5.1	Implementasi Program .....	57
5.2	Implementasi pengumpulan data celah keamanan .....	57
5.3	Implementasi pengumpulan data untuk solusi .....	107
5.4	Implementasi Program Identifikasi celah Keamanan .....	112
<b>BAB VI</b>	<b>HASIL PENGUJIAN DAN PEMBAHASAN .....</b>	<b>116</b>
6.1	Pengujian dalam mendeteksi celah keamanan komputer.....	116
6.2	Rancangan Pembahasan dan pengujian .....	117
6.3	Pengujian Scanning .....	119
6.4	Pengujian pada target komputer Windows.....	134
6.5	Pengujian Gaining Access pada target Windows .....	134
6.6	Pengujian Maintaining Access pada target Windows .....	137
6.7	Pengujian Covering Tracks pada target Windows .....	142
6.8	Pengujian pada komputer dengan OS Windows 7 .....	142
6.9	Pengujian pada komputer dengan OS Windows 8.1 .....	143
6.10	Pengujian pada komputer dengan OS Linux Debian 6 .....	144
6.11	Pengujian Gaining Access pada target Linux Debian 6 .....	144
6.12	Pengujian Maintaining Acces pada target Linux Debian 6.....	145
6.13	Pengujian Covering Tracks pada target Linux Debian 6 .....	147
6.14	Pengujian dengan Firewall .....	147
6.15	Pengujian pada komputer dengan OS Linux Ubuntu 13.10.....	149
6.16	Pengujian Gaining Access pada target linux Ubuntu 13.10 .....	149
6.17	Pengujian Maintaining Access pada target Linux Ubuntu 13.10	151
6.18	Pengujian Covering Tracks pada target Linux Ubuntu 13.10.....	153
6.19	Pengujian untuk linux Ubuntu 15.04 .....	153
6.20	Pengamanan dan pengujian.....	154
6.21	Pembahasan hasil .....	167
<b>BAB VII</b>	<b>PENUTUP.....</b>	<b>171</b>
7.1	Kesimpulan.....	171
7.2	Saran .....	171
<b>DAFTAR PUSTAKA.....</b>		<b>173</b>

## DAFTAR GAMBAR

Gambar 3.1	Hasil banner grabbing pada port 80 .....	21
Gambar 3.2	Susunan register memory dalam stack (Perdhana, M, R, 2011) ...	27
Gambar 3.3	Tampilan dikirimkannya 200 bytes ke command USER pada FTP . Server FreeFloat .....	31
Gambar 3.4	Tampilan pesan error setelah dikirimkannya paket 2000 bytes ke co command USER pada program FTP Server Freefloat .....	32
Gambar 3.5	Tampilan register EIP pada program FTP Server Freefloat tertimpa paket fuzzer dan aplikasi mengalami crash.....	32
Gambar 3.6	Tampilan paket tidak menimpa EIP dari All Media Service di Windows XP SP3 .....	34
Gambar 3.7	Tampilan menu SEH chain pada Immunity Debugger .....	34
Gambar 3.8	Tampilan SEH chain yang menunjukkan bahwa paket dari Fuzzer . dilempar ke fungsi SEH .....	35
Gambar 3.9	Tampilan module yang memilih proteksi SafeSEH dan module yang tidak memiliki proteksi SafeSEH .....	36
Gambar 3.10	Tampilan penggunaan metode POP POP RETN pada Immunity DebuDebugger untuk mencari letak alamat yang dapat dimasukkan shellcode.....	36
Gambar 3.11	Tampilan dari hasil metode POP, POP, RETN pada program All..... Media Server .....	37
Gambar 3.12	Tampilan mencari alamat register ESP dengan perintah JMP ESP pada program FTP Server Freefloat .....	38
Gambar 3.13	Tampilan hhasil dari perintah JMP ESP untuk mencari alamat register ESP pada FTP Server Freefloat .....	38
Gambar 3.14	Tampilan banyaknya module yang diproteksi oleh ASLR pada program FTP Server Freefloat.....	39
Gambar 3.15	Tampilan banyak module yang terproteksi ASLR pada program All Media Server .....	40
Gambar 3.16	Tampilan tabel module dari program All Media Server yang tidak memiliki proteksi ASLR .....	40
Gambar 4.1	Flowchart penelitian untuk mencari data .....	44
Gambar 4.2	Flowchart penelitian Vulnerability Development pada FTP Server .....	45
ambar 4.3	Skema dalam membuat program identifikasi.....	46
Gambar 4.4	Flowchart program Identifikasi celah keamanan dengan metode banner grabbing.....	49
Gambar 4.5	Flowchart penelitian saat pengujian Program identifikasi celah keamanan remote pada komputer OS Windows .....	52
Gambar 4.6	Diagram penelitian .....	56
Gambar 5.1	Topologi jaringan komputer training ruangfokus media dan tambahan komputer baru untuk mendukung penelitian.....	59
Gambar 5.2	Tampilan login TP-LINK ADSL 2+ Modem Router TD-8840T ..	60
Gambar 5.3	Tampilan halaman admin TP-LINK ADSL2+ Modem Router TD-	

	8840T .....	60
Gambar 5.4	Tampilan contoh brute force pada login TP-LINK ADSL2+ Modem Router TD8840T .....	61
Gambar 5.5	Konfigurasi LAN Settings pada TP-LINK ADSL2+ Modem Router TD-8840T.....	61
Gambar 5.6	Tampilan fitur DMZ pada TP-LINK ADSL2+ Modem Router TD-8840T .....	62
Gambar 5.7	Hasil ping ip publik untuk mengetahui keberadaan salah satu komputer di jaringan private .....	62
Gambar 5.8	Hasil ping ip publik untuk mengetahui service pada salah satu komputer di jaringan private .....	63
Gambar 5.9	Hasil ping ip publik berupa <i>request timed out</i> .....	63
Gambar 5.10	Tampilan informasi celah keamanan di cvedetails.com.....	66
Gambar 5.11	Tampilan program Filezilla FTP Server akan dilakukan fuzzing .	66
Gambar 5.12	Tampilan program Filezilla setelah dilakukan fuzzing .....	67
Gambar 5.13	Tampilan informasi celah keamanan pada FreeSSHD dari cvedetails.com.....	68
Gambar 5.14	Tampilan exploit freeSSHD .....	68
Gambar 5.15	Tampilan exploit freeSSHD dijalankan .....	69
Gambar 5.16	Tampilan saat akan masuk ke server melalui telnet .....	70
Gambar 5.17	Tampilan masuk ke dalam komputer target .....	70
Gambar 5.18	Tampilan informasi celah keamanan pada program PCman's dari cvedetails.com.....	70
Gambar 5.19	Tampilan exploit PCman's (Buffer Overflow - MKD Command) yang dibuat oleh R-73eN saat di uji.....	71
Gambar 5.20	Tampilan exploit Pcmn's - STOR Command - Buffer Overflow Exploit saat diuji .....	72
Gambar 5.21	Tampilan exploit PCman's, PASS Command – Buffer OverflowExploit saat diganti ip address untuk uji coba .....	72
Gambar 5.22	Tampilan Exploit Pcmn's, PASS Command - Buffer Overflow Exploit saat diuji .....	73
Gambar 5.23	Tampilan saat FTP Client mengirimkan paket.....	74
Gambar 5.24	Tampilan Wireshark .....	74
Gambar 5.25	Tampilan program PCManFTPD2 .exe akan dibuka melalui Immunity Debugger .....	75
Gambar 5.26	Tampilan saat program PCManFTPD2 .exe dibuka melalui Immunity Debugger .....	77
Gambar 5.27	Tampilan setelah program fuzzingdi jalankan dengan mengirimkan "\x41" sebanyak 1000 .....	77
Gambar 5.28	Tampilan EIP tidak tertimpa paket "\x41" .....	77
Gambar 5.29	Tampilan program fuzzing dengan pengiriman paket "\x41" sebanyak 2500.....	78
Gambar 5.30	Immunity Debugger menampilkan paket "\x41" menimpa EIP ...	78
Gambar 5.31	Tampilan saat program pattern_create.rb membuat data dummies yang terstruktur .....	79
Gambar 5.32	Tampilan EIP memberikan nilai setelah dikirim data dummies yang	

	terstruktur .....	81
Gambar 5.33	Tampilan pattern_offset.rb di jalankan untuk mengetahui jumlah data yang diperlukan untuk mencapai EIP .....	81
Gambar 5.34	Tampilan informasi module yang tidak memiliki proteksi ASLR pada program FTP Server Pcmans pada Windows XP SP3 .....	82
Gambar 5.35	Tampilan informasi module yang tidak memiliki proteksi SafeSEH pada program FTP Server Pcmans di Windows XP SP3 .....	83
Gambar 5.36	Tampilan informasi module yang tidak memiliki proteksi SafeSEH pada Windows XP tanpa service pack.....	84
Gambar 5.37	Tampilan Executable Modules pada program PCMan's .....	85
Gambar 5.38	Tampilan menu untuk masuk di command agar dapat memasukkan JMP ESP.....	85
Gambar 5.39	Immunity Debugger menampilkan nilai dari JMP ESP .....	86
Gambar 5.40	Pengujian sebelum eksploitasi pada PCMan's FTP Server .....	86
Gambar 5.41	Tampilan setelah exploit PCMan's dijalankan .....	87
Gambar 5.42	Tampilan saat dijalankan NMAP untuk scanning port dan service pada target setelah exploit PCMan's dijalankan .....	88
Gambar 5.43	Tampilan akses telnet ke dalam komputer clone.....	87
Gambar 5.44	Tampilan hasil NMAP untuk mendeteksi keberadaan FTP Server PCman's pada Windows 7.....	88
Gambar 5.45	FTP Server mengalami crash dan pada pointer EIP nilainya 41414141.....	89
Gambar 5.46	Tampilan nilai EIP setelah dilakukan fuzzing dengan data dummies yang terstruktur.....	89
Gambar 5.47	Tampilan hasil dari program pattern offset. ....	90
Gambar 5.48	Tampilan informasi module yang tidak memiliki proteksi SafeSEH pada Windows 7. ....	90
Gambar 5.49	Tampilan informasi module yang tidak memiliki proteksi ASLR pada Windows 7. ....	91
Gambar 5.50	Tampilan nilai hasil dari perintah JMP ESP pada program FTP Server PCman's di Windows 7.....	92
Gambar 5.51	Tampilan setelah masuk ke dalam komputer target dengan menguji perintah ver.....	92
Gambar 5.52	Tampilan informasi module yang tidak memiliki proteksi ASLR pada FTP Server PCman's di Windows Vista. ....	93
Gambar 5.53	Tampilan informasi module yang tidak memiliki proteksi SafeSEH pada FTP Server PCman's di Windows Vista. ....	93
Gambar 5.54	Tampilan informasi module yang tidak memiliki proteksi SafeSEH pada FTP Server PCman's di Windows Vista. ....	94
Gambar 5.55	Tampilan informasi module yang tidak memiliki proteksi ASLR pada FTP Server PCman's di Windows Server 2008.....	94
Gambar 5.56	Hasil scanning dengan NMAP pada komputer OS Windows 8.1..	95
Gambar 5.57	Tampilan kiriman paket dari Fuzzer menimpa register EIP pada program PCman's yang berjalan di Windows 8.1.....	96
Gambar 5.58	Tampilan hasil dari JMP ESP pada program PCman's yang berjalan di Windows 8.1.....	97

Gambar 5.59	Hasil scanning port dan service pada target Linux Debian 6.....	98
Gambar 5.60	Informasi dari CVEdetails.com untuk keamanan ProFTPD 1.3.3	98
Gambar 5.61	Hasil pencarian celah ProFTPD 1.3.3a berupa exploit dengan bahasa ruby.....	99
Gambar 5.62	Tampilan menu exploit Prftpd_telnet_iac di Metasploit Framework .....	99
Gambar 5.63	Hasil dari eksploitasi celah telnet_IAC pada ProFTPD 1.3.3a pada port 21 .....	100
Gambar 5.64	Hasil scanning pada komputer Ubuntu 13.10 dengan NMAP ....	101
Gambar 5.65	Tampilan informasi celah keamanan dari CVE Details untuk program ProFTPD 1.3.5rc3.....	101
Gambar 5.66	Tampilan hasil pencarian exploit untuk ProFTPD 1.3.5 .....	102
Gambar 5.67	Tampilan exploit untuk ProFTPD 1.3.5 .....	102
Gambar 5.68	Tampilan file exploit telah diletakkan pada folder tempat metasploit akan menjalankannya .....	103
Gambar 5.69	Tampilan dari hasil perintah search ProFTPD yang menunjukkan keberadaan exploit untuk ProFTPD 1.3.5 .....	103
Gambar 5.70	Tampilan menggunakan exploit ProFTPD 1.3.5 .....	104
Gambar 5.71	Tampilan hasil eksploitasi pertama pada ProFTPD 1.3.5 .....	105
Gambar 5.72	Tampilan hasil eksploitasi kedua pada ProFTPD 1.3.5.....	105
Gambar 5.73	Tampilan hasil eksploitasi ketiga pada ProFTPD 1.3.5 .....	106
Gambar 5.74	Hasil scanning port dan service pada target Ubuntu 15.04.....	106
Gambar 5.75	Hasil pencarian informasi celah keamanan VSFTPD 3.0.2 di cvedetails.com.....	107
Gambar 6.1	Hasil Scan menggunakan program identifikasi celah keamanan dengan metode banner grabbing pada komputer dengan ip address 192.168.1.127.....	119
Gambar 6.2	Hasil Scan menggunakan program identifikasi celah keamanan dengan metode banner grabbing pada komputer dengan ip address 192.168.1.128.....	122
Gambar 6.3	Hasil Scan menggunakan program identifikasi celah keamanan dengan metode banner grabbing pada komputer dengan ip address 192.168.1.58.....	124
Gambar 6.4	Hasil Scan menggunakan program identifikasi celah keamanan dengan metode banner grabbing pada komputer dengan ip address 192.168.1.65.....	125
Gambar 6.5	Hasil Scan menggunakan program identifikasi celah keamanan dengan metode banner grabbing pada komputer dengan ip address 192.168.1.83.....	126
Gambar 6.6	Hasil Scan menggunakan program identifikasi celah keamanan dengan metode banner grabbing pada komputer dengan ip address 192.168.1.61.....	127
Gambar 6.7	Hasil Scan menggunakan program identifikasi celah keamanan dengan metode banner grabbing pada komputer dengan ip address 192.168.1.109.....	129
Gambar 6.8	Tampilan untuk pengujian bahwa tidak ada port 7777 yang aktif	

	pada komputer target.....	135
Gambar 6.9	Tampilan exploit FreeSSHD 1.0.9 yang dijalankan untuk target komputer dengan ip address 192.168.1.127.....	135
Gambar 6.10	Tampilan hasil eksploitasi FreeSSHD dalam bentuk telnet yang diujikan sekaligus untuk menambah user dan menjadikannya administrator .....	136
Gambar 6.11	Tampilan hasil eksploitasi FTP Server PCman's yang diuji hak akses pada target untuk membuat user dan menjadikan user tersebut sebagai administrator.....	137
Gambar 6.12	Sharing folder dengan nama datadata pada komputer penetration tester .....	138
Gambar 6.13	Tampilan komputer target menghubungkan diri dengan komputer penetration tester agar komputer dengan perintah <i>net use</i> .....	139
Gambar 6.14	Tampilan tasklist pada komputer target .....	140
Gambar 6.15	Tampilan file backdoor telnet di copy ke dalam komputer target	140
Gambar 6.16	Tampilan program telnet backdoor dijalankan.....	141
Gambar 6.17	Tampilan aplikasi FTP Server PCman's 2.0 mengalami <i>crash</i> saat exploit dijalankan di Windows 7 .....	142
Gambar 6.18	Tampilan aplikasi FTP Server PCman's 2.0 yang dijalankan di Windows 8.1 mengalami <i>crash</i> saat proses fuzzing mengirimkan data 3500 bytes pada command USER .....	143
Gambar 6.19	Tampilan berhasil masuk ke dalam target dengan payload linux/x86/shell/bind_tcp.....	144
Gambar 6.20	Tampilan hak akses yang dimiliki penyerang adalah akses root.	145
Gambar 6.21	Tampilan berhasil membuat user di Linux Debian 6 .....	145
Gambar 6.22	Tampilan dapat membuat user baru di target Linux Debian 6 ....	146
Gambar 6.23	Hasil masuk ke dalam komputer linux Debian 6 melalui backdoor 8000.....	146
Gambar 6.24	Tampilan tidak berhasil masuk dengan payload linux/x86/shell/bind_tcp dengan kondisi firewall linux menyala	147
Gambar 6.25	Tampilan berhasil masuk dengan payload linux/x86/shell/revere_tcp dengan kondisi firewall linux menyala .....	148
Gambar 6.26	Hasil tampilan eksploitasi menggunakan payload cmd/unix/bind_perl pada target dengan firewall tidak aktif .....	150
Gambar 6.27	Hasil tampilan eksploitasi menggunakan payload cmd/unix/reverse_perl pada target dengan firewall aktif.....	150
Gambar 6.28	Tampilan hasil melakukan download file r57.txt untuk backdoor pada komputer OS linux Ubuntu 13.10.....	151
Gambar 6.29	Tampilan halaman web Backdoor R57 PHP Shell .....	152
Gambar 6.30	Tahap back-connect untuk mendapatkan akses shell lebih luas pada komputer linux Ubuntu 13.10 .....	153
Gambar 6.31	Tampilan tambahan banner Testing 123 setelah melakukan login SSH .....	154
Gambar 6.32	Pengujian penggantian default banner pada FTP Server PCman's .....	155

Gambar 6.33	Tampilan penggantian <i>default banner</i> dan mengujinya dengan FTP Client melakukan koneksi ke FTP Server .....	158
Gambar 6.34	Tampilan dan hasil penggantian default banner pada Filezilla Server .....	158
Gambar 6.35	Hasil tampilan scanning dengan program identifikasi celah keamanan dengan menggunakan metode banner grabbing saat FTP Server yang diuji dilakukan penggantian pada <i>default banner</i> .....	160
Gambar 6.36	Contoh tampilan hasil <i>brute force</i> pada FTP Server .....	162
Gambar 6.37	Tampilan saat mempunyai akses di <i>/etc/</i> untuk melihat keberadaan aplikasi ProFTPD .....	162
Gambar 6.38	Tampilan saat mempunyai akses di <i>/var/log/proftpd</i> untuk melihat keberadaan aplikasi ProFTPD.....	163
Gambar 6.39	Gambar 6.39, Tampilan saat FTP Client melakukan koneksi ke FTP Server yang masih menampilkan banner nama aplikasi dan versinya .....	163
Gambar 6.40	Tampilan saat FTP Client melakukan koneksi ke FTP Server yang sudah mengganti banner nama aplikasi dan versinya dengan nama FTP Server.....	164
Gambar 6.41	Tampilan sebelum diubah pada <i>default banner</i> dan sesudah diganti pada vsFTPD 3.0.2 .....	164
Gambar 6.42	Tampilan program identifikasi celah keamanan dengan menggunakan metode banner grabbing tidak mampu mendeteksi vsFTPD yang telah diganti pada <i>default banner</i> .....	165

## DAFTAR TABEL

Tabel 2.1	Perbandingan Tinjauan Pustaka .....	14
Tabel 3.1	Konsep-konsep Hacking For Penetration Testing .....	20
Tabel 3.2	Tabel General Purpose Register pada IA-32 Intel Architecture (Perdhana, M, R, 2011) .....	28
Tabel 5.1	Hasil dari implementasi pengujian pada komputer-komputer target	109
Tabel 6.1	Tabel laporan informasi celah keamanan dan solusi pada komputer Windows XP dengan ip address 192.168.1.128 .....	131
Tabel 6.2	Tabel laporan informasi celah keamanan dan solusi pada komputer Windows XP dengan ip address 192.168.1.127 .....	131
Tabel 6.3	Tabel laporan informasi celah keamanan dan solusi pada komputer Windows 7 dengan ip address 192.168.1.58 .....	132
Tabel 6.4	Tabel laporan informasi celah keamanan dan solusi pada komputer Windows 8.1 dengan ip address 192.168.1.65 .....	132
Tabel 6.5	Tabel laporan informasi celah keamanan dan solusi pada komputer Linux OS Debian 6 dengan ip address 192.168.1.83 .....	133
Tabel 6.6	Tabel laporan informasi celah keamanan dan solusi pada komputer OS Linux Ubuntu 13.10 dengan ip address 192.168.1.61 .....	133
Tabel 6.7	Tabel laporan informasi celah keamanan dan solusi pada komputer OS Linux Ubuntu 15.04 dengan ip address 192.168.1.109 .....	133

## DAFTAR TABEL

Tabel 2.1	Perbandingan Tinjauan Pustaka .....	14
Tabel 3.1	Konsep-konsep Hacking For Penetration Testing .....	20
Tabel 3.2	Tabel General Purpose Register pada IA-32 Intel Architecture .....	28
Tabel 5.1	Hasil dari implementasi pengujian pada komputer-komputer target	109
Tabel 6.1	Tabel laporan informasi celah keamanan dan solusi pada komputer Windows XP dengan ip address 192.168.1.128 .....	131
Tabel 6.2	Tabel laporan informasi celah keamanan dan solusi pada komputer Windows XP dengan ip address 192.168.1.127 .....	131
Tabel 6.3	Tabel laporan informasi celah keamanan dan solusi pada komputer Windows 7 dengan ip address 192.168.1.58 .....	132
Tabel 6.4	Tabel laporan informasi celah keamanan dan solusi pada komputer Windows 8.1 dengan ip address 192.168.1.65 .....	132
Tabel 6.5	Tabel laporan informasi celah keamanan dan solusi pada komputer Linux OS Debian 6 dengan ip address 192.168.1.83 .....	133
Tabel 6.6	Tabel laporan informasi celah keamanan dan solusi pada komputer OS Linux Ubuntu 13.10 dengan ip address 192.168.1.61 .....	133
Tabel 6.7	Tabel laporan informasi celah keamanan dan solusi pada komputer OS Linux Ubuntu 15.04 dengan ip address 192.168.1.109 .....	133