

DAFTAR ISI

HALAMAN SAMBUTAN	i
HALAMAN JUDUL.....	ii
HALAMAN PERSETUJUAN.....	iii
HALAMAN PENGESAHAN.....	iv
HALAMAN PERNYATAAN KEASLIAN	v
HALAMAN PERSEMBAHAN	vi
HALAMAN MOTTO	vii
KATA PENGANTAR	viii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xi
DAFTAR GAMBAR	xii
DAFTAR LAMPIRAN.....	xiii
INTISARI.....	xiv
<i>ABSTRACT</i>	xv
BAB I PENDAHULUAN.....	1
A. Latar Belakang Masalah	1
B. Rumusan Masalah.....	6
C. Batasan Masalah	6
D. Tujuan Penelitian	7
E. Manfaat Penelitian	8
BAB II TINJAUAN PUSTAKA.....	9
A. Landasan Teori.....	9
B. Penelitian Sebelumnya.....	29
BAB III METODE PENELITIAN.....	34
A. Tempat dan Waktu Penelitian.....	34
B. Metode Pengumpulan Data.....	34
C. Alat dan Bahan Penelitian.....	38
D. Desain Penelitian	40
E. <i>Operasional Variabel</i>	45

BAB IV HASIL DAN PEMBAHASAN	47
A. <i>Planning and Preparation</i>	47
B. <i>Reconnasissance</i>	49
C. <i>Discovery</i>	51
D. <i>Report</i>	61
BAB V PENUTUP.....	64
A. Kesimpulan	64
B. Saran	64
DAFTAR PUSTAKA	
LAMPIRAN	



DAFTAR TABEL

Tabel 2. 1 Perbandingan Penelitian Sebelumnya.....	33
Tabel 3. 1 Data Protokol Keamanan WPA2	37
Tabel 3. 2 Jenis Serangan <i>Brute Force Attack</i>	46



DAFTAR GAMBAR

Gambar 3. 1 Desain Penelitian.....	41
Gambar 4. 1 Topologi jaringan	50
Gambar 4. 2 <i>Install Ipcalc</i>	53
Gambar 4. 3 Hasil <i>Ifconfig</i>	53
Gambar 4. 4 Hasil <i>Ipcalc</i>	54
Gambar 4. 5 Status SSH <i>Active</i>	55
Gambar 4. 6 Hasil <i>Netdiscover</i>	55
Gambar 4. 7 Mencari Port SSH Terbuka	56
Gambar 4. 8 <i>Wordlist rockyou.txt</i>	57
Gambar 4. 9 File <i>Wordlist Userlist dan Passlist</i>	58
Gambar 4. 10 Proses <i>Brute Force Attack</i>	59
Gambar 4. 11 <i>Login</i> ke SSH IP 192.168.1.13	60
Gambar 4. 12 Berhasil Masuk ke SSH Perangkat Lain	60
Gambar 4. 13 Mengakses Direktori <i>File</i>	60
Gambar 4. 14 Mencari <i>File</i> Yang Akan Ditransfer.....	61
Gambar 4. 15 Transfer Data Berhasil	61
Gambar 4. 16 Data Berhasil Ditransfer.....	62

DAFTAR LAMPIRAN

Lampiran 1. Kartu Bimbingan

Lampiran 2. Dokumentasi dengan *owner* perusahaan

