

SKRIPSI

**ANALISIS KEAMANAN JARINGAN TERHADAP SERANGAN
BRUTE FORCE DOS DAN SQL ATTACK MENGGUNAKAN
HONEYPOT KIPPO DAN HONEYPOT DIONAEA**

*NETWORK SECURITY ANALYSIS AGAINST BRUTE FORCE
DOS AND SQL ATTACKS USING HONEYPOT KIPPO AND
HONEYPOT DIONAEA*



Disusun oleh

**REDI IRHAMNI
18101171**

**PROGRAM STUDI S1 TEKNIK TELEKOMUNIKASI
FAKULTAS TEKNIK TELEKOMUNIKASI DAN ELEKTRO
INSTITUT TEKNOLOGI TELKOM PURWOKERTO**

2023

SKRIPSI

**ANALISIS KEAMANAN JARINGAN TERHADAP SERANGAN
BRUTE FORCE DOS DAN SQL ATTACK MENGGUNAKAN
HONEYPOT KIPPO DAN HONEYPOT DIONAEA**

*NETWORK SECURITY ANALYSIS AGAINST BRUTE FORCE
DOS AND SQL ATTACKS USING HONEYPOT KIPPO AND
HONEYPOT DIONAEA*



Disusun oleh

**REDI IRHAMNI
18101171**

**PROGRAM STUDI S1 TEKNIK TELEKOMUNIKASI
FAKULTAS TEKNIK TELEKOMUNIKASI DAN ELEKTRO
INSTITUT TEKNOLOGI TELKOM PURWOKERTO**

2023

**ANALISIS KEAMANAN JARINGAN TERHADAP SERANGAN
BRUTE FORCE DOS DAN SQL ATTACK MENGGUNAKAN
HONEYPOT KIPPO DAN HONEYPOT DIONAEA**

***NETWORK SECURITY ANALYSIS AGAINST BRUTE FORCE
DOS AND SQL ATTACKS USING HONEYPOT KIPPO AND
HONEYPOT DIONAEA***

**Skripsi ini digunakan sebagai salah satu syarat untuk memperoleh
Gelar Sarjana Teknik (S.T.)
Di Institut Teknologi Telkom Purwokerto
2023**

Disusun oleh

**REDI IRHAMNI
18101171**

DOSEN PEMBIMBING

**Jafaruddin Gusti Amri Ginting, S.T, M.T.
Eka Wahyudi, S.T., M.Eng.**

**PROGRAM STUDI S1 TEKNIK TELEKOMUNIKASI
FAKULTAS TEKNIK TELEKOMUNIKASI DAN ELEKTRO
INSTITUT TEKNOLOGI TELKOM PURWOKERTO**

2023

HALAMAN PENGESAHAN


ANALISIS KEAMANAN JARINGAN TERHADAP SERANGAN BRUTE FORCE DOS DAN SQL ATTACK MENGGUNAKAN HONEYPOT KIPPO DAN HONEYPOT DIONAEA


NETWORK SECURITY ANALYSIS AGAINST BRUTE FORCE DOS AND SQL ATTACKS USING HONEYPOT KIPPO AND HONEYPOT DIONAEA

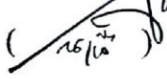
Disusun oleh
REDI IRHAMNI
18101171


Telah dipertanggung jawabkan di hadapan Tim Penguji pada tanggal 17 Oktober
2023

Susunan Tim Penguji

Pembimbing Utama : Jafaruddin Gusti Amri Ginting, S.T., M.T. ()
NIDN. 0620108901

Pembimbing Pendamping : Eka Wahyudi, S.T., M.Eng. : ()
NIDN. 0617117601

Penguji 1 : Bongga Arifwidodo, S.ST., M.T. ()
NIDN. 0603118901

Penguji 2 : Fauza Khair, S.T., M.Eng () 28/10/23
NIDN. 0622039001

Mengetahui,

Ketua Program Studi SI Teknik Telekomunikasi
Institut Teknologi Telkom Purwokerto


Prasetyo Kusumantoro, S.T., M.T
NIDN. 020079201

HALAMAN PERNYATAAN ORISINALITAS

Dengan ini saya, **REDI IRHAMNI**, menyatakan bahwa skripsi dengan judul “**ANALISIS KEAMANAN JARINGAN TERHADAP SERANGAN BRUTE FORCE DOS DAN SQL ATTACK MENGGUNAKAN HONEYPOT KIPPO DAN HONEYPOT DIONAEA**” adalah benar-benar karya saya sendiri. Saya tidak melakukan penjiplakan kecuali melalui pengutipan sesuai dengan etika keilmuan yang berlaku. Saya bersedia menanggung risiko ataupun sanksi yang dijatuhkan kepada saya apabila ditemukan pelanggaran terhadap etika keilmuan dalam skripsi saya ini.

Purwokerto, 17 Oktober 2023

Yang menyatakan,



(Redi Irhamni)

PRAKATA

Puji dan syukur penulis panjatkan kehadiran Allah SWT yang telah melimpahkan kasih dan sayang-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul **“ANALISIS KEAMANAN JARINGAN TERHADAP SERANGAN BRUTE FORCE DOS DAN SQL ATTACK MENGGUNAKAN HONEYPOT KIPPO DAN HONEYPOT DIONAEA”**.

Maksud dari penyusunan skripsi ini adalah untuk memenuhi salah satu syarat dalam menempuh ujian sarjana Teknik Telekomunikasi pada Fakultas Teknik Telekomunikasi dan Elektro Institut Teknologi Telkom Purwokerto.

Dalam penyusunan skripsi ini, banyak pihak yang sangat membantu penulis dalam berbagai hal. Oleh karena itu, penulis sampaikan rasa terima kasih yang sedalam-dalamnya kepada:

1. Orang tua yang memberikan dukungan serta doa dalam mengerjakan tugas akhir.
2. Bapak Jafaruddin Gusti Amri Ginting, S.T, M.T selaku pembimbing Utama.
3. Bapak Eka Wahyudi, S.T., M.Eng. selaku pembimbing Pendamping.
4. Bapak Prasetyo Yuliantoro., S.T., M.T. ketua Program Studi S1 Teknik Telekomunikasi.
5. Ibu Dr. Anggun Fitriani Isnawati, S.T., M.Eng. selaku Dekan Fakultas Teknik Telekomunikasi dan Elektro Institut Teknologi Telkom Purwokerto.
6. Ibu Dr. Tenia Wahyuningrum, S.Kom., M.T Selaku Rektor Institut Teknologi Telkom Purwokerto.
7. Seluruh dosen, staff, dan karyawan Program Studi S1 Teknik Elektro Institut Teknologi Telkom Purwokerto.
8. Kepada Yayah Ebierti, Muhammad Rifai, Risma, Caca, Maghfiroh, Usi, serta teman-teman dan sahabat yang tidak bisa disebutkan satu persatu.

Purwokerto, 17 Oktober 2023

(Redi Irhamni)

DAFTAR ISI

HALAMAN JUDUL	I
HALAMAN PENGESAHAN.....	II
HALAMAN PERNYATAAN ORISINALITAS	II
PRAKATA	II
ABSTRAK	III
ABSTRACT	IV
DAFTAR ISI.....	V
DAFTAR GAMBAR.....	VIII
DAFTAR TABEL	X
BAB 1	1
PENDAHULUAN.....	1
1.1 LATAR BELAKANG	1
1.2 RUMUSAN MASALAH.....	2
1.3 BATASAN MASALAH.....	2
1.4 TUJUAN PENELITIAN.....	3
1.5 MANFAAT PENELITIAN.....	3
1.6 SISTEMATIKA PENULISAN.....	3
BAB 2	4
KAJIAN PUSTAKA & DASAR TEORI.....	4
2.1 KAJIAN PUSTAKA.....	4
2.2 DASAR TEORI	5
2.2.1 SERVER	5
2.2.2 DANIEL OF SERVICE (DOS).....	5
2.2.3 BRUTE FORCE	7
2.2.4 SECURE SHELL (SSH)	8
2.2.5 HONEYPOT.....	8
2.2.6 VIRTUALBOX.....	9
2.2.7 LINUX.....	10
2.2.8 NETWORK MAPPER (NMAP)	10
2.2.9 LOW ORBIT ION CANNON (LOIC)	11

2.2.10 STRUCTURED QUERY LANGUAGE (SQL).....	12
2.2.11 PUTTY.....	12
2.2.12 PORT (JARINGAN KOMPUTER).....	13
BAB 3	14
METODE PENELITIAN	14
3.1 ALAT DAN PARAMETER YANG DITELITI.....	14
3.1.1 PERANGKAT KERAS	14
3.1.2 PERANGKAT <i>SERVER</i>	14
3.1.3 TOPOLOGI JARINGAN	15
3.2 DIAGRAM ALUR PENELITIAN.....	16
3.3 METODE PENELITIAN	19
3.4 KONFIGURASI SISTEM	19
3.4.1 KONFIGURASI <i>APACHE2</i>	19
3.4.2 KONFIGURASI <i>HONEYPOT</i> KIPPO GRAPH	23
3.4.3 KONFIGURASI <i>HONEYPOT</i> DIONAEA	26
3.5 PERANCANGAN SKENARIO	27
3.5.1 SKENARIO PENGUJIAN	27
3.5.1.1 SKENARIO PERTAMA	27
3.5.1.2 SKENARIO KEDUA	28
3.5.2 SKENARIO PENYERANGAN	30
3.5.2.1 SKENARIO PERTAMA	31
3.5.2.2 SKENARIO KEDUA	33
3.5.2.3 SKENARIO KETIGA	34
BAB IV	38
ANALISIS DAN PEMBAHASAN.....	38
4.1 HASIL PENGUJIAN <i>BRUTE FORCE</i>	39
4.1.1 SKENARIO PERTAMA MENYERANG <i>SERVER HONEYPOT</i>	39
4.1.2 SKENARIO KEDUA MENYERANG <i>SERVER</i> ASLI	44
4.2 HASIL PENGUJIAN <i>DANIEL OF SERVICE</i> (DOS).....	46
4.2.1 SKENARIO PERTAMA SERANGAN DOS PADA <i>SERVER</i> TIRUAN	46
4.2.2 SKENARIO KEDUA SERANGAN DOS PADA <i>SERVER</i> ASLI	47
4.3 HASIL PENGUJIAN SQL	50

4.3.1 SKENARIO PERTAMA SERANGAN SQL PADA <i>SERVER</i> TIRUAN.	50
4.3.2 SKENARIO KEDUA SERANGAN SQL PADA <i>SERVER</i> ASLI.....	52
4.4 PARAMETER KEAMANAN	54
BAB V.....	56
KESIMPULAN DAN SARAN	56
5.1 KESIMPULAN	56
5.2 SARAN.....	56
DAFTAR PUSTAKA	57

DAFTAR GAMBAR

Gambar 2. 1 LOIC	11
Gambar 2. 2 PuTTY	Er
ror! Bookmark not defined.	
Gambar 3. 1 Topologi Jaringan.....	15
Gambar 3. 2 Alur Penelitian	17
Gambar 3. 3 Tampilan Running <i>Apache2</i>	20
Gambar 3. 4 Tampilan <i>hostname server</i>	20
Gambar 3. 5 Tampilan <i>Hostname Server Asli</i>	21
Gambar 3. 6 Konfigurasi DVWA	22
Gambar 3. 7 Konfigurasi <i>php.ini</i>	23
Gambar 3. 8 Tampilan Edit File Config Kippo.....	24
Gambar 3. 9 <i>Username Dan Password</i>	24
Gambar 3. 10 Tampilan Kippo Secara Interactive.....	25
Gambar 3. 11 Tampilan Putty	26
Gambar 3. 12 Tampilan Dionaea.....	27
Gambar 3. 13 Skenario Pertama (Tanpa Blok IP)	28
Gambar 3. 14 Skenario Kedua (penyerang menyerang <i>server asli</i>)	29
Gambar 3. 15 Tampilan Nmap	30
Gambar 3. 16 Serangan <i>Brute Force</i>	31
Gambar 3. 17 <i>Username.txt</i>	32
Gambar 3. 18 <i>Password.txt</i>	32
Gambar 3. 19 Serangan Medusa	33
Gambar 3. 20 Serangan DoS	34
Gambar 3. 21 LOIC	34
Gambar 3. 22 Serangan SQLMap	35
Gambar 3. 23 Perintah Serangan <i>Sqlmap database</i>	35
Gambar 3. 24 Perintah Membuka Database <i>dvwa</i>	36
Gambar 3. 25 Perintah Membuka Database <i>dvwa Table Users</i>	36
Gambar 3. 26 Perintah Membuka Database <i>dvwa user dan password</i>	36
Gambar 4. 1 Hasil Nmap.....	38

Gambar 4. 2 Tampilan IP Terblokir	39
Gambar 4. 3 Tampilan Nmap Menyerang <i>Server Asli</i>	39
Gambar 4. 4 Tampilan Hasil Serangan <i>Brute Force</i>	40
Gambar 4. 5 Tampilan Log Saat Ada Yang Mencoba Masuk.....	41
Gambar 4. 6 Tampilan Saat Penyerang Berhasil Mendapatkan <i>Username</i> Dan <i>Password</i>	41
Gambar 4. 7 <i>Fail2ban</i> Berhasil Memblokir Penyerang	42
Gambar 4. 8 Medusa Gagal Melanjutkan Pencobaan <i>Login</i>	42
Gambar 4. 9 Kippo Gagal Mendapatkan Data Dari Penyerang	43
Gambar 4. 10 Tampilan SSH <i>Attacker</i> Pada <i>Honeypot</i>	43
Gambar 4. 11 Tampilan SSH <i>Client</i> Sah.....	44
Gambar 4. 12 Tampilan Serangan Medusa Pada <i>Server Asli</i>	44
Gambar 4. 13 Tampilan IP Yang Sudah Terblokir	45
Gambar 4. 14 Tampilan <i>Attacker</i> Gagal Masuk Ke SSH <i>Server</i>	45
Gambar 4. 15 Tampilan <i>Client</i> sah Berhasil Mengakses SSH <i>Server</i>	45
Gambar 4. 16 Loic Melancarkan Serangan.....	46
Gambar 4. 17 Hasil Log Dionaea.....	47
Gambar 4. 18 Tampilan Saat <i>Client</i> Uji Ketersediaan <i>Server</i>	47
Gambar 4. 19 Tampilan Loic Menyerang <i>Server Asli</i>	48
Gambar 4. 20 Tampilan <i>Attacker</i> Mengakses http <i>Server</i>	49
Gambar 4. 21 Tampilan Saat <i>Client</i> Mengakses <i>Web Server</i>	49
Gambar 4. 22 Serangan SQL	50
Gambar 4. 23 Tampilan Database Pada Honeypot	50
Gambar 4. 24 Tampilan Database dvwa.....	51
Gambar 4. 25 Tampilan Database dvwa Table users	51
Gambar 4. 26 Tampilan Database dvwa Table user dan password.....	51
Gambar 4. 27 Tampilan SQL Menyerang <i>Server Asli</i>	52
Gambar 4. 28 Tampilan <i>Web Server Asli</i> Penyerang.....	53
Gambar 4. 29 Tampilan Saat <i>Client</i> Mengakses Alamat Url <i>Server Asli</i>	53

DAFTAR TABEL

Tabel 3. 1 Spesifikasi Laptop	12
Table 3. 2 <i>Software</i> Yang Digunakan	12
Tabel 3. 3 Pengalamatan IP	14
Tabel 3. 4 <i>Timeline</i> Kegiatan.....	31