

SKRIPSI

**ANALISIS KINERJA SISTEM *HONEY POT* DALAM
MENDETEKSI SERANGAN *BRUTE FORCE* DAN *DDOS*
(*DISTRIBUTED DENIAL OF SERVICE*) PADA *SERVER***

***ANALYSIS OF HONEY POT SYSTEM PERFORMANCE IN
DETECTING BRUTE FORCE AND DDOS (DISTRIBUTED
DENIAL OF SERVICE) ATTACKS ON SERVER***



Disusun oleh

**YUSUP SYUHADA
16101078**

**PROGRAM STUDI S1 TEKNIK TELEKOMUNIKASI
FAKULTAS TEKNIK TELEKOMUNIKASI DAN ELEKTRO
INSTITUT TEKNOLOGI TELKOM PURWOKERTO
2021**

**ANALISIS KINERJA SISTEM *HONEY POT* DALAM
MENDETEKSI SERANGAN *BRUTE FORCE* DAN *DDOS*
(*DISTRIBUTED DENIAL OF SERVICE*) PADA *SERVER***

***ANALYSIS OF HONEY POT SYSTEM PERFORMANCE IN
DETECTING BRUTE FORCE AND DDOS (DISTRIBUTED
DENIAL OF SERVICE) ATTACKS ON SERVER***

**Skripsi ini digunakan sebagai salah satu syarat untuk memperoleh
Gelar Sarjana Teknik (S.T.)
Di Institut Teknologi Telkom Purwokerto
2021**

Disusun oleh

**YUSUP SYUHADA
16101078**

**DOSEN PEMBIMBING
Syariful Ikhwan, ST.,MT.
Bongga Arifwidodo, S.ST., M.T.**

**PROGRAM STUDI S1 TEKNIK TELEKOMUNIKASI
FAKULTAS TEKNIK TELEKOMUNIKASI DAN ELEKTRO
INSTITUT TEKNOLOGI TELKOM PURWOKERTO
2021**

HALAMAN PENGESAHAN

ANALISIS KINERJA SISTEM *HONEYBOTT* DALAM MENDETEKSI SERANGAN *BRUTE FORCE* DAN DDOS (*DISTRUBUTED DENIAL OF SERVICE*) PADA SERVER

*ANALYSIS OF HONEYBOTT SYSTEM PERFORMANCE IN DETECTING
BRUTE FORCE AND DDOS (*DISTRUBUTED DENIAL OF SERVICE*)
ATTACKS ON SERVER*

Disusun Oleh :

YUSUP SYUHADA
16101078

Telah dipertanggung jawabkan di hadapan Tim Penguji
pada tanggal 5 Maret 2021.

Susunan Tim Penguji

Pembimbing Utama

: Syariful Ikhwan, ST.,MT.
NIDN. 0605048201

Pembimbing Pendamping

: Bongga Arifwidodo, S.ST., M.T.
NIDN. 0603118901

Penguji 1

: Kukuh Nugroho, S.T., M.T.
NIDN. 0606088303

Penguji 2

: Eka Wahyudi, S.T., M.Eng.
NIDN. 0617117601

Mengetahui,

Ketua Program Studi S1 Teknik Telekomunikasi
Institut Teknologi Telkom Purwokerto

Herryawan Pujiharsono, S.T., M.Eng.
NIDN. 0617068801

HALAMAN ORISINALITAS

Dengan ini saya, **YUSUP SYUHADA**, menyatakan bahwa skripsi dengan judul "**ANALISIS KINERJA SISTEM HONEYPOT DALAM MENDETEKSI SERANGAN BRUTE FORCE DAN DDOS (DISTRIBUTED DENIAL OF SERVICE) PADA SERVER**" adalah benar-benar karya saya sendiri. Saya tidak melakukan penjiplakan kecuali melalui pengutipan sesuai dengan etika keilmuan yang berlaku. Saya bersedia menanggung resiko ataupun sanksi yang dijatuahkan kepada saya apabila ditemukan pelanggaran terhadap etika atau keilmuan dalam skripsi saya ini.

Purwokerto, 5 Maret 2021

Yang menyatakan,



(Yusup Syuhada)

PRAKATA

Puji dan syukur penulis panjatkan kehadirat Allah SWT yang telah melimpahkan kasih dan sayang-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul **“ANALISIS KINERJA SISTEM HONEYPOT DALAM MENDETEKSI SERANGAN BRUTE FORCE DAN DDOS (DISTRIBUTED DENIAL OF SERVICE) PADA SERVER”**.

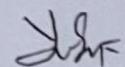
Maksud dari penyusunan skripsi ini adalah untuk memenuhi salah satu syarat dalam menempuh ujian sarjana Teknik Telekomunikasi pada Fakultas Teknik Telekomunikasi dan Elektro Institut Teknologi Telkom Purwokerto.

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. Allah S.W.T yang telah memberikan berbagai kenikmatan berupa nikmat iman, Islam, sehat, hidup, dan nikmat-nikmat lainnya.
2. Kedua orang tua yang telah memberikan motivasi, doa, dan nasihat sehingga membangkitkan semangat untuk terus berjuang.
3. Bapak Syariful Ikhwan, ST.,MT. selaku pembimbing I.
4. Bapak Bongga Arifwidodo, S.ST., M.T selaku pembimbing II.
5. Bapak Kukuh Nugroho, S.T., M.T. dan Bapak Eka Wahyudi, S.T., M.Eng. selaku penguji saat sidang.
6. Bapak Herryawan Pujiharsono, S.T.,M.Eng. Ketua Program Studi S1 Teknik Telekomunikasi.
7. Bapak Dr. Ali Rohman., M.Si. selaku Rektor Institut Teknologi Telkom Purwokerto.
8. Seluruh Dosen, staf dan karyawan Program studi S1 Teknik Telekomunikasi Institut Teknologi Telkom Purwokerto.
9. Seluruh teman-teman terutama Aditya yang telah menjadi notulen saat sidang dan Muzaki, Bagas, Wisnu, Maxwell, Bayu dan teman-teman kelas S1 TT 04 B 2016 yang telah menonton sidang dan menyemangati saat sebelum sidang dan

lainnya yang tidak bisa disebutkan satu persatu yang telah memberi semangat dalam proses penyusunan tugas akhir ini.

Purwokerto, 5 Maret 2021



(Yusup Syuhada)

DAFTAR ISI

HALAMAN PENGESAHAN	iii
PRAKATA	v
ABSTRAK	vii
ABSTRACT	viii
DAFTAR GAMBAR	xi
DAFTAR TABEL	xiii
BAB 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 DASAR TEORI	4
2.1. KAJIAN PUSTAKA	4
2.2. DASAR TEORI	8
2.2.1. Server	8
2.2.1. DDoS (<i>Distributed Denial of Service</i>)	9
2.2.2. Brute Force	9
2.2.3. SSH (<i>Secure Shell</i>)	9
2.2.4. Firewall NAT (<i>Network Address Translation</i>)	10
2.2.5. Honeypot Cowrie	10
2.2.6. Mikrotik RouterOS	12
2.2.7. MySQL	12
2.2.8. PuTTY	13
2.2.9. VirtualBox	14
2.2.10. Ubuntu	14
2.2.11. Kippo Graph	14
2.2.12. Nmap (<i>Network Mapper</i>)	15
2.2.13. LOIC (<i>Low Orbit Ion Cannon</i>)	15
BAB 3 METODE PENELITIAN	17
3.1. KONSEP HONEYPOT	17

3.2. ALAT YANG DIGUNAKAN	18
3.1.1. Perangkat Keras (<i>Hardware</i>)	18
3.1.2. Perangkat Lunak (<i>Software</i>).....	19
3.3. ALUR PENELITIAN.....	19
3.4. TOPOLOGI JARINGAN	21
3.5. INSTALASI DAN KONFIGURASI	23
3.4.1. Konfigurasi <i>Firewall</i> Mikrotik <i>RouterOS</i>	23
3.4.2. Instalasi dan Konfigurasi <i>Honeypot</i>	25
3.6. SKENARIO PENGUJIAN	29
3.5.1. Skenario Pertama	29
3.5.2. Skenario Kedua	30
BAB 4 HASIL DAN PEMBAHASAN	32
4.1. HASIL PENGUJIAN	32
4.2. ANALISIS CPU (<i>Central Processing Unit</i>)	37
4.3. ANALISIS MEMORI	39
4.4. ANALISIS <i>LOG</i>.....	42
4.4.1. <i>Log</i> Serangan Skenario Pertama	42
4.4.2. <i>Log</i> Serangan Skenario Kedua	43
BAB 5 KESIMPULAN DAN SARAN	45
5.1. KESIMPULAN	45
5.2. SARAN	45
DAFTAR PUSTAKA	46
LAMPIRAN A	51
LAMPIRAN B	56

DAFTAR GAMBAR

Gambar 2.1 Mikrotik <i>RouterOS</i> [30]	12
Gambar 2.2 MySQL	13
Gambar 2.3 Aplikasi PuTTY	13
Gambar 2.4 Aplikasi LOIC	16
Gambar 3.1 Konsep Kerja <i>Honeypot</i> [43].....	17
Gambar 3.2 Alur Penelitian	20
Gambar 3.3 Topologi Jaringan.....	22
Gambar 3.4 <i>Port Forwarding</i> 80 Mikrotik <i>RouterOS</i>.....	24
Gambar 3.5 <i>Port Forwarding</i> 22 Mikrotik <i>RouterOS</i>	24
Gambar 3.6 <i>Update</i> dan <i>Upgrade Repository</i>	25
Gambar 3.7 Memilih Konfigurasi	25
Gambar 3.8 Menambahkan <i>User</i>.....	26
Gambar 3.9 Memasang Paket.....	26
Gambar 3.10 Mengunduh <i>File Cowrie</i>	26
Gambar 3.11 Proses Membuat <i>Virtualenv</i>	27
Gambar 3.12 Menduplikat <i>File</i>	27
Gambar 3.13 Update <i>IPTables</i>	27
Gambar 3.14 Menjalankan <i>Cowrie</i>.....	28
Gambar 3.15 <i>Sudoers</i>	28
Gambar 3.16 Mengedit <i>Sudoers</i>.....	28
Gambar 3.17 Skenario Pertama	29
Gambar 3.18 Skenario Kedua.....	30
Gambar 4.1 Aplikasi LOIC	33
Gambar 4.2 Aplikasi Nmap.....	34
Gambar 4.3 Hasil Grafik Serangan.....	35
Gambar 4.4 Aplikasi PuTTY	36
Gambar 4.5 Penyerang Berhasil Masuk Ke <i>Server Honeypot</i>	37
Gambar 4.6 CPU Skenario Pertama	38
Gambar 4.7 CPU Skenario Kedua	39

Gambar 4.8 Memori Skenario Pertama	40
Gambar 4.9 Memori Skenario Kedua.....	41
Gambar 4.10 <i>Log Rata-Rata Serangan Skenario Pertama.....</i>	42
Gambar 4.11 Top 10 <i>Username</i> Pada Skenario Kedua	43
Gambar 4.12 Top 10 <i>Password</i> Pada Skenario Kedua	44
Gambar 4.13 Top 10 <i>Input</i> Pada Skenario Kedua	44

DAFTAR TABEL

Tabel 3.1 Spesifikasi Perangkat	18
Tabel 3.2 <i>Software</i> Yang Digunakan	19
Tabel 3.3 Pengalamanan IP	23
Tabel 4.1 Serangan Skenario Pertama.....	32
Tabel 4.2 Serangan <i>Brute Force</i>.....	35