

**IMPLEMENTASI HONEYPOT COWRIE UNTUK
MENDETEKSI SERANGAN PROTOKOL SSH PADA
SERVER BESERTA WEB MONITORING DAN
NOTIFIKASI OTOMATIS
(STUDI KASUS UPT TIK UNDIKSHA)**



**OLEH :
PUTU BAYU MEGAWANTA
1615051020**

**PROGRAM STUDI PENDIDIKAN TEKNIK INFORMATIKA
JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN KEJURUAN
UNIVERSITAS PENDIDIKAN GANESHA
SINGARAJA**

2023

**IMPLEMENTASI HONEYPOT COWRIE UNTUK
MENDETEKSI SERANGAN PROTOKOL SSH PADA
SERVER BESERTA WEB MONITORING DAN
NOTIFIKASI OTOMATIS
(STUDI KASUS UPT TIK UNDIKSHA)**

SKRIPSI

**Diajukan kepada
Universitas Pendidikan Ganesha
Untuk Memenuhi Satu Syarat dalam Menyelesaikan Program Sarjana
Pendidikan Teknik Informatika**

**Oleh
Putu Bayu Megawanta
NIM 1615051020**

**PROGRAM STUDI PENDIDIKAN TEKNIK INFORMATIKA
JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN KEJURUAN
UNIVERSITAS PENDIDIKAN GANESHA
SINGARAJA**

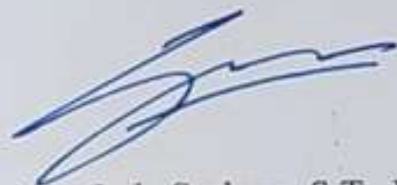
2023

Skripsi oleh Putu Bayu Megawanta

Telah dipertahankan di depan dewan penguji

Pada Tanggal,

Dewan Penguji,



Gede Arna Jude Saskara, S.T., M.T
NIP. 199105152020121003

(Ketua)



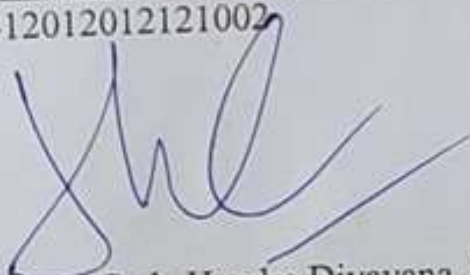
Dr. I Made Gede Sunarya, S.Kom., M.Cs.
NIP. 198307252008011008

(Anggota)



Ketut Resika Arthana, S.T., M.Kom.
NIP. 198412012012121002

(Anggota)



Prof. Dr. Dewa Gede Hendra Divayana, S.Kom., M.Kom.
NIP. 198407242015041002

(Anggota)

SKRIPSI

**DIAJUKAN UNTUK MELENGKAPI TUGAS-TUGAS
DAN MEMENUHI SYARAT-SYARAT UNTUK
MENCAPAI GELAR SARJANA PENDIDIKAN**

Menyetujui,

Pembimbing I



I Ketut Resika Arthana, S.T., M.Kom.
NIP. 198412012012121002

Pembimbing II



Prof. Dr. Dewa Gede Hendra Divayana, S.Kom, M.Kom.
NIP. 198407242015041002

Diterima oleh Panitia Ujian Fakultas Teknik dan Kejuruan
Universitas Pendidikan Ganesha
Guna memenuhi syarat-syarat untuk mencapai gelar sarjana pendidikan

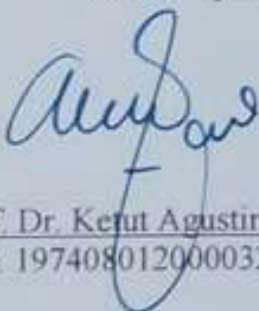
Pada :

Hari : Jumat

Tanggal : 21 Juli 2023

Menyetujui

Ketua Ujian,



Prof. Dr. Ketut Agustini, S.Si., M.Si
NIP. 197408012000032001

Sekretaris Ujian,



Dr. phil. Dessy Seri Wahyuni, S.Kom., M.Eng.
NIP. 198502152008122007

Mengesahkan
Wakil Rektor Bidang Akademik Dan Kerjasama




Prof. Dr. Gede Rasben Dantes, S.T., M.T.I.
NIP. 197502212003121001

PERNYATAAN

Dengan ini saya nyatakan bahwa, karya tulis yang berjudul “ **Implementasi Honeypot Cowrie Untuk Mendeteksi Serangan Protokol SSH Pada Server Beserta Web Monitoring dan Notifikasi Otomatis (Studi Kasus: UPT TIK Undiksha)** ” beserta seluruh isinya adalah benar karya sendiri, dan tidak melakukan penjiplakan atau mengutip dengan cara yang tidak sesuai dengan etika yang berlaku di dalam masyarakat keilmuan. Atas pernyataan ini saya siap bertanggung jawab serta menanggung resiko/sanksi yang dijatuhkan kepada saya apabila kemudian ditemukan adanya pelanggaran atas etika keilmuan di dalam karya ini.

Singaraja, 27 Juli 2023
Yang membuat pernyataan



Putu Bayu Megawanta

PERNYATAAN

Dengan ini saya nyatakan bahwa, karya tulis yang berjudul “ **Implementasi Honeypot Cowrie Untuk Mendeteksi Serangan Protokol SSH Pada Server Beserta Web Monitoring dan Notifikasi Otomatis (Studi Kasus: UPT TIK Undiksha)** ” beserta seluruh isinya adalah benar karya sendiri, dan tidak melakukan penjiplakan atau mengutip dengan cara yang tidak sesuai dengan etika yang berlaku di dalam masyarakat keilmuan. Atas pernyataan ini saya siap bertanggung jawab serta menanggung resiko/sanksi yang dijatuhkan kepada saya apabila kemudian ditemukan adanya pelanggaran atas etika keilmuan di dalam karya ini.



KATA PERSEMBAHAN

TERIMA KASIH SAYA UCAPKAN KEPADA :

IDA SANG HYANG WIDHI WASA

Atas berkat rahmat dan restu beliau skripsi ini dapat diselesaikan.

SKRIPSI INI SAYA DEDIKASIKAN KEPADA KELUARGA TERCINTA

(Nyoman Dogen & Luh Srinadi)

Yang telah berperan besar sebagai orang tua dengan merawat, membesarkan serta membimbing saya dengan penuh kasih sayang dan selalu memberikan saya semangat, motivasi, serta doa dalam setiap tahapan saya menempuh jenjang Pendidikan.

(I Made Indra Yoga Prana)

Yang telah memberikan saya semangat yang luar biasa dari jiwa seorang adik untuk menyelesaikan skripsi ini.

(I Wayan Budi Joyo & Keluarga)

Yang telah memberikan support serta memotivasi saya dalam hal tantangan kehidupan yang bermanfaat untuk masa depan saya.

DAN JUGA TERIMA KASIH YANG TERAMAT DALAM PENULIS
UCAPKAN KEPADA

SELURUH STAF DOSEN PTI

Yang telah bersedia membimbing penulis dalam menyelesaikan skripsi ini.

TEMAN-TEMAN SEPERJUANGAN

Yang tidak dapat saya sebutkan satu-persatu yang telah mendukung dan memberikan semangat.

PRAKATA

Puji syukur penulis panjatkan kehadirat Tuhan Yang Maha Esa, Ida Sang Hyang Widhi Wasa. Karena atas rahmat dan karunia-Nya penulis dapat menyelesaikan sebuah karya tulis berupa skripsi yang berjudul **“Implementasi HoneyPot Cowrie Untuk Mendeteksi Serangan Protokol SSH Pada Server Beserta Web Monitoring Dan Notifikasi Otomatis”**. Adapun tujuan dari penulisan skripsi ini dimaksudkan untuk memenuhi salah satu persyaratan untuk memperoleh gelar Sarjana Pendidikan di Universitas Pendidikan Ganesha.

Skripsi ini dapat terselesaikan atas bimbingan serta bantuan dari berbagai pihak. Penulis menyampaikan penghargaan dan ucapan terima kasih kepada yang terhormat:

1. Prof. Dr. I Wayan Lasmawan, M.Pd selaku Rektor Universitas Pendidikan Ganesha.
2. Prof. Dr. I Gede Sudirtha, S.Pd.,M.Pd. selaku Dekan Fakultas Teknik dan Kejuruan Universitas Pendidikan Ganesha.
3. Dr.phil., Dessy Seri Wahyui, S.Kom.,M.Eng. selaku Koordinator Program Studi Pendidikan Teknik Informatika Universitas Pendidikan Ganesha.
4. Gede Arna Jude Saskara, S.T., M.T. selaku penguji I yang telah memberikan arahan kepada penulis sehingga dapat terselesaikannya skripsi ini.
5. Dr. I Made Gede Sunarya, S.Kom., M.C, selaku penguji II yang senantiasa memberikan dukungan untuk penyelesaian skripsi ini.
6. I Ketut Resika Arthana, S.T., S.Kom. selaku pembimbing I yang selalu memberikan solusi untuk setiap masalah yang penulis hadapi saat Menyusun skripsi ini.
7. Prof. Dr. Dewa Gede Hendra Divayana, S.Kom., M.Kom. selaku pembimbing II yang selalu memberikan bimbingan serta arahan agar dapat terselesaikannya skripsi ini.
8. Bapak dan Ibu staf dosen di lingkungan Fakultas Teknik dan Kejuruan yang selalu membimbing dan mendidik selama penulis menempuh Pendidikan di Jurusan Teknik Informatika.

9. Keluarga atas segala dorongan, dukungan, dan motivasi baik dari segi material maupun moril demi keberhasilan studi penulis.
10. Rekan-rekan mahasiswa Prodi Pendidikan Teknik Informatika yang telah mendukung dan memberikan motivasi dalam penyelesaian skripsi ini.

Menyadari atas segala keterbatasan kemampuan penulis bahwa skripsi ini masih jauh dari kata sempurna, maka dari itu penulis mengharapkan saran serta perbaikan dari para pembaca sebagai bahan masukan bagi penulis di masa yang akan datang. Penulis berharap semoga skripsi ini dapat bermanfaat bagi para pembaca.



DAFTAR ISI

	Halaman
PERNYATAAN.....	vii
KATA PERSEMBAHAN.....	viii
MOTTO	ix
PRAKATA.....	x
DAFTAR ISI.....	xii
DAFTAR TABEL.....	xv
DAFTAR GAMBAR	xvi
DAFTAR LAMPIRAN.....	xviii
ABSTRAK	xix
ABSTRACT.....	xx
BAB I PENDAHULUAN.....	1
1.1 LATAR BELAKANG	1
1.2 IDENTIFIKASI MASALAH	5
1.3 RUMUSAN MASALAH.....	5
1.4 TUJUAN PENELITIAN.....	6
1.5 MANFAAT HASIL PENELITIAN.....	6
1.6 BATASAN MASALAH.....	7
BAB II LANDASAN TEORI.....	8
2.1 PENELITIAN TERKAIT	8
2.2 KAJIAN TEORI	13
2.2.1 KONSEP KEAMANAN KOMPUTER DAN JARINGAN.....	13
2.2.2 UPT TIK (UNIT PELAKSANA TEKNIS TEKNOLOGI, INFORMASI, DAN KOMUNIKASI) UNDIKSHA.....	15
2.2.3 SSH PROTOCOL VULNERABLE	17
2.2.4 PASSWORD.....	18
2.2.5 SSH BRUTE FORCE ATTACK.....	20
2.2.6 PASSWORD BRUTE-FORCE SOFTWARE.....	21
2.2.7 HONEYPOT	22
2.2.8 NDLC (NETWORK DEVELOPMENT LIFE CYCLE).....	31
2.2.9 COWRIE HONEYPOT	32

2.2.10	CONFUSION MATRIX.....	35
2.2.11	SOFTWARE PENDUKUNG PENELITIAN.....	37
4.1.6.3	TELEGRAM	37
4.1.6.4	ORACLE VM VIRTUAL BOX.....	38
4.1.6.5	PYTHON.....	39
4.1.6.6	MYSQL.....	40
4.1.6.7	KIPPO-GRAPH.....	40
4.1.6.8	FAIL 2 BAN.....	41
BAB III METODE PENELITIAN.....		43
3.1	TEMPAT DAN WAKTU PENELITIAN.....	43
3.2	METODE PENELITIAN	43
3.2.1	TAHAP ANALYSIS	44
3.2.2	TAHAP DESIGN	50
3.2.3	TAHAP PROTOTYPE DAN IMPLEMENTASI.....	55
3.2.4	TAHAP MONITORING	58
3.2.5	TAHAP MANAGEMENT	67
BAB IV HASIL DAN PEMBAHASAN		69
4.1	HASIL PENELITIAN	69
4.1.1	ANALISIS DATA SPESIFIKASI PERANGKAT.....	69
4.1.2	ANALISIS TOPOLOGI	73
4.1.3	DESAIN TOPOLOGI DAN PERANCANGAN SISTEM.....	73
4.1.4	DATA SIMULASI / PROTOTYPING.....	76
4.1.5	IMPLEMENTASI SISTEM	79
4.1.5.1	IMPLEMENTASI SISTEM PROTOTYPING / SIMULASI	79
4.1.5.2	IMPLEMENTASI SERVER PADA UPT TIK.....	87
4.1.6	MONITORING SISTEM HONEYPOT.....	90
4.1.6.1	HASIL PENGUJIAN SIMULASI	90
4.1.6.2	HASIL PENGUJIAN SISTEM HONEYPOT UPT TIK	94
4.1.7	SISTEM MANAJEMEN COWRIE HONEYPOT.....	104
4.2	PEMBAHASAN PENELITIAN.....	104
BAB V PENUTUP.....		106
5.1	KESIMPULAN.....	106



DAFTAR TABEL

Tabel 2. 1 Contoh password yang mudah ditebak	19
Tabel 2. 2 Perbandingan implementasi honeypot dengan konsep keamanan lainnya.....	24
Tabel 2. 3 Sektor dan kemungkinan bagian serangan berdasarkan frekuensi	25
Tabel 2. 4 Perbandingan berbagai jenis honeypot	30
Tabel 2. 5 Implementasi berbagai level honeypot	34
Tabel 2. 6 Confusion Matrix	35
Tabel 3. 1 Tabel variabel simulasi serangan BruteForce	51
Tabel 3. 2 Skenario dengan tahapan serangan ZEH	59
Tabel 3. 3 Tabel acuan parameter CIA	62
Tabel 4. 1 Data spesifikasi perangkat server untuk Cowrie Honeypot.....	70
Tabel 4. 2 Detail spesifikasi perangkat untuk melakukan simulasi	71
Tabel 4. 3 Daftar versi software pendukung penelitian	72
Tabel 4. 4 Detail Virtual Box Server Xyz untuk Simulasi / Prototyping.....	77
Tabel 4. 5 Detail Virtual Box Cowrie Honeypot untuk Simulasi / Prototyping ...	78
Tabel 4. 6 IP address Virtual Box Machine	83
Tabel 4. 7 Langkah Instalasi Cowrie Honeypot.....	83
Tabel 4. 8 Langkah Instalasi Database Cowrie.....	85
Tabel 4. 9 Hasil simulasi serang menggunakan ZEH Method.....	91
Tabel 4. 10 Hasil Resource Usage pada simulasi/prorotype.....	93
Tabel 4. 11 Hasil serangan ke server Cowrie Honeypot UPT TIK.....	94
Tabel 4. 12 Hasil resource usage pada server Cowrie Honeypot UPT TIK	96
Tabel 4. 13 Data traffic dan waktu operasional pengujian honeypot UPT TIK ...	96
Tabel 4. 14 Nilai Confusion pada Cowrie Honeypot UPT TIK.....	99
Tabel 4. 15 Hasil nilai pada parameter CIA Cowrie Honeypot UPT TIK.....	101

DAFTAR GAMBAR

Gambar 2. 1 Diagram Fishbone Penelitian Terkait.....	13
Gambar 2. 2 CIA Triad Computer and Network Security	15
Gambar 2. 3 Open port Scanning dengan menggunakan Tool Nmap.....	16
Gambar 2. 4 Basic Attack Method ZEH (Zero Entity Hacking).....	17
Gambar 2. 5 SSH Client Server	18
Gambar 2. 6 Gambaran proses Salting pada plaintext password serta proses otentikasinya	19
Gambar 2. 7 Diagram alir Brute-Force attack.....	20
Gambar 2. 8 Logo Nmap.....	21
Gambar 2. 9 Logo THC Hydra	22
Gambar 2. 10 Gambaran Sistem Honeypot	23
Gambar 2. 11 IT Infrastructure dengan Honeypot	27
Gambar 2. 12 NDLC Chart	31
Gambar 2. 13 Logo Telegram	37
Gambar 2. 14 Logo Oracle VM Virtual Box	38
Gambar 2. 15 Logo Python	39
Gambar 2. 16 Logo MySQL	40
Gambar 2. 17 Logo Kippo Graph	40
Gambar 2. 18 Logo Fail 2 Ban.....	41
Gambar 3. 1 Chart Metode NDLC.....	44
Gambar 3. 2 Desain Topologi UPT TIK.....	50
Gambar 3. 3 FlowChart Port Scanning dan Bruteforce	52
Gambar 3. 4 Desain Topologi Simulasi sisi Admin.....	53
Gambar 3. 5 Desain Topologi Simulasi sisi Attacker	54
Gambar 3. 6 Desain Implementasi di Virtual Box.....	54
Gambar 3. 7 Rancangan Implementasi Honeypot Cowrie.....	55
Gambar 3. 8 Use Case Diagram Admin Server dengan Honeypot	56
Gambar 3. 9 Rancangan Topologi Implementasi Blocklist IP dengan menggunakan Firewall	57
Gambar 3. 10 Flowchart Implementasi Blocklist IP dengan menggunakan Firewall	58

Gambar 4. 1 Topologi server secara sederhana yang terimplementasi di UPT TIK	73
Gambar 4. 2 Topologi rancangan untuk simulasi	74
Gambar 4. 3 Topologi rancangan implementasi pada server Xyz UPT TIK.....	74
Gambar 4. 4 Rancangan Topologi untuk system informasi Cowrie Honeypot	75
Gambar 4. 5 Blocklist IP Fail2ban dalam pencegahan ke server internal honeypot system.....	76
Gambar 4. 6 Detail Virtual Box untuk simulasi/prorotyping Cowrie Honeypot..	80
Gambar 4. 7 Detail Virtual Box untuk simulasi/prototyping server Xyz	81
Gambar 4. 8 Konfigurasi Nat Network pada Virtual Box	81
Gambar 4. 9 Port forwarding pada Virtual Box	82
Gambar 4. 10 Konfigurasi IP Address pada Virtual Box Machine	82
Gambar 4. 11 Cowrie Configuration SSH	86
Gambar 4. 12 Cowrie Configuration MySQL.....	86
Gambar 4. 13 Status UFW Firewall.....	87
Gambar 4. 14 SSH Server Cowrie	87
Gambar 4. 15 Interface pada server Honeypot Cowrie.....	88
Gambar 4. 16 API Telegram Cowrie Honeypot.....	89
Gambar 4. 17 before.rules configuration untuk melakukan port forwarding NAT	89
Gambar 4. 18 Konfigurasi SSH Blocklist pada fail2ban	89
Gambar 4. 19 Konfigurasi database config.php pada kippo-graph untuk visualisasi	90

DAFTAR LAMPIRAN

Lampiran 1. Surat Ijin Wawancara dari Fakultas ke UPT TIK.....	112
Lampiran 2. Tabel Wawancara dari pihak UPT TIK.....	113

