PROPOSAL SKRIPSI

PENGEMBANGAN DAN PENERAPAN SISTEM HONEYPOT BERBASIS CONTAINER UNTUK DETEKSI DAN KLASIFIKASI SERANGAN EMPIRIS DI JARINGAN KAMPUS

OLEH:
IRFAN MAULANA
NIM. 2022903430067

PROGRAM STUDI
TEKNOLOGI REKAYASA KOMPUTER JARINGAN
JURUSAN TEKNOLOGI INFORMASI & KOMPUTER
POLITEKNIK NEGERI LHOKSEUMAWE
2026

LEMBAR PENGESAHAN PROPOSAL SKRIPSI

Judul Skripsi : Pengembangan dan Penerapan Sistem Honeypot Berbasis Container untuk Deteksi dan Klasifikasi Serangan Empiris di Jaringan Kampus

Nama Mahasiswa : IRFAN MAULANA

NIM : 2022903430067

Program Studi : Teknologi Rekayasa Komputer Jaringan

Proposal telah diuji pada tanggal <dd mm yyyy> dan sudah diperbaiki sesuai saran pembahas seminar dan pembimbing.

Menyetujui,

Dosen Pembimbing Pendamping	Dosen Pembimbing Utama
Muhammad Khadafi, ST., MT.	**Aswandi, S.Kom., M.Kom.**
NIP. 197507182002121004	NIP. 197209242010121001

Mengetahui,
Ketua Program Studi
Teknologi Rekayasa Komputer Jaringan

Nanda Saputri, S.S.T., M.T.
NIP. 199111202022032010

RINGKASAN

Keamanan jaringan kampus menjadi perhatian penting seiring dengan meningkatnya pemanfaatan jaringan untuk mendukung kegiatan akademik, administrasi, dan layanan informasi. Infrastruktur jaringan kampus yang bersifat terbuka bagi banyak pengguna memiliki tingkat kerentanan yang tinggi terhadap berbagai jenis serangan jaringan. Kondisi tersebut menuntut adanya sistem yang mampu mendeteksi dan menganalisis serangan jaringan secara empiris serta menyediakan data yang terukur sebagai dasar evaluasi keamanan jaringan.

Penelitian ini bertujuan untuk mengembangkan dan menerapkan sistem honeypot berbasis container dalam mendeteksi dan mengklasifikasikan serangan jaringan di lingkungan kampus. Sistem honeypot dirancang untuk mensimulasikan layanan jaringan palsu yang berfungsi sebagai umpan bagi penyerang, sehingga aktivitas serangan dapat direkam dan dianalisis secara langsung. Data serangan yang diperoleh diklasifikasikan berdasarkan kategori serangan jaringan dan dievaluasi menggunakan parameter teknis jaringan.

Metode penelitian yang digunakan adalah metode eksperimen dengan pendekatan kuantitatif. Evaluasi sistem dilakukan menggunakan metrik terukur yang meliputi tingkat keberhasilan serangan, waktu respons sistem, kestabilan koneksi klien, serta analisis paket jaringan. Hasil penelitian ini diharapkan dapat memberikan gambaran objektif mengenai kondisi keamanan jaringan kampus dan menjadi acuan dalam upaya peningkatan sistem keamanan jaringan.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan jaringan komputer di lingkungan kampus mendorong meningkatnya pemanfaatan layanan jaringan untuk mendukung kegiatan akademik, administrasi, dan penelitian. Infrastruktur jaringan kampus umumnya bersifat terbuka bagi pengguna, sehingga memiliki tingkat kerentanan yang tinggi terhadap berbagai ancaman keamanan jaringan. Kondisi tersebut menjadikan jaringan kampus sebagai target potensial terjadinya serangan jaringan, baik dalam bentuk pemindaian, percobaan akses tidak sah, maupun eksploitasi layanan.

Serangan jaringan di lingkungan kampus sering kali sulit terdeteksi secara dini karena sistem pengamanan yang digunakan masih bersifat pasif dan terbatas pada mekanisme pencegahan. Sistem seperti firewall dan intrusion detection system belum sepenuhnya mampu menyediakan data empiris mengenai pola serangan, metode yang digunakan, serta dampaknya terhadap performa jaringan. Akibatnya, proses analisis dan evaluasi keamanan jaringan tidak didukung oleh data serangan yang komprehensif dan terukur.

Perkembangan teknologi virtualisasi dan keamanan jaringan mendorong penerapan pendekatan yang lebih adaptif, salah satunya melalui pengembangan honeypot berbasis container. Pendekatan ini memungkinkan pengamatan aktivitas serangan secara langsung, fleksibel, dan efisien dengan pemanfaatan sumber daya yang ringan. Dengan demikian, pengembangan dan penerapan sistem honeypot berbasis container diperlukan untuk mendeteksi dan mengklasifikasikan serangan jaringan secara empiris serta menghasilkan data terukur sebagai dasar peningkatan keamanan jaringan kampus.

1.2 Rumusan masalah

Permasalahan dalam penelitian ini adalah belum tersedianya sistem yang mampu mendeteksi dan merekam aktivitas serangan jaringan secara empiris di lingkungan jaringan kampus. Mekanisme pengamanan jaringan yang ada masih terbatas dalam menyediakan data serangan yang menerima dengan baik untuk keperluan analisis dan evaluasi keamanan jaringan

Permasalahan berikutnya berkaitan dengan belum optimalnya sistem dalam melakukan klasifikasi jenis serangan jaringan serta pengukuran dampak serangan berdasarkan parameter teknis jaringan. Dengan demikian, diperlukan pengembangan sistem honeypot berbasis container yang mampu mengklasifikasikan serangan secara sistematis dan menghasilkan metrik terukur, meliputi tingkat keberhasilan serangan, waktu respons sistem, kestabilan koneksi klien, serta analisis paket jaringan.

1.3 Tujuan Penelitian

Penelitian ini bertujuan untuk mengembangkan dan menerapkan sistem honeypot berbasis container pada jaringan kampus guna mendeteksi dan merekam aktivitas serangan jaringan secara empiris. Sistem yang dikembangkan diharapkan mampu menyediakan data serangan yang relevan untuk keperluan analisis keamanan jaringan.

Selain itu, penelitian ini bertujuan untuk mengklasifikasikan jenis serangan jaringan berdasarkan karakteristik trafik dan layanan yang diserang serta mengukur dampak serangan menggunakan parameter teknis jaringan. Hasil pengukuran diharapkan dapat memberikan gambaran objektif mengenai kondisi keamanan jaringan kampus.

1.4 Batasan Masalah

Penelitian ini dibatasi pada penerapan sistem honeypot berbasis container dalam lingkungan jaringan kampus. Jenis serangan yang dianalisis meliputi serangan jaringan yang umum terjadi, seperti scanning, brute force, eksploitasi layanan, dan denial of service.

Sistem honeypot yang dikembangkan difokuskan pada proses pendeteksian, pencatatan, dan klasifikasi serangan jaringan. Penelitian ini tidak membahas implementasi sistem pengamanan jaringan secara menyeluruh di luar lingkup honeypot.

1.5 Manfaat Penelitian

Manfaat akademik dari penelitian ini adalah memberikan kontribusi terhadap pengembangan ilmu pengetahuan di bidang keamanan jaringan, khususnya terkait penerapan honeypot berbasis container untuk analisis serangan jaringan secara empiris. Penelitian ini dapat menjadi referensi bagi penelitian selanjutnya dengan topik serupa.

Manfaat praktis dari penelitian ini adalah menyediakan sistem pendukung keamanan jaringan yang mampu membantu pengelola jaringan kampus dalam memahami pola serangan yang terjadi. Data empiris yang dihasilkan diharapkan dapat digunakan sebagai dasar evaluasi dan peningkatan keamanan jaringan.

BAB II

TINJAUAN PUSTAKA

2.1 *State of the art*

Honeypot merupakan salah satu pendekatan keamanan jaringan yang digunakan untuk mendeteksi dan mengamati aktivitas serangan secara langsung dengan menyediakan layanan umpan yang menyerupai sistem nyata. Pendekatan ini memungkinkan pengumpulan data serangan secara empiris, sehingga pola dan karakteristik serangan dapat dianalisis lebih mendalam dibandingkan dengan sistem keamanan pasif.

Penelitian oleh **Aulia et al. (2025)** menunjukkan bahwa penerapan honeypot berbasis Cowrie efektif dalam mendeteksi serangan brute force terhadap layanan SSH dan merekam pola aktivitas penyerang. Hasil penelitian tersebut membuktikan bahwa honeypot mampu menyediakan data serangan yang relevan untuk analisis keamanan jaringan. Namun, penelitian tersebut masih terbatas pada satu jenis layanan dan belum membahas klasifikasi serangan secara sistematis.

Penelitian lain oleh **Nanlohy dan Faizin (2025)** menerapkan honeypot sebagai mekanisme deteksi dini serangan jaringan. Hasil penelitian menunjukkan bahwa honeypot mampu meningkatkan visibilitas terhadap aktivitas serangan yang masuk ke sistem. Namun, penelitian tersebut belum membahas pengukuran dampak serangan menggunakan parameter teknis jaringan secara terstruktur.

Selanjutnya, **Susanto dan Romli (2025)** mengkaji penerapan honeypot dalam konteks keamanan jaringan dan menekankan perannya sebagai alat monitoring aktivitas serangan. Penelitian ini memberikan gambaran umum mengenai efektivitas honeypot, tetapi belum mengarah pada analisis empiris berbasis metrik jaringan yang terukur.

Pendekatan honeypot low-interaction juga dibahas oleh **Ubaidillah et al. (2023)** melalui implementasi Honeyd untuk mendeteksi aktivitas scanning dan serangan awal jaringan. Meskipun mampu mengidentifikasi pola serangan dasar, keterbatasan interaksi layanan menyebabkan data serangan yang diperoleh kurang mendalam. Sementara itu, **Damanik et al. (2025)** mengembangkan sistem honeypot real-time dengan integrasi beberapa jenis honeypot dan analisis paket jaringan, namun kompleksitas arsitektur menjadi tantangan dalam implementasinya.

Berdasarkan penelitian-penelitian tersebut, dapat disimpulkan bahwa honeypot efektif dalam mendeteksi dan merekam aktivitas serangan jaringan. Namun, masih terdapat celah penelitian terkait penerapan honeypot berbasis container yang mampu melakukan klasifikasi serangan secara sistematis serta menghasilkan metrik teknis jaringan yang terukur. Oleh karena itu, penelitian ini diarahkan pada pengembangan sistem honeypot berbasis container yang lebih fleksibel, efisien, dan sesuai dengan kebutuhan analisis keamanan jaringan kampus.

No	Penulis/Tahun	Judul Artikel	Metode yang digunakan	Hasil yang diperoleh	Perbandingan Penelitian	
					Persamaan	Perbedaan
1	Aulia et al., 2025	Implementasi dan Analisis Honeypot Berbasis Cowrie untuk Mendeteksi Serangan Siber	Honeypot Cowrie (low-interaction)	Honeypot mampu mendeteksi dan merekam serangan brute force pada layanan SSH	Sama-sama menggunakan honeypot untuk mendeteksi serangan jaringan	Penelitian ini menggunakan honeypot berbasis container serta melakukan klasifikasi serangan dan pengukuran metrik jaringan
2	Nanlohy & Faizin, 2025	Implementasi Honeypot untuk Mendeteksi Serangan Jaringan	Honeypot sebagai deteksi dini	Honeypot efektif dalam mendeteksi aktivitas serangan jaringan	Sama-sama berfokus pada pendeteksian serangan jaringan	Penelitian ini menambahkan klasifikasi serangan dan analisis metrik teknis jaringan
3	Susanto & Romli, 2025	Penerapan Honeypot dalam Keamanan Jaringan	Monitoring honeypot	Honeypot membantu proses evaluasi keamanan jaringan	Sama-sama memanfaatkan honeypot sebagai alat keamanan jaringan	Penelitian ini menekankan data empiris dan pengukuran performa jaringan

No	Penulis/Tahun	Judul Artikel	Metode yang digunakan	Hasil yang diperoleh	Perbandingan Penelitian	
					Persamaan	Perbedaan
4	Ubaidillah et al., 2023	Analisis dan Implementasi Honeypot Honeyd sebagai Low-Interaction Honeypot	Honeypot Honeyd	Berhasil mendeteksi aktivitas scanning dan serangan awal jaringan	Sama-sama menerapkan honeypot low-interaction	Penelitian ini menggunakan teknologi container untuk efisiensi dan fleksibilitas sistem
5	Damanik et al., 2025	Sistem Deteksi dan Pencegahan Serangan Jaringan Menggunakan Real-Time Honeypot	Multi honeypot dan analisis paket jaringan	Deteksi serangan dilakukan secara real-time dengan monitoring paket	Sama-sama melakukan pemantauan aktivitas serangan jaringan	Penelitian ini menggunakan arsitektur honeypot berbasis container yang lebih sederhana dan terukur

Tabel 2.1 State of the Arts

2.2 Tinjauan Teoritis

Honeypot adalah sistem keamanan yang dirancang untuk menarik perhatian penyerang dengan menyediakan layanan atau sumber daya palsu yang tampak seperti sistem nyata. Seluruh aktivitas yang terjadi pada honeypot dianggap sebagai aktivitas mencurigakan dan dicatat untuk keperluan analisis keamanan. Berdasarkan tingkat interaksinya, honeypot diklasifikasikan menjadi low-interaction, medium-interaction, dan high-interaction honeypot.

Teknologi container merupakan bentuk virtualisasi ringan yang memungkinkan aplikasi dijalankan secara terisolasi dalam satu sistem operasi. Penggunaan container dalam pengembangan honeypot memberikan keuntungan berupa efisiensi penggunaan sumber daya, kemudahan deployment, serta fleksibilitas dalam menjalankan berbagai layanan honeypot secara bersamaan. Hal ini menjadikan container sebagai solusi yang sesuai untuk implementasi honeypot di lingkungan jaringan kampus.

Serangan jaringan merupakan aktivitas yang bertujuan untuk mengganggu, menyusup, atau mengeksploitasi sistem jaringan. Secara umum, serangan jaringan dapat diklasifikasikan ke dalam beberapa tahap, yaitu reconnaissance, intrusion attempt, exploitation, dan disruption. Klasifikasi ini digunakan sebagai dasar dalam pengelompokan dan analisis serangan yang terdeteksi oleh sistem honeypot.

Pengukuran keamanan jaringan dilakukan menggunakan metrik teknis yang relevan, seperti tingkat keberhasilan serangan, waktu respons sistem, kestabilan koneksi klien, serta karakteristik paket jaringan. Metrik tersebut umum digunakan dalam rumpun Teknologi Rekayasa Komputer Jaringan untuk mengevaluasi performa sistem keamanan secara objektif dan terukur.

BAB III

METODOLOGI PENELITIAN

Metodologi penelitian adalah kerangka (*framework*) atau rencana atau gambaran urutan langkah pelaksanaan penelitian. Penelitian ini mencakup pendekatan, metode, teknik pengumpulan data, dan analisis yang digunakan untuk mencapai tujuan penelitian. Dengan demikian dapat diperkirakan hasil penelitian yang akan diperoleh secara utuh. Dalam bagian metodologi penelitian perlu diuraikan beberapa hal berikut:

3.1 Metode dan Variable Penelitian

Penelitian ini menggunakan metode **eksperimen** dengan pendekatan **kuantitatif**. Metode eksperimen dipilih karena penelitian berfokus pada pengamatan langsung terhadap aktivitas serangan jaringan yang diarahkan ke sistem honeypot. Seluruh data yang diperoleh merupakan data empiris hasil interaksi antara penyerang dan layanan honeypot yang disediakan.

Pendekatan kuantitatif digunakan untuk mengukur kinerja sistem honeypot berbasis container menggunakan parameter teknis jaringan yang terukur. Metode ini sesuai dengan rumpun Teknologi Rekayasa Komputer Jaringan karena pengukuran dilakukan berdasarkan performa jaringan dan karakteristik trafik secara objektif.

3.2 Data dan Pengumpulan Data

Sistem honeypot dirancang menggunakan teknologi container untuk mensimulasikan beberapa layanan jaringan palsu dalam lingkungan terisolasi. Arsitektur sistem bertujuan untuk menangkap, mencatat, dan menganalisis aktivitas serangan jaringan tanpa mengganggu layanan utama jaringan kampus.

Arsitektur sistem terdiri atas beberapa komponen utama, yaitu sumber trafik serangan, perangkat jaringan penghubung, jaringan terisolasi honeypot, container honeypot yang menjalankan layanan palsu, serta sistem logging dan penyimpanan data. Seluruh trafik yang mengarah ke layanan honeypot akan dicatat sebagai data serangan dan digunakan dalam proses analisis.

Arsitektur ini memungkinkan sistem melakukan pengamatan serangan secara langsung dan terkontrol, sehingga data yang diperoleh bersifat valid dan dapat digunakan sebagai dasar evaluasi keamanan jaringan.

3.3 Rancangan Sistem (Hardware/Software)

Kategorisasi serangan dilakukan secara sistematis berdasarkan karakteristik trafik dan jenis layanan yang diserang. Pengelompokan serangan bertujuan untuk memudahkan analisis pola dan tujuan serangan yang terjadi pada jaringan kampus.

Kategori serangan yang digunakan dalam penelitian ini adalah sebagai berikut:

a. **Reconnaissance**, yaitu aktivitas pengintaian jaringan seperti port scanning dan service probing.
b. **Intrusion Attempt**, yaitu percobaan akses tidak sah ke layanan jaringan, seperti brute force login.
c. **Exploitation**, yaitu upaya pemanfaatan celah keamanan layanan untuk mendapatkan akses atau kontrol sistem.
d. **Disruption**, yaitu serangan yang bertujuan mengganggu ketersediaan layanan, seperti denial of service.

3.4 Teknik Pengujian

Data penelitian diperoleh dari aktivitas serangan jaringan yang terekam oleh sistem honeypot berbasis container. Data yang dikumpulkan meliputi alamat IP sumber serangan, waktu serangan, jenis layanan yang diserang, log koneksi, serta data paket jaringan.

Pengumpulan data dilakukan secara otomatis melalui mekanisme logging pada honeypot. Selain itu, perekaman paket jaringan dilakukan selama periode pengujian untuk mendukung analisis karakteristik trafik serangan secara lebih mendalam.

3.5 Metrik Pengukuran dan Parameter Evaluasi

Pengukuran kinerja sistem dilakukan menggunakan metrik teknis jaringan yang umum digunakan dalam rumpun Teknologi Rekayasa Komputer Jaringan, yaitu:

1. **Keberhasilan Serangan**
   Diukur berdasarkan jumlah percobaan serangan yang berhasil berinteraksi dengan layanan honeypot dibandingkan dengan total serangan yang tercatat.
2. **Waktu Respons Sistem**
   Diukur dari selisih waktu antara permintaan (request) yang dikirimkan ke layanan honeypot dan respons yang diberikan oleh sistem.
3. **Kestabilan Koneksi Klien**
   Diukur menggunakan parameter jaringan seperti latency dan packet loss selama berlangsungnya aktivitas serangan.
4. **Analisis Paket Jaringan**
   Dilakukan dengan mengamati karakteristik paket jaringan, meliputi jenis protokol, ukuran paket, dan pola payload yang digunakan dalam serangan.

Metrik-metrik tersebut digunakan untuk menilai dampak serangan terhadap sistem serta kinerja honeypot dalam merekam aktivitas serangan.

3.6 Teknik Pengujian Sistem

Pengujian sistem dilakukan dengan mengarahkan berbagai jenis serangan jaringan ke layanan honeypot yang telah dikonfigurasi. Setiap serangan diuji untuk mengetahui kemampuan sistem dalam mendeteksi, mencatat, dan mengklasifikasikan aktivitas serangan.

Hasil pengujian dianalisis berdasarkan metrik yang telah ditentukan untuk mengetahui efektivitas sistem honeypot berbasis container dalam lingkungan jaringan kampus.

3.7 Hasil yang Diharapkan

Penelitian ini diharapkan menghasilkan sistem honeypot berbasis container yang mampu mendeteksi dan mengklasifikasikan serangan jaringan secara empiris. Selain itu, sistem diharapkan dapat menghasilkan data metrik jaringan yang terukur sebagai dasar evaluasi keamanan jaringan dan pengambilan keputusan dalam peningkatan keamanan jaringan kampus.

JADWAL KEGIATAN PENELITIAN

Jadwal kegiatan penelitian yang akan dilakukan mencakup seluruh tahapan dari penyusanan proposal hingga revisi laporan dan persiapan siding. Rincian jadwal kegiatan ada di dalam Table 3.1 berikut:

No	Kegiatan	Feb	Mar	Apr	Mei	Jun	Jul
1	Studi literatur dan penyusunan proposal	✓					
2	Seminar proposal dan revisi	✓	✓				
3	Perancangan arsitektur sistem		✓	✓			
4	Implementasi honeypot berbasis container			✓	✓		
5	Pengujian sistem dan pengumpulan data				✓	✓	
6	Analisis data dan evaluasi sistem					✓	
7	Penyusunan laporan skripsi					✓	✓
8	Revisi laporan dan persiapan sidang						✓

Table 3.1 Jadwal Penelitian

Catatan Jadwal Kegiatan

1. Jadwal penelitian disusun untuk jangka waktu enam bulan, terhitung mulai bulan Februari sampai dengan Juli.
2. Kegiatan penelitian dilaksanakan secara bertahap, dimulai dari studi literatur dan penyusunan proposal.
3. Tahap selanjutnya meliputi perancangan arsitektur sistem dan implementasi honeypot berbasis container.
4. Pengujian sistem dan pengumpulan data serangan dilakukan setelah sistem selesai diimplementasikan.

5. Analisis data dan evaluasi sistem dilakukan berdasarkan metrik teknis jaringan yang telah ditentukan.
6. Penyusunan laporan skripsi dilakukan setelah seluruh data penelitian diperoleh dan dianalisis.
7. Jadwal kegiatan bersifat fleksibel dan dapat disesuaikan dengan hasil bimbingan serta kondisi pelaksanaan penelitian.

RENCANA ANGGARAN PENELITIAN

No	Uraian Kebutuhan	Perkiraan Biaya (Rp)
1	Sewa VPS/Server untuk honeypot (± 6 bulan)	300.000 – 600.000
2	Koneksi internet pendukung penelitian	100.000 – 200.000
3	Instalasi dan konfigurasi sistem	0 – 100.000
4	Pengujian dan monitoring jaringan	0 – 100.000
5	Dokumentasi dan pencetakan laporan	150.000 – 300.000
6	ATK (alat tulis, kertas, dll.)	50.000 – 100.000
	Total Perkiraan Anggaran	**600.000 – 1.400.000**

Table 3.2 Perkiraan Anggaran Penelitian

Catatan Anggaran Penelitian

1. Biaya yang dicantumkan merupakan perkiraan dan dapat berubah sesuai kondisi pelaksanaan penelitian.
2. Penggunaan fasilitas kampus, seperti laboratorium dan jaringan internal, dapat mengurangi kebutuhan biaya penelitian.
3. Anggaran disusun secara realistis dan efisien sesuai kebutuhan penelitian.

DAFTAR PUSTAKA

Aulia, D. R., Rahman, W. A., & Zhacque, V. A. (2025). Implementasi dan analisis honeypot berbasis Cowrie untuk mendeteksi serangan siber. *Jurnal Teknologi Informasi dan Keamanan*, 10(1), 45–54. https://www.researchgate.net/publication/390316056

Damanik, H. A., Siregar, R., & Lubis, A. R. (2025). Sistem deteksi dan pencegahan serangan jaringan menggunakan real-time honeypot. *Jurnal Teknologi Informasi dan Ilmu Komputer*, 12(2), 101–112. https://jtiik.ub.ac.id/index.php/jtiik/article/download/9271/1501

Nanlohy, O. P., & Damanik, H. A. (2025). Implementasi honeypot untuk mendeteksi serangan jaringan. *Jurnal Aplikasi Teknologi Informasi*, 9(1), 15–24. https://ejournal.itn.ac.id/jati/article/view/15590

Susanto, C. (2025). Penerapan honeypot dalam keamanan jaringan. *J-INTECH: Journal of Information Technology*, 6(1), 33–41. https://jurnal.ubhinus.ac.id/index.php/J-INTECH/article/view/1924

Ubaidillah, U. (2023). Analisis dan implementasi honeypot Honeyd sebagai low-interaction honeypot. *Jurnal Teknologi dan Ilmu Komputer*, 8(2), 67–75. https://journal.sekawan-org.id/index.php/jtim/article/view/405

LAMPIRAN