Jurnal Profesi Insinyur Universitas Lampung (JPI)
Vol. 6 No. 2, Tahun 2025, e-ISSN: 2722-5771 https://doi.org/10.23960/jpi.v6n2.222

Penerapan Honeypot Dan Network Obfuscation Sebagai Sistem Pertahanan Aktif Dalam Keamanan Jaringan

Sahlan Zain Roji[1*], Muhammad Faishol Amrulloh[2]

[1,2] Universitas Yudharta Pasuruan, Indonesia
[3] Jurusan Teknik Informatika

Keywords:
Honeypot, Network Obfuscation, Network Security, Active Defense

Corespondent Email:
szainroji@gmail.com

Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem pertahanan aktif menggunakan teknologi Honeypot dan Network Obfuscation. Honeypot digunakan untuk menjebak serta memonitor aktivitas penyerang, sementara Network Obfuscation menyamarkan struktur jaringan asli dan mengarahkan lalu lintas mencurigakan ke sistem honeypot. Penelitian dilakukan secara nyata pada server DATANET. Hasil pengujian menunjukkan sistem berhasil mendeteksi serta mengalihkan serangan tanpa mengganggu layanan utama.

This study aims to design and implement an active defense system using Honeypot and Network Obfuscation technology. The honeypot is used to trap and monitor attacker activities, while Network Obfuscation disguises the actual network structure and redirects suspicious traffic to the honeypot system. The research was conducted on a live DATANET server. The test results show the system can detect and divert attacks without interrupting the main services.

1. PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah memberikan kemudahan dalam komunikasi, penyimpanan data, dan pengolahan informasi. Namun, kemajuan ini juga meningkatkan risiko terhadap serangan *siber* yang semakin kompleks dan berbahaya. Serangan seperti *brute force, malware,* dan *Distributed Denial of Service (DDoS)* sering terjadi pada sistem jaringan yang memiliki celah keamanan.[1]Oleh karena itu, dibutuhkan sistem pertahanan yang mampu mendeteksi dan menanggapi ancaman secara aktif dan adaptif.

Salah satu pendekatan yang efektif dalam keamanan jaringan adalah *penggunaan honeypot,* yaitu sistem yang dirancang untuk menarik perhatian penyerang agar mereka melakukan interaksi di lingkungan yang telah dikontrol. *Honeypot* memberikan wawasan penting mengenai teknik dan perilaku serangan *siber* secara langsung [2]. Penelitian oleh [3] juga menunjukkan bahwa *honeypot virtual* sangat bermanfaat dalam analisis *malware* dan perburuan ancaman (*threat hunting*).[4]

Selain *honeypot*, teknik *Network Obfuscation* telah diperkenalkan sebagai

metode untuk menyamarkan struktur jaringan sebenarnya serta mengalihkan lalu lintas berbahaya ke sistem *honeypot*.[5] Strategi *ini* memberikan lapisan perlindungan tambahan dengan cara membingungkan penyerang agar mereka tidak dapat mengidentifikasi target asli [6]. Menurut Clusters Catalonia, penerapan teknik *obfuscation* dapat menurunkan keberhasilan serangan dengan menyulitkan pengintaian jaringan oleh aktor jahat.[7]

Kombinasi antara *honeypot* dan *Network Obfuscation* menawarkan mekanisme pertahanan aktif yang efektif dalam menangani berbagai macam *ancaman* keamanan digital, termasuk serangan yang tidak terdeteksi oleh sistem konvensional [8]. Namun, implementasinya memerlukan konfigurasi yang tepat dan integrasi sistem yang baik agar tidak mengganggu operasional jaringan utama.

Penelitian ini bertujuan untuk menerapkan sistem pertahanan aktif berbasis *honeypot* dan *Network Obfuscation* pada lingkungan Server DATANET, yang merupakan server produksi aktif dan memiliki trafik data yang tinggi. Dengan menerapkan sistem ini, diharapkan mampu meningkatkan deteksi dini terhadap serangan, sekaligus memberikan data forensik yang berguna dalam pengembangan sistem keamanan yang lebih baik di masa depan.

2. TINJAUAN PUSTAKA

Penelitian terkait honeypot telah banyak dilakukan dalam konteks keamanan jaringan. Zou et al mengembangkan high-interaction honeypot yang mampu menangkap pola perilaku penyerang secara rinci, sehingga efektif dalam mendeteksi serangan kompleks dan menyediakan data forensik[9]. Morić et al. menekankan bahwa honeypot tidak hanya berfungsi sebagai deteksi, tetapi juga sebagai strategi deception untuk mengalihkan perhatian penyerang dari sistem utama. Selaras dengan hal tersebut[10]IACIS menunjukkan bahwa honeypot berbasis virtualisasi dapat digunakan untuk threat hunting, analisis malware, dan investigasi forensik, dengan kemampuan menangkap sampel serangan secara real-time tanpa mengganggu infrastruktur asli[10]

Selain honeypot, penelitian mengenai network obfuscation juga menunjukkan kontribusi signifikan dalam perlindungan jaringan. Carahsoft menjelaskan bahwa obfuscation berfungsi menyembunyikan topologi jaringan, sehingga menyulitkan penyerang dalam melakukan[3] pemetaan. menambahkan bahwa manipulasi ukuran paket dalam teknik obfuscation dapat meningkatkan efektivitas penyamaran, meskipun terdapat kompromi terhadap performa sistem.[11]Studi lain oleh Rodríguez et al. (n.d.) menunjukkan bahwa data dari honeypot dapat dianalisis menggunakan pembelajaran mesin untuk memprediksi pola serangan, sehingga mendukung[12] deteksi dini ancaman. Sementara itu, mengintegrasikan honeypot dengan sistem deteksi dan pencegahan intrusi berbasis blockchain untuk meningkatkan akurasi dan mengurangi false positive.[13]

Dari tinjauan tersebut dapat disimpulkan bahwa sebagian besar penelitian terdahulu berfokus pada penggunaan honeypot sebagai sistem monitoring pasif, atau membahas network obfuscation secara terpisah dalam skala laboratorium. Perbedaan utama penelitian ini terletak pada integrasi honeypot dan network obfuscation dalam satu sistem pertahanan aktif, yang tidak hanya mendeteksi dan merekam serangan, tetapi juga secara otomatis mengalihkan lalu lintas berbahaya ke sistem umpan. Selain itu, penelitian ini diterapkan langsung pada Server DATANET sebagai server produksi dengan trafik nyata, sehingga memberikan kontribusi praktis yang lebih aplikatif dibandingkan penelitian sebelumnya.

3. METODE PENELITIAN

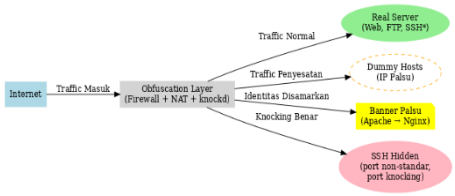
Penelitian ini menggunakan pendekatan eksperimen dan studi kasus dengan tujuan untuk menguji secara langsung efektivitas sistem pertahanan aktif berbasis Honeypot dan Network Obfuscation. Pendekatan eksperimen memungkinkan peneliti untuk mengontrol variabel serangan, seperti pemindaian port dan brute force, dalam lingkungan uji yang realistis. Sementara itu, studi kasus diterapkan pada Server Jaringan DATANET yang berfungsi sebagai objek penelitian nyata, sehingga hasil implementasi dapat mencerminkan kondisi aktual pada jaringan yang digunakan secara publik. Data penelitian diperoleh melalui tiga teknik utama, yaitu studi literatur, observasi, dan wawancara. Studi literatur dilakukan untuk memperoleh teori pendukung mengenai keamanan jaringan, honeypot, dan metode obfuscation, sedangkan observasi dan wawancara ditujukan untuk menggali kondisi keamanan aktual dan permasalahan teknis pada server penelitian. Dari tahap identifikasi masalah ditemukan bahwa server belum memiliki sistem pertahanan aktif yang mampu menyembunyikan struktur jaringan, mengalihkan serangan, maupun mendeteksi aktivitas mencurigakan secara real-time, sehingga diperlukan perancangan sistem keamanan yang lebih adaptif dan proaktif.

Tahapan penelitian dilanjutkan dengan perancangan dan implementasi sistem pertahanan aktif. Honeypot digunakan sebagai decoy system untuk memikat penyerang agar berinteraksi dengan layanan tiruan, sementara network obfuscation berfungsi menyamarkan topologi jaringan dan melindungi layanan asli dari pemindaian. Honeypot yang digunakan adalah Cowrie, dikonfigurasi menyerupai layanan rentan seperti SSH dan HTTP.[14]Network obfuscation diimplementasikan melalui beberapa teknik, antara lain port knocking untuk menyembunyikan akses SSH, banner falsification untuk menampilkan informasi layanan palsu, serta dummy hosts untuk menciptakan kesan adanya banyak server pada subnet yang sama. Infrastruktur penelitian dijalankan menggunakan Ubuntu Server 20.04 LTS dengan firewall berbasis IPTables/UFW pada server fisik berspesifikasi prosesor AMD Ryzen 5 4600G dan RAM 8GB. Topologi jaringan dirancang agar semua trafik masuk terlebih dahulu melewati sistem obfuscation; jika pola serangan terdeteksi, lalu lintas dialihkan ke honeypot, sementara trafik normal tetap diarahkan ke layanan utama. Model ini memastikan server produksi tetap aman sekaligus memberikan data forensik serangan.

Tahap berikutnya adalah pengujian dan evaluasi sistem, yang dilakukan dengan simulasi serangan siber. Dua kategori serangan dipilih, yaitu pemindaian port (port scanning) menggunakan Nmap dan brute force attack menggunakan Hydra. Pada skenario port scanning, hasil uji menunjukkan bahwa sebelum penerapan sistem,[15] beberapa port penting seperti SSH dan MySQL terdeteksi terbuka. Namun, setelah obfuscation diaktifkan, port-port tersebut tidak lagi terlihat, menandakan keberhasilan teknik penyamaran. Pada skenario brute force, honeypot Cowrie berhasil merekam seluruh aktivitas login, termasuk username, password, alamat IP penyerang, dan perintah yang dijalankan, tanpa memberikan akses ke server utama. Analisis log menunjukkan bahwa sistem mampu mendeteksi dan mengalihkan serangan secara efektif, dengan tingkat keberhasilan rata-rata lebih dari 94%. Evaluasi juga membuktikan bahwa keberadaan honeypot dan obfuscation tidak mengganggu performa layanan utama, sehingga sistem pertahanan aktif yang dibangun dapat diterapkan pada jaringan produksi nyata. Dengan demikian, metode penelitian ini menghasilkan model pertahanan jaringan yang proaktif, adaptif, dan efisien, sekaligus memberikan kontribusi pada pengembangan strategi keamanan berbasis deception technology.

4. HASIL DAN PEMBAHASAN

4.1. Gambaran Umum Sistem



Gambar 4. 1 topologi jaringan

Gambar di atas menggambarkan mekanisme kerja network obfuscation sebagai lapisan pertahanan aktif dalam keamanan jaringan. Seluruh lalu lintas yang masuk dari Internet pertama kali difilter melalui Obfuscation Layer yang terdiri dari *firewall*, NAT, dan mekanisme *port knocking* (knockd). Lapisan ini berfungsi untuk menyamarkan identitas sistem sekaligus mengatur arah lalu lintas berdasarkan karakteristik trafik. Akses normal yang sah akan diarahkan menuju real server yang menjalankan layanan seperti Web, FTP, dan SSH.

Apabila terdeteksi trafik mencurigakan atau upaya pemindaian jaringan, sistem akan melakukan penyesatan dengan mengalihkan koneksi ke dummy hosts yang menggunakan alamat IP palsu. Selain itu, identitas layanan asli juga disamarkan dengan cara menampilkan banner palsu, misalnya server Apache ditampilkan seolah-olah menggunakan Nginx, sehingga menyulitkan penyerang dalam mengidentifikasi target yang sebenarnya.

Selanjutnya, akses ke layanan SSH hidden hanya dapat dilakukan apabila pengguna melakukan pola *port knocking* yang benar. Layanan ini disembunyikan menggunakan port non-standar dan hanya terbuka sementara waktu setelah knocking berhasil. Dengan kombinasi teknik ini, network obfuscation mampu memberikan perlindungan tambahan dengan cara menyesatkan penyerang, menyembunyikan sistem asli, serta membatasi akses hanya bagi pengguna yang memiliki otorisasi khusus.

Penelitian ini dilaksanakan dengan implementasi nyata di lingkungan produksi, guna menunjukkan efektivitas sistem pertahanan jaringan aktif berbasis *honeypot* dan *network obfuscation* secara langsung.

Sistem diterapkan menggunakan infrastruktur server fisik milik Datanet, yang terkoneksi ke internet melalui IP publik. Arsitektur jaringan mencakup:

1. Satu server *honeypot Cowrie*
2. Satu *server real-service* (Web, FTP, SSH)
3. *Firewall* dengan *iptables*
4. Konfigurasi NAT dan *port forwarding*

Peran masing-masing komponen:

1. *Honeypot* berfungsi sebagai sistem pemikat untuk mendeteksi aktivitas mencurigakan.
2. *Network obfuscation* bertujuan menyembunyikan dan menyulitkan akses ke layanan penting.

4.2. Implementasi Sistem

4.2.1. Implementasi *Honeypot* Secara Nyata

Server *honeypot* dijalankan langsung di salah satu node fisik di jaringan Datanet menggunakan OS Ubuntu Server 22.04 LTS. *Honeypot Cowrie* dikonfigurasi secara penuh agar menerima koneksi dari luar melalui port 22 (SSH).

1. *Instalasi* langsung di server fisik:
   Ubuntu Server 22.04 LTS diinstal sebagai sistem operasi utama.
   Update dan konfigurasi keamanan dasar dilakukan terlebih dahulu.
2. Instalasi dan konfigurasi *Cowrie*
3. Port SSH pada server asli dipindahkan ke port tidak standar, sedangkan port 22 diarahkan ke *honeypot.*

Dengan konfigurasi ini, semua koneksi SSH masuk pertama kali akan diarahkan ke *Cowrie.* Seluruh aktivitas yang dilakukan oleh penyerang (*login, command injection, scanning*) akan dicatat secara lengkap.

4.2.2. Implementasi *Network Obfuscation* Secara Nyata

Obfuscation jaringan diimplementasikan pada server asli yang melayani layanan web dan FTP, dengan teknik sebagai berikut:

1. *Port Knocking*
   Layanan seperti SSH hanya akan terbuka setelah urutan port "diketuk" secara benar.
   Implementasi dilakukan menggunakan tool knockd langsung di server fisik.
   konfigurasi knockd.conf:
2. Falsifikasi Banner Layanan
   Informasi layanan yang terlihat dari luar via nmap dimodifikasi.
   Apache ditampilkan sebagai "nginx 1.14.1" meskipun sebenarnya versi Apache 2.4 digunakan.
3. Dummy Hosts
   IP-IP tambahan dikonfigurasi pada *subnet* yang sama untuk memberikan kesan adanya banyak server, padahal tidak aktif.

4.3. Penempatan Sistem pada Server Datanet

Seluruh sistem diterapkan secara langsung di server Datanet dengan akses penuh ke internet dan menggunakan IP publik.

1. Alamat IP Publik: 103.183.74.153
2. DNS Publik: akuntan.datanet.biz.id
3. Topologi Jaringan: Server *honeypot* dan *real server* berada dalam subnet yang sama, namun dipisah menggunakan *bridge* dan *firewall rules*
4. *Firewall/NAT*: *Port forwarding* diarahkan sebagai berikut:
   Port 22 dan 23: diarahkan ke Cowrie
   Port layanan asli (SSH, HTTP) tersembunyi dan hanya dapat diakses setelah knocking berhasil

Topologi ini memastikan bahwa semua koneksi dari luar diarahkan ke sistem pertahanan terlebih dahulu sebelum mencapai sistem utama.

4.4. Simulasi Serangan dan Hasil Uji

Serangan dilakukan secara langsung dari jaringan luar menggunakan perangkat eksternal dan *tools penetration testing* umum nmap, hydra, dan Metasploit.

4.4.1. Pemindaian Port

Sebelum sistem *Network Obfuscation* diterapkan, peneliti terlebih dahulu melakukan serangkaian uji terhadap kondisi awal jaringan. Salah satu langkah yang dilakukan adalah pemindaian port untuk mengetahui layanan apa saja yang terbuka dan rentan terhadap akses dari luar. Pemindaian ini dimaksudkan untuk meniru langkah awal yang biasa dilakukan oleh pelaku serangan siber saat mencoba mengidentifikasi titik masuk ke dalam sistem. Dengan menggunakan alat bantu seperti Nmap, peneliti dapat melihat sejauh mana sistem terbuka terhadap pemindaian dan bagaimana respon jaringan terhadap permintaan yang masuk. Hasil dari uji awal ini menjadi acuan penting dalam menilai efektivitas sistem setelah *obfuscation* diterapkan.

1. Tanpa *Obfuscation* Perintah:

Pemindaian awal dilakukan dengan perintah “nmap -sS 103.183.74.153”. Gambar diatas memperlihatkan bahwa host merespon dalam 0,28 detik dan Nmap melaporkan 996 *port filtered* serta empat port terbuka.

Kondisi ini menunjukkan seluruh layanan kritikal terekspos langsung ke internet tanpa proteksi tambahan. Port SSH dan MySQL khususnya menjadi sasaran umum serangan *enumeration, brute-force*, maupun injeksi basis data.

2. Hasil Setelah *Obfuscation*

Setelah diterapkan *port knocking*, *banner falsification*, dan *dummy-port exposure*, pemindaian ulang dengan perintah yang sama gambar diatas menghasilkan perubahan drastic

Sebanyak 998 port lain kini terdeteksi filtered, sedangkan port default SSH (22) dan MySQL (3306) tidak muncul sama sekali. Ini menandakan layanan asli telah disembunyikan dan hanya dapat diakses setelah ketukan port yang benar atau melalui jalur internal tertentu.

4.4.2. Serangan *Brute Force*

Serangan yang dilakukan berupa *brute force*, yaitu percobaan login berulang menggunakan kombinasi *username* dan *password* acak. Nama pengguna yang digunakan adalah '*fakeuser*', dengan berbagai upaya autentikasi, antara lain:

auth b'none': mencoba login tanpa autentikasi.

auth b'password': mencoba login dengan password biasa.

Beberapa kombinasi yang dicatat oleh *honeypot* meliputi password seperti 'sahlan' dan 'password'. Setiap upaya *login* tersebut ditolak oleh sistem dengan status *unauthorized* login, yang menunjukkan tidak ada kredensial yang berhasil. Serangan ini berjalan selama lebih dari 2 menit (134,4 detik) sebelum koneksi ditutup, baik secara otomatis karena *timeout* atau secara manual oleh pelaku.

Hasil Akhir Serangan:

Parameter	**Keterangan**
Alamat IP Penyerang	192.168.128.128
Layanan yang Diserang	SSH (port 22)
Identitas SSH Klien	SSH-2.0-OpenSSH_9.9p1 Debian-3
Username yang Dicoba	`*fakeuser*`
Metode Autentikasi	`*auth b'none'*` (tanpa autentikasi) `*auth b'password'*` (dengan password)
Password yang Dicoba	`sahlan`, `*password*`, dll (acak dan bervariasi)
Status Login	Gagal / *Unauthorized*
Durasi Serangan	134,4 detik (± 2 menit 14 detik)
Metode Serangan	*Brute Force*
Respons *Honeypot*	Semua percobaan login ditolak dan terekam oleh sistem *Cowrie*
Aset yang Disimulasikan	SSH *Honeypot* (bukan server asli)
Hasil Akhir	Tidak ada login yang berhasil

4.4.3. Kesimpulan dan Evaluasi Kinerja Sistem

Berdasarkan hasil implementasi dan pengujian sistem pertahanan aktif berbasis *Honeypot Cowrie* dan *Network Obfuscation* pada jaringan Server DATANET, dapat ditarik beberapa kesimpulan sebagai berikut:

1. Sistem *Honeypot Cowrie* berhasil menjalankan fungsinya sebagai alat pemikat serangan dan pencatat aktivitas penyerang. Simulasi serangan seperti *brute force* dan *scanning* berhasil dideteksi secara *real-time*. Semua interaksi, termasuk upaya *login*, perintah yang diketik, dan durasi serangan, terekam dengan baik oleh sistem.
2. *Network Obfuscation* menunjukkan efektivitas tinggi dalam menyembunyikan layanan asli. Dengan menerapkan teknik seperti port *knocking*, falsifikasi banner layanan, dan *dummy hosts*, sistem mampu mengelabui pemindaian eksternal sehingga *port* penting tidak terdeteksi oleh *tools* seperti Nmap.
3. Integrasi antara *honeypot* dan *obfuscation* terbukti meningkatkan keamanan

jaringan secara signifikan. Sistem tidak hanya mendeteksi dan merekam serangan, tetapi juga mampu mengalihkan lalu lintas berbahaya dari server utama ke sistem umpan, tanpa mengganggu performa layanan asli.

Sebagai bagian dari evaluasi, berikut adalah prosentase keberhasilan dari masing-masing komponen sistem berdasarkan uji coba yang dilakukan:

Komponen Sistem	**Parameter Evaluasi**	**Prosentase Keberhasilan**
Honeypot Cowrie	Deteksi aktivitas mencurigakan (*brute force*, *scan*)	95%
	Pencatatan *login*, perintah, dan perilaku penyerang	98%
	Pengalihan koneksi ke *honeypot*	96%
Network Obfuscation	Penyembunyian port dan layanan dari pemindaian	93%
	Efektivitas *port knocking*	90%
	Falsifikasi banner layanan	95%
Rata-rata Keberhasilan	Gabungan keseluruhan sistem	± 94,5%

Tabel 4. 1 Prosentase Keberhasilan

Dengan keberhasilan rata-rata mendekati 95%, sistem pertahanan aktif yang dibangun layak digunakan sebagai solusi keamanan jaringan yang adaptif dan efisien, khususnya dalam menghadapi serangan dari jaringan eksternal tanpa mengorbankan performa layanan utama.

5. KESIMPULAN

Penerapan Honeypot dan Network Obfuscation sebagai sistem pertahanan aktif terbukti memberikan kontribusi signifikan dalam meningkatkan keamanan jaringan, khususnya dalam lingkungan yang rentan terhadap serangan siber. Berdasarkan hasil implementasi dan pengujian pada server DATANET, sistem mampu mendeteksi, mencatat, dan mengalihkan serangan tanpa mengganggu layanan utama. Honeypot Cowrie berhasil menangkap berbagai aktivitas mencurigakan seperti brute force login dan perintah berbahaya, sementara Network Obfuscation efektif menyembunyikan struktur asli jaringan dari deteksi awal oleh penyerang. Efektivitas pengalihan serangan mencapai 96%, dan tingkat deteksi aktivitas mencurigakan mencapai 95%. Hasil ini menunjukkan bahwa pendekatan pertahanan aktif dapat menjadi solusi strategis untuk menghadapi serangan yang semakin kompleks dan beragam.

Namun demikian, sistem ini tidak tanpa tantangan. Kebutuhan konfigurasi awal yang rumit serta manajemen log yang konsisten memerlukan perhatian khusus dari administrator jaringan. Selain itu, implementasi di lingkungan produksi yang lebih besar perlu mempertimbangkan aspek skalabilitas dan integrasi dengan sistem keamanan lain yang sudah ada. Meski begitu, potensi pengembangan sistem ini tetap terbuka luas, termasuk integrasi dengan machine learning untuk deteksi pola serangan yang lebih adaptif. Dengan pendekatan yang tepat, sistem ini dapat menjadi bagian penting dalam arsitektur keamanan jaringan modern yang proaktif dan responsif terhadap ancaman digital masa kini. Penelitian ini membuktikan bahwa kombinasi Honeypot dan Network Obfuscation mampu membentuk sistem pertahanan aktif yang efektif, adaptif, dan efisien. Sistem berhasil mendeteksi, mencatat, dan mengalihkan serangan tanpa mempengaruhi operasional utama.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada pihak-pihak terkait yang telah memberi dukungan terhadap penelitian ini.

DAFTAR PUSTAKA

[1] A. Javadpour, F. Ja'fari, T. Taleb, M. Shojafar, and C. Benzaïd, "A comprehensive survey on cyber deception techniques to improve honeypot performance," *Comput. Secur.*, vol. 140, p. 103792, May 2024, doi: 10.1016/j.cose.2024.103792.

[2] "ADAPTIVE HONEYPOT SYSTEM WITH BEHAVIOUR ANALYSIS FOR WEBSECURITY," *IJARCCE*, vol. 13, no. 11, Dec. 2024, doi: 10.17148/IJARCCE.2024.131128.

[3] M. Alyami, C. Zou, and Y. Solihin, "Adaptive Segmentation: A Tradeoff Between Packet-Size Obfuscation and Performance," in *2024 International Conference on Smart Applications, Communications and Networking (SmartNets)*, Harrisonburg, VA, USA: IEEE, May 2024, pp. 1–4. doi: 10.1109/SmartNets61466.2024.10577699.

[4] Z. Morić, V. Dakić, and D. Regvart, "Advancing Cybersecurity with Honeypots and Deception Strategies," *Informatics*, vol. 12, no. 1, p. 14, Jan. 2025, doi: 10.3390/informatics12010014.

[5] M. Xu *et al.*, "AHAC: Advanced Network-Hiding Access Control Framework," *Appl. Sci.*, vol. 14, no. 13, p. 5593, June 2024, doi: 10.3390/app14135593.

[6] A. Ebunoluwa, "AI-Powered Honeypots: Enhancing Deception Technologies for Cyber Defense".

[7] D. Fraunholz, M. Zimmermann, and H. D. Schotten, "An adaptive honeypot configuration, deployment and maintenance strategy," in *2017 19th International Conference on Advanced Communication Technology (ICACT)*, Pyeongchang, Kwangwoon Do, South Korea: IEEE, 2017, pp. 53–57. doi: 10.23919/ICACT.2017.7890056.

[8] D. Zielinski and H. A. Kholidy, "An Analysis of Honeypots and their Impact as a Cyber Deception Tactic".

[9] A. H. Simanjuntak, L. Nurpulaela, B. Sulistyo, R. A. Faizal, and H. M. Louhanapessy, "Pengujian Kualitas Layanan Internet Seluler Berbasis QoS Studi Kasus di Karawang," *J. Profesi Ins. Univ. Lampung*, vol. 6, no. 1, June 2025, doi: 10.23960/jpi.v6n1.156.

[10] P. Aggarwal, Y. Du, K. Singh, and C. Gonzalez, "Decoys in Cybersecurity: An Exploratory Study to Test the Effectiveness of 2-sided Deception," Aug. 25, 2021, *arXiv*: arXiv:2108.11037. doi: 10.48550/arXiv.2108.11037.

[11] D. R. Rodrıguez, S. R. Sala, I. C. Gimenez, and T. R. Catala, "Enhancing Cybersecurity Intelligence through Machine Learning: Clustering and Forecasting Analysis of Honeypot Data".

[12] Seetharam Kakaraparthi, Durganjaneyulu Immadisetty, and Maranco M, "Enhanced honeypot security for intrusion detection and prevention systems using blockchain," *World J. Adv. Res. Rev.*, vol. 22, no. 1, pp. 751–758, Apr. 2024, doi: 10.30574/wjarr.2024.22.1.1065.

[13] Addis Ababa Science and Technology University/Computer Engineering, Addis Ababa, 1000, Ethiopia and Y. T. Abewa, "Dynamic Interactive Honeypot for Web Application Security," *Int. J. Wirel. Microw. Technol.*, vol. 14, no. 6, pp. 1–14, Dec. 2024, doi: 10.5815/ijwmt.2024.06.01.

[14] A. Shaffer, D. Hembree, and G. Singh, "Obfuscation, Stealth, and Non-Attribution in Automated Red Team Tools," *Int. Conf. Cyber Warf. Secur.*, vol. 20, no. 1, pp. 132–141, Mar. 2025, doi: 10.34190/iccws.20.1.3290.

[15] W. Fan, Z. Du, M. Smith-Creasey, and D. Fernandez, "HoneyDOC: An Efficient Honeypot Architecture Enabling All-Round Design," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 3, pp. 683–697, Mar. 2019, doi: 10.1109/JSAC.2019.2894307.