

Munawaroh, S.Kom,M.Kom  
Chandra Insan Prasetyo, S.Kom



# ***OPTIMASI HONEYPOT T-POT***

***MENGGUNAKAN PORT KNOCKING SEBAGAI PENDETEKSI  
SERANGAN DALAM JARINGAN KOMPUTER***

# OPTIMASI HONEYPOT T-POT

MENGGUNAKAN PORT KNOCKING SEBAGAI PENDETEKSI  
SERANGAN DALAM JARINGAN KOMPUTER

Honeypot adalah suatu sistem atau perangkat lunak yang dirancang untuk menarik perhatian penyerang dan merekam aktivitas yang mencurigakan atau serangan terhadap jaringan komputer. T-Pot adalah sebuah proyek honeypot open-source yang menciptakan lingkungan simulasi yang menarik bagi penyerang. Penelitian ini bertujuan untuk mengoptimalkan keefektifan honeypot T-Pot dengan mengimplementasikan teknik keamanan tambahan, khususnya menggunakan port knocking sebagai metode deteksi serangan.

Port knocking adalah teknik di mana penyerang harus "memukul" atau melakukan urutan akses pada sejumlah port tertentu untuk membuka akses ke sistem. Dalam konteks honeypot, port knocking dapat diimplementasikan sebagai lapisan tambahan untuk mendeteksi pola akses yang mencurigakan atau tidak lazim.

Langkah-langkah optimasi honeypot T-Pot menggunakan port knocking melibatkan:  
Implementasi Port Knocking:

Mengintegrasikan mekanisme port knocking ke dalam honeypot T-Pot untuk memeriksa apakah ada upaya akses yang sesuai dengan pola knocking yang ditentukan.

Konfigurasi Pola Knocking:

Menentukan pola knocking yang aman dan sesuai dengan kebutuhan lingkungan jaringan. Pola ini dapat terdiri dari urutan akses pada sejumlah port yang harus diikuti untuk membuka akses.

Pemantauan Aktivitas Port Knocking:

Memonitor dan mencatat aktivitas port knocking untuk menganalisis pola akses yang mencurigakan atau tidak wajar. Hal ini dapat melibatkan analisis waktu, frekuensi, dan variasi pola knocking.

Respons Terhadap Pola Tidak Wajar:

Mengimplementasikan respons otomatis atau pemberitahuan kepada administrator jika terdeteksi pola knocking yang mencurigakan. Respons ini dapat mencakup peningkatan tingkat keamanan atau tindakan mitigasi yang sesuai.

Evaluasi dan Peningkatan:

Melakukan evaluasi periodik terhadap efektivitas port knocking dalam mendeteksi serangan. Jika diperlukan, melakukan penyesuaian atau peningkatan terhadap konfigurasi dan kebijakan port knocking.



eureka  
media aksara  
Anggota IKAPI  
No. 225/JTE/2021

0858 5343 1992  
eurekamediaaksara@gmail.com  
Jl. Banjaran RT.20 RW.10  
Bojongsari - Purbalingga 53362

ISBN 978-623-151-920-7



9 786231 519207

# OPTIMASI HONEYPOT T-POT MENGUNAKAN PORT KNOCKING SEBAGAI PENDETEKSI SERANGAN DALAM JARINGAN KOMPUTER

Munawaroh, S.Kom, M.Kom  
Chandra Insan Prasetyo, S.Kom



**eureka**  
media aksara

PENERBIT CV.EUREKA MEDIA AKSARA

**OPTIMASI HONEYPOT T-POT MENGGUNAKAN PORT  
KNOCKING SEBAGAI PENDETEKSI SERANGAN DALAM  
JARINGAN KOMPUTER**

**Penulis** : Munawaroh, S.Kom, M.Kom  
Chandra Insan Prasetyo, S.Kom

**Desain Sampul** : Ardyan Arya Hayuwaskita

**Tata Letak** : Meilita Anggie Nurlatifah

**ISBN** : 978-623-151-920-7

Diterbitkan oleh : **EUREKA MEDIA AKSARA, NOVEMBER 2023**  
**ANGGOTA IKAPI JAWA TENGAH**  
**NO. 225/JTE/2021**

**Redaksi:**

Jalan Banjaran, Desa Banjaran RT 20 RW 10 Kecamatan Bojongsari  
Kabupaten Purbalingga Telp. 0858-5343-1992  
Surel : eurekamediaaksara@gmail.com  
Cetakan Pertama : 2023

**All right reserved**

Hak Cipta dilindungi undang-undang  
Dilarang memperbanyak atau memindahkan sebagian atau seluruh  
isi buku ini dalam bentuk apapun dan dengan cara apapun,  
termasuk memfotokopi, merekam, atau dengan teknik perekaman  
lainnya tanpa seizin tertulis dari penerbit.

## KATA PENGANTAR

Alhamdulillah, segala puji bagi Allah yang telah memberikan segala bimbingan-Nya kepada penulis untuk menyelesaikan buku optimasi honeypot t-pot menggunakan port knocking sebagai pendeteksi serangan dalam jaringan komputer ini. Buku ini dipergunakan sebagai Referensi Jaringan Komputer bagi yang ingin memperluas ilmu mengenai jaringan komputer. Sasaran dari Jaringan Komputer ini adalah memberikan pengetahuan kepada mahasiswa dan khalayak umum tentang optimasi honeypot t-pot menggunakan port knocking sebagai pendeteksi serangan dalam jaringan komputer mulai dari instalasi sistem operasi, perintah-perintah dasar Linux sampai dengan membangun internet server yang meliputi mail server, DNS server, web server, proxy server, dan lain sebagainya. Selain itu buku ini dapat digunakan sebagai panduan bagi mahasiswa atau khalyak umum saat melaksanakan penelitian mengenai jarigan komputer tersebut. Penulis menyadari bahwa buku ini jauh dari sempurna, oleh karena itu penulis akan memperbaikinya secara berkala.Saran dan kritik untuk perbaikan buku ini sangat kami harapkan. Akhir kata, semoga buku ini bermanfaat bagi mahasiswa dan khalayak umum dalam mempelajari Jaringan Komputer. Amin.

Pamulang, 26 November 2023

Penulis

## DAFTAR ISI

<b>KATA PENGANTAR.....</b>	<b>iii</b>
<b>DAFTAR ISI.....</b>	<b>iv</b>
<b>DAFTAR GAMBAR.....</b>	<b>v</b>
<b>DAFTAR TABEL .....</b>	<b>viii</b>
<b>BAB 1 PENDAHULUAN.....</b>	<b>1</b>
<b>BAB 2 LANDASAN TEORI.....</b>	<b>5</b>
A. Dasar Teori .....	7
<b>BAB 3 METODE PENELITIAN.....</b>	<b>62</b>
A. Pengumpulan Data.....	63
B. Analisa Penelitian .....	63
C. Persiapan .....	65
D. Perancangan Jaringan.....	66
E. Instalasi.....	68
F. Pengujian.....	72
<b>BAB 4 ANALISA PENGUJIAN.....</b>	<b>76</b>
A. Implementasi Mesin Virtualisasi.....	76
B. Implementasi Jaringan dan Sistem.....	83
C. Pengujian Sistem.....	94
D. Pengujian Serangan .....	102
E. Hasil Pengujian Sistem dan Serangan.....	106
F. Pembahasan .....	112
<b>BAB 5 PENUTUP.....</b>	<b>114</b>
A. Kesimpulan .....	114
B. Saran .....	114
<b>DAFTAR PUSTAKA.....</b>	<b>115</b>
<b>TENTANG PENULIS.....</b>	<b>118</b>

## DAFTAR GAMBAR

Gambar 2. 1. Aspek Keamanan Informasi .....	9
Gambar 2. 2. Clearing Tracks .....	16
Gambar 2. 3. TCP/IP Layer.....	44
Gambar 2. 4. Port Knocking .....	53
Gambar 2. 5. 5 Tampilan GNS3.....	56
Gambar 2. 6. VMware Workstation.....	57
Gambar 2. 7. Metasploit.....	59
Gambar 3. 1. Diagram Alir Penelitian .....	62
Gambar 3. 2. Arsitektur Honeypot T-Pot.....	63
Gambar 3. 3. Topologi jaringan.....	67
Gambar 3. 4. Integrasi Perangkat Lunak.....	68
Gambar 3. 5. Instalasi Ubuntu Server 20.40.....	69
Gambar 3. 6. Dashboard Web UI Honeypot T-Pot.....	70
Gambar 3. 7. Instalasi Kali Linux.....	71
Gambar 3. 8. Instalasi Router OS Mikrotik.....	71
Gambar 3. 9. Diagram Alir Pengujian Sistem.....	72
Gambar 3. 10. Skenario Pengujian .....	74
Gambar 4. 1. Instalasi VMware Workstation.....	76
Gambar 4. 2. Tampilan VMware Workstation .....	77
Gambar 4. 3. Instalasi GNS3.....	77
Gambar 4. 4. Tampilan GNS3 .....	78
Gambar 4. 5. Topologi Virtualisasi Jaringan.....	78
Gambar 4. 6. Konfigurasi Virtualisasi Pada Server .....	79
Gambar 4. 7. Script Website Utama.....	79
Gambar 4. 8. Konfigurasi Default Port SSH Web Server .....	80
Gambar 4. 9. Tampilan Server Honeypot T-Pot .....	81
Gambar 4. 10. Konfigurasi Virtualisasi Pada Router .....	81
Gambar 4. 11. Instalasi Router OS Mikrotik .....	82
Gambar 4. 12. Konfigurasi Virtualisasi Pada Client Penyerang ...	82
Gambar 4. 13. Instalasi Kali Linux.....	83
Gambar 4. 14. Konfigurasi Mikrotik.....	84
Gambar 4. 15. Konfigurasi DHCP Server.....	84
Gambar 4. 16. Network Interface.....	85
Gambar 4. 17. Static IP Server .....	85

Gambar 4. 18. Konfigurasi Firewall .....	87
Gambar 4. 19. Konfigurasi Anti DDoS.....	88
Gambar 4. 20. Konfigurasi Port Knocking.....	89
Gambar 4. 21. Landing Page Honeypot T-Pot .....	90
Gambar 4. 22. Admin Menu Honeypot T-Pot.....	90
Gambar 4. 23. Halaman Utama Honeypot T-Pot.....	91
Gambar 4. 24. Konfigurasi SFTP .....	92
Gambar 4. 25. Akses SFTP .....	92
Gambar 4. 26. Instal Apache2.....	93
Gambar 4. 27. Direktori Penyimpanan Website Utama .....	93
Gambar 4. 28. File index.html.....	93
Gambar 4. 29. Pengujian Jaringan Router Mikrotik .....	94
Gambar 4. 30. Pengujian Jaringan Web Server .....	94
Gambar 4. 31. Pengujian Jaringan Server Honeypot .....	95
Gambar 4. 32. Pengujian Konektifitas Router Mikrotik .....	95
Gambar 4. 33. Pengujian Konektifitas Web Server .....	96
Gambar 4. 34. Pengujian Halaman Website Utama.....	96
Gambar 4. 35. Pengujian Konektifitas Server Honeypot T-Pot .....	97
Gambar 4. 36. Pengujian Halaman Admin Honeypot T-Pot.....	97
Gambar 4. 37. Pengujian Update Web Server .....	98
Gambar 4. 38. Pengujian Update Web Server .....	98
Gambar 4. 39. Update Honeypot T-Pot .....	99
Gambar 4. 40. Update System Honeypot T-Pot .....	99
Gambar 4. 41. Akses port 14022 Tanpa Knocking .....	100
Gambar 4. 42. Akses Mikrotik Tanpa Knocking .....	100
Gambar 4. 43. Proses Knocking .....	101
Gambar 4. 44. Akses Port 14022 Dengan Knocking.....	101
Gambar 4. 45. Akses Mikrotik Dengan Knocking .....	102
Gambar 4. 46. Akses Website Pengujian Serangan .....	102
Gambar 4. 47. Scanning Port.....	103
Gambar 4. 48. Serangan DDoS Menggunakan LOIC .....	104
Gambar 4. 49. List Username dan Password Serangan.....	104
Gambar 4. 50. Serangan Menggunakan Hydra.....	105
Gambar 4. 51. Akses SSH Server .....	106
Gambar 4. 52. Firewall Tanpa Knocking .....	107
Gambar 4. 53. Firewall Dengan Knocking.....	108



Gambar 4. 54. Firewall Connection Setelah Knocking.....	108
Gambar 4. 55. Blokir Serangan DDoS.....	109
Gambar 4. 56. Resource Server Utama .....	109
Gambar 4. 57. Website Server Utama Saat Proses Serangan .....	109
Gambar 4. 58. Record Serangan Honeypot T-Pot.....	110
Gambar 4. 59. Password Record Serangan .....	111
Gambar 4. 60. Cockpit Honeypot T-Pot.....	111
Gambar 4. 61. Web Admin Honeypot T-Pot.....	112

## DAFTAR TABEL

Tabel 3. 1. Service dan Port Honeypot T-Pot .....	64
Tabel 3. 2. Pengalamatan IP .....	66
Tabel 4. 1. Hasil Pengujian Sistem.....	112
Tabel 4. 2. Hasil Pengujian Serangan.....	113

# BAB 1

## PENDAHULUAN

Internet sudah menjadi bagian dari kehidupan bagi sebagian besar penduduk dunia. Dari urusan mencari informasi, bekerja, belanja maupun bersosial media untuk menyapa teman, kerabat maupun keluarga. Berdasarkan data *internetworldstats*, pengguna internet Indonesia mencapai 212,35 juta jiwa pada Maret 2021. Dengan jumlah tersebut, Indonesia berada di urutan ketiga dengan pengguna internet terbanyak di Asia. Hampir semua fungsi dapat dilakukan di dunia menggunakan internet, seperti bisnis, perbankan, pendidikan, pemerintahan, kesehatan dan masih banyak lainnya. Kemudahan dan fasilitas yang ditawarkan oleh jaringan berbasis internet ini menjadikan kebutuhan utama yang tidak bisa dipisahkan dari kehidupan sehari-hari baik secara individu ataupun organisasi.

Banyak organisasi atau perusahaan yang kemudian melibatkan teknologi informasi dan internet sebagai bagian yang tak terpisahkan dari aktivitas operasionalnya, tentunya hal ini akan menimbulkan dampak teror yang luar biasa terhadap penyerangan sistem jaringan dan komputer yang dimiliki. Banyak jenis kejahatan siber terjadi dikarenakan rendahnya sistem keamanan yang diterapkan, sehingga pelaku berupaya mengakses data secara tidak sah, mengganggu operasi digital atau merusak informasi. Ancaman dunia maya ini bisa berasal dari berbagai hal termasuk mata-mata perusahaan, peretas (*hacker*), kelompok teroris, organisasi kriminal hingga karyawan yang merasa tidak puas dengan perusahaan. Dilansir dari portal berita CNN Indonesia (2022), Indonesia sendiri masuk dalam jajaran 10 besar kasus kebocoran data tertinggi pada

# BAB 2

## LANDASAN TEORI

Untuk melakukan pengembangan yang lebih lanjut, pendalaman kajian terhadap penelitian yang telah dilakukan sebelumnya sangat dibutuhkan. Hasil dari kajian tersebut kemudian akan digunakan sebagai dasar pengetahuan awal untuk pengembang dan inovasi dari penelitian.

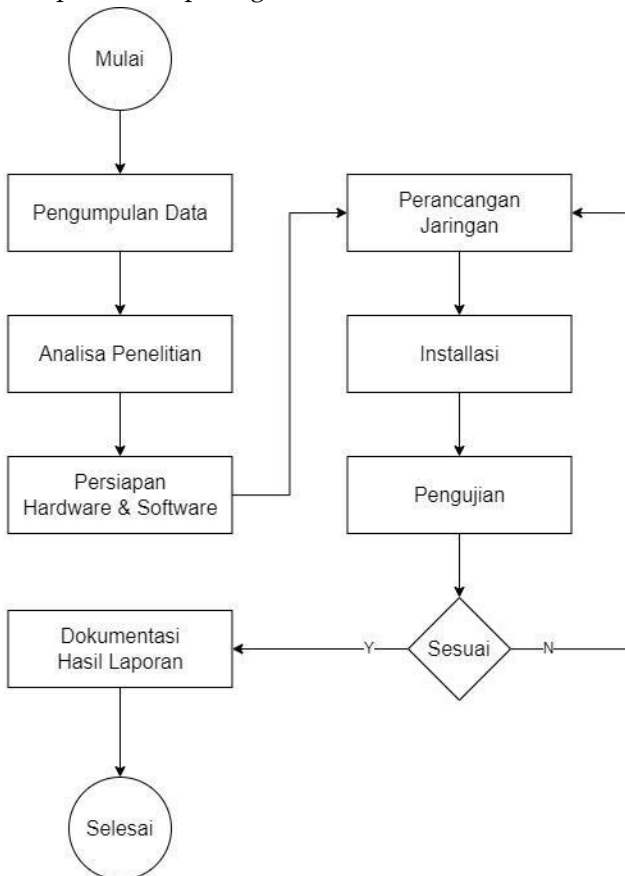
Pada penelitian yang dilakukan oleh (Fitri & Dian Nathasia, 2018) melakukan uji coba keamanan menggunakan metode Port Knocking dan Honeypot sebagai keamanan jaringan pada server. Port Knocking dapat didefinisikan sebagai suatu komunikasi antara dua komputer, sedangkan Honeypot sebagai pengalihan agar intruder (penyusup) masuk ke server tiruan, dengan Honeypot bisa melihat log/aktifitas yang dikerjakan oleh intruder terhadap server. Dalam uji coba penyerangan server digunakan dua aplikasi yaitu Putty dan Moba Xtreem sehingga didapatkan hasil uji coba yaitu, uji coba pertama menggunakan aplikasi Putty dan didapatkan hasil yaitu intruder (penyusup) berhasil dialihkan ke server bayangan. Pada uji coba ini intruder/penyusup mencoba me-remote dengan menggunakan port 22,8000, dan 9000 dengan menggunakan IP Address 192.168.43.231. Pada uji coba ini, intruder/penyusup berhasil dialihkan ke server bayangan atau server Honeypot. Pada server Honeypot ini intruder/penyusup mencoba log in dengan user root dan seolah-olah penyusup berhasil masuk ke server utama dan penyusup membuat folder pada server Honeypot.

Penelitian yang dilakukan (Budiono, 2019) dengan judul “Rancang Bangun Sistem Monitoring Keamanan Jaringan”. Menggunakan Cowrie Honeypot berbasis Web. Sedangkan

# BAB 3

## METODE PENELITIAN

Terdapat beberapa langkah-langkah atau proses yang akan dilakukan dalam penelitian ini. Langkah-langkah dan proses tersebut dapat dilihat pada gambar berikut:



Gambar 3. 1. Diagram Alir Penelitian

# BAB 4

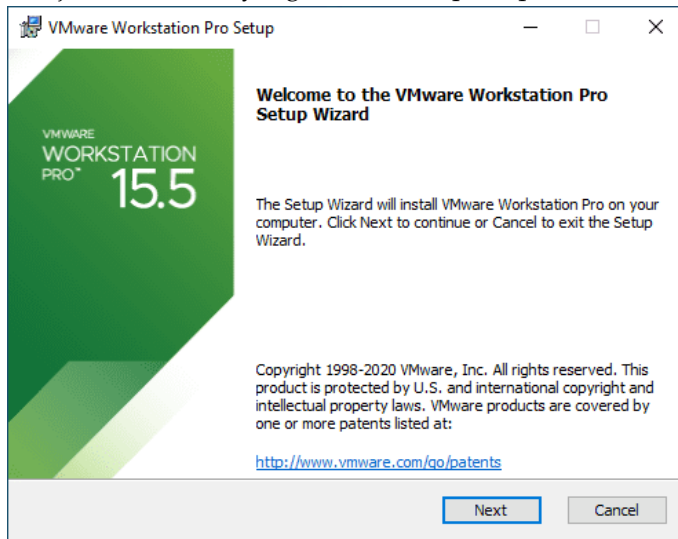
## ANALISA PENGUJIAN

### A. Implementasi Mesin Virtualisasi

Mesin Virtualisasi adalah Software virtualisasi yang berguna untuk menjalankan sistem operasi lain di dalam sistem operasi utama. Pada penelitian ini, sisi client dan server akan dibuat menggunakan bantuan mesin virtualisasi.

#### 1. Virtualisasi Server

Mesin virtualisasi untuk menjalankan sistem operasi menggunakan VMware Workstation Pro dengan versi 15.5 yang nantinya akan dipasangkan sistem operasi untuk menjalankan servis yang dibutuhkan pada penelitian ini.



Gambar 4. 1. Instalasi VMware Workstation

# BAB

# 5

# PENUTUP

## A. Kesimpulan

Berdasarkan hasil perancangan dan pengujian serangan yang telah dilakukan, dapat disimpulkan bahwa:

1. Dengan adanya penambahan perancangan metode Port Knocking, dan Honeypot T-Pot dapat meningkatkan keamanan pada server maupun keamanan jaringan.
2. Berdasarkan hasil pengujian metode Port Knocking dapat memblokir akses yang tidak di izinkan yang mencoba masuk ke sistem jaringan. Sistem Honeypot T-Pot juga dapat mengalihkan akses serangan yang dilakukan, serta memberikan laporan pola aktifitas serangan yang terjadi pada server dan jaringan yang di tampilkan pada web console guna menjadi bahan pengembangan sistem keamanan.

## B. Saran

Terdapat beberapa saran yang dapat dijadikan bahan pertimbangan untuk pengembangan penelitian ini adalah:

1. Menambah aturan pada sistem untuk memberikan respon terhadap penyerang pada Honeypot T-Pot
2. Peningkatan spesifikasi server yang digunakan untuk menjalankan Honeypot T-Pot untuk meingkatkan kinerja penanganan jika terdapat banyak serangan dalam waktu yang bersamaan.

## DAFTAR PUSTAKA

- Arif setiadi, P. H. (2021). Manajemen Pada Jaringan Mikrotik Menggunakan Metode Hierarchical Token Bucket (HTB) dan Keamanan Firewall Intrusion Detection System. JARKOM, Vol. 9, No. 1 , 1-9.
- Budiono, Adhima Arisandi. (2019). Rancang Bangun Sistem Monitoring Keamanan Jaringan Menggunakan Cowrie Honeypot Berbasis Web. Vocational (Diploma) thesis, University of Muhammadiyah Malang.
- Cloud Computing Indonesia. (2022). Kaspersky Mencatat Indonesia Hadapi 11 Juta Serangan Siber pada Kuartal Pertama 2022. Retrieved from <https://www.cloudcomputing.id/berita/kaspersky-mencatat-indonesia-hadapi-serangan-siber>.
- CNN Indonesia. (2022). Kasus Kebocoran 1,3 Miliar Data di RI Disebut Terbesar di Asia. Retrieved from <https://www.cnnindonesia.com/teknologi/20220909190301-192-845818/kasus-kebocoran-13-miliar-data-di-ri-disebut-terbesar-di-asia>
- Databoks. (2021). Retrieved from Pengguna Internet Indonesia Peringkat ke-3 Terbanyak di Asia: <https://databoks.katadata.co.id/datapublish/2021/10/14/pengguna-internet-indonesia-peringkat-ke-3-terbanyak-di-asia>
- Iga Revva Princiss Jeinever, A. R. (2018). Penerapan Sistem Keamanan Jaringan Menggunakan Random Port Knocking Berbasis Raspberry PI yang Dikirim Melewati Telegram. JARTEL, Vol. 7, No. 2 , 61- 67.
- Hasbi Muhammad, I. A. (2019). Analisa Perbandingan Sistem Autentikasi Port Knocking dan Single Packet Authotization Pada Server Raspbia. JIRE, Vol. 2, No 1, 36.



- Inda Sari, M. Y. (2019). Sistem Monitoring Serangan Jaringan Komputer Berbasis Web Service menggunakan Honeygot sebagai Intrusion Prevention System. *semanTIK*, Vol. 5, No. 1 , 35-44.
- Jane Blanken-Webb, I. P.-E. (2018). A Case Study-based Cybersecurity Ethics Curriculum. 1-12.
- Kompas.com. (2022). BSSN Sebut Ada 1,6 Miliar Serangan Siber Selama 2021. Retrieved from <https://nasional.kompas.com/read/2022/03/07/20162321/bssn-sebut-ada-16-miliar-serangan-siber-selama-2021>
- Novandha Yudyanto, S. &. (2020). Integrasi Modern Honey Network Dengan Grafana Untuk Visualisasi. *REPOSITOR*, Vol. 2, No. 10, Pp 1380-1389.
- Primartha, I. S. (2019). Network security dan cyber security : teori dan praktik cisco CCNA, linux, windows, amazon AWS, android. Bandung: Informatika Bandung.
- Sakti, N. A. (2019). Implementasi Low Interaction Honeygot Untuk Peningkatan Keamanan Server dan Analisa Serangan Pada Protokol SSH. *Jurnal Nasional Teknologi dan Sistem Informasi* , 112-120.
- tempo.co. (2022). Inilah 7 Kasus Dugaan Kebocoran Data Pribadi Sepanjang 2022. Retrieved from <https://nasional.tempo.co/read/1632043/inilah-7-kasus-dugaan-kebocoran-data-pribadi-sepanjang-2022>
- The Honeygot Project. (2022). T-Pot. Retrieved from <https://www.honeygot.org/projects/active/t-pot/>
- Thilakarathne, N. N. (2020). Security and Privacy Issues in IoT Environment. *International Journal of Engineering and Management Research*, Vol. 10, No. 1 , 26-29.
- Trivedi, D. (2021). Cybersecurity 101 - A Practical Approach to Attacking CIA Triad.

- Wilman Wilman, I. F. (2018). Port Knocking dan Honeypot sebagai Keamanan Jaringan pada Server Ubuntu Virtual. JIMP - Jurnal Informatika Merdeka Pasuruan, Vol. 3, No. 1 , 27-33.
- Zymer, I. (2021). Honeypots: A Means of Sensitizing Awareness of Cybersecurity Concerns. 1-39. :

## TENTANG PENULIS



**Munawaroh, S.Kom.,M.Kom.** Dosen Tetap di Universitas Pamulang. Ia menyelesaikan S1 di Universitas Pamulang Jurusan Teknik Informatika lulus pada tahun 2013 dan melanjutkan S2 di STIMIK Eresha lulus pada tahun 2016. Awal berkarir menjadi seorang guru smpoa, guru SD dan pernah menjadi asisten dosen di Universitas Pamulang. Pengalaman bekerja lainnya yaitu menjadi programmer EDP di PT BPR Bona Pasogit pada tahun 2015-2017. Sekarang ia menjadi dosen tetap mengampu mata kuliah Bidang AI serta Algoritma dan Pemrograman Universitas Pamulang.



**Chandra Insan Prasetyo, S.Kom,** Lahir di Jakarta pada 20 Februari 1991. Pengalaman pekerjaannya antara lain Mechanical Engineering (2009-2014), Purchasing (2014-2015) di PT Lotte Data Communication, Technical Support (2015-2019) di PT Mediatama Anugrah Citra, kemudian menjadi IT Infrastructure (2019-2023) di PT Andalan Finance Indonesia dan sekarang menjadi IT Infrastructure dan Security di PT Anabatic Technologies Tbk.