Journal of Internet and Software Engineering Vol: 1, No 3, 2024, Page: 1-10

Keamanan IoT dan Sistem Terdistribusi

Ahmadiki Firman Dwi Suryawan, Fauzan Graha Dwi Putra, Vanya Amanda Lovely*, Aep Setiawan

Teknologi Rekayasa Komputer, Sekolah Vokasi, Institut Pertanian Bogor

Abstrak: Di era digital yang semakin kompleks, perangkat *Internet of Things* (IoT) dan sistem terdistribusi telah menjadi bagian penting dari kehidupan kita, memberikan berbagai manfaat dan kemudahan yang signifikan dalam meningkatkan efisiensi, produktivitas, dan kualitas hidup. Namun, tingginya tingkat konektivitas dan kompleksitas ini juga membawa risiko keamanan yang besar, memungkinkan serangan siber yang dapat menyebabkan kerugian finansial, kerusakan reputasi, dan bahkan ancaman terhadap keamanan nasional. Makalah ini mengidentifikasi risiko utama yang dihadapi perangkat IoT dan sistem terdistribusi, termasuk risiko keamanan data, serangan siber, dan kerusakan sistem, serta mengembangkan strategi keamanan yang komprehensif dan efektif untuk menghadapi ancaman-ancaman tersebut. Dengan menekankan pada kontrol akses yang ketat, enkripsi data yang aman, dan pembaruan perangkat lunak secara berkala, penelitian ini bertujuan untuk meningkatkan keamanan dan integritas sistem, serta melindungi data sensitif dan informasi penting dari ancaman serangan siber dan ketidakstabilan keamanan. Oleh karena itu, penelitian ini sangat penting untuk meningkatkan kesadaran dan kemampuan dalam menghadapi ancaman keamanan yang semakin kompleks dan dinamis di era digital ini.

Kata Kunci: IoT, Sistem Terdistribusi, Keamanan Siber, Nmap

DOI: https://doi.org/10.47134/pjise.v1i3.2619
*Correspondence: Vanya Amanda Lovely
Email: vnyamndal03@gmail.com

Received: 15-05-2024
Accepted: 30-06-2024
Published: 31-07-2024

Copyright: © 2024 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution-ShareAlike (CC BY SA) license (http://creativecommons.org/licenses/by-sa/4.0/).

Abstract: *In the increasingly complex digital era, Internet of Things (IoT) devices and distributed systems have become vital parts of our lives, offering significant benefits and conveniences in enhancing efficiency, productivity, and quality of life. However, the high level of connectivity and complexity also brings substantial security risks, enabling cyber attacks that can lead to financial losses, reputational damage, and even threats to national security. This paper identifies the main risks faced by IoT devices and distributed systems, including data security risks, cyber attacks, and system failures, and develops comprehensive and effective security strategies to address these threats. By focusing on strict access control, secure data encryption, and regular software updates, this research aims to enhance the security and integrity of systems, and protect sensitive data and critical information from cyber threats and security instability. Therefore, this research is crucial for raising awareness and improving capabilities in facing the increasingly complex and dynamic security threats in this digital era.*

Keywords: *IoT, Distributed Systems, Cybersecurity, Nmap*

Pendahuluan

Isu mengenai keamanan siber mulai mendapat perhatian lebih setelah berakhirnya Perang Dingin. Hal ini disebabkan kemunduran minat negara dalam memperkuat nuklir dan ingin memperkuat teknologi di sektor lainnya. Ancaman dunia siber kemudian menjadi perhatian kebijakan politik dan pertahanan. Dalam penyelenggaraan keamanan siber tentu berkaitan erat dengan serangan siber, yang secara konvensional digambarkan sebagai aktivitas kriminal yang diarahkan untuk menyerang teknologi informasi dan komunikasi tertentu yang menggunakan medium komputer (Annef, 2021).

Keamanan Siber atau *cybersecurity* dapat dikatakan sebagai sebuah rangkaian aktifitas ataupun pengukuran yang dimaksudkan untuk melindungi dari disrupsi, serangan, atau ancaman yang lainnya melalui elemen-elemen *cyberspace* baik *software*, *hardware*, *computer network* (Primawanti & Pangestu, 2020).

Tingginya angka aktif pengguna internet seharusnya juga dibarengi dengan tingkat keamanan *cyber* itu sendiri, sehingga aktivitas di dunia internet tersebut dapat terjamin keamanan dan kerahasiaannya. Sementara kondisi *Cyber security* di Indonesia masih sangat lemah dan buruk. Pembuatan kebijakan di bidang keamanan *cyber* saat ini menghadapi banyak paradoks, pemilihan satu arah dapat mengorbankan arah lain, sedangkan ada argumen untuk berjalan dua arah. Kemajuan teknologi, peperangan kini telah merambah dunia maya yang mengakibatkan munculnya medan *cyber*, pun ujungnya adalah tetap mengarah pada perang fisik. *Cyber security* juga melakukan tinjauan tentang aktivitas internet dan motivasi penggunaan oleh anak-anak dan mengidentifikasi beberapa risiko yang mereka hadapi. Mereka mengklasifikasikan risiko menjadi lima kategori:

1. risiko konten
2. risiko kontak
3. anak-anak yang ditargetkan sebagai konsumen
4. risiko ekonomi, dan
5. risiko privasi online (Aziz, 2023).

Definisi Diplomasi Siber (*Cyber Security*) menurut Barrinha dan Renard adalah salah satu bentuk dari diplomasi yang dilakukan di ranah atau domain siber, di mana sumber daya, kinerja serta fungsi diplomatik digunakan untuk mengamankan kepentingan nasional terkait dengan dunia maya yang dilakukan dalam format bilateral maupun multilateral. Dalam hal ini, agenda diplomatik yang menjadi isu utamanya mencakup isu *cyber security*, *cyber-crime*, *confidence-building*, *internet freedom*, dan *internet governance*. Diplomasi pertahanan dibidang siber sendiri dinilai berkembang sangat pesat dalam mendefinisikan dan merangkum upaya yang terus-menerus dilakukan untuk menyelesaikan jenis konflik baru yang terjadi di dunia maya. Dialog yang dijalankan antar aktor dalam kegiatan diplomasi merupakan salah satu jalan untuk meraih sebuah keuntungan bersama, begitu pula dengan peran utama diplomasi dunia maya yaitu menghasilkan keuntungan melalui dialog tentang masalah keamanan siber itu sendiri (Ar rahman, 2021).

Di era globalisasi seperti ini ilmu pengetahuan dan teknologi informasi selalu berkembang dan semakin maju. Penggunaan perangkat elektronik yang terus maju seiring

berjalannya waktu dalam kehidupan sehari-hari. Dunia elektronik adalah teknologi yang sangat luas, banyak sekali perkembangan yang terjadi dari waktu ke waktu. Salah satunya perkembangan teknologi di bidang elektronik saat ini adalah IoT (*Internet of Things*) (Putri & Hambali, 2023).

Pada tahun 1980 awal "*connected thing*" atau "*connected device*" yang pertama kali terhubung dengan internet adalah Vending Machine Coca Cola yang dioperasikan oleh *programmer* di Carnegie Melon University. Mereka mengintegrasikan *micro switches* ke dalam *vending machine* dan menggunakan internet untuk melihat apakah *Cooling device* menjaga minuman tetap dingin serta melihat stok coca cola nya. Penemuan ini mendorong untuj pengembangan lebih lanjut ke berbagai bidang di seluruh dunia. Di tahun 1990 John Romkey menciptakan 'perangkat', pemanggang roti yang bisa dinyalakan dan dimatikan melalui Internet. Satu tahun kemudian ilmuan dari University of Cambridge menemukan ide untuk menggunakan *prototype web camera* pertama di dunia untuk mengambil gambar jumlah kopi sebanyak tiga kali dalam satu menit dan mengirimkan gambar tersebut ke komputer yang terkoneksi di jaringan lokal agar semua orang dapat melihat apakah kopi masih ada atau tidak. Wear Cam dibuat pada tahun 1994 oleh Steve Mann. Pada tahun 1997 Paul Saffo memberikan penjelasan singkat pertama tentang sensor dan masa depan.. IOT pada tahun 1999 diciptakan oleh seorang anggota Radio Komunitas Kevin Ashton pengembangan *Frequency Identification* (RFID) dan dia juga sebagai direktur eksekutif Auto ID Centre, MIT dan baru-baru ini menjadi lebih relevan dengan praktik dunia sebagian besar karena pertumbuhan perangkat seluler, komunikasi tertanam dan di mana-mana, komputasi awan dan analisis data (Selay et al., 2022).

Internet of Things (IoT) merupakan suatu teknologi yang mendukung konektivitas semua benda seperti komputer, telepon pintar, sabak elektronik (*tablet*), Televisi pintar, perangkat rumah dengan sensor, aktuator dan perangkat lunak. Konektivitas ini membuat perangkat-perangkat tersebut dapat berkomunikasi dan bertukar data melalui infrastruktur jaringan yang tersedia seperti Internet. Setiap perangkat dengan identitas unik terhubung dengan perangkat lain membangun bentuk baru komunikasi antara orang dengan orang, antara orang dengan benda, dan antara benda dengan benda. IoT merupakan suatu teknologi yang terdiri dari teknik akuisisi data di lingkungan di mana saja (sensor), teknologi komunikasi (jaringan sensor, komunikasi *device-to-device*, komunikasi *machine-to machine*, komputasi kabut (gerbang IoT) dan komputasi awan (*cloud*) (Fitriawan et al., 2020).

IoT bekerja dengan cara memanfaatkan suatu argumentasi pemrograman, setiap perintah argumen akan menghasilkan suatu interaksi yang terjadi antara mesin dengan mesin dan terhubung otomatis tidak ada campur tangan seseorang dan tidak dibatasi jarak. Yang menjadi penghubung antara interaksi kedua mesin adalah internet, sementara tugas manusia hanya sebagai pengatur dan mengawasi alat tersebut bekerja secara langsung (Heru Sandi & Fatma, 2023).

Mesin dibuat agar pekerjaan manusia menjadi lebih mudah, pada awalnya mesin dibuat hanya untuk membantu manusia dan dioperasikan secara manual, lambat laun mesin bisa berjalan sendiri (otomatis), tetapi dalam perkembangannya pemanfaatan mesin sebagai alat dalam sebuah sistem akan menemui kendala jika sudah menyangkut jarak dan waktu. dengan jarak yang begitu jauh maka mesin tidak akan bisa berinteraksi dengan

mesin yang lain, untuk mengatasi hal inilah diterapkan gagasan *internet of things* dinama semua mesin dengan pengenal IP address dapat menggunakan jaringan internet sebagai media komunikasi (Saling bertukar data) (Efendi, 2018).

Arsitektur dari *Internet of Things* terdiri atas beberapa jaringan dan sistem yang kompleks serta sekuriti yang sangat ketat, jika ketiga unsur tersebut dapat dicapai, maka kontrol automatisasi di dalam *Internet of Things* dapat berjalan dengan baik, juga dapat digunakan dalam jangka waktu yang lama sehingga menghasilkan profit yang banyak bagi suatu perusahaan. Namun dalam membangun ketiga arsitektur itu banyak sekali perusahaan pengembang IoT yang gagal, karena dalam membangun arsitektur itu membutuhkan waktu yang lama serta biaya yang tidak sedikit (Susanto et al., 2022).

Pada dasarnya setiap mesin mempunyai sistem untuk mengoperasikannya. Banyak alat yang bisa dipakai yang dapat di gunakan dalam kehidupan sehari-hari yang menggunakan sistem operasi. Sistem operasi merupakan penghubung antara pengguna mesin dan perangkat keras yang di miliki mesin tersebut (Supriyono, 2018).

Windows adalah salah satu *software* sistem operasi yang dikembangkan oleh Microsoft Inc. Windows adalah sistem operasi terpopuler untuk para pengguna *personal computer* (PC). Sejarah sistem operasi ini dimulai dari DosShell for Dos 6, dan Microsoft ingin menyaingi larisnya penjualan Apple Macintosh yang menggunakan GUI. Kini Windows memiliki dukungan *hardware* dan *software* yang sangat beragam. Hal ini juga dipicu oleh banyaknya pengguna dari Windows (Sandhiyadini Rosari et al., 2022).

Nmap ("*Network Mapper*") adalah sebuah *tool open source* untuk eksplorasi dan audit keamanan jaringan. Nmap menggunakan paket IP raw untuk mendeteksi *host* yang terhubung dengan jaringan dilengkapi dengan layanan (nama aplikasi dan versi) yang diberikan, sistem operasi (dan versi), apa jenis *firewall*/filter paket yang digunakan, dan sejumlah karakteristik lainnya. Output Nmap adalah sebuah daftar target *host* yang diperiksa dan informasi tambahan sesuai dengan opsi yang digunakan. Hal kunci di antara informasi itu adalah "tabel *port* menarik". Tabel tersebut berisi daftar angka *port* dan protokol, nama layanan, dan status. Statusnya adalah terbuka (*open*), difilter (*filtered*), tertutup (*closed*), atau tidak difilter (*unfiltered*). Terbuka berarti bahwa aplikasi pada mesin target sedang mendengarkan (*listening*) untuk koneksi/paket pada *port* tersebut (Fergina et al., 2023).

Fungsi utama dari Nmap adalah sebagai *port scanning*, menurut definisinya *port scanning* adalah kegiatan *probe* dalam jumlah yang besar dengan menggunakan *tool* secara otomatis, dalam hal ini adalah Nmap. Sebuah *scanner* sebenarnya adalah *scanner* untuk port TCP/IP, yaitu sebuah program yang menyerang *port* TCP/IP dan servis-servisnya (telnet, ftp, http, https dan lain-lain) dan mencatat respons dari komputer target. Dengan cara seperti ini, *user* program *scanner* dapat memperoleh informasi yang berharga dari *host* yang menjadi target (Dwiyatno, 2020).

Nmap di kenal sebagai salah satu *Tool* yang dapat melakukan eksplorasi pada jaringan dengan cepat sekalipun itu pada ekosistem jaringan yang besar, tak hanya digunakan untuk menemukan celah keamanan dengan teknik *port scanning*, identifikasi *host*, dan Nmap *Scipting Engine* (*NSE*). Teknik Port *scanning* adalah bug yang kedua paling banyak di temukan di *website* yang ada di internet (Sudirman & Akma Nurul Yaqin, 2021).

Teknik *port scanning* ini bertujuan memindai *port host* tertentu apakah sedang terbuka. Jika *port* suatu aplikasi dalam jaringan komputer terbuka, maka siapapun akan bisa masuk dan dapat mengakses aplikasi tersebut. Selain dapat melihat status terbuka atau tertutup sebuah *port* dalam jaringan, Nmap juga bisa melihat status lainnya seperti: *filtered*, *unfiltered*, *open/filtered*, dan *closed/filtered* (Mira Orisa & Ardita, 2021).

Command prompt (cmd) atau sering disebut juga cmd pada dasarnya adalah aplikasi *command line interpreter* (cli) yang berfungsi untuk menjalankan perintah yang dimasukkan oleh penggunanya (Rosalina et al., 2022).

Sebagian besar dari perintah yang digunakan untuk mengotomatisasi tugas-tugas melalui *script* dan *file batch*, dengan melakukan fungsi administratif m, dan untuk memecahkan masalah dan memecahkan beberapa jenis masalah yang biasa pada Windows. *Command Prompt* secara resmi disebut juga sebagai Windows Command Processor tetapi juga kadang-kadang disebut *shell command* atau dengan cmd.exe nama file-nya. *Command Prompt* tersedia pada setiap sistem operasi yang berbasis Windows NT yang meliputi Windows 10, Windows 8, Windows 7, Windows Vista, Windows XP, Windows 2000, serta Windows Server 2012/2008/2003 (Yusnanto & Lestiono, 2019).

Perangkat lunak ini dimanfaatkan untuk memeriksa informasi jaringan *wireless interface* yang terdapat pada komputer *client* untuk memastikan bahwa *client* telah mendapatkan alamat IP secara otomatis, dan juga digunakan untuk menguji bahwa sistem *web filtering* telah berhasil dan bekerja dengan baik, yaitu dengan melakukan *name server lookup* (nslookup) (Randy Ikhsan Ramadhan & Siti Madinah Ladjamuddin, 2022).

Adapun beberapa fungsi dari *Command Prompt* di windows adalah sebagai berikut:

a. Meng-*handle* beberapa masalah saat versi GUI (*Grafik User Interface*) pada Windows kita bermasalah diakibatkan virus. Seperti hilangnya *folder options* pada explorer, *task manager* yang di-*disable*, tidak bisa membuka msconfig dan sebagainya. Lebih lanjut kita bisa menangani virus lewat cmd.
b. Seperti namanya, "Prompt" sendiri arti harafiahnya adalah Quick atau cepat jadi kita bisa mengeksekusi sebuah perintah lebih cepat dengan menggunakan cmd. Selain lebih cepat cmd ini juga lebih ringan dibanding dengan explorer saat melakukan perintah masuk pada direktori tertentu, atau mencari file tertentu.
c. Kegunaan lain dari Command Prompt ini adalah untuk membiasakan menggunakan command line pada cmd agar nantinya terbiasa dengan server core yang menggunakan OS berbasis text (Ekojono et al., 2016).

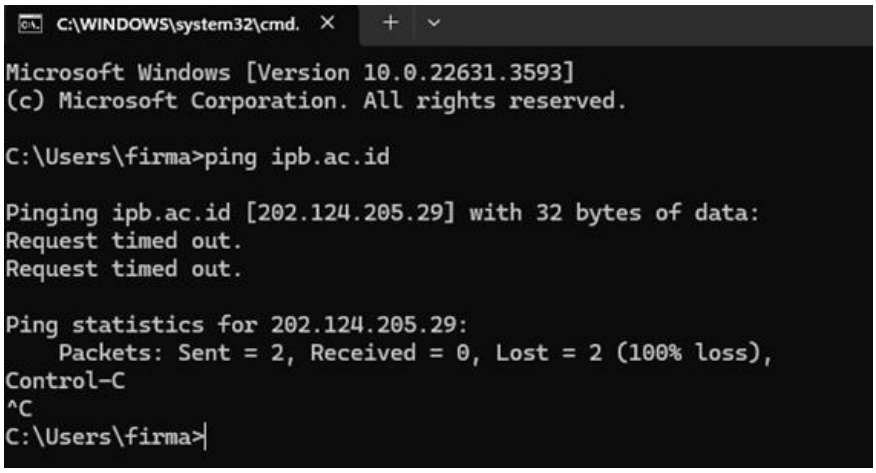
Metode

Penelitian ini menggunakan metode studi literatur untuk mengkaji keamanan dalam *Internet of Things* (IoT) dan sistem terdistribusi. Studi literatur dilakukan dengan mengumpulkan dan meninjau literatur yang relevan dari berbagai sumber akademik dan industri. Sumber-sumber utama yang digunakan meliputi jurnal ilmiah, buku, makalah konferensi, dan laporan teknis yang diperoleh melalui *database* akademik seperti IEEE Xplore, ScienceDirect, dan Google Scholar. Proses seleksi literatur dilakukan dengan mempertimbangkan relevansi, kualitas, dan kontribusi setiap karya terhadap topik

penelitian. Artikel-artikel yang terpilih dianalisis secara mendalam untuk mengidentifikasi tren terkini, tantangan utama, serta solusi yang telah diusulkan dan diimplementasikan dalam konteks keamanan IoT dan sistem terdistribusi. Hasil analisis literatur ini kemudian disintesis untuk memberikan pemahaman yang komprehensif mengenai isu-isu keamanan, sekaligus mengidentifikasi gap penelitian yang masih ada dan rekomendasi untuk penelitian lebih lanjut.

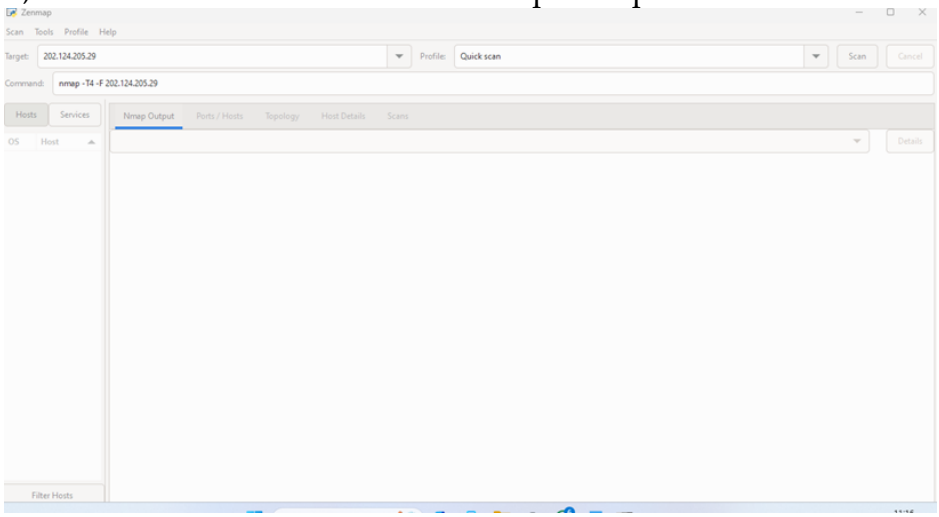
Hasil dan Pembahasan

Langkah pertama yang perlu dilakukan adalah melakukan ping terhadap server yang ingin dihubungkan. Proses ping ini merupakan cara untuk menguji apakah server tersebut dapat dijangkau dan seberapa cepat responsnya. Untuk melakukannya, buka *Command Prompt* atau Terminal. Kemudian, ketik perintah "ping" diikuti oleh nama domain atau alamat server yang ingin diuji. Setelah menjalankan perintah ping, hasilnya akan menjadi seperti di bawah ini.



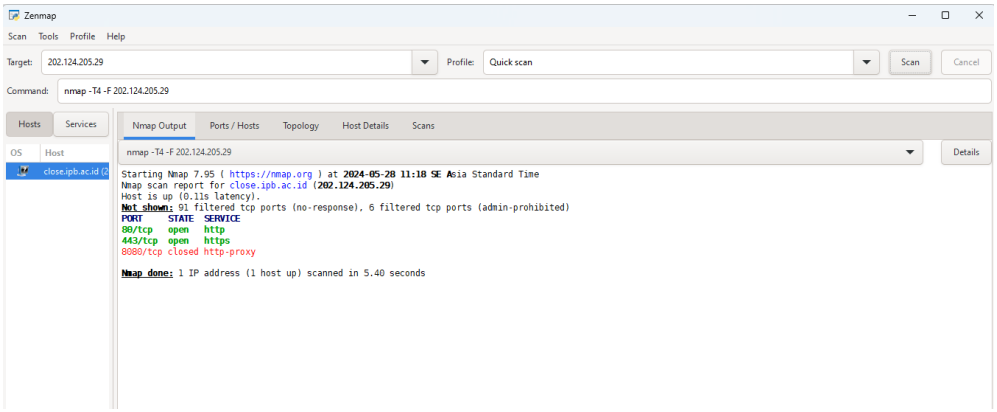
Gambar 1. Ping Terhadap Server

Berikutnya, buka aplikasi Nmap. Setelah aplikasi terbuka, tempelkan alamat IP yang sudah di-*copy* sebelumnya ke dalam kolom yang tersedia. Pilih opsi "*Quick Scan*" dari menu pilihan *scan*. Terakhir, klik tombol "*Scan*" untuk memulai proses pemindaian.



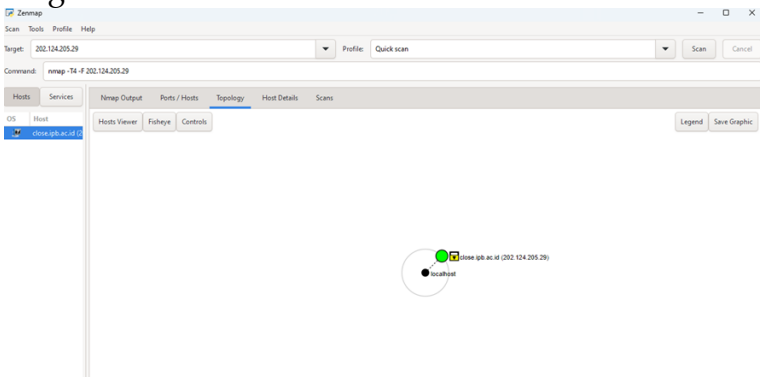
Gambar 2. Pemindaian Alamat IP

Setelah selesai di-*scan*, maka akan terlihat hasilnya. Hasil ini menunjukkan jumlah *port* yang digunakan oleh server, serta *port* mana yang aktif dan *port* mana yang tidak aktif.



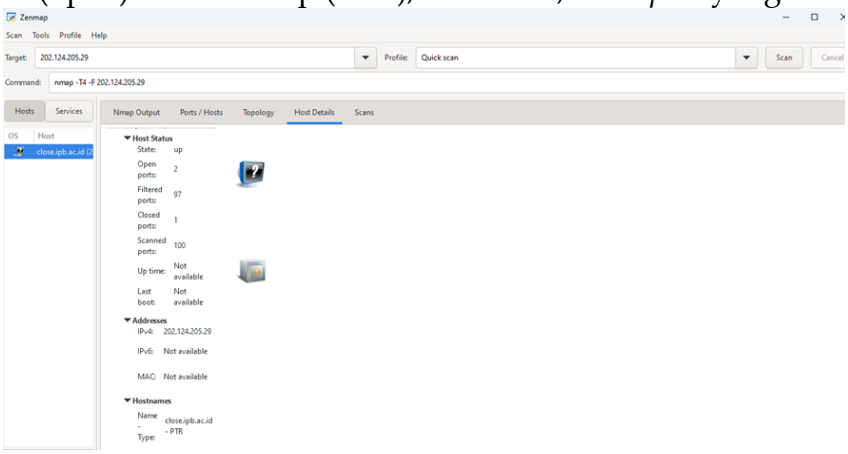
Gambar 3. Jumlah Port

Selanjutnya, kita bisa melihat topologi jaringan menggunakan Nmap. Dapat dilihat, bagaimana perangkat-perangkat dalam jaringan saling terhubung serta melihat alamat IP masing-masing perangkat tersebut.



Gambar 4. Topologi Jaringan

Setelah itu, kita juga bisa melihat detail *host* yang ditampilkan. Detail ini mencakup jumlah *port* yang terbuka (open) dan tertutup (*close*), alamat IP, serta *port* yang terfilter.



Gambar 5. Detail Jumlah Port

Dalam penelitian ini, kami menyampaikan pentingnya keamanan dalam era digital, khususnya yang berkaitan dengan *Internet of Things* (IoT) dan sistem terdistribusi. Kedua teknologi ini telah menjadi bagian integral dari kehidupan sehari-hari kita, memberikan kemudahan dan efisiensi melalui pengumpulan dan pertukaran data secara *real-time*. Namun, kemajuan ini juga membawa berbagai risiko keamanan. Perangkat IoT, misalnya, sangat rentan terhadap serangan *malware*, peretasan data, dan pelanggaran privasi. Demikian pula, sistem terdistribusi menghadapi tantangan seperti serangan terdistribusi, kegagalan node, dan masalah skalabilitas. Oleh karena itu, penelitian ini menekankan pentingnya penerapan strategi keamanan yang efektif untuk melindungi data dan menjaga integritas sistem.

Salah satu alat yang digunakan dalam penelitian ini adalah Nmap, sebuah alat untuk eksplorasi dan audit keamanan jaringan. Nmap berguna untuk mendeteksi *host* yang terhubung ke jaringan dan menyediakan informasi tambahan seperti layanan, sistem operasi, jenis *firewall*, dan karakteristik lainnya. Informasi ini sangat penting untuk mengidentifikasi dan mengatasi potensi ancaman keamanan. Penggunaan Nmap membantu dalam memahami struktur dan kerentanan jaringan, sehingga memungkinkan penerapan langkah-langkah keamanan yang lebih tepat dan efektif. Dalam konteks ini, langkah-langkah keamanan yang direkomendasikan meliputi penerapan kontrol akses yang ketat, enkripsi data, dan pembaruan perangkat lunak secara berkala. Selain itu, penerapan kebijakan privasi yang jelas dan kontrol akses yang ketat juga sangat penting untuk melindungi data sensitif dan privasi pengguna. Keamanan siber bukan hanya tentang teknologi, tetapi juga melibatkan kebijakan, konsep keamanan, peraturan, dan pendekatan manajemen risiko yang komprehensif. Dengan pendekatan yang menyeluruh dan terkoordinasi, risiko keamanan dapat diminimalkan, dan manfaat dari teknologi IoT dan sistem terdistribusi dapat dimaksimalkan.

Simpulan

Dari hasil di atas, dapat disimpulkan bahwa keamanan siber merupakan aspek yang sangat penting dalam pengembangan dan penggunaan teknologi IoT dan sistem terdistribusi. Meskipun teknologi ini menawarkan banyak manfaat seperti efisiensi dan kemudahan, mereka juga membawa risiko keamanan yang signifikan. Oleh karena itu, diperlukan strategi keamanan yang efektif untuk melindungi data dan menjaga integritas sistem. Penggunaan alat seperti Nmap sangat membantu dalam audit keamanan jaringan dan identifikasi potensi ancaman. Selain itu, penerapan kontrol akses yang ketat, enkripsi data, dan pembaruan perangkat lunak secara berkala adalah langkah-langkah penting dalam meningkatkan keamanan. Dengan demikian, kita dapat menciptakan lingkungan digital yang lebih aman dan terpercaya, meminimalkan risiko keamanan, dan memaksimalkan manfaat dari teknologi IoT dan sistem terdistribusi.

Daftar Pustaka

Annef, A. B. (2021). Ancaman Siber Di Tengah Pandemi Covid-19 : Tinjauan Terhadap Keamanan Non-Tradisional Dan Keamanan Siber Di Indonesia. *Sriwijaya Journal of International Relations*, *1*(1), 18–33. https://doi.org/10.47753/sjir.v1i1.3

Ar rahman, L. L. (2021). Implikasi Diplomasi Pertahanan terhadap Keamanan Siber dalam Konteks Politik Keamanan. *Jurnal Diplomasi Pertahanan*, *6*(2). https://doi.org/10.33172/jdp.v6i2.654

Aziz, A. (2023). Pentingnya pengetahuan cyber security untuk publik dan negara (The importance of cyber security knowledge for the public and the country). *Jurnal Prosiding SAINTEK: Sains Dan Teknolog*, *2*(1), 75–82.

Dwiyatno, S. (2020). Analisis Monitoring Sistem Jaringan Komputer Menggunakan Software Nmap. *PROSISKO: Jurnal Pengembangan Riset Dan Observasi Sistem Komputer*, *7*(2), 108–115. https://doi.org/10.30656/prosisko.v7i2.2522

Efendi, Y. (2018). Internet Of Things (Iot) Sistem Pengendalian Lampu Menggunakan Raspberry Pi Berbasis Mobile. *Jurnal Ilmiah Ilmu Komputer*, *4*(2), 21–27. https://doi.org/10.35329/jiik.v4i2.41

Ekojono, E., Affandi, L., & Suryani, D. (2016). Metode Pemanfaatan Command Line Untuk Direct Printing Pada Aplikasi Berbasis Web. *Jurnal Teknologi Informasi*, 117–126. https://doi.org/10.36382/jti-tki.v7i2.222

Fergina, A., Setia, M. I., Yusuf, M., & ... (2023). Analisis Monitoring Sistem Keamanan Jaringan Komputer menggunakan Software NMAP (Studi Kasus Jaringan di Universitas Nusa Putra). *… Ilmu Komputer …*. http://prosiding.sentimeter.nusaputra.ac.id/index.php/prosiding/article/view/45%0A http://prosiding.sentimeter.nusaputra.ac.id/index.php/prosiding/article/download/45/41

Fitriawan, H., Despa, D., & Kustiani, I. (2020). Potensi Internet of Things (IoT) dan Ragam Sensor untuk Layanan Kesehatan. *Jurnal Profesi Insinyur Universitas Lampung*, *1*(1), 1–4. https://doi.org/10.23960/jpi.v1n1.10

Heru Sandi, G., & Fatma, Y. (2023). Pemanfaatan Teknologi Internet of Things (Iot) Pada Bidang Pertanian. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *7*(1), 1–5. https://doi.org/10.36040/jati.v7i1.5892

Mira Orisa, & Ardita, M. (2021). Vulnerability Assesment Untuk Meningkatkan Kualitas Kemanan Web. *Jurnal Mnemonic*, *4*(1), 16–19. https://doi.org/10.36040/mnemonic.v4i1.3213

Primawanti, H., & Pangestu, S. (2020). Diplomasi Siber Indonesia Dalam Meningkatkan Keamanan Siber Melalui Association of South East Asian Nation (Asean) Regional Forum. *Global Mind*, *2*(2), 1–15. https://doi.org/10.53675/jgm.v2i2.89

Putri, I. K., & Hambali, H. (2023). Sistem Kontrol Instalasi Rumah Berbasis IoT (Internet of Things). *JTEIN: Jurnal Teknik Elektro Indonesia*, *4*(2), 675–682. https://doi.org/10.24036/jtein.v4i2.479

Randy Ikhsan Ramadhan, & Siti Madinah Ladjamuddin. (2022). Perancangan Sistem Web Filtering Dengan Metode Dns Forwarding Pada Jaringan Komputer Berbasis Mikrotik

Routeros. *Jurnal Informatika Dan Tekonologi Komputer (JITEK)*, *2*(2), 146–157. https://doi.org/10.55606/jitek.v2i2.231

Rosalina, O., Pujianto, D., Fakih, A., Asia, M., Jend, J., Yani, A., 267a, N., Baru, T., & Korespondensi, S. (2022). Sistem Informasi Perpustakaan Menggunakan Embarcadero Xe2 Berbasis Client Server Di Sd Negeri 43 Oku. *Jurnal Sistem Informasi Mahakarya (JSIM) JSIM*, *5*(1), 28–35.

Sandhiyadini Rosari, H., Syaibani Al Hakim, M., Sibagariang, E., Rosadi Kardian, A., & Siber dan Sandi Negara, P. (2022). Analisis Kecepatan MySQL dan PostgreSQL pada Windows 11 dan Kali Linux 2022. *Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)*, *8*(1), 213. https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

Selay, A., Andgha, G. D., Alfarizi, M. A., Bintang, M. I., Falah, M. N., Khaira, M., & Encep, M. (2022). Karimah Tauhid, Volume 1 Nomor 6 (2022), e-ISSN 2963-590X. *Karimah Tauhid*, *1*(2963-590X), 861–862.

Sudirman, D., & Akma Nurul Yaqin. (2021). Network Penetration dan Security Audit Menggunakan Nmap. *SATIN - Sains Dan Teknologi Informasi*, *7*(1), 32–44. https://doi.org/10.33372/stn.v7i1.702

Supriyono, S. (2018). Membangun Server Repository Di Windows Guna Mempermudah Pemasangan Aplikasi Pada Sistem Operasi Windows Di Laboratorium Informatika S-1 Itn Malang. *Industri, Fakultas Teknologi*, *2*(1), 199–205.

Susanto, F., Prasiani, N. K., & Darmawan, P. (2022). Implementasi Internet of Things Dalam Kehidupan Sehari-Hari. *Jurnal Imagine*, *2*(1), 35–40. https://doi.org/10.35886/imagine.v2i1.329

Yusnanto, T., & Lestiono, D. (2019). Optimalisasi Penggunaan Cmd Dan Sysinternalsuits Sebagai Malware Detection. *Jurnal Transformasi*, *15*(1), 66–74.