P-ISSN 2654-5438
E-ISSN 2828-4917

PENGUJIAN KUANTITAS DAN KUALITAS WI-FI PADA GEDUNG ANNEX PT. PUPUK SRIWIDJAJA PALEMBANG.

[1]Aidil Nur Riyansyah, [2*]Vivi Sahfitri
[1]Teknik Komputer, Fakultas Vokasi, Universitas Bina Darma Palembang
[2*]Manajemen Informatika, Fakultas Vokasi, Universitas Bina Darma Palembang
E-mail : aidilkenzo2019@gmail.com
*E-mail : universitas@binadarma.ac.id

Abstract *– Technology is a means related to managing data into information and the process of distributing that data/information within the boundaries of space and time. Testing was carried out using the Nmap tool in the form of Nmap (Network Mapper) which is professional security scanning software. Ethical Hacking is an activity to penetrate a system. This research was carried out using the Ethical Hacking method, where researchers will emphasize research in the FootPrinting and Vulnerability Scanning stages. This test uses 5 targets to test the quantity and quality of Wi-Fi. By using Target IP 10.10.69.3. Initial Network Testing 1 Target. Search for IP Address using CMD. Final Network testing 5 Targets. Nmap –T4 –A –V 10.10.69.3., Nmap-sS 10.10.69.3, Nmap-sS -sv 10.10.69.3, Nmap –script – version 10.10.69.3e.Nmap –sn 10.10.69.3 , The quantity produced is the amount devices connected to the network, as well as the number of open ports on each device.*

Keywords : Wi-Fi, Technology, Nmap, PT.Pusri.

Abstrak - Teknologi merupakan sarana yang berhubungan dengan pengelolaan data menjadi informasi dan proses penyaluran data/informasi tersebut dalam batas-batas ruang dan waktu. Pengujian dilakukan dengan menggunakan tools Nmap yang berupa, Nmap (Network Mapper) merupakan perangkat lunak pemindaian profesional keamanan. Ethical Hacking merupakan suatu aktifitas melakukan penetrasi ke suatu sistem. Penelitian ini dilakukan menggunakan metode Ethical Hacking, dimana peneliti akan menekankan penelitian dalam tahapan FootPrinting dan Vulnerability Scaning. Pengujian ini menggunakan 5 Target untuk menguji kuantitas dan kualitasWi-Fi tersebut. Dengan menggunakan IP Target 10.10.69.3. pengujian Jaringan Awal 1 Target. Mencari Alamat IP menggunakan CMD . pengujian Jaringan Akhir 5 Target. Nmap –T4 –A –V 10.10.69.3.,Nmap-sS 10.10.69.3, Nmap-sS -sv 10.10.69.3, Nmap –script –version 10.10.69.3e.Nmap –sn 10.10.69.3 , Kuantitas yang dihasilkan berupa jumlah perangkat yang terhubung ke jaringan, serta jumlah port yang terbuka pada setiap perangkat.

Kata kunci : Wi-Fi, Teknologi, Nmap, PT.Pusri.

1. Pendahuluan

Teknologi adalah pusaat proses penyaluran data/informasi serta pengolahan data dengan menggunakan jaringan internet. Jaringan internet sendiri merupakan jaringan global yang terhubung secara luas dan kompleks yang menghubungkan perangkat komputer di seluruh dunia menggunakan TCP/IP *(Transmission Control Protocol/Internet Protocol),* untuk mengatur cara data dikirimkan dan diterima antara perangkat yang terhubung, internet juga menghubugkan berbagai jenis jaringan, termasuk Lokal (LAN), jaringan wilayah luas (WAN)[8]. Wi-Fi *(Wireless Fidelity)* merupakan salah satu bagian dari teknologi, yang merupakan teknologi nirkabel yang terhubung ke Jringan internet atau jaringan lokal tanpa menggunakan kabel fisik.

PT. Pupuk Sriwidjaja (PUSRI) adalah salah satu perusahaan produsen pupuk terkemuka di Indonesia. PT. Pupuk Sriwidjaja juga merupakan salah satu perusahaan produsen pupuk terbesar di Indonesia dan gedung Annex juga merupakan salah satu gedung penting yang di dalamnya merupakan gedung penting dalam kompleks teknologi atau data penting perusahaan. Pengujian ini menggunakan software NMAP *(Network Mapper)* merupakan perangkat lunak pemindaian profesional keamanan dan administrator jaringan untuk mengeksplorasi jaringan, mengguakan host yang aktif, menganalisis layanan yang berjalan di host tersebut, serta menidentifikasi celah keamanan. NMAP juga berungsi untuk melakukan pemindaian port mana yang terbuka pada target yang ditentukan. Pengguna dapat menentukan layanan apa saja yang berjalan di host, dan mengetahui apakan ada potensi kerentanannya.[9]

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka dapat dibuat suatu perumusan masalah, yaitu : "Bagaimana pengujian kuantitas dan kualitas wi-fi pada gedung annex PT. Pupuk Sriwidjaja Palembang?"

1.3 Batasan Masalah

Terdapat 4 pembahasan masalah pada pengujian ini, yaitu :

1. Pengujian dengan Nmap dapat dibatasi hanya pada perangkat yang dapat diakses dari titik akses wi-fi tertentu.
2. Pada jaringan wi-fi di gedung annex PT. Pupuk Sriwidjaja, pencarian dibatasi hanya pada jaringan yang diidentifikasi dengan SSID tertentu yang ada di gedung ersebut.
3. Waktu yang digunakan dalam pengujian dari 14 Juni 2023 – 21 Juni 2023 juga bisa menjadi pertimbangan untuk melakukan pengujian kuantitas dan kualitas wi-fi tersebut.
4. Tujuan pengujian untuk menguji kuantitas jaringan seperti jumlah perangkat yang terhubung atau kualitas jaringan sepeeti, kecepatan latensi dan stabilitas koneksi.

1.4 Tujuan dan Manfaat Penelitian

1.4.1 Tujuan Penelitian

Adapun tujuan daari pengujian ini adalah melakukan pengujian kuantitas dan kualitas jaringan wi-fi pada gedung annex PT. Pupuk Sriwidjaja Palembang.

1.4.2 Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah sebagai berikut:

1. Penggunaan Nmap dapat memastikan dan analisis terhadap jaringan gedung annex PT. Pupuk Sriwidjaja. Hal ini membantu dalam mengidentifikasi kerentanan keamanan jaringan dan menemukan celah yang mungkin dieksplooitasi oleh pihak yang tidak berwenang.
2. Dengan menggunakan Nmap, pengujian dapat melacak penggunaan sumber daya jaringan seperti bandwith dan penggunaan CPU.

P-ISSN 2654-5438
E-ISSN 2828-4917

3. Hasil dari penelitian menggunakan Nmap dapat membantu dalam perencanaan dan pengembangan jaringan di gedung annex PT. Pupuk Sriwidjaja. Data yang diperoleh dapat digunakan untuk membuat strategi pengembangan jaringan yang lebih efisien, meningkatkan keandalan, dan mengoptimalkan kinerja jaringan.

2. Tinjauan Pustaka

2.1 Wi-Fi

Wi-Fi *(Wireless Fidelity)* merupakan salah satu bagian dari teknologi, yang merupakan teknologi nirkabel yang terhubung ke Jaringan internet atau jaringan lokal tanpa menggunakan kabel fisik[6].

2.2 Jaringan Komputer

Jaringan komputer adalah mengacu pada perangkat komputer yang saling terhubung serta dapat bertukar data dan berbagi sumber daya satu sama lain[4].

2.3 Local Area Network (LAN)

Local Area Network (LAN) adalah kumpulan perangkat yang terhubung menjadi suatu jaringan kompuuter yang hanya mencakup wilayah local saja seperti gedung, kantor, dan rumah[7].

2.4 Wide Area Network (WAN)

Wide Area Network (WAN) adalah sekumpulan dari LAN atau sebuah jaringan yang berkomunikasi dengan jaringan yang lain. WAN memiliki jangkauan yang sangat luas dan besar sehingga mampu menjangkau negara, benua hingga seluruh dunia[7].

2.5 Penelitian Terlebih Dahulu

Sebagai dasar refrensi dalam penelitian yang dilakukan maka penulis sangat perlu mencantumkan hasil dari penelitian terdahulu yang dapat digunakan sebagai salah satu data pendukung untuk penelitian ini.

Berikut ini merupakan hasil dari penelitian terdahulu yang relevan dengan peneliti yang sedang penulis teliti.:

Nama Peneliti	Judul Penelitian	Hasil Penelitian
(Muhyidin et al., 2015)	*Pebandingan Tingkat Keamanan Website menggunakan Nmap Dengan Metode Ethical Hacking.*	Hasil penelitian ini telah menemukan informmasi terkait dengan websitetarget yaitu, A,B, dan C, dapat *diketahui IP target, hostname target, port target.*

P-ISSN 2654-5438
E-ISSN 2828-4917

(Kasus et al., 2020)	*Analisis Monitoring Sistem Kemanan Jaringan Komputer Menggunakan Software NMAP (Studi KasusSMK Negeri 1 Kota Serang)*	Dengan menggunakan *software NMAP* seorang user dapat mengetahui port-port layanan, versi jaringan dengan versi layanan dan mesin pendeteksi sistem operasi.
(Fahlevi et al., 2021)	*Analisis Monitoring & Kinerja Sistem Keamanan Jaringan Komputer Menggunakan NMAP (Studi Kasus Raz Hotel & Convention Medan*	Hasil penelitian agar dapat menngetahui kelemahan dan kel ebihan, serta melihat terdapat layanan dan port apa saja pada layanan ini.
(Karim et al., 2021)	*Network Penetration dan Security Audit Menggunakan Nmap*	Hasil yang di peroleh dengan penetrasi port Scanning menggunakan Nmap pada jaringan target dapat membuka informasi lalu lintas pada jaringan, seperti jumlah host pada perangkat terhubung, IP Address, Network, perangkat Router, Port TCP/UDP terbuka dan tertutup.

3. Metodologi Penelitian

Penelitian ini dilakukan menggunakan metode Ethical Hacking, Ethical Hacking merupakan suatu aktifitas melakukan penetrasi ke suatu sistem, jaringan, dan aplikasi dengan cara mengeksploitasi kelemahan dengan maksud untuk mendapatkan hak akses atau data sistem, tujuannya adalah membantu perusahaan menguji keamanan sistem dan jaringan yang mereka miliki. Orang yang melakukan Ethical hacking disebut Ethikal Hacker. Teknik yang digunakan oleh Ethikal Hacker dan Hacker hampir sama hanya saja tujuannya berbeda.

3.1 Vulnerability Assesement

Vulnerability assesment dilakukan untuk mengetahui celah-celah yang berpotensi masuuknya serangan. Selain itu dapat mengetahui masa berlaku versi sebuah software, port yang terbuka, dan aplikasi yang sedang berjalan pada sistem tersebut dan untuk mendeteksi kelemahan dalam jaringan.[2].

3.2 Information Gathering

Pencarian informasi *(Information Gathering)* adalah fase untuk mendapatkan informasi target serangan baik individu ataupun perusahaan untuk mendapatkan informasi yang akurat[2].

P-ISSN 2654-5438
E-ISSN 2828-4917

3.3 Reconnaissance

Reconnaissance adalah sebuah fase persiapan sebelum melakukan penyerangan *(attacker)* melakukan penyerangan, dimana kegiaan intinya adalah mengumpulkan informasi sebanyak mungkin mengenai sasaran. Pada *reconnaissane* ini menyertakan *Network Scanning* baik melalui jaringan *internal* atau *eksternal*[2].

3.4 Foot Printing

Footprinting adalah tahap mengumpulkan informas sebelum melakukan penyerangan terhadap wi-fi dengan cara mengumpulkan informasi target yang tujuannya untuk merangkai pa yang ditemukn *(Blueprint)* dari suatu jaringan[2].

3.5 Network Scanning

Network Scanning merupakan cara yang digunakan untuk melakukan sanning pada mesin jaringan, mendapatkan IP, Port, paket data yang keluar masuk jaringan, termasuk merekam aktifitas broswing[2].

3.5 Port Scanning

Port Scanning adalah aktifitas yang dilakukan untuk dilakukan untuk memeriksa status port TCP dan UDP pada UDP pada sebuah mesin, tujuannya adalah untuk mengetahui kelemahan suatu sistem jaringan dari port yang terbuka dan OS yang digunakan[2].

4. Hasil dan Pembahasan

4.1 Hasil

Dari hasil Pengujian Kuantitas dan Kualitas Wi-Fi pada Gedung Annex PT. Pupuk Sriwidjaja Palembang dalam pengujian ini menggunakan 2 proses untuk menguji kuantitas dan kualitas Wi-Fi tersebut. Dengan menggunakan IP Target 10.10.69.3.

Terdapat 2 cara proses scanning yaitu :

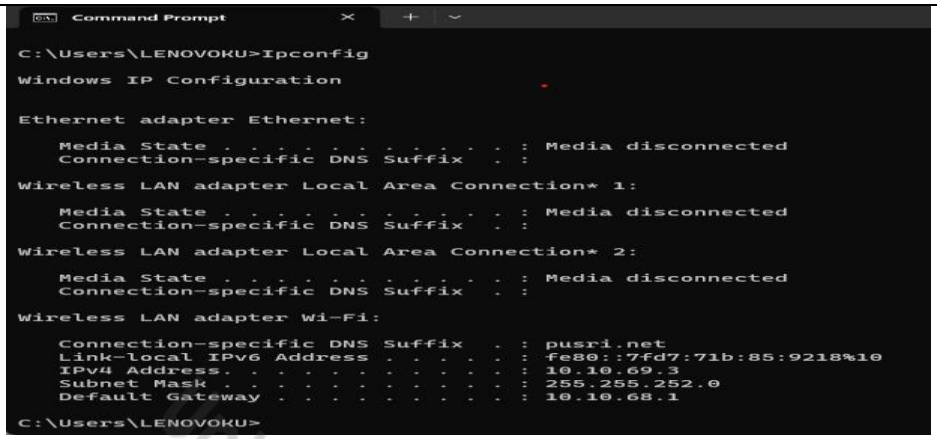
1. Jaringan Awal IP Address
    a. Mencari Alamat IP menggunakan CMD
2. Jaringan Akhir Menggunakan Target
    a. Nmap –sn 10.10.69.3

4.2 Pembahasan

4.2.1 Pengujian Jaringan Awal

Pada tahap ini user menggunakan komputer yang telah terhubung pada jaringan wi-fi pada gedung annex PT. Pupuk Sriwidjaja Palembang. Setelah terhubung pada jaringan wi-fi, user harus mencari host target untuk dilakkan scanning jaringan menggunakan software Nmap. Pada gambar 4.1 menunjukkan hasil dalam mencari host target dengan menggunakan **CMD** :

P-ISSN 2654-5438
E-ISSN 2828-4917



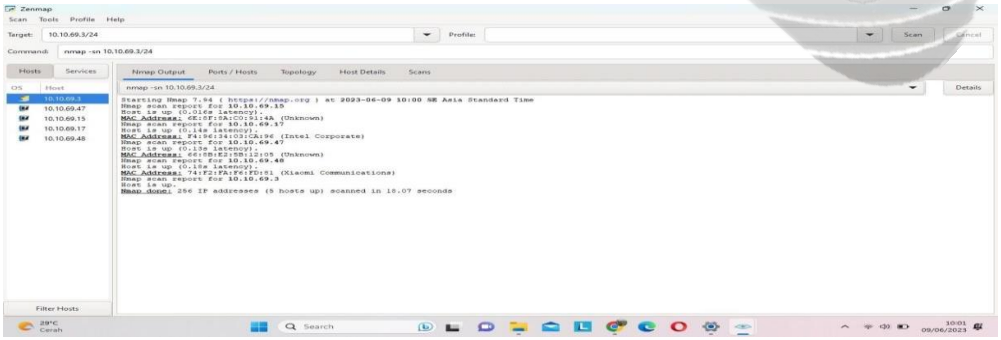
Gambar 4. 1 Mencari Host Target pada Komputer User

Pada Gambar 4.1 user dapat mengetahui host target yang akan dilakuukan scanning jaringan menggunaan software Nmap dengan melihat hasil dari Ethernet adapter Ethernet.

1. Default Gateway : IP Address 10.10.68.1
   Default Gateway adalah gerbang jaringan pada perangkat komputer user yang terhubung dengan jaringan wi-fi.
2. Subnet Mask : IP Address 255.255.255.0
   Subnet Mask adalah alamat kelaas C. Sub profilnya yaitu/24
3. Ipv4 : IP Address 1010.69.3
   Merupakan alamat IP Address Laptop user dengan protocol IP versi 4, Ipv4 IP Address 10.10.69.3 akan menjadi host target yang akan dilakukan scanning jaringan menggunakan softwware Nmap.

4.2.2 Pengujian Jaringan Akhir

4.2.2.1 Pengujian Host Target Nmap –sn



Gambar 4. 2 Pengujian Host Target Nmap -sn 10.10.69.3

Pada Gambar 4.2 merupakan hasil dari pengujian dengan host target Nmap –sn dengan melakukan pemindaian host dengan tujuan untuk mendeteksi ketersediaan mereka tanpa melakukan pemindaian port. Ini juga disebut juga sebagai “ping scan” atau “host discovery”.

P-ISSN 2654-5438
E-ISSN 2828-4917

Mac Address	IP Address	Latency	Perangkat
6E:8F:8A:C0:91:4A	10.10.69.17	0.16s	Unknown
F4:96:34:03:CA:96	10.10.69.47	0.14s	Intel Corporate
66:8b:E2:5B:12:05	10.10.69.48	0.13s	Unknown
74:F2:FA:F6:FD:81	10.10.69.3	0.18s	Xiaomi Communications

Tabel 4. 1 Hasil Pengujian Host Target Nmap –sn

Pada table 4.2 pengujian Nmap –sn dengan melakukan peminidaian di alamat IP 10.10.69.3 untuk mendeteksi host yang aktif. Jika host aktif ditemukan, 'nmap' akan menampilkan alamat IP host yang terdeteksi. Serta menampilkan latency yang berkisar dari beberapa milidetik hingga beberapa puluh milidetik dikategorikan latency standar, yang dimana pemindaian pada tabel 4.2 termasuk dalam keadaan lancar dan baik, jika latency tersebut sudah mencapai ratussan milidetik maka pemindaian jaringan disebut lambat atau kurang baik.

5. Kesimpulan

Berdasarkan hasil dari penelitian yang telah dilakukan oleh peneliti dapat disimpulkan bahwa:

1) Kuantitas yang dihasilkan dalam penelitian ini berupa jumlah perangkat yang terhubung kejaringan, serta jumlah port yang terbuka pada setiap perangkat. Jumlah port yang terdeteksi dalam jaringan wi-fi dengan target Nmap –sn 10.10.69.3 terdapat 4 port terbuka dan scanning hasil perangkat yang terhubung dalam wifi tersebut.
2) Kualitas yang dihasilkan dalam penelitian ini berupa kecepatan dalam scanning yang dilakukan sesuai target pendeteksi. Jumlah latency pada target Nmap –sn 10.10.69.3 yaitu (0,0014s), pada target Nmap –sn tergantung pada Mac Address yang terhubung.
3) Dari hasil scanning yang dilakukan terhadap beberapa layanan masih banyak potensi kerentanan keamanan akan timbul dikarenakan beberapa port yang masih terbuka *(open)*.

P-ISSN 2654-5438
E-ISSN 2828-4917

Referensi

[1] A.F. (2023). *Apa itu Latenc? Definisi, Pennyebab, dan Cara mengatasinya.*
[2] Alwi,E,I., Herdianti, H., & Umar,F. (2020). Analisis Keamanan Website Menggunakan Teknik Footprinting dan Vulnarebility Scanning. INFORMAL: Informatics Journal, 5(2), 43. https://doi.org/10.19184/isj.v5i2.18941
[3] Fahlevi, M.R., D., Putri., D., Rekayasa, J., Komputer, S., Utama, U. P., Rekayasa, J., Lunak, P., Utama, U. P., & Scanning,P. (2021). ANALISIS MONITORING & KINERJA SISTEM KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN NMAP (STUDI KASUS : RAZ HOTEL & CONVENTION MEDAN). 35-43.
[4] Fatriawans, R. (2017). *Pengertian Jaringan Router*. *Pengertian Jaringan Router*, *2*, 1-5.
[5] HOSTING, R, J. (2022). *Apa itu Latency? Penyebab, dan Cara Menghitungnya?*
[6] Karim, R, SUMENDEP, S.S., & Koagouw,F. V.i (2021). Pentingnya Penggunaan Jaringan Wifi Dalam Kebutuhan Informasi Pemustaka. *Acta Diurna*, 5(2). 1-2
[7] KOMUKATAMA, D. G. (2020). P*ENGERTIAN KABEL LAN, FUNGSI, JENIS SERTA CARA MEMBUATNYA.* http://www.dataglobal.co.id/pengertian-kabel-lan-fungsi-jenis-serta-cara-membuatnya/
[8] T. Ariyadi, T. L. Widodo, N. Apriyanti, and F. S. Kirana, "Analisis Kerentanan Keamanan Sistem Informasi Akademik Universitas Bina Darma Menggunakan OWASP," *Techno.Com*, vol. 22, no. 2, pp. 418–429, 2023, doi: 10.33633/tc.v22i2.7562.
[9] Tamsir, "ANALISIS KUALITAS JARINGAN LAN DENGAN METODE QOS DI PT. SEMEN BATURAJA (PERSERO) Tbk," *Pros. Semin. Has. Penelit. Vokasi*, vol. 1, no. 1, pp. 150–157, 2019.