ANALISIS *MONITORING* SISTEM KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN SOFTWARE NMAP (STUDI KASUS JARINGAN DI UNIVERSITAS NUSA PUTRA)

Anggun Fergina[1)], Moch Ichwan Setia[2)], Maulana Yusuf[3)], M. Azmi Fauzan[4)], Dini Aryani[5)], Siti Farda Maulina[6)]

[1,2,3,4,5,6)]Teknik Informatika Universitas Nusa Putra

Jl. Raya Cibatu Cisaat No.21, Cibolang Kaler, Kec. Cisaat, Kabupaten Sukabumi, Jawa Barat 43152

e-mail: anggun.fergina@nusaputra.ac,id[1)], moch.ichwan_ti18@nusaputra.ac,id[2)], maulana.yusuf_ti20@nusaputra.ac.id[3)], azmi.fauzan_ti20@nusaputra.ac.id[4)], dini.aryani_ti20@nusaputra.ac.id[5)], siti.farda_ti20@nusaputra.ac.id[6)]

ABSTRAK

Keamanan Jaringan dalam jaringan komputer sangat penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah. Tujuan dari penelitian ini untuk mendeteksi port terbuka, mengetahui perangkat keras dan perangkat lunak yang dipakai dalam jaringan, me-monitoring jaringan dengan melakukan network scanning dan port scanning serta dapat mengeksplorasi sistem keamanan jaringan dan mengaudit keamanan jaringan yang digunakan. Sistem keamanan jaringan alias network security system merupakan perangkat yang bertugas untuk menghindari aktivitas tidak sah atau ilegal dalam sebuah jaringan komputer. Aktivitas tersebut berupa penyelundupan sebuah jaringan dengan tujuan mencuri data atau menanam virus di dalamnya. Jaringan komputer atau (computer network) adalah jaringan telekomunikasi yang memungkinkan antar komputer untuk saling berkomunikasi dengan bertukar data. Tujuan dari jaringan komputer adalah agar dapat mencapai tujuannya, setiap bagian dari jaringan komputer dapat meminta dan memberikan layanan (service). NMAP adalah singkatan dari Network Mapper yang merupakan sebuah tool atau alat yang bersifat open source. Alat ini hanya digunakan secara khusus untuk eksplorasi jaringan serta melakukan audit terhadap keamanan dari jaringan.

Kata kunci: *Computer Network, Keamanan Jaringan Komputer, NMAP*

ABSTRACT

Network Security in computer networks is very important to monitor network access and prevent unauthorized use of network resources. The purpose of this study is to detect open ports, find out the hardware and software used in the network, monitor the network by performing network scanning and port scanning and can explore network security systems and audit the network security used. A network security system, aka a network security system, is a device whose job is to prevent unauthorized or illegal activities on a computer network. This activity is in the form of smuggling a network with the aim of stealing data or planting viruses in it. A computer network or (computer network) is a telecommunications network that allows computers to communicate with each other by exchanging data. The purpose of a computer network is to achieve its goals, every part of a computer network can request and provide services. NMAP stands for Network Mapper which is an open source tool or tool. This tool is only used specifically for network exploration and auditing the security of the network.

Keywords : *Computer Network, Computer Network Security, NMAP*

I. PENDAHULUAN

Pengamanan Jaringan Komputer sangat diperlukan seiring berkembangnya teknologi dan internet. Berbagai cara dilakukan untuk mempertahankan pengamanan dari ancaman yang beragam, baik ancaman fisik, virus, trojan, dan serangan-serangan lainnya. Banyak teknik yang dapat mendeteksi keamanan jaringan seperti seperti packet sniffing, network scanning, dan monitoring layanan,. Aplikasi layanan jaringan sendiri mungkin mempunyai beberapa kelemahan, seperti kesalahan pemrograman, penggunaan autentikasi atau password yang lemah, sensitive data tidak terenkripsi atau mengijinkan koneksi dari berbagai alamat IP dan lain sebagainya. Kelemahan-kelemahan tersebut memungkinkan host yang menyediakan layanan tersebut rentan terhadap serangan. Oleh karena itu sebaiknya host hanya menyediakan layanan yang diperlukan saja, atau dengan kata lain meminimalkan port yang terbuka.

Universitas Nusa Putra merupakan kampus yang terletak di Sukabumi Jawa Barat, saat ini Universitas Nusa putra berkembang sangat pesat, bisa kita lihat dari gencarnya pembangunan, juga jumlah mahasiswa yang semakin meningkat setiap tahun nya. Universitas Nusa Putra memiliki 4000 Mahasiswa di tahun 2022 ini, dengan mahasiswa yang banyak tentunya banyak fasilitas yang dapat digunakan di kampus, salah satunya wifi kampus. Jaringan internet di kampus ini sudah cukup baik, namun terkadang jika banyak penggunanya maka jaringan nya menjadi tidak stabil. Oleh karena itu, monitoring keamanan jaringan juga tidak kalah pentingnya dari perkembangan yang lain, karena semakin banyak civitas akademik maka semakin banyak pula para pengguna jaringannya. Selain untuk menjaga kestabilan jaringan, monitoring ini juga ditujukan untuk mencegah terjadinya serangan pada jaringan.

Nmap di desain untuk dapat melakukan scan jaringan yang besar, juga dapat digunakan untuk melakukan scan host tunggal. NMAP adalah singkatan dari Network Mapper, merupakan tool opensource yang digunakan untuk eksplorasi dan audit keamanan jaringan. Nmap menggunakan paket IP untuk menentukan host-host yang aktif dalam suatu jaringan, port-port yang terbuka, sistem operasi yang dipunyai, tipe firewall yang dipakai.

II. TINJAUAN PUSTAKA

A. Konsep Dasar Jaringan

Jaringan komputer adalah kumpulan beberapa komputer (dan perangkat lain seperti router, switch dan sebagainya) yang saling terhubung satu sama lain melalui media perantara. Media perantara ini bisa berupa media kabel ataupun media tanpa kabel (Iwan Sofana, 2013).

Jaringan komputer (jaringan) adalah jaringan telekomunikasi yang memungkinkan antar komputer untuk saling berkomunikasi dengan bertukar data. Tujuan dari jaringan komputer adalah agar dapat mencapai tujuannya, setiap bagian dari jaringan komputer dapat meminta dan memberikan layanan (service). Pihak yang meminta/menerima layanan disebut klien (client) dan yang memberikan/mengirim layanan disebut peladen (server). Desain ini disebut dengan sistem clientserver, dan digunakan pada hampir seluruh aplikasi jaringan komputer (curlie.org, 2019).

B. Sistem Keamanan Jaringan Komputer

Dalam bukunya “An Analysis of security incidents on the internet”, menurut John D. Howard (1997), yang menyatakan bahwa Keamanan komputer merupakan suatu tindakan pencegahan perangkat dari agresi pengguna personal komputer atau pengakses jaringan yang bukan bertanggung jawab.

Menurut Gollmann pada tahun 1999 dalam bukunya yang berjudul “Computer Security” menyatakan bahwa: Keamanan suatu komputer merupakan berhubungan dengan pencegahan diri dan deteksi terhadap tindakan yang mengganggu yang tidak dikenali di dalam sistem komputer. Pada keamanan sistem komputer yang harus dilakukan adalah untuk mempersulit orang lain mengganggu sistem yang sedang digunakan, baik menggunakan komputer yang sifatnya pribadi, jaringan lokal ataupun jaringan global. Harus dimastikan sistem dapat berjalan dengan baik atau lancar serta kondusif, selain itu program dari aplikasinya masih dapat dipakai tanpa adanya suatu masalah.

Menurut (Garfinkel dan Spafford, 2018), seorang ahli dalam computer security, menyatakan bahwa “A computer is secure if you can depend on it and its software to behave as you expect (intend). Trust describes our level of confidence that a computer system will behave as expected. (intended)" yang dapat

diartikan bahwa komputer dikatakan aman apabila dapat diandalkan serta perangkat lunaknya bekerja sesuai dengan apa yang diharapkan.

Dalam menjaga kemanan jaringan, diterapkan konsep atau hukum dasar yang biasa disebut dengan CIA yang merupakan, Confidentiality (kerahasiaan), Integrity (integritas),dan Availability (ketersediaan). Confidentiality adalah seperangkat aturan yang membatasi akses ke informasi. Integrity adalah jaminan bahwa informasi itu dapat dipercaya dan akurat, serta Availability yang merupakan konsep dimana informasi tersebut selalu tersedia ketika dibutuhkan oleh orang-orang yang memiliki akses atau wewenang.

C. *NMAP (Network Mapper)*

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 diantara 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.

Nmap melaporkan kombinasi status open|filtered dan closed|filtered ketika tidak dapat menentukan status manakah yang menggambarkan sebuah port. Tabel port mungkin juga menyertakan detil versi software ketika diminta melakukan pemeriksaan versi. Ketika sebuah pemeriksaan protokol IP diminta (-sO), Nmap memberikan informasi pada protokol IP yang didukung alih-alih port-port yang mendengarkan.

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 respon dari komputer target. Dengan cara seperti ini, user program scanner dapat memperoleh informasi yang berharga dari host yang mejadi target (Rosenelly dan Pulungan, 2011).

III. METODE PENELITIAN

A. Metode Penelitian

Penelitian yang penulis lakukan menggunakan metode Analisis Monitoring dengan teknik port scanning. Port Scanning merupakan aplikasi yang digunakan untuk melihat informasi atau status dari protocol dan port yang terbuka dari sebuah perangkat. Dengan aplikasi ini bisa jadi merupakan sebuah awal dari dimulainya serangan terhadap sebuah resource di jaringan. Tempat penelitian yang dilakukan yaitu di Universitas Nusa Putra.

B. Metode Pengumpulan Data

Pengumpulan data dilakukan dengan tiga metode yaitu: Studi pustaka, dengan mengumpulkan data dari berbagai buku, artikel, jurnal, dan sebagainnya yang berhubungan dengan penelitian sebagai pendukung pembuatan penelitian. Observasi, dengan mengamati objek yang dianalisis monitoring secara langsung. Wawancara dengan memberikan pertanyaan kepada petugas Universitas Nusa Putra yang bertanggung jawab di bidangnya.

C. Peralatan Pendukung

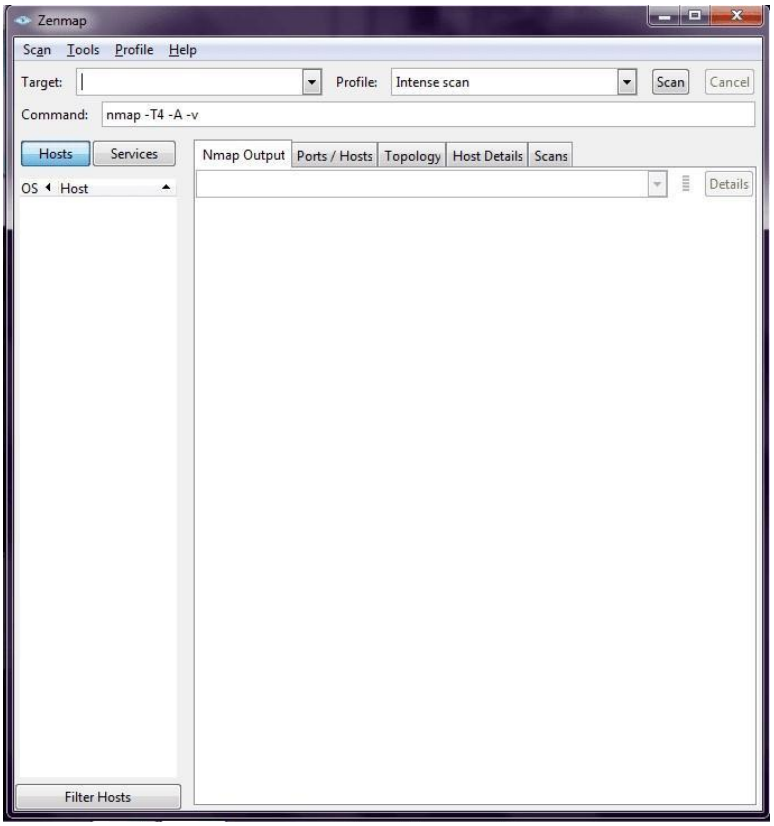
Alat dan peralatan yang mendukung penelitian ini adalah sebagai berikut: Laptop, Komputer Client, OS Windows 10, Software Nmap.

IV. HASIL DAN PEMBAHASAN

A. Pengujian Jaringan Awal

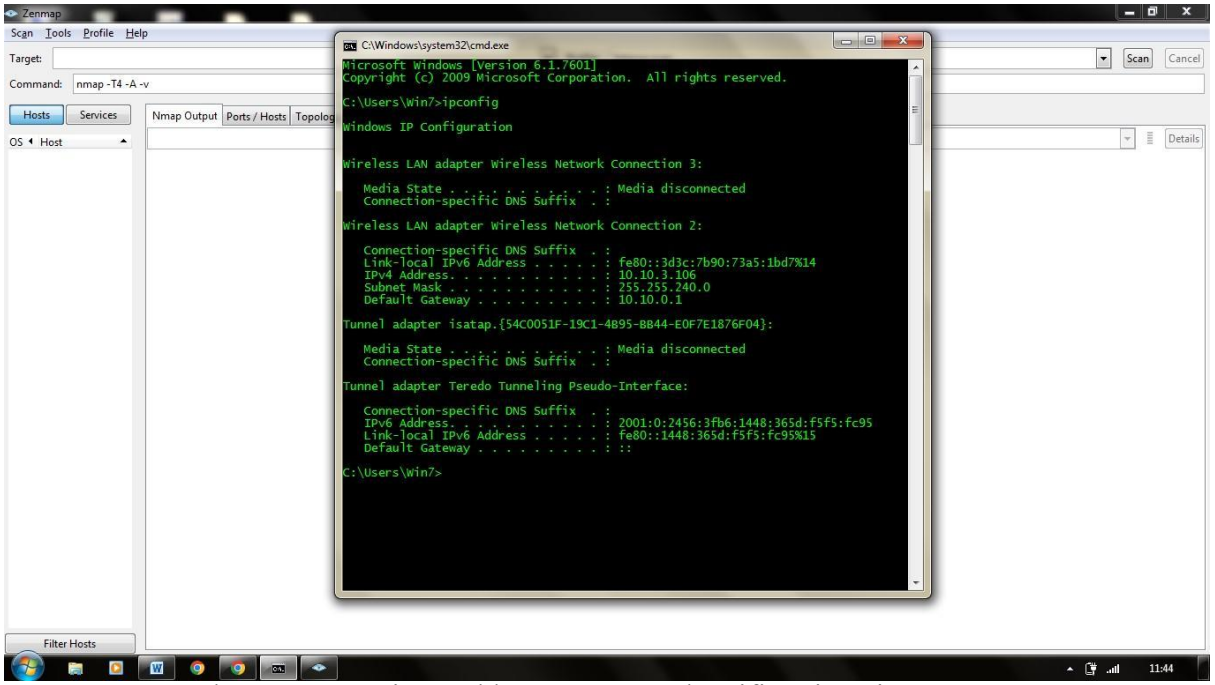
Langkah prtama yang di lakukan adalah membuka aplikasi NMAP untuk melakukan port scanner. Berikut logo aplikasi beserta tampilan awal NMAP

Gambar 1 logo aplikasi NMAP



Gambar 2 tampilan awal aplikasi NMAP

Langkah selanjutnya yang di lakukan adalah mencari ip addrerss dari ssid wifi Universitas Nusaputra. Menggunakan komputer yang telah terhubung pada jaringan wifi Universitas NusaPutra dengan mengunakan perintah ipconfig di aplikasi CMD.



Gambar 3. Mencari IP Address Target pada wifi Universitas Nusaputra

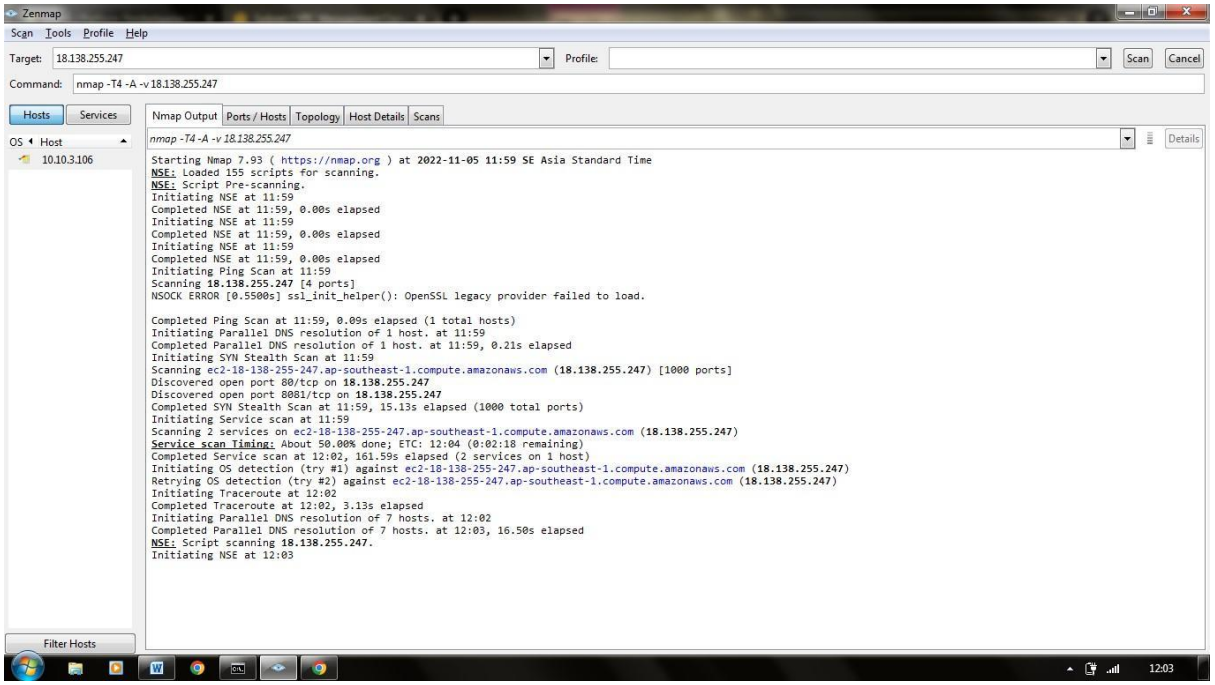
Pada gambar di atas dapat ditahui host gateway dari ssid wifi Universitas Nusaputra yang akan dilakukan scanning jaringan menggunakan software Nmap dengan melihat hasil dari Ethernet adapter Ethernet. Berikut daftar pada hasilnya:

a. Default Gateway: IP Address 10.10.0.1
   Default Gateway adalah gerbang jaringan pada perangkat Komputer user yang terhubung dengan jaringan LAN.
b. Subnet Mask: IP Address 255.255.240.0
   Subnet Mask dengan alamat kelas C. Sub prefinya yaitu /24
c. Ipv4: IP Address 10.10.3.106
   Merupakan alamat IP Address Laptop user dengan protocol IP versi 4.

B. Pengujian Jaringan Akhir

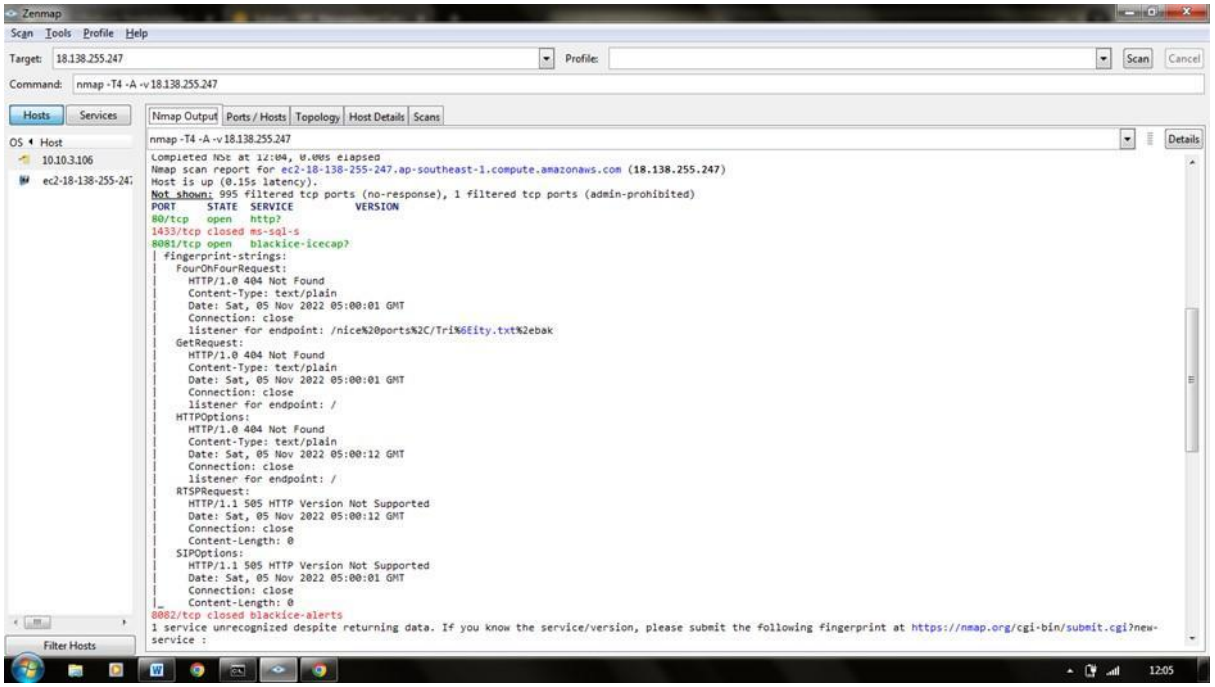
Pengujian Host Target Jaringan pada Komputer

Setelah megetahui ip address yang akan menjadi target untuk di lakukannya port scanner langkah selanjutnya adalah melakukan port scanner pada jaringan Universitas Nusa Putra dan website siakad.nusaputra.ac.id

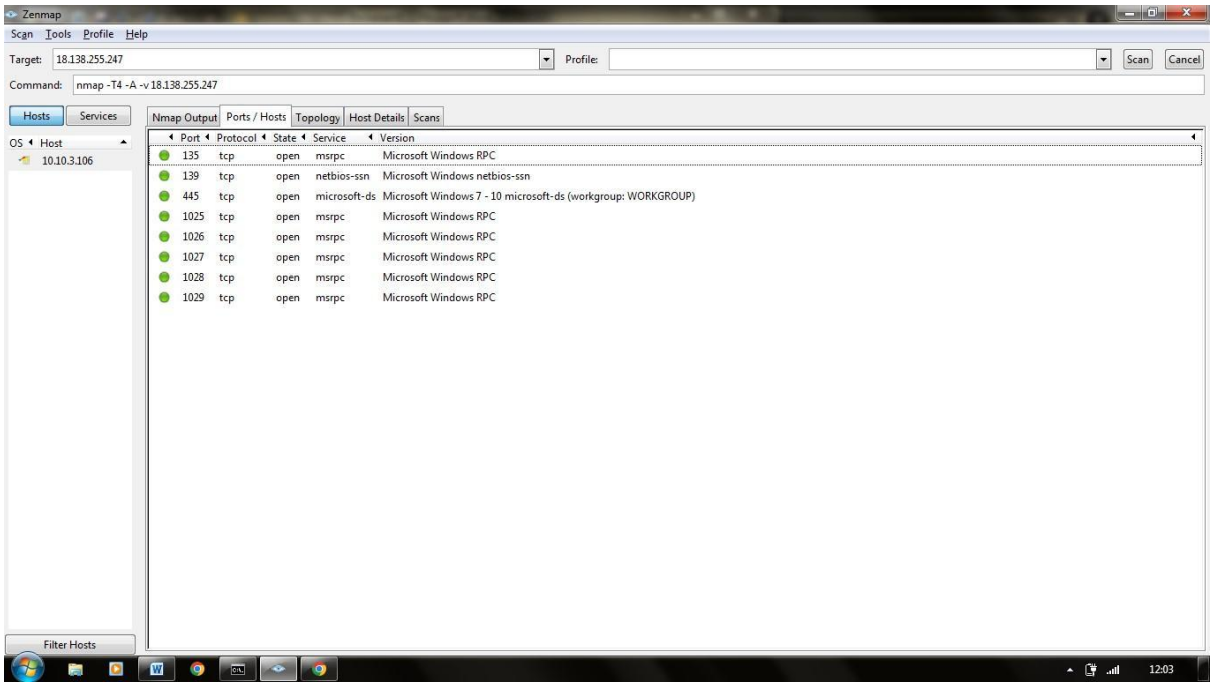


Gambar 4. Pengujian Host Target

Pada gambar di atas menggunakan perintah nmap –T4 –A –v 18.138.255.247. Saya melakukan scanning pada host target berupa IP Default Gateway jaringan wifi Universitas Nusaputra yang digunakan. Saya menggunakan perintah flag –T4 untuk mempercepat hasil scanning, flag –A untuk melakukan Aggresive Detection dan flag –v untuk menampilkan hasil Nmap lebih detil.



Gambar 5. Hasil Port Scanning 18.138.255.247



Gambar 6. Hasil Port Scanning siakad.nusaputra.ac.id/

Pada gambar di atas merupakan hasil dari *scanning* yang dilakukan oleh nmap pada website siakad.nusaputra.ac.id/ Pada hasil menunjukkan beberapa port yang terbuka (*open*) dan ter-*filtered*. beberapa port yang terbuka ini bisa jadi merupakan sebuah awal dari dimulainya serangan terhadap sebuah resource di jaringan

V. PENUTUP

A. Kesimpulan

Dari hasil penelitian "Analisis Sistem Keamanan Jaringan Komputer Menggunakan Software NMAP" (Studi Kasus di Universitas Nusa Putra). Didapat bahwa Nmap mampu melakukan scanning dan mendeteksi port-port mana saja yang terbuka pada sebuah jaringan. Menguraikan dan memberikan gambaran sebuah jaringan serta setiap perangkat, port, atau service yang terhubung dengannya. Menemukan celah-celah keamanan yang kemungkinan dapat dieksploitasi di sebuah jaringan.

Port Scanner merupakan aplikasi yang digunakan untuk melihat informasi atau status dari protocol dan port yang terbuka (open) dari sebuah perangkat. Dengan aplikasi ini bisa jadi merupakan sebuah awal dari dimulainya serangan terhadap sebuah resource di jaringan.

B. Saran

Dari hasil Port Scanner yang di lakukan di jaringan Universitas Nusa Putra dan situs siakad.nusaputra.ac.id menunjukkan beberapa port yang terbuka (*open*) dan ter-*filtered*. Port yang terbuka ini bisa jadi merupakan sebuah awal dari dimulainya serangan terhadap sebuah resource di jaringan. Ada beberapa saran yang dapat dijadikan pertimbangan untuk mencegah serangan terhadap sebuah resource di jaringan diantaranya:

1. Monitoring traffic secara reguler
   Hal pertama yang perlu di lakukan untuk mencegah serangan adalah dengan memantau traffic situs web secara rutin. Sehingga, kamu memiliki gambaran jelas tentang bagaimana tren traffic di website.
2. Mengunakan Firewall

Firewall merupakan contoh jenis aplikasi network security yang paling banyak ditemui. Firewall adalah sebuah tools yang berfungsi sebagai dinding penghalang antara jaringan internal dan eksternal. Tujuan penghalang tersebut yakni untuk memastikan koneksi tetap aman sebelum dialihkan ke jaringan eksternal. Menggunakan proteksi berlapis adalah cara terbaik untuk mencegah serangan pada website.

3. Mengunakan proteksi berlapis
   Kamu bisa menambah keamanan situs web dengan menggunakan beberapa layanan penyedia proteksi, anti-spam, content filtering, Virtual Private Network (VPN), maupun sistem keamanan lainnya.
4. Bangun redundancy server
   Membangun redundancy dengan menyediakan server tambahan yang dapat digunakan pada saat runtime untuk pencadangan, penyeimbangan beban, atau penghentian sementara server utama saat tiba waktu pemeliharaan.

VI. Daftar Pustaka