Deteksi ARP Spoofing pada Jaringan Wireless Menggunakan Metode String Matching dengan Algoritma Boyer Moore dan Brute Force

1st Syafrullah Anwar
Fakultas Informatika
Universitas Telkom
Bandung, Indonesia
syafrullah@student.telkomuniversity.ac.id

2nd Siti Amatullah Karimah
Fakultas Informatika
Universitas Telkom
Bandung, Indonesia
karimahsiti@telkomuniversity.ac.id

3rd Erwid Musthofa Jadied
Fakultas Informatika
Universitas Telkom
Bandung, Indonesia
jadied@telkomuniversity.ac.id

Abstrak—Address Resolution Protocol (ARP) adalah protokol yang digunakan untuk menerjemahkan alamat Internet Protocol (IP) menjadi alamat Media Access Protocol (MAC) pada suatu jaringan. Sebuah ARP request secara broadcast untuk mendapatkan alamat perangkat MAC tujuan yang dimana berguna untuk komunikasi antar perangkat. Ketika host menerima alamat ARP request yang ditujukan kepadanya, perangkat penerima akan mengirimkan paket ARP reply kepada perangkat pengirim. Protokol ARP mempunyai celah keamanan yang membuat celah keamanan tersebut dapat diserang oleh spoofing. ARP spoofing adalah serangan yang mengirimkan ARP palsu yang sudah dimodifikasi untuk meracuni ARP cache table korban, serangan ini mendukung terjadinya serangan jaringan komputer lainnya seperti denial of service (DoS) attack, Man in the Middle Attack, dan lain-lain. Pada penelitian ini dilakukan deteksi terhadap ARP spoofing dengan mencari sebuah MAC Address yang telah diubah oleh Attacker menggunakan string matching dengan algoritma boyer moore dan brute force.

Kata kunci—ARP, ARP spoofing, string matching, boyer moore, brute force

Abstract—Address Resolution Protocol (ARP) is a protocol used to translate Internet Protocol (IP) addresses into Media Access addresses Protocol (MAC) on a network. An ARP request broadcast for get the MAC address of the destination device which is useful for communication between devices. When the host receives the address of the ARP request that addressed to it, the receiving device will send an ARP reply packet to the sending device. The ARP protocol has a significant security vulnerability make these security holes can be attacked by spoofing. ARP spoofing is an attack that sends a fake ARP that has been modified to poison the victim's ARP cache table, this attack supports the occurrence of attacks other computer networks such as denial of service (DoS) attacks, Man in the Middle Attack, and others. In this study, detection of ARP spoofing was carried out by looking for a MAC Address that has been changed by the Attacker using string matching with Boyer Moore algorithm and brute force.

Keywords—ARP, arp spoofing, string matching, boyer moore, brute force

I. PENDAHULUAN

A. Latar Belakang

Lebih dari 3,73 milliar orang di seluruh dunia memanfaatkan akses internet dan memanfaatkannya dalam aktivitas sehari-hari [1], dengan itu ancaman serangan bisa saja terjadi ketika kita menggunakan jaringan wireless yang dapat menyebabkan data pengguna dicuri oleh pihak yang tidak bertanggung jawab,
ancaman serangan Spoofing adalah termasuk salah satu serangan dengan frekuensi tertinggi [2] yang terjadi di jaringan wireless.

ARP (Address Resolution Protocol) adalah sebuah protokol dalam TCP/IP yang bertanggung jawab dalam menerjemahkan alamat IP ke alamat MAC (Media Access Control) Address, ARP spoofing attack alamat MAC dapat dimodifikasi oleh penyerang dengan menautkan alamat MAC-nya sendiri ke alamat IP yang diberikan [3], sehingga membuatnya rentan terhadap serangan spoofing. ARP
spoofing adalah serangan yang mengirimkan ARP palsu yang sudah dimodifikasi untuk meracuni ARP cache table korban, serangan ini mendukung terjadinya serangan jaringan komputer lainnya seperti denial of service (DoS) attack, Man in the Middle Attack, dan lain-lain.

Penelitian yang dilakukan juga menggunakan aplikasi nettcut untuk melakukan serangan spoofing yang dilakukan pada jaringan WLAN (Wireless Local Area Network) juga mendapatkan persentase tinggi [4]. Salah satu upaya untuk meminimalkan kemungkinan adanya serangan yang terjadi dalam suatu jaringan komputer ketika terkoneksi internet yaitu dengan membangun suatu sistem yang nantinya mampu meningkatkan keamanan jaringan. Salah satu teknik yang digunakan untuk melindungi kemanan jaringan yaitu dengan membangun sistem yang menggunakan metode string matching dengan algoritma boyer moore dan brute force, string matching akan mencari MAC address yang mencurigakan, kemudian sistem yang dibangun akan memberikan laporan atau notifikasi bahwa komputer sedang disadap.

B. Topik dan Batasannya

Permasalahan pada tugas akhir ini akan membahas tentang bagaimana cara kerja metode *string matching* untuk mendeteksi ARP spoofing menggunakan algoritma *boyer moore* dan *brute force*, serta bagaimana kecepatan waktu deteksi pada ARP spoofing menggunakan

metode *string matching* dengan algoritma *boyer moore* dan *brute force*.

C. Tujuan

Tujuan penelitian ini adalah untuk Merancang string matching dengan algoritma boyer moore untuk mendeteksi perubahan MAC address dan Melakukan analisis waktu deteksi pada sistem yang dibangun dengan metode string matching dengan algoritma boyer moore dan brute force.

II. KAJIAN TEORI

Pada penelitian oleh Ilham Firdaus. et al [6] yang menguji aplikasi yang dibangun menggunakan metode string matching dengan algoritma *Knutt Morris Pratt* (KMP) pada *Intrusion Detection System* (IDS) Snort, penelitian ini bertujuan untuk mendeteksi serangan *ARP Spoofing* pada jaringan wifi publik, metode string matching dengan algoritma KMP diterapkan untuk mencari pola teks pada file snort.conf dan file logging snort, sehingga dapat mempermudah konfigurasi IDS snort dan memberikan alert bahwa komputer sedang disadap. Hasil dari penelitian ini mendapat kesimpulan bahawa metode ini mampu mendeteksi bahwa jaringan yang sedang digunakan sedang disadap.

Kemudian penelitian yang dilakukan oleh Veny Charnita Br Ginting. et al [7] yang melakukan pendeteksian serangan ARP Spoofing dengan memeriksa log file dan melaukan analisis pada paket-paket data yang beredar pada jaringan komputer, implementasi pengujian ini dilakukan dengan menganalisis paket ARP. Untuk melakukan deteksi serangan ini maka digunakan sebuah detektor host yang melakukan analisis lalu lintas paket ARP pada jaringan tersebut.

Kemudian penelitian yang dilakukan oleh Imam Ahmad. et al [8] melakukan pengecekan terhadap judul skripsi/TA mahasiswa yang satu dengan yang lain baik secara disengaja maupun tidak disengaja yang bertujuan untuk menghidari plagiat judul, metode yang digunakan yaitu matching dan pencocokan antara pattern dan text dengan memperhatikan urutan yang dimulai dari karakter paling kanan terlebih dahulu kemudian kekiri. Dengan penerapan algoritma Boyer Moore, hasil pengujian lainnya menunjukkan bahwa algoritma ini membutuhkan waktu yang cepat dalam proses string matching. Dengan percobaan 100 sampai 500 data rata-rata adalah 34%.

Kemudian penelitian yang dilakukan oleh Desti Mualfah. et al [9] menggunakan Intrusion Detection System (IDS) seperti snort. Snort adalah sebuah tools yang digunakan untuk mendeteksi serangan, semua aktivitas lalu lintas jaringan tersimpan didalam log file, kemudian akan dianalisis pada log file tersebut. Pada penelitian ini fokus kepada serangan yang terjadi di jaringan komputer.

Kemudian penelitian yang dilakukan oleh Ervin Kusuma Dewi. et al [10] mengimplementasikan snort dan menganalisis log snort dengan menggunakan Network Forensik dengan melakukan investigasi dari data serangan yang tersimpan pada log snort, dengan hasil pengujian bahwa snort dapat mendeteksi serangan dan akan memberikan alert sehingga dapat mempermudah administrator menangani hal tersebut. Dan hasil lainnya dapat melihat bukti serangan yang didalamnya terdapat tanggal dan bulan saat menyerang, IP penyerang, jenis serangan, waktu serangan dan jumlah packet yang dikirim

Kemudian penelitian yang dilakukan oleh Darmawan Utomo. et al [5] melakukan pengujian algoritma *Boyer Moore* (BM), *Knuth Morris Pratt* (KMP), *Brute Force* (BF), dan *Karp Rabin* (KR) untuk digunakan pada pencarian pola di alkitab. Dari penelitian ini waktu rata – rata untuk mencari pola sebanyak 280 pola sebagai berikut, Boyer Moore (BM) : 0,92 detik, Brute Force (BF) : 0,98 detik, Knuth Morris Pratt (KMP) : 0,99 detik, Karp Rabin (KR) : 3,46 detik, dapat disimpulkan algoritma boyer moore adalah algoritma yang paling efisien untuk digunakan dalam proses pencarian pola.

A. ARP (Address Resolution Protocol)

Address Resolution Protocol (ARP) adalah proses pencarian alamat MAC (Media Access Protocol) komputer dalam sebuah jaringan. Pada dasarnya yaitu ARP menerjemahkan IP address ke MAC address dan bekerja pada layer 2 yaitu Data Link Layer**.** ARP Spoofing pada jaringan bekerja ketika dua perangkat terhubung dalam jaringan yang dimana masing – masing perangkat mempunyai IP Address dan MAC Address yang berbeda.

B. ARP Spoofing Attack

ARP Spoofing Attack merupakan suatu kejahatan atau serangan yang dapat terjadi pada suatu jaringan dengan cara memalsukan isi table ARP yang terdapat pada satu host didalam jaringan [12]. Cara kerja penyerang yaitu dengan cara memodifikasi MAC Address, sehingga memiliki dua IP Address tetapi hanya mempunyai satu MAC Address. Ketika Perangkat 1 dan 2 saling bertukar data, maka paket data tersebut terlebih dahulu melewati perangkat attacker, sehingga attacker dapat memantau lalu lintas dari perangkat 1 dan perangkat 2.

C. String Matching

String adalah kumpulan karakter yang dapat berisi spasi dan angka. String Matching adalah teknik untuk memecahkan masalah di berbagai bidang seperti, pemrosesan Bahasa alami, pemrosesan gambar, pemrosesan ucapan, visi komputer dan pengenalan pola. Metode ini digunakan untuk mengindeks dan mengambil informasi dari database, fungsi dari String Matching yaitu menemukan abjad yang sesuai dari String teks dan String pattern.

D. Boyer Moore

Algoritma *Boyer Moore* adalah salah satu algoritma untuk string matching, algoritma ini memiliki kecepatan yang lebih baik dibandingkan dengan algoritma brute force karena memiliki metode yang berbeda dalam pencariannya. Pertama *pattern* akan disamakan dengan teks dari kiri, tetapi pengecekan karakter dimulai dari kanan dan sistem akan melakukan pengecekan dari *pattern* kanan sampai kiri, jika ada yang tidak cocok maka ada tiga pilihan. Pertama yaitu jika karakter salah yang salah ada di teks berada pada posisi kiri *pattern*, maka karakter dalam pattern tersebut akan disejajarkan dengan karakter yang sama didalam teks dan program akan mengecek dari kanan lagi. Kedua, jika karakter salah yang ada di teks berada pada posisi kanan pattern makan pattern akan di geser sebanyak satu karakter dan program akan mencari ke karakter selanjutnya. Ketiga, jika karakter salah yang ada

di teks tidak ada di dalam *pattern* sama sekali, maka *pattern* akan di geser ke kanan sampai melewati karakter tersebut.

E. Brute Force

Algoritma *Brute Force* dalam string matching adalah algoritma pencocokan string yang pencarian pattern akan dicari secara satu per satu dalam suatu teks dari kiri atau dari kanan sampai akhir string tersebut. Jika *pattern* yang tidak match dengan teks, maka *pattern* akan bergerser satu kali dan akan melakukan pencarian dari awal *pattern* tersebut. Berikut ilustrasi dari gambar pencocokan string.

III. METODE

Sistem ini dirancang untuk melakukan pendeteksian terhadap sejumlah aktifitas mencurigakan yang sedang terjadi pada jaringan komputer. Sistem akan menampilkan MAC address aktual dan MAC address saat ini, sistem akan membandingkan MAC address actual dan MAC address saat ini, ketika MAC address aktual sama dengan MAC address saat ini maka sistem berjalan terus – menerus karena tidak terjadi perubahan MAC address, tetapi ketika MAC address aktual tidak sama dengan MAC address saat ini, maka sistem akan mendeteksi terjadi perubahan MAC address di tabel ARP. Kemudian sistem akan mengeluarkan notifikasi bahwa komputer telah disadap.

A. Perancangan Arsitektur Jaringan

akan disimulasikan dijaringan *Wireless Local Area Network* (WLAN) yang dimana terdapat 2 host attacker, 2 host client dan akan terhubung di satu router atau jaringan yang sama. Semua host akan terhubung dalam satu jarigan yang sama dengan menggunakan jaringan *Wireless Local Area Network* (WLAN).

GAMBAR 1
TOPOLOGI JARINGAN

B. Perancangan Host Client

Host akan menggunakan sistem operasi Windows dan akan terhubung di jaringan. Host akan mengunjungi website dan akan menginputkan username dan password.

C. Perancangan Host Attacker

Perancangan host attacker ini akan di install pada virtual box dan menggunakan sistem operasi linux dan akan menggunakan tools ettercap sebagai tools untuk serangan sniffing, dengan menggunakan tools ettercap host attacker dapat mendapat informasi dari host client yaitu username dan password.

D. Skenario Pengujian

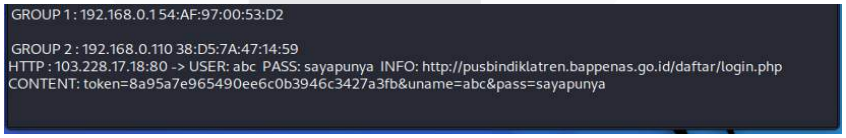
Berikut skenario pengujian yang akan dilakukan untuk mengukur akurasi waktu serangan sebagai berikut:

TABEL 1
SKENARIO PENGUJIAN BOYER MOORE DAN BRUTE FORCE

Skenario		
No.	**Boyer Moore**	**Brute Force**
1.	Host attacker melakukan satu kali serangan ARP Spoofing dan host client akan menjalankan program deteksi menggunakan boyer moore.	Host attacker melakukan satu kali serangan ARP Spoofing dan host client akan menjalankan program deteksimenggunakan brute force.
2.	Host attacker melakukan dua kali serangan ARP Spoofing dalam waktu yang berbeda dan host client akan menjalankan program deteksi menggunakan boyer moore.	Host attacker melakukan dua kali serangan ARP Spoofing dalam waktu yang berbeda dan host client akan menjalankan program deteksi menggunakan brute force.
3.	2 Host attacker melakukan serangan ARP Spoofing dalam waktu yang sama dan host client akan menjalankan program deteksi menggunakan boyer moore.	2 Host attacker melakukan serangan ARP Spoofing dalam waktu yang sama dan host client akan menjalankan program deteksi menggunakan brute force.

IV. HASIL DAN PEMBAHASAN

A. Identifikasi Masalah



GAMBAR 2
USERNAME DAN PASSWORD

Data dari penelitian ini diambil pada website dan membuktikan hasil dari penyerangan ARP *Spoofing* bahwa pengguna atau host client tidak menyadari username dan password pengguna telah dicuri oleh penyerang seperti gambar dibawah ini.

B. Hasil Pengujian

Berdasarkan tahapan skenario dan simulasi akan dilakukan sebanyak 30 kali waktu deteksi dan dapat melihat waktu atau durasi yang dibutuhkan dalam mendeteksi serangan seperti pada tabel dibawah ini.

TABEL 2
HASIL SKENARIO UJI BOYER MOORE

No.	Skenario Brute Force	Waktu Deteksi (ms)
1.	Host attacker melakukan satu kali serangan spoofing dan host client akan menjalankan program deteksi menggunakan brute force.	0.00357
2.	Host attacker melakukan dua kali serangan *spoofing* dalam waktu yang berbeda dan host client akan menjalankan program deteksi menggunakan brute force.	0.00393
3.	2 Host attacker melakukan serangan *spoofing* dalam waktu yang sama dan host client akan menjalankan program deteksi menggunakan brute force.	0.00406

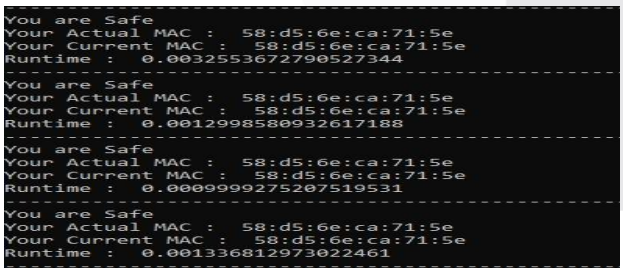
TABEL 3
HASIL SKENARIO UJI BRUTE FORCE

No.	Skenario Boyer Moore	Waktu Deteksi (ms)
1.	Host attacker melakukan satu kali serangan *spoofing* dan host client akan menjalankan program deteksi menggunakan boyer moore.	0.00211
2.	Host attacker melakukan dua kali serangan *spoofing* dalam waktu yang berbeda dan host client akan menjalankan program deteksi menggunakan boyer moore.	0.00229
3.	2 Host attacker melakukan serangan *spoofing* dalam waktu yang sama dan host client akan menjalankan program deteksi menggunakan boyer moore.	0.00233

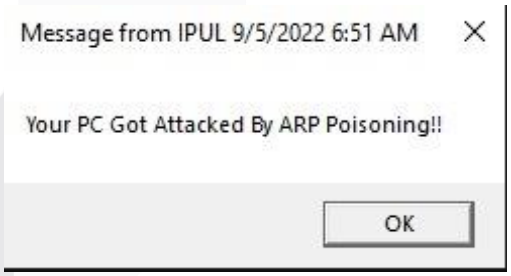
C. Analisis Hasil Pengujian

1. Sebelum terjadi spoofing dan menggunakan sistem deteksi

Ketika sistem berjalan dan MAC address masih tetap sama atau belum ada perubahan maka sistem akan berjalan terus – menerus sampai menemukan perubahan MAC address, seperti yang pada gambar dibawah ini.

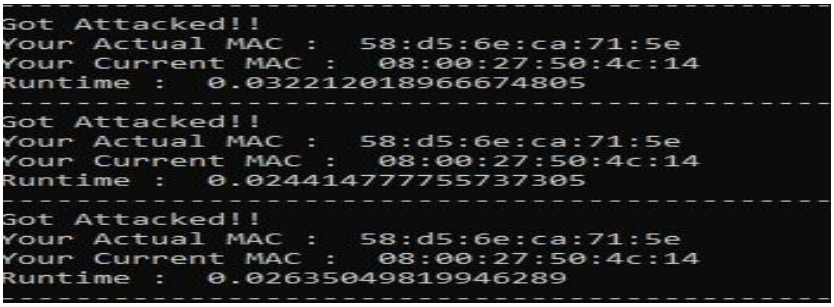


GAMBAR 3
TIDAK TERJADI PERUBAHAN MAC ADDRESS



GAMBAR 4
TERJADI PERUBAHAN MAC ADDRESS

2. Setelah terjadi spoofing dan menggunakan sistem deteksi



GAMBAR 5
NOTIFIKASI ATAU ALERT

Ketika sistem berjalan dan terjadi perubahan pada MAC address maka sistem akan memberitahu atau menampilkan notifikasi bahwa komputer sedang disadap menggunakan serangan spoofing, seperti yang ada pada gambar dibawah ini.

V. KESIMPULAN

Dalam penelitian ini dengan merancang dan membangun sistem deteksi ARP spoofing sebagai mekanisme keamanan tambahan yang dapat mencegah terjadinya spoofing yang dapat merugikan pengguna pada penggunaan web. Hasil percobaan perubahan MAC address pada jaringan wireless menggunakan metode string matching dengan algoritma boyer moore dan brute force terbukti dapat mendeteksi terjadinya perubahan MAC address dengan waktu mendeteksi yang berbeda, dengan menggunakan algoritma boyer moore akan lebih efisien dibandingkan dengan algoritma brute force.

Salah satu langkah awal ketika terjadi spoofing yaitu dengan menambahkan VPN (Virtual Private Network) pada web ekstensi untuk membuat koneksi menjadi lebih aman dan menyamarkan alamat IP asli menjadi alamat IP lain sehingga orang lain tidak akan tahu alamat IP sebenarnya. Dengan mengaktifkan VPN pada saat terjadi serangan maka IP asli akan menjadi IP baru agar host attacker tidak mendapatkan informasi dari host client.

REFERENSI

[1] R. Pandita, "Internet a change agent: An overview of internet penetration and growth across the world," *International Journal of Information Dissemination and Technology*, vol. 7, no. 2, p. 83, 2017, doi: 10.5958/2249-5576.2017.00001.2.

[2] H. D. J. Jeong *et al.*, "Analysis and detection of anomalous network traffic," in *Proceedings - 2016 10th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2016*, Dec. 2016, pp. 403–408. doi: 10.1109/IMIS.2016.101.

[3] V. Rohatgi and S. Goyal, "A detailed survey for detection and mitigation techniques against ARP spoofing," in *Proceedings of the 4th International Conference on IoT in Social, Mobile, Analytics and Cloud, ISMAC 2020*, Oct. 2020, pp. 352–356. doi: 10.1109/I-SMAC49090.2020.9243604.

[4] M. I. Susanto, A. Hasad, and M. Amin Bakri, "Sistem Proteksi Jaringan Wlan Terhadap Serangan Wireless Hacking."

[5] K. Morris Pratt, B. Moore, D. Karp Rabin Pada, D. Utomo, E. Wijaya Harjo, and D. Utomo Eric Wijaya Harjo Handoko, "PERBANDINGAN ALGORITMA STRING SEARCHING BRUTE FORCE."

[6] Ilham Firdaus, Januar Al Amien, and S. Soni, "String Matching untuk Mendeteksi Serangan Sniffing (ARP Spoofing) pada IDS Snort," *Jurnal CoSciTech (Computer Science and Information Technology)*, vol. 1, no. 2, pp. 44–49, Oct. 2020, doi: 10.37859/coscitech.v1i2.2180.

[7] V. Charnita, B. Ginting, M. Data, and D. P. Kartikasari, "Deteksi Serangan ARP Spoofing berdasarkan Analisis Lalu Lintas Paket Protokol ARP," 2019. [Online]. Available: http://j-ptiik.ub.ac.id

[8] I. Ahmad, R. Indra Borman, G. G. Caksana, and J. Fakhrurozi, "SINTECH Journal | 53 IMPLEMENTASI STRING MATCHING DENGAN ALGORITMA BOYER-MOORE UNTUK MENENTUKAN TINGKAT KEMIRIPAN PADA PENGAJUAN JUDUL SKRIPSI/TA MAHASISWA (STUDI KASUS: UNIVERSITAS XYZ)", [Online]. Available: https://doi.org/10.31598

[9] D. Mualfah and I. Riadi, "Network Forensics For Detecting Flooding Attack On Web Server," 2017. [Online]. Available: https://sites.google.com/site/ijcsis/

[10] E. K. Dewi, "ANALISIS LOG SNORT MENGGUNAKAN NETWORK FORENSIC," *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 2, no. 2, Dec. 2017, doi: 10.29100/jipi.v2i2.370.

[11] B. Wijaya and A. Pratama, "Deteksi Penyusupan Pada Server Menggunakan Metode Intrusion Detection System (IDS) Berbasis Snort," *Sistem Informasi dan Komputer)*, vol. 09, pp. 97–101, doi: 10.32736/sisfokom.v9.i1.770.

[12] M. N. Hafizh, I. Riadi, and A. Fadlil, "Forensik Jaringan Terhadap Serangan ARP Spoofing menggunakan Metode Live Forensic," *Jurnal Telekomunikasi dan Komputer*, vol. 10, no. 2, p. 111, Aug. 2020, doi: 10.22441/incomtech.v10i2.8757.