Indonesian Journal on Data Science
ISSN 2987-7423 - Vol. 2, No. 1, July 2024, hlm 10-18

Analisis Transfer Data Pada Jaringan Terdampak *ARP Spoofing* Menggunakan Metode *ARP Poisoning*

Sudaryanto [a,1,*], Dwi Nugraheny [b,2,*], Kelfin Leo Dwi Prakoso [b3,*], Nurcahyani Dewi Retnowati [b,4,*], Haruno Sajati [b,5,*], Salam Aryanto [b.6,*]

[a,b] Program Studi Informatika. ITD Adisutjipto Yogyakarta
[1] sudaryanto@itda.ac.id*; [2]henynug@gmail.com; [3] kelfinnleo12@gmail.com, [4] ndewiret@gmail.com, [5]harunosajati@staff.itda.ac.id, [6] salam@itda.ac.id

* corresponding author

ABSTRAK

Jaringan yang terhubung dengan perangkat jaringan biasanya rentan terhadap peretasan. *Hacking* adalah suatu aktivitas yang memungkinkan seseorang atau kelompok mengubah atau mengambil data untuk kepentingan pribadi. Pengujian dan analisis untuk mengetahui kondisi dan mengukur tingkat keamanan sistem informasi intra kampus dan jaringan komputer ITDA Yogyakarta. Mendeskripsikan *security gap* dan mengukur tingkat keamanan perlu segera diperbaiki sehingga dapat membantu memperbaiki kegagalan dalam menjaga keamanan sistem informasi dan jaringan intra kampus ITDA Yogyakarta. Menggunakan *statistik deskriptif* dengan 20 unit PC sebagai sampel. Terdapat empat pengujian dalam penelitian ini dengan total keberhasilan 16 dari 20 sampel. Dari hasil *ARP SPOOFING* pada jaringan lokal dapat disimpulkan bahwa setelah jaringan lokal disusupi oleh penyerang dengan metode *ARP SPOOFING* maka trafik target akan dialihkan ke perangkat penyerang. Hal ini memungkinkan penyerang memantau dan memahami isi lalu lintas data di jaringan lokal. Mengubah alamat MAC penyerang sangat diperlukan karena jika MAC tidak diubah maka lalu lintas jaringan tidak akan dialihkan ke perangkat penyerang.

ARTICLE INFO

Article history
Received: 10 Juni 2024
Revised: 27 Juni 2024
Accepted: 2 July 2024

Keywords
Penetration Testing
Web Application Security
Descriptive Statistic
ARP Poisoning
Ettercap

I. Pendahuluan

Jaringan *client server* diartikan sebagai suatu perancangan jaringan komputer yang mana perangkat *client* melakukan proses meminta data [1], dan *server* yang bertugas untuk memberikan *respon* dari *feedback* yang berupa data. *Client* adalah individu yang terhubung ke *server* untuk meminta data atau layanan dari *server* sementara *server* adalah individu yang menyediakan data atau layanan yang diharapkan oleh *client* [2].

Masalah keamanan jaringan komputer merupakan hal yang sangat penting dan perlu diperhatikan dalam pengembangan jaringan komputer. Peretasan merupakan suatu kegiatan yang memungkinkan seseorang atau kelompok untuk mengubah atau mengambil data untuk kepentingan pribadi. Contohnya seperti upaya untuk mendapatkan informasi data seseorang dengan teknik pengelabuan *(phising*) dimana terdapat informasi berupa *username*, *password* atau informasi pribadi lainnya yang dapat disalahgunakan dan menyebabkan kerugian bagi pihak lain. ARP merupakan protokol dalam TCP/IP *Protocol Suite* yang bekerja diantara *network layer* dan data *link layer* dan bertanggung jawab dalam melakukan resolusi pencatatan dan pencocokan alamat IP ke dalam alamat *Media Access Control* (MAC *Address*) lalu hasilnya letakkan di dalam ARP *cache* [3][4][5]. Saat membangun sistem keamanan jaringan, perlu lebih memperhatikan perlindungan sumber daya yang

tersimpan di jaringan agar meminimalisir adanya kebocoran data, terutama jaringan perusahaan atau pemerintah yang menyimpan banyak data penting [6][7][8]. Terdapat juga penelitian dengan *forensik* jaringan yang dapat merekam kejadian atau aktifitas lalu lintas data pada sebuah jaringan. Setelah diinvestigasi dan dilakukan analisa diduga dapat ditemukan bukti aliran paket yang mencurigakan, hal tersebut bertujuan untuk menemukan IP *address* penyusup [9][10]. Setelah ditemukannya serangan maka diperlukan pengambilan keputusan terhadap ancaman yang terjadi, diharapkan terdapat rekomendasi *tools* yang berfungsi untuk mendeteksi dan mengidentifikasi serangan serta menangani dan upaya pencegahan serangan ARP [11].

Berdasarkan latar belakang dan fenomena tersebut, maka analisis transfer data pada jaringan terdampak kejahatan siber yang perlu diwaspadai karena dapat berpengaruh buruk pada *website* (ARP *Spoofing*) menggunakan ARP *Poisoning* dan statistik deskriptif sangat diperlukan praktisi dan administrator agar dapat memberikan pencegahan ketika perangkat jaringan terkena ARP *Poisoning*.

2. Metode Penelitian

2.1 Teknik Pengumpulan Data Observasi

Penelitian ini menggunakan seperangkat peralatan jaringan yang ada dari Laboratorium Siopi Institut Teknologi Dirgantara Adisutjipto. Metode *ARP-Spoofing* digunakan untuk mengumpukan data mengenai objek penelitian.

2.2 Wawancara

Pada tahap ini melakukan wawancara kepada pihak pengelola lab ITDA dan administrator jaringan ITD Adisutjipto pada tanggal 17 dan 18 juli 2023 dengan durasi waktu masing-masing sekitar 45 menit untuk kebutuhan barang dan bahan apa saja yang diperlukan saat melakukan penelitian.

2.3 *Information Gathering / Reconnaissance*

Tahapan *information gathering* merupakan tahapan awal untuk melakukan penyerangan pada personal komputer untuk memperoleh informasi berupa IP, di mana dalam tahapan ini bertujuan untuk mengumpulkan informasi sebanyak-banyaknya untuk membantu dalam proses penyerangan dapat dilihat pada Tabel 1.

Tabel 1. Tahapan *Information Gathering / Reconnaissance*

No	Metodologi	Tahapan	*Tools*	Tujuan
1	***Reconnaissance***	*Internet Protocol*	Terminal	Mengidentifikasi alamat IP.
		Mac Address	Terminal	Mencari tahu alamat fisik dari *device* yang terdapat pada jaringan

2.4 *Attacking*

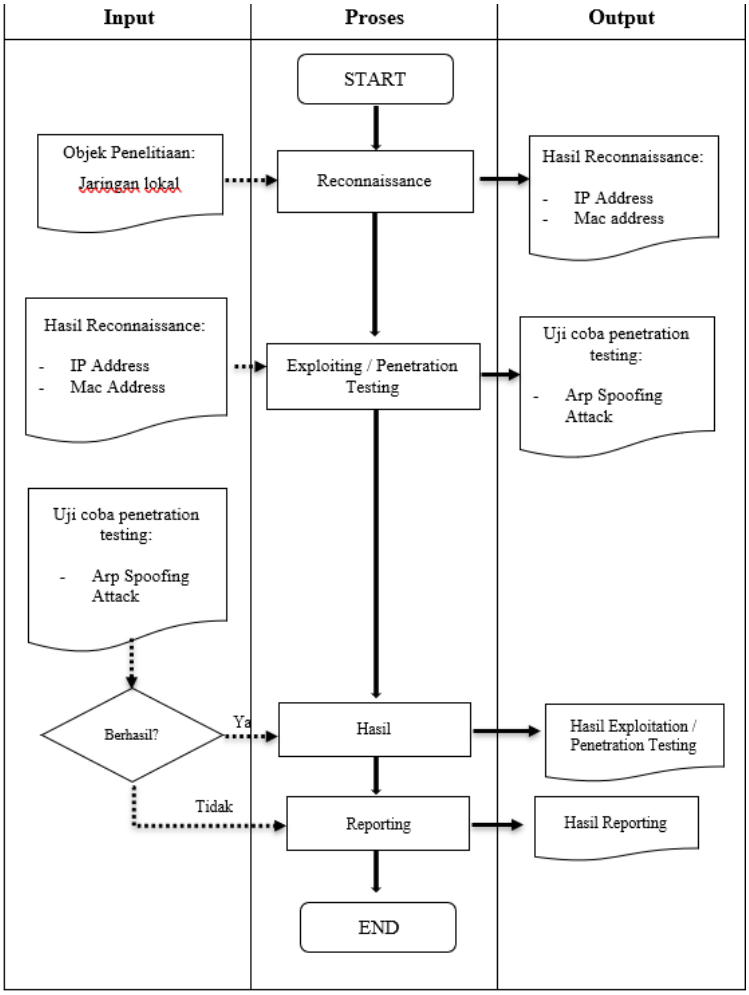
Tahapan selanjutnya setelah melakukan *information gathering* adalah dengan melakukan penyerangan menggunakan *tools* kali *linux* yaitu *ettercap* berdasarkan informasi yang telah didapatkan saat *information gathering*. Setelah melakukan penyerangan hasil penelitian akan dirangkum dari hasil penyerangannya.

2.5 Perancangan Jaringan

Topologi *star* (topologi bintang) adalah sebuah topologi yang model jaringannya menyerupai bintang dengan *server* yang berada di tengah sebagai pusatnya [12], sedangkan perangkat komputer terletak seperti cabang-cabang dari *server* tersebut. Pusat *server* yang terletak pada topologi jaringan *star* yakni berupa *hub* atau *switch*. Perangkat tersebut kemudian akan terhubung dengan masing-masing komputer yang ada. Dengan model jaringan seperti ini, proses pengiriman data akan melalui pusat *server* terlebih dulu, baru setelah itu data akan dikirimkan ke seluruh komputer *client* atau komputer tertentu sesuai tujuannya. Berdasarkan prinsip kerja tersebut, topologi ini seringkali

digunakan pada perusahaan yang memiliki alur data terpusat. Sehingga semua data yang dikirim dan diterima akan di-*filter* terlebih dulu oleh *server* pusat, kemudian akan diteruskan ke *node* tujuan.

2.6 Proses Penelitian



Gambar 1. Diagram alir penelitian

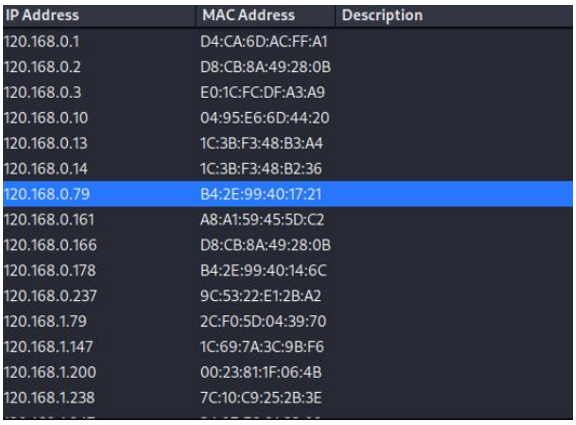
Pada tahap awal Gambar 1 mempersiapkan beberapa perangkat yang akan digunakan untuk pengambilan data. Proses pengiriman data akan melalui pusat *server* terlebih dulu, baru setelah itu data akan dikirimkan ke seluruh komputer *client* atau komputer tertentu sesuai tujuannya. Sehingga semua data yang dikirim dan diterima dan di *filter* terlebih dahulu oleh *server* pusat, kemudian akan diteruskan ke *node* tujuan. Langkah pertama yaitu mengetahui informasi IP *Address* yang digunakan pada jaringan tersebut, berdasarkan data yang telah diperoleh dari jaringan akan dilakukan percobaan *penetration testing* dengan menggunakan *tools Ettercap* dan *arpspoof*. *Penetration* digunakan untuk memanfaatkan celah keamanan, pada percobaan ini melakukan pencegahan terhadap ARP *spoofing* jika berhasil maka hasil *exploitation* atau *penetration test* akan dicatat dan jika tidak berhasil akan dilakukan laporan hasil *penetration*.

3. Hasil dan Pembahasan

Berdasarkan data yang telah diperoleh dari jaringan lokal akan dilakukan percobaan *penetration testing* dengan menggunakan *tools ettercap*, dan *arpspoof*, untuk melakukan memanfaatkan celah keamanan.

3.1 ARP *Spoofing Attack*

Serangan ARP *Spoofing* merupakan salah satu serangan yang mengancam keamanan jaringan. Serangan ini melibatkan manipulasi tabel ARP pada jaringan, di mana penyerang akan memalsukan atau mencurangi alamat IP dan MAC *Address* untuk mendapatkan akses tidak sah ke jaringan yang ada. Dalam konteks jaringan lokal, serangan ARP *Spoofing* dapat mengakibatkan gangguan serius, seperti peretasan data, pengintaian, dan bahkan pemalsuan identitas. Berikut proses ARP Spoofing: *Identify the Headings*. Gambar 2 merupakan proses ARP *Spoofing* menggunakan *Ettercap* dan *Tool Arp Spoof*, dengan target serangan IP 192.168.0.79. Dengan *tool* ini semua komunikasi data IP 192.168.0.79 akan dibalas atau diarahkan PC penyerang.



Gambar 2. *ARP Spoofing* jaringan lokal

3.2 Hasil Pengujian

Pada Tabel 2 terdapat 10 PC yang diuji dan ada 7 IP yang berhasil ter-*capture* dan 3 IP yang tidak, sedangkan pada Tabel 3 terdapat 20 PC yang diuji dan 16 IP yang berhasil dan 4 IP yang tidak berhasil ter-*capture*. Alasan terdapat IP yang berhasil di *capture* karena masih dalam satu lingkup jaringan, dan yang tidak adalah IP yang digunakan oleh *router* sehingga aksesnya terbatas pada *router* tersebut dan tidak termasuk ke dalam IP pada *server*. Sebenarnya bisa di lakukan penyerangan jika penyerang menggunakan jaringan yang terhubung oleh *router* tetapi karena keterbatasan, sehingga hanya dilakukan penyerangan menggunkan IP yang sudah tersedia oleh *switch* (*server*).

Tabel 2. Pengujian penyerangan 10 PC pada Lab SIOPI ITDA

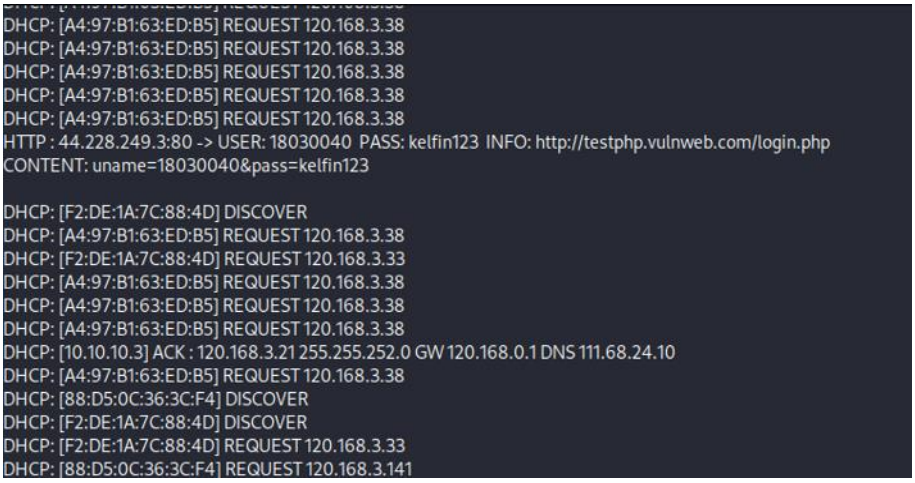
PC	IP	Subnetmask	Status
1	120.168.0.79	255.255.252.0	Berhasil
2	120.168.0.178	255.255.252.0	Berhasil
3	120.168.0.77	255.255.252.0	Berhasil
4	120.168.3.14	255.255.252.0	Berhasil
5	120.168.0.106	255.255.252.0	Berhasil
6	120.168.2.208	255.255.252.0	Berhasil
7	120.168.2.216	255.255.252.0	Berhasil
8	120.168.1.79	255.255.252.0	Gagal
9	120.168.1.147	255.255.252.0	Gagal
10	120.168.1.200	255.255.252.0	Gagal

Tabel 3. Pengujian penyerangan 20 PC pada Lab SIOPI ITDA

PC	IP	Subnetmask	Status
1	120.168.0.79	255.255.252.0	Berhasil
2	120.168.0.178	255.255.252.0	Berhasil
3	120.168.0.77	255.255.252.0	Berhasil
4	120.168.3.14	255.255.252.0	Berhasil
5	120.168.0.106	255.255.252.0	Berhasil

6	120.168.2.208	255.255.252.0	Berhasil
7	120.168.2.216	255.255.252.0	Berhasil
8	120.168.2.224	255.255.252.0	Berhasil
9	120.168.3.3	255.255.252.0	Berhasil
10	120.168.0.176	255.255.252.0	Berhasil
11	120.168.2.201	255.255.252.0	Berhasil
12	120.168.3.179	255.255.252.0	Berhasil
13	120.168.2.207	255.255.252.0	Berhasil
14	120.168.0.224	255.255.252.0	Berhasil
15	120.168.0.155	255.255.252.0	Berhasil
16	120.168.2.57	255.255.252.0	Berhasil
17	120.168.1.79	255.255.252.0	Gagal
18	120.168.1.147	255.255.252.0	Gagal
19	120.168.1.200	255.255.252.0	Gagal
20	120.168.1.238	255.255.252.0	Gagal

Berdasarkan dari data pada Tabel 2 dapat disimpulkan bahwa IP yang terscan melalui *tools Ettercap* ada yang berhasil dan ada yang tidak. Dijelaskan bahwa IP yang dapat ter-*capture* adalah IP yang masih dalam lingkup satu jaringan atau masih berada pada satu *server*, sedangkan yang tidak adalah IP yang digunakan oleh *router* sehingga aksesnya terbatas pada *router* tersebut dan tidak termasuk ke dalam IP pada *server*. Sebenarnya bisa dilakukan penyerangan jika penyerang menggunakan jaringan yang terhubung oleh *router* tetapi karena keterbatasan, sehingga hanya dilakukan penyerangan menggunakan IP yang sudah tersedia oleh *switch (server).*

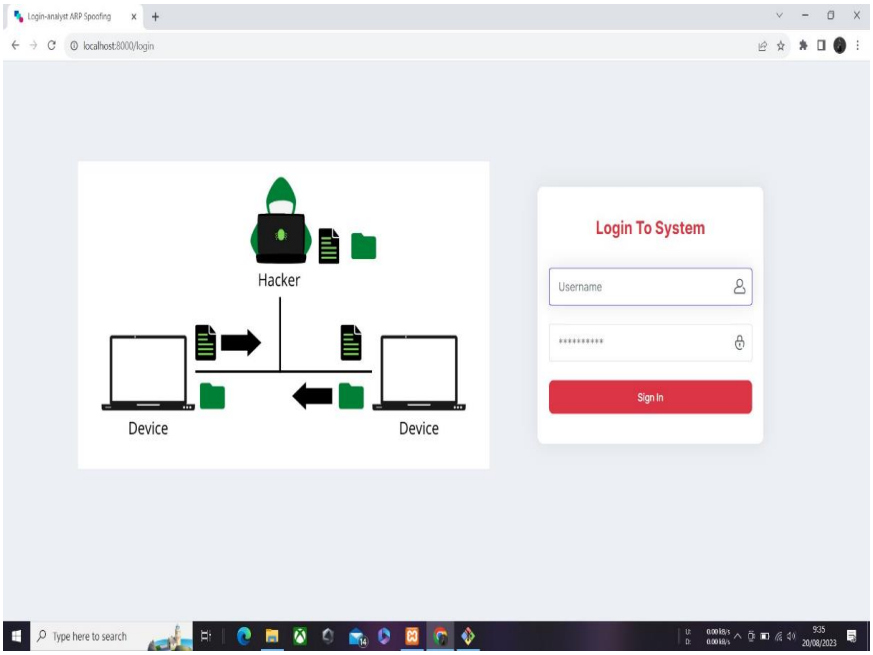


Gambar 3. Hasil *scanning* dengan *tool Ettercap*

Gambar 3 merupakan hasil *scanning* komunikasi data antara kedua ip tersebut menggunakan *tool ettercap*, dari *scanning* didapatkan hasil diantaranya berupa *request* http dan *post* http sebuah halaman *login*.

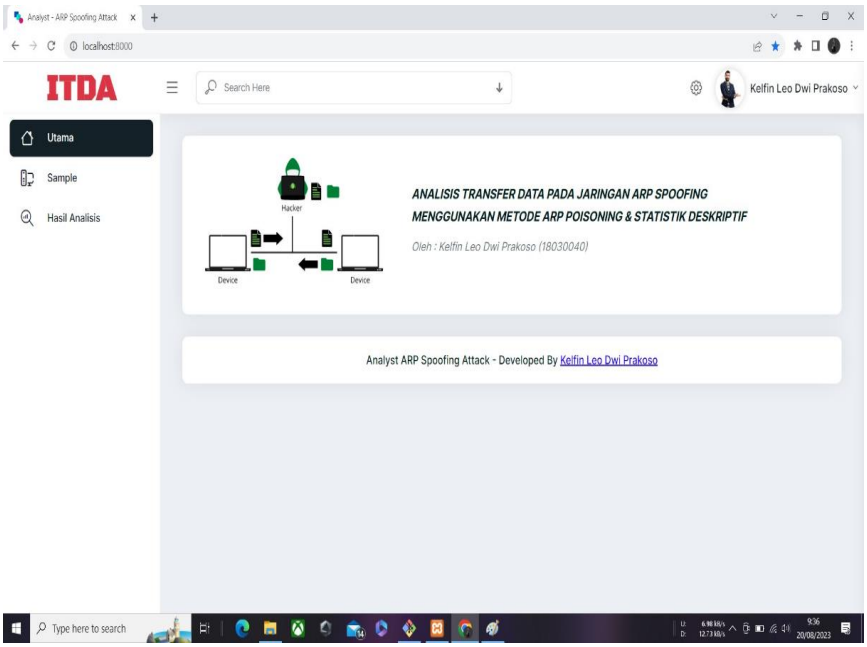
3.3 Representasi Hasil Pengujian

Hasil penelitian direpresentasikan melalui aplikasi *web* agar lebih mudah dipahami. Berikut adalah tampilan aplikasi *web* yang telah dibuat.



Gambar 4. Halaman *login*

Pada Gambar 5 terdapat halaman *dashboard* ditampilkan sub menu berupa sampel dan hasil analisis yang dihitung pada aplikasi *web*. Pada halaman ini dapat dipillih menu sampel untuk menambah sampel data agar dapat dihitung di aplikasi, dan pada menu hasil analisis terdapat *output* yang telah di *input* pada halaman sampel.

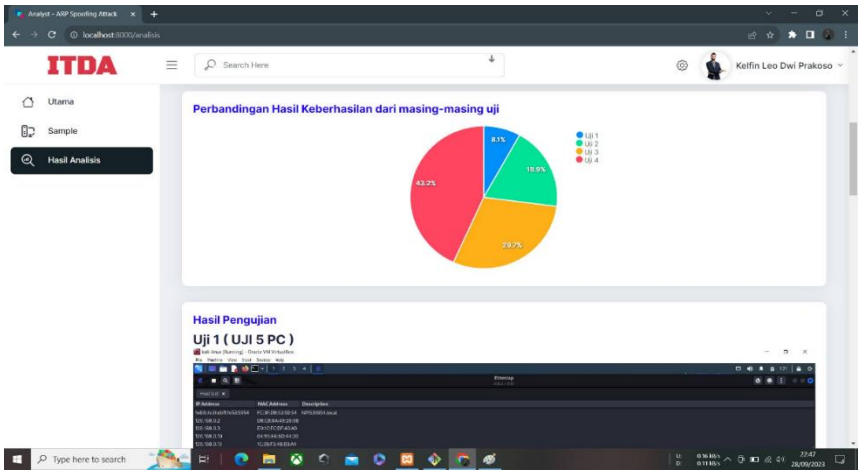


Gambar 5. Halaman *dashboard*

Setelah melakukan penyerangan seperti pada Tabel 3 dijabarkan perbandingan hasil uji analisis seperti yang terlihat pada grafik Gambar 6 yang merupakan hasil perhitungan persentase dari aplikasi yang dibuat. Pada Gambar 6 diperlihatkan uji pertama warna menggunakan 5 unit PC dengan total keberhasilan 3. Uji kedua warna hijau mendapat total keberhasilan 7 unit PC. Uji ketiga warna kuning menggunakan 15 unit PC dengan total keberhasilan 11. Sedangkan uji keempat warna merah dengan 20 unit PC dan total keberhasilan sebanyak 16.

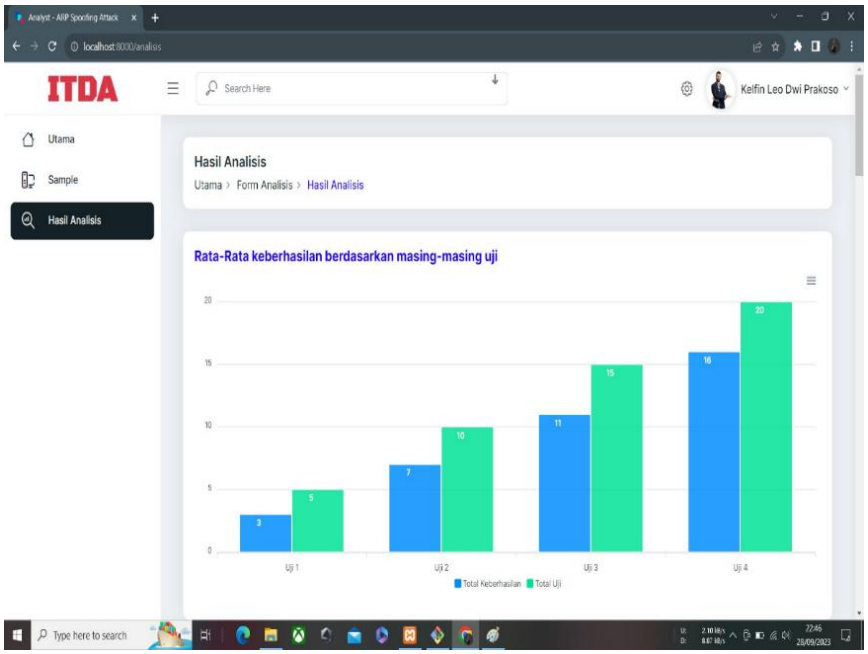
Kesimpulannya dari data tersebut total berhasilnya adalah 37, jadi persentase hasil uji 1 adalah

$\frac{3}{37}$ x 100 = 8.1% . Hasil uji 2 adalah $\frac{7}{37}$ x 100 = 18.9%. Hasil uji 3 adalah $\frac{11}{37}$ x 100 = 29.7% sedangkan hasil uji 4 adalah $\frac{16}{37}$ x 100 = 43,2%.



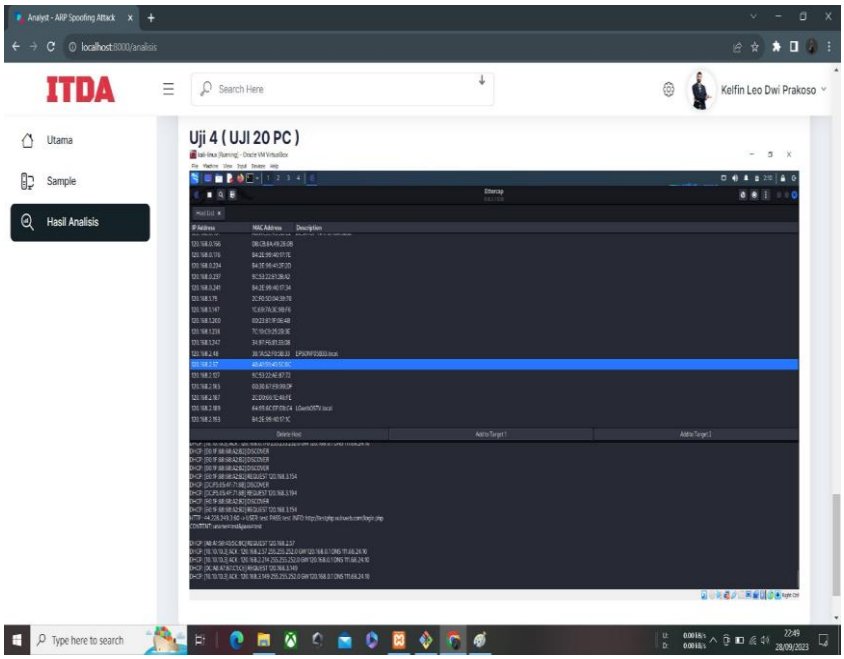
Gambar 6. Perbandingan hasil keberhasilan uji

Gambar 7 menampilkan grafik rata-rata keberhasilan berdasarkan masing-masing uji:



Gambar 7. Rata-rata keberhasilan uji

Pada Gambar 7 terdapat tampilan menu yang menampilkan perbandingan hasil keberhasilan dari masing-masing uji yang telah diinput pada aplikasi *web*. Hasil *output* berupa gambar yang telah diinput pada halaman sampel dan terdapat persentase perbandingan dari beberapa uji coba. Sedangkan Gambar 8 yaitu tampilan setelah melakukan *scanning* dan tahap penyerangan dengan menggunakan *ARP Poisoning* sehingga *username* dan *password* pada PC dengan IP yang dipilih dapat ter-*capture*. Tetapi pada tahap ini dilakukan *scanning* dengan keadaan 20 PC yang sudah menyala.



Gambar 8. Hasil analisis

4. Kesimpulan

Penyerang menggunakan metode ARP *Spoofing* yang menyebabkan lalu lintas target akan di *redirect* ke *device* penyerang sehingga penyerang dapat memantau dan mengetahui isi lalu lintas data pada jaringan lokal, penggantian *Mac Address* penyerang sangat diperlukan karena jika *mac* tidak diganti maka lalu lintas jaringan tidak akan ter-*redirect* ke *device* penyerang.

References

[1] YUDIANTO, M. Jafar Noor; NOOR, Jafar. Jaringan komputer dan Pengertiannya. Ilmukomputer. com, 2014, 1: 1-10.

[2] ENGEBRETSON, Patrick. The basics of hacking and penetration testing: ethical hacking and penetration testing made easy. Elsevier, 2013.

[3] Fachri, F., Fadlil, A., & Riadi, I. (2021). Analisis Keamanan Webserver Menggunakan Penetration Test. Jurnal Informatika. Yogyakarta: Universitas Ahmad Dahlan.

[4] Fauzan, F. Y., & Syukhri. (2021). Analisis Metode Web SecurityPTES (Penetration Testing Execution And Standart) Pada Aplikasi E-LearningUniversitas Negeri Padang. Jurnal Vocational Teknik Elektronika dan Informatika: Universitas Negeri Padang.

[5] Fauzan, R. H. (2019). Pengujian Keamanan Sistem Informasi Akademik Menggunakan Metode Penetration Testing. Studi Kasus: Institut Pertanian Stiper Yogyakarta.

[6] Fauzan, R. H. (2019). Pengujian Keamanan Sistem Informasi Akademik Menggunakan Metode Penetration Testing. Studi Kasus: Institut Pertanian Stiper Yogyakarta.

[7] Hidayatulloh, S., & Saptadiaji, D. (2021). Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP). Jurnal Algoritma. Garut: Sekolah Tinggi Teknologi Garut.

[8] Ghanem, M. C., & Chen, T. M. (2020). Reinforcement learning for efficient network penetration testing. Information (Switzerland), 11(1), 1–23. https://doi.org/10.3390/info11010006

[9] Ismail, R. W., & Pramudita, R. (2020). Metode Penetration Testing pada Keamanan Jaringan Wireless Wardriving PT. Puma Makmur Aneka Engineering Bekasi. Jurnal Mahasiswa Bina Insani, 5(1), 53–62.

[10] [10] Ismail, R. W., & Pramudita, R. (2020). Metode Penetration Testing pada Keamanan Jaringan Wireless Wardriving PT. Puma Makmur Aneka Engineering Bekasi. Jurnal Mahasiswa Bina Insani, 5(1), 53–62.

[11] Kelrey, A. R., & Muzaki, A. (2019). Pengaruh Ethical Hacking Bagi Keamanan Data Perusahaan. CyberSeccurity Dan Forensik Digital, 2(2), 77–81.

[12] Anendya, aorinka. (2023). Mengenal Topologi Star yang Praktis dan Mudah Digunakan dari https://www.dewaweb.com/blog/mengenal-topologi-star/

[13] A, Bayu. (2022). Networking : Penjelasan Jaringan komputer Artikel ini di Kutip dari Website https://www.menggunakan.id/jaringan-komputer/

[14] Bin Ibrahim, A., & Kant, S. (2018). Penetration Testing Using SQL Injection to Recognize the Vulnerable Point on Web Pages. International Journal of Applied Engineering Research, 13(8), 5935–5942. http://www.ripublication.com

[15] Elanda, A., & Buana, R. L. (2020). Analisis Keamanan Sistem Informasi Berbasis Website dengan Metode Open Web Application Security Project (OWASP) Versi 4: Systematic Review. Journal of Computer Engineering System and Science. Karawang: Sekolah Tinggi Manajemen Ilmu Komputer Rosma.