SEMINAR NASIONAL TEKNOLOGI DAN MULTIDISIPLIN ILMU (SEMNASTEKMU)
Vol. 4 No. 1 Desember 2024
e-ISSN: 2809-1574; p-ISSN: 2809-1566, Hal 12-25

Strategi Mitigasi Serangan Phishing Dengan Menggunakan Teknik DHCP Snooping Dan Port Security

R. Rizky Khaerul M.R.
Universitas STEKOM

Alamat: Jln. Majapahit No. 605 Semarang - Jawa Tengah
Korespondensi : rizky.rakasiwi@gmail.com

Abstract. *Security of computer network systems has recently become a major focus of attention. Recently, numerous cybercrimes have occurred due to vulnerabilities in network systems. These vulnerabilities are exploited by attackers to take advantage of the resources within the system. As a result, several companies have suffered data breaches or system attacks. One of the causes of such vulnerabilities is internal company actions, such as employees unknowingly accessing unauthorized websites and falling victim to online fraud or phishing. In this study, the author attempts to mitigate phishing incidents. The author employs DHCP Snooping and Port Security methods to restrict access from unauthorized devices from providing DHCP services to clients, thereby preventing manipulation of the DHCP server and avoiding DNS spoofing. The results show that before implementing DHCP Snooping, in 10 test attempts where clients requested an IP from the DHCP server, the percentage of clients receiving an IP address from the authorized DHCP server was 50%, while the remaining IPs came from a rogue DHCP server (attacker). After implementing DHCP Snooping, 100% of the clients successfully received IP addresses from the authorized DHCP server. To further enhance network security, the author applied Port Security on switches connected to the server, ensuring that only authorized servers can connect to the network.*

Keywords: *Phishing, DHCP Snooping, DNS Spoofing, Port Security.*

Abstrak. Keamanan sistem jaringan komputer akhir-akhir ini banyak menjadi pusat perhatian. Belum lama ini banyak terjadi tindak kejahatan siber yang disebabkan adanya celah kerentanan dalam sistem jaringan. Celah tersebut dimanfaatkan oleh attacker dalam mengeksploitasi sumber daya yang ada dalam sistem. Akibatnya beberapa perusahaan harus mengalami kebocoran data atau serangan sistem. Salah satu penyebab celah kerentanan sistem dapat terjadi karena tindakan pihak internal perusahaan, misalnya karyawan tidak menyadari telah mengakses web yang tidak sah dan kemudian terjebak dalam penipuan online atau phishing. Dalam penelitian ini, penulis mencoba untuk memitigasi terjadinya phishing tersebut. Penulis menggunakan metode DHCP Snooping dan port security dengan tujuan membatasi akses dari perangkat yang tidak sah untuk memberikan layanan DHCP kepada klien, sehingga dapat menghindari terjadinya manipulasi pada server DHCP dan mencegah terjadinya DNS Spoofing. Hasinya, sebelum dilakukan teknik DHCP Snooping, dari 10 kali percobaan klien request IP ke server DHCP, prosentase klien mendapatkan IP DHCP dari server DHCP Authorized adalah 50% sisanya dari server DHCP Rogue (attacker). Kemudian setelah dilakukan DHCP Snooping, prosentase klien mendapatkan IP DHCP dari server DHCP Authorized adalah 100%. Untuk menambah keamanan sistem jaringan, penulis menambahkan

Received November 30, 2024; Revised Desember 12, 2024; Accepted Desember 20, 2024
* Dayanni Vera Versanika, dayanniveraversanika@gmail.com

metode port security pada switch yang terhubung ke server, sehingga hanya authorized server yang dapat terhubung ke jaringan.

Kata kunci: Phishing, DHCP Snooping, DNS Spoofing, Port Security.

LATAR BELAKANG

Perkembangan teknologi informasi dan digital berkembang sangat cepat. Hal itu selaras dengan kemudahan yang didapatkan oleh masyarakat saat ini akibat dari kemajuan teknologi. Seperti misalnya saat ini orang tidak perlu pergi ke bank untuk melakukan transfer uang, cukup menggunaan layanan m-banking atau i-banking. Kemudian jika seseorang ingin berbelanja kebutuhan pokok atau makanan, cukup melalui aplikasi layanan pemesanan barang atau E-commerce. Dibalik kemudahan yang didapatkan, ada bahaya yang mengancam jika tidak berhati-hati dalam memanfaatkan teknologi dan menjaga keamanan sistem informasi. Semakin maju sebuah teknologi, maka dibutuhkan sistem keamanan yang semakin kuat. Berbicara tentang keamanan sistem informasi, keamanan jaringan komputer adalah hal yang sangat penting dan harus diperhatikan saat ini. Banyak terjadi kejahatan-kejahatan siber yang berakibat sangat merugikan sebuah perusahaan atau instansi. Kerugian tersebut tidak hanya kerugian berupa finansial tetapi juga kerugian tentang turunnya reputasi atau tingkat keepercayaan masyarakat kepada sebuah perusahaan atau instansi, apalagi jika perusahaan tersebut adalah perusahaan yang menyediakan layanan atau jasa kepada pelanggan, maka reputasi perusahaan akan dianggap sangat penting demi menjaga kepercayaan pelanggan.

Salah satu bentuk kejahatan dunia siber yang akhir-akhir ini marak terjadi adalah phishing. Phishing merupakan jenis serangan siber yang dilakukan oleh peretas yang menyamar sebagai suatu organisasi atau seseorang yang dapat dipercaya untuk memperoleh informasi rahasia dari target, misalnya nomor kartu kredit, alamat email pribadi, dan informasi pribadi lainnya. Hal ini biasanya biasanya dilakukan melalui email, SMS , atau situs web palsu yang dimanipulasi agar terlihat sah. Serangan phishing dapat menyebabkan kerugian finansial, pencurian identitas, dan pelanggaran data (Dewanto dkk, 2024).

Dalam mengantisipasi terjadinya phishing, dapat dimitigasi dengan berbagai cara. Mencegah serangan dari luar, atau memperkuat sistem internal, baik secara sistem

jaringan internal maupun sumber daya manusianya. Pencegahan serangan dari luar tidak dapat dilakukan secara maksimal karena penyerang akan melakukan berbagai macam cara untuk dapat masuk ke dalam sistem jaringan suatu perusahaan. Sehingga hal yang harus dilakukan adalah memperkuat sistem internal dengan beberapa metode atau teknik seperti pemasangan firewall, Intrusion Detection System (IDS), Access Control List (ACL), DHCP Snooping, dan port security. Pemberian pelatihan tentang security awareness kepada seluruh sumber daya manusia di suatu perusahaan juga sangat penting untuk mengantisipasi serangan yang berupa Social engineering.

Dalam penelitian ini, penulis memanfaatkan teknik DHCP Snooping dan port security untuk meningkatkan keamanan sistem jaringan internal dalam skala perusahaan kecil hingga menengah dengan tujuan untuk memitigasi adanya serangan phishing. DHCP (Dynamic Host Configuration Protocol) adalah salah satu protocol penting dalam jaringan komputer yang bertugas mendistribusikan alamat IP secara otomatis sesuai dengan permintaan klien. Secara sederhana mekanisme ini melibatkan komunikasi yang intens antara klien dan server DHCP yang tersedia di sistem jaringan. Klien tidak mengetahui perangkat mana yang bertindak sebagai server DHCP dalam suatu jaringan. Proses awal klien mencari dan membuka komunikasi dengan server DHCP, kemudian klien akan menerima setiap pesan dalam bentuk penawaran konfigurasi IP (Penawaran DHCP) dari server sebagai respon terhadap DHCP Discover yang dikirim oleh klien (Pradana dan Budiman, 2021). DHCP Snooping merupakan fitur keamanan layer 2 pada jaringan komputer yang diharapkan dapat membantu melindungi keamanan sistem jaringan dari operasi server DHCP palsu atau yang biasa disebut dengan Rogue DHCP server. Dimana Rogue DHCP server ini dapat berpotensi mendistribusikan konfigurasi alamat IP kepada klien dengan tidak sah sehingga dapat membahayakan keamanan jaringan. Dengan adanya DHCP Snooping, distribusi alamat IP kepada klien dapat dipastikan bersumber dari server DHCP yang sah.

Fitur keamanan pada layer 2 lainnya yang dapat digunakan dalam meningkatkan keamanan jaringan adalah port security. Dengan adanya fitur port security, switch dapat membatasi akses sebuah port. Jika ada port pada switch yang terhubung ke suatu perangkat yang memiliki peran penting, maka fitur ini dapat disetting pada port tersebut, sehingga hanya perangkat tertentu yang dapat terhubung pada port tersebut dengan cara

mendaftarkan MAC address perangkat tersebut. Sehingga apabila ada perangkat lain yang belum terdaftar pada port tersebut, maka perangkat tersebut tidak akan bisa terkoneksi ke jaringan melalui port pada switch tersebut. Hal ini dapat mencegah akses yang tidak sah dari perangkat yang tidak sah, misalnya perangkat attacker yang mencoba terkoneksi dengan jaringan melalui switch. Switch port security juga bisa dikatakan sebagai metode yang akan memperbolehkan user tertentu yang bisa mengakses jaringan melewati port yang disediakan di switch untuk mengamankan jaringan LAN (Local Area Network) (Dara dkk, 2022).

Pada tahun 2017, Ariyadi menganalisa serangan DHCP Starvation yaitu penyerang membanjiri server dengan permintaan IP palsu hingga pool habis, kemudian mendistribusikan IP dari server palsu untuk mencuri data pengguna. Kemudian memitigasi dengan Filter DHCP dengan cara menggunakan hostname yang terdaftar di server Mikrotik, permintaan DHCP Discover yang tidak dikenali dapat diblokir. Metode ini efektif mencegah serangan (Tamsir, 2022).

Pada tahun 2018, Zaeni Miftah mengimplementasikan DHCP Snooping dan berhasil memvalidasi dan memfilter DHCP Server yang terpercaya dan mencegah DHCP Rogue memberikan alamat IP palsu. Tanpa DHCP Snooping, beberapa perangkat mendapatkan alamat IP dari server untrusted. Dengan DHCP Snooping, semua perangkat hanya mendapatkan IP dari server DHCP trusted (Miftah, 2018).

Pada tahun 2019, Akashi dan Tong melakukan penelitian dengan menganalisa DHCP Snooping yang efekttif melindungi dari serangan dalam jaringan. DHCP Snooping gagal mencegah serangan luar karena paket DHCP dapat dengan mudah bocor dari segmen jaringan. Pemanfaatan Aturan Longest Matching Prefix yaitu penyerang dapat mengarahkan lalu lintas klien ke server palsu dengan memanfaatkan kelemahan dalam implementasi aturan longest matching prefix (Akashi dan Tong, 2019).

Pada tahun 2023, Putra dan Azis meneliti tentang DHCP Snooping dan berhasil mencegah DHCP Rogue memberikan alamat IP kepada perangkat klien. IP yang diterima oleh klien selalu berasal dari DHCP Server yang telah dikonfigurasi. VLAN memastikan perangkat dari laboratorium yang berbeda tidak dapat berkomunikasi langsung tanpa pengaturan tambahan. Monitoring menggunakan Wireshark berhasil mendeteksi dan

memvalidasi protokol DHCP, termasuk aktivitas DHCP Rogue yang terdeteksi namun tidak berdampak (Putra dan Azis, 2023).

Pada tahun 2024, Nurfaishal dan Akbar membandingkan efektivitas berbagai algoritma keamanan yang diterapkan pada layer 2 switch, yaitu MAC Address Filter, Port Security, VLAN Hopping Mitigation, dan DHCP Snooping. Hasilnya port security dapat membatasi perangkat yang dapat terhubung ke jaringan berdasarkan MAC address yang efektif mencegah spoofing dan akses tidak sah, seperti saat kabel jaringan diganti dengan perangkat asing. DHCP Snooping dapat mengontrol distribusi alamat IP hanya melalui DHCP server tepercaya dan berhasil mencegah serangan DHCP Rogue yang mencoba mengganggu alokasi IP. VLAN Hopping Mitigation efektif mengisolasi lalu lintas jaringan antar VLAN untuk mencegah akses tidak sah dan menjaga segmentasi serta mencegah manipulasi segmen jaringan (Nurfaishal dan Akbar, 2024).

Dalam penelitian ini, penulis bertujuan menggabungkan dua metode tersebut yaitu DHCP Snooping dan port security sebagai langkah dalam memitigasi serangan phishing pada sebuah lingkungan perusahaan skala kecil sampai dengan menengah. Walaupun dalam penelitian ini penulis menggunakan simulator jaringan yaitu Packet Tracer, penulis berharap dapat mengidentifikasi dan menganalisa keefektifan dari kombinasi dua metode tersebut. Sehingga serangan phishing dalam sistem jaringan dapat diminimalisir.

KAJIAN TEORITIS

2.1 Phishing

Phishing adalah upaya memperoleh informasi pribadi seseorang dengan menggunakan teknik penipuan. Data yang biasanya dicuri dengan teknik phishing pada umumnya mencakup informasi pribadi (nama, umur, alamat), informasi akun (nama pengguna dan kata sandi), dan informasi keuangan (informasi kartu kredit, akun). Istilah resmi untuk phishing adalah phishing, dan asal usulnya adalah ``fishing" yang berarti ``memancing." Phishing bertujuan untuk mengelabui orang agar mengungkapkan informasi pribadi tanpa sepengetahuan mereka. Informasi yang diberikan akan digunakan untuk tujuan kriminal (Hidayat dkk, 2023). Jumlah situs phishing dan penipuan semakin meningkat dari tahun ke tahun seiring dengan meningkatnya pemanfaatan teknologi digital di lingkungan masyarakat. Salah satu contohnya pada tahun 2022, terjadi

pembobolan di BRI di Sumatera Barat. Kejadian ini terungkap setelah korban menerima informasi melalui WhatsApp mengenai perubahan biaya transfer dan mengklik tautan yang diberikan oleh pelaku. Korban kemudian mengisi formulir yang disediakan oleh pelaku, memberikan username dan password-nya. Akibatnya, korban mengalami kerugian sebesar 1,1 miliar rupiah. Laporan kejadian ini dibuat pada 31 Mei 2022 dan saat ini kasusnya sedang ditangani Reserse Kriminal Khusus Polda Sumbar (Sinaga dkk, 2023). Dengan semakin banyaknya kasus phishing yang menimbulkan dampak kerugian besar, maka semua pengguna teknologi digital harus semakin waspada dalam mengelola akun digital dan berhati-hati terhadap halaman web atau link yang belum jelas asal usulnya untuk mencegah kejahatan phishing itu terjadi.

2.2 DHCP Snooping

DHCP Snooping adalah fitur keamanan jaringan pada layer 2 yang memiliki kemampuan untuk mencegah Rogue DHCP Server atau server DHCP yang tidak sah untuk melayani permintaan alamat IP DHCP dari klien. DHCP Snooping sangat bermanfaat untuk melindungi arsitektur jaringan dari serangan. Secara lebih luas, DHCP Snooping dapat digunakan untuk mencegah berbagai jenis serangan pada jaringan, seperti serangan dari Server DHCP tidak resmi,Man In The Middle (MITM), Attack dan serangan Spoofing IP yang membanjiri permintaan IP DHCP ke server DHCP resmi. Cara kerja DHCP Snooping yaitu ketika server DHCP mengalokasikan alamat IP untuk klien di LAN, DHCP snooping dapat dikonfigurasi pada switch LAN untuk mengizinkan hanya klien dengan IP tertentu dan alamat MAC untuk memiliki akses ke jaringan. DHCP snooping dapat memastikan integritas IP pada Layer 2 switched domain. Dengan DHCP snooping , informasi tentang alamat IP dan sesuai alamat MAC disimpan dalam database pada switch (Tamsir, 2022).

2.3 Switch Port Security

Switch Port Security merupakan metode yang bisa dilakukan pada switch agar dapat memberikan akses hanya kepada klien yang Mac addressnya sudah tercatat dalam Mac address table sebuah switch, sehingga host lain yang tidak bertanggung jawab tidak akan mudah terhubung ke dalam jaringan menggunakan setiap port yang berada di switch (Tamsir, 2022). Switch Port Security juga bisa dikatakan sebagai metode yang akan memperbolehkan user tertentu yang bisa mengakses jaringan melewati port yang

disediakan di switch untuk mengamankan jaringan LAN (Local Area Network) (Zara dkk, 2020).

2.4 DNS Spoofing

DNS Spoofing adalah serangan yang memungkinkan penyerang untuk memanipulasi atau mengalihkan lalu lintas yang ditujukan untuk satu domain situs web asli atau sah ke situs web lain milik penyerang, dengan tujuan penyerang dapat mengambil alih kendali lalu lintas korban. DNS spoofing dapat dimanfaatkan penyerang untuk tindak kejahatan phishing.

2.5 Cisco Packet Tracer

Cisco Packet Tracer adalah simulator jaringan komputer dari Cisco yang dapat digunakan untuk membuat desain dan konfigurasi jaringan secara virtual. Selain itu dengan Cisco Packet Tracer, pengguna juga dapat melakukan eksperimen dan menguji berbagai skenario jaringan yang diinginkan. Dalam Packet Tracer, terdapat banyak perangkat jaringan virtual yang bentuk dan fungsinya sama dengan perangkat nyata. Cisco Packet Tracer dapat digunakan secara gratis. Pemanfaatan packet tracer sangat berguna bagi peneliti maupun praktisi dalam mendesain jaringan virtual sebelum melakukan konfigurasi pada jaringan nyata.

METODE PENELITIAN

Dalam penelitian ini, penulis menggunakan simulator Cisco Packet Tracer versi 8.2.2 dalam mendesain, mengkonfigurasi, dan menguji sistem jaringan yang dibangun. Metode yang dipakai adalah DHCP Snooping dan switch port security. Penulis membuat desain dan konfigurasi topologi suatu jaringan dalam sebuah perusahaan dengan menggunakan server DHCP, DNS, dan HTTP asli dengan switch server untuk konfigurasi DHCP Snooping, kemudian menggunakan router untuk merutrekan jaringan, dan ada 4 grup VLAN untuk masing-masing divisi. Penulis juga menambahkan server DHCP, DNS, dan HTTP palsu yang digunakan oleh penyerang dalam melakukan kejahatan phishing. Adapun langkah-langkah skenario pengujian jaringan sebagai berikut :

1. Mendesain topologi jaringan menggunakan Cisco Packet Tracer.

2. Konfigurasi pada setiap device seperti pada Router, Switch, dan Server, dan PC / klien.

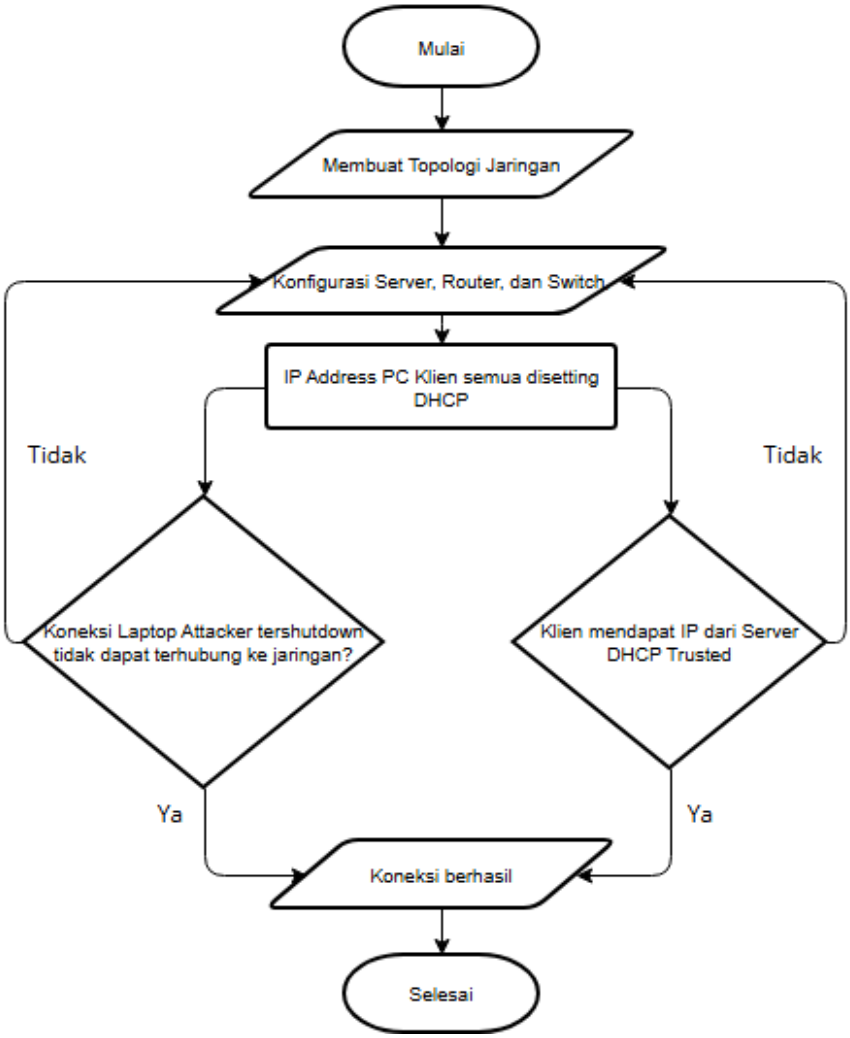
3. Skenario 1 : Pengujian DHCP Discovery atau permintaan IP DHCP dari klien (korban) sebelum dilakukan setting DHCP Snooping

4. Skenario 2 : Korban melakukan akses ke web palsu pada saat mendapatkan IP DHCP dari Rogue DHCP Server, dan menjadi korban phishing.

5. Skenario 3 : Pengujian DHCP Discovery dari klien (korban) setelah dilakukan setting DHCP Snooping, kemudian PC KORBAN melakukan akses ke web dan selalu diarahkan ke web yang sah.

6. Skenario 4 : Melakukan setting port security untuk memastikan hanya perangkat yang sah yang dapat terhubung ke Switch Server dan perangkat Attacker tidak dapat terhubung ke Switch Server.

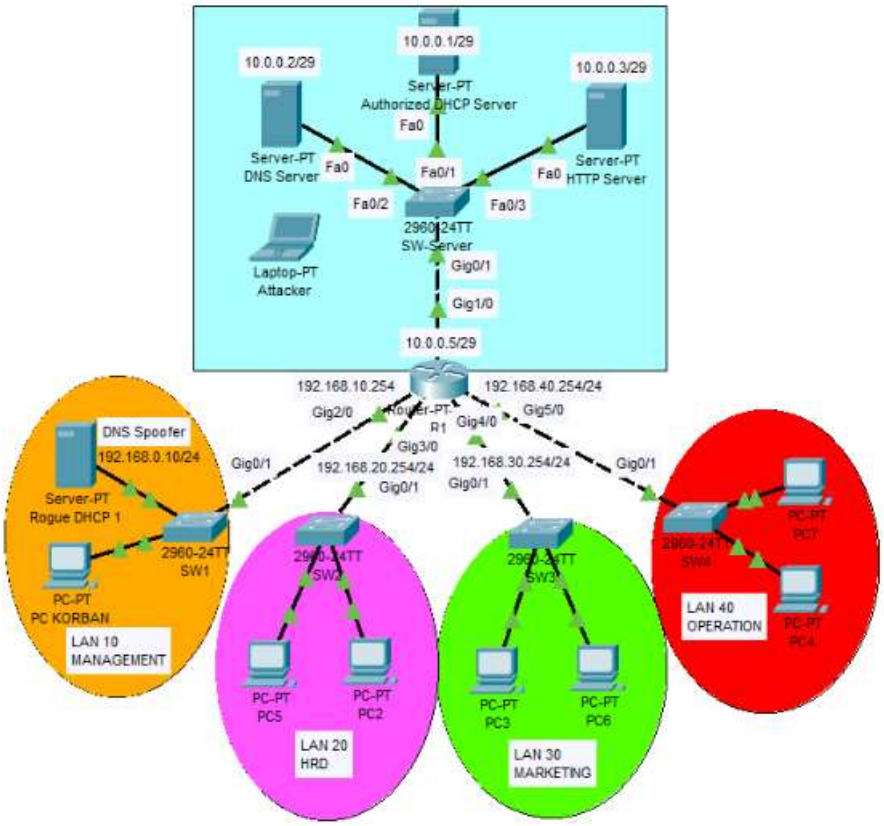
Diagram alur atau flowchart metode penelitian ditunjukkan pada Gambar 1.



Gambar 1. Flowchart Penelitian

HASIL DAN PEMBAHASAN

Hasil dari desain dan topologi jaringan pada penelitian ini ditunjukkan Gambar 2.



Gambar 2. Topologi Jaringan

4.1 Skenario 1

Pengujian DHCP Discovery atau permintaan IP DHCP dari klien (PC KORBAN) sebelum dilakukan setting DHCP Snooping dilakukan sebanyak 10 kali percobaan. Hasilnya ditunjukkan pada table 1.

Tabel 1. Hasil IP Address DHCP yang didapat PC KORBAN sebelum dilakukan setting DHCP Snooping

Percobaan ke-	IP Address DHCP	Subnet Mask	Gateway	DNS	DHCP Server
1	192.168.0.101	255.255.255.0	192.168.0.10	192.168.0.10	Rogue DHCP
2	192.168.10.4	255.255.255.0	192.168.10.254	10.0.0.2	Authorized
3	192.168.0.100	255.255.255.0	192.168.0.10	192.168.0.10	Rogue DHCP
4	192.168.10.3	255.255.255.0	192.168.10.254	10.0.0.2	Authorized
5	192.168.0.103	255.255.255.0	192.168.0.10	192.168.0.10	Rogue DHCP
6	192.168.10.4	255.255.255.0	192.168.10.254	10.0.0.2	Authorized
7	192.168.0.101	255.255.255.0	192.168.0.10	192.168.0.10	Rogue DHCP

8	192.168.10.2	255.255.255.0	192.168.10.254	10.0.0.2	Authorized
9	192.168.10.1	255.255.255.0	192.168.10.254	10.0.0.2	Authorized
10	192.168.0.103	255.255.255.0	192.168.0.10	192.168.0.10	Rogue DHCP

Dari hasil percobaan skenario 1 dapat dilihat bahwa dalam 10 kali percobaan PC KORBAN melakukan permintaan IP Address DHCP, diperoleh data 5 kali PC KORBAN mendapatkan IP Address dari Rogue DHCP server atau Server DHCP penipu. Artinya prosentase PC KORBAN untuk mendapatkan IP Address DHCP yang sah hanya 50%, sedangkan 50% nya dalam ancaman dari serangan Rogue DHCP Server. Hal ini menunjukkan adanya celah kerentanan yang besar dalam suatu keamanan jaringan, karena dikhawatirkan PC KORBAN akan diarahkan ke alamat web palsu, dan rawan terjebak phishing.

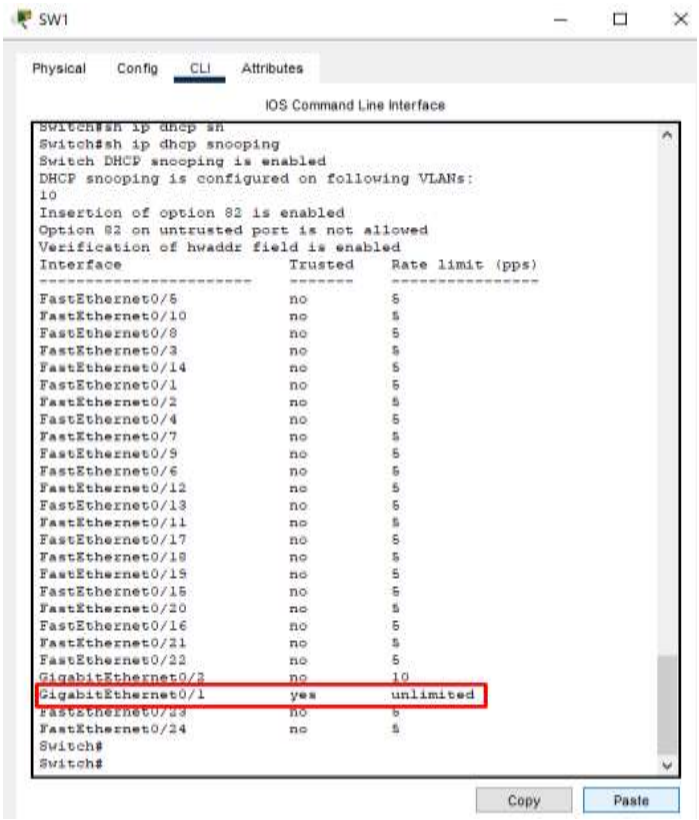
4.2 Skenario 2

Gambar 3 menunjukkan PC KORBAN diarahkan ke alamat web palsu ketika mendapatkan IP address dari Rogue DHCP server dan setelah login ada perintah mengisi data pribadi. Jika hal itu terjadi, artinya attacker berhasil mendapatkan data pribadi PC KORBAN.

Gambar 3. Halaman Web Palsu (Phishing)

4.3 Skenario 3

Dengan melakukan setting dan konfigurasi DHCP Snooping, diperoleh konfigurasi Switch Server yang terbaru ditunjukkan Gambar 4. Gambar 4 menunjukkan setting dan konfigurasi Switch SW1 yang ada pada jaringan LAN PC KORBAN. Terlihat bahwa hanya interface GigabitEthernet0/1 yang dipercaya untuk memberikan akses layanan Authorized DHCP Server. Setelah dilakukan konfigurasi DHCP Snooping pada Switch SW1, dilakukan 10 kali percobaan DHCP Discovery dari PC KORBAN. Hasil percobaan tersebut ditunjukkan pada tabel 2.



Gambar 4. Konfigurasi DHCP Snooping Pada Switch SW1 (PC KORBAN)

Tabel 2. Hasil IP Address DHCP yang didapat PC KORBAN setelah dilakukan setting DHCP Snooping

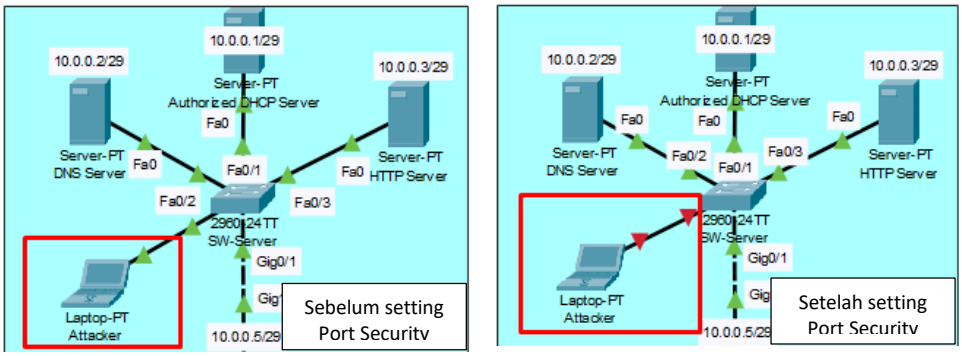
Percobaan ke-	IP Address DHCP	Subnet Mask	Gateway	DNS	DHCP Server
1	192.168.10.1	255.255.255.0	192.168.10.254	10.0.0.2	Authorized
2	192.168.10.2	255.255.255.0	192.168.10.254	10.0.0.2	Authorized
3	192.168.10.1	255.255.255.0	192.168.10.254	10.0.0.2	Authorized
4	192.168.10.2	255.255.255.0	192.168.10.254	10.0.0.2	Authorized
5	192.168.10.1	255.255.255.0	192.168.10.254	10.0.0.2	Authorized
6	192.168.10.2	255.255.255.0	192.168.10.254	10.0.0.2	Authorized
7	192.168.10.2	255.255.255.0	192.168.10.254	10.0.0.2	Authorized
8	192.168.10.1	255.255.255.0	192.168.10.254	10.0.0.2	Authorized
9	192.168.10.2	255.255.255.0	192.168.10.254	10.0.0.2	Authorized
10	192.168.10.1	255.255.255.0	192.168.10.254	10.0.0.2	Authorized

Dari Tabel 2 dapat dilihat bahwa dalam 10 kali percobaan DHCP Discovery, PC KORBAN selalu mendapatkan IP DHCP dari Authorized DHCP Server. Artinya koneksi yang dihasilkan dalam 10 kali percobaan tersebut 100% aman, karena akses dari PC KORBAN ke halaman web akan selalu diarahkan ke alamat web asli, seperti ditunjukkan pada Gambar 5. Hal ini akan meningkatkan keamanan sistem jaringan.

Gambar 5. Halaman Web Asli

4.4 Skenario 4

Untuk lebih meningkatkan keamanan pada sisi server, penulis melakukan setting dan konfigurasi port security pada switch server SW-Server. Dengan cara mendaftarkan MAC Address server yang terhubung SW-Server dan mematikan semua port yang tidak terpakai. Hasilnya laptop Attacker yang tadinya terhubung ke SW-Server menjadi tidak dapat terhubung walaupun dihubungkan dengan kabel dan dikonfigurasi dengan tepat dikarenakan port tersebut sudah dinonaktifkan, seperti yang ditunjukkan pada Gambar 6.



Gambar 6. Hasil Setting Port Security

```
Switch#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0007.ec60.e905    STATIC      Fa0/3
   1    0009.7c5e.72e8    STATIC      Fa0/1
   1    0090.2199.e635    DYNAMIC     Gig0/1
   1    00e0.a372.a353    STATIC      Fa0/2
Switch#
```

Gambar 7. MAC Address Table

Gambar 7 menunjukkan MAC Address table yang terdaftar pada Switch SW-Server. Artinya , hanya perangkat yang memiliki MAC Address tersebutlah yang dapat terhubung dan berkomunikasi melalui SW-Server.

KESIMPULAN DAN SARAN

Berdasarkan hasil pengujian pada simulasi, maka dapat disimpulkan bahwa penggunaan metode DHCP Snooping sangat efektif untuk menghindari adanya distribusi IP DHCP dari Rogue DHCP Server. Hal itu terbukti pada percobaan setelah dilakukan setting dan konfigurasi DHCP Snooping, PC KORBAN 100% mendapatkan IP DHCP dari Authorized DHCP Server. Hal ini akan lebih meningkatkan keamanan jaringan terutama ancaman DNS Spoofing dan phishing.

Penggunaan teknik switch port security juga efektif dalam mengatasi user asing atau attacker yang mencoba ingin masuk ke jaringan. Karena user hanya akan berhasil terkoneksi jika port yang digunakan aktif dan MAC Address user sudah tercatat pada MAC Address table. Hasil prosentase pengujian laptop Attacker yang berhasil terkoneksi ke jaringan sebelum adanya switch port security adalah 100% dan setelah adanya switch port security, laptop Attacker yang berhasil terkoneksi kedalam jaringan adalah 0%.

DAFTAR REFERENSI

Dewanto, M. A. B., Fathurrahman, M., Firdaus, D. R., & Setiawan, A. (2024). Penipuan Penambah *Followers* Instagram: Analisis Serangan *Phising* dan Dampaknya pada Keamanan Data. *Journal of Internet and Software Engineering*, 1(4), 11-11.

Pradana, D. A., & Budiman, A. S. (2021). The DHCP Snooping and DHCP alert method in securing DHCP server from DHCP rogue attack. *IJID (International Journal on Informatics for Development)*, 10(1), 38-46.

Dara, Y. C., Hariadi, F., & Lede, P. A. R. L. (2022). Analisis Penerapan Sistem Keamanan Jaringan Menggunakan Metode DHCP Snooping Dan Switch Port Security. *Jurnal Inovatif*, 1(3), 187-196.

Tamsir Ariyadi, T. (2022). Desain keamanan DHCP snooping untuk mengurangi serangan Local Area Network (LAN).

Miftah, Z. (2018). Simulasi keamanan jaringan dengan metode DHCP SNOOPING dan VLAN. *Faktor Exacta*, 11(2), 167.

Akashi, S., & Tong, Y. (2019). Classification of DHCP spoofing and effectiveness of DHCP snooping. *In Proceedings on 2018 International Conference on Advances in Computer Technology, Information Science and Communication*, edited by Wen-Bing Horng and Yong Yue (pp. 233-238).

Putra, W. P., & Azis, M. Z. (2023). Penggunaan Metode DHCP Snooping Dalam Melakukan Pencegahahan Terhadap DHCP Rogue Di Laboratorium Teknik Informatika. *Journal of Informatics and Computing*, 2(1), 48-54.

Nurfaishal, M. D., & Akbar, Y. (2024). Analisis Efektivitas Keamanan Jaringan Layer 2: Port Security, VLAN Hopping, DHCP Snooping. *Jurnal Indonesia: Manajemen Informatika dan Komunikasi*, 5(3), 3278-3290.

Hidayat, W., Ramli, H., Ikhram, P. M. B., Ridhawi, A. R., Mukhtar, N. A., & Junedy, R. (2023). Analisa Clustering Phising Untuk Meningkatkan Kesadaran Mahasiswa Terhadap Keamanan Data Pribadi Mahasiswa Universitas Negeri Makassar. *Vokatek: Jurnal Pengabdian Masyarakat*, 28-33.

Sinaga, M. P., Ginting, E., Nurdin, M. R., & Putra, M. D. (2023). Analisis Ancaman Phising Terhadap Layanan Online Perbankan. *UNES Journal of Scientech Research*, 8(1), 041-047.

Zara, S. S., Elhanafi, A. M., & Handoko, D. (2020). Pemodelan Jaringan Wan Dengan Teknologi Frame Relay Dengan Memanfaatkan Switch Port Security Sebagai Sistem Keamanan Jaringan. *Semin. Nas. Teknol. Inf. Komun. Ke*, *7*.