IMPLEMENTASI PENETRASI JARINGAN *PUBLIC WIFI* MENGGUNAKAN *ARP SPOOFING* DENGAN METODE *PENETRATION TESTING*

TUGAS AKHIR

FITRAH CAHYA

1162001029

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNIK DAN ILMU KOMPUTER

UNIVERSITAS BAKRIE

JAKARTA

2023

IMPLEMENTASI PENETRASI JARINGAN *PUBLIC WIFI* MENGGUNAKAN *ARP SPOOFING* DENGAN METODE *PENETRATION TESTING*

TUGAS AKHIR

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer

FITRAH CAHYA

1162001029

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNIK DAN ILMU KOMPUTER

UNIVERSITAS BAKRIE

JAKARTA

2023

Halaman Pernyataan Orisinalitas

Tugas Akhir ini adalah hasil karya saya sendiri, dan
semua sumber baik yang dikutip maupun dirujuk
telah saya nyatakan dengan benar.

Nama	: Fitrah Cahya
NIM	: 1162001029
Tanda Tangan	: 
Tanggal	: 21 Agustus 2023

Halaman Pengesahan

Tugas akhir ini diajukan oleh :

Nama	: Fitrah Cahya
NIM	: 1162001029
Program Studi	: Teknik Informatika
Fakultas	: Teknik dan Ilmu Komputer
Judul Tugas Akhir	: Implementasi Penetrasi Jaringan *Public Wifi* Menggunakan ARP *Spoofing* Dengan Metode *Penetration Testing*

Telah berhasil dipertahankan dihadapan Dewan Penguji sebagai persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi Informatika Fakultas Teknik dan Ilmu Komputer, Universitas Bakrie.

DEWAN PENGUJI

Pembimbing 1	: Iwan Adhicandra, MIIE, MIET, MBCS	(.....)
Pembimbing 2	: Prof. Dr. Hoga Saragih, S.T, M.T	(.....)
Penguji 1	: Albert A. Sembiring, S.T., M.T	(.....)
Penguji 2	: Ihsan Ibrahim, S.T., M.T	(.....)

Ditetapkan : Jakarta

Tanggal : 21 Agustus 2023

Ungkapan Terima Kasih

Bismillahirrahmanirrahim. Puji syukur kepada Allah SWT atas rahmat dan karunia-Nya sehingga Tugas Akhir dengan judul "Implementasi Penetrasi Jaringan *Public Wifi* Menggunakan ARP *Spoofing* Dengan Metode *Penetration Testing*" dapat diselesaikan. Tugas akhir ini merupakan syarat untuk dapat memperoleh gelar Sarjana Komputer di Program Studi Teknik Informatika Fakultas Teknik dan Ilmu Komputer Universitas Bakrie.

Saat mengerjakan Tugas Akhir ini Penulis sangat menghargai bimbingan, bantuan, dukungan dan nasihat yang didapatkan oleh penulis dari orang tua, keluarga, teman, dosen, mentor dan pihak-pihak lain yang telah membantu dalam proses penelitian dan penyusunan Tugas Akhir ini. Maka dari itu, dengan segala kerendahan hati, izinkan penulis mengucapkan terima kasih kepada:

1. Almarhumah Nenek Uminah dan anak-anaknya yaitu Kak Endang dan Kak Aci yang telah merawat dan menemani perjalanan hidup penulis hingga saat ini.

2. Keluarga besar penulis yaitu Mamah Novendrawati, Ayah Madiyo, Kak Chandra, Kak Wawan, Aji, Tika, Amelia, Riswanda, Kak Rini dan Kak Rina. Terima kasih telah menjadi keluarga terbaik yang telah membimbing, mengajari, dan membantu penulis hingga saat ini.

3. Bapak Iwan Adhichandra, MIIE., MIET., MBCS. sebagai dosen pembimbing Tugas Akhir yang sudah memberikan bimbingan, perhatian dan saran selama pengerjaan penelitian tugas akhir ini.

4. Bapak Albert A. Sembiring, S.T., M.T. dan Bapak Ihsan Ibrahim. S.T., M.T. sebagai dosen pembahas seminar proposal yang sudah memberikan bimbingan dan saran untuk perbaikan penelitian tugas akhir ini.

5. Bapak Guson P. Kuntarto, S.T., M.Sc. selaku dosen pembimbing akademik yang telah memberikan bimbingan, saran, nasihat dan pengajaran baik pada saat perkuliahan dan diluar perkuliahan.

6. Seluruh dosen Teknik Informatika yang telah mengajar dan mendidik saat proses pembelajaran di Universitas Bakrie sehingga penulis mendapatkan banyak ilmu pengetahuan dan wawasan yang bermanfaat.

7. A. Gregory Qonitah Michelle yang telah banyak sekali membantu penulis dengan memberikan nasihat, saran, serta bantuan untuk menyusun dan mengerjakan penelitian ini.

8. Mutiara Julia Ifra dan Hafiz Kurnia Aji yang telah mengerjakan tugas akhir ini bersama-sama di Lab B Universitas Bakrie dan telah memberikan bimbingan, nasihat dan saran dalam mengerjakan Tugas Akhir ini.

9. Elsismone Utari Fitri yang telah memberikan nasihat, saran, serta perhatian mengenai kemajuan pembuatan tugas akhir penulis.

10. Aiy, Rafi, Michelle, Husen, Nida dan Laode yang sering mengajak main dan menjaga silaturahmi yang akhirnya selalu memberikan nasihat dan saran dalam pengerjaan tugas akhir ini.

11. Seluruh teman-teman seperjuangan Teknik Informatika 2016 yang sudah berjuang hingga saat ini. Terima kasih untuk kenangan bahagia, sedih, lucu, seru, dan capeknya pada 7 tahun ini. Mungkin kalau tidak ada Covid kita masih bisa terus ngumpul bareng.

12. Universitas Bakrie sebagai tempat untuk belajar dan bertemunya teman-teman, dosen, kakak angkatan dan adik angkatan. Terima kasih telah menyediakan Lab B sebagai tempat untuk mengerjakan tugas akhir ini. Serta Mba Maudy sebagai pengurus Lab B Universitas Bakrie yang telah memberikan izin menggunakan ruangan Lab B.

13. Seluruh pihak yang terlibat, baik saudara dan teman-teman yang telah membantu dan memberikan semangat serta doa dalam pengerjaan tugas akhir ini.

Semoga Allah SWT membalas segala kebaikan yang telah diberikan berupa rezeki dan rahmat-Nya. Tugas akhir ini penulis buat dengan masih banyak kekurangan, semua kritik dan saran akan membantu untuk bisa membuat Tugas Akhir ini lebih baik lagi dan harapannya dapat bermanfaat bagi banyak di masa yang akan datang.

Jakarta, 21 Agustus 2023

Penulis

Fitrah Cahya

Halaman Pernyataan Persetujuan Publikasi

Sebagai civitas akademik Universitas Bakrie, saya yang bertanda tangan dibawah ini :

Nama	: Fitrah Cahya
NIM	: 1162001029
Program Studi	: Teknik Informatika
Fakultas	: Teknik dan Ilmu Komputer

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Bakrie **Hak Bebas Royalti Noneksklusif *(Non-exclusive Royalty Free Right)*** atas karya ilmiah saya yang berjudul :

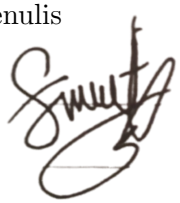
Implementasi Penetrasi Jaringan *Public Wifi* Menggunakan ARP *Spoofing* Dengan Metode *Penetration Testing*

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Bakrie berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (database), merawat dan mempublikasikan tugas akhir saya sebagai penulis/pencipta dan pemilik Hak Cipta untuk kepentingan akademis.
Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di	: Jakarta
Tanggal	: 21 Agustus 2023

Jakarta, 21 Agustus 2023

Penulis



Fitrah Cahya

IMPLEMENTASI PENETRASI JARINGAN *PUBLIC WIFI* MENGGUNAKAN *ARP SPOOFING* DENGAN METODE *PENETRATION TESTING*

Fitrah Cahya

ABSTRAK

Jaringan internet menjadi kunci utama untuk seseorang dapat mengakses internet untuk mengerjakan pekerjaannya sehingga seseorang dapat terhubung satu sama lain. Jaringan wifi merupakan salah satu jenis jaringan yang dapat menghubungkan perangkat ke suatu jaringan. *Wireless router* merupakan perangkat digunakan untuk menyedeiakan jaringan wifi. Untuk melakukan koneksi ke jaringan wifi biasanya seseorang diharuskan mengisi *password* wifi sebagai bentuk keamanan agar tidak semua orang dapat terkoneksi ke jaringan tersebut. Berbeda dengan jaringan *public wifi*, jaringan ini merupakan tipe jaringan yang tidak memiliki sistem keamanan jaringan. Hal ini membuat jaringan *public wifi* rentan terhadap serangan, salah satu jenis serangan jaringan adalah ARP *spoofing/poisoning*. ARP *spoofing* memungkinkan untuk dapat menangkap data-data target penyerangan melalui router/*gateway* yang terkoneksi oleh perangkat korban dan komputer penyerang. Untuk melakukan serangan ARP *spoofing* komputer penyerang dan perangkat korban harus menggunakan koneksi jaringan yang sama karena hal ini public wifi sangat rentan terhadap serangan ini. Saat melakukan koneksi jaringan wifi, router mengirimkan alamat ip ke setiap perangkat yang terkoneksi jaringan, perangkat mengirimkan alamat MAC ke router. Berdasarkan hal ini ARP *spoofing* menggunakan alamat MAC korban dan mengirimkannya ke router seolah-olah komputer penyerang merupakan perangkat target, sehingga router mengirimkan data-data korban yang mengakses internet dikirimkan ke komputer penyerang. Penelitian ini melakukan pengujian observasi perubahan halaman *website* setelah dilakukan penyerangan ARP *spoofing* dan melakukan pengujian autentikasi halaman *website* berupa username dan password yang diakses perangkat target. Hasilnya perangkat target dapat mengetahui dirinya diserang berdasarkan perubahan pada halaman *website*, perangkat target tidak mengetahui jika data *username* dan *password* yang diakses pada halaman *website* berhasil dicuri, dan terbukti bahwa perangkat penyerang mengelabui perangkat target dengan seolah-olah mengira dirinya adalah *gateway*.

Kata Kunci : ***Wifi, Public wifi, ARP, Spoofing, Ip, MAC, Router, Wireless router, pengujian, halaman website, website, perangkat target, gateway***

IMPLEMENTASI PENETRASI JARINGAN *PUBLIC WIFI* MENGGUNAKAN *ARP SPOOFING* DENGAN METODE *PENETRATION TESTING*

Fitrah Cahya

ABSTRACT

The internet network is the main key for someone to access the internet to do their work so that people can connect to each other. A wifi network is one type of network that can connect devices to a network. Wireless router is a device used to provide a wifi network. To connect to a wifi network, usually someone is required to fill in a wifi password as a form of security so that not everyone can connect to the network. Unlike the public wifi network, this network is a type of network that does not have a network security system. This makes public wifi networks vulnerable to attacks, one type of network attack is ARP spoofing / poisoning. ARP spoofing makes it possible to capture attack target data through a router/gateway connected to the victim's device and the attacker's computer. To carry out an ARP spoofing attack, the attacker's computer and the victim's device must use the same network connection because public wifi is very vulnerable to this attack. When connecting to a wifi network, the router sends an ip address to each device connected to the network, the device sends the MAC address to the router. Based on this, ARP spoofing uses the victim's MAC address and sends it to the router as if the attacker's computer is the target device, so that the router sends the victim's data accessing the internet sent to the attacker's computer. This research tests the observation of changes in web pages after an ARP spoofing attack and tests the authentication of web pages in the form of usernames and passwords accessed by the target device. The result is that the target device can know that it is being attacked based on changes to the web page, the target device does not know if the username and password data accessed on the web page has been successfully stolen, and it is proven that the attacker device tricks the target device into thinking it is a gateway

Kata Kunci : ***Wifi, Public wifi, ARP, Spoofing, Ip, MAC, Router, Wireless router, tests, web pages, website, target device, gateway***

Daftar Isi

Daftar Tabel

Daftar Gambar

Daftar Singkatan

Singkatan	Penjelasan
IP	: *Internet Protocol*
MAC	: *Media Access Control*
ARP	: *Address Resolution Protocol*
MTM	: *Man in The Middle*
DoS	: *Denial of Service*
LAN	: *Local Area Network*
WAN	: *Wide Area Network*
WLAN	: *Wireless Local Area Network*
AP	: *Access Point*
WEP	: *Wired Equivalent Privacy*
WPA	: *Wireless Protected Access*
WPA2-PSK	: *Wireless Fidelity Protected Access 2- Pre-Shared Key*
SQL	: *Structured Query Language*
SIM	: *Subscriber Identification Module*
HTML	: *HyperText Markup Language*
XML	: *Extensible Markup Language*
HTTP	: *Hypertext Transfer Protocol*
CPU	: *Central Processing Unit*
RAM	: *Random Access Memory*
OSI	: *Open System Interconnect*
DNS	: *Domain Name System*
FTP	: *File Transfer Protocol*