

**ANALISIS KEAMANAN WIFI PUBLIK MENGGUNAKAN METODE
PENETRATION TESTING EXECUTION STANDARD(PTES)
(STUDI KASUS: KANTOR SEKRETARIAT DAERAH KABUPATEN
SLEMAN)**

SKRIPSI



disusun oleh

Akhmad Atthar

18.83.0189

**PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2022**

**ANALISIS KEAMANAN WIFI PUBLIK MENGGUNAKAN
METODE PENETRATION TESTING EXECUTION
STANDARD (PTES)
(STUDI KASUS: KANTOR SEKRETARIAT DAERAH
KABUPATEN SLEMAN)**

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Teknik Komputer



disusun oleh

Akhmad Atthar

18.83.0189

**PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2022**

PERSETUJUAN

SKRIPSI

**ANALISIS KEAMANAN WIFI PUBLIK MENGGUNAKAN METODE
PENETRATION TESTING EXECUTION STANDARD (PTES)
(STUDI KASUS: KANTOR SEKRETARIAT DAERAH KABUPATEN
SLEMAN)**

yang dipersiapkan dan disusun oleh

Akhmad Atthar

18.83.0189

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 5 April 2022

Dosen Pembimbing,

Banu Santoso, S.T.,M.Eng.
NIK. 190302327

PENGESAHAN

SKRIPSI

**ANALISIS KEAMANAN WIFI PUBLIK MENGGUNAKAN METODE
PENETRATION TESTING EXECUCION STANDARD(PTES)
(STUDI KASUS: KANTOR SEKRETARIAT DAERAH KABUPATEN
SLEMAN)**

yang dipersiapkan dan disusun oleh

Akhmad Atthar

18.83.0189

telah dipertahankan di depan Dewan Penguji
pada tanggal 20 April 2022

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Wahid Miftahul Ashari, S.Kom., M.T.
NIK. 190302452

Senle Destva, M.Kom.
NIK. 190302312

Banu Santoso, S.T., M.Eng.
NIK. 190302327

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
20 April 2022

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, M.Kom.
NIK.190302096

PERNYATAAN

PERNYATAAN

Saya yang bertanda tangan di bawah ini menyatakan bahwa, bahwa saya merupakan karya saya sendiri (ASLI), dan di dalam karya ini tidak terdapat karya yang pernah dipublikasikan oleh orang lain, atau pernah dipublikasikan pada skripsi di suatu institusi pendidikan tinggi manapun, dan pernyataan pengesahan saya juga tidak terdapat karya lain, pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diuraikan dalam naskah ini dan diuraikan dalam daftar pustaka.

Segala sesuatu yang terkait dengan karya dan karya saya tidak akan pernah dipublikasikan kembali oleh orang lain.

Yogyakarta, 4 April 2022

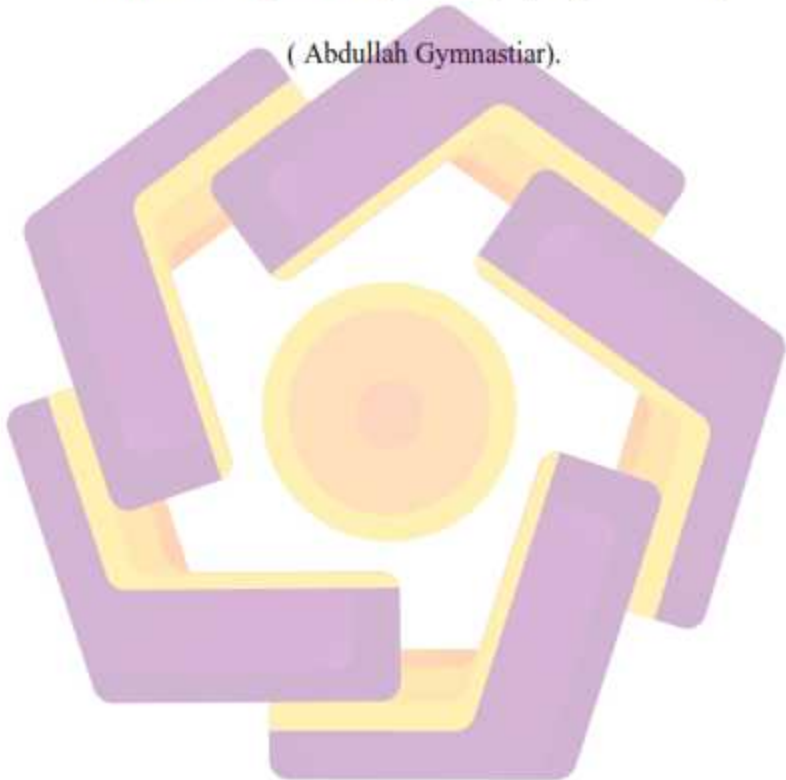


Ahmad Athir
NIM. 1803.0189

MOTTO

"Sesekali berhentilah sekadar untuk bersantai. Bukan untuk terlena, namun membangun semangat untuk perjuangan berikutnya."

(Abdullah Gymnastiar).



PERSEMBAHAN

Dengan rasa syukur yang mendalam bersamaan dengan telah diselesaikannya skripsi ini, Penulis mempersembahkannya kepada:

1. Keluarga besar penulis khususnya Ayah dan Ibu serta adik yang telah senantiasa menemani dan membantu menyelesaikan skripsi ini.
2. Para Dosen-dosen SI Teknik Komputer yang telah membimbing penulis hingga terselesaikannya skripsi ini.
3. Bapak Jojo , Bapak Koko , Ibu Hani yang telah menyediakan tempat penelitian
4. Teman teman penulis baik itu teman kuliah seangkatan, adik kelas , kakak kelas pada Fakultas Ilmu Komputer Universitas Amikom Yogyakarta yang telah banyak memberi masukan , semangat , serta arahan sehingga dapat terselesaikannya skripsi ini.
5. Teman teman bermain game khususnya teman pada discord, yang senantiasa memberikan alasan bagi penulis untuk segera menyelesaikan skripsi ini.

KATA PENGANTAR

Alhamdulillah, Puji Syukur penulis panjatkan kepada Allah Subhanahu Wata'ala, atas ridhonya penulis dapat menyelesaikan penyusunan skripsi yang berjudul **"Analisis Keamanan Wifi Publik Menggunakan Metode Penetration Testing Execution Standard (PTES)"** Studi kasus pada Kantor Sekretariat Daerah Kabupaten Sleman.

Skripsi ini diajukan untuk memenuhi syarat kelulusan mata kuliah skripsi pada Fakultas Ilmu Komputer Amikom Yogyakarta. Penulis menyadari bahwa skripsi ini tidak akan selesai tanpa orang-orang disekeliling saya yang senantiasa mendukung dan membantu. Oleh karena itu, penulis dengan penuh rasa syukur dan hormat mengucapkan terimakasih kepada

1. Bapak Prof. Dr. M. Suyanto, M.M. selaku Rektor Universitas Amikom Yogyakarta
2. Bapak Hanif Al Fatta, S.Kom., M.Kom. selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta
3. Bapak Dony Ariyus, M.Kom. selaku ketua Prodi Teknik Komputer Universitas Amikom Yogyakarta
4. Bapak Banu Santoso, S.T., M.Eng. selaku Dosen Pembimbing
5. Bapak Suyudi, MM selaku Pembina Tingkat I Kantor Sekretariat Daerah Kabupaten Sleman

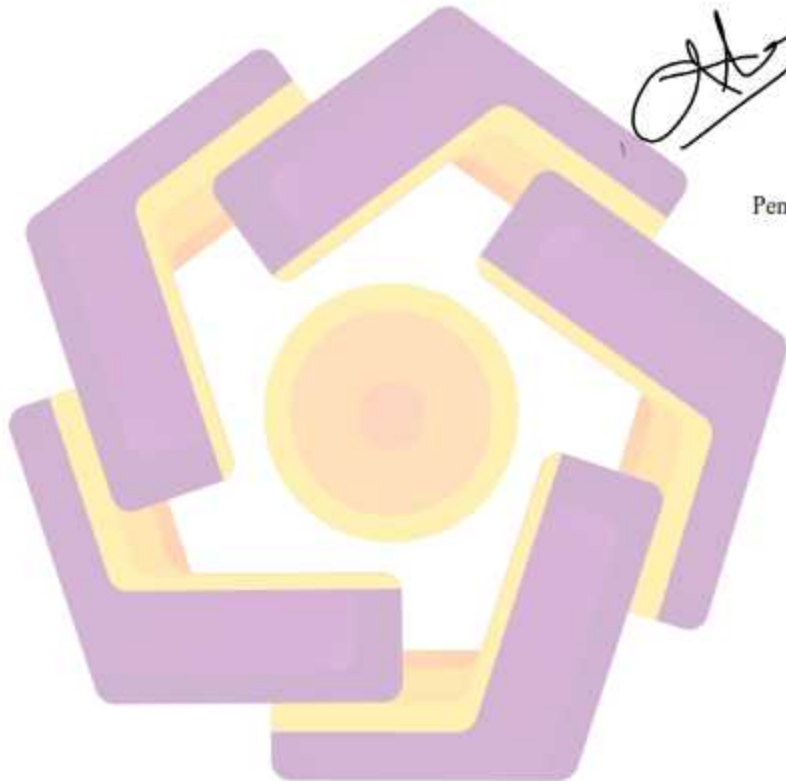
Ucapan terimakasih penulis sampaikan kepada semua pihak yang telah membantu dalam melakukan penelitian yang tidak dapat penulis sebutkan satu persatu.

Akhir kata penulis ingin meminta maaf atas segala kekurangan yang terdapat pada penulisan skripsi ini . Penulis berharap semoga skripsi ini dapat menjadi bacaan yang bermanfaat serta menambah wawasan bagi pembaca.

Sleman, 4 April 2022



Penulis

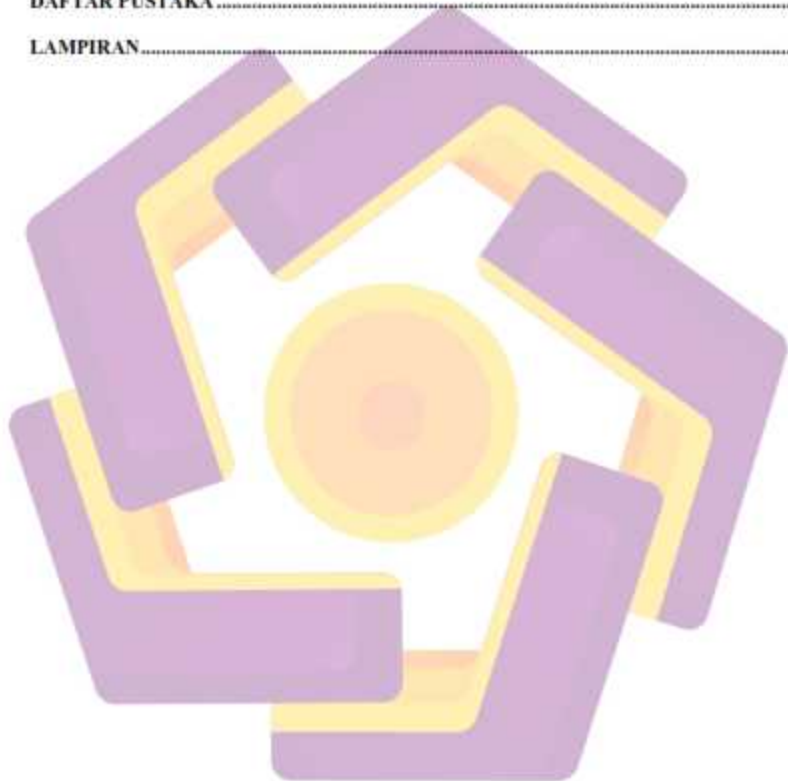


DAFTAR ISI

HALAMAN JUDUL	II
HALAMAN PERSETUJUAN.....	III
HALAMAN PENGESAHAN	IV
HALAMAN PERNYATAAN.....	V
HALAMAN MOTTO	VI
HALAMAN PERSEMBAHAN.....	VII
KATA PENGANTAR.....	VIII
DAFTAR ISI.....	X
DAFTAR TABEL.....	XIII
DAFTAR GAMBAR	XIV
<i>INTISARI</i>	XVI
<i>ABSTRACT</i>	XVII
BAB I PENDAHULUAN.....	1
1.1. LATAR BELAKANG.....	1
1.2. RUMUSAN MASALAH.....	2
1.3. PERTANYAAN PENELITIAN.....	2
1.4. BATASAN MASALAH.....	3
1.5. MAKSUD DAN TUJUAN PENELITIAN.....	3
1.6. MANFAAT PENELITIAN.....	3
1.7. METODE PENELITIAN.....	4
1.8. SISTEMATIKA PENULISAN.....	6
BAB II LANDASAN TEORI.....	8
2.1. KAJIAN PUSTAKA.....	8
2.2. JARINGAN KOMPUTER	11
2.2.1. <i>Klasifikasi Jaringan Berdasarkan Cakupan Geografis.....</i>	<i>12</i>
2.2.2. <i>Klasifikasi Jaringan Berdasarkan Distribusi Sumber informasi.....</i>	<i>14</i>
2.2.3. <i>Klasifikasi Jaringan Berdasarkan Media Transmisi Data.....</i>	<i>14</i>
2.3. GAMBARAN UMUM KEAMANAN JARINGAN.....	15
2.4. PENETRATION TESTING STANDARD.....	16
2.5. PERBANDINGAN METODE PENETRATION TESTING STANDARD.....	18

2.6.	PENETRATION TESTING EXECUTION STANDARD.....	19
2.7.	TEKNIK PENGULIAN	22
2.8.	ALAT DAN SOFTWARE YANG DIGUNAKAN	23
2.7.1.	<i>Kali Linux</i>	24
2.7.2.	<i>Nessus</i>	24
2.7.3.	<i>Nmap/Zenmap</i>	25
2.7.4.	<i>DMitry</i>	26
2.7.5.	<i>Ettercap</i>	26
2.7.6.	<i>Driftnet</i>	27
2.7.7.	<i>Aircrack-ng</i>	27
2.7.8.	<i>Bettercap</i>	27
2.7.9.	<i>Dsniff</i>	28
2.7.10.	<i>Airgeddon</i>	28
2.7.11.	<i>Fluxion</i>	28
2.7.12.	<i>Wireshark</i>	28
2.7.13.	<i>Macchanger</i>	29
BAR III METODE PENELITIAN		30
3.1.	WAKTU DAN TEMPAT PENELITIAN	30
3.1.1.	<i>Waktu Penelitian</i>	30
3.1.2.	<i>Tempat Penelitian</i>	30
3.2.	ANALISA PERMASALAHAN.....	30
3.3.	ALAT DAN BAHAN PENELITIAN	31
3.3.1.	<i>Perangkat Keras (Hardware)</i>	31
3.3.2.	<i>Perangkat Lunak (Software)</i>	32
3.4.	METODE PENGUMPULAN DATA	33
3.5.	KERANGKA PEMIKIRAN	33
3.6.	TEKNIK PENGULIAN KEAMANAN.....	36
3.7.	METODE ANALISIS YANG AKAN DIGUNAKAN.....	37
BAR IV HASIL DAN PEMBAHASAN.....		43
4.1.	PENERAPAN	43
4.2.	PENERAPAN PENYERANGAN	43
4.2.1.	<i>ARP Spoofing (Man-In-The-Middle-Attack)menggunakan Ettercap, Bettercap, Dsniff, Driftnet, Wireshark</i>	43
4.2.2.	<i>Wifi Deauthentication Attack menggunakan Aireplay(Aircrack-ng)</i>	52
4.2.3.	<i>Evil Twin attack menggunakan Airgeddon dan Fluxion</i>	58
4.2.4.	<i>Mac Spoofing attack menggunakan Macchanger</i>	68

4.3.	HASIL ANALISIS DAN REPORT HASIL PENYERANGAN.....	70
4.3.1.	<i>Usulan Peningkatan Keamanan</i>	73
BAB V	PENUTUP	74
5.1	KESIMPULAN.....	74
5.2	SARAN.....	75
DAFTAR PUSTAKA	76
LAMPIRAN	79



DAFTAR TABEL

Tabel 1. 1 Alat dan Software.....	4
Tabel 1. 2 Software yang akan digunakan	5
Tabel 1. 3 Ekspektasi Hasil.....	5
Tabel 2. 1 Penelitian Terkait	9
Tabel 2. 2 Perbandingan Metode Penetration Testing Standard	18
Tabel 3. 1 Spesifikasi Laptop Attacker	31
Tabel 3. 2 Spesifikasi Laptop Victim.....	31
Tabel 3. 3 Spesifikasi Android Victim	32
Tabel 3. 4 Serangan yang akan digunakan.....	36
Tabel 4. 2 Hasil penyerangan menggunakan Penetration Testing Execution Standard.....	71

DAFTAR GAMBAR

Gambar 2. 1 Alur PTES[13].....	19
Gambar 3. 1 <i>flowchart</i> alur penelitian	34
Gambar 3. 2 <i>flowchart</i> alur pengumpulan dan pengolahan data[15].....	35
Gambar 3. 3 SSID Wifi yang terdeteksi.....	39
Gambar 4. 1 Alamat IP pada Laptop Korban.....	44
Gambar 4. 2 Tampilan Ettercap	44
Gambar 4. 3 Scan host pada ettercap	45
Gambar 4. 4 Hasil scanning host pada ettercap	45
Gambar 4. 5 Konfigurasi ip static pada laptop korban.....	46
Gambar 4. 6 Tampilan bettercap.....	47
Gambar 4. 7 Tampilan net.probe on.....	47
Gambar 4. 8 tampilan ipconfig pada laptop korban.....	48
Gambar 4. 9 tampilan command echo 1 > /proc/sys/net/ipv4/ip_forward.....	49
Gambar 4. 10 tampilan command arp spoofing pada software dsniff.....	49
Gambar 4. 11 Tampilan filter arp pada wireshark	50
Gambar 4. 12 pengecekan hasil arp spoofing dengan membuka website http.....	50
Gambar 4. 13 Tampilan filter http pada wireshark	51
Gambar 4. 14 tampilan filter ip addr pada wireshark.....	51
Gambar 4. 15 informasi lengkap wireless pada laptop korban.....	52
Gambar 4. 16 melakukan scanning wifi pada wlan0	53
Gambar 4. 17 hasil scanning network.....	53
Gambar 4. 18 Melakukan scanning host pada salah satu network.....	54
Gambar 4. 19 hasil scanning host pada network.....	54
Gambar 4. 20 Mengirimkan paket deauth.....	55
Gambar 4. 21 Network dc pada laptop korban	55
Gambar 4. 22 Informasi Wifi pada Android.....	56
Gambar 4. 23 Death attack ke Android Device	56
Gambar 4. 24 Death attack sedang berlangsung.....	57

Gambar 4. 25 Network dc pada Android	57
Gambar 4. 26 Konfigurasi evil twin airgeddon.....	58
Gambar 4. 27 Airgeddon hasil scanning.....	59
Gambar 4. 28 Konfigurasi evil twin fluxion	59
Gambar 4. 29 Fluxion hasil scanning.....	60
Gambar 4. 30 List wifi pada laptop attacker.....	60
Gambar 4. 31 List wifi pada laptop korban.....	61
Gambar 4. 32 Alamat IP Laptop korban yang terkoneksi dengan wifi tiruan	62
Gambar 4. 33 Scan host Ettercap pada EvilTwin	62
Gambar 4. 34 target arp spoofing.....	63
Gambar 4. 35 arp spoofing telah berjalan	63
Gambar 4. 36 Pengecekan arp spoofing dengan wireshark	64
Gambar 4. 37 pengecekan dengan membuka website http.....	64
Gambar 4. 38 cek lalu lintas traffic menggunakan wireshark.....	65
Gambar 4. 39 tcp stream pada wireshark	65
Gambar 4. 40 online pcap viewer	66
Gambar 4. 41 online pcap viewer 2	66
Gambar 4. 42 drifnet	67
Gambar 4. 43 Hasil dari software driftnet.....	67
Gambar 4. 44 Tampilan MAC address Laptop Attacker	68
Gambar 4. 45 Tampilan macchanger	69
Gambar 4. 46 Tampilan mac address beserta ping	69
Gambar 4. 47 Tampilan Mac address yang kembali seperti semula.....	70

INTISARI

Pertumbuhan teknologi informasi yang semakin pesat tentu semakin memudahkan kebutuhan masyarakat dalam hal informasi.. Wifi Publik adalah salah satu contoh dari perkembangan teknologi informasi. Namun seiring dengan perkembangan teknologi wifi tersebut,berkembang pula ancaman terhadap keamanan teknologi wifi. Kantor Sekretariat Daerah Kabupaten Sleman adalah tempat layanan administrasi yang ramai dikunjungi oleh masyarakat dimana kantor tersebut menyediakan layanan jaringan internet publik atau Wifi bagi masyarakat.

Analisis keamanan wifi publik pada Kantor Sekretariat Daerah Kabupaten Sleman dilakukan dengan menerapkan metode *Penetration Testing Execution Standard*. Dimana penulis akan mengumpulkan informasi mengenai jaringan wifi publik tersebut lalu dilakukan sebuah serangan menggunakan empat parameter yaitu: *ARP Spoofing (Man-In-The-Middle-Attack)*, *Wifi Deauthentication Attack*, *Evil Twin Attack*, *Mac Spoofing* guna mengetahui tingkat keamanan wifi publik tersebut.

Diketahui dari hasil analisis keamanan yang telah dilakukan, bahwa wifi publik pada kantor Sekretariat Daerah Kabupaten Sleman belum cukup aman, dimana dari empat parameter serangan tersebut terdapat dua parameter serangan yang berhasil dilakukan yaitu *evil twin attack* dan *Wifi Deauthentication Attack*. Sedangkan untuk dua parameter lainnya yaitu *arp-spoofing(man-in-the-middle-attack)* dan *mac spoofing* tidak berhasil dilakukan. Agar keamanan wifi publik menjadi lebih aman perlu diadakannya *rule* yang akan menghentikan tindakan *mass packet* serta melakukan monitoring ssid jaringan guna mencegah tindakan *evil twin*.

Kata kunci: Wifi Publik, *Penetration Testing Execution Standard (PTES)*, *ARP Spoofing (Man-In-The-Middle-Attack)*, *Wifi Deauthentication Attack*, *Evil Twin Attack*

ABSTRACT

The rapid growth of information technology has made it easier for the public in terms of information. Public Wifi os one example of the development of information technology. Regional Secretary Office of Sleman District is an administrative service place that is crowded by the public where the office provides public internet or Wifi network services for the community.

Analysis of public wifi security at the Regional Secretary Office of Sleman District was carried out by applying the Penetration Testing Execution Standard method. Where the author will collect information about the public wifi network then an attack is carried out using four parameters ARP Spoofing (Man-In-The-Middle-Attack), Wifi Deauthentication Attack, Evil Twin Attack, Evil Twin Attack(Man-In-The -Middle-Attack) , Mac Spoofing to find out the level of security of the public wifi.

It is known from the results of the security analysis that has been carried out, that the public wifi at the Regional Secretarial office of Sleman Regency is not safe enough, where from the four attack parameters there are two attack parameters that were successfully carried out, namely evil twin attack and Wifi Deauthentication Attack. Meanwhile, the other two parameters, namely arp-spoofing(man-in-the-middle-attack) and mac spoofing were not successful. In order for public wifi security to be more secure, it is necessary to have a rule that will stop mass packet actions and monitor network SSID to prevent evil twin attacks.

Keyword: *Public Wifi, Penetration Testing Execution Standard (PTES), ARP Spoofing (Man-In-The-Middle-Attack), Wifi Deauthtentation Attack, Evil Twin Attack*