PENGUJIAN CELAH KEAMANAN UNTUK MENGETAHUI KERENTANAN KEAMANAN JARINGAN *WIRELESS* DENGAN METODE *PENETRATION TESTING EXECUTION STANDARD* (PTES) PADA PT. QWE

SKRIPSI

RULLI AZANI AKBAR

1810511122

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

FAKULTAS ILMU KOMPUTER

PROGRAM STUDI INFORMATIKA

2022

PENGUJIAN CELAH KEAMANAN UNTUK MENGETAHUI KERENTANAN KEAMANAN JARINGAN *WIRELESS* DENGAN METODE *PENETRATION TESTING EXECUTION STANDARD* (PTES) PADA PT. QWE

SKRIPSI

Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Sarjana Komputer

RULLI AZANI AKBAR

1810511122

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

FAKULTAS ILMU KOMPUTER

PROGRAM STUDI INFORMATIKA

2022

PERNYATAAN ORISINALITAS

PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri, dan sumber yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar.

Nama : Rulli Azani Akbar

NIM : 1810511122

Tanggal : 18 Juli 2022

Bilamana dikemudian hari ditemukan ketidaksamaan dengan pernyataan ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 18 Juli 2022

Rulli Azani Akbar

PERNYATAAN PERSETUJUAN PUBLIKSASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademik Universitas Pembangunan Nasional Veteran Jakarta, saya yang bertanda tangan dibawah ini:

Nama	: Rulli Azani Akbar
NIM	: 1810511122
Fakultas	: Ilmu Komputer
Program Studi	: Informatika

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

Pengujian Celah Keamanan Untuk Mengetahui Kerentanan Keamanan Jaringan Wireless Dengan Metode Penetration Testing Execution Standard (PTES) Pada PT. QWE

Beserta perangkata yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih-meida/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di :Jakarta

Pada tanggal : 18 Juli 2022

Yang menyatakan,

Rulli Azani Akbar

LEMBAR PENGESAHAN

LEMBAR PENGESAHAN

Dengan ini dinyatakan bahwa Skripsi berikut:

Nama	: Rulli Azani Akbar
Nim	: 1810511122
Program Studi	: S1 Informatika
Judul	: Pengujian Celah Keamanan Untuk Mengetahui Kerentanan Keamanan Jaringan Wireless Dengan Metode Penetration Testing Execution Standard (PTES) Pada PT. QWE

Telah berhasil dipertahankan di hadapan Tim penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi S1 Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.

Bayu Hananto, S.Kom., M.Kom.
Penguji 1

I Wayan Widi P, S.Kom., MTI.
Penguji 2

Jayanta, S.Kom., M.Si.
Dosen Pembimbing 1

Henki Bayu Seta, S.Kom., MTI.
Dosen Pembimbing 2

Dr. Ermatita, M.Kom.
Dekan

Desta Sandya Prasvita, S.Kom., M.Kom.
Ketua Program Studi

Ditetapkan di : **Jakarta**

Tanggal pengesahan : **18 Juli 2022**

PENGUJIAN CELAH KEAMANAN UNTUK MENGETAHUI KERENTANAN KEAMANAN JARINGAN *WIRELESS* DENGAN METODE *PENETRATION TESTING EXECUTION STANDARD* (PTES) PADA PT. QWE

Rulli Azani Akbar

ABSTRAK

Keamanan jaringan *wireless* diperlukan demi untuk perlindungan serta pencegahan dari tindakan kejahatan pencurian informasi. Aspek tersebut sering diabaikan pada setiap instansi karena menganggap bahwa jaringan *wireless* selalu dianggap aman karena bagi setiap instansi akan merasa aman jika permasalahan tersebut belum mengganggu aktivitas pekerjaan dengan memasang *antivirus* maupun *firewall*. Masih banyak instansi yang meremehkan soal ini. Sehingga, perlu dilakukan *penetration testing* untuk mengetahui kerentanan pada jaringan *wireless* dengan metode yang digunakan PTES (*Penetration Testing Execution Standard*) untuk dijadikan standar dalam melakukan analisis sistem keamanan jaringan *wireless* dalam mencari celah keamanan pada sebuah instansi dalam kasus ini yaitu jaringan *wireless local area network* (WLAN) pada PT. Sehat Tentrem dimana pada penelitian ini ditemukan kerentanan berupa *bypassing,, arp spoofing*, *certificate cannot be trusted*, dan adanya kegiatan *sniffing* yang dapat dilakukan pada jaringan *wireless* untuk dieksploitasi,

Kata Kunci : Keamanan Jaringan, vulnerabilities, penetration testing, penetration testing execution standards, sniffing, arp spoofing.

PENGUJIAN CELAH KEAMANAN UNTUK MENGETAHUI KERENTANAN KEAMANAN JARINGAN *WIRELESS* DENGAN METODE *PENETRATION TESTING EXECUTION STANDARD* (PTES) PADA PT. QWE

Rulli Azani Akbar

ABSTRACT

Wireless network security is necessary for the protection and prevention of criminal acts of information theft. This aspect is often ignored by every agency because it assumes that a wireless network is always considered safe because every agency will feel safe if the problem does not interfere with work activities by installing an antivirus or firewall. There are still many institutions that underestimate this. Thus, it is necessary to carry out penetration testing to find out vulnerabilities in wireless networks with the method used by PTES (Penetration Testing Execution Standard) to be used as a standard in analyzing wireless network security systems in finding security holes in an agency in this case, namely the wireless local area network (Wireless Local Area Network). WLAN) at PT. Sehat Tentrem where in this study found vulnerabilities in the form of bypassing, arp spoofing, certificate can not be trusted, and sniffing activities that can be carried out on wireless networks to be exploited,

Keyword *: wireless network security, vulnerabilities, penetration testing, penetration testing execution standards, sniffing, arp spoofing.*

KATA PENGANTAR

Segala puji dan syukur penulis panjatkan kehadirat Tuhan Yang Mahakuasa atas limpahan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan SkripsiTugas Akhir. Skripsi tugas akhir ini disusun sebagai syarat Tugas Akhir Program Studi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta.

Dalam penyelesaian karya tulis ilmiah ini tidak lepas dari bantuan banyak pihak yang telah memberikan masukan kepada penulis. Untuk itu penulis mengucapkan terima kasih kepada:

1. Allah SWT yang senantiyasa selalu memberikan nikmat sehat
2. Dr. Ermatita, M.Kom., selaku dekan Fakultas Ilmu Komputer
3. Desta Sandya Prasvita, S.Kom., M.Kom. selaku Ketua Program Studi Sarjana Jurusan S1 Informatika.
4. Jayanta,S.Kom., M.Si. selaku dosen pembimbing 1 dari pihak jurusan.
5. Henki Bayu Seta, S.Kom., MTI. selaku dosen pembimbing 2 dari pihak jurusan.
6. Orang tua yang telah memberikan dukungan baik secara moril maupun materil
7. Teman seperjuangan yang telah saling memberi support dalam melakukan STI ini Khususnya HOLI
8. Untuk Shalsa yang selalu dengerin ocehan setiap malam juga
9. Seluruh pihak yang terlibat dalam kelancaran pembuatan makalah karya ilmiah ini yang belum disebutkan satu satu

Penulis menyadari bahwa masih banyak kekurangan dari laporan ini, baik dari materi maupun teknik penyajiannya. Oleh karena itu, kritik dan saran yang membangun penulis harapkan.

Jakarta, 18 Juli 2022

Rulli Azani Akbar

DAFTAR ISI

PERNYATAAN ORISINALITAS..... ii

PERNYATAAN PERSETUJUAN PUBLIKSASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS..... iii

LEMBAR PENGESAHAN iv

ABSTRAK v

ABSTRAK vi

KATA PENGANTAR..... vii

DAFTAR ISI..... viii

DAFTAR GAMBAR..... xii

DAFTAR TABEL xiv

DAFTAR SIMBOL..... xv

BAB I PENDAHULUAN..... 1

1.1 Latar Belakang Masalah.....**1**

1.2 Rumusan Masalah.....**3**

1.3 Tujuan Penelitian **3**

1.4 Manfaat Penelitian **4**

1.5 Ruang Lingkup.....**4**

1.6 Luaran Yang Diharapkan **5**

1.7 Sistematika Penulisan **5**

BAB II TINJAUAN PUSTAKA..... 7

2.1 Jaringan Komputer.....**7**

2.1.1 *Wireless*.....**8**

2.1.2 Mekanisme Jaringan *Wireless* 8

2.2 Keamanan Jaringan Komputer 9

2.2.1 Keamanan Komputer 10

2.3 Konsep Keamanan Jaringan 10

2.3.1 Ancaman 11

2.3.2 Kelemahan 11

2.4 *Penetration Testing* 12

2.5 *Wireless Area Network (Wlan) Penetration Testing* 12

2.5.1 *Cracking the encryption* 12

2.5.2 *ARP Spoofing* 13

2.5.3 *Sniffing* 13

2.5.3.1 Cara Kerja Packet Sniffing 13

2.5.4 *Bypassing MAC Address* 14

2.6 *Vulnerability Assessment* 14

2.7 *Penetration Testing Execution Standard* (PTES) 15

2.7.1 *Wireless Reconnaissance* 16

2.7.2 *Identify Wireless Networks* 16

2.7.3 *Vulnerability Research* 16

2.7.4 *Exploitation* 16

2.7.5 *Reporting* 16

2.7.6 *Remediation And Security Controls* 16

2.8 *Nessus* 16

2.9 *Ettercap* 17

2.10 *Nmap* 17

2.11 *Metasploit framework*.....17

2.12 Penelitian Terdahulu.....18

BAB III METODOLOGI 21

3.1 Tahapan Penelitian 21

3.2 Metode Penelitian.....21

3.2.1 Identifikasi Masalah 22

3.2.2 Perumusan Masalah 22

3.2.3 Studi Literatur.....22

3.3 Metode *Penetration Testing Execution Standard* (PTES).....22

3.4 Rencana Penelitian.....26

3.4.1 Layout Jaringan Komputer 26

3.4.2 Posisi Tempat Penyerangan.....26

3.4.3 Teknis Pengujian Keamanan.....27

3.5 Alat Bantu Penelitian.....28

3.6 Waktu Kegiatan.....29

BAB IV HASIL DAN PEMBAHASAN 30

4.1 *Wireless Reconnaissance* 30

4.2 *Identify Wireless Network*.....30

4.2.1 *Internal Footprinting*.....30

4.3 *Vulnerability Analysis*.....34

4.4 *Exploitation* 37

4.4.1 *Exploit*.....38

4.4.1.1 *SSL Certificate Cannot Be Trusted* 38

4.4.1.2 *DNS Server Cache Snooping Remote Information Disclosure* 40

4.4.2 *Scanning SSL*.....41

4.4.2.1 *TLS Version 1.1 Protocol Detection*.....41

4.4.3 *SSL/TLS Certificate Known Hard Coded Private Key*.....42

4.4.2.1 Implementasi Penyerangan.....43

4.5 *Reporting*.....64

4.6 *Remediation And Security Controls*.....65

4.6.1 Usulan Sistem.....66

4.6.2 Usulan Pembuatan Jaringan.....69

BAB V PENUTUP..... 71

5.1 Kesimpulan.....71

5.2 Saran.....72

DAFTAR PUSTAKA..... 73

RIWAYAT HIDUP..... 76

LAMPIRAN..... 77

DAFTAR GAMBAR

Gambar 2.1 *Flowchart tahapan penelitian (Purplesec, 2021)* 15
Gambar 3.1 Flowchart alur penelitian.....21
Gambar 3.2 *Layout* Jaringan 26
Gambar 3.3 Posisi tempat/ lokasi penyerangan 27
Gambar 4.1 mencari Ip addres 31
Gambar 4.2 Ping Target 31
Gambar 4.3 Scanning informasi.....32
Gambar 4.4 Jaringan Wlan0.....33
Gambar 4.5 Nessus :Scanning Port.....34
Gambar 4.6 Nessus: Scanning OS (Sistem Operasi) 34
Gambar 4.7 Tingkat Kerentanan Pada Nessus.....35
Gambar 4.8 Nessus Scanning Vulnerability 35
Gambar 4.9 Msfconsole 38
Gambar 4.10 Daftar Modul SSL cert 39
Gambar 4.11 Perintah auxiliary SSL cert 39
Gambar 4.12 Informasi Dari Cert 40
Gambar 4.13 Daftar Modul DNS.....41
Gambar 4.14 SSL Scanning 41
Gambar 4.15 SSL Scanning 42
Gambar 4.16 Pencarian Interface.....44
Gambar 4.17 Masuk Kedalam Monitor Mode 44
Gambar 4.18 Masuk Kedalam Monitor Mode 45
Gambar 4.19 Jaringan *wlan0* dalam mode monitor 45
Gambar 4.20 Perintah Aireplay-ng 46
Gambar 4. 21 WPA handshake 47
Gambar 4.22 Hasil dari *handshake* 47
Gambar 4.23 Pengecekan.....47
Gambar 4.24 Hasil Tidak Ditemukan 48
Gambar 4.25 Hasil dari percobaan kedua 49
Gambar 4.26 Proses Scanning Jaringan Wireless 50
Gambar 4.27 Melakukan ARP Spoofing 51

Gambar 4.28 Print Screen halaman pengguna *offline* 52
Gambar 4.29 Scanning Jaringan 53
Gambar 4.30 Down wlan0 53
Gambar 4.31 Tools Macchanger 54
Gambar 4.32 Perubahan MAC 54
Gambar 4.33 Mac *address* sebelum diubah 54
Gambar 4. 34 Mac Address setelah diubah 55
Gambar 4.35 Wi-Fi yang tetap Terhubung 55
Gambar 4.36 Tools Ettercap 56
Gambar 4.37 Tampilan Jaringan *Wlan0* 57
Gambar 4.38 Scanning host 57
Gambar 4. 39 Pemilihat Target 1 & 2 58
Gambar 4.40 Melakukan Serangan *Sniffing* 59
Gambar 4. 41 Serangan *Sniffing* 60
Gambar 4.42 Serangan *Sniffing* 60
Gambar 4.43 Tampilan *Keyloger* 61
Gambar 4.44 Tampilan Jaringan 62
Gambar 4.45 Setting Set host 62
Gambar 4.46 Proses Berjalan 63
Gambar 4.47 Korban telah *connected* 63
Gambar 4. 48 Hasil sniffing 63
Gambar 4.49 Usulan Jaringan Baru 69

DAFTAR TABEL

Tabel 2.1 Penelitian Terdahulu 18
Tabel 3.1 Pertanyaan Network penetration testing 23
Tabel 3.2 Pertanyaan Wireless Network Penetration Testing.....24
Tabel 3.3 Pertanyaan Admin Sistem.....24
Tabel 3.4 Pertanyaan Vulnerability Analysis.....25
Tabel 3.5 Jadwal Penelitian 29
Tabel 4.1 Tingkat Kerentanan Menurut Vulnerability.....35
Tabel 4.2 Jenis Kerentanan 36
Tabel 4.3 Jenis Serangan Yang Akan dilakukan.....42
Tabel 4.4 Reporting.....64