EVALUASI KEAMANAN WIRELESS LAN MENGGUNAKAN ISSAF (INFORMATION SYSTEM SECURITY ASSESSMENT FRAMEWORK)

Afrial Zein
Program Studi Sistem Informasi Universitas Pamulang
Jl. Raya Puspitek Serpong No. 10 Tangerang Selatan Banten
e-mail : zeinafrizal@gmail.com

Abstrak

Penelitian ini untuk mengetahui tingkat keamanan terhadap jaringan wireless yang diterapkan. Diperlukan pengujuan kemanan (pentesting) dengan memanfaatkan ISSAF (Information System Security Assessment Framework). ISSAF Framework merupakan metode untuk mengevaluasi keamanan pada sistem komputer atau jaringan dengan mensimulasikan serangan dari sumber yang berbahaya. Proses ini melibatkan analis aktif terhadap sistem untuk setiap kerentanan potensial yang diakibatkan oleh sistem yang lemah atau menggunakan konfigurasi sistem yang tidak benar maupun kelemahan operasional dalam proses teknis lainnya. Masalah kemaanan yang ditemukan akan disampaikan kepada pemilik sistem bersama dengan penilaian dampak dan mitigasi (solusi teknis) dari setiap kerentanan yang ditemukan.

Kata Kunci : Evaluasi Keamanan; ISSAF, Wireless, LAN

Abstract

The growth of COVID-19 cases continues to increase sharply. In fact, in recent days there has been an increase in cases almost doubled from the previous day. As of March 29, 2020, as stated by the Government spokesperson for handling COVID-19, Achmad Yurianto, has reached 1286 cases, 114 died, 64 recovered. The death rate is 114 cases, which is the highest mortality rate in Southeast Asia. This study tried to predict the spread of covid-19 using Richard's Curve model from early March to the end of June 2020. The results obtained from this study peaked the spread in early May and subsided at the end of June with the results of a prediction of 15 thousand infected people.

Keywords*: Security Evaluation; ISSAF, Wireless, LAN*

1. PENDAHULUAN

Di era teknologi digital, perkembangan teknologi jaringan wireless sangat berperan dalam menunjang kegiatan pada semua bidang pekerjaan baik dikantor-kantor maupun ditempat lainnya. Pada saat ini teknologi mengalami booming untuk digunakan sebagai akses jaringan dan internet hotspot.

Namun banyak sekali perusahaan, institusi dan perumahan melakukan implementasi jaringan wireless dengan tidak memperdulikan tingkat kemanannya, baik kerentanan potensial yang diakibatkan oleh sistem yang lemah atau konfigurasi sistem yang tidak sesuai atau kelemahan operasional dalam hal teknis. Selain itu, penyerangan jaringan wireless begitu sangat mudah dilakukan oleh banyak orang dikarenakan sifat jaringan wireless yang menggunakan teknologi gelombang radio dalam mengirimkan paket datanya sehingga sangat rentan sekali terhadap serangan-serangan.

Menurut Cintia Elindria (2007) Serangan yang biasa dilakukan terhadap jaringan wireless, diantaranya: MAC Spoofing, Client to client Hijacking,

DOI: https://doi.org/10.37277/stch.v32i2 (https://ejournal.istn.ac.id/index.php/sainstech/article/view/1294/858)

Attacking WEP, Attacking WPA, WPA Downgrade, Remote Resetter, Local Resetter, Bypass Radius Server, Roque AP, Evil Twin, Fake AP, Denial of Service, Kill Arround Traffic, Jamming, Share Port Attacking dan System Pwned.

Untuk mengetahui tingkat keamanan terhadap jaringan wireless yang diterapkan diperlukan pengujuan kemanan (pentesting) dengan memanfaatkan ISSAF (Information System Security Assessment Framework). ISSAF Framework merupakan metode untuk mengevaluasi keamanan pada sistem komputer atau jaringan dengan mensimulasikan serangan dari sumber yang berbahaya. Proses ini melibatkan analis aktif terhadap sistem untuk setiap kerentanan potensial yang diakibatkan oleh sistem yang lemah atau menggunakan konfigurasi sistem yang tidak benar maupun kelemahan operasional dalam proses teknis lainnya. Masalah kemaanan yang ditemukan akan disampaikan kepada pemilik sistem bersama dengan penilaian dampak dan mitigasi (solusi teknis) dari setiap kerentanan yang ditemukan.

Pada proses evaluasi kemaanan wireless LAN yang akan dilakukan menggunakan ISSAF (Information System Security Assessment Framework) untuk dapat mengetahui kerentanan yang ada sehingga bisa dilakukan proses mitigasi yang baik dan benar, sedangkan untuk proses monitoring keamananterhadap jaringan wireless diperlukan solusi teknis dengan mendirikan wireless IDS (Intrider Detection System). IDS sendiri merupakan aplikasi yang dapat mendeteksi aktivitas-aktivitas yang mencurigakan dalam sebuah jaringan komputer, sedangkan wireless IDS tentu saja berbasis wireless yang digunakan untuk memantau aktifitas yang mencurigakan pada jaringan wireless. Wireless IDS ini bekerja dengan melakukan kegiatan traffic sniffing pada gelombang radio untuk emmantau paket-paket data yang mencurigakan.

Hasil yang diharapkan dalam tesis ini antara lain menghasilkan model proses evaluasi keamanan wireless menggunakan ISSAF (Information System Security Assessment Framework), diantaranya: Planning, Assessment dan Reporting sehingga memberikan rasa aman dan nyaman bagi pengguna jaringan wireless dilingkungan institusi tersebut dikarenakan jaringan wirelessnya aman. (Dr. Raden Teduh Dirgahayu, 2016).

2. Tinjauan Pustaka

Teknologi bergerak (mobile) dan teknologi wireless (nirkabel) merupakan teknologi yang tergolong baru dan terus berkembang. Salah satu yang menjadi perhatian utama adalah masalah keamanannya. Karena jaringan wireless menggunakan sinyal radio yang lalu lalang pada atsmosfer sehingga rawan terhadap kegiatan penyadapan informasi pada jalur transmisi (eavesdropped) dan penghentian jalur transmisi (intercepted).

Dalam penilaian keamanan, ada beberapa standar dan pedoman pengujian yang secara terbuka bisa dipergunakan untuk umum dan tersedia di internet, diantaranya seperti: Open Source Security Test Methodology Manual (OSSTMM), Open Web Application Security Project (OWASP), Information System Security Assessment Framework (ISSAF) dan Payment Card Industry Data Security Standard (DSS). Security Assessment merupakan evaluasi mendalam tentang aplikasi web atau sistem yang berharga, yang menunjukan kelemahan serta menyediakan prosedur mitigasi yang tepat dan diperlukan untuk menghilangkan kelemahan-kelemahan atau mengurangi resiko. Dalam penilaian tersebut dijelaskan bahwa Penetration Testing Methodology terdiri dari 3 (tiga) fase yaitu: Data Gathering, Attacks dan Reporting.

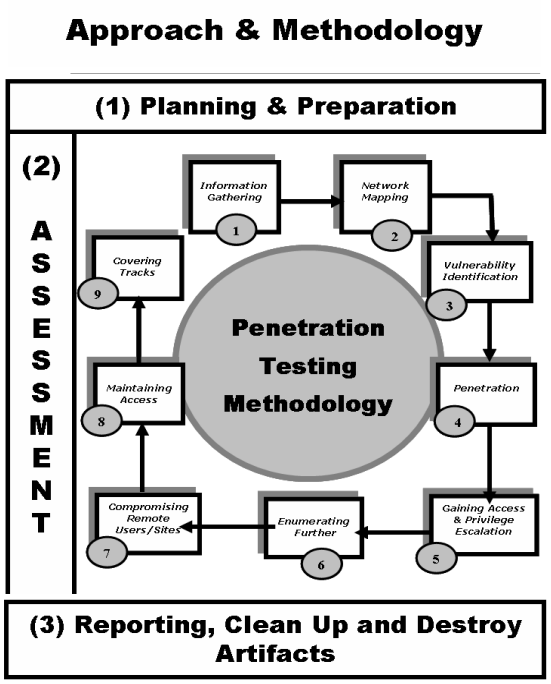
Information System Security Assessment Framework (ISSAF) merupakan hasil review terstruktur

DOI: https://doi.org/10.37277/stch.v32i2 (https://ejournal.istn.ac.id/index.php/sainstech/article/view/1294/858)

yang dikeluarkan oleh Open Information System Security Group yang telah mengkategorikan penilaian keamanan sistem informasi dalam beberapa domain. (Ho Kang 2008). Dari jurnal tersebut dijelaskan bahwa Information System Security Assessment Framework (ISSAF) digunakan untuk melakukan penilaian terhadap keamanan informasi denga kriteria evaluasi yang sangat rinci dan butuh pengujian khusus untuk masing-masing domain. ISSAF menjadi hal utama yang digunakan dalam memenuhi persyaratan penilaian keamanan.

3. Metodologi Penelitian

Information System Security Assessment Framework (ISSAF) memiliki penetration methodology yang digunakan untuk melakukan evaluasi terhadap keamanan jaringan komputer, sistem dan aplikasi kontrol.



Gambar 1. . Metodologi ISSAF

ISSAF terdiri dari 3 (tiga) pendekatan dan memiliki 9 (sembilan) langkah penilaian. Pendekatan ISSAF terdiri dari 3 (tiga) tahap, yaitu :

1. Planning dan Preparation

Tahap ini merupakan tahap awal untuk mendapatkan informasi awal, merencanakan dan mempersiapkan proses tes, pendekatan, metodologi dan persetujuan terhadap spesific test case dan escalation paths.

2. Assessment

Assessment merupakan tahap penetration test yang dilakukan dengan beberapa tahapan, diantaranya :

a. Information Gathering
   Mendapatkan informasi tentang target yang akan diaudit, baik itu informasi teknis maupun non teknis guna mengekplorasi beberapa kemungkinan terhadap pemahaman target dan sumber dayanya.
b. Network Mapping
   Menentukan topologi jaringan yang menjadi target, network device dan aplikasi yang digunakan dalam tahap ini untuk membantu penemuan teknis informasi tentang host dan jaringan yang terlibat diantaranya.

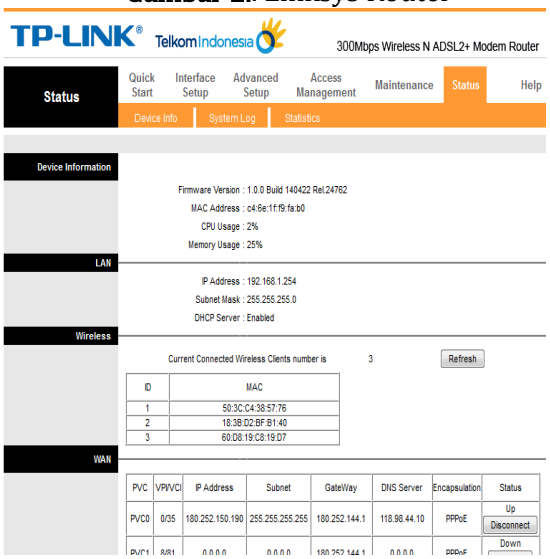
4. HASIL DAN PEMBAHASAN

4.1. Analisa Kebutuhan Data

Analisa kebutuhan data ini adalah analisa terhadap kebutuhan data yang akan digunakan dalam analisa keamanan wireless LAN. Data-data yang dibutuhkan antara lain:

a. Data Router, yaitu data spesifikasi yang dimiliki oleh router. Data yang berhubungan dengan spesifikasi router antara lain:
   1. Merk dan tipe router, yaitu merek dan tipe beserta series yang dikeluarkan oleh vendor yang digunakan.
   2. Versi hardware router, merupakan versi perkembangan hardware yang dikeluarkan oleh vendor tersebut.
   3. Versi Firmware router, merupakan versi software yang dimasukan kedalam flash memory router oleh vendor.

Gambar 2.. Linksys Router



Gambar 3. Versi Firmware Router

b. Data Wireless LAN, yaitu data yang didapatkan dengan cara melakukan kegiatan war driving dan scanning pada wireless LAN. Data yang berhubungan dengan wireless LAN yang dibutuhkan antara lain:
   1. SSID (Service Set Identifier), nama identitas dari wireless LAN yang dibuat oleh pemilik.
   2. Tx-Power, kekuatan sinyal yang dipancarkan dan terbaca oleh host.
   3. Beacons, frame terpendek yang dikirimkan oleh access point ke station untuk mengatur sinkronisasi komunikasi.
   4. Mac Address (BSSID), mac address yang dimiliki oleh access point.
   5. Data, besarnya paket data yang dimiliki oleh access point.
   6. Channel, jalur yang digunakan oleh access point.
   7. Encryption, jenis enkripsi yang digunakan oleh access point.
   8. Chiper & Authentication, algoritma enkripsi yang digunakan oleh akses point.
   9. Station, mac address milik host yang terkoneksi pada access point.

Selain itu data-data lainnya yang berhubungan dengan jaringan antara lain:

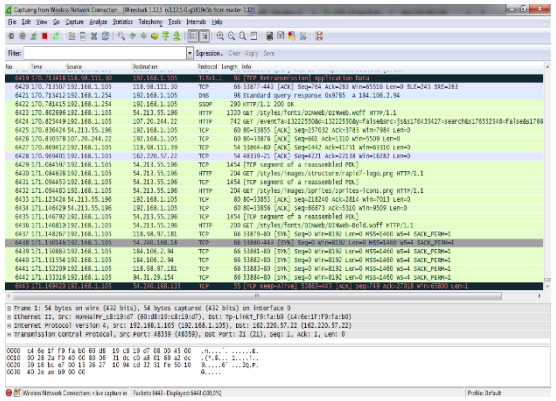
a. TCP/IP, yaitu IP address yang digunakan oleh router.
b. Port, nomor layanan yang digunakan oleh router.
c. State, status layanan yang sedang berlangsung (clored/open).
d. Service, layanan yang dijalankan oleh router.

DataWireless IP cammera, yaitu data yang didapat dengan cara melakukan kegiatan war driving pada wireless LAN dan scanning pada wireless IP camera. Data yang berhubungan dengan wireless IP camera yang dibutuhkan antara lain:

1. Merek, versi firmware dan tipe beserta kode series.
2. TCP/IP, alamat IP yang digunakan.
3. Port, nomor layanan yang diguanakan.
4. State, status layanan yang ada (open/closed).
5. Service, layanan yang dijalankan.

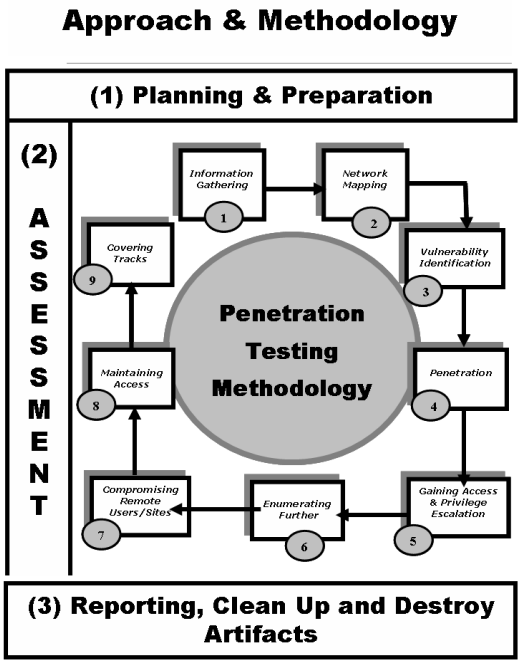
Paket Data dan Traffic Wireless LAN, yaitu besarnya paket data yang ada pada radio wireless access point serta paket data yang keluar masuk pada jaringan wireless. Data-data tersebut didapat dari proses monitoring terhadap wireless LAN.

DOI: https://doi.org/10.37277/stch.v32i2 (https://ejournal.istn.ac.id/index.php/sainstech/article/view/1294/858)



Gambar 4. Data Packet Monitoring

Data-data tersebut akan digunakan dalam analisis kegiatan pengujian keamanan wireless LAN, termasuk didalamnya pengujian router dan wireless IP camera Perancangan penelitian merupakan metode yang lebih menekankan kepada aspek pemahaman secara mendalam terhadap suatu masalah daripada melihat permasalahan untuk penelitian generalisasi. Perancangan penelitian dalam tesis ini menggunakan beberapa langkah sesuai dengan framework ISSAF yang dapat digambarkan pada diagram dibawah ini



Gambar 5. Assessment ISSAF

Seperti yang telah dijelaskan diatas, sebelumnya bahwa terdapat 3 langkah utama dalam ISSAF yang harus dilaksanakan yaitu:

1. Planning dan Preparation
2. Assessment, dan
3. Penyusunan hasil laporan

Untuk menggunakan data-data yang dibutuhkan dan perangkat keras serta perangkat lunak banyak dilakukan dalam tahap assessment yang dijelaskan sebagai berikut:

Information Gathering

Langkah awal dalam melakukan assessment adalah information gathering untuk mendapatkan informasi tentang target yang akan diaudit dalam komponen keamanan informasi. Untuk dapat melakukan information gathering diperlukan beberapa perangkat keras dan perangkat lunak serta hasilnya data yang akan diperoleh terdiri dari : SSID name, Channel, Encryption, tx-Power, Beacons, Size Of Data Packet, Chiper, Mac Address, Station Mac Address dan Kekuatan Sinyal. Untuk perangkat keras dan perangkat lunak yang digunakan adalah Wireless USB sesuai dengan gambar 3.6 dengan menggunakan antena yang sesuai dengan gambar 3.7 dan 3.8 serta menggunakan beberapa aplikasi, diantaranya Kismet, Airodump dan inSSIDer

Network Mapping

Menentukan gambaran topologi dari jaringan yang menjadi target, detwork device dan aplikasi yang digunakan untuk membantu penemuan teknis informasi tentang host dan jaringan yang terlibat. Pada tahap inipun masih menggunakan wireless usb sesuai dengan spesifikasi dan menggunakan aplikasi NMAP

Vulnerability Identication

Tujuan dari tahapan ini adalah untuk mengembangkan daftar rincian vulnerability (kelemahan, kekurangan dan kerentanan) sistem yang dapat dieksploitasi atau dimanfaatkan potensi threat-source. Pada proses ini dibutuhkan wireless usb, wireless toolbox dan aplikasi: NMAP, Router Auditing Tools dan beberapa tools exsploit script.

Attacking & Pentesting

Tujuan langkah ini adalah untuk melakukan penyerangan dan

memastikan kerentanan keamanan yang ada. Pada proses ini masih membutuhkan wireless usb sesuai dengan spesifikasi dan juga dibutuhkan aplikasi: NMAP, nbtscan, Wireshark, smbclient, aircrack, airodump, reaver, wifi jamming, wifite dan eksploit script.

Gaining Access

Kegiatan untuk mendapatkan hak istimewa root atau administrator. Pada proses ini masih tetap menggunakan wireless usb sesuai
spesifikasi, wireless toolbox dan dibutuhkan aplikasi: nmap, wireshark dan exploit script.

Enumeration Further

Proses penggabungan informasi yang telah didapat dari proses sebelumnya, sehingga menghasilkan exsploitasi yang dapat digunakan. Pada proses ini tetap menggunakan wireless usb dengan dukungan aplikasi: Whireshark, John The Ripper dan Metasploit

Maintaining Access

Tahapan untuk mempertahankan hak priviledge yang sudah didapatkan sebelumnya. Pada penelitian ini tidak digunakan karena sangat berbahaya bagi network.

Covering Track

Tahapan untuk melakukan aktifitas penghapusan activity log pada mesin target. Kegiatan ini bisa dilakukan jika mesin target bisa dikuasai secara penuh. Pada proses ini aplikasi yang digunakan adalah Metasploit

Setelah proses assessment dilakukan maka akan diadakan proses untuk menjaga tingkat keamanan yang lebih baik lagi dari Wireless LAN yang telah diaplikasikan, yaitu dengan cara:

1. Mitigation
   Proses mengurangi tingkat keretanan yang ada. Pada proses ini dibutuhkan aplikasi: FMK (Firmware Modification Kit, Binwalk dan MkSquashFS.
2. Monitoring
   Proses memantau serangan-serangan yang ditunjukan pada wireless LAN sehingga setiap bentuk serangan dapat diketahui dengan baik dan cepat. Pada tahap ini dibutuhkan aplikasi : wids.py dan waids.py.

5. KESIMPULAN

Dari penelitian yang telah dilakukan, dapat ditarik kesimpulan bahwa:

1. Menghasilkan model/teknik evaluasi terhadap wireless LAN dengan melakukan penetration testing terhadap mode (topologi) jaringan wireless.
2. Menghasilkan model proses assessment wireless LAN menggunakan ISSAF (Information System Security Assessment Framework), diantaranya: Planning, Assessment dan Reporting
3. Untuk melakukan perhitungan terhadap tingkat kerentanan keamanan yang ada pada wireless LAN dapat dilakukan dengan menggunakan CVSS (Common Vulnerability Scoring System).
4. Menghasilkan tingkat akurasi wireless IDS yang memungkinkan berbagai serangan dapat diketahui dengan cepat dan bisa diantisipasi sedini mungkin.

6. DAFTAR PUSTAKA

Sattarova Y Alisherov, A., Farkhod., Feruza, International Journal of of Grid and Distributed Computing, Methodology for Penetration Testing: Republic of Korea

Yuan, X, Bacudio, A.G.;.; Chu, B.T.B.; Jones, M., 10 Desember 2012, An Overview Of Penetration Testing, http://airccse.org/journal/nsa/1111nsa02.pdf

Chow, E., 1 Desember 2011, Ethical Hacking & Penetration Testing, http://uwcisa.uwaterloo.ca/Biblio2/Topic/ACC626%20Ethical%20Hacking%20and%20PenetrationTesting%20E%20Chow.pdf

Martinsons, M. G, Davison, R. M.,., Kock N., (2004), Journal : Information

Systems Journal : Principles of Canonical Action Research 14, 65–86

Whitaker, A.; Newman, D.P., 1 Desember 2012, Penetration Testing and Network Defense, http://www.ciscopress.com/store/penetration-testingand-network-defense-9781587052088

Afrizal Zein (2018),, *Pendeteksian Kantuk Secara Real Time Menggunakan Pustaka Opencv Dan Dlib Python,* Sainstech: Jurnal Penelitian dan Pengkajian Sains, 2018