 ISSN: 1411-3201

EVALUASI KEAMANAN WIRELESS LOCAL AREA NETWORK MENGGUNAKAN METODE PENETRATION TESTING (KASUS : UNIVERSITAS MUHAMMADIYAH MAGELANG)

Bambang Pujiarto[1)], Ema Utami[2)], Sudarmawan[3)]

[1)] Universitas Muhammadiyah Magelang
[2,3)] STMIK AMIKOM Yogyakarta
email: bpujiarto@ummgl.ac.id[1)], ema.u@amikom.ac.id[2)], sudarmawan@amikom.ac.id[3)]

Abstraksi

Wireless Local Area Network (WLAN) merupakan jaringan yang banyak digunakan pada beberapa institusi untuk menyediakan akses informasi secara bersama. Keamanan jaringan wireless menjadi perhatian utama bagi pengelola jaringan untuk menjaga kualitas sistem jaringan. Untuk melihat kualitas keamanan jaringan maka perlu dilakukan evaluasi terhadap sistem keamanan yang ada dalam jaringan tersebut. Salah satu metode yang dapat digunakan untuk mengevaluasi adalah dengan penetration testing terhadap jaringan tersebut. Penetration testing adalah tindakan pengujian sistem dengan cara mensimulasikan bentuk-bentuk serangan terhadap sistem tersebut sehingga akan diketahui tingkat kerentanannya. Pengujian dengan metode ini tentunya akan beresiko yang dapat mempengaruhi sistem. Serangan yang dilakukan terhadap sistem dapat merugikan pihak target pengujian dan bagi pelaku tentunya merupakan sebuah tindakan pelanggaran apabila tidak adanya kesepakatan atas tindakan yang akan dilakukan dan konsekuensi terhadap akibat dari tindakan tersebut. Oleh sebab itu untuk menerapkan pada institusi perlu adanya perencanaan dan persiapan yang baik agar tidak merugikan masing-masing pihak. Penelitian ini menggunakan kasus di Universitas Muhammadiyah Magelang sebagai institusi yang dijadikan objek untuk menerapkan model evaluasi keamanan WLAN dengan penetration testing.

Kata kunci:
Wireless Local Area Network, keamanan jaringan, penetration testing

Pendahuluan

Perkembangan teknologi jaringan komputer semakin memudahkan masyarakat dalam memenuhi kebutuhan informasi. Salah satu teknologi yang dikembangkan adalah teknologi media transmisi nirkabel atau wireless. Media transmisi nirkabel atau wireless yang digunakan untuk LAN (Lokal Area Network) banyak dijumpai diberbagai tempat umum yang menyediakan akses informasi. Saat ini layanan akses informasi semakin dipermudah dengan banyaknya produk-produk alat komunikasi yang menyediakan fitur Wi-Fi. Infrastruktur jaringan wireless untuk kebutuhan LAN atau biasa disebut dengan WLAN (Wireless LAN) sudah distandarkan dengan nama IEEE 802.11.

Mudahnya pengguna umum terhubung dengan jaringan WLAN tentunya masalah keamanan perlu diperhatikan, apalagi didalam sebuah korporasi atau sebuah lembaga yang peduli dengan keamanan data. Jaringan wireless menggunakan gelombang radio sebagai media transmisi sehingga jaringan akan lebih mudah dimasuki oleh penyusup dan serangan yang berasal dari semua arah [7]. Pada jaringan yang diakses secara bersama seperti jaringan hotspot memiliki kerentanan terhadap serangan atau gangguan terhadap sistem sehingga perlu dilakukan aturan terhadap sistem jaringan. Beberapa aturan diberlakukan untuk mengontrol kinerja maupun kondisi jaringan sehingga sistem berjalan sesuai dengan yang diharapkan. Untuk melihat kualitas keamanan jaringan maka perlu dilakukan evaluasi terhadap sistem keamanan yang ada dalam jaringan tersebut.

Salah satu metode yang dapat digunakan dalam mengevaluasi jaringan adalah dengan cara melakukan pengujian terhadap sistem dengan mensimulasikan bentuk-bentuk serangan terhadap jaringan atau biasa yang dikenal dengan Penetration Testing. Teori tentang penetration testing sudah lama dikembangkan oleh beberapa peneliti dalam bidang keamanan sistem informasi dan jaringan komputer.\

Tindakan penetrasi sebenarnya tindakan yang bersifat membahayakan bagi sistem. Penetration tester adalah ethical hacker yang dipekerjakan untuk melakuakan percobaan yang membahayakan terhadap jaringan komputer di perusahaan dengan tujuan untuk menilai keamanan data [8]. Apabila kegiatan ini dilakukan pada perusahaan atau sebuah institusi dengan mempertimbangkan resiko dari tindakan *penetration testing* maka perlu adanya perencanaan yang baik untuk meberikan jaminan terhadap pihak target maupun pelaku penetrasi. Jaminan ini berkaitan dengan hukum yang berlaku di negara tentang penggunaan teknologi informasi.

Tujuan penelitian ini adalah mengetahui tingkat kerentanan *WLAN* menggunakan metode *penetration*

 ISSN: 1411-3201

testing dan membuat perencanaan, penilaian dan laporan evaluasi keamanan jaringan yang dapat dijadikan pedoman untuk melakukan *penetration testing* pada institusi.

Penelitian ini akan mengacu pada beberapa penelitian yang pernah dilakukan berkaitan dengan keamanan jaringan wireless dan metode Penetration Test, antara lain:

a. Emily Chow (2011) dalam judul "*Ethical Hacking & Penetration Testing*", menyimpulkan bahwa *ethical hacking* dan *penetration testing* dianggap sebagai cara yang efisien dan efektif dalam mengatasi celah keamanan dan kelemahannya sebelum adanya tindakan eksploitasi dari *hacker* jahat [3].
b. Aileen G. Bacudio (2011) dalam judul "*An Overview Of Penetration Testing*", melakukan pengujian terhadap aplikasi web dengan metode *penetration testing* dan menyimpulkan tentang metode *penetration testing* merupakan metode yang komprehensif untuk mengidentifikasi kerentanan sistem [2].
c. Farkhod Alisherov A dan Feruza Sattarova Y (2009) dalam judul "Methodology for Penetration Testing" menyimpulkan bahwa metodologi dibutuhkan untuk pengujian yang efektif dan menyarankan untuk membuat kebijakan antara pihak perusahaan dan pelaku penguji [1].
d. Byeong-Ho Kang (2008) dalam penelitian yang berjudul "*About Effective Penetration Testing Methodology*" menyimpulkan dalam melakukan penetration testing dibutuhkan sebuah metodologi formal untuk mencapai keberhasilan [5].

Salah satu framework yang dapat digunakan untuk melakukan penetration testing adalah ISSAF (Information System Security Assessment Framework). Framework ini dikembangkan oleh OISSG (Open Information System Security Group). Metode ISSAF Penetration Testing dirancang dalam melakukan evaluasi menggunakan pendekatan tiga fase yaitu [6]:

a. *Phase – I: Planning and Preparation*

Tahap ini merupakan tahap pengenalan dan penyesuaian antara pelaku penetrasi dan pihak yang akan dijadikan objek dengan saling bertukar informasi. Kesepakatan kedua pihak sangat dibutuhkan untuk perlindungan hukum bersama. Tahap ini juga menentukan tim yang terlibat dalam pengujian, rencana waktu yang tepat dan aturan lainnya.

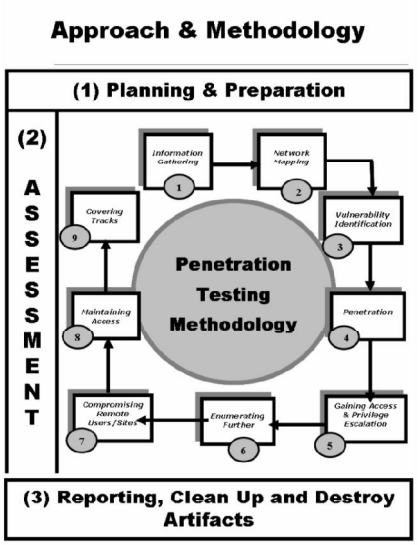
b. *Phase – II: Assessment*

Tahap ini merupakan tahap dilakukan penetration testing yang terdiri dari beberapa pendekatan berlapis. Layer-layer disini adalah sebagai berikut :

1) *Information Gathering*
2) *Network Mapping*
3) *Vulnerability Identification*
4) *Penetration*
5) *Gaining Access & Privilege Escalation*
6) *Enumerating Further*
7) *Compromise Remote Users/Sites*
8) *Maintaining Access*
9) *Covering Tracks*

c. *Phase – III: Reporting, Clean-up and Destroy Artefacts*

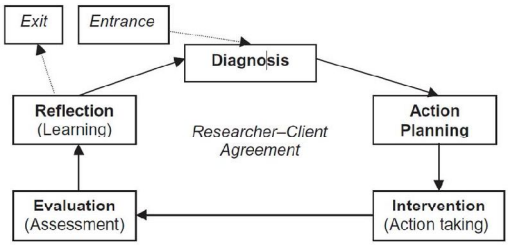
Tahap akhir dari pengujian dengan membuat beberapa laporan hasil penemuan selama melakukan *penetration testing.* Setelah melakukan tindakan perlu menghapus log yang bisa membahayakan sistem yang dapat dimanfaatkan orang lain.



Gambar 1. Pendekatan dan Metodologi ISSAF Penetration Testing [6]

Metode Penelitian

Penelitian ini menggunakan pendekatan *action research* model yang membagi beberapa tahap yaitu *diagnosing, action planning, intervention, evaluation,* dan *reflection* [4].



Gambar 2. Action Research Prosess Model[4]

Siklus *action research* diatas merupakan gambaran proses penelitian kemudian untuk proses evaluasi keamanan WLAN dengan menerapkan metode *ISSAF Penetration Testing.*

a. Diagnosis

Tahap awal dilakukan dengan melakukan identifikasi permasalahan yang ada berkaitan dengan

 ISSN: 1411-3201

sistem jaringan *WLAN* melalui wawancara dengan pihak pengelola.

b. Action Planning

Tahap selanjutnya dilakukan perencanaan dan persiapan yang dibutuhkan dalam penelitian. Permasalahan yang akan diangkat adalah evaluasi terhadap jaringan WLAN dengan menggunakan metode *Penetration Testing*. Tahap ini menggunakan *planning and preparation phase* didalam *ISSAF* yang mencakup kegiatan sebagai berikut:

1) Mengidentifikasi pelaku penetrasi beserta orang dari pihak lembaga yang bertanggung jawab terhadap sistem jaringan.
2) Konfirmasi dengan pihak manajemen berkaitan dengan ruang lingkup pengujian serta pendekatan dan metodologi pengujian yang akan digunakan.
3) Membuat semacam perjanjian dan kesepakatan secara formal yang dapat memberi jaminan hukum terhadap pelaku penetrasi dan pihak institusi yang dijadikan target penetrasi.

c. Intervention

Setelah perencanaan dibuat selanjutnya melakukan tindakan dengan mengimplementasikan pada objek penelitian. Tahap ini merupakan tahap *assessment* didalam *ISSAF* dimana metode yang digunakan adalah sebagai berikut :

1. Information gathering

Tahap ini dimulai dengan pengumpulan data dengan cara melakukan *scanning* terhadap jaringan.

2. Analysis and research

Data yang diperoleh dari tahap selanjutnya kemudian dilakukan analisis. Kegiatan ini meliputi :

a) Identifikasi jaringan wireless.
b) Mempelajari karakteristik *access point* yang digunakan.
c) Menentukan jenis serangan untuk jaringan *wireless*.

3. Exploit and attack

Tahap ini menentukan *tools* yang akan digunakan dilanjutkan dengan kegiatan eksploitasi dan serangan terhadap jaringan.

d. Evaluation

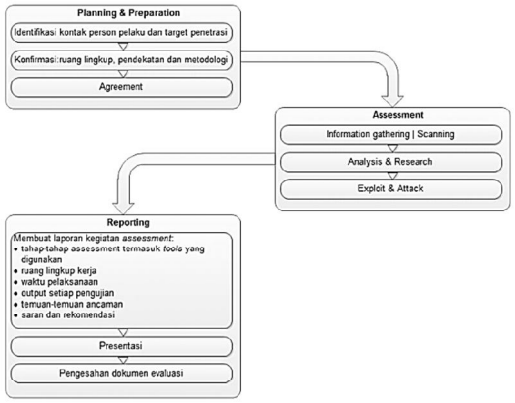
Setelah dilakukan tindakan selanjutnya dilakukan evaluasi terhadap hasil dari masing-masing tindakan pengujian dengan melibatkan pihak pengelola jaringan untuk mendiskusikan hal yang berkaitan dengan pengaturan keamanan WLAN.

e. Reflection

Tahap ini merupakan akhir dari rangkaian siklus dan metode yang digunakan adalah *reporting phase* pada *ISSAF*. Pihak pelaku evaluasi membuat laporan dari hasil yang sudah didapat pada fase sebelumnya sebagai bentuk pertanggung jawaban terhadap kegiatan yang dilakukan oleh pelaku pengujian sistem jaringan kepada pihak institusi. Kegiatan pada tahap ini adalah sebagai berikut:

1. Menyusun laporan kegiatan *assessment* yang meliputi:
   a) tahap-tahap *assessment* termasuk *tools* yang digunakan
   b) ruang lingkup kerja
   c) waktu pelaksanaan
   d) output setiap pengujian
   e) temuan-temuan ancaman
   f) saran dan rekomendasi
2. Mempresentasikan hasil pengujian kepada pihak manajemen.
3. Mengesahkan dokumen evaluasi dan menyerahkan kepada pihak manajemen

Proses keseluruhan sistem evaluasi dibagi menjadi 3 bagian fase utama yaitu *planning and preparation*, *assessmet, dan reporting*. Gambaran proses seperti pada gambar 3.



Gambar 3. Proses Evaluasi

Hasil Penelitian dan Pembahasan

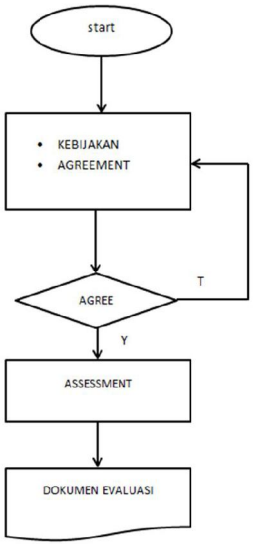
Penelitian ini menggunakan metodologi *ISSAF* sebagai framework evaluasi sistem keamanan dengan metode penetration testing. Proses evaluasi dibagi menjadi tiga fase yaitu *planning and preparation*, *assessment*, dan *reporting*. Hasil penelitian ini secara garis besar ditunjukkan pada tabel 3.

Tabel 1. Hasil Penelitian

No.	Proses	Hasil
1	*Planning and Preparation*	- Kebijakan - *Agreement*
2	*Assessment*	Dokumen assessment
3	*Reporting*	Dokumen Evaluasi

Masing-masing proses dan keluaran saling menentukan dan mempengerahui proses lainnya sehingga sebuah metodologi yang dibangun merupakan sebuah kesatuan yang tidak terpisahkan di dalam penelitian ini. Hubungan proses penelitian dan keluaran dapat dijelaskan pada gambar 4.

 ISSN: 1411-3201



Gambar 4. Hubungan keluaran setiap fase

Penilaian keamanan jaringan WLAN dilakukan berdasarkan tingkat kerentanan dengan menggunakan nilai seperti yang ditentukan dalam ISSAF. Parameter yang digunakan dalam memberikan nilai tingkat kerentanan dijelaskan dalam tabel 2.

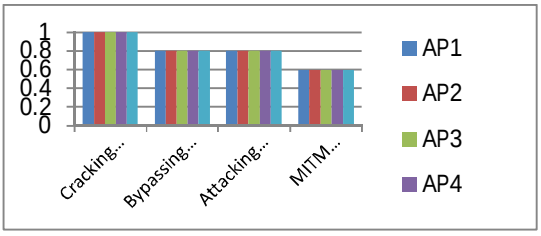
Tabel 2. Nilai tingkat kerentanan [6]

Vulnerability Level	Assigned Value
Extremely Vulnerable	1
Highly Vulnerable	0.8
Average	0.6
Low	0.4
Extremely Low	0.2

Hasil yang didapat dari pengujian jaringan WLAN di Universitas Muhammadiyah Magelang dapat disajikan dalam tabel 3. dan gambar 5.

Tabel 3. Hasil Pengujian jaringan WLAN

Jenis Tindakan	AP1	AP2	AP3	AP4	AP Omni
Cracking the encryption	1	1	1	1	1
Bypassing WLAN Authentication	0.8	0.8	0.8	0.8	0.8
Attacking the Infrastructure	0.8	0.8	0.8	0.8	0.8
MITM Attack	0.6	0.6	0.6	0.6	0.6



Gambar 5. Grafik Kerentanan Jaringan WLAN

Hasil keseluruhan yang didapat dari empat jenis pengujian menunjukkan rata-rata tingkat kerentanannya adalah 0.8 dengan kata lain secara keseluruhan jaringan *WLAN* di Universitas Muhammadiyah Magelang memiliki tingkat kerentanan (*vulnerability*) tinggi.

Hasil pengujian jaringan *WLAN* didapat dari proses *assessment* namun untuk melakukan proses tersebut harus di dahului proses-proses sebelumnya yang dalam penelitian ini dimasukkan dalam fase *planning and preparation*. Tanpa adanya kesepakatan antara pihak pelaku dan pihak lembaga institusi maka tindakan *penetration testing* seharusnya tidak boleh dilakukan karena tidak memiliki jaminan hukum dari masing-masing pihak.

Dokumen evaluasi yang dihasilkan didapatkan dari dua fase sebelumnya yaitu *planning and preparation* dan *assessment*. Isi dari dokumen terdiri dari data-data kegiatan evaluasi dari tahap awal hingga akhir. Adanya dokumen evaluasi bagi lembaga sangat membutuhkan khususnya bagi pihak pengelola jaringan *WLAN*. Selain data administrasi isi dari dokumen merupakan gambaran yang jelas tentang kerentanan keamanan jaringan *WLAN* yang dimiliki Universitas Muhammadiyah Magelang sehingga pengelola diharapkan dapat mengambil kebijakan untuk meningkatkan sistem keamanan yang lebih baik.

Metodologi yang meliputi fase *planning and preparation*, *assessment* dan *reporting* dapat dijadikan pedoman untuk melakukan *penetration testing* pada institusi. Keluaran dari tiap fase adalah sebagai berikut:

a. *Planning and preparation*, mengahasilkan dokumen kebijakan dan *agreement*.
b. *Assessment*, menghasilkan dokumen *assessment*
c. *Reporting*, menghasilkan dokumen evaluasi

Keluaran yang dihasilkan tiap fase menentukan fase berikutnya sehingga ketiga fase tersebut merupakan satu rangkaian proses yang tidak dapat dipisahkan.

Daftar Pustaka

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

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

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

[4] Davison, R. M., Martinsons, M. G., Kock N., (2004), Journal : Information Systems Journal : Principles of Canonical Action Research 14, 65–86

 ISSN: 1411-3201

[5] Kang, B.; 27 November 2012, About Effective Penetration Testing Methodology, http://www.sersc.org/journals/JSE/vol5_no5_2008/8.pdf
[6] Rathore, B.; Herrera, O.; Raman, S.; Brunner, M.; Brunati, P.; Chavan, U.; Dilaj, M.; Subramaniam, R.K., 7 Oktober 2012, Information Systems Security Assessment Framework (ISSAF) draft 0.2.1A, http://www.oissg.org/files/issaf0.2.1A.pdf
[7] Thomas, T., 2005, Network Security First-Step, Ed. I., ANDI, Yogyakarta
[8] Whitaker, A.; Newman, D.P., 1 Desember 2012, Penetration Testing and Network Defense, http://www.ciscopress.com/store/penetration-testing-and-network-defense-9781587052088