ISSN: 2087-1716
Jurnal Ilmiah ILKOM Volume 8 Nomor 3 (Desember 2016)

DETEKSI PINEAP PADA FIRMWARE WIFI *PINEAPPLE* MENGGUNAKAN SMARTPHONE BERBASIS ANDROID

Fahmi Romisa[1], Bambang Sugiantoro[2]
[1]romy.rockwell@gmail.com, [2]bambang.sugiantoro@uin-suka.ac.id
[1]Magister Teknik Informatika Universitas Islam Indonesia, [2]Teknik Informatika UIN Sunan Kalijaga Yogyakarta

Abstrak

Kebutuhan akan akses jaringan nirkabel atau *wireless* saat ini sangat dibutuhkan oleh hampir semua orang, hampir di semua tempat terdapat akses jaringan *wifi*. Sebuah ilmu penetrasi jaringan semakin lama selama meningkat, tidak hanya menggunakan suatu penetrasi yang menggunakan perangkat lunak, tetapi sudah merambah ke perangkat keras yang sudah berubah fungsi, tidak lagi berfungsi sebagai menyebar sebuah koneksi data, tetapi sudah merambah sebagai alat penetrasi jaringan, sistem ini berguna untuk mendeteksi adanya sebuah *router* yang dapat menduplikasi semua *router* sekitar dengan permintaan *probe request*, maka dari itu diperlukan suatu alat pendeteksian yang dapat mendeteksi secara *real time* terhadap *router* tersebut . Penelitian ini menghasilkan suatu alat pendeteksian yang *user friendly* menggunakan *smartphone* berbasis *android*, beserta analisis dan melakukan suatu uji beda pada *router* yang memiliki *firmware wifi pineapple* yang memiliki *core pineap.*

Kata kunci: Deteksi, Jaringan nirkabel, Wifi *Pineapple*, Pineap.

1. Pendahuluan

Menurut sebuah survey yang berasal dari laporan Fortinet, yang menyebutkan bahwa jaringan nirkabel merupakan infrastruktur IT yang paling rentan terhadap berbagai serangan, disusul dengan endpoint, core network, database, aplikasi, email, dan media penyimpanan[1]. Perkembangan openwr*t* tanpa henti berdampak pada evolusi penggunaan router. Router tidak lagi hanya untuk menyebar sebuah koneksi data, tetapi sudah merambah ke berbagai fungsi diluar fungsi tersebut. Beberapa darinya digunakan untuk melakukan penetrasi terhadap suatu jaringan. Kebanyakan dari orang awam dalam membangun suatu jaringan tidak memperhatikan sisi keamanannya, terutama dalam membangun suatu jaringan nirkabel atau wireless.

Saat ini sistem untuk mendeteksi adanya *pineap atau rogue access point* pada router sangat minim, sebagai contoh pendeteksian yang dibuat oleh Neha Agrawal, & Shashikala Tapaswi, yang menggunakan pendekatan hybrid dan sistem deteksi anomaly, pendeteksian tersebut tidak memiliki user interface yang mudah digunakan, sistem tersebut hanya mendeteksi kegiatan yang mencurigakan melalui lalu lintas pada suatu jaringan[2]. Sistem pendeteksian lainnya dibuat oleh Asaf Tzur dkk, dengan melakukan eliminasi, untuk tujuan keamanan pada sebuah organisasi, dengan menggunakan metode autonomous Direction Finding (DF), yaitu, suatu alat yang dapat mengidentifikasi Angle of Arrival (AoA), dalam menerima sinyal wifi, menggunakan standar komunikasi jaringan nirkabel, seperti Wi-Fi (IEEE 802.11n).

Kontribusi utama dalam penelitian teresbut yaitu melakukan pendekatan dari beberapa antena penerima, dengan OFDM Channel State Information (CSI) sebagai dasar untuk menerapkan alat interferometry DF. Pendekatan ini secara teoristis diselidiki melalui analisis numerik, dan validasi oleh alat *prototype* [3]. Sistem yang ditawarkan saat ini belum adanya suatu sistem deteksi yang *user friendly* terhadap pengguna, seperti menggunakan suatu metode pendekatan, tidak mendeteksi secara *real time* yang berisi informasi pendukung, dan secara *manual* melalui proses yang cukup rumit. Hasil akhir dari penelitian ini berupa solusi terbaik dan penting untuk mendeteksi adanya pineapp atau *fake probe request* yang berada disekitar, yaitu dengan menggunakan smartphone berbasis android, yang dapat mendeteksi secara real time. Beserta analisis jaringan pada router tersebut, lalu mengumpulan data eksperimen pada penyebaran *beacon frame* dengan uji t.

2. Landasan Teori

2.1 *Cybercrime*

Cybercrime didefinisikan sebagai kejahatan di mana komputer adalah objek kejahatan tersebut dengan menggunakan teknik seperti *hacking*, *phishing*, *spam*, dan sebagainya. Pelaku *cybercrime* dapat menggunakan teknologi komputer untuk mengakses informasi pribadi, rahasia dagang bisnis, atau menggunakan internet yang bertujuan untuk eksploitatif. Penjahat juga dapat menggunakan komputer sebagai alat bantu penyadapan alat komunikasi dan dokumen atau penyimpanan suatu data. Penjahat yang melakukan kegiatan ilegal seperti ini sering disebut sebagai hacker. *Cybercrime* juga dapat disebut sebagai kejahatan komputer.

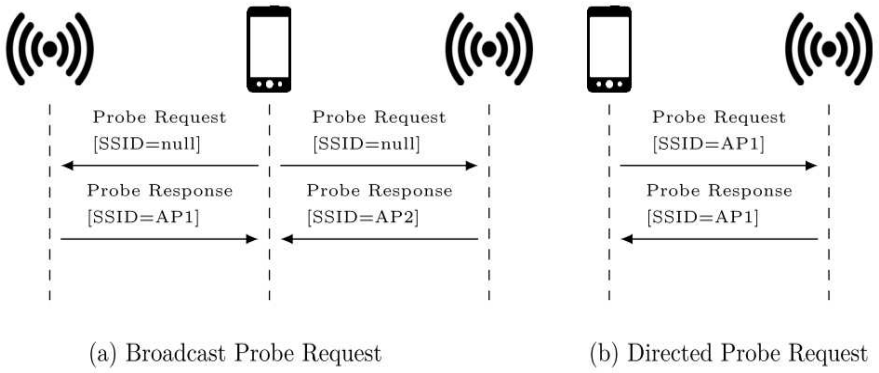
Cybercrime dapat diklasifikasikan menjadi 3 kategori yaitu [3]:

1. Terhadap individu
   Ini adalah kejahatan atau tindakan yang berkomitmen terhadap seseorang. Kejahatan-kejahatan ini termasuk pelecehan melalui e-mail, cyber stalking, penyebaran materi cabul di internet atau intranet, pencemaran nama baik, hacker/cracking, dll. di samping itu, ini termasuk kejahatan terhadap kekayaan dari seorang individu, vandalisme komputer, dan transmisi virus. Penyusupan Internet dan pengendalian yang tidak sah atas sistem komputer.
2. Terhadap organisasi
   kejahatan yang memiliki komitmen terhadap organisasi termasuk departemen pemerintah, perusahaan swasta, perusahaan, kelompok individu. Distribusi perangkat lunak bajakan juga bisa dimasukkan dalam kategori ini sebagai kejahatan cyber.
3. Terhadap masyarakat luas
   Ini adalah tindak kejahatan yang berdampak bahwa masyarakat luas pada umumnya. Contohnya pornografi merupakan contoh khas dari kejahatan tersebut**.**

2.2 *Probe request*

Probe request merupakan suatu respon yang dikirimkan yang dapat memeriksa apakah ada suatu jaringan wireless yang tersedia atau tidak, ada dua mode yaitu *directed* dan *broadcast.* Mode directed meminta suatu jaringan yang tersedia yang tersedia, yang telah digunakan sebelumnya, dan beberapa permintaan untuk pemeriksaan beberapa jaringan yang ada. Mode broadcast yaitu hanya satu permintaan yang dikirim pada setiap jaringan yang ada, dan diharapkan dapat merespon.

Komparasi pada mode tersebut, mode directed yang lebih rentan terhadap serangan, karena beberapa SSID dapat menghubungkan seseorang dari lokasi yang berbeda. Gambar 1 menunjukan perbedaan tersebut [4].



Gambar 1. Perbedaan broadcast *probe request* dan directed *probe request*

2.3 PineAP

PineAp merupakan *module* pada wifi *pineapple* yang dapat mengomatisasi serangan MITM terhadap klien. Perangkat nirkabel mengirimkan permintaan *probe request* dari *Preferred Network List* pada perangkat nirkabel ke area sekitar, perangkat android mengirimkan permintaan tersebut secara terus menerus. Misalnya apakah ada jaringan rumah disini?, apakah ada jaringan kerja disini ?. perangkat akan terus melakukan pengiriman permintaan *probe request* dari *Preferred Network List* pada setiap perangkat, ketika perangkat nirkabel mengkonfirmasi adanya jaringan yang tersimpan di PNL maka akan secara otomatis akan terhubung[5].

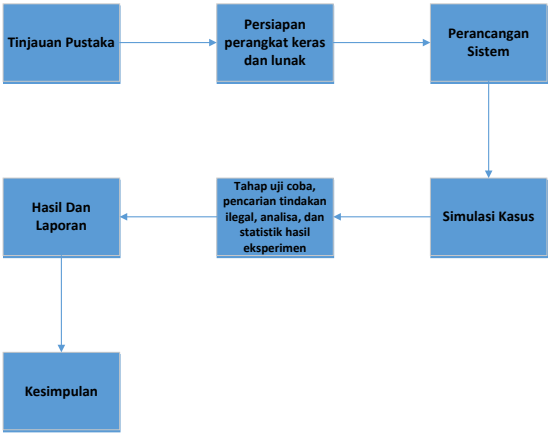
PineAP terdiri dari sejumlah komponen:

1. PineAP merupakan salah satu rangkaian alat

2. Dogma yang berfungsi untuk mengirimkan beacon kedalam daftar SSID perangkat device sekitar.
3. Beacon merespon untuk mengikuti semua *probe request* dengan sejumlah beacon yang menanggapi permintaan client.
4. Harvester mengumpulkan semua SSID yang dapat digunakan untuk Dogma.

3. Metode

Penelitian ini menggunakan beberapa tahapan metode, yang dapat dilihat pada gambar 2 dibawah ini.



Gambar 2. Metodologi Penelitian

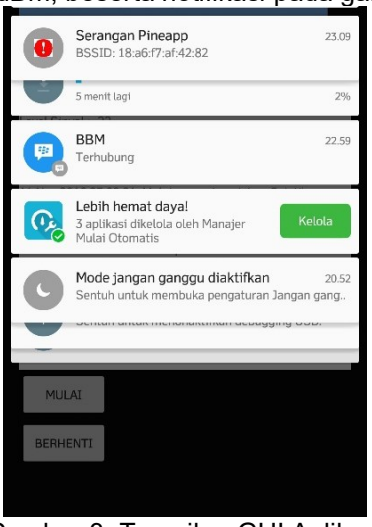
Menunjukan penelitian ini menggunakan 7 tahapan metodologi penelitian yaitu.

1. Literature Review
2. Preparation : Hardware and Software
3. System Planning
4. Simulation Case
5. The test phase, the search for illegal actions, analysis, statistics and experimental results
6. Results and Reports
7. Conclusion

4. Hasil

4.1 Deteksi

Fungsi mulai file berfungsi untuk melakukan suatu perintah *scanning* pada jaringan sekitar berbasis *wireless*, apakah kemungkinan adanya *rogue access point,* dengan pemberitahuan berupa notifikasi. dan berhenti adalah suatu perintah yang berfungsi untuk menghentikan semua proses scanning pada jaringan wireless sekitar, dalam menu tersebut terdapat frekuensi pencarian yang dapat di ubah nilainya dalam satuan detik, beserta time stamp kapan sistem tersebut dimulai, dan list hasil BSSID beserta level sinyal dalam dBm, beserta notifikasi pada gambar 3.

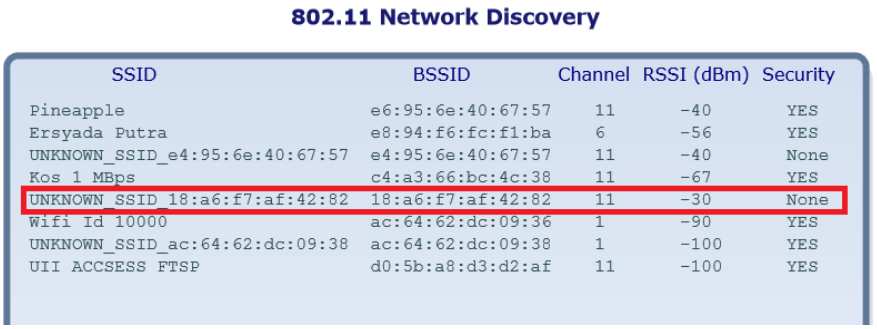


Gambar 3. Tampilan GUI Aplikasi

Sistem tersebut menampilan pemberitahuan berupa notifikasi yang berisi informasi, berupa mac address atau BSSID pada router yang berusaha melakukan serangan terhadap jaringan wireless di sekitarnya. BSSID pada router tersebut 18:a6:f7:af:42:82.

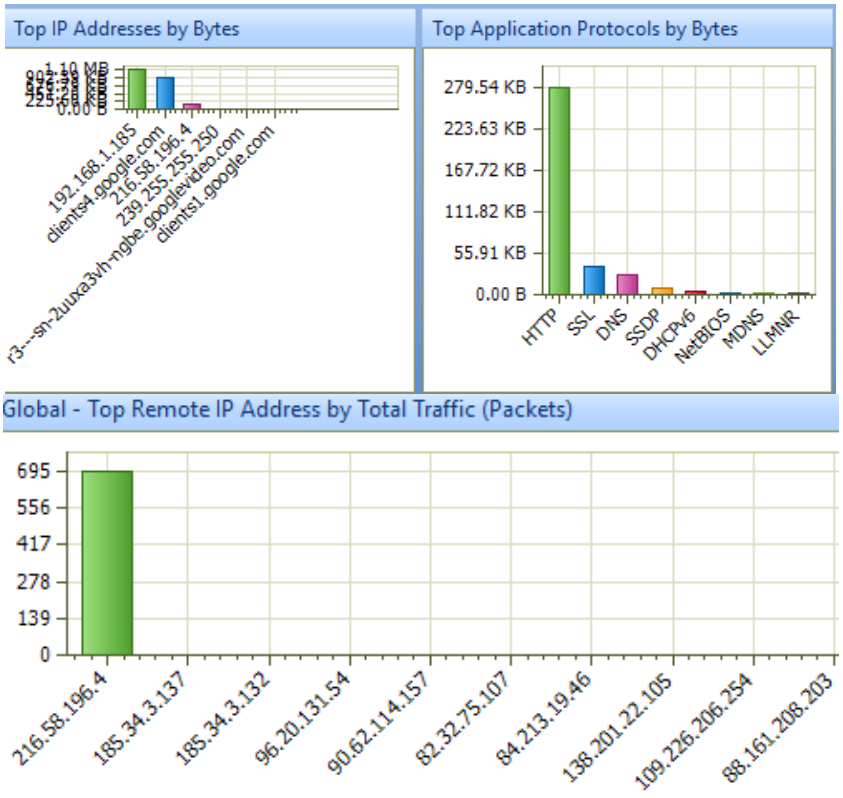
4.2 Analisis

Pencarian tindakan illegal dimulai dengan menggunakan tool aplikasi Net Surveyor, yaitu dengan mengetahui secara spesifik informasi berupa SSID, BSSID, Channel, Beacon, kualitas sinyal dan enkripsi. Karena informasi yang didapat sebelumnya yaitu berupa BSSID, dan BSSID tidak mungkin di duplikasi oleh seseorang, terkecuali duplikasi pada SSID pada sebuah router, maka dari itu informasi BSSID merupakan hal yang valid dalam membedakan sebuah router.Pada hasil pendeteksian sebelumnya diketahui bahwa BSSID yang dicurigai sebagai rogue access point atau yang dapat menduplikasi semua access point disekitarnya adalah 18:a6:f7:af:42:82 .

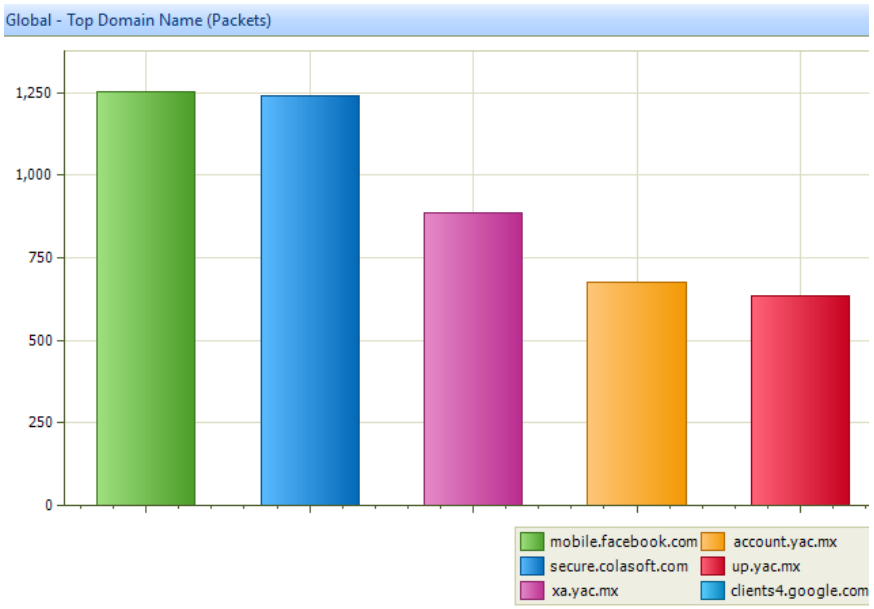


Gambar 4. List SSID

Pada gambar 5 terlihat pada *top remote IP address by total traffic* (*packets*), IP address 216.58.196.4 merupakan IP address yang selalu melakukan *conversation* terhadap pengguna yaitu IP Address pengguna adalah 192.168.1.185. dan pada gambar 6 domain yang paling tinggi melakukan conversation adalah mobile.facebook.com.



Gambar 5. Trafik Jaringan

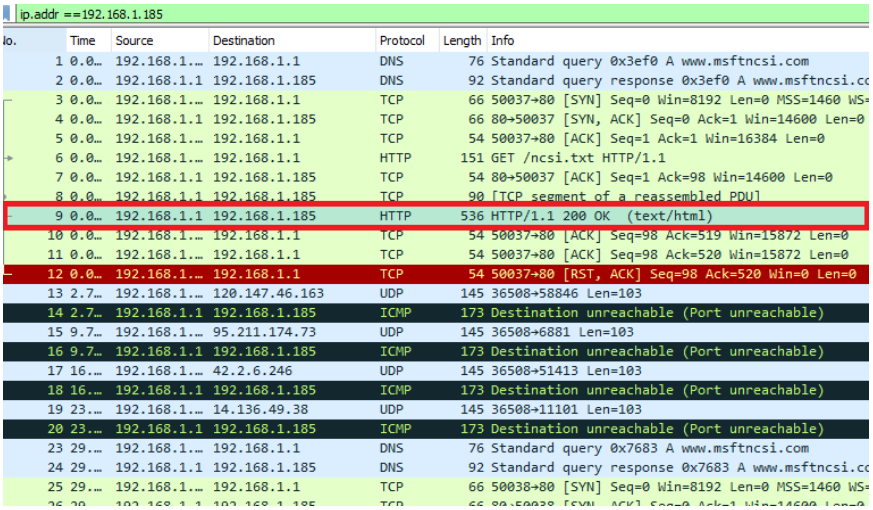


Gambar 6. Top Domain

Setelah melakukan percobaan akses terhadap IP Address 216.58.196.4 ternyata langsung menampilkan suatu halaman website phising, urlnya yaitu mobile.facebook.com/login.html terlihat pada gambar 7 berikut.

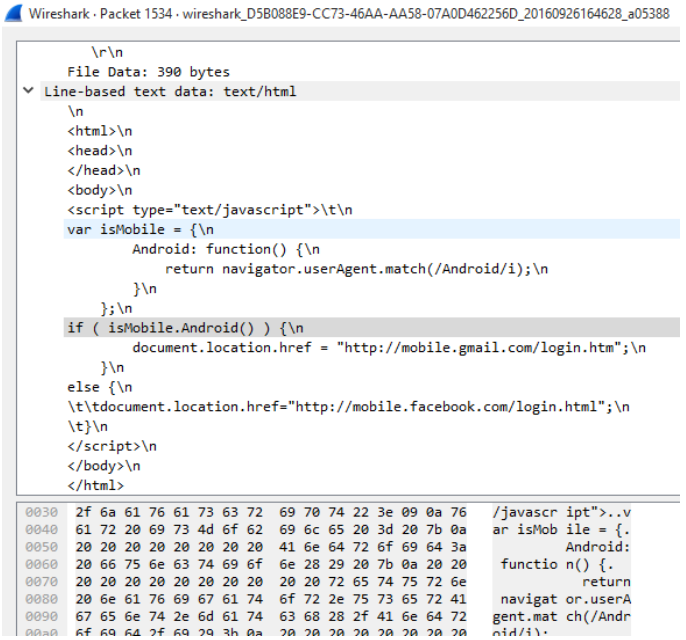
Gambar 7. Halaman Web Phising

Analisis selanjutnya menggunakan tool wireshark yaitu melakukan filter pada IP pengguna 192.168.1.185. dengan menggunakan perintah ip.addr ==192.168.1.185 filter tersebut berguna untuk mengetahui seberapa banyak conversation pada ip address tersebut terhadap IP address lainnya. Gambar 8 terlihat permintaan suatu proses antara IP address 192.168.1.1 ke 192.168.1.185 melalui protocol HTTP menggunakan HTTP/1.1 berbasis text/html.



Gambar 8. Hubungan IP Address 192.168.1.1 ke 192.168.1.185

Pada Gambar 8 terlihat IP Address 192.168.1.1 mengirimkan sebuah halaman website terhadap IP Address 192.168.1.185 yang dibuktikan dengan adanya suatu syntax berbasis html yang dikirimkan.



Gambar 9. Syntax HTML

4.1 Pengumpulan Data Eksperimen

Karena *beacon frame* merupakan hal yang penting pada suatu router dalam penyebaran informasi termasuk melakukan *probe request* authentication and association pada device sekitar, maka dari itu pengumpulan data bertujuan untuk mengetahui suatu proses yang berjalan sebanyak 30 kali pengulangan pada kedua firmware dengan waktu interval setiap 15 menit, *beacon frame* yang digunakan sebagai data yaitu *beacon frame* yang menyentuh angka minimal 80 ke atas, yang bertujuan untuk mengetahui apakah penyeberan *beacon frame* pada router penyerang sama dengan penyebaran *beacon frame* pada firmware wifi *pineapple* nano atau tidak.

Dari 30 data yang ada, selanjutnya mencari nilai rata-rata pada data, yang dibagi menjadi enam data dari setiap lima data rekapitulasi yang ada pada tabel 1 dan tabel 2.

Tabel 1. penyebaran *beacon frame firmware* penyerang

P1	79.4	P4	77.6
P2	73.6	P5	76.4

P3	76.4	P6	78

Tabel 2. Rata-rata penyebaran *Beacon frame firmware* wifi *pineapple* nano

N1	84.8	N4	81.6
N2	78	N5	76.6
N3	83.2	N6	75

Hipotesis:

H0 : Penyebaran *beacon frame* pada firmware penyerang (*pineapple* mark III) = Penyebaran *beacon frame* pada firmware wifi *pineapple* nano.

H1 : Penyebaran *beacon frame* pada firmware penyerang (*pineapple* mark III) ≠ Penyebaran *beacon frame* pada firmware wifi *pineapple* nano.

Taraf kepercayaan sebesar 99% atau 0,09 dengan tingkat kepercayaan 1% atau 0,01.

a. Uji Normalitas

Uji Normalitas pada setiap variable *beacon frame* dapat di lihat pada tabel 3 berikut;

Tabel 3 tabel uji normalitas

		Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Firmware	Statistic	Df	Sig.	Statistic	df	Sig.
Ratar atape nyeb aran	Firmware Penyerang	.233	6	.200*	.949	6	.733
	Firmware wifi *pineapple* nano	.184	6	.200*	.941	6	.665

Metode analitis menggunakan Shapiro-Wilk, Pada kedua variabel tersebut menunjukan bahwa nilai signifikansi Shapiro-Wilk lebih dari 0.05, jadi kedua data variable tersebut di asumsikan berdistribusi normal, dan dapat dilakukan suatu uji t dua sampel independen (independent sample t-test).

b. Uji T Dua Sampel Independen (Independent Sample T Test)

Uji normalitas pada data masing-masing variable *beacon frame firmware penyerang (mark III) dan firmware wifi pineapple nano* telah memenuhi syarat untuk dilakukannya uji T dua independent (*Independent sample t-test*) yaitu angka signifikansinya **0.733** dan **0.665**, pada tabel 4 berikut hasil uji hipotesis pada kedua variabel;

Tabel 4 Independent Sample T-Test

Levene's Test for Equality of Variances		t-test for Equality of Means						
							99% Confidence Interval of the Difference	
F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
6.508	.029	-1.662	10	.128	-2.9667	1.7854	-8.6252	2.6919
		-1.662	7.382	.138	-2.9667	1.7854	-9.1062	3.1728

Selang kepercayaan yang dikehendaki sebesar 99% , 100-99 = 1% atau 0.01 jadi signifikan levelnya adalah 0,01, yang menentukan apakah H0 diterima jika nilai sig. > 0,01 atau sebaliknya H0 ditolak jika nilai sig. < 0,01, bila H0 ditolak maka konsekuensinya hipotesis alternatif H1 diterima.

Dari hasil pengujian tersebut terlihat nilai signifikan menunjukan angka 0.029, nilai tersebut lebih besar dari 0.01 yang berarti H0 diterima, yaitu penyebaran *beacon frame* pada firmware penyerang (*pineapple* mark III) = penyebaran *beacon frame* pada firmware wifi *pineapple* nano. Jadi penyebaran *beacon frame* pada firmware penyerang (wifi *pineapple* mark III) sama dengan penyebaran *beacon frame* yang dimiliki oleh firmware wifi *pineapple* nano yang sangat berguna untuk melakukan *probe request* authentication and association pada device sekitar.

5. Kesimpulan dan Saran

5.1 Kesimpulan

1. Penelitian yang telah dilakukan menghasilkan suatu alat pendeteksian yang cukup mudah untuk mendeteksi adanya suatu permintaan *probe request*, yang bersifat dapat menduplikasi access point di sekitarnya berupa informasi BSSID yang valid untuk membedakan access point di sekitarnya.
2. Firmware wifi *pineapple* mark III memiliki mini web server 1.0 yang merupakan server ringan HTTP berbasis Bahasa C, yang berguna untuk melakukan phising pada suatu website.
3. Penyebaran *beacon frame* pada *firmware* penyerang (wifi *pineapple* mark III) sama dengan penyebaran *beacon frame* yang dimiliki oleh firmware wifi *pineapple* nano yang sangat berguna untuk melakukan *probe request* authentication and association pada device sekitar.

5.2 Saran

1. Alat pendeteksian menggunakan berbagai macam sistem operasi khususnya pada smartphone berbasis ios maupun sistem operasi blackberry yang dapat mendeteksi serangan.
2. Device wifi *pineapple* yang menggunakan alat terbaru dan firmware terbaru.
3. Analisa forensik dari sisi hardware maupun syntax pada firmware wifi *pineapple*.

Daftar Pustaka

[1] Fortinet. (2015). Wireless Security Survey 2015. https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/Survey-ReportWireless-Security-Survey-2015-v3.pdf, diakses 20 April 2016.

[2] Agrawal, N., & Tapaswi, S., 2015, Wireless Rogue Access Point Detection Using Shadow Honeynet. http://doi.org/10.1007/s11277-015-2408-0.

[3] Tzur, A., Amrani, O., & Wool, A. 2015. Direction Finding of rogue Wi-Fi access points using an off-the-shelf MIMO – OFDM receiver. Physical Communication, 17, 149–164. http://doi.org/10.1016/j.phycom.2015.08.010.

[4] Barbera, M. V, Epasto, A., Mei, A., Perta, V. C., & Stefa, J. (2013). Signals from the Crowd : Uncovering Social Relationships through Smartphone Probes

[5] John Wang. (2012). Advancing the Service Sector with Evolving Technologies: Techniques and Principles : Business Science Reference (an imprint of IGI Global)

[6] License, I. (2016). An Augmented Penetration Testing Framework for Mobile Devices on 802 . 11 ac Wireless Networks, 0–76.