Analisis Tingkat Keamanan pada Dinas XYZ Terhadap Serangan Pengguna Wifi

Bambang Sugiantoro
UIN Sunan Kalijaga Yogyakarta
Alamat, Jl. Marsda Adisucipto Yogyakarta
e-mail: Bambang.sugiantoro@uin-suka.ac.id

Abstrak

Kantor dinas yang tersebar diseluruh indonesia telah banyak yang menggunakan teknologi wifi. Perlu dilakukan analisis keamanan untuk Maturity Model dengan skala 0-5 dan dilanjutkan dengan penetration test menggunakan metode ARP Spoofing dengan menggunakan tools yakni CommView for Wifi ver.6.3, Aircrack-ng 1.1 serta Cain and Abel ver.4.9.35. Dari hasil berhasil menangkap username dan password yang dikirim dari komputer client. Oleh karena itu jaringan wireless yang diterapkan di kantor dinas XYZ tergolong belum cukup aman dalam hal keamanan jaringan. Dan hasil dari analisis tersebut jaringan wireless termasuk golongan Repeatable but Intuitive, yakni masih menggunakan konsep basic pemasangan dan belum berfokus penuh dalam hal keamanan jaringan dimana nilai akhirnya adalah sebesar 1.678.

Kata kunci: *Analisis keamanan , Maturity Model , metode ARP Spoofing*

Abstract

Government offices In Indonesia have many who use wifi technology. Security analysis for Maturity Model with 0-5 scale and followed by penetration test using ARP Spoofing method using CommView for Wifi tools ver.6.3, Aircrack-ng 1.1 and Cain and Abel ver.4.9.35. From the results managed to capture the username and password sent from the client computer. Therefore, the wireless network that is applied in XYZ office is classified as not secure enough in terms of network security. And the result of the analysis is wireless network including class Repeatable but Intuitive, which still use basic installation concept and not yet full focus in terms of network security where the end value is equal to 1,678.

Key words*: Security analysis, Maturity Model, ARP Spoofing method*

1. Pendahuluan

ARP (*Address Resolution Protocol*) adalah sebuah protokol dalam TCP/IP Protocol Suite yang bertanggung jawab dalam melakukan resolusi alamat IP ke dalam alamat *Media Access Control* (MAC Address). Dalam hal ARP Spoofing, hal tersebut mampu untuk memalsukan MAC Address router / proxy sehingga seluruh komputer intranet yang terhubung ke internet melalui proxy akan dikelabui untuk melewati komputer penyerang dan ini akan meneruskan akses router ini (*transparent proxy*).Dinas XYZ mempunyai tugas pokok untuk melaksanakan urusan kepemerintahan Daerah berdasarkan asas otonomi dan tugas pembantuan di bidang Kebudayaan dan Kepariwisataan.

Untuk mendukung kinerja pegawai serta untuk memperlancar program kerja, maka terdapat suatu jaringan WLAN di XYZ, Letak berada di persimpangan jalan utama, begitu strategis bagi lalu lalang kendaraan baik itu kendaraan ringan maupun berat. Secara lokasi, di seberang gedung dibangun suatu restoran dan tempat yang sering digunakan oleh remaja untuk bersantai ketika jam kerja selesai. Untuk mencegah adanya celah keamanan *wireless* maka dibutuhkan suatu pengujian demi mengamankan akses data jaringan.

2. Metodologi Penelitian

Penelitian dimulai dengan pengumpulan data, dilanjutkan dengan mem buat skenario pengujian, pengujian penetrasi tes dan perhitungan tingkat kematangan [1][2][3][4][5].

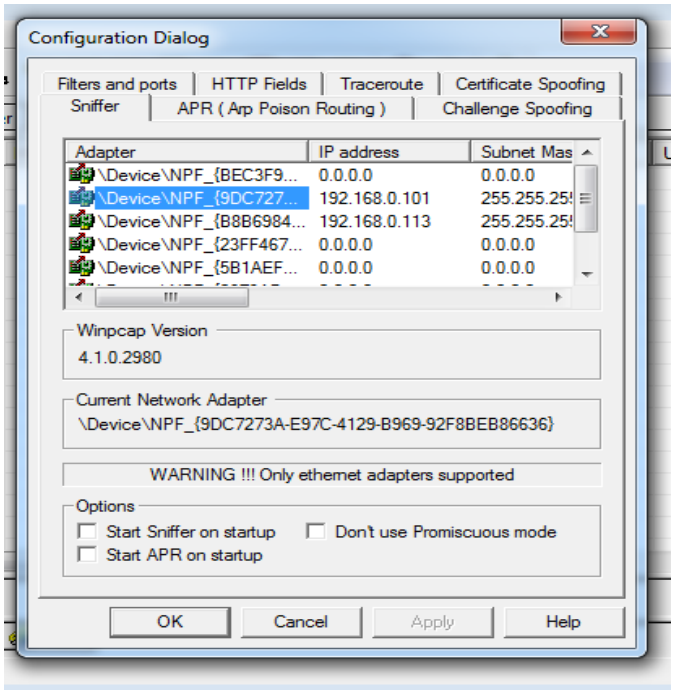
3. Analisa dan Hasil

3.1 ARP Spoofing

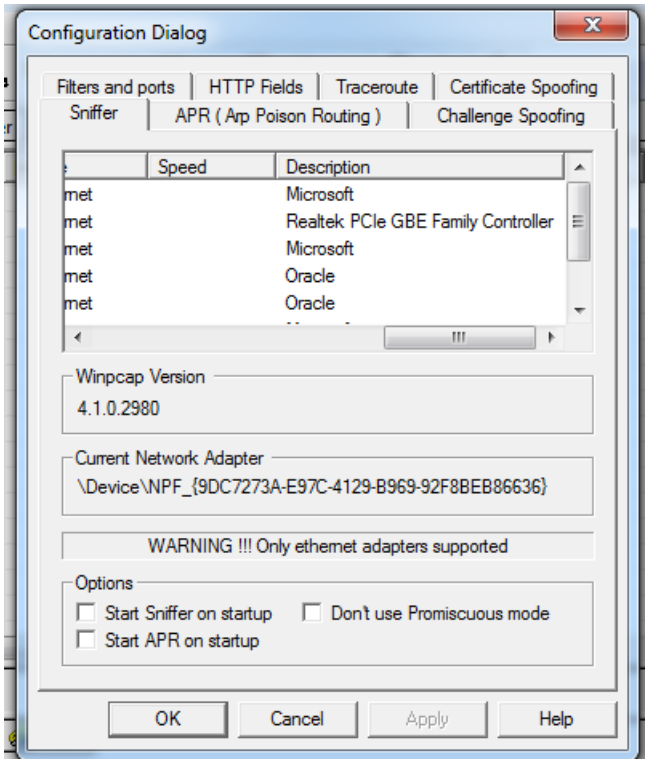
Dalam pengujian yang kedua ini, peneliti menggunakan tools Cain and Abel ver.4.9.35 dan tetap menggunakan *wireless adapter* TP-Link TLWN722N. Langkah pertama yang peneliti

ISSN (Printed) : 2579-7271
ISSN (Online) : 2579-5406

ambil ialah menonaktifkan Windows Firewall lalu menjalankan tools Cain and Abel. Konfigurasi yang peneliti lakukan adalah memilih adapter *wireless* bawaan Laptop Asus A46CB yakni dari Realtek.



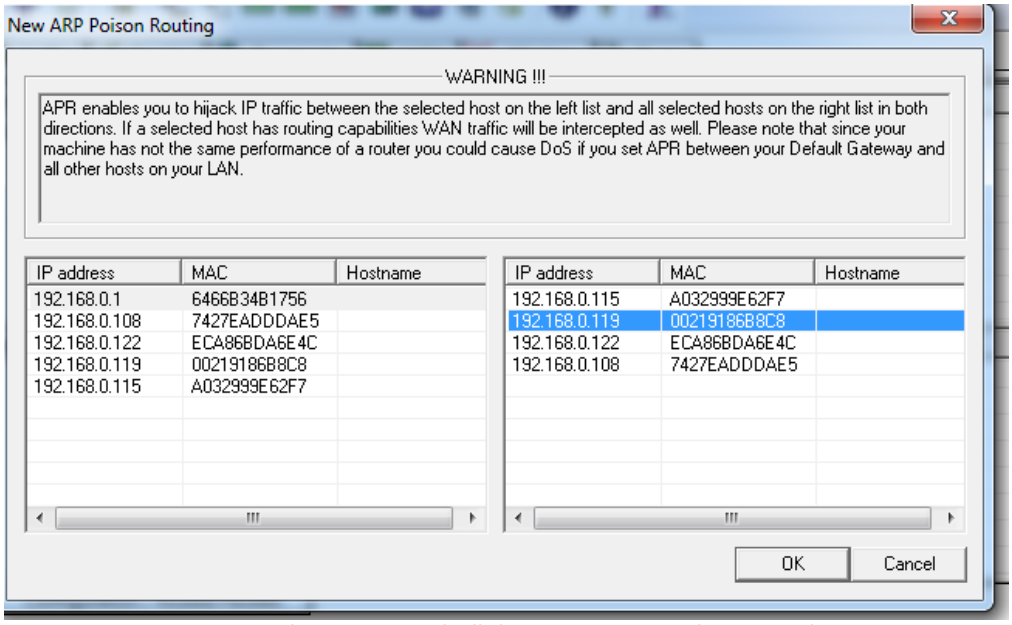
Gambar 3.1 *Device* yang peneliti pakai



Gambar 3.2 Deskripsi *wireless* adapter dari device

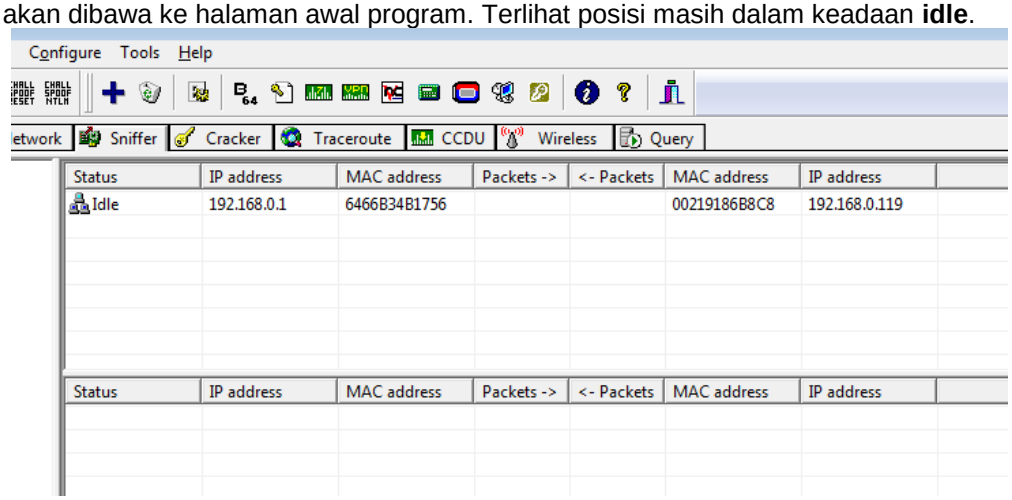
Lalu peneliti ulangi langkah klik tombol **+** dan muncul kotak dialog **New ARP Poison Routing**. Di dalam kotak dialog tersebut, terdapat dua tabel. Untuk tabel kiri dipilih sebagai IP gateway nya, dan sebelah kanan adalah target yang secara otomatis, IP dari klien akan dijadikan target.

ISSN (Printed) : 2579-7271
ISSN (Online) : 2579-5406



Gambar 3.3 Kotak dialog New ARP Poison Routing

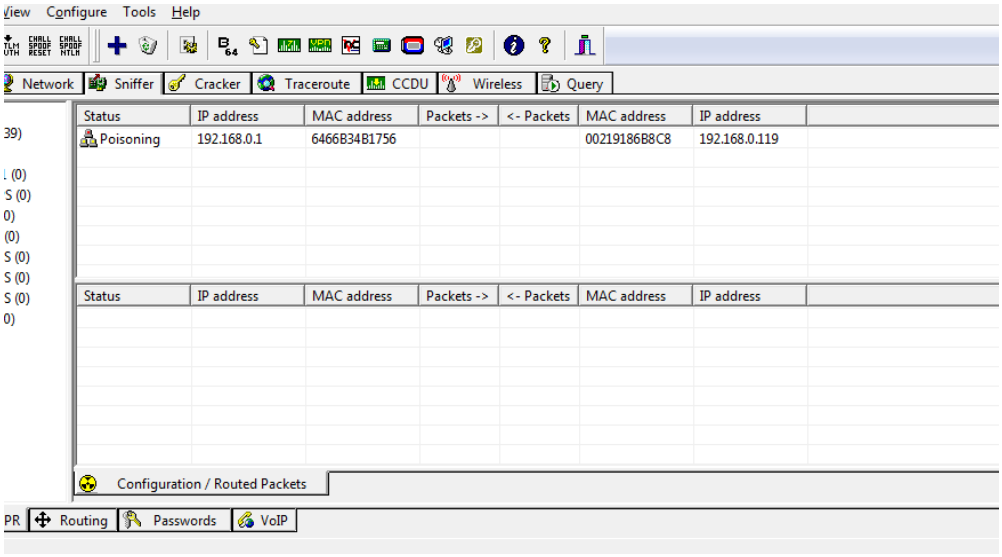
Peneliti mengambil target dengan IP 192.168.0.119, lalu peneliti klik **OK**. Selanjutnya, peneliti akan dibawa ke halaman awal program. Terlihat posisi masih dalam keadaan **idle**.



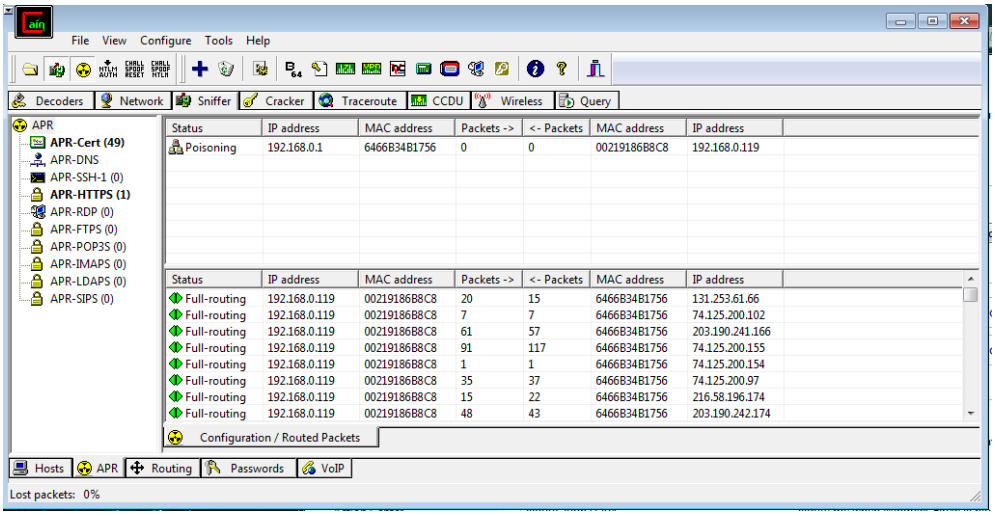
Gambar 3.4 Kondisi Idle

Setelah beberapa saat kondisi **Idle** akan berubah menjadi kondisi **Poisoning**. Sedangkan pada bagian bawah akan terjadi **Full-routing**. Langkah yang penulis ambil selanjutnya ialah menunggu ketika komputer target melakukan suatu login terhadap website tertentu.

ISSN (Printed) : 2579-7271
ISSN (Online) : 2579-5406



Gambar 3.5 Kondisi *Poisoning*

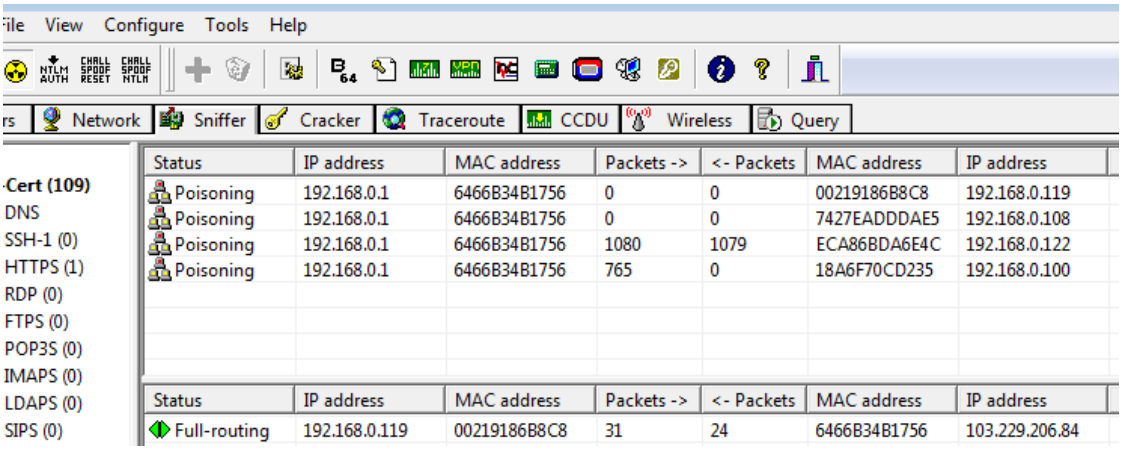


Gambar 3.6 Kondisi *Full-Routing*

Pada kolom sebelah kiri bagian APR-HTTPS akan menampilkan data yang ter-capture. Apabila di klik, akan menampilkan website yang berhasil ditangkap oleh tools tersebut. Dalam melakukan penelitian ini, peneliti bekerja sama dengan pihak administrator untuk mencoba memasukkan *username* dan *password* dari suatu website yang sering dikunjungi oleh klien Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali. Bila peneliti masuk ke tab **Password** lalu di panel sebelah kiri masuk **HTTP** maka username dan password yang terdeteksi akan tertampil disana. Sebagai contoh administrator masuk ke situs www.liputan6.com selanjutnya melakukan login *username* dan *password*, dari program Cain and Abel akan menangkap sandi yang dikirimkan oleh komputer yang digunakan administrator melewati laptop peneliti yang menggunakan Cain and Abel.

Selanjutnya peneliti melakukan spoofing menggunakan 4 target, IP masing-masing 192.168.0.119; 192.168.0.108; 192.168.0.122; dan 192.168.0.100.

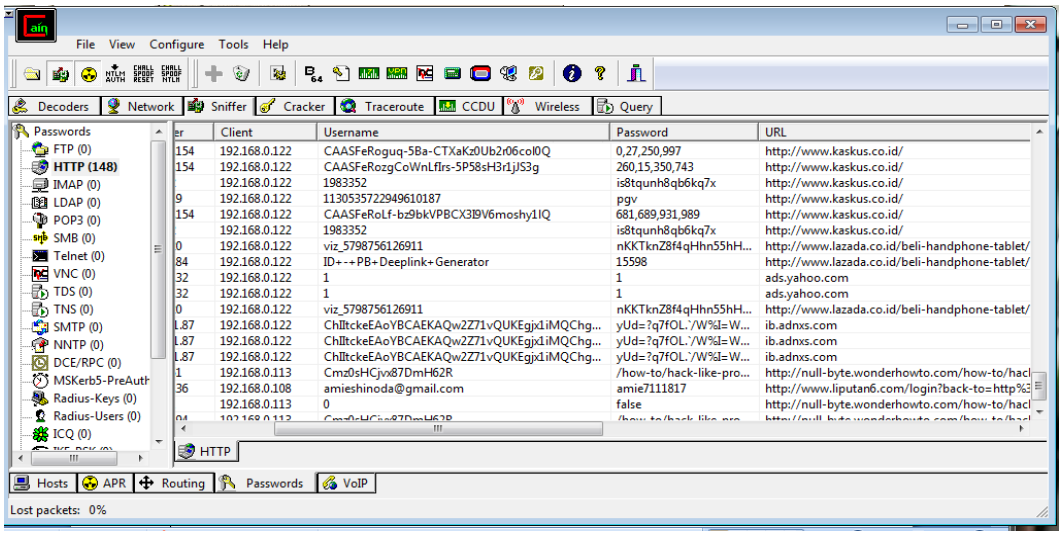
ISSN (Printed) : 2579-7271
ISSN (Online) : 2579-5406



Gambar 3.7 Target yang ter-*poisoning*

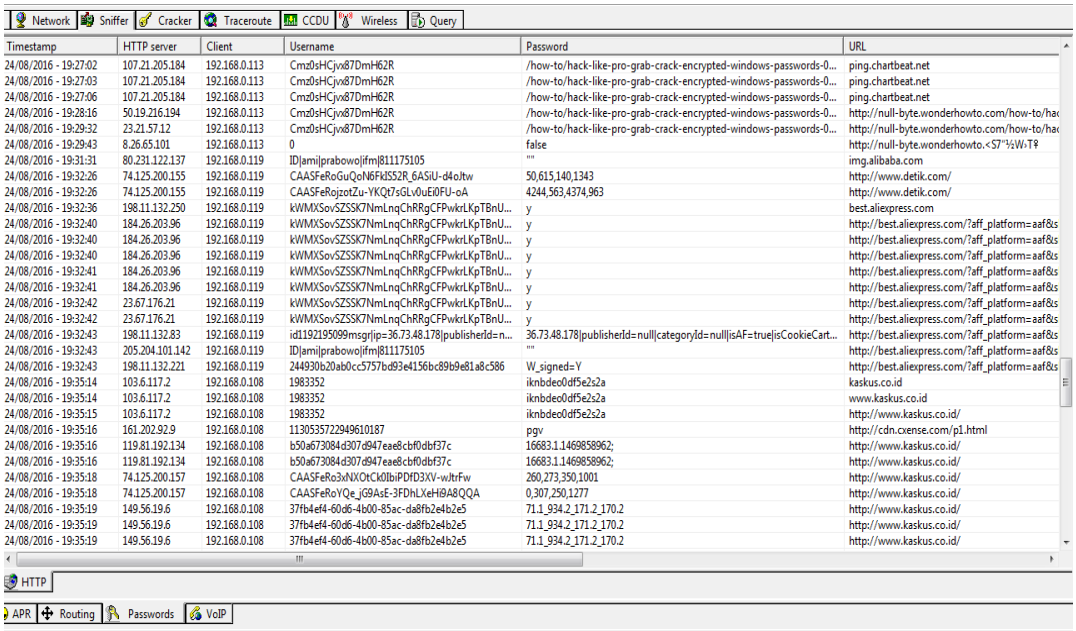
Kembali ke langkah dimana penulis dan administrator Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali mencoba untuk memasukkan username dan sandi sembarang pada situs-situs yang dianggap sering dikunjungi oleh pihak pegawai maupun stakeholder ketika menggunakan jaringan *wireless* kantor. Berikut daftar website yang peneliti jadikan target untuk penetration test ARP Spoofing:

Dari website yang peneliti jadikan target penelitian terdapat beberapa website yang terekam username dan sandi yang dimasukkan di komputer *client*. Namun ternyata didapati beberapa website hanya bisa ter-*capture username* nya saja, seperti login di website alibaba.com dan aliexpress.com. Namun banyak pula yang tidak mampu terekam *username* beserta *password* yang dikirimkan dari komputer client. Dan berikut hasil *screenshot* tersebut:

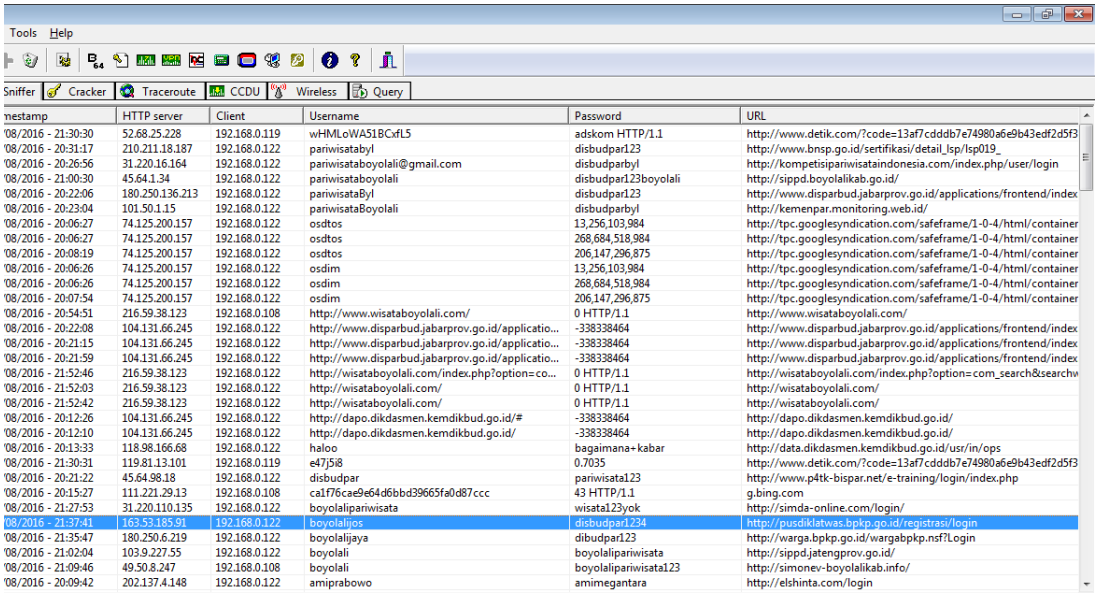


Gambar 3.8 Website Kaskus dan *capture* Liputan6

ISSN (Printed) : 2579-7271
ISSN (Online) : 2579-5406



Gambar 3.9 *Capture* website Alibaba dan Aliexpress



Gambar 3.10 Website target

4. Kesimpulan

Tingkat keamanan WLAN pada Dinas XYZ maka untuk hasil dari audit sendiri didapatkan bahwa dari 56 *checklist* yang disediakan *Wireless Security Checklist* oleh Rao Vallabhaneni hanya 36 *checklist* yang masuk kriteria penilaian, sedangkan sebanyak 20 *checklist* belum masuk kriteria aman dengan nilai total kematangan tiap poin adalah 94. Apabila diambil rerata, maka nilai tingkat kematangan (*Maturity Level*) keamanan dari jaringan *wireless* Dinas XYZ adalah 1.6785, yang masuk ke dalam kriteria *Repeatable but Intuitive*. Sedangkan total target kematangan yang diharapkan dari pihak Dinas XZY adalah sebesar 2.30357 yang mana masih masuk kriteria *Repeatable but Intuitive* menghasilkan selisih 0.6249 poin dari total poin kematangan akhir terhadap target poin yang diharapkan.

ISSN (Printed) : 2579-7271
ISSN (Online) : 2579-5406

Daftar Pustaka

[1] Danawiputra, Andhika. 2011. ”Audit Keamanan Jaringan Wireless Menggunakan Wireess Security Checklist ISO 27001 Studi Kasusu di BPKB DIKPORA Provinsi DIY”. *Skripsi*. Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.

[2] Nugroho, Agung. 2012. “Analisa Keamanan Jaringan Wireless Local Area Networ Dengan Access Point TP-LINK WA500G”. *Skripsi*. Fakultas Komunikasi dan Informatika Universitas Muhammadiyah Surakarta.

[3] Romadhon, Pearl Pratama. 2014. “Analisis Kinerja Jaringan Wireless LAN Menggunakan Metode QOS dan RMA Pada PT Pertamina EP Ubep Ramba (Persero)”. *Skripsi*. Universitas Bina Darma Palembang.

[4] Indrarukmana, Faizal. 2014. “Optimasi Keamanan Jaringan Terhadap Serangan Botnet (Studi Kasus Serangan DNS Poisoning Pada DNS Server)”. *Skripsi*. Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.

[5] Stiawan, Heri. 2015. “Audit Sistem Informasi Rumah Sakit Menggunakan Standar ISO 27001 (Studi Kasus di RSU PKU Muhammadiyah Bantul)”. *Skripsi*. Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.