

# 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 pemerintahan Daerah berdasarkan asas otonomi dan tugas pembantuan di bidang Kebudayaan dan Kepariwisata.

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**

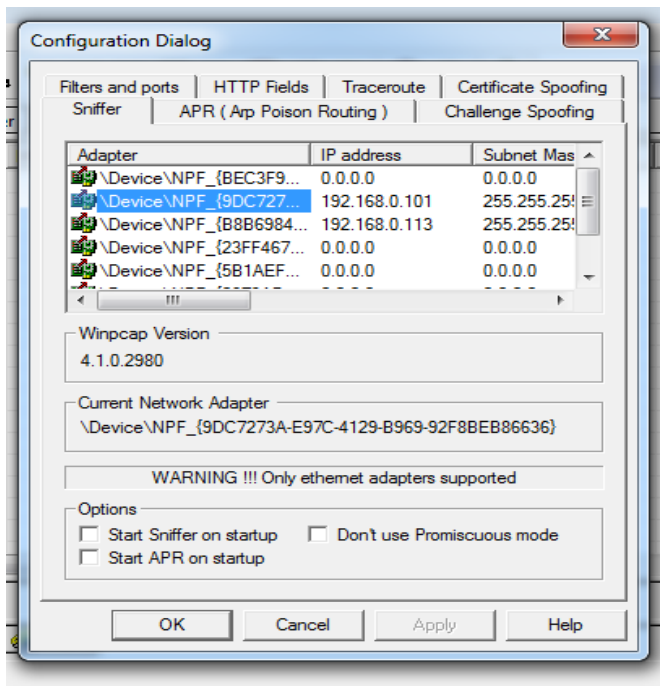
Penelitian dimulai dengan pengumpulan data, dilanjutkan dengan mem buat skenario pengujian, pengujian penetrasi tes dan perhitungan tingkat kematangan [1][2][3][4][5].

## **3. Analisa dan Hasil**

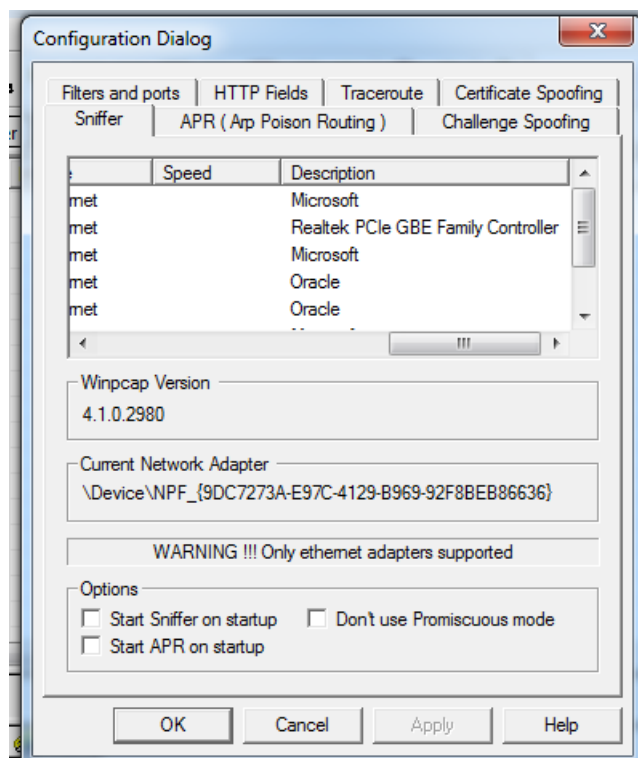
### **3.1 ARP Spoofing**

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

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.

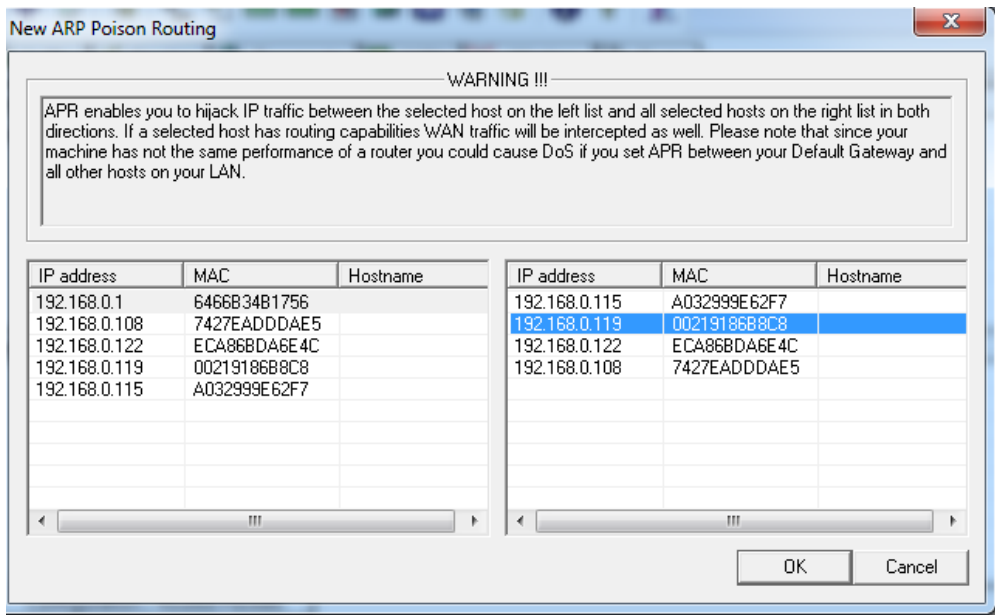


Gambar 3.1 Device yang peneliti pakai



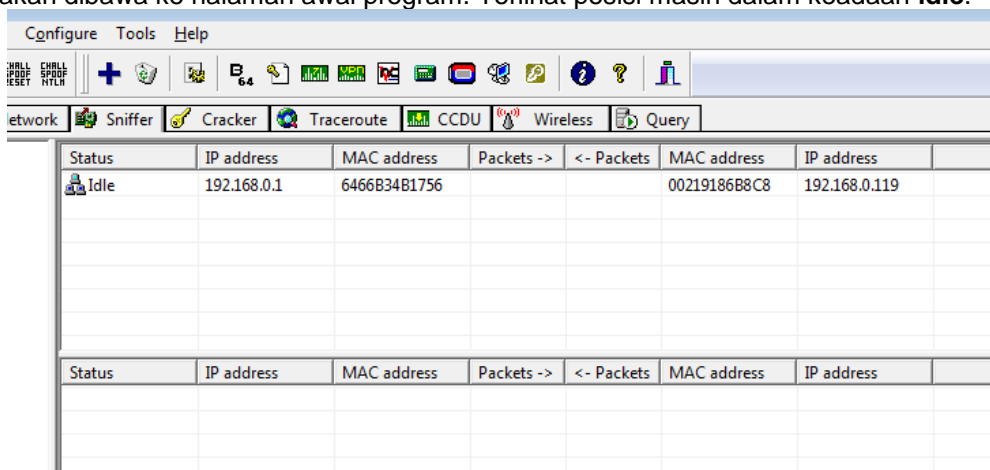
Gambar 3.2 Deskripsi wireless adapter dari device

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.



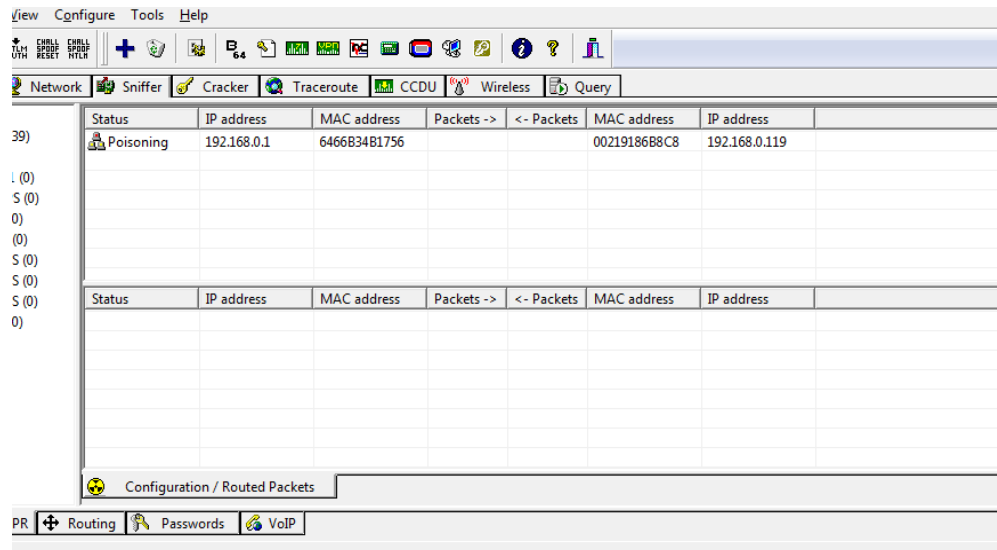
Gambar 3.3 Kotak dialog New ARP Poison Routing

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**.

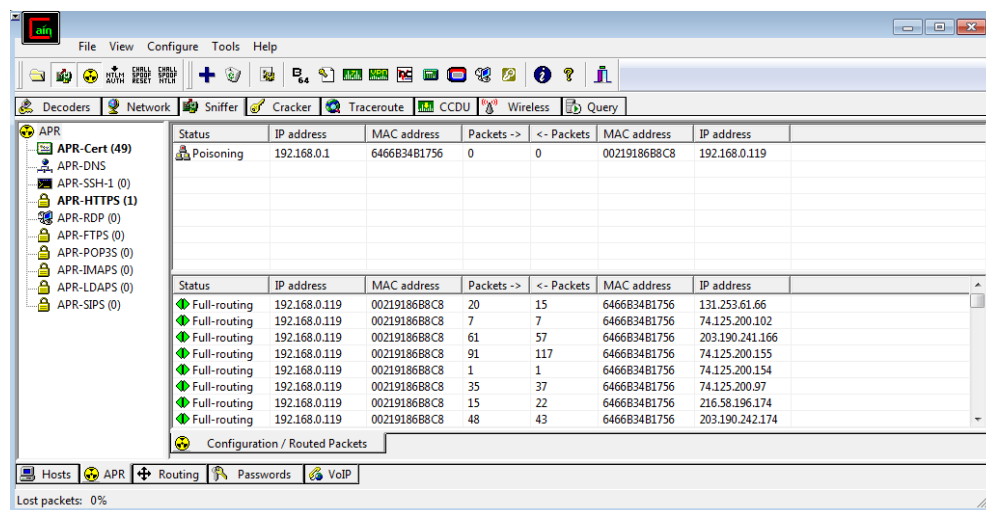


Gambar 3.4 Kondisi Idle

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.



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](http://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.

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	192.168.0.1	6466B34B1756	0	0	00219186B8C8	192.168.0.119
Poisoning	192.168.0.1	6466B34B1756	0	0	7427EADDDAE5	192.168.0.108
Poisoning	192.168.0.1	6466B34B1756	1080	1079	ECA86BDA6E4C	192.168.0.122
Poisoning	192.168.0.1	6466B34B1756	765	0	18A6F70CD235	192.168.0.100
<hr/>						
Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Full-routing	192.168.0.119	00219186B8C8	31	24	6466B34B1756	103.229.206.84

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:

Client	Username	Password	URL
192.168.0.122	CAASFeRogug-5Ba-CTXaKz0Ub2r06co0Q	0,27,250,997	http://www.kaskus.co.id/
192.168.0.122	CAASFeRozgCoWnLfirs-5P58s+H3r1jJ53g	260,15,350,743	http://www.kaskus.co.id/
192.168.0.122	1983352	is8tqnh8qb6kq7x	http://www.kaskus.co.id/
192.168.0.122	1130535722949610187	pgv	http://www.kaskus.co.id/
192.168.0.122	CAASFeRoLf-bz9bkVPBCX3B9V6moshy1IQ	681,689,931,989	http://www.kaskus.co.id/
192.168.0.122	1983352	is8tqnh8qb6kq7x	http://www.kaskus.co.id/
192.168.0.122	viz_5798756126911	nKKTknZ8f4qHhn55hH...	http://www.lazada.co.id/beli-handphone-tablet/
192.168.0.122	ID++PB+Deeplink+ Generator	15598	http://www.lazada.co.id/beli-handphone-tablet/
192.168.0.122	1	1	ads.yahoo.com
192.168.0.122	1	1	ads.yahoo.com
192.168.0.122	viz_5798756126911	nKKTknZ8f4qHhn55hH...	http://www.lazada.co.id/beli-handphone-tablet/
192.168.0.122	ChlltckeEAoYBCAEKAQw2Z71vQUKEgjd:iMQChg...	yUd=?q7fOL:7W%id=W...	ib.adnxs.com
192.168.0.122	ChlltckeEAoYBCAEKAQw2Z71vQUKEgjd:iMQChg...	yUd=?q7fOL:7W%id=W...	ib.adnxs.com
192.168.0.122	ChlltckeEAoYBCAEKAQw2Z71vQUKEgjd:iMQChg...	yUd=?q7fOL:7W%id=W...	ib.adnxs.com
192.168.0.113	Cmz0sHCjv87Dmh62R	/how-to/hack-like-pro...	http://null-byte.wonderhowto.com/how-to/hac...
192.168.0.108	amieshinoda@gmail.com	armie7111817	http://www.liputan6.com/login?back-to=http%...
192.168.0.113	0	false	http://null-byte.wonderhowto.com/how-to/hac...

Gambar 3.8 Website Kaskus dan capture Liputan6

Timestamp	HTTP server	Client	Username	Password	URL
24/08/2016 - 19:27:02	107.21.205.184	192.168.0.113	CmzdHCjv87DmH62R		ping.chartbeat.net
24/08/2016 - 19:27:03	107.21.205.184	192.168.0.113	CmzdHCjv87DmH62R		/how-to/hack-like-pro-grab-crack-encrypted-windows-passwords-0...
24/08/2016 - 19:27:06	107.21.205.184	192.168.0.113	CmzdHCjv87DmH62R		ping.chartbeat.net
24/08/2016 - 19:28:16	59.19.216.194	192.168.0.113	CmzdHCjv87DmH62R		http://null-byte.wonderhowto.com/how-to/hac...
24/08/2016 - 19:29:32	23.21.57.12	192.168.0.113	CmzdHCjv87DmH62R		http://null-byte.wonderhowto.com/<S7%WtR
24/08/2016 - 19:29:43	8.26.65.101	192.168.0.113	0	false	http://null-byte.wonderhowto.com/<S7%WtR
24/08/2016 - 19:31:31	80.231.122.137	192.168.0.119	IDJamiprabowojf811175105	'''	img.alibaba.com
24/08/2016 - 19:32:26	74.125.200.155	192.168.0.119	CAASFeRoGuQhN6Kf5S2R_6ASUj-d4oIhw	50.615.140.1343	http://www.detik.com/
24/08/2016 - 19:32:26	74.125.200.155	192.168.0.119	CAASFeRoJoztZu-VKQ7sGLvUe0FUo-a	4244.563.4374.963	http://www.detik.com/
24/08/2016 - 19:32:36	198.11.132.250	192.168.0.119	KWMMXsovSZSK7NmLqChRRgCFPwktLgTBnU...	y	best.aliexpress.com
24/08/2016 - 19:32:40	184.26.203.96	192.168.0.119	KWMMXsovSZSK7NmLqChRRgCFPwktLgTBnU...	y	http://best.aliexpress.com/?aff_platform=aa&is
24/08/2016 - 19:32:40	184.26.203.96	192.168.0.119	KWMMXsovSZSK7NmLqChRRgCFPwktLgTBnU...	y	http://best.aliexpress.com/?aff_platform=aa&is
24/08/2016 - 19:32:40	184.26.203.96	192.168.0.119	KWMMXsovSZSK7NmLqChRRgCFPwktLgTBnU...	y	http://best.aliexpress.com/?aff_platform=aa&is
24/08/2016 - 19:32:41	184.26.203.96	192.168.0.119	KWMMXsovSZSK7NmLqChRRgCFPwktLgTBnU...	y	http://best.aliexpress.com/?aff_platform=aa&is
24/08/2016 - 19:32:41	184.26.203.96	192.168.0.119	KWMMXsovSZSK7NmLqChRRgCFPwktLgTBnU...	y	http://best.aliexpress.com/?aff_platform=aa&is
24/08/2016 - 19:32:42	23.67.176.21	192.168.0.119	KWMMXsovSZSK7NmLqChRRgCFPwktLgTBnU...	y	http://best.aliexpress.com/?aff_platform=aa&is
24/08/2016 - 19:32:42	23.67.176.21	192.168.0.119	KWMMXsovSZSK7NmLqChRRgCFPwktLgTBnU...	y	http://best.aliexpress.com/?aff_platform=aa&is
24/08/2016 - 19:32:43	198.11.132.83	192.168.0.119	id119219509mssgijpe=36.73.48.178;publishid=n...	36.73.48.178;publisherId=null;categoryId=null;isAF=true;isCookieCat...	http://best.aliexpress.com/?aff_platform=aa&is
24/08/2016 - 19:32:43	205.204.101.142	192.168.0.119	IDJamiprabowojf811175105	'''	http://best.aliexpress.com/?aff_platform=aa&is
24/08/2016 - 19:32:43	198.11.132.221	192.168.0.119	244930b20ab0c5757b0d93e4156bc89b9e81a8c586	W_signed=Y	http://best.aliexpress.com/?aff_platform=aa&is
24/08/2016 - 19:35:14	103.6.117.2	192.168.0.108	1983352	iknbdeo0df5e2z2a	kaskus.co.id
24/08/2016 - 19:35:14	103.6.117.2	192.168.0.108	1983352	iknbdeo0df5e2z2a	www.kaskus.co.id
24/08/2016 - 19:35:15	103.6.117.2	192.168.0.108	1983352	iknbdeo0df5e2z2a	http://www.kaskus.co.id/
24/08/2016 - 19:35:16	161.202.92.9	192.168.0.108	1130535722949610187	pgv	http://cdn.cense.com/p1.html
24/08/2016 - 19:35:16	119.81.192.134	192.168.0.108	b50a673084d907e947ee8cbf0dbf37c	16683.1.1469858962;	http://www.kaskus.co.id/
24/08/2016 - 19:35:16	119.81.192.134	192.168.0.108	b50a673084d907e947ee8cbf0dbf37c	16683.1.1469858962;	http://www.kaskus.co.id/
24/08/2016 - 19:35:18	74.125.200.157	192.168.0.108	CAASFeRo3XvOChCK0lbPFD3XV-wtrFw	260.273.350.1001	http://www.kaskus.co.id/
24/08/2016 - 19:35:18	74.125.200.157	192.168.0.108	CAASFeRoYQe_jG9AsE-3FDhLxH8A8QQA	0.307.250.1277	http://www.kaskus.co.id/
24/08/2016 - 19:35:19	149.56.19.6	192.168.0.108	37fb4ef4-6046-4b00-85ac-da8fb2e4b2e5	71.1_934_2_171_2_170.2	http://www.kaskus.co.id/
24/08/2016 - 19:35:19	149.56.19.6	192.168.0.108	37fb4ef4-6046-4b00-85ac-da8fb2e4b2e5	71.1_934_2_171_2_170.2	http://www.kaskus.co.id/
24/08/2016 - 19:35:19	149.56.19.6	192.168.0.108	37fb4ef4-6046-4b00-85ac-da8fb2e4b2e5	71.1_934_2_171_2_170.2	http://www.kaskus.co.id/

Gambar 3.9 Capture website Alibaba dan Aliexpress

Timestamp	HTTP server	Client	Username	Password	URL
08/2016 - 21:30:30	52.68.25.228	192.168.0.119	wHMLcWAS1BCxfl5	adskom HTTP/1.1	http://www.detik.com/?code=13af7cddb7e74980a6e9b43eef2d5f3
08/2016 - 20:31:17	210.211.18.187	192.168.0.122	pariwisata123	disbudpar123	http://www.bnsp.go.id/serifikasidetil_jsp/isp019
08/2016 - 20:26:56	31.220.116.164	192.168.0.122	pariwisataboyolali@gmail.com	disbudparbyl	http://kompetisipariwisataindonesia.com/index.php/user/login
08/2016 - 21:00:30	45.64.1.34	192.168.0.122	pariwisataboyolali	disbudpar123boyolali	http://sippd.boyalikalab.go.id/
08/2016 - 20:22:06	180.250.136.213	192.168.0.122	pariwisataByl	disbudpar123	http://www.disparbud.jabarprov.go.id/applications/frontend/index
08/2016 - 20:23:04	101.50.1.15	192.168.0.122	pariwisataBoyolali	disbudparbyl	http://kemempar.monitoring.web.id/
08/2016 - 20:06:27	74.125.200.157	192.168.0.122	osditos	13,256,103,984	http://tpc.googleusercontent.com/safeframe/1-0-4/html/container
08/2016 - 20:06:27	74.125.200.157	192.168.0.122	osditos	268,684,518,984	http://tpc.googleusercontent.com/safeframe/1-0-4/html/container
08/2016 - 20:08:19	74.125.200.157	192.168.0.122	osditos	206,147,296,875	http://tpc.googleusercontent.com/safeframe/1-0-4/html/container
08/2016 - 20:06:26	74.125.200.157	192.168.0.122	osdim	13,256,103,984	http://tpc.googleusercontent.com/safeframe/1-0-4/html/container
08/2016 - 20:06:26	74.125.200.157	192.168.0.122	osdim	268,684,518,984	http://tpc.googleusercontent.com/safeframe/1-0-4/html/container
08/2016 - 20:07:54	74.125.200.157	192.168.0.122	osdim	206,147,296,875	http://tpc.googleusercontent.com/safeframe/1-0-4/html/container
08/2016 - 20:54:51	216.59.38.123	192.168.0.108	http://www.wisataboyolali.com/	0 HTTP/1.1	http://www.wisataboyolali.com/
08/2016 - 20:22:08	104.131.66.245	192.168.0.122	http://www.disparbud.jabarprov.go.id/applicatio...	-338338464	http://www.disparbud.jabarprov.go.id/applications/frontend/index
08/2016 - 20:21:15	104.131.66.245	192.168.0.122	http://www.disparbud.jabarprov.go.id/applicatio...	-338338464	http://www.disparbud.jabarprov.go.id/applications/frontend/index
08/2016 - 20:21:59	104.131.66.245	192.168.0.122	http://www.disparbud.jabarprov.go.id/applicatio...	-338338464	http://www.disparbud.jabarprov.go.id/applications/frontend/index
08/2016 - 21:52:46	216.59.38.123	192.168.0.122	http://wisataboyolali.com/index.php?option=com...	0 HTTP/1.1	http://wisataboyolali.com/index.php?option=com_search&searchv
08/2016 - 21:52:03	216.59.38.123	192.168.0.122	http://wisataboyolali.com/	0 HTTP/1.1	http://wisataboyolali.com/
08/2016 - 21:52:42	216.59.38.123	192.168.0.122	http://wisataboyolali.com/	0 HTTP/1.1	http://wisataboyolali.com/
08/2016 - 20:12:26	104.131.66.245	192.168.0.122	http://dapo.dikdasmen.kemdikbud.go.id/#	-338338464	http://dapo.dikdasmen.kemdikbud.go.id/
08/2016 - 20:12:10	104.131.66.245	192.168.0.122	http://dapo.dikdasmen.kemdikbud.go.id/	-338338464	http://dapo.dikdasmen.kemdikbud.go.id/
08/2016 - 20:13:33	118.98.166.68	192.168.0.122	haloo	bagaimana+ kabar	http://data.dikdasmen.kemdikbud.go.id/usr/in/ops
08/2016 - 21:30:31	119.81.13.101	192.168.0.119	e475i8	0.7035	http://www.detik.com/?code=13af7cddb7e74980a6e9b43eef2d5f3
08/2016 - 20:21:22	45.64.98.18	192.168.0.122	disbudpar	pariwisata123	http://www.p4tk-bispar.net/e-training/login/index.php
08/2016 - 20:15:27	111.221.29.13	192.168.0.108	ca1f76cae9e64d6bbd39665fa0d87ccc	43 HTTP/1.1	g.bing.com
08/2016 - 21:27:53	31.220.110.135	192.168.0.122	boyolalipariwisata	wisata123yok	http://simda-online.com/login/
08/2016 - 21:37:41	163.53.185.91	192.168.0.122	boyolalinos	disbudpar1234	http://pusdiklatwas.bpkk.go.id/registrasi/login
08/2016 - 21:35:47	180.250.6.219	192.168.0.122	boyolalijaya	disbudpar123	http://warga.bpkk.go.id/wargabpkk.nsf?login
08/2016 - 21:02:04	103.9.227.55	192.168.0.122	boyolali	boyolalipariwisata	http://sippd.jatengprov.go.id/
08/2016 - 21:09:46	49.50.8.247	192.168.0.108	boyolali	boyolalipariwisata123	http://simonev-boyolikalab.info/
08/2016 - 20:09:42	202.137.4.148	192.168.0.122	amiprabowo	amimegantara	http://elshint.com/login

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 XYZ 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.

#### Daftar Pustaka

- [1] Danawiputra, Andhika. 2011. "Audit Keamanan Jaringan Wireless Menggunakan Wireess Security Checklist ISO 27001 Studi Kasus 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.