ANALISIS KEAMANAN WLAN TERHADAP GANGGUAN ARP SPOOFING (STUDI KASUS KANTOR DINAS KEBUDAYAAN DAN PARIWISATA KABUPATEN BOYOLALI)

SKRIPSI

Untuk memenuhi sebagai persyaratan

mencapai derajat Sarjana S-1

Program Studi Teknik Informatika

Disusun oleh :

Ami Megantara Prabowo

12650013

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2017

Universitas Islam Negeri Sunan Kalijaga FM-UINSK-BM-05-07/R0

PENGESAHAN SKRIPSI/TUGAS AKHIR

Nomor : B-344 /Un.02/DST/PP.05.3/01/2016

Skripsi/Tugas Akhir dengan judul	:	Analisis Keamanan WLAN Terhadap Gangguan ARP Spoofing (Studi Kasus Kantor Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali)
Yang dipersiapkan dan disusun oleh	:	
Nama	:	Ami Megantara Prabowo
NIM	:	12650013
Telah dimunaqasyahkan pada	:	24 Januari 2017
Nilai Munaqasyah	:	A-

Dan dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga

TIM MUNAQASYAH :

Ketua Sidang

Dr.Bambang Sugiantoro
NIP. 19751024 200912 1 002

Penguji I

Agung Fatwanto, Ph.D
NIP.19770103 200501 1 003

Penguji II

M. Didik R.Wahyudi, M.T
NIP.19760812 200901 1 015

Yogyakarta, 31 Januari 2017
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
Dekan

Dr. Murtono, M.Si
NIP. 19691212 200003 1 001

Universitas Islam Negeri Sunan Kalijaga FM-UINSK-BM-05-03/R0

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal :

Lamp :

Kepada

Yth. Dekan Fakultas Sains dan Teknologi

UIN Sunan Kalijaga Yogyakarta

Di Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikanseperlunya, maka kami selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama	:Ami Megantara Prabowo
NIM	:12650013
Judul Skripsi	:Analisis Keamanan WLAN Terhadap Gangguan ARP Spoofing (Studi Kasus Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali

sudah dapat diajukan kembali kepada Program Studi Teknik Informatika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam Teknik Informatika

Dengan ini kami mengharap agar skripsi/tugas akhir Saudara tersebut di atas dapat segera dimunaqsyahkan. Atas perhatiannya kami ucapkan terima kasih.

Yogyakarta, 10 Januari 2017

Pembimbing

Dr. Bambang Sugiantoro, MT.

NIP.19751024 200912 1 002

PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan di bawah ini :

Nama : Ami Megantara Prabowo

NIM : 12650013

Program Studi : Teknik Informatika

Fakultas : Sains dan Teknologi

Menyatakan bahwa skripsi dengan judul **"ANALISIS KEAMANAN WLAN TERHADAP GANGGUAN ARP SPOOFING (Studi Kasus Kantor Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali)"** tidak terdapat karya yang perna diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang ditulis atau diterbitkan oleh orang lain, kecuali yang telah ditulis dan diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 17 Januari 2017

Yang menyatakan,

Ami Megantara Prabowo

NIM. 12650013

KATA PENGANTAR

Segala puji bagi Allah SWT, Tuhan semesta alam. Atas berkat Rahmat dan Hidayat - Nya, kita semua masih diberi nikmat sehat, nikmat sempat, dan nikmat iman. Shalawat serta salam saya haturkan kepada baginda Nabi Muhammad SAW, sebagai pencerah ilmu, pemimpin umat muslim, yang mengajarkan kepada kita untuk selalu beriman kepada Allah SAW.

Dalam penulisan skripsi ini penulis peneliti mengucapkan terimakasih banyak kepada:

1. Yang terhormat Bapak Dr. Murtono, selaku Dekan Fakultas Sains dan Teknologi yang telah memberikan kesempatan bagi saya untuk menimba ilmu keinformatikaan sejak pertama masuk kuliah.
2. Yang terhormat Bapak Dr. Bambang Sugiantoro, MT., selaku Kepala Program Pendidikan Teknik Informatika Fakultas Sains dan Teknologi yang memberikan dorongan kepada penulis untuk selalu semangat dalam menyelesaikan penulisan ini serta sebagai pembimbing yang telah memberikan waktu, tenaga serta aspirasi ide pemikirannya untuk membimbing penulis dalam menyelesaikan penulisan ini.
3. Yang terhormat, Bapak Aulia Faqih Rifa'i, selaku Pembimbing Akademik mahasiswaTeknik Informatika periode 2012 yang senantiasa mendidik dan membimbing kami dalam belajar selama menjadi mahasiswa UIN Sunan Kalijaga.
4. Kedua orang tua penulis tercinta, kagumi dan banggakan, Ibu Hanik Shofia dan Bapak Supriyono, yang tak pernah menyerah menyemangati penulis, yang selalu

memberikan dukungan moril, kasih sayang, sampai selesainya tugas penulis di perkuliahan.

5. Kedua kakak penulis sayangi, Mbak Mia, Mba Im serta kakak ipar penulis, Mas Zul, Mas Kas, yang penuh semangat mendukung penulis dalam menyelesaikan tugas akhir ini.

6. Almer, Faiz, dan Bintang, calon anak-anak berjiwa pemimpin yang sholeh, sholehah yang telah memberikan senyuman semangat bagi penulis.

7. Pihak Komando Resimen Mahasiswa Periode 2012, 2013, 2014 dan 2015, yang memberikan kesempatan dan pendidikan kemenwaan bagi penulis hingga purna tugas, keluarga besar Resimen Mahasiswa Satuan/Batalyon 03 UIN Sunan Kalijaga Yogyakarta terutama seluruh personil seperjuangan Yudha 36, Rozi, Agung, Ahsin, Alwi, Azza, Imam, Zarkasi, Roki, Hida, Risna, Jidda yang selalu memberikan semangat luar biasa dalam mempertahankan korps satuan antar personilyang memberi semangat komando dan inspirasi bagi penulis.

8. Keluarga besar Part Time Perpustakaan UIN Sunan Kalijaga Yogyakarta Periode 2016, yang telah mewarnai kehidupan penulis selama satu tahun terakhir pengabdian penulis di kampus tercinta ini.

9. Bapak Mulyono Santoso, selaku Kepala Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali, Mas Agus Budi Wijayanto dan Mas Rus serta seluruh keluarga besar Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali yang telah memberikan ijin penelitian bagi penulis hingga selesainya penulisan ini.

10. Citra Marlina Handayani yang selalu memberikan motivasi, senyuman dan bantuannya bagi peneliti.

11. Ukm sahabat, Lina, Indah, Ismah, yang sering memotivasi penulis.
12. Keluarga besar SMP Muhammadiyah 1 Mlati, Pak Bin, Mas Bowo, Mas Ari, serta pembina UKM MA Pandanaran, Bu Sithoh, yang telah memberikan izin kesempatan penulis dalam mendalami dunia pendidikan.
13. Keluarga Markas Besar Afha, Afif, Alfani, Alfian, Faris, Fuad, Mustafid, Saiful, Weddy, yang memberikan semangat, canda tawa, dan saling berbagi satu sama lain.
14. Keluar besar iFree‘12 yang memberikan kenangan indah selama menempuh masa studi.
15. Serta seluruh pihak yang memberikan penulis bantuan, bimbingan, dan do’a yang tidak dapat disebutkan satu persatu.

Semoga segala amal dapat dicatat sebagai amal kebaikan dan dibalas berlipat ganda oleh Allah SWT. *Aamiin.*

Tak ada gading yang tak retak, penulis pun menyadari kritik saran membangun sangat penulis terima dengan senang hati demi menyempurnakan penelitian ini. Semoga penulisan ini dapat bermanfaat bagi seluruh pembaca. Terakhir, penulis memohon maaf apabila terdapat kesalahan dalam penulisan tugas akhir ini.

Yogyakarta, 10 Januari 2017

Penulis

Ami Megantara Prabowo
NIM.12650013

This is The End of Beginning

PERSEMBAHAN

Untuk

1. ***Mama tercinta, yang telah memberikan kasih sayang, pengorbanan dan perhatian yang luar biasa dan doanya demi kesuksesan penulis.***
2. ***Papa yang tanpa lelah menyemangati, mendorong, mendoakan dan memotivasi studi penulis serta tanpa pamrih berkorban materil maupun non materil demi kelancaran penulis.***
3. ***Mba Mia Mba Im yang selalu membimbing dan memotivasi penulis.***

Analisis Keamanan WLAN Terhadap Gangguan ARP Spoofing

(Studi Kasus Kantor Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali)

Ami Megantara Prabowo

NIM.12650013

Intisari

Dalam menganalisis keamanan jaringan di Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali, memerlukan pemeriksaan dari ke tiga hal berikut, yakni Kontrol Manajemen; Kontrol Teknikal; dan Kontrol Operasional. Pemeriksaan dinilai menggunakan konsep kedewasaaan/kematangan (*Maturity Model*) dengan skala 0-5. Pemeriksaan 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 yang didapat beberapa kali penulis dapat menangkap *username* dan *password* yang dikirim dari komputer *client*. Oleh karena itu jaringan *wireless* yang diterapkan di Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali tergolong belum cukup aman dalam hal keamanan jaringan. Dan hasil dari analisis tersebut jaringan *wireless* Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali 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: Keamanan, ARP Spoofing, Analisis Jaringan, WLAN.

WLAN Security Analysis Against ARP Spoofing

(Case Study Department of Culture and Tourism of Boyolali Regency)

Ami Megantara Prabowo

NIM.12650013

Abstract

When analyzing network security at Department of Culture and Tourism Boyolali, will require three inspection, that is Management Controls, Technical Controls and Operational Controls. Assessment using Maturity Concept / Maturity Model with scale from 0 to 5. Examination was followed by Penetration Test using ARP Spoofing method with CommView for Wifi ver.6.3, Aircrack.ng 1.1 and Cain and Abel ver. 4.9.35 for tools. From Penetration Test, several times writer can capture usernames and passwords sent from clien computer. Therefore, wireless network that implemented in Department of Culture and Tourism Boyolali classified as not safe enough in terms of network security. And the result of the analysis of wireless network was classified in "Repeatable but Intuitife" class, which still using basic concept from first instalation and not fully focused yet in terms of network security. Final values is equal to 1.678.

Keyword: *Security, ARP Spoofing, Network Analysis, WLAN.*

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pesatnya teknologi jaringan komputer sampai saat ini tidak terlepas dari sejarah yang melatar belakangi dari waktu kewaktu. Komputer yang terhubung bisa saja menggunakan teknologi trasnmisi dengan media kabel, saluran telepon, gelombang radio, satelit, atau sinar infra merah. Untuk menjalankan satu jaringan, ada beberapa komponen peralatan atau perangkat keras jaringan komputer dan konfigurasi yang harus dilakukan agar jaringan komputer bisa dipakai.

Perjalanan akan kemajuan jaringan komputer dibarengi dengan banyak keuntungan dalam mempermudah pekerjaan manusia. Akan tetapi aspek negatif juga tidak sedikit timbul, seperti kejahatan komputer yang meliputi pencurian data, melakukan suatu interupsi komputer tanpa sepengetahuan pengguna dan sebagainya. Jatuhnya suatu informasi ke tangan pihak lain dapat menimbulkan suatu kerugian bagi pemilik informasi.

Pada dasarnya, jaringan komputer internet yang sifatnya publik dan global tidak aman. Pada saat data terkirim dari suatu komputer ke komputer lainnya, data itu akan melewati sejumlah komputer yang lain yang berarti

akan memberi kesempatan pada pengguna internet yang lain untuk menyadap atau mengubah data tersebut.

Dilain sisi, 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 Kebudayaan dan Pariwisata Kabupaten Boyolali mempunyai tugas pokok untuk melaksanakan urusan kepemerintahan Daerah berdasarkan asas otonomi dan tugas pembantuan di bidang Kebudayaan dan Kepariwisataan.

Dalam melaksanakan tugas pokok tersebut, Dinas Kebudayaan dan Parwisata mempunyai fungsi sebagai penyelenggaraan urusan pemerintahan dan pelayanan umum di bidang kebudayaan dan kepariwisataan, pembinaan dan pelaksanaan tugas bidang kebudayaan dan kepariwisataan serta pengelolaan Unit Pelaksana Teknis Dinas (UPTD). Untuk mendukung kinerja pegawai serta untuk memperlancar program kerja, maka terdapat suatu jaringan WLAN di kantor Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali.

Letak Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali berada di persimpangan jalan utama, yakni jalan Perintis Kemerdekaan dan jalan Ahmad Yani, 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.

Pada penulisan ini, penulis akan mengeksplorasi penyerangan pada kantor Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali dengan menggunakan ARP Spoofing. Pengujian penyerangan ini dilakukan untuk mengetahui cara kerja penyerangan.

1.2 Perumusan Masalah

Masalah yang diambil dari latar belakang tersebut adalah:

1. Bagaimana peta jaringan di Kantor Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali?
2. Bagiamana tingkat keamanan WLAN pada jaringan kantor Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali?
3. Apakah infrastruktur Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali yang ada saat ini sudah mengakomodir kebutuhan akan keamanan jaringan komputer nirkabel?

4. Bagaimana hasil pengujian penetrasi dengan melakukan ARP Spoofing tehadap jaringan di Kantor Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali?

1.3 Batasan Masalah

Batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Pengujian tingkat keamanan berdasarkan acuan audit keamanan oleh *Rao Vallabhaneni.*
2. Data hasil pengujian tingkat keamanan diperoleh dari hasil observasi dan wawancara.
3. Pengujian penetrasi dalam menggunakan ARP Spoofing menggunakan tools atau aplikasi dari CommView dan Cain and Abel untuk menganalisa keamanan jaringan *wireless* di kantor Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali.
4. Pengujian penetrasi menggunakan target 4 komputer.
5. Pengujian tidak bertujuan untuk mengetahui tingkat keamanan suatu website.
6. Tidak melakukan peningkatan keamanan jaringan yang sudah ada dan hanya memberikan saran yang sebaiknya dilakukan .

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk:

1. Memberikan gambaran akan peta jaringan di Kantor Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali.
2. Mengetahui tingkat keamanan WLAN pada jaringan kantor Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali.
3. Mengetahui infrastruktur Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali yang ada saat ini apakah sudah mengakomodir kebutuhan akan keamanan jaringan komputer nirkabel atau belum.
4. Mengetahui hasil pengujian penetrasi dengan melakukan ARP Spoofing tehadap jaringan di Kantor Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali.

1.5 Manfaat Penelitian

Hasil dari penulisan ini seusai penelitian diharapkan penulis dan pihak instansi memperoleh masukan-masukan dan manfaat. Adapun manfaat yang didapat ialah antara lain:

1. Memberikan pemahaman yang baik bagi pengelola manajemen jaringan *wireless* Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali.

2. Membantu memberikan pemahaman kepada karyawan, stackholder, maupun pihak terkait mengenai keamanan jaringan *wireless.*
3. Membantu memberikan gambaran pihak Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali dalam meningkatkan keamanan jaringan yang sudah dipakai.
4. Menjadi acuan penelitian selanjutnya apabila terdapat kesamaan dalam tema penelitian atau adanya keterkaitan dengan keamanan jaringan *wireless* baik dengan objek penelitian Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali maupun yang lainnya.
5. Diharapkan berguna untuk meningkatkan keamanan jaringan WLAN Kantor Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali.

1.6 Kontribusi Penelitian

Kontribusi yang peneliti harapkan adalah untuk memberikan kemajuan wawasan mengenai jaringan WLAN terutama tentang keamanan bagi pegawai dan menambah pengetahuan mengenai perkembangan dan keamanan jaringan komputer di kantor Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali.

1.7 Keaslian Penelitian

Penelitian yang berhubungan dengan Analisis Keamanan WLAN Terhadap Gangguan ARP Spoofing sudah pernah dilakukan sebelumnya, akan tetapi penelitian tentang Analisis Keamanan WLAN Terhadap Gangguan ARP Spoofing pada Kantor Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali sepengetahuan penulis belum pernah dilakukan.

1.8 Sistematika Penulisan

Laporan penelitian tugas akhir ini disusun secara sistematis dan dibagi dalam beberapa bagian bab. Penulisan laporan tugas akhir ini memiliki urutan yang dimulai dari BAB I sampai BAB V.

BAB I. PENDAHULUAN

Bagian ini menerangkan tentang latar belakang, rumusan masalah, batasan penelitian, tujuan penelitian, manfaat penelitian, keaslian penelitian dan sistematika penulisan.

BAB II. TINJAUAN PUSTAKA DAN LANDASAN TEORI

Bagian ini berisi tentang tinjauan pustaka dan landasan teori yang berhubungan dengan topic yang akan dibahas dalam penelitian ini.

BAB III. METODE PENELITIAN

Bagian ini berisi tentang uraian rinci tentang metode penelitian yang memberikan penjelasan mengenai detail langkah-langkah yang dilakukan untuk mencapai tujuan dan simpulan akhir penelitian.

BAB IV. HASIL DAN PEMBAHASAN

Pada bab ini memuat hasil dari penelitian dan pembahasan penelitian yang telah dilakukan.

BAB V. PENUTUP

Bagian ini berisi tentang kesimpulan dan saran-saran untuk penelitian selanjutnya.

BAB V

PENUTUP

5.1 Kesimpulan

Dilihat dari hasil penelitian yang tertulis dari Bab 1 hingga Bab 4, maka kesimpulan yang diapat adalah:

1. Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali menggunakan jaringan *wireless* dengan topologi jaringan infrastruktur dengan 1 wireless *access point* dan Internet Service Provider dari Telkom. Access point yang digunakan yakni dari ZTE serie ZXHN F609 dengan menggunakan enkripsi WPA dan *channel* yang digunakan yakni channel 6. Jumlah perangkat tetap yang digunakan total ada 15 perangkat. Di lantai 1 terdapat 9 perangkat komputer dan di lantai 2 terdapat 6 perangkat.

2. Dalam rangka mengetahui tingkat keamanan WLAN pada Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali, 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 Kebudayaan dan Pariwisata Kabupaten Boyolali adalah 1.6785, yang masuk ke dalam kriteria *Repeatable but Intuitive*. Sedangkan total target kematangan yang diharapkan dari pihak Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali adalah sebesar 2.30357 yang mana masih masuk kriteria *Repeatable but Intuitive*

(berdasarkan Tabel 3.2). Angka ini akan menghasilkan selisih 0.6249 poin dari total poin kematangan akhir terhadap target poin yang diharapkan**.**

3. Infrastruktur jaringan WLAN yang diterapkan Dinas Kebudayaan dan Standar keamanan ternyata belum sepenuhnya dapat mengakomodir kebutuhan akan keamanan WLAN, karena masih ada celah-celah keamanan seperti autentikasi koneksi ke WPA2, kebijakan keamanan dimana sebagai peraturan dasar akan penggunaan jaringan *wireless*, serta penerepan kontrol akses untuk memanajemen klien menjadikan tingkat keamanan memiliki kerentanan terhadap upaya penyalahgunaan oleh pihak yang tidak bertanggung jawab, baik dari pihak internal maupun eksternal. Dari hasil perhitungan diatas, didapatkan kriteria *Repeatable but Intuitive* dimana penerapan keamanan jaringan masih menggunakan konsep sebelumnya atau menggunakan konsep saat pertama penggunaan jaringan tersebut. Hal ini masih tergolong belum cukup aman bagi penggunaan WLAN di lingkungan Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali.

4. Hasil *Penetration Test* yang dilakukan peneliti melalui dua tahap yakni melakukan pembobolan terhadap sandi WPA serta melakukan ARP Spoofing masih bisa dilakukan. Namun dari hasil ARP Spoofing, terdapat beberapa website yang peneliti serta administrator coba untuk diteliti apakah bisa ter-*capture* atau tidak *username* dan *password* yang kami masukkan, ternyata untuk beberapa ada yang bisa dan ada yang hanya ter-*capture username* nya saja, seperti di alibaba.com, atau tidak sama sekali (khususnya website yang memiliki keamanan https) dan diketahui bahwa sebagian besar website yang bisa ter-*capture* adalah website pemerintahan yang memiliki kemungkinan besar untuk diakses oleh

pihak Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali. Hal ini pun menjadikan jaringan *wireless* di kantor Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali rentan akan penyalahgunaan oleh pihak yang tidak bertanggung jawab. Sebagai gambaran apabila keamanan pertama yakni enkripsi WPA telah berhasil ditembus, maka akan tidak aman dari gangguan atau serangan berikutnya seperti pencurian *bandwith*, penyusupan, bahkan penyerangan.

5.2 Saran

Dari hasil kesimpulan penulis menyarankan agar upaya penerapan kebijakan keamanan perlu diadakan dengan membuat kebijakan baru yang diusulkan oleh pihak administrator kepada pimpinan dinas dan diketahui oleh pegawai maupun stakeholder terkait agar pemanfaatan jaringan *wireless* dapat dilaksanakan secara aman. Serta penulis menyarankan agar menerapkan saran yang penulis cantumkan setahap-demi setahap agar peningkatan keamanan dapat terealisasi secara konsisten hingga terpenuhi dari semua *checklist* yang disediakan menurut *Wireless Security Checklist* oleh Rao Vallabhaneni.

Untuk meningkatkan keamanan dalam gangguan *Man in the Middle Attack* khususnya ARP Spoofing, pihak Dinas Kebudayaan dan Pariwisata dapat memasang tools penangkal ARP Spoofing, sebagai contoh ARP Static Changer yang berfungsi mengubah ARP static routing secara otomatis.

Saran bagi peneliti, auditor maupun penulis selanjutnya, agar dapat menerapkan penetration test lebih banyak sebagai bahan evaluasi bagi pihak terkait untuk meningkatkan keamanan jaringan yang dipakai saat penelitian dilaksanakan.

DAFTAR PUSTAKA

Buku

Vallabhaneni, S.Rao. 2008. *Corporate Management, Governance, and Ethics Best Practice*. New Jersey: John Wiley & Sons, Inc.

Buku Pintar Penanganan Jaringan Komputer. Yogyakarta: Andi

Sopandi, Dede. 2010. *Instalasi dan Konfigurasi Jaringan Komputer*. Yogyakarta: Informatika.

Sarno, Riyanarto. 2009. *Audit Sistem informasi & Teknologi Informasi*. Surabaya*:* ITS Press.

Membangun Sistem Jaringan Wireless untuk Pemula. Yogyakarta: Andi Offset.

Arifin, Zaenal. 2005. *Langkah Mudah Membangun Jaringan Komputer*. Yogyakarta: Andi.

S'to. 2015. *Wireless Kungfu Networking & Hacking Edisi 2015*. Penerbit Jasakom.

Zam, Efvy. 2014. *Wireless Hacking Edisi Revisi*. Jakarta: Elex Media Computindo.

Zam, Efvy. 2016. *Buku Sakti Wireless Hacking.* Jakarta: Elex Media Computindo.

Kristanto, Andri. 2003. *Keamanan Data Pada Jaringan Komputer*. Yogyakarta: Gava Media.

Purbo, Onno W. 2000. *Buku Pintar Internet Keamanan Jaringan Internet*. Jakarta: Elex Media Komputindo

Skripsi

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.

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

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.

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.

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.

Jurnal

Rumalutur, Sonny. 2014. "Analisis Keamanan Jaringan Wireless LAN (WLAN) Pada PT. PLN (Persero) Wilayah P2B Area Sorong". *Jurnal Teknologi dan Rekayasa.* Volume 19 No 3. Depok. Fakultas Teknologi Industri Universitas Gunadarma.

Makalah

Nauri, Yogi Ichwan. 2013 "Analisis dan Perancangan Jaringan Komputer Tanpa Hardisk (Diskless) Menggunakan Linux Ubuntu 12.10" *Makalah*. Fakultas Komunikasi dan Informatika Universitas Muhammadiyah Surakarta.

Dewi, Gilang Kumala. 2016. "Anasila Keamanan Jaringan Wireless di Sekolah Menengah al Firdaus" *Makalah*. Fakultas Komunikasi dan Informatika Universitas Muhammadiyah Surakarta.

Nugroho, Bayu Arie. 2012. "Analisis Keamanan Jaringan pada Fasilitas Internet (WIFI) Terhadap Serangan Packet Sniffing". *Makalah*. Fakultas Komunikasi dan Informatika Universitas Muhammadiyah Surakarta.

Dokumen Lainnya

Rachman, Derry Arif. 2014. "Keamanan Sistem Informasi (Studi: Spoofing)". Universitas Komputer Indonesia Bandung

Ismayudi dkk, **"**Analisis Keamanan Jaringan Wifi SMPN 1 Sembawa". Universitas Bina Darma

Tautan

Said, Zulhikam El. 2014. "Teknologi Jaringan Komputer". http://jaringankomputer.org/teknologi-jaringan-komputer/ diakses 19 november 2016 7:09 PM

Ansor, M. Choirul. 2012. "Pemilihan Channel untuk Optimasi Sinyal Wireless" http://appstrack.blogspot.co.id/2012/05/pemilihan-channel-untuk-optimasi-sinyal.html#.V75XAE197IU. 25 Agustus 2016

Wikipedia Indoesia. "Keamanan Komputer" https://id.wikipedia.org/wiki/Keamanan_komputer . 23 November 2016 3:00 PM

Jaelani, Ahmad. 2014. "Metode - Metode Dalam Penelitian" https://sites.google.com/a/student.unsika.ac.id/metodepenelitian-owl/Tugas-updates/metode-metodedalammetodologipeneitian . 24 November 2016 4.53 PM

Priawadi ,Ozi. 2015. "Pengertian Spamming, Snooping, Spoofing, Phising, Jamming dan kawan-kawannya" http://www.priawadi.com/2012/05/pengertian-spamming-snooping-spoofing.html 25 November 2016. 06.00 PM

Comodo. “What is PKI?”

https://www.comodo.com/resources/small-business/digital-certificates1.php 5 Desember 2016 11:13 AM

“User Manager Sebagai Radius Server Wireless & DHCP“

http://mikrotik.co.id/artikel_lihat.php?id=88 6 Desember 2016 10:15 AM

Sanha. 2015. “Pengertian Access Point dan Fungsinya”

http://www.wirelessmode.net/pengertian-access-point-dan-fungsinya.html 6 Desember 2016 9.15 PM

Wikipedia. 2013. ”Kerberos (Protokol)”

https://id.wikipedia.org/wiki/Kerberos_(protokol) . 12 Desember 2016

Tamo Soft. 2016. “Download Commview for Wifi”

http://www.tamos.com/products/commwifi/adapterlist.php

LAMPIRAN

Lampiran A: Daftar Wireless Adapter yang Kompatibel dengan Tools

Daftar Wireless Adapter yang Kompatibel dengan Tools

The following adapters have been tested and are compatible with CommView for WiFi:

802.11ac Adapters

Adapter	802.11 Bands	Form Factor	Supported OS	Limitations or Comments	Sensitivity on a 1-5 scale
Alfa Networks AWUS036ACH	2.4 GHz/5 GHz	USB	Windows 7 or higher	See tech. notes	3
Belkin F9L1109 v1	2.4 GHz/5 GHz	USB	Windows 7 or higher	Recommended See tech. notes	4
Buffalo AC866 (WI-U2-866D)	2.4 GHz/5 GHz	USB	Windows 7 or higher	See tech. notes	4
D-Link DWA-180 rev A1	2.4 GHz/5 GHz	USB	Windows 7 or higher	See tech. notes	4
D-Link DWA-182 rev A1	2.4 GHz/5 GHz	USB	Windows 7 or higher	See tech. notes	4
D-Link DWA-182 rev C1	2.4 GHz/5 GHz	USB	Windows 7 or higher	Recommended See tech. notes	5
Edimax EW-7822UAC BEST	2.4 GHz/5 GHz	USB	Windows 7 or higher	Recommended See tech. notes	5
EnGenius EUB1200AC	2.4 GHz/5 GHz	USB	Windows 7 or higher	See tech. notes	3
IKross AC1200	2.4 GHz/5 GHz	USB	Windows 7 or higher	See tech. notes	3
Intel AC 3160, 3165	2.4 GHz/5 GHz	Integrated	Windows 7 or higher	Recommended See tech. notes	Not rated *
Intel AC 7260, 7265	2.4 GHz/5 GHz	Integrated	Windows 7 or higher	Recommended See tech. notes	Not rated *
Intel AC 8260	2.4 GHz/5 GHz	Integrated	Windows 7 or higher	Recommended See tech. notes	Not rated *
Linksys WUSB6300 BEST	2.4 GHz/5 GHz	USB	Windows 7 or higher	Recommended See tech. notes	4
NETGEAR A6200	2.4 GHz/5 GHz	USB	Windows 7 or higher	See tech. notes	4
NETGEAR A6210	2.4 GHz/5 GHz	USB	Windows 8 or higher	Recommended See tech. notes	5
Proxim ORiNOCO 9100 BEST	2.4 GHz/5 GHz	USB	Windows 7 or higher	Recommended See tech. notes	5
Qualcomm Atheros 61x4, 9377, and 988x	2.4 GHz/5 GHz	Integrated	Windows 7 or higher	Recommended	Not rated *
Rosewill RNX-AC1200UB	2.4 GHz/5 GHz	USB	Windows 7 or higher	See tech. notes	3

802.11ac Adapters

Adapter	802.11 Bands	Form Factor	Supported OS	Limitations or Comments	Sensitivity on a 1-5 scale
TP-LINK Archer T4U	2.4 GHz/5 GHz	USB	Windows 7 or higher	See tech. notes	4
TP-LINK Archer T4UH	2.4 GHz/5 GHz	USB	Windows 7 or higher	Recommended See tech. notes	5
TRENDnet TEW-805UB	2.4 GHz/5 GHz	USB	Windows 7 or higher	See tech. notes	3
ZyXEL AC240 BEST	2.4 GHz/5 GHz	USB	Windows 7 or higher	Recommended See tech. notes	5

802.11n Adapters

Adapter	802.11 Bands	Form Factor	Supported OS	Limitations or Comments	Sensitivity on a 1-5 scale
Atheros AR5008, AR5009, AR92xx	2.4 GHz or 2.4/5 GHz	Integrated	XP or higher	See tech. notes	Not rated *
Atheros AR9380, AR9382, AR9390	2.4 GHz/5 GHz	Integrated	Windows 7 or higher	Recommended	Not rated *
Atheros AR9485	2.4 GHz only	Integrated	Windows 7 or higher		Not rated *
Atheros AR9462 (aka WB222, AR5BMD222)	2.4 GHz/5 GHz	Integrated	Windows 7 or higher	Recommended	Not rated *
Atheros AR956x, AR958x	2.4 GHz/5 GHz	Integrated	Windows 7 or higher	Recommended	Not rated *
Broadcom 802.11n	2.4 GHz or 2.4/5 GHz	Integrated	Vista or higher	See tech. notes	Not rated *
D-Link DWA-160 v.A1 and v.A2	2.4 GHz/5 GHz	USB	XP or higher		4
D-Link DWA-160 v.B2 and v.C1 BEST	2.4 GHz/5 GHz	USB	Windows 7 or higher	Recommended	5
D-Link DWA-643	2.4 GHz only	ExpressCard	XP or higher		3
Dell Wireless 1505, 1510, 1515, 1520, 1530, 1540	2.4 GHz/5 GHz	Integrated	Vista or higher	See tech. notes	4
Dell Wireless 1702	2.4 GHz only	Integrated	XP or higher		4
Edimax EW-7733UnD BEST	2.4 GHz/5 GHz	USB	Windows 7 or higher	Recommended	4
Intel 1000	2.4 GHz only	Integrated	Windows 7 - 8.1	See tech. notes	4
Intel 4965	2.4 GHz/5 GHz	Integrated	Vista or Windows 7	See tech. notes	5

802.11n Adapters

Adapter	802.11 Bands	Form Factor	Supported OS	Limitations or Comments	Sensitivity on a 1-5 scale
Intel 5100, 5150, 5300, 5350	2.4 GHz/5 GHz	Integrated	Windows 7 - 8.1	See tech. notes	5
Intel 6200, 6250, 6300, 6350	2.4 GHz/5 GHz	Integrated	Windows 7 - 8.1	See tech. notes	5
Intel N 7260, 7265	2.4 GHz/5 GHz	Integrated	Windows 7 or higher	Recommended See tech. notes	Not rated *
Linksys AE2500	2.4 GHz/5 GHz	USB	Vista or higher	See tech. notes	5
Linksys AE3000	2.4 GHz/5 GHz	USB	Windows 7 or higher		4
Linksys WEC600N	2.4 GHz/5 GHz	ExpressCard	Vista or higher	See tech. notes	4
Linksys WUSB600N	2.4 GHz/5 GHz	USB	Vista or higher	See tech. notes	3
NETGEAR WN111 v2	2.4 GHz only	USB	XP or higher	See tech. notes	5
NETGEAR WNDA3100 v1	2.4 GHz/5 GHz	USB	XP or higher		4
NETGEAR WNDA3100 v2	2.4 GHz/5 GHz	USB	Vista or higher	See tech. notes	4
Proxim ORiNOCO 8494	2.4 GHz/5 GHz	USB	XP or higher	Recommended	5
SMC Networks SMCWUSB-N2	2.4 GHz only	USB	XP or higher		5
Sony UWA-BR100	2.4 GHz/5 GHz	USB	Windows 7 or higher	See tech. notes	4
TP-Link TL-WDN3200 BEST	2.4 GHz/5 GHz	USB	Windows 7 or higher	Recommended	5
TP-Link TL-WN721N and WN722N	2.4 GHz only	USB	Windows 7 or higher	See tech. notes	4
TP-Link TL-WN821N v1 and v2	2.4 GHz only	USB	XP or higher		5
TP-Link TL-WN821N v3	2.4 GHz only	USB	Windows 7 or higher	See tech. notes	4
TP-Link TL-WN822N v1	2.4 GHz only	USB	XP or higher		5
TP-Link TL-WN822N v2	2.4 GHz only	USB	Windows 7 or higher	See tech. notes	4
Ubiquiti SR71X	2.4 GHz/5 GHz	ExpressCard	XP or higher		5
Ubiquiti SR71-USB	2.4 GHz/5 GHz	USB	XP or higher		5
CACE AirPcap Nx USB	2.4 GHz/5 GHz	USB	XP or higher	See tech. notes	4

Lampiran B: *Wireless Security Checklist Target Value*

WIRELESS SECURITY CHECKLIST

by RAO VALLABHANENI

No	Type	Procedure	Maksud/Point	Value	Notes
1.	Management Control	Develop an agency security policy that addresses the use of wireless technology, including 802.11.	Poin ini memeriksa apakah objek telah menerbitkan kebijakan keamanan yang berhubungan dengan penggunaan teknologi wireless termasuk di dalamnya teknologi 802.11 (*WIreless LAN*) di lingkungan jaringan wireless Disbudpar Boyolali.	1	Memulai membuat suatu buku kebijakan khusus dalam hal pemakaian (aturan, penggunaan, batasan dll) teknologi wireless.
2.	Management Control	Ensure that users on the network are fully trained in computer security awareness and the risks associated with wireless technology.	Di poin ini memastikan bahwa para pengguna yang terjalin dalam jaringan telah sepenuhnya terlatih dalam hal pentingnya keamanan komputer dan telah memahami resiko akan penggunaan teknologi wireless.	3	Peningkatan dan lebih dirutinkan dalam latihan dan pemahamanan *wireless technology*.

3.	Management Control	Perform a risk assessment to understand the value of the asset in the ageny that need protection.	Poin ini untuk mengetahui nilai dan memastikan apakah aset peralatan membutuhkan suatu perlindungan	5	Sudah terasetkan dan lebih didetailkan serta terdaftar secara online
4.	Management Control	Ensure that the client NIC and AP support firmware upgrade so that security patches may be deployed as they become avaliable (prior to purchase).	Di poin ini memastikan bahwa pembaharuan firmware dari kartu jaringan (Network Interface Controler) dan access point telah dilakukan sehingga patch keamanan sudah dapat digunakan ketika pembaharuan itu tersedia.	5	Pembaruan diharapkan dapat terpantau secara realtime dari meja administrator.
5.	Management Control	Perform comprehensive security assessment at regular and random intervals (including validating that rogue APs do not exist in the 802.11 WLAN) to fully understand the wireless network security posture.	Poin ini memastikan telah ditinjaunya penilaian keamanan pada waktu berkala maupun di sembarang waktu guna mengetahui bagaimana keadaan keamanan jaringan wireless	2	harapannya penilaian terhadap jaringan wireless terutama disisi keamanan serta pengecekan terhadap rouge access point bisa dimulai.

6.	Management Control	Ensure that external boundary protection is in place around the perimeter of the building or buildings of the agency.	Poin ini memastikan bahwa apakah pihak kantor Disbudpar Kabupaten Boyolali sudah memiliki keamanan terhadap gedung di batas luarnya atau belum.	5	Tergantung kebijakan pemerintah pusat. Namun saat ini sudah ada pengamanan baik dari sdm maupun secara fisik.
7.	Management Control	Deploy physical access controls of the building and other secure areas (e.g., photo ID, card badge readers).	Poin ini memastikan bahwa pihak kantor Disbudpar telah meluncurkan akses kontrol	5	Pemindai retina dan kartu id sudah ada, dan data sudah terkirim ke pusat.
8.	Management Control	Complete a site survey to measure and establish the AP coverage for the agency.	Point ini membahas tentang cakupan lokasi yang ada di tiap *access point* dengan mengukur dan menetapkan cakupan untuk agent.	1	Penilaian terhadap lingkup harusnya dimulai karena jangkauan sinyal wireless hingga halaman gedung sudah mulai melemah.

9.	Management Control	Take a complete inventory of all APs and 802.11 wireless devices.	Poin ini memastikan bahwa kantor Disbudpar Kabupaten Boyolali telah melakukan inventarisasi terhadap semua perlengkapan wireless 802.11	5	Inventarisasi dapat dilakukan secara otomatis dan terdaftar di database, sehingga administrator dapat memantau secara realtime.
10.	Management Control	Ensure that wireless networks are not used untel they comply with the agency's security policy.	Poin ini memastikan bahwa jaringan w*ireless* berjalan sesuai dengan kebijakan yang ada.	1	pemakaian jaringan *wireless* diharapkan digunakan berdasarkan kebijakan dalam pemakaian jaringan *wireless* agar keselamatan akan keamanan jaringan bisa lebih dijaga.

11.	Management Control	Locate APs on the interior of buildings instead of near exterior walls and windows as appropriate.	Point ini memastikan bahwa *access point* di tempatkan pada interior bangunan, bukan pada dinding eksterior atau dengan jendela.	4	Harapannya bisa digantung/ di luar jangkauan user biasa.
12.	Management Control	Place APs in secured areas to prevent unauthorized physical access and user manipulation.	Poin ini memastikan bahwa access point diletakkan di area yang aman	4	*Sama dengan atas.*
13.	Technical Control	Empirically test AP range boundaries to determine the precise extent of the wireless coverage.	Point ini menguji batas dari jangkauan *access point* yang ada di lapangan untuk menentukan jarak optimal dari jaringan *wireless* tersebut	3	access point bisa lebih optimal.
14.	Technical Control	Make sure that APs are turned off during when they are not used (e.g., after hours and on weekends).	memastikan bahwa access point dalam posisi mati (off) saat access point sedang tidak digunakan	0	access point belum bisa dimatikan selepas jam kerja selesai. Karena terhubung dengan telepon.

15.	Technical Control	Make sure that the reset function on APs is being used only when needed and is only invoked by an authorized grup of people.	Point ini memastikan bahwa fungsi reset di halaman *administrator acssess point* hanya boleh digunakan oleh pihak yang berwenang	3	sudah dioperasikan oleh satu orang petugas yang berwenang.
16.	Technical Control	Restore the APs to the latest security setting when the reset functions are used.	Point ini memastikan pengaturan keamanan *access point* berada pada kondisi keamanan terbaru ketika fungsi *reset* digunakan.	1	Belum pernah di reset, akan tetapi administrator mencoba untuk meninjau kembali ketika reset digunakan.
17.	Technical Control	Change the default SSID in the APs.	Point ini memastikan bahwa *default* SSID (*service set identifier) dan* IP Address dari produsen WAP telah diganti	4	Sudah diganti "Disbudpar". Dan kedepannya tetap seperti ini.
18.	Technical Control	Disable the broadcast SSID feature so that the client SSID	Point ini memastikan fitur SSID *broadcast*	0	SID broadcast masih dalam kondisi aktif,

		must match that of the AP.	tidak di aktifkan		dan tetap aktif untuk memudahkan pegawai.
19.	Technical Control	Validate that the SSID character string does not reflect the agency's name (division, department, street, etc) or product.	Poin ini memastikan bahwa karakter dari SSID tidak mencerminkan pihak Disbudpar Boyolali	2	SSID memang dibuat secara tidak langsung mencerminkan nama kantor agar pegawai termudahkan.
20.	Technical Control	Ensure that AP channels are at least five channels different from any other nearby wireless networks to prevent interference.	Memastikan bahwa setidaknya ada lima (5) channel dari access point berbeda yang digunakan	2	pihak Disbudpar hanya menggunakan 1 channel. Dan kedepan belum ada penambahan hingga 5 AP.
21.	Technical Control	Understand and make sure that all default parameters are	Point ini memastikan bahwa seluruh parameter default telah dirubah dan sudah dipahami	3	parameter default dirubah menyesuaikan

		changed.			dengan kemudahan pegawai (SSID, sandi *wifi,* dll).
22.	Technical Control	Disable all insecure and nonessential manaement protocols on the APs.	Memastikan bahwa seluruh protokol yang tidak aman dan yang tidak penting dalam access point sudah dalam posisi tidak aktif	0	Kedepannya protokol yang masih belum aman (DHCP) memang masih digunakan.
23.	Technical Control	Enable all security features of the WLAN product, including the cryptographic authentcation and WEP privacy feature.	Poin in memastikan fitur keamanan semua produk WLAN termasuk autentikasi kriptografi dan WEP telah diaktifkan	3	Harapannya fitur otentikasi sebelum mengakses perangkat WLAN diaktifkan seperti saat penelitian ini dibuat.
24.	Technical Control	Ensure that encryption key sizes are at least 128-bits or as large as possible	ukuran sandi enkripsi sekurang-kurangnya 128-bit atau lebih besar	0	Penggunaan sandi 128-bit tidak diinginkan mengingat untuk kemudahan

					pegawai.
25.	Technical Control	Make sure that default shared keys are periodically replaced by more secure unique keys.	memastikan bahwa sandi yang telah dibagikan bagi pegawai Disbudpar Kabupaten Boyolali agar diganti secara berkala dengan kombinasi unik	2	Kedepannya tetap tidak menggunakan kombinasi unik (penggabungan huruf kecil - besar, angka, ataupun tanda baca) hanya menggunakan kata-kata unik.
26.	Technical Control	Install a properly configured firewall between the wired infrastructure and the wireless network (AP or hub to APs).	Poin ini memastikan bahwa firewall di tiap access point sudah ter-install dengan benar antara jaringan kabel dan nirkabel	1	penggunaan firewall di *access point* bisa mulai diterapkan.
27.	Technical Control	Install antivirus software on all wireless clients.	Poin ini memastikan software antivirus sudah terinstall di seluruh client.	5	Seluruh client dapat mengatur antivirus secara otomatis dan berkala.

28.	Technical Control	Install personal firewall software on all wireless clients.	Poin ini memastikan bahwa software firewall sudah terinstall di seluruh client yang menggunakan wifi.	0	Belum ada rencana tentang firewall .
29.	Technical Control	Disable file sharing on wireless clients (especially in untrusted environments).	Poin ini memastikan bahwa fitur file sharing dalam jaringan wireless sudah dinonaktifkan	3	fitur file sharing dinonaktifkan dan menggunakan server.
30.	Technical Control	Deploy MAC access control lists.	memastikan bahwa fitur *control list* Mac Address sudah di aktifkan	0	fitur control list Mac Address memang tidak akan diaktifkan
31.	Technical Control	Consider installation of Layer 2 switches in lieu of hubs for AP connectivity.	Memastikan bahwa pemasangan layer 2 Switch sebagai pengganti Hub sudah direncakanan/dilaksanakan sebagai konektifitas bagi access point	1	infrastruktur jaringan di Disbudpar Kabupaten Boyolali bisa menggunakan switch
32.	Technical Control	Deploy IPsec-based Virtual Private Network (VPN) technology for wireless	Poin ini memastikan bahwa fitur IPsec berdasarkan teknologi VPN telah digunakan.	1	penggunaan IP security berbasis VPN bisa mulai

		communications.			diterapkan
33.	Technical Control	Ensure that encryption being used is sufficient given the sensitivity of the data on the network and the processor speeds of the computer.	Memastikan bahwa penggunaan enkripsi sudah dirasa cukup dilihat dari kemampuan prosesor dan kesensitifan data.	3	Sampai saat ini baru enkripsi WPA dan komputer tidak terbebani dan kedepannya penggunaan enkripsi bisa dioptimalkan.
34.	Technical Control	Fully test and deploy software patches and upgrades on a regular basis.	Memastikan bahwa seluruh perangkat lunak yang digunakan telah di update secara berkala.	5	Update bisa dilakukan secara berkala dan otomatis.
35.	Technical Control	Ensure taht all APs have strong administrative passwords.	Poin ini memastikan bahwa semua *Access Point* memiliki *password* yang kuat.	3	Sandi bisa diubah dan dikondisikan apabila ada pergantian administrator.

36.	Technical Control	Ensure that all passwords are being changed regularly	memastikan bahwa semua sandi yang ada dalam penggunaan wifi telah diganti secara berkala.	1	Kedepannya memang jarang dirubah secara berkala untuk memudahkan pegawai.
37.	Technical Control	Deploy user authentication such as biometrics, smart cards, two-factor authentication and PKI	Poin ini menjelaskan tentang penggunaan otentikasi seperti biometri, *smart card,* autentikasi dua faktor dan PKI.	1	Autentikasi pengguna seperti tersebut bisa mulai diterapkan.
38.	Technical Control	Ensure that the “ad hoc mode” for 802.11 has been disabled unless the environment is such that the risk is tolerable. Note: some products do not allow disabling this feature; use with caution or use different vendor.	Poin ini memastikan bahwa mode ad hoc untuk penggunaan wifi 802.11 telah dinonaktifkan.	3	Kedepannya tetap tidak diaktifkan.
39.	Technical Control	Use static IP addressing on	Menggunakan IP Statis dalam alamat network.	0	Kedepannya penggunaan ip

		network.			address secara static tidak diterapkan.
40.	Technical Control	Disable DHCP.	Menonaktifkan DHCP.	0	Kedepannya protokol DHCP tetap diterapkan di jaringan wireless Disbudpar Kabupaten Boyolali. Karena perangkat mobile (laptop, smartphone) bisa bertambah atau berkurang.
41.	Technical Control	Enable user authentication mechanism for the management interfaces of the AP.	Poin ini melakukan peninjauan, bahwa mekanisme otentikasi user untuk antar muka manajemen WAP diaktifkan.	4	Tetap.
42.	Technical Control	Ensure that management traffic destined for APs is on a	memastikan bahwa arus yang menuju ke access point telah menggunakan kabel khusus subnet.	3	kabel khusus yang menghubungkan access point sudah

		dedicated wired subnet.			terpasang
43.	Technical Control	Use SNMPv3 and / or SSL/TLS for web-based management of APs.	Poin ini memastikan bahwa penggunaan SNMPv3 dan atau SSL/TLS dalam pengaturan secara web untuk access point telah diterapkan.	1	Penggunaan fitur SNMPv3 ataupun SSL/ TLS dalam manajemen access point bisa mulai dipakai oleh Disbudpar Kabupaten Boyolali.
44.	Operational Control	Configure SNMP Settings on APs for least privilege (I.e.,read only). Disable SNMPv1 and SNMPv2 are not recommended.	Poin ini memastikan bahwa fitur pengaturan dalam SNMP untuk acccess point sudah diaktifkan sepenuhnya. Baik yang versi 1 atau versi 2.	1	Penggunaan SNMP bisa mulai diterapkan.
45.	Operational Control	Enhance AP management traffic security by using SNMPv3 or equivalent	Poin ini bermaksud untuk meningkatkan manajemen lalu lintas keamanan dengan menggunakan protocol cryptography yang	1	Manajemen SNMPv3 bisa mulai

		cryptographically protected protocol.	dilindungi SNMPv3		diterapkan.
46.	Operational Control	Use a local serial port interface for AP configuration to minimize the exposure of sensitive management information.	Poin ini memastikan bahwa interface pada local serial port untuk konfigurasi access point telah digunakan untuk meminimalisir terjadinya kebocoran informasi manajemen yang sensitif.	3	Kedepannya tetap seperti ini.
47.	Operational Control	Consider other forms of authentication for wireless network such as RADIUS and Kerberos	Poin ini melakukan peninjauan terhadap bentuk lain autentikasi pada jaringan nirkabel seperti *Radius server* dan *Kerberos*	1	penggunaan otentikasi untuk jaringan wireless bisa dimulai/diterapkan user autentikasi baik dari Radius maupun Kerberos.
48.	Operational Control	Deploy intrusion detection agents on the wireless part of the network to detect suspisious behavior or unauthorized	Poin ini memastikan bahwa telah digunakannya suatu fitur (IDS) yang dapat mendeteksi adanya suatu akses mencurigakan atau akses yang tidak sah dalam aktifitas di	1	Kedepannya bisa mulai diterapkan.

		access and activity.	jaringan wireless.		
49.	Operational Control	Deploy auditing technology to analyze the records produced by RADIUS for suspicious activity.	Poin ini memastikan bahwa penggunaan audit untuk menganalisis seluruh rekam aktifitas yang dihasilkan oleh RADIUS dalam hal aktifitas yang mencurigakan sudah dilaksanakan	2	Penggunaan audit dalam meningkatkan sistem keamanan oleh RADIUS bisa mlai diterapkan.
50.	Operational Control	Deploy an 802.11 security product that offers other security features such as enhanced cryptographic protection or user authorization features.	Poin ini memastikan bahwa penggunaan keamanan dalam teknologi 802.11 yang menawarkan berbagai fitur keamanan seperti perlindungan dengan kriptografi atau fitur otorisasi pengguna telah digunakan.	2	Kedepannya penerapan teknologi produk keamanan dari 802.11 bisa digunakan.
51.	Operational Control	Enable utilization of key-mapping keys (802.1) rather than default keys so that sessions use distinct WEP keys	Poin ini memastikan bahwa penggunaan sandi key-mapping (802.1) telah dilakukan sehingga ketika session habis sudah menggunakan sandi yang berbeda menggunakan sandi WEP.	2	kedepannya untuk fitur session bisa diterapkan.

52.	Operational Control	Fully understand the impacts of deploying any security feature or product prior to deployment.	Memastikan operator atau pun pihak yang terkait telah mengerti secara penuh mengenai dampak dari penggunaan berbagai macam fitur keamanan atau fitur yang sebelumnya pernah dipakai untuk Disbudpar Kabupaten Boyolali.	5	Kedepannya pihak administrator dan pihak terkait mengerti tentang dampak penggunaan fitur keamanan yang sebelumnya hingga sampai saat penelitian ini dibuat secara bertahap.
53.	Operational Control	Designate an individual to track the progress of 802.11 security products and standarts (IETF, IEEE, etc.) and the threats and vulnerabilities with the technology	Poin ini memastikan bahwa penunjukan seseorang sebagai pengamat kemajuan teknologi di bidang nirkabel 802.11 terutama dalam hal keamanan dan standar internasional yang sudah ada	2	Kedepannya penunjukan secara khusus seseorang yang memahami seluk beluk kemajuan 802.11 terutama di bidang keamanan bisa diadakan. Tugas dari administrator

					sendiri hanya mengatur lancarnya jaringan wireless Disbudpar Kabupaten Boyolali.
54.	Operational Control	Wait until future release of 802.11 WLAN technologies incorporate fixes to the security features or provide enhanced security features.	Poin ini memastikan bahwa menantikan penggunaan fitur keamanan dari teknologi 802.11 terbaru untuk memperbaiki atau menyempurnakan fitur keamanan terkini.	4	Tetap.
55.	Operational Control	When disposing access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.	Poin ini memastikan bahwa ketika access point sudah tidak dipergunakan lagi oleh pihak Disbudpar Kabupaten Boyolali, maka oleh pihak terkait sudah melakukan penghapusan atau pengembalian ulang (reset) access point.	5	Kedepannya tetap dilaksanakan secara terstruktur

56.	Operational Control	If the access points supports logging,turn it on and review thelogs on a regular basis.	Poin ini memastikan bahwa jika access point mendukung fitur logging, maka sudah diaktifkan dan hasil dari log tersebut ditinjau secara teratur.	1	Fitur logging bisa mulai diaktifkan
Total				**129 point**	

Lampiran C: *Wireless Security Checklist Reality Value*

WIRELESS SECURITY CHECKLIST

by RAO VALLABHANENI

No	Type	Procedure	Maksud/Point	Value	Notes
1.	Management Control	Develop an agency security policy that addresses the use of wireless technology, including 802.11.	Poin ini memeriksa apakah objek telah menerbitkan kebijakan keamanan yang berhubungan dengan penggunaan teknologi wireless termasuk di dalamnya teknologi 802.11 (*WIreless LAN*) di lingkungan jaringan wireless Disbudpar Boyolali.	0	agar dibuat suatu buku acuan mengenai keamanan dan resiko penggunaan jaringan wireless
2.	Management Control	Ensure that users on the network are fully trained in computer security awareness and the risks associated with wireless technology.	Di poin ini memastikan bahwa para pengguna yang terjalin dalam jaringan telah sepenuhnya terlatih dalam hal pentingnya keamanan komputer dan telah memahami resiko akan penggunaan teknologi wireless.	3	Agar dilakukan penyuluhan di tiap pengguna agar lebih mandiri

3.	Management Control	Perform a risk assessment to understand the value of the asset in the ageny that need protection.	Poin ini untuk mengetahui nilai dan memastikan apakah aset peralatan membutuhkan suatu perlindungan	4	Sudah terasetkan
4.	Management Control	Ensure that the client NIC and AP support firmware upgrade so that security patches may be deployed as they become avaliable (prior to purchase).	Di poin ini memastikan bahwa pembaharuan firmware dari kartu jaringan (Network Interface Controler) dan access point telah dilakukan sehingga patch keamanan sudah dapat digunakan ketika pembaharuan itu tersedia.	2	
5.	Management Control	Perform comprehensive security assessment at regular and random intervals (including validating that rogue APs do not exist in the 802.11 WLAN) to fully understand the wireless network security posture.	Poin ini memastikan telah ditinjaunya penilaian keamanan pada waktu berkala maupun di sembarang waktu guna mengetahui bagaimana keadaan keamanan jaringan wireless	0	sebaiknya penilaian terhadap jaringan wireless terutama disisi keamanan serta pengecekan terhadap rouge access point bisa dimulai.

6.	Management Control	Ensure that external boundary protection is in place around the perimeter of the building or buildings of the agency.	Poin ini memastikan bahwa apakah pihak kantor Disbudpar Kabupaten Boyolali sudah memiliki keamanan terhadap gedung di batas luarnya atau belum.	5	
7.	Management Control	Deploy physical access controls of the building and other secure areas (e.g., photo ID, card badge readers).	Poin ini memastikan bahwa pihak kantor Disbudpar telah meluncurkan akses kontrol	4	
8.	Management Control	Complete a site survey to measure and establish the AP coverage for the agency.	Point ini membahas tentang cakupan lokasi yang ada di tiap *access point* dengan mengukur dan menetapkan cakupan untuk agent.	0	seberapa efektifnya penggunaan jaringan wirelese dalam hal jangkauan sinyal.
9.	Management Control	Take a complete inventory of all APs and 802.11 wireless devices.	Poin ini memastikan bahwa kantor Disbudpar Kabupaten Boyolali telah melakukan inventarisasi terhadap semua perlengkapan wireless 802.11	3	
10.	Management	Ensure that wireless networks	Poin ini memastikan bahwa jaringan w*ireless*	0	sebaiknya pemakaian

	Control	are not used untel they comply with the agency's security policy.	berjalan sesuai dengan kebijakan yang ada.		jaringan wireless tidak digunakan terlebih dahulu sebelum kebijakan dalam pemakaian jaringan wireless agar keselamatan akan keamanan jaringan bisa lebih dijaga
11.	Management Control	Locate APs on the interior of buildings instead of near exterior walls and windows as appropriate.	Point ini memastikan bahwa *access point* di tempatkan pada interior bangunan, bukan pada dinding eksterior atau dengan jendela.	4	
12.	Management Control	Place APs in secured areas to prevent unauthorized physical access and user manipulation.	Poin ini memastikan bahwa access point diletakkan di area yang aman	3	access point berada di tengah gedung dan bersebelahan dengan administrator

13.	Technical Control	Empirically test AP range boundaries to determine the precise extent of the wireless coverage.	Point ini menguji batas dari jangkauan *access point* yang ada di lapangan untuk menentukan jarak optimal dari jaringan *wireless* tersebut	3	access point melebihi batas optimal
14.	Technical Control	Make sure that APs are turned off during when they are not used (e.g., after hours and on weekends).	memastikan bahwa access point dalam posisi mati (off) saat access point sedang tidak digunakan	0	access point tidak dimatikan selepas jam kerja selesai
15.	Technical Control	Make sure that the reset function on APs is being used only when needed and is only invoked by an authorized grup of people.	Point ini memastikan bahwa fungsi reset di halaman *administrator acssess point* hanya boleh digunakan oleh pihak yang berwenang	3	sudah dioperasikan oleh satu orang petugas yang berwenang
16.	Technical Control	Restore the APs to the latest security setting when the reset functions are used.	Point ini memastikan pengaturan keamanan *access point* berada pada kondisi keamanan terbaru ketika fungsi *reset* digunakan.	1	Belum pernah di reset, akan tetapi administrator mencoba untuk meninjau kembali

					ketika reset digunakan
17.	Technical Control	Change the default SSID in the APs.	Point ini memastikan bahwa *default* SSID (*service set identifier) dan* IP Address dari produsen WAP telah diganti	4	Sudah diganti "Disbudpar"
18.	Technical Control	Disable the broadcast SSID feature so that the client SSID must match that of the AP.	Point ini memastikan fitur SSID *broadcast* tidak di aktifkan	0	SID broadcast masih dalam kondisi aktif
19.	Technical Control	Validate that the SSID character string does not reflect the agency's name (division, department, street, etc) or product.	Poin ini memastikan bahwa karakter dari SSID tidak mencerminkan pihak Disbudpar Boyolali	2	SSID secara tidak langsung masih mencerminkan nama kantor
20.	Technical Control	Ensure that AP channels are at least five channels different from any other nearby wireless networks to prevent	Memastikan bahwa setidaknya ada lima (5) channel dari access point berbeda yang digunakan	2	pihak Disbudpar hanya menggunakan 1 channel.

		interference.			
21.	Technical Control	Understand and make sure that all default parameters are changed.	Point ini memastikan bahwa seluruh parameter default telah dirubah dan sudah dipahami	3	beberapa parameter default sudah dirubah
22.	Technical Control	Disable all insecure and nonessential manaement protocols on the APs.	Memastikan bahwa seluruh protokol yang tidak aman dan yang tidak penting dalam access point sudah dalam posisi tidak aktif	1	terdapat protokol yang masih belum aman
23.	Technical Control	Enable all security features of the WLAN product, including the cryptographic authentcation and WEP privacy feature.	Poin in memastikan fitur keamanan semua produk WLAN termasuk autentikasi kriptografi dan WEP telah diaktifkan	3	fitur otentikasi sebelum mengakses perangkat WLAN telah diaktifkan
24.	Technical Control	Ensure that encryption key sizes are at least 128-bits or as large as possible	ukuran sandi enkripsi sekurang-kurangnya 128-bit atau lebih besar	0	ukuran sandi masih kurang dari 128-bit
25.	Technical Control	Make sure that default shared keys are periodically replaced	memastikan bahwa sandi yang telah dibagikan bagi pegawai Disbudpar Kabupaten Boyolali agar diganti secara berkala dengan kombinasi	2	belum menggunakan kombinasi unik (penggabungan huruf

		by more secure unique keys.	unik		kecil - besar, angka, ataupun tanda baca) hanya sudah menggunakan kata-kata unik
26.	Technical Control	Install a properly configured firewall between the wired infrastructure and the wireless network (AP or hub to APs).	Poin ini memastikan bahwa firewall di tiap access point sudah ter-install dengan benar antara jaringan kabel dan nirkabel	0	penggunaan firewall di access point masih belum diterapkan
27.	Technical Control	Install antivirus software on all wireless clients.	Poin ini memastikan software antivirus sudah terinstall di selurh client.	3	didapati bahwa antivirus di tiap client sudah di aktifkan
28.	Technical Control	Install personal firewall software on all wireless clients.	Poin ini memastikan bahwa software firewall sudah terinstall di seluruh client yang menggunakan wifi.	2	firewall yang dari windows saja yang masih diaktifkan
29.	Technical Control	Disable file sharing on wireless clients (especially in untrusted	Poin ini memastikan bahwa fitur file sharing dalam jaringan wireless sudah dinonaktifkan	0	fitur file sharing masih aktif

		environments).			
30.	Technical Control	Deploy MAC access control lists.	memastikan bahwa fitur *control list* Mac Address sudah di aktifkan	0	fitur control list Mac Address belum diaktifkan
31.	Technical Control	Consider installation of Layer 2 switches in lieu of hubs for AP connectivity.	Memastikan bahwa pemasangan layer 2 Switch sebagai pengganti Hub sudah direncakanan/dilaksanakan sebagai konektifitas bagi access point	0	infrastruktur jaringan di Disbudpar Kabupaten Boyolali belum menggunakan switch
32.	Technical Control	Deploy IPsec-based Virtual Private Network (VPN) technology for wireless communications.	Poin ini memastikan bahwa fitur IPsec berdasarkan teknologi VPN telah digunakan.	0	penggunaan IP security berbasis VPN belum diterapkan
33.	Technical Control	Ensure that encryption being used is sufficient given the sensitivity of the data on the network and the processor	Memastikan bahwa penggunaan enkripsi sudah dirasa cukup dilihat dari kemampuan prosesor dan kesensitifan data.	2	Sampai saat ini baru enkripsi WPA dan komputer tidak terbebani

		speeds of the computer.			
34.	Technical Control	Fully test and deploy software patches and upgrades on a regular basis.	Memastikan bahwa seluruh perangkat lunak yang digunakan telah di update secara berkala.	2	Masih menggunakan versi yang lama
35.	Technical Control	Ensure taht all APs have strong administrative passwords.	Poin ini memastikan bahwa semua *Access Point* memiliki *password* yang kuat.	2	sandi yang digunakan masih menggunakan sandi default
36.	Technical Control	Ensure that all passwords are being changed regularly	memastikan bahwa semua sandi yang ada dalam penggunaan wifi telah diganti secara berkala.	1	jarang dirubah secara berkala.
37.	Technical Control	Deploy user authentication such as biometrics, smart cards, two-factor authentication and PKI	Poin ini menjelaskan tentang penggunaan otentikasi seperti biometri, *smart card,* autentikasi dua faktor dan PKI.	0	Autentikasi pengguna seperti tersebut belum diterapkan
38.	Technical Control	Ensure that the “ad hoc mode” for 802.11 has been disabled unless the environment is such	Poin ini memastikan bahwa mode ad hoc untuk penggunaan wifi 802.11 telah dinonaktifkan.	3	Tidak diaktifkan,

		that the risk is tolerable. Note: some products do not allow disabling this feature; use with caution or use different vendor.			
39.	Technical Control	Use static IP addressing on network.	Menggunakan IP Statis dalam alamat network.	0	penggunaan ip address secara static belum diterapkan
40.	Technical Control	Disable DHCP.	Menonaktifkan DHCP.	0	DHCP masih diterapkan di jaringan wireless Disbudpar Kabupaten Boyolali
41.	Technical Control	Enable user authentication mechanism for the management interfaces of the AP.	Poin ini melakukan peninjauan, bahwa mekanisme otentikasi user untuk antar muka manajemen WAP diaktifkan.	4	antarmuka pengaturan access point sudah didukung mekanisme autentikasi pengguna

42.	Technical Control	Ensure that management traffic destined for APs is on a dedicated wired subnet.	memastikan bahwa arus yang menuju ke access point telah menggunakan kabel khusus subnet.	3	kabel khusus yang menghubungkan access point sudah terpasang
43.	Technical Control	Use SNMPv3 and / or SSL/TLS for web-based management of APs.	Poin ini memastikan bahwa penggunaan SNMPv3 dan atau SSL/TLS dalam pengaturan secara web untuk access point telah diterapkan.	0	Dari hasil observasi ditemukan bahwa belum diimplementasikan fitur SNMPv3 ataupun SSL/ TLS dalam manajemen access point yang dipakai oleh Disbudpar Kabupaten Boyolali.
44.	Operational Control	Configure SNMP Settings on APs for least privilege (I.e.,read only). Disable SNMPv1 and	Poin ini memastikan bahwa fitur pengaturan dalam SNMP untuk acccess point sudah diaktifkan sepenuhnya. Baik yang versi 1 atau	0	Penggunaan SNMP belum diterapkan.

		SNMPv2 are not recommended.	versi 2.		
45.	Operational Control	Enhance AP management traffic security by using SNMPv3 or equivalent cryptographically protected protocol.	Poin ini bermaksud untuk meningkatkan manajemen lalu lintas keamanan dengan menggunakan protocol cryptography yang dilindungi SNMPv3	0	bahwa penggunaan SNMPv3 belum digunakan.
46.	Operational Control	Use a local serial port interface for AP configuration to minimize the exposure of sensitive management information.	Poin ini memastikan bahwa interface pada local serial port untuk konfigurasi access point telah digunakan untuk meminimalisir terjadinya kebocoran informasi manajemen yang sensitif.	3	Konfigurasi menggunakan interface serial port local sudah digunakan.
47.	Operational Control	Consider other forms of authentication for wireless network such as RADIUS and Kerberos	Poin ini melakukan peninjauan terhadap bentuk lain autentikasi pada jaringan nirkabel seperti *Radius server* dan *Kerberos*	0	penggunaan otentikasi untuk jaringan wireless didapati belum menerapkan user autentikasi baik dari

					Radius maupun Kerberos.
48.	Operational Control	Deploy intrusion detection agents on the wireless part of the network to detect suspisious behavior or unauthorized access and activity.	Poin ini memastikan bahwa telah digunakannya suatu fitur (IDS) yang dapat mendeteksi adanya suatu akses mencurigakan atau akses yang tidak sah dalam aktifitas di jaringan wireless.	0	Belum ada suatu alat baik berupa hardware maupun software yang melakukan pendeteksian dini untuk akses yang mencurigakan
49.	Operational Control	Deploy auditing technology to analyze the records produced by RADIUS for suspicious activity.	Poin ini memastikan bahwa penggunaan audit untuk menganalisis seluruh rekam aktifitas yang dihasilkan oleh RADIUS dalam hal aktifitas yang mencurigakan sudah dilaksanakan	0	Radius tidak ada, untuk itu rekam aktifitas dari Radius tidak tercatat dan penggunaan hasil audit tidak dapat dilakukan.
50.	Operational	Deploy an 802.11 security product that offers other	Poin ini memastikan bahwa penggunaan keamanan dalam teknologi 802.11 yang	1	SDM tidak memenuhi, maka

	Control	security features such as enhanced cryptographic protection or user authorization features.	menawarkan berbagai fitur keamanan seperti perlindungan dengan kriptografi atau fitur otorisasi pengguna telah digunakan.		penerapan teknologi produk keamanan dari 802.11 belum digunakan.
51.	Operational Control	Enable utilization of key-mapping keys (802.1) rather than default keys so that sessions use distinct WEP keys	Poin ini memastikan bahwa penggunaan sandi key-mapping (802.1) telah dilakukan sehingga ketika session habis sudah menggunakan sandi yang berbeda menggunakan sandi WEP.	1	hasil observasi diketahui bahwa penggunaan sandi menerapkan WPA, namun untuk fitur session tidak diterapkan.
52.	Operational Control	Fully understand the impacts of deploying any security feature or product prior to deployment.	Memastikan operator atau pun pihak yang terkait telah mengerti secara penuh mengenai dampak dari penggunaan berbagai macam fitur keamanan atau fitur yang sebelumnya pernah dipakai untuk Disbudpar Kabupaten Boyolali.	4	bahwa pihak administrator mengerti tentang dampak penggunaan fitur keamanan yang sebelumnya hingga sampai saat

					penelitian ini dibuat.
53.	Operational Control	Designate an individual to track the progress of 802.11 security products and standarts (IETF, IEEE, etc.) and the threats and vulnerabilities with the technology	Poin ini memastikan bahwa penunjukan seseorang sebagai pengamat kemajuan teknologi di bidang nirkabel 802.11 terutama dalam hal keamanan dan standar internasional yang sudah ada	2	Penunjukan secara khusus seseorang yang memahami seluk beluk kemajuan 802.11 terutama di bidang keamanan belum ada. Tugas dari administrator sendiri hanya mengatur lancarnya jaringan wireless Disbudpar Kabupaten Boyolali.
54.	Operational Control	Wait until future release of 802.11 WLAN technologies incorporate fixes to the security features or provide enhanced	Poin ini memastikan bahwa menantikan penggunaan fitur keamanan dari teknologi 802.11 terbaru untuk memperbaiki atau menyempurnakan fitur keamanan terkini.	4	Dari hasil observasi didapati bahwa access point yang dipakai di Disbudar

		security features.			Kabupaten Boyolali menggunakan keamanan WPA2-Personal.
55.	Operational Control	When disposing access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.	Poin ini memastikan bahwa ketika access point sudah tidak dipergunakan lagi oleh pihak Disbudpar Kabupaten Boyolali, maka oleh pihak terkait sudah melakukan penghapusan atau pengembalian ulang (reset) access point.	5	Sudah dan pernah dilaksanakan secara terstruktur
56.	Operational Control	If the access points supports logging,turn it on and review thelogs on a regular basis.	Poin ini memastikan bahwa jika access point mendukung fitur logging, maka sudah diaktifkan dan hasil dari log tersebut ditinjau secara teratur.	0	Fitur logging tidak diaktifkan
Total				**94 point**	

Lampiran C Darftar Sistus yang Berhasil ter-Capture

Daftar Situs yang Berhasil ter-*capture*

No	Nama Instansi	Website	Caputure	
			Username	Password
1	PT Darta Media Indonesia	kaskus.co.id	x	x
2	Lazada Indonesia	lazada.co.id	x	x
3	PT Agranet Multicitra Siberkom	detik.com	x	x
4	E-Commerce Alibaba	alibaba.com	√	x
5	E-Commerce Alibaba	aliexpress.com	√	x
6	Surya Citra Televisi	liputan6.com	√	√
7	Badan Nasional Sertifikasi Profesi	bspb.go.id	√	√
8	Kementerian Pariwisata	kompetisipariwisataindonesia.com	√	√

9	Kabupaten Boyolali	sippd.boyolalikab.go.id	√	√
10	Dinas Pariwisata Jawa Barat	disparbud.jabarprov.go.id	√	√
11	Kementerian Pariwisata	kemenpar.monitoring.web.id	√	√
12	Kementerian Pendidikan dan Kebudayaan	data.dikdasmen.kemdikbud.go.id	√	√
13	Kementerian Pendidikan dan Kebudayaan	p4tk-bispar.net	√	√
14	Badan Pengawasan Keuangan dan Pembangunan Daerah	simda-online.com	√	√
15	Badan Pengawasan Keuangan dan Pembangunan Daerah	pusdiklatwas.bpkb.go.id	√	√

16	Badan Pengawasan Keuangan dan Pembangunan Daerah	warga.bpkb.go.id	√	√
17	Pemerintah Jawa Tengah	sippd.jatengprov.go.id	√	√

Lampiran D: Surat Rekomendasi Penelitian

PEMERINTAH KABUPATEN BOYOLALI

KANTOR KESATUAN BANGSA DAN POLITIK

(KESBANGPOL)

Kompleks Perkantoran Terpadu Jl. Merdeka Timur Telp.(0276) 321087 Fax. (0276) 321087 Kemiri, Boyolali

SURAT REKOMENDASI PENELITIAN

NOMOR : 070/369/ VIII/32/2016

I. DASAR :
1. Peraturan Menteri Dalam Negeri Republik Indonesia. Nomor 7 Tahun 2014. Tanggal 20 Desember 2011 Tentang Perubahan Atas Permendagri Nomor 64 Tahun 2011 Tentang Pedoman Penerbitan Rekomendasi Penelitian;
2. Surat Edaran Gubernur Jawa Tengah Nomor 070/265/2004. Tanggal 20 Februari 2004 Tentang Penyederhanaan Prosedur Permohonan Riset, KKN, PKL di Jawa Tengah.

II. MEMBACA : Surat dari BPMD Provinsi Jawa Tengah Nomor : 070/2055/04.3/2016 tanggal, 08 Agustus 2016, Perihal : ***Permohonan Rekomendasi Ijin Penelitia***

III Prinsipnya TIDAK KEBERATAN / Dapat Menerima atas pelaksanaan Penelitian di Kabupaten Boyolali.

1. Nama / NIM : **AMI MEGANTARA PRABOWO / 12650013**
2. Alamat : Susiloharjo, Rt. 04/12, Siswodipuran, Boyolali.
3. Pekerjaan : Mahasiswa
4. Penanggung Jawab : Agung Fatwanto, Ph.D
5. Judul Magang : " ***ANALISIS KEAMANAN WLAN TERHADAP GANGGUAN ARP SPOOFING (Studi kasus Kantor Dinas Pariwisata Kabupaten Boyolali)*** "
6. Lokasi : Disbudpar, Kab. Boyolali.
7. Peserta : 1 Orang

IV Ketentuan-ketentuan sebagai berikut :
1. Sebelum melakukan kegiatan terlebih dahulu melaporkan kepada Pejabat Setempat / Lembaga Swasta yang akan dijadikan objek lokasi untuk mendapatkan petunjuk seperlunya dengan menunjukkan Surat Pemberitahuan ini.
2. Pelaksanaan Penelitian tidak di salahgunakan untuk tujuan tertentu yang dapat mengganggu kestabilan pemerintahan. Untuk penelitian yang mendapat dukungan dana dari sponsor baik dari dalam negeri maupun luar negeri, agar dijelaskan pada saat mengajukan perijinan. Tidak membahas masalah politik dan / atau agama yang dapat menimbulkan terganggunya stabilitas keamanan dan ketertiban.
3. Surat Rekomendasi dapat dicabut dan dinyatakan tidak berlaku apabila pemegang Surat Rekomendasi ini tidak mentaati / mengindahkan peraturan yang berlaku atau obyek penelitian menolak untuk menerima Peneliti.
4. Setelah Penelitian selesai, supaya menyerahkan hasilnya kepada Kantor Kesatuan Bangsa dan Politik Kabupaten Boyolali.

IV Surat Rekomendasi Penelitian berlaku :
1. Berlaku : Dari tanggal : **22 Agustus 2016** S/d tanggal : **22 September 2016**
2. Perpanjangan : Dari tanggal : - S/d tanggal : -

Dikeluarkan di : BOYOLALI
Pada tanggal : 22 Agustus 2016

An.KEPALA KANTOR KESBANGPOL
KABUPATEN BOYOLALI
Kasubag TU

AGUS DARYANTO,S.Sos
Penata Tingkat I
NIP.19640418 198603 1 019

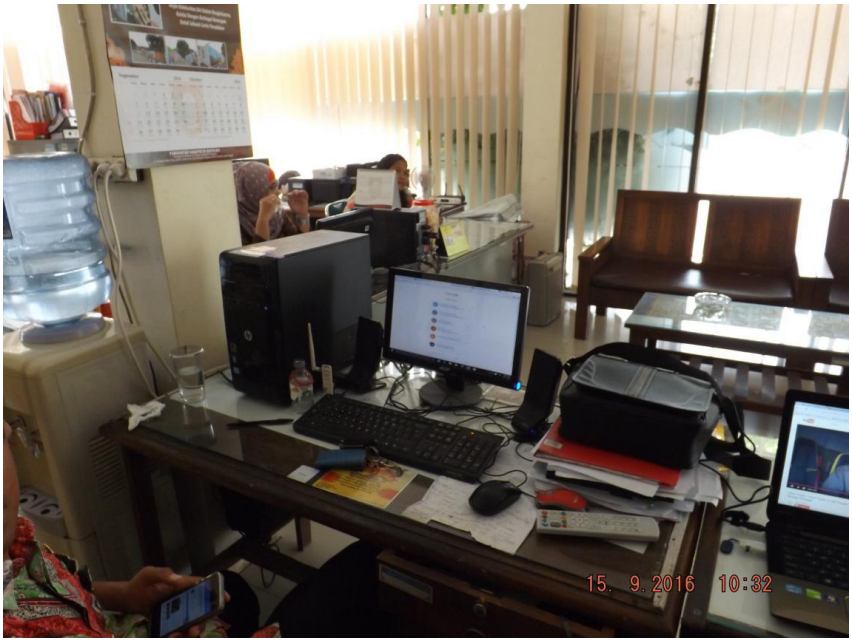
TEMBUSAN Kepada Yth :
1. Bupati Boyolali (sebagai laporan);
2. Dandim 0724 Boyolali :
3. Kapolres Boyolali;
4. Kepala Bappeda Kab. Boyolali;
5. Kepala Disbudpar, Kab. Boyolali;
6. Dekan UIN Sunan Kalijaga Yogyakarta;
7. Yang bersangkutan;
8. Pertinggal.

Lampiran E: Dokumentasi

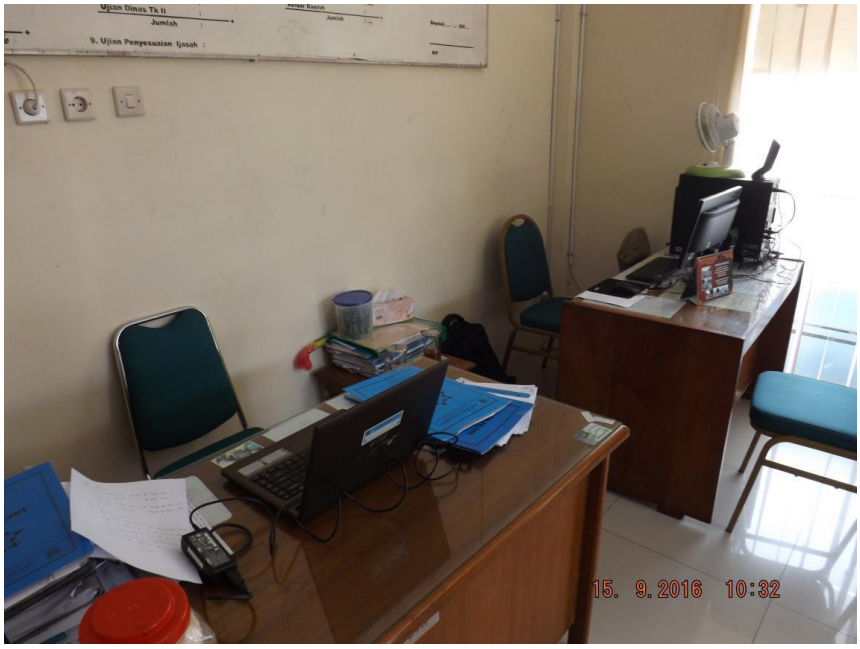
DOKUMENTASI

Dari kiri: PC 4 - PC 5

Suasana Lt.1

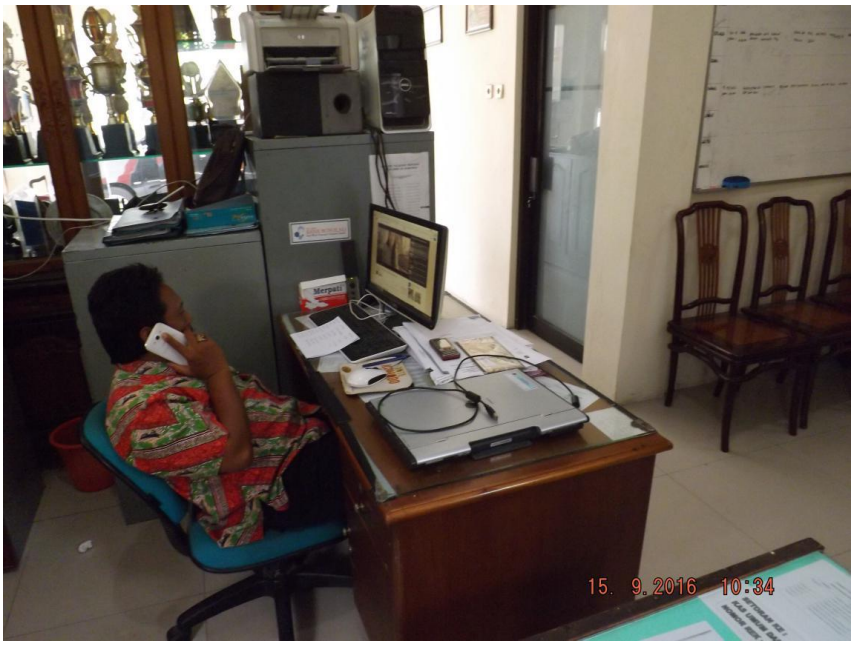


PC 4

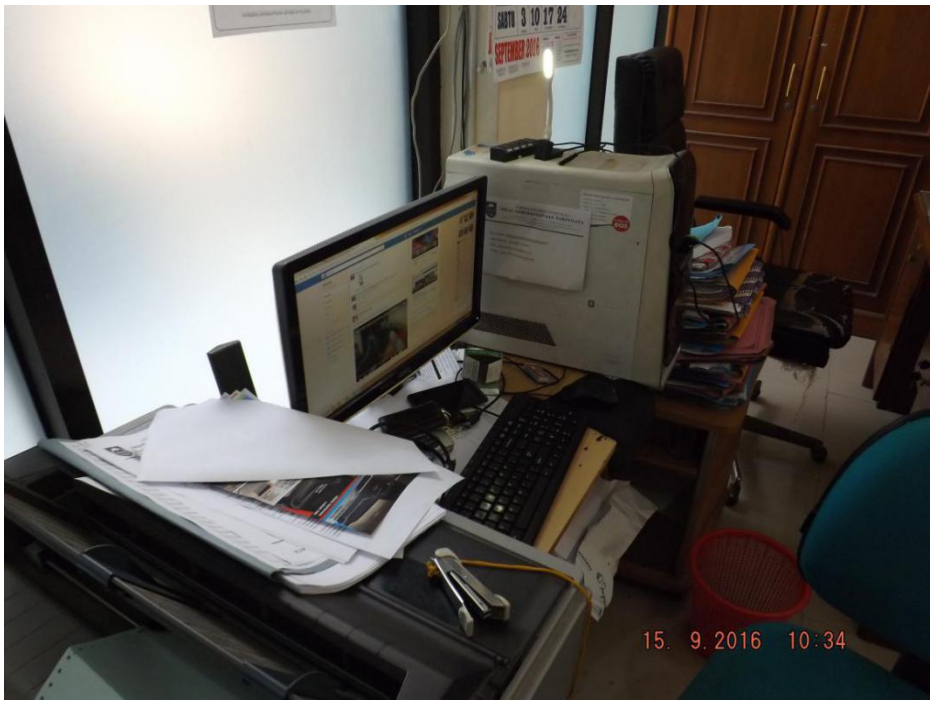


Dari kiri: Laptop 3 - PC 6

Suasana Lt.2



PC 3



PC 2

PC 1

Dari atas: Access Point - Router

Suasana Lt. 2

Laptop 7

Dari kiri: PC 8-PC 7

PC 10

PC 9

DAFTAR RIWAYAT HIDUP

I. DATA PRIBADI

Nama	: Ami Megantara Prabowo
Tempat/Tanggal Lahir	: Boyolali, 12 Februari 1994
Jenis Kelamin	: Laki-laki
Agama	: Islam
Kebangsaan	: Indonesia
Status	: Belum Menikah
Alamat tetap	: Jl. Pisang Susiloharjo, RT05/12 Kel. Siswodipuran, Kec. Boyolali, Kab Boyolali, Jawa Tengah. 57311
Alamat indekost	: Jl. Bimokurdo No.37, RT24/VII, Sapen, Kel.Demangan, Yogyakarta. 55221
Hp	: 0896-7336-0246
Email	: amiprabowo@outlook.com
Facebook	: facebook.com/ami.prabowo
Twitter	: @amiprabowo
Instagram	: @amieshinoda
Whatsapp	: 0896-7336-0146
Telp.	: 0276-322794

II. PENDIDIKAN

A. Pendidikan Formal

1. 2000 – 2006 SD Negeri Susiloharjo
2. 2006 – 2009 SMP Negeri 2 Boyolali
3. 2009 – 2012 SMA Negeri 3 Boyolali
4. 2012 – sekarang Teknik Informatika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sunan Kalijaga

B. Pendidikan Nonformal

Pendidikan dan Pelatihan

1. 2010 : Pelatihan Pasukan Pengibar Bendera Kabupaten Boyolali
2. 2010 : Orientasi Ketahanan Bangsa (ORKETBANG) Kabupaten Boyolali
3. 2013 : Pendidikan Dasar Menwa Mahakarta, Yogyakarta
4. 2013 : Pendidikan dan Pemantapan Provoost Menwa se-Indonesia

Forum Ilmiah dan Seminar

1. 2012 : User Educartion Perpustakaan UIN Sunan Kalijaga Yogyakarta
2. 2012 : Seminar Langkah Awal menjadi Wirausahawan IT Muda Berbakat
3. 2012 : Seminar Technopreneurship "Bisnis Dengan Opensource"
4. 2012 : Konverensi Internasional "*Islamic Perspectives On Terrorism and Corruption*"
5. 2013 : Seminar *Go Open Source with Firefox OS*
6. 2013 : Seminar Nasional *Perceptual Computing*
7. 2013 : *Workshop Game Development Using HTML5*

8. 2013 : Seminar Nasional “Menumbuhkembangkan Jiwa Kewirausahaan Pada Generasi Muda Indonesia”
9. 2013 : Seminar Penyadapan Network
10. 2015 : Seminar Pengembangan dan Implementasi Jurnalisme Desa

Kursus

1. 2010 : Kursus Bahasa Inggris ELTI
2. 2012 : English and Computer Training “Higher Learning”
3. 2013 : Kursus Bahasa Inggris “Marvelous” Pare, Kediri.

III. PRESTASI

1. 2007 : Juara II Lomba Upacara Tingkat SMP/MTS Se-Kabupaten Boyolali
2. 2008 : Juara III Lomba Komputer Tingkat SMP Se-Kabupaten Boyolali
3. 2009 : Juara I Lomba Komputer Tingkat SMP Se-Kabupaten Boyolali
4. 2010 : Variasi Terbaik 2 LBB Antar SMA & SMK se-Eks Kars. Surakarta
5. 2010 : Juara III LBB Antar SMA & SMK se-Eks Kars. Surakarta

IV. PENGALAMAN ORGANISASI

- Paskibra SMA Negeri 3 Boyolali
- Patroli Keamanan Sekolah SMA Negeri 3 Boyolali
- UKM Resimen Mahasiwa UIN Sunan Kalijaga Yogyakarta

Kemampuan Pribadi

- Mendongeng
- Mampu berbahasa Inggris. (pasif)
- Merakit plastik model Gundam
- Mampu penyuluhan akan peraturan Lalu Lintas
- Mampu melatih gerakan baris-berbaris

Hobby

- Merakit Plastik Model Gundam
- Travelling
- Merakit Papercraft