```php
<?php

namespace App\Controllers;
use CodeIgniter\I18n\Time;

class Dashboard extends BaseController
{
    public function index(){
        $penggunaModel = new \App\Models\Pengguna();
        $pengguna = $penggunaModel -> countAll();
        $data = ['title'=> 'Dashboard | User Security Wireless Teknik Komputer',
        'pengguna'=> $pengguna,
        ];

        if(session()->get('username')==''){
            session()->setFlashdata('login_error','Silahkan login untuk mengakses sistem');
            return redirect()->to(base_url('/login'));
        } elseif(session()->get('status')=='inactive'){
            return redirect()->to(base_url('/login/aktivasi'));
        }
        session()->setFlashdata('login', 'Di Dashboard Aplikasi Keamanan Data User');
        return view('dashboard/dashboard', $data);
    }

    public function logout(){
        session()->destroy();
        session()->setFlashdata('login_error','Anda berhasil logout');
        return redirect()->to(base_url('/login'));
    }

    public function profile(){
        $usersModel = new \App\Models\Users();
        $users = $usersModel -> where(['id' => session() -> get('id')]) -> first();
        $data = [
            'title'=>"Profile | Teknik Komputer",
            'users' => $users
    ];
        if(session()->get('username')==''){
            session()->setFlashdata('login_error','Silahkan login untuk mengakses sistem');
            return redirect()->to(base_url('/login'));
        } elseif(session()->get('status')=='inactive'){
            return redirect()->to(base_url('/login/aktivasi'));
        }

        return view('dashboard/profile', $data);
    }


        public function update_profile(){
        $usersModel = new \App\Models\Users();
        $id = $this-> request -> getVar('id');
        $file_foto = $this->request->getFile('foto');
        $foto_lama = $this-> request -> getVar('foto_lama');
        $extension = $file_foto->getExtension();
        $size = $file_foto->getSize();
        $email_lama = $this-> request -> getVar('email_lama');
```

```
        $email = $this-> request -> getVar('email');
        $cari_email = $usersModel -> where(['email' => $email]);
        $hitung_email = $cari_email->countAllResults();
        $username = $this-> request -> getVar('username');
        $username_lama = $this-> request -> getVar('username_lama');
        $cari_username = $usersModel -> where(['username' => $username]);
        $hitung = $cari_username->countAllResults();
        $status_lama = $this-> request -> getVar('status_lama');
        $uniid_lama = $this-> request -> getVar('uniid_lama');

        if($email_lama != $email){
            $status = 'inactive';
            $uniid = md5(str_shuffle('abcdefghijklmnopqrstuvwxyz'.time()));
        } else {
            $status = $status_lama;
            $uniid =$uniid_lama;
        }

        if($size>3000000){
            session()->setFlashdata('gagal', 'File foto terlalu besar! maksimal 3MB.');
            return redirect()->to(base_url('/dashboard/profile'));
        } elseif($file_foto -
> getError() != 4 && $extension != 'jpg' && $extension!='png' && $extension!='jpeg'){
            session()-
>setFlashdata('gagal', 'Format foto salah! Sialahkan upload foto berupa jpg / jpeg / png.');
            return redirect()->to(base_url('/dashboard/profile'));
        } elseif($email_lama != $email && $hitung_email == 1){
            session()-
>setFlashdata('gagal', 'Email telah digunakan! Silahkan gunakan Email lain.');
            return redirect()->to(base_url('/dashboard/profile'));
        } elseif($username_lama != $username && $hitung == 1){
            session()-
>setFlashdata('gagal', 'Username telah digunakan! Silahkan gunakan Username lain.');
            return redirect()->to(base_url('/dashboard/profile'));
        } else{
            if($file_foto -> getError() == 4){
                $nama_foto = $foto_lama;
            } elseif($foto_lama != 'default.png') {
                unlink('images/admin/'.$foto_lama);
                $nama_foto = $file_foto->getName();
                $file_foto -> move('images/admin');
            } else{
                $nama_foto = $file_foto->getName();
                $file_foto -> move('images/admin');
            }
            $data = [
            'nama' => $this-> request -> getVar('nama'),
            'email' => $this-> request -> getVar('email'),
            'username' => $this-> request -> getVar('username'),
            'foto' => $nama_foto,
            'status' => $status,
            'uniid' => $uniid,
            'updated_at' => date('Y-m-d h:i:s')
            ];
            $usersModel->set($data);
            $usersModel->where(['id' => $id]);
```

```
            $usersModel->update();
            session()->set('nama',$data['nama']);
            session()->set('email',$data['email']);
            session()->set('username',$data['username']);
            session()->set('foto',$data['foto']);
            session()->set('status',$data['status']);
            session()->set('uniid',$data['uniid']);
            session()->setFlashdata('berhasil', 'Berhasil Memperbarui Profile');
            return redirect()->to(base_url('/dashboard/profile'));
        }
    }

    public function password(){
        $usersModel = new \App\Models\Users();
        $users = $usersModel -> where(['id' => session() -> get('id')]) -> first();
        $data = [
            'title'=>"Ubah Password | Teknik Komputer",
            'users'=>$users
    ];
        if(session()->get('username')==''){
            session()->setFlashdata('login_error','Silahkan login untuk mengakses sistem');
            return redirect()->to(base_url('/login'));
        } elseif(session()->get('status')=='inactive'){
            return redirect()->to(base_url('/login/aktivasi'));
        }

        return view('dashboard/ubah_password', $data);
    }

    public function update_password(){
        $usersModel = new \App\Models\Users();
        $id = $this->request->getVar('id');
        $password1 = md5($this->request->getVar('password_lama'));
        $users = $usersModel -> where(['id' => $id]) -> first();
        $password_lama = $users['password'];
        $password_baru = $this->request->getVar('password_baru');
        $uppercase = preg_match('@[A-Z]@', $password_baru);
        $lowercase = preg_match('@[a-z]@', $password_baru);
        $number    = preg_match('@[0-9]@', $password_baru);
        $password2 = md5($this->request->getVar('password_baru'));
        $password3 = md5($this->request->getVar('ulang_password_baru'));

        if($password1 != $password_lama){
            session()-
>setFlashdata('gagal', 'Password lama tidak sesuai! silahkan masukkan password lama dengan benar.
');
            return redirect()->to(base_url('/dashboard/password'));
        } elseif(!$uppercase || !$lowercase || !$number || strlen($password_baru)<8){
            session()-
>setFlashdata('gagal', 'Password harus lebih dari 8 karakter, mengandung huruf BESAR, huruf kecil
 dan angka.');
            return redirect()->to(base_url('/dashboard/password'));
        } elseif($password2 != $password3){
            session()->setFlashdata('gagal', 'Silahkan ulangi password dengan benar.');
            return redirect()->to(base_url('/dashboard/password'));
        } else {
```

```
            $data = [
                'password' => $password3
            ];
            $usersModel->set($data);
            $usersModel->where(['id' => $id]);
            $usersModel->update();
            session()->setFlashdata('berhasil', 'Berhasil Memperbarui Password');
            return redirect()->to(base_url('/dashboard/password'));
        }
    }

    public function admin(){
        $usersModel = new \App\Models\Users();
        $keyword = $this->request->getVar('keyword');
        if($keyword){
           $users = $usersModel->orderby('id', 'desc')->search($keyword);
        }else {
            $users = $usersModel->orderby('id', 'desc');
        }
        $users = $users -> paginate(7, 'users');
        $pager = $usersModel -> pager;
        $current_page = $this->request->getVar('page_users') ? $this->request-
>getVar('page_users') : 1;
        $jumlah_users = $usersModel -> countAllResults();
        $data = [
            'title'=>"Data Admin | Teknik Komputer",
            'users' => $users,
            'pager' => $pager,
            'jumlah_users' => $jumlah_users,
            'current_page' => $current_page
    ];
        if(session()->get('username')==''){
            session()->setFlashdata('login_error','Silahkan login untuk mengakses sistem');
            return redirect()->to(base_url('/login'));
        } elseif(session()->get('status')=='inactive'){
            return redirect()->to(base_url('/login/aktivasi'));
        }

        return view('dashboard/admin', $data);
    }

    public function save_admin(){
        $usersModel = new \App\Models\Users();
        $file_foto = $this->request->getFile('foto');
        $size      = $file_foto->getSize();
        $extension = $file_foto->getExtension();
        $email = $this-> request -> getVar('email');
        $cari_email = $usersModel -> where(['email' => $email]);
        $hitung_email = $cari_email->countAllResults();
        $username = $this-> request -> getVar('username');
        $cari_username = $usersModel -> where(['username' => $username]);
        $hitung = $cari_username->countAllResults();
        $password1 = md5($this->request->getVar('password'));
        $password2 = md5($this->request->getVar('ulangi_password'));

        if($password1 != $password2){
            session()->setFlashdata('gagal', 'Silahkan ulangi password dengan benar.');
```

```
            session()->setFlashdata('gagal', 'Silahkan ulangi password dengan benar.');
            return redirect()->to(base_url('/dashboard/admin'));
        } elseif($size>3000000){
            session()->setFlashdata('gagal', 'File foto terlalu besar! maksimal 3MB.');
            return redirect()->to(base_url('/dashboard/admin'));
        } elseif($file_foto -
> getError() != 4 && $extension != 'jpg' && $extension!='png' && $extension!='jpeg'){
            session()-
>setFlashdata('gagal', 'Format foto salah! Sialahkan upload foto berupa jpg / jpeg / png.');
            return redirect()->to(base_url('/dashboard/admin'));
        } elseif($hitung_email == 1){
            session()-
>setFlashdata('gagal', 'Email telah digunakan! Silahkan gunakan Email lain.');
            return redirect()->to(base_url('/dashboard/admin'));
        } elseif($hitung == 1){
            session()-
>setFlashdata('gagal', 'Username telah digunakan! Silahkan gunakan Username lain.');
            return redirect()->to(base_url('/dashboard/admin'));
        } else{
            if($file_foto->getError() == 4){
                $nama_foto = 'default.png';
            }else{
                $nama_foto = $file_foto->getName();
                $file_foto -> move('images/admin');
            }

            $uniid = md5(str_shuffle('abcdefghijklmnopqrstuvwxyz'.time()));
            $data = [
            'nama' => $this-> request -> getVar('nama'),
            'email' => $email,
            'username' => $username,
            'password' => $password2,
            'foto' => $nama_foto,
            'level' => $this-> request -> getVar('level'),
            'uniid' => $uniid,
            'activation_date' => date("Y-m-d h:i:s")
            ];
            $usersModel->insert($data);
            session()-
>setFlashdata('berhasil', 'Berhasil Menambahkan Data Admin Baru! Silahkan cek Email yang didaftar
kan untuk aktivasi akun.');
            return redirect()->to(base_url('/dashboard/admin'));
        }
    }

    public function update_admin(){
        $usersModel = new \App\Models\Users();
        $id = $this-> request -> getVar('id');
        $file_foto = $this->request->getFile('foto');
        $foto_lama = $this-> request -> getVar('foto_lama');
        $extension = $file_foto->getExtension();
        $size = $file_foto->getSize();
        $email_lama = $this-> request -> getVar('email_lama');
        $email = $this-> request -> getVar('email');
        $cari_email = $usersModel -> where(['email' => $email]);
        $hitung_email = $cari_email->countAllResults();
```

```
        $username = $this-> request -> getVar('username');
        $username_lama = $this-> request -> getVar('username_lama');
        $cari_username = $usersModel -> where(['username' => $username]);
        $hitung = $cari_username->countAllResults();
        $status_lama = $this-> request -> getVar('status_lama');
        $uniid_lama = $this-> request -> getVar('uniid_lama');

        if($email_lama != $email){
            $status = 'inactive';
            $uniid = md5(str_shuffle('abcdefghijklmnopqrstuvwxyz'.time()));
        } else {
            $status = $status_lama;
            $uniid =$uniid_lama;
        }

        if($size>3000000){
            session()->setFlashdata('gagal', 'File foto terlalu besar! maksimal 3MB.');
            return redirect()->to(base_url('/dashboard/admin'));
        } elseif($file_foto -
> getError() != 4 && $extension != 'jpg' && $extension!='png' && $extension!='jpeg'){
            session()-
>setFlashdata('gagal', 'Format foto salah! Sialahkan upload foto berupa jpg / jpeg / png.');
            return redirect()->to(base_url('/dashboard/admin'));
        } elseif($email_lama != $email && $hitung_email == 1){
            session()-
>setFlashdata('gagal', 'Email telah digunakan! Silahkan gunakan Email lain.');
            return redirect()->to(base_url('/dashboard/admin'));
        } elseif($username_lama != $username && $hitung == 1){
            session()-
>setFlashdata('gagal', 'Username telah digunakan! Silahkan gunakan Username lain.');
            return redirect()->to(base_url('/dashboard/admin'));
        } else{
            if($file_foto -> getError() == 4){
                $nama_foto = $foto_lama;
            } elseif($foto_lama != 'default.png') {
                unlink('images/admin/'.$foto_lama);
                $nama_foto = $file_foto->getName();
                $file_foto -> move('images/admin');
            } else{
                $nama_foto = $file_foto->getName();
                $file_foto -> move('images/admin');
            }
            $data = [
            'nama' => $this-> request -> getVar('nama'),
            'email' => $this-> request -> getVar('email'),
            'username' => $this-> request -> getVar('username'),
            'foto' => $nama_foto,
            'level' => $this-> request -> getVar('level'),
            'status' => $status,
            'uniid' => $uniid,
            'updated_at' => date('Y-m-d h:i:s')
            ];
            $usersModel->set($data);
            $usersModel->where(['id' => $id]);
            $usersModel->update();
            session()->setFlashdata('berhasil', 'Berhasil Memperbarui Data Admin');
```

```
            return redirect()->to(base_url('/dashboard/admin'));
        }
    }

    public function delete_admin($id){
        $usersModel = new \App\Models\Users();
        $users = $usersModel -> find($id);
        if($users['foto'] != 'default.png'){
            unlink('images/admin/'.$users['foto']);
        }
        $usersModel->delete($id);
        session()->setFlashdata('berhasil', 'Berhasil Menghapus Data Admin');
        return redirect()->to(base_url('/dashboard/admin'));
    }

    public function update_passworda(){
        $usersModel = new \App\Models\Users();
        $id = $this->request->getVar('id');
        $password_baru = $this->request->getVar('password_baru');
        $uppercase = preg_match('@[A-Z]@', $password_baru);
        $lowercase = preg_match('@[a-z]@', $password_baru);
        $number    = preg_match('@[0-9]@', $password_baru);
        $password2 = md5($this->request->getVar('password_baru'));
        $password3 = md5($this->request->getVar('ulang_password_baru'));

        if(!$uppercase || !$lowercase || !$number || strlen($password_baru)<8){
            session()-
>setFlashdata('gagal', 'Password harus lebih dari 8 karakter, mengandung huruf BESAR, huruf kecil
 dan angka.');
            return redirect()->to(base_url('/dashboard/admin'));
        } elseif($password2 != $password3){
            session()->setFlashdata('gagal', 'Silahkan ulangi password dengan benar.');
            return redirect()->to(base_url('/dashboard/admin'));
        } else {
            $data = [
                'password' => $password3
            ];
            $usersModel->set($data);
            $usersModel->where(['id' => $id]);
            $usersModel->update();
            session()->setFlashdata('berhasil', 'Berhasil Memperbarui Password Admin');
            return redirect()->to(base_url('/dashboard/admin'));
        }
    }


    public function pengguna(){
        $penggunaModel = new \App\Models\Pengguna();
        $keyword = $this->request->getVar('keyword');
        if($keyword){
           $pengguna = $penggunaModel->orderby('id', 'desc')->search($keyword);
        }else {
            $pengguna = $penggunaModel->orderby('id', 'desc');
        }
        $pengguna = $pengguna -> paginate(8, 'pengguna');
        $pager = $penggunaModel -> pager;
```

```
        $current_page = $this->request->getVar('page_pengguna') ? $this->request-
       >getVar('page_pengguna') : 1;
        $jumlah_pengguna = $penggunaModel -> countAllResults();
        $data = [
            'title'=>"Data Pengguna | Teknik Komputer",
            'pengguna' => $pengguna,
            'pager' => $pager,
            'jumlah_pengguna' => $jumlah_pengguna,
            'current_page' => $current_page
        ];

        if(session()->get('username')==''){
            session()->setFlashdata('login_error','Silahkan login untuk mengakses sistem');
            return redirect()->to(base_url('/login'));
        } elseif(session()->get('status')=='inactive'){
            return redirect()->to(base_url('/login/aktivasi'));
        }
        return view('dashboard/pengguna',$data);
    }

    public function save_pengguna(){
        $penggunaModel = new \App\Models\Pengguna();
        $file_foto = $this->request->getFile('foto');
        $nama_foto = $file_foto->getName();
        $extension = $file_foto->getExtension();
        $size      = $file_foto->getSize();
        $nim = $this-> request -> getVar('nim');
        $cari_nim = $penggunaModel -> where(['nim' => $nim]);
        $hitung_nim = $cari_nim->countAllResults();
        $mac = $this-> request -> getVar('mac');
        $cari_mac = $penggunaModel -> where(['mac' => $mac]);
        $hitung_mac = $cari_mac->countAllResults();

        if($size>3000000){
            session()->setFlashdata('gagal', 'File foto terlalu besar! maksimal 3MB.');
            return redirect()->to(base_url('/dashboard/pengguna'));
        } elseif($file_foto -
> getError() != 4 && $extension != 'jpg' && $extension!='png' && $extension!='jpeg'){
            session()-
>setFlashdata('gagal', 'Format foto salah! Sialahkan upload foto berupa jpg / jpeg / png.');
            return redirect()->to(base_url('/dashboard/pengguna'));
        }elseif($hitung_nim == 1){
            session()->setFlashdata('gagal', 'NIM Tidak Boleh Sama!.');
            return redirect()->to(base_url('/dashboard/pengguna'));
        }elseif($hitung_mac == 1){
            session()->setFlashdata('gagal', 'MAC Address Tidak Boleh Sama!.');
            return redirect()->to(base_url('/dashboard/pengguna'));
        } else{
            $data = [
            'nim' => $this-> request -> getVar('nim'),
            'nama' => $this-> request -> getVar('nama'),
            'jk' => $this-> request -> getVar('jk'),
            'pendidikan' => $this-> request -> getVar('pendidikan'),
            'mac' => $this-> request -> getVar('mac'),
            'foto' => $nama_foto
            ];
            $file_foto -> move('images/pengguna');
```

LITERATUR JURNAL

NO	RP	Judul Jurnal	Permasalahan Jurnal	Solusi Jurnal
1	RP1	*Optimalisasi Keamanan Jaringan Wireless Menggunakan Firewall Filtering MAC Address* Rachmat Adi Purnama Universitas Bina Sarana Informatika 2019	Banyak pengguna jaringan wireless tidak mengetahui jenis bahaya apa yang sedang menghampiri mereka saat terhubung kedalam Jaringan Wireless Access Point (WAP), misalnya seperti sinyal WLAN yang dapat disusupi oleh hacker [4]. Keamanan wireless WEP (Wired Equivalent Privacy) merupakan standart dari keamanan wireless yang sebelumnya mampu meminimalisir pembatasan hak akses kedalam jaringan wireless. Namun kini keamanan wireless menggunakan WEP sudah mudah dipecahkan dengan berbagai tools yang tersedia didalam jaringan internet.	Maka dengan menerapkan security MAC Address setiap pengguna layanan jaringan yang ingin terhubung kedalam jaringan harus melakukan pendaftaran MAC Addressnya. Hal ini dapat digunakan untuk meminimalisir pengguna layanan jaringan yang seharusnya tidak mendapatkan akses. Firewall filtering MAC Address telah dikembangkan untuk memberikan perlindungan terhadap pelayanan jaringan wireless. Penggunaan filtering MAC Address mampu membatasi beberapa komputer yang dapat terhubung kedalam wireless hotspot dengan mempertimbangkan IP Address dan MAC Address yang terdaftar [7]. Diharapkan pengimplementasian keamanan secara ganda mampu meningkatkan keamanan didalam jaringan komputer. Kerena pemakaian frekwensi yang sifatnya lebih terbuka dibanding dengan menggunakan kabel, maka kerentanan keamanan jalur komunikasi akan lebih berbahaya dibandingkan menggunakan kabel. Untuk itu perlu dilakukan penanganan keamanan yang lebih ekstra pada jaringan wireless [8].
2	RP2	ANALISIS WIRELESS LOCAL AREA NETWORK (WLAN) DAN PERANCANGAN MAC ADDRESS FILTERING MENGGUNAKAN MIKROTIK (STUDI KASUS PADA PT.GRAHA	Keamanan jaringan WLAN sebagai bagian dari sebuah sistem sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunaannya. Sistem keamanan jaringan WLAN harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh	Atas dasar permasalahan tersebut, penulis ingin menganalisa keamanan jaringan WLAN pada PT.Graha Prima Swara. Sehingga jaringan WLAN PT.Graha Prima Swara dapat dimanfaatkan secara optimal dan juga memiliki keamanan jaringan yang aman.

LITERATUR JURNAL

		PRIMA SWARA JAKARTA) Kurani Mega Asteroid[1] Yayan Hendrian[2]	pihak yang tidak berhak. Dari segi keamanan, jaringan WLAN dengan sistem keamanan WPA2– PSK mudah ditembus oleh user lain yang tidak mempunyai hak untuk mengakses internet diarea tersebut.	
3	RP3	Rancang Bangun Jaringan Wirelless Di Politeknik Negeri Bengkalis Menggunakan MAC Filtering Agus Tedyyana Teknik Informatika Politeknik Negeri Bengkalis 2016	Banyak vendor yang menyediakan fasilitas yang memudahkan pengguna atau admin jaringan sehingga sering ditemukan wireless yang masih menggunakan konfigurasi wireless default bawaan vendor. Seringkali wireless yang dipasang pada jaringan masih menggunakan setting default bawaan vendor seperti SSID, IP Address, remote manajemen, DHCP enable, kanal frekuensi, tanpa enkripsi bahkan user/password untuk administrasi wireless tersebut masih standart bawaan pabrik. Banyak pengguna jaringan wireless tidak bisa membayangkan jenis bahaya apa yang sedang menghampiri mereka saat sedang berasosiasi dengan wireless access point (WAP), misalnya seperti sinyal WLAN dapat disusupi oleh hacker	Pengelolaan jaringan lokal (Local Area Network, LAN) merupakan salah satu alternatif penyelesaian masalah supaya didapatkan layanan yang maksimal. pembagian akses jaringan menggunakan teknologi nirkabel/ wireless saat ini semakin menjadi pilihan. Cakupan area, kemudahan serta sifat flexible pada wireless menjadi alasan admin jaringan menggunakan nya. Alasan keamanan merupakan hal yang sangat penting dalam jaringan komputer, terutama dalam jaringan wireless.
4	RP4	Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus : TP-Link Archer A6) Haeruddin1, Arif Kurniadi2 2021	Beberapa vendor menyediakan fitur-fitur yang memudahkan pengguna maupun administrator jaringan untuk menggunakannya, sehingga sering dijumpai masih menggunakan konfigurasi default dari vendor. Oleh karena itu, para hacker sering melakukan aksinya untuk menguji kemampuan yang telah dipelajari sebelumnya. Kemudian terhubung dalam satu jaringan yang sama dan mengambil data pengguna lainnya secara illegal(Wahyudi, 2018). Namun para hacker melancarkan aksinya ditempat umum seperti kafe,	Dikarenakan lebih rentan diserang oleh hacker, maka dibutuhkan sebuah metode untuk melakukan ujicoba apakah jaringan wireless yang telah terpasang sudah aman atau sesuai dengan standard operasional. Metode ini biasa disebut dengan metode penetration testing. Metode Penetration Testing adalah proses simulasi serangan pada sistem yang memerlukan sertifikasi keamanan jaringan untuk mencegah peretas atau penyerang jaringan yang menyebabkan kehilangan data pribadi dan data perusahaan. Orang yang melakukan metode ini juga disebut sebagai

LITERATUR JURNAL

			public hotspot, dan restoran. Karena sebagian pengguna tidak peduli dengan keamanan komunikasi data di tempat publik, maka tempat hacker untuk melakukan uji coba illegal melalui jaringan wireless yang terhubung ke hacker(Samsumar & Gunawan, 2017). Dibanding dengan jaringan kabel atau LAN, jaringan wireless lebih rentan dan mudah masuk kedalam jaringan wireless yang tersedia. Cukup mendapatkan password wifi sudah bisa terhubung ke jaringan yang dituju oleh hacker(Amarudin, 2018).	pentester(Mushlih et al., 2019). Dalam pengujian ini, perlu disetujui oleh pemilik sistem, jika tidak maka disebut sebagai tindakan illegal atau di-hack. Hasil test pentest sangat penting bagi administrator jaringan untuk meningkatkan keamanan sistem perusahaan.
5	RP5	KEAMANAN JARINGAN WLAN TERHADAP SERANGAN WIRELESS HACKING PADA DINAS KOMUNIKASI & INFORMATIKA DIY Mochamad Gilang Hari Wibowo1 , Joko Triyono2 , Edhy Sutanta3 1,2,3 Jurusan Teknik Informatika, FTI, IST AKPRIND Yogyakarta	Keamanan jaringan WLAN merupakan hal penting yang perlu diketahui oleh pengelola jaringan, agar dapat diketahui tingkat keamanan jaringan yang disediakan. Dinas Komunikasi dan Informatika Daerah Istimewa Yogyakarta (Dinas Kominfo DIY) merupakan salah satu lembaga dalam lingkungan Pemerintah DIY yang menerapkan jaringan komputer kabel dan WLAN sebagai media pertukaran data/informasi untuk pelayanan umum atau komersial, kepegawaian, dan lainnya. Penggunaan media WLAN tersebut rentan terhadap ancaman serangan karena menggunakan gelombang radio.	Penelitian ini dilakukan untuk memperoleh hasil pengujian keamanan jaringan wireless pada Dinas Kominfo DIY, sehingga bisa digunakan sebagai masukan bagi pengelola dalam rangka menjaga dan/atau meningkatkan kualitas layanan koneksi jaringan WLAN yang disediakan
6	RP6	IMPLEMENTASI PENANGANAN SERANGAN MAC-CLONE PADA HOTSPOT MIKROTIK DI STMIK PRADNYA PARAMITA MALANG (STUDI KASUS: STMIK PRADNYA PARAMITAMALANG)	STMIK Pradnya Paramita merupakan Sekolah Tinggi yang berdiri sejak 26 Juli 2000 di Malang. Keamanan jaringan merupakan yang penting untuk diperhatikan oleh sebuah Sekolah Tinggi. Oleh karena itu, diperlukan penanganan jaringan dari berbagai serangan, salah satunya yaitu serangan MACclone. Adanya penanganan serangan MACclone dapat mengembalikan hak autoritas pemilik user, agar user yang dimiliki tidak mudah di duplikat oleh pengguna lain.	Bagaimana cara mengatasi serangan MAC-clone pada jaringan mikrotik STMIK Pradnya Paramita Malang

LITERATUR JURNAL

		Santi Dwi Ratnasari1), Dwi Safiroh Utsalina2)		
7	RP7	Pembatasan Jumlah Client Menggunakan Security MACAddress with Cisco Martias, Ramda Fadillah Djuanda Universitas Bina Sarana Informatika 2018	Keamanan jaringan yaitu proses pencegahan yang dilakukan oleh penyerang untuk terhubung ke dalam jaringan komputer melalui akses yang tidak sah atau peggunaan secara ilegal dari komputer dan jaringan [2]. Wifi Protected Access2 (WPA2) adalah protokol keamanan baru yang dirancang untuk memperbaiki beberapa kerentanan keamanan hadir dalam WPA asli [3]. Keamanan jaringan pada kantor PT. Pertamina Patra Niaga menggunakan keamanan yang masih kurang, dikarenakan masih menggunakan keamanan model Wifi Protected Access2 (WPA2) pada jaringan access point, sedangkan yang dimaksud dengan Wireless Access Point adalah suatu piranti yang memungkinkan piranti nirkabel untuk terhubung ke dalam jaringan dengan menggunakan WI-FI, Bluetooth atau standar lain [4]. Dengan mengandalkan sistem keamanan seperti ini, maka 1 password dapat digunakan oleh banyak user. Hal ini pula dapat menyebabkan user yang tidak berhak akses kedalam jaringan PT. Pertamina Patra Niaga masih dapat melakukan akses jaringan.	Untuk membatasi jumlah user yang dapat terkoneksi, penulis menyarankan untuk membuat jaringan usulan dengan menggunakan Security MAC-address With Cisco sebagai batasan jumlah client yang dapat melakukan akses. Jadi, hanya client yang telah didaftarkan MAC-addressnya saja yang dapat terkoneksi. MAC (Mac Access Control) address adalah alamat sebuah hardware atau alamat fisik yang secara unik mengidentifikasi setiap komputer atau alat yang terhubung dalam jaringan, MAC address juga sering disebut physical/hardware address [5].
8	RP8	INTRANET SISTEM INFORMASI AKADEMIK STMIK AUB SURAKARTA BERBASIS MAC ADDRESS UNTUK AUTO LOGIN Jamal Nasirudin, H. Ary Setyadi 2015	contoh riil sistem Teknologi Informasi yang sekarang ini sedang diusahakan oleh pemerintah Indonesia adalah sistem EBudgeting, E-ticketing, dan baru – baru ini adalah Ujian Nasional (UN) berbasis komputer atau bisa disebut juga Computer Base Test (CBT). Meskipun sistem Ujian Nasional (UN) berbasis komputer masih terbilang baru namun dianggap lebih efisien karena bisa menghemat biaya untuk pencetakan soal – soal Ujian Nasional (UN) secara manual. Media yang diujikan pun sudah kompleks seperti soal visual,	Dari contoh tersebut maka dapat inspirasi penulis untuk membuat sebuah sistem yang berbasis intranet. Dari pengamatan penulis selama ini sistem yang ada di Kampus STMIK AUB Surakarta sudah baik namun kurang dimanfaatkan oleh mahasiswa. Salah satu sistem yang baik itu namun kurang dimanfaatkan oleh mahasiswa adalah sistem pengisian Kartu Rencana Studi (KRS) online. Hanya beberapa saja diantara sekian banyak mahasiswa. Salah satu alasan mengapa mahasiswa enggan memanfaatkan sistem KRS online adalah karena masih saja merepotkan mahasiswa

LITERATUR JURNAL

			audio visual. Ini adalah salah satu contoh pemanfaatan media internet yang digunakan oleh pemerintahan Indonesia dibawah pimpinan Presiden Jokowi	dalam mengurus administrasi meskipun sudah mengisi KRS online. Alasan paling sederhana adalah sistem KRS online tersebut memakan biaya bandwidth karena menggunakan internet dimana server utamanya berada di lokasi yang jauh bahkan bisa berada di luar negeri. Untuk alasan itulah penulis mencoba membuat sebuah sistem Kartu Rencana Studi (KRS) dan beberapa sistem lainnya yang dapat dimanfaatkan oleh mahasiswa secara online namun tidak mengeluarkan biaya yaitu dengan memanfaatkan jaringan intranet menggunakan wifi sebagai media penghubung server dengan kliennya (smartphone atau laptop mahasiswa).
9	RP9	Keamanan Jaringan Menggunakan Switch Port Security Khashaaisha Al Fikri, Djuniadi Universitas Negeri Semarang 2021	kebutuhan manusia terhadap jaringan komputer semakin bertambah banyak dan penting dalam berbagai bidang. Misalnya dalam bidang pendidikan, jaringan komputer digunakan untuk siswa memperoleh pelajaran. Dalam bidang pekerjaan, jaringan komputer digunakan untuk mengirim dan menerima data/dokumen penting. Bahkan dalam sebuah permainan, jaringan digunakan untuk bertemu teman dan bermain secara online. Penggunaan jaringan komputer ini sudah dilakukan sejak tahun 1988 untuk membantu menyelesaikan pekerjaan di universitas-universitas dan perusahaan-perusahaan [1]. Karena jaringan ini telah menjadi bagian dari setiap kegiatan manusia tentu dalam pengelolaannya tidak boleh luput dalam segi keamanan. Kemanan jaringan digunakan untuk mencegah tindakan kejahatan yang mungkin dilakukan oleh orang yang tidak bertanggung jawab seperti tindakan penipuan, cracking, dsb.	Teknik keamanan jaringan yang dapat dilakukan untuk mencegah tindakan kejahatan dalam jaringan ini banyak sekali. Contohnya adalah firewall, metode ini digunakan pada software maupun hardware untuk melindungi, menyaring bahkan menolak kegiatan pada jaringan yang berpotensi untuk merusak atau mendapatkan informasi pribadi melalui software/hardware tersebut. Cara kerja firewall ini cukup sederhana, bila ada traffic data masuk ke suatu jaringan firewall memeriksa traffic tersebut kemudian meneruskannya ke tujuan [2]. Kemudian terdapat teknik pengamanan sederhana dalam lingkup lokal dengan menggunakan port security. Teknik port security merupakan teknik yang membatasi penggunaaan akses jaringan melalui port pada switch oleh perangkat yang MAC address-nya sudah terdaftar. Perangkat computer MAC address-nya belum terdaftar tidak memiliki hak untuk mengakses port tersebut. Port sendiri merupakan bagian yang dapat dikatakan sebagai pintu keluarmasuknya data pada komputer [3].

LITERATUR JURNAL

10	RP10	Implementasi Sistem Keamanan Hotspot Jaringan Menggunakan Metode OpenSSL (Secure Socket Layer) M. Syaiful Anam1 , Dedy Hermanto2 1Teknik Informatika, STMIK GI MDP 2020	Keamanan jaringan wireless pada perangkat access point yang sering digunakan adalah metode WEP/WPA/WPA2. Hampir semua pengguna jaringan wireless rata-rata mengimplemetasikan perangkat access pointnya dengan menggunakan metode tersebut. Metode tersebut dikenal baik dalam hal kemampuan pengamanan security jaringan wireless tetapi metode WEP/WPA/ WPA2 masih bisa ditembus oleh aplikasi hacking dengan metode brute-force attack dan dictionary	Solusi keamanan wireless hotspot adalah dengan menerapkan Metode SSL (Secure Socket Layer). Metode Secure Socket Layer telah banyak digunakan dalam pengamanan website atau situs web yang membutuhkan pengamanan tingkat tinggi seperti website perbankan, hosting, jual beli online dan sebagainya yang biasanya pada website tersebut menggunakan protocol HTTPS (Hyper Text Transfer Protocol Secure)