PRAKTIKUM 1: AUTENTICATION

Pertemuan ke : 1

Total Alokasi Waktu : 90 menit
- Materi : 15 menit
- Pre-Test : 15 menit
- Praktikum : 45 menit
- Post-Test : 15 menit

Total Bobot Penilaian : 100%
- Pre-Test : 20 %
- Praktik : 30 %
- Post-Test : 50 %

Pemenuhan CPL dan CPMK:

CPL-07	Mampu memilih, membuat dan menerapakan teknik, sumber daya, penggunaan perangkat teknik modern dan implementasi teknologi informasi untuk memecahkan masalah.
CPMK-03	Memahami prinsip otentikasi pengguna sistem elektronik dan prinsip kontrol akses untuk meningkatkan keamanan.

1.1. DESKRIPSI CAPAIAN PEMBELAJARAN

Setelah mengikuti praktikum ini mahasiswa diharapkan mampu:
1. Memahami dan mengimplementasikan prinsip autentikasi.

1.2. INDIKATOR KETERCAPAIAN PEMBELAJARAN

Indikator ketercapaian diukur dengan:

CPL-07	CPMK-03	Mahasisiwa mampu menganalisa dan menerapkan prinsip autentikasi pengguna elektronik berbasis password, token,biometric dan Remote User Authentication.

1.3. TEORI PENDUKUNG

Tuliskan teori pendukung disini. Contoh penulisan Gambar 1.1.

Auntetikasi adalah suatu Langkah untuk menentukan atau mengidentifikasi bahwa seseorang (atau sesuatu) adalah autentik atau asli. Melakukan autentikasi terhadap sebuah objek adalah melakukan konfirmasi terhadap kebenarannya. Sedangkan melakukan autentikasi terhadap seseorang biasanya adalah untuk memverifikasi identitasnya. Pada suatu sistem komputer, autentikasi biasanya terjadi pada saat login atau permintaan akses.

Selain itu authentification juga merupakan salah satu dari banyak metode yang digunakan untuk menyediakan bukti bahwa dokumen tertentu yang diterima secara elektronik benar-benar datang dari

orang yang bersangkutan dan tak berubah caranya adalah dengan mengirimkan suatu kode tertentu melaui e-mail dan kemudian pemilik e-mail mereplay email tersebut atau mengetikan kode yang telah dikirimkan.

1.4. HARDWARE DAN SOFTWARE

Hardware dan software yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. Sublem/ Notepad++/ Atom
3. XAMPP

1.5. PRE-TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-03	Jelaskan apa itu authentikasi!	30
2.	CPL-07	CPMK-03	Bagaimana cara kerja atau konsep dari authentikasi!	40
3.	CPL-07	CPMK-03	Analisislah kapan authentikasi diperlukan pada sebuah sistem!	30

1.6. LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-07	CPMK-03	Selesaikan langkah praktikum 1 – 4	Hasil praktikum langkah 1 – 4	100

Langkah-Langkah Praktikum:

1. Membuat suatu folder autentifikasi pada local web server masing-masing
2. Membuat file **index.php** dengan kode php sebagai berikut:

```
<form name="FormLogin" method="post" action="auth.php">
    <tr bgcolor="#dfe9ff" >
        <td width="73" height="18"><font size="2" face="Verdana,
         Arial, Helvetica, sans-serif"> User </font></td>
        <td width="948"><font size="2" face="Verdana, Arial,
         Helvetica, sans-serif">:<input name="TxtUserID"
         type="text" size="10" maxlength="30"></font></td>
    </tr>
    <tr bgcolor="#dfe9ff" >
        <td height="18" ><font size="2" face="Verdana, Arial,
         Helvetica, sans-serif"> Password</font></td>
        <td><font size="2" face="Verdana, Arial, Helvetica,
         sans-serif">:<input name="TxtPassID" type="password"
         size="10" maxlength="30"></font></td>
    </tr>
    <tr>
```

```
        <td ><font size="2" face="Verdana, Arial, Helvetica,
         sans-serif"> </font></td>
        <td > <font size="2" face="Verdana, Arial, Helvetica,
         sans-serif"><input type="submit" name="TbLogin"
         value="Login"></font></td>
    </tr>
    <tr>
        <td><font size="2" face="Verdana, Arial, Helvetica,
         sans-serif"> </font></td>
        <td><font size="2" face="Verdana, Arial, Helvetica,
         sans-serif"> </font></td>
    </tr>
</form>
```

3. Membuat file **auth.php** dengan kode sebagai berikut:

```
<?
    session_start();

    if ($_POST['TbLogin']) {
        $TxtUserID = $_POST['TxtUserID'];
        $TxtPassID = $_POST['TxtPassID'];
        if (trim($TxtUserID)=="") {
            $pesan[] = "Data User Name kosong";
        }
        if (trim($TxtPassID)=="") {
            $pesan[] = "Data Password kosong";
        }
        if (($TxtUserID=="admin") && ($TxtPassID=="admin")) {
            $SES_USERPLG = $TxtUserID;
            session_register("SES_USERPLG");
            $SES_UIDPLG = $TxtPassID;
            session_register("SES_UIDPLG");
            echo "<B>Berhasil Login.<br> Menu Admin ada
            disini</b>";
            exit;
        }
        else {
            $pesan[] = "User dan Passord lama belum benar";
        }
        if (! count($pesan)==0 ) {
            $TxtUserID = $_POST['TxtUserID'];
            echo "<br><br>";
            echo "<div align='left'>";
            echo "  <b> Kesalahan Input : </b><br>";
            foreach ($pesan as $indeks=>$pesan_tampil) {
                $urut_pesan++;
                echo "<font color='#FF0000'>";
                echo "   ";
                echo "$urut_pesan . $pesan_tampil <br>";
                echo "</font>";
            }
            echo "</div><br>";
        }
    }
?>
```

4. Lakukan pengujian pada halaman web diatas melalui web browser dengan login yang benar, user: admin, password: admin, lalu lakukan Kembali dengan mengisi user yang kosong dan salah.

1.7. POST TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-03	Buatlah suatu sistem authentikasi (web) dengan menggunakan php dan phpmyadmin semenarik mungkin	50
2.	CPL-07	CPMK-03	Pada sistem tambahkan alert jika user salah mengisi username atau password	25
3.	CPL-07	CPMK-03	Tambahkan fitur logout	25

1.8. HASIL CAPAIAN PRAKTIKUM

Diisi oleh asisten setelah semua assessment dinilai.

No	Bentuk Assessment	CPL	CPMK	Bobot	Skor (0-100)	Nilai Akhir (Bobot x Skor)
1.	Pre-Test	CPL-07	CPMK-03	20%	100	20
2.	Praktik	CPL-07	CPMK-03	30%	100	30
3.	Post-Test	CPL-07	CPMK-03	50%	100	50
					Total Nilai	100

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

Nama : **NIM :**	**Asisten:** **Paraf Asisten:**	**Tanggal:** **Nilai:**

PRAKTIKUM 2: PASSWORD MANAJEMEN

Pertemuan ke : 2

Total Alokasi Waktu : 90 menit
- Materi : 15 menit
- Pre-Test : 15 menit
- Praktikum : 45 menit
- Post-Test : 15 menit

Total Bobot Penilaian : 100%
- Pre-Test : 20 %
- Praktik : 30 %
- Post-Test : 50 %

Pemenuhan CPL dan CPMK:

CPL-07	Mampu memilih, membuat dan menerapakan teknik, sumber daya, penggunaan perangkat teknik modern dan implementasi teknologi informasi untuk memecahkan masalah.
CPMK-03	Mahasiswa mampu memahami pengertian dan pentingnya keamanan data dan sistem komputer.

2.1. DESKRIPSI CAPAIAN PEMBELAJARAN

Setelah mengikuti praktikum ini mahasiswa diharapkan mampu:
1. Memahami dan mengimplementasikan prinsip autentikasi.

2.2. INDIKATOR KETERCAPAIAN PEMBELAJARAN

Indikator ketercapaian diukur dengan:

CPL-07	CPMK-03	Mahasisiwa mampu menganalisa dan menerapkan prinsip autentikasi pengguna elektronik berbasis password, token,biometric dan Remote User Authentication.

2.3. TEORI PENDUKUNG

Untuk dapat mengakses system operasi Linux digunakan mekanisme password. Pada distribusidistribusi Linux yang lama, password tersebut disimpan dalam suatu file text yang terletak di /etc/passwd. File ini harus dapat dibaca oleh setiap orang (world readable) agar dapat digunakan oleh program-program lain yang menggunakan mekanisme password tersebut.

Contoh isi file /etc/passwd:

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin:
adm:x:3:4:adm:/var/adm:
```

```
rms:x:100:100:Richard M Stallman:/home/rms:/bin/bash
dmr:x:101:101:Dennis M Ritchie:/home/dmr:/bin/bash
linus:x:102:102:Linus Torvalds:/home/linus:/bin/bash
```

Keterangan :
Field pertama : nama login
Field kedua : password yang terenkripsi
Field ketiga : User ID
Field keempat : Group ID
Field kelima : Nama sebenarnya Field
Field keenam : Home directory user Field
Field ketujuh : User shell

Password login yang terdapat pada file /etc/passwd dienkripsi dengan menggunakan algoritma DES yang telah dimodifikasi. Meskipun demikian hal tersebut tidak mengurangi kemungkinan password tersebut dibongkar(crack). Karena penyerang (attacker) dapat melakukan dictionary-based attack dengan cara:

Menyalin file /etc/passwd tersebut.

Menjalankan program-program yang berguna untuk membongkar password, contohnya adalah John the Ripper (www.openwall.com/john/) .

Untuk mengatasi permasalahan ini pada distribusi-distribusi Linux yang baru digunakan program Utility shadow password yang menjadikan file /etc/passwd tidak lagi berisikan informasi password yang telah dienkripsi, informasi tersebut kini disimpan pada file /etc/shadow yang hanya dapat dibaca oleh root.

Berikut ini adalah contoh file /etc/passwd yang telah di-shadow :

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin:
adm:x:3:4:adm:/var/adm:
rms:x:100:100:Richard M
Stallman:/home/rms:/bin/bash
dmr:x:101:101:Dennis M
Ritchie:/home/dmr:/bin/bash
linus:x:102:102:Linus
Torvalds:/home/linus:/bin/bash
```

Dengan demikian, penggunaan shadow *password* akan mempersulit attacker untuk melakukan *dictionary-based* attack terhadap file *password*.

Selain menggunakan *shadow password* beberapa distribusi Linux juga menyertakan program hashing MD5 yang menjadikan *password* yang dimasukkan pemakai dapat berukuran panjang dan relatif mudah diingat karena berupa suatu *passphrase*.

Mekanisme yang telah disediakan sistem operasi tersebut di atas tidaklah bermanfaat bila pemakai tidak menggunakan password yang "baik". Berikut ini adalah beberapa kriteria yang dapat digunakan untuk membuat password yang "baik" :

1. Jangan menggunakan nama *login* anda dengan segala variasinya.
2. Jangan menggunakan nama pertama atau akhir anda dengan segala variasinya.
3. Jangan menggunakan nama pasangan atau anak anda.

4. Jangan menggunakan informasi lain yang mudah didapat tentang anda, seperti nomor telpon, tanggal lahir.
5. Jangan menggunakan *password* yang terdiri dairi seluruhnya angka ataupun huruf yang sama.
6. Jangan menggunakan kata-kata yang ada di dalam kamus. Atau daftar kata lainnya.
7. Jangan menggunakan *password* yang berukuran kurang dari 6 karakter.
8. Gunakan *password* yang merupakan campuran antara huruf kapital dan huruf kecil.
9. Gunakan *password* dengan karakter-karakter non alfabet.
10. Gunakan *password* yang mudah diingat, sehingga tidak perlu ditulis,
11. Gunakan *password* yang mudah diketikkan, tanpa perlu melihat pada keyboard.

Beberapa *tool* yang bisa dipakai untuk melihat kuat tidaknya *password* adalah Jhon the Ripper. Kita bisa memakai utility ini untuk melihat kuat tidaknya suatu *password* yang ada pada komputer.

2.4. HARDWARE DAN SOFTWARE

Hardware dan software yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. Sistem Operasi Linux
3. Notepad

2.5. PRE-TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-03	Apa itu password management?	30
2.	CPL-07	CPMK-03	Sebutkan kriteria apa saja yang dapat digunakan untuk membuat password yg baik?	30
3.	CPL-07	CPMK-03	Menurut kalian bagaimana cara memanagement password kita agar tidak lupa dan tidak mudah diketahui orang lain?	40

2.6. LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-07	CPMK-03	Selesaikan langkah praktikum 1 – 6	Hasil praktikum langkah 1 – 6	100

Langkah-Langkah Praktikum:

1. Login sebagai root dan buatlah beberapa 5 user baru, selanjutnya beri password setiap komputer. Berikan 3 user baru bad password yang hanya terdiri dari 4 karakter. Selanjutnya sisanya buat strong password buat minimal 8 karakter didalamnya kombinasi angka huruf dan karakter special seperti $#@%^&.
2. Lakukan installasi John the Ripper, ambil source yang sudah disiapkan oleh dosen/asisten praktikum.
3. Jalankan John the Ripper :

```
# cd /var/lib/john #
```

```
umask 077
# unshadow /etc/passwd /etc/shadow >
mypasswords # john mypasswords

Untuk melihat password jalankan command berikut
: # john -show mypasswords

Anda dapat menginstruksikan john the ripper unutk melihat password user atau
gorup tertentu dengan option sebagai berikut : -users:u1,u2,... or -groups:g1,g2,...,

# john -users:nama_user1,nama_user2,nama_user3 mypasswords
```

4. Untuk memastikan password kita baik atau tidak, buatlah program dibawah ini, untuk melakukan testing bagaimanan password yang baik dan yang jelek.

```
#include <stdlib.h> #include <unistd.h>
#include <stdio.h> #include <crack.h>
#define DICTIONARY "/usr/lib/cracklib_dict"

int main(int argc, char *argv[]) {
    char *password; char *problem; int
    status = 0;
    printf("\nEnter an empty password or Ctrl-D to quit.\n");
    while ((password = getpass("\nPassword: ")) != NULL &&
*password ) {
        if ((problem = FascistCheck(password, DICTIONARY)) !=
NULL) {
            printf("Bad password: %s.\n", problem); status = 1;
        }
        else {
            printf("Good password!\n");
        }
    }
    exit(status);
}
```

5. Kompilasi program yang sudah anda buat dan jalankan, berikut contoh kompilasi dan cara menjalankan.

```
$ gcc cracktest.c -lcrack -o cracktest

$ ./cracktest

Enter an empty password or Ctrl-D to quit. Password: xyz

Bad password: it's WAY too
short. Password: elephant

Bad password: it is based on a dictionary word.
Password: kLu%ziF7

Good password!
```

6. Dalam suatu system kita juga bisa mencari user yang tidak diberi password, jalankan perintah berikut :

```
# awk -F: '$2 == "" { print $1, "has no password!" }' /etc/shadow.
```

2.7. POST TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-03	Jelaskan Langkah instalasi sampai bisa membuat menggunakan aplikasi 1password	50
2.	CPL-07	CPMK-03	Berikan contoh password yang baik sesuai dengan kriteria yang ada	50

2.8. HASIL CAPAIAN PRAKTIKUM

Diisi oleh asisten setelah semua assessment dinilai.

No	Bentuk Assessment	CPL	CPMK	Bobot	Skor (0-100)	Nilai Akhir (Bobot x Skor)
1.	Pre-Test	CPL-07	CPMK-03	20%	100	20
2.	Praktik	CPL-07	CPMK-03	30%	100	30
3.	Post-Test	CPL-07	CPMK-03	50%	100	50
					Total Nilai	100

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

Nama : **NIM :**	**Asisten:** **Paraf Asisten:**	**Tanggal:** **Nilai:**

PRAKTIKUM 3: DIGITAL SIGNATURE

Pertemuan ke : 3

Total Alokasi Waktu : 90 menit
- Materi : 15 menit
- Pre-Test : 15 menit
- Praktikum : 45 menit
- Post-Test : 15 menit

Total Bobot Penilaian : 100%
- Pre-Test : 20 %
- Praktik : 30 %
- Post-Test : 50 %

Pemenuhan CPL dan CPMK:

CPL-07	Mampu memilih, membuat dan menerapakan teknik, sumber daya, penggunaan perangkat teknik modern dan implementasi teknologi informasi untuk memecahkan masalah.
CPMK-03	Memahami prinsip otentikasi pengguna sistem elektronik dan prinsip kontrol akses untuk meningkatkan keamanan.

3.1. DESKRIPSI CAPAIAN PEMBELAJARAN

Setelah mengikuti praktikum ini mahasiswa diharapkan mampu:
1. Memahami dan mengimplementasikan prinsip autentikasi.

3.2. INDIKATOR KETERCAPAIAN PEMBELAJARAN

Indikator ketercapaian diukur dengan:

CPL-07	CPMK-03	Mahasisiwa mampu menganalisa dan menerapkan prinsip autentikasi pengguna elektronik berbasis Digital signature.

3.3. TEORI PENDUKUNG

Tanda tangan digital digital merupakan salah satu cara untuk memberikan authentication, integrity, dan non-repudiation pada dokumen digital yang akan dikirimkan/didistribusikan. Prinsip yang digunakan dalam tanda tangan digital adalah data yang dikirimkan harus ditanda tangani oleh pengirim dan tanda tangan bisa diperiksa oleh penerima untuk memastikan keaslian data yang dikirimkan. Proses ini menganalogikan proses penandatanganan dokumen kertas oleh yang berwenang sebelum dikirimkan. Dengan cara ini pengirim bertanggung jawab terhadap isi dokumen dan dapat dicek keaslian dokumen oleh penerima. Menurut Arrianto Mukti Wibowo [1] sifat dimiliki oleh tanda tangan digital adalah:

1. Otentik, tak bisa/sulit ditulis/ditiru oleh orang lain. Pesan dan tanda tangan pesan tersebut juga dapat menjadi barang bukti, sehingga penandatangan tak bisa menyangkal bahwa dulu ia tidak pernah menandatanganinya.
2. Hanya sah untuk dokumen (pesan) itu saja ayau kopinya yang sama persis. Tanda tangan itu tidak bisa dipindahkan ke dokumen lainnya, meskipun dokumen lain itu hanya berbeda sedikit. Ini juga berate bahwa jika dokumen itu diubah, maka tanda tangan digital dari pesan tersebut tidak lagi sah.
3. Dapat diperiksa dengan mudah, termasuk oleh pihak-pihak yang belum pernah bertatap muka langsung dengan penandatangan.

Menurut Arrianto Mukti Wibowo, dkk [3], penggunaan digital signature berawal dari penggunaan teknik kriptografi yang digunakan untuk mengamankan informasi yang hendak ditransmisikan/disampaikan kepada orang yang lain yang sudah digunakan sejak ratusan tahun yang lalu. Dalam suatu kriptografi suatu pesan dienkripsi (encrypt) dengan menggunakan suatu kunci (key). Hasil dari enkripsi ini adalah berupa chipertext tersebut kemudian dikirimkan kepada tujuan yang dikehendakinya. Chipertext tersebut kemudian didekripsi (decrypt) dengan suatu kunci untuk mendapatkan informasi yang telah enkripsi tersebut. Terdapat dua macam cara dalam melakukan enkripsi yaitu dengan menggunakan kriptografi simetris (symetric crypthography/secret key crypthography) dan kriptografi simetris (asymetric crypthography) yang kemudian lebih dikenal sebagai public key crypthography. Teknologi tanda tangan digital memanfaatkan teknologi kunci publik. Sepasang kunci publik-privat dibuat untuk keperluan seseorang. Kunci privat disimpan oleh pemiliknya, dan dipergunakan untuk membuat tanda tangan digital. Sedangkan kunci publik dapat diserahkan kepada siapa saja yang ingin memeriksa tanda tangan digital yang bersangkutan pada suatu dokumen. Proses pembuatan dan pemeriksaan tanda tangan ini melibatkan sejumlah teknik kriptografi yaitu fungsi hash dan sistem kripto kunci public.

3.4. HARDWARE DAN SOFTWARE

Hardware dan software yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. Microsoft Word
3. Paint

3.5. PRE-TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-03	Jelaskan dengan bahasamu apa itu Digital Signature	30
2.	CPL-07	CPMK-03	Bagaimana Cara mekanisme kerja dari Digital Signatre sertai dengan illustrasi	40
3.	CPL-07	CPMK-03	Berdasarkan sertifikasi kelas Digital Signature, Sebutkan dan jelaskan kelas kelas tersebut	30

3.6. LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-07	CPMK-03	Selesaikan langkah praktikum 1 – 5	Hasil praktikum langkah 1 – 5	100

Langkah-Langkah Praktikum:

Digital signature dengan Microsoft Word

1. Jalankan Ms Word terlebih dahulu.
2. Dalam text editor tersebut buatlah suatu naskah yang nantinya merupakan dokumen pribadi anda.
3. Membuat tanda tangan digital:
    a. Pada tampilan menu utama pilih Signature → create key , maka akan muncul jendela baru untuk membuat kunci enkripsi dan kunci dekripsi. Yang perlu diisi cukup nama dan email saja, kemudian Generate key dan kemudian save key.
    b. Setelah disimpan, maka tanda tangan tersebut dapat digunakan kapan saja pada aplikasi Ms Word. File dengan ekstensi .dse merupakan file yang digunakan untuk menyimpan kunci public yang akan digunakan untuk memberikan tanda tangan digital pada dokumen.
    c. File/ kunci tersebut dapat diketahui oleh siapa saja. File dengan ekstensi .dsd merupakan file yang digunakan untuk menyimpan kunci private yang akan digunakan untuk memvalidasi dokumen. File ini hanya boleh diketahui/dimiliki oleh pemilik tanda tangan.
4. Memberikan tanda tangan digital pada dokumen/menandatangani dokumen secara digital. Setelah kita memiliki tanda tangan digital yg terseimpan dalam file dengan eksteni .dse dan .dsd maka kita tinggal membubuhkan tanda tangan tersebut pada dokumen, dengan memilih menu Signature Validate signature. Teks box tidak perlu diisi, cukup buka file kunci private (.dsd) dengan button browse key.
5. Simpan dokumen tersebut, sehingga document tersebut berarti sudah merupakan dokumen yang memuat tanda tangan digital kita. Digital signature pas Ms Word dalam Microsoft Office (word, excel, power point, ouytlook) juga tersedia digital signature, namun penyimpanan kunci/tamda tangannya secara online dan berbayar. Anda bisa memilih prepare pada office button (sudut kiri atas), maka ada beberapa menu pengamanan dokumen dan salah satunya digital signature.

3.7. POST TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-03	Buatlah Sebuah Surat perjanjian dengan topik bebas (Semenarik mungkin) kemudian sertakan minimal 4 pihak yang terlibat dengan masing masing pihak memiliki tanda tangan digital	50
2.	CPL-07	CPMK-03	Analisislah apakah tanda tangan digital sangat diperlukan pada zaman sekarang ini?, keluarkan semua opini kalian (opini yang logis akan mendapatkan nilai yang logis juga)	50

3.8. HASIL CAPAIAN PRAKTIKUM

Diisi oleh asisten setelah semua assessment dinilai.

No	Bentuk Assessment	CPL	CPMK	Bobot	Skor (0-100)	Nilai Akhir (Bobot x Skor)
1.	Pre-Test	CPL-07	CPMK-03	20%	100	20

2.	Praktik	CPL-07	CPMK-03	30%	100	30
3.	Post-Test	CPL-07	CPMK-03	50%	100	50
					Total Nilai	100

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

Nama : **NIM :**	**Asisten:** **Paraf Asisten:**	**Tanggal:** **Nilai:**

PRAKTIKUM 4: KRIPTOGRAFI KLASIK

Pertemuan ke : 4

Total Alokasi Waktu : 90 menit
- Materi : 15 menit
- Pre-Test : 15 menit
- Praktikum : 45 menit
- Post-Test : 15 menit

Total Bobot Penilaian : 100%
- Pre-Test : 20 %
- Praktik : 30 %
- Post-Test : 50 %

Pemenuhan CPL dan CPMK:

CPL-07	Mampu memilih, membuat dan menerapakan teknik, sumber daya, penggunaan perangkat teknik modern dan implementasi teknologi informasi untuk memecahkan masalah.
CPMK-02	Kemampuan memahami dan menerapkan konsep kriptografi, steganografi, digital signature dan manajemen key untuk meningkatkan kemanan

4.1. DESKRIPSI CAPAIAN PEMBELAJARAN

Setelah mengikuti praktikum ini mahasiswa diharapkan mampu:
1. Menjelaskan konsep enkripsi.
2. Menerapkan penggunaan konsep.

4.2. INDIKATOR KETERCAPAIAN PEMBELAJARAN

Indikator ketercapaian diukur dengan:

CPL-07	CPMK-02	Mahasisiwa memaham dan menerapkan kriptografi monoalphabetic, polyalphabetic, block cipher dan stream cipher.

4.3. TEORI PENDUKUNG

A. Caesar

Metode ini menggunakan pergeseran sederhana, sehingga metode ini tergolong dalam kelompok metode stream. Algoritma dasar dari metode ini sangat simple, setiap kunci diganti dengan huruf ketiga setelah kunci yang bersangkutan. Misalnya kita memiliki plaintext seperti berikut.

I CAME I SAW I CONQUERED

Maka kalau kita enkripsikan dengan metode ini, didapatkan cipherteksnya adalah

L FDPH L VDZ L FRQTXHUHG

Atau secara umum substitusi tersebut dapat digambarkan seperti berikut :

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Plain :	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher :	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Secara umum proses Cipher dapat didefinisikan enkripsi dapat dikodekan dengan :

Enkripsi : **Ek : i → (i+k) mod 26**
Dekripsi : **Dk : i → (i-k) mod 26**

Keterangan :
i : huruf yang akan dienkripsi/dekripsi
k : kunci (pada Caesar cipher maka kunci adalah 3)

Modulus 26 digunakan untuk plaintext dengan basis 26 karakter. Untuk plainteks dengan basis ASCII maka digunakan modulus 256

B. Vigenere

Metode ini juga merupakan dasar dari polyalphabetic substitution cipher. Beberapa ketentuan dalam metode ini antara lain :

- Setiap kunci dapat disubstitusi dengan bermacam-macam kunci yang lain.
- Menggunakan kata kunci.
- Kata kunci digunakan secara berulang.
- Kata kunci digunakan untuk menetukan enkripsi setiap alphabet dalam plainteks.
- Huruf ke-i dalam plainteks dispesifikasikan oleh alphabet yang digunakan dalam kunci.
- Penggunaan alphabet bisa berluang.

Contoh, kita akan melakukan enkripsi pesan plainteks :

Pi : TO BE OR NOT TO BE THAT IS THE QUESTION

Dengan menggunakan kata kunci RELATIONS. Kita mulai dengan menuliskan kunci, berulang kali di bagian atas plaintext message.

Keyword :	R	E	L	A	T		I	O	N	S	R		E	L	A	T	I		O	N	S	R	E		L	A	T	I	O		N	S	R	E	L
Plaintext :	T	O	B	E	O		R	N	O	T	T		O	B	E	T	H		A	T	I	S	T		H	E	Q	U	E		S	T	I	O	N
Ciphertext:	K	S	M	E	H		Z	B	B	L	K		S	M	E	M	P		O	G	A	J	X		S	E	J	C	S		F	L	Z	S	Y

Secara umum proses enkripsi pada vigenere dapat dituliskan :

Ek : Ci → (Mi + (Kj – A)) mod 26

Untuk Dekripsi maka:

Pi = (Ci – Ki) mod 26

Keterangan :

Ci : nilai decimal karakter ciphertext ke-i

Pi : nilai decimal karakter plaintext ke-i

Ki : nilai decimal karakter kunci ke-i

4.4. HARDWARE DAN SOFTWARE

Hardware dan software yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. Dev C++
3. Tabel ASCII

4.5. PRE-TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-02	Jelaskan apa itu kriptografi !	25
2.	CPL-07	CPMK-02	Sebutkan dan Jelaskan Jenis - Jenis kriptografi !	25
3.	CPL-07	CPMK-02	Enkripsikan Plaintext Berikut kedalam Caesar Cipher Plaintext : Saya (Nama Lengkap) Mahasiswa Faktultas Teknologi Industri Teknik Informatika Universitas Ahmad Dahlan Kerjakan lengkap dengan langkah2nya !	50

4.6. LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-07	CPMK-02	Selesaikan langkah praktikum 1 – 3	Hasil praktikum langkah 1 – 3	100

Langkah-Langkah Praktikum:

1. Buka Dev C++
2. Membuat program C++ untuk proses enkripsi dan dekripsi kalimat (belum ada source code nya)
3. Jalankan.

4.7. POST TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-02	Lakukan Proses Enkripsi dan dekripsi dengan Metode vigenere secara manual pada plaintext: Plaintext : TEKNIK INFORMATIKA FTI UNIVERSITAS AHMAD DAHLAN YOGYAKARTA Key : GADALAWAN	50
2.	CPL-07	CPMK-02	Berdasarakan Proses Enkripsi dan deskripsi yang anda lakukan pada soal point 1 maka implementasikanlah kedalam program menggunakan C++.	50

4.8. HASIL CAPAIAN PRAKTIKUM

Diisi oleh asisten setelah semua assessment dinilai.

No	Bentuk Assessment	CPL	CPMK	Bobot	Skor (0-100)	Nilai Akhir (Bobot x Skor)
1.	Pre-Test	CPL-07	CPMK-02	20%	100	20
2.	Praktik	CPL-07	CPMK-02	30%	100	30
3.	Post-Test	CPL-07	CPMK-02	50%	100	50
					Total Nilai	100

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

Nama : **NIM :**	**Asisten:** **Paraf Asisten:**	**Tanggal:** **Nilai:**

PRAKTIKUM 5: KRIPTOGRAFI MODERN

Pertemuan ke : 5

Total Alokasi Waktu : 90 menit
- Materi : 15 menit
- Pre-Test : 15 menit
- Praktikum : 45 menit
- Post-Test : 15 menit

Total Bobot Penilaian : 100%
- Pre-Test : 20 %
- Praktik : 30 %
- Post-Test : 50 %

Pemenuhan CPL dan CPMK:

CPL-07	Mampu memilih, membuat dan menerapakan teknik, sumber daya, penggunaan perangkat teknik modern dan implementasi teknologi informasi untuk memecahkan masalah.
CPMK-02	Kemampuan memahami dan menerapkan konsep kriptografi, steganografi, digital signature dan manajemen key untuk meningkatkan kemanan

5.1. DESKRIPSI CAPAIAN PEMBELAJARAN

Setelah mengikuti praktikum ini mahasiswa diharapkan mampu:

1. Memahami konsep dan peneranapan Kriptografi Asimetrik dan Public Key Infrastructure.

5.2. INDIKATOR KETERCAPAIAN PEMBELAJARAN

Indikator ketercapaian diukur dengan:

CPL-07	CPMK-02	Mahasisiwa mampu memahami dan menerapkan kriptografi Asymetric cryptography & Public Key Infrastructure: Komponen-komponen, kebijakan, penerapan hash function, secret sharing

5.3. TEORI PENDUKUNG

Dalam kriptografi, **MD5 (Message-Digest algorithm 5)** ialah fungsi hash kriptografik yang digunakan secara luas dengan hash value 128-bit. Pada standard Internet (RFC 1321), MD5 telah dimanfaatkan secara bermacam-macam pada aplikasi keamanan, dan MD5 juga umum digunakan untuk melakaukan autentikasi suatu data digital atau pengujian integritas sebuah file.

MD5 didesain oleh Ronald Rivest pada tahun 1991 untuk menggantikan hash function sebelumnya, yaitu MD4 yang berhasil diserang oleh kriptanalis. Perlu ditegaskan bahwa Algoritma MD5 dengan ukuran input berapapun akan menghasilkan pesan ringkas yang panjangnya sama/ tetap yang dinyatakan dalam kode heksadesimal yang panjangnya 128 bit, perlu diingat bahwa satu karakter heksadesimal = 4 bit, berarti panjang outputnya 32 karakter heksa.

Terkadang kita menginginkan isi arsip tetap terjaga keasliannya, bila terjadi perubahan kecil

pada arsip tersebut maka akan mengalami kesulitan dalam mendeteksinya jikalau ia berukuran besar. Fungsi hash dapat digunkan untuk menjaga keutuhan data, caranya bangkitkan message digest dari isi arsip dengan menggunakan algoritma MD5 dan datanya bisa disimpan dalam basis data, kemudian verifikasi isi arsip dapat dilakukan secara berkala dengan membandingkan message digest.

Jika terjadi perbedaan antara isi arsip sekarang dengan message digest dari arsi asli maka disimpulkan ada modifikasi terhadap isi arsip. Aplikasi ini didasarkan pada kenyataan bahwa perubahan 1 bit pada pesan akan mengubah secara rata- rata setengah dari bit-bit message digest, dengan kata lain fungsi hash sangat peka terhadap perubahan sekecil apa pun pada data masukan.

Contoh : file txt yang berisi teks berikut

Aplikasi dari fungsi hash antara lain untuk memverifikasi kesamaan Salinan suatu arsip dengan arsip aslinya yang tersimpan di dalam sebuah basisdata terpusat, kemudian apa pengertian dari Fungsi Hash Satu Arah(one-way Hash) yaitu fungsi hash yang bekerja dalam stu arah, dan pesan yang sudah diubah menjadi message digest tidak dapat dikembalikan lagi menjadi pesan semula, bila dua pesan yang berbeda akan selalu menghasilkan nilai Hash yang berbeda pula.

Memiliki hash MD5 : 4B97E98235F061A3923C4B005E9704A9

Jika huruf “A” pada awal kalimat aplikasi diganti dengan huruf “a” sehingga menjadi “aplikasi” ternyata nilai hash MD5-nya berubah sangat signifikan yaitu : 44333411A4F8A0FDB901F1596D743668.

5.4. HARDWARE DAN SOFTWARE

Hardware dan software yang digunakan dalam praktikum ini yaitu:

1. Software MD5 Check Utility V2.31. Software ini ukurannya cukup kecil yaitu 99,3 Kb, dan dapat di download pada link berikut http://www.thefreecountry.com/utilities/free-md5- sum-tools.shtml
2. Beberapa file yang sudah ada pada computer
3. Tidak tertutup kemungkinan menggunakan software lain yang mengimplementasikan metode kriptosistem MD5, yang cukup banyak tersedia diinternet.

5.5. PRE-TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-02	Jelaskan Perbedaan Kriptografi Klasik dan Modern	30
2.	CPL-07	CPMK-02	Sebutkan dan jelaskan jenis jenis algoritma yang termasuk dalam kriptografi Modern	30
3.	CPL-07	CPMK-02	Jelaskan perbandingan (Kelebihan dan Kekurangan) antara algoritma enkripsi MD5 dan SHA1	40

5.6. LANGKAH PRAKTIKUM

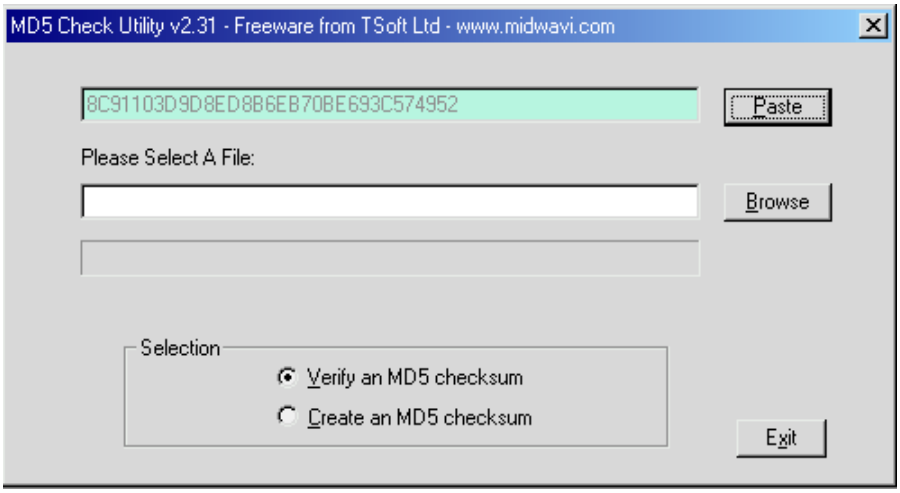
Aturan Penilaian (Total Skor: 100):

No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-07	CPMK-02	Selesaikan langkah praktikum A-D	Hasil praktikum langkah A-D	100

Langkah-Langkah Praktikum:

A. PENGGUNAAN TOOL

1. Dst Pastikan anda telah mengcopy file MD5.rar dengan nilai hash MD5 : 8C91103D9D8ED8B6EB70BE693C574952 , dalam file tersebut terdapat 2 file MD5.exe dan MD5 Readme.txt
2. Esktrak file tersebut dan jalankan file MD5 (untuk menjalankan aplikasi ini tidak perlu diinstal), sehingga akan menampilkan use interface seperti berikut :



Gambar 5. 1 UI MD5 Utility

Catatan: nilai pada *textbox* yang atas (sebelah paste) sesuai isi *clipboard*, kalau *clipboard* kosong *textbox* tersebut juga kosong.

B. AUTENTIKASI FILE

1. Bukalah sembarangan file yang ada di computer anda namun dengan syarat file yang digunakan mudah untuk dilakukan pengeditan, missal MS Word, atau teks. (Hal ini digunakan untuk mempermudah penjelasan dan keterkaitan pemberian contoh selanjutnya). Perlu diingat nama file dan lokasi penyimpanan serta ukuran dari file tersebut.
2. Hitunglah nilai hash-nya dengan aplikasi di atas, dengan cara :
   - Pilih create an MD5 Checksum
   - Pilih file yang sudah dibuat
   - Lalu pilih OK
   - Akan muncul nilai hash, silahkan di copy-paste pada notepad
3. Buatlah sedikit perubahan pada file tersebut walaupun hanya 1 bit atau 1 byte, misalnya huruf “a” diganti huruf “B”, lali simpan file tersebut.
4. Verifikasilah nilai hash tersebut dengan nilai asli (cek langkah 2) dengan cara :
   - Copy nilai hash yang ada pada notepad (hasil Langkah 2)
   - Pilih verify an MD5 Checksum pada aplikasi MD5
   - Pilih paste
   - Pilih Browse dan pilih hasil file yang sudah di edit (Langkah no 3)
5. Untuk membuktikan dan memastikan, lakukan autentikasi (langkah 1-4) untuk format file lain dengan ukuran yang lebih besar.

C. DIGITAL SIGNATURE

1. Autentikasi juga dapat dilakukan pada bagian/komponen dari dokumen, salah satunya autentikasi tandatangan digital.

D. APLIKASI LAIN

1. Aplikasi yang disediakan yaitu software MD5 Check Utility V2.31 hanya merupakan salah satu software yang mengimplementasikan metode MD5. Banyak apliaksi sejenis yang beredar secara freeware.

5.7. POST TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-02	Tuliskan Langkah - langkah dalam mengenkripsi disertai dengan Screen Capture dan jelaskan tujuan pada setiap langkah langkahnya!	50
2.	CPL-07	CPMK-02	Analisis dan simpulkan apakah semua jenis file dapat di enkripsi dengan algoritma MD5?, Jelaskan jawaban anda!	50

5.8. HASIL CAPAIAN PRAKTIKUM

Diisi oleh asisten setelah semua assessment dinilai.

No	Bentuk Assessment	CPL	CPMK	Bobot	Skor (0-100)	Nilai Akhir (Bobot x Skor)
1.	Pre-Test	CPL-07	CPMK-02	20%	100	20
2.	Praktik	CPL-07	CPMK-02	30%	100	30
3.	Post-Test	CPL-07	CPMK-02	50%	100	50
					Total Nilai	100

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

Nama : **NIM :**	**Asisten:** **Paraf Asisten:**	**Tanggal:** **Nilai:**

PRAKTIKUM 6: INFORMATION HIDING

Pertemuan ke : 6

Total Alokasi Waktu : 90 menit
- Materi : 15 menit
- Pre-Test : 15 menit
- Praktikum : 45 menit
- Post-Test : 15 menit

Total Bobot Penilaian : 100%
- Pre-Test : 20 %
- Praktik : 30 %
- Post-Test : 50 %

Pemenuhan CPL dan CPMK:

CPL-07	Mampu memilih, membuat dan menerapakan teknik, sumber daya, penggunaan perangkat teknik modern dan implementasi teknologi informasi untuk memecahkan masalah.
CPMK-03	Memahami prinsip otentikasi pengguna sistem elektronik dan prinsip kontrol akses untuk meningkatkan keamanan.

6.1. DESKRIPSI CAPAIAN PEMBELAJARAN

Setelah mengikuti praktikum ini mahasiswa diharapkan mampu:

1. Memahami konsep, prinsip information hiding, teknik steganografi dan watermarking untuk proteksi hak cipta.

6.2. INDIKATOR KETERCAPAIAN PEMBELAJARAN

Indikator ketercapaian diukur dengan:

CPL-07	CPMK-03	Mahasiswa mampu menerapkan penyembunyian pesan dengan information hiding, teknik LSB dalam steganografi dan watermarking.

6.3. TEORI PENDUKUNG

Tuliskan teori pendukung disini. Contoh penulisan Gambar 1.1.

Steganography berbeda dengan cryptography, letak perbedaan adalah komponen input dan hasil keluarannya. Proses steganography membutuhkan minimal 2 komponen input/objek yaitu file host (stego medium) yang akan dijadikan sebagai induk penyembunyian dan informasi digital yang akan di sembunyikan. Hasil dari cryptography biasanya berupa data yang berbeda dari bentuk aslinya dan biasanya data seolah-olah berantakan (namun dapat dikembalikan ke data semula), sedangkan hasil keluaran dari steganography secara visual (indrawi) memiliki bentuk yang sama dengan data aslinya, tentu saja persepsi ini oleh indra manusia, tetapi tidak oleh computer atau pengolah data digital lainnya. Selain itu pada steganography keberadaan informasi disembunyikan/tidak diketahui dan terjadi penyampulan tulisan (covered writing). Sedangkan pada cryptography informasi dikodekan dengan

enkripsi atau metode pengkodean dan informasi diketahui keberadaannya tetapi tidak dimengerti maksudnya. Istilah dalam information hiding dapat dijelaskan sebagai berikut:

File host : file objek yang akan disisipi data digital lain
File informasi : file yang akan disisipkan dalam data digital lain
File stego medium : file induk yang sudah disisipi file informasi

6.4. HARDWARE DAN SOFTWARE

Hardware dan software yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. Command Prompt
3. Notepad

6.5. PRE-TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-03	Jelaskan Apa itu Information Hidding dan Steganografi!	30
2.	CPL-07	CPMK-03	Jelaskan Perbedaan Steganografi dan Kriptography!	20
3.	CPL-07	CPMK-03	Jabarkan Konsep dari Stegabografi disertai ilustrasi gambar!	40

6.6. LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-07	CPMK-03	Selesaikan langkah praktikum 1-4	Hasil praktikum langkah 1 – 4	100

Langkah-Langkah Praktikum:

1. Penggunaan tool
    a. Pastikan anda sudah mengcopy file software S-Tool4. Jalankan program tersebut (tanpa harus diinstall)
2. Penyembunyian data
    a. Tentukan file host/induk (yang akan disisipi) kemudian drag and drop pada window tersebut
    b. Tentukan file informasi yg akan disembunyikan, drag and drop pd file host yg telah ada pada window Stool masukan password sesuai dgn selera
3. Sehingga terbentuk stego medium yang telah disisipi dengan file informasi dengan nama window hiden data,simpanlah file tersebut. Lakukan analisa atas file stego medium dan host yg belum ditempeli.
    a. Lakukan revealing dgn click kanan. Betulkah data yg termuat (hasil revealing)
    b. Lakukan modifikasi terhadap file stego medium
4. Lakukan Langkah b-c tersebut dengan menggunakan minimal 2 jenis data host yang berbeda, missal :
    a. Gambar
    b. Audio

c. Dokumen

6.7. POST TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-03	Lakukan kembali proses Menyisipkan informasi berupa: a. Nama Lengkap b. NIM c. Kelas d. Hoby e. Ceritakan Sedikit tentang apa yang akan anda lakukan setelah lulus dari TIF UAD semua informasi diatas disimpan dalam file gambar foto terbaik diri anda, laporan berupa langkah dan hasil dari proses penyisipan informasi	100

6.8. HASIL CAPAIAN PRAKTIKUM

Diisi oleh asisten setelah semua assessment dinilai.

No	Bentuk Assessment	CPL	CPMK	Bobot	Skor (0-100)	Nilai Akhir (Bobot x Skor)
1.	Pre-Test	CPL-03	CPMK-01	20%	100	20
2.	Praktik	CPL-03	CPMK-01	30%	100	30
3.	Post-Test	CPL-03	CPMK-01	50%	100	50
					Total Nilai	100

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

Nama : **NIM :**	**Asisten:** **Paraf Asisten:**	**Tanggal:** **Nilai:**

PRAKTIKUM 7: FIREWALL

Pertemuan ke : 7

Total Alokasi Waktu : 90 menit
- Materi : 15 menit
- Pre-Test : 15 menit
- Praktikum : 45 menit
- Post-Test : 15 menit

Total Bobot Penilaian : 100%
- Pre-Test : 20 %
- Praktik : 30 %
- Post-Test : 50 %

Pemenuhan CPL dan CPMK:

CPL-07	Mampu memilih, membuat dan menerapakan teknik, sumber daya, penggunaan perangkat teknik modern dan implementasi teknologi informasi untuk memecahkan masalah.
CPMK-04	Memahami pentingnya keamanan sistem dan jaringan komputer (wireless Network security).

7.1. DESKRIPSI CAPAIAN PEMBELAJARAN

Setelah mengikuti praktikum ini mahasiswa diharapkan mampu:

1. Memahami dan menerapkan penggunaan firewall untuk pengaturan kebijakan akses untuk filtering instruksi.

7.2. INDIKATOR KETERCAPAIAN PEMBELAJARAN

Indikator ketercapaian diukur dengan:

CPL-07	CPMK-04	Mahasisiwa memahami karakteristik, tipe firewall, mampu membangun firewall sebagai kebijakan akses untuk filtering instruksi.

7.3. TEORI PENDUKUNG

Firewall adalah system atau sekelompok system yang menetapkan kebijakan kendali akses antara dua jaringan. Secara prinsip, firewall dapat dianggap sebagai sepasang mekanisme : yang pertama memblok lalu lintas, yang kedua mengijinkan lalu lintas jaringan. Firewall dapat digunakan untuk melindungi jaringan anda dari serangan jaringan oleh pihak luar, namun firewall tidak dapat melindungi dari serangan yang tidak melalui firewall dan serangan dari seseorang yang berada di dalam jaringan anda, serta firewall tidak dapat melindungi anda dari program-program aplikasi yang ditulis dengan buruk.

Secara umum, firewall biasanya menjalankan fungsi :

- **Analisa dan filter paket**

Data yang dikomunikasikan lewat protocol di internet, dibagi atas paket-paket. Firewall dapat menganalisa paket ini, kemudian memperlakukan sesuai kondisi tertentu. Misal, jika ada paket a makan akan dilakukan b. Untuk filter paket, dapat dilakukan di Linux tanpa program tambahan.

- **Blocking isi dan protocol**
  Firewall dapat melakukan blocking terhadap isi paket, misalnya berisi applet jave, ActiveX, VBScript, Cookie.
- **Autentikasi koneksi dan enkripsi**
  Firewall umumnya memiliki kemampian untuk menjalankan enkripsi dalam autentikasi identitas user, integritas dari satu session, dan melapisi transfer data dari intipan pihak lain. Enkripsi yang dimaksud termasuk DES, Triple DES, SSL, IPSEC, SHA, MD5, BlowFish, IDEA, dsb

Secara konseptual, terdapat dua macam firewall yaitu

- **Network level**
  Firewall network level mendasarkan keputusan mereka pada alamat sumber, alamat tujuan dan port yang terdapat dalam setiap paket IP. Network level firewall sangat cepat dan sangat transparan bagi pemakai. Application level firewall biasanya adalah host yang berjalan sebagai proxy server, yang tidak mengijinkan lalu lintas antar jaringan, dan melakukan logging dan auditing lalu lintas yang melaluinya.
- **Application level**
  Application level firewall menyediakan laporan audit yang lebih rinci dan cenderung lebih memaksakan model keamanan yang lebih konservatif daripada network level firewall. Firewall ini bisa dikatakan sebagai jembatan. Application-Proxy Firewall biasanya berupa program khusus, misal squid

Firewall IPTabels packet filtering memiliki tiga aturan (policy), yaitu :

- **INPUT**
  Mengatur paket data yang memasuki firewall dari arah intranet maupun internet. kita bisa mengelola komputer mana saja yang bisa mengakses firewall. misal: hanya komputer IP 192.168.1.100 yang bisa SSH ke firewall dan yang lain tidak boleh.
- **OUTPUT**
  Mengatur paket data yang keluar dari firewall kea rah internet. Biasanya output tidak diset, karena busa membatasi kemampuan firewall itu sendiri.
- **FORWARD**
  Mengatur paket data yang melintasi firewall dari arah internet ke intranet maupun sebaliknya. Policy forward paling banyak dipakai saat ini untuk mengatur koneksi internet berdasarkan port, mac address dan alamat IP.

Selain aturan (policy) firewall iptables juga mempunyai parameter yang disebut dengan TARGET, yaitu status yang menentukan koneksi di iptables diizinkan lewat atau tidak. **Target ada tiga macam**, yaitu :

- **ACCEPT**
  Akses diterima dan diizinkan melewati firewall
- **REJECT**
  Akses ditolak, koneksi dari computer klien yang melewati firewall langsung terputus, biasanya terdapat pesan “Connection Refused”. Target Reject tidak menghabiskan bandwidth internet karena akses langsung ditolak, hal ini berbeda dengan DROP.

- **DROP**
  Akses diterima tetapi paket data langsung dibuang oleh kernel, sehingga pengguna tidak mengetahui kalau koneksinya dibatasi oleh firewall. Pengguna melihay seakan-akan server yang dihubungi mengalami permasalahan teknis. Pada koneksi internet yang sibuk dengan trafik tinggi Target Drop sebaiknya jangan digunakan.

7.4. HARDWARE DAN SOFTWARE

Hardware dan software yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. Command Prompt
3. Notepad

7.5. PRE-TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-04	Jelaskan apa itu firewall!	30
2.	CPL-07	CPMK-04	Sebutkan dan jelaskan fungsi dari firewall.	40
3.	CPL-07	CPMK-04	Jelaskan 2 macam firewall	30

7.6. LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-07	CPMK-04	Selesaikan langkah praktikum 1 – 11	Hasil praktikum langkah 1 – 11	100

Langkah-Langkah Praktikum:

a. Mengatur firewall pada OS linux dengan iptables:
   1. Install iptables
      Sudo apt-get install iptables
   2. Melihat chain iptables : input, forward dan output
      iptables –L –v
   3. Melihat policy iptables
      sudo iptables –L | grep policy
   4. Mengatur rules iptables
      - **Koneksi dari satu IP Address**
        iptables –A INPUT –s 192.168.70.1 –j DROP
      - **Koneksi dari range IP Address**
        iptables –A INPUT –s 192.168.70.1/24 –j DROP
        atau
        iptables –A INPUT –s 192.168.70.1/255.255.255.0 –j DROP

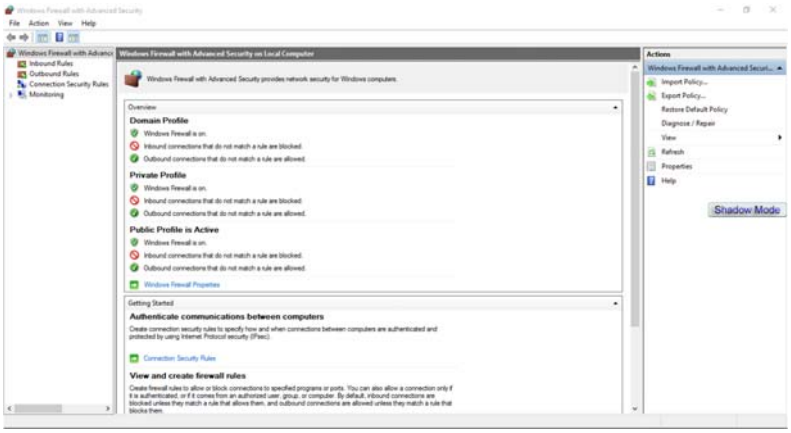
- **Koneksi dari port tertentu**
  iptables –A INPUT –p tcp –dport ssh –s 192.168.70.1 –j DROP -> dari satu IP Address
  iptables –A INPUT –p tcp –dport ssh –j DROP -> dari semua IP Address

- **Menyimpan rules iptables**
  Ubuntu:
  sudo /sbin/iptables-save
  Red Hat/CentOS
  /sbin/service iptables save
  atau
  /etc/init.d/iptables save

b. Mengatur firewall pada OS windows dengan Windows Firewall with Advanced Security

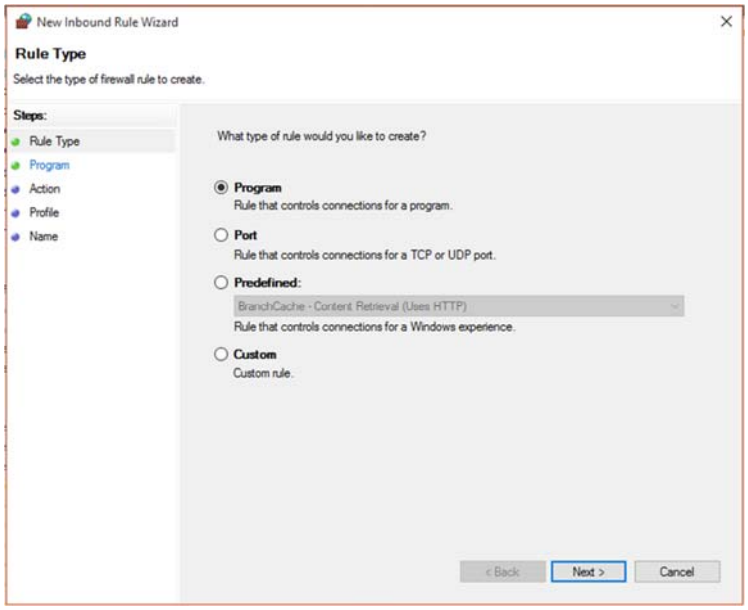
1. Buka Windows Firewall with Advanced Security
   Klik Start->Windows Administrative Tools->Windows Firewall with Advanced Security
   Atau pada command prompt

2. Klik Inbound Rules → Klik New Rules



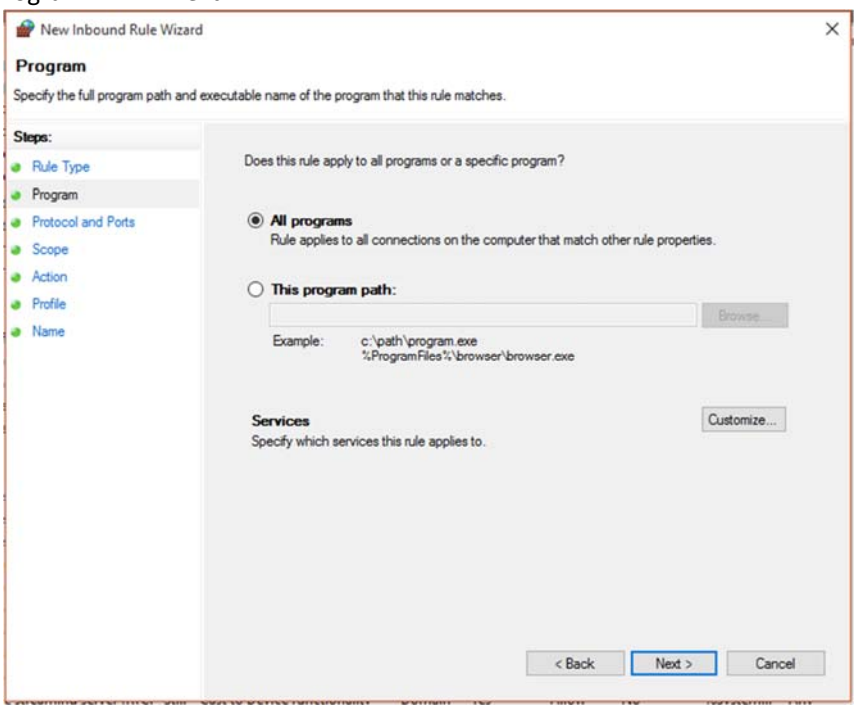
Gambar 7. 1 Proses inbound rule firewall 1

3. Pilih Custom → klik next



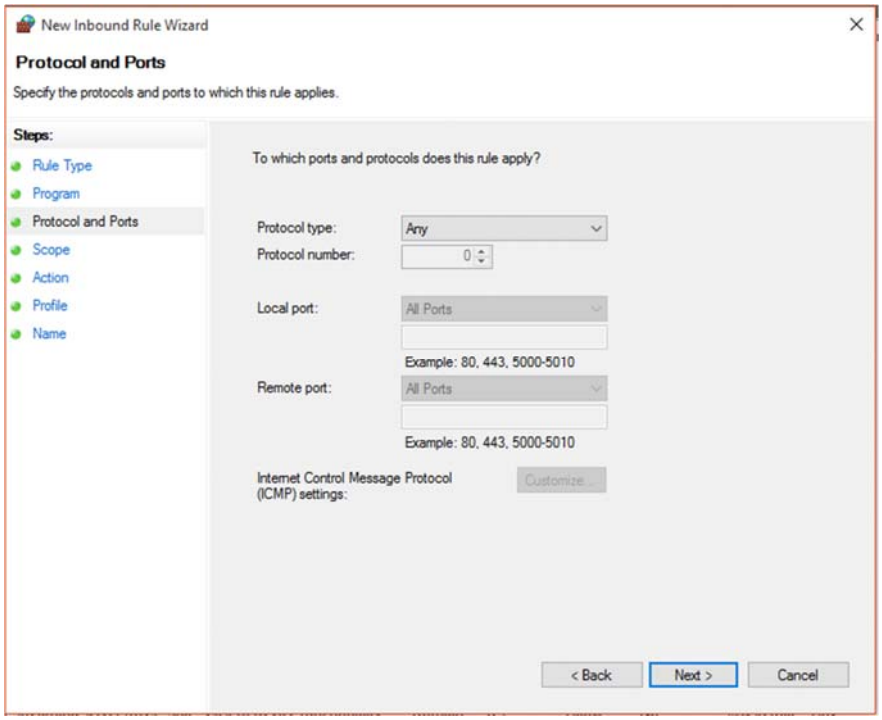
Gambar 7. 2 Proses inbound rule firewall 2

4. Pilih All Program → Klik next



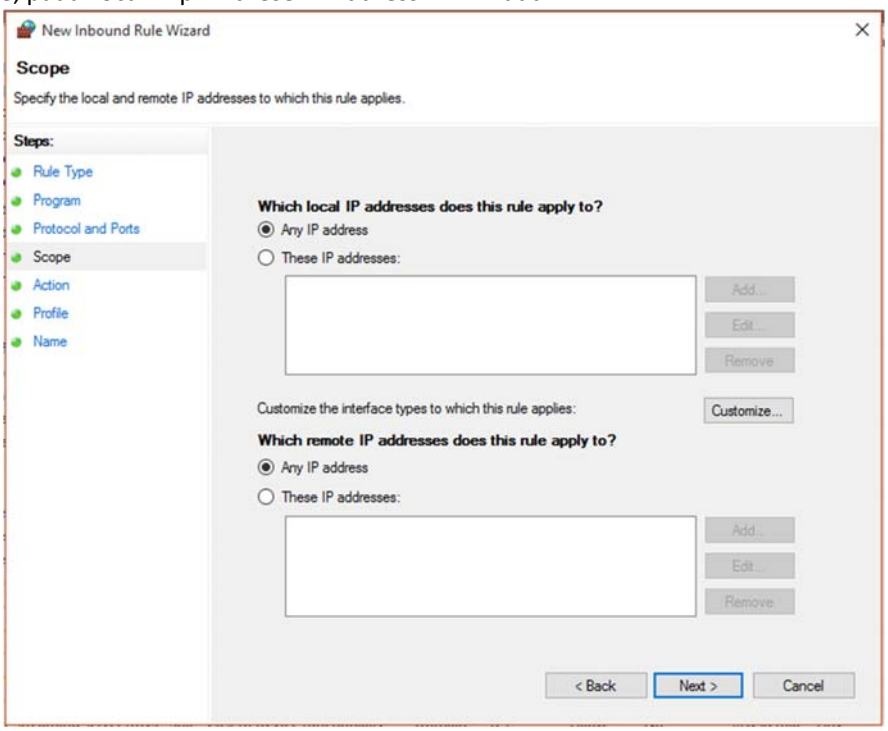
Gambar 7. 3 Proses inbound rule firewall 3

5. Protocol and Ports, klik next



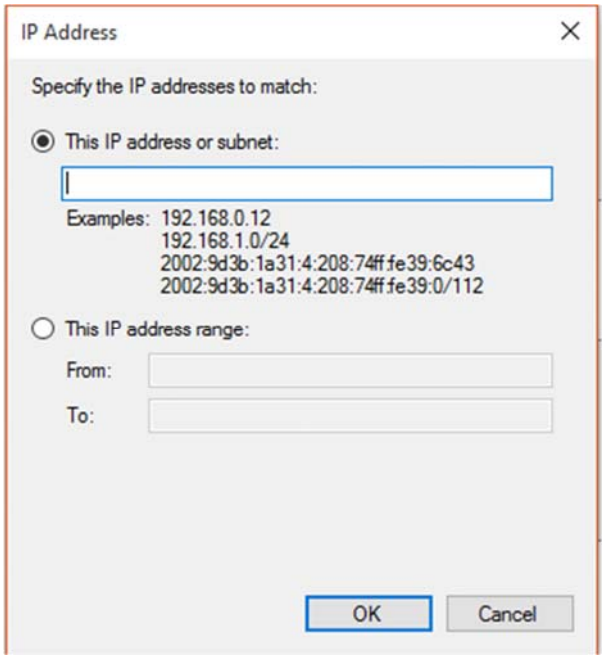
Gambar 7. 4 Proses Inbound rule firewall 4

6. UI Scope, pada Local IP pilih these IP Address → klik add



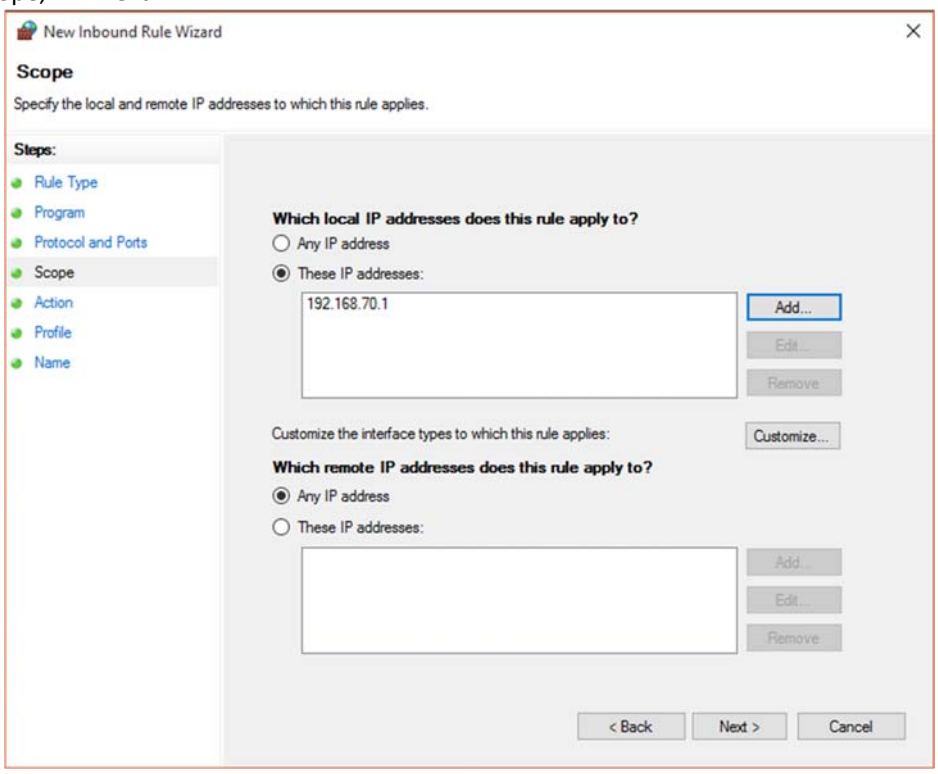
Gambar 7. 5 Proses Inbound Rule Firewall 5

7. Masukkan IP Address → klik OK



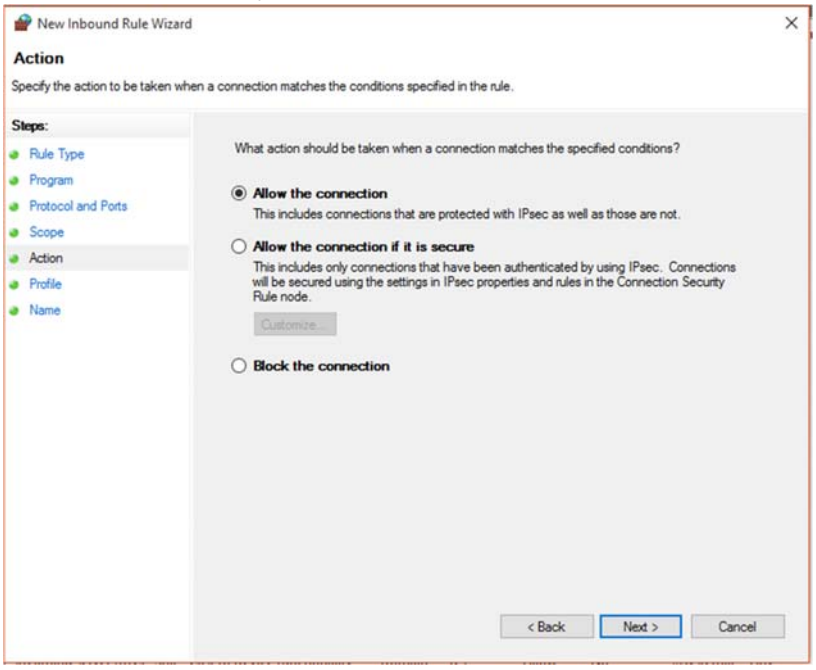
Gambar 7. 6 Proses inbound rule firewall 6

8. UI Scope, klik Next



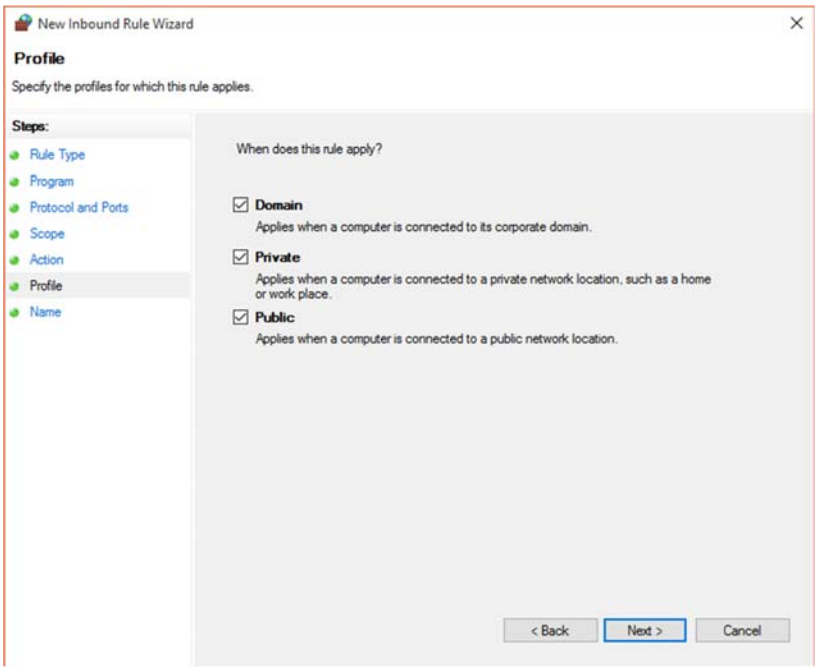
Gambar 7. 7 Proses inbound rule firewall 7

9. Pada user Interface Action, ada 3 pilihan,



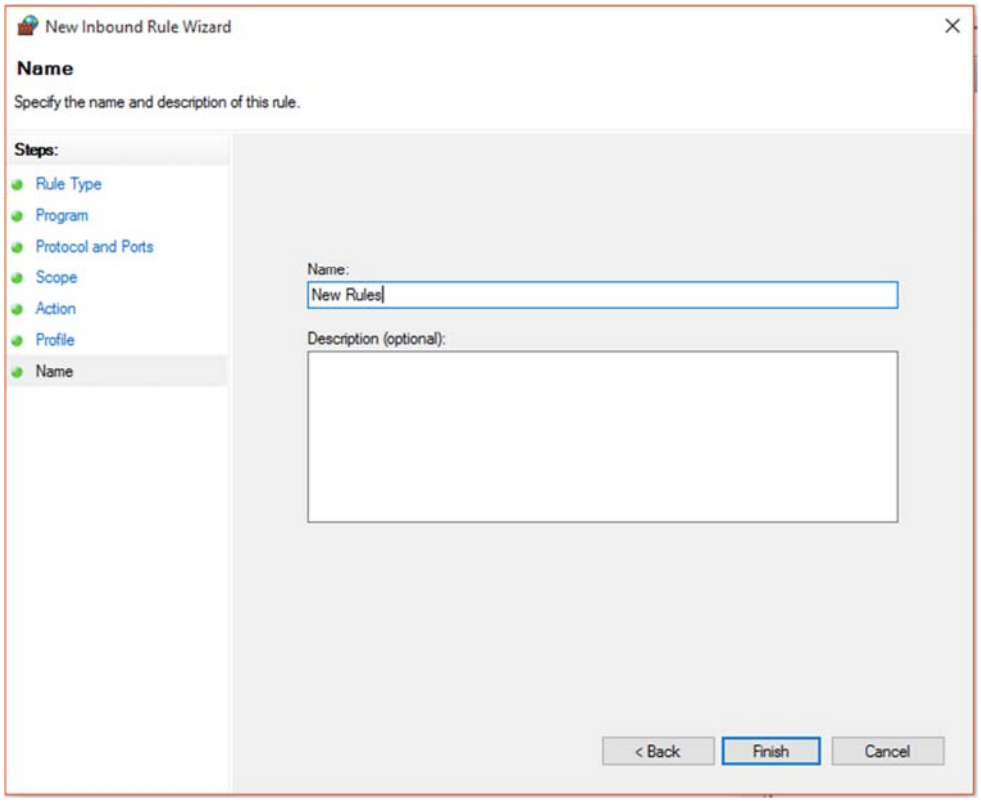
Gambar 7. 8 Proses inbound rule firewall 8

10. Pada user interface Profile, ada 3 checkbox berisikan Domain, Private dan Public,



Gambar 7. 9 Proses inbound rule firewall 9

11. Masukkan nama rules dan deskripsi rules, bila sudah diisikan maka klik finish.



Gambar 7. 10 Proses inbound rule firewall 10

7.7. POST TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-04	Block Facebook, Instagram screenshot hasilnya	100

7.8. HASIL CAPAIAN PRAKTIKUM

Diisi oleh asisten setelah semua assessment dinilai.

No	Bentuk Assessment	CPL	CPMK	Bobot	Skor (0-100)	Nilai Akhir (Bobot x Skor)
1.	Pre-Test	CPL-03	CPMK-01	20%	1oo	20
2.	Praktik	CPL-03	CPMK-01	30%	100	30
3.	Post-Test	CPL-03	CPMK-01	50%	100	50
					Total Nilai	100

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

Nama : **NIM :**	**Asisten:** **Paraf Asisten:**	**Tanggal:** **Nilai:**

PRAKTIKUM 8: WIRELESS NETWORK SECURITY

Pertemuan ke : 8

Total Alokasi Waktu : 90 menit
- Materi : 15 menit
- Pre-Test : 15 menit
- Praktikum : 45 menit
- Post-Test : 15 menit

Total Bobot Penilaian : 100%
- Pre-Test : 20 %
- Praktik : 30 %
- Post-Test : 50 %

Pemenuhan CPL dan CPMK:

CPL-07	Mampu memilih, membuat dan menerapakan teknik, sumber daya, penggunaan perangkat teknik modern dan implementasi teknologi informasi untuk memecahkan masalah.
CPMK-04	Memahami pentingnya keamanan sistem dan jaringan komputer (wireless Network security)

8.1. DESKRIPSI CAPAIAN PEMBELAJARAN

Setelah mengikuti praktikum ini mahasiswa diharapkan mampu:

1. Memahami dan mampu menerapkan konsep wireless network security, snapping paket data.

8.2. INDIKATOR KETERCAPAIAN PEMBELAJARAN

Indikator ketercapaian diukur dengan:

CPL-07	CPMK-04	Mahasiswa mampu memahami dan menerapkan wireless security, mobile device security dan wireless LAN security.

8.3. TEORI PENDUKUNG

Jaringan Tanpa Kabel (Wireless)

Sistem jaringan Wireless atau WIFI tidak memerlukan media jaringan berupa kabel jaringan, tetapi memerlukan ruangan atau space dimana jarak jangkauan jaringan ditentukan oleh kekuatan pancaran signal radio dari masing-masing device wireless yang digunakan. System Wireless mempunyai beberapa keuntungan antara lain pemakai tidak dibatasi oleh ruang gerak dan hanya dibatasi pada jarak jangkauan dari satu titik pemacar WIFI. Untuk jarak pada sistem WIFI mampu menjangkau area sekitar 100 feet atau 30M radius.

Selain itu dapat diperkuat dengan perangkat khusus seperti booster yang berfungsi sebagai relay yang mampu menjangkau ratusan bahkan beberapa kilometer ke satu arah (directional). Bahkan hardware terbaru, terdapat perangkat dimana satu perangkat Access Point dapat saling merelay

(disebut bridge) kembali ke beberapa bagian atau titik sehingga memperjauh jarak jangkauan dan dapat disebar dibeberapa titik dalam suatu ruangan untuk menyatukan sebuah network LAN.

Beberapa keuntungan yang dimiliki oleh Wireless LAN :

- Mobility
- Lebih cepat dalam instalasi
- Simple
- Installation flexibility
- Reduced cost of ownership

Keamanan Wireless :

- Hidden SSID
- Disable default authenticate
- Mac address list
- WEP
- Didepan server VPN
- Menggunakan hotspot

Security Profile z

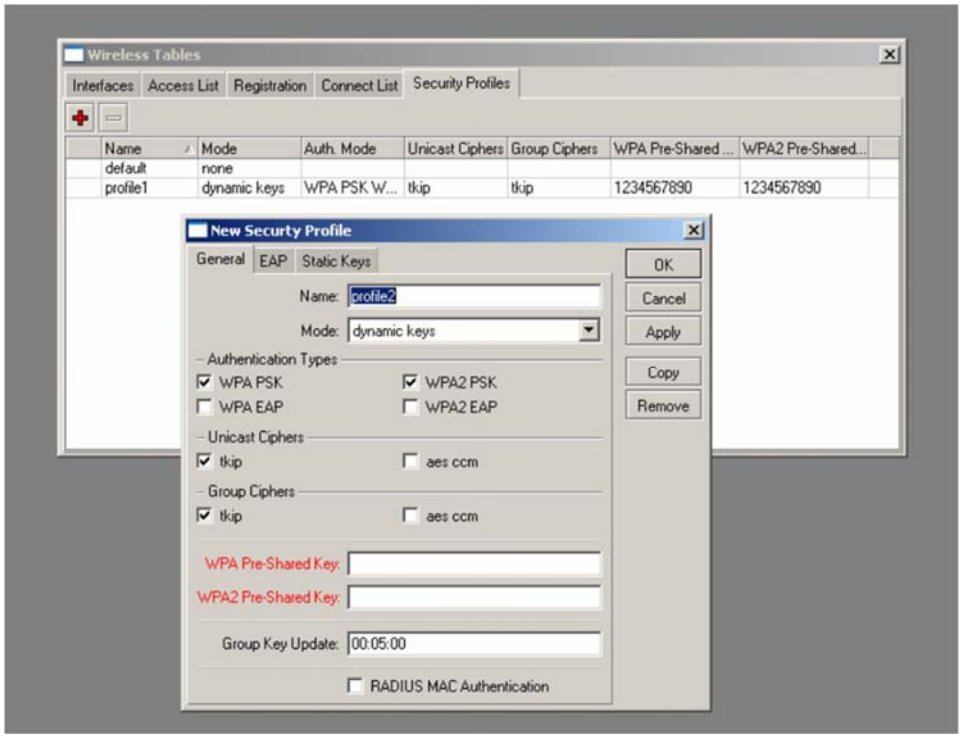
WEP = Wired Equivalent Privacy

- Enkripsi data hanya pada 802.11 menggunakan static key
- Sangat simple -40 bit = menggunakan enkripsi 40 bit (juga dikenal sebagai 64bit-WEP)
- 104 bit = menggunakan enkripsi 104bit (juga dikenal sebagai 128bit-WEP)
- Static key = text (dalam hexa key)

WPA = Wi-Fi Protection Access

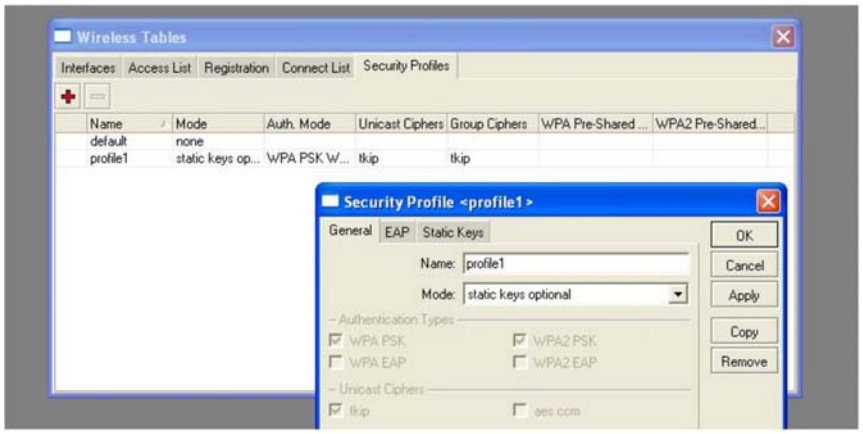
- Kombinasi dari 802.1x, EAP, MIC, TKIP dan AES

Security Profiles Dalam Winbox



Gambar 8. 1 Security Profiles Winbox

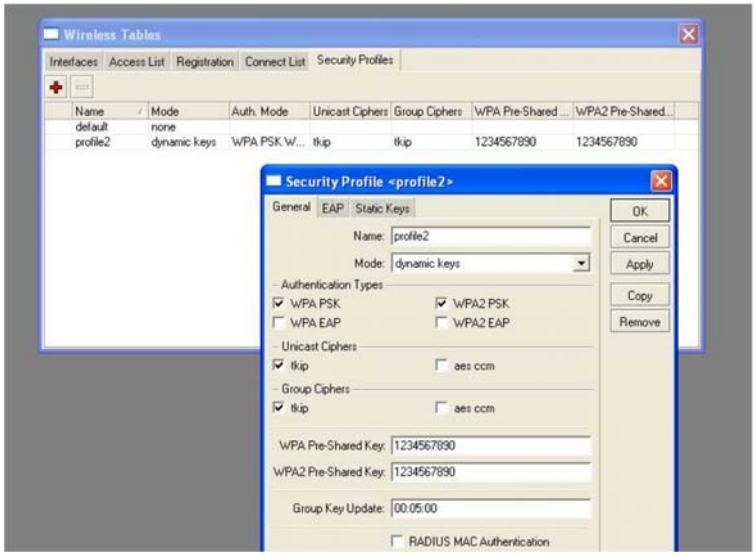
Aplikasi WEP Security



Gambar 8. 2 WEP Security 1

Gambar 8. 3 WEP Security 2

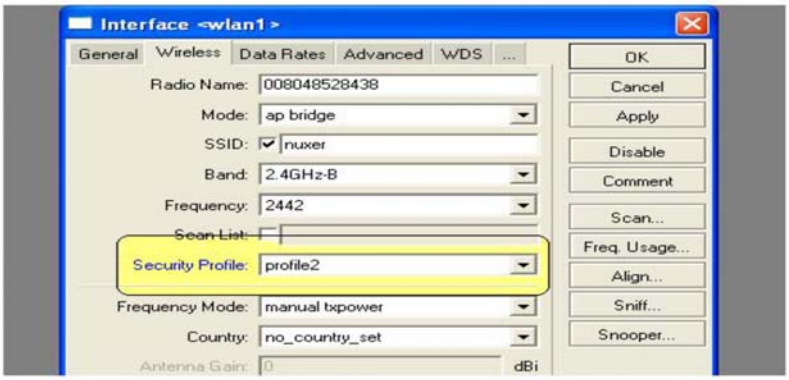
Aplikasi WPA Security



Gambar 8. 4 WPA Security 1

Note : pada kedua router (AP dan Station set WPA harus sama persis)

Penggunaan WPA Security



Gambar 8. 5 WAP Security 2

8.4. HARDWARE DAN SOFTWARE

Hardware dan software yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. Notepad

8.5. PRE-TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-04	Jelaskan menurut anda apa yang dimaksud dengan jaringan wireless!	30
2.	CPL-07	CPMK-04	Sebutkan dan jelaskan jenis jaringan wireless.	30
3.	CPL-07	CPMK-04	Sebutkan kelemahan dan keuntungan dari jaringan wireless	40

8.6. LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-07	CPMK-04	Selesaikan langkah praktikum 1 – 5	Hasil praktikum langkah 1 – 5	100

Langkah-Langkah Praktikum:

1. Nyalakan komputer.
2. Buka aplikasi winbox.
3. Pastikan winbox sudah terkoneksi dengan routernya.
4. Lakukan proses seperti pada gambar di atas.

5. Wi-Fi sudah siap digunakan.

8.7. POST TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-04	Jelaskan menurut anda apa yang akan terjadi jika di suatu wlan memiliki celah keamanan!	50
2.	CPL-07	CPMK-04	Ada berapa banyak client yang dapat terhubung kedalam sistem infrastruktur wlan	50

8.8. HASIL CAPAIAN PRAKTIKUM

Diisi oleh asisten setelah semua assessment dinilai.

No	Bentuk Assessment	CPL	CPMK	Bobot	Skor (0-100)	Nilai Akhir (Bobot x Skor)
1.	Pre-Test	CPL-03	CPMK-01	20%	100	20
2.	Praktik	CPL-03	CPMK-01	30%	100	30
3.	Post-Test	CPL-03	CPMK-01	50%	100	50
					Total Nilai	100

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

Nama : **NIM :**	**Asisten:** **Paraf Asisten:**	**Tanggal:** **Nilai:**