PP/018/VII/R2

LABORATORIUM
S1 INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS AHMAD DAHLAN

PETUNJUK PRAKTIKUM

EDISI KURIKULUM OBE

KEAMANAN INFORMASI

Penyusun:
Nuril Anwar, S.T., M.Kom.
Dr. Imam Riadi, M.Kom.

2022

HAK CIPTA

PETUNJUK PRAKTIKUM KEAMANAN INFORMASI

Diterbitkan oleh:
Program Studi S1 Informatika
Fakultas Teknologi Industri
Universitas Ahmad Dahlan
Jalan Ring Road Selatan, Tamanan, Banguntapan, Bantul Yogyakarta 55166

Penulis	: Nuril Anwar, S.T., M.Kom. Dr. Imam Riadi, M.Kom.
Editor	: Laboratorium S1 Informatika, Universitas Ahmad Dahlan
Desain sampul	: Laboratorium S1 Informatika, Universitas Ahmad Dahlan
Tata letak	: Laboratorium S1 Informatika, Universitas Ahmad Dahlan
Ukuran/Halaman	: 21 x 29,7 cm / 97 halaman

Didistribusikan oleh:

Laboratorium S1 Informatika
Universitas Ahmad Dahlan
Jalan Ring Road Selatan, Tamanan, Banguntapan, Bantul Yogyakarta 55166
Indonesia

KATA PENGANTAR

Puji syukur ke hadirat Tuhan Yang Maha Esa, yang telah memberikan rahmat-Nya sehingga Modul Praktikum Keamanan Informasi untuk mahasiswa/i S1 Informatika Fakultas Teknologi Industri Universitas Ahmad Dahlan ini dapat diselesaikan dengan sebaik-baiknya.

Modul praktikum ini dibuat sebagai pedoman dalam melakukan kegiatan praktikum Keamanan Informasi yang merupakan kegiatan penunjang mata kuliah Keamanan Informasi pada Program Studi S1 Informatika Universitas Ahmad Dahlan. Modul praktikum ini diharapkan dapat membantu mahasiswa/i dalam mempersiapkan dan melaksanakan praktikum dengan lebih baik, terarah, dan terencana. Pada setiap topik telah ditetapkan tujuan pelaksanaan praktikum dan semua kegiatan yang harus dilakukan oleh mahasiswa/i serta teori singkat untuk memperdalam pemahaman mahasiswa/i mengenai materi yang dibahas.

Penyusun menyakini bahwa dalam pembuatan Modul Praktikum Keamanan Informasi ini masih jauh dari sempurna. Oleh karena itu penyusun mengharapkan kritik dan saran yang membangun guna penyempurnaan modul praktikum ini dimasa yang akan datang.

Akhir kata, penyusun mengucapkan banyak terima kasih kepada semua pihak yang telah membantu baik secara langsung maupun tidak langsung.

Yogyakarta, 28 Oktober 2022

Penyusun

DAFTAR PENYUSUN

Nuril Anwar, S.T., M.Kom.

NIDN : 0509048901
NIY : 60160980
Jabatan : Asisten Ahli
S1 : S1 Informatika UAD – Indonesia
S2 : S1 Informatika UII – Indonesia
Bidang Minat : Computer Network & Security, Digital Forensics.
Email : nuril.anwar@tif.uad.ac.id

Dr. Imam Riadi, M.Kom.

NIDN : 0510088001
NIY : 60020397
Jabatan : Lektor Kepala
S1 : Universitas Negeri Yogyakarta
S2 : Universitas Gadjah Mada
S3 : Universitas Gadjah Mada
Bidang Minat : Computer Network & Security, Digital Forensics.
Email : imam.riadi@is.uad.ac.id

HALAMAN REVISI

Yang bertanda tangan di bawah ini:

Nama : Nuril Anwar. S.T., M.Kom

NIK/NIY : 60160980

Jabatan : Dosen Pengampu Mata Kuliah Keamanan Informasi

Dengan ini menyatakan pelaksanaan Revisi Petunjuk Praktikum Keamanan Informasi untuk Program Studi S1 Informatika telah dilaksanakan dengan penjelasan sebagai berikut:

No	Keterangan Revisi	Tanggal Revisi	Nomor Modul
1.	Versi Beta	28 Oktober 2022	PP/018/VII/R1

Yogyakarta, 28 Oktober 2022

Penyusun

Nuril Anwar, S.T., M.Kom
NIY. 60160980

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini:

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

NIK/NIY : 60150773

Jabatan : Kepala Laboratorium Praktikum S1 Informatika

Menerangkan dengan sesungguhnya bahwa Petunjuk Praktikum ini telah direview dan akan digunakan untuk pelaksanaan praktikum di Semester Genap Tahun Akademik 2022/2023 di Laboratorium Praktikum S1 Informatika, Program Studi S1 Informatika, Fakultas Teknologi Industri, Universitas Ahmad Dahlan.

Yogyakarta, 28 Oktober 2022

Mengetahui, Ketua Kelompok Keilmuan Rekayasa Perangkat Lunak dan Data (RELATA)	Kepala Laboratorium Praktikum S1 Informatika
Guntur Maulana Zamroni, B.Sc., M.Kom	**Lisna Zahrotun, S.T., M.Cs.**
NIY. 60181172	NIY. 60150773

VISI DAN MISI PRODI S1 INFORMATIKA

VISI

Menjadi Program Studi S1 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 S1 INFORMATIKA

DOSEN/KOORDINATOR PRAKTIKUM

1. Dosen harus hadir saat praktikum minimal 15 menit di awal kegiatan praktikum 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:
   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. 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 S1 Informatika.

Yogyakarta, 28 Oktober 2022

Kepala Laboratorium
Praktikum S1 Informatika

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

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

SKENARIO PRAKTIKUM SECARA DARING

Nama Mata Praktikum : Keamanan Informasi
Jumlah Pertemuan : 10 praktikum

Tabel 1 TABEL SKENARIO PRAKTIKUM DARING

Pert. ke	Judul Materi	Waktu *	Skenario **
1	Secure VPN Configuration and Management	1 pekan	WAG, Google Classroom
2	Network Security Threats and Vulnerabilities	1 pekan	WAG, Google Classroom
3	Hacking Wireless Networks	1 pekan	WAG, Google Classroom
4	Host Security	1 pekan	WAG, Google Classroom
5	Bug Bounty	1 pekan	WAG, Google Classroom
6	Data Backup and Recovery	1 pekan	WAG, Google Classroom
7	Hacking Webservers	1 pekan	WAG, Google Classroom
8	Hacking Web Applications	1 pekan	WAG, Google Classroom
9	System Hacking	1 pekan	WAG, Google Classroom
10	Footprinting and Reconnaissance	1 pekan	WAG, Google Classroom

Ketarangan :
* Waktu (Lama praktikum sampai pengumpulan postest)
** Skenario Praktikum dari pemberian pretest, postest dan pengumpulannya serta mencantumkan metode yang digunakan misal video, WhatsApp Group, Google Meet atau lainnya

PRAKTIKUM 1: SECURE VPN CONFIGURATION AND MANAGEMENT

Pertemuan ke : 1

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

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

Pemenuhan CPL dan CPMK

CPL-06	Memahami tanggung jawab profesional dan menerapkan pengetahuan serta berkomunikasi efektif dalam melakukan penilaian berdasar informasi dan praktek computing dengan berpedoman pada prinsip-prinsip legal dan etika
CPMK-03	Mahasiswa mampu melakukan penetration tester dan memberikan rekomendasi resiko terhadap sistem keamanan informasi

1.1. DESKRIPSI CAPAIAN PEMBELAJARAN

Setelah mengikuti praktikum ini mahasiswa diharapkan: (sesuai dengan RPS)
1. Mampu mengkonfigurasikan VPN dikomputer masing-masing
2. Mampu menganalisis sebelum dan sesudah menggunakan aplikasi VPN

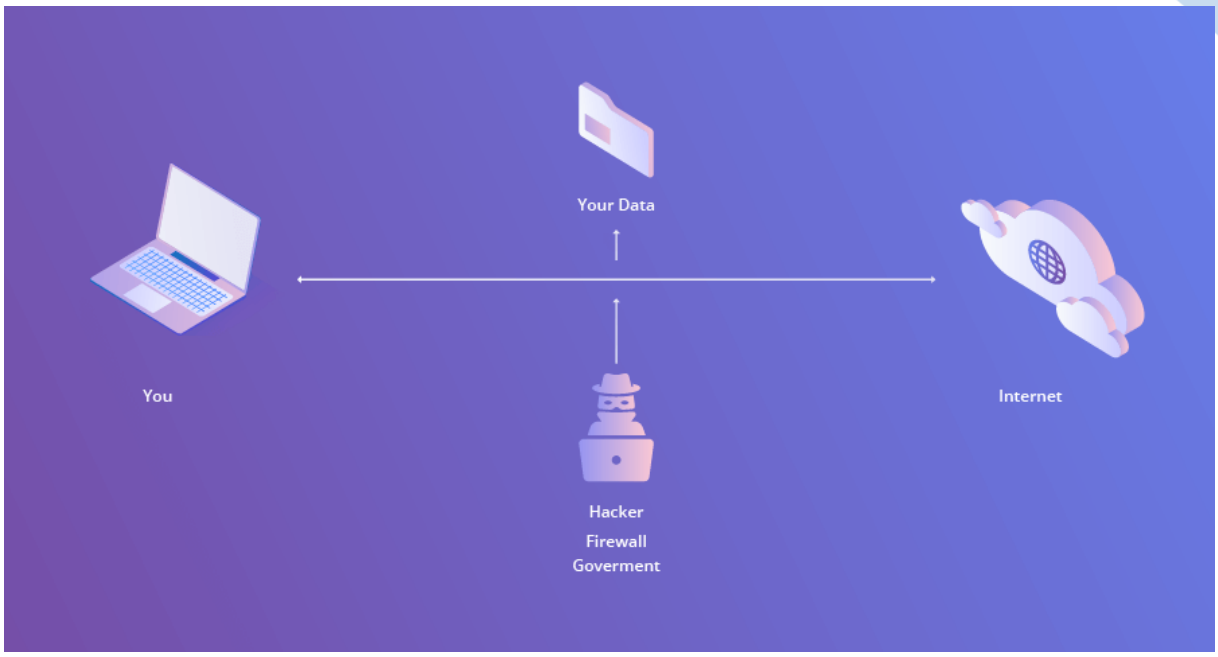
1.2. INDIKATOR KETERCAPAIAN PEMBELAJARAN

CPL-06	CPMK-03	Mahasiswa memahami tahapan konfigurasi VPN

1.3. TEORI PENDUKUNG

VPN (Virtual Private Network) adalah layanan koneksi yang memberikan akses ke website secara aman (secure) dan pribadi (private) dengan mengubah jalur koneksi melalui server dan menyembunyikan pertukaran data yang terjadi. Sederhananya, VPN mengkoneksikan smartphone, tablet, PC ke komputer yang lain (biasa disebut dengan VPN Server) di suatu tempat yang terhubung dengan internet, dan mengizinkan untuk menjelajah internet menggunakan jaringan internet komputer. Jadi jika komputer (server) di negara yang berbeda, itu akan menjadi negara yang digunakan ketika internet mencoba mengenai pengguna melalui koneksi tersebut dan pengguna dapat mengakses sesuatu yang tidak bisa diakses dari negara penggunanya.

Cara kerja VPN adalah melakukan enkripsi pertukaran data bahkan sebelum koneksi publik di tempat kopi atau warung internet membacanya. Ketika terhubung dengan internet menggunakan koneksi VPN itu seperti mengakses internet menggunakan lorong khusus, tidak menggunakan jaringan utama. Server VPN bertugas untuk meneruskan koneksi ke situs yang ingin diakses. Jadi koneksi yang dilakukan akan dikenali sebagai koneksi dari jaringan server VPN bukan jaringan yang digunakan pada saat itu. Jadi ketika menggunakan jaringan tanpa VPN maka koneksi yang dilakukan secara langsung (direct) tanpa enkripsi. Sedangkan jika menggunakan VPN, maka koneksi yang dilakukan terenkripsi dan dilewatkan terlebih dahulu melalui VPN server. Berikut ini ilustrasi koneksi melalui jaringan tanpa VPN dan menggunakan VPN.



Gambar 1.1 Ilustrasi VPN

Koneksi ini memang sudah menjadi standar yang digunakan ketika menggunakan internet. Tidak ada enkripsi dan semua data yang yang terlibat dalam proses pertukaran data antara pengguna dan aplikasi yang di internet dapat saja dilihat oleh banyak orang. Tidak masalah jika data yang diproses hanyalah data mengenai pencarian di Google, hiburan atau semacamnya. Ini akan menjadi masalah jika data yang diproses adalah perbankan online, email bisnis, atau apa pun yang sedikit lebih sensitif. Tentu saja ini akan menjadi cerita yang berbeda. Untuk melakukan serangan online, biasanya pada hacker menggunakan S1 serangan Man in The Middle (MITM). Ketika menggunakan VPN (biasanya menggunakan aplikasi), data dienkripsi oleh aplikasi dan baru dikirimkan melalui ISP kemudian ke server VPN. Server VPN menjadi perangkat ketiga untuk menghubungkan pengguna dengan situs atau layanan online. Ini akan dapat memecahkan masalah privasi dan keamanan data saat melakukan pertukaran data.

Ada beberapa manfaat yang bisa didapatkan saat menggunakan VPN, antara lain seperti melakukan remote access. Remote access mengizinkan mengakses internet menggunakan jaringan kantor, dari mana saja selama terhubung ke internet. Jadi meskipun menggunakan jaringan luar, ketika menggunakan VPN maka jaringan bisa dikenali oleh internet menggunakan jaringan kantor. Selain itu, berikut ini adalah beberapa manfaat dari VPN:

1. ByPass

Pembatasan terhadap situs streaming atau video. Misalnya oleh pemerintah untuk mengakses situs yang dianggap membahayakan, dan lain sebagainya.

2. Pengamanan Data di Jaringan Publik

Manfaat VPN lainnya adalah melindungi pertukaran data yang dilakukan dari WiFi atau jaringan yang tidak dapat dipercaya. Ini akan membantu ketika menggunakan jaringan publik di kafe, bar, dan semacamnya.

3. Mengamankan Informasi Pribadi Secara Anonim

VPN menyembunyikan lokasi secara realtime ‘secara langsung’. Jadi, tidak sembarangan orang dapat mengetahui lokasi berada saat melakukan akses. Biasanya lokasi yang terdeteksi adalah lokasi server VPN berada.

4. Data Dienkripsi

Saat memproses pertukaran data antara dan web aplikasi online, data dienkripsi. Sehingga meskipun seseorang melihat apa yang komputer kirimkan, mereka hanya melihat informasi yang sudah terenkripsi, bukan data mentah saja.

5. Enkripsi Informasi Perangkat

Seseorang tidak bisa dengan mudah mengidentifikasi perangkat yang digunakan, atau apa yang dilakukan. VPN dapat membuat koneksi sangat aman, tetapi itu juga tergantung dengan protokol (jalan) yang digunakan untuk melakukan koneksi. Pengguna VPN saat ingin melakukan aktivitas-aktivitas berikut:

- Membantu mendapatkan koneksi yang lebih aman ketika menggunakan WiFi publik.
- Mengenkripsi aktivitas di situs web.
- Menyembunyikan aktivitas terhadap orang-orang yang ingin mencoba mengetahui secara diam-diam.
- Menyembunyikan lokasi, dan mengizinkan mengakses geo-blocked content 'konten-konten yang diblok berdasarkan wilayah geografis'.
- Memastikan lebih anonim di dalam situs web.

Pengguna bisa mendapatkan akses VPN secara gratis. Ada beberapa situs penyedia VPN Gratis yang bisa dicoba. Situs-situs penyedia VPN Gratis ini menyediakan layanan aplikasi VPN yang dapat digunakan di perangkat desktop. Sedangkan jika ingin menggunakan VPN pada perangkat mobile maupun desktop dapat mencoba aplikasi seperti Hotspot Shield atau Tunnel Bear & Hide.me VPN dapat membantu pengguna untuk mengamankan koneksi yang dilakukan, begitu pula dengan identitas dan data pribadi. Meskipun ada kekurangan, tetapi itu menjadi bagian yang tidak bisa dipisahkan di dalam sebuah aplikasi.

1.4. HARDWARE DAN SOFTWARE

Alat dan bahan yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. VPN.

1.5. PRE-TEST

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

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-06	CPMK-03	1. Jelaskan apa yang dimaksud dengan VPN? 2. Sebutkan dan jelaskan kelebihan menggunakan VPN! 3. Sebutkan contoh layanan VPN apa saja yang Free min 5	100

1.6. LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-06	CPMK-03	Materi dan praktikum: Pertemuan Pertama tentang Secure VPN Configuration and Management untuk link vpn : openvpn.net Ikuti Langkah yang ada di video: https://www.youtube.com/watch?v=ecCAq-GvJk4	Screen Shot Hasil praktikum	100

POSTEST

1. IP Awal

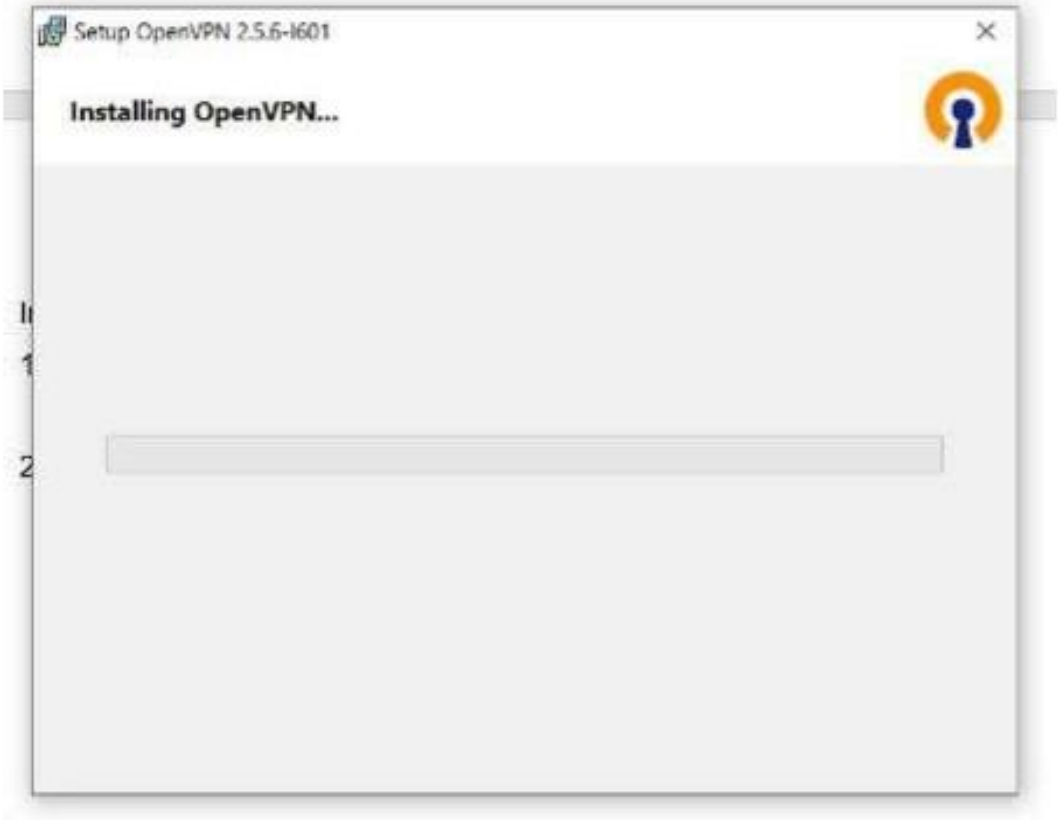
Gambar 1.2 Cek IP Asal

2. Akses url: https://www.halftheskymovement.org/

Gambar 1.3 Akses Alamat Terbatas

3. Install VPN

1) Install Aplikasi OpenVPN

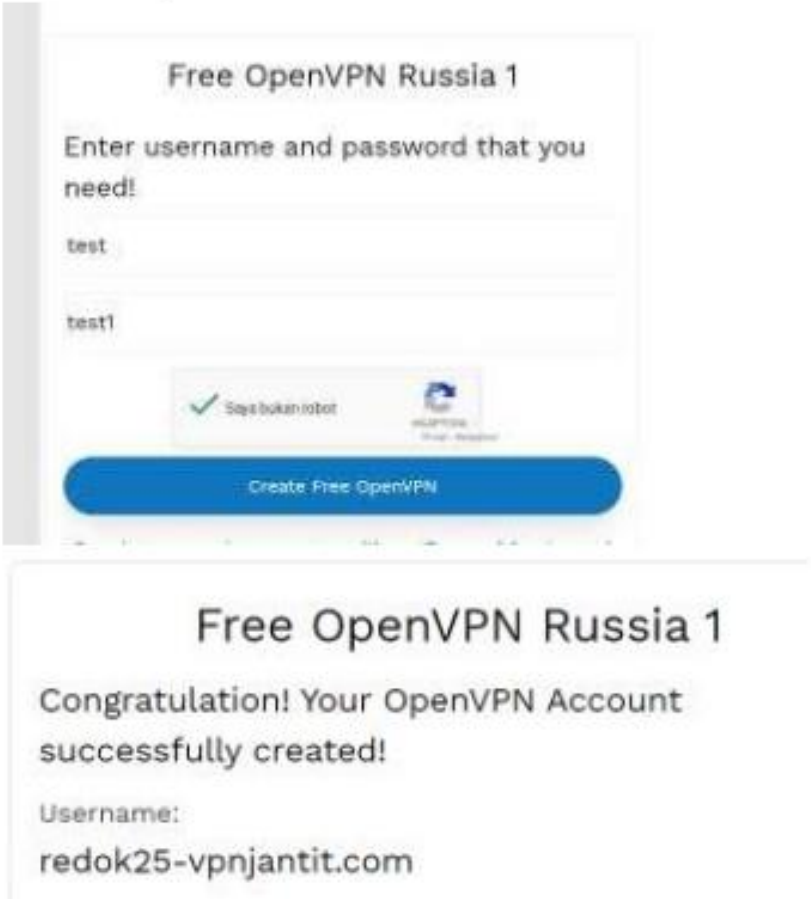


Gambar 1.4 Install Open VPN

2) Akses situs penyedia VPN gratis

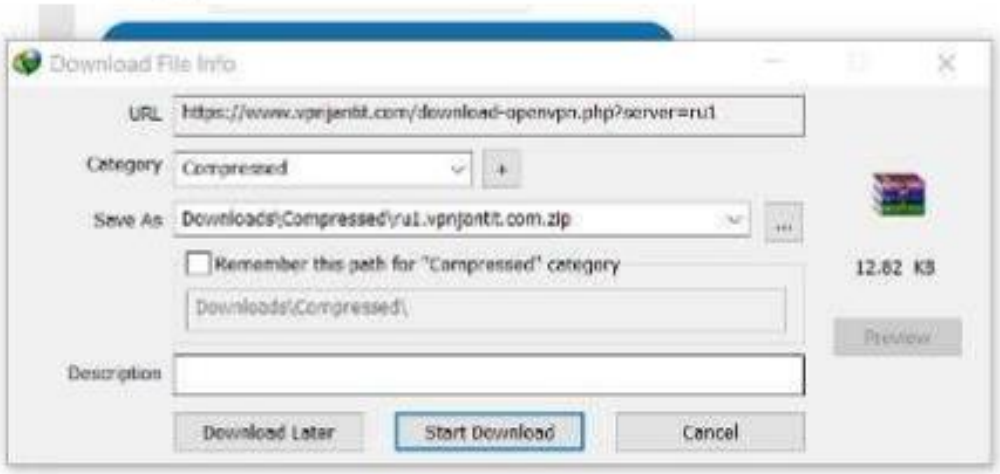
Gambar 1.5 Akses Penyedia VPN Free

3) Buat akun OpenVPN



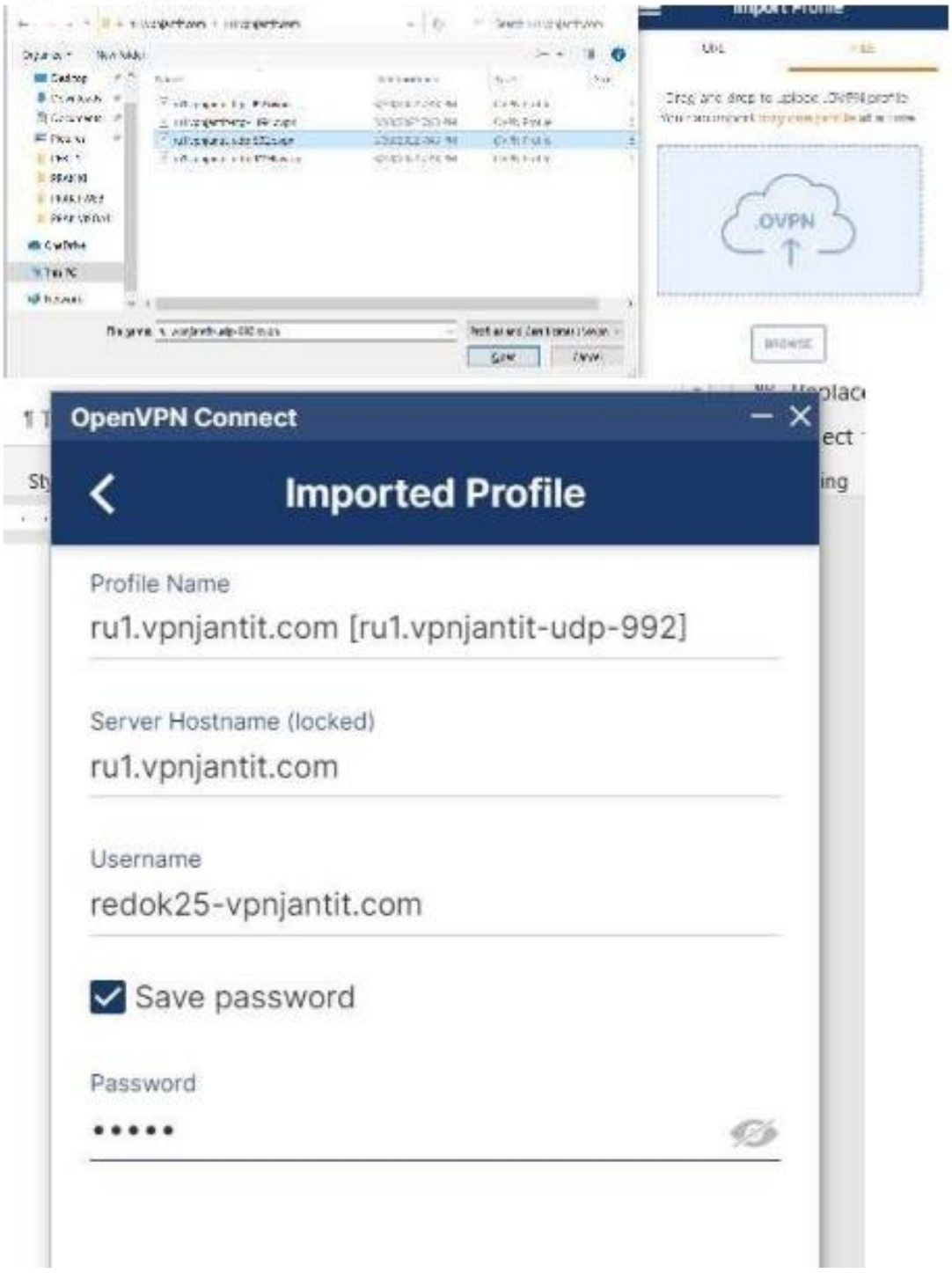
Gambar 1.6 Create Account Open VPN

4) Download config vpn



Gambar 1.7 Download & Configure Open VPN

5) Import config yang sudah didownload



Gambar 1.8 Import Config

6) VPN berhasil connect

Gambar 1.9 Open VPN Connected

4. Cek kembali IP setelah VPN terpasang

Gambar 1.10 Cek Open VPN IP New

5. Akses kembali url: https://www.halftheskymovement.org/

Gambar 1.11 Cek URL VPN IP Unblock

1.7. POST TEST

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-06	CPMK-03	1. Silahkan cek IP anda, lalu screenshoot IP awal anda. 2. Silahkan coba akses link https://www.halftheskymovement.org/ lalu screenshoot. 3. Buatlah laporan langkah praktikum sesuai dengan yang di youtube. Menyertakan ss IP awal dan nomor 2. 4. Setelah VPN berhasil teristal dan sudah on, silahkan cek lagi IP anda lalu akses https://www.halftheskymovement.org/ . 5. Jangan lupa untuk screenshoot tampilan akhir ketika berhasil akses https://www.halftheskymovement.org/.	100

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-06	CPMK-03	20%		
2.	Praktik	CPL-06	CPMK-03	30%		
3.	Post-Test	CPL-06	CPMK-03	50%		
					Total Nilai	

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

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

PRAKTIKUM 2: NETWORK SECURITY THREATS & VULNERABILITIES

Pertemuan ke : 2

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

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

Pemenuhan CPL dan CPMK

CPL-06	Memahami tanggung jawab profesional dan menerapkan pengetahuan serta berkomunikasi efektif dalam melakukan penilaian berdasar informasi dan praktek computing dengan berpedoman pada prinsip-prinsip legal dan etika
CPMK-03	Mahasiswa mampu melakukan penetration tester dan memberikan rekomendasi resiko terhadap sistem keamanan informasi

2.1. DESKRIPSI CAPAIAN PEMBELAJARAN

Setelah mengikuti praktikum ini mahasiswa diharapkan: (sesuai dengan RPS)
1. Mampu melakukan scaning network dengan tools nmap Linux
2. Mampu mengidentifikasi jenis-jenis tools Network Security Threats & Vulnerabilities

2.2. INDIKATOR KETERCAPAIAN PEMBELAJARAN

CPL-06	CPMK-03	Mahasiswa dalam menerapkan Proses scaning network & Analisisi Network Security Threats & Vulnerabilities

2.3. TEORI PENDUKUNG

Kemanan jaringan (network security) merupakan bagian dari sebuah sistem informasi, yang fungsinya sangat penting untuk menjaga validitas dan integritas data serta menjamin keterrsediaan layanan begi penggunanya. Oleh karena itu, sistem harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak berhak. Komputer yang terhubung ke jaringan mengalami ancaman keamanan yang lebih besar daripada host yang tidak terhubung kemana-mana. Dengan mengendalikan network security, resiko tersebut dapat dikurangi. Namun network security biasanya bertentangan dengan network acces. Pasalnya, bila network acces semakin mudah, network security makin rawan. Sebaliknya, bila network security makin baik, network acces semakin tidak nyaman. Suatu jaringan didesain sebagai komunikasi data highway dengan tujuan meningkatkan akses ke sistem komputer, sementara keamanan didesain untuk mengontrol akses. Penyediaan network security adalah sebagai aksi penyeimbang antara open acces dengan security.

Network security melibatkan otorisasi akses ke data di dalam jaringan, yang dikendalikan oleh administrator jaringan. Pengguna (users) memilih atau diberi ID dan password atau informasi otentikasi lain yang memungkinkan mereka untuk mengakses informasi dan program dalam wewenang mereka sendiri. Network security mencakup berbagai jaringan komputer, baik publik maupun pribadi, yang digunakan dalam pekerjaan sehari-hari; melakukan transaksi dan komunikasi di antara bisnis, instansi pemerintah dan individu. Dalam menjaga kemanan jaringan, diterapkan konsep atau hukum dasar yang biasa disebut dengan CIA, yaitu Confidentiality (kerahasiaan), Integrity (integritas), dan Availability (ketersediaan). Kerahasiaan berhubungan dengan hak akses untuk membaca data atau informasi dan suatu sistem computer. Dalam hal ini suatu sistem komputer dapat

dikatakan aman jika suatu data atau informasi hanya dapat dibaca oleh pihak yang telah diberi hak atau wewenang secara legal.

Integritas berhubungan dengan hak akses untuk mengubah data atau informasi dari suatu sistem computer. Dalam hal ini suatu sistem komputer dapat dikatakan aman jika suatu data atau informasi hanya dapat diubah oleh pihak yang telah diberi hak. Sedangkan, Ketersediaan berhubungan dengan ketersediaan data atau informasi pada saat yang dibutuhkan. Dalam hal ini suatu sistem komputer dapat dikatakan aman jika suatu data atau informasi yang terdapat pada sistem komputer dapat diakses dan dimanfaatkan oleh pihak yang berhak. Serangan terhadap suatu data dalam suatu jaringan dapat dikategorikan menjadi dua, yaitu serangan pasif dan serangan aktif. Serangan Pasif merupakan serangan pada sistem autentikasi yang tidak menyisipkan data pada aliran data, tetapi hanya mengamati atau memonitor pengiriman informasi ke tujuan. Serangan pasif ini sulit dideteksi karena penyerang tidak melakukan perubahan data. Karenanya, untuk mengatasi serangan pasif ini lebih ditekankan pada pencegahan daripada pendeteksiannya. Sedangkan serangan Aktif mencoba memodifikasi data, mencoba mendapatkan autentikasi, atau mendapatkan autentikasi dengan mengirimkan paket-paket data yang salah ke dalam data stream atau dengan memodifikassi paket-paket yang melewati data stream. Kebalikan dari serangan pasif, serangan aktif sulit untuk dicegah karena untuk melakukannya dibutuhkan perlindungan fisik untuk semua fasilitass komunikassi dan jalur-jalurnya setiap saat. Yang dapat dilakukan adalah mendeteksi dan memulihkan keadaan yang disebabkan oleh serangan ini. Adapun bentuk-bentuk ancamannya, seperti: menyerang database password atau menyerang login prompt yang sedang aktif, serangan yang membuat jaringan tidak bisa diakses (Deniel of Services), Spoofing attack, serangan keamanan jaringan Man-in-the-middle (serangan pembajakan), Spamming, Sniffer (atau dikenal sebagai snooping attack), dan Crackers. Sementara itu, tipe dari perangkat network security ini dapat dibagi menjadi empat. Pertama, Active Devices. Beberapa contoh dari tipe network security ini meliputi Firewalls, perangkat scanning antivirus, dan perangkat content filtering yang memblokir trafik yang berlebihan. Kedua, Passive Devices. Perangkat ini mengidentifikasi dan melaporkan trafik yang tidak diinginkan, seperti intrusion detection appliances. Ketiga, Preventative Devices. Perangkat ini memindai jaringan dan mengidentifikasi masalah keamanan yang potensial. Contohnya, penetration testing devices dan vulnerability assesment appliances. Keemat, Unified Threat Management (UTM). Perangkat ini berfungsi sebagai perangkat keamanan all-in-one. Contohnya termasuk Firewall, content filtering, web caching, dan lain-lain.

Securing your network Melindungi jaringan komputer memerlukan implementasi dan pemeliharaan berbagai langkah keamanan. Peretas (hacker) pun bukanlah satu-satunya ancaman terhadap sistem jaringan, perangkat, dan data. Prosedur yang buruk, ketidaktahuan tentang kebijakan, kurangnya kesadaran keamanan, dan akses fisik yang tidak sesuai ke sistem dapat meningkatkan risiko terhadap data, personel, dan perangkat. Network security adalah salah satu aspek yang paling penting untuk dipertimbangkan ketika bekerja melalui internet, LAN atau metode lain. Tidak peduli seberapa kecil atau besar bisnis pengguna. Meskipun tidak ada jaringan yang kebal terhadap serangan, sistem keamanan yang stabil dan efisien sangat penting untuk melindungi data klien. Sistem keamanan jaringan yang baik mampu membantu bisnis tertentu dalam mengurangi risiko terhadap pencurian data dan sabotage. Dengan terhubung ke internet berarti akan menerima banyak trafik. Trafik yang besar dapat menyebabkan masalah stabilitas dan dapat menyebabkan kerentanan dalam sistem. Maka dengan peran penting dari network security ini dapat memantau hal tersebut dengan baik dari transaksi yang mencurigakan di dalam sistem.

Vulnerability Assessments dan Penetration Tests Bagi perusahaan yang menggunakan komputer sebagai alat penunjang bisnisnya maka wajib menyewa konsultan keamanan komputer atau ethical hacker untuk melakukan Vulnerability Assessments dan Penetration Tests.

Vulnerability assessment adalah proses mendefinisikan,mengidentifikasi,mengelompokan dan memprioritaskan kelemahan dalam sistem komputer,aplikasi dan infrastruktur jaringan sebagai dasar suatu organisasi untuk melakukan tindakan pencegan atas resiko yang bisa ditimbulkan oleh kelemahan sistem dimasa mendatang. Biasanya yang melakukan semua ini adalah ethical hacker yang telah disewa dan diberi izin secara resmi untuk melakukan penetration testing terhadap lingkungan IT perusahaan guna menguji ketahanan dan menemukan vulnerability. Untuk membantu proses

pentesting seorang ethical hacker biasanya menggunakan tool hacking yang sudah terkenal di internet seperti Metasploit, nmap, wireshark, aircrack-ng, netcat, BeEF dll.

Semua system mempunyai vulnerability Setiap jam setiap hari sistem komputer terus berkembang, penyempurnaan demi penyempurnaan terus dilakukan untuk membangun sistem yang aman. Ketika sebuah sistem ketinggalan versi (tidak pernah diupdate) maka sistem tersebut memiliki kerentanan untuk di exploitasi. Alasan utama sebuah sistem mempunyai versi baru adalah karena sistem yang lama telah ditemukan kelemahan/bug/vulnerability dan disempurnakan pada versi yang paling baru. Jadi semua sistem mempunyai vulnerability hanya tinggal menunggu waktu sampai seseorang menemukan nya. Vulnerability dan exploit yang beredar di internet biasanya untuk aplikasi versi lama,tentu vendor sudah membuat perbaikan di versi baru untuk menambal vulnerability yang sudah terpajang di internet. jadi melalkukan update adalah solusi untuk menghindari exploit.

2.4. HARDWARE DAN SOFTWARE

Alat dan bahan yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. Kali Linux
3. Nmap

2.5. PRE-TEST

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

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-06	CPMK-03	1. Jelaskan fungsi tools Nmap dan Nessus 2. Jelaskan pengertian tentang keamanan data dan informasi! 3. Jelaskan kegunaan metasploit!	100

2.6. LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-06	CPMK-03	Selesaikan langkah praktikum berikut dengan masing-masing tools nmap pada computer anda	Screen Shot Hasil praktikum	100

POSTEST

A. Implementasikanlah salah satu dari video materi yang ada

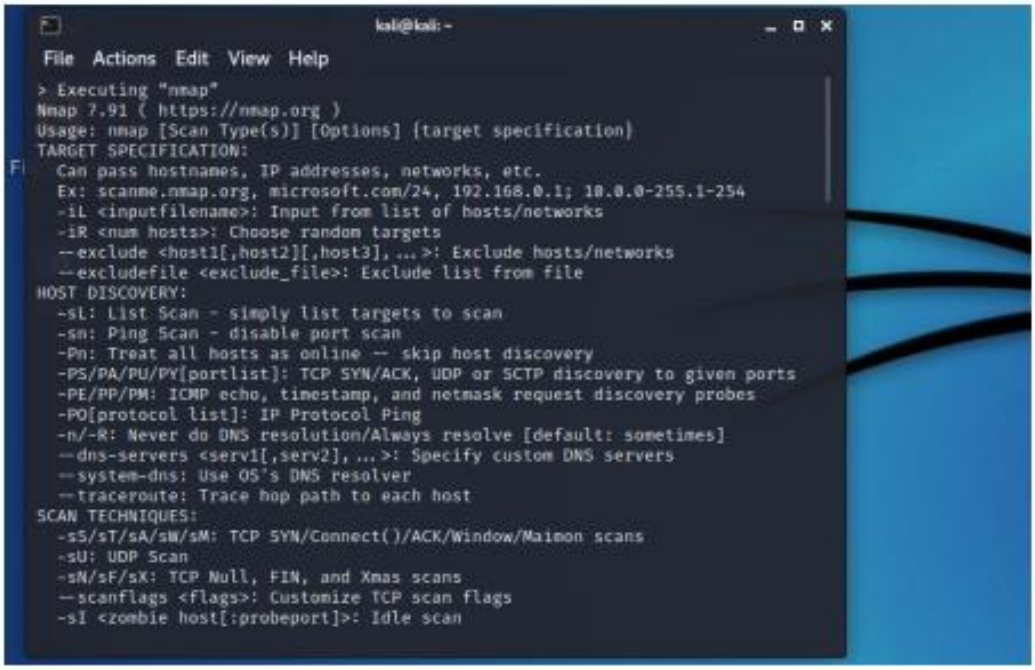
Video yang akan diimplementasikan adalah berikut:

https://www.youtube.com/watch?v=5MTZdN9TEO4

- Buka Linux

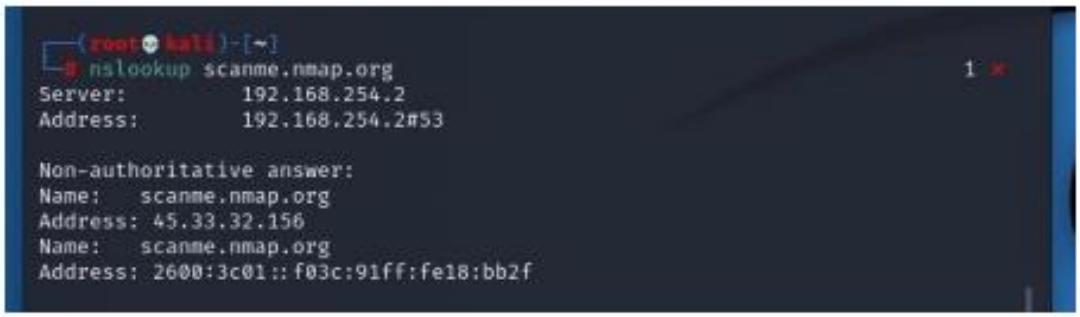
Gambar 2.1 Tampilan Awal Linux Kali

- Buka Nmap



Gambar 2.2 Tampilan Awal Nmap

- Jalankan command nslookup scanme.nmap.org, untuk mendapatkan IP addres dari situ tersebut

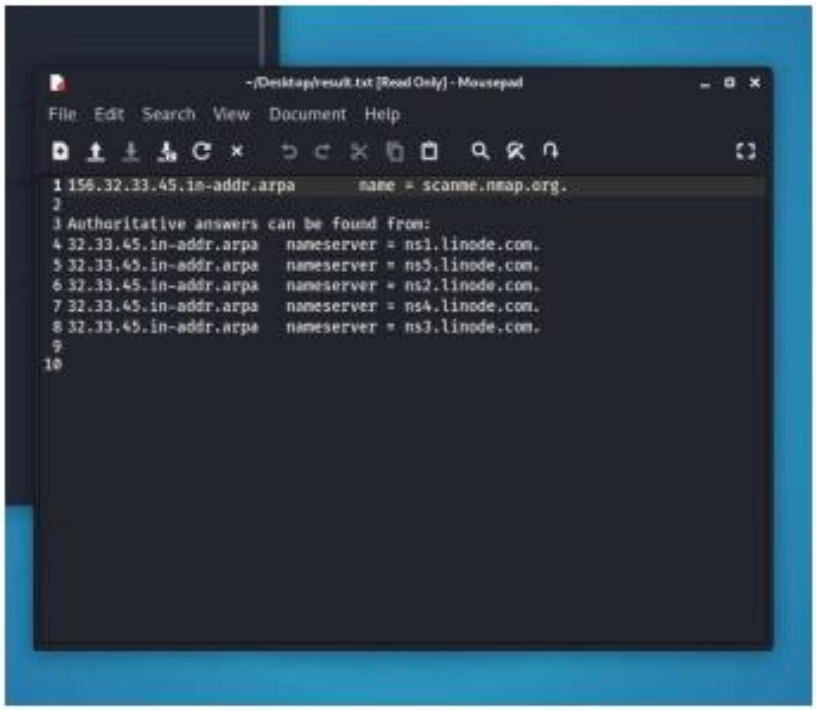


- Jalankan command nslookup kembali dengan beberapa command tambahan

- Command di atas akan menghasilkan sebuah file txt.

Gambar 2.3 Nslookup Scanme

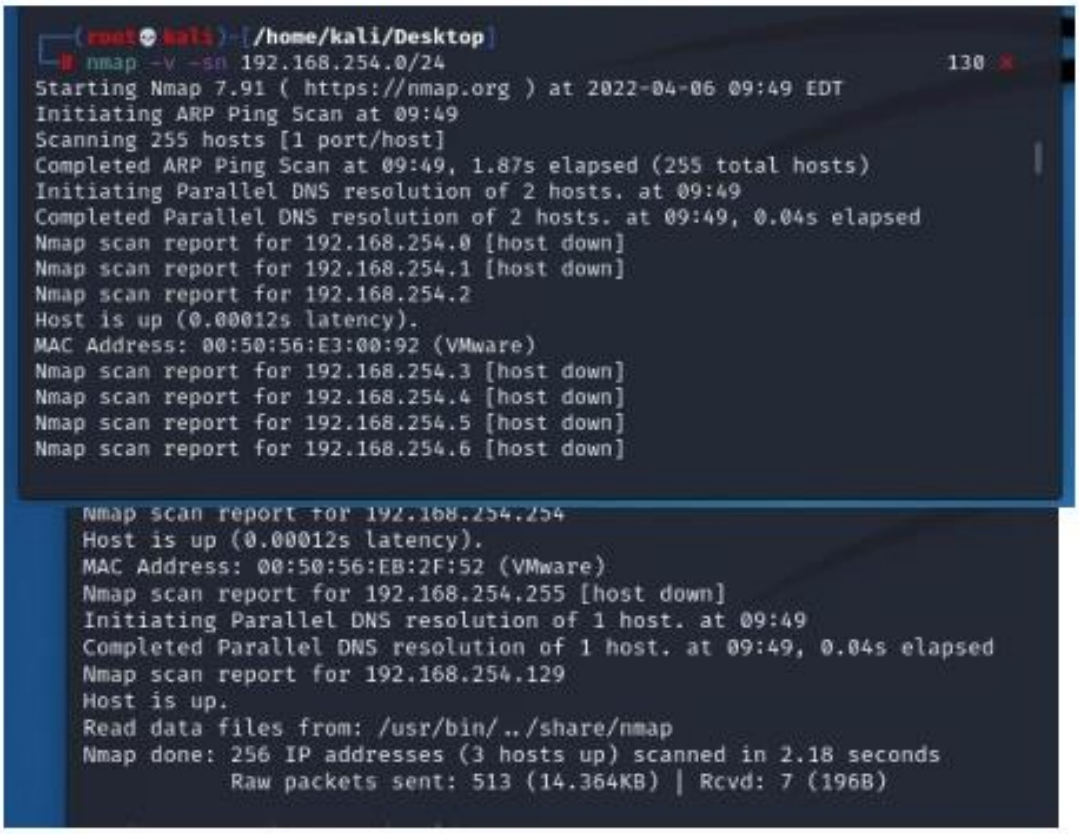
- Dan ini isi dari file tersebut



Gambar 2.4 Tahapan Scanning Network Nmap

B. Lalu silahkan scan minimal 1 IP atau web.

- Scanning dengan NMAP terhadap IP 192.168.254.0/24



Gambar 2.5 Proses Scanning IP Network

2.7. POST-TEST

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

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-06	CPMK-03	Implementasikanlah salah satu dari video materi yang ada, bila menggunakan windows nilai maksimal 85, bila menggunakan kali linux nilai maksimal 100. Lalu silahkan scan minimal 1 IP atau web.	100

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-06	CPMK-03	20%		
2.	Praktik	CPL-06	CPMK-03	30%		
3.	Post-Test	CPL-06	CPMK-03	50%		
					Total Nilai	

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

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

PRAKTIKUM 3: HACKING WIRELESS NETWORKS

Pertemuan ke : 3

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

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

Pemenuhan CPL dan CPMK

CPL-06	Memahami tanggung jawab profesional dan menerapkan pengetahuan serta berkomunikasi efektif dalam melakukan penilaian berdasar informasi dan praktek computing dengan berpedoman pada prinsip-prinsip legal dan etika
CPMK-03	Mahasiswa mampu melakukan penetration tester dan memberikan rekomendasi resiko terhadap sistem keamanan informasi

3.1. DESKRIPSI CAPAIAN PEMBELAJARAN

Setelah mengikuti praktikum ini mahasiswa diharapkan: (sesuai dengan RPS)
1. Mampu melakukan melakukan pencarian atau filtering pada aplikasi Wireshark
2. Mampu mengidentifikasi jenis-jenis transaksi network

3.2. INDIKATOR KETERCAPAIAN PEMBELAJARAN

CPL-06	CPMK-03	Kemampuan mahasiswa dalam menerapkan pencarian atau filtering pada aplikasi Wireshark & mengidentifikasi jenis-jenis transaksi network

3.3. TEORI PENDUKUNG

Dengan kemudahan mengakses internet melalui wireless, banyak pengguna laptop selalu mencari atau memanfaatkan hotspot yang ada untuk selalu aktif. Ada yang hanya sekedar buka email, ada yang cuman sekedar browsing, bahkan, ada juga yang sampai mengirim tugas kantor. Para pemilk dan pengguna hotspot tidak menyadari bahwa mungkin, diantara mereka ada yang berniat jahat. Untuk kasus sederhana, sebuah hotspot umum palsu dapat menjebak para pemakainya untuk memberikan username dan password mereka tanpa mereka sadari bahwa mereka telah memberikannya. dalam artikel ini, akan saya jelaskan beberapa trik yang digunakan oleh beberapa orang yang berniat jelek dalam memakai wireless. Untuk masalah pencegahannya, bisa dilihat di artikel lain di website ini yang memberikan solusi dan pencegahannya. Untuk melakukan wireless hacking, langkah pertama yang dilakukan adalah mencari wireless network yang terdekat. Hal itu bisa dilakukan dengan wardrive (jika dilakukan diluar ruangan) atau berkeliling mengitari hotspot yang ada (jika di dalam ruangan). Dalam artikel ini, penulis mencoba menguraikan cara menggunakan wardrive karena lebih aman dan mengingat hanya mencoba untuk mengetahui jaringan wireless mana saja yang lemah.

Wardrive adalah ekspedisi memancing elektronik untuk mencari jaringan wireless yang lemah di sekitar pengguna. Kebanyakan, sebagian besar dari jaringan wireless tersebut bahkan tidak diberi password atau enkripsi untuk melindunginya. Kegiatan ini dilakukan untuk mencari jaringan mana saja yang akan dijadikan obyek serangan. Sehingga, bisa melakukan serangan terhadap jaringan wireless yang telah jadikan target. Untuk melakukan kegitan ini, diperlukan peralatan sederhana untuk memulainya.

Daftar peralatan yang dibutuhkan:

• GPS receiver

jika daerah tertentu sudah memiliki GPS, dapat dengan mudah menandai daerah mana saja yang sudah pernah dijelajahi dan memberi tanda khusus dimana dalam daerah yang sudah dijelajahi tersebut terdapat jaringan wireless yang lemah.

• Wireless PCMI card

Peralatan ini dibutuhkan untuk memperluas jaringan wireless. Biasanya, peralatan ini dilengkapi dengan jack untuk wireless antenna receiver atau mensupport jaringan selular untuk memperoleh jaringan yang lebih luas.

• Wireless antenna receiver

Peralatan ini dibutuhkan untuk menambah jangkauan wireless PCMI card dengan menghubungkan jack yang dimilikinya ke dalam wireless card. Jika wireless card yang dimiliki tidak mempunyai jack, maka dapat membeli wireless antenna yang memakai port usb yang sudah banyak beredar di pasaran. Tapi, jika merasa tidak puas dengan kemampuan memperoleh jaringan menggunakan peralatan yang dimiliki. Pencarian Wireless Network, Kebanyakan jaringan wireless yang beredar tidak mempunyai sekuriti atau enkripsi yang melindunginya. Untuk melacaknya, dibutuhkan peralatan yang mendukung.

• Network Stumbler atau lebih dikenal NetStumbler

Software berbasis windows ini sangat mudah mencari sinyal wireless yang dipancarkan dari hotspot ke pengguna. Penulis banyak menjumpai para pengguna wireless memakai software ini untuk mencari lokasi yang tepat untuk mendapat sinyal wireless dari hotspot yang kuat atau mensurvei apakah hotspot di daerahnya cukup bagus atau tidak.

• Kismet

Salah satu fungsi yang hilang dari NetStumbler adalah kemampuan untuk menampilkan SSID dari hotspot. pada access point, mereka selalu rutin membroadcast info ini. cuman, info tersebut kebanyakan berisi SSID yang tidak terbaca atau terenkripsi. Program ini akan mencari dan menampilkan SSID yang tidak di broadcast oleh hotspot dan sangat penting untuk mencari jaringan wireless yang akan diuji.

Memasuki jaringan wireless yang telah ditemukan Setelah menemukan sebuah jaringan network, langkah selanjutnya adalah mencoba untuk menghubungkan ke jaringan tersebut. Jika jaringan tersebut tidak menggunakan sekuriti enkripsi, bisa langsung mengakses ke SSID. Jika SSID tidak di broadcast, dapat masuk dengan SSID yang sedang tidak di broadcast. Tentu saja, didapat dengan mudah menemukan yang tidak di broadcast menggunakan fitur yang ada kismet, Jika jaringan tersebut dienkripsi, maka membutuhkan salah satu dari peralatan dibawah ini.

• CowPatty

Software ini menggunakan metode brute force untuk membuka WPA-PSK, yang mana PSK sendiri dianggap sebagai WEP baru unrtuk keamanan sekuriti wireless di rumah. Progam ini mencoba beberapa dari berbagai pilihan yang berasal dari file dictionary apakah ada yang sesuai dengan apa yang digunakan sebagai kunci tersebut

• ASLeap

jika ada jaringan yang menggunakan LEAP, alat ini bisa digunakan untuk mencari data semacam username dan password yang sedang online di jaringan, dan mengoverride akses pemiliknya.LEAP tidak memproteksi proses tersebut seperti EAP, yang mana itu menjadi kelemahan utama bagi LEAP.

Mengendus atau mencuri Data Wireless

Tidak peduli apakah pengguna terkoneksi langsung ke jaringan wireless atau tidak,, jika ada jaringan wireless di dalam daerah sekitar, selalu ada data yang lewat di dalam jaringan kapan pun itu. Untuk mengambil data itu, diperlu peralatan untuk mengambil atau melihat data tersebut.

• Wireshark (pendahulu Ethereal)

dimana masih terjadi perdebatan bagaimana cara ynag tercepat dalam menyikapi program ini, tidak ada keraguan lagi bahwa software ini sangat berguna. ia dapat mencari jaringan wireless yang ada lengkap dengan info sekuriti. software ini dapat mecuri data dari 802.11 manajemen hotspot dan bisa juga digunakan sebagai alat untuk mencari hotspot yang tidak memproteksi dirinya dengan SSID.

• SwitchSniffer

Software ini adalah program yang bisa mencari user yang aktif di jaringan switch LAN dan dapat mengambil seluruh packet data tanpa persetujuan user yang bersangkutan, software ini juga dapat mendeteksi program arpspoofer sedang berjalan dan membokir sesi pertahanan semacam firewal. jika ingin menggabungkan program ini dengan program sniffer yang lain, didapat dengan melihat dan mengambil id user dan password dari user lain di dalam sebuah jaringan.

Tindakan selanjutnya? Setelah mengetahui bagaimana proses hacking, terserah mau diapakan data ataupun hotspot yang telah ditemukan dan dieksploitasi. jika akan melaporkan ke admin hotspot bahwa ada kelemahan, maka telah menjadi bagian dari Ethical hacker. tapi, jika malah makin mengeksploitasi hotspot tersebut, maka dapat menjadi Blackcap Hacker.

3.4. HARDWARE DAN SOFTWARE

Alat dan bahan yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. Wireshark

3.5. PRE-TEST

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

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-06	CPMK-03	1. Apa yang anda ketahui tentang hacking wireless Network	50
2.	CPL-06	CPMK-03	2. Software apa saja yang dapat digunakan untuk hacking wifi	50

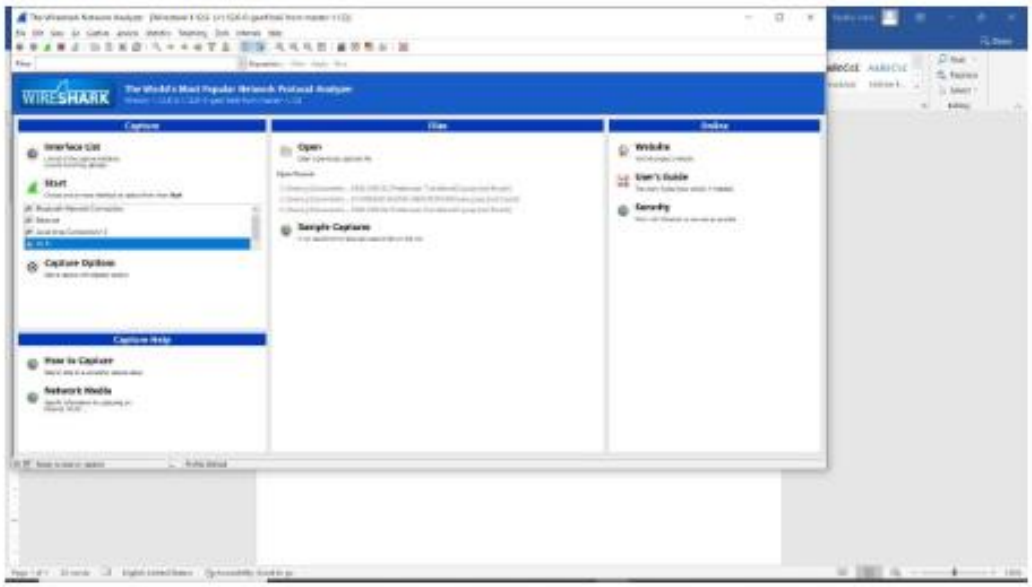
3.6. LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

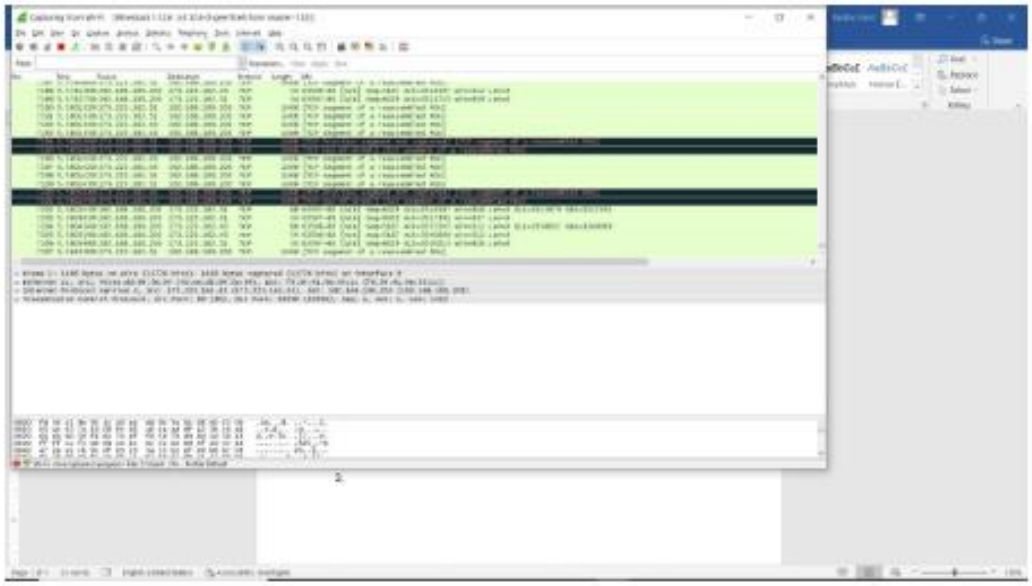
No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor

1.	CPL-06	CPMK-03	Selesaikan langkah praktikum berikut ini	Screen Shot Hasil praktikum	100

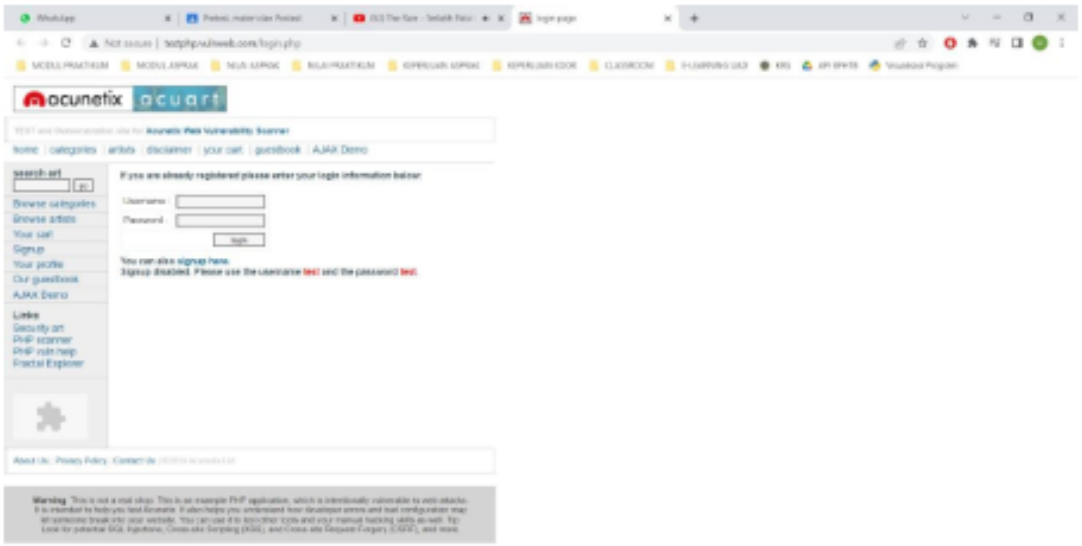
1. Buka aplikasi wireshark



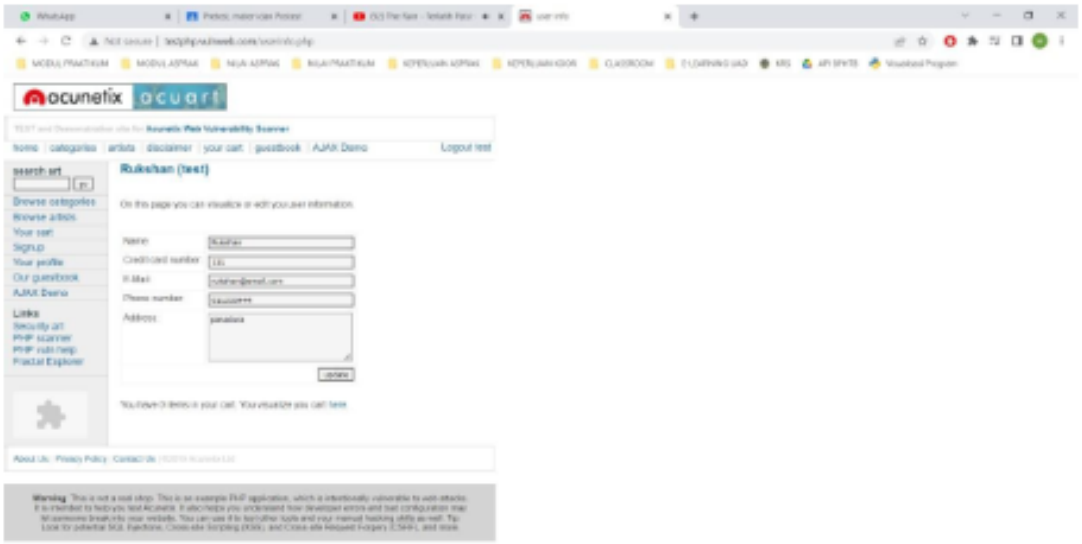
2. Scan jaringan yang digunakan



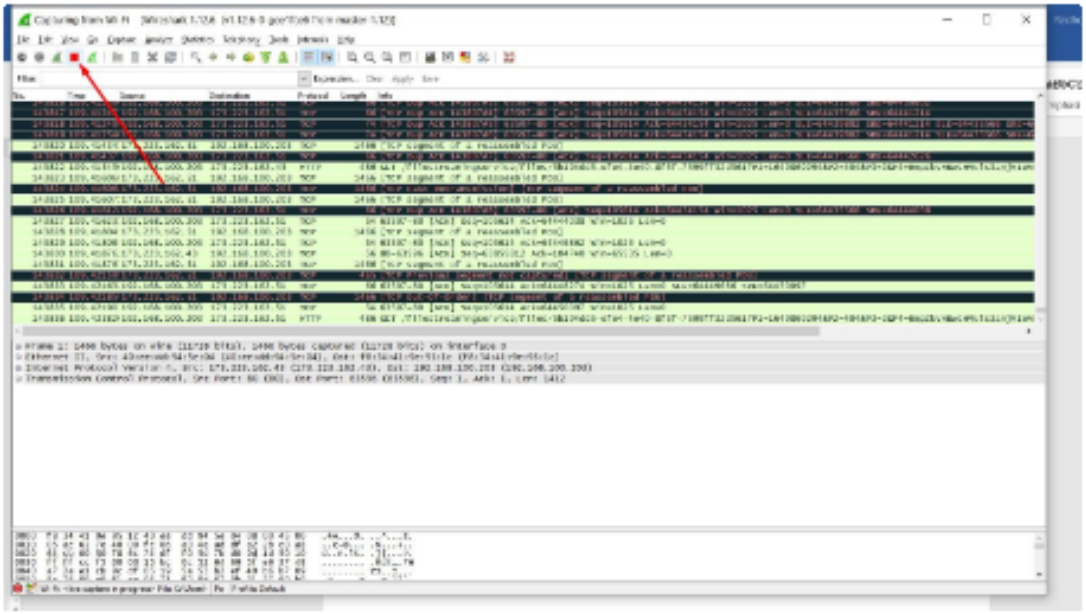
3. Buka website yang ingin kita sniffing, di sini saya menggunakan website http://testphp.vulnweb.com/login.php



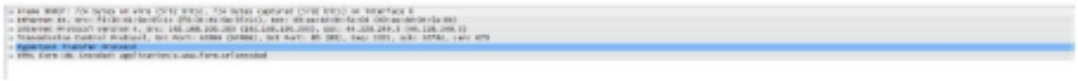
4. Selanjutnya login seperti biasa



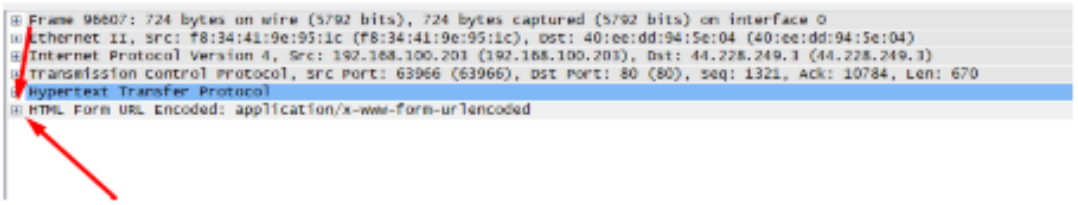
5. Kemudian jika sudah login pause scan yang ada pada wireshark



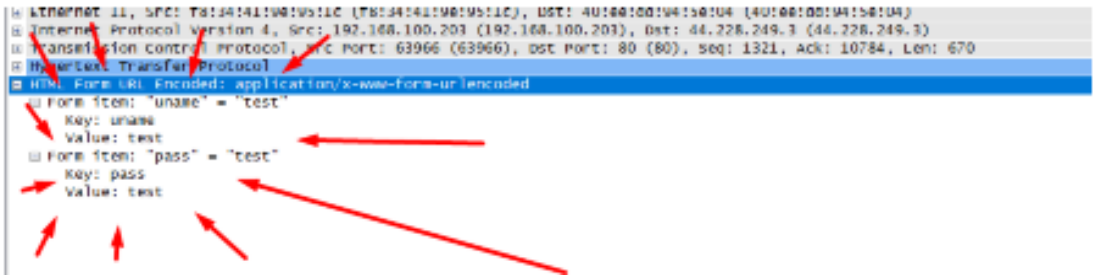
6. Jika sudah maka kita lakukan filter dengan query “http.request.method == "POST"” karena saat kita melakukan login disana terjadi sebuah request dari form input ke server dengan method POST



7. Setelah itu buka paket data yang sudah kita filter tadi, dan expand pada tab “HTML Form URL Encoded”



8. Setelah itu nanti muncul username dan password yang sudah kita inputkan di website tadi



3.7. POST TEST

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

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-06	CPMK-03	Lakukan langkah untuk sniffing mencari user name dan password, terserah menggunakan software apa saja, buat laporannya menggunakan kalimat yang baik dan mudah dipahami!	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-06	CPMK-03	20%		
2.	Praktik	CPL-06	CPMK-03	30%		
3.	Post-Test	CPL-06	CPMK-03	50%		
					Total Nilai	

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

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

PRAKTIKUM 4: HOST SECURITY

Pertemuan ke : 4

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

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

Pemenuhan CPL dan CPMK

CPL-06	Memahami tanggung jawab profesional dan menerapkan pengetahuan serta berkomunikasi efektif dalam melakukan penilaian berdasar informasi dan praktek computing dengan berpedoman pada prinsip-prinsip legal dan etika
CPMK-03	Mahasiswa mampu melakukan penetration tester dan memberikan rekomendasi resiko terhadap sistem keamanan informasi

4.1. DESKRIPSI CAPAIAN PEMBELAJARAN

Setelah mengikuti praktikum ini mahasiswa diharapkan: (sesuai dengan RPS)

1. Mampu melakukan analisisi keamanan menggunakan tools Host Security

4.2. INDIKATOR KETERCAPAIAN PEMBELAJARAN

CPL-06	CPMK-03	Kemampuan mahasiswa dalam melakukan Proses analisis menggunakan tools Host Security

4.3. TEORI PENDUKUNG

Setiap perangkat yang memiliki *IP address* dan terhubung ke jaringan dianggap sebagai *host*. *Host Security* adalah metode yang mengarah ke *hardening* setiap *host* yang ada di jaringan, termasuk di dalamnya *hardening* sistem operasi dan aplikasi untuk menjamin perlindungan *host* dari resiko dan ancaman yang mungkin terjadi, perusahaan harus memastikan *confidentiality*, *availability*, dan *integrity* dari *host* dan data yang mereka punya, sebuah konfigurasi yang tidak aman dari suatu *host* bisa menjadi resiko untuk keseluruhan jaringan.

Host bisa mendapat resiko dari ancaman internal dan eksternal, ancaman internal biasa terjadi pada suatu organisasi dan kerusakan diakibatkan oleh ancaman-ancaman yang berakhir pada kerugian aset yang besar pada suatu organisasi. Ancaman-ancaman ini dapat berupa serangan *malware*, pencurian data, *unauthorized access*, penggunaan *resource* perusahaan secara ilegal, dll. Setiap jenis dari serangan dapat berdampak ke *End User* dan bisnis dari perusahaan itu sendiri, para admin harus melakukan evaluasi *host* mereka menghadapi kemungkinan terjadinya ancaman internal dan eksternal.

Seorang penyerang dapat mengambil keuntungan dari berbagai jenis celah yang ada dengan tujuan untuk menyerang *host* tertentu. Ancaman dari eksploitasi celah yang ada pada suatu *host* dapat membuka beberapa jalan ke dalam sistem dan kemudian dapat menginfeksi sistem tersebut. Kurangnya pengetahuan, kemampuan dan konfigurasi yang tidak aman pada *host* dapat membuka celah keamanan, contohnya seperti komputer yang tidak di-*patch*, *phising* dan spam pada email, *internet download* dari sumber yang tidak dipercaya yang mengarah pada *malware*, *social engineering* untuk mendapat *unauthorized access*, dll.

Host pada jaringan dikonfigurasi dan ditujukan untuk melakukan beberapa fungsi tertentu, *host* ini menyimpan dan menangani berbagai jenis informasi sensitif dan menyediakan beberapa servis dari perusahaan. Jenis *host* yang berbeda membutuhkan level keamanan yang berbeda sesuai dengan data atau servis yang ditangani, contohnya *host* yang berfungsi sebagai *server* pada jaringan, menyimpan informasi sensitif, dan melakukan fungsi yang kritikal membutuhkan tingkat keamanan yang lebih dari *host* lain.

Teknik Hardening **Security Baseline** mengacu kepada standar konfigurasi security minimum (juga diketahui sebagai petunjuk dan ceklis) yang dibuat untuk setiap *host* yang ada di jaringan. **Hardening** adalah berbagai teknik yang digunakan pada *host* untuk menutup celah yang ada dan secara umum melindungi sistem dari berbagai macam ancaman dan serangan, salah satunya adalah dengan mengikuti *security baseline* yang ada. Beberapa tipe *Hardening* yang umum yaitu:

Hardening Sistem Operasi:

- Windows Server
- Red Hat Family
- Linux lainnya

Hardening Aplikasi:

- Aplikasi Mobile
- Aplikasi Web
- Aplikasi Desktop

Hardening Jaringan:

- Router dan Switch
- Access Point
- Firewall
- IPS/IDS
- SIEM

Framework:

- CIS
- EC-Council
- ISSAF
- NSA
- PCI
- Red Hat Hardening
- dll

4.4. HARDWARE DAN SOFTWARE

Alat dan bahan yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. Tools Spytech
3. Tools MBSA

4.5. PRE-TEST

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

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-06	CPMK-03	1. Jelaskan apa itu host security dan jelaskan fungsi dari host security ?	50
2.	CPL-06	CPMK-03	2. Ancaman apa saja yang bisa terjadi jika pengguna mengabaikan host security?	50

4.6. LANGKAH PRAKTIKUM

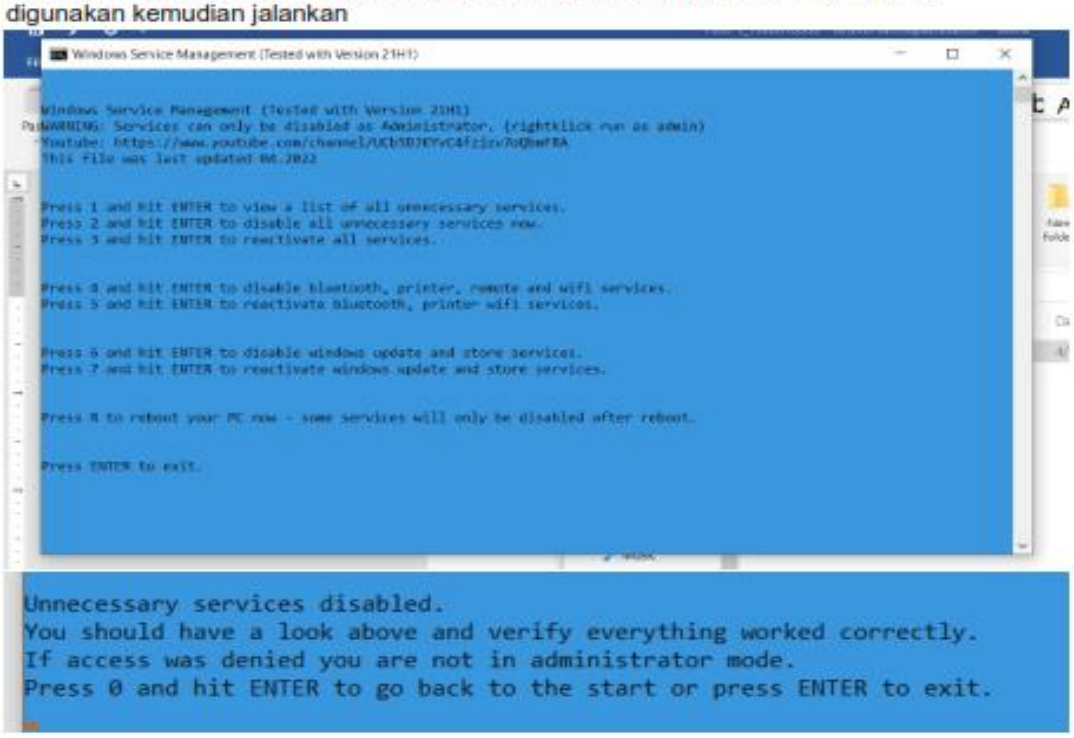
Aturan Penilaian (Total Skor: 100):

No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-06	CPMK-03	Selesaikan langkah praktikum berikut?	Screen Shot Hasil praktikum	100

A. METODE 1

Link: https://www.youtube.com/watch?v=_F0i5HiT9eM

- Download aplikasi yang sudah dibuat, karena bisa mematikan service yang tidak digunakan kemudian jalankan



B. METODE 2

Link: https://www.youtube.com/watch?v=Hfam2DRz0gw

- Download MBSA

- Install MBSA

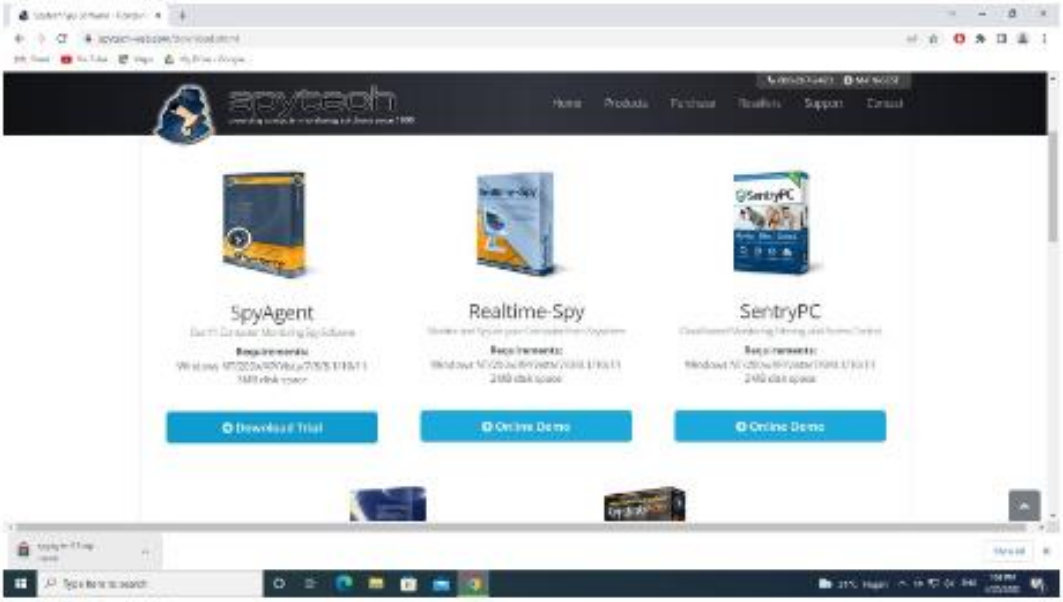
- Jika sudah terinstal lakukan scanning terhadap PC

- Berikut adalah hasil dari scanning tersebut

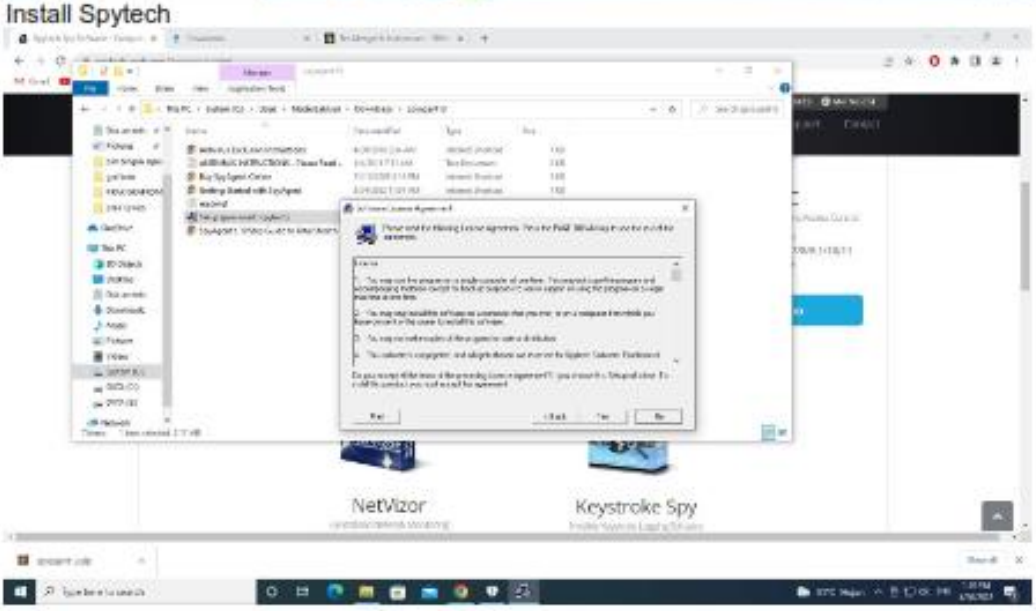
C. METODE 3

Link: https://www.youtube.com/watch?v=yLab7Z4J57w

- Download Spytech

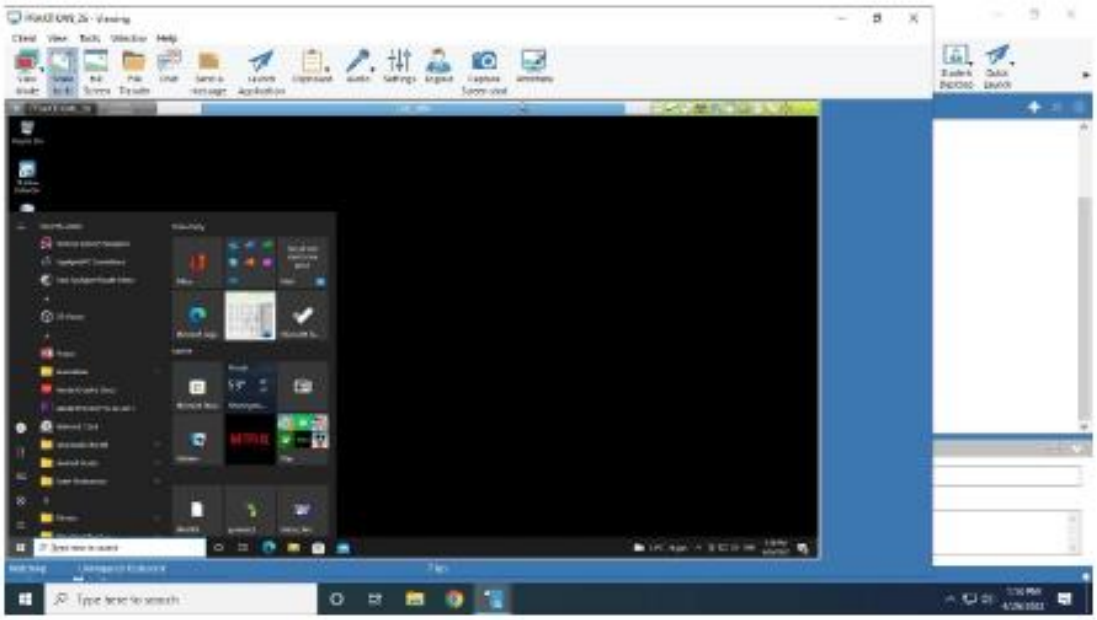


- Install Spytech

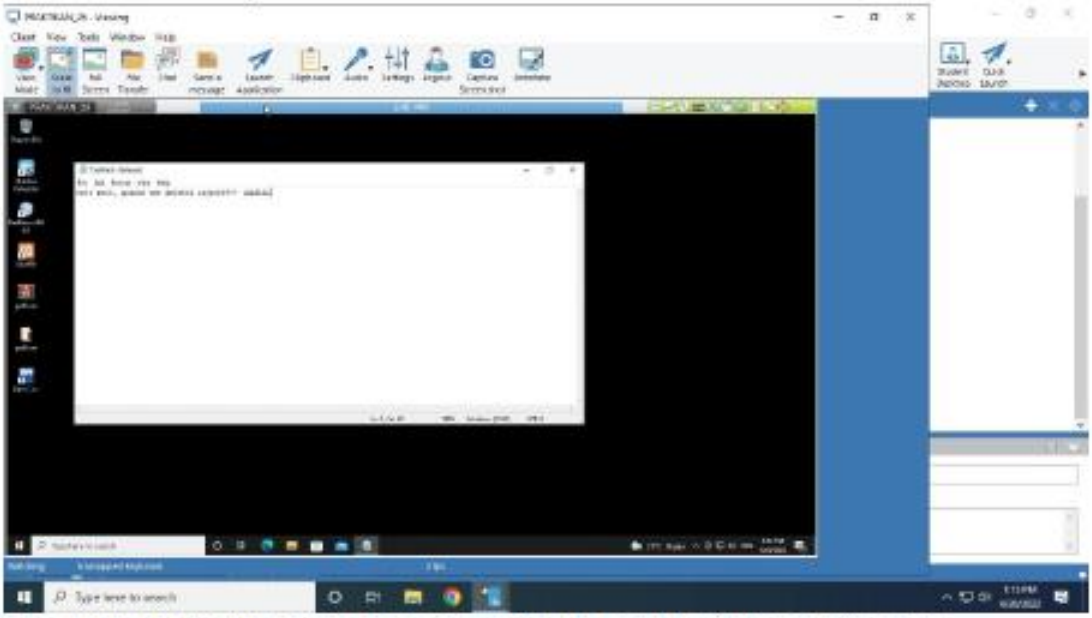


- Start monitoring Spytech

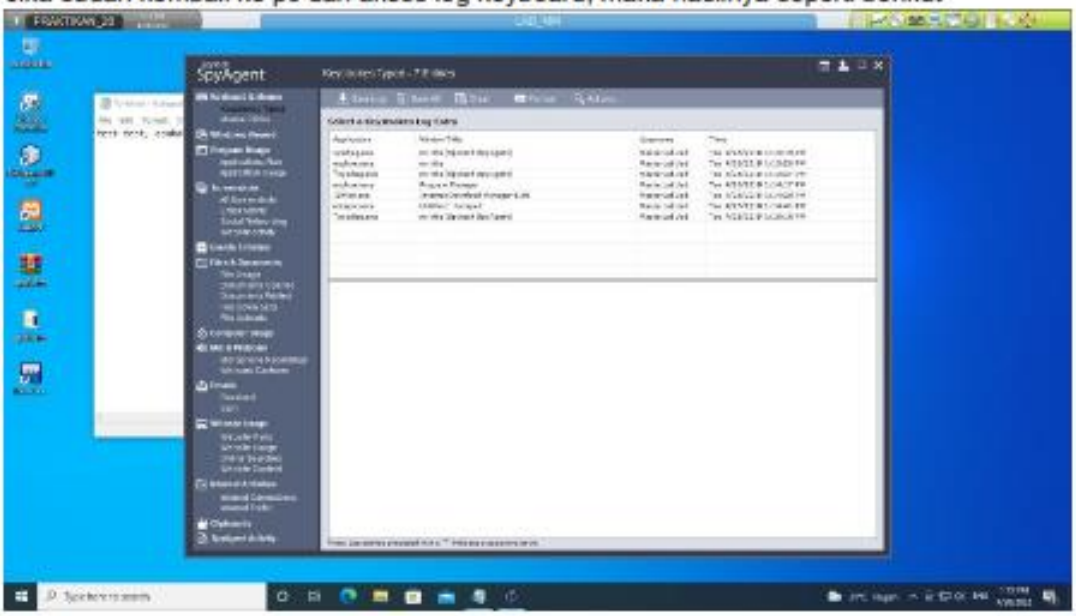
- Jika sudah start monitoring, saatnya kita simulasikan dengan cara meremote PC ini

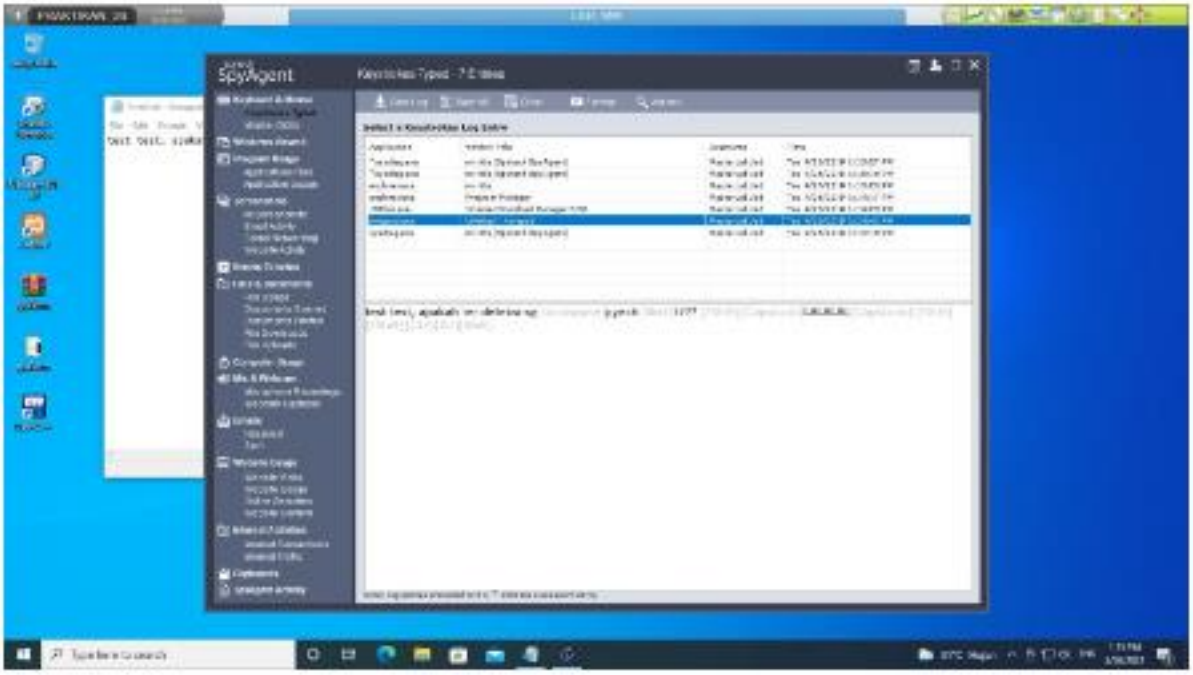


- Tulis sesuatu di notepad



- Jika sudah kembali ke pc dan akses log keyboard, maka hasilnya seperti berikut





4.7. POST TEST

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

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-06	CPMK-03	Silahkan lakukan pengamanan Host security pada laptop masing-masing seperti yang ada pada materi yang sudah di berikan (minimal 3 metode dari materi diatas). Lalu buatkan dokumentasi dari pengamanan dan sertakan tutorialnya.	100

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-06	CPMK-03	20%		
2.	Praktik	CPL-06	CPMK-03	30%		
3.	Post-Test	CPL-06	CPMK-03	50%		
					Total Nilai	

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

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

PRAKTIKUM 5: BUG BOUNTY

Pertemuan ke : 5

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

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

Pemenuhan CPL dan CPMK

CPL-07	Mampu memilih, membuat dan menerapakan teknik, sumber daya, penggunaan perangkat teknik modern dan implementasi teknologi informasi untuk memecahkan masalah
CPMK-03	Mahasiswa mampu melakukan penetration tester dan memberikan rekomendasi resiko terhadap sistem keamanan informasi

5.1. TUJUAN DAN INDIKATOR CAPAIAN

Setelah mengikuti praktikum ini mahasiswa diharapkan;
1. Praktikan mampu menganalisis web Vlun berupa bug tertentu
2. Praktikan mampu melakukan perbaikan dari system bug yang ditemukan

5.2. INDIKATOR KETERCAPAIAN PEMBELAJARAN

CPL-07	CPMK-03	Kemampuan mahasiswa menganalisis web Vlun dan merepresentasikan hasil temuan selanjutnya melakukan perbaikan

5.3. TEORI PENDUKUNG

Bug hunter adalah istilah yang ditujukan kepada seseorang yang bekerja dalam menemukan bug di suatu sistem atau aplikasi. Dalam penerapannya, bug hunter menjalankan program yang dikenal dengan sebutan bug bounty program. Bug bounty program ini sendiri sudah banyak digunakan oleh perusahaan-perusahaan besar, seperti Google, Facebook, hingga Yahoo. Nantinya, perusahaan tersebut akan memberikan penawaran menarik kepada bug hunter apabila berhasil menemukan masalah pada aplikasinya. Jadi dengan kata lain, bug bounty program yang dijalankan oleh bug hunter ini adalah kegiatan yang dibayar untuk menemukan kerentanan dalam perangkat lunak, situs web, hingga aplikasi web. Hal ini dilakukan sebab tidak semua tim keamanan IT di perusahaan memiliki cukup waktu untuk mengatasi banyaknya bug yang dialami. Karena keberadaannya sangat dibutuhkan, profesi bug hunter ini bisa mendapatkan bayar hingga puluhan ribu dolar per tahunnya. Kendati demikian, ada beberapa syarat yang memang harus dimiliki oleh seorang bug hunter, yakni rasa ingin tahu yang tinggi, keahlian teknis dalam web dan jaringan, hingga kemampuan untuk memecahkan masalah.

Jika melihat penjelasan yang ada di atas, tentu bisa mengetahui bahwa bug hunter bukan profesi yang mudah untuk dijalani. Oleh karena itu, penting untuk seseorang yang tertarik di profesi ini mengetahui bagaimana cara kerja dari bug hunter. Cara kerja bug hunter ini dapat dipelajari lebih lanjut, supaya kedepannya memiliki bayangan tersendiri.

Hal pertama yang perlu diketahui adalah cara kerja dari suatu aplikasi dan bagaimana arsitektur dari aplikasi tersebut. Kamu bisa memulai dengan mengetahui dasar dari aplikasi maupun web,

seperti HTML, CSS, PHP, hingga JavaScript. Selain itu, pemahaman yang kuat tentang meningkatkan dan menganalisis masalah bug juga dibutuhkan oleh seorang bug hunter. Itu sebabnya, ada beberapa komponen yang dibutuhkan untuk menjadi seorang bug hunter, di antaranya:

- Local & Remote file inclusion
- Information Disclosure
- Remote Code Execution (RCE)
- Pengumpulan informasi
- SQL Injection
- Cross-Site Scripting (XSS)
- Server Side Request Forgery (SSRF)

Untuk gambaran lebih jelasnya, salah satu seseorang yang bekerja menjadi seorang bug hunter adalah James Kettle. Karena keahlian yang dimilikinya, James mampu mencari kesalahan kode yang mungkin dapat ditemukan oleh penjahat untuk masuk ke sistem jaringan dan mencuri data.

Dalam pengerjaannya, James membutuhkan 50 jam untuk menguji satu bug agar benar-benar valid dan tidak terjadi kesalahan. Kini, James menjadi salah satu bug hunter di Hasker One, layanan yang bekerjasama dengan perusahaan dan pemerintah yang mencari para ahli untuk menguji perangkat lunak milik mereka.

Perbedaan Bug Hunter dan Hacker

Secara sekilas akan menganggap bahwa bug hunter mirip dengan hacker. Padahal, kedua istilah ini memiliki perbedaan yang signifikan, sebab bug hunter memiliki nilai yang lebih positif daripada hacker. Kendati demikian, ada juga beberapa hacker yang memang bekerja dengan tidak merugikan orang lain. Lebih jelasnya, hacker adalah seseorang yang memiliki skill pemrograman dan memanfaatkannya untuk melakukan tindakan pencurian data pribadi atau perusahaan. Sementara bug hunter adalah seseorang yang memiliki skill pemrograman namun memanfaatkannya untuk menemukan dan melaporkan bug pada suatu perusahaan.

Oleh karena itu, bug hunter dinilai lebih bermanfaat dan tidak merugikan siapapun dibandingkan dengan hacker. Jadi, jangan heran ya, apabila bug hunter hingga kini menjadi profesi diinginkan oleh beberapa orang yang menggeluti dunia teknologi.

Daftar Bug Bounty Program

Sebelumnya sudah dijelaskan bahwa bug bounty program adalah program yang dijalankan oleh bug hunter. Lebih lengkapnya, bug bounty program adalah kesempatan yang ditawarkan oleh organisasi, situs web, maupun para pengembang software kepada individu untuk melaporkan bug.

Perlu diketahui bahwa setiap bug bounty program yang dikuratori oleh perusahaan terkemuka memiliki imbalan yang akan diberikan kepada bug hunter. Ingin tahu apa saja daftar bug bounty program dari perusahaan-perusahaan besar? Berikut informasinya, yakni:

- **Google**. Bug bounty program pada Google menawarkan pembayaran minimum $300 hingga hadiah tertinggi $31.337 untuk aplikasi Google.
- **Quora**. Bug bounty program pada Quora menawarkan pembayaran minimum $100 hingga $7000 apabila menemukan dan melaporkan bug dalam aplikasi mereka.
- **Mozilla**. Bug bounty program pada Mozilla menawarkan pembayaran $500 hingga $5000 untuk menemukan bug di layanan mozilla, seperti Firefox, Thunderbird, dan aplikasi serta layanan lainnya.
- **Microsoft**. Bug bounty program pada Microsoft menawarkan pembayaran sebesar $15.000 hingga $250.000 untuk menemukan bug kritis.
- **Twitter**. Bug bounty program pada Twitter menawarkan program yang dimulai dari $140 hingga $15000.

5.4. HARDWARE DAN SOFTWARE

Alat dan bahan yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. Kali Linux
3. Tools Bug Bounty Uniscan

5.5. PRE-TEST

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

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-03	1. Apa yang dimaksud dengan Bug Hunter dan Bug Bounty? 2. Apa perbedaan Bug Hunter dengan Hacker?	50
2.	CPL-07	CPMK-03	3. Metode apa saja yang digunakan oleh Bug Hunter dalam menemukan Bug? Jelaskan! 4. Jelaskan fungsi dari kegiatan Bug Hunter?	50

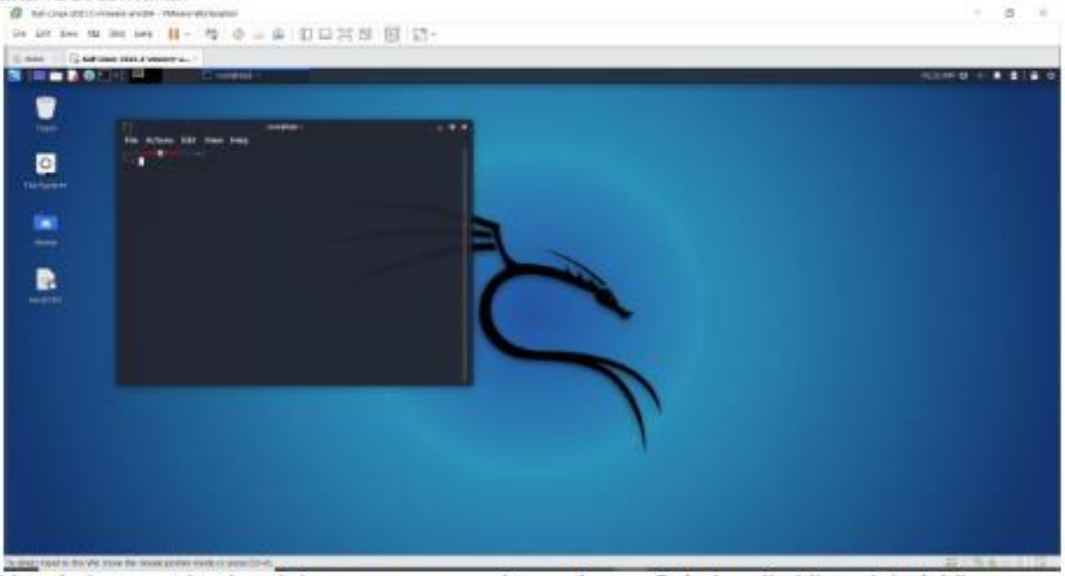
5.6. LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

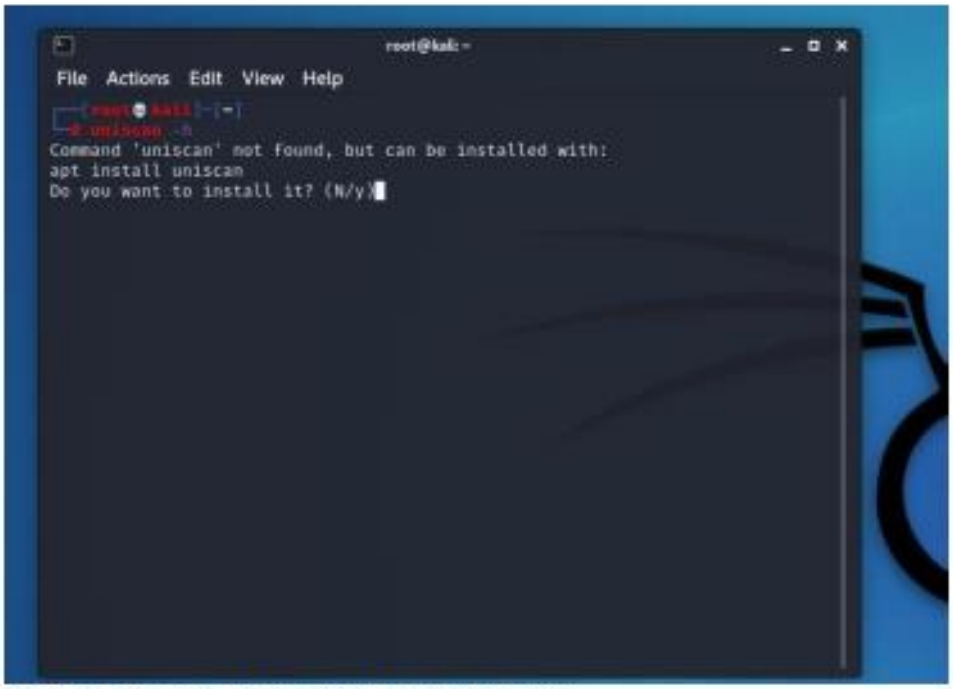
No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-07	CPMK-03	Selesaikan langkah praktikum berikut!	Screen Shot Hasil praktikum	100

1. Jalankan OS Kali Linux

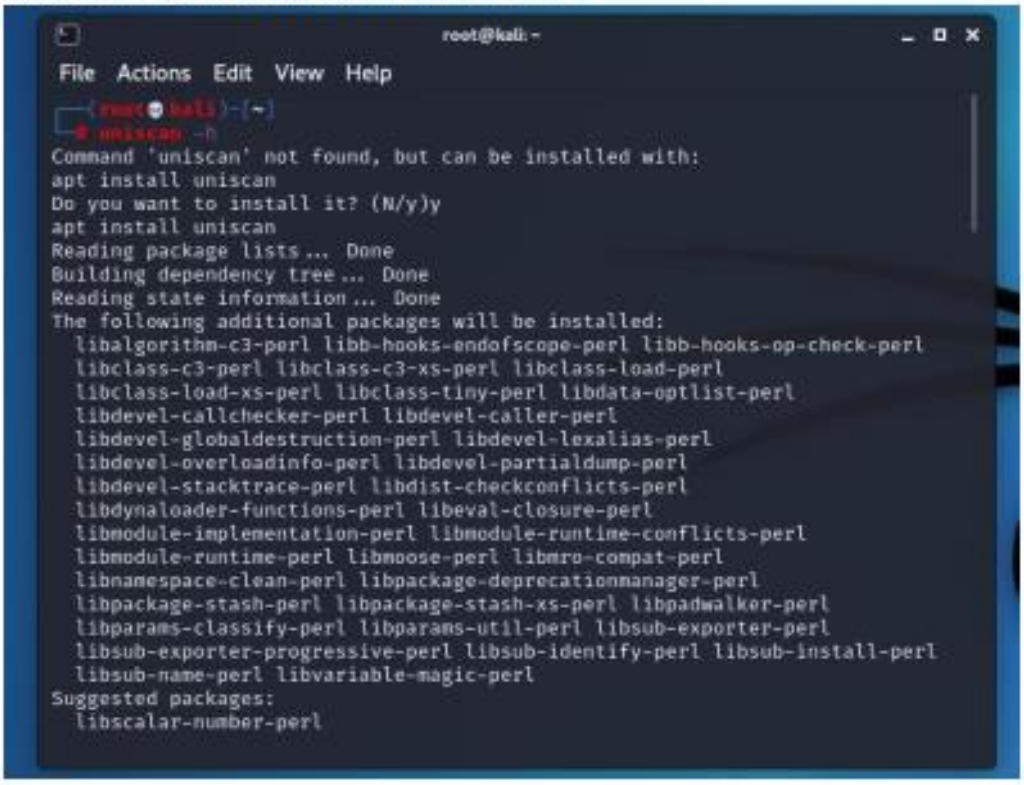
2. Buka root terminal



3. Di langkah pencarian bug ini, saya menggunakan uniscan. Sebelum itu kita cek terlebih dahulu apakah uniscan sudah terinstal atau belum



4. Karena belum terinstal kita install terlebih dahulu



5. Jika sudah terinstal mari kita cek kembali, dengan menjalankan command uniscan -h

```
┌──(root💀kali)-[~]
└─# uniscan -h
#######################################
# Uniscan project                     #
# http://uniscan.sourceforge.net/     #
#######################################
V. 6.3


OPTIONS:
        -h      help
        -u      <url> example: https://www.example.com/
        -f      <file> list of url's
        -b      Uniscan go to background
        -q      Enable Directory checks
        -w      Enable File checks
        -e      Enable robots.txt and sitemap.xml check
        -d      Enable Dynamic checks
        -s      Enable Static checks
```

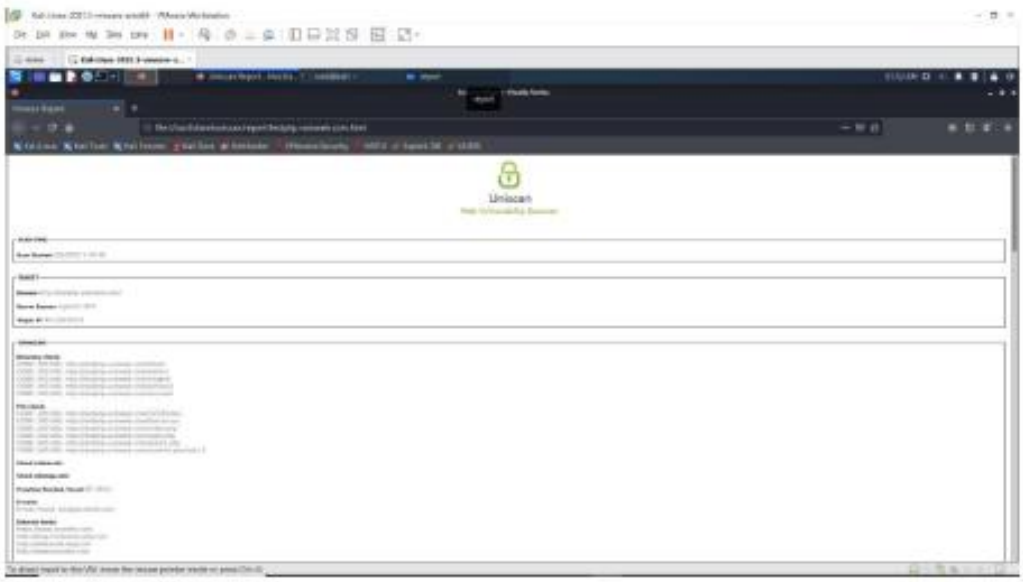
6. Selanjutnya adalah mencari target website yang ingin kita cari bugnya, di sini saya menggunakan website http://testphp.vulnweb.com/

7. Oke selanjutnya kita jalankan uniscan, dan tunggu hingga proses scanning selesai

```
┌──(root💀kali)-[~]
└─# uniscan -u http://testphp.vulnweb.com/ -qweds
#######################################
# Uniscan project                     #
# http://uniscan.sourceforge.net/     #
#######################################
V. 6.3


Scan date: 3-5-2022 1:29:16
═══════════════════════════════════════════════════════════════
┌──────────────────
| Domain: http://testphp.vulnweb.com/
| Server: nginx/1.19.0
| IP: 44.228.249.3
└──────────────────
```

8. Beriku hasil scan dari uniscan



Untuk bagian code semuanya lancer karena, uniscan memberikan code 200. Tetapi pada dynamic test website ada bug seperti sql injeksi dan XSS

5.7. POST TEST

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

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-03	Lakukanlah kegiatan Bug Bounty pada beberapa website yang memiliki Vuln dan carilah informasi dan Bug yang terdapat didalam website tersebut. Silahkan buat langkah dan jelaskan step by step dari langkah bug Bounty yang di lakukan. Dilarang menggunakan website kampus dan website yang sama.	100

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: DATA BACKUP AND RECOVERY

Pertemuan ke : 6

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

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

Pemenuhan CPL dan CPMK

CPL-07	Mampu memilih, membuat dan menerapakan teknik, sumber daya, penggunaan perangkat teknik modern dan implementasi teknologi informasi untuk memecahkan masalah
CPMK-03	Mahasiswa mampu melakukan penetration tester dan memberikan rekomendasi resiko terhadap sistem keamanan informasi

6.1. TUJUAN DAN INDIKATOR CAPAIAN

Setelah mengikuti praktikum ini mahasiswa diharapkan:
1. Praktikan mampu membuat dan melakukan backup menggunakan tools tertentu
2. Praktikan mampu melakukan recovery dengan tools terkait

6.2. INDIKATOR KETERCAPAIAN PEMBELAJARAN

CPL-07	CPMK-03	Kemampuan mahasiswa dalam melakukan backup dan recovery

6.3. TEORI PENDUKUNG

Kebutuhan backup bagi sebuah perusahaan di era digital ini telah menjadi kebutuhan yang utama dan wajib sebagai bagian dari *business continuity plan*. Dikarenakan data merupakan aset perusahaan yang sangat penting sehingga perlu dijaga dan mutlak untuk dibuatkan suatu sistem untuk bisa merawatnya. Tanpa backup dan restore, maka perusahaan tersebut beresiko kehilangan aset penting perusahaan. Sistem Backup data yang baik dan benar akan membantu baik manajemen perusahaan atau juga para pelaku dibidang teknologi informasi untuk bisa menyimpan data perusahaan sebaik mungkin dan mengembalikan data tersebut apabila diperlukan oleh pihak yang membutuhkannya.

Di era digital ini, telah banyak masyarakat umum, individu, dan organisasi-organisasi lainnya yang telah mengerti dan memahami pentingnya menggunakan teknologi backup berbasis cloud untuk mengamankan sebuah data. Fungsi backup data berbasis cloud untuk mengamankan dan melakukan restore data apabila sewaktu-waktu data rusak, hilang, atau terkena virus. Untuk menjawab kebutuhan yang tinggi akan backup berbasis cloud untuk masyarakat yang 'sibuk' bekerja dan fokus pada pengembangan bisnis utama. Tentu akan berpotensi data tidak terbackup secara benar.

Perlunya penyimpanan data cadangan atau backup data telah didukung oleh Perpres 95 tahun 2018 pasal 40 ayat (1) dan ayat (4) tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) mewajibkan penyediaan cadangan (backup) atau dan pemulihan (restore). Jangan pernah mengabaikan proses backup dan restore data bisnis tertentu, karena bisa mengakibatkan bisnis berhenti beroperasi.

Backup data adalah sebuah proses menyalin data fisik atau file ke penyimpanan sekunder, seperti flashdisk, hardisk eksternal, sistem cloud atau media lainnya, hal ini mengantisipasi apabila data primer mengalami kerusakan atau hilang. Kerusakan data primer disebabkan oleh beberapa

kondisi, seperti kerusakan pada perangkat itu sendiri diakibatkan bencana alam, data yang corrupt, serangan (virus atau malware), atau menghapus data dengan tidak sengaja(human error). Sehingga ketika sewaktu-waktu data utama hilang, Pengguna masih dapat mengembalikan data-data secara penuh tanpa adanya kerusakan maupun kehilangan. Selain itu, ada beberapa manfaat yang diperoleh dari backup yang akan dijelaskan di bawah ini.

Manfaat Backup Data

1. Memberikan kemudahan untuk mengakses file dengan cepat
2. Ketika telah membuat cadangan data (backup), saat data diperlukan dapat diakses dengan cepat hitungan detik saja. Apalagi, kini sudah ada teknologi cloud yang memungkinkan untuk melakukan pencadangan data secara otomatis dan dapat diakses dengan cepat menggunakan koneksi internet.
3. Melindungi perangkat dari kehilangan daya
   Tanpa disadari, computer sangat rentan terhadap berbagai kerusakan, seperti kerusakan sistem, bencana alam, pemadaman listrik sehingga merusak kinerja dari hardisk komputer. Dengan begitu, pengguna perlu membuat cadangan data perusahaan Anda secara berkala agar tidak perlu khawatir akan hilangnya data penting didalamnya.
4. Memulihkan sistem operasi yang gagal
   Pada umumnya, kerusakan pada komputer bisa terjadi karena sistem operasi gagal dalam memproses berbagai program yang terus bertambah setiap waktunya dan ditambah lagi dengan pengalokasian ruang memori yang kurang tepat. Jadi, melakukan backup data dinilai lebih efisien untuk mengamankan data dari kegagalan sistem operasi. Dengan sistem backup berbasis cloud, tidak perlu memakan waktu lama untuk pengadaan barang. cukup menghubungi Elitery untuk berlangganan menggunakan Elivault untuk memudahkan proses backup perusahaan tertentu.

Apa itu Restore Data?Dalam terjemahan Bahasa Inggris arti restore adalah mengembalikan, jadi restore adalah proses mengembalikan kembali sebuah data atau file ke tempat semula. Jadi misalnya data pengguna terhapus secara tidak sengaja, maka masih dapat mencari file data tersebut dalam recycle bin komputer untuk kemudian dikembalikan ke tempat lokasi semula file itu berada, di suatu folder tertentu.

Hal ini juga berlaku untuk sistem maupun aplikasi yang telah terinstall. Lalu bagaimana jika data yang terhapus tersebut sudah tidak berada dalam recycle bin padahal data tersebut sangat penting, masih dibutuhkan dan tidak sengaja terhapus? Tentu saja solusi terbaik adalah memiliki backup data di suatu media penyimpanan lainnya seperti cloud.

Fungsi Restore Data Prinsip restore bersifat untuk mengembalikan data, file, maupun system dalam keadaan semula. Ada dua jenis restore data, pertama adalah system restore dan yang kedua adalah system image backup. System storage data dilakukan untuk melakukan pengembalian pengaturan software dan sistem aplikasi yang telah terinstall di dalam sistem komputer tanpa mempengaruhi data-data personal yang ada didalamnya.

Jika pengguna secara tidak sengaja menghapus data, pengguna dapat menggunakan system image backup untuk mengembalikan seluruh sistem aplikasi beserta file-file personal berupa data dan media lainnya. Jadi tipe restore ini lebih menyeluruh karena dapat mencakup restore data beserta sistemnya seperti sedia kala. Secara prinsip, restore memang hampir sama dengan backup yang memiliki tujuan untuk menyelamatkan data. Bedanya, jika backup ini cara kerjanya dengan cara menduplikasi atau menyalin data, sedangkan restore yang bertugas mengembalikan data maupun sistem sama seperti pada keadaan awalnya.

Pengertian Recovery Data Arti kata Recovery data adalah suatu proses pemulihan sistem yang bermasalah agar bisa pulih seperti sedia kala. Recovery pada komputer dilakukan akibat adanya serangan virus atau malware yang menyerang sistem komputer dan menimbulkan kerusakan yang cukup parah. Recovery data sangat tepat dipakai saat tidak memiliki aplikasi antivirus pada sistem komputer. Melakukan proses recovery data ini dijamin sangat efektif dalam mengembalikan sistem yang error bahkan yang terjangkit virus karena tidak dapat ditangani antivirus. Recovery data juga dapat memulihkan berbagai data yang ada di media penyimpanan seperti hardisk, flashdisk, memory card, kamera digital dan lain-lainnya.

Perbedaan Backup Restore dengan Recovery Sebelumnya juga telah dijelaskan bahwa recovery ini hampir sama dengan backup dan restore. Ketiga aktivitas tersebut memang saling berkaitan, namun pada nyatanya memiliki pengertian yang berbeda. Backup data adalah tindakan pencegahan yang dilakukan untuk berjaga-jaga apabila data mengalami kerusakan atau hilang. Biasanya suatu sistem menjadi rusak atau error dapat disebabkan melalui faktor internal dan eksternal. Dari faktor internal misalnya karena kelalaian manusia/human error, kerusakan hardware, maupun kurangnya maintenance dan perawatan. Sedangkan faktor eksternal yang dapat mempengaruhi kerusakan sistem dapat terjadi karena sistem terkena virus. Jadi proses backup dilakukan sebelum terjadi adanya kerusakan atau kehilangan.Sedangkan proses restore adalah kegiatan memulihkan data yang tidak sengaja di hapus. Biasanya data yang terhapus akan secara otomatis tersimpan di recycle bin. Proses restore dapat dilakukan dengan mudah yaitu dengan membuka halaman recycle bin dan lakukan restore. Jadi proses restore hanya dapat dilakukan apabila data terhapus ada di dalam halaman recycle bin.

6.4. HARDWARE DAN SOFTWARE

Alat dan bahan yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. Tools Recovery AOMEI Standart
3. Tools Easus Backup

6.5. PRE-TEST

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

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-03	1. Jelaskan apa fungsi dari backup data? 2. Jelaskan fungsi dari Recovery data?	50
2.	CPL-07	CPMK-03	3. Sebutkan jenis-jenis dari backup data? 4. Jelaskan apakah data yang bisa terhapus permanen apakah bisa direcovery atau tidak?	50

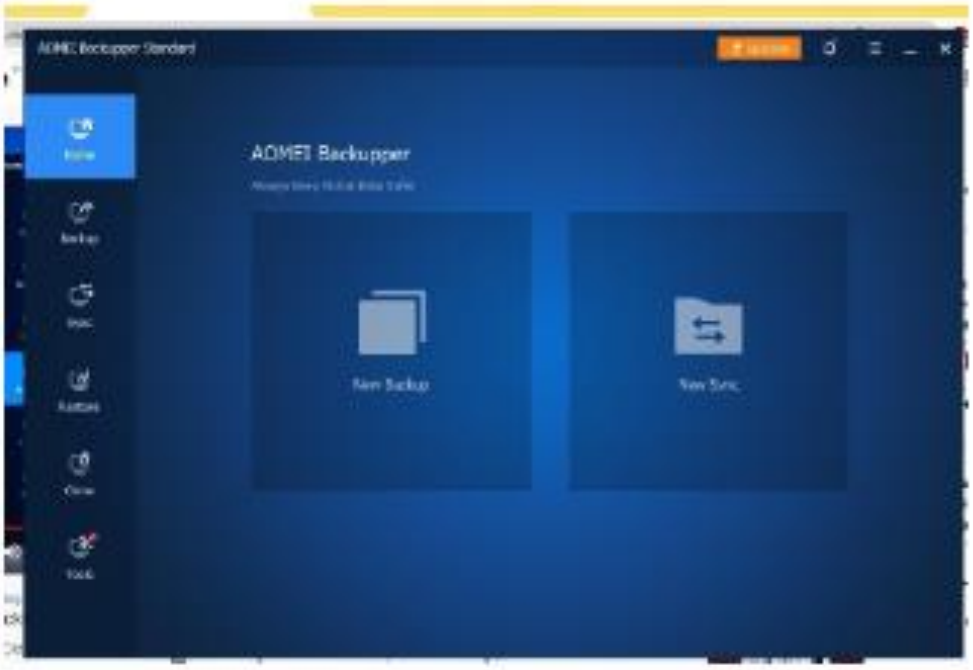
6.6. LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

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

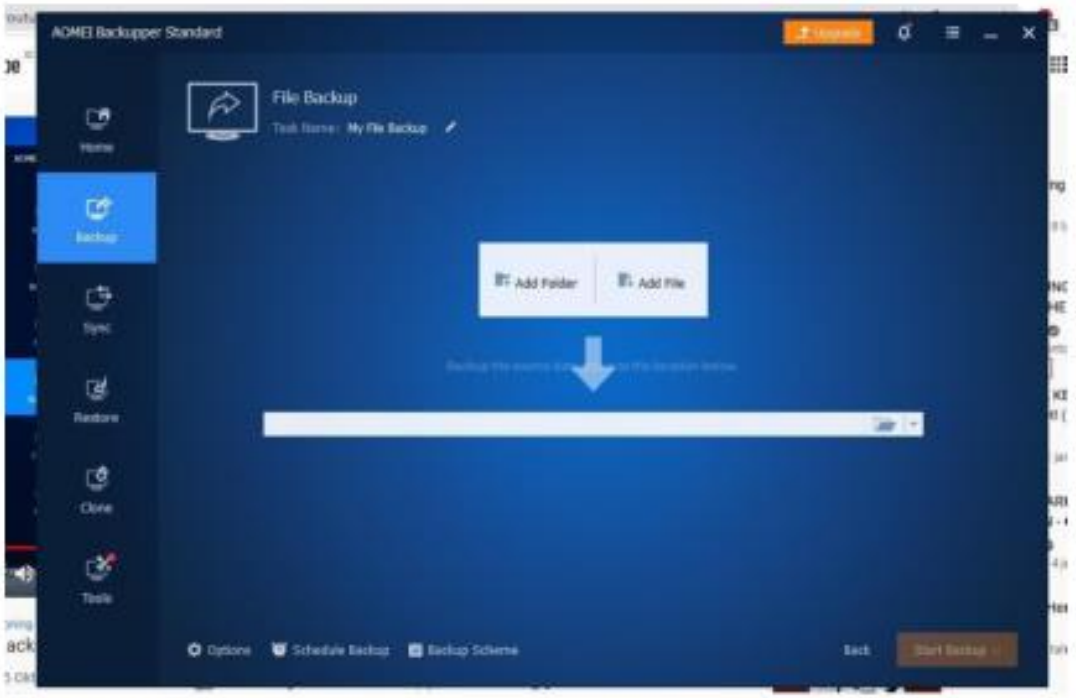
Backup Data

1. Buka Aplikasi AOMEI BACKUPPER

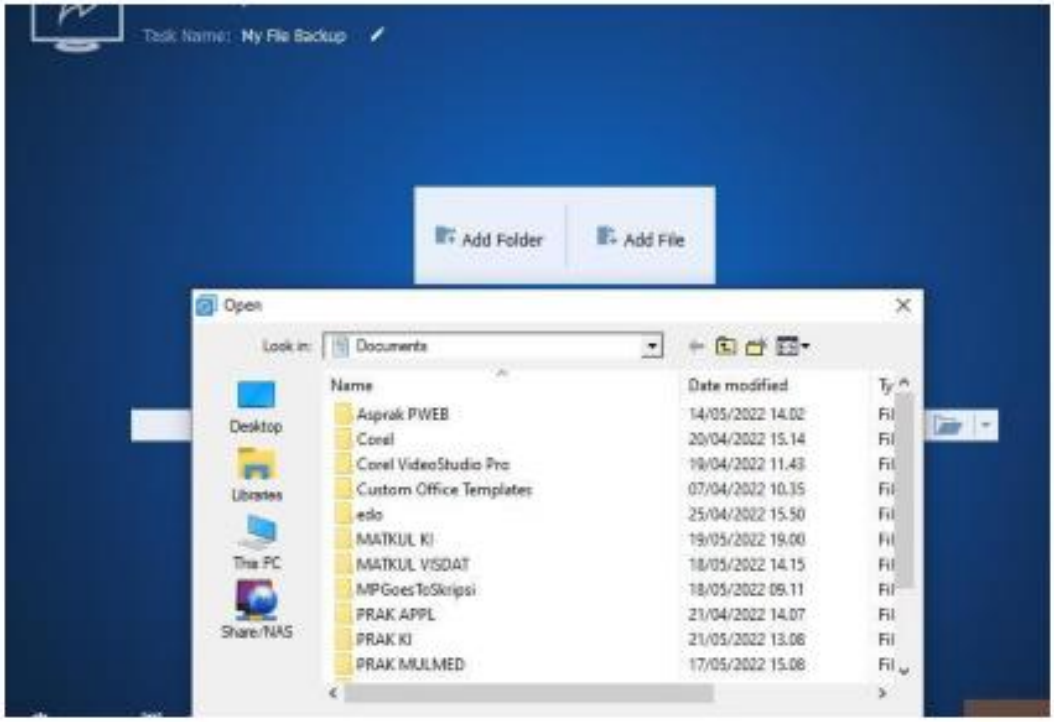


2. Pilih menu backup

3. Pilih menu file backup



4. Klik add folder



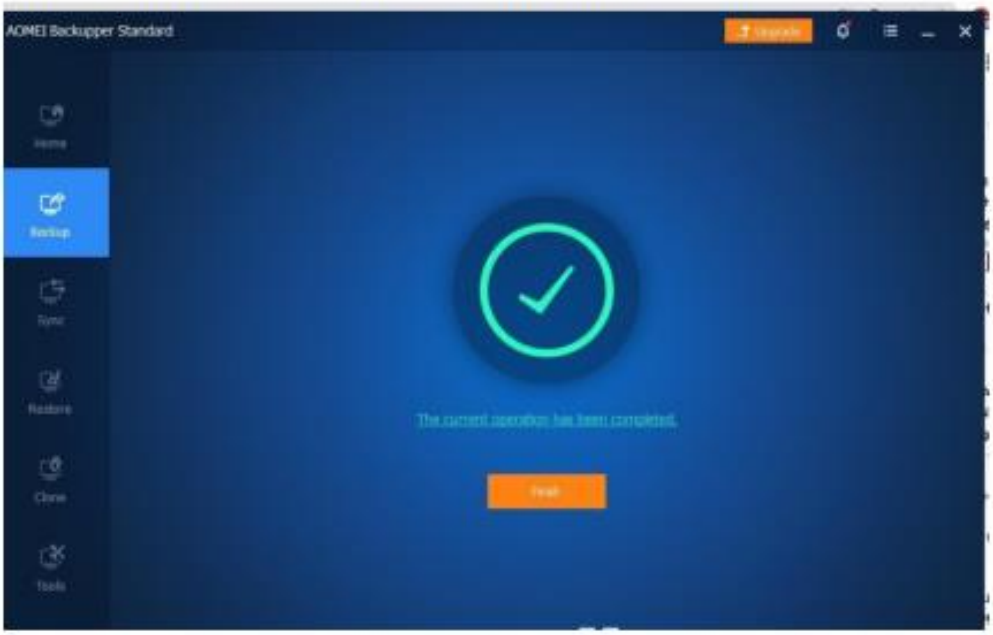
5. Pilih folder yang ingin di backup

6. Kemudian pilih lokasi backupnya akan di simpan

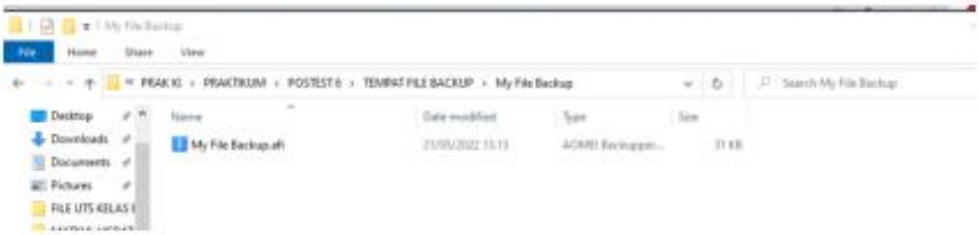
7. Jika sudah klik start backup

8. Tunggu prosesnya hingga selesai

9. Jika sudah terbackup akan muncul gambar seperti berikut

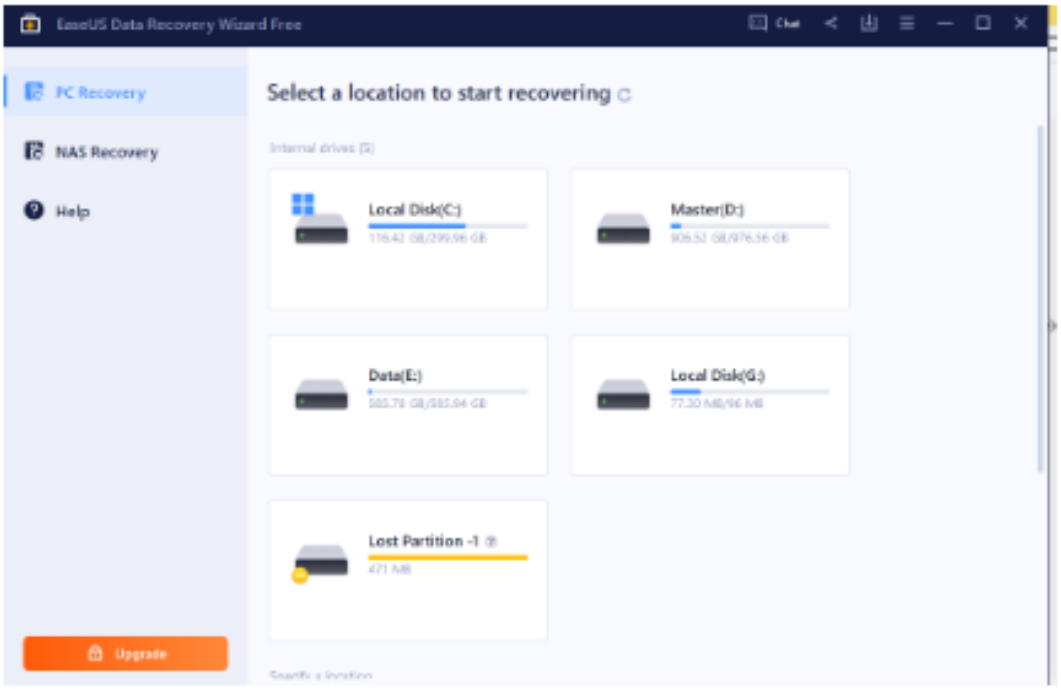


10. Kalau kita cek di lokasi penyimpanan hasil backupnya akan menghasilkan sebuah file dengna ekstensi .afi

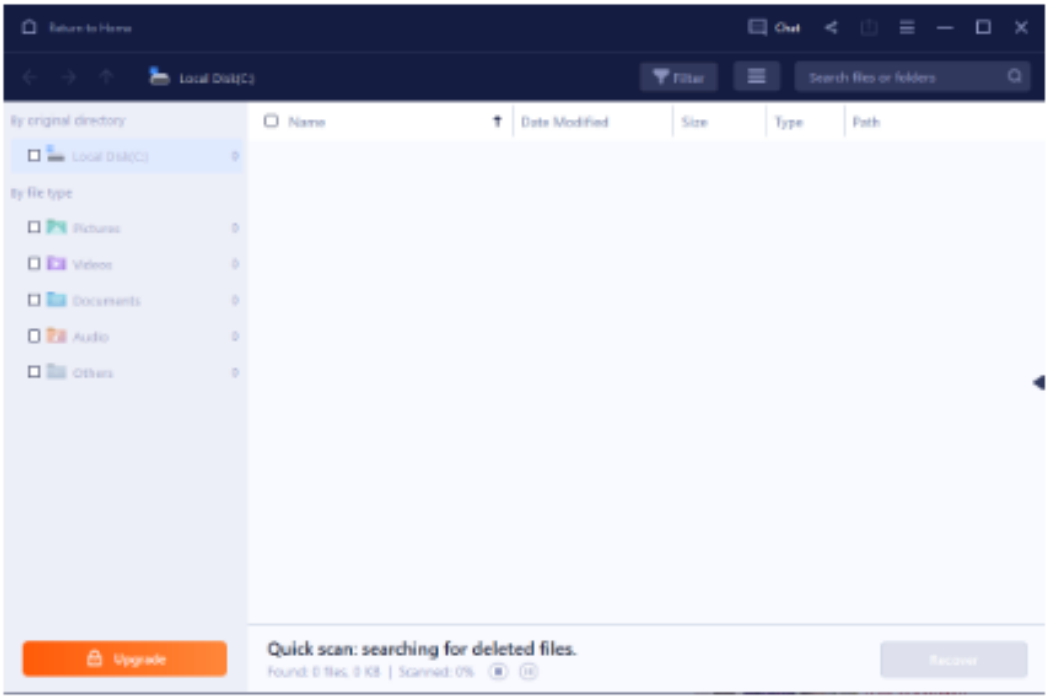


Recovery Data

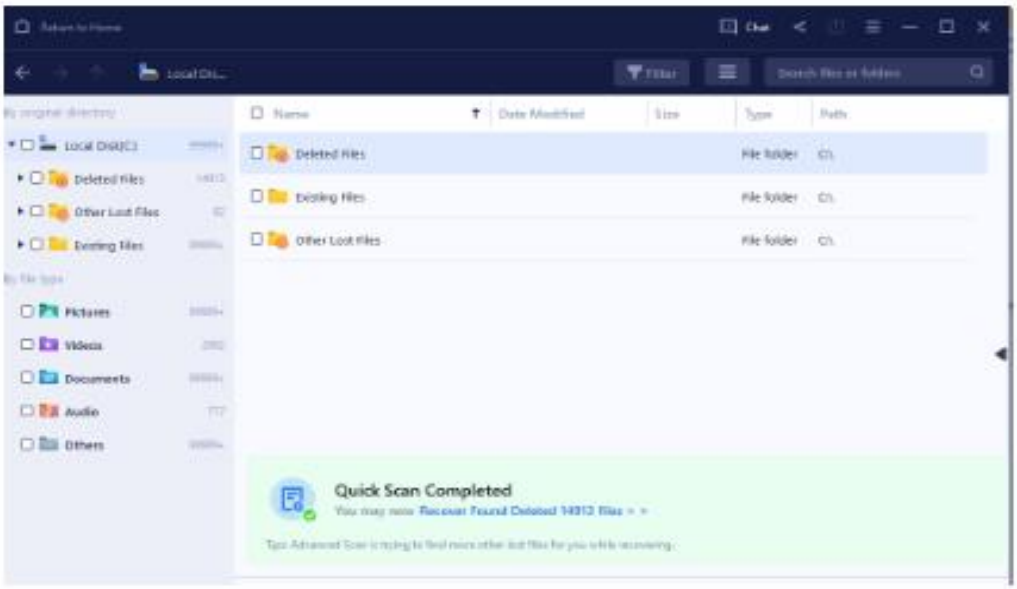
1. Buka aplikasi EaseUS Data Recovery Wizard



2. Scan lokasi file yang terhapus, dalam kasus ini file yang terhapus ada didrive C, dan tunggu hingga proses scanningnya selesai

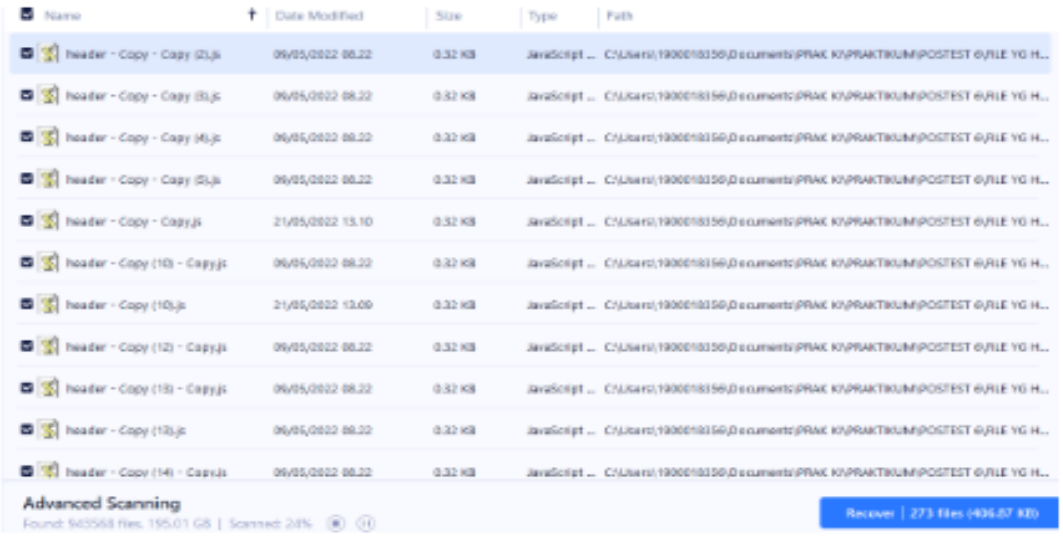


3. Jika sudah selesai akan muncul seperti ini

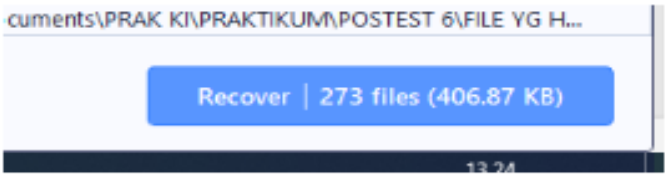


4. Lankah selanjutnya silahkan pilih deleted files, dan selanjutnya arahkan ke lokasi file yang hilang. Dalam kasus ini file yang hilang terletak di ***Users>1900018356>Documents>PRAK KI>RPRAKTIKUM>POSTEST 6>FILE YANG HARUS DI BACKUP***

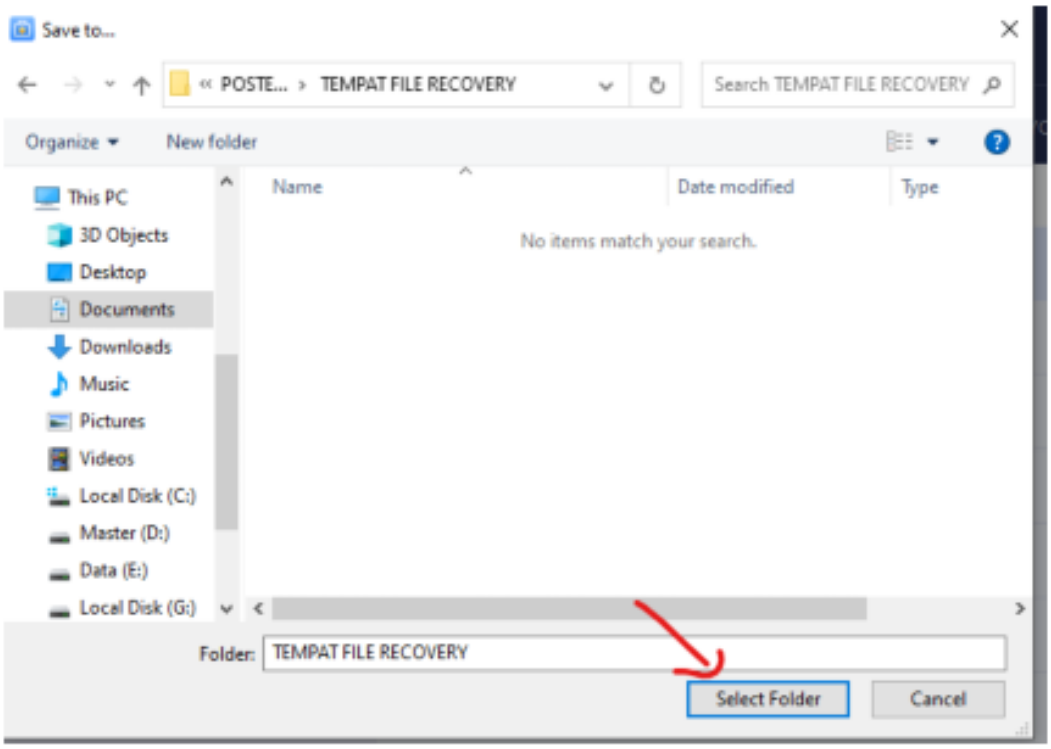
5. Setelah itu select semua file yang ingin di recovery



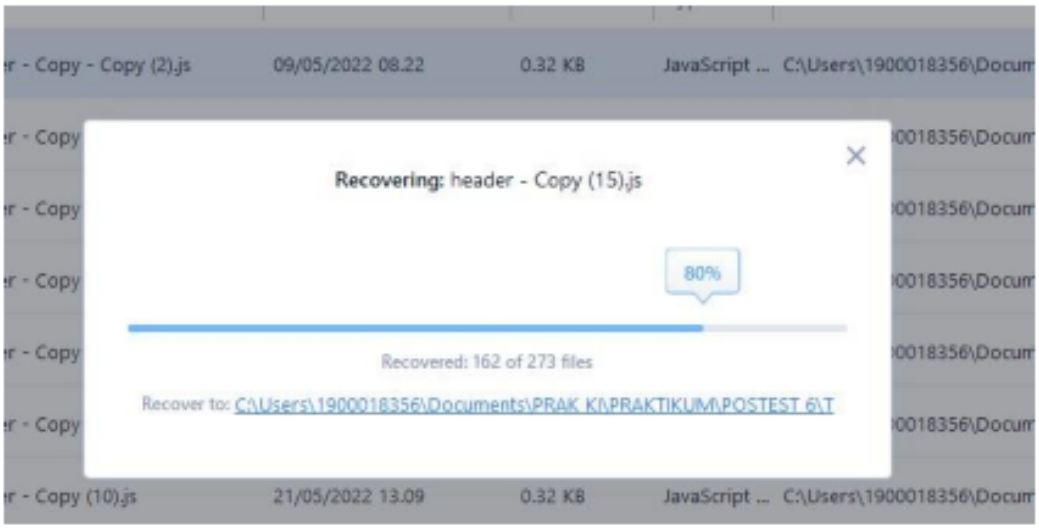
6. Dan klik tombol recover



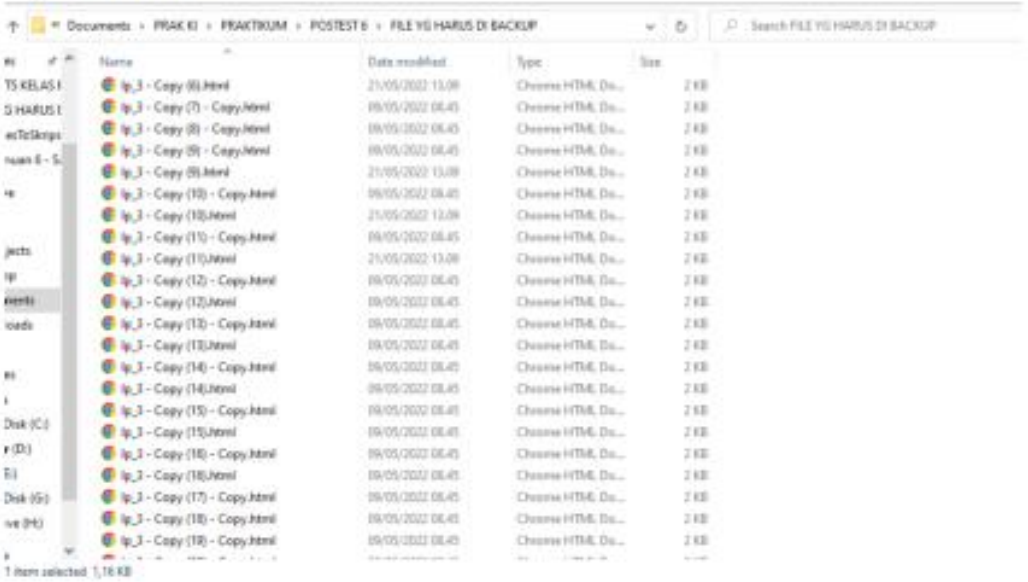
7. Kemudian taruh hasil recovery ke folder yang kita inginkan dan klik tombol select folder



8. Tunggu hingga prosesnya selesai



9. Jika sudah nanti akan diarahkan langsung ke folder yang sudah kita pilih, seperti berikut:



6.7. POST TEST

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

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-03	Lakukanlah Backup data dengan AOMEI Standart Backuper, lalu lakukanlah Recovery data yang dengan EaseUS Data Wizard dan Quick Recovery Tools dan dokumentasikan langkahnya dengan cara membuat tutorialnya.	100

6.8. HASIL CAPAIAN PRAKTIKUM

Diisi oleh asisten setelah semua assessment dinilai.

No	Bentuk Assessment	CPL	CPMK	Bobot	Skor (0-100)	Nilai Akhir (Bobot x Skor)
1.	Pre-Test	CPL-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: HACKING WEBSERVERS

Pertemuan ke : 7

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

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

Pemenuhan CPL dan CPMK

CPL-07	Mampu memilih, membuat dan menerapakan teknik, sumber daya, penggunaan perangkat teknik modern dan implementasi teknologi informasi untuk memecahkan masalah
CPMK-03	Mahasiswa mampu melakukan penetration tester dan memberikan rekomendasi resiko terhadap sistem keamanan informasi

7.1. TUJUAN DAN INDIKATOR CAPAIAN

Setelah mengikuti praktikum ini mahasiswa diharapkan: (sesuai dengan RPS)
1. Praktikan mampu mengidentifikasi serangan web server
2. Praktikan mampu menggunakan tools penetration tester

7.2. INDIKATOR KETERCAPAIAN PEMBELAJARAN

CPL-06	CPMK-03	Kemampuan mahasiswa dalam identifikasi serangan dan menggunakan tools yang tepat dalam melakukan pentest

7.3. TEORI PENDUKUNG

World Wide Web (www) merupakan bagian dari Internet yang paling populer, sehingga serangan paling banyak terjadi lewat port 80 atau yang dikenal sebagai web hacking, berupa deface situs, SQL injection, serta memanfaatkan kelemahan scripting maupun HTML form. Port 80, Web Server Port ini biasanya digunakan untuk web server.

Apa itu Web Hacking? Web hackin bukan hal baru lagi bagi jawara internet (hacker) baik aliran putih maupun aliran hitam (cracker). Apakah yang dimaksud dengan web hacking? Untuk mendapatkan definisi kedua kata tersebut (web dan hacking) Secara semantik, web didefinisikan menjadi Data yang direpresentasikan di world wide web. Adapun hacking didefinisikan menjadi Tindakan di luar otoritas atau tindakan mematahkan/membobol mekanisme keamanan sebuah sistem informasi atau sistem jaringan. Jadi, web hacking dapat diartikan Tindakan menerobos mekanisme keamanan dari suatu sistem yang direpresentasikan dalam world wide web.

Siapa yang Melakukan Web Hacking? Menerobos mekanisme keamanan suatu jaringan, bukanlah tindakan yang gampang untuk dilakukan. Jadi, siapakah pelaku web hacking tersebut? Seiring perkembangan internet yang benar-benar pesat dan diiringi perkembangan security dan underground, membuat siapa saja dapat menjadi pelaku. Tidak ada keharusan bahwa pelaku web hacking adalah orang yang pintar komputer dan internet, atau lain sebagainya.

Mengapa Melakukan Web Hacking? Jika semua bisa menjadi pelaku web hacking, tentu Ada alasan jika sampai melakukannya dan pertanyaan adalah Mengapa? Ada banyak alasan orang melakukan web hacking, diantaranya adalah: - Wanna Be A Hacker (ingin menjadi seorang hacker). - Mendapatkan popularitas. - Ingin mendapat pujian. Alasan-alasan tersebut di atas cukup bisa dicerna logika. Kapan dan Dimana? Internet merebak harum di Indonesia, bisa dikatakan mulai pada hitungan tahun 90-an. Internet yang sebelumnya merupakan sebagai hal yang mustahil untuk dirasakan oleh rakyat kelas bawah, semakin terjangkau dengan laris manisnya bermunculan warnet (warung

internet). Ada ujaran yang mengatakan Kejahatan ada karena ada kesempatan. Ujaran tersebut mungkin belum dapat ditujukan kepada pelaku web hacking. Dengan banyaknya kehadiran warnet bahkan ada yang buka 24 jam, membuat web hacking dapat dilakukan kapan saja dan dimana saja, tanpa harus menunggu waktu.

Bagaimana Web Hacking Dilakukan? Bagaimana seseorang melakukan web hacking? Internet sudah hampir menjangkau segala sisi kehidupan yang ada di dunia ini. Informasi mengenai web hacking dapat di temukan dengan berselancar ke Google. Google, search engine yang terkenal menjawab pertanyaan Bagaimana. Dengan memasukkan kata (keyword) pada baris isian pencarian maka akan dibawa ke tempat-tempat yang berhubungan dengan web hacking. Jenis serangan yang mungkin terjadi pada web;

1. Pembajakan Password FTP Di pertengahan 2009, maraknya satu bentuk pembajakan password FTP yang disebut juga serangan “gumblar” atau “martuz” , mempatenkan model pencurian ini menjadi salah satu cara yang paling sering digunakan untuk melakukan hacking. Cara kerja gumblar atau martuz adalah memodifikasi hasil pencarian Google sehingga setiap klik pada link yang tampil di hasil pencarian akan diredirectkan ke situs penyedia badware. Serangan ini mengambil keuntungan dari sebuah fakta bahwa ada banyak PC yang miskin perlindungan di dunia. Dan personal komputer tersebut nahasnya adalah milik webmaster yang informasi login websitenya disimpan di personal komputer mereka. Karena itulah, lengkapi personal computer dengan perlindungan antivirus yang memadai untuk pencegahan infeksi gumblar atau martuz di situs tertentu. Dan jangan sekali-kali membookmark informasi login.
2. Serangan Remote File Inclusion (RFI) Sebelum kemunculan gumblar atau martuz, serangan RFI adalah satu bentuk ancaman terbesar. Prinsip kerja serangan RFI adalah menipu sebuah website yang telah berjalan untuk mengcopy kode dari website eksternal. Kode yang dicopy menyusup ke dalam script yang dieksekusi, dan menjadi bagian di dalamnya. Sehingga, setiap script tersebut dieksekusi kembali, sebaris kode tersebut juga ikut dieksekusi. Sebaris kode tersebut fungsinya adalah untuk mendownload badware ke komputer pengakses. Adapun indikasi serangan RFI adalah di akses log website tertentu dan akan tampil koding.
3. Serangan Local File Inclusion (LFI) Serangan LFI hampir sama seperti RFI, bedanya mereka mencoba untuk menipu sebuah halaman web agar menampilkan konten dari file sistem server yang penting, yang seharusnya restricted dan tidak boleh diakses. Indikasi serangan LFI adalah di akses log website tertentu akan tampil koding seperti ini: Cara menanggulangi serangan LFI adalah dengan melatih kemampuan koding dan memperdalam pengetahuan tentang pembatasan htaccess.
4. Serangan Injeksi SQL Pada dasarnya serangan ini sama dengan RFI dan LFI, bedanya obyek yang diserang adalah halaman web yang menggunakan Structured Query Language (SQL) untuk melakukan query dan memanipulasi database, semisal MySQL. Cara kerjanya adalah dengan menanamkan komando SQL di sebaris koding untuk menipu sistem agar membocorkan informasi rahasia. Berikut salah satu contoh dari serangan injeksi SQL yang nantinya akan muncul pada akses log website.
5. Password Attack Di samping gumblar, ada cara lain bagi penyerang untuk mencuri password situs yaitu dengan berulang-ulang mencoba untuk login dengan kombinasi user ID dan password yang berbeda, berharap untuk menebak.

7.4. HARDWARE DAN SOFTWARE

Alat dan bahan yang digunakan dalam praktikum ini yaitu:

1. Komputer
2. Tools Id Serve

7.5. PRE-TEST

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

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-06	CPMK-03	1. Apa itu web server hacking? 2. Bagaimana webserver hacking dilakukan?	50

2.	CPL-06	CPMK-03	3. Jenis serangan apa saja yang anda ketahui? dan apa dampaknya? ceritakan dengan singkat!	50

7.6. LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-06	CPMK-03	Selesaikan langkah praktikum berikut!	Screen shot Hasil praktikum	100

1. Download aplikasi id serve

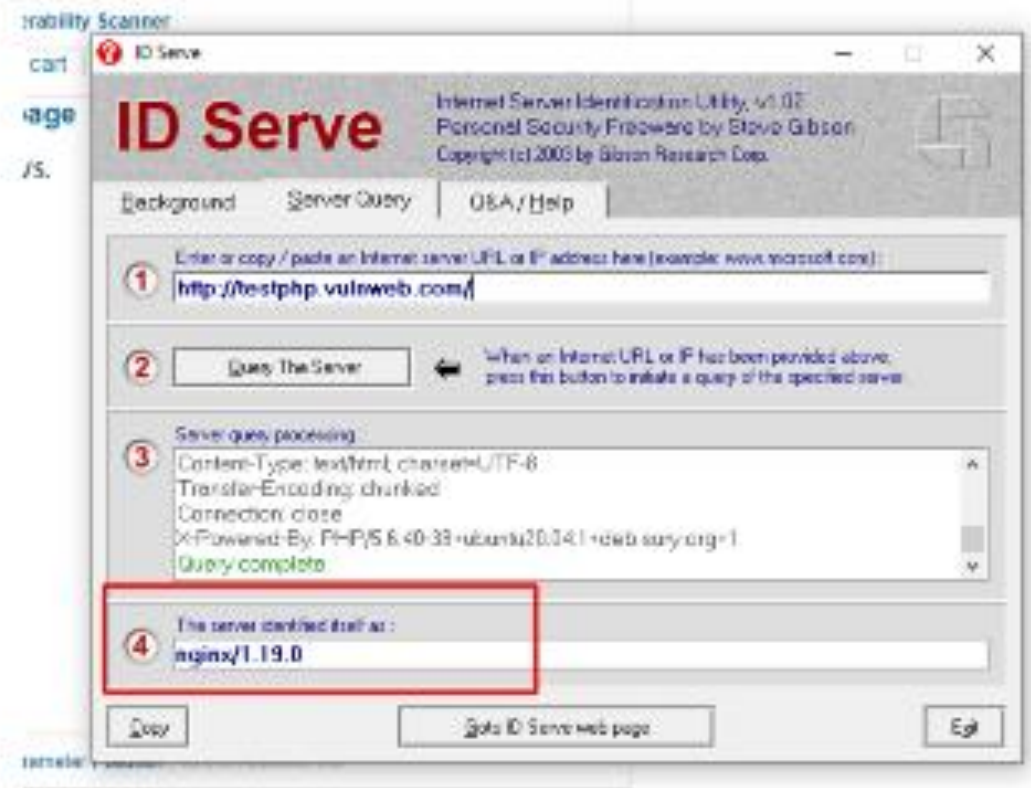
2. Buka aplikasi id serve

3. Pilih tab server query

4. Masukan url yang ingin diidentifikasi

5. Klik tombol query server

6. Dan server yang dipakai akan tampil di kolom keempat



7.7. POST TEST

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

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-06	CPMK-03	1. Lakukan salah satu S1 yang ada di video materi. Kemudian silakan buat langkah dan jelaskan step by step dari langkah S1 yang kalian pilih!	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-06	CPMK-03	20%		
2.	Praktik	CPL-06	CPMK-03	30%		
3.	Post-Test	CPL-06	CPMK-03	50%		
					Total Nilai	

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

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

PRAKTIKUM 8: HACKING WEB APPLICATIONS

Pertemuan ke : 8

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

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

Pemenuhan CPL dan CPMK

CPL-07	Mampu memilih, membuat dan menerapakan teknik, sumber daya, penggunaan perangkat teknik modern dan implementasi teknologi informasi untuk memecahkan masalah
CPMK-03	Mahasiswa mampu melakukan penetration tester dan memberikan rekomendasi resiko terhadap sistem keamanan informasi

8.1. TUJUAN DAN INDIKATOR CAPAIAN

Setelah mengikuti praktikum ini mahasiswa diharapkan;
1. Praktikan mampu mengidentifikasi jenis serangan web aplikasi
2. Praktikan dapat membuat menganalisis jenis serangannya

8.2. INDIKATOR KETERCAPAIAN PEMBELAJARAN

CPL-07	CPMK-03	Kemampuan mahasiswa dalam mengidentifikasi dan menganalisa jenis serangan pada aplikasi web

8.3. TEORI PENDUKUNG

Web Application Security, Dengan seiring semakin maraknya bermunculan Startup-startup berbasis digital, mereka hadir dengan bisnis yang membutuhkan implementasi teknologi handal dalam waktu yang singkat. Teknologi yang mendukung kemampuan akses dari lintas geografis dan tanpa ada batasan waktu, kemampuan mengelola data dalam jumlah yang sangat-sangat besar untuk kemudian diproses menjadi informasi dan knowledge. Dengan situasi ini sering kali bicara mengenai performance, scalability, cloud, big data, microservices dan kosakata lainnya didunia IT. Perekrutan personil, adaptasi teknologi, research and awareness, semua fokus pada hal-hal yang telah disebutkan diatas. Walaupun betapa pentingnya sebuah keamanan digital, tetapi tidak banyak startup yang menempatkan perhatian khusus pada keamanan digital terutama di layer aplikasi. Entah karena keterbatasan pengetahuan terhadap ancaman dan jenis pengamanannya, atau dikarenakan masih lebih memprioritaskan kebutuhan bisnis.

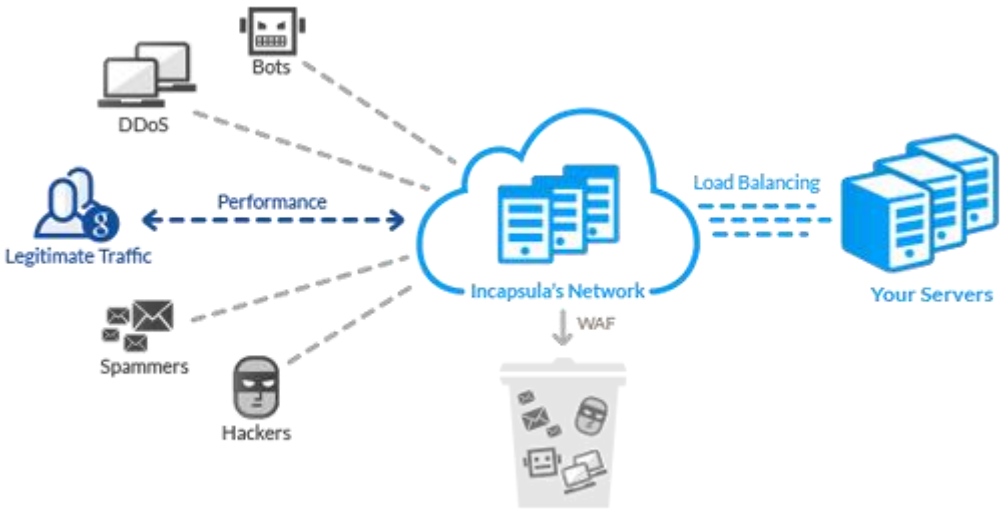
Ancaman Web Application, bicara ancaman-ancaman di level Infrastruktur, di bagian network, perangkat, system operasi, service dan server. Dari ancaman-ancaman tersebut pada akhirnya diciptakan perangkat-perangkat yang khusus dirancang sebagai bentuk pengamanan terhadap infrastruktur IT. Perangkat-perangkat seperti Firewall, IDS, IPS, IPtables, bisa dijadikan pilihan untuk mencegah, mengidentifikasikan, bahkan sampai menangkal serangan hacker. Tetapi seiring dengan perkembangan teknologi informasi dan komunikasi yang tak pernah berhenti, telah menjadikan dunia web sebagai platform di jaringan internet yang sangat populer. Dengan semakin populernya dunia web ini maka secara tidak langsung akan semakin besar pula resiko dan ancaman keamanannya. Para Hacker mulai mencari celah keamanan dan membuat tools untuk memudahkan apabila mereka ingin melakukan aksinya kembali. Tetapi pada praktiknya tools-tools tersebut dapat dengan mudah di

download di Internet, dibuat agar mudah digunakan bahkan untuk seorang yang awam di dunia hacking. Sehingga menjadikan resiko digital semakin tinggi.

Di level Infrastruktur mengenal serangan-serangan seperti DOS, DDOS, DNS poisoning, Worm dan Trojan Horse. Sedangkan serangan-serangan di level aplikasi ini seperti SQL Injection, File Injection dan XSS. Metode hacking tersebut akan mencari kelemahan pada sistem walaupun secara logic bisnis dapat diterima.

Web Application Security Seorang developer dapat meminimalisir celah keamanan aplikasi dengan cara memaksimalkan tugas-tugas QA. Memastikan aplikasi lolos testing di unit test, functional test,UAT, Blackbox dan Whitebox testing, sehingga dapat mengurangi kemungkinan-kemungkinan dari input dan behaviour yang diluar skenario. Tetapi metode dan teknik hacker semakin hari semakin canggih. Dibutuhkan layer pertahanan tambahan untuk menangkal serangan di level ini. Dan salah satu cara untuk meng-implementasi web application security adalah dengan menggunakan Web Application Firewall atau disingkat menjadi WAF. Seperti halnya dengan firewall yang sudah dikenal selama ini, WAF memiliki bentuk hardware dan perangkat lunak, dan juga dalam bentuk layanan Cloud. Untuk yang hardware biasanya fitur ini sudah ter-bundling dengan perangkat Network Firewall. Ada yang bisa langsung digunakan, ada juga yang harus membayar subscription atau sebagai module tambahan. Tidak hanya di perangkat keras, WAF tersedia juga sebagai aplikasi yang dapat di install di sistem. Dengan beberapa settingan dan sudah bisa mendapatkan proteksi dari WAF ini. List beberapa aplikasi WAF yang populer bisa dilihat disini. Yang biasa diketemui di beberapa infrastruktur, biasanya mereka menggunakan mod_security yang bisa dipasang di Nginx dan Apache, atau Naxsi (Nginx Anti XSS and SQL Injection). Dan hadir pula WAF berbasis cloud seperti Akamai, Cloudflare dan Amazon WAF. Akamai dan Cloudflare merupakan penyedia layanan khusus CDN, dan Amazon mengkhususkan pada layanan Cloud. Disini terlihat bahwa WAF melengkapi layanan cloud yang diberikan oleh mereka.

Amazon AWS – WAF Serupa dengan firewall jenis proteksi network, WAF bekerja berdasarkan pola-pola transaksi web yang dianggap mencurigakan. Dari pola-pola tersebut dijadikan aturan-aturan yang menjadi dasar penilaian (scoring) seberapa besar resiko atau ancaman yang sedang terjadi.



Gambar 8.1 WAF Skema

source: https://www.cwp.govt.nz/about/selecting-the-right-instance-for-your-website/

Aturan-aturan tersebut terdiri dari aturan SQL injection, aturan File injection, XSS, Directory Traversal dan lainnya. Setiap pola yang terdeteksi melanggar aturan tersebut akan diberikan score atau nilai. Dari nilai tersebut lah WAF akan menilai tingkat ancamanyang selanjutnya akan diambil tindakan yang diperlukan. Apakah akan men-drop transaksi tersebut, atau mengirim peringatan ke sistem notifikasi internal IT.

Contoh aturan untuk SQL Injection seperti mengamati pola-pola yang mencurigakan pada request seperti penggunaan kata-kata DATABASE**,** DROP**,** TABLE**,** UNION**,** CONCAT, **/***, ***/** atau encoding yang menggunakan hex. Untuk file injection memiliki aturan-aturan seperti mengawasi penggunaan file extension dan mime type yang tidak diharapkan oleh aplikasi. Dan untuk aturan-

aturan XSS contohnya seperti mencurigai penggunaan request yang terdapat karakter **<**, **>**, **:**, **~**, **;** dan lainnya. Aturan-aturan yang terdapat di WAF sebagian besar dari referensi Open Web Application Security Project (OWASP). Dari web tersebut bisa lihat bagaimana teknik dan metode yang digunakan untuk hacking aplikasi web. Dengan mempelajari cara kerjanya, akan memudahkan pada saat implementasi WAF di internal IT. Karena akan berhubungan dalam menentukan aturan-aturan yang akan digunakan, skoring, dan bagaimana desain dan flow aplikasi web yang dimiliki.

Kemudian menjadi tanggung jawab siapakah keamanan di level aplikasi web ini? apakah masih dalam ranah tim Infrastruktur yang saat ini memegang wewenang di Firewall Infrastruktur IT? atau tanggung jawab seorang developer yang notabene pembuat aplikasi itu sendiri?, Dengan semakin tingginya resiko dan ancaman pada aplikasi web maka kesadaran akan bahaya ini sudah seharusnya dirubah menjadi sebuah aksi. Siapapun yang akan memangku tanggung jawab pada web application security ini pada akhirnya akan membutuhkan kordinasi antara tim developer dan tim infrastruktur. Gunakanlah waktu untuk proses "learning" dengan baik. Pastikan pada saat implementasi WAF tidak akan mengganggu user experience. Jangan sampai WAF salah mengidentifikasikan antara rekues 'TABLE FROM ITALY' dengan 'DROP TABLE'. Yang perlu digaris bawahi disini adalah, ancaman pada aplikasi web sedang menjadi trend di dunia hacking. Tempatkanlah area IT ke dalam zone aman dari semua resiko tersebut.

8.4. HARDWARE DAN SOFTWARE

Alat dan bahan yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. Tools OWASP
3. Tools Acunetix

8.5. PRE-TEST

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

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-03	1. Apa itu hacking web application, bagaimana hacking web application terjadi? dan apa tujuannya?	50
2.	CPL-07	CPMK-03	2. Apa saja perbedaan metode untuk hacking web application?	50

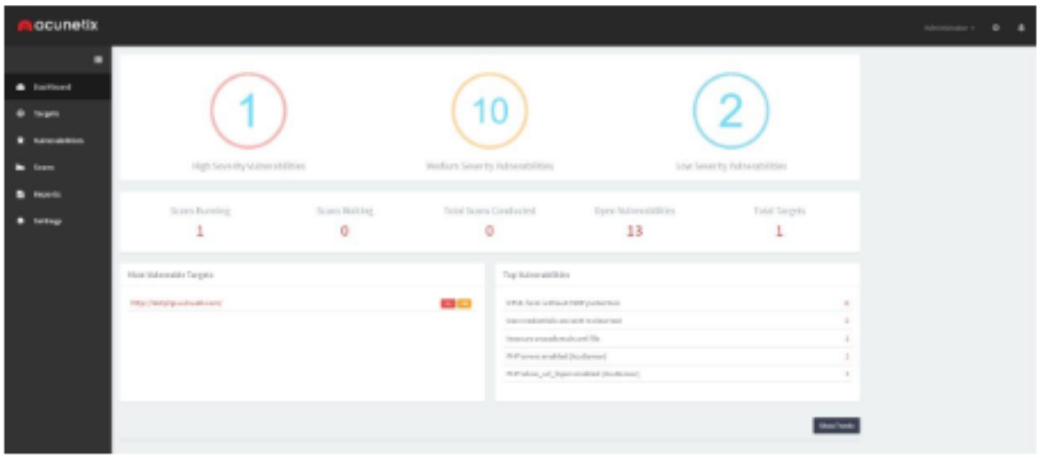
8.6. LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

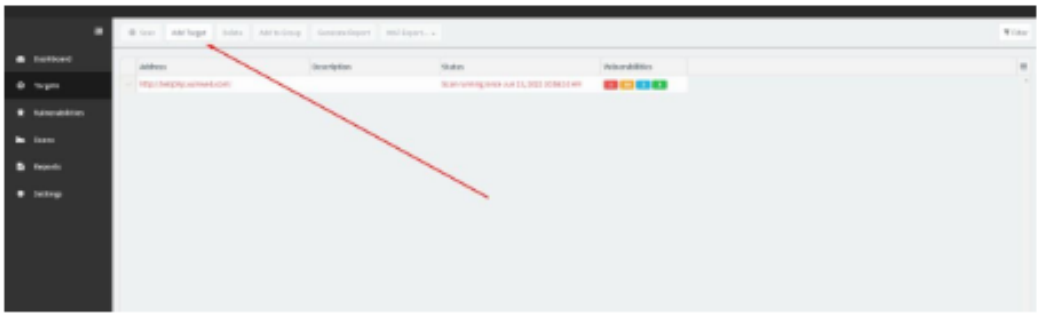
No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-07	CPMK-03	Selesaikan langkah praktikum berikut!	Screen shot Hasil praktikum	100

POSTEST
METODE ACUNETIX

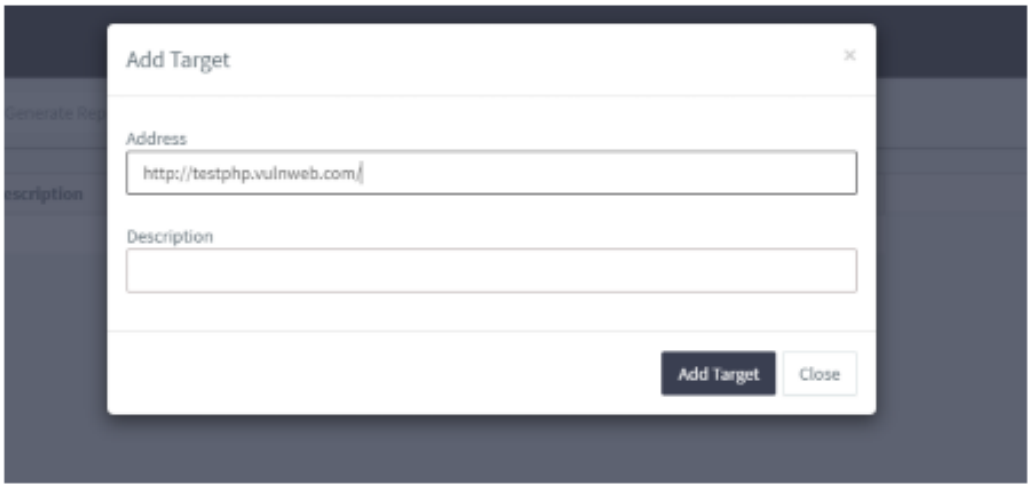
1. Buka aplikasi Acunetix



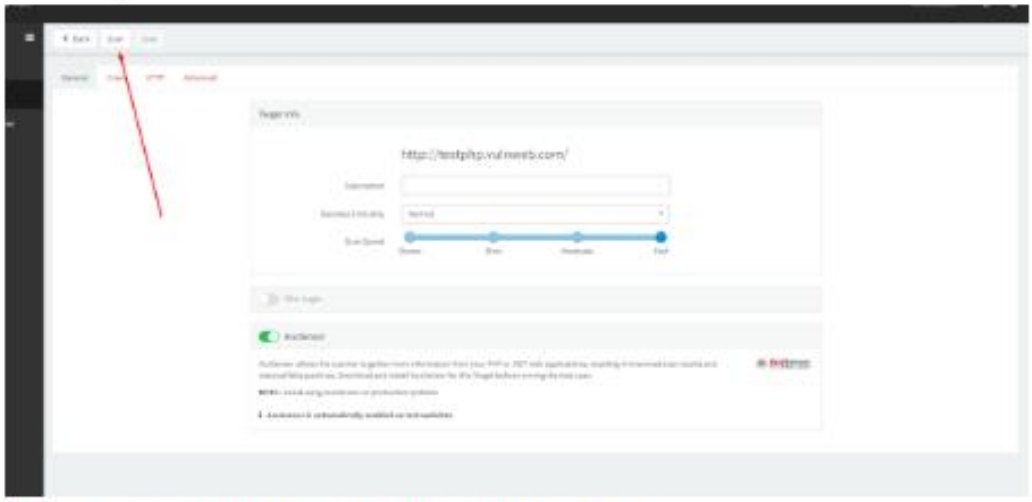
2. Klik tombol target, dan pilih add target



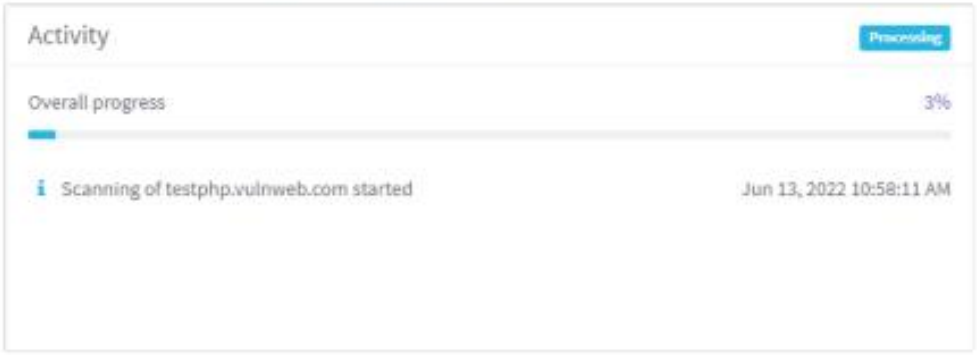
3. Masukan URL website yang ingin kita scan, lalu add target



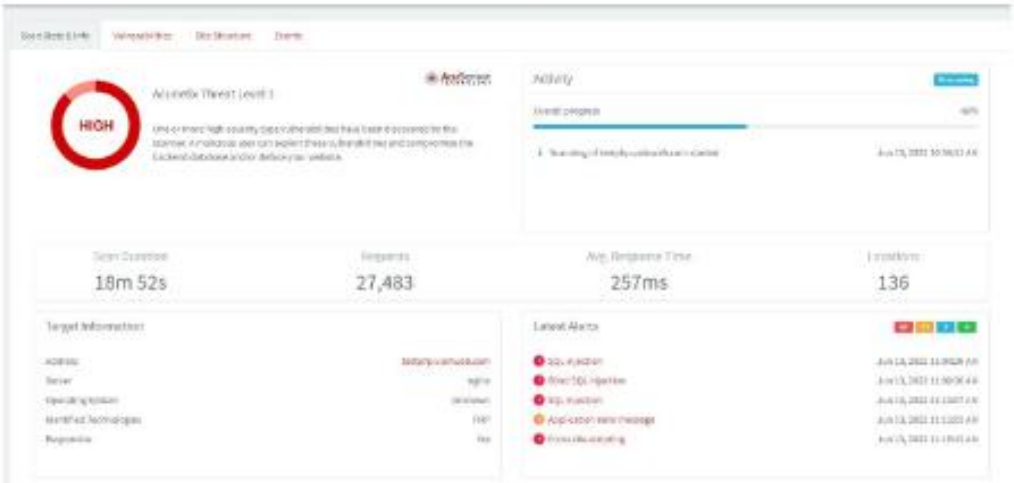
4. Kemudian jika sudah klik tombol scan



5. Dan proses scanning akan dimulai, tunggu hingga selesai

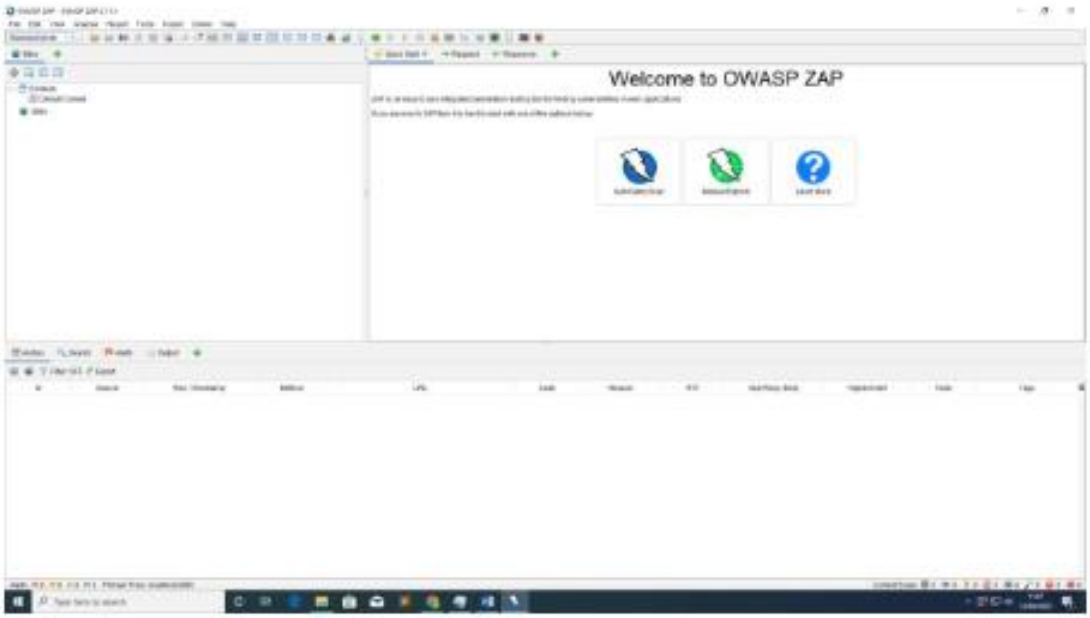


6. Hasil dari proses scanning adalah sebagai berikut:

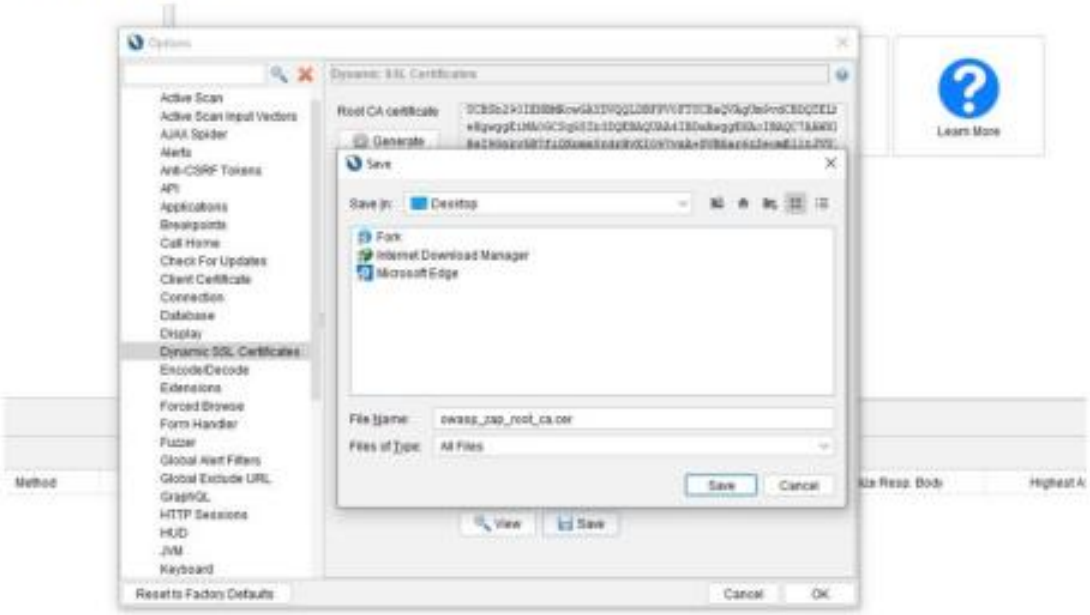


METODE OWASP ZAP

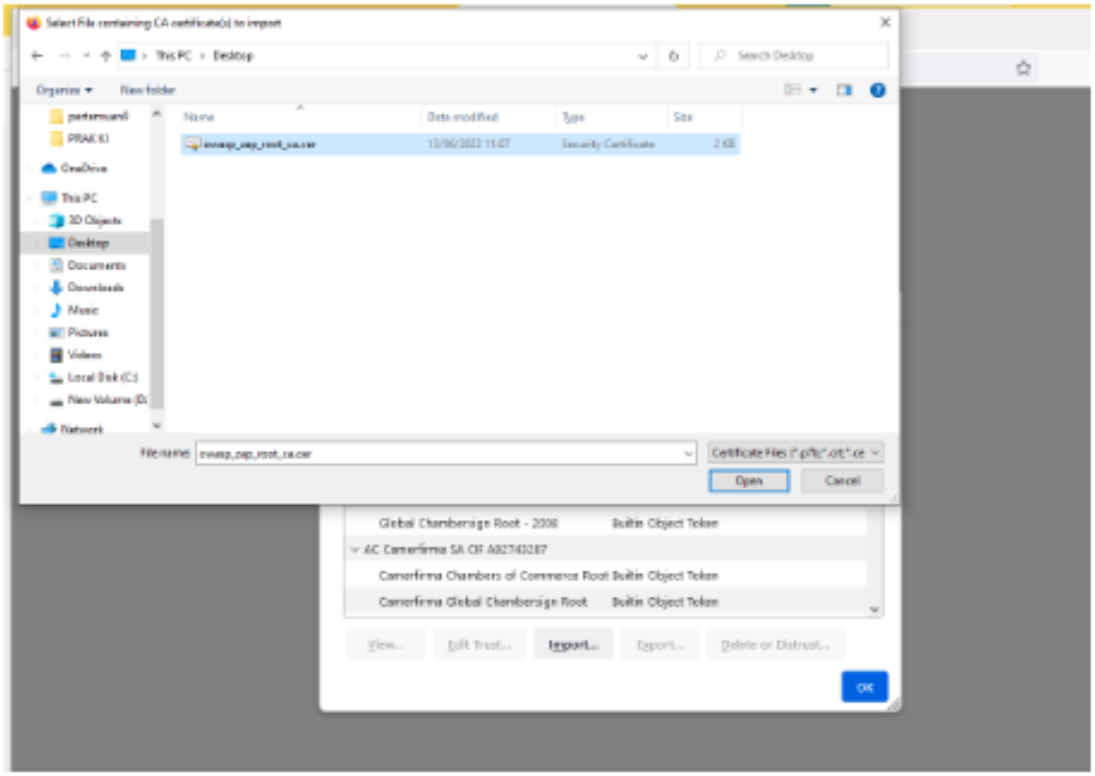
1. Buka aplikasi OWASP ZAP



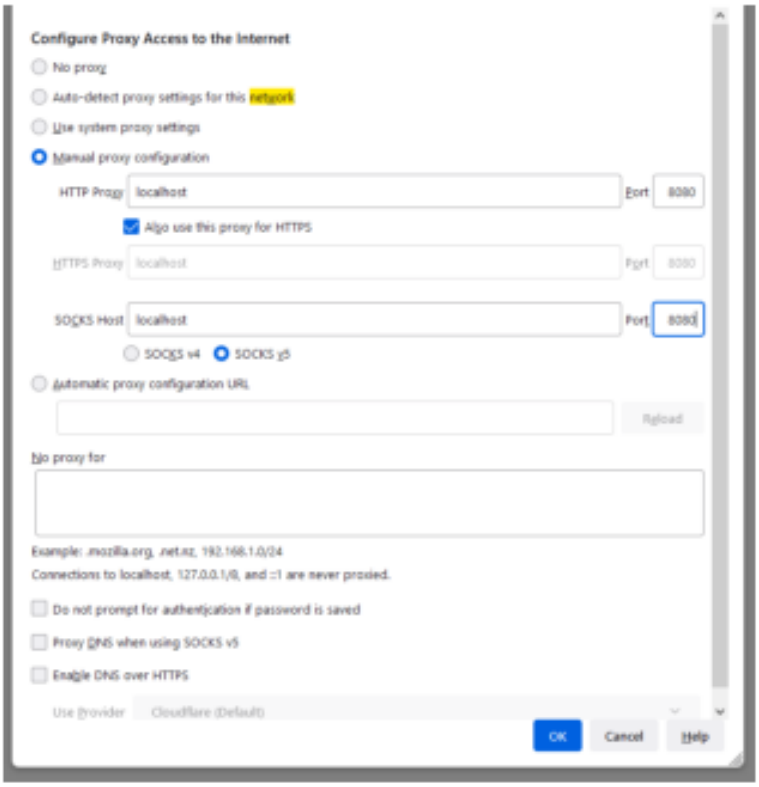
2. Generate Certificate



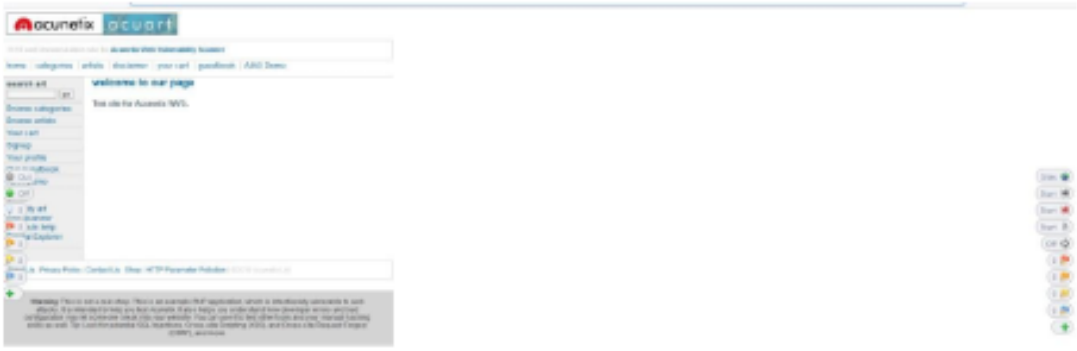
3. Import certificate



4. Setting Proxy



5. Jika sudah saatnya buka aplikasi yang ingin di test vlun-nya melalui mozila



6. Hasil dari scanning terkait websitenya bisa cek di menu di bawah sebelah kiri

8.7. POST TEST

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

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-03	Carilah kelemahan website dengan kedua metode yang digunakan (Acunetix dan OWASP ZAP), disertai dengan langkah-langkah! Dan jelaskan perbedaan kedua metode tersebut!	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-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 9: SYSTEM HACKING

Pertemuan ke : 9

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

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

Pemenuhan CPL dan CPMK

CPL-07	Mampu memilih, membuat dan menerapakan teknik, sumber daya, penggunaan perangkat teknik modern dan implementasi teknologi informasi untuk memecahkan masalah
CPMK-03	Mahasiswa mampu melakukan penetration tester dan memberikan rekomendasi resiko terhadap sistem keamanan informasi

9.1. TUJUAN DAN INDIKATOR CAPAIAN

Setelah mengikuti praktikum ini mahasiswa diharapkan:
1. Praktikan mampu mengidentifikasi serangan system hacking
2. Praktikan dapat membuat menganalisis jenis serangannya

9.2. INDIKATOR KETERCAPAIAN PEMBELAJARAN

CPL-07	CPMK-03	Kemampuan mahasiswa dalam mengidentifikasi dan menganalisis serangan berupa system hacking

9.3. TEORI PENDUKUNG

Peretasan Sistem atau system hacking merupakan tujuan dari setiap aksi peretasan. Setiap peretas mengolah semua informasi yang didapat melalui teknik footprinting, scanning, dan enumerasi untuk dapat meretas target atau sistem. Dalam melakukan peretasan, peretas mengikuti beberapa tahapan seperti yang sudah disebut sebelum nya hingga akhir nya melakukan masuk kedalam sistem. Menurut CEH Hacking Methodology (CHM) ada 3 tahapan yang harus dilakukan:

1. Gaining Access
   Meliputi aktifitas pengumpulan informasi terhadap target untuk menemukan pola agar dapat melakukan cracking password. Beberapa teknik yang digunakan seperti brute-forcing, password guessing, dan social engineering dan menerobos hak akses untuk mendapat privileges setingkat level administrator.
2. Maintaining Access
   Setelah sukses mendapatkan akses pada target sistem, peretas akan melakukan maintain terhadap sistem, agar dapat melakukan tindakan illegal pada sistem seperti meng-eksekusi aplikasi illegal, mencuri data, dan men-tamper data pada system yang bersifat sensitive.
3. Clearing logs
   Karena peretas telah mendapatkan full aksess, maka peretas dapat melakukan penghapusan jejak, agar menjadi tidak terdeteksi. Hal yang dapat dilakukan seperti menghapus log yang terdapat pada sistem.

Setiap aksi peretasan, peretas atau hacker memiliki tujuan dibalik aksi nya. Beberap tujuan akhir dari tahap peretasan dapat dilihat pada diagram berikut:

a. Gaining Access, Pada tahapan hacking, pertama kali peretas akan mencoba mendapatkan akses ke target sistem dengan menggunakan information gathering dan celah yang terdapat pada sistem. Ketika peretas berhasil mendapatkan akses ke sistem, maka peretas dapat melakukan berbagai hal kesistem seperti mencuri data, mengimplementasikan aplikasi penyadap data yang terdapat pada jaringan dan menginfeksi sistem. Pada tahapan ini, peretas menggunakan beberapa teknik seperti password cracking dan social engineering untuk mendapatkan akses kesistem.
b. Escalating Privileges, Setelah mendapatkan akses ke sistem dengan menggunakan privileges low user, peretas akan mencoba meningkatkan hak akses mendekati administrator agar nantinya dapat men-cover aksi nya selama didalam sistem. Untuk mendapatkan hak askes administrator, hacker bisa menggunakan teknik exploit.
c. Executing Application, Ketika berhasil mendapat hak akses selevel administrator, maka peretas bisa meng-eksekusi aplikasi illegal. Aplikasi illegal tersebut seperti Trojans, Backdoors, Rootkits, dan keyloggers.
d. Hiding Files, Hacker bisa menggunakan Rootkits dan teknik steganography untuk menyembunyikan file yang telah terdapat pada sistem yang digunakan untuk keperluan peretas.
e. Covering Tracks, Terakhir, agar tidak terdeteksi, maka peretas harus dapat menghapus jejak dan bukti didalam sistem dengan menghapus log, mengubah log, dll.

9.4. HARDWARE DAN SOFTWARE

Alat dan bahan yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. Tools Wintrgen

9.5. PRE-TEST

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

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-03	1. Sebutkan tools untuk crack password!	50
2.	CPL-07	CPMK-03	2. Sebutkan tools untuk menyembunyikan files!	50

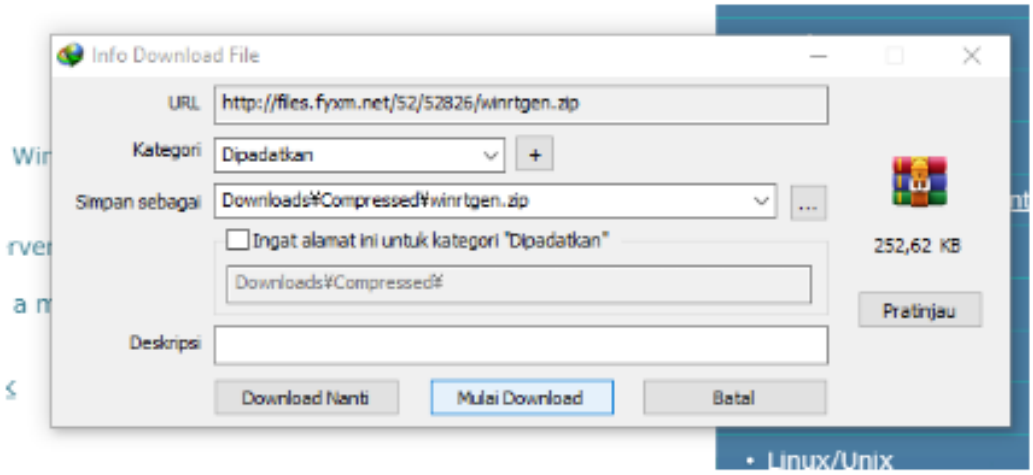
9.6. LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

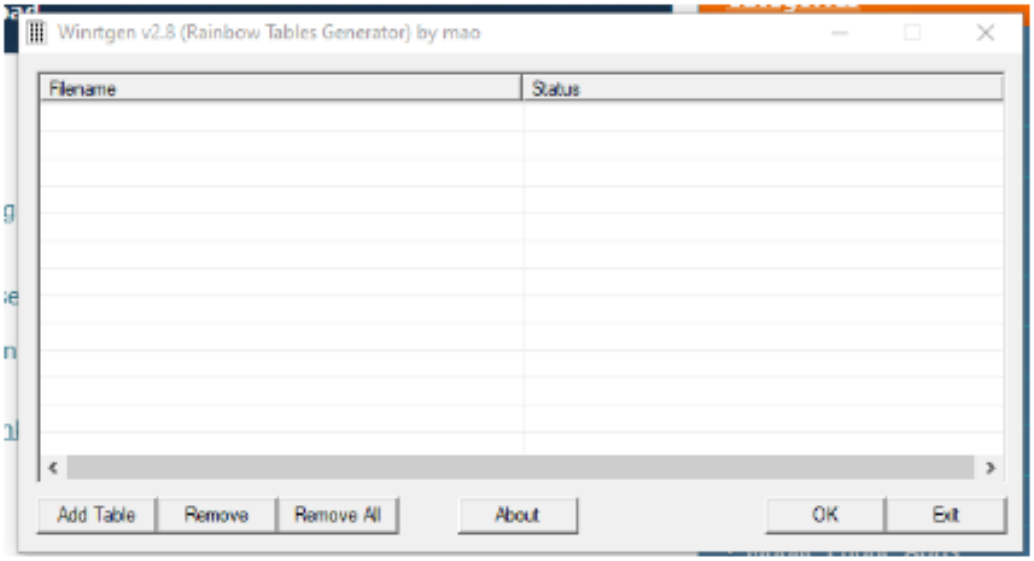
No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-07	CPMK-03	Selesaikan langkah praktikum berikut!	Screen Shot Hasil praktikum	100

Menggunakan Link Berikut: https://www.youtube.com/watch?v=IBi5OeHROPk

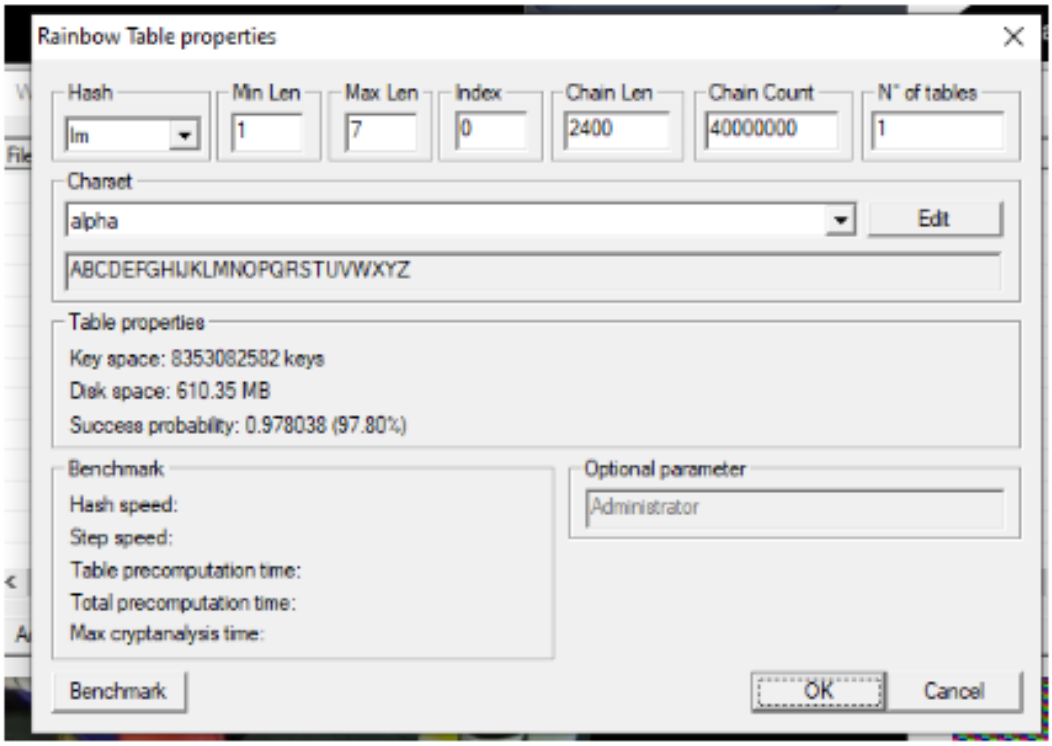
1. Download Software



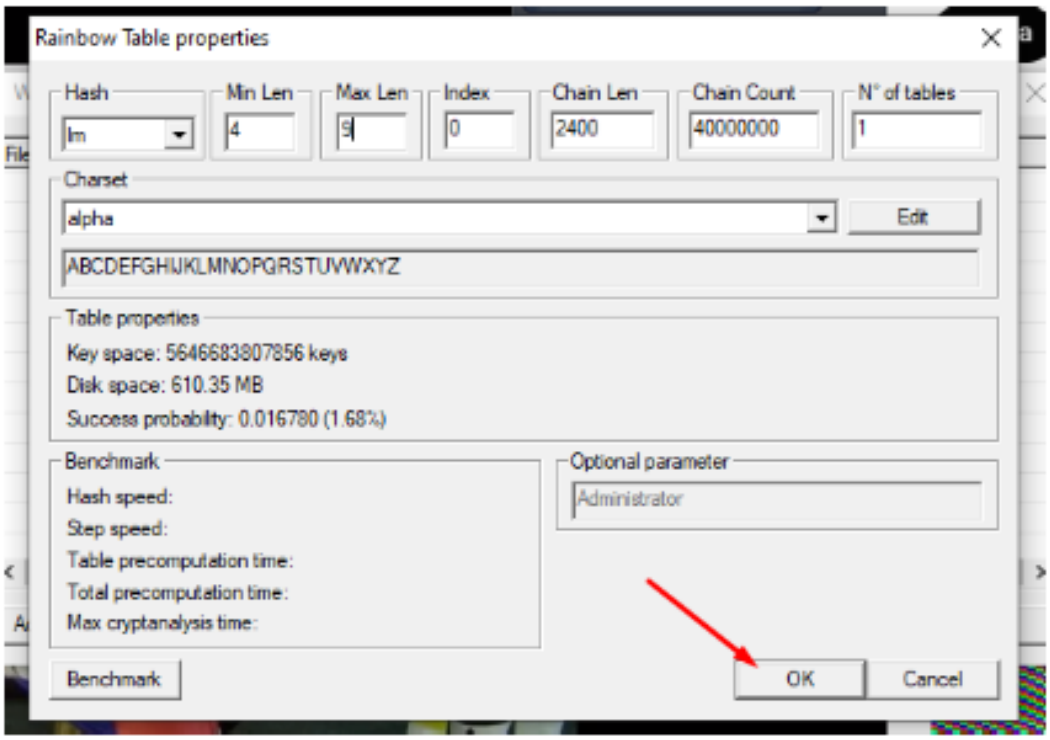
2. Jalankan Wintrgen



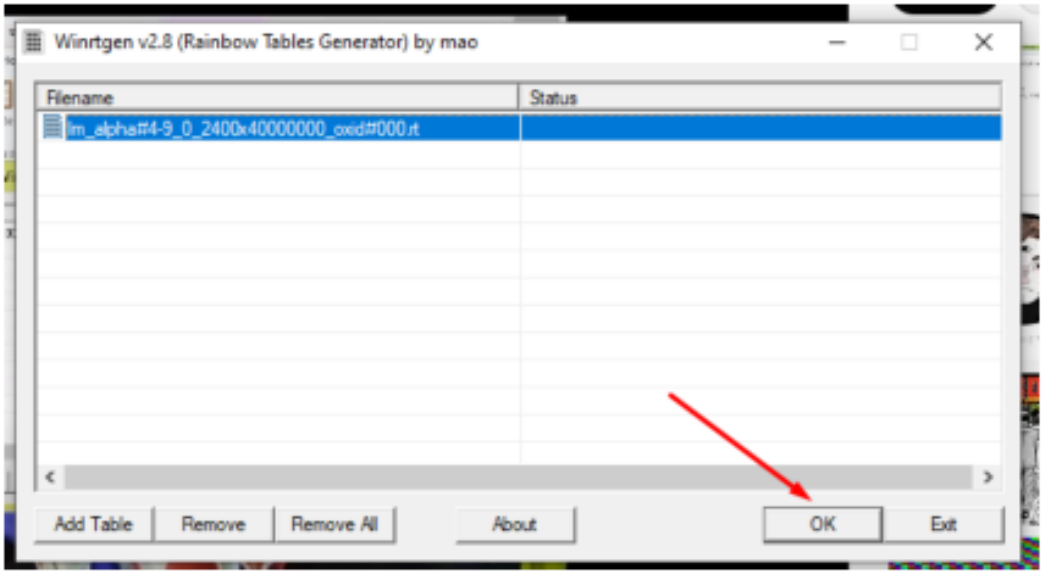
3. Klik Add Table



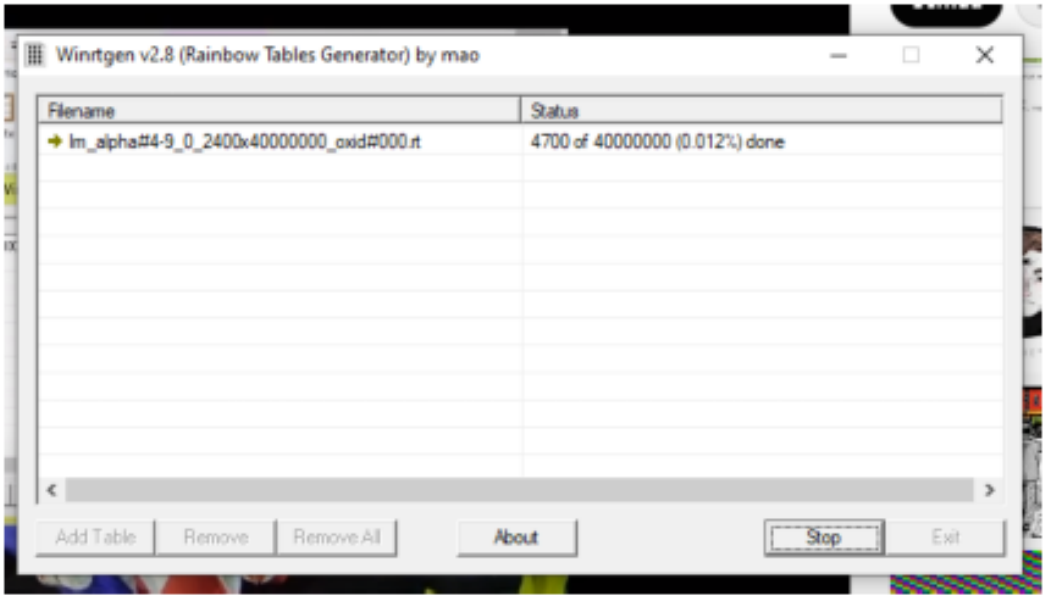
4. Setting kriteria table yang ingin dibuat, lalu oke



5. Klik table yang sudah dibuat, lalu oke



6. Tunggu proses selesai dan langkahnya selesai sampai disini



9.7. POST TEST

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

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-03	Pilih salah satu video pada materi yg ada kemudian implementasikan video tersebut, buatlah langkah-langkahnya dan beri penjelasan!	100

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-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 10: FOOTPRINTING AND RECONNAISSANCE

Pertemuan ke : 10

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

Total Skor 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	Mahasiswa mampu membuat penilaian tingkat keamanan dan kesiapan berdasarkan standarisasi ISO

10.1. TUJUAN DAN INDIKATOR CAPAIAN

Setelah mengikuti praktikum ini mahasiswa diharapkan: (sesuai dengan RPS)
1. Mampu mengimplementasikan footprinting & reconnaissance berupa pelacakan informasi pengenai pelakuperetasan
2. Mampu menganalisis keamanan sebuah sistem dan rekomendasi tingkat keamanan sistem

10.2. INDIKATOR KETERCAPAIAN PEMBELAJARAN

CPL-07	CPMK-04	Kemampuan mahasiswa dalam mengimplementasikan footprinting & reconnaissance selanjutnya menganalisis tingkat keamanannya

10.3. TEORI PENDUKUNG

Footprinting adalah langkah awal sebelum penyerang (*attacker*) melakukan penyerangan, yakni mengumpulkan informasi mengenai target, yang tujuannya adalah untuk merangkai apa yang ditemukan (*blueprint* dari suatu jaringan), sehingga ia mendapatkan gambaran yang jelas tentang sistem keamanan yang dimiliki target. Informasi yang ditampilkan dalam kegiatan ini, dapat berupa sejarah perusahaan, nama domain, VPN (*Virtual Private Network*) *point*, nomor telepon, nama orang-orang yang terkait di dalamnya, alamat email perusahaan, hubungan dengan perusahaan lain, lokasi perusahaan, topologi peta dan informasi penting lainnya. Fase footprinting adalah fase untuk menemukan blueprint dari jaringan keamanan suatu organisasi melalui pendekatan medotologis, artinya merangkai apa yang ditemukan sehingga mendapatkan gambaran yang jelas tentang sistem keamanan sasaran (apakah mereka menggunakan internet, ISP nya siapa, backbone nya, wireless SSID nya, metode pengamanan wirelessnya, Ada diChannel berapa, dimana lokasi nya, berapa mesin yang aktif, menemukan port yang terbuka, mendeteksi sistem operasi, network map dll). Hampir 90% waktu seorang attacker digunakan untuk menemukan profile dari sasaran, sisanya 10 % untuk meluncurkan serangan itu sendiri. *Footprinting* terdiri dari:

1. *Inner footprinting* adalah kegiatan mencari informasi mengenai target, dimana pencarian tersebut dilakukan dalam satu jaringan, sehingga dapat dimungkinkan posisi penyerang berada dalam satu gedung dengan target.
2. *Outer footprinting* adalah kegiatan mencari informasi mengenai target, dimana pencarian informasi dilakukan di luar area jaringan dengan target, sehingga posisi penyerang jauh dari target.

Reconnaissance adalah tahap kegiatan dimana penyerang mengumpulkan informasi sebanyak-banyaknya mengenai target. Informasi yang ditampilkan dari hasil kegiatan ini adalah berupa *network* target: TCP (*Transmission Control Protocol*) / IP (*Internet Protocol*). Reconnaissance merupakan sebuah fase persiapan sebelum (attacker) melakukan penyerangan, dimana kegiatan intinya adalah mengumpulkan informasi sebanyak mungkin mengenai sasaran. Teknik ini akan menyertakan network scanning baik melalui jaringan internal atau external yang tentu saja tanpa mengantongi ijin. Reconnaissance, terdiri dari:

1. *Active reconnaissance* adalah aktivitas pengumpulan data dengan bertatap muka langsung dengan target. Aktivitas tersebut dapat dilakukan baik secara fisik maupun non-fisik, seperti mengunjungi situs utama dari target.
2. *Passive reconnaissance* adalah aktivitas pengumpulan data melalui media perantara, seperti berita media masa televisi, radio, koran, maupun internet, dimana berita tersebut disajikan oleh pihak di luar target.

Perlu diketahui, bahwa dalam melakukan *footprinting* dan reconnaissance ini, ada beberapa tahapan yang lebih rinci yang dilakukan penyerang dalam melakukan *penetration testing*, yakni metode untuk mengevaluasi keamanan sistem komputer atau jaringan, dengan melakukan simuasi serangan dari sumber yang berbahaya. Tujuannya adalah untuk mengetahui kelemahan dari suatu sistem, dimana hal ini menjadi penting untuk dilakukan, karena ada bagian dari perusahaan yang sangat perlu untuk dilindungi, yakni informasi aset dari perusahaan itu sendiri. Tahapan lebih rinci yang dimaksud adalah adanya pembagian yang lebih spesifik dari langkah *footprinting* dan reconnaissance, yakni

1. *Information Gathering* adalah langkah mengumpulkan informasi secara umum mengenai target, seperti informasi administrasi dari suatu perusahaan, alamat perusahaan berada, nomor telepon perusahaan, alamat email perusahaan dan lain sebagainya. Contoh *tools* yang digunakan untuk melakukan langkah ini adalah perintah *ping*, *whois* dan *dnsmap* pada terminal, dapat pula menggunakan aplikasi maltego untuk melakukan *capture* terhadap arsitektur jaringan pada target, serta dengan menggunakan browser mantra dari perusahaan OWASP Mantra. Dengan browser mantra ini, penyerang akan dapat mengetahui informasi target secara lebih mendetail, yakni terkait sistem operasi, *web server*, dan sistem manajemen konten yang digunakan apa, serta informasi *traceroute*, dan informasi lainnya mengenai target.
2. *Service Enumeration* adalah tahapan kelanjutan dari *information gathering*. Dengan langkah ini, dapat mengetahui kondisi target dan layanan port apa saja yang sedang terbuka. Untuk mengimplementasikannya, dan dapat melakukannya dengan memberikan perintah *nmap* biasa pada terminal, contoh: nmap (alamat ip), dan dapat pula dengan mengakses menu "pr > Enumeration > Netcraft - Site Report" pada browser mantra di pojok kanan bawah. Menu tersebut *invisible*/tidak terlihat. Baru akan terlihat, ketika kursor diarahkan ke pojok kanan bawah browser.
3. *Vulnerability Assesment* awal adalah tahap dimana penyerang mencari celah dari komputer target, dengan tujuan memperoleh informasi target secara lebih mendetail, terkait informasi port yang terbuka, nama *service* dari port tersebut, jumlah hop, dan mengetahui celah yang disarankan sistem *attacker* untuk masuk ke dalam sistem target. Langkah ini dapat dilakukan dengan melakukan *nmap* lebih mendalam, contoh: nmap -T4 -Pn -v -A (alamat ip).

Tools Reconnaissance & Footprinting adalah antara lain :

- Readnotify untuk melakukan track email (apakah email tersebut akfif, melakui mana saja dll)
- Whois (menemukan registrant website, dimana dihosting, alamat contactnya , alamat telp, dll)
- Nslookup, Samspade script (bisa melakukan scan alamat, crawl website, browse web, traceroute, s-lang command, decode url, parse email headers dll)
- Google untuk menemukan apakah ada internal link dari sasaran (tidak jarang ada intranet organisasi yang di broadcast juga ke internet namun dengan di cover oleh login untuk masuk)
- www.archive.org untuk menemukan kapan web dari sasaran di launch untuk pertama kali, update nya sampai dengan sekarang ini. Untuk sasaran personal bisa menggunaka http://people.yahoo.com atau www.intellius.com(mencari lokasi kediaman, tanggal lahir, lokasi terakhir dll.)

- Google Map untuk mencari lokasi organisasi sasaran.
- Melalui Jobsite misalnya jobsdb bisa diketahui mereka butuh pekerja apa, informasi hardware, informasi software dll. Jadi misalnya mereka posting butuh karyawan untuk network dengan spesifikasi CCNA, MCDBA maka bisa asumsikan mereka menggunakan infrastruktur Cisco, Database SQL
- Waybackmachine.com Semacam archive dari website

10.4. HARDWARE DAN SOFTWARE

Alat dan bahan yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. Tools Nslookup

10.5. PRE-TEST

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

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-04	1. jelaskan pengertian Footprinting & Reconnaissance!	50
2.	CPL-07	CPMK-04	2. sebut dan jelaskan tools untuk Reconnaissance & Footprinting, minimal 5!	50

10.6. LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

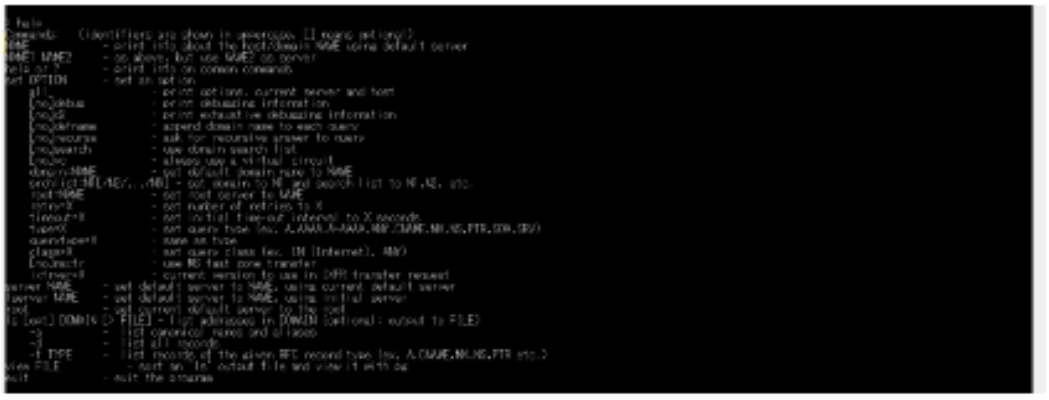
No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-07	CPMK-04	Selesaikan langkah praktikum berikut ini!	Screen Shot Hasil praktikum	100

Menggunakan Link Berikut: https://www.youtube.com/watch?v=T-x7Z1UCsGY

1. Buka CMD dengan Run Administrator

2. Ketik "Nslookup", dan enter

3. Ketik "Help" dan enter untuk melihat syntax syntax yang bisa digunakan dalam Nslookup



4. Ketik set type=a
5. Ketik www.google.com

```
> set type=a
> www.google.com
Server:  UnKnown
Address:  103.19.180.213

Non-authoritative answer:
Name:    www.google.com
Addresses:  172.217.194.106
          172.217.194.147
          172.217.194.99
          172.217.194.103
          172.217.194.105
          172.217.194.104
```

6. Ketik set type=cname
7. Ketik www.google.com

```
> set type=cname
> www.google.com
Server:  UnKnown
Address:  103.19.180.213

google.com
        primary name server = ns1.google.com
        responsible mail addr = dns-admin.google.com
        serial  = 457432753
        refresh = 900 (15 mins)
        retry   = 900 (15 mins)
        expire  = 1800 (30 mins)
        default TTL = 60 (1 min)
>
```

8. Ketik server 8.8.8.8

```
> server 8.8.8.8
Default Server:  dns.google
Address:  8.8.8.8
```

9. Ketik kembali set type=a
10. Ketik www.google.com

```
> set type=a
> www.google.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    www.google.com
Addresses:  172.217.194.105
          172.217.194.99
          172.217.194.147
          172.217.194.106
          172.217.194.104
          172.217.194.103
```

11. Ketik kembali set type=cname

12. Ketik www.google.com

```
> set type=cname
> www.google.com
Server:  dns.google
Address:  8.8.8.8

google.com
        primary name server = ns1.google.com
        responsible mail addr = dns-admin.google.com
        serial  = 457432753
        refresh = 900 (15 mins)
        retry   = 900 (15 mins)
        expire  = 1800 (30 mins)
        default TTL = 60 (1 min)
>
```

13. Ketik set type=mx

14. Ketik www.google.com

```
> set type=mx
> www.google.com
Server:  dns.google
Address:  8.8.8.8

google.com
        primary name server = ns1.google.com
        responsible mail addr = dns-admin.google.com
        serial  = 457432753
        refresh = 900 (15 mins)
        retry   = 900 (15 mins)
        expire  = 1800 (30 mins)
        default TTL = 60 (1 min)
>
```

10.7. POST TEST

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

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-04	Pilih salah satu video atau tutorial pada materi di modul yg ada kemudian implementasikan video tersebut, buatlah langkah-langkahnya dan beri penjelasan!	100

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:**

DAFTAR PUSTAKA

1. https://www.niagahoster.co.id/blog/apa-itu-vpn/
2. https://nagitec.com/network-security-untuk-apa/
3. https://www.tembolok.id/pengertian-vulnerability-contoh-dan-pencegahan/
4. https://www.ethicalhacker.net/content/view/16/24/
5. https://www.dewaweb.com/blog/pengertian-bug-hunter/
6. https://www.elitery.com/id/articles/perbedaan-backup-restore-recover-data-elitery/
7. http://cgeduntuksemua.blogspot.com/2012/05/pengertian-dan-jenis-web-hacking.html
8. https://indosystem.com/blog/web-application-security/
9. https://if.polibatam.ac.id/rekayasa-keamanan-siber/blog/?p=115
10. https://www.greenteaslash.com/2014/11/footprinting-dan-reconnaissance.html


LABORATORIUM
TEKNIK INFORMATIKA
UNIVERSITAS AHMAD DAHLAN


UNIVERSITAS AHMAD DAHLAN