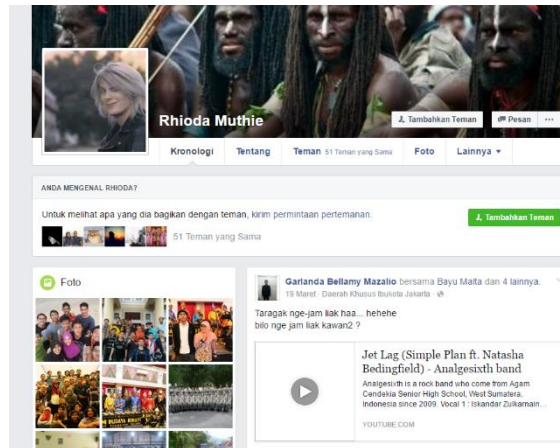


Nama	Arga Nur Pratama
Tugas #1	Pilih salah satu akun facebook yang tidak ada identitas foto asli dan buktikan bahwa akunnya palsu
Implementasi	<p>Metode #1</p> <ol style="list-style-type: none"> Melakukan <i>information gathering</i> terlebih dahulu. Untuk mencari akun palsu, butuh “kolam” yang tepat untuk mempersempit pencarian. Maka proses pencarian akun dilakukan melalui Group – Group Facebook.
	 <p style="text-align: center;">Gambar 1 List Group</p> <p>Diatas merupakan beberapa Group Facebook yang dimiliki. Setelah didapati Group-nya, untuk mempermudah pencarian maka dipilih salah satu dari Group yang ada. Saya memilih Group “Aliansi Sekuler Indonesia”, alasan saya memilih ini dikarenakan banyaknya propaganda – propaganda yang dilakukan di dalam Group tersebut. Saya mengasumsikan, bahwa untuk melakukan propaganda tersebut mereka membutuhkan akun – akun palsu untuk bisa mengamankan identitas diri mereka yang sebenarnya.</p> <ol style="list-style-type: none"> Setelah itu, saya mencari dan mengidentifikasi terhadap anggota yang ada di Group tersebut.
	

Karena tugasnya adalah mencari akun palsu yang tidak ada “Foto Aslinya”, maka dari 27.795 akun Facebook yang ada di Group tersebut, saya mempersempit pencarian dengan melihat akun yang tidak menggunakan foto aslinya.

3. Saya mulai memilih akun yang bernama “[Rhioda Muthie](#)”. Karena akun tersebut tidak menggunakan foto aslinya. Kemudian saya coba membuka profilnya untuk mengetahui informasi akun tersebut lebih jauh.



Gambar 3 Profil Akun

Informasi yang saya dapat, bahwa akun ini ternyata memiliki 51 mutual friends dengan saya. Jumlah tersebut bisa dikatakan cukup banyak, terlebih lagi pada album koleksi fotonya terdapat foto – foto dari aktivitasnya. Asumsi saya, akun ini merupakan akun asli. Hal ini juga diperkuat ketika saya melihat isi *timeline* akun tersebut, dimana banyak foto dari akun lainnya yang men-*tag* akun Rhioda Muthie.



Gambar 4 Akun lain men-*tag* akun Rhioda Muthie

Adanya bukti men-*tag* Rhioda Muthie ini memberikan bukti jika identitas ini memang benar – benar ada dan merupakan akun asli.

4. Sampai beberapa akun yang terdapat di Group tersebut saya lakukan proses identifikasi dan analisa yang sama. Hingga kemudian saya menemukan akun yang bernama [Jefri Pangaribuan](#)

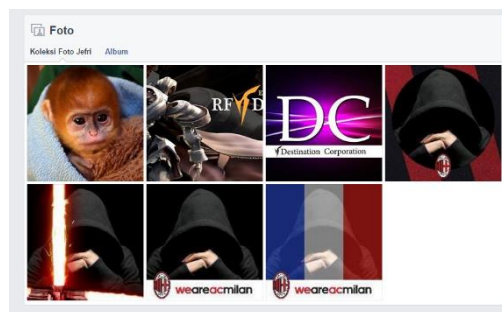


Gambar 5 Akun Jefri Pangaribuan

Saya mulai menelusuri timeline dan profil dari akun berikut untuk mendapatkan lebih banyak informasi dan memperkuat hipotesis saya bahwa akun ini adalah “Akun Palsu”.


Dimulai dari Follower akun, dimana akun ini hanya “Diikuti oleh 62 Orang”.

Lalu saya melihat album fotonya, dimana hanya terdapat foto – foto seperti berikut :



Gambar 6 Album Foto dari akun Jefri

Namun ini masih belum cukup, saya melanjutkan kembali proses pencarian informasi dengan melihat aktifitas akun ini pada *timeline*-nya.

	<p>Log Aktivitas akun tersebut :</p> <p>2 Mei 2016 Update Foto Profile</p> <p>23 Februari 2016 Update Sampul Foto</p> <p>23 Februari 2016 Update Sampul Foto</p> <p>30 Januari 2016 Update Foto Profile</p> <p>17 Desember 2015 Update Foto Profile</p> <p>4 Desember 2015 Update Foto Profile</p> <p>4 Desember 2015 Update Foto Profile</p> <p>19 Agustus 2015 Update Sampul Foto</p> <p>19 Agustus 2015 Update Foto Profile</p> <p>4 Agustus 2015 Share Video</p> <p>4 Agustus 2015 Membagikan Pertemanan</p> <p>1 Agustus 2015 Membagikan Album Foto</p> <p>21 Agustus 2011 Update Status</p> <p>Hal yang mencurigakan adalah terjadinya kekosongan aktivitas yang cukup jauh dari tahun 2011 hingga tahun 2015. Awalnya saya mengira, bisa saja aktivitasnya di <i>hide</i>. Namun rentang waktu dari 2011 hingga 2015 adalah empat tahun, dengan jarak waktu seperti itu tentu akan ada banyak aktivitas yang harus di-<i>hide</i> (jika memang ada aktivitasnya).</p> <p>Namun dengan melihat dari sudut pandang lain, yaitu dari Log Aktivitas-nya terlihat hanya sedikit sekali aktivitas yang dilakukan tiap tahunnya. Pada 2016 hanya ada empat kali aktivitas saja, 2015 ada 8 Aktivitas, lalu masuk ke 2011 hanya ada 1 aktivitas saja.</p> <p>Dengan pertimbangan :</p> <ul style="list-style-type: none"> - Kondisi aktifitas yang jarang aktif, - Album foto yang tidak ada identitas aslinya - Ataupun Foto yang menggambarkan aktivitas dunia nyata pemilik akun, - Follower 62 Orang - Dan alamat akun dengan samaran https://www.facebook.com/SonOfAnubiz <p>Saya menyimpulkan jika akun ini merupakan akun palsu.</p>
Tugas #2	<i>Pilih salah satu akun facebook dan hack sampai dapat password-nya tanpa diketahui</i>
Implementasi	<ol style="list-style-type: none"> 1. Melakukan <i>information gathering</i> untuk mencari celah – celah keamanan yang dapat dieksploitasi dari Facebook. 2. Dimulai dari melihat fitur – fitur yang ada di Facebook. 

3. Saya menggunakan hipotesis awal bahwa sistem keamanan yang dimiliki facebook termasuk kuat. Oleh karena itu saya mencoba mengesampingkan penggunaan tools seperti **nmap**, **hydra**, **metasploit** ataupun **sqlmap**. Cara lain yang digunakan adalah dengan memanfaatkan fitur “Ada Masalah?” yang terdapat di bawah textfield username dan login.

A screenshot of the Facebook login interface. It features two input fields: 'Email atau Telepon' and 'Kata Sandi'. Below the 'Kata Sandi' field, the link 'Ada masalah?' is circled in red. A 'Masuk' button is located to the right of the password field.

Mengapa pilihan ini yang saya ambil, karena saya pernah membaca berita bahwa ada peretas (hacker) yang menggunakan fitur tersebut untuk dieksploitasi. Dengan menginspeksi nomor telpon konfirmasi si victim, lalu mengubahnya ke nomor telepon attacker. Sehingga kode verifikasi akan dikirimkan ke nomor telepon attacker. Akan tetapi bug tersebut kemudian dilaporkan ke Facebook, dan attacker mendapat reward atas reportnya. Dan Facebook pun sebenarnya sudah memperbaiki celah tersebut, namun kembali pada hakikatnya tidak ada sistem yang 100% aman.

4. Saya coba mengklik fitur “**Ada masalah?**”, dan mengikuti langkah berikutnya.

A screenshot of the Facebook 'Temukan Akun Anda' (Find Your Account) page. It prompts the user to enter 'Email, Telepon, Nama Pengguna, atau Nama Lengkap'. Below the input field is a blue envelope icon. At the bottom, there is a message 'Saya tidak dapat mengidentifikasi akun saya.' and two buttons: 'Cari' and 'Batalan'.

Nah, disini barulah saya memilih akun mana yang akan diretas. Tentunya saya akan memilih akun yang dimana saya sudah memiliki banyak informasi tentang akun tersebut. Akun yang saya coba retas adalah [Tides Anugraha](#). Maka saya isikan pada kolom tersebut nama akunnya.

A screenshot of the Facebook 'Atur Ulang Kata Sandi Anda' (Reset Your Password) page. It asks 'Cara apa yang Anda inginkan untuk mengatur ulang kata sandi?'. There are two radio button options: 'Kirim saya tautan untuk mengatur ulang kata sandi' (selected) and 'Kirim saya SMS berisi kode untuk mengatur ulang kata sandi'. The first option shows an email address '*****a@gmail.com'. The second option shows a phone number '*****95'. On the right, there is a profile picture and the name 'Tides Anugraha' with the title 'Pengguna Facebook'. At the bottom, there is a link 'Tidak punya akses ke sini lagi?' and two buttons: 'Lanjutkan' and 'Bukan Anda?'.

Pada gambar diatas tertera alamat email dan juga nomor HP yang dimiliki oleh victim. Melalui alamat – alamat tersebutlah

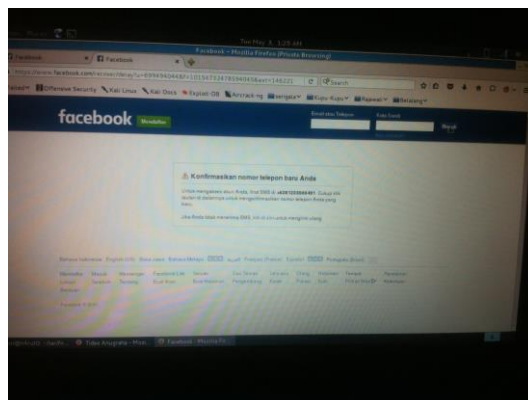
nantinya akan dikirimkan kode verifikasi. Karena alamat dan juga nomor HP diatas di-hide, dan maka saya harus mencari lagi alamat – alamat tersebut. Dan seandainya pun saya mendapatkan alamat email dan nomor HP diatas, saya masih harus berusaha untuk meretas hak aksesnya.

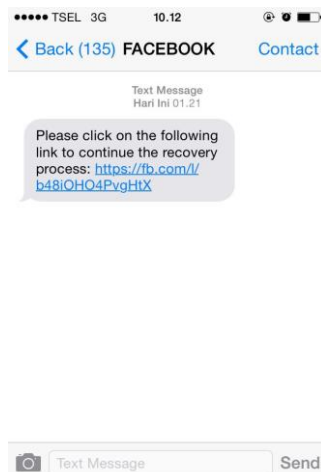
Akhirnya saya coba gunakan fitur “Tidak punya akses ke sini lagi?”. Saya coba memanfaatkan fitur ini, karena memberikan peluang bagi saya untuk mendapatkan kode verifikasi dengan tidak mengetahui sama sekali alamat email dan nomor HP victim.



Setelah diklik fitur diatas, saya mendapati kolom *textfield* yang harus diisi nomor hp. Maka disini saya mengisi nomor HP saya agar mendapatkan kode verifikasi dari facebook.

Setelah mendapatkan kode verifikasi yang dikirim ke nomor hp saya, kemudian memasukkan kode tersebut ke *textfield* kode verifikasi. Jika berhasil, maka akan dihadapkan pada **Pertanyaan Keamanan** terlebih dahulu sebelum masuk ke tahap pemulihan password. Pertanyaan keamanannya adalah **“Di kota manakah ibu anda dilahirkan?”**. Nah disinilah kemudian fungsi information gathering itu diperlukan. Namun karena saya sudah mendapatkan banyak informasi yang didapat dari akun victim, saya pun telah mendapatkan informasi dari pertanyaan diatas. Jawabannya adalah **“Palembang”**. Saya coba isikan jawaban tersebut, dan berhasil. Lalu saya diminta untuk mengakses link pemulihan password yang dikirimkan ke nomor HP yang saya input sebelumnya.



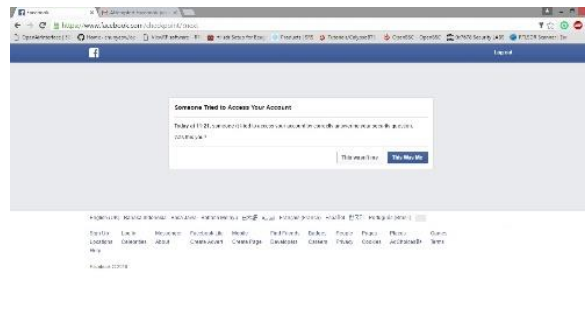


Gambar diatas adalah pesan yang dikirimkan oleh facebook yang berisikan link pemulihan password. Kemudian saya klik, dan akhirnya password berhasil dipulihkan.

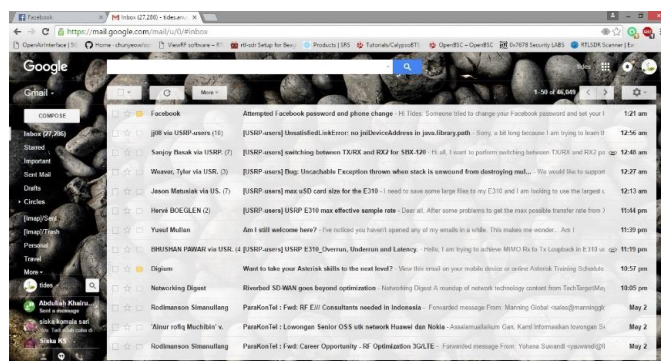
Saya diminta untuk memasukkan password yang baru, dan password tersebut diisi dengan 'industri2014". Jika sudah berhasil diinput password yang baru, tinggal kita mencoba masuk ke facebook dengan cara seperti biasa. Input username dan password yang terbaru. Dan hasilnya adalah seperti berikut :



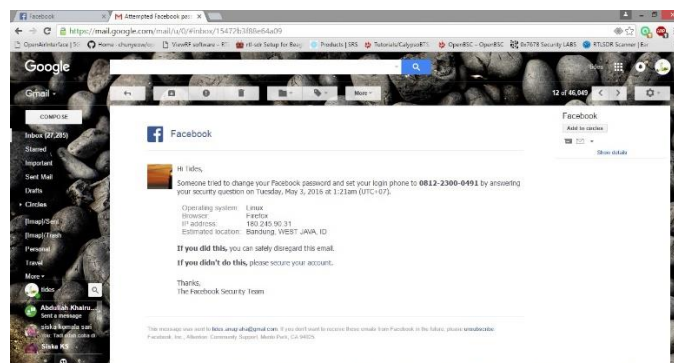
Hanya saja yang menjadi tantangan adalah kita harus menunggu 24 Jam untuk bisa mengakses akun facebook yang kita retas passwordnya. Selain itu, dari sistem facebook juga memberikan "alert" kepada pengguna melalui notifikasi di facebook dan juga email.



Pada halaman diatas ada pilihan “This wasn’t me” dan “This was me”. Jika user memilih “This was me”, maka attacker akan aman. Namun jika pilihan “This wasn’t me”, maka akses pemulihan password akan gagal.



Email notifikasi dari facebook.



Pilihan yang sama juga diberikan di notifikasi email. Dengan memberikan pilihan apakah user yang melakukan pemulihan password adalah user yang sebenarnya atau seorang attacker.

User : tides.anugraha
Pass : industri2014