Latar Belakang Toolkit Keamanan Siber GCA:
Kotak Peralatan
Lebih dari Sekadar Kata Sandi Sederhana

Salah satu metode paling umum yang digunakan penjahat siber untuk mendapatkan akses ke akun, jaringan, dan informasi Anda adalah dengan menggunakan kredensial Anda, yaitu lewat nama pengguna (*username*) dan kata sandi. Perlu diperhatikan pentingnya menggunakan kata sandi (atau frasa sandi) yang kuat dan unik untuk tiap-tiap akun serta menjaga kerahasiaan dan keamanan kata sandi, dan tidak sekali-kali memakai ulang kata sandi.

- Memakai ulang kata sandi yang sama di beberapa akun dapat berarti bahwa jika penjahat siber berhasil mendapatkan salah satu kata sandi Anda, mereka mendapat celah yang sempurna untuk masuk ke semua akun yang menggunakan kata sandi tersebut.
    - *Nama pengguna dan kata sandi yang sama akan dicoba di banyak aplikasi umum.*

Ada banyak teknik yang akan digunakan penjahat siber untuk mendapatkan akses ke kata sandi Anda. Ada juga pasar yang sangat aktif di Internet (terkadang disebut juga 'web gelap') untuk membeli dan menjual informasi pribadi ini jika salah satu perusahaan yang akunnya Anda miliki dibobol.

Metode yang digunakan meliputi:

- **Serangan brutal**: Menggunakan kemampuan komputasi untuk secara otomatis memasukkan semua kemungkinan kombinasi.
    - *Gunakan frasa sandi atau kata sandi yang panjang dan karakter khusus untuk menambah tingkat kesulitan.*
- **Serangan kamus** : Bentuk serangan brutal yang menggunakan kata/frasa kamus yang diketahui atau kata sandi yang umum.
    - *Gunakan kata/kata sandi yang mudah diingat tetapi bukan kata-kata yang diambil dari kamus, kata sandi yang umum, atau kata sandi yang dapat dikaitkan dengan Anda. Misalnya: kata sandi dengan nama kota, nama jalan, dan lainnya.*
- **Isian kredensial** : Setelah satu akun berhasil dibobol, mereka akan mencoba nama pengguna/kata sandi yang sama di tempat lain.
    - *Gunakan kata sandi yang berbeda untuk setiap akun serta perlindungan tambahan (Autentikasi 2 Faktor – 2FA) untuk akun yang memiliki fasilitas ini.*
- **Phishing surat elektronik:** yakni, 'Saatnya mengatur ulang kata sandi Anda' dengan tautan ke situs web berbahaya atau *keylogger* yang langsung terinstal saat Anda

membuka lampiran berbahaya (*keylogger* akan melacak penggunaan keyboard oleh Anda).
    - *Waspadalah ketika membuka, mengeklik tautan, atau mengunduh lampiran dari surat elektronik apa pun meskipun diterima dari seseorang atau organisasi yang Anda kenal.*

- **Rekayasa Sosial** : Perekayasa sosial sangat terampil dalam memanipulasi percakapan dan menggunakan berbagai media (panggilan telepon, pesan teks, atau media sosial) untuk memperdaya Anda agar memberikan kata sandi dan informasi pribadi lainnya dengan cara yang tampak sah.
    - *Jangan sekali-kali memberikan kata sandi Anda, atau bagian daripadanya, kepada siapa pun. Perusahaan yang sah tentu tidak akan bertanya. Selain itu, jangan langsung percaya jika seseorang mengaku sebagai anggota keluarga Anda.*
- **Menebak-nebak**: Informasi pribadi yakni, jika nama dan tanggal lahir digunakan sebagai bagian dari kata sandi Anda.
    - *Jangan masukkan data pribadi pada kata sandi – ingatlah hal yang mungkin diungkap di web dan media sosial tentang Anda dan hindari penggunaan informasi tersebut pada kata sandi Anda.*
- **Mengintip Bahu** : Di tempat umum, atau bahkan di meja kerja Anda, mungkin ada seseorang yang 'mengintip' aktivitas Anda.
    - *Periksa siapa atau apa pun yang mungkin berada di belakang atau di samping Anda, atau di tempat yang terpantau kamera, terutama saat memasukkan informasi sensitif.*
- **Intersepsi** : Kata sandi dapat dicegat saat ditransmisikan melalui jaringan.
    - *Periksa tanda gembok https di situs web dan berhati-hatilah saat menggunakan Wi-Fi di tempat umum; situs web mungkin tidak aman atau 'dibajak' dengan nama serupa yang memungkinkan orang lain 'melihat' apa yang Anda transmisikan* **.**

Kemampuan komputasi telah meningkat secara eksponensial dari waktu ke waktu, seperti halnya penggunaan Internet dan media sosial. Semua ini telah mempermudah dan mempercepat penjahat siber untuk mendapatkan akses ke informasi Anda:

	1984 Apple MacIntosh PC:	2019 iMac ‘Core i5’ (standar)	Perbedaan:
RAM:	128K	8G	Meningkat 64.500.000%
Kecepatan pemrosesan:	8MHz	3GHz	Lebih cepat 37.400%
Biaya:	$2.500	$1.500	Pengurangan 40%

- Kemajuan teknologi yang cepat telah benar-benar bekerja untuk keuntungan peretas karena laptop dan program modern dapat memecahkan kata sandi lebih cepat daripada sebelumnya.

- *Kebutuhan untuk mengikuti kata sandi yang lebih panjang dan lebih kompleks serta metode perlindungan tambahan meningkat bersamaan dengan kemajuan teknologi ini.*

Autentikasi Dua Faktor (2FA):

2FA memberikan tingkat perlindungan sekunder sehingga jauh lebih sulit bagi penyerang untuk mendapatkan akses ke akun Anda karena bergantung pada:

- Sesuatu yang Anda tahu:
  - Kata sandi
- Dan/atau sesuatu yang Anda miliki:
  - Token (Google Authenticator, Okta, RSA)
  - Kode verifikasi yang dikirim ke ponsel Anda (SMS)

- Atau sesuatu pada diri Anda:
  - Sidik jari atau wajah (biometrik)

2FA membutuhkan ini sebelum memberikan akses, yang memberikan lapisan pertahanan ekstra.

Ada banyak panduan yang tersedia untuk membuat kata sandi atau frasa sandi yang panjang dan kuat. Apa pun panduan yang Anda ikuti, pastikan untuk:

- Pastikan Anda memiliki kebijakan kuat yang diterapkan di seluruh perusahaan dan sistem yang melarang penggunaan kata sandi yang lemah.
- Hindari nama hewan peliharaan, nama anggota keluarga, atau kata sandi yang bisa ditebak melalui media sosial.
- Gunakan kata sandi yang berbeda untuk setiap akun.
- Pertimbangkan untuk menggunakan pengelola kata sandi untuk menyimpan kata sandi jika diinginkan.

Selain itu:

- Perbarui kata sandi Anda di akun mana pun yang telah dibobol (Anda dapat memeriksanya melalui alat 'Apakah Saya Telah Kena Pwned' di kotak peralatan).
- Hapus akun dan hapus instalan aplikasi yang sudah tidak digunakan.
- Pastikan Anda menggunakan kata sandi unik dan kuat di semua akun.
- Aktifkan 2FA di semua akun Anda (apabila 2FA didukung).
- Periksa pengaturan admin/default admin di perangkat yang dapat diakses secara jarak jauh. Selalu ubah kata sandi bawaan yang dapat ditebak sebelum digunakan untuk pertama kali.

Gunakan alat di Kotak Peralatan Lebih dari Sekadar Kata Sandi Sederhana untuk melihat panduan, memeriksa apakah salah satu akun Anda diketahui telah dibobol, dan membantu Anda menerapkan penyempurnaan.

https://gcatoolkit.org/id/umkm/lebih-dari-sekadar-kata-sandi-sederhana/?_tk=kata-sandi-yang-kuat