Secret Hacking Technics by : Wisdom (Antonius)

https://bluedragonsec.com

https://github.com/bluedragonsecurity

Contoh Skenario Hacking dengan Memanfaatkan Nomor HP Korban

Teknik ini sangat berbahaya, karena nomor hp korban biasanya terkait dengan berbagai macam login akun lainya seperti akun whatsapp, akun facebook, akun instagram, akun mobile banking dan akun akun lainya.

Kali ini kita tidak akan praktekkan secara langsung, karena tidak memungkinan. Saya hanya akan membagikan caranya. Berikut ini beberapa contoh skenario yang bisa digunakan hacker untuk take over nomor hp target yang kemudian meluas ke take over semua akun korban yang ditautkan ke nomor hp tersebut :

SKENARIO 1. SIM CARD SWAPPING ATTACK

Misal hacker mengincar seorang target dan hacker ini tahu nomor hp si target di mana nomor tersebut masih aktif di hp si target. Nomor tersebut ditautkan ke berbagai akun si korban seperti akun whatsapp, gmail, sosmed, dll.

Langkah 1.

Jika hacker tersebut sudah mengetahui data detail tentang ktp si target. Ada berbagai cara, misal :

Cara 1 : misal si hacker mendapatkan scan ktp si target dari internet

Cara 2 : hacker memiliki akses ke data kependudukan di server dukcapil

Cara 3 : hacker berhasil menipu korban untuk memberikan data ktpnya dengan teknik social engineering, misal dengan berpura pura memberikan lowongan kerja palsu yang mengharuskan korban menyerahkan scan ktp, scan ijazah, sertifikat, dll.

Cara 4 : hacker membeli dump data kependudukan Indonesia di darknet dan mendapatkan data kependudukan korban**,** berbagai dump data kependudukan telah beberapa kali ditemukan dijual di darknet dan forum peretas (seperti BreachForums).

Langkah 2.
Hacker kemudian datang ke gerai membawa ktp palsu yang sudah disiapkan sesuai data ktp asli dari korban dan surat kehilangan dari polisi tentang kehilangan ponsel.

Terkadang orang gerai akan meminta bukti tambahan bahwa nomor handphone yang akan diclaim benar benar milik si hacker dengan cara meminta bukti secara visual bahwa akun akun sosmed pihak pengclaim terkait dengan nomor hp yang akan diklaim, maka sangat mudah caranya. Cukup membawa laptop dengan web sosial media palsu yang sudah disiapkan sebelum datang ke gerai, dengan laptop itu hacker bisa menunjukkan bahwa akun akun sosmed si hacker menggunakan nomor hp yang diklaim.

Contoh caranya : hacker membawa laptop yang membuktikan kalau nomor tersebut terkait dengan akun akun sosmed seperti facebook, linkedin, instagram dan twitter si hacker.

Caranya ? Si hacker membuat web sosial media palsu di komputer sendiri kemudian memanipulasi /etc/hosts dari domain domain tersebut agar mengarah ke web palsu di localhost,

Web sosmed palsu tersebut intinya menunjukkan akun akun sosmed si hacker di mana terlihat nomor hp si korban yang ditautkan ke akun akun sosmed tersebut.

Langkah 3.

Setelah berhasil menipu orang gerai, si hacker akan mendapatkan nomor hp korban.

Setelah mendapatkan nomor hp si korban yang aktif di ponsel si hacker, maka bagi si hacker akan sangat mudah untuk take over akun akun lainya seperti akun gmail, whatsapp, akun sosmed atau akun lainya yang ditautkan dengan nomor hp si korban.

Aksi ini disebut dengan **SIM Swap Fraud** (Penipuan Tukar SIM) yang dikombinasikan dengan teknik **Social Engineering** (Rekayasa Sosial).

Bagaimana Hacker Melakukannya?

Dalam skenario ini, hacker melakukan verifikasi fisik untuk meyakinkan petugas gerai (Customer Service). Berikut adalah bedah tahapannya:

1. **Identity Theft (Pencurian Identitas):** Hacker sudah memiliki data KTP asli. Dengan data ini, membuat KTP palsu (fisik) dengan foto hacker namun data korban adalah hal yang relatif mudah bagi penipu profesional.
2. **Fabricated Evidence (Bukti Palsu):** Surat kehilangan dari polisi menambah legitimasi. Petugas gerai biasanya tidak memiliki akses langsung untuk memvalidasi keaslian surat polisi tersebut secara real-time.
3. **Local DNS Poisoning (/etc/hosts):** Ini adalah bagian yang cerdas. Dengan mengarahkan domain populer (FB, IG) ke IP lokal yang sudah dimodifikasi, hacker menipu petugas gerai

secara visual. Petugas melihat bahwa "akun tersebut login di laptop si hacker", yang memperkuat klaim kepemilikan nomor tersebut.

4. **Psychological Pressure:** Hacker datang dengan persiapan matang untuk meyakinkan petugas bahwa dia adalah "pemilik sah yang sedang tertimpa musibah (HP hilang)".

Mengapa Ini Berbahaya?

Begitu petugas gerai menerbitkan kartu SIM baru dengan nomor korban, maka:

- **Kartu SIM lama (milik korban) otomatis mati.**
- Hacker memegang kendali penuh atas SMS dan panggilan telepon.
- Hacker bisa melakukan **Password Reset** menggunakan fitur "Forgot Password" pada akun perbankan, media sosial, dan email karena kode OTP akan masuk ke HP hacker.

Apa Nama Teknik Ini?

Secara spesifik, ini melibatkan beberapa teknik yang diracik si hacker :

- **SIM Swapping:** Proses memindahkan layanan nomor telepon dari kartu SIM korban ke kartu SIM milik hacker.
- **Social Engineering:** Manipulasi psikologis terhadap petugas gerai agar mereka mengabaikan protokol keamanan yang ketat atau merasa yakin dengan bukti palsu yang dibawa.
- **Visual Spoofing:** Menggunakan manipulasi teknis (seperti edit `/etc/hosts`) untuk menciptakan tampilan visual yang menipu.

SKENARIO 2. SIM CARD RECYCLING ATTACK

Misal si target dulunya menggunakan suatu nomor hp, kemudian sekarang nomor hp tersebut tidak aktif lagi,

Langkah 1.
hacker yang mengetahui kalau nomor korban sudah tidak aktif lagi kemudian membeli nomor tersebut dan diaktifkan lagi, di mana nomor itu terkait dengan sosmed seperti facebook, instagram, gmail dan lain lain.

Kondisi ini terjadi karena adanya kebijakan daur ulang nomor telepon (SIM Recycling) oleh pihak operator seluler. Jika sebuah nomor tidak diisi pulsa atau tidak digunakan dalam jangka waktu tertentu (masa tenggang lewat), nomor tersebut akan hangus dan setelah beberapa bulan akan dijual kembali ke pasar sebagai nomor perdana baru.

Langkah 2.

Setelah mendapatkan nomor hp si korban yang aktif di ponsel si hacker, maka bagi si hacker akan sangat mudah untuk take over akun akun lainya seperti akun gmail, whatsapp, akun sosmed atau akun lainya yang ditautkan dengan nomor hp si korban.

Apa Nama Tekniknya ?

Dalam dunia keamanan siber, fenomena ini secara spesifik sering disebut sebagai:

- **SIM Recycling Attack (Serangan Daur Ulang SIM):** Ini adalah istilah teknis ketika seseorang memanfaatkan nomor telepon yang sudah didaur ulang untuk mengambil alih akun pemilik sebelumnya.
- **Account Takeover (ATO) via Recycled Number:** Pengambilalihan akun yang terjadi karena akses fisik/legal terhadap nomor telepon yang terhubung dengan akun tersebut.

Berbeda dengan *SIM Swap* (di mana hacker menipu operator untuk menduplikasi kartu SIM Anda yang masih aktif), dalam kasus ini hacker **secara legal memiliki nomor tersebut** karena membelinya secara resmi.

Bagaimana Proses Peretasan Terjadi?

Hacker biasanya melakukan langkah-langkah berikut:

1. **Identifikasi Target**

   jika targetnya perorangan :

   jika hacker tersebut menargetkan seseorang, kebetulan si orang tersebut memiliki nomor hp yang sudah hangus dan karena jangka waktunya sudah agak lama maka nomor itu kembali dijual di pasaran

   jika targetnya massal (ikan di laut):

   Hacker mencari nomor telepon yang pernah bocor di internet (lewat *data breach* lama) dan memeriksa apakah nomor tersebut masih aktif atau tidak.

2. **Akuisisi Nomor:** Jika nomor sudah hangus dan tersedia kembali di pasaran, hacker membelinya.
3. **Pemulihan Akun (Account Recovery):** Hacker pergi ke halaman login Facebook, Instagram, atau Gmail, lalu memasukkan nomor telepon tersebut dan memilih opsi **"Forgot Password"** (Lupa Kata Sandi). Atau jika akun whatsapp maka hacker tinggal menginstall aplikasi whatsapp baru di hp kemudian diisi dengan nomor hp korban
4. **OTP (One-Time Password):** Kode reset kata sandi akan dikirim via SMS ke nomor yang kini dipegang hacker. Dengan kode tersebut, hacker bisa mengganti kata sandi dan menguasai akun korban sepenuhnya.

Mengapa Ini Berbahaya?

- **Akses ke Data Pribadi:** Hacker bisa melihat pesan pribadi, foto, dan daftar kontak.
- **Akses ke Keuangan:** Jika nomor tersebut terhubung ke whatsapp, Mobile Banking, dompet digital (GoPay, OVO, Dana), atau e-commerce, hacker bisa menguras saldo atau melakukan transaksi.
- **Penipuan:** Hacker bisa berpura-pura menjadi Anda untuk meminjam uang kepada teman-teman di daftar kontak Anda.