Nama : Gonewaje
NIM : 09011181419005

Hack Login Password Windows All Version

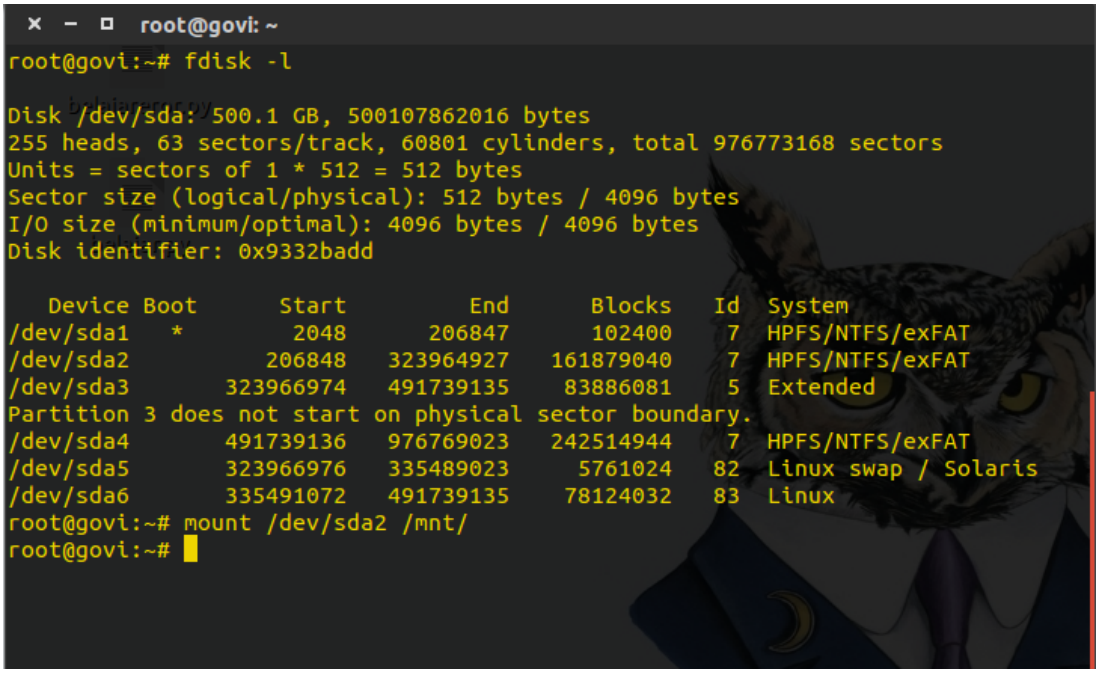
Celah keamanan system operasi windows satu ini cukup dikenal sejak zaman Windows XP, bahkan hingga sampai saat era Windows 10 ini kelemahan ini masih juga bisa diterapkan. Tidak jelas siapa yg pertama kali mempublikasikan celah keamanan ini dan juga tidak jelas kenapa Microsoft belum juga menambal (patch/update) celah yg satu ini.

Inti dari exploitasi celah kemanan ini adalah, meng-akses Command Prompt (cmd.exe) pada login screen. Normalnya, kita tidak bisa menjalankan program apapun (termasuk cmd) yang ada dikomputer windows sebelum login, akan tetapi backdoor yg satu ini memungkinkan "memanggil" cmd di login screen. Parahnya lagi, windows menganggap cmd yang berjalan ini adalah bagian dari system sehingga memilik Privilege Administrator yang memungkinkan kendali penuh atas komputer target.

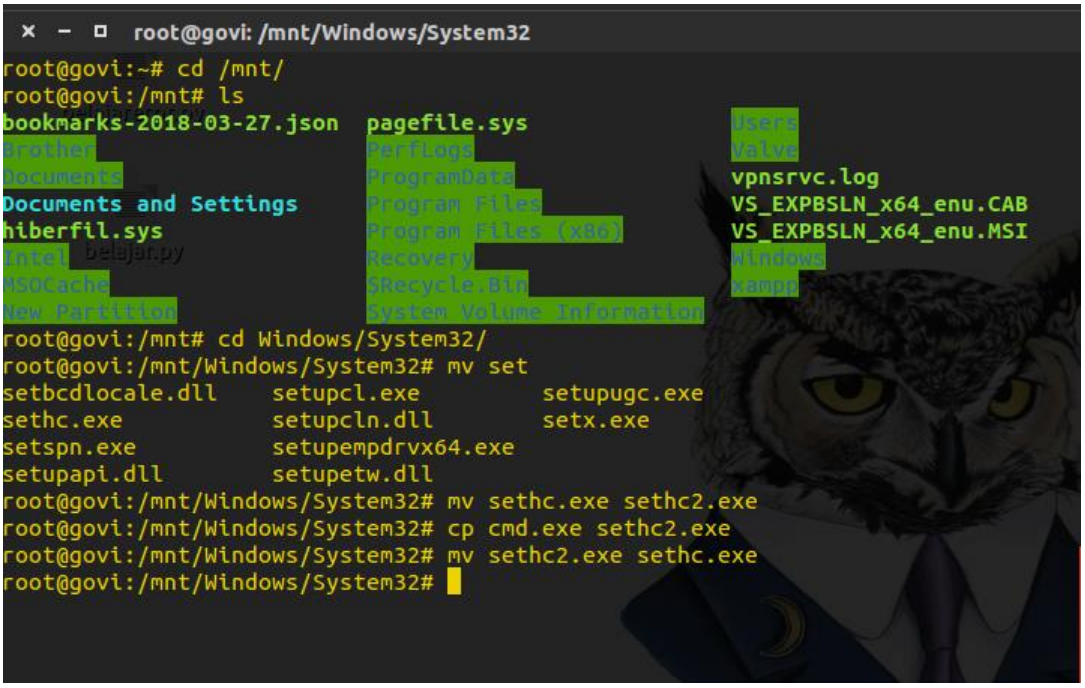
Salah satu contoh penggunaan backdoor ini adalah untuk membypass password login tanpa perlu login dan tahu password aslinya, seperti pada contoh dibawah

1. Buatlah sebuah bootable linux, mengapa harus membuat bootable linux?karena dengan linux kita dapat melakukan live USB/CD tanpa harus instalasi OS tersebut, live USB/CD ini digunakan agar dapat masuk kedalam sistem windows melalui terminal linux.
2. Masuk ke terminal (root access) dan ketikkan perintah “**fdisk -l**”, perintah ini akan menampilkan daftar disk yang aktif dan kita akan melakukan mount sekaligus masuk ke sistem windows (Disk C)
3. Setelah daftar disk muncul, saatnya masuk kedalam disk C windows, bagaimana untuk mengetahui lokasi dari disk C tersebut?biasanya disk dev/sda1 merupakan disk yang berisi grub windows karena ukurannya hanya 2MB dan format disk C adalah NTFS jadi dapat kita simpulkan bahwa disk C windows berlokasi di /dev/sda2, lakukan mount dengan perintah “**mount /dev/sda2 /mnt/**”

Nama : Gonewaje
NIM : 09011181419005

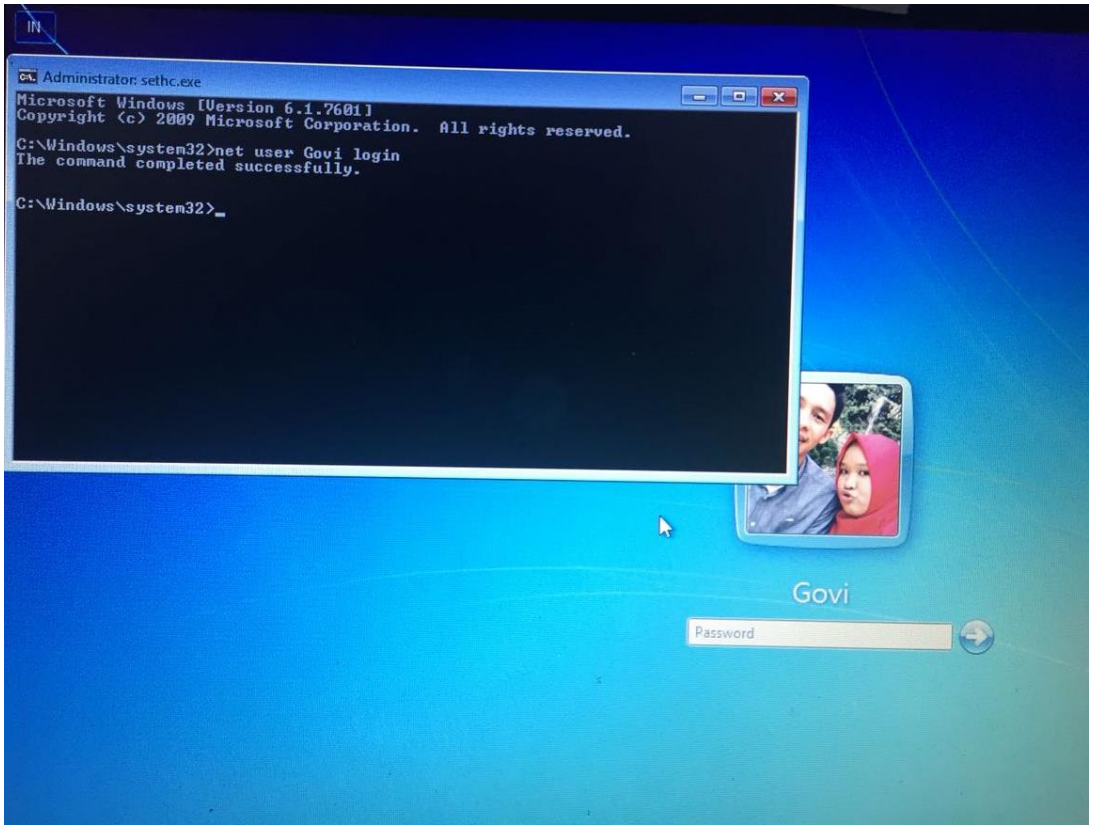


4. Masuk ke direktori mount yang telah dibuat (/mnt/) dengan perintah "**cd /mnt/**" dan cek isi dari disk tersebut untuk memastikan bahwa disk tersebut benar merupakan disk C (sistem) windows dengan perintah "**ls**", setelah yakin maka masuk ke direktori Windwos -> System32 dengan perintah "**cd Windows/System32/**"
5. Langkah terakhir adalah melakukan copy/cut-paste file **cmd.exe** kedalam file **sethc.exe**, **sethc.exe** merupakan sebuah aplikasi mini yang dapat dijalankan melalui login screen windows dengan cara menekan tombol shift sebanyak 5x.



6. Restart komputer lalu masuk ke login screen windows, tekan tombol "**shift**" pada keyboard sebanyak 5x maka akan terbuka cmd, masukkan perintah "**net user Govi**

login" yang mana '**Govi**" adalah username komputer target dan "**login**" merupakan password baru untuk tersangka login kedalam windows korban.



Bagaimana ini bisa terjadi?

Caranya sebenarnya cukup sederhana. pada Login Screen, memang tidak bisa menjalankan program/aplikasi manapun sebelum login. tapi sebenarnya ada 2 aplikasi mini yg bisa dijalankan pada login screen, yaitu StickyKeys dan Utility Manager. Ironisnya, kedua aplikasi yg sebenarnya dibuat untuk membantu orang yg mempunyai beberapa keterbatasan fisik, justru bisa dimanfaatkan untuk membuat backdoor. stickykeys bisa dijalankan dengan menekan 5 kali tombil Shift secara beruntun, sementara utility manager bisa dijalankan dengan kombinasi tombil Win+U atau tombol kecil disudut kiri bawah login screen. file executeable untuk utility manager adalah utilman.exe, sedangkan file executeable untuk stickykeys adalah sethc.exe, sementara file executeable command prompt adalah cmd.exe. jika cmd.exe ini di rename sesuai nama kedua aplikasi tadi, maka terciptalah sebuah celah yg bisa disusupi. selanjutnya tinggal memanggil aplikasi yg file exe-nya telah dimodifikasi. Saat dijalankan, system windows tidak akan melakukan verifikasi apakah file exe yang dijalankan memang benar atau tidak, windows hanya melihat dari nama file exe-

nya saja, disinilah kelemahan terjadi. Bukan aplikasi bersangkutan yg berjalan, justru cmd lah yg terbuka.

Tentu untuk me-rename kedua file tersebut tidak mudah jika dilakukan dari dalam windowsnya sendiri (dengan asumsi kita bisa login ke salah satu usernya), windows akan menjaga ketat kedua file tersebut untuk di modifikasi oleh karena itu dapat digunakan cara live cd bootable linux untuk mengakses file tersebut secara penuh. Bagaimana melakukan pertahanan terhadap backdoor ini? banyak cara, namun yang paling efektif (sekaligus extreme) adalah dengan BitLocker.