PROJECT 2
Hijack This

Kebutuhan Projek:

- Sebuah computer yang menjalankan Windows versi apa saja, dengan akses internet
- Privilege administrator pada komputer tersebut.

Perhatian! "Sebaiknya jangan menggunakan akses online shopping, personal e-mail, atau pekerjaan yang bersifat pribadi di dalam laboratorium" karena mahasiswa yang mengikuti mata kuliah ethical hacking bisa saja melakukan capturing passwords di labor FORESEC. Jika memungkinkan buat password baru hanya untuk digunakan di lab. Tidak ada yang bersifat pribadi yang dikerjakan di laboratorium!

Pemilihan Operating System

1. Jalankan komputer. Setiap komputer di lab. Foresec memiliki banyak Sistem Operasi virtual, dan saudara bisa menggunakan salah satunya.
2. Untuk projek ini, direkomendasikan menggunakan Windows 7 atau XP. Log in sebagai **Student tanpa** password.

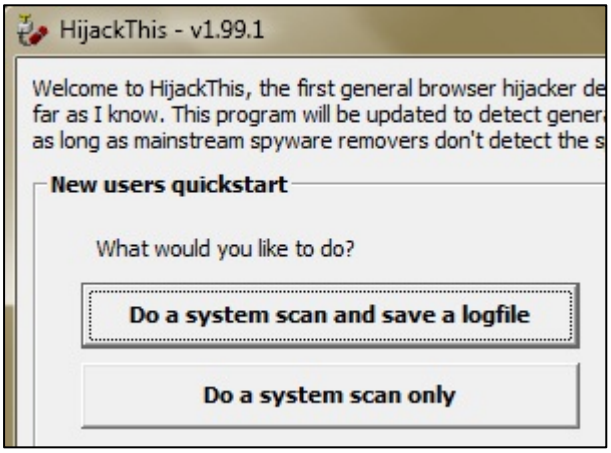
Menginstal HijackThis

3. Buka Firefox. Buka situs **majorgeeks.com**
4. Pada sisi kiri halaman, click **Anti-Spyware**.
5. Scroll ke bawah sampai setengah halaman dan cari **HijackThis**. Click link **HijackThis**. Click salah satu link pada bagian **DOWNLOADS** dan ikuti petunjuk pada layar untuk mendownload HijackThis. Jika download tidak mulai, periksa apakah NoScript membloknya. Jika terlihat pesan "**Scripts Currently Forbidden**" di jendela bawah Firefox, click tombol **Options** kemudian "***Temporarily Allow All This Page***".
6. Simpan file **hijackthis_sfx.exe** ***di desktop***.
7. Minimize semua jendela. Pada desktop, klik kanan file **hijackthis_sfx.exe** dan click "**Run as Administrator**".
8. Pada kotak "Open File – Security Warning", click **Run**.
9. Pada kotak "User Account Control", click **Yes**.
10. Pada kotak "WinZip Self-Installer", click **Unzip**. Kotak pops up akan tampil "1 file(s) unzipped successfully". Click **OK**. Tutup kotak "WinZip Self-Installer".

Menjalankan HijackThis

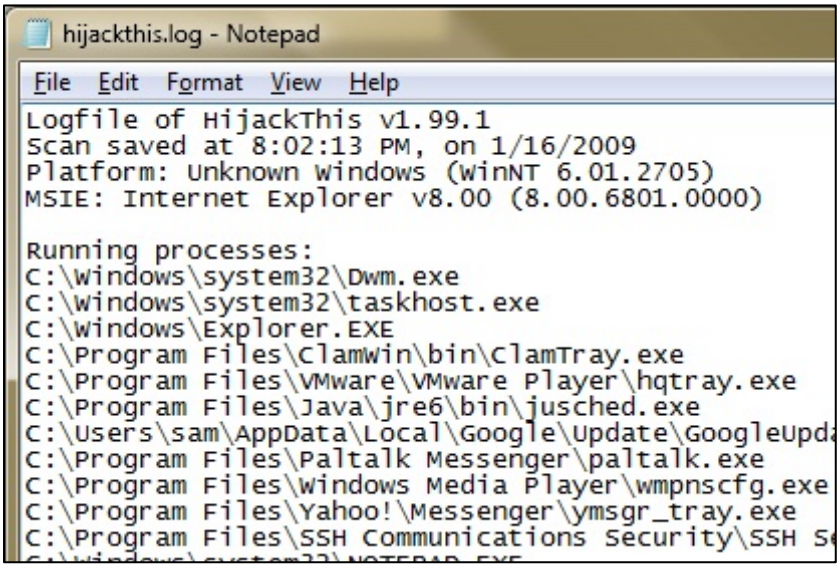
11. Click **Start**, **Computer**. Double-click pada drive **C:** untuk membukanya. Jika tidak Nampak file atau folder, click "Show contents".
12. Double-click folder "**Program Files**".
13. Double-click folder "**HijackThis**".
14. Klik kanan file "**HijackThis.exe**" dan click "**Run as Administrator**".
15. Pada kotak "User Account Control", click **Yes**.

16. Kotak pops up **HijackThis** dengan pesan berupa peringatan. Baca dan click **OK**.
17. Kotak **HijackThis akan tampak**, seperti terlihat pada gambar sebelah kanan. Click tombol "**Do a system scan and save a logfile**" button.



Menganalisa file log HijackThis.de

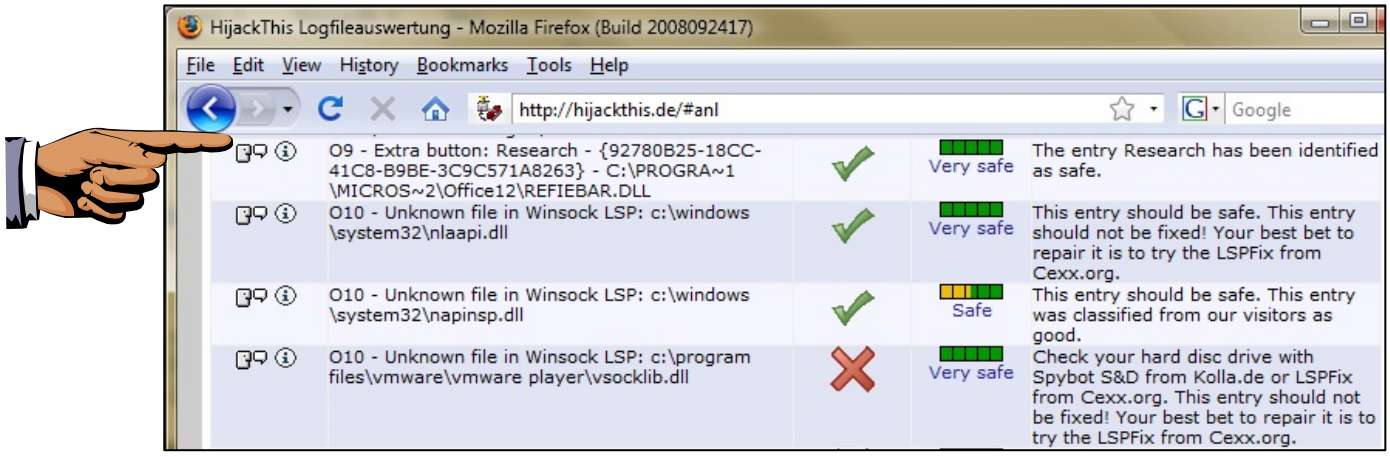
18. Logfile akan tampak di Notepad, dengan daftar processes dan registry keys, seperti pada gambar sebelah kanan. Daftar ini agak sulit dimengerti, kita bisa menggunakan free online tool untuk menterjemahkannya.
19. Pada jendela, buka website **hijackthis.de**
20. Pada jendela bagian bawah Firefox, akan tampak pesan "**Scripts Partially Allowed**". Click tombol **Options** dan click "***Allow hijackthis.de***".



21. Halaman akan di reload, dan kemudian pesan "**Scripts Partially Allowed**"akan kembali tampak, tapi tidak masalah karena scripts yang kita butuhkan berasal dari hijackthis.de.
22. Click pada jendela Notepad lihat file log. Tekan Ctrl+A untuk memilih semua text, dan Ctrl+C untuk mengkopinya ke dalam Clipboard.
23. Pada jendela Firefox, di halaman **hijackthis.de**, arhkan ke kotak besar berjudul "**You can paste a logfile in this textbox**". Klik kanan dan click **Paste**. Maka text akan Nampak di kotak tersebut.
24. Pada halaman **hijackthis.de**, di bagian bawah, click tombol **Analyze**.
25. Maka akan terlihat daftar list yang ada di komputer saudara, dengan grafik rating tip item keamanan, seperti Nampak di bawah ini. Hal ini sangat penting ketika kita ingin membersihkan spyware pada komputer terinfeksi!

Menyimpan Screen Image

26. Pastikan halaman web hijackthis.de masih terbuka, yang menampilkan beberapa items dari komputer saudara dengan rating keamanan.



27. Tekan tombol **PrintScrn** di sisi kanan atas keyboard. Dengan demikian akan mengkopi seluruh desktop ke dalam clipboard.
28. Click **Start**. Type **PAINT** dan click **Paint**. Click pada jendela **untitled - Paint** dan tekan **Ctrl+V**.
29. Simpan gambar dengan nama file **NamaKamu_Proj2**. Pilih **Save as type** sebagai **JPEG** atau **IMG.**
30. Kirim gambar tadi melalui elearning.

Last Modified: 2-10-12