
KNOW.YOUR.ENEMIES
UNIX.SECURITY
60.H4CK.YOVRS3LF
PROTECT.YOUR.NETWORK.FROM.BLACKHAT
FULL.DISCLOSURE_BUG.TRACKING

JIM GEOVEDI
{jim.geovedi@UNIX.NET}

- Orang **INDONESIA** biasa!
- Information Security Engineer
  Sering jadi **SATPAM** kalau kepepet
- **Natural Born Junker**
  Udah gak tau mo ngapain lagi di Internet(tm)
- Pendukung gerakan OpenSource
  FreeBSD & OpenBSD developer - port maintainer
- "will**hack**for**bandwidth**"
- ...

UNIX SECURITY?

COREBSD
DIGITAL RESEARCH GROUP

- Beberapa anggapan yang kurang benar mengenai Unix Security:
  - ''Secure by default'', karena menggunakan Linux, FreeBSD, OpenBSD, Solaris, etc..
  - Tidak ada virus, worm, dan trojan di Unix
  - Ribet, euy!

BASIC HOST SECURITY

COREBSD
DIGITAL RESEARCH GROUP

- Security Layers
  - Perimeter security
  - System security
  - Kernel security

PERIMETER SECURITY

- Problems:
  - Unauthorized access
    - Portscanning
  - Unauthorized program access
    - Miskonfigurasi aplikasi/service remote
    - Eksploitasi aplikasi secara remote
  - Denial of Service attacks

PERIMETER SECURITY (CONT.)

- How to protect yourself
  - Disable/turn-off service yang tidak dibutuhkan
    Services yang tidak dibutuhkan secara fungsional sebaiknya dinonaktifkan seperti: identd, named, rpc.statd, httpd, ftpd, etc.
  - Portsentry
    - Melakukan monitoring koneksi port untuk menghentikan portscanning dan aktifitas berbahaya lainnya.
    - http://www.psionic.com/
  - Menggunakan firewall sebagai kontrol akses
    Linux: iptables, ipchains
    FreeBSD: ipfw, IPF, PF
    OpenBSD: PF
    NetBSD: IPF
    Solaris: IPF

SYSTEM SECURITY

- Problems:
  - Vulnerable applications
    - SUID/SGID programs
  - Vulnerable libraries
    - LibSafe

SYSTEM SECURITY (CONT.)

- How to protect yourself
  - Hanya menginstal program yang benar-benar/akan dibutuhkan
  - Meningkatkan “security value” pada services
    - snmp
    - tcpwrappers (/etc/hosts.allow dan /etc/hosts.deny)
    - content filtering pada proxy dan mailserver

SYSTEM SECURITY (CONT.)

COREBSD DIGITAL RESEARCH GROUP

- How to protect yourself (cont.)
  - Hostsentry
    - Masih dalam taraf pengembangan
    - mengatur user login berdasarkan kebutuhan
    - http://www.psionic.com/
  - SUID/SGID files
    - file yang dapat dieksekusi dengan privilege “user” yang terbatas tanpa harus menjadi “user” tersebut
      contoh: sendmail, password, traceroute, ping
    - Mencari dan menghilangkan SUID/SGID file

```
# find / type f \( -perm -04000 -o -perm -02000 \) -exec ls -lg {} \;
# chmod -s /usr/sbin/whatever
```

KERNEL SECURITY

- Problems:
  - executable stack
  - ptrace race conditions
  - More info:
    http://www.securityfocus.com/infocus/1539
- How to protect yourself
  - Selalu menggunakan kernel versi STABLE terakhir
  - Apply security patches
  - Konfigurasi kernel
  - Build dan install kernel

KERNEL SECURITY (CONT.)

- Menggunakan kernel versi STABLE terakhir
  - Linux: http://www.kernel.org/pub/linux/kernel/
  - *BSD: cvsup, cvs, sup
- Security patch
  - Linux
    grsecurity - http://www.grsecurity.net/
  - OpenBSD:
    Stephanie - http://www.innu.org/~brian/Stephanie/

KERNEL SECURITY (CONT.) - GRSECURITY

COREBSD DIGITAL RESEARCH GROUP

- grsecurity patch pada kernel Linux
  - extract source kernel Linux

    ```
    # cd /usr/src
    # tar -zxvf .../linux-2.4.X.tar.gz
    ```
  - kernel patching

    ```
    # patch -p0 < .../grsecurity-1.9.X-2.4.X.patch
    ```
  - kernel configuration

    ```
    # cd /usr/src/linux
    # make menuconfig
    ```
  - lakukan konfigurasi seperti biasanya sampai pada option grsecurity
    - Aktifkan semua options kecuali “Gcc trampoline support”
    - Access Control Lists
      - Disable grsecurity ACL system
    - Aktifkan semua option “Filesystem protection”
    - Kernel Auditing
      - Disable “Single group for auditing”
      - Aktifkan semua options kecuali "Exec logging", "Chdir logging", dan "Signal logging"

KERNEL SECURITY (CONT.) - GRSECURITY

-
  - Executable Protections
    - Aktifkan semua options kecuali "Limit UID/GID changes to root", "Fork-bomb protection", Trusted path execution, dan "Allow ptrace for group"
  - Network Protections
    - Aktifkan semua options kecuali "Socket restrictions"
  - Sysctl support
    - Aktifkan "sysctl support"
  - Lain-lain
    - Disable "BSD-style coredumps"
  - Compile kernel

```
# make dep
# make bzImage
# make modules
```

  - Install kernel baru

```
# make modules_install
# cp arch/i386/boot/bzImage /boot/
# edit your lilo.conf and run /sbin/lilo
# reboot
```

SECURE USER ACCESS

- SUDO (SuperUser Do)
  - Unix “Freeware” (lisensi BSD)
  - Maintainer: Todd C. Miller
    Todd.Miller@courtesan.com
  - Informasi dan download - http://www.sudo.ws/
  - Mendukung hampir semua Unix flavors
  - Memungkinkan melakukan proses authentikasi tanpa harus menggunakan password superuser (root)

SECURE USER ACCESS (CONT.)

COREBSD DIGITAL RESEARCH GROUP

- Mengapa butuh SUDO?
  - Mempunyai akses root adalah hal yang berharga atau tidak ada gunanya sama sekali
  - Jika memiliki banyak admin/staff, tidak perlu menyebarkan password root
  - Dapat dikustomisasi sehingga user hanya dapat menjalankan program tertentu saja

SECURE USER ACCESS (CONT.)

```
# visudo
   ...
   # User privilege specification
   root    ALL=(ALL) ALL
   %wheel  ALL=(ALL) ALL
   ...

$ grep ^wheel /etc/group
wheel:*:0:root,user

$ sudo tcpdump
Password: paswertnuaingtea
tcpdump: WARNING: en0: no IPv4 address assigned
tcpdump: listening on en0
^C
```

FIREWALL

- Apa yang sebuah firewall dapat lakukan?
  - Translasi IP address
  - Port forwarding yang fleksibel
  - Mendukung multi-DMZ
  - Routing yang fleksibel untuk VPN
  - Kombinasi packet-filtering dengan load-balancing

FIREWALL (CONT.) - IPTABLES

- Prinsip iptables yang mendasar:
  - iptables adalah bagian dari netfilter: kernel dan user-level tools
    http://www.netfilter.org/
  - iptables terintegrasi pada kernel Linux versi 2.4, menggantikan ipchains (2.2) dan ipfw (2.0)
  - “Tables” terdiri dari “chains”, “chains” terdiri dari “rules”, “rules” mencocokkan setiap “packet” dan memberlakukan aturan yang sesuai (policy)

FIREWALL (CONT.) - IPTABLES

COREBSD DIGITAL RESEARCH GROUP

- Fitur netfilter/iptables:
  - Mangling: memodifikasi header dan menandai setiap packet
  - Network Address Translation (NAT): menulis-ulang “from” dan “to” alamat
  - Filtering: Memutuskan packet mana yang boleh “lewat” dalam kondisi tertentu

FIREWALL (CONT.) - IPTABLES - NAT

COREBSD DIGITAL RESEARCH GROUP

- NAT? Untuk apa?
  - Menyembunyikan private address
  - Mengurangi jumlah public address yang dibutuhkan
  - Membuat pemetaan “one-to-many” dan “many-to-one” antara box yang ada dibelakang firewall dengan external address
  - Solusi bagi masalah seputar routing
  - Tipe NAT:
    - destination NAT: mengubah baris “to” dari packet
    - source NAT: mengubah “from” dari packet

FIREWALL (CONT.) - IPTABLES - MANGLE

COREBSD DIGITAL RESEARCH GROUP

- Memodifikasi atau menandai setiap packet
  - Selalu didahulukan sebelum proses translasi address dan filtering
  - Built-in chains (versi kernel linux 2.4.18):
    - PREROUTING: untuk semua packet masuk
    - FORWARD: untuk semua packet yang di-forward
    - INPUT: untuk semua packet yang ditujukan pada firewall atau hosts dibelakang firewall
    - OUTPUT: untuk semua packet yang berasal dari firewall atau hosts dibelakang firewall
    - POSTROUTING: untuk semua packet yang keluar

FIREWALL (CONT.) - IPTABLES - NAT

- Melakukan dan mengkonfigurasi NAT
- Dilakukan setelah proses mangle
- Build-in “chains”:
  - PREROUTING: untuk setiap packet yang datang ke target NAT
  - OUTPUT: meneruskan “destination” dari firewall
  - POSTROUTING: untuk mengatur source NAT pada network packets

FIREWALL (CONT.) - IPTABLES - SAMPLE 01

COREBSD DIGITAL RESEARCH GROUP

- Block semua koneksi "inbound" WAN
  - Asumsikan bahwa eth0 adalah LAN dan eth1 adalah WAN (DSL/Cable) – gunakan ppp0 untuk dialup
  - LAN addresses adalah 192.168.X.Y dan firewall adalah 192.168.1.1
  - Buat sebuah "chain" untuk memfilter "packet state":

```
iptables -N block
iptables -A block -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A block -m state --state NEW -i ! eth1 -j ACCEPT
iptables -A block -j DROP
```

  - Link ke "chain"

```
iptables -A INPUT -j block
iptables -A FORWARD -j block
```

FIREWALL (CONT.) - IPTABLES - SAMPLE 02

COREBSD DIGITAL RESEARCH GROUP

- Selektif terhadap ports
  - Block koneksi dari eth1 pada ports tertentu (masukkan rules baru 1 dan 2 pada input chains)

```
iptables -I INPUT 1 --dport 0:1023 -i eth1 -p tcp -j DROP
iptables -I INPUT 2 --dport 0:1023 -i eth1 -p udp -j DROP
```

  - Ijinkan koneksi web untuk masuk

```
iptables -I INPUT 1 --dport 80 -p tcp -i eth1 -j ACCEPT
```

  - Ijinkan koneksi ssh dari host yang dipercaya

```
iptables -I INPUT 1 --dport 22 -p tcp -s 123.45.67.89 -j ACCEPT
```

FIREWALL (CONT.) - IPTABLES - SAMPLE 03

- IPv4 routing
  - Sebagai root, lakukan
    ```
    # echo 1 > /proc/sys/net/ipv4/ip_forward
    ```
  - Gunakan private IP subnets (192.168.X.Y, 172.16.X.Y, 10.X.Y.Z)
  - Non-aktifkan dengan
    ```
    # echo 0 > /proc/sys/net/ipv4/ip_forward
    ```

FIREWALL (CONT.) - IPTABLES - SAMPLE 04

COREBSD DIGITAL RESEARCH GROUP

- Masquerading
  - Membuat masquerading untuk "outbound connections" ke "dynamic WAN address"

```
iptables -t nat -A POSTROUTING -o eth1 -s 192.168.0.0/16 -j \
MASQUERADE
```

  - Membuat masquerading untuk "outbound connection" ke "static address 12.34.56.78"

```
iptables -t nat -A POSTROUTING -o eth1 -s 192.168.0.0/16 \
-j SNAT --to 12.34.56.78
```

  - MASQUERADE "melupakan" koneksi jika WAN down, sementara SNAT tidak
  - Kesalahan umum yang berakibat fatal

```
iptables -t nat -A POSTROUTING -j MASQUERADE
```

    bekerja dari LAN, namun mengijinkan outsider untuk melakukan masquerading melalui firewall Anda

FIREWALL (CONT.) - IPTABLES - SAMPLE RULE


```
iptables -t filter -F
iptables -t nat -F
iptables -t filter -X noext 2>/dev/null

ETH1=203.77.222.241
iptables -t filter -P FORWARD DROP
iptables -t filter -I FORWARD -s 10.200.10.0/24 -i eth1 -j DROP
iptables -t filter -N noext
iptables -t filter -A noext -i eth1 -j REJECT --reject-with icmp-port-unreachable
iptables -t filter -A INPUT -p tcp --dport 515 -j noext
iptables -t filter -A INPUT -p tcp --dport 23 -j noext
iptables -t filter -A INPUT -p tcp --dport 21 -j noext
iptables -t filter -A INPUT -p tcp --dport 25 -j noext
iptables -t filter -A INPUT -p tcp --dport 53 -j noext

iptables -t filter -A FORWARD -i eth0 -s 10.200.10.0/24 -j ACCEPT
iptables -t filter -A FORWARD -p tcp -d 10.200.10.17 --dport 22 -j ACCEPT
iptables -t filter -A FORWARD -p tcp -d 10.200.10.13 --dport 22 -j ACCEPT
iptables -t filter -A FORWARD -p tcp -d 10.200.10.5 --dport 22 -j ACCEPT
iptables -t nat -A POSTROUTING -d 192.168.0.0/16 -j SNAT --to 192.168.14.4
iptables -t nat -A POSTROUTING -s 10.200.10.0/24 -o eth1 -j SNAT --to $ETH1
iptables -t nat -A PREROUTING -p tcp -d $ETH1 --dport 221 -j DNAT --to 10.200.10.17:22
iptables -t nat -A PREROUTING -p tcp -d $ETH1 --dport 222 -j DNAT --to 10.200.10.13:22
iptables -t nat -A PREROUTING -p tcp -d $ETH1 --dport 223 -j DNAT --to 10.200.10.5:22
iptables -t filter -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

FIREWALL (CONT.) - IPTABLES - MORE INFO

- Netfilter

  `http://www.netfilter.org/ - http://www.iptables.org/`

- IPTABLES tutorial

  `http://www.linuxvoodoo.com/resources/howtos/iptables-tutorial/`

- Packet Filtering HOWTO

  `http://www.netfilter.org/documentation/HOWTO/packet-filtering-HOWTO.html`

- IP Masquerading HOWTO

  `http://www.e-infomax.com/ipmasq/howto/c-html/`

TCPDUMP

- “packet capture” adalah pengumpulan data secara “real-time” yang menjelajahi sebuah jaringan
- “packet” adalah pesan yang terenkapsulasi dalam berbagai header yang menggunakan protokol IP untuk berkomunikasi
- tcpdump adalah tool yang mampu melakukan “capturing data”

TCPDUMP (CONT.)

COREBSD
DIGITAL RESEARCH GROUP

- basic usage:

```
# tcpdump
23:29:04.050167 gorilla.3224 > monyet.6020: . ack 36517 win 16044
23:29:04.059645 monyet.6020 > gorilla.3224: P 36517:37969(1452) ack 1 win
5840 (DF)
23:29:04.092955 orangutan.netbios-ns > simpanse.netbios-ns: nbt-query-req-
bcast
23:29:04.093587 orangutan.netbios-ns > simpanse.netbios-ns: nbt-query-req-
bcast
```

- mengambil contoh data:

```
# tcpdump > textfile
```

atau

```
# tcpdump | tee textfile
```

- menyimpan data capture ke format tcpdump binary

```
# tcpdump -w binaryfile &
```

membaca kembali file binary tersebut

```
# tcpdump -r binaryfile
```

TCPDUMP (CONT.)

- intermediate usage:

  # tcpdump -i en0 -c 100 -s 400

  mengcapture 100 packets dan mengambil 400 bytes dari setiap packet-nya pada NIC en0

- mengambil informasi mac address:

```
 # tcpdump -qec1
00:57:06.154240 0:a0:4d:3:e0:1d 0:50:be:2b:44:8f 60: gorilla.4454 >
orangutan.ssh: tcp 0

# tcpdump -qec1 -x
01:04:18.762895 0:50:ba:2b:44:8f 0:a0:4b:3:e0:1d 118: orangutan.ssh >
gorilla.4454: tcp 64 (DF) [tos 0x10]
                         4510 0068 ca56 4000 4006 ec92 c0a8 011e
                         c0a8 0128 0016 1166 fe89 6677 1140 5338
                         5018 4470 9250 0000 3b6e e13e c39e cebe
                         6ad5 5a78 8d62 090c 7dcf e1f1 37e0 9f64
                         1c54 0ef7 8534 1ec9 0240 d02d c8a1 e54b
                         fa3b
```

- address filtering

  # tcpdump host gorilla

  # tcpdump dst host simpanse

  # tcpdump src host orangutan

TCPDUMP (CONT.)

- protocol filtering

```
# tcpdump udp
```

- port filtering

```
# tcpdump port 22
```

- compound filtering

```
# tcpdump not port 22
# tcpdump not port 22 and host gorilla
# tcpdump not (port 22 and host gorilla and host simpanse)
# tcpdump not “(port 22 and host gorilla and host simpanse)”
```

- whoooaaaahhhh....!!!!

```
# tcpdump -i en0 -nq \
      not "(port 22 and host gorilla)" \
      and not "(port 53 or 80 or 110 or 119 or 443)" \
      and dst host 203.77.222.242
```

COREBSD
DIGITAL RESEARCH GROUP

Question?

jim.geovedi@UNIX.NET
negative (irc.efnet.nl) - http://corebsd.or.id/