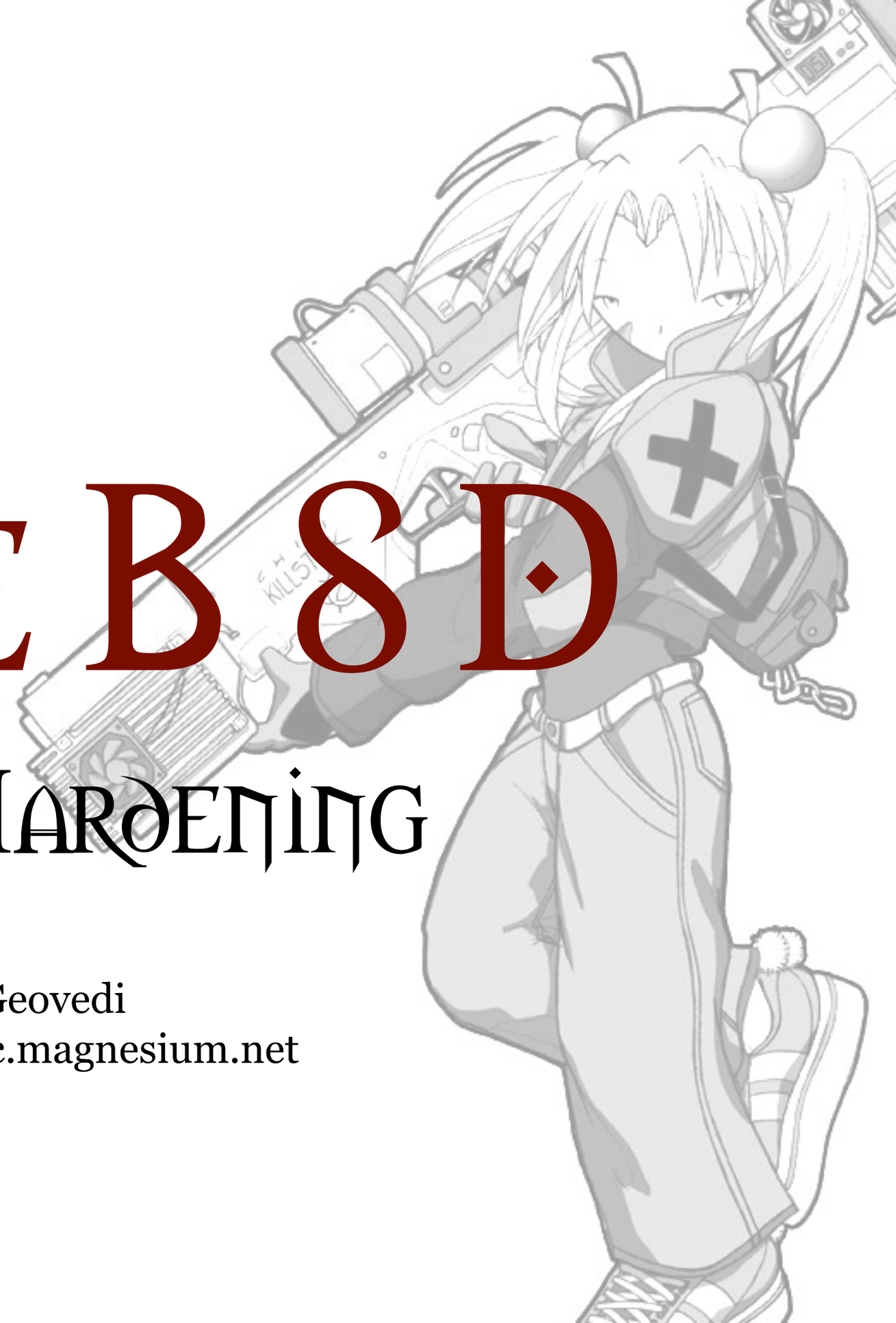
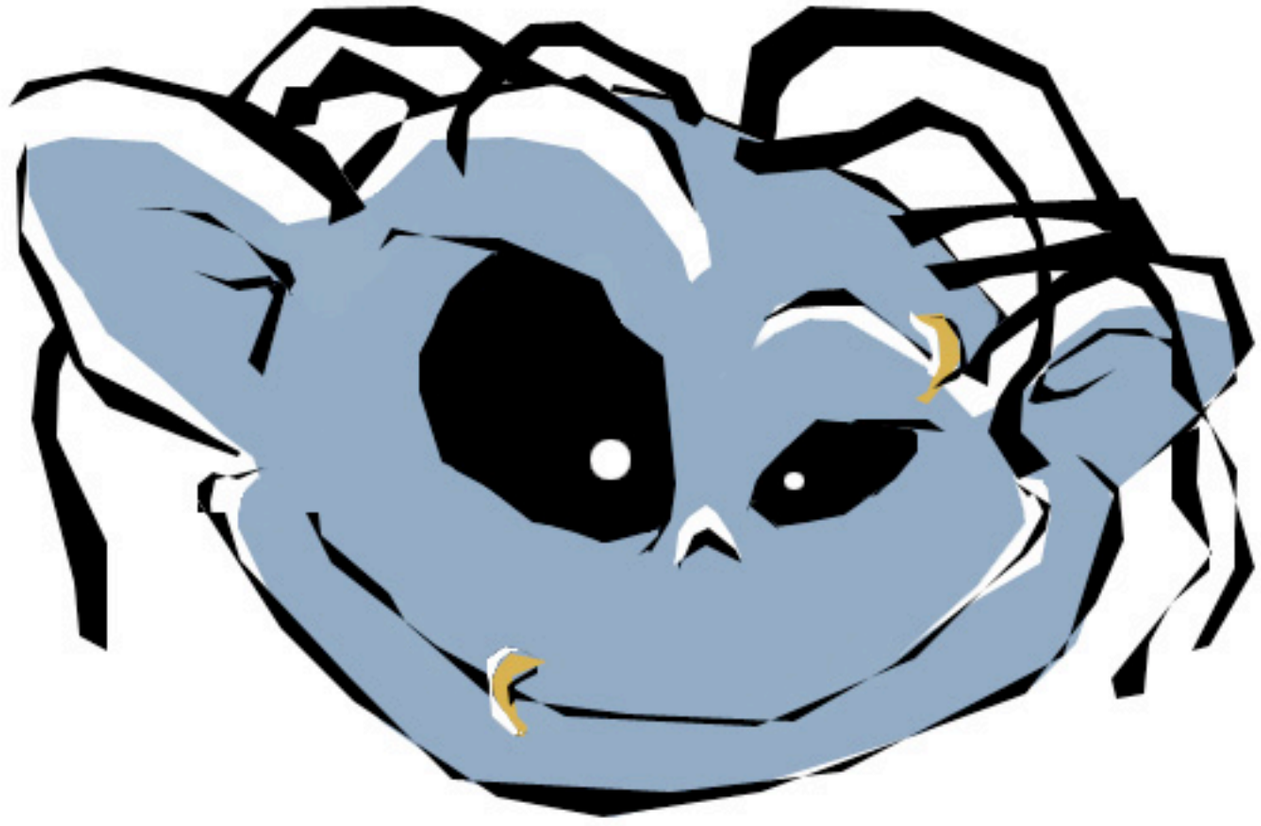
FreeBSD

System Hardening



Jim Geovedi
negative@toxic.magnesium.net



hello, humans!

FOKUS PRESENTASI

- *System Hardening* FreeBSD OS untuk digunakan dalam lingkungan produksi.
- Tips dan trik seputar FreeBSD *Security*.

PERLU DIINGAT!

- Selalu membuat **BACKUP** sebelum melakukan segala sesuatunya.

BASIC SYSTEM HARDENING

BASIC SYSTEM HARDENING

- Gunakan selalu FreeBSD versi **STABLE**
- Jangan menjalankan *services* yang tidak perlu.
  lihat /etc/inetd.conf, /etc/rc.conf

SERVICES PROTECTION

SERVICES PROTECTION

- Gunakan chroot(8) atau jail(8) untuk menjalankan program-program yang berisiko *vulnerable*.
- Memfilter setiap akses terhadap *services* menggunakan Firewall atau *Packet Filtering software* seperti ipfw atau IPF (ipfilter).
- Aktifkan *option* log_in_vain="YES" untuk melihat koneksi ke port-port TCP/UDP yang tidak menjalankan *services*.

SECURE LOGGING

SECURE LOGGING

- Non-aktifkan syslogd *logging* ke mesin *remote*.
  gunakan *option* "-s -s"

- Pastikan pada /etc/syslog.conf terdapat:

```
security.*      /var/log/security
ftp.*           /var/log/ftpd.log
auth.*          /var/log/auth.log
```

- Aktifkan ipfw atau IPF *logging* pada /etc/syslog.conf

BOFH

(BASTARD OPERATOR FROM HELL)

B O F H

(BASTARD OPERATOR FROM HELL)

- Gunakan AllowUsers/AllowGroups pada konfigurasi SSH untuk menentukan siapa saja user yang dapat login menggunakan SSH.

- Gunakan *tcp wrappers* untuk mengijinkan atau melarang akses pada *tcp-based services*.

- Berikan *shell* /sbin/nologin pada user yang hanya membutuhkan akses ftp.

- Lakukan *user accounting*.
  accounting_enable="YES"

LOCKING-DOWN FILESYSTEM

LOCKING-DOWN FILESYSTEM

- Selalu membuat beberapa partisi.
- *Mount* semua partisi kecuali /usr dengan argument 'nosuid'
- Hilangkan *suid bits* pada binary yang tidak digunakan (seperti pada UUCP *binary files*)
- Gunakan chflags dengan variable sappnd pada *logfiles*, dan schg pada *binary files*.

```
# ls -lo /usr/bin/su
-r-sr-x---  1 root  wheel  schg 8200 May  1 09:37 /usr/bin/su
```

KERNEL SECURELEVELS

KERNEL SECURELEVELS

- Variable *kernel securelevels* menunjukkan level security.
- *Value* antara '-1' sampai '3', dan '0' adalah 'insecure mode'.
- *Securelevel* hanya dapat meningkat nilainya, dan tidak dapat turun pada *multiuser mode*.
- *Securelevel* dikontrol menggunakan sysctl(8) dan sysctl.conf(5).

KERNEL SECURELEVELS

- **Securelevel 1** = *flag* sappnd dan schg tidak dapat diubah, *kernel module* tidak dapat di*load/unload*.
- **Securelevel 2** = securelevel 1 + tidak dapat menulis pada disk kecuali mount(2)
- **Securelevel 3** = securelevel 2 + ipfw *rules* tidak dapat dimodifikasi

KERNEL STATES CONTROL
&
SYSTEM CONFIGURATION

sysctl & rc.conf

- net.inet.tcp.blackhole=2, net.inet.udp.blackhole=1 untuk tidak membuat RST pada *portscan*
- kern_securelevel_enable="YES", kern_securelevel="?" # range: -1..3;
- icmp_drop_redirect="YES"
- fsck_y_enable="YES"

SECURE REMOTE CONNECTIONS

SECURE REMOTE CONNECTIONS

- Non-aktifkan telnet, dan r* commands, gunakan SSH atau OpenSSH sebagai pengganti
- Gunakan sftp sebagai pengganti ftp
- Gunakan otentifikasi *pubkey* pada SSH
- Pertimbangkan kembali penggunaan OTP (*One-Time-Password*)

FIREWALL / PACKET FILTERING

FIREWALL / PACKET FILTERING

- Sebuah firewall dapat:
  - melakukan deny/permit packets
  - membedakan rules setiap interfaces

FIREWALL / PACKET FILTERING

- Software yang dapat digunakan:
  - ipfw (IPFirewall):

options IPFIREWALL	enable ipfw
options IPFIREWALL_VERBOSE	enable firewall logging
options IPFIREWALL_VERBOSE_LIMIT	limit firewall logging
options IPDIVERT	enable divert(4) sockets

  - IPF (IPFilter):
    http://coombs.anu.edu.au/~avalon/
  - PF (PacketFilter):
    http://pf4freebsd.love2party.net/

SECURITY CHECKS

SECURITY CHECKS

- nmap, *swiss-army knife, err network mapper ;)*
  http://www.insecure.org/nmap/

- snort, *Lightweight network intrusion detection system*
  http://www.snort.org/

- tripwire, *Filesystem security & verification program*
  http://www.tripwire.org/

- chkrootkit, memeriksa apakah terdapat rootkit pada *local system*.
  http://www.chkrootkit.org/

- dsniff, monkey watch monkey sniff
  http://www.monkey.org/~dugsong/dsniff/

WHAT'S NEXT?

What's Next?

- FreeBSD Security web page:
  http://www.freebsd.org/security/security.html
- FreeBSD Security How-To:
  http://people.freebsd.org/~jkb/howto.html
- FreeBSD Security advisories:
  ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/
- FreeBSD Hardening Project:
  http://www.watson.org/fbsd-hardening/

What's next?

- FreeBSD ipfw howto:
  http://www.freebsd-howto.com/HOWTO/Ipfw-HOWTO
- IPF (ipfilter) howto:
  http://www.obfuscation.org/ipf/ipf-howto.html
- Cerb, security kernel module:
  http://cerber.sourceforge.net/
- Packetstorm Defense Tools:
  http://packetstormsecurity.nl/defense.html

ACKNOWLEDGMENTS

- **CoreBSD**, “will hack for bandwidth”
- **BHC Community**, “Iblis imut doyan MMX”
- **Universitas Katolik Parahyangan**
- **C2FORCE@Dago374**, “we make IT simple”
- #indofreebsd/dalnet, id-freebsd@yahoogroups.com

THE END

GOT ROOT, err QUESTION ?