Server Management

Josua M Sinambela
CompTIA Security+, CCNA

Workshop Server Management, 28 Agustus 2007
PPTIK UGM, Yogyakarta

josh at gadjahmada edu
http://josh.staff.ugm.ac.id

Pembahasan

- Sistem Operasi Server
- OS Hardenings
  - Linux Hardening
  - BSD Hardening
  - Windows Hardening
- Apache Web Server dan Aplikasi Web
  - Keamanan Apache Web server
  - Aplikasi Web berbasis PHP
  - Teknik Backup Konten

Pembahasan (cont)

- Mail Server
  - Mail Transfer Agent (MTA)
  - Keamanan Mail Server
    - Open Relay, Anti Spam, Anti Virus
    - Menggunakan SSL/TLS pada Mail
  - Backup Mail Server
- DNS Server
  - Layanan DNS
  - Keamanan DNS Server

Sistem Operasi Server

- Open Source Based OS
  - Unix : FreeBSD, OpenBSD, NetBSD, OpenSolaris, OpenDarwin
  - Linux (Distro: Redhat, Fedora, Debian, Slackware, Ubuntu, Mandriva, SuSe, Mikrotik)
- Proprietary OS
  - Microsoft Windows : WinNT, Win2000, Win2003
  - SunOS

Anda pakai yang mana ? Perlu diingat untuk keamananan Server, semua bergantung pada administrator.

"man behind the gun"

OS Hardening : Linux Hardening

- Dimulai saat pemilihan Distro dan menyiapkan CD Installer OS tersebut
- Partisi Hardisk (/tmp /var /home /boot)
  - Gunakan opsi noexec, nodev, nosuid, usrquota
- Install paket minimal & up date
  - Jangan menginstall paket yang tidak digunakan
  - SysAdmin =! Newbie
- Gunakan policy untuk user system & password.
- Disable services yang tidak digunakan.
- Remote Login Hardening
  - Gunakan SSH (protokol SSH v 2)
  - Aktifkan hanya untuk user tertentu (allowusers, allowgroups)
  - Gunakan TCPwrapper sebagai lapisan keamanan

OS Hardening : Linux Hardening (cont)

- Proteksi Bruteforce attack untuk SSH (beberapa pilihan)
  - Gunakan Strong Password
  - Gunakan Otentikasi RSA (key based otentikasi)
  - Gunakan iptables rules
    - iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --set --name SSH -j ACCEPT
    - iptables -A INPUT -p tcp --dport 22 -m recent --update --seconds 60 --hitcount 4 --rttl --name SSH -j LOG --log-prefix "SSH_brute_force "
    - iptables -A INPUT -p tcp --dport 22 -m recent --update --seconds 60 --hitcount 4 --rttl --name SSH -j DROP
  - Gunakan log SSH untuk melakukan blocking
    - Sshfilter, Fail2Ban, DenyHosts
- Chroot(jail) untuk Layanan Aplikasi yang vulnerable

OS Hardening : Linux Hardening (cont)

- Setup Iptables sebagai Host Firewall
- Kernel Parameter
  - net.ipv4.tcp_syncookies = 1
  - net.ipv4.icmp_echo_ignoreb_roadcasts = 1
  - net.ipv4.conf.all.rp_filter = 1
  - net.ipv4.conf.all.accept_redirects = 0
  - net.ipv4.conf.all.accept_source_route = 0
- Install HIDS (Host Based Intrusion Detection System)
  - Samhain (http://la-samhna.de/samhain/)
  - AIDE (http://sourceforge.net/projects/aide)
  - TripWare (http://www.tripwire.com/)
- Advanced Security
  - SELinux http://www.nsa.gov/selinux/
  - Grsecurity http://www.grsecurity.net/index.php

OS Hardening : FreeBSD Hardening

- Proses Hardening mirip dengan Linux (sintaks/path yang berbeda)
- Tambahan
  - Pastikan OS sudah versi Stable (upgrade !!)
  - Gunakan Kernel Securelevel (-1 sampai 3)
  - Firewall
    - 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/

OS Hardening :
Windows 2000 Hardening

- Terapkan Account Procedure
  - Disable guest account
  - Configure Administrator account
  - Gunakan Strong Password
  - Account Lockout policy
  - Account Expiration
- Restrict Group membership
  - Buat group dengan fungsi kerja khusus
  - Policy membership yang jelas
- Restriction Permission
  - Pengamanan Registry
  - Pengamanan File Sharing
  - Pengamanan system informasi authority

OS Hardening :
Windows 2000 Hardening

- Restriction Executables
  - Gunakan appsec.exe (ada di Resource Kit)
  - AppSense Application Manager (Third Party Product)
- Software Restriction Policy
- Disable Service yang tidak digunakan (bukan sekedar di STOP)
- Microsoft Solution for Securing Win2000 Server (MSS Security)
- Security Tools (Resource Kit)
  - Xcacls , Auditpol, EventComb, NetLogon Debug

Apache Web Server

- Apache is well known Applications Server
- Open Source Code
- http://httpd.apache.org || Newest v2.2.4
- Tersedia : Windows/Unix/Linux

Apache Web Server Security

- Apache Web Server yang aman belum menjamin Security.
  - Aplikasi dan Coding yang berjalan diatasnya sangat menentukan.
  - Serangan terhadap Applikasi/Coding :
    - SQL Injection
    - Cross Site Scripting
    - Information Leakage
- Keamanan Apache web server menjadi lapisan keamanan dan dapat mempengaruhi pengkodean aplikasi (security)

Apache Web Server Security(cont)

- Keamanan pada httpd.conf
  - General Option
    - Userdir enable

      Userdir disable root
    - ServerTokens Prod
    - ServerSignature Off
  - Pengamanan Cross site Scripting
    - ReWriteEngine on
    - ReWriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
    - ReWrite .*-[F]

Apache Web Server Security(cont)

- Keamanan pada httpd.conf (cont)
  - Pembatasan Resource user apache
    - RlimitCPU
    - RlimitMEM
    - RlimitPROC
    - LimitRequestBody
    - LimitRequestFields
    - LimitRequestFieldSize
    - LimitRequestLine
  - Access Control
    - Order allow,deny
    - allow from all
    - deny from 222.124., .hacker.com
  - User Otentikasi (Basic, LDAP, Database dst)

Apache Web Server Security(cont)

- Apache Module
  - mod_ssl untuk HTTPS
- 3rd Party Apache Module
  - mod_security
  - mod_bandwidth atau mod_throttle
  - mod_evasive
  - mod_hackprotect
  - mod_parmguard
- More see : http://www.apachesecurity.net/about/links.html

Aplikasi Web berbasis PHP

- Tips proteksi aplikasi PHP melalui php.ini
  - safe_mode = On
  - register_globals = Off
  - magic_quote=On
  - display_errors = Off
  - disable_functions = phpinfo

Backup Content Web

- Backup ke Server Local Khusus Backup
- Gunakan tools ssh/scp dan archieve menggunakan tar –preserve
- Buat automatic script shell tar, scp/ssh dengan Pubkey Otentikasi
- Tools lain : http://linux.about.com/od/softbackup/Linux_Software_Backup_Solutions.htm

Mail Server

- MTA (Mail Transfer Agent)
  - Exim http://exim.org
  - Courier-MTA http://courier-mta.org
  - Postfix http://postfix.org
  - Qmail http://cr.yp.to/qmail.html
  - Sendmail http://sendmail.org
- Perbandingan MTA
  - http://shearer.org/MTA_Comparison
  - http://www.geocities.com/mailsoftware42/

Perbandingan MTA terbaru 2007

http://shearer.org/MTA_Comparison

MTA Suitability from 0 (bad) to 3 (good)					
if you are...	**qmail**	**Exim**	**Sendmail**	**Postfix**	**Notes**
Inexperienced	0	3	1	3	Exim and Postfix have good docs and clear examples
Worried about security	3	2	0	3	Postfix is secure and modern; qmail is secure but very old and cranky; Exim is secure to different criteria (read above.)
Relying on Sendmail milters	0	1	3	2	Postfix can run milters; can use equivalent Exim routers/filter script
Wanting minimum hassle	0	3	0	3	Sendmail has some easy front-ends, but the deeper you go the worse it gets. Postfix and Exim are more predictable.
Resource-constrained	3	2	1	2	See *Embedded Application* below for other comments
On Windows	0	2	3	0	Sendmail has a native Windows port; Exim is in the Cygwin distro
Needing commercial support	1	3	3	3	There are competent companies for all MTAs; qmail is inherently less supportable being so old

Keamanan Mail Server

- Serangan pada Mail Server
  - Mail Server Network
  - OS (Operating System)
  - Aplikasi Lawas (Buggy)
  - Proteksi Account mail yang lemah
  - Open Relay
  - Spam
  - Virus
  - Attachment (trojan)
  - Penyadapan (sniffing)
  - Altering (modification)

Keamanan Mail Server (Cont)

- Lokasi Mail Server (DMZ)
- Aplikasi MTA selalu mengikuti Patch|Update|Newest
- Disable Banner OS pada pesan Pop3, IMAP, SMTP
- Aktifkan SSL pada Pop3 dan IMAP dan Authentication pada SMTP (SMTP Auth)
  - Pop3 + SSL = Pop3s
  - IMAP + SSL = IMAPs
- Check Openrelay
  - RBL
  - Openrelay Online Checker
    - http://www.abuse.net/relay.html
    - http://www.antispam-ufrj.pads.ufrj.br/test-relay.html

Keamanan Mail Server (Cont)

- AntiSPAM
  - Tidak ada AntiSpam yang sempurna
  - Harus hati-hati dan banyak percobaan pada scoring SPAM
  - SpamAsassin.
  - Update !!
- AntiVirus
  - Memproteksi User pengguna Windows
  - Banyak pilihan antivirus
  - Clamav (Amavis)

DNS Server

- Komunikasi Jaringan berbasis IPAddress
- Memetakan Domain ←→ IP Address
- Menggunakan system database terdistribusi dengan Hirarki.
- Manfaat DNS
  - Nama domain lebih mudah diingat (convenience)
  - Nama domain relatif jarang di rubah, IP address bisa saja berubah (consistency)

Keamanan DNS Server

- Serangan pada Domain Name System
  - Footprinting
  - Redirection
  - Denial of Service (DoS)
  - Data modification/ IP spoofing
  - DNS cache poisoning

Keamanan DNS Server (cont)

- Mengamankan dari serangan DoS
  - Tidak memposisikan semua Name Server pada satu subnet.
  - Tidak memposisikan semua Name server dibelakang router yang sama.
  - Tidak memposisikan semua Name Server menggunakan jalur ISP/Internet yang sama.
  - Membuat server backup sebagai Slave Name server

Keamanan DNS Server (cont)

- Membatasi zone transfers untuk melindungi dari:
  - Orang lain yang memanfaatkan Resource Server DNS kita
  - Hacker/Cracker yang ingin mendapatkan listing content dari zona yang kita maintenance dengan tujuan
    - Identifikasi target (Mail & Name Server)
    - Mendapatkan informasi penting lainnya, spt Jumlah host, nama host, dll

Sekian

Q&A ?