Habilitando servidores Linux orientados a las PyMES

José Luis Hernández López
Georgina Pérez Hernández
Simbiótica Seguridad en Redes.
jhdz@simbiotica.net
http://www.simbiotica.net

Reconociendo la seguridad

- Muchas empresas cuando instalan un servidor en muchos de los casos no han hecho una planeación sobre los esquemas de seguridad a seguir, así pues algunos de los elementos a considerar son:
  - Los servicios que se requieren
  - Las políticas de seguridad a implementar

Los servicios

- Los servicios básicos que toda empresa necesita son:
  - Servidor de Web (http)
  - Servidor de Correo (smtp y pop3)
  - Servidor de DNS (bind)
  - Proxy
  - Administración Remota
  - Backup
  - Y servicios adicionales como:
    - Samba
    - Appletalk

Servidor Web (http)

- puerto 80
- Apache
- Cuenta con módulos de muy diversa índole
  - perl
  - php
  - python
  - tomcat (java servlets)
  - ssl

Servidor de Correo (smpt y pop3)

- Puerto 25 y 110
- La principal fuente de infección por virus proviene del correo, otro problema muy grande es el spam, las herramientas que nos pueden ayudar son:
  - Amavis puerto 10025 (amavis.sourceforge.net)
    - Spamassassin (http://spamassassin.apache.org)

Ejemplo de amavis

A L E R T A D E V I R U S

Nuestro viruschecker encontro un virus

EICAR test file

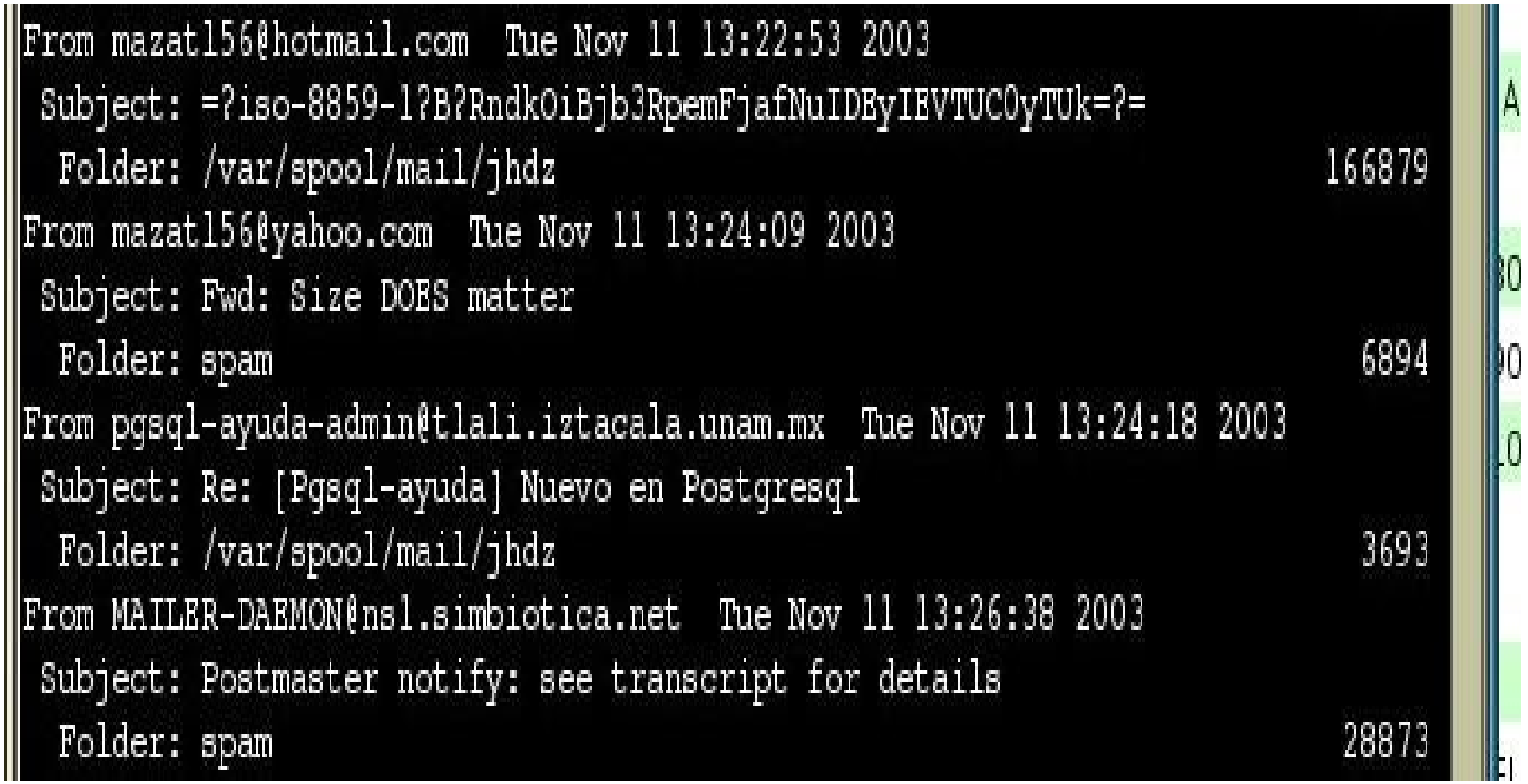
Los virus(es) se encontraron en las siguientes direcciones:

La entrega de su correo a sido detenida!!

Cheque que su computadora no tenga virus, o pregunte a su administrador de sistemas.

Para mayores referencias aqui están los encabezados de su mail:

Deteniendo el spam



Las políticas de seguridad a implementar

- En donde andan mis usuarios?
  - Squid (http://www.squid-cache.org)
  - Sarg (http://sarg.sourceforge.net)

Las políticas de seguridad a implementar

- Ejemplo de un reporte de sarg.

SARG Squid Analysis Report Generator

Reporte de uso de Internet

ARCHIVO/PERIODO	FECHA CREACION	USUARIOS	BYTES	PROMEDIO
31May2005-01Jun2005	Wed Jun 1 01:01:03 CST 2005	24	652.64M	27.19M
30May2005-31May2005	Tue May 31 01:01:01 CST 2005	22	741.30M	33.69M
29May2005-29May2005	Mon May 30 01:01:01 CST 2005	2	2.44K	1.22K
28May2005-28May2005	Sun May 29 01:01:01 CST 2005	4	4.44K	1.11K
27May2005-27May2005	Sat May 28 01:01:02 CST 2005	25	671.02M	26.84M
26May2005-26May2005	Fri May 27 01:01:02 CST 2005	22	479.37M	21.78M
24May2005-25May2005	Thu May 26 04:08:40 CST 2005	24	618.32M	25.76M
24May2005-24May2005	Wed May 25 01:01:02 CST 2005	18	15.13M	840.61K
08Jun2005-09Jun2005	Thu Jun 9 01:01:03 CST 2005	24	178.65M	7.44M
07Jun2005-08Jun2005	Wed Jun 8 01:01:02 CST 2005	21	671.90M	31.99M
06Jun2005-06Jun2005	Tue Jun 7 01:01:02 CST 2005	23	93.39M	4.06M
05Jun2005-05Jun2005	Mon Jun 6 01:01:01 CST 2005	3	1.27M	423.50K
04Jun2005-05Jun2005	Sun Jun 5 01:01:01 CST 2005	3	5.97M	1.99M
03Jun2005-03Jun2005	Sat Jun 4 01:01:02 CST 2005	22	146.69M	6.66M
02Jun2005-03Jun2005	Fri Jun 3 01:01:02 CST 2005	23	428.95M	18.65M
01Jun2005-02Jun2005	Thu Jun 2 01:01:02 CST 2005	24	493.15M	20.54M

Generado por sarg-2.0.7 May-02-2005 el 09/Jun/2005-01:01

Las políticas de seguridad a implementar

SARG Squid Analysis Report Generator

Reporte de uso de Internet

Período: 31May2005-01Jun2005
Clasificado por: BYTES, reverse
Topuser Reporte

Topsites Reporte
Sitios y Usuarios Reporte
Bajados Reporte
Denegado Reporte

NUM		USERID	CONEXION	BYTES	%BYTES	ENTRADA-CACHE-SALIDA		TIEMPO UTILIZADO	MILISEC	%HORA
1		192.168.0.45	2.31K	523.40M	80.20%	0.27%	99.73%	01:48:04	6.48M	32.22%
2		192.168.0.10	4.38K	44.03M	6.75%	2.46%	97.54%	00:35:22	2.12M	10.55%
3		192.168.0.1	1.50K	23.37M	3.58%	3.88%	96.12%	00:14:46	886.39K	4.40%
4		192.168.0.21	2.24K	12.76M	1.96%	8.00%	92.00%	00:15:43	943.77K	4.69%
5		192.168.0.19	2.52K	12.69M	1.94%	10.11%	89.89%	00:24:08	1.44M	7.20%
6		192.168.0.12	1.65K	8.64M	1.33%	6.74%	93.26%	00:31:01	1.86M	9.25%
7		192.168.0.47	1.69K	6.11M	0.94%	5.39%	94.61%	00:07:41	461.51K	2.29%

Las políticas de seguridad a implementar

SARG Squid Analysis Report Generator

Reporte de uso de Internet

Período: 31May2005-01Jun2005
Usuario: 192.168.0.45
Clasificado por: BYTES, reverse
Usuario Reporte

SITIO ACCEDIDO	CONEXION	BYTES	%BYTES	ENTRADA-CACHE-SALIDA		TIEMPO UTILIZADO	MILISEC	%HORA
liveupdate.symantecliveupdate.com	432	513.17M	98.04%	0.00%	100.00%	01:28:14	5.29M	81.65%
www.segundamano.com.mx	400	3.15M	0.60%	22.18%	77.82%	00:04:56	296.80K	4.58%
p.tradercom.es	363	2.54M	0.49%	9.82%	90.18%	00:04:49	289.61K	4.47%
www.autofoto.com.mx	160	1.23M	0.24%	5.76%	94.24%	00:01:48	108.66K	1.68%
www.gob.mx	247	671.33K	0.13%	15.38%	84.62%	00:00:45	45.84K	0.71%
www.cemex.com	34	379.42K	0.07%	0.00%	100.00%	00:00:12	12.32K	0.19%
www.economia.gob.mx	41	297.70K	0.06%	0.00%	100.00%	00:00:12	12.10K	0.19%
www.economia-snci.gob.mx	34	292.85K	0.06%	0.00%	100.00%	00:00:47	47.70K	0.74%
www.banorte.com	52	188.41K	0.04%	0.00%	100.00%	00:00:30	30.67K	0.47%
pagead2.googlesyndication.com	82	173.26K	0.03%	0.00%	100.00%	00:00:26	26.98K	0.42%
www.economista.com.mx	16	165.74K	0.03%	21.15%	78.85%	00:00:04	4.06K	0.06%
www.rafe.com.br	14	156.92K	0.03%	0.00%	100.00%	00:00:30	30.27K	0.47%
www.banamex.com	57	124.28K	0.02%	70.10%	29.90%	00:00:02	2.36K	0.04%
secure-uk.imrworldwide.com	167	105.16K	0.02%	8.40%	91.60%	00:02:13	133.18K	2.05%
www.delicato.com.br	10	98.71K	0.02%	0.00%	100.00%	00:00:21	21.55K	0.33%
br.i1.yimg.com	9	84.36K	0.02%	13.46%	86.54%	00:00:02	2.77K	0.04%
www.elasesor.com.mx	14	83.05K	0.02%	0.00%	100.00%	00:00:43	43.68K	0.67%
mx.search.yahoo.com	8	62.92K	0.01%	0.00%	100.00%	00:00:05	5.13K	0.08%
analesdemedicina.com	24	55.75K	0.01%	1.40%	98.60%	00:00:12	12.28K	0.19%
www.bancomext.com	2	50.88K	0.01%	0.00%	100.00%	00:00:09	9.93K	0.15%

Las políticas de seguridad a implementar

- Squid es un proxy sumamente versatil con el podemos definir que sitios son validos y que sitios no son validos para los usuarios que lo están utilizando.
- Squidguard tiene una lista de sitios porno de más de 100,000 entradas (http://www.squidguard.org)

Las políticas de seguridad a implementar

- Usar tcp wrappers
- El uso de iptables
  - Prevención de ataques de denegación de servicios (DoS)
  - Puertos disponibles
    - Msn
    - Yahoo
    - Icq
    - Redes p2p

Firewall Básico

- Filtro syn flood
  - echo "1" > /proc/sys/net/ipv4/tcp_syncookies
  - El syn flood es el envió de conecciones tcp más rápido de lo que la computadora lo puede procesar.
- Poner nuestro filtro antispoofin (http://www.fortunecity.com/westwood/calvin/275/tcpip/ipspoof.txt)
  - echo "1" >/proc/sys/net/ipv4/conf/eth0/rp_filter
- El spoofin es el intento de suplantar un host.

Firewall Básico

- Quien esta del otro lado?
- Si al dar un ping, no hay respuesta nuestro atacante puede quedar desconcertado
  - echo "1" >/proc/sys/net/ipv4/icmp_echo_ignore_all
- Protegiendo nuestro servidor de un icmp broadcast
  - echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts

Firewall Básico

- El ping de la muerte
  - echo "1" > /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses

Firewall Básico

- Modificando nuestro kernel para tratar de evitar un ataque DoS
  - echo "10" > /proc/sys/net/ipv4/tcp_fin_timeout
  - echo "1800" > /proc/sys/net/ipv4/tcp_keepalive_time
  - echo "0" > /proc/sys/net/ipv4/tcp_window_scaling
  - echo "0" > /proc/sys/net/ipv4/tcp_sack
- Man tcp

Firewall básico II

- Cerrando los puertos
  - iptables -t filter -P INPUT DROP
  - iptables -t filter -P FORWARD DROP
- Abrimos el acceso al localhost
  - iptables -t filter -A INPUT -i lo -j ACCEPT
  - iptables -t filter -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

Firewall Básico III

- Aceptamos la red local
  - iptables -A INPUT -s 192.168.0.0/24 -i eth0 -j ACCEPT
- Abriendo los puertos necesarios
  - iptables -t filter -A INPUT -p tcp --dport 80 -j ACCEPT
  - iptables -t filter -A INPUT -p tcp --dport 25 -j ACCEPT
  - iptables -t filter -A INPUT -p tcp --dport 110 -j ACCEPT
  - iptables -t filter -A INPUT -p udp --dport 110 -j ACCEPT

Firewall Básico III

- Restablecemos el forward
  - iptables -t filter -A INPUT -j DROP
  - iptables -t filter -A FORWARD -i eth0 -j ACCEPT
  - iptables -t filter -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
  - iptables -t filter -A FORWARD -j DROP

Firewall Básico IV

- Ponemos el proxy transparente
  - iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 3128
- Abrimos los puertos necesarios
  - iptables -t nat -A POSTROUTING -p tcp --dport 25 -j MASQUERADE
  - iptables -t nat -A POSTROUTING -p tcp --dport 110 -j MASQUERADE
  - iptables -t nat -A POSTROUTING -p tcp --dport 80 -j MASQUERADE

Vigilando nuestro servidor

- Portsentry un guardia en nuestro servidor
- Logcheck, analizando las bitacoras de nuestro servidor.
  - http://sourceforge.net/projects/sentrytools/

Administración Remota

- Utilización de ssh
- scp o sftp en lugar de ftp
- Inseguros, viajan en texto plano
  - telnel pto.23
  - ftp pto.21
  - pop3 pto.110

Backups

- Las copias de seguridad o backups son el pilar sobre el que se construye cualquier sistema de seguridad.
- Backups remotos, este tipo de respaldos se conciben para asegurar la información en caso de fuerza mayor, vandalismo, desastres, etc.
- Raid
  - diferentes niveles

Conclusiones

- Definir en las politicas de seguridad, unicamente los puertos que realmente vamos a utilizar.
- Poner un firewall-proxy transparente
- Definir una política de login y password apropiados
- Revizar de forma constante las actualizaciones y sobre todo hacer un analísis del funcionamiento de nuestros servidores.

Preguntas?

Contacto

Simbiótica Seguridad en Redes.
http://www.simbiotica.net
jhdz@simbiotica.net