Incidente 2007-12-06: Indisponibilidad de servicios web □□□□□□□□□□.com y □□□.com.ve

2007-12-07

1.0

Historia de Versiones

- 2007-12-07: Primera edición

Incidente 2007-12-06: Indisponibilidad de servicios web □□□□□□□□□□.com y □□□.com.ve
2007-12-07

Resumen

El 6 de diciembre del 2007, personal de □□□□□□□□ se comunicó con itverx para consultar sobre un problema con los servicios web de los dominios □□□□□□□□.com y □□□□□□□□.com.ve. Los servicios dejaron de estar disponibles durante la noche del 5 al 6 de diciembre y la poca información disponible no permitía descartar ninguna hipótesis.

Itverx inició un proceso de diagnóstico sistemático, con el objeto de comprender las razones del incidente y de apoyar la reactivación de los servicios web antes señalados. Al final del proceso de despistaje, se encontró evidencia de que la causa más probable del incidente, tuvo su origen en una falla de hardware, específicamente sobre la controladora SmartArray, encargada del acceso a los discos del servidor.

1 Situación General

Las aplicaciones web de □□□□□□□□.com y de □□□□□□□□.com.ve corren en un sistema Ubuntu GNU/Linux y usan PHP, MySQL y Apache en la típica implantación de tecnología LAMP. Cuando itverx comenzó su investigación, se determinó la imposibilidad de establecer sesiones de acceso administrativos vía SSH, como se evidencia en la siguiente salida:

```
~$ ssh root@157.238.□□□.□□2
ssh_exchange_identification: Connection closed by remote host
```

En la Figura 1 se muestra una versión abreviada de la topología, tal como nos fue descrita por el personal de □□□□□□□□ a lo largo del proceso de diagnóstico. Aquí aparece el servidor maestro o principal, así como un servidor designado como backup o respaldo, utilizado para restituir temporalmente el servicio en situaciones de contingencia.

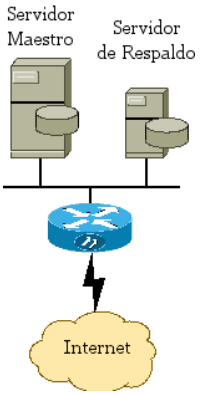

Figura 1: Topología simplificada de □□□□□□□□.com y □□□□□□□□.com.ve

La información sobre las características técnicas de los equipos se adquirió progresivamente durante el proceso de diagnóstico, pero se presenta completa en esta sección para facilitar las explicaciones posteriores y ubicar al lector en un mejor contexto.

El servidor maestro es un equipo Compaq/HP de la serie DL, con un CPU Intel® Xeon™ de 3.6 Ghz y 2GB de memoria RAM. Este servidor utiliza una tarjeta RAID SmartArray para manejar sus discos y proveer almacenamiento tolerante a fallas. La versión de Linux utilizada, era la 2.6.15-27.

El servidor de respaldo es un equipo Compaq Proliant 1600R, con un CPU Intel® Pentium™ III de 500 Mhz y 384 MB de RAM. Cuenta con una tarjeta RAID SmartArray y utilizaba la misma versión de Linux que el equipo maestro.

Ambos servidores comparten una red LAN Ethernet provista vía un conmutador, en modalidad 100-BaseTX.

Sobre el servidor maestro estaban configuradas las direcciones IP 157.238.□□□.□□2, 157.238.□□□.□□3 y 157.238.□□□.□□4. Este servidor tiene instalada una tarjeta Compaq/HP iLO *(Integrated Lights Out)* para administración remota, con dirección

IP 157.238.□□□.□□9. Esta tarjeta no pudo ser utilizada ya que □□□□□□□□ desconocía su clave de acceso.

A continuación se muestran los fragmentos relevantes a esta información, tomados del servidor maestro o principal:

```
Dec 6 12:29:20 □□□□□□□□vlnx1 kernel: Linux version 2.6.15-27-386
(buildd@terranova) (gcc version 4.0.3 (Ubuntu 4.0.3-1ubuntu5)) #1 PREEMPT Fri
Dec 8 17:51:56 UTC 2006
Dec 6 12:29:20 □□□□□□□□vlnx1 kernel: Memory: 2068648k/2097100k available (1976k
kernel code, 27144k reserved, 606k data, 288k init, 1179596k highmem)
Dec 6 12:29:20 □□□□□□□□vlnx1 kernel: CPU: Intel(R) Xeon(TM) CPU 3.60GHz
stepping 09
Dec  6 12:29:20 □□□□□□□□vlnx1 kernel: HP CISS Driver (v 2.6.8)
```

En el bastidor en que están instalados estos equipos, existe al menos un dispositivo de distribución eléctrica administrable remotamente, que permite apagar y encender los equipos allí conectados.

No se evidenció la presencia de mecanismos de restricción de tráfico – firewall – u otros dispositivos de seguridad.

2 Acciones de Diagnóstico y Respuesta

Las secciones siguientes describen las acciones generales de diagnóstico ejecutadas sobre los equipos antes mencionados. También se describen las acciones posteriores, dirigidas a la activación del servidor de contingencia. La presentación trata en lo posible de ceñirse a un orden cronológico, aunque se emplea la totalidad de la información obtenida en fases posteriores para ubicar las acciones y hallazgos en contexto.

2.1 Identificación Remota de Servicios Activos

Dada la imposibilidad de obtener acceso al servidor principal, itverx inició un proceso de identificación remota de servicios activos. Los resultados de este proceso no fueron completos, porque la actividad se interrumpió por restricciones de tiempo. Se encontró un número de servicios expuestos, como sigue:

```
Host 157.238.□□□.□□3 appears to be up ... good.
Interesting ports on 157.238.□□□.□□3:
PORT      STATE    SERVICE        VERSION
21/tcp    open     ftp?
22/tcp    open     ssh            OpenSSH 4.2p1 Debian 7ubuntu3.1 (protocol
2.0)
53/tcp    open     domain
80/tcp    open     http?
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
199/tcp   open     smux           Linux SNMP multiplexer
443/tcp   open     https?
445/tcp   filtered microsoft-ds
6000/tcp  open     X11             (access denied)
```

Varios de estos servicios son superfluos dadas las funciones de los equipos estudiados. El listado de servicios activos en el servidor principal y el de respaldo son similares, salvo por X11[1], que no se encontraba activo en este último.

2.2 Reinicio del Servidor Principal y Revisión de Configuración

Debido a la urgencia por restaurar los servicios web, □□□□□□□□ sugirió reiniciar el servidor principal. Esta acción requirió del concurso de personal en sitio, que ejecutó manualmente el reinicio del servidor. Esta acción recibió seguimiento telefónico. Durante el proceso de inicio, el personal en sitio reportó la aparición de mensajes de error antes del proceso de arranque del sistema Linux. El contenido y naturaleza del mensaje de error no pudo ser constatado con detalle suficiente como para utilizarlo en el proceso de análisis del incidente.

Luego de reiniciar el servidor principal, fue posible accederlo vía SSH[2] a las 2007-12-06T13:30, hora local del servidor. Esto permitió una revisión más cercana de su configuración a través de una sesión administrativa.

Con la ventaja del acceso al servidor, procedimos a revisar los servicios de red activos, con el objeto de identificar procesos o servicios anómalos o inusuales. Lo que sigue, muestra los servicios de red que estaban activos en este punto:

```
root@□□□□□□□□VLNX:/etc# netstat -na
Active Internet connections (servers and established)
Proto Recv-Q Send-Q      Local Address Foreign Address State
tcp        0      0       0.0.0.0:3306       0.0.0.0:* LISTEN
tcp        0      0         0.0.0.0:21       0.0.0.0:* LISTEN
tcp        0      0 157.238.□□□.□□1:53       0.0.0.0:* LISTEN
tcp        0      0       127.0.0.1:53       0.0.0.0:* LISTEN
tcp        0      0         0.0.0.0:25       0.0.0.0:* LISTEN
tcp        0      0      127.0.0.1:953       0.0.0.0:* LISTEN
tcp6       0      0             :::993            :::* LISTEN
tcp6       0      0             :::995            :::* LISTEN
tcp6       0      0             :::110            :::* LISTEN
tcp6       0      0             :::143            :::* LISTEN
tcp6       0      0              :::80            :::* LISTEN
tcp6       0      0              :::22            :::* LISTEN
tcp6       0      0              :::25            :::* LISTEN
tcp6       0      0            ::1:953            :::* LISTEN
tcp6       0      0              :::443           :::* LISTEN
udp        0      0     0.0.0.0:32769      0.0.0.0:*
udp        0      0 157.238.□□□.□□1:53       0.0.0.0:*
udp        0      0       127.0.0.1:53       0.0.0.0:*
udp6       0      0           :::32770            :::*
[...]
```

Este listado muestra varios servicios que no deberían estar activos en el servidor. Esta información concuerda con los hallazgos parciales del análisis remoto. Pudimos comprobar que el espacio ocupado en disco mostraba un nivel de utilización por debajo de la capacidad máxima, como sigue:

1 X11 es el servicio responsable del manejo de consolas gráficas en sistemas Unix. Su arquitectura permite mostrar *ventanas* de aplicaciones que se ejecutan en un servidor, en una consola remota.

2 *Secure Shell*, un protocolo para acceso remoto que provee protección criptográfica.

```
root@□□□□□□□□vlnx1:~# df -k
Filesystem        1K-blocks Used     Available Use% Mounted on
/dev/cciss/c0d0p1 67140468  12264500 51465372  20%  /
...
```

Posteriormente determinamos que el servidor se instaló con una sola partición, como se muestra a continuación:

```
root@□□□□□□□□vlnx1:~# mount
/dev/cciss/c0d0p1 on / type ext3 (rw,errors=remount-ro)
...
```

Esta modalidad de instalación complica varios procesos normales de administración de sistemas tales como el respaldo y recuperación. Un inconveniente adicional, es que cualquier problema con el sistema de archivos puede propagarse a toda la instalación, amplificando su efecto sobre el servicio y el riesgo a la integridad y disponibilidad de los datos.

2.3 Transferencia y Revisión de Registros de Actividad

Una vez que fue posible acceder administrativamente al servidor principal, iniciamos un proceso de transferencia de los registros de actividad almacenados, con el objeto de hacer un análisis de los eventos que sucedieron inmediatamente antes del inicio de este incidente.

Usando el protocolo SSH, se transfirieron 2 412 archivos de registro, ocupando un espacio de 25 249 815 octetos luego de la transferencia. Estos registros se preservaron en un CD-R para efectos de eventuales estudios posteriores. La firma MD5 de la concatenación de dichos archivos es f44eacf988b804a3919dddbe3e61bdc7.

Haciendo un análisis de los registros presentes, encontramos que todas las bitácoras del sistema dejaron de registrarse a partir de 2007-12-05T18:28:00, hora local del servidor. Los registros comenzaron a almacenarse correctamente luego de reiniciar físicamente el servidor principal, en 2007-12-06T12:29:20, hora local del servidor.

Ninguno de los archivos de registro muestra evidencia de actividad anormal antes de que dejaran de almacenarse eventos. Los registros normales de actividad típicos de la operación de los diferentes servicios que operan en el servidor principal ocurridos antes del evento, aparecen en sus correspondientes archivos.

El registro de acceso remoto muestra únicamente accesos asociados al servicio FTP hasta antes de nuestro acceso, como se ve a continuación:

```
$ who ./wtmp
...
admin    ftpd10207    2007-12-04 15:11 (190.74.254.143)
root     pts/0        2007-12-06 13:30 (200.84.243.27)
```

2.4 Depuración de Configuraciones

Visto el acceso al servidor principal, los servicios superfluos que habían sido identificados con antelación en la sección 2.2 y la imposibilidad de descartar la hipótesis de la intrusión para ese momento, se optó por depurar la configuración tanto del servidor principal como del servidor de

respaldo. Esto, con la intención de reducir la probabilidad de que una eventual vulnerabilidad de seguridad explotada por un hipotético atacante, pudiese volver a suprimir los servicios.

La depuración consistió en la eliminación de los servicios Samba[1], Courier POP, Courier IMAP[2], MTA[3] y BIND9[4]. En el servidor principal también se desactivó X11, que sólo estaba activo en este equipo como se explicó en la sección 2.1.

Una vez hecha esta eliminación, se procedió a hacer una actualización del *kernel* a la última versión disponible para la distribución Ubuntu GNU/Linux instalada en los equipos. Esta es la versión 2.6.15-27, que data de finales del 2006. Como es normal luego de este tipo de actualizaciones, reiniciamos los equipos. Vale decir que fue necesaria la intervención del personal en sitio para encender el equipo. Esto sugiere la posibilidad de que se deban aplicar actualizaciones al BIOS del servidor, lo cual no resultaba posible en las condiciones presentes durante la respuesta al incidente.

Una vez que los servidores principal y de respaldo se encontraban actualizados, se practicó una revisión de rutina sobre los archivos de registro para identificar problemas particulares. No se identificó ningún problema atribuible a la actualización.

2.5 Intento de Poner el Servidor Principal en Funcionamiento

Una vez hechas las actualizaciones y depuraciones de rigor descritas en la sección 2.4 y en ausencia de mayor información, no era posible aun descartar la hipótesis de la intrusión. En este punto, poner al servidor de respaldo a dar servicio, hubiera expuesto la única copia confiable del entorno web de los dominios □□□□□□□□.com y □□□□□□□□.com.ve, sin una estrategia clara de recuperación en caso de que el servidor de respaldo resultara comprometido.

Los representantes de □□□□□□□□ e itverx decidieron entonces intentar poner al aire nuevamente al servidor principal, con el objeto de evaluar mejor el daño y devolver la operatividad a las páginas antes citadas. Se hizo un número de intentos por reactivar el servicio. Invariablemente, los procesos que se ejecutaban en el servior se bloqueaban paulatinamente, quedando en estado “D”, que la documentación del sistema define como *“Uninterruptible sleep (usually IO)”*. Típicamente esto se asocia con actividad de disco de corta duración.

Tras cada intento de reactivar los servicios web, era necesario reiniciar físicamente el servidor principal debido a que se volvía imposible impartir comandos o forzar la terminación de los procesos bloqueados. Reduciendo agresivamente el número de procesos de servicio web que se activaban, pudimos demostrar que por un lapso muy breve, los procesos de servicio podían atender solicitudes web, como se muestra a continuación:

1 Servicio de acceso a volúmenes compartidos con el protocolo SMB, usado tradicionalmente por equipos Windows®. Este servicio es *inseguro* cuando se usa para transportar archivos a través de redes públicas.

2 Servicio para acceso a buzones de correo a través de los protocolos POP e IMAP.

3 En los servidores primario y de respaldo, se encontraban instalados sendmail y postfix respectivamente. Estos programas proveen servicio de transporte de correo, innecesario para las tareas actualmente asignadas a esos equipos.

4 Servicio para ofrecer resolución de nombres. Resulta innecesario porque no hay ninguna *zona* de resolución de nombres que haya sido delegada a las direcciones IP de ninguno de los servidores.

```
$ wget -O /dev/null -S http://□□□□□□□□.com:8080/
--16:45:11-- http://□□□□□□□□.com:8080/
=> `/dev/null'
Resolving □□□□□□□□.com... 157.238.□□□.□□3
Connecting to □□□□□□□□.com|157.238.□□□.□□3|:8080... connected.
HTTP request sent, awaiting response...
HTTP/1.1 200 OK
Date: Thu, 06 Dec 2007 20:38:27 GMT
Server: Apache/2.2.3 (Unix) ...
Last-Modified: Fri, 31 Oct 2003 21:15:12 GMT
Content-Length: 163
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
Length: 163 [text/html]

100%[====================================>] 163 --.--K/s

16:45:11 (24.73 MB/s) - `/dev/null' saved [163/163]
```

Pero los procesos caían inmediatamente en estado “D”. Iniciar el servicio de base de datos o el servicio de acceso vía FTP no causó un efecto como el antes descrito.

Vista la similitud de lo observado con algunos escenarios de fallas en el acceso a disco, hicimos una nueva verificación en las bitácoras, encontrando mensajes de error reveladores, como se muestra a continuación:

```
root@□□□□□□□□vlnx1:/var/log# egrep cciss /var/log/syslog | egrep -v 'has
been found|splash|Adding|EXT3|DAC cycles|p1 p2'
Dec 6 15:01:11 □□□□□□□□vlnx1 kernel: cciss: cmd dfb40000 has CHECK CONDITION byte 2 = 0x3
Dec 6 15:03:03 □□□□□□□□vlnx1 kernel: cciss: cmd dfb40000 has CHECK CONDITION byte 2 = 0x3
Dec 6 15:04:55 □□□□□□□□vlnx1 kernel: cciss: cmd dfb40250 has CHECK CONDITION byte 2 = 0x3
Dec 6 15:10:30 □□□□□□□□vlnx1 kernel: cciss: cmd dfb40250 has CHECK CONDITION byte 2 = 0x3
Dec 6 15:10:30 □□□□□□□□vlnx1 kernel: cciss: cmd dfb40000 has CHECK CONDITION byte 2 = 0x3
Dec 6 15:10:30 □□□□□□□□vlnx1 kernel: cciss: cmd dfb40000 has CHECK CONDITION byte 2 = 0x3
```

Estos mensajes están relacionados con un problema en el hardware de la controladora de discos SmartArray. También pudimos constatar que dichos mensajes no se habían registrado en el pasado reciente, sino luego del reinicio físico que hicimos con posterioridad a las actualizaciones descritas en la sección 2.2. La evidencia de esto se muestra a continuación:

```
root@□□□□□□□□vlnx1:/var/log# head -1 /var/log/syslog
Dec 6 12:35:10 □□□□□□□□vlnx1 syslogd 1.4.1#17ubuntu7.1: restart.
root@□□□□□□□□vlnx1:/var/log# tail -1 /var/log/syslog
Dec 6 16:21:28 □□□□□□□□vlnx1 mysqld_safe[4959]: ended
root@□□□□□□□□vlnx1:/var/log# zegrep cciss /var/log/syslog.1.gz | egrep
-v 'has been found|splash|Adding|EXT3|DAC cycles|p1 p2'
root@□□□□□□□□vlnx1:/var/log# egrep cciss /var/log/syslog.0 | egrep -v
'has been found|splash|Adding|EXT3|DAC cycles|p1 p2'
root@□□□□□□□□vlnx1:/var/log#
```

Visto lo anterior, se determinó que la causa más probable del incidente estaba relacionada con una falla de hardware que afecta los accesos a disco. El limitado acceso administrativo al equipo y la ausencia de registros de actividad *durante* la falla, hacen imposible un diagnóstico más preciso.

2.6 Transferencia de Direcciones IP

Dado que la conclusión del trabajo de análisis descrito anteriormente apuntaba hacia una falla de hardware, el representante de □□□□□□□□ solicitó activar al servidor de respaldo para que pudiese dar servicio. Para esto y en coordinación con su personal técnico, desactivamos las direcciones IP 157.238.□□□.□□2 y 157.238.□□□.□□3 del servidor principal y las configuramos sobre el servidor de respaldo.

3 Conclusiones y Recomendaciones

Con base en lo aprendido durante el análisis de este incidente y a la información a la que itverx tuvo acceso, se pueden enunciar conclusiones y formular las siguientes recomendaciones.

- **Reforzar la habilidad de gestión remota:** La acción sobre los equipos resultó engorrosa y compleja debido a la baja capacidad de operación y gestión remota existente. Se requiere urgentemente la dotación de mecanismos de gestión remota que permitan una administración de sistemas cómoda y eficiente, sin necesidad de ubicar personal físicamente en el centro de hospedaje.
- **Implantar mecanismos de monitoreo de indicadores clave:** Observamos que para □□□□□□□□ fue imposible determinar con precisión cuándo se perdió el servicio de las páginas web de □□□□□□□□.com y □□□□□□□□.com.ve. La operación de un sitio web requiere un seguimiento minucioso y continuo de las variables relevantes de los elementos de infraestructura, así como un detallado registro de las actividades que se ejecutan sobre ellos.
- **Normalizar la instalación de los servidores:** Pudimos ver que las instalaciones de ambos servidores – principal y de respaldo – se hicieron manualmente y sin seguir un proceso documentado. Como consecuencia, cada instalación es única y diferente de las demás, lo que complica los procesos de administración de sistemas normales. La instalación de los servidores debe estar automatizada, ser repetible y consistente.

  Como ejemplo adicional de la importancia de este punto, obsérvese el siguiente extracto de los registros, donde se evidencia que **el segundo procesador presente en el servidor no se está usando.**

```
$ egrep 'NR_CPU|Processor' messages
Dec 6 12:29:20 □□□□□□□□vlnx1 kernel: Processor #0 15:4 APIC version 20
Dec 6 12:29:20 □□□□□□□□vlnx1 kernel: Processor #1 15:4 APIC version 20
Dec 6 12:29:20 □□□□□□□□vlnx1 kernel: WARNING: NR_CPUS limit of 1 reached. Processor
ignored.
```

- **Revisar la arquitectura de la plataforma de servicios:** La plataforma presenta múltiples debilidades desde el punto de vista de diseño, producto de un crecimiento sin la debida planificación. Es vital trabajar este punto para hacer converger la infraestructura existente hacia una plataforma que pueda prestar los servicios que □□□□□□□□ necesita para sí y sus clientes.
- **Desarrollar mecanismos de instalación remota:** En caso de que hubiese sido necesario reinstalar los servidores, esto hubiese sido imposible sin desplazar personal desde Caracas. Esta es claramente una forma costosa de operar, que no ofrece tiempos de respuesta

apropiados de acuerdo a las expectativas de los clientes de □□□□□□□□. Más aun, el despliegue de un nuevo servidor requiere de logísticas comparativamente complejas. Resulta mucho más sencillo aprovechar las ventajas de Linux en el frente de la administración remota o distribuida, para que estas tareas puedan ejecutarse de forma totalmente desasistida y remota.

- **Desarrollar una estrategia de registro remoto de bitácoras:** Contar con bitácoras de eventos accesibles en todo momento, facilita las tareas de diagnóstico y los procesos de monitoreo. Debe implantarse un mecanismo de registro remoto y respaldo de los eventos de bitácora.
- **Desarrollar herramientas y procesos de análisis de bitácoras:** Las bitácoras de eventos deben ser analizadas de forma sistemática para identificar tempranamente condiciones de riesgo operacional.
- **Formular planes de contingencia completos:** Observamos que el plan de contingencia de □□□□□□□□ estaba elaborado en términos genéricos y amplios, dejando un número de decisiones para ser tomados durante el evento. Esta práctica demora la solución de problemas y expone a los clientes de □□□□□□□□ a una situación de riesgo aumentado, en el caso de que esas decisiones resulten erradas. Se debe formular un plan de contingencia detallado, completo hasta el nivel de comandos a ejecutar. El plan se debe ensayar periódicamente bajo condiciones controladas, para comprobar su efectividad.
- **Mejorar la documentación:** Observamos que aspectos como las conexiones de red y eléctricas de los equipos no estaban documentadas con la precisión y detalle necesarios. En una operación remota es indispensable que todos los conectores estén etiquetados y todas las conexiones documentadas en forma clara y consistente.