Incidente ******** 2007-12-06

Informe, Conclusiones y Recomendaciones

********, C.A.

itverx

Contenido Protegido

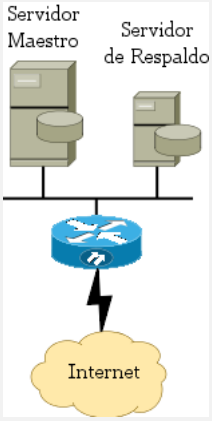
itverx

Agenda

itverx

Inicio del Incidente

Hechos e Información Disponible



- Los servicios web de **********.com y ***.com.ve dejaron de estar disponibles durante la noche del 5 al 6 de diciembre
- Fallas en el acceso administrativo – SSH
- Despliegue de un mensaje de error alusivo a problemas con la base de datos al conectarse vía web
- Confusión sobre la hora de inicio del incidente

itverx

Inicio del Incidente

Hipótesis Iniciales

Ataque de un *hacker* La única hipótesis inicial manejada por ********, C.A. era que el servidor que aloja los sitios web, había sido atacado exitosamente por un hacker

Reconocimiento Remoto

Determinación de Condiciones Técnicas Iniciales

- Determinación de posibles *backdoors* activos e información sobre el estado real del servidor principal
- Se ejecutó un reconocimiento de puertos usando la herramienta `nmap`, identificando múltiples puertos activos:

```
Starting Nmap 4.11 at 2007-12-06 11:47 VET
Initiating SYN Stealth Scan [65535 ports/host] at 11:47
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 (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
593/tcp   filtered http-rpc-epmap
6000/tcp  open     X11             (access denied)
```

Reconocimiento Remoto

Servicios Superfluos

- Sólo se requieren los siguientes servicios activos

  21/FTP Servicio para transferencia de archivos. **Es altamente recomendable reemplazar este servicio**

  22/SSH Acceso administrativo protegido con autenticación robusta y criptografía. Puede reemplazar a FTP de forma segura

  80/http, 443/https Servicio web con y sin SSL

- El resto de los servicios es superfluo y constituye un riesgo adicional a la operación

Acceso Administrativo

Ingreso via SSH al Servidor Principal

- Luego de reiniciar el servidor principal, el acceso administrativo quedó disponible
- El listado local de servicios activos confirma la presencia de servicios superfluos

```
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      0.0.0.0:25         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:*
udp6  0      0      :::32770           :::*
```

Preservación de Registros

- Se hizo una copia local de los registros de actividad existentes hasta el momento en el servidor de producción
- Se transfirieron 25 249 815 octetos en 2 412 archivos de registro
- El registro de nuevos eventos se interrumpió a aproximadamente 2007-12-05T18:28:00, hora del servidor
- El registro de eventos se restableció en 2007-12-06T12:29:20, luego de reiniciar el servidor
- **La hora local del inicio del incidente se ubica hacia 2007-12-05T18:28:00**

Depuración de la Configuración

Eliminación de Servicios Superfluos

- Se eliminaron los siguientes servicios

Samba Un servicio que permite el acceso a archivos en el servidor usando el protocolo SMB. Esto permite la conexión con volúmenes compartidos de Microsoft® Windows

Courier POP e IMAP Servicios para acceso a buzones de correo usando protocolos POP3 e IMAP4

MTA Distintos servicios en el servidor principal y de respaldo, que se usan para el transporte de email

BIND Servicio para proveer resolución de nombres. En este caso, no se requiere que el servidor sea parte de la infraestructura de resolución de nombres

Diagnóstico de Hardware

Identificación de Causa Raíz del Incidente

- Resultó imposible volver a poner el servidor principal en servicio
- Un nuevo análisis de los registros de eventos mostró evidencia de errores de hardware

```
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
```

- Como consecuencia, se inició la transferencia del servicio hacia el servidor de respaldo

itverx

Análisis de Causa Raíz

- Una falla en el controlador SmartArray del servidor principal jugó un papel determinante en la materialización del incidente
- Las debilidades en procesos clave relacionados con el manejo de contingencias, complicaron la respuesta
- La falta de indicadores básicos hicieron imposible determinar con precisión cuándo se inició el incidente

itverx

Gestión y Acceso Remoto

- Se requiere reforzar la capacidad de gestión remota de la plataforma
- La autenticación debería estar basada en el uso de certificados, no sólo en claves
- La transferencia de contenido debe hacerse bajo protección criptográfica y autenticación robusta

Monitoreo de Indicadores

- Es necesario monitorear y registrar variables e indicadores sobre disponibilidad de servicio y recursos
- Las desviaciones de los valores observados deben investigarse prontamente, para evitar la materialización de incidentes y fallas

Normalización de Instalación

- La instalación de servidores debe hacerse de acuerdo a un plan específico y repetible, que garantice que todos los equipos tienen configuraciones idénticas
- La automatización del proceso de instalación garantiza la consistencia del proceso y reduce la carga de trabajo asociada a la respuesta a incidentes y a la administración de sistemas, especialmente cuando se dan aumentos de capacidad
- Se deben incluir tareas de control de configuración, para asegurar que sólo se mantienen los componentes necesarios y que estos están actualizados hasta la versión recomendada

itverx

Revisión de Arquitectura

- El nivel de servicio que ******** desea ofrecer a sus clientes requiere la revisión de la arquitectura de sus plataformas. Algunos ejemplos de aspectos a considerar:
  - Firewalls y dispositivos de seguridad
  - Mecanismos de gestión de contenido
  - Acceso remoto de contingencia a los equipos
- El modelo actual depende de la existencia de un nivel de soporte en sitio del que no se tienen garantías

itverx

Instalación Remota

- Las operaciones geográficamente dispersas deben considerar entre sus procesos, un mecanismo que permita hacer la instalación estándar de software a los equipos remotos
- ******** requiere sincronizar sus procesos y los niveles de servicio de recursos en sitio, para lograr la habilidad de instalar un nuevo servidor de forma totalmente remota

itverx

Registro Remoto y Análisis de Bitácoras

- Las bitácoras de eventos deben quedar registradas *fuera* del servidor para permitir accederlas aun cuando se presentan fallas catastróficas en el equipo
- Los registros de bitácora deben ser analizados sistemáticamente, buscando eventos anormales para generar alarmas y disparar acciones de repspuesta

itverx

Planes de Contingencia

- Los planes de contingencia deben estar documentados con un nivel de detalle suficiente como para minimizar la necesidad de tomar decisiones durante la crisis
- Deben programarse simulacros y pruebas para validar el alcance y correctitud de los planes de contingencia

Mejoras a la Documentación

- En operaciones remotas, es vital saber cómo están conectados los equipos. Los cables y conectores deben estar etiquetados de forma consistente y legible, para simplificar la tarea del personal en sitio
- La documentación debe estar disponible tanto durante la operación normal como durante la resolución de incidentes, en forma completa