Universidad de los Andes
Infraestructura Computacional

Integrantes:

- Juan Diego González – 201531418
- Carlos Peñaloza – 201531973
- Camilo Montenegro – 201531747

Caso 2

Análisis y Entendimiento del Problema

Amenazas:

1. Catástrofes Naturales. Una de las amenazas que se le puede presentar a Colpensiones es la caída de sus servidores. Los desastres naturales, como terremotos, incendios o incluso inundaciones pueden afectar fuertemente la infraestructura de TI de la empresa. Si llegase a ocurrir uno de estos eventos y el servidor queda destrozado, Colpensiones se vería en grandes apuros, ya que tendría que reconstruir su centro de datos y además perdería la información que estaba almacenada anteriormente.
2. Spoofing o Suplantación de Identidades. Existen varios tipos de Spoofing, pero la más amenazante para Colpensiones es el Spoofing ARP ya que las peticiones de los clientes pueden ser interceptados por un host atacante y este sujeto podrá saber los mensajes que se están intercambiando. Este tipo de ataques pueden ser muy frecuentes en esta empresa, ya que no tienen ningún sistema de protección contra estos en específico. Cabe aclarar que los FireWalls que implementen Colpensiones no pueden defender este tipo de ataques.
3. Denegation of Services. Si llegase a existir un ataque cibernético en el cual se inunda el servidor principal de Afiliados con peticiones y mensajes basura, los más afectados serían los clientes externos, es decir, las sucursales y los computadores de la red interna (los trabajadores de Colpensiones). Estos no podrían acceder a las aplicaciones y servicios que se les ofrece de manera oportuna, ya que el servidor estaría ocupado y las peticiones legítimas se demorarían mucho en procesar.
4. Elevation of Privilege. La información relacionada con la seguridad informática de Colpensiones no nos muestra con claridad la matriz de control de acceso que maneja el sistema operativo de Colpensiones. Si asumimos de manera pesimista que un atacante logra acceder al sistema como un super usuario, este lograría tener todos los permisos posibles. De esta manera los datos se verían vulnerados y el atacante podría hacer un daño importante en el servidor de afiliados. Esto puede implicar muchas más amenazas.

Vulnerabilidades:

1. Se pueden ver contraseñas débiles y fáciles de encontrar por medio de algún método de password-cracker (ataque de fuerza bruta). Si no se toman decisiones importantes con respecto a este asunto, cualquier atacante podría encontrar una entrada al sistema.
2. No se implementa algún control para saber la cantidad de peticiones que genera un cliente al servidor. Si no se tiene algún tipo de control sobre esto, se pueden generar ataques de tipo DOS (Denial of Services). Existe un tipo de estos ataques en donde un atacante genera todas las peticiones "basura" desde una máquina. Si se llega a implementar algún control, se pueden detectar ataques fácilmente y se niegan las peticiones provenientes de la máquina remitente.
3. No se ve algún tipo de defensa ante ataques de tipo malware. Debido a que no se nos suministra información completa sobre esto, se asume el peor caso. Por ello, se da por sentado que el sistema es vulnerable a todo tipo ataque cibernético relacionado con malwares. Así mismo, el servidor siempre se encuentra conectado a la red de Internet, por lo que este tipo de ataques pueden ser más frecuentes.
4. Se utilizan algoritmos de cifrado conocidos y utilizados en la industria. Este tipo de algoritmos (DES y RC4) son tan conocidos que se vuelven vulnerables. Se podría comenzar a utilizar otro tipo de algoritmos de cifrado un poco más robustos y menos conocidos en la industria.

Propuesta de Soluciones

1. El servidor principal debería estar construido dentro de una edificación segura ante cualquier tipo de catástrofes naturales o incendios. Es por esto, que se debe ubicar esta construcción en una región geográficamente estratégica, para evitar daños por sismos o terremotos. Por otro lado, se debería tener una edificación anti-sismos para mitigar daños en el caso que se genere un sismo.
2. Debido a que el spoofing ARP funciona con la clonación de las direcciones MAC de los computadores y servidores, es pertinente tener ciertos artefactos o softwares que ayudan a comprobar el uso de MACs clonadas. Cabe aclarar que se pueden clonar las direcciones MAC de forma legítima. Por otro lado, se puede tener una herramienta como ArpWatch, la cual avisa cuando se detecta alguna amenaza de este tipo de ataques. Así mismo, se podría cifrar los mensajes que se van a enviar de manera que sólo lo puedan descifrar los host verdaderos y no los atacantes. Esto podría afectar el tiempo de respuesta del servidor, lo que hace que Colpensiones tenga que analizar sus prioridades y definir qué hacer para asegurar su información y sistemas
3. Debido a que hoy en día los ataques DOS son muy frecuentes, hay empresas especializadas en prestar servicios en la nube para mitigar este tipo de ataques. Lo bueno de utilizar este tipo de servicios es que este tipo de empresas tienen personal capacitado y expertos en los temas de seguridad informática. También, al ofrecer un ancho de banda más extenso, los ataques no serán tan fuertes y no afectarán de

manera contundente el servidor de Colpensiones. Por otro lado, como se dijo anteriormente, se puede tener algún tipo de control de peticiones en donde se cuentan la cantidad de mensajes que un cliente envía al servidor. Si se detecta una alta cantidad de mensajes de un cliente, este será restringido y no se bloquearan las peticiones que este haga.

4. Para poder mitigar el problema de elevación de privilegios se debe definir de manera apropiada una matriz de control de accesos robusta. Así mismo, se debe limitar el acceso a ciertos usuarios a la información vulnerable (por medio de la matriz de control de accesos). Por otro lado, es importante implementar un antivirus para proteger al servidor de ataques de malware que pueden invadir el sistema operativo y cambiar los privilegios del usuario.

Bibliografía

- Overview of Web Application Security Threats (n.d.). Retrieved October 26, 2017, from https://msdn.microsoft.com/en-us/library/f13d73y6.aspx
- Sean Leach, VP of Technology, Verisign, special to Network World. (2013, September 17). Four ways to defend against DDoS attacks. Retrieved October 26, 2017, from https://www.networkworld.com/article/2170051/security/tech-primers-four-ways-to-defend-against-ddos-attacks.html