Reporte de Penetración.

Este documento describe el pentesting que se le hizo al servidor **truerandom.bid**.

26 DE MARZO DE 2019

Hernández González Ricardo Omar

Indice.

RESUMEN EJECUTIVO.

Objetivo.

El objetivo de este pentesting es prácticar lo visto en el curso de Pruebas de Penetración, el cual nos enseñó a buscar vulnerabilidades y saber por dónde y cómo explotarlas.

Resumen de Resultados.

Análisis de Resultados.

La prueba de penetración identificó 4 vulnerabilidades en el aplicativo web. De estos resultados dos fueron rankeados como un riesgo alto, las otras fueron un riesgo intermedio. El de mayor riesgo fue relacionado con el password del servicio mysql, donde su contraseña se encuentra entre las 100 contraseñas más usuales. Solo fue necesario un diccionario en donde se encontraban estás contraseñas para encontrarla fácilmente. Este descubrimiento puede ser remediado poniendole seguridad a su contraseña, usando caracteres, longitud mayor a 8 caracteres, mayusculas y minusculas.

La siguiente de riesgo alto fue por lo mismo, un ataque de fuerza bruta al CMS de wordpress. Al igual que la solución anterior se recomienda darle más seguridad a los password, y principalmente a los de administrador.

La siguiente vulnerabilidad encontrada fue un ftp anónimo, esta es de las principales vulnerabilidades encontrada en ftp. Por último la vulnerabilidad de Tomcat, donde se aprovecha de un framework que contiene este servicio.

Descripciones de Niveles de Seguridad.

10	**Worst Pain You Can Imagine**
7-9	**Severe Pain** **Pain keeps you from doing your regular activities.** ⑨ Pain is so bad that you can't do any of your regular activities, including talking or sleeping. ⑧ Pain is so intense that you have trouble talking. ⑦ Pain distracts you and limits your ability to sleep.
4-6	**Moderate Pain** **Pain may interfere with your regular activities.** ⑥ Pain makes it hard to concentrate. ⑤ You can't ignore the pain but you can still work through some activities. ④ You can ignore the pain at times.
1-3	**Mild Pain** **Pain doesn't interfere with your regular activities.** ③ You may notice the pain but you can tolerate it. ② You may feel some twinges of pain. ① You may barely notice the pain.
0	**No Pain**

DETALLES DE RESULTADOS.

Fuerza bruta mysql con autenticación remota.

Descripción:

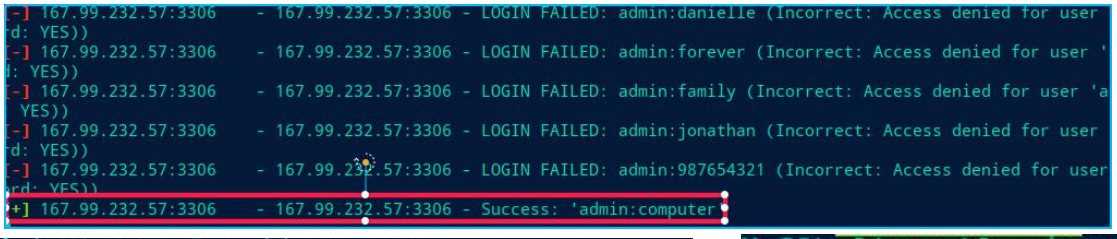
Una contraseña débil fue identificada en el servicio de mysql, el cual probando con usuarios comunes como root y admin, y un diccionario de contraseñas que contiene las más comunes, fue muy sencillo poder acceder al servicio de manera remota.
Las políticas de las contraseñas especifican que para que una contraseña pueda ser segurda, debe contrar con al menos 8 caracteres, una mayúscula, una mínúscula y un caracter especial, esto para darle complejidad y que sea muy difícil poder encontrarla.

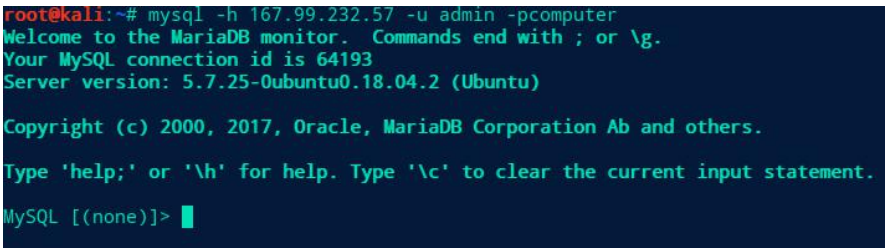
Host Afectados:

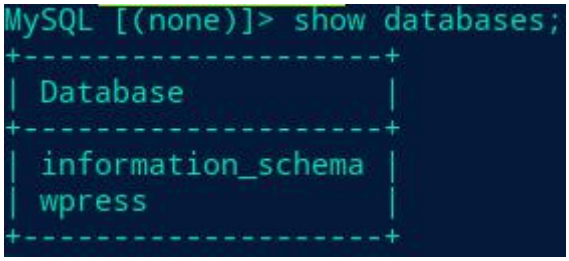
http://truerandom.bid

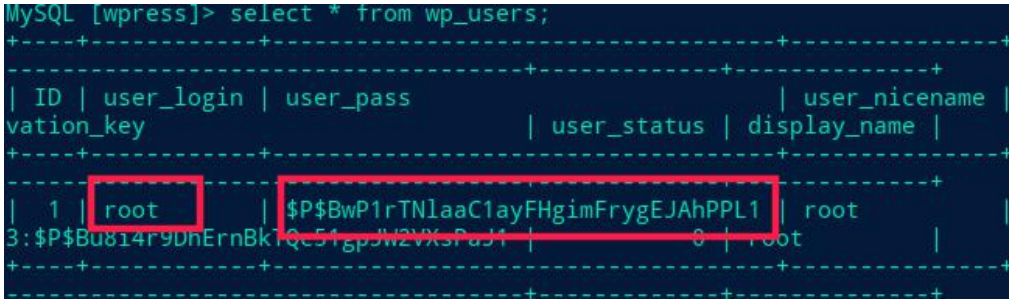
Solución:

Es recomendable contar con una contraseña segura, así como lo dictan las políticas. El usuario que sea distinto a los comúnes, como root o admin.
También como recomendación, restringir el acceso a la base de datos, no permitiendo que desde cualquier lado puedan accesar a ella.









FTP anónimo.

Descripcion:

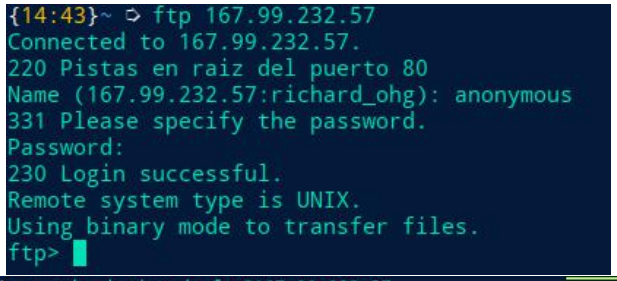
El FTP anónimo se llama anónimo porque no necesita identificarse antes de acceder a los archivos. En general, ingresa la palabra anonymous o ftp cuando el host le solicita un nombre de usuario, puede ingresar cualquier cosa para la contraseña. En muchos casos, cuando accede a un sitio FTP anónimo, ni siquiera se le pedirá su nombre y contraseña.
Puede usar el sistema para obtener archivos y subirlos, como por ejemplo, colocar una llave para ssh y entrar al servidor sin ningún problema.

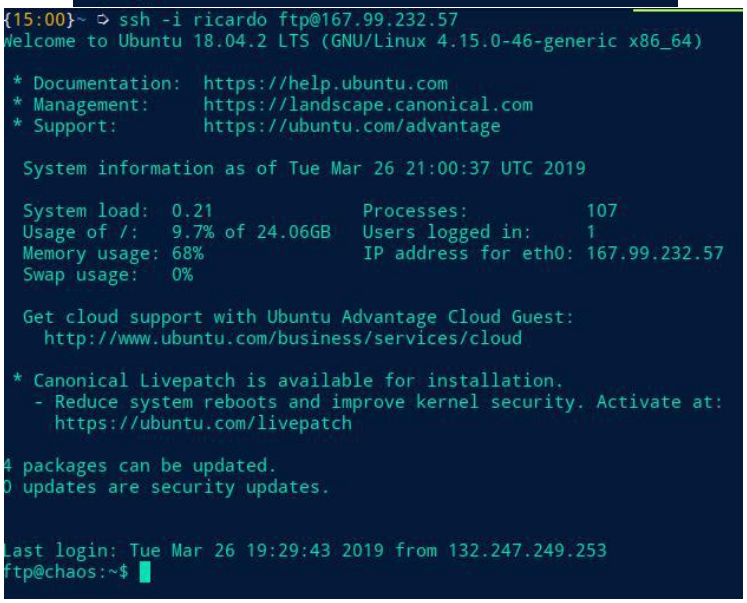
Host Afectados:

http://truerandom.bid

Solución:

Es necesario desactivar la autenticación anónima en su servidor FTP, para que no cualquier persona pueda entrar al servidor y pueda subir archivos que puedan dañar contra la integridad de sus datos o en todo caso puedan causar que abran una puerta trasera y se conecten sin ser detectados.





Fuerza bruta con wordpress.

Descripción.