Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

Hogwash: mezcla de Firewall y NIDS. (10992 lectures)

Per **Carlos Cortes Cortes**, ***carcoco*** (http://bulma.net/~carcoco/)

Creado el 05/11/2001 21:04 modificado el 05/11/2001 21:04

> **Hogwash**, es una especie de híbrido entre un **firewall** y un **NIDS** (Network Intrusion Detection System), de forma que correctamente configurado nos permitira protegernos de ataques externos que podrían pasar inadvertidos para un firewall ...

Los firewall clásicos lo que hacen es modificar sus **reglas**, para denegar cualquier petición que se suponga ilegal, esto que en un principio es lo correcto y lo que queremos, también implica que el atacante pueda realizar un **ataque DoS** (Denegación de Servicio) muy fácilmente.

Imaginad que el atacante al detectar nuestra defensa, empieza a mandarnos peticiones falsas de accesos desde Bulma, Freshmeat o nuestro servidor **DNS**. ¿Qué pasaría entonces? que nos estaríamos denegando nosotros mismo el acceso a estos sitios, y si no podemos acceder a nuestro servidor DNS, perdemos el acceso a practicamente *TODO*.

La solucion es utilizar **hogwash**, que en lugar de cerrar puertos y denegar acceso, lo que hace es rechazar y modificar determinados paquetes en función de la identificación de *signaturas/patrones*, para lo cual se apoya en el potente **Snort** y su amplia y completa colección de *reglas*.

"Hogwash is designed to take out 95% of the stock attacks all the kiddies throw at your network. Hogwash lives inline like a firewall, but it works differently. Instead of closing ports like a traditional firewall, it drops or modifies specific packets based on a signature match. Hogwash lives directly on top of the network driver, so it doesn't require an IP stack to work. It stops attacks that can't be blocked by a traditional firewall and can be used to protect systems that are unpatchable for one reason or another. The signature matching engine is based on Snort."

http://hogwash.sourceforge.net(1)
http://www.snort.org(2)

--
Carlos Cortes (aka carcoco)
http://bulma.net/todos.phtml?id_autor=132 (3)

Lista de enlaces de este artículo:

1. http://hogwash.sourceforge.net/
2. http://www.snort.org
3. http://bulma.net/todos.phtml?id_autor=132

E-mail del autor: carcoco _ARROBA_ gmail.com
Podrás encontrar este artículo e información adicional en: http://bulma.net/body.phtml?nIdNoticia=969