Evaluating and Tuning Web Application Firewalls

OWASP-KC
6-13-2007

Barry Archer

(Experiences of a corporate security geek, squeezing in evaluations between meetings)

Evaluating and Tuning Web Application Firewalls

Since last we talked...

More Phishing -it isn't just for email any more... lots of inventive ways to drop malware on a PC

A whole lot more Bots out there – great for good old spam, and for a kiddie's own anonymous relay, scanning and attacks, etc.

Evaluating and Tuning Web Application Firewalls

I've had a chance to do some evaluation of WAFs:

Apache mod_security (& friends)

Brand X (commercial product)

Evaluating and Tuning Web Application Firewalls

Both mod_security and Brand X provide:

Security-oriented HTTP Request/Reply logging

Real time monitoring and attack detection

Ability to act as a reverse web proxy

Evaluating and Tuning Web Application Firewalls

Both mod_security+ and Brand X provide:

Attack prevention capabilities (different approaches)

- Negative security rules and language
- Different philosophies around positive security

Evaluating and Tuning Web Application Firewalls

Why is WAF logging important?

- Most web logging is for *Marketing*
- Anomalous behavior isn't always obvious
- A well designed log format really speeds up forensic audit work
- It's invaluable for tuning your app's protection
- Sometimes you just have to see it to believe it

Evaluating and Tuning Web Application Firewalls

Why is real time monitoring/detection important?

NIDS just don't *get* the application layer

Sometimes, even script kiddies get lucky

WAFs can be set up to take action immediately

Evaluating and Tuning Web Application Firewalls

Who cares if you're a reverse web proxy?

You do, if you want to scale to more than one or two servers

You can protect *those* kinds of app servers

The bad guys certainly will care...

Evaluating and Tuning Web Application Firewalls

Isn't an ounce of prevention too expensive?

Negative security model – provides part of a daily, healthy layered approach

Positive security model – gives you a place to implement what you learn from threat modeling

Absolutely Positive security model – if you can capture correct behavior for your site, then this works *very* well

Evaluating and Tuning Web Application Firewalls

Which to choose: Mod_Security or Brand X?

Both are well developed and maintained.

Both have support you can purchase.

Both come with basic rules and sample configurations.

Evaluating and Tuning Web Application Firewalls

Which to choose: Mod_Security or Brand X?

Mod_Security and associated modules require more DIY Open Source knowledge to get up and running, especially on Windows.

Brand X does scale better and provide an excellent solution for a corporate Internet presence.

Evaluating and Tuning Web Application Firewalls

Which to choose: Mod_Security or Brand X?

Either one will require planning, effort
– and both understanding and tuning

Neither is a magical fix - you have to understand:
How HTTP works
How to 'tune'
How your application is suppose to work
How user input is suppose to look

Evaluating and Tuning Web Application Firewalls

Which to choose: Mod_Security or Brand X?

Whichever will work best for you
- ability to implement is important

Other brands may work as well – just make sure they do everything you need (correctly)

Evaluating and Tuning Web Application Firewalls

Additional Apache security modules:

Mod_Rewrite, Mod_Log_Forensic and Mod_Dosevasive

Mod_Security Resources:

www.modsecurity.org (home for Mod_Security)

http://www.owasp.org/index.php/Category:OWASP_WeBekci_Project
(Configuration tool)

www.apachesecurity.net

"Preventing Web Attacks with Apache", Ryan C. Barnett