

Forum:[Hack Forums](#)

Thread: [Need help regarding IDS and IPS.](#)

Pirate - June 1, 2015, 3:22 am

I just want to know that if I can monitor for any unusual activities on my website and also to block any particular IP which is trying to inject any malicious scripts in my website, and this process should be automatic. I just searched for this in google and got some results about Intrusion Detection System and Intrusion Prevention System but cannot find more detailed description. So if any of you could help me in this that would be a real great favor. So my questions are,

Can a firewall monitor suspicious activity like injecting scripts on the address bar and take action like a temporary block to that IP?

Can I make this process to be automatic?

Can I display a custom message to the IP through the page itself in which the unusual activity takes place?

Scy7e - June 1, 2015, 3:25 am

(Jun 1, 2015 03:22 AM)?Pulsar 220™ Wrote: [\[CITE\]](#) Can a firewall monitor suspicious activity like injecting scripts on the address bar and take action like a temporary block to that IP?

Can I make this process to be automatic?

Look up fail2ban, this does exactly what you want.

(Jun 1, 2015 03:22 AM)?Pulsar 220™ Wrote: [\[CITE\]](#) Can I display a custom message to the IP through the page itself in which the unusual activity takes place?

I don't see why you would want to do that. It's doable but not worth the effort.

Foundry - June 1, 2015, 4:28 am

An IPS acts as a watchdog, monitoring all incoming and outgoing packets from a network and matching data in the packets against a signature database (sometimes dynamic, usually not) against what it considers to be normal traffic. The difference between an IDS and an IPS is that an intrusion detection system is just meant to log threats and generate alerts for the sysadmin. Intrusion prevention systems can react to what they detect, and take steps to prevent the attack or mitigate the potential damage.

What you are looking for is a WAF, or Web Application Firewall. To steal some content from the SANS explanation:

Quote:IPSs do not have the ability to understand web application protocol logic. Hence, IPSs cannot fully distinguish if a request is normal or malformed at the application layer (OSI Layer 7). This short coming could potentially allow attacks through without detection or prevention, especially newer attacks without signatures.

Because there are so many different types of web applications in existence, there will be many vulnerabilities for an attacker to exploit which an IPS just won't be able to cover. It might even end up generating more false positives than anything, which just makes the sysadmin's job harder.

So enter the WAF: It's designed to protect web applications and web servers from attacks that IPSs

cannot prevent. Similar to an IPS, WAFs can be network or host based. They too sit in line and monitor all incoming and outgoing traffic from a web server for potentially malicious activity. Basically, the difference is in the level of ability to analyze the Layer 7 web application logic.

To steal even more from the SANS explanation:

Quote:Where IPSs interrogate traffic against signatures and anomalies, WAFs interrogate the behavior and logic of what is requested and returned. WAFs protect against web application threats like SQL injection, cross-site scripting, session hijacking, parameter or URL tampering and buffer overflows. They do so in the same manner an IPS does, by analyzing the contents of each incoming and outgoing packet.

WAFs not only detect attacks that are known to occur in web application environments, they also detect (and can prevent) new unknown types of attacks. By watching for unusual or unexpected patterns in the traffic they can alert and/or defend against unknown attacks. For example- if a WAF detects that the application is returning much more data than it is expected to, the WAF can block it and alert someone.

What I'd advise you to do is look at [ModSecurity](#), which is an open-source WAF supporting custom rulesets for what kinds of web-based attacks to detect and how to react to them. You'll need root access to your web server to install it, but that's a given seeing as you will be analyzing all traffic interacting with your web server and then making the web server do whatever is necessary to mitigate an attack. Once it's installed, I'd advise that you download the [OWASP ModSecurity Core Rule Set](#) and start using it. If you want to get a more advanced ruleset, Trustwave Spiderlabs (Makers of ModSecurity) offers a commercial ruleset which has more advanced mitigations and detection techniques (If you actually want a commercial solution, get the [Atomicorp rulesets](#) instead. Just saying!) But don't let that fool you, there are other rulesets available for free online that can serve your purpose just as well including the [Comodo rulesets](#).

Make sure to read the [FAQ](#)!

To answer the rest of your questions: Yes, this process is entirely automatic. The only user interaction that is really required is getting the WAF and the appropriate rulesets set up.

I'm not really sure if you can pop up that kind of message to an attacker though.

Pirate - June 1, 2015, 4:39 am

(Jun 1, 2015 03:25 AM)Scy7e Wrote: [\[CITE\]](#) Look up fail2ban, this does exactly what you want.

I don't see why you would want to do that. It's doable but not worth the effort.

I took a look over fail2ban.org and it seems to be fulfilling my needs, any detailed description or reference would be appreciated, thanks.

I'm working as a security engineer in a reputed website and I just gave the idea of live monitoring of suspicious activity in the meeting held last week and everyone appreciated and they wanted me to create a detailed PPT on this and I'm looking forward to it. The idea of showing the dox'd info to the exploiter along with a warning message seemed kinda cool to me also it can prevent them from proceeding of the exploitation.

Thank you very much for your time man, it is really appreciated.

(Jun 1, 2015 04:28 AM)|Foundry Wrote: [\[CITE\]](#) An IPS acts as a watchdog, monitoring all incoming and outgoing packets from a network and matching data in the packets against a signature database (sometimes dynamic, usually not) against what it considers to be normal traffic. The difference between an IDS and an IPS is that an intrusion detection system is just meant to log threats and generate alerts for the sysadmin. Intrusion prevention systems can react to what they

detect, and take steps to prevent the attack or mitigate the potential damage.

What you are looking for is a WAF, or Web Application Framework. To steal some content from the SANS explanation:

Because there are so many different types of web applications in existence, there will be many vulnerabilities for an attacker to exploit which an IPS just won't be able to cover. It might even end up generating more false positives than anything, which just makes the sysadmin's job harder.

So enter the WAF: It's designed to protect web applications and web servers from attacks that IPSs cannot prevent. Similar to an IPS, WAFs can be network or host based. They too sit in line and monitor all incoming and outgoing traffic from a web server for potentially malicious activity. Basically, the difference is in the level of ability to analyze the Layer 7 web application logic.

To steal even more from the SANS explanation:

What I'd advise you to do is look at [ModSecurity](#), which is an open-source WAF supporting custom rulesets for what kinds of web-based attacks to detect and how to react to them. You'll need root access to your web server to install it, but that's a given seeing as you will be analyzing all traffic interacting with your web server and then making the web server do whatever is necessary to mitigate an attack. Once it's installed, I'd advise that you download the [OWASP ModSecurity Core Rule Set](#) and start using it. If you want to get a more advanced ruleset, Trustwave Spiderlabs (Makers of ModSecurity) offers a commercial ruleset which has more advanced mitigations and detection techniques (If you actually want a commercial solution, get the [Atomicorp rulesets](#) instead. Just saying!) But don't let that fool you, there are other rulesets available for free online that can serve your purpose just as well including the [Comodo rulesets](#).

Make sure to read the [FAQ](#)!

To answer the rest of your questions: Yes, this process is entirely automatic. The only user interaction that is really required is getting the WAF and the appropriate rulesets set up.

I'm not really sure if you can pop up that kind of message to an attacker though.

One post taught me a lot more than number of google searches, I really owe you man. You spread the helping tendency! ?

BTW buddy, My company uses a firewall already and can I suggest them to add any of those WAF you have mentioned above as a secondary FW? Does the usage of two firewalls cause any harm like slow traffic etc?

hahdbwoannniabs - June 1, 2015, 8:11 am

The Sucuri WebSite Firewall and Cloudflare are both pretty good for what you're wanting.

|Foundry - June 1, 2015, 1:49 pm

(Jun 1, 2015 04:39 AM)?Pulsar 220™ Wrote: [\[CITE\]](#) I took a look over fail2ban.org and it seems to be fulfilling my needs, any detailed description or reference would be appreciated, thanks.

I'm working as a security engineer in a reputed website and I just gave the idea of live monitoring of suspicious activity in the meeting held last week and everyone appreciated and they wanted me to create a detailed PPT on this and I'm looking forward to it. The idea of showing the dox'd info to the exploiter along with a warning message seemed kinda cool to me also it can prevent them from proceeding of the exploitation.

Thank you very much for your time man, it is really appreciated.

One post taught me a lot more than number of google searches, I really owe you man. You spread the helping tendency! ?

It's just that fail2ban is only really suitable for brute-force mitigation

BTW buddy, My company uses a firewall already and can I suggest them to add any of those WAF you have mentioned above as a secondary FW? Does the usage of two firewalls cause any harm like slow traffic etc?

Alright, from my understanding of what you're saying it should go like this.

> Incoming traffic to your IP hits your firewall: If it is on a valid port, pass the traffic through to your network. If it's on a blocked port, stop it in its tracks. Since this is just a firewall and not an IDS/IPS, it won't analyze the contents of the traffic; only where it came from [client], where it's going [server], and how it intends to get there [port].

> Traffic on accepted ports (in the case of a web server, these are ports 80 and 443) gets passed along to your network, and subsequently to your web server. At this point, any IDS/IPS you have will probably have scanned the traffic for any detected malicious intent and reacted accordingly. If you don't have anything like that set up, then this step can be shortened down to the traffic just getting to the web server.

> Once the traffic is about to hit the web server, that's when the Web Application Firewall (WAF) comes in to play. It'll analyze the logic of the request which was sent to your website, and determine if it's a harmless query or a potential threat. If it seems alright, it will pass it to your webapp and the client will get the response. If the query seemed to be trying to achieve XSS, SQL injection, file upload, RCE, or anything else that a hacker would use to get control of your website, it will deny the traffic and throw an error to the client who tried it.

Just an FYI, WAFs can work in different ways depending on which solution you chose. Sometimes the WAF will act as a proxy and sit between the network and the web server (which is honestly the most secure solution), but this can be problematic if downtime is an issue. For that situation, solutions usually let you do a kind of port mirroring from your web server so that all traffic is split between the web server and the WAF so that if something goes wrong, there will always be a second path to the web server to minimize customer downtime.

In terms of what solution you use, everything has its own pros and cons. I suggested that you use ModSecurity since it is open source and free, but there are other options available to you if you're doing it for work (and if you can convince your management that its worth it, haha). You can do a bit of google-fu and try to figure out what best suits your needs.

So to answer your question, it won't cause network congestion or unnecessary speed issues since the two things are happening at different times in different ways. Your firewall is like the bouncer at a nightclub, but you still have to treat the girls nice inside or else you'll get kicked out for trying anything funny. ?

Best of luck with getting your intruder mini-doxing system set up, seems like a pretty neat idea!

I'll just throw this out there: fail2ban is woefully inadequate for protecting your web site since an attacker could just fuzz whatever he wants by switching IPs, or use his own commonly-unpatched exploit against your website to then compromise it. Fail2ban will do -absolutely nothing- since it thinks "oh well it only happened once so i don't think anything is wrong!", and the attacker would have gotten XSS, stolen information from your database, or done whatever else he wanted without fail2ban raising an eyebrow. Also, not everything is written to a log in a parseable format for tools like this, which may leave holes in your system which you think are covered.

I'm not saying this as an advertisement for WAFs since I'm not professionally affiliated with any company which offers that kind of service by the way ?

Pirate - June 3, 2015, 12:54 am

(Jun 1, 2015 01:49 PM)|Foundry Wrote: [\[CITE\]](#) Alright, from my understanding of what you're saying it should go like this.

I'm not saying this as an advertisement for WAFs since I'm not professionally affiliated with any company which offers that kind of service by the way ?

Thank you very much man, I really really owe you! :) Will surely get back to you if I get struck anywhere! Thanks again! :)

mkbuzz - June 3, 2015, 6:30 pm

Lookup for modsecurity - an open source web application firewall. or if you want cloud solution then cloudflare is best option as they also provide free service for protecting your website. You just need to change the DNS and redirect them to cloudflare one.

Cheers,