FACULDADE DE TECNOLOGIA SENAC GOIÁS
Segurança da Informação

Aldo Brito
Leniker Lettierre
Matheus Mello
Rony Carneiro

WEB APPLICATION FIREWALL

Fernando Pirkel Tsukahara

GOIÂNIA,
2017

Aldo Brito
Leniker Lettierre
Matheus Mello
Rony Carneiro

WEB APPLICATION FIREWALL

Relatório apresentado como requisito parcial para obtenção de aprovação no Projeto Integrador, no Curso de Segurança da Informação, na Faculdade de Tecnologia Senac Goiás.

Fernando Pirkel Tsukahara

GOIÂNIA,
2017

SUMÁRIO

1 WEB APPLICATION FIREWALL (WAF)

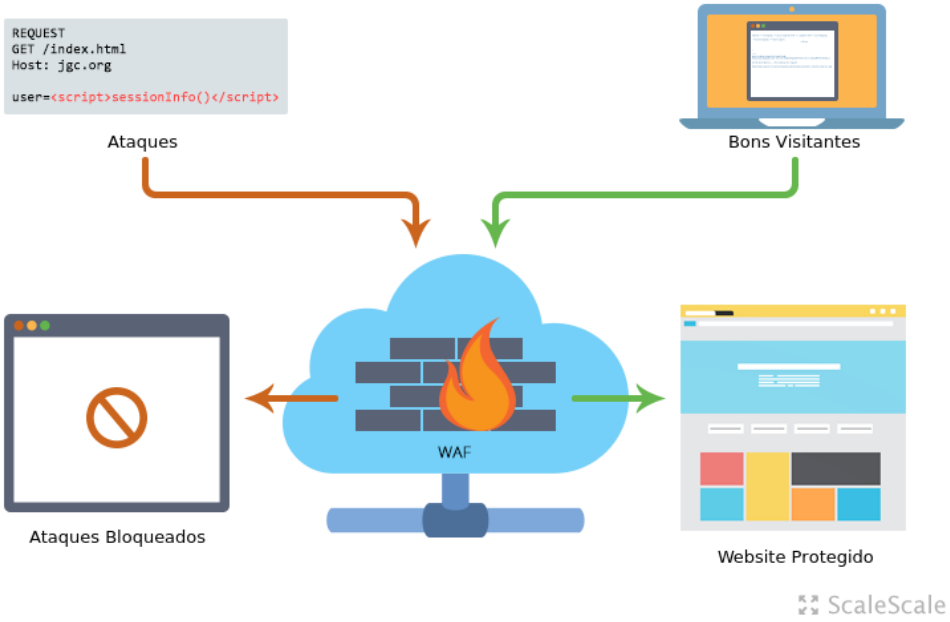
Ataques às aplicações web são constantes, com os atacantes buscando acesso não-autorizado para dados sensíveis como cartões de crédito e dados de usuários. Essas informações permitem aos criminosos realizarem crimes em nome de outras pessoas, fraudes financeiras entre outros crimes. Como muitos desses dados estão acessíveis via back-end das aplicações web, os criminosos frequentemente atacam as aplicações para conseguir esses dados sensíveis.

O WAF (Web Application Firewall - Firewall de Aplicação Web) é um aparelho, plugin do servidor, ou filtro que se aplica um conjunto de regras para uma conversa HTTP. Geralmente, estas regras cobrem ataques comuns, tais como Cross-site Scripting (XSS) e SQL Injection. Ao personalizar as regras para sua aplicação, muitos ataques podem ser identificados e bloqueados.

O WAF foi criado para prevenir que esses ataques às aplicações web comprometesse os servidores e as bases de dados que estão por trás deles, em última instância prevenindo vazamentos de dados. Ainda que todas as aplicações web que uma empresa pode utilizar podem ser protegidas por um WAF, o melhor ROI ocorre quando a empresa protege aplicações desenvolvidas por terceiros, às quais ela não possui acesso ao código fonte. Nesse cenário, a empresa não pode corrigir diretamente as vulnerabilidades presentes nessas aplicações. Não existe forma para a empresa fazer essa correção, a não ser requisitando ao desenvolvedor por mudanças e aguardando atualizações de correção. Isso deixa um gap de médio e curto prazo, às vezes até de longo prazo, onde a empresa precisa intervir e colocar uma camada de WAF de forma a compensar por essas vulnerabilidades presentes na aplicação.

1.1 COMO UM WAF FUNCIONA

Um WAF pode ser implementado de diferentes formas, incluindo uma appliance física, uma appliance virtual ou um serviço baseado na nuvem, posicionado em frente aos servidores web; também pode ser posicionado como um add-on baseado em servidor que funciona diretamente em cada servidor web. Independente da forma como é implementado, um WAF intercepta as requisições de protocolo HTTP, garantindo que são benignas antes que os servidores iniciem o processamento. O WAF analisa cada requisição HTTP assim como cada resposta dos servidores web, considerando dezenas de tipos de ataques conhecidos a aplicações web como: hijacking de sessão, caminho transversal, buffer overflow, DDoS, XSS e SQL Injection. Se o WAF detecta um ataque, ele pode bloquear as requisições ou as respostas correspondentes de atingir o alvo, dessa forma prevenindo que o ataque seja bem-sucedido.



1.2 FERRAMENTAS WAF

Assim como em outros ativos de solução, diferentes WAF podem ter diferentes capacidades. Obviamente, é ideal que o WAF detecte os ataques às aplicações web as quais ele foi implementado para proteger. Os ataques em aplicações web estão cada vez mais customizados para atingir alvos particulares, tornando difícil que tecnologias básicas consigam identificá-los. Para deter esses ataques avançados, os gestores de segurança devem buscar por WAF's que detectem novos ataques, incluindo ataques de zero-day em vulnerabilidades previamente desconhecidas.

Ao mesmo tempo, é importante que os gestores considerem no momento da aquisição um WAF que não gere tantos falsos positivos. Um falso positivo ocorre quando uma atividade legítima é erroneamente categorizada como maliciosa e inadvertidamente bloqueada, atrapalhando a performance das operações. Um WAF deve ter medidas para minimizar falsos positivos, ou barrar uma onda massiva de alertas que, no final das contas, causarão tantos problemas que os gestores irão acabar por desabilitar o WAF ou parte de suas funcionalidades, deixando o ambiente inseguro.

Outra capacidade a ser identificada é a utilização de uma inteligência de ameaças de alta qualidade. Os serviços de reputação possuem dados sobre IP's maliciosos, domínios e outras características de rede que podem ser associadas à atividades maliciosas. WAF's e outros ativos podem usar essa informação para identificar os pontos de ataque antes mesmo deles ocorrerem. No mínimo, um bom WAF deve receber um feed constante e sempre atualizado com informações sobre reputação.

1.3 MODSECURITY

O ModSecurity é um WAF Open Source que trabalha em conjunto como um módulo do apache ou do Nginx. Neste projeto ele foi instalado juntamente com o apache onde está o sistema, ele poderia ter sido instalado em um proxy apache.

Apesar dele ser um bom WAF, ele possui um nível de complexidade em sua implementação, pois o pacote que está no repositório do Debian tem uma versão obsoleta. Então para utilizar as versões mais recentes é necessário compilar o ModSecurity. A versão utilizada do modSecurity foi a 2.8.0.

Apenas a instalação do ModSecurity é inútil, ele necessita de regras para funcionar, sendo essas regras disponibilizadas pela própria equipe que o mantém. Há regras gratuitas e pagas, no nosso projeto utilizamos regras gratuitas versão 2.2.9. Também é possível criar regras específicas para a aplicação, diminuindo assim os falsos positivos e mitigando mais tipos de ataques.

2 CONCLUSÃO

OS WAF's são soluções muito úteis para proteger suas aplicações web contra uma ampla variedade de ataques. Ao passo em que os WAF são mais úteis para aplicações às quais a empresa não possui o código fonte, outras aplicações web podem se beneficiar do fato de que os WAF's oferecem proteção durante o gap de descoberta de vulnerabilidade e aplicação de patches de correção. Empresas que possuem dados sensíveis em aplicações web definitivamente devem utilizar ativos de WAF como uma linha de defesa importantíssima contra incidentes de segurança.

REFERÊNCIAS BIBLIOGRÁFICAS

https://realprotect.net/blog/web-application-firewall-waf-interrompa-os-ataques-aplicacoes-web/

http://blog.siteblindado.com/2014/02/07/o-que-e-waf/

ModSecurity: https://github.com/SpiderLabs/ModSecurity

Regras do ModSecurity: https://github.com/SpiderLabs/owasp-modsecurity-crs/

Documentação ModSecurity: https://github.com/SpiderLabs/ModSecurity/wiki

Documentação das Regras: https://www.modsecurity.org/CRS/Documentation/