FORTINET
NSE Training Institute

NSE 2 Web Application Firewall Scripts—Spanish Version

¡Hola! En esta clase, hablaremos de los firewalls de aplicaciones web, o WAF, y de cómo han evolucionado con el tiempo. ¿Qué es un WAF y en qué se diferencia de un firewall perimetral tradicional?

Un WAF es un dispositivo o un software que monitorea el tráfico HTTP/HTTPS y puede bloquear el tráfico malicioso desde una aplicación web y hacia ella. La diferencia con un firewall perimetral tradicional es que el objetivo de un WAF es el contenido de aplicaciones web específicas y a nivel de la aplicación. En cambio, los firewalls perimetrales crean puertas de enlace seguras entre la red de área local y los servidores externos a nivel de la red. En concreto, al inspeccionar el tráfico HTTP, un WAF puede detener los ataques que se originan en fallas de seguridad de las aplicaciones web, como la inyección SQL, el scripting entre sitios, la inclusión de archivos y las configuraciones incorrectas de seguridad. Como dedicamos mucho tiempo a interactuar con aplicaciones y servidores web, tanto en el trabajo como en el hogar, los WAF son un elemento esencial para la lucha contra los agentes maliciosos y sus actividades en línea.

El antecedente del WAF es el firewall de aplicaciones que se creó en la década de 1990. Aunque era sobre todo un firewall basado en la red, funcionaba con ciertas aplicaciones o protocolos, como el protocolo de transferencia de archivos, o FTP, y Remote Shell, o RSH, un programa informático de línea de comandos. La aparición de la red informática mundial o WWW en 1991 fue el *big bang* del universo de internet, que desde entonces se viene expandiendo a un ritmo acelerado. La accesibilidad y la apertura de internet permitieron que **cualquiera** pudiera buscar y explorar, pero también que los agentes maliciosos la usaran para sus propios fines oscuros.

A medida que más personas y organizaciones eran víctimas de espionaje, robo y otros delitos, el desarrollo de una defensa contra los ciberataques basados en HTTP se convirtió en una prioridad fundamental. Los WAF no podían confiar en los métodos tradicionales de los firewall perimetrales, que basaban sus decisiones en una lista negra de direcciones de red y bloqueaban ciertos protocolos y números de puerto. Como todas las aplicaciones web utilizaban HTTP y el puerto 80 o el 443, este enfoque no era muy práctico.

Veamos ahora un método común de ataque llamado "inyección SQL". Imagine que tiene un negocio en línea y que los clientes y los socios inician sesión en su sitio para adquirir productos y servicios. En general, las páginas de inicio de sesión solicitan un nombre de usuario y una contraseña. Una persona, digamos Juan Pérez, escribe su nombre de usuario (jperez) y su contraseña. Esta información se verifica en una base de datos de *back-end*. Si la contraseña es correcta, Juan Pérez ingresa, pero si es incorrecta, no puede hacerlo.

Ahora bien, un agente malicioso probablemente no conozca la contraseña de Juan. Podría intentar adivinarla, pero le llevaría mucho tiempo. En cambio, en lugar de la contraseña, el agente malicioso escribe "abc123 o 2 + 2 = 4". Cuando las credenciales de Juan se envían a la base de datos para su verificación, es probable que la contraseña "abc123" sea incorrecta. Sin embargo, la expresión 2 + 2 = 4 es verdadera. Debido a esta falla, el agente malicioso puede ingresar a algunos sitios. La primera generación de WAF utilizaba listas negras y atributos HTTP basados en firmas para alertar al firewall sobre un ataque, por lo que los ataques de inyección SQL como este dejaron de ser exitosos.

Debido al gran crecimiento de internet, al poco tiempo, la enorme cantidad de aplicaciones web y su complejidad cada vez mayor hicieron que el enfoque basado en firmas se volviera obsoleto. Además, el número de falsos positivos (las alertas de ataques que, en realidad, eran conexiones legítimas) creció en proporciones que superaron la capacidad de los equipos de seguridad de TI. La siguiente generación de WAF era más inteligente, ya que los firewalls tenían un componente de aprendizaje. Los WAF podían aprender el comportamiento de las aplicaciones y establecer una referencia para evaluar si los intentos de acceder a las aplicaciones eran normales o si, en cambio, eran irregulares y, por lo tanto, sospechosos. Esta nueva generación también introdujo el monitoreo de sesiones y el método heurístico, lo que permitía al firewall detectar variantes de firmas conocidas. Si bien fue un avance, como el aprendizaje de las aplicaciones era supervisado por los equipos de seguridad de TI, la defensa no podía estar al día con la creciente cantidad de mutaciones en los métodos existentes ni con las nuevas vulnerabilidades. Además, no existía una defensa contra las vulnerabilidades de día cero, que aprovechaban una falla desconocida en el código de una aplicación.

Lo lógico era que el desarrollo de los WAF incluyera el aprendizaje automático sin supervisión humana. Así, el análisis del comportamiento podía realizarse a la velocidad de la máquina y adaptarse a los atributos de las amenazas, que cambiaban constantemente. También se agregaron otras características de seguridad a los firewalls. Entre otros, estos recursos incluían:

- defensa contra ataques de denegación de servicio distribuido o DDoS
- reputación de IP
- antivirus
- prevención de pérdida de datos o DLP

De este modo, los firewalls podían realizar un monitoreo de HTTP y detener cualquier acción que no representara un comportamiento aceptable. Eran capaces de identificar al usuario y correlacionarlo con la acción que intentaba llevar a cabo con sus permisos, y podían detenerla si excedía las funciones del usuario. Los WAF también se diseñaron para compartir información y colaborar con los demás dispositivos de seguridad en la red, como otros firewalls y entornos de sandbox. Así fue posible integrar los firewalls con sistemas de defensa colectiva que estaban interconectados, en lugar de trabajar de manera independiente. Y los entornos de sandbox permitieron que los elementos sospechosos se probaran de forma segura y aislados de la red. Los ataques de día cero podían detectarse y ponerse en cuarentena en estos entornos seguros, y sus firmas podían compartirse con otros dispositivos de la red. Además, los nuevos descubrimientos podían enviarse a un centro de información sobre amenazas en internet, donde a su vez podían comunicarse a otras redes.

Fortinet ofrece un WAF conocido como FortiWeb™. FortiWeb™ puede integrarse con FortiGate® y con FortiSandbox™. FortiGuard® Labs es el centro de información sobre amenazas de Fortinet y brinda actualizaciones para FortiWeb™ y otros productos de Fortinet Security Fabric.

Gracias por su tiempo, y no olvide responder las preguntas a continuación.