ManageEngine
Log360

A beginner's handbook on

Web server auditing

www.manageengine.com/log360

Introduction

Virtually every business today has its own website, and for many, websites are a direct source of revenue. The web servers businesses use to run their website may be accessed by employees, customers, or business partners, meaning they deal with a lot of sensitive information.

Recent attacks have highlighted the importance of information security by reminding businesses of the repercussions of a cyber breach—legal action, fines, and a loss of customer trust. As a result of these high-profile breaches, regulatory mandates across the world are insisting on tighter security systems to improve incident detection and resolution. They're also stressing mandatory breach notifications that alert governing authorities about a breach within a stipulated time frame.

It's safe to say that the recent spate of cyber breaches and stringent compliance mandates have prompted many security professionals, perhaps even yourself, to reassess their security strategy and tools. All of these developments have made securing all your business's applications, particularly business-critical ones like web servers, even more crucial. Remember, attacks can happen to anyone, which is why it's important for small and medium sized enterprises to increase their IT security budget and procure cutting-edge security technology.

In this handbook, you will learn about the basics of web server auditing and how it can help you implement a tighter application security program in your enterprise.

Web server threats

Web servers are the gateway for communication between the internet and your enterprise network. Web applications require that certain ports be open for communication with end users, which means hackers can use sophisticated attack techniques to exploit a vulnerability in your web server and compromise your network security.

Web servers are prone to many different security threats, such as requests that try to run malicious scripts. Other common attacks include:

- DDoS
- SQL injection
- XSS (Cross-site scripting)

Ensuring web server security and business continuity

Since web servers are front-end facing applications that customers use to access data stored in your database, hardening web server security is important to protect sensitive data. Administrators are always concerned about ensuring IT is up and running for business continuity. If your website gets attacked, it will not only affect business continuity, but also put your enterprise at risk of losing customers' trust. Further, in case you do encounter an attack, your enterprise will be liable to compliance and legal penalties if found not to have proper security systems in place.

It can be challenging to monitor the traffic going through your application layer, and firewalls and IDS/IPS systems alone won't be enough to safeguard your web server. All these points make a strong case for going beyond traditional security defenses and looking at specialized tools to mitigate attacks and ensure your web server is always up and running.

Auditing web server activity

Web server logs contain crucial security information, not limited to important events pertaining to web server usage and errors. Further, FTP server logs contain valuable information about files being uploaded and shared by users. If activity on the web server is unchecked, and threats aren't detected at an early stage, then the consequences can be dire.

IT teams need to track web server activities to identify different security events of interest. This audit information will put security teams in a position to discover web server threats as soon as possible and quickly take action to curb attacks.

Configuring logging on your web server

The first step for tracking web server activity is to configure logging on your web server. This entails defining an audit policy that specifies what events need to be tracked and what information about those events needs to be recorded.

As an administrator, your job is to select the information that needs to be present in the log message, such as the date, time, and client IP address. Then you need to specify which directory log files will be stored in, schedule the generation of log files, and specify other details pertaining to file naming and rollover. Overall, it is important to audit the right set of events and specify a time interval that meets your requirements and bandwidth.

Analyzing logs using a SIEM solution

Once you have specified an audit policy, you need to centralize these logs for analysis, correlate event data, and extract meaningful information that can help in detecting and thwarting threats. It can be challenging to peruse through large volumes of log data to pinpoint an event which could raise a security concern. This is where a security information and event management (SIEM) solution can help.

A SIEM solution can analyze large volumes of audit data, correlate the events involved, and send you alerts for security events of interest. With the help of a SIEM tool, you can run reports on what exactly is going on in your web server and get a clear picture of important events such as failed authentication, bad requests, and more. You will also receive alerts for events that pose a threat to security. In this way, you can leverage a SIEM solution to reduce the time it takes to detect and respond to threats.

Web servers are an important log source in any SIEM solution. You can set up your SIEM tool to periodically import log data from the location you specified while configuring your web server's

ManageEngine
Log360

Log360, a SIEM tool from ManageEngine, can thoroughly audit IIS and Apache web server logs with its predefined reports and alert profiles. The graphical reports neatly present important audit information and can easily be drilled down to the raw log data. Log 360's alert profiles ensure you are alerted about critical events that could pose a threat to your security. Its built-in incident management console can automatically raise an alert as a ticket that's assigned to a designated administrator, ensuring efficient and accountable incident responses. The solution also helps with forensic analysis in the event of a breach, so you can file a detailed incident report for auditors.

Log360's auditing and alerting capabilities can help in:

1 Detecting and responding to web server threats

Log360 can help in detecting malicious activity and targeted attacks on your web server. The solution can detect and alert you about malicious URL requests from the same source within a short period of time, repeated SQL injection attempts, and other activities that pose a threat to web server security. Receive alerts via SMS or email, or configure Log360 to automatically raise a ticket based on an alert and delegate that ticket to the right administrator, ensuring incidents are responded to quickly.

2 Auditing web server usage and errors

Log360's "Top" reports display the most frequent web server visitors and errors, as well as the most frequently accessed pages and other important information at a glance. The "Trend" reports offer an overview of usage trends in a neat, graphical format.

Your web server might generate thousands of HTTP status codes on any given day. Although difficult to monitor manually, errors on your web server are important for understanding your end users' experience. Anomalous activity, such as a sudden spike in a particular HTTP error code (e.g. HTTP 200 errors), could also indicate potential misuse or an attack on your web server. Log360 can help you visualize all these HTTP status codes, identify the top errors, and detect sharp deviations from routine behavior which could mean an attack is underway.

3 Forensic analysis and reporting breaches

Despite administrators' best efforts, not all attacks can be prevented. A SIEM solution can not only help with threat mitigation, but also with damage control. Log360 collects and archives log data, and allows you to easily search through large data sets to find specific details about an attack.

For instance, if you face an attack like SQL injection, your web server logs will record important information about the attack, such as the date, time, and the IP address that launched the attack. This information is critical while reporting a breach and filing an incident report, which is a crucial aspect of meeting regulatory mandates.

4 User and Entity Behaviour Analytics (UEBA)

Take your organization's network security up a notch by using ManageEngine's Log360 UEBA add-on. This add-on monitors user activity captured in logs to identify behavioral changes using machine-learning algorithms. It also gives actionable insights to the IT administrator with the use of risk scores, anomaly trends, and intuitive reports. User activities that would otherwise go unnoticed are flagged, reducing the time it takes to detect and respond to threats.

The highlights of Log360 UEBA include:

- Anomaly detection: Spots deviant user and entity behavior such as logons at unusual hours, excessive logon failures, and file deletions from a host that is not generally used by a particular user.
- Score-based risk assessment: Generates a risk score for each user and entity based on how dangerous their behavior is, helping security admins determine which threats merit investigation.
- Threat corroboration: Identifies indicators of compromise and indicators of attack, exposing major threats including insider threats, account compromise, and data exfiltration.

Click here to know more about Log360's UEBA add-on.

Conclusion

Auditing your web server logs with a SIEM solution helps you monitor web server activity and stay on top of attacks. Generate reports, configure alerts for security threats, and conduct a forensic investigation in case something goes wrong using a SIEM tool like Log360.

About the author

Siddharth Sharathkumar is a computer science engineer who works in ManageEngine's product marketing team. He writes IT security articles and technical guides, presenting webinars on key security topics to educate security professionals and help enterprises solve their security challenges as well.

Check out his blogs here.

About ManageEngine

ManageEngine delivers the real-time IT management tools that empower an IT team to meet an organization's need for real-time services and support. Worldwide, more than 60,000 established and emerging enterprises — including more than 60 percent of the Fortune 500 — rely on ManageEngine products to ensure the optimal performance of their critical IT infrastructure, including networks, servers, applications, desktops and more. ManageEngine is a division of Zoho Corp. with offices worldwide, including the United States, United Kingdom, India, Japan and China.