ManageEngine
EventLog Analyzer

Malicious script detection through web server auditing

www.eventloganalyzer.com

Introduction

In today's digitally-focused world, almost every business has an online presence, and many of those that do even provide a good portion of their services online. These services typically involve the exchange of sensitive business and end-user information, such as names, contact details, or payment information. An organization's website and web applications are therefore crucial elements in building relationships with its target audience. An attack on its web servers would cause a severe disruption to business continuity.

And yet, according to Verizon's Data Breach Investigations Report 2018, web application attacks were the most common form of attack, as these attacks were involved in 18.5% of all security incidents. The IT and retail industries are particularly susceptible to these types of attacks. So why is it that we're witnessing such a disturbing trend of attacks on web applications?

This might be because security is often overlooked in an effort to provide light, fast, and easy-to-use applications. Security loopholes, such as poor data protection and weak input validation, allow hackers to retrieve sensitive data or inject malicious scripts into websites or web servers. In this guide, we discuss malicious script execution and how you can detect it using web server auditing.

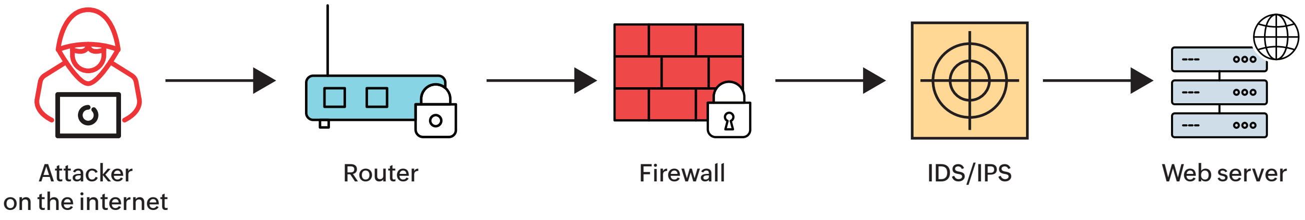
The use of malicious scripts to attack web servers

A preferred method to breach web servers is by injecting malicious code into the website or web server. This code either targets your organization's systems, or it tries to gather confidential information from the users visiting your website—neither of which paint a very pleasant picture for your business. Malicious scripts can be used to achieve a variety of things, such as:

- **Gaining control of a target system, which could be a file server or database that holds confidential information.**
- **Utilizing infected systems in botnet attacks.**
- **Spying on user activity.**
- **Retrieving sensitive data.**
- **Redirecting users to malicious sites.**
- **Hosting malicious or unwanted advertisements.**
- **Launching cryptomining malware.**

Put simply, if an attacker is creative enough, there's no limit to the ways they can exploit a website vulnerability.

Anatomy of a web server attack



An attacker can communicate with your organization's web server through your website or web application. By exploiting vulnerabilities, they are able to include malicious content in their communication. As seen above, the network packet has to pass through a few security layers before reaching your web server. By auditing your network at each of these stages, you can ensure that your web server stays protected from attacks.

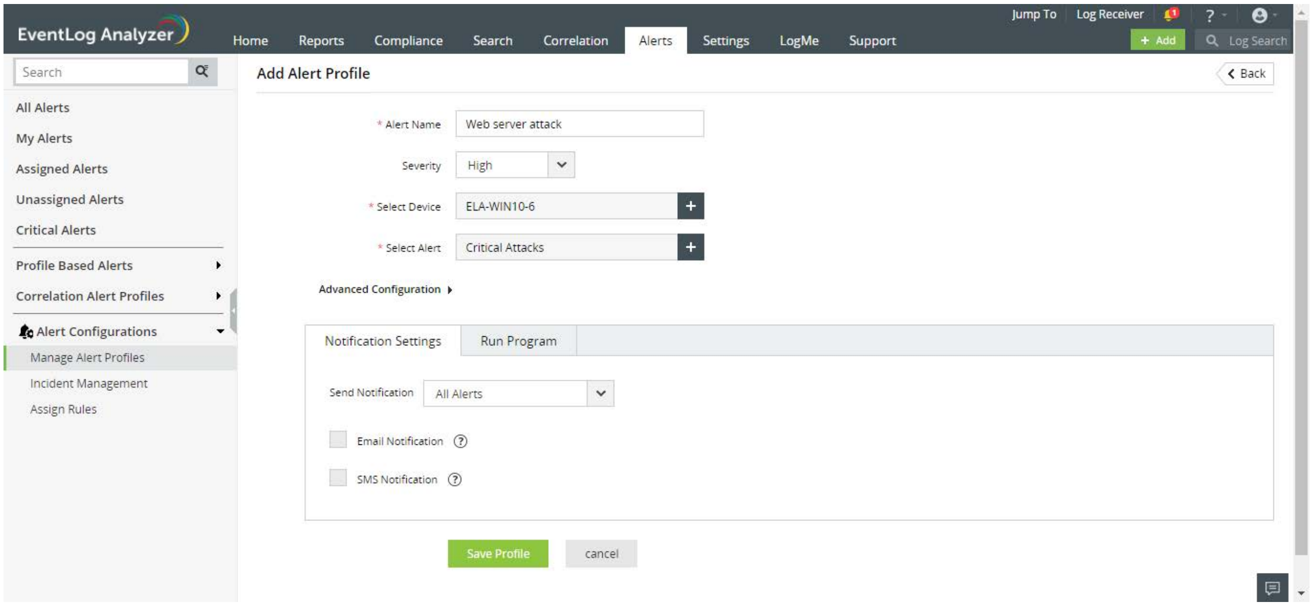
Leveraging EventLog Analyzer to detect web server attacks

EventLog Analyzer is a comprehensive log management software that is capable of tracking any malicious activity on web servers. It gives you a complete overview of the activities on your web servers, including crucial insight into usage patterns. The analytics are presented in the form of comprehensive and intuitive reports that are categorized into:

- **Top reports:** Track the most frequently occurring activity with respect to users, methods, pages, and more.
- **Error reports:** Track the errors that users face on your website.
- **Attack reports:** Track attempted attacks on your web server.

Here are a few techniques you can use to detect and investigate attacks targeting your web server using EventLog Analyzer:

1. Set up alerts for potential attacks detected by your network devices.



Add Alert Profile

* Alert Name: Web server attack

Severity: High

* Select Device: ELA-WIN10-6

* Select Alert: Critical Attacks

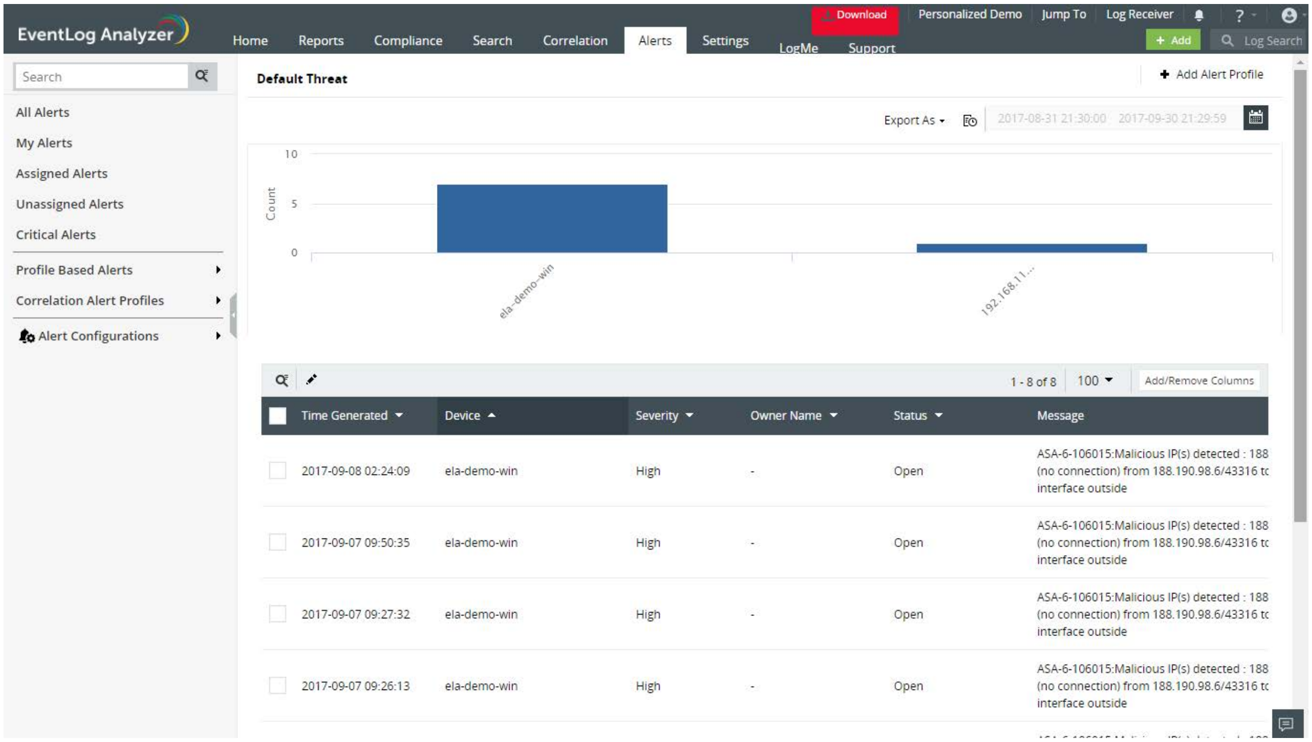
Send Notification: All Alerts

□ Email Notification

□ SMS Notification

You can be notified instantly via email or SMS if potential attacks or malicious traffic are detected by your web server. This includes alerts for denial of service (DoS) attacks and malicious URL requests. You can even set up alerts at the intrusion detection system (IDS) or firewall stage. You can also use the product's built-in ticketing features to manage each alert as an incident ticket, assign it to an owner, and track its status.

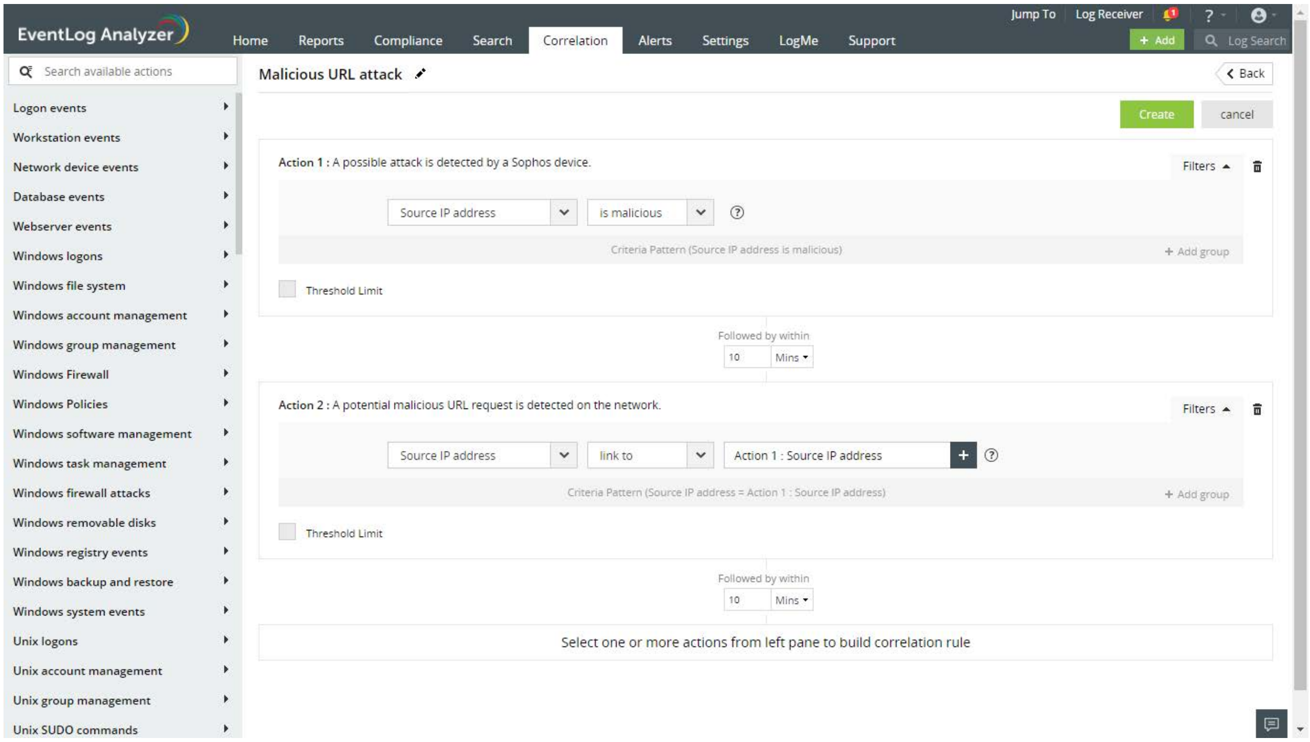
2. Flag traffic from malicious sources with threat intelligence.



□	Time Generated	Device	Severity	Owner Name	Status	Message
□	2017-09-08 02:24:09	ela-demo-win	High	-	Open	ASA-6-106015:Malicious IP(s) detected : 188 (no connection) from 188.190.98.6/43316 tc interface outside
□	2017-09-07 09:50:35	ela-demo-win	High	-	Open	ASA-6-106015:Malicious IP(s) detected : 188 (no connection) from 188.190.98.6/43316 tc interface outside
□	2017-09-07 09:27:32	ela-demo-win	High	-	Open	ASA-6-106015:Malicious IP(s) detected : 188 (no connection) from 188.190.98.6/43316 tc interface outside
□	2017-09-07 09:26:13	ela-demo-win	High	-	Open	ASA-6-106015:Malicious IP(s) detected : 188 (no connection) from 188.190.98.6/43316 tc interface outside

If a malicious network packet is well concealed, your network devices may not pick up on it. However, the source may be a known malicious entity. EventLog Analyzer's threat intelligence platform processes more than 600 million malicious IP/URL sources to help you detect threat actors in your network. The threat database is automatically updated with the latest information on a daily basis. EventLog Analyzer's real-time alerting console is closely tied with this database. The preconfigured threat alert traces any incoming and outgoing traffic from malicious sources and alerts you in real time.

3. Use event correlation to validate a potential attack pattern.



Malicious URL attack

Action 1 : A possible attack is detected by a Sophos device.

Source IP address | is malicious

Criteria Pattern (Source IP address is malicious)

□ Threshold Limit

Followed by within 10 Mins

Action 2 : A potential malicious URL request is detected on the network.

Source IP address | link to | Action 1 : Source IP address

Criteria Pattern (Source IP address = Action 1 : Source IP address)

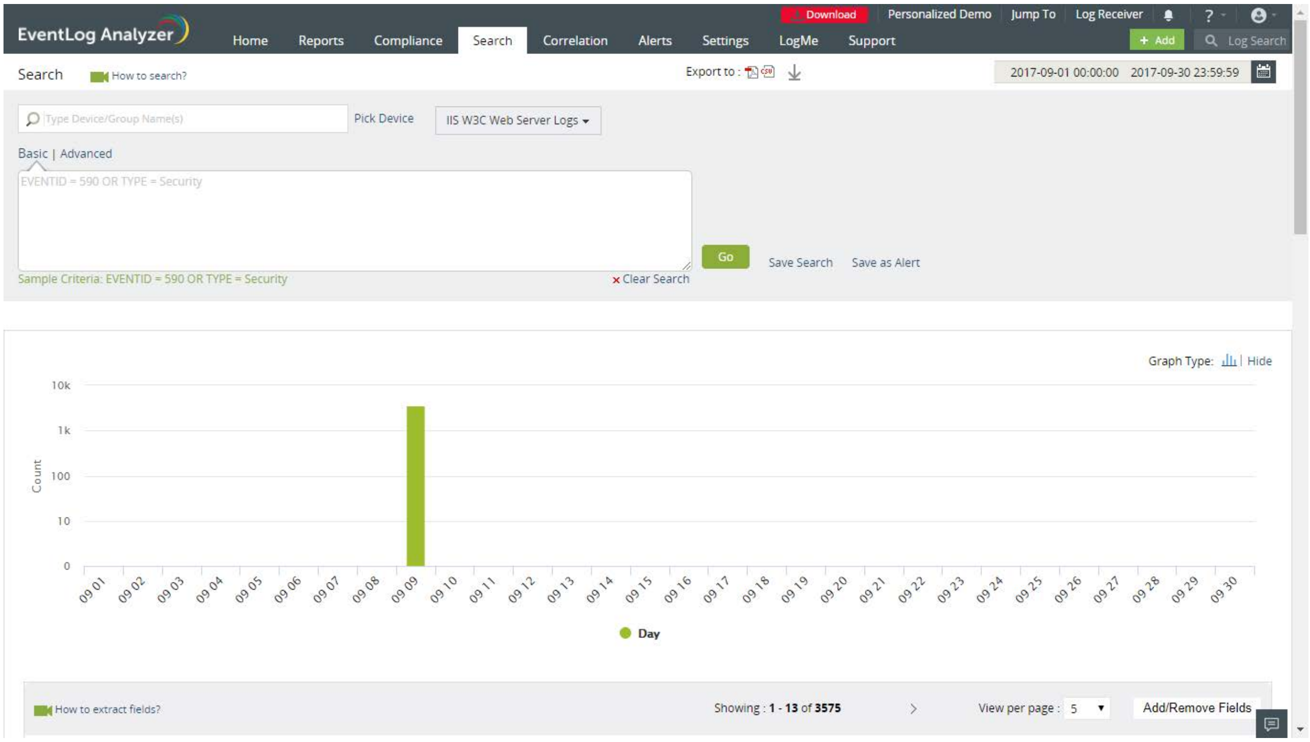
□ Threshold Limit

Followed by within 10 Mins

Select one or more actions from left pane to build correlation rule

You can use the product's event correlation module to add more context and validate events from your web server with those from other network devices—such as your firewall or IDS—and raise an alert only if the event seems suspicious. For example, you can create a rule to be notified if a possible attack is detected by your IDS and your web server flags a potentially malicious URL request from the same IP address.

4. Conduct forensic investigations using search.



2017-09-01 00:00:00 2017-09-30 23:59:59

Type Device/Group Name(s)

IIS W3C Web Server Logs

EVENTID = 590 OR TYPE = Security

Sample Criteria: EVENTID = 590 OR TYPE = Security

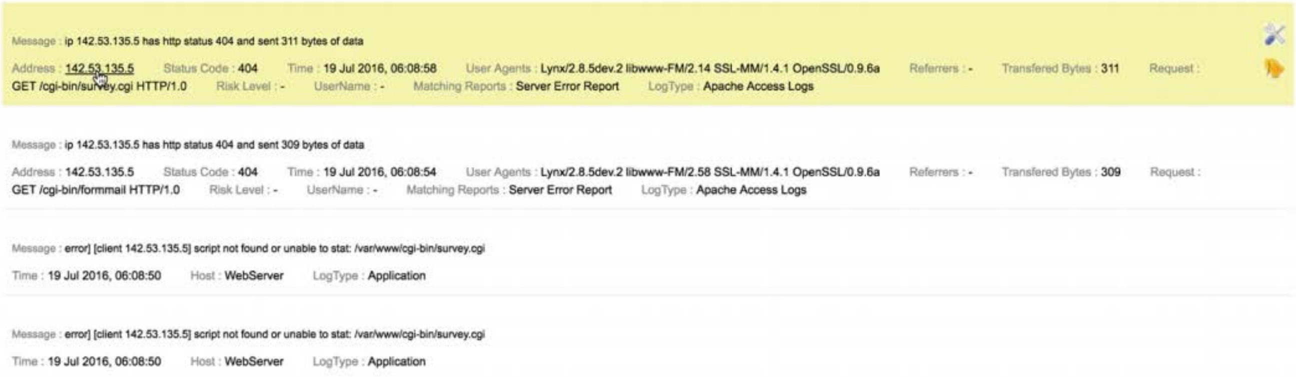
Showing : 1 - 13 of 3575

You can also use EventLog Analyzer's powerful search engine to backtrack any event and discover its source. The procedure to do this is explained in the next section.

Backtracking attacks with EventLog Analyzer

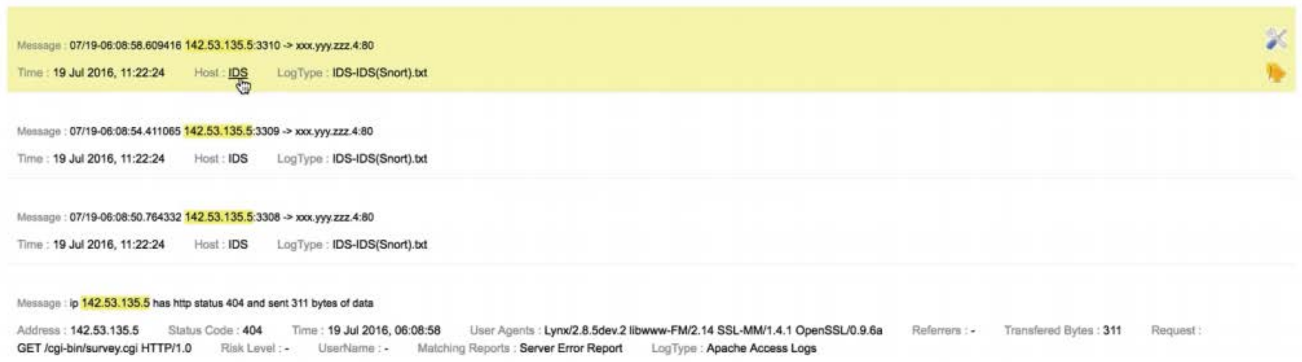
When you receive an alert about a possible malicious request to your web server, you can launch a search of your web server logs and investigate the attack pattern. A sample investigation is illustrated below:

- When going through the logs of your web server where the compromise was indicated, there's an entry for a request to access the web server via an open SSL connection.



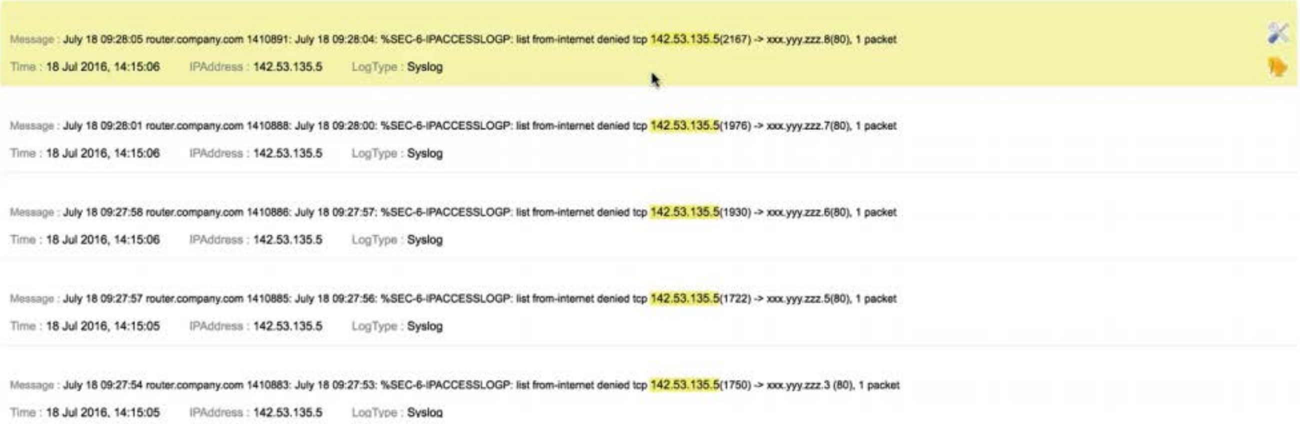
```
Message : ip 142.53.135.5 has http status 404 and sent 311 bytes of data

Address : 142.53.135.5     Status Code : 404     Time : 19 Jul 2016, 06:08:58     User Agents : Lynx/2.8.5dev.2 libwww-FM/2.14 SSL-MM/1.4.1 OpenSSL/0.9.6a     Referrers : -     Transfered Bytes : 311     Request :
GET /cgi-bin/survey.cgi HTTP/1.0     Risk Level : -     UserName : -     Matching Reports : Server Error Report     LogType : Apache Access Logs

Message : ip 142.53.135.5 has http status 404 and sent 309 bytes of data

Address : 142.53.135.5     Status Code : 404     Time : 19 Jul 2016, 06:08:54     User Agents : Lynx/2.8.5dev.2 libwww-FM/2.58 SSL-MM/1.4.1 OpenSSL/0.9.6a     Referrers : -     Transfered Bytes : 309     Request :
GET /cgi-bin/formmail HTTP/1.0     Risk Level : -     UserName : -     Matching Reports : Server Error Report     LogType : Apache Access Logs

Message : error] [client 142.53.135.5] script not found or unable to stat: /var/www/cgi-bin/survey.cgi

Time : 19 Jul 2016, 06:08:50     Host : WebServer     LogType : Application

Message : error] [client 142.53.135.5] script not found or unable to stat: /var/www/cgi-bin/survey.cgi

Time : 19 Jul 2016, 06:08:50     Host : WebServer     LogType : Application
```

- Following the access request, there will be a request from that same IP address to run a script.
- Click on the **Address** field in the log message to view the details of all the requests made by that particular IP address to the specified web server.
- Then, check where else this IP address hit your network by typing the concerned IP address into the search field. Go through these logs and see whether or not the IP address hit the IDS.



```
Message : 07/19-06:08:58.609416 142.53.135.5:3310 -> xxx.yyy.zzz.4:80
Time : 19 Jul 2016, 11:22:24      Host : IDS      LogType : IDS-IDS(Snort).txt

Message : 07/19-06:08:54.411065 142.53.135.5:3309 -> xxx.yyy.zzz.4:80
Time : 19 Jul 2016, 11:22:24      Host : IDS      LogType : IDS-IDS(Snort).txt

Message : 07/19-06:08:50.764332 142.53.135.5:3308 -> xxx.yyy.zzz.4:80
Time : 19 Jul 2016, 11:22:24      Host : IDS      LogType : IDS-IDS(Snort).txt

Message : ip 142.53.135.5 has http status 404 and sent 311 bytes of data
Address : 142.53.135.5    Status Code : 404    Time : 19 Jul 2016, 06:08:58    User Agents : Lynx/2.8.5dev.2 libwww-FM/2.14 SSL-MM/1.4.1 OpenSSL/0.9.6a    Referrers : -    Transfered Bytes : 311    Request :
GET /cgi-bin/survey.cgi HTTP/1.0    Risk Level : -    UserName : -    Matching Reports : Server Error Report    LogType : Apache Access Logs
```

- You can also check if there are log entries that correspond with this IP address from the firewall and router.



```
Message : July 18 09:28:05 router.company.com 1410891: July 18 09:28:04: %SEC-6-IPACCESSLOGP: list from-internet denied tcp 142.53.135.5(2167) -> xxx.yyy.zzz.8(80), 1 packet
Time : 18 Jul 2016, 14:15:06      IPAddress : 142.53.135.5      LogType : Syslog

Message : July 18 09:28:01 router.company.com 1410888: July 18 09:28:00: %SEC-6-IPACCESSLOGP: list from-internet denied tcp 142.53.135.5(1976) -> xxx.yyy.zzz.7(80), 1 packet
Time : 18 Jul 2016, 14:15:06      IPAddress : 142.53.135.5      LogType : Syslog

Message : July 18 09:27:58 router.company.com 1410886: July 18 09:27:57: %SEC-6-IPACCESSLOGP: list from-internet denied tcp 142.53.135.5(1930) -> xxx.yyy.zzz.6(80), 1 packet
Time : 18 Jul 2016, 14:15:06      IPAddress : 142.53.135.5      LogType : Syslog

Message : July 18 09:27:57 router.company.com 1410885: July 18 09:27:56: %SEC-6-IPACCESSLOGP: list from-internet denied tcp 142.53.135.5(1722) -> xxx.yyy.zzz.5(80), 1 packet
Time : 18 Jul 2016, 14:15:05      IPAddress : 142.53.135.5      LogType : Syslog

Message : July 18 09:27:54 router.company.com 1410883: July 18 09:27:53: %SEC-6-IPACCESSLOGP: list from-internet denied tcp 142.53.135.5(1750) -> xxx.yyy.zzz.3 (80), 1 packet
Time : 18 Jul 2016, 14:15:05      IPAddress : 142.53.135.5      LogType : Syslog
```

- Analyzing the log data from all these devices will help reconstruct the attack.
- By examining the logs, you can perform a thorough forensic analysis of the attack to determine whether it was indeed an attack or if it was a false positive. If it was an attack, you can immediately block the IP address to minimize the damage.

Armed with features that help you detect, investigate, and manage security incidents on your web server, you can secure your website and ensure that neither you nor your website visitors are adversely affected.

ManageEngine

EventLog Analyzer

EventLog Analyzer is a web-based, real-time log management and IT compliance solution that combats network security attacks. With comprehensive log management capabilities, EventLog Analyzer helps organizations meet their diverse auditing needs. It also offers out-of-the-box compliance reports and alerts that meet stringent IT regulatory mandate requirements with ease.

$ Get Quote   Download

☎	Toll Free +1 844 649 7766	Direct Dialing Number US : +1-408-352-9254

✉ eventlog-support@manageengine.com

www.eventloganalyzer.com