Aaron Robert Wilson

Full Sail University

NSS

John Cabibbo
January 13, 2016

LOG ANALYSIS

Examine the each of the logs and answer the following questions:

1. What application do the logs come from?

From my perspective, it appears that the dominant application type that is pulling a GET request is a web browser. Mozilla seems to be the main browser that these log files come from.

2. What are the dates which are represented by the logs?

The time period to which these logs where created were in the months of November and December of 2013. The dates to be exact are between 11/10/2013 and 12/08/2013.

3. How many unique IP addresses appear?

Based upon my research on the way IP addresses work, it's actually tricky to determine if these IP addresses are actually "unique IP addresses". Now, if the question is asking approximately how many "different IP addresses" appear on these log files in general, I would say roughly about 134 different IP addresses where logged and referenced in these log files.

I have to say this question required the most research because I used Sublime Text's FIND feature to execute my process of elimination of each IP address throughout the log files. Then mathematics

to come up with a unique mean of individually different IP addresses as a rough estimate of 134 different IPs.

4. What was the largest file export logged? and does it look out of the ordinary?

The largest of the log files is “secure.log” at 1.7MB. The “out of the ordinary” aspect of this file is the fact that this log file contains attempted logins from multiple users, or potentially an intrusive user posing as different users with the intent to gain unauthorized access to the server.

5. What is the most common error found in the error logs?

Again, I used the FIND IN FILES command in Sublime Text 2 to perform my search. The error; "File does not exist:" produced 733 found results.

6. Do you see anything which is out of the ordinary?

Through my own investigative research, I’ve found out that all the references throughout the log files to bots made me question the intent to spread malware across servers through malicious use of php code in phpmyadmin. Also this user would deploy bots to carry out this hack of the desired server. There were two logs that stuck out to me in the “error_log” files the:

[error] [client 80.86.84.72] File does not exist: /var/www/html/w00tw00t.at.blackhats.romanian.anti-sec:)

My research dug up this nugget of info on this:

“These types of attacks are how BlackHat SEO scams are propagated, which target search results in order to spread rogue anti-virus or other malware. In addition, compromised hosts are also leveraged for other schemes, such as spam or botnet control.”

These are referred to as “knock knock” strings.

7. Write a short synopsis of what you found.

In summary, I’ve found that through research of my own, these log files are a representation of the recorded proof that an unauthorized user attempted to gain access to multiple Mozilla web browsers

on a network to deploy malicious bots, spyware, adware, and malwares in order to carryout a campaign of intrusion of that particular network. The user's actual intent is unknown whether they were to use this network for hacking purposes, scams, and other illegal activities. But, these logs serve as the proof that with a little knowledge of how a network works, and the tools like terminal, apache, php, and the intelligence to read log files, we can protect ourselves from these types of invasions from happening in the future. These logs can be an active monitor of our networks to be vigilant and protect both ourselves, and the valuable information from being violated by hackers.

Citation:

In reference to the quote in Question 6;

Ragan, S. (2011, November 5). Hacked MIT Server Used to Stage Attacks, Scan for Vulnerabilities | SecurityWeek.Com. Retrieved January 13, 2016, from http://www.securityweek.com/hacked-mit-server-used-stage-attacks-scan-vulnerabilities