LAB14B: Detecting XSS and SQL with Snort

[Simon X. Camilo. Cybersecurity Student]

[Redacted]

Introduction

This document will show how Snort can be used to detect web injection attacks on a website, such as XSS and SQLI.

## What is **Snort**?

Snort is an IDS, but it’s also an IDP, which stands for Intrusion Detection System. These systems monitor traffic coming through a server or device, and it blocks activities that are considered suspicious by the network administrators. The administrators usually give rules to the IDP (snort in this case), if there is a match they will know about the suspicious activity, but Snort won’t take any action against it.

# Analysis

In order to write a rule that will prevent both XSS and SQL attacks, it’s important to know what the “pcre” option is. Pcre is a lot more effective than contain. PCRE is “a set of functions that implement regular expression pattern matching using the same syntax and semantics as Perl 5.” (Philip Hazel, 2/23/2001). This is essential in being able to block most attacks that attackers might try. The snort rule would like:

alert tcp any any → any any (msg:”Web injection”; flow:to\_server,established; pcre:”/(%3C)|(<)|(%3E)|(>)|(%27)|(‘)/i”; sid:1000042;)

This rule takes consideration of the values and the hexadecimal versions of these values, that are usually used in xss and sqli attacks. The characters that are blocked are “<’>”.

Explaining pcre is complicated, some takeaways I had taken from doing research online are

* It needs to start and end with slashes
* Signs (such as % and <) need to be closed in parenthesis
* | is used for value that needs should be filtered. Could be also interpreted as “or”

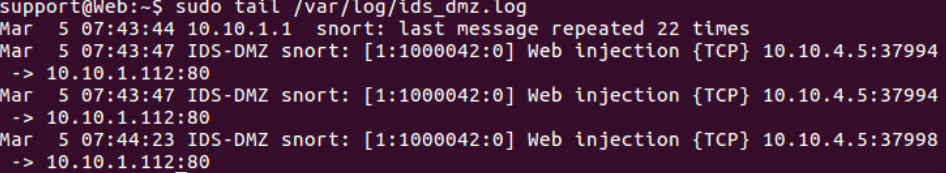
(User1801810, 2/142014)

To test that this works, two attacks are going to be run:

XSS: urbank.com/?myusername=<script>alert('Owned')</script>

SQLi: 1’ or 1=1-- -

After running snort with the new filters in place, image 1 shows that snort was effective in detecting these attacks.

  
**Image 1**

*Snort detects both attacks in the packets*

# Conclusion

Snort is a very effective and useful tool that is able to look at every piece of data inside a packet, and if it matches the filters it can alert the system administrators of this attack. If a system administrator learn to use snort to it’s full capacity, they will have a lot of power in preventing attackers from stopping an attack. The “pcre” option is a very effective tool that system administrators can use, since it can take multiple variables and it provides a lot of additional control when using snort.

References

Hazel, P. (2001, February 23). Perl compatible regular expressions. Retrieved March 05, 2021, from <https://www.pcre.org/>

User1801810. (2014, February 14). How to use an or condition with the content of a snort rule. Retrieved March 05, 2021, from <https://security.stackexchange.com/questions/51551/how-to-use-an-or-condition-with-the-content-of-a-snort-rule>