Dalton Murray

INT 7223 Cybersecurity

Dr. Hany Othman

June 19, 2023

Research Assignment #3

Question

9.14 Consider the example Snort rule given in Chapter 8 to detect a SYN-FIN attack. Assuming this rule is used on a Snort Inline IPS, how would you modify the rule to block such packets entering the home network?

The example Snort rule given in Chapter 8 to detect a SYN-FIN attack can be seen below:

```
Alert tcp $EXTERNAL_NET any -> $HOME_NET any\

(msg: “SCAN SYN FIN” flags: SF, 12;\

reference: arachnids, 198; classtype: attempted-recon;)
```

(Stallings & Brown, 2018. p. 284).

If we assume this rule is used on a Snort Inline IPS, in order to block the packets all we have to do is simply change “Alert” to “block” as seen below (Stallings & Brown, 2018. p. 309):

```
drop tcp $EXTERNAL_NET any -> $HOME_NET any\
```

(msg: “SCAN SYN FIN” flags: SF, 12;\

reference: arachnids, 198; classtype: attempted-recon;)

This is quite a simple change, but it changes the overall functionality of the rule. If the rule is set to “Alert” it will generate a report/alert but setting it to block will generate the report/alert and also immediately block the packet, preventing it from entering the home network. This is a critical difference from allowing a packet into your network to blocking it and is not a mistake that should be made.

References

Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice*. Pearson.

I have neither given nor received unauthorized aid in completing this work, nor have I presented someone else's work as my own.

Dalton Murray