SUNY POLYTECHNIC INSTITUTE

NCS 450

NETWORK SECURITY

Project Proposal: Snort

Author:
Jess YANARELLA
Tony PEREZ

Professor:
Ronny BULL

March 2nd 2015

1 Description: Snort

We will be setting up a intrusion detection system using Snort. Using this IDS we will be able set rules that will warn us when something in our network occurs that we were watching out for. We can write rules of well-known and common vulnerability exploitation attempts, violations of your security policy, and conditions under which you think a network packet(s) might be anomalous[2]. This is done by "sniffing" the packet and comparing it with our set rules.

Any suspicious activity can be detected and displayed. In snorts FAQ page it states that: "It can perform protocol analysis, content searching/matching, and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more" [1].

1.1 Snorby

After successfully installing and setting up snort we will be using an open source ruby-on-rails app that will be used as our front end to show what snort has logged and detected. This will be an add on to show Snort working using a dashboard so other can easily understand it better.

1.2 Results

In the end we will have a Snort IDS setup up with a front end using Snorby. We will also have rules written to use in our Snort system and will test them by attempting to not follow them and set the alarm off. Snort should detect it and Snorby should display it.

2 Resource Requirements

Equipment needed:

3-4 Hosts (laptop or desktop)
1 Cisco Catalyst 3550
1 Computer as our IDS (Snort & Cent OS)

We will be using a Cisco switch so we can monitor a port using SPAN and mirror the packets into Snort so it can analyze them. We will be needed some host machines to test our rules and generate alerts.

3 Timeline

TABLE 1 Timeline

Week 1	Setup Equipment & Install OS
Week 2	Install Snort
Week 3-4	Setup & Test rules
Week 5	Install Snorby
Week 6	Wrap-Up: Produce Demo

References

[1] Snort faq.

[2] Patrick B. O'Keefe. Writing rules and understanding alerts for snort, a network intrusion detection system.