Scarletshield: A Lightweight, Linux-Based Network Security Solution Suite
Val A. Red, Jeff Adler, Eric Cuiffo, Jeff Rabinowitz and Parth Desai
scarletshield@rutgers.edu http://scarletshield.rutgers.edu
Advisor: Prof. Manish Parashar

What is Scarletshield?

Scarletshield is a network security system deployable via Linux, capable of thwarting threats by employing a synergized suite of intrusion detection and prevention tools such as Snort and Fail2ban – all interfaced with iptables to maximize network security and present a proof-of-concept for a defense-in-breadth approach to supplement the defense-in-depth standard.

Motivations and Mission

Motivations

- Network security is highly contested: there is very little standardization or “best practices” available for network administrators that are up and coming.
- Many tools are available, but they are seldom consolidated into more robust network security solutions.

Mission

- Deploy a scalable network security suite that employs a synergy between existing intrusion detection, intrusion prevention, and firewall tools to defend against a full spectrum of threats.

Research Challenges

- False positives – There is always a limited possibility that legitimate traffic (flash mobs, etc.) might be seen as malicious
  * We mitigated this through careful throttling and only banning for cases of definite intended harm (i.e. logs showing a brute-force login attempt over SSH)
- Communicating ongoing exploits and distributed denial-of-service attacks across important nodes and gateways covered by Scarletshield.
  * Centralizing a blacklist on a completely private, internal network

Acknowledgement

We would like to thank our advisor Dr. Manish Parashar for his guidance, as well as Rutgers Engineering Computing Services for the use of their networks and servers.

Methodology

Below is a diagram outlining all facets of Scarletshield’s synergized defense mechanism:

1. All packets first are vetted through the gateway via Scarletshield’s iptables firewall with fail2ban providing rules, dropping packets from all known malicious sources.
2. New packets from various unknown clients are then passed through Snort, with a thorough rigorous set of pattern-matching tests and (3) rulesets updated monthly via Pulled Pork.
3. Snort logs packets through the efficient u2 format.
4. This log is then parsed and inspected by Barnyard2.
5. Detection signatures in the log are parsed & fed to a MySQL database.
6. An administrator may view all this data via a web interface (deployed on Drupal/PHP).

This diagram illustrates our current, working, and live production build of Scarletshield, which actually acts as a server gateway accessible over the web via http://scarletshield.rutgers.edu

Between our first production build launch from late March and today, over 100,000 packet signatures have been processed and countless suspicious IP addresses banned!

Results

Scarletshield has been live for a month, proactively analyzing countless packets while keeping record of potential threats and exploits, centralizing this information in its database and securely informing its neighbors of traffic to watch out for and even throttle.

Metrics regarding the types of traffic caught by are suite can be found to the right:

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>80</td>
</tr>
<tr>
<td>ICMP</td>
<td>5</td>
</tr>
<tr>
<td>UDP</td>
<td>&lt; 1%</td>
</tr>
</tbody>
</table>

*UDP accounted for less than 1%

References


http://scarletshield.rutgers.edu