Scarletshield: A Lightweight, Linux-Based Network Security Solution Suite

Val A. Red, Jeff Adler, Eric Cuiffo, Jeff Rabinowitz and Parth Desai

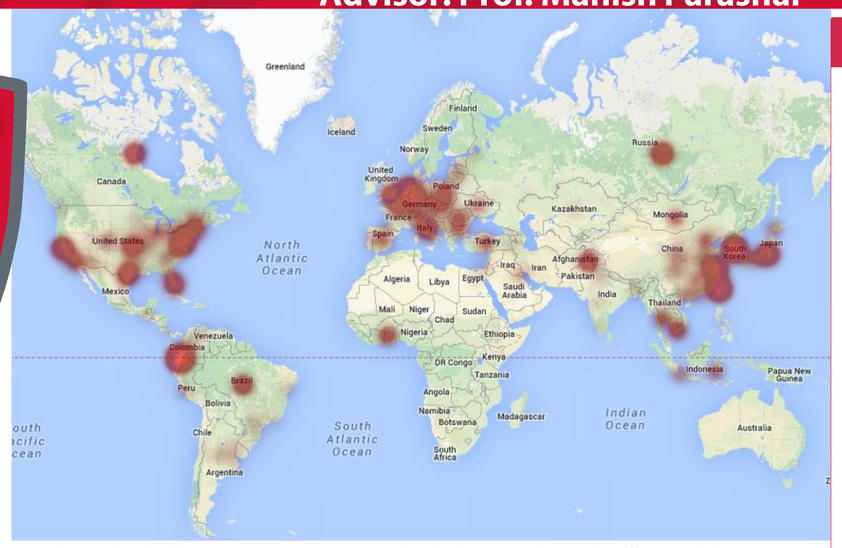
scarlet.shield@rutgers.edu http://scarletshield.rutgers.edu

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**[2] standard.

Scan our QR code to check out Scarletshield in action!



The Scarletshield **server threat heat map** – highlighting geolocated traffic caught by Snort to be potential attempts at exploitation and unauthorized access against our server. (***http://scarletshield.rutgers.edu/map***)

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. [1]

❑ 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

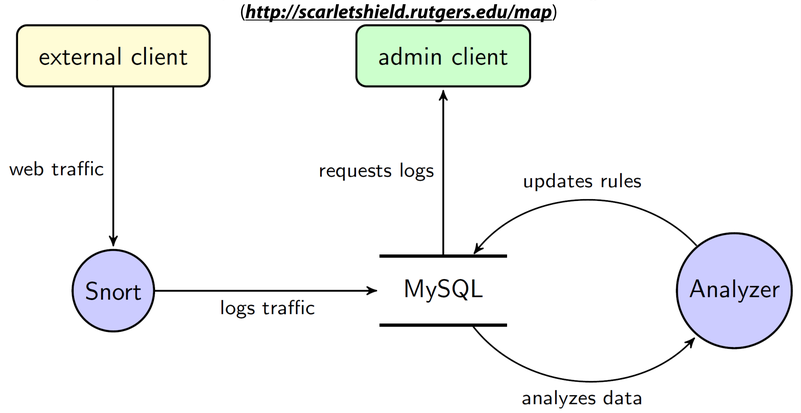
* We mitigated this through careful throttling and only banning for cases of definite intended harm (i.e. logs showing a brute-force login attempt over SSH)

❑ 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

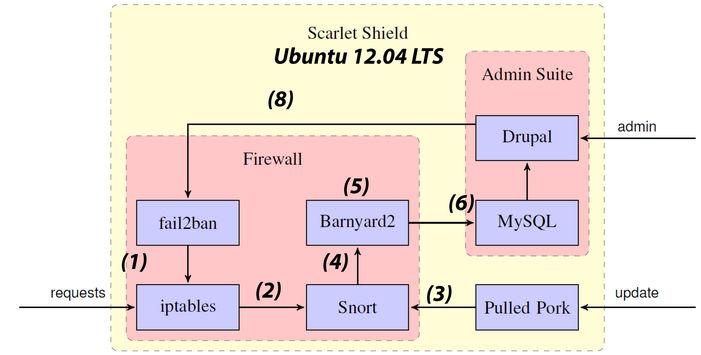
We would like to thank our advisor Dr. Manish Parashar for his guidance, as well as Rutgers Engineering Computing Services for the use of their networks and servers.



The diagram above demonstrates a normal use case for Snort, which we heavily expand upon with Scarletshield by integrating it to a more robust, fully featured suite as illustrated and discussed to the right.

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[3], with a even more rigorous set of pattern-matching tests and **(3)** rulesets updated monthly via Pulled Pork.
(4) Snort logs packets through the efficient u2 format.
(5) This log is then passed to and inspected by Barnyard2
(6) Detection signatures in the log are parsed & fed to a MySQL db
(7) An administrator may view all this data via a web interface (deployed on Drupal/PHP), **(8)** who can then take action by adjusting fail2ban rulesets flexibly against what Snort has detected.

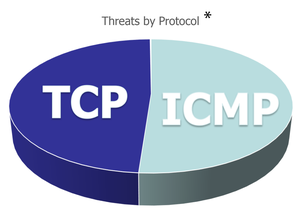
This diagram illustrates our current, working, and live production build of Scarletshield, which actually exists as a server gateway accessible over the web via http://scarletshield.rutgers.edu

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:



*UDP accounted for less than 1%

Most Caught Attempts:

- Brute force attempts over SSH
- DDoS/Reflector Attacks via "PROTOCOL-DNS DNS query amplification attempt"
- ICMP Flood

References

[1] Rash, Michael. Linux Firewalls: Attack Detection and Response with Iptables, Psad, and Fwsnort. San Francisco: No Starch, 2007.
[2] United States National Security Agency, "Defense in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments." 2012. http://www.nsa.gov/ia/_files/ support/defenseindepth.pdf
[3] Sourcefire. "Snort 2.9.3." 2012. http://www.snort.org/assets/158/snortinstallguide293.pdf

http://scarletshield.rutgers.edu