Abstract:

Scarletshield is a network security suite built within a customized Ubuntu 12.04 LTS distribution that may be deployed flexibly to manage independent computers, servers, or whole computer and server networks by robustly consolidating tools such as the intrusion detection system (IDS) Snort, and the intrusion prevention system (IPS) Fail2ban, synergizing these typically independently utilized tools and combining their capabilities with the internal Linux iptables firewall to present an interdependent, reinforced total defensive mechanism featuring both depth and breadth. In addition, Scarletshield boasts a web frontend including a threat heatmap that provides detailed snapshots of past and ongoing threats to a network, spanning the full spectrum of networking protocols while tracking exact signatures of packets as threats are raised against and caught by Scarletshield. This is intended to bridge the gap between the classically contrasted network security doctrines of defense-in-depth and defense-in-breadth by applying both layers of defense mechanisms and a wide-scale, synergetic interoperability such that total defense capabilities within a network are maximized.

Due to the elegance of our solution suite setup of deploying Scarletshield on an existing Linux distribution with universally stable builds of tools such as the Snort IDS and Fail2ban IPS, it may be easily replicated, easily customized, easily extended, and easily scaled for practically all *nix network and system administrators’ needs. This is unique in that it does not require administrators to completely commit to our specific Scarletshield build and operating system, as in the case of a the security suite Linux distribution known as Security Onion. Instead, Scarletshield presents the essentials within existing frameworks in order to make it extensible and accessible for all purposes and network scales. This makes a great proof-of-concept for standardization and “best practices” of network security, which has been generally lacking over the past several of years.

As of April 2014, the original Scarletshield build runs and defends over its own webserver, http://scarletshield.rutgers.edu. Existing within Rutgers University Engineering Computing Services, the success of Scarletshield is slowly creeping its way to the entire School of Engineering in that we are transitioning to replicate Scarletshield across our gateways and switches throughout campus.

Finally, Scarletshield is intended to not only be a standalone security suite, but also capable of advanced communication of threats between other, similar suites within internal, private networks. This is the most unique aspect of Scarletshield in that it can potentially communicate details of threat origins with other gateways to determine whether entire networks should drop packets from specific sources, potentially greatly mitigating future Distributed Denial of Service (DDoS) attacks.

Scarletshield is the realization of greater suppleness and synergy applied between network security tools, methodologies, and systems applied in a way that is practical and extensible over entire enterprise networks. To date, Scarletshield has successfully defended itself against over 100,000 threats.