CCDCOE

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

Locked Shields 2014 After Action Report

Executive Summary

Locked Shields (LS) 2014 was a technical cyber defence exercise conducted on May 20-24, 2014. The game-based scenario placed the teams in a fictional country of Berylia which fell under increasing cyber attacks. The real-time network defence exercise was built up as a competitive game in which the defending teams were scored based on their performance.

LS14 was organised in cooperation with the NATO Cooperative Cyber Defence Centre of Excellence, Estonian Defence Forces, the Estonian Information Systems Authority, the Estonian Cyber Defence League, Finnish Defence Forces and many other partners.

Twelve Blue Teams consisting of up to 16 members were tasked to protect pre-built networks of fictional organizations against Red Teams' attacks; handle the incidents and share the findings with the White Team and other Blue Teams; respond to legal, media and scenario injects; and solve forensic challenges. The teams were participating from their home countries; exercise control was located in Tallinn, Estonia.

Main Findings

The network the Blue Teams had to defend was larger than in previous years and consisted of 50 virtual machines per team. It was the first LS where the technical environment had full IPv6 support, which was implemented in dual-stack configuration. The training audience was also challenged with technologies with which many were not very familiar - FreeBSD based pfSense firewalls, Voice-over-IP infrastructure built on Cisco Unified Communications Manager, IP cameras and Android VMs.

Based on the lessons learned from Locked Shields 2013, the Red Team was strengthened significantly. In general, the attackers were again very successful, although one has to take into account that LS is designed to favour the Red Team as RT members are not part of the training audience. They had separate workshops to practice teamwork, full knowledge of the systems and vulnerabilities, and were allowed to use pre-planted malicious code.

The following areas were the most challenging for Blue Teams:

- Filtering and detecting malicious traffic over **IPv6**.
- Monitoring for malicious WAN route changes and **preventing BGP hijacking/man-in-the-middle**.
- Protecting custom **web applications**.
- Finding pre-planted malicious programs and **coping with** RT's **Anti-Virus evasion** techniques (publicly available free tools were in most cases enough to evade AV solutions).
- **Sharing actionable information** with other Blue Teams.
- **Writing good situation reports** under serious time pressure.

The Gamenet routing infrastructure was not as stable as expected under the increased load. Better technologies are required to implement BGP routers (physical or virtual devices that are used in real-world ISPs not just in lab environment) and more real-world WAN routing experts engaged into the Green Team.