Thunderlab: Facilitating (cyber)security research

Author
Eyle Brinkhuis, SURFnet, eyle.brinkhuis@surfnet.nl
Albert Hankel, SURFnet, albert.hankel@surfnet.nl
Roland van Rijswijk-Deij, SURFnet, roland.vanrijswijk@surfnet.nl

Keywords
Cybersecurity, Botnets, Research Facility, Security Lab, DDoS

Abstract
The Internet continues to grow, both in number of available services and in the number of connected systems and users. In parallel to this, (cyber)security attacks, viruses, DDoSes, malware, botnets and other threats to network security and stability also increase in scale and number. Over the past several years, SURFnet has given scholars access to a secluded part of the SURFnet network called “Onweer” (Thunderlab). In this lab scholars are able to research the dark side of the web. This includes things such as building honeypots, performing DNS research and DDoS experimentation.

Delivering and managing such an obscured facility comes with many challenges. For example: What research do we find ethically acceptable? What if research breaks the law? Where do we draw the line? How do we promote Thunderlab without drawing undue attention from "bad guys"?

In this presentation, we will:
- Explain SURFnet’s motivation for setting up a cybersecurity research facility;
- Provide insight into the technical setup of Thunderlab;
- Discuss how we evaluate and accept new research proposals and what restrictions we place on researchers through our AUP;
- Outline how we intend to further improve Thunderlab in terms of connectivity and other facilities to keep the facility future proof.

Thunderlab is specifically designed to be an accessible *playground* for researchers; without an SLA and guarantees about performance, availability or scalability. Everyone who wants access to the Thunderlab facilities needs to send in a research proposal and agrees to the Acceptable Use Policy and terms of service. The proposal is evaluated based on several factors:
- What is the research about?
- How is this research going to be performed?
- Why is this research performed?
- Are there any ethical and/or legal issues involved in this research and if so, how are these addressed?

Through the AUP we make sure that scholars understand the limits of this facility, what they can expect from SURFnet and what the consequences are if the AUP is not complied with. This setup ensures accessibility as well as allows us to take direct measures in case of a problem.

From a technical perspective, Thunderlab is a network on its own. Being physically as well as logically separated from the production network ensures that our regular connected institutions do not experience any inconvenience while security researchers are still able to analyze real network traffic, set up honeypots or perform large-scale DNS-research.

Projects

We will illustrate how Thunderlab has been used in practice to support various security research projects. In particular, we will discuss three case studies:

- Support for the HoneyNed Anansi project[1] that focuses on developing a centralized honeypot framework which uses 'dumb' sensors that tunnel attacks through VPN to a centralized server that runs multiple honeypots and/or analyzing algorithms.
- Support for the AmpPot[2] project that observes ongoing amplification attacks, their victims and the DDoS techniques used by distributing honeypots around the world that mimic services known to be vulnerable to amplification attacks like DNS and NTP.
- Support for Jair Santanna's PhD thesis[3] (DDoS-as-a-Service: Investigating Booter Websites) which focusses on understanding the technical and non-technical characteristics of DDoS attacks that use so-called 'Booters' to support further mitigation actions.

Future

To continue delivering a highly appreciated, cutting edge facility that enables researchers to perform research on an unprecedented scale, we plan on upgrading Thunderlab's connectivity to 100GBit/s to facilitate DDoS research and simulation, expanding the OpenStack environment to provide more capacity for (large) projects and the addition of high speed storage to enable high performing big-data searches.

[1] See https://honeyned.nl/

[2] See https://christian-rossow.de/publications/amppot-raid2015.pdf

[3] See http://jairsantanna.com/papers/jjsantanna_thesis.pdf