Simulating anomalous events on normal DNS traffic data

Javiera B. Alegría
NIC Chile Research Labs, Universidad de Chile
Santiago, Chile
javi@niclabs.cl

Valeria Valdés
NIC Chile Research Labs, Universidad de Chile
Santiago, Chile
valeria@niclabs.cl

ABSTRACT

This work aims to give a solution to the problem of not having data about DNS server under attacks by providing data for testing tools that prevent and protect a DNS server and thus improve its performance. For this, we developed a simulator for different types of attack in function of the traces left in the server data flow. This determined the importance of having real data from a server in ordinary circumstances. One of the pillars of the internet is the DNS protocol, which strongly depend on DNS servers. Thus it is of utmost importance to protect them. For this, we have different tools like DNS server monitoring [3] and troubleshooting tools. However little data is currently available to test these tools due to almost nonexistent repositories available and a low amount of publications.

Given the characteristics of the DNS server, the simulations just consider the attacks that leave traces in the dataflow, and meet the requirements needed for the optimum development of the simulations. Therefore, the simulations include UDP, TCP SYN and DNS floods[2], Port Scans[4], Random Subdomain[1], and Amplification attacks[5] which stand out for being frequent and well-known types of attacks.

While some attacks look for vulnerabilities to attack the server (Port Scan), most of them focus on disabling the server through the overload of queries, either by non-existing domains (Random Subdomain, DNS Flood), connection queries (TCP and UDP Flood) or just responses that were never requested (Amplification).

We developed DNS floods, Port Scans, Random Subdomain, and Amplification simulations attacks. Each simulation was done in a script that receives a .pcap file with the real traces and returns another .pcap file with the traces that would appear if the server suffered the selected attack (see figure 1).

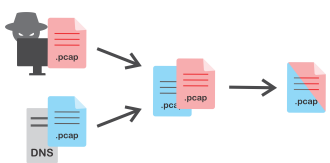

Figure 1: Diagram of the simulation process

Each original file is divided into small time frames where the malicious packets are inserted. Unlike existing data, our simulations are highly customizable, allowing us to set specific characteristics of the simulated attack like its duration, the number of computers attacking, whether its a botnet or a single machine,and the server capacity. Most of the characteristics are optional and their default value is indicated when the help command is called. With this, we can distinguish the realism of the result while giving usability.

As a result we obtained a simulator for DNS floods, Port Scans, Random Subdomain, and Amplification attacks that leaves traces into original server data flow files. Each file is modified by adding new packets that represent the attack.

With these simulators and their level of customization it is possible to simulate different attack scenarios for each data flow record of each server and then, test and improve the protection tools for servers by having new information of how these attacks would leave traces in the server data flow. Another possible use is to train artificial intelligence to predict and prevent these attacks.

About how we can continue this project, creating a data set simulating these attacks is definitely the next step.

KEYWORDS

DNS, TCP, UDP, DNS server, Server attack

REFERENCES

[1] Yehuda Afek, Anat Bremler-Barr, Edith Cohen, Shir Landau Feibish, and Michal Shagam. 2016. Efficient Distinct Heavy Hitters for DNS DDoS Attack Detection. (2016), 5-6. https://arxiv.org/abs/1612.02636v1

[2] Glenn Carl, George Kesidis, Richard R. Brooks, and Suresh Rai. 2006. Denial-of-service attack-detection techniques. *IEEE Internet Computing* 10 (2006), 83. https://doi.org/10.1109/MIC.2006.5

[3] Yong Jin, Hikaru Ichise, and Katsuyoshi Iida. 2015. Design of Detecting Botnet Communication by Monitoring Direct Outbound DNS Queries. *IEEE 2nd International Conference on Cyber Security and Cloud Computing* (2015), 1-5. https://doi.org/10.1109/CSCloud.2015.53

[4] Atul Kant Kaushik, Emmanuel S. Pilli, and R.C. Joshi. 2010. Network forensic system for port scanning attack. *IEEE 2nd International Advance Computing Conference (IACC)* (2010), 310-313. https://doi.org/10.1109/IADCC.2010.5422935

[5] Laura Mutu, Rania Saleh, and Ashraf Matrawy. 2015. Improved SDN Responsiveness to UDP Flood Attacks. *IEEE Conference on Communications and Network Security (CNS)* (2015), 716. https://doi.org/10.1109/CNS.2015.7346900