Security Metrics - Economics of Cyber Security - Group 11

Menno Bezema, Cas Bilstra, Roemer Hendrikx, Stijn Pletinckx, Jelle Vos

September 21, 2020

1 Introduction

Nowadays, many digital services are exposed through the internet [4, 2, 1]. While many of these services can be safely exposed from a cybersecurity point of view[1], vulnerabilities for these services are found regularly [6]. While patches for these vulnerabilities will become available, they may not be immediately installed by their users [5, 1]. But from the point that a vulnerability is disclosed to the public, this vulnerability can be exploited by adversaries. Depending on the vulnerability, the exploitation of this vulnerability can be catastrophic to an organization [3]. While metrics such as "Days to patch" [8] exist for measuring the time between a vulnerability disclosure and patch, the question is how organizations perform on this metric and if this metric is useful in practise at all.

This report will investigate which (if any) security metrics can be derived from large-scale network scan data. This will be done using network scan data from Rapid7 [7]. We will first explain our methodology, then we will go into the steps used to perform our method and finally we will shortly discuss some preliminary results we found.

1.1 Methodology

Using this large-scale network scan data, version numbers of exposed services can be identified. Vulnerability disclosure dates can then be combined with the identified version numbers of services to investigate if a service was vulnerable at some point in time. Because the dataset contains data for 12 months, the amount of patched services over the course of one year can be tracked. It can then be investigated what security metrics would be helpful for measuring the level of cybersecurity of an organization. For now, only services running at port 22 (SSH) and port 23 (Telnet) will be investigated due to limited time for this investigation. Other ports – such as 443 – could be looked at, but identifying versions and software vulnerabilities on those ports will be much more difficult due to the large amounts of information sent over those ports.

1.2 Steps

In order to perform our research we have defined a list of steps which we want to take, during each step we will update the report. The steps are as followed:

1. Extract the network scan data and preprocess it for use, extracting version numbers.
2. Create a list of vulnerabilities to assess and find out when they were patched.
3. Combine network scan data and patch dates to find out what services were vulnerable.
4. Track the change of version numbers to see when vulnerabilities were patched.
5. Analyse the results

[1] An exposed service is not vulnerable if it contains no vulnerabilities

Weeknr	39	40	41	42	43	44	45
Deadline	21/09/2020	28/09/2020	05/10/2020	12/10/2020	-	26/10/2020	06/11/2020
Deliverable	Draft: Security Metrics	Security Metrics	Draft: Policy Interventions	Policy Interventions		Draft: Empirical Question	Empirical Question

Figure 1: Timeline of the project

6. Try to conclude

1.3 Preliminary results

Before looking through the data set, we did an initial search for disclosed vulnerabilities in 2012. From this search, we stumbled upon CVE-2012-0920[2], which is a CVE that describes a vulnerability in Dropbear SSh Server 0.52 through 2012.54. It's publication date is 2012-06-05, which makes it interesting to investigate in our data set.

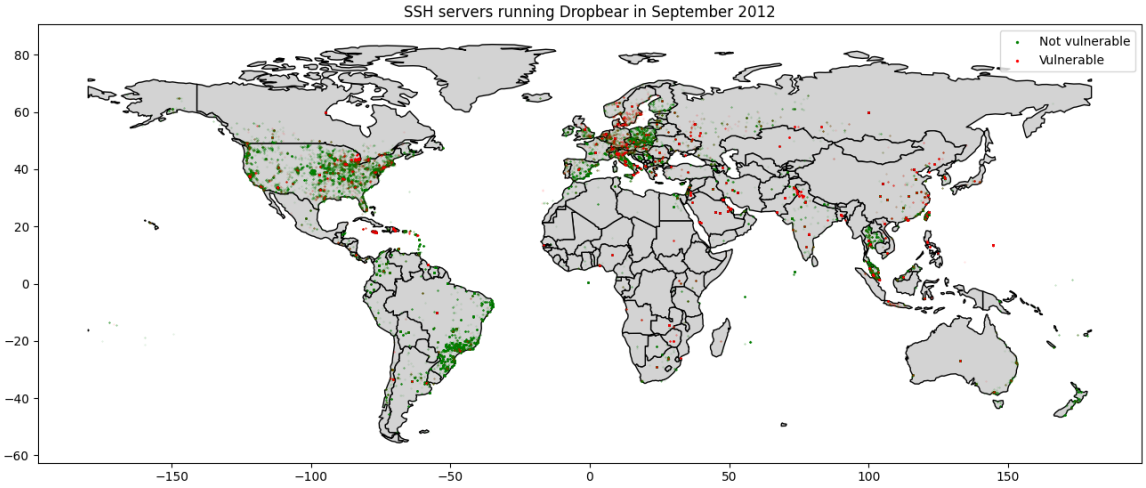

Figure 2: Servers running (sometimes vulnerable) software called Dropbear

Figure 2 shows a global depiction of servers running Dropbear SSH software, as found by probes sent in September 2012. Remarkably, even though a vulnerability was found for specific Dropbear versions in June, our analysis shows that the results of the port scans still reveal vulnerable software versions, months after their official disclosure.

As a potential research angle, our group is interested in the responsiveness of certain demographics to CVE-2012-0920 related to Dropbear SSH.

[2] `https://www.cvedetails.com/cve/CVE-2012-0920/`

References

[1] E. Bertino and N. Islam. "Botnets and Internet of Things Security". In: *Computer* 50.2 (2017), pp. 76–79.

[2] Roland Bodenheim et al. "Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices". In: *International Journal of Critical Infrastructure Protection* 7.2 (2014), pp. 114–123. ISSN: 1874-5482. DOI: https://doi.org/10.1016/j.ijcip.2014.03.001. URL: http://www.sciencedirect.com/science/article/pii/S1874548214000213.

[3] Platon Kotzias et al. "Mind Your Own Business: A Longitudinal Study of Threats and Vulnerabilities in Enterprises." In: *NDSS*. 2019.

[4] K. Mathew, M. Tabassum, and M. V. Lu Ai Siok. "A study of open ports as security vulnerabilities in common user computers". In: *2014 International Conference on Computational Science and Technology (ICCST)*. 2014, pp. 1–6.

[5] A. Nappa et al. "The Attack of the Clones: A Study of the Impact of Shared Code on Vulnerability Patching". In: *2015 IEEE Symposium on Security and Privacy*. 2015, pp. 692–708.

[6] B. A. Navamani, C. Yue, and X. Zhou. "An Analysis of Open Ports and Port Pairs in EC2 Instances". In: *2017 IEEE 10th International Conference on Cloud Computing (CLOUD)*. 2017, pp. 790–793.

[7] Rapid7. *Critical.IO Service Fingerprints*. https://opendata.rapid7.com/sonar.cio/. [Online; accessed 17-September-2020]. 2013.

[8] Richard de Vries. *How Do You Measure the Success of Your Patch Management Efforts?* https://securityintelligence.com/posts/how-do-you-measure-the-success-of-your-patch-management-efforts/. [Online; accessed 20-September-2020]. 2020.