SHORT TERM SCIENTIFIC MISSION (STSM)
SCIENTIFIC REPORT

This report is submitted for approval by the STSM applicant to the STSM coordinator

Action number: CA15127
STSM title: Hiding the information on network structure/architecture
STSM start and end date: 23/06/2017 to 02/07/2017
Grantee name: Wojciech Kmiecik
Home Institution: Wroclaw University of Science and Technology, Faculty of Electronics, Department of Systems and Computer Networks
Host Institution: SBA Research, Vienna, Austria
Host: Dr Tomasz Miksa
Working group: WG4

PURPOSE OF THE STSM:

(max.200 words)

Main purpose of the STSM was to investigate the topic of hiding the security-wise critical information on network structure/architecture. Communication networks, especially the Internet, once it became essential for everyday life for billions of people, also emerge more and more as the favorite attackers land to launch a broad variety of threats. In order to keep the network safe, it is essential to know the way attackers gain the information about network architecture. There are three essential steps that a hacker, have to perform to get a good picture of an network architecture layout - Foot printing, scanning and Enumeration [3]. We believe there is a big need for a proper analyze of the process of gathering data about network structure and as a result – new ideas and guidelines how to proof the network from such a process. Failure in securing network structure information can lead to successful attack, which will result in huge revenue and trust losses and can be fatal to any company or organization.

Another purpose of this STSM was to start new collaborations with the researchers of SBA research, namely my host, Dr. Tomasz Miksa.

Finally, topic of cyber security is a completely new research field for me and expanding my competences was also a big motivation for this STSM.

DESCRIPTION OF WORK CARRIED OUT DURING THE STSMS

(max.500 words)

During the STSM, a visit to Dr. Tomasz Miksa “SBA Research” research center was conducted. I got to meet Dr. Miksa’s colleagues and give short presentation about my STSM entitled “Hiding

the information on network structure/architecture - introduction". Then, several topics related to my STSM subject were discussed. We narrowed them down to three main topics/questions:

- Thorough literature study is crucial in order to understand how third party (hacker) gathers information about the network.
- What are the most efficient tools for gathering data about network structure/architecture?
- Would it be best to make experiments in real-life networks, or in configuration prepared in a lab?

I have conducted state-of-the-art literature study on the subject of cyber security, gathering data about the network and ways of preventing from it. It was crucial for me to better understand a subject that is new for me.

Finally, after choosing a number of software tools for gathering data, we decided to "attack" real-life network of Faculty of Electronics, Wroclaw University of Science and Technology. We were able to successfully obtain a lot of information about network structure, type or routers used in the network and its operating software. Next step is to find a network based on juniper routers/switches to compare its security features with our studies on Cisco-based network. Hopefully, all of the knowledge gathered will ultimately help us in configuring SDN routers in way that will reveal as little information about the network to the third party as possible.

DESCRIPTION OF THE MAIN RESULTS OBTAINED

1. Literature Study

The authors of [1] propose SANE, a protection architecture for enterprise networks. SANE defines a single protection layer that governs all connectivity within the enterprise. All routing and access control decisions are made by a logically-centralized server that grants access to services by handing out capabilities (encrypted source routes) according to declarative access control policies (e.g., "Alice can access http server foo"). The authors claim that SANE could be deployed in current networks with only a few modifications, and it can easily scale to networks of tens of thousands of nodes. Biggest disadvantage of this proposal is one, centralized serve controlling whole system. Another authors framework called TrustR is proposed in [5]. It integrates collaborating security primitives including cryptography based security mechanisms, trust management system, and trusted platform module. A simple but efficient method for detecting deceptive routing messages is also proposed. The deployment of TrustR is introduced. Simulation results show that TrustR is effective in resisting attacks and improving network performance.
In [7] authors so-called flow watermarking is discussed. It is primarily used for linking network flows in application scenarios where packet contents are stripped of all linking information. This chapter reviews network traffic analysis and its utilization in linking network flows, that is, through flow watermarks. It briefly describes different application scenarios for network flow. Similar topic is discussed in [2] in a context of Internet "traffic analysis" (TA). The authors state that TA can also be exploited by an attacker in order to infer private or sensitive information about the user's communication. For example, TOR, Crowds, Anonymizer.com, and other technological platforms developed to provide anonymous and private communication can be vulnerable to watermark attack.
Very interesting overview is presented in [6]. It starts with presenting a review of the state of computer and network security in 1986, along with how certain facets of it have changed. Next, it talks about today's security environment, and finally discusses some of today's many computer and network attack methods that are new or greatly updated since 1986.
[4] is a practical guide to creating a secure network infrastructure, understanding security technologies, identifying the threats and common attacks to a network.

2. Experiments

We decided to perform our experiments in real-life computer network of Faculty of Electronics, Wroclaw University of Science and Technology. Below we list some of the tools/software used to In order to obtain information about the network:

- Nmap - a security scanner used to discover hosts and services on a computer network, thus building a "map" of the network.
- OpenVAS - a framework of several services and tools offering a vulnerability scanning and vulnerability management solution.
- Amap - attempts to identify applications even if they are running on a different port than normal.
- Cisco Torch - mass scanning, fingerprinting, and exploitation tool.It uses several methods of application layer fingerprinting simultaneously, if needed.
- CDPSnarf is a network sniffer exclusively written to extract information from CDP packets.
- Miranda is a Python-based Universal Plug-N-Play client application designed to discover, query and interact with UPNP devices, particularly Internet Gateway Devices (aka, routers).

We are able to obtain many information about network structure, devices functioning in the network and types of network hardware that are important part of the network. Below we present a graph that is representing a part of the network in a graphic way:

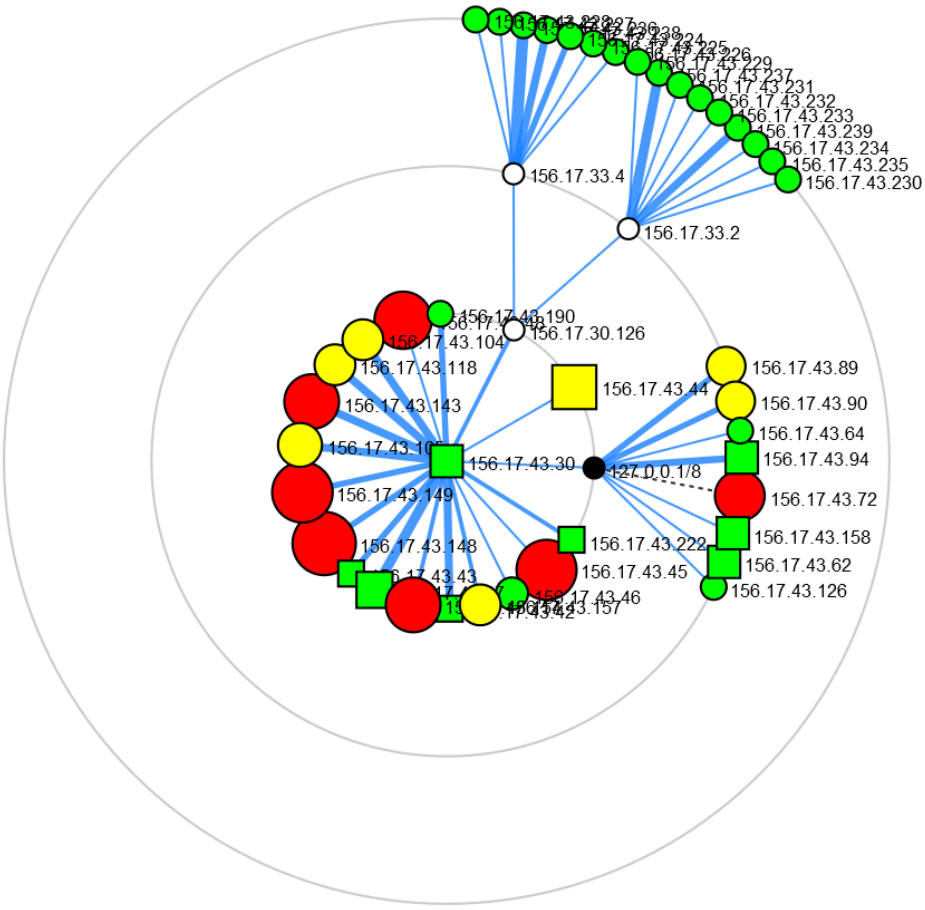

Figure 1 – visualization of network architecture (part)

Also, one of the network devices description, that reveals important information like type of the hardware and operating system version, is presented below:

Nmap scan report for syriusz.kssk.pwr.wroc.pl (156.17.43.30)

Host is up (0.0014s latency).

Not shown: 65534 closed ports

PORT STATE SERVICE VERSION

23/tcp open telnet Cisco IOS telnetd

OS details: Cisco 836, 890, 1751, 1841, 2800, or 2900 router (IOS 12.4 - 15.1), Cisco Aironet 1141N (IOS 12.4) or 3602I (IOS 15.3) WAP, Cisco Aironet 2600-series WAP (IOS 15.2(2))

Network Distance: 1 hop

TCP Sequence Prediction: Difficulty=263 (Good luck!)

IP ID Sequence Generation: Randomized

Service Info: OS: IOS; Device: switch; CPE: cpe:/o:cisco:ios

Listing1 – acquired information about one of the core router in the network.

Overall, we gathered research material that will be a base for rest of the planned research (Juniper hardware and SDN routers).

FUTURE COLLABORATIONS (if applicable)

I would like to co-author a chapter in RECODIS book "Guide to Disaster-Resilient Communication Networks" by Springer. To achieve that goal I would like to continue a collaboration with Dr. Tomasz Miksa and also find another partner from third country who will be willing to cooperate in area of cyber-security. Hopefully she/he will have access to Juniper-based network, as I would like to also examine this brand of network hardware. This may lead to another STSM in order to finish planned research and start abovementioned collaboration.

Another plan is to prepare a shorter research material and submit a paper to one of the well-recognized cyber security conferences:

- IEEE Conference on Communications and Network Security 2018
- 9th IFIP International Conference on New Technologies, Mobility & Security
- IEEE International Conference On Cyber Security And Protection Of Digital Services 2018

References:

[1] M. Casado, T. Garfinkel, A. Akella, M. J. Freedman, D. Boneh, N. McKeown, and S. Shenker, “SANE: A Protection Architecture for Enterprise Networks,” in *Proceedings of the 15th Conference on USENIX Security Symposium - Volume 15*, 2006.

[2] A. Iacovazzi and Y. Elovici, “Network Flow Watermarking: A Survey,” *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1. pp. 512–530, 2017.

[3] Ida Mae Boyd, “The Fundamentals Of Computer HACKING,” 2000. [Online]. Available: https://www.sans.org/reading-room/whitepapers/hackers/fundamentals-computer-hacking-956. [Accessed: 10-Jul-2017].

[4] M. Kaeo, *Designing Network Security, Second Edition*. Cisco Press, 2003.

[5] S. Tan, X. Li, and Q. Dong, “TrustR: An Integrated Router Security Framework for Protecting Computer Networks,” *IEEE Communications Letters*, vol. 20, no. 2. pp. 376–379, 2016.

[6] E. L. Witzke, “Computer network security: Then and now,” *2016 IEEE International Carnahan Conference on Security Technology (ICCST)*. pp. 1–7, 2016.

[7] “Network Flow Watermarking,” in *Information Hiding in Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures*, John Wiley & Sons, Inc., 2016, pp. 139–162.