NETWORK INFRASTRUCTURE FOR CYBERSECURITY ANALYSIS

Linko G. Nikolov, PhD; Vasil O. Slavyanov

linkonikolov@abv.bg; vasil.slavyanov@gmail.com

***Abstract**: Applications and protocols, serving trillions of devices worldwide, have weak points and vulnerabilities. Malicious intends of hackers exploit those vulnerabilities, which can lead to information leakage, network and systems malfunction and even serious money loss. Before giving birth to an app, service or network resource facing internet, serious tests and analysis should be performed. In this paper, a proposed basic network infrastructure for applications and systems vulnerability analysis is shown.*

***Keywords**: CYBERSECURITY, VULNERABILITY ANALYSIS, NETWORK PENTESTING, NETWORK SECURITY, COMPUTER SECURITY*

1. Why cybersecurity analysis?

Cybersecurity becomes even popular with the extreme evolution of internet-connected devices such as smartphones, laptop workstations and Internet-of-Things (IoT). The vast amount of network protocols and applications, with their functionality, become a source of weak points in the IT infrastructure. Such vulnerabilities may be exploited by hackers or attackers whose aim is to acquire benefits form the access granted [1]. The benefits are various including wreaking havoc, money for ransom, administrative access to sensitive data [10] and so on. If the developed applications were to be examined for security flaws, the chance of hacker’s success minimizes. Furthermore, if the network resource is constantly under security provision, penetration would be extremely difficult. With some ordinary security measures in networks and systems being implemented, companies and enterprises believe their infrastructure is shielded enough. This is neither true, nor does a hacker thinks so. Networks and systems on the global range are being under attack almost constantly 24/7/365 according to Norse Corporation’s website. What about institutions dealing with classified information? Sooner or later, if precautions are not enough, breakage can occur.

With proper security testing, administrators of IT infrastructures become more aware of the real world e-threads. Security engineers have developed software platforms and penetration testing environments which are very helpful concerning cybersecurity. The goal of this paper is to model a typical network infrastructure, capable of exploring possible threads and previously unknown vulnerabilities.

2. Network topology with devices, systems and security test platforms

Simulation software is available on the market to perform network flow imitation. But having real hardware devices, the cybersecurity analysis results can be more realistic. This is the place to stress out that complex large scale SCADA, ICS (Industrial Control System) and DCS (Distributed Control Systems) systems are impossible to testify [9] with the proposed small scale network. Application, web and LAN network security are successfully tested instead.

The network topology includes three routers, two cable switches and one Wi-Fi access point for wireless LAN access (fig. 1). Two servers and three hosts are deployed as end devices. One computer with open source operating system KALI LINUX plays the role of attacking system.

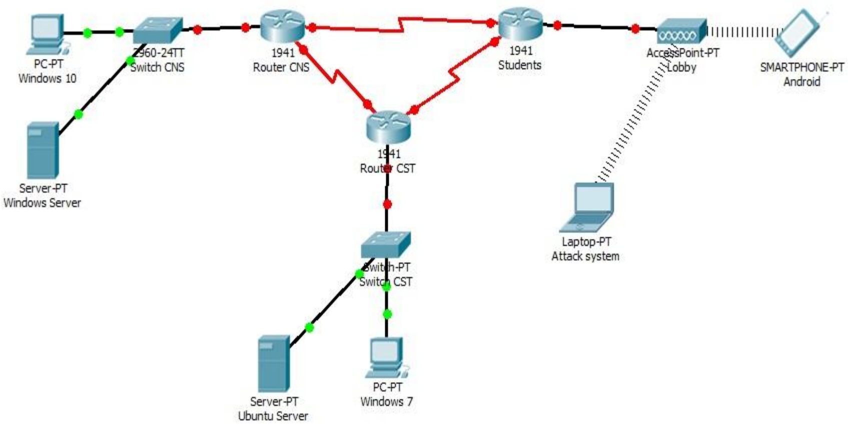

***Figure 1** – Sample hardware network infrastructure for cybersecurity analysis*

The law concerns are explicitly followed and the applications will be internal for the network only. Connection to Internet will have occasional manner. The more diverse the applications, the more efficient will be the analysis. A firewall appliance is predicted, but will be for further protocols flaw explorations. The proposed network infrastructure does not pretend to be innovative, but somewhat educational and moreover – the first line starting cybersecurity investigation in a real hardware manner. Servers can be either e-mail, web, or other widespread services. Depending on the target, the tested services may vary. In table 1 an example of useful instruments is shown:

Table 1: Testbeds for cybersecurity [8]:

Testbed	**Focus area**
Anubis	Malware analysis
Connected Vehicle Testbed	Connected vehicles
DETER	Cybersecurity experimentation and testing
DRAKVUF	Virtualized, desktop dynamic malware analysis
EDURange	Training and exercises
Emulab	Network testbed
Future Internet of Things (FIT) Lab	Wireless sensors and Internet of Things
Future Internet Research & Experimentation (FIRE)	European federation of testbeds
GENI (Global Environment for Network Innovations)	Network and distributed systems
NITOS (Network Implementation Testbed using Open Source)	Wireless
OFELIA (OpenFlow in Europe: Linking Infrastructure and Applications)	OpenFlow software-defined networking
ORBIT (Open-Access Research Testbed for Next-Generation Wireless Networks)	Wireless
PlanetLab	Global-scale network research
Starbed	Internet simulations

DETER, Emulab and DRAKVUF are network testbeds that apply resource time-sharing among many users. It means users acquire physical resources from the testbed and abandon them when deciding it is out of need for a couple of hours. Testbeds skip experiment definition consisting of node names and topology, OS and node type choices, etc. so that a user can rebuild the experiment later. Testbeds bring a set of OS images that can be loaded on analyzed machines. An OS image is a block level image of the filesystem on a node. Base images usually involve several Linux flavors, such as Ubuntu, Red Hat and some Windows platforms, such as Windows Server 2016. While the attacking system performs network Penetration testing, application vulnerability scanning or fuzzy logic implementation for test randomization [9], the end computers may have installed software monitoring services, antivirus and firewall applications.

3. Short example cybersecurity tests and analysis

For adequate results, systems should be limited of outside networks and the operation system environment should be as real as possible (in a customer's view). In this paper the recent tools are used such as "Nmap" [2], "OpenVas" [3], the Metasploit Framework [4] and some others. The full cycle for cybersecurity analysis can be copied from the ethical hacking [7] steps, which are:

1. Footprinting and reconnaissance.
2. Network scanning and enumeration.
3. Sniffing and evasion.
4. Privilege escalation and persistent access.
5. Presence diminishing.

For example, the first task of a malicious hacker is to sniff around the network and draw a gesture of the topology. The tool, trying to connect to open TCP ports and IP addresses may be "Nmap". One example syntax in Kali Linux is as shown below:

root@kali:~# *nmap –A –T4 192.168.1.115*

where "nmap" is a command in the shell, and 192.168.1.115 is the IPv4 network address of the target device. The results after hitting this command are shown in fig. 2.

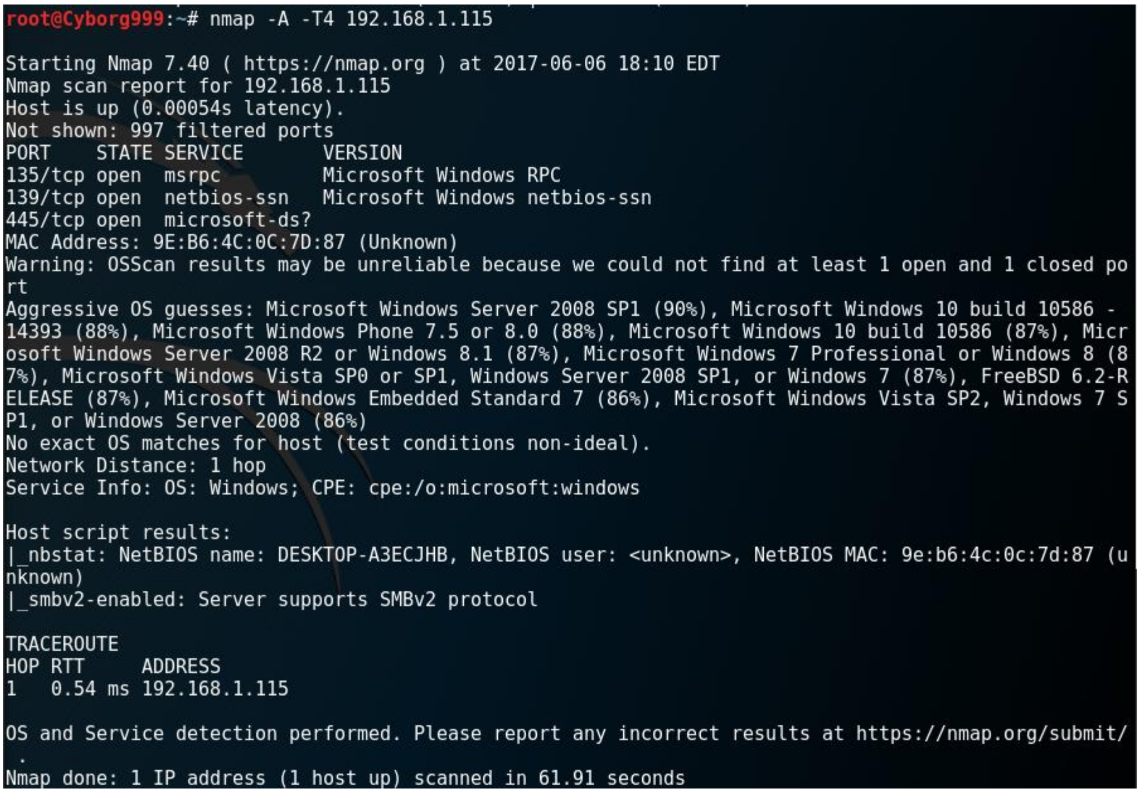

***Figure 2** – Example of network reconnaissance with nmap*

For scanning and enumeration, a tool Lynis in Kali (fig. 3) finds its way for exploration where computer operation system is the target object. Which in turn can give the attacker useful information about breaking points, backdoors or possible system vulnerabilities.

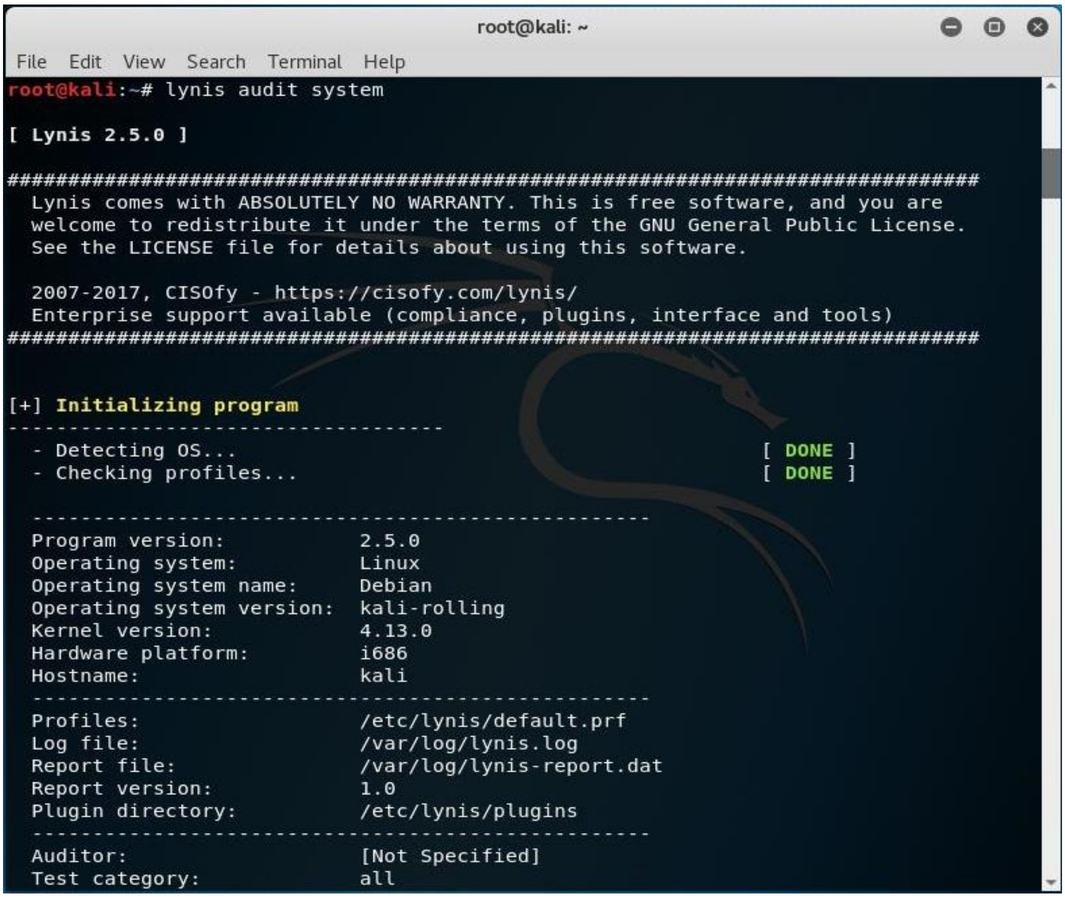

Figure 3 *– Lynis Audit result*

Further step in the cybersecurity test can be the critical vulnerability exploration. The results obtained can be in the sense of a CVE – Common Vulnerabilities and Exposures [3]. Fig. 4 shows the results of analyzing with OpenVas:

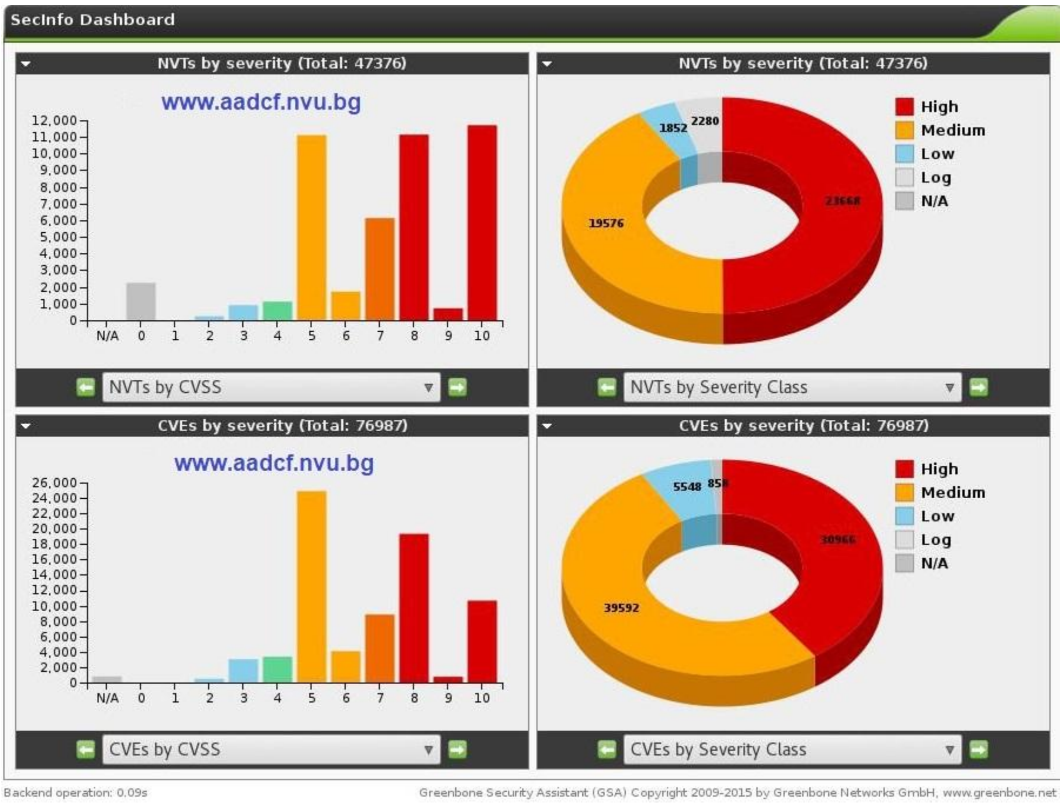

Figure 4 *– Example of OpenVas web-application vulnerabilities analysis*

The research area in cybersecurity seems as vast as the world ocean, but the good news is cyberawareness has already been woken. Terms for future development are cyberhygiene, cybercrime forensics, as well as cyber resilience. Everyday's virus signature reports and zero-day attack patches help improve systems' cybersecurity. The test results help administrators and security officers define weak points and avoid deep impacts from information losses when possible.

4. Conclusion

Subject of review in this paper was network building and cybersecurity testbed preparation for network protocols and applications exploration in a manner of computer security. The Proposed framework seems to be a helpful tool for considering good practices for cyber analysis, the goal of which is "to ensure secure systems planning and operation, response and support". Essentials in cybersecurity include investigations from detection systems, impact of an incident understanding, forensics performed, and incidents categorized with response plans.

Cybersecurity analysis is an important aspect of the understanding, development, and practice of network, computer and cloud security. Cybersecurity is a broad category, covering the technical practices for computer networks, computers, and data protection from harm and destroy. Scientists, industry workers and government clerks use formal and informal science to create and expand cybersecurity knowledge. As a testbed, the field of cybersecurity requires authentic knowledge to explore and reason about the "how and why" security controls to be built or deployed.

References:

[1] Kizza, J., "Guide to Computer Network Security", Springer, 2017 ISBN 978-3-319-55605-5

[2] Gordon "Fyodor" Lyon, "Nmap Network Scanning", ISBN 978-0-9799587-1-7, https://nmap.org/book/

[3] URL: http://www.openvas.org/about.html

[4] URL: https://metasploit.help.rapid7.com/docs

[5] URL: https://www.cybersecurityanalysis.com/

[6] Robert, W. Beggs, "Mastering Kali Linux for Advanced Penetration Testing", PACKT, 2014, ISBN 978-1-78216-312-1

[7] Цокев, Ал., „Етично хакерство", БАРЗИКТ, 2017, ISBN 978-619-7382-00-6

[8] Dykstra, J., "Essential cybersecurity science", O'REILLY, 2016, ISBN 978-1-491-92094-7

[9] Slavyanov, Krasimir, "An algorithm of fuzzy inference system for human resources selection tools", International Scientific Conference, Rezekne, Latvia, 2018.

[10] Цанков Ц. С., „Киберпрестъпността като основна съвременна заплаха за големите организации", „МАТТЕХ" Шумен 2016.