DOI 10.34054/bdc005

THE IMPORTANCE OF ELABORATED TRAINING FOR INFORMATION SECURITY SPECIALISTS IN THE SUCCESSFUL DEVELOPMENT OF THE COUNTRY IN CURRENT CONDITIONS

Petro Venherskyi,

Doctor of Physics and Mathematics Science, professor of information systems department, faculty of applied mathematics and informatics Ivan Franko National University of Lviv, Ukraine

Michael Kropyva

InfoSec Director, SoftServe, a computer and cybersecurity expert with almost 18 years of hands-on experience.

Promote Ukraine

Conference proceeding

Behind the Digital Curtain. Civil Society vs State Sponsored Cyber Attacks

Brussels - 25/06/2019

DOI 10.34054/bdc000

Cybersecurity is no longer an issue to be taken lightly. Be it an individual or a corporation it brings a huge amount of damage. Last year was terrible for a bunch of not only organizations but countries at large which were infected by global massive ransomware. Cyber-attacks are now on the rise coming in many different forms and are always evolving. To fight them efficiently we need a pool of qualified professionals who will continuously assess existing and potential threats and adjust security systems respectively and make them resistant to attacks.

Key words: educational program, cyberattack, application, network, operations security, attack scenario.

I. Introduction.

As of now, Ukraine has a great potential in terms of talents but educational opportunities do not meet current needs to the fullest[1]. To nourish a strong community of cyber security specialists we've united the efforts and developed an up-to-date bachelor program which balances theoretical knowledge and practical experience on real-life projects with seasoned IT experts[2,3]. Due to the fruitful collaboration of Lviv IT community and educational establishments we all benefit - students get high-quality education based on the latest tech developments, and companies get motivated graduates with relevant knowledge and experience.

II. The threat towards information security caused by the current war in the eastern part of the country.

During last five years cybersecurity attacks become real threat for the whole Ukraine making significant impact to critical infrastructure. Ukraine power grid cyberattack took place on 23 December 2015 and is considered to be the first known successful cyberattack on a power grid. Hackers were able to successfully compromise information systems of three energy distribution companies in Ukraine and temporarily disrupt electricity supply to the end consumers.

Most affected were consumers of «Prykarpattyaoblenergo» (Ukrainian: Прикарпаттяобленерго; servicing Ivano-Frankivsk Oblast): 30 substations were switched off, and about 230 thousand people were left without electricity for a period from 1 to 6 hours.

At the same time consumers of two other energy distribution companies, «Chernivtsioblenergo» (Ukrainian: Чернівціобленерго; servicing Chernivtsi Oblast) and «Kyivoblenergo» (Ukrainian: Київобленерго; servicing Kyiv Oblast) were also affected by a cyberattack, but at a smaller scale. According to representatives of one of the companies, attacks were conducted from computers with IP addresses allocated to the Russian Federation.

A series of powerful cyberattacks using the Petya malware began on 27 June 2017 that swamped websites of Ukrainian organizations, including banks, ministries, newspapers and electricity firms. Similar infections were reported in France, Germany, Italy, Poland, Russia, United Kingdom, the United States and Australia.

III. Security measures showcased at SoftServe.

During the attack an actor focused on all aspects of application and IT infrastructure security.

1. On the side of Application Security, it was found several software flaws in corporate applications that allowed actor to successfully penetrate the external network perimeter and get a foothold in the internal corporate network. Those were vulnerabilities of insecure file upload and SQL injection
2. On the side of Network Security, an actor was able to successfully escalate the initial penetration to the level of network access to several hundreds of internal network hosts, due to the lack of efficient network segmentation and access controls. Access to some critical business systems was obtained from the very initial point of penetration. The most significant role in successful penetration was caused by the fact that some development-related systems had both external (Internet) and internal network accesses.
3. On the side of Operations Security, an actor was able to find a set of severe weaknesses, that affect corporate security posture. They have found multiple operational deficiencies, such as improper security administration practices and insufficient attention to user authentication controls and access management. The most severe cases were “default” root or Administrator

During last five years cybersecurity attacks become real threat for the whole Ukraine making significant impact to critical infrastructure.

passwords set on multiple operating systems. Using these weaknesses, it was possible to penetrate multiple corporate systems, including Jenkins software, Cisco and Citrix networking devices, and Windows- and Unix-based OS.

Attack scenario

FIND AVAILABLE DIRECTORIES\FILES OR RESOURCES AT THE KNOWN DOMAINS

Using the **dirburster** utility an actor has found a publicly available directory that contained PHP script with functionality of unauthenticated upload (without any verification). Thus it was possible to upload an arbitrary executable file to a victim system and get interactive access to the web server.

GET CONTROL OVER A WEB SERVER

It was uploaded a web shell, that allowed actor to control the server remotely with www-data permissions.

SCAN INTERNAL NETWORK

It was installed nmap and masscan utilities on the web server which allowed actor to scan internal network for available services.

ESTABLISH PERSISTENT ACCESS TO INTERNAL NETWORK

It was installed a reverse SOCKS proxy that allowed actor to stay connected to the internal network even if the initial penetration vector was detected and remediated.

GET ACCESS TO SYSTEM ACCOUNTS

Actor discovered several Jenkins instances that allowed access without prior authentication to sensitive information, such as source code, list of users, stored credentials.

USE THE DEFICIENCY IN PASSWORD MANAGEMENT TO OBTAIN ROOT ACCESS TO UNIX-BASED HOSTS

It was revealed a password for “root” account. This gave an actor root access to many Unix-based hosts, where the same typical password was utilized.

USE JENKINS VULNERABILITY TO GET ACCESS TO WINDOWS-BASED HOST

The Jenkins Remote Code Execution vulnerability was used to extract NTLM hashes for the administrative accounts on corporate systems.

USE THE DEFICIENCY IN PASSWORD MANAGEMENT TO OBTAIN ADMINISTRATIVE ACCESS TO WINDOWS-BASED HOSTS

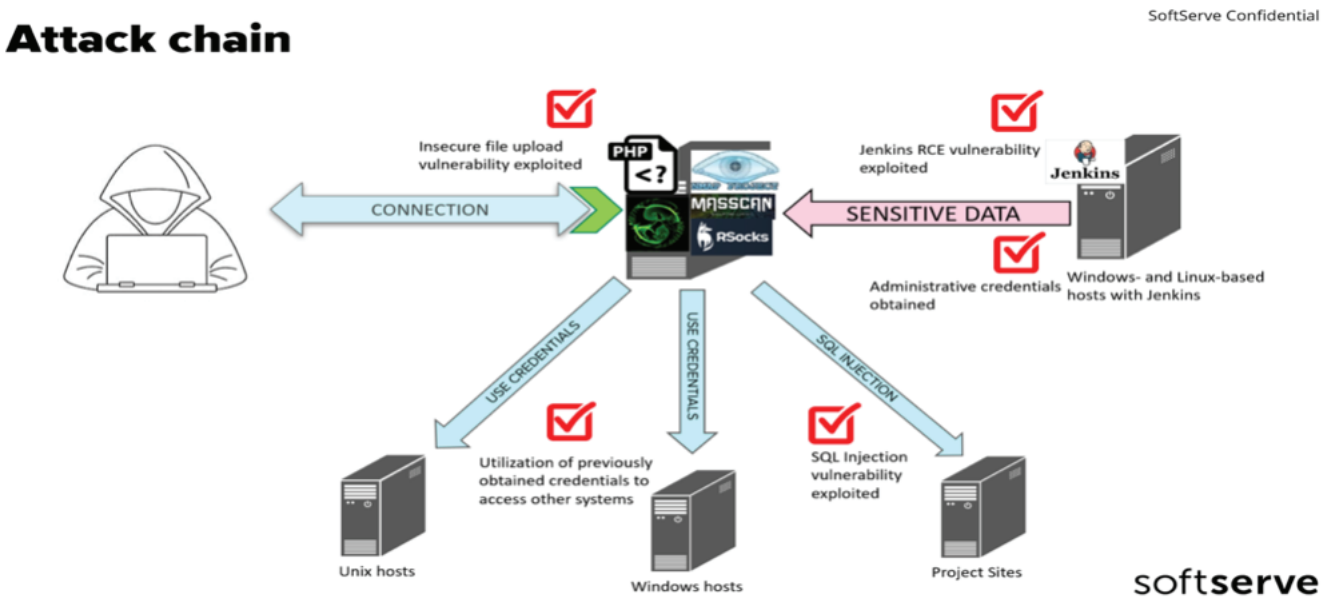
Administrator account had the same password on different hosts. This allowed an actor to get access to exploit Pass-The-Hash attack and get access to multiple Windows-based hosts, where the same credentials were utilized.

USE TIME-BASED SQL INJECTION ON VULNERABLE AAPLICATIONS

An actor used sqlmap tool to inject commands via the Login parameter and remote code execution.

USE OUTDATED VULNERABLE VERSIONS OF WORDPRESS

An actor utilized the wp-scan utility and found some outdated vulnerable WordPress instances.



Lessons learned and recommendations:

1. The dual-home networked hosts pose significant risk to the security of the IT infrastructure as they enable access to internal network once a relevant software vulnerability is found and exploited from the outside. Such deficiency must be eliminated on the level of network security design and security operations.

2. Setting unique and complex credentials to high-privilege user accounts is an essential practice of a modern security program. For secure management of local administrative credentials of Windows systems, using LAPS4 is strongly recommended.

3. Not all security vulnerabilities are easily discoverable by contemporary network-centric vulnerability scanners. Corporation must pay attention to a robust enterprise-wide application security testing program that would start from reviewing all potentially risky applications' security and continue by tracking changes made to those applications over time and testing the security of these incremental changes.

4. Obsolete operation systems are vulnerable to many known exploits. To resolve this security issue, the workstations should be upgraded to a more recent version of OS.

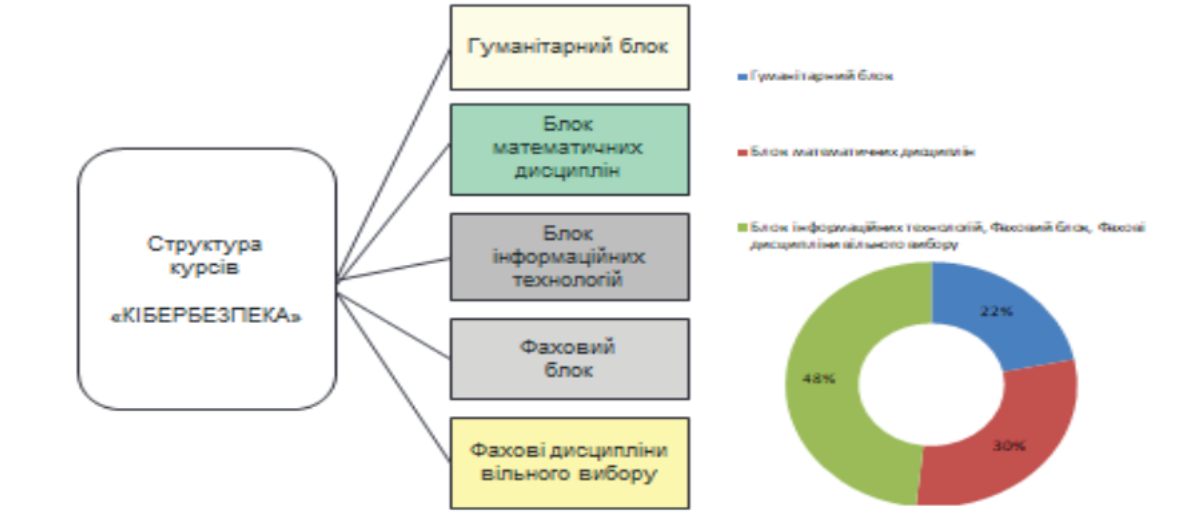
5. Changing the password of the krbtgt account as often as ppossible (e.g. once in a month or two) is significant to prevent the "Golden Ticket" attacks.

6. All scripts and applications with sensitive functionality should implement an

authentication mechanism. Any upload functionality should validate files that are uploaded.

7. Enable robust authentication mechanisms at all Jenkins instances in the organization.

Fig. 1 Structure of the education program cybersecurity.



8. Update all the default or primitive password. Wherever possible implement a reasonable password policy.

9. Restrict direct SSH and RDP access under administrative accounts. sudo and “Run as...” should be used for getting administrative access once logged in. Consider implementing a more sophisticated password management practices, such as Local Administrator Password Solution (LAPS).

10. Login parameter should be validated by the web application server and sanitized from any characters not expected as part of the login string according to the usernames convention.

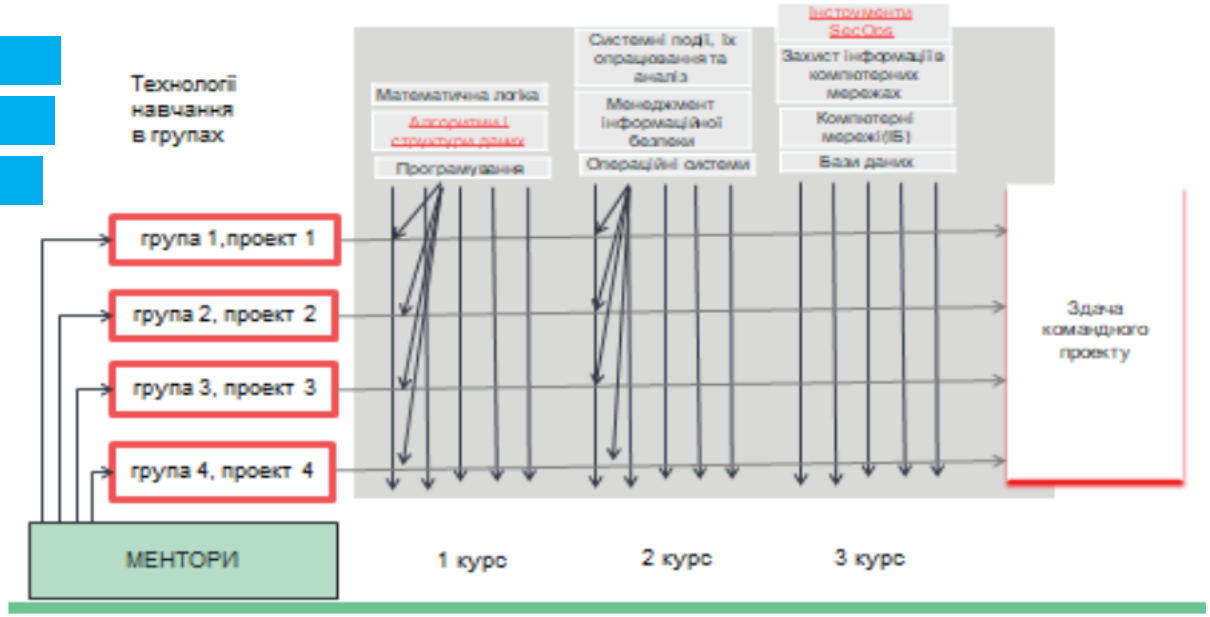
IV. Lack of cybersecurity specialists and their training at higher educational institutions.

The necessity of implementation of the provisions of European and international organizations aimed at introduction of modern educational and professional programs for the preparation of bachelor’s degrees in cyber security, the development of modern curricula and programs based on the development of mini-projects with the support of mentors from IT companies for the development of professional skills of cyber security specialists, providing the required number of specialists able to effectively solve the problems of information security of society.

V. Joint educational programs on cybersecurity. The example of training provided at Ivan Franko National University of Lviv.

One example of such educational programs is the development of a new, innovative, practical cyber security program at the Ivan Franko National University of Lviv, which combines the study of the basics of cyber security, the legal and organizational principles of combating cybercrime, software, cryptographic mechanisms and technical means of personal protection, enterprises , institutions and the country as a whole. The structure of such a program is shown in Fig. 1, where the display of the prevailing part of the disciplines of information technology, the professional unit and the block of free choice of the student.

Fig. 2 Technologies of implementation of mini-projects.



It is also worth noting the practical orientation of this curriculum, so from the first year students study the basics of cybersecurity and the basis of team work, which then would use this knowledge in the implementation of team mini-projects. When performing mini projects, students have the opportunity to consult with the mentor appointed from the IT companies and help to execute the mini-project qualitatively (fig.2).

Our program is different from other applications, that is, the development of applications for security, this is more application programming, the development of information systems for business, as we have a high level of mathematical training, then students have a logic of programming, they can manage projects and be able to climb higher the level for development management, that high level of programming is confirmed by prize-winning places on olympiads, hackathons and others.

VI. Summary and outlook.

Professional ability to analyze potential threats and risks of cybersecurity, the ability to detect signs of external influence, to simulate the possible such effects, to predict their consequences, the use of systemic software tools, the analysis of information security of objects and systems, using national and european standards, the formation of the complex measures to manage cybersecurity are the foundation, the main requirements of the professional competencies of educational programs for future cyber security specialists.

VII. References.

1. The Law of Ukraine of 10.05.2017 No 2163-VI “On the Basic Principles of Cybersecurity Protection of Ukraine”.

2. The standard of higher education in Ukraine: the first (bachelor’s) level, the branch Knowledge 12 - Information Technology, specialty 125 - Cybersecurity.

3. May, M. & Elliott, D. Consortium for Research on Information Security and Policy. https://fsi.stanford.edu/research/consortium_for_research_on_ information_ security_and_policy.

Web: www.promoteukraine.org
Contact: info@promoteukraine.org

Promote Ukraine is a non-profit start-up. It is a politically and governmentally independent organization situated in Belgium. It consists of a thriving team of professionals who on pro bono basis seek to give voice to Ukrainian civil society in Europe and, in particular, throughout Belgium. We believe in European values such as civil rights, good governance and equal opportunities. Through connecting EU businesses and politicians with Ukrainian stakeholders, we facilitate the sharing of best practices between EU and Ukrainian partners with the goal to bring Ukraine closer to EU norms and values from a bottom-up perspective.

promoteukraine

promoteukraine

promoteukraine