PHD TESIS AUTHOR'S REVIEW

NATIONAL UNIVERISTY OF PUBLIC SERVICE
Doctoral Council

ISTVÁN PARÁDA

Penetration test methodology for cyber operations

author's review of PhD thesis

Scientific supervisor:

General László Kovács Professor

Budapest, 2022

DEFINING THE SCIENTIFIC PROBLEM

Due to the continuous development of technology, with the advent of new security challenges and threats, information operations as well as cyber operations have become an everyday part of military activities. The European Union, the North Atlantic Treaty Organization (NATO), the United States of America and Hungary have also recognized the legitimacy and ever-increasing tendencies of this capability. It is clear that almost all countries are seeking solutions to cybersecurity security issues at the national level from a security policy perspective. So what links military cyber operations closely to security policy is security itself. If we are talking about security or cyber operations being handled on a national scale, it means that its interpretation must be carried out at military level. A fundamental question is how national strategies deal with the IT revolution and the accompanying rapid development of information and technology. Are they ignored, integrated into the processes, or exploited by their potential?

The modalities and procedures of cyber warfare and cyber operations can be examined from several perspectives.

Among the cyber capabilities, one of such important research elements is penetration testing, with which we reveal the shortcomings of our own IT systems by modeling cyber attacks. **Based on all this, I consider the scientific problem that determines my research to be that since international examples cannot be fully transposed into domestic procedures (as they are usually not intended for military use), Hungary must independently define and develop a method that provides an adequate basis for IT network testing and substantiated by detailed evidence.**

My choice of topic was basically determined by the experience gained during my years as a network system engineer at the Hungarian Defence Forces „vitéz Szurmay Sándor" Budapest Garrison Brigade, Central Information Center and the NATO Cooperative Cyber Defense Center of Excellence Participation in the course BOTNET Reduction and Cyber Defense at the Operational Level. In addition, the time spent as a lecturer at the National Univerity of Public Service, Faculty of Military Science and Officer Training Department, during which I came to the conclusion that it is necessary to incorporate the basic methods of ethical hacking procedures into education. In the course of my scientific research, I carry out the scientific elaboration and further development of my own testing methodology and applicable activity processes.

It is my professional conviction that the IT and information security specialists of the Hungarian Defence Forces perform their operational tasks with the greatest possible expertise. However, testing is a basic and statutory requirement to increase and maintain the security of your IT system. One of the most important such security tests is the penetration test, the first level of which is network discovery.

As there are generalized activity descriptions at the time of writing, their obsolescence and general nature allow me to suggest specific technical solutions that I intend to support with real alternatives.

DEFINITION OF RESEARCH HYPOTHESES

During the preparation of my doctoral (PhD) dissertation I formulated the following research hypotheses:

- Having an appropriate IT testing methodology, the Hungarian Defence Forces can effectively respond to the new types of challenges and threats of the age and exploit the capabilities of fourth generation warfare, information operations, computer network, network - centric warfare and network capabilities. One such opportunity inherent in cyber operations capabilities is to test your own network and infrastructure.
- The creation of an advanced, up-to-date, technology-based penetration test framework ensures the examination of the basic security of the infocommunication systems of the Hungarian Defense Forces and its achievement. The discovery solutions and processes used in cyber operations, mainly with technical characteristics, provide the framework for testing and evaluating our own infocommunication systems and networks.
- The cyber operation penetration methodology should be a cost-effective solution that supports the doctrinal task system. This can be done on the basis of the current infocommunication toolkit, with an emphasis on open source software.
- At the executive level, the capabilities elements of the cyber operations penetration methodology need to be focused in order to make optimal use of available resources. This is most effectively accomplished by developing the current cyber operations subunit, consolidating capability modules, and leading and managing an existing military organization. Its structure should be defined in such a way as to suit both the national system of tasks and the system and nature of international offerings.

In my research, I basically rely on the current information used by the Hungarian Defence Forces and the principles and procedures set out in NATO and US strategies, doctrines and basic documents.

DEFINITION OF RESEARCH GOALS

During the preparation of my doctoral (PhD) dissertation I considered the following to be the basic objectives:

- Examine the definitions of cyberspace, cyber defense, and cyber operation, and analyze the development of NATO and US cyber defense.
- To determine the basic definitions, the key features of the test and the structure of the main international infocommunication security tests by examining the examples of international penetration test models and methods, through the available open source domestic, NATO and US legislation. Based on all this, create a self-approach classification of penetration tests.
- To examine and evaluate the requirements of the legal background of the Hungarian Defence Forces and its connection points with a penetration test, and to create a model of the penetration test applicable in the Hungarian Defence Forces based on these.
- Based on the results of the analysis of international, NATO, US and domestic regulations, standards, documents and relevant scientific literature, to determine the steps for the development of cyber warfare network exploration related to cyber warfare. Demonstrate the steps, demonstrations, and conclusions of each technical activity through specific demonstrations, focusing on the analysis of published data and port scanning.

UTILIZED RESEARCH METHODOLOGY

During the preparation of my doctoral (PhD) dissertation I used the following research methods:

- Literature research, study, processing in relation to the relevant literature. I research, collect, review, analyze and process the relevant regulatory background, laws, regulations, instructions, decisions and measures related to the sub-areas covered by my dissertation, research and research;
- I collect, systematize, analyze and explain the relevant concepts related to my research topic in my opinion;
- Based on the available NATO and international regulations, I examine the possible models and directions used for similar testing;
- I am conducting secondary analysis of research such as that of the NATO CCDCOE (NATO Cooperative Center for Excellence in Cyber Defense) and U.S. Pat. cyber operations capabilities, research, examination. I draw conclusions about the

effectiveness of this and the extent of the possibilities for adaptation. I examine the expectations and regulations of the Hungarian Cyber Defense Strategy. I draw conclusions for the development of the model and methodology;

- Based on the results of the above examinations and my professional experience, I determine the elements of the model and methodology of the penteration test. While studying the system, I examine the procedures of the methodology. I analyze the properties of the methods made up of these. I work out the procedure of the methodology and the technical solutions of its operation.
- I process the available technical literature, by reproducing them I measure the legitimacy of software implementations;
- I perform empirical measurements of feasible testing mechanisms and evaluate the data obtained from the experiments, which I perform with the Kali Linux operating system;
- I draw conclusions from the evaluation of the data based on the experimental measurements and make them.

SHORT DESCRIPTION OF THE RESEARCH IN POINTS

In terms of its structure, my dissertation contains four chapters, each of which concludes with a section containing partial conclusions, findings and sub-summaries.

The first chapter of my dissertation is “Cyberspace and Cyber Operation”. As part of this, in order to articulate my scientific results, I will present cyberspace and cyber operations in detail. Among other things, I detail the layers of cyberspace, cyber supremacy, characteristics, principles and types of cyber operations. In addition, I detail the challenges and the need for a penetration test. I will then present the evolution of NATO and US cyber defense policies.

I have given the title of the second chapter of my dissertation the “Fundamentals and Classification of Cyber Operations Penetration Test”, which is one of the most important pillars of my scientific research. Therefore, I present the basics of the cyber operation penetration test. Among other things, I will detail the difference between the penetration test and the vulnerability analysis, and explain the purpose of such a test, which has its properties and limitations. In addition, I detail the challenges and the need for the test. Next, I present the classification of penetration tests themselves and their characteristics. I describe in general all the concepts that I consider necessary and lead me to formulate and validate my scientific results.

In the third chapter, I make suggestions on the issue of the "Cyber Operations Penetration Test and its Workflow" and formulate my scientific findings. To this end, as an introduction, I examine and present the possible workflow of the methodology and its relationship with the Hungarian Defence Forces. Then, in the planning and preparation phase, I describe the plan itself and its criteria, definition of scope and commitment. I am working on the issue of documentation and reporting.

In the fourth and final chapter, I present the cyber operation penetration test, with special regard to the collection of information within network technical reconnaissance through published data and the demonstration of network mapping. Using a scientific method, I make certain technical steps repeatable, which after implementation and its description become a methodology in the framework I have designed. I thoroughly categorize or group these studies and help them understand them with a theoretical description.

SUMMARY, FINAL CONCLUSIONS

I have processed and interpreted the basic concepts related to cyberspace and cyber operation. I have summarized the essential elements of cyberspace operations, including their characteristics, principles and types. I have examined and presented the two main directions of cyber defense development from the perspective of NATO and the USA, respectively. From these, I concluded that the interpretation of networks has changed significantly nowadays, with the addition of a network of cyber-physical devices as well as social networks created by humans. Due to the networking capabilities of cyberspace, information operations capabilities and impacts are also reflected in military operations. Cyber operations can be used for influence, counteraction, and defense. In my opinion, NATO has made and will continue to make significant efforts to develop and develop capabilities related to cyber operations, so as a NATO member, Hungary and the Hungarian Defence Forces must do likewise. Within the Hungarian Defence Forces, in line with the cyber security strategy, the development of cyber security capabilities can be vital for future tasks.

I have developed the guidelines of international standards, the basic concepts of penetration testing and its interpretations. I summarized the essential elements of the different penetration test system models, I analyzed in detail the most open penetration test standards and recommendations openly available. From these, I concluded that the cyber security penetration test provides a thorough study of IT systems. This testing method provides a complex analysis that covers the IT and cybersecurity issues of the system and the organization,

and can greatly contribute to the cyber operations efforts of the Hungarian Defense Forces. The methodologies take a different approach to performing the penetration test or security test. In order to understand these differences, I compared the different methodologies, examining their objectives, the activities of the tests performed in practice. Comparing the methods, it becomes clear that all four methodologies offer different approaches to performing the penetration test and are not necessarily compatible with each other. I processed and interpreted and grouped the classification of the penetration test based on the international literature. Distinguishing characteristics in the classification of tests include, for example, the size and structure of the systems tested and the precautionary or aggressive nature of the tests. The characteristics that apply to a particular penetration test should be tailored to the purpose of the test in order to perform an efficient and effective test.

I defined the relationship of the penetration test methodology with the Hungarian Defence Forces at the operational and organizational level, and I defined the military nature of the test. I proposed a workflow for the penetration test. Based on all this, I developed the various elements of a cyber operation penetration test plan document. Based on these, I declare that military systems are now digital systems, so a penetration test is a basic requirement for military digital infocommunication networks. These experiences can provide clues as to which cyberspace layer the attacking party should be in and how to attack. Attacking military infocommunication systems in cyberspace is considered military activity. Under current domestic laws and regulations, the Ministry of Defense operates its own organization providing cyber protection for closed and open defense systems within the framework of the Military National Security Service, which supports the security of IT systems for defense purposes, the management of security incidents at the sectoral level, and the implementation of vulnerability investigations. The cyber operation penetration test methodology provides a basic framework for laying down important initial and post-investigation information that can be used by individual units to prepare for the audits and inspections they intend to perform. The application of the cyber operation penetration test plan and test report enables a more efficient flow of information, more effective cooperation between the decision-making and executive levels, and the joint execution of tasks in the field of IT security and cyber security.

I defined the steps of information gathering and network mapping, their technical descriptions and their theoretical background. I have verified and performed the essential elements of the operational and technical applications of search engine, web service, website information gathering, and information extraction through WhoIs and DNS information extraction with measurements and tests via the Internet. In my own test environment, I verified

and performed the essential elements of the operational and technical applications of target discovery, port scanning with measurements and tests. Based on these, I came to the conclusion that the spread and success of the adaptive procedures already successfully applied in civilian IT systems provide a basis for reviewing their military application. In the case of military adaptation, the standard systems of NATO and other nations in force must be examined. Based on the methodology of the military penetration test, it is also possible to implement information collection and network mapping in the technical process of network reconnaissance, using technical documentation and reporting procedures designed specifically for military applications, as well as emphasizing motivation.

SCIENTIFIC RESULTS

- I have examined the definitions of cyberspace, cyber defense, and cyber operation, and I have analyzed and processed the development of cyber defense in NATO and the United States.
- I analyzed the international penetration test models. I defined the basic definitions, the key features of the test, and the structure of the major international infocommunication security tests. Based on all this, I created my own approach to the classification of penetration tests.
- I evaluated the requirements of the legal background of the Hungarian Defence Forces and its connection points with a penetration test, and based on these I created a model of the penetration test process applicable in the Hungarian Defence Forces. I have created the steps for implementing the penetration test methodology applicable in cyber operations.
- I created and presented the steps of the technical implementation of the network discovery elements of the penetration test methodology applicable in cyber operations, especially for the open source technical information collection and network mapping solutions, in accordance with the classification approach I created. I proved and proved the applicability of the steps and its results through technical implementations.

RECOMMENDATIONS FOR PRACTICAL USAGE

- I propose to examine the model of the technical process of the penetration test methodology applicable in cyber operations - in the framework of cyber and news and IT system exercises - and to integrate the practical experience into the constantly changing, changing news support system.
- I propose Decree 1838/2018 on the Strategy for the Security of Network and Information Systems in Hungary. (XII. 28.) that the establishment of a cyber defense reporting chain and link between the Military National Security Service and the NATO Strategic Airlift Capability (SAC) located in Hungary, at the Pápa AirBase in Hungary, providing cyber defense , including the cyber operations capability of vulnerability analysis.
- I recommend that my dissertation and the results of my research be processed by a designated officer / chief officer serving at all three levels of management, participating in the development of the leadership and management of cyber operations and news and IT perspectives.
- I recommend the review and teaching of the theoretical system of the penetration test methodology applicable in cyber operations at the specialist departments of the Faculty of Military Sciences and Officer Training of the National University of Public Service.
- I propose to treat the examination of the technical solutions of the penetration test methodology applicable in cyber operations as a further research basis.

LIST OF PUBLICATIONS

1. Paráda, István: Műholdas antennarendszerek gyakorlati alkalmazhatósága a Magyar Honvédségben. Kommunikáció Budapest: Magyarország Zrínyi Miklós Nemzetvédelmi Egyetem, (2010) pp. 327-336. 10 p.
2. Paráda, István: NATO-ban használt műholdas antennarendszerek. HÍRVILLÁM = SIGNAL BADGE 2010: 1 pp. 100-105. Paper: 2061-9499, 6 p. (2010)
3. Pándi Erik, Paráda István, Jobbágy Szabolcs: A hálózat aktív és passzív eszközeinek, protokolljainak sebezhetőségére épülő támadások, szolgáltatások HÍRVILLÁM = SIGNAL BADGE V: 1 pp. 167-186., 20 p. (2014)
4. Bodnár István, Paráda István: Jelszó ellopás social engineering, e-mail spoofing és fake URL segítségével HÍRVILLÁM = SIGNAL BADGE 7: 1 pp. 139-147., 9 p. (2016)
5. Paráda, István: SNMP alapú hálózat monitoring program fejlesztése és alkalmazása-I. HÍRVILLÁM = SIGNAL BADGE 6: 1 pp. 73-88. Paper: 2061-9499, 16 p. (2015)
6. Pándi Erik, Paráda István: Network monitoring program development based on SNMP protocol HÍRVILLÁM = SIGNAL BADGE 6: 1 pp. 177-184., 8 p. (2015)

7. Paráda, István: Webkamera Hack – Penetration test, Hadmérnök XII: különszám pp. 204-216., 13 p. (2017)
8. Paráda, István: A NATO kibervédelmi irányelveinek fejlődése Honvédségi szemle: A magyar honvédség központi folyóirata 146: 3 pp. 3-13., 10 p. (2018)
9. Paráda, István: Requirements for developing the Cisco Net Academy to Pearson Vue Exam Center HÍRVILLÁM = SIGNAL BADGE 9: 1 pp. 20-36., 17 p. (2018)
10. Paráda, István: Felderítés és analízis a penetrációs tesztben – 1. Információgyűjtési technikák, Hadmérnök 15: 1 pp. 159-182., 24 p. (2020)
11. „A Metasploit tulajdonságai egy biztonságos FTP démon exploit tükrében", Hadmérnök 15: 3 pp. 219-230., 12 p. (2020)
12. Social engineering in inforamtion infrastucture – cybersapce In: Ivan, MAJCHÚT; Vladimír, ANDRASSY; Štefan, GANOCZY; Michal, HRNČIAR; Ondrej, KREDATUS; Gabriela, KREDATUSOVÁ; Jakub, SASARÁK; Juraj, ŠIMKO; Jaroslav, VARECHA; Lubomír, BELAN; Stanislav, MORONG (szerk.) 8. medzinárodná vedecká konferencia: "NATIONAL AND INTERNATIONAL SECURITY 2017" Liptovsky Mikulas, Szlovákia: Akadémia ozbrojených síl generála Milana Rastislava Štefánika, (2017) pp. 344-351., 8 p.
13. Possible classification of cybersecurity penetration test, Hadmérnök 13: 4 pp. 329-339., 11 p. (2018)
14. Cyberstrategy of united States – Cronology Process in the Light of the Goals, Hadtudományi szemle XI: 3 pp. 137-153., 17 p. (2018)
15. Basic of cybersecurity penetration test, Hadmérnök 13.: 3. pp. 435-442., 8 p. (2018)

PROFESSIONAL - SCIENTIFIC CURRICULUM VITAE

Personal data:

Name: Paráda István
Date and place of birth: Kisvárda, 08.02.1991.
Family status: married, father of two child
Constant/postal address: 6400 Kiskunhalas Kármán street 27.
Phone: 06-30-203-7729
E-mail: paradaistvan@gmail.com

Professional experience

2021-	NSPA - NATO Support and Procurement Agency CIS Operation Officer/ Service Desk Manager
2019- 2021	Mercedes-Benz Manufacturing Hungary Kft. IT Project Manager / Network Engineer
2016-2019	National University of Public Service Faculty of Military Science and Officer Training - IT Network Instructor
2013 -2015	Hungarian Defense Forces - Network Engineer

Lectures

2016-	National University of Public Service Doctoral School of Military Engineering PHD Student
2013 - 2015	Óbudai University Kandó Kálmán (MSc) Electric engineer
2009-2013	National University of Public Service (BSc) Faculty of Military Science and Officer Training Military and Security Engineer

Language knowledge:

English Proficiency C1
Germany Basic B1

Courses, professional knowledge:

- Crypto Administration (0004-221064 NCIA)
- Cards for NATO Crypto Custodian (0006-221080 NCIA)
- Cisco Certified Network Associate Routing and Switching (CCNA) 437794169816JODK
- Cisco Certified Entry Networking Technician (CCENT) 435274170890HLYG
- Manager responsible for the protection of electronic information systems PN-0277-1401-MS
- Incidentmanagement PN-0449-1710-MS-C1
- Targeted cyber attacks PN-0470-1712-MS-C1
- CCNA Cyber security Operations
- CISCO ICND1. Instruktor
- CISCO ICND2. Instruktor
- EUROPEAN SECURITY AND DEFENCE COLLEGE Kurzus (ESDC-CEPOL-NKE)
- CYBER DEFENCE AT OPERATIONAL LEVEL Kurzus (NATO CCDCOE)
- IST-143 - LS on Cyber Security Science & Engineering
- CNA Introduction to Cyber security
- CNA Cyber security Essentials
- CNA Connecting Things

Scientific recognitions, awards

- „Az év információvédelmi szak- és diplomadolgozata – 2013” 1st price
- Magyar Hadtudományi Társaság commemorative medal

Scientific research, lectures

- 6 month „Good Governance Knowledge Transfer Program NUPS – USA" 2018.01.03-2018.05.06 University of North Georgia Dahlonega USA
- David Aghmashenebeli National Defence Academy of Georgia (under Russia in Gori) - Cybersecurity course;
- Nicolae Bălcescu Land Forces Academy, Sibiu, Romania - IT Networking course;
- University of Defence, Brno, Czech Republic - Cyber Security course;
- The Armed Forces Academy of General Milan Rastislav Štefánik, Liptovský Mikuláš, Slovak Republic - Cyber Security course;
- Researchers' night lecture;
- Communication conference presentation;
- Military information security conference presentation.

Experiences abroad

- Cyber Shield 2019 Indiana, United States of America.
- David Aghmashenebeli National Defence Academy of Georgia (under Russia in Gori) - IT Networking course
- NATO Cyber security conference in Lisbon as subject matter expert (SME)
- 6 month „Good Governance Knowledge Transfer Program NUPS – USA" 2018.01.03-2018.05.06 University of North Georgia Dahlonega USA
- Nicolae Bălcescu Land Forces Academy, Sibiu, Romania - IT Networking course
- University of Defence, Brno, Czech Republic - IT Networking course
- Saber Guardian NATO exercise– Multi National Division, IT Planning Officer, Bulgaria
- 5 month Poland Warsaw at Wojskowa Akademia Techniczna within Erasmus program

Others

- Member of Puskás Tivadar Signals Fellowship
- Honorary member of Puskás Tivadar Engineer Advanced College