PhD in Information Technology and Electrical Engineering
Università degli Studi di Napoli Federico II

PhD Student: Nicola d'Ambrosio

Cycle: XXXVII

Training and Research Activities Report

Academic year: 2022-23 - PhD Year: Second

Tutor: Prof. Simon Pietro Romano

Co-Tutor:

Date: December 11, 2023

1. Information:

- **PhD student: Nicola d'Ambrosio PhD Cycle: XXXVII**
- **DR number: DR996111**
- **Date of birth: 15/07/1994**
- **Master Science degree: Computer Engineering**
- **University: University of Naples Federico II**
- **Scholarship type: MUR PON**
- **Tutor: Simon Pietro Romano**

2. Study and training activities:

Activity	Type[1]	Hours	Credits	Dates	Organizer	Certificate[2]
Virtualization technologies and their applications	Course	n.d.	5	n.d.	DIETI Dr. Luigi De Simone	Y
PhD School: CNTC2023 Complex Networks and Telecommunications: Third edition	Course	n.d.	4	n.d.		Y
Artificial Intelligence and Natural Language Processing	Course	n.d.	3	n.d.	DIETI Prof. Francesco Cutugno	Y
IEEE NFV-SDN	Seminar	10	20	7-9/11/2022	IEEE	Y
Robotics Meets AI & 5G: The Future is Now!	Seminar	3	0.3	30/10/2023	Prof. Bruno Siciliano	Y
Migration of legacy IT infrastructures into the cloud.	Seminar	2	0,4	23/5/2023	DIETI Prof. Roberto Canonico	N
RAILS Final & Roadmapping Events	Seminar	2	0.4	30/5/2023	DIETI Prof. Valeria Vittorini	N
Traffic Engineering with Segmented Routing: optimally addressing popular use cases	Seminar	1	0,2	23/6/2023	DIETI Valerio Persico	N

1) Courses, Seminar, Doctoral School, Research, Tutorship
2) Choose: Y or N

2.1. Study and training activities - credits earned

	Courses	Seminars	Research	Tutorship	Total
Bimonth 1	0	0	8	0	8
Bimonth 2	5	0	5	0	10
Bimonth 3	0	1	9	0	10
Bimonth 4	4	0	6	0	10
Bimonth 5	0	0.3	9.7	0	10
Bimonth 6	3	2	5	0	10
Total	12	3.3	42,7	0	
Expected	30 - 70	10 - 30	80 - 140	0 – 4.8	

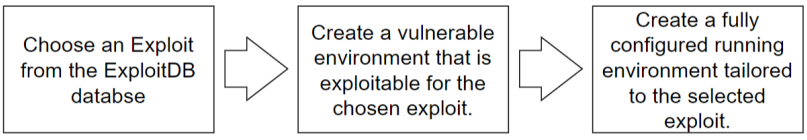
3. Research activity:

In the second year of my Ph.D. program, I actively engaged in a series of research activities within my specialized field:

- **Automate-2-image: an automated platform for testing vulnerabilities exploitability**

The increasing complexity of software leads to a surge in the number of vulnerabilities discovered. These vulnerabilities are defects in software components that can seriously compromise the security and integrity of entire computer systems. Exploiting these vulnerabilities can lead to unauthorized access, data breaches, and system malfunctions. Therefore, identifying weaknesses and assessing potential security issues within IT systems is crucial and should be done as soon as possible. One security methodology employed for this purpose is Penetration Testing (PT). PT involves emulating the actions of a malicious attacker to uncover potential weaknesses and vulnerabilities that could be exploited.By performing these simulated attacks, the tester can assess the severity of threats posed by both internal and external adversaries. Unfortunately, conducting a penetration test is not straightforward mainly for three primary reasons. Firstly, it requires a highly skilled and knowledgeable tester who is familiar with different attack techniques and vulnerabilities in order to efficiently identify potential security gaps within the targeted system. Secondly, conducting a penetration test can be time-consuming, especially during the exploitation phase. Lastly, the testers must conduct assessments in a manner that does not disrupt the company's daily operations.

To address these issues, we have developed the Automate-2-image process. This innovative process streamlines the setup of two distinct environments: one designed to replicate vulnerabilities for testing purposes and another that simplifies the execution of exploits.



This model allows us to efficiently assess the effectiveness of various exploits and identify vulnerabilities in a controlled and repeatable manner. In fact, automating the setup of these environments helps us to save significant time that would otherwise have been spent on manual

configurations. Moreover, this project can aid researchers in developing and evaluating new cyber defense strategies by constructing a repository of test programs with documented weaknesses, which can be used to replicate and compare experimental results. Indeed, the automated setup of these environments ensures consistency and accuracy in testing, reducing the risk of human error and increasing the reliability of the results obtained. Consequently, this collection of test programs can also be used to develop more robust and effective defenses against emerging threats.

- **A Software-Defined Approach for Mitigating Insider and External Threats via Moving Target Defense**

Simultaneously, cyber-attacks have become increasingly precise and sophisticated over time. Adversaries continuously refine their techniques and leverage advanced tools to breach cyber defenses. In this landscape, conventional security measures like firewalls, authentication controls, and intrusion prevention systems (IPS) may prove insufficient in preventing infiltration attempts. As a solution, the concept of \textit{defensive deception} has emerged as an additional layer of defense to enhance cyber-defense strategies. This approach involves the implementation of deceptive techniques aimed at misleading attackers, diverting their attention, and detecting their activities. Honeypots, Honeynets, and Moving Target Defense are examples of such techniques. By incorporating defensive deception into their cybersecurity frameworks, organizations can bolster their defenses against evolving cyber threats. These techniques serve to confuse and misdirect attackers, ultimately buying precious time for detection and response. By integrating elements such as honeypots and honeynets, organizations can gather valuable intelligence about the tactics and objectives of adversaries. Moving Target Defense, on the other hand, introduces dynamic and unpredictable changes to the network infrastructure, making it harder for attackers to exploit vulnerabilities. Unfortunately, to the best of the authors' knowledge, there are currently no available frameworks that effectively address the defense against both external and insider threats using the aforementioned approach.

We propose a framework that combines Honeypots and Moving Target Defense as defensive deception techniques within a business network to address security issues posed by both external and internal threats. In detail, the aim is to detect the attacker's scanning and exploitation activities by combining MTD and honeypots and redirecting all connections towards a Honeynet for further analysis and protection of critical assets. Additionally, proactive and reactive port hopping techniques are strategically employed to confuse and mislead the attacker. Through these techniques, we are able to fortify network defenses, increase the complexity faced by potential attackers, and acquire valuable knowledge about their tactics.

- **Cyber Range data collector**

Our objective is to create a tool that can effectively gather all relevant data on hacker behavior during a cyber security exercise within a cyber range. Indeed, we aim to generate a strucured dataset that can be easily analyzed and visualized. To achieve this, we collect input, output, and timestamps of every command executed in the shell. Additionally, we take screenshots of the active window at specific instants of time. Finally, the collected data is processed to create a JSON file containing information about each terminal session. We also generate a GIF that displays all the screenshots collected over time, shown in sequence. The collected information is then effectively stored, indexed, searched and visualized.

- **Threat Scenarios to Attack Emulation**

We have developed a framework for generating threat scenarios and emulating attacks. This framework consists of two main tools: Cassandra and AttackGenerationTool. Cassandra uses the STPA model to represent the safety model of an industrial architecture and identify cyber security threats that may compromise safety features, also known as Hazard Control Actions (HCA). Additionally, Cassandra employs the STRIDE threat model and MulVal to identify cybersecurity threats and find attack paths that could trigger these HCAs. The AttackGenerationTool uses the information generated by Cassandra to perform the attack as described previously. We tested the effectiveness of this framework by successfully simulating safety-critical attacks on an Alternate Current (AC) Micro Grid (MG) testbed in a controlled environment. This testbed was set up using real hardware devices, docker containers, and virtual machines.

- **OSINT-Collector**

We are developing a tool that helps users manage data from open sources. Our goal is to make it easy for users to collect, organize, and analyze information. The project has three modules: the Tool Classifier, the Data Collector, and the Data Visualization module. The Tool Classifier is crucial because it suggests the best OSINT tools to use based on the user's needs. It uses an ontology-based approach to make automatic recommendations. The Data Collector module stores the data in a graph database, making it easy to organize and find connections. This helps users gain insights from the data. Finally, the Data Visualization module provides an interface that presents the analyzed data in visual formats.

- **A containerized testbed for benchmarking QUIC protocol implementations in satellite-enabled scenarios**

The goal of this project is to create a containerized test environment that focuses on benchmarking QUIC (Quick UDP Internet Connections) protocol implementations for satellite-based scenarios. This test environment will offer a controlled and replicable setting for running benchmark tests, allowing comparisons between different QUIC implementations. The aim is to identify the most efficient protocol for this specific context, enhancing the QUIC protocol for what concerns congestion control.

- **From closed systems to open platforms: designing an Open microservices-based architecture for drone control**

Unmanned Aerial Vehicles (UAVs) have become a crucial tool in both military and civilian operations, including the important tasks of surveillance and inspection. Nevertheless, the current use of monolithic architectures in drone platforms limits their ability to quickly and effectively incorporate new features and improvements. To address these challenges, we propose an open system approach based on microservices and open standards in this context. This new paradigm holds the promise of increased overall security, better interoperability, and simplified implementation of feature updates. Additionally, embracing this approach can aid us in more effectively assessing the safety and cyber security aspects of drone development.

4. Research products:

F. Caturano, N. d'Ambrosio, G. Perrone, L. Previdente and S. P. Romano, "ExploitWP2Docker: a Platform for Automating the Generation of Vulnerable WordPress Environments for Cyber Ranges," 2022 International Conference on Electrical, Computer and Energy Technologies (ICECET), Prague, Czech Republic, 2022, pp. 1-7, doi: 10.1109/ICECET55527.2022.9872859.

N. d'Ambrosio, E. Melluso, G. Perrone and S. P. Romano, "A Software-Defined Approach for Mitigating Insider and External Threats via Moving Target Defense," 2023 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Dresden, Germany, 2023, pp. 213-219, doi: 10.1109/NFV-SDN59219.2023.10329613.

Nicola d'Ambrosio, Gaetano Perrone, Simon Pietro Romano, "Including insider threats into risk management through Bayesian threat graph networks", Computers & Security, Volume 133, 2023, 103410, ISSN 0167-4048, doi: 10.1016/j.cose.2023.103410.

5. Conferences and seminars attended

6. Periods abroad and/or in international research institutions

Abroad research period at the Accenture Cyber Fusion Center of Prague, Czech Republic, under the supervision of Jiri Dostal The research activities carried out in this period were focused on a field study on Automotive Security and Automotive Penetration Testing. The abroad research period took place from July 1st, 2023, to December 31st, 2023 (July 1st to September 1st was conducted in smart working). Additionally, as part of the PhD, I worked for four months at Accenture Italy in a remote working. The scholarship project outlines a duration of six months at Accenture Prague and six months at Accenture Italy.

7. Tutorship

8. Plan for year three

In the next year, I plan to:

- enhance our ability to detect malicious activities in the Honey-MTD project by exploring advanced IDSs and anomaly detection techniques that leverage machine learning.
- the Proof of Concept (PoC) for OSINT-Collector, with a specific focus on developing a robust platform or script designed to systematically gather data from diverse open sources.
- write my PhD thesis