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

Year: First

Tutor: prof. Simon Pietro Romano

Co-Tutor:

Date: December 15, 2022

1. Information:

- **PhD student: Nicola d'Ambrosio**
- **DR number: DR996111**
- **Date of birth: 15/07/1994**
- **Master Science degree: Computer Engineering University: Università degli studi di Napoli Federico II**
- **Doctoral Cycle: XXXVII**
- **Scholarship type: PON Dottorati di ricerca su tematiche dell'innovazione e green - Azione IV.4 (Innovazione)**
- **Tutor: Simon Pietro Romano**
- **Co-tutor:**

2. Study and training activities:

Activity	Type[1]	Hours	Credits	Dates	Organizer	Certificate[2]
Probability calculus and elements of stochastic modelling	Courses		4	10 January 2022 | 6-week course duration	Massimiliano Giorgio	Y
Risk Management	Courses		6	07/3/2022 | 17 weeks	Alessandra De Benedictis	Y
Software Security	Courses		6	07/3/2022 | 17 weeks	Roberto Natella	N
Operational Research: Mathematical Modelling, Methods and Software Tools for Optimization Problems	Courses		4		Adriano Masone	Y
RAILS MID-TERM WORKSHOP	Seminar		1	25/2/2022	Roadmaps for A.I. Integration in the Rail Sector	Y
Project Vāc: Can a Text-to-Speech Engine Generate Human Sentiments?	Seminar		0,4	28/2/2022	Prof. V.K. Gubani	Y
IEEE Authorship and Open Access Symposium: Tips and	Seminar		0,4	30/3/2022	IEEE	Y

Best Practices to Get Published from IEEE						
2nd Workshop on Virtualization Technologies and their Applications (VIRTECH)	**Seminar**		**0,8**	**08/3/2022**	**Luigi De Simone**	**Y**
Fixed Wireless Access	**Seminar**		**1**	**17/5/2022**	**5G Academy**	**N**
5G Networks in Action – The Private Mobile Era	**Seminar**		**0,2**	**11/5/2022**	**5G Academy**	**N**
AR for remote use of measurement instrumentation	**Seminar**		**0,3**	**24/5/2022**	**5G Academy**	**N**
Human-Multi-Robot Systems: Challenges for Real World Applications	**Seminar**		**1**	**27/10/2022**	**IROS 2022**	**N**
PRIVACY-PRESERVING MACHINE LEARNING	**Seminar**		**0,2**	**14/10/2022**	**DIETI - UniNa**	**N**
Connecting the dots: Investigating an APT campaign using Splunk	**Seminar**		**0,4**	**11/11/2022**	**DIETI - UniNa**	**Y**
Privacy and Data Protection	**Seminar**		**0,4**	**22/11/2022**	**DIETI - UniNa**	**Y**

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**	**1,4**	**8,6**	**0**	**10**
Bimonth 2	**0**	**1,2**	**8,0**	**0**	**9,2**
Bimonth 3	**10**	**1,5**	**5**	**0**	**16,5**
Bimonth 4	**0**	**0**	**10**	**0**	**10**
Bimonth 5	**0**	**1,2**	**8,8**	**0**	**10**
Bimonth 6	**10**	**0,8**	**0,2**	**0**	**11**
Total	**20**	**6,1**	**40,6**	**0**	**67,7**
Expected	**30 - 70**	**10 - 30**	**80 - 140**	**0 – 4.8**	

3. Research activity:

During my first year of PhD, I carried out three research activities within my research field:

- **ExploitWP2Docker: a Platform for Automating the Generation of Vulnerable WordPress Environments for Cyber Ranges**

Cyber ranges are interactive, virtual representations of networks, systems, tools, and applications that enable learners to both practice and assess the acquired skills. These virtual scenarios provide a safe and legal environment to gain hands-on cyber skills, to learn secure development, and, more in general, to test an organization's security posture. Unfortunately, the development and maintenance of a cyber range can become cumbersome. In fact, the realization of the vulnerable environment used to train is often done manually and requires a lot of time, effort, and skills. To address these challenges, we present an approach, called ExploitWP2Dcoker, that automatically creates and configures cyber range scenarios. The strength of this work is that the proposed method automates the generation of vulnerable CMS platforms for cyber ranges, which significantly reduces the amount of manual work required.

We show how it is possible to automatically generate vulnerable WordPress environments by thoroughly analyzing well-documented public exploits collected into exploit databases. The vulnerable container generation starts by selecting a public WordPress exploit present on ExploitDB. The exploit title and the metadata are analyzed and converted into helpful information to find a Docker image that satisfies the exploit preconditions. The search is performed on Docker Hub, the world's largest repository of Docker images. When an image is found, it is used as the base for generating a Dockerfile containing all the instructions needed to setup the vulnerable environment. The process is completed by installing all the components required to reproduce the vulnerability, as well as the required CMS plugins and themes.

With our approach, we were able to build more than four hundred vulnerable WordPress environments. The number of such vulnerable environments will certainly increase over time with the release of new exploits. Our future work will expand the focus towards other systems beyond WordPress, starting from other CMS, such as Joomla and PHP-based web applications.

- **SCASS: an Industrial Testbed**

An ICS (industrial control systems) testbed is a simulated environment that is used to test the security and performance of industrial control systems. This type of testbed is typically used by researchers and engineers to evaluate new technologies and protocols, and to identify and mitigate potential vulnerabilities in ICS systems. An ICS testbed may be a physical, hybrid or virtual environment. A physical testbed is a real-world environment that is used to test and evaluate new technologies and systems. This type of testbed typically includes real hardware and components, and it provides a realistic and comprehensive environment for testing. A virtual testbed is a simulated environment that is used to test and evaluate new technologies and systems. This type of testbed does not use real hardware or components, and it allows for testing in a controlled and reproducible environment. Therefore, when a physical testbed is not practicable, virtual testbeds are frequently utilized. A hybrid testbed is a combination of physical and virtual components, and it allows for testing in both real-world and simulated environments. The advantages of both physical and virtual testbeds are given by this kind of testbed, which also offers grater testing flexibility and control.

In this context, we design and implement SCASS (SCAda Systems Security), a hybrid modular testbed, that emulates a physical micro-grid testbed presented by Kandasamy et al. [1], called EPICTWIN. The hybrid nature of our testbed lets us obtain a more scalable and maintainable environment.

The SCASS environment mainly consists of five different components:

- Different Intelligent Electronic Devices (IEDs) that are used to measure Current, Voltage, Power and Frequency for the three phases buses. All these components are virtualized using python scripts.
- A Supervisory Control and Data Acquisition (SCADA) module is used to monitor and control industrial processes. This component is virtualized using Node Red flows.
- Different Programmable Logic Controllers (PLCs) that are used to automate and control industrial processes. They can disconnect a specified component from the main grid.
- A Data Historian that is used to collect, store, and analyze historical data from various sources.

The outcome of this research activity represents a strong foundation for our next research project. Indeed, this cyber range can be used:

- to train individuals and teams in cybersecurity skills such as penetration testing, incident response, and network security;
- to measure the effectiveness of proactive cyber defense strategies, like cyber deception and moving target defense, in industrial environments;
- to verify if our innovative cyber defense strategy can affect the safety of our industrial environment;
- to validate cyber security risk and safety assessment methodologies.

- **Including Insider Threats into Risk Management through Bayesian Threat Graph Networks**

Cyber risk management is the process of identifying, assessing, and controlling threats to an organization's information and systems. These threats, also known as cyber risks, could come in the form of hacking, data breaches, viruses, and other types of cyber-attacks. The goal of cyber risk management is to minimize the negative impact of these risks on an organization and to maximize the security of its information and systems. This is typically done through a combination of technical controls, such as firewalls and encryption, as well as policies and procedures, such as user training and incident response plans.

Our work widens the research scope to include insider threats in risk management processes. In fact, even if risk management frameworks are extensively adopted to prevent security risks in companies, their application to address insider threats is relatively unexplored. To address this challenge, we show a network security risk management framework based on Bayesian Decision Networks that allows the selection of the best security controls' combination under budget constraints. In particular, we first enrich an interesting work proposed by Khosravi and Bafghi [2] based on Bayesian Decision Networks to cover a broader range of threats. Then, we formalize several concepts, such as the security control coverage and the risk strategy and show that our model can easily integrate insider threats when specific properties are defined. Finally, to address insider threats, we integrate particular security controls that differ from the standard ones, such as technical IT training sessions and employee satisfaction surveys. As future work we will focus on applying such error models in order to evaluate their effectiveness in quantifying security risks that human errors introduce.

- **References**

[1] Kandasamy, Nandha Kumar, et al. "EPICTWIN: an electric power digital twin for cyber security testing, research and education." arXiv preprint arXiv:2105.04260 (2021).

[2] Khosravi-Farmad, M., Ghaemi-Bafghi, A. Bayesian Decision Network-Based Security Risk Management Framework. J Netw Syst Manage 28, 1794–1819 (2020). https://doi.org/10.1007/s10922-020-09558-5

4. Research products:

Francesco Caturano, Nicola d'Ambrosio, Gaetano Perrone, Luigi Previdente, Simon Pietro 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). IEEE, 2022. [published]

5. Conferences and seminars attended

Francesco Caturano, Nicola d'Ambrosio, Gaetano Perrone, Luigi Previdente, Simon Pietro 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). IEEE, 2022. [published]

6. Activity abroad:

7. Tutorship