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

PhD Student: Luciano Pianese

Cycle: XXXIX

Training and Research Activities Report

Year: First

Tutor: prof. Roberto Natella

Co-Tutor: BRACCIOLI Marco

Date: October 31, 2024

Training and Research Activities Report

PhD in Information Technology and Electrical Engineering

Cycle: XXXIX **Author: Luciano Pianese**

1. Information:

- **PhD student:** **Luciano Pianese**
- **DR number:** **DR997206**
- **Date of birth:** **08/10/1998**
- **Master Science degree:** **Computer Engineering**
- **University:** **Università degli Studi di Napoli Federico II**
- **Doctoral Cycle:** **XXXIX**
- **Scholarship type:** **PNRR - DM 117/2023**
- **Tutor:** **Roberto Natella**
- **Co-tutor:** **Marco Braccioli**

2. Study and training activities:

Activity	Type[1]	Hours	Credits	Dates	Organizer	Certificate[2]
Ensuring Electronic Reliability Against CERN's Radiation Environment	**Seminar**	**2**	**0.4**	**01/12/2023**	**Prof. Francesco Fienga**	**Y**
Energy-Efficient Data Science	**Seminar**	**1**	**0.2**	**13/12/2023**	**Prof. Elio Masciari**	**Y**
Virtualization technologies and their applications	**Course**	**24**	**5**	***08-10-15-19-24-25-29-31/01/2024, 05-07-26/02/2024***	**Prof. Luigi De Simone**	**Y**
Strategic Orientation for STEM Research & Writing	**Course**	**24**	**5**	***07-15/12/2023 – 12-19/01 - 09-23/02/2024***	**Sig.ra Adriana D'Auria**	**Y**
HOMINIS	**Seminar**	**5**	**1**	***21/02/2024***	**Prof. Carlo Sansone**	**Y**
Hands-on Network Intrusion Detection via Machine and Deep Learning	**Course**	**16**	**4**	***09-11-16-17-18/01/2024, 04/04/2024***	**dr. Antonio Montieri**	**Y**
Statistical data analysis for science and engineering research	**Course**	**16**	**4**	***15-19-21-23-27-29/02/2024 ,29/04/2024***	**Prof. Roberto Pietrantuono**	**Y**

Analytic center selection of optimization-based controllers for robot ecology	**Seminar**	**1**	**0.2**	***09/04/2024***	**Prof. Bruno Siciliano**	**Y**
Using Deep Learning Properly",	**Course**	**16**	**4**	***23-25-30/01/2024 01-06-08/02/2024 , 30/06/2024***	**dr. Andrea Apicella,**	**Y**
Resource management and orchestration for mixed-criticality cloud/distributed systems	**Seminar**	**1**	**0.2**	***27/06/2024***	**Prof. Marcello Cinque**	**Y**
Real-time Resource Management for Adaptive Embedded Systems and Applications",	**Seminar**	**1**	**0.2**	***26/06/2024***	**Prof. Marcello Cinque**	**Y**
On the Single Allocation hub location problems: New formulations and Solving Methods	**Seminar**	**1**	**0.2**	***26/06/2024***	**Prof. Maurizio Boccia**	**Y**
IEEE Authorship and Open Access Symposium: Tips and Best Practices to get Published from IEEE Editors	**Seminar**	**1.5**	**0.4**	***07/05/2024***	**ITEE Authorship & Open Access Symposium**	**Y**
Regolamentazione in tema di intelligenza artificiale alla luce dell'AI Act",	**Seminar**	**5**	**1**	***13/05/2024***	**Prof. A.M. Tulino**	**Y**
Generative AI for Software Engineering: Strategies, Impacts and Practical Application"	**Seminar**	**5**	**1**	***29/05/2024***	**Prof. A.M. Tulino**	**Y**

Social Network Analysis Methods and Applications",	**Seminar**	**2**	**0.4**	***07/06/2024***	**Prof. Giancarlo Sperlì**	**Y**
Introduction to Large Language Models Evolution and the current state	**Seminar**	**2**	**0.4**	***10/06/2024***	**Prof. Giancarlo Sperlì**	**Y**
Sustainable IT: Strategies and Best Practices for a Green Engineering Future	**Seminar**	**5**	**1**	***27/05/2024***	**Prof. A.M. Tulino**	**Y**
Machine Deception	**Seminar**	**1**	**0.2**	***23/05/2024***	**Prof. Alessandra Rossi**	**Y**
Innovation and Entrepreneurship	**Course**	**16**	**4**	***12-14-19-21-26/06/2024, 11/07/2024***	**prof. Pierluigi Rippa**	**Y**
Topological Signal processing and Learning	**Seminar**	**1**	**0.2**	***17/07/2024***	**Prof. A.M. Tulino**	**Y**
TA Springer Nature & Care – CRUI: Research Integrity	**Seminar**	**1**	**0.2**	***08/10/2024***	**Elisa Magistrelli- Springer Nature**	**Y**
TA Springer Nature & Care – CRUI: How to Write a scientific paper	**Seminar**	**1**	**0.2**	***07/10/2024***	**Elisa Magistrelli Springer Nature**	**Y**
Author Journey TA Springer Nature & Care - CRUI	**Seminar**	**1**	**0.2**	***09/10/2024***	**Elisa Magistrelli Springer Nature**	**Y**
From ACE Technologies to Sustainable, Accessible and Equitable Urban Mobility: An Optimization Journey	**Seminar**	**2**	**0.4**	***16/09/2024***	***Prof. Stefania Santini***	**Y**
Learning in nonstationary environments	**Seminar**	**2**	**0.4**	***15/10/2024***	**Prof. Carlo Sansone**	**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**	**0.6**	**5.8**	**0**	**6.4**
Bimonth 2	**10**	**1**	**1**	**0**	**12**
Bimonth 3	**8**	**0.2**	**1.8**	**0**	**10**
Bimonth 4	**4**	**5**	**1**	**0**	**10**
Bimonth 5	**4**	**0.2**	**5.8**	**0**	**10**
Bimonth 6	**0**	**1.4**	**10.2**	**0**	**11.6**
Total	**26**	**8.4**	**25.6**	**0**	**60**
Expected	**30 - 70**	**10 - 30**	**80 - 140**	**0 – 4.8**	

3. Research activity:

My research activity centers on advancing deep learning techniques to automate offensive security strategies, focusing on adversary emulation.

Background

In the IT Security landscape, "Advanced Persistent Threats" (APTs) represent the new challenge for organizations' digital assets and data. APT refers to all these scenarios in which an intruder aims to gain access to IT infrastructures and establish a persistent and undetected presence to persecute malicious actions for an extended period (1). Intending to address these new threats, organizations change their approaches from reactive to "proactive security" to anticipate malicious actions before they occur. In this scenario, "Adversary Emulation" becomes one of the best strategies to combat APTs. These strategies aim to emulate the real-world threat actor within a target IT infrastructure, utilizing information gathered from real-world incidents (2). The objective of this undertaking is twofold: firstly, to enhance defensive capabilities and secondly, to improve the efficacy of training programs.

Nevertheless, implementing adversary emulation leads to substantial costs due to the need for specialized personnel to conduct the emulation effectively, which makes it impractical for small/medium enterprises. Therefore, to overcome this limitation, novel techniques based on deep learning approaches may prove beneficial in automating multiple stages of an emulation. In my first year, I addressed two issues:

1. Structuring information about APTs from unstructured CTIs mapping into a standardized format
2. Generate malicious from a natural language description.

Mapping unstructured CTIs in a standardized form

The initial step of Adversary emulation is the information retrieval from the so-called cyber threat intelligence (CTI) (2). These sources are often incident reports written by cybersecurity analysts or leaked documents from attacker groups (3) (4). However, the information in CTIs is often available in an unstructured, bare natural language text.

My contributions to the theme are as follows:

1. The core contribution is the presentation of a deep-leaning-based pipeline for structuring CTIs into an adversary emulation plan, including strategies for pre-processing CTI documents.
2. An evaluation of LLMs at classifying natural language sentences into adversary's tactics
3. An Evaluation of the pipeline concerning complete APT campaigns from authentic CTI documents written by cybersecurity analysts

Our proposal is effective as a recommender system for helping cybersecurity analysts better understand APT behavior and realistically emulate it.

Generate PowerShell attacks from Natural Language.

The second contribution is positioned at the end of the Adversary emulation chain, focusing on the automation of attacks in a post-compromised scenario. In these scenarios, cybersecurity professionals emulate malicious pos-exploitation actions such as credential stealing, lateral movement, and others (5) to gain insight into how attackers may exploit vulnerabilities and to identify strategies for mitigating attacks (1) (6).

Since Windows stands out as one of the most targeted OSs (7), PowerShell has become a pivotal tool for malicious actors and cybersecurity professionals. Furthermore, since writing offensive code demands a high degree of expertise and effort, we put forth the following proposals:

1. The first proposal is the development of multiple AI code generators for PowerShell offensive code.
2. A Methodology to train mainstream programming language models for the PowerShell domain
3. Establish a procedure to assess the efficacy of code generators based on a set of defined criteria. It begins with a comprehensive syntax analysis and culminates in an in-depth examination of the code's performance within a post-compromised emulated environment.
4. The latter proposal is a further comparison with general-purpose state-of-the-art text generators.

The results show the feasibility of using NMT models to generate attacks in PowerShell for security context.

Bibliography

1. *Intelligent, automated red team emulation.* **Applebaum, A., Miller, D., Strom, B., Korban, C., & Wolf, R.** s.l. : Proceedings of the 32nd annual conference on computer security applications, 2016.

2. *Cyber threat intelligence sharing: Survey and research directions.* **TD Wagner, K Mahbub, E Palomar, AE Abdallah.** 2019, Computers & Security.

3. **The Record.** Inside Conti leaks: The Panama Papers of ransomware. *The Record news.* [Online] https://therecord.media/conti-leaks-the-panama-papers-of-ransomware.

4. *Automatic mapping of unstructured cyber threat intelligence: an experimental study:(practical experience report).* **Orbinato, V., Barbaraci, M., Natella, R., & Cotroneo, D.** s.l. : IEEE, 2022.

5. *Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains.* **E. M. Hutchins, M. J. Cloppert, R. M. Amin.** s.l. : Leading Issues in Information Warfare & Security Research, 2011, Vol. 1.

6. *Offensive security: Towards proactive threat hunting via adversary emulation.* **A. B. Ajmal, M. A. Shah, C. Maple, M. N. Asghar, and S. U. Islam.** s.l. : IEEE Access, 2021, Vol. 9 .

7. **B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thoma.** Mitre att&ck: Design and philosophy," in Technical report.

4. Research products:

- *Liguori, P., Marescalco, C., Natella, R., Orbinato, V., & **Pianese, L**. (2024). The Power of Words: Generating PowerShell Attacks from Natural Language. Proceedings of the 18th USENIX WOOT Conference on Offensive Technologies*

5. Conferences and seminars attended

- *ITASEC 2024, Italian Conference on Cyber Security 2024, Salerno Italy 8/04/2024*

6. Activity abroad:

7. Activity in partner companies:

The cooperation lasted from March to July 2024 and from September to October 2024 occurred on site. During this period, several tasks were completed pertaining to the generation of PowerShell attacks in a business context. These included data collection, training and testing.

8. Tutorship