PhD in Information Technology and Electrical Engineering

Università degli Studi di Napoli Federico II

PhD Student: Gaetano Perrone

XXXIV Cycle

Training and Research Activities Report – First Year

Tutor: Simon PietroRomano

Table Of Contents

1. Information

My name is Gaetano Perrone. I obtained Master Degree in Computer Engineering at the University Federico II in July 2017. Actually I am attending PhD in Information Technology and Electrical Engineering without fundings. I am a PhD student that works in Epsilon S.R.L., a Consultant Company with a strong liason with the University and with the research field. My tutor is Professor Simon Pietro Romano. My research is mainly focused on Network Security field. Finally, I am cofounder of SecSI a security startup focused on SECurity Solutions for Innovation.

2. Study and Traning Activities

During my first year of the PhD I have followed different courses aimed at improving my knowledge in securitty and virtualization techniques. I have attended the following courses:

- ***Cloud and Datacenter Networking (Prof. Canonico):*** I have learnt interesting switch virtualization techniques (openvswitch) that I am going to use in order to improve Docker Security Playground (a project that I have developed during my Thesis) networking layer. I have also obtained interesting research ideas to improve the reproducibility of network experiments by using DSP.
- ***Metodi Algebrici per la Crittografia (Prof. Dardano, 06/03/19 – 11/06/19)***: I chose this course to learn mathematical theory under cryptography. I am using acquired knowledge to explore a way to encrypt music by using ECC.

I have attended the folowing modules:

- ***Scale e Scalari (Prof. Dardano***): an exploration among mathematical and musical links.
- ***Advanced Techniques for software robustness and security testing (Natella)***: useful to improve my knowledge in black box fuzzing and symbolic execution techniques
- ***In-Network Machine Learning for Networks (Prof. Bifulco)***: I have improved my knowledge about basic machine learning techniques used in Networking field
- ***Big Data (Prof Picariello and Sperlì):*** an interesting overview of Big Data techniques and tools.
- ***Ciberconflitti (Siroli, Generale Vestito, Prof, Simon Pietro Romano, Daniele Amoroso):*** exploring the current state of cybersecurity world in Italy, an overview of main Incident Response areas in Italy
- ***Data Science and Optimization (Prof. Gaudioso, Prof. Palagi, Prof. Messina):*** an overview of main optimization techniques and some interesting analysis of satte of art papers.
- ***Costruire un business plan e Finanza per le startup (Campania New Steel):*** an interesting introduction to startup world.

I have also attended the MLS School in September 2019, where I have acquired knowledge about robusteness Machine Learning techniques, and interesting information about behaviour analysis of attackers in complex networking systems.

Student: Name Surname
gaetano.perrone@unina.it

Tutor: Name Surname
spromano@unina.it

Cycle XXXIV

	Credits year 1							
	Planned	month 1	month 2	month 3	month 4	month 5	month 6	year
Modules	18	1.4	1.2	6	0.4		9.6	**18.6**
Seminars	13	0	0			0	5	**5**
Research	34	6	6	6	6	5	7.4	**36.4**
	65	7.4	7.2	12	6.4	5	22	**60**

Year	Lecture/Activity	Type	Credits	Certification
1	Cloud and Datacenter Networking	MS Module	3	x
1	MAC	MS Module	6	x
1	Scale e Scalari	Ad Hoc Module	0.6	x
1	MLS School	Doctoral School	5	x
1	Advanced techniques and software robusteness and security testing	MS Module	3	x
1	In-Network Machine Learning for Networks	MS Module	0.4	x
1	Big Data	MS Module	3	x
1	Ciberconflitti	Seminar	0.8	x
1	Data Science and Optimization	MS Module	1.2	x
1	L'accademia delle Startup	MS Module	0.6	x

3. Research Activity

Main area of my research is Network Security. My principal topics are:

- The application of Artificial Intelligence to develop an intelligent agent able to use hacking techniques to detect web application vulnerabilities.
- The application of virtualization techniques to create network security scenarios for educational purposes.

My research is conducted in collaboration with Francesco Caturano. We have created a working group focused on network security field.

The first topic is conducted in collaboration with NTT Data, a security consultant company: they commissioned me a security consulence to create models for web application vulnerabilities. Final goal of the project is the realization of Ch4PT3r, a Collaborative Ethical Hacking Platform for

Penetration Test techniques. Ch4PT3r software aims to automate web application Penetration Test (WAPT). WAPT is a security activity used by companies to detect vunerabilities in web applications. Main modules of Ch4PT3r are:

- A Virtual Security Analyst that uses AI engine to suggest best actions to perform against webserver target
- Hacktuator: the "armed arm", it sends actions against the webserver target and acquires observation from the environment (from the webserver)
- AI Engine: it implements AI models that are useful to make inference about the best actions to do in order to detect web vulnerabilities.

The second topic is the continuation of my thesis project, the realization of a Micro-services based platform to create Network Security Scenarios (Docker Security Playground). Actually we are exploring advanced techniques to improve overlay network, and we are exploring if it is possible to implement features to convert metadata description of an experiment in a virtualized environment to reproduce networking experiments. The project is open source and it is gaining popularity in hacker community (https://github.com/giper45/DockerSecurityPlayground).

4.Product

During my first year of PhD I have explored the research tematic about the application of AI techniques in security test field. Actually we are preparing two main papers regarding:

- The application of Reinforcement Learning techniques to detect SQL Injection vulnerabilities
- The application of Model Markov techniques and Q-learning techniques to detect XSS vulnerabilities

We have realized a paper that explores the Role of Microservices in Security Playground. The paper should be improved (it obtained a Major Revision), our goal is to improve the paper in order expose our contribution in reasearch field and to improve the related work section. Our last goal is the formalization of attack models created during the development of Ch4PT3r.