UNIVERSITÀ DEGLI STUDI DI NAPOLI
FEDERICO II

itee PhD
information technology
electrical engineering

DIETI. UNINA

Nicola d'Ambrosio

Attack-defense strategies in challenging cybersecurity environments

Tutor: Simon Pietro Romano

Cycle: XXXVII Year: First

itee PhD
information technology
electrical engineering

My background

- MSc degree: Computer Engineering
- First Year PhD: Academic Year 2021-2022
- PhD start date: 1/1/2022
- Laboratory: SecSI (Security Solutions for Innovation)
- Scholarship type: PON Dottorati di ricerca su tematiche dell'innovazione e green - Azione IV.4 (Innovazione)

Summary of study activities

	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

Research field of interest

- Proactive strategies that work beyond traditional detect-then-prevent techniques and block malicious activities in the early stages of a cyber attack
- Cybersecurity for Critical Infrastructure Control Systems
- Introducing insider threats into standard risk management frameworks

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

- Cyber range
  - interactive, virtual representations of networks, systems, tools, and applications that enable users to acquire new cybersecurity skills
- The development and maintenance of a cyber range can become cumbersome:
  - It requires an isolated system in which to inject the vulnerability
  - The configuration of vulnerable applications is often done manually and requires a lot of time and effort
- The main goal is to simplify the vulnerable scenario creation so that it requires minimal user effort
- ***ExploitDB2Docker:***
  - a container-based architecture to automate the generation of vulnerable CMS platforms
    - obtains vulnerability information from ExploitDB
    - finds a Docker image that satisfies the exploit preconditions...
    - ...then, it installs necessary components such as plugins and themes to reproduce the vulnerability

Products

[P1]	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), 2022, pp. 1-7, doi: 10.1109/ICECET55527.2022.9872859.

Including Insider Threats into Risk Management through Bayesian Threat Graph Networks

- Cyber risk management:
  - the process of identifying, assessing, and controlling threats to an organization's information and systems
  - goal is to minimize the negative impact of these risks on an organization and to maximize the security of its information and systems
  - its application to address insider threats is relatively unexplored
- Our work widens the research scope to include insider threats in risk management processes
- We design a network security risk management framework based on Bayesian Decision Networks that allows the selection of the best security controls' combination under budget constraints

SCASS: a hybrid Industrial Testbed (1/2)

- An ICS (Industrial Control System) 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
- SCASS (SCAda Systems Security):
  - a hybrid and modular testbed*
  - the hybrid nature of our testbed lets us obtain a scalable and maintainable environment
  - the outcome of this research activity represents a strong foundation for our upcoming research

*Inspired by state-of-the-art work like Kandasamy et al. [1], who propose a physical micro-grid testbed called EPICTWIN

SCASS: a hybrid Industrial Testbed (2/2)

- The 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 strike an optimal balance between security and safety in industrial environments;
  - to validate cyber security risk and safety assessment methodologies.