# Προτεινόμενα Θέματα Μεταπτυχιακών Διατριβών – Αν. Καθ. Παναγιώτης Κοτζανικολάου
## Ακαδημαϊκό έτος 2023-24

### (1) Cyber Range Development:Environment-Networking-Monitoring Setup

**Description:** The proposed thesis project involves setting up a comprehensive corporate cyber range that will incorporate a variety of components. Specifically, the cyber range will consist of a Windows AD environment, Linux virtual machines, and a Linux server, as well as a small-scale implementation of an IoT environment in the healthcare, maritime, or energy sector. To ensure the security of the infrastructure, the student will need to split it into multiple zones using networking and implement different firewall rulesets to create distinct security layers. Additionally, the student will need to introduce vulnerabilities in specific components of the infrastructure to demonstrate the effectiveness of monitoring and defense solutions. To monitor the traffic and logging activities on the network, the student will be required to install an open source Intrusion Detection System (IDS) such as Snort or Suricata agent at different layers of the infrastructure. This will enable the student to monitor for different types of threats that may be targeted towards specific components. The successful completion of this thesis project will require the student to have a deep understanding of cybersecurity principles and knowledge of networking and operating systems. The project's expected outcome will be a comprehensive report detailing the setup, configuration, and implementation of the cyber range infrastructure. The report will also include a detailed analysis of the vulnerabilities identified, the effectiveness of the monitoring and defense solutions deployed, and recommendations for improving the security posture of the infrastructure.

**Dependencies:**
- The rules should be related to the botnet capabilities.
- The framework should be compatible with the Front End-XDR project (IDS capabilities to communicate with the ELK stack)
- The project has to mitigate at least one threat from almost every layer (OSI)

**Final Requirements (Equipment will be provided by UPRC):**

- Windows VMs/AD
- Linux machines + or server
- IoT example (Raspberry pi's)
- Networking

**References:**
https://github.com/Orange-Cyberdefense/GOAD
https://github.com/splunk/attack_range
https://attack-range.readthedocs.io/en/latest/Attack_Range_Local.html
https://detectionlab.network/
https://www.hindawi.com/journals/jece/2022/3073932/
https://www.mdpi.com/2076-3417/11/12/5713

**Contact point:** Christos Grigoriadis <adventchris2@gmail.com>

## (2) Traffic Generation Botnet

**Description:** In this thesis project, the student will be tasked with developing and testing traffic generators for the various components and networks within a corporate infrastructure. The infrastructure will include an Active Directory server with a few Windows machines, a few Linux desktops, one Linux server, and a smart office IoT environment, which was developed in a previous thesis project.

The student will need to develop traffic generators that can produce both legitimate and malicious traffic to test the security of the infrastructure. The legitimate traffic generators will aim to replicate the typical traffic patterns observed in the different components and networks of the infrastructure. The malicious traffic generators, on the other hand, will aim to simulate different types of attacks, such as DDoS, malware, and phishing attacks.

To ensure the effectiveness of the traffic generators, the student will need to conduct extensive testing and analysis of the generated traffic. The student will also be required to evaluate the performance of different network and security monitoring solutions in detecting and mitigating the generated traffic.

The student will need to develop a comprehensive methodology for testing the traffic generators on the infrastructure. This will include identifying the different types of traffic generators required for each component and network, determining the metrics for evaluating the effectiveness of the traffic generators, and outlining the procedures for testing and analyzing the generated traffic.

The successful completion of this thesis project will require the student to have a strong understanding of network protocols, traffic patterns, and attack vectors. Additionally, the student will need to possess skills in programming and experience in using network and security monitoring tools. The project's expected outcome will be a detailed report outlining the methodology, results, and recommendations for improving the security posture of the infrastructure based on the testing and analysis conducted using the developed traffic generators.

**Final Requirements**

- AD Services legitimate/malicious Traffic Generator (eg SMB)
- Ubuntu server legitimate/malicious Traffic Generator
- IoT Traffic Generator

**References:**

https://www.enisa.europa.eu/topics/incident-response/glossary/botnets
https://github.com/topics/botnet-tools
https://github.com/netzob/netzob
https://conf.splunk.com/files/2019/slides/SEC1375.pdf

**Contact point:** Christos Grigoriadis <adventchris2@gmail.com>

### (3) Front End-XDR Development

**Description:** In this thesis project, the student will be tasked with developing and testing a custom Extended Detection and Response (XDR) system utilizing a cybersecurity ontology and threat and vulnerability databases developed by the research lab. The XDR system will be based on the ELK stack and will be similar to existing solutions such as Wazuh. The student will need to utilize known Intrusion Detection System (IDS) solutions and the threat and vulnerability databases to create a system that can correlate logs and alerts to specific threats. The XDR system will need to be designed to work with different types of data sources, including network logs, endpoint logs, and IoT device logs.

To ensure the effectiveness of the XDR system, the student will need to conduct extensive testing and analysis of the system's ability to detect and respond to different types of threats. Specifically, the XDR system will be tested on the traffic, logs, and alerts created by the corporate cyber range infrastructure and traffic generator developed in the previous thesis projects.

The student will need to develop a comprehensive methodology for testing the XDR system. This will include identifying the different types of threat and vulnerability data sources required for the system, determining the metrics for evaluating the system's effectiveness in detecting and mitigating the generated traffic and alerts, and outlining the procedures for testing and analyzing the system's performance.

The successful completion of this thesis project will require the student to have a strong understanding of network protocols, traffic patterns, and attack vectors. Additionally, the student will need to possess skills in programming and experience in using network and security monitoring tools. The project's expected outcome will be a detailed report outlining the methodology, results, and recommendations for improving the security posture of the infrastructure based on the testing and analysis conducted using the custom XDR system.

**Final Requirements :**

- Front End project-github repo (ideally dockerized)
- Communication & Authentication with database API
- ELK implementation
- Testing on developed environment from the Environment-Networking-Monitoring Setup

**References:**

https://wazuh.com/
https://link.springer.com/chapter/10.1007/978-3-030-95484-0_2
https://www.elastic.co/what-is/elk-stack
https://www.paloaltonetworks.com/cortex/cortex-xdr
(https://www.elastic.co/blog/performing-real-user-monitoring-rum-with-elastic-apm)

**Contact point:** Christos Grigoriadis <adventchris2@gmail.com>

**(4) θεωρητική και πειραματική μελέτη ασφάλειας πρωτοκόλλων επικοινωνίας για περιβάλλον IoT (MQTT, COAP, HTTP/2, HTTP/3, XMPP)**

**Θεωρητικό μέρος**

1. Ανάλυση λειτουργίας των πρωτοκόλλων
2. Ανάλυση αρχιτεκτονικής του κάθε πρωτοκόλλου
3. Σύγκριση των πρωτοκόλλων με βάση επιχειρησιακά (π.χ. πεδίο εφαρμογής) και τεχνικά κριτήρια (π.χ. απόδοση, κατανάλωση, ασφάλεια κτλ).

**Πρακτικό μέρος**

1. Δημιουργία HTTP3 client server σύνδεσης (python)
2. Δημιουργία MQTT client server σύνδεσης (python)
3. Δημιουργία CoAP client server σύνδεσης (python)
4. Σύγκριση των συνδέσεων σε επίπεδο ασφάλειας (ως προς το επίπεδο ακεραιότητας, διαθεσιμότητας, εμπιστευτικότητας)
5. Πλεονεκτήματα και μειονεκτήματα σε επίπεδο λειτουργιών

Λέξεις-κλειδιά: Python, client server implementation with CoAP-MQTT-HTTP3

**Χρήσιμες πηγές**

[01] https://github.com/diekmann/Iptables_Semantics
[02] https://towardsdatascience.com/python-text-analysis-with-the-schrutepy-package-234bc70f3916
[03] https://www.nltk.org/
[04] https://textblob.readthedocs.io/en/dev/
[05] https://spacy.io/
[06] https://numpy.org/
[07] https://matplotlib.org/stable/tutorials/introductory/pyplot.html
[08] https://bokeh.org/
[09] https://pypi.org/project/gensim/
[10] Marmorstein, R., & Kearns, P. (2005). A tool for automated iptables firewall analysis. USENIX 2005 Annual Technical Conference, 71–81.
[11] Diekmann, C., Hupel, L., Michaelis, J., Haslbeck, M., & Carle, G. (2018). Verified iptables Firewall Analysis and Verification. Journal of Automated Reasoning, 61(1-4), 191–242.
[12] Al-Shaer, E., & Hamed, H. (2004). Modeling and Management of Firewall Policies. IEEE Transactions on Network and Service Management, 1(1), 2-10.
[13] Golnabi, K., Min, R., Khan, L., & Al-Shaer, E. (2006). Analysis of Firewall Policy Rules Using Data Mining Techniques. In 2006 IEEE/IFIP Network Operations and Management Symposium NOMS 2006 (pp. 305-315).
[14] Al-Shaer, E. (2014). Automated Firewall Analytics.
[15] Katic, T., & Pale, P. (2007). Optimization of Firewall Rules. In 2007 29th International Conference on Information Technology Interfaces (pp. 685-690).
[16] Shanbhag, S., & Wolf, T. (2011). Automated composition of data-path functionality in the future internet. IEEE Network, 25(6), 8-14.
[17] El-Atawy, A., Samak, T., Wali, Z., Al-Shaer, E., Lin, F., Pham, C., & Li, S. (2007). An Automated Framework for Validating Firewall Policy Enforcement. In Eighth IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'07) (pp. 151-160).
[18] Khelf, R., & Ghoualmi-Zine, N. (2018). IPsec/Firewall Security Policy Analysis: A Survey. In 2018 International Conference on Signal, Image, Vision and their Applications (SIVA) (pp. 1-7).

**Επικοινωνία:** Δημήτρης Κούτρας <dkoutras@unipi.gr>

**(5) Σχεδιασμός, υλοποίηση και δοκιμή τεχνικών μηχανικής μάθησης για την ανίχνευση επιθέσεων σε πρωτόκολλα επικοινωνίας επιπέδου δικτύου και επιπέδου εφαρμογής**

Σε αυτή την εργασία θα γίνει ανάλυση και ανίχνευση επιθέσεων σε συγκεκριμένα πρωτόκολλα επικοινωνίας για το επίπεδο δικτύου και το επίπεδο εφαρμογής του OSI (η επιλογή των υπό μελέτη πρωτοκόλλων επικοινωνίας θα γίνει σε συνεργασία με το φοιτητή).

1. Καταγραφή των γνωστών επιθέσεων ασφάλειας των υπό μελέτη πρωτοκόλλων επικοινωνίας.
2. Εκτέλεση των επιθέσεων σε εργαστηριακό/εικονικό περιβάλλον και μη ανίχνευσή τους με μη αυτοματοποιημένες μεθόδους.
3. Δημιουργία σχετικού dataset
4. Εκπαίδευση, δοκιμή και σύγκριση μοντέλου ML – AI για την αυτοματοποιημένη ανίχνευση αυτών με την χρήση νέου ή έτοιμου dataset.

**Βοηθητική βιβλιογραφία και αναλυτικό πλάνο θα δοθεί μετά την πρώτη επικοινωνία με τον φοιτητή.*

**Επικοινωνία:** Δημήτρης Κούτρας <dkoutras@unipi.gr>

**(6) Risk Assessment roadmap in critical infrastructures**

**Description:** This thesis will explore the current status and future research and practice roadmap of risk assessment methodologies for Critical Infrastructures. The analysis will cover the theoreticas a aspect with a practical case study on a specific infrastructure. In particular the thesis will include:

1. Proactive Cyber Defense (risk assessment/gap assessment/ draft incident response plan)
2. Active Cyber Defense Cycle (Threat Intelligence, Visibility, Threat Detection, Incident Response, Threat & Environment Manipulation)
3. State of the Practice
4. State of the Art
5. Case Study - Attacks/Lessons Learned
6. Conclusion - Future research

**Contact point:** Dr. Ioannis Stellios <jstellios@unipi.gr>

**(7) Ανάπτυξη κατανεμημένου συστήματος διαχείρισης δεδομένων σε φυσικό δίκτυο με χρήση raspberry pi's και τεχνολογιών Blockchain, (υποδομή αντίστοιχη με το Inter-Planetary File System - IPFS).**

Στην παρούσα εργασία θα γίνει μια σύντομη επισκόπηση της διεθνούς βιβλιογραφίας σχετικά με κατανεμημένα συστήματα δεδομένων και θα αναπτυχθεί μια υποδομή σε Raspberry pi - model 4.

**Προαπαιτούμενες γνώσεις:**
Blockchain (Ethereum or Hyperledger), Programming skills (Solidity or Go – similar to javascript), Dockers

**Πηγές**

(1)_x0001_Nizamuddin, Nishara, et al. "Decentralized document version control using ethereum blockchain and IPFS." Computers & Electrical Engineering 76 (2019): 183-197.
(2)_x0001_Vimal, S., and S. K. Srivatsa. "A new cluster p2p file sharing system based on ipfs and blockchain technology." Journal of Ambient Intelligence and Humanized Computing (2019): 1-7.
(3)_x0001_Kumar, Randhir, and Rakesh Tripathi. "Implementation of Distributed File Storage and Access Framework using IPFS and Blockchain." 2019 Fifth International Conference on Image Information Processing (ICIIP). IEEE, 2019.

**Επικοινωνία:** Βαγγέλης Μάλαμας <bagmalamas@unipi.gr>