

Portofolio

Cyber Security Semester 4



June 18, 2023

Vasile mihai glodici

Fontys University of Applied Sciences

# Version Control Table:

|  |  |  |
| --- | --- | --- |
| Version | Date | Changes/Additions |
| 0.1 | 22/05/2023 | First Version |
| 0.2 | 18/06/2023 | Integrated feedback:  *Improved PVI time allocation evidence Report writing in group projects integration (Network Infiltratration, LAN Scanning, Secure Solution and Pentest, spellchecking documents etc.)*  *Integrated Penetration Test learning outcomes (Network infiltration, Enumeration, LAN CVE scanning)*  *Secure Solution contribution (designing network routes and segmentation, diagram, HIDS, PfSense network interface troubleshooting)*  *Attached network infiltration video to pen test hand-in Lowered my self-grade* |

Contents

[Version Control Table: 1](#_Toc138009488)

[1) Introduction: 2](#_Toc138009489)

[2) Learning Outcomes: 2](#_Toc138009490)

[3) Personal Projects 9](#_Toc138009491)

[4) Overall Conclusion and Reflection: 11](#_Toc138009492)

# Introduction:

**What was your relevant prior knowledge and experience on security, Linux and networking or what did you do to obtain this knowledge?** Before starting my journey in cybersecurity, I had a foundational understanding of computer networks, operating systems, and basic security principles. My knowledge in Linux was primarily from my previous Infrastructure Semesters, supplemented by online resources and tutorials. I familiarized myself with various Linux distributions, command-line interfaces, and shell scripting. My understanding of networking was gained through coursework and practical experiments with network configurations, protocols, and hardware.

**What was your preferred learning style. Why?** My preferred learning style is a blend of theoretical and practical learning. Cybersecurity, like many technical subjects, is best understood via practice. This method helps me understand the fundamentals and apply them to real-world situations. I also tend to grasp concepts more quickly when all the styles are combined in an interactive presentation, followed by hands-on exercises, homework, and individual research.

**What motivated you to join cyber security?** The ever-evolving landscape of cybersecurity intrigued me. The constant innovation, the intellectual challenge, and the opportunity to make a real difference in protecting information and systems motivated me to join this field. Moreover, the increasing demand for cybersecurity professionals across all sectors presented a promising career path.

**What are your strengths and weaknesses? My analytical thought process is one of my fundamental abilities.** I am good at recognizing patterns and answers and enjoy fixing problems. This trait is especially valuable in cybersecurity, where threat analysis and mitigation need a high level of analytical reasoning. Perseverance, attention to detail, and a great drive to learn are also among my other talents.

Time management is one of my weaknesses, particularly when juggling many activities or projects. However, I'm actively working on improving this by using various time management strategies and tools.

Based on my strengths and shortcomings, my personal growth objectives include refining my time management abilities, continuing to increase my cybersecurity knowledge, and acquiring more hands-on experience in the industry. I also intend to improve my problem-solving abilities and apply them to increasingly difficult cybersecurity situations.

2) Learning Outcomes:  
Learning Outcome - Ethical Hacker:

As an Ethical Hacker, I have gained a comprehensive understanding of computer systems, networks, and programming to identify system and network vulnerabilities. I have simulated attacks that could be carried out by hostile hackers using a range of techniques, tools, and methodologies. Some of the most prominent methods I have employed include penetration testing, vulnerability scanning, and social engineering.

Penetration testing involves attempting to break a system's defenses to identify weaknesses (SQLi, XSS & CSRF, Path Traversal, (remote) File inclusion and Command Injection) whereas vulnerability scanning involves automated technologies (Sqlmap, Nmap) to scan systems for known vulnerabilities. Social engineering was used to create Rogue Access Points and phishing mails, it is also known as the use of human psychology to manipulate individuals into disclosing sensitive information or performing acts that could jeopardize system security.

I have worked with the WinIT organization to uncover potential flaws, and then reported my findings back to the organization so that the vulnerabilities can be fixed. In addition to possessing technological expertise, I have a solid grasp of ethics and professional responsibility. I have been lawful, ethical, transparent, and have not damaged the organization or its systems.

I have also gained practical experience in monitoring/cracking wireless networks, capturing handshakes and PMKIDs, and cracking keys using tools like aireplay and aircrack. Additionally, I have explored the use of Evil Twin attacks and captive portals to collect user credentials in plain text, bypassing the need to decrypt hashes.

Furthermore, I have learned about mitigating wireless attacks, with a focus on detecting rogue access points, increasing user awareness, and implementing robust security measures. By employing strategies such as deploying wireless honeypots, conducting security audits, and developing comprehensive security awareness programs, organizations can better defend their networks against wireless threats.

Lastly, Conducting Footprinting and Reconnaissance made me understand the value of keeping data more secure and how leaked information can be detrimental to security. Every attack starts on these steps.

My experience with tools like Airgeddon has given me practical insights into real-world Man in the Middle and WiFi attack scenarios, strengthening my ability to protect critical digital assets.

questions for the LO-Area Ethical Hacker:

1. **How did you obtain Body of Knowledge about the involved subjects?** I obtained the Body of Knowledge through Basic and Advanced hands-on exercises, examining course slides and the internet (sources in the BoK) to better understanding the scope of cybercrime.

The following exercises were done by me:

* Basic Hacking and Pentesting
* Threat + Risk Analysis
* Footprinting, Reconnaissance and Social Engineering Basic Exercises
* Path Traversal, (remote) File inclusion and Command Injection Basic + Advanced exercises
* Web Application Firewalls Basic exercise
* SQL Injection Basic and Some Advanced
* HIDS Basic
* Network Scanning and Enumeration Basic and Advanced
* Secure Network Connections (HTTPS/TLS/SSH) Basic exercises
* Law, Ethics and Responsible Disclosure Basic exercises
* Network Separation and Segmentation (Firewalls)(Basic)
* VPN: How to manage a Web Shop with Secure Remote Access and Management by VPN Basic
* Network Spoofing and Man in The Middle Attacks (MITM) Basic & Advanced
* WiFi Hacking Basic & Advanced
* Network Intrusion Detection and Prevention (NIDS/IPS) Basic
* IT Basic Monitoring (availability) + IT Security Monitoring (integrity and confidentiality)
* Identity Management, Authentication and Access Control
* Basic & Advanced
* Password Cracking (system and network) Basic and continued to Advanced for my PSP
* Security Incident Management Basic
* IT System Hardening + Common Vulnerabilities and Exposures (CVE's) Basic
* SIEM tooling (and Blue Teaming) Basic

1. **How did you apply your skills in the project?** I applied my skills in the group project by conducting penetration testing, vulnerability scanning, and social engineering. I also used tools like aireplay, aircrack, and Airgeddon to simulate real-world attack scenarios.  
   My work is best described in the pentest-report paper, however I will briefly describe my contributions which fit in the Ethical Hacking area. Initially, I evaluated the security of WPS with null and known database PIN attacks utilizing Reaver and Bully. Then, I attempted an "all-in-one" attack on the WEP protocol. Next, I created a fake AP that successfully grabbed the company's password. With my AP and after acquiring network access, I attempted Man in the Middle sniffing and hooking. Using Hashcat and John the Ripper, I successfully cracked the WPA2 handshake and PMKID hashes by combining my own targeted wordlists with rules. My PSP contains a guide for password cracking, and my PVI contains a guide for network testing. I will also share a video demonstrating my procedure at the company.
2. **What have you learned considering this Learning Outcome?** I have learned the importance of ethical hacking in identifying and mitigating security threats. I also gained knowledge of various offensive strategies and how to defend against them.
3. **What are you proud of?** I am proud of my ability to understand and apply various hacking techniques ethically. I am also proud of my understanding of different tools and methodologies used in ethical hacking. Understanding how networks might be infiltrated and how password hashes are susceptible to cracking enables me to acknowledge the need for strong administration rules and the utilization of the most recent WiFi technologies such as WPA3. In addition, I am confident in my abilities to educate colleagues about the dangers of weak passwords, fake access points, and credential leakage on illicit marketplaces. Lastly, I've incorporated the information I've learned into my own environment and password lists, making me feel more protected against attacks.
4. **Which aspects do you want to develop further**? I'd want to develop my skills in advanced penetration test methods and have a deeper understanding of impending threats and how to defend against them.
5. **What will you do differently next time?** I'll focus more on recent cybersecurity threat developments and countermeasures next time. I will also attempt to code my own scripts for automating the process of testing.
6. **What grade would you give yourself on the corresponding Learning Outcome?** Based on my ability to grasp and apply of the knowledge, I would give myself an G for the Ethical Hacker Learning Outcome.

Learning Outcome - Risk Consultant:

As a Risk Consultant, I have analyzed security threats and resulting business risks according to a common risk analysis method. I have advised a real client on security improvements of an IT environment on a physical, technical, and organizational level.

I have gained a deeper understanding of how web applications work, which has enabled me to inspect page source code. This understanding has allowed me to better protect systems against attacks by identifying vulnerabilities in web applications. By inspecting the code, I was able to determine how the Website's input validation and sanitization are configured. This allowed me to execute SQL injections against the DVWA at all security levels.   
My step-by-step procedure is described in the BoK with screenshots and explanations of how to locate input blacklists and my workaround. Finally, I discovered how to better defend Web Applications by installing Firewalls, implementing input blacklists to prevent SQLi and XSS, and separating the internet-facing services in a Demilitarized (DMZ) subnet.

Furthermore, I have learned the importance of having efficient and reliable tools at my disposal, such as John the Ripper, and the value of using comprehensive password lists like rockyou.txt for cracking hashes. This knowledge has helped me assess the strength of password policies and recommend improvements to enhance security.

Lastly, I have recognized the limitations of hardware resources when conducting brute force attacks. In the future, I will need to be mindful of allocating sufficient resources or leveraging specialized hardware like GPUs to improve the efficiency.

questions for the LO-Area Risk Consultant:

1. **How did you obtain Body of Knowledge about the involved subjects?** I obtained the Body of Knowledge through studying high-risk vulnerabilities, examining responsible disclosure policies of organizations, conducting Threat and Risk Analysis with some sources of my previous Infrastructure Semesters and consulting course slides and the internet (sources in BoK).
2. **How did you apply your skills in the project?** I applied my skills in the secure-solution project by conducting risk analysis, advising and implementing security improvements such as HIDS, Network security planning by devising subnets, creating Firewall rules and a Network diagram, Encryption, VPN, running scans within and outside our network, troubleshooting pfSense network adapters, writing documentation of my implementation and proofreading my team's work.  
    In the pen-testing project, I have executed and documented my attacks, as well as made recommendations to enhance mitigation. There is additional information in the Ethical Hacking Learning Outcome, my BoK, PVI, and PSP.
3. **What have you learned considering this Learning Outcome?** I have learned the importance of risk analysis in identifying and mitigating security threats. I have also learned about various attack techniques and how to use different tools to protect against these threats. Lastly, learned to treat data with confidentiality and understand the importance of the Privacy, Confidentiality, Integrity, and Availability (CIA) classification system.
4. **What are you proud of?** I am proud of my ability to understand and apply various risk analysis techniques both theoretically and practically.
5. **Which aspects do you want to develop further?** I would like to further develop my skills in advanced risk analysis techniques and learn more about emerging threats and how to mitigate them.
6. **What will you do differently next time?** Next time, I will place greater effort into providing industry standard mitigation and handling strategies of cyber threats, while also experimenting more with tools like Metasploit and advanced password lists with rules.
7. **What grade would you give yourself on the corresponding Learning Outcome?** Considering my understanding and application of the skills, I would give myself an G for the Learning Outcome of Risk Consultant.

Learning Outcome, Security Engineer & Security Analyst:As a Security Engineer, I've learned to realize a secure IT infrastructure environment, considering functional requirements as well as the following non-functional requirements: security, monitoring, ethics, compliance, usability. I've gained hands-on experience in building a HIDS solution and learned how to install and configure Wazuh on an Ubuntu machine, thereby increasing my ability to deploy security monitoring tools. Configured a VPN connection, installed a Web Application Firewall, IDS/IPS attached Firewalls, created self-signed certificates for encryption, segmented my network and much more Basic and Advanced Exercises described in the Bok.

As a Security Analyst, I've learned to realize procedural response for security incidents and analyse these in an efficient and methodical way. I've understood the importance of security incident management in enterprises to mitigate business disruptions. This involves technological, management, and legal responses and continual security assessment and improvement. I have also conducted Wireshark sniffing to assess the confidentiality of my network’s data.

1. **How did you obtain Body of Knowledge about the involved subjects?** I obtained the Body of Knowledge through a combination of theoretical learning and practical exercises. I studied the principles of network security and incident response, and then applied these principles in hands-on exercises. My favourite subjects were network intrusion detection and prevention.
2. **How did you apply your skills in the project?** I applied my skills in the project by designing and implementing a secure IT infrastructure environment in vSphere for personal use, the project and at home. This involved considering functional requirements as well as non-functional requirements such as security, monitoring, ethics, compliance, and usability. Created a network Diagram and designed the environment and worked on Documentation as well.
3. **What have you learned considering this Learning Outcome?** I've learned the importance of designing and implementing secure IT infrastructure business environment. I've also learned to react to security issues in a fast and professional way. The biggest takeaway for me has been the refresher of deploying more secure networks by utilizing new and old tools from previous semesters.
4. **What are you proud of?** I am pleased with my abilities to deploy a safer IT infrastructure environment at home and in VSphere that may satisfy both functional and non-functional objectives (content feedback would greatly be appreciated). I'm also pleased with my knowledge of the incident response procedure, which I've detailed in my BoK. My testing of a safer IT environment concluded with nmap scanning, vulnerability scanning, troubleshooting, and network route configuration. Considering these observations, I look forward to my classmates potentially compromising my infrastructure as part of a class exercise at the end of the semester so that I may hopefully learn how to improve my security measures.
5. **Which aspects do you want to develop further?** I would like to further develop my skills in advanced network security techniques by creating my custom monitoring rules and grading my security incidents based on severity more often to allow prioritizing of events.
6. **What will you do differently next time?** I would like to further explore activities that would fit into the role of a Security Analyst, like analyzing and grading logs of my SoCs, while also improving my Engineering skills by deploying more custom rule monitoring secured environments.
7. **What grade would you give yourself on the corresponding Learning Outcome?** Based on my understanding and application of the concepts, I would give myself a grade of G for Learning Outcome 3 and 4.

Learning Outcome - Security Professional:

As a Security Professional, I've learned the importance of ethical hacking and risk analysis. I've understood the importance of being lawful, ethical, transparent, and not damaging the organization or its systems. I've also learned about the Cyber Kill Chain, a model that explains the various phases an attacker takes to successfully penetrate a target network or system.

**How did you obtain Body of Knowledge about the involved subjects?** I obtained the Body of Knowledge through a combination of theoretical learning and practical exercises. I studied the principles of cybersecurity and professional development from the course slides and external resources (links in BoK), and then applied these principles in hands-on exercises. My favourite subjects were cybercrime investigations and vulnerability management.

1. **How did you apply your skills in the project?** I applied my skills in the pen test and secure solution projects by demonstrating my professional development as a cybersecurity student. This involved performing IT tasks in which both the process and the results were visible. The process and results have been documented in my PSP, PVI, group documents, BoK and videos. These tasks included writing documentation, meeting deadlines, visiting and conducting a pen test and secure solutions after documented agreements, keeping in touch with groupmate’s progress and offering help, conducting presentations both at school and at the company I have signed documents with.
2. **What have you learned considering this Learning Outcome?** In the field of cybersecurity, I've realized how critical it is to maintain a high level of ongoing professional development. In comparison to prior semesters, my process and result reporting skills have improved, and this trend will continue as I spend more time developing documentation.
3. **What are you proud of?** I'm proud of my ability to demonstrate my professional development through authentic IT professional documented tasks. I'm also proud of my understanding of the Cyber Kill Chain and how it can be used to protect against cyber attacks.
4. **Which aspects do you want to develop further? I wish to further expand my professional skills by completing projects for actual companies. This method will teach me how to enhance my research and documentation skills. Lastly, I intend to conduct security evaluations in an ethical and non-destructive manner (there have been times where I caused some issues like DoS, using up too much hardware resources or insecurely opening ports due to inexperience).**
5. **What will you do differently next time?** Next time, I'd like to delve deeper into the processes of the Kill chain, even engaging in Red Teaming with a higher level of complexity to see just how far social engineering, malware deployment, and data exfiltration may go.
6. **What grade would you give yourself on the corresponding Learning Outcome?** Based on my understanding and application of the concepts, I would give myself a grade A for this Learning Outcome.

# 3) Personal Projects

How did you spend your hours for:

**1.Personal Vulnerability Investigation (expected about 5x4h = 20 hours)**

Time Allocation:

Initial Research, tool testing, vulnerability analysis, and report writing needed a total of 24 hours for this research report. The allocation of time is as follows:

**Initial Investigation of PVI Choice:** 3 hours

* Watching various WiFi cracking tutorials and using course work as beginning.

**Tool testing and vulnerability analysis:** 9 hours

* My initial attempt to deploy my AP using the Fluxion script was unsuccessful. I went to school to replace my Wifi card and received two new ones (extra one for tracking APs that change channels).
* Switched and got used to the Airgeddon framework and deployed my 2.4Ghz AP.   
  Spent time attempting to deploy and attack 5Ghz networks, however the ISSD sticks did not support it.
* Tested all vulnerabilities from the framework on various hardware (Android, iOS, Ubuntu, Windows).
* Explored WEP, WPS vulnerabilities briefly as preparation for my test cases in the Pentest.
* Prepared video Demo and explained the steps in my documentation.

**Troubleshooting:** 5 hours  
  
VirtualBox was initially utilized but was later replaced with VMWare because my Wi-Fi USBs were not being detected/cloned reliably.

Unrecognized Wi-Fi sticks are solved by plugging them in after machine startup and driver update.

Because the previous script's use of "Fluxion" rendered the hardware unidentifiable, snapshots were utilized to return to previously functioning system states.

5Ghz AP attempts and WPA3 were unsuccessful.

**Report writing & Powerpoint**: 7 hours:

* Initial PVI proposition created and talked about with my coach. It was not however uploaded to early enough.
* Library research*,* Field research, Lab research explored further and added to the PVI document.  
  Powerpoint and Live Interactive Demo with the whole class prepared.

**2.Internship Preparation (expected about 10 hours)**

Participated in the Career Day and scheduled three individual appointments with organizations.  
 I received interest and invitations to meet with recruiters, which I will do after completing all my coursework.   
This took approximately six hours, and I will utilize the remaining time to update my resume, reach out to my contacts, and apply to further companies.

**3.Personal Specialisation Project (expected about 10x4h = 40 hours)**

Time allocation:

* Problem definition and goal clarification: 2 hours
* Literature review and answering of sub-questions + PPT Presentation: 8 hours
* Setting up the tools (John the Ripper, Hashcat, Google Colab, Tor66, Pipal, Cewl, ChatGPT, Hash-Identifier, and CUPP): 5 hours
* Initial password cracking tests and learning the ropes: 5 hours
* Extensive testing of rules and munging techniques for password cracking: 5 hours
* Analysis of current password creation and protection methods: 3 hours
* Understanding and using cloud resources and AI for improved efficiency: 3 hours
* Investigating and understanding hash salting and its cracks: 2 hours
* Creating and executing a targeted list crack: 3 hours
* Compiling results in documents, dealing with errors, and proposing solutions: 6 hours  
    
  Total: 42 hours

# 4) Overall Conclusion and Reflection:

My path in the field of cybersecurity has been both demanding and rewarding. With a solid grasp of computer networks, operating systems, and fundamental security principles, I began on my adventure with a great interest in the ever-changing cybersecurity scene. Throughout this journey, my analytical thinking, persistence, attention to detail, and strong drive to learn have been my greatest qualities. However, I recognized time management as a weakness and set a personal development goal to improve it.

My learning approach, a combination of academic and practical learning, has enhanced my comprehension of cybersecurity significantly. The use of theoretical knowledge has enabled me to comprehend the fundamental ideas and their application to real-world scenarios.

As an Ethical Hacker, I have studied computer systems, networks, and programming to detect system and network vulnerabilities. I've simulated attacks, conducted penetration testing, vulnerability scanning, and social engineering. I've also gained practical experience in monitoring/cracking wireless networks, capturing handshakes and PMKIDs, and cracking hashes with customized lists.

As a Risk Consultant, I've analyzed security threats and resulting business risks according to a common risk analysis method. I've advised a real client on security improvements of an IT environment on a physical, technical, and organizational level.

As a Security Engineer, I've learned to realize a secure IT infrastructure environment, considering functional requirements as well as the following non-functional requirements: security, monitoring, ethics, compliance, usability. As a Security Analyst, I've learned to realize procedural response for security incidents and analyze these in an efficient and methodical way.

As a Security Professional, I've learned the importance of ethical hacking and risk analysis. I've understood the importance of being lawful, ethical, transparent, and not damaging the organization or its systems. Lastly, I have greatly improved my document writing and tracking of my progress and work.

In conclusion, my journey in cybersecurity has been a continuous learning process. I've learned to identify my strengths and weaknesses and set personal development goals accordingly.