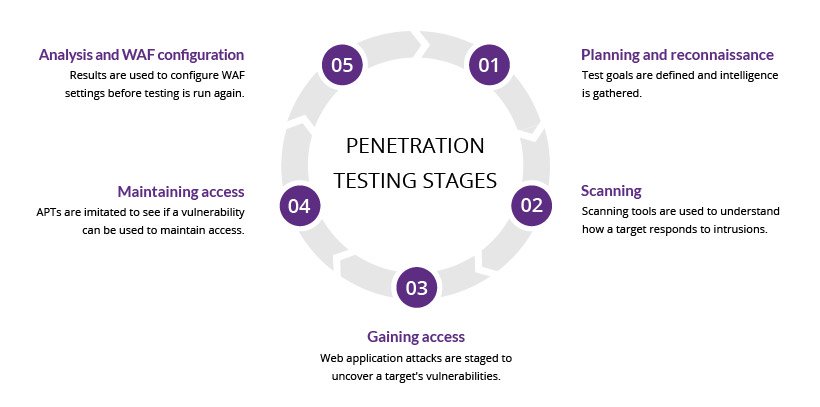
**What interest you in cyber:**

* In a growing technology-based world its required everywhere.
* It’s a maternal trait I gained with a growing family – my little brothers

**What part of cyber:**



**1. Planning and reconnaissance**  
The first stage involves:

* Defining the scope and goals of a test, including the systems to be addressed and the testing methods to be used.
* Gathering intelligence (e.g., network and domain names, mail server) to better understand how a target works and its potential vulnerabilities.

**2. Scanning**  
The next step is to understand how the target application will respond to various intrusion attempts. This is typically done using:

* **Static analysis** – Inspecting an application’s code to estimate the way it behaves while running. These tools can scan the entirety of the code in a single pass.
* **Dynamic analysis** – Inspecting an application’s code in a running state. This is a more practical way of scanning, as it provides a real-time view into an application’s performance.

**3. Gaining Access**  
This stage uses web application attacks, such as [cross-site scripting](https://www.imperva.com/learn/application-security/cross-site-scripting-xss-attacks/), [SQL injection](https://www.imperva.com/learn/application-security/sql-injection-sqli/) and [backdoors](https://www.imperva.com/learn/application-security/backdoor-shell-attack/), to uncover a target’s vulnerabilities. Testers then try and exploit these vulnerabilities, typically by escalating privileges, stealing data, intercepting traffic, etc., to understand the damage they can cause.

**4. Maintaining access**  
The goal of this stage is to see if the vulnerability can be used to achieve a persistent presence in the exploited system— long enough for a bad actor to gain in-depth access. The idea is to imitate [advanced persistent threats](https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/), which often remain in a system for months in order to steal an organization’s most sensitive data.

**5. Analysis**  
The results of the penetration test are then compiled into a report detailing:

* Specific vulnerabilities that were exploited
* Sensitive data that was accessed
* The amount of time the pen tester was able to remain in the system undetected

## **Penetration testing and web application firewalls**

Penetration testing and WAFs are exclusive, yet mutually beneficial security measures.

For many kinds of pen testing (with the exception of blind and double blind tests), the tester is likely to use WAF data, such as logs, to locate and exploit an application’s weak spots.

In turn, WAF administrators can benefit from pen testing data. After a test is completed, WAF configurations can be updated to secure against the weak spots discovered in the test.

Finally, pen testing satisfies some of the compliance requirements for security auditing procedures, including [PCI DSS](https://www.imperva.com/learn/data-security/pci-dss-certification/) and [SOC 2](https://www.imperva.com/learn/data-security/soc-2-compliance/). Certain standards, such as PCI-DSS 6.6, can be satisfied only through the use of a certified WAF. Doing so, however, doesn’t make pen testing any less useful due to its aforementioned benefits and ability to improve on WAF configurations.

Disruption is better us than others and therefore we founded a company builder here in Berlin and the start-up ecosystem and the target for this start-up is to make our company obsolete and if they succeeded 4200 people working today for our company hopefully in future are working for the start up here in Berlin. Two students I have a lot of

I heard a great because the ask you how is the industry and what's coming next 1020 years I cannot tell you what comes in the next 10 years because the world is changing so dramatically fast I heard a great saying the last days people say it's so fast these days someone said it will never ever be so cool and cozy and lazy as it is today and I think there is a lot of truth in it I have no clue what at the end happens in logistics the only thing is students as well as we are companies we need to be prepared and to be open for change and this is what I tried to convince people off the open and not being static because things are changing logistics is changing dramatically so we had globalisation and everybody said we have the big globe as a as a traitor and we can trade all over the globe yeah I know we see was protectionism in the US we see with Brexit we see with

**What are your career goals for the next five years?**

In the next five years, my career goals are focused on growing as a cybersecurity professional and making significant contributions to the field. Specifically:

1. Achieve Industry Certifications

b

• Short-Term (1-2 Years): I plan to obtain key industry certifications such as CompTIA A+, Network+, and Security+ within the next year. These certifications will solidify my foundational knowledge and prepare me for more advanced roles.

• Mid-Term (3-4 Years): After securing these certifications, I aim to pursue more specialized credentials like Certified Information Systems Security Professional (CISSP) or Certified Ethical Hacker (CEH) to deepen my expertise in cybersecurity and ethical hacking.

2. Gain Hands-On Experience in Cybersecurity

• I want to gain substantial hands-on experience working on real-world cybersecurity challenges, particularly in areas like threat analysis, incident response, and security architecture. This experience will help me develop practical skills and understand the complexities of protecting critical infrastructures.

• I also hope to work on projects that involve emerging technologies such as cloud security and IoT security, as these are increasingly important in the industry.

3. Contribute to Security Innovation

• Continuous Learning: I am committed to continuous learning and staying updated with the latest trends, tools, and techniques in cybersecurity. I plan to engage in ongoing professional development through courses, conferences, and involvement in cybersecurity communities.

• Innovation and Problem-Solving: I aim to contribute to the development of innovative security solutions, whether through research, developing new security protocols, or participating in cybersecurity initiatives within my organization.

4. Progress into Leadership Roles

• Mid to Long-Term (3-5 Years): As I gain experience and expertise, I aspire to take on leadership roles within cybersecurity teams. My goal is to eventually lead a team of cybersecurity professionals, guiding strategy and mentoring junior team members.

• Mentorship: I am passionate about sharing knowledge and helping others grow in their careers. I aim to become a mentor for aspiring cybersecurity professionals, helping them navigate their career paths.

5. Contribute to a Secure Digital Environment

• My overarching goal is to make a meaningful impact in the cybersecurity field by helping organizations protect their assets and data. I am driven by the desire to create safer digital environments for individuals and businesses, and I see this as a long-term mission throughout my career.

These goals reflect my commitment to continuous growth, professional excellence, and contributing to the broader cybersecurity community.