HN Security (https://security.humanativaspa.it/) is a boutique company part of the Humanativa Group that provides tailored **offensive security services** (**penetration test & red team**). We enable our customers to gain a strategic advantage against malicious adversaries by proactively testing their security posture.

Our team brings together well-known cybersecurity pioneers with 20+ years of experience with Italy's best talents, trusted by the most important corporations both in Italy and abroad. We aim to partner with our customers to define an actionable security strategy and provide the most suitable and cost-effective services.

We have specialists in every technology, from legacy platforms to the latest innovations. Our proven assessment methodology allows us to discover and exploit vulnerabilities that are often overlooked by competitors. We take pride in the quality of our work and we stand up to any challenge.

Analyzing and attacking today's web applications

Web applications are increasingly present in our lives, and at the same time, the risks and cyber threats are growing. This thesis aims to study the steps necessary for a complete analysis and possible attack on a web application. The steps vary from the analysis of user-supplied input, client-side and server-side controls to possible attacks such as SQL injection, template injection and more.

Development of a payload generation framework for AV/EDRs bypass

Most of organization relies on AV (antiviruses) or EDR (Endpoint Detection and Response) products, in order to detect/prevent intrusion from threat actors. Typically, threat actors use Command and Control frameworks (commercial or open-source) in order to get initial access in a victim company's network. These C2s works by generating agents (executable files or shellcode) that have to be executed on the victim machine, in order to control it. These agents are typically flagged as malicious by AVs/EDRs. Therefore, in order to bypass AVs/EDRs the agents generated by the C2 are usually embedded inside other malicious artifacts, called payloads, that execute the agent but still looks legit to AVs/EDRs and therefore allows to bypass them.

Power analysis and attacks on security electronic safe locks

Side channel analysis is a type of analysis that exploits the information released by an electronic device such as electromagnetic radiation, power consumption, heat dissipated, etc. Power analysis is based on monitoring power consumption to retrieve secret keys. A practical application is bypassing the security code of electronic safe locks: studying the attack, possible replications on other types of electronic locks and possible limitations.