Cooperation feedback to Noctua Sec

First off, this is an absolutely outstanding piece of work. The level of detail, professionalism, and methodological rigor is truly impressive, especially for a student project. You should be incredibly proud of what you've accomplished.

Here are a few things that really stood out to me as exceptional:

- **Professional Report Structure:** The report is incredibly well-organized. It follows logically from the Executive Summary and Scope to a detailed chronological breakdown of the operation. The inclusion of a formal Risk Assessment , Risk Matrix , and actionable Recommendations makes the report immediately useful to the client.
- **Industry-Standard Alignment:** Your use of established frameworks is top-notch. Referencing PTES, OWASP WSTG, and meticulously mapping your TTPs to the MITRE ATT&CK® framework adds a significant layer of professional credibility to your findings.
- **Deep Technical Skill:** Developing a custom C# Backdoor with sandbox evasion , persistence via Registry Run Keys , and a clever C2 channel over the Telegram Bot API is seriously impressive. This demonstrates a practical understanding of modern adversary techniques that goes far beyond basic tool usage.
- **Mature Analysis of Failure:** This might be the most important strength I saw. When the phishing campaign didn't achieve initial access, you didn't see it as a technical failure. Instead, you performed a brilliant analysis, correctly identifying that the lack of success was due to operational factors like timing (summer holidays) and a non-urgent pretext. Your conclusion that "the human element proved to be the strongest layer of defense in this engagement" shows a level of strategic insight that is the hallmark of a great Red Team.

Here are a couple of small, constructive ideas for future engagements:

- **Formalize Target Context Analysis:** Given that timing was the critical factor here, you could consider formally adding a "Target Context Analysis" sub-phase to your methodology. This could live within the Intelligence Gathering or Threat Modeling phases and would focus on assessing the target's current operational tempo (e.g., are they on holiday, in an exam period, etc.) to optimize the timing of the active exploitation phase.
- **Executive Summary Refinement:** The executive summary is already good, but for future reports intended for non-technical stakeholders, you could make it even more direct. For instance, leading with the primary outcome: "The operation determined that while the organization has a strong technical security posture, its greatest (and in this case, successful) defense was the operational context of its members, which prevented a simulated phishing attack from succeeding."

Overall, this is a fantastic report that showcases not just strong technical abilities but, more importantly, the critical thinking, adaptability, and analytical mindset required for high-level security work.

Thank you for your cooperation!

Sincerely,
Mykyta Borshchov & BioInformatics club
bio@pjwstk.edu.pl
09 September 2025
https://bioinformaticsclub.pl/