Select domain – Malware

Provide a brief justification for why you selected this domain and its relevance to modern cybersecurity challenges.

Choose perspective – Attacker

Rigorously review at least 5 developments – 15 references, 3 for each

2 Implementations – demonstrated using screenshots

Show how you set up your environment, how you installed/configured the tool or proof-of-concept code, and the observed outcomes/results.

All implementations/experiments must occur in a controlled sandbox environment (virtual machines, containerized environments).

Analyse the results of your implementation, If you implemented an attack, explain its success rate, stealth, and effectiveness, If you implemented a defense mechanism, explain its detection accuracy, false positive/negative rates, and overall system impact.

A 3-minute live demonstration is required to demonstrate your implementations.

Compare and contrast the five selected developments by highlighting their respective strengths, weaknesses, applicability, and overall impact on cybersecurity. If your review centers on attacks, determine which method poses the most severe adversarial threat based on factors such as stealth, destructive potential, and ease of execution. Conversely, if you are reviewing defensive measures, identify which approach offers the best protection for the chosen application or scenario by considering aspects like resource requirements, technical complexity, and integration with existing infrastructure.

Identify the best (or “most adversarial”) development out of the five reviewed. Justify your conclusion with critical analysis and references to your experiments and literature review.

Also mention about the learnings from each malware and their real life application

Now let us start with the implementation ,but before that have a lot to share first

Study through the report and also go to the internet and study the references I would share for more depth and also the implementations we discussed , will also share u the requirements , documents , marking schema and my system constraints

System constraints – I have a windows 11 , with VM ware workstation pro installed to create VMS , we need to create a local sandbox (vnet 7 ) with host vm(attacker) and victim vm and implement our 2 implementations

Lets do in thorough detail , one by one

Explain every step sequentially to me in simple layman terms , but with full details , spoon feeding me all the way A-Z