**P.T Project**

By Stanislav Kolbeshkin

As a part of Cyber studying in John Bryce we were asked to make an automated process with a script to scan a range or a single ip address and map it vurnlabilities and weak credentials, the tools we were suggest to use is nmap and masscan for active scanning. Its pointless to say that the P.T world finished in this small procedure, the PT world is huge and contains a lot of other points of interest as auxilliries used by msfconsole and more.

In this project we just showed the little of the huge and amazing world of Penetration Testing!

In my project I was using nmap to scan the client with hes input of the range he would like to test, needless to say the higher the count of the addresses the more time it would take, because of the high time wait we gave the client an option, to choose between the basic scan and the full scan options, the difference between them in the depth that each scan goes, in the basic scan you would only get the visible version of service’s you run, the services themselves and open UDP ports that could be use for infiltration.

On the other hand the full scan goes even deeper testing the malwares vulnerabilities and even credentials that’s can be gathered or tested by the client input.

At the end the client can check the reports with created html file for comfortable view and to zip all the results with the reports as he would like.

The project was tough, it holds an amazing potential for creativity and creation which with every new opening of its code endet up in extra hours perfecting and tunning each line into something more sophisticated.

With the help of our teacher Doron Zohar and a little bit tunning of deepseek Ai I was able to reach a finishing point of the project!

Here are some pictures from it as it ran:

