Stealthy Scan: Proposal

We will research stealthy scans and security implications associated with these types of network scans. We will identify how these scans are performed and the reasons behind these scans. The goal of our research is to deliver corroboration on how stealthy scans can be useful, while at the same time being a source of computer security problems.

Our research will focus on how scans are performed to avoid detection compared to methods in which these stealthy scans may be able to be recognized.

Each team member will research the areas of this topic they find significant, then our group will work together to combine the ideas and knowledge that will give a great work to the paper. And our plan is, we have to have an outline of out paper by the end of June, and the rough draft would be done by July 19th. So the final research paper delivered by August 15th.

The reason we choice on this topic, “Stealthy Scan”, is the importance of prevent attacks by attackers, and can be considered a major threat. But it is also very important for administrator should run stealth scans on the systems or computer too, in order to test logging facilities and intrusion detection systems for their capability to detect these stealth scans. So that we can say stealthy scan provides security to our system environment.

Possible references:

<https://ieeexplore.ieee.org/abstract/document/1306976>

<https://apps.dtic.mil/sti/pdfs/ADA448156.pdf> (Detecting Scans ISP level)

Decentralized multi-dimensional alert correlation for collaborative intrusion detection -<https://www-sciencedirect-com.mtrproxy.mnpals.net/science/article/pii/S1084804509000435>

Practical automated detection of stealthy portscans -<https://web-a-ebscohost-com.mtrproxy.mnpals.net/ehost/pdfviewer/pdfviewer?vid=1&sid=0e88b900-e467-49b9-ba05-f332288c2b56%40sessionmgr4007>

Inter-domain stealthy port scan detection through complex event processing -<https://dl-acm-org.mtrproxy.mnpals.net/doi/abs/10.1145/1978582.1978597>

Global Information Assurance Certification Paper - <https://www.giac.org/paper/gsec/1985/stealth-port-scanning-methods/103446#:~:text=There%20are%20many%20types%20of,another%20is%20invented%20and%20implemented.>

TCP SYN (Stealth) Scan (-sS) -

<https://nmap.org/book/synscan.html>

Performing Stealth Scans with Nmap -

<https://linuxhint.com/stealth_scans_nmap/>

Practical Automated Detection of Stealthy Port-scans -

<https://cs.fit.edu/~pkc/id/related/staniford-jcs02.pdf>