To: William H. Flathead III

From: Matteo Franzil

Subject: NMap scan explaination

Date: October 19, 2021

I am writing this memo in order to respond to the questions asked in the last few days.

Recently, in the wake of the serious security design problems that were detected in our company, my workgroup decided to set up a testbed - a sort of internal honeypot, with services matching our ones - in order to conduct some aggressive testing and try to detect as many security issues as possible.

Indeed, the first area that we wanted to tackle was the reconnaisance one. Modern day attackers no longer smash through the front door with a sledgehammer, they'd rather visit the bar you and your coworkers go during breaks and overhear your conversations, trying to gather as much information as possible. This is how reconnaisance works: you first gather data about your target, then you make a proper attack plan. Usually, we divide it into passive and active reconnaisance. The passive reconnaisance is related to information gathering - i.e., `WHOIS` information - while the active one is when attackers actively try to scan and obtain information about our internal networks. And that's where our work started.

We set up a quite complex network, but for our explaination purposes we're fine to assume we have just a single, vulnerable machine and a single attacker, and traffic all going through a single firewall. Using `NMap` - a very powerful open source tool that allows you to make several different scans on networks - we realized that the configuration of our firewall isn't just ideal, is really outdated. Indeed, we're still using a stateless firewall, which is quite a big deal in 2021. For example, this means that attackers can gather information about open ports on our server by sending ACK packets that actually don't belong to any open connection - since the firewall won't actively try to block them, being unaware of open or non-open connections in the network.

This is just an example of what our network is vulnerable of. I've gathered all the information on our findings in a special document, called `instructions.pdf`. You can have a look at it in order to take a full grasp of what are the extents of our researches.