To: Fabio Massacci, Giorgio Di Tizio
From: Claudio Facchinetti
Subject: Nmap scan report
Date: October 23, 2021

What are the different probes used by Nmap? When running a scan with no flags Nmap tries to execute different probes; a quick look at the `tcpdump` results and also on the Nmap docs reveal that it sends:

- an ICMP echo request;
- an ICMP timestamp request;
- a TCP ACK packet to both ports 443 and 80.

Why do you see differences when scanning the top 1500 ports?
When we scan the top 1500 ports we notice that there is another port: this happens because by default Nmap scans the top 1000 ports.

Can you explain why the ports previously classified as ’OPEN’ are now ’OPEN|FILTERED’?
The ports now appear as ’OPEN|FILTERED’ instead of ’OPEN’ probably because they do not send any response: Nmap is able to classify ports based on the response they send, if no response is sent then the packet has been blocked or the service listening is expecting something more.

What is the type of firewall of the company?
The company is using a stateless firewall: in case of a stateful firewall an ACK packet belonging to no enstablished connection would have been immediately dropped. In this case, however, the packet is able to reach the host, therefore the firewall is stateless.

What are the versions of the services? Can you find the path to reach the host?
The Apache webserver is version 2.4.49, while the ssh daemon is OpenSSH version 7.6p1.
In order to reach the host the packet, from the attacker machine, travels first through the router (1.1.2.2) and then arrives to the server machine (5.6.7.8).