The Important of the Scope of Engagement

Penetration testing is a critical part of securing businesses; however, without limitations, it can be very damaging to an organization. The scope of engagement provides a concrete definition of what the penetration tester is allowed to do. Without that list, the penetration tester will break into whatever machines are on the network. This is bad because if there is highly sensitive information on a particular machine or you do not own certain devices on the network, or if the availability of certain devices is critical to the business. Without defining the scope upfront can lead to problems not only for the company but also for the penetration tester. The scope of engagement protects the tester from being prosecuted for unauthorized access by establishing goals, objectives, deliverables, outlining the scope of the penetration test, and by establishing communication plans. In project two, there were several different machines on the network. There was the capstone server, the elastic stack server, and the kali machine. The capstone server was the one that we were going to infiltrate. The elastic stack server was set up to gather the logs from the capstone server so that we could analyze the penetration test and develop alerts. The kali machine was our attacker machine, we used it to find and exploit vulnerabilities on the capstone server. The elastic stack server was out of the scope of the engagement. By attacking the elastic server we could get access to files and data that we should not have had access to. Because the elastic stack can gather all the logs to every machine on the network, we could gain access to company critical data. To identify our targets we used nmap to run a port scan on the network. This returned all the devices on the network and their open ports. While this tool did not cause any harm to machines not in the scope, it did affect the other machines. In the logs you would be able to see that the machine has had icmp requests on the most thousand common ports. You would also be able to see in the nmap report all the services running on those machines. When performing an engagement it is inevitably possible that you will affect other machines or services that people on the network are using. This is because if one of the machines relies on a service that is hosted on the target machine, that machine may become inoperable until that service is online. It is also possible that passwords uncovered on the target system are also used on other machines, or that a number is inputted wrong and the wrong machine is attacked.

Revision #1

Created 2025-11-25 18:34:35 UTC by David Rizzo

Updated 2025-11-25 18:34:47 UTC by David Rizzo