Chase Atkinson

Cyber Security

Engagement Scope

What is an engagement scope and why is it important to an attacker? The engagement scope, by definition, sets boundaries of the engagement and outlines what will be included in the review. When I personally read this definition to understand it best I look for the keywords of boundaries, outlines, and review. Boundaries and outlines mean that when preparing my attack I am going to set a plan to most efficiently attack a target. In this activity we specifically gained access to the secret\_folder first because the folder contained contents that made penetrating the webdav server much easier than without the contents. So inside the engagement scope was the secret\_folder first and then the webdav server. After this we use the ELK stack to log the data from the test to better organize the information for the final keyword of the engagement scope definition, review. So we targeted the secret\_folder with a hydra brute force password crack, then we crack the hashed password and use it to upload our msfvenom payload to the webdav server, and finally we use msf console to launch a meterpreter session on the capstone server and recover the data we were looking for. We then document all the data that was logged from our attack and organize it so that we may better understand countermeasures and mitigation techniques to keep a similar attack from happening in the future.

In Project 2 there were four total Virtual Machines on the Red vs Blue network. The host machine was accessed from the attackers personal machine. Next is the KALI linux machine that was used in all of the activities to penetrate the online repository as well as create the msfvenom payload and metasploit session. The next machine is the Capstone WebDAV server that we were penetrating to obtain the data we were targeting. Finally the ELK stack, which was the server we used to record and log the data that was generated in our attack.

The only machine that was not infiltrated per say was the ELK machine. The testers used this machine to gather all the data from the attack into one place so that the data could be sorted through and organized in a way that we could compare the results with previous and future tests to recognize if our mitigation strategies are successful or not. Nevertheless this machine is no less important than the attacking machine or the target machine. Even if machines are out of scope I still think that it is important to infiltrate them if possible because they may have information important to the rest of the process. Infiltrating them as a part of a penetration test can also provide vulnerabilities for that machine which inturn can develop mitigation strategies to not only secure the machines with the important information but the network as a whole. The more secure the network the more secure each machine or server in it.