Updated Nov 21, 2022

Lab 11.1 Metasploit

💀 It's important to understand some of the technical underpinnings associated with system exploitation before employing automated tools to do the work for us. Relying on a tool without understanding what is going on and the ramifications of the tool's use is a recipe for disaster. The term "script-kiddie" describes this undesirable behavior.

Metasploit is a sophisticated tool. It can greatly enhance the efficiency of a pen test. It can also be extended to deal with new exploits as they are discovered. Before launching an exploit, it is advisable to look at the metasploit exploit ruby module description and code. In many cases, they credit the work of someone who took the time to find the exploit by hand.

Revisiting Cupcake

In the following video, LCDI Intern, Mohammed Hussein illustrates the process of using the Metasploit Framework to achieve a foot hold on cupcake. If you've had experience with Metasploit in the past, feel free to exploit cupcake without use of the video. For a challenge, see if you can use the Metasploit Framework to also escalate privileges to root/Administrator.

Deliverable 1. A screenshot showing your session information from your foothold session and optionally, a screenshot showing your root shell.

Another Target

Deliverable 2. Gain a foothold on Nancurinir using Metasploit. Provide a short video or series of screenshots that document your interactions with the target via your Metasploit session(s).

Alternatively you can use metasploit on a home target such as metasploitable2 or hackthebox target for this second target.

Deliverable 3. Document Metasploit usage to include Exploit selection, Payload selection and the other SET instructions required to get your exploits and metasploit sessions to work. Reflect on this activity and compare the relative merits of exploiting with the frameworks as compared to your hand crafted exploits.