Overview

This exercise will cover the usage of Eternal Blue, a well-known exploit against Windows hosts supporting the vulnerable SMB version 1, establishing a shell on a Windows host, migrating services, and utilizing functions built into the Meterpreter shell. We will also cover the knowledge portion of how Active Directory maintains the directory of it’s users and their associated passwords, as well as comparing that to how a Windows end-user host stores usernames and passwords locally to host, not domain credentials. We will enumerate Active Directory in a way that allow an attacker to determine their ideal existing victim, based upon their objectives.

Objectives

1. Introduce students to utilizing Metasploit
2. Introduce students to the Eternal Blue exploit
3. Differentiate between Domain and non-Domain credentials
4. Enumerate users and groups in Domain and non-Domain environments.
5. Introduce students to credential stealing through hands-on application

ROEs

1. Do not enumerate the network. All IPs will be assigned to individual students
2. Do not interfere with another student’s instance.