Overview

This exercise will cover the usage of the Damn Vulnerable Web Application (DVWA) when using Local File Inclusion and Command Injection on insecure web servers, as well as an introduction to the tool known as Hydra, which is a popular password cracking tool, which will allow us access to the DVWA admin page. Web applications have the largest footprint on the Internet, and are one of the largest targets to attackers. Many programs exist to assist in the improvement of organizations’ web application, which you may be familiar with. HackerOne is an example of a portal where organizations pay individuals for the private disclosure of these vulnerabilities.

Local File Inclusion is the ability for an attacker to access files from a web server’s operating system. For instance, a web server is hosting a file in /var/www/html/jobs/resume-template.docx, which appears to the end-user under a Jobs tab, and a link to the file. With an insecure web server, attackers have the ability to replicate the GET request or URL parameters to access a file that was never meant to be served, like /etc/passwd.

Command injection is a vulnerability that allows attackers to inject arbitrary commands to the web server host operating system. In DVWA, this is demonstrated through a simple web for that asks you what IP you would like to Ping. You type an IP address into the field, and the OS returns the values from the PING <IP>. If a web application is not secure, this allows an attacker to pass additional commands, such as PING <IP> || whoami || ip a

Objectives

1. Introduce students to accessing the AWS range.
2. Introduce students to the DVWA user interface.
3. Introduce student to Hydra through hands-on application
4. Introduce students to the Local File Inclusion vulnerability through hands-on application
5. Introduce students to the Command Injection vulnerability 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.