**Metasploit Executive Summary**

The Metasploit assignment was done against Metasploitable, a vulnerable Ubuntu package. The tools used during this assignment included: **Metasploit** – **NMAP** – **Nessus** – **Metasploitable**

Metasploitable is known to be an extremely vulnerable package of Ubuntu. For this experiment instead of just using NMAP for identifying vulnerabilities, I used a few tools and techniques to take advantage of the powerful Metasploit. I started with first identifying the IP Address and services through NMAP, proceeded to conduct a Nessus scan, and used the results from Nessus within Metasploit to check for exploits.

**Steps conducted for the experiment using Kali:**

1. **NMAP used to scan**

In Metasploit, I ran NMAP with argument ‘-O’ on a range of IP address to get the one for the Linux machine. I was successful in getting the IP address along with the running services. To do a formal vulnerability scan, I decided to use Nessus.

1. **Nessus Scan**

Instead of running Nessus within Metasploit, I decided to load Nessus manually. I conducted a basic network scan using the IP Address I found during the NMAP scan. After the scan completed, I exported the results into a ‘.nessus’ file format then navigated back to Metasploit.

1. **Metasploit Exploit attempt**

In Metasploit, I used the command ‘db\_import \*file location\*’ to import the scan results. By using ‘vulns’ I was able to view all the vulnerabilities Nessus found in a digestible format. Not surprisingly, there were was a huge amount of vulnerabilities. I found one vulnerability named ‘vsftpd Smiley Face Backdoor’ that piqued my interest.

The ‘Smiley Face Backdoor’ vulnerability had an OSVDB ID associated with it, and knowing that OSVDB/CVE/and other ID types can be used to search for exploits from within Metasploit, I used the ‘search’ command with ‘OSVDB:73573’ that belonged to this vulnerability. Luckily, Metasploit had an exploit module named ‘vsftpd\_234\_backdoor’ that can be used to exploit this vulnerability. I loaded the exploit using the ‘use’ command, ‘set’ the ‘RHOST’, and entered ‘exploit’. The exploit was successful, as I was given root access to the target’s shell.

**Conclusion**

Demonstrating how to exploit a vulnerable machine through Metasploit has taught me how powerful and flexible Metasploit is. Having so many tools at your disposal, as well as a working DB, makes Metasploit extremely versatile, allowing users to conduct effective pen tests.