Kyuande Johnson

Ethical Hacking

VM Used Kali Linux ( Metasploitable 2)

To test the sql injection attack I used metasploitable. In metasploitable 2 there is a server that is vulnerable to sql injection. Using the Ifconfig command I found the IP address of the vulnerable server on a Metasploitable image. After finding the IP. I searched the address in the firefox search bar and it took me to the Metasploitable splash page. The Metasploitable splash page has many vulnerable sites to perform various network attacks. In this situation I used a SQL injection attack against Mutillidee. On the Mutillidae site I navigated to a username and password page that's vulnerable to SQL injection attacks. To start the attack I pointed my firefox web browser to a Proxy Server.

127.0. 0.1 is the loopback Internet protocol used to establish an IP connection to the same machine or computer being used by the end-user. Once connected to the Proxy Server Next, we need to configure the browser to work with Burp Suite since it acts as a proxy to intercept and modify requests.

From there I opened the Burp Suite app in Kali, started a new project to ensure that "Intercept is on" is pressed. This will allow us to modify the request from the web page and insert different values to test for SQL injection. Back on the login page, I have entered an arbitrary username and attempted to log in. You can view the raw request as well as parameters, headers, and even hex information. Once you view the information and confirm that Burb Suite intercepted the information. You can modify the Username field on the site and use a sniper attack.” Which runs through a list of values in the payload and tries them one at a time , Once the payload is complete go through each attempt to see a response. Burb Suite has a unique features that renders a web page. By running the intruder attack in burbSuite I was able to view a Database of Username and password credentials.