F4rmC0rp's New Start

Friday 11th December, 2020

Description

After going through a recession, F4rmC0rp is having a fresh start. The first thing need to do is update their website which is main source of promotional opportunity for the company to grow. But, because of the recent recession, they cannot afford to hire an experienced software developer. So, Brandon, who is a fresh graduate is assigned the task of updating/developing the website. Your task is to see if Brandon has made any mistakes and check for potential exploits.

Goal

The goal for this exercise is to:

1. Run any scan and check for deficiencies (nmap, nikto, OpenVAS)

2. Use Dirbuster or any equivalent tool for scanning other web pages on the site.

2. Use Metasploit to gain shell access to a machine.

Tasks

1. Log into your Kali machine.
2. Start scanning using either nmap or OpenVAS and check for open ports on the target machine.
3. Inspect for vulnerabilities. If not found, check if any other webpage has any vulnerability.
4. Use nikto to scan the vulnerable webpage. Note what the vulnerability is.

5. Do what is necessary to start up the metasploit console.

6. Once in metasploit, search for the vulnerability and see if there is any exploit for it.

7. Choose any of the exploits, set the correct options and run the exploit.

8. A key is available in the file system on the target machine. (Or is it?)