Specialized Scanners

This document contains several screen shots showing the various nmap, dirbuster, WPscan, and Nikto scans that I ran against the target Windows machine. In my option each scanning tool has pluses and minuses that make them essential be used together to enumerate the target machine. For this assignment I turned to Google and YouTube to help me figure out the steps to obtain the flag. I think dirbuster and WPscan returned the best results and information on the target machine. I like how dirbuster shows you the directory structure and the WPscan provided me with users and had I had 4 days it might have provided me the passwords for all the accounts as well. Below you will find y screen shots and what information I believe I was able to locate from the various tools used in the assignment.

After running an nmap scan to determine my target machine I did my go to nmap -sV 10.0.9 scan against the target machine. I noticed that when I did this, I did not find port 8585 listed in my results. I then performed a scan using nmap -p- 10.0.2.9 this did show that port 8585 was up but it came back as an unknown service.

Text

Description automatically generated

Since I was able to confirm that port 8585 was up, I performed a dirbuster scan. I didn’t complete the scan because I used wordlist that would take several to days to completed. So far out of the two tools used, nmap and dirbuster, this one has produced the best results thus far. It was able to show me directory and file information.

Text

Description automatically generated

Table

Description automatically generated

Table

Description automatically generated

I ran two Nikto scans. The first was just nikto -h 10.0.2.9. This produces limited results that didn’t provide much information. I then uses nikto -h 10.0.2.9:8585 and the results changed. The first scan came back as a Microsoft-IIS/7.5 server. The second scan showed that an Apache Web Server was on port 8585. From here I went to google and typed in <http://10.0.2.9:8585> in my browser that directed me to webpage that I felt initially didn’t have anything of value.

Text

Description automatically generated

Text

Description automatically generated

Graphical user interface, text

Description automatically generated

From here I turned to Google and spent some time looking for a scanner specific to port 8585. What I found was a WordPress scanner called WPscan. It took me some time to figure out as I ran a couple of different scripts I found on Google. My first scan was wpscan –url <http://10.0.2.9:8585/wordpress> returned that at first, I didn’t think meant anything important. I believe to find the flag I could have stopped here but I didn’t. It wasn’t until retrospect that I noticed this scan provided me with four plus URLs that I could look at see where each URL would take me. What I liked about this scanner and results is that it had information that tied back to the Metasploit framework.

I ran several different scans with WPscan. I was able to determine that there are four usernames. They are admin, manager, vagrant, and user. I attempted to brute force the passwords with WPscan but once again it would take like 4 days to complete, and the target machines shuts down every hour so that was not productive.

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

This set of screen shots shows the various webpages that were brought up in the first scan.

Graphical user interface, application

Description automatically generated

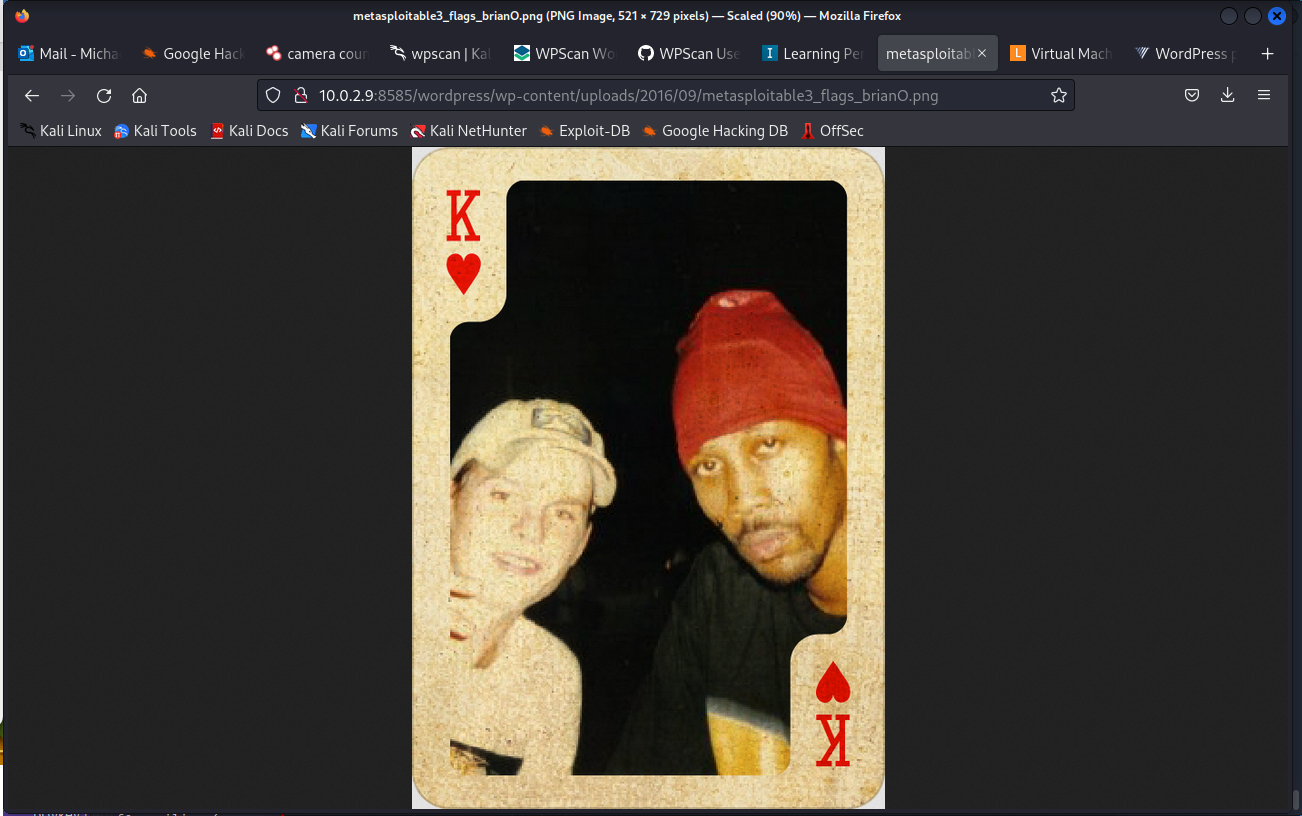
Graphical user interface, application

Description automatically generated

When I investigated the <http://10.0.2.9:8585/wordpress/wpcontent/uploads> page I discovered that this was a page I could explore. This is where I obtained the flag of the king of hearts, which is the last screen shot in the document.

Graphical user interface, text, application

Description automatically generated



One thing I know I learned is to take some time on each scan and see where the information takes one to. I initially skimmed over information that I didn’t think was important but ended up being crucial to the success of the assignment.