Investigate Web Attack Challenge

I will be completing the LetsDefend Investigate Web attack Challenge. For this challenge, I need to answer seven questions based on given log files.

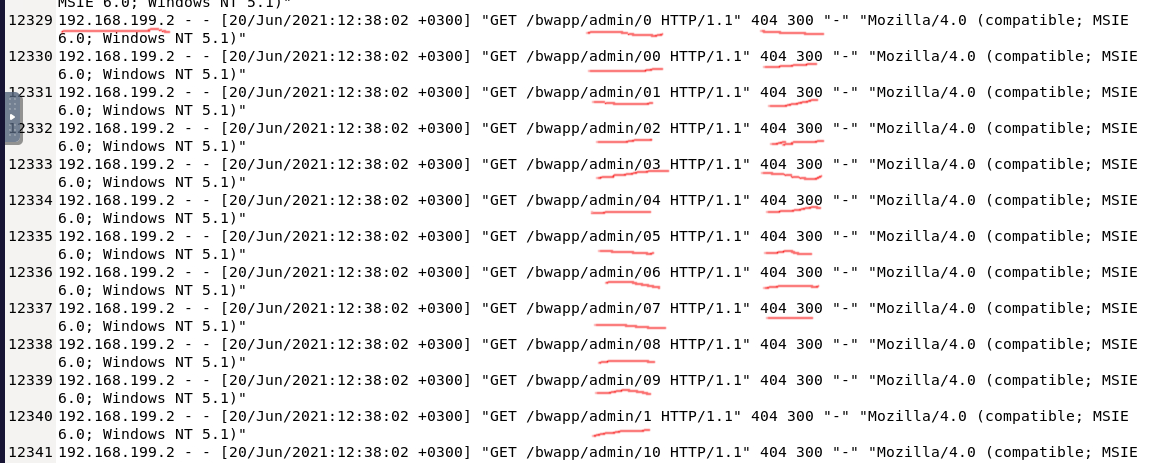
1. Which automated scan tool did the attacker use for web reconnaissance?

Scrolling through the log file, Nikto was used for several requests. A quick search shows that Nikto is an open source (GPL) web server scanner commonly used to check for outdated web server software.



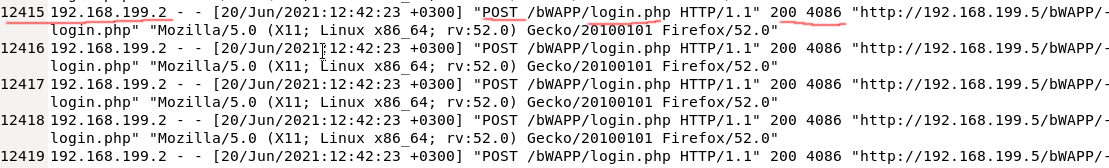
1. After web reconnaissance activity, which technique did the attacker use for directory listing discovery?

The attacker used a Directory Brute Force method. As seen in the screenshot bellow, the attacker is using an automated tool to find subdirectories of the admin folder. In return he is receiving 404 client side error, which means the specific sup folder does not exist.



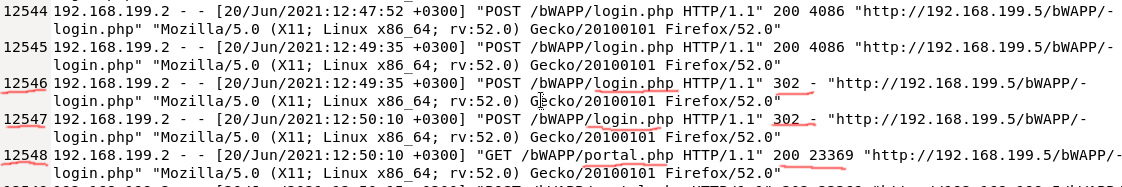
1. What is the third attack type after directory listing discovery?

Starting at line 12415, the attacker implements a Brute Force attack repeatedly sending in login attempts. From the 200 status we can tell the login request was successful, but from the size of the log (4086) remaining constant, we can assume that they are receiving a error message or unsuccessful login.



1. Is the third attack successful?

Line 12546 and 12547 the attacker receives a 302 status code which shows how they are being redirected. In the next line 12548 we see that they are now in portal.php and can see from the size returned that they have much more data. This unfortunately means that the bruce force was successful, and the attacker was able to log in.

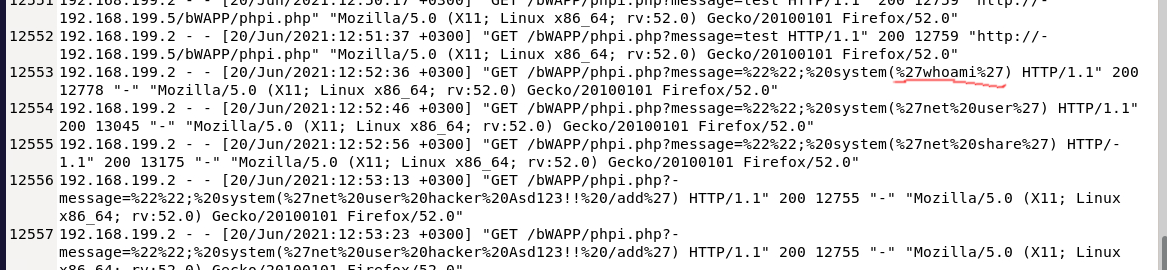


1. What is the name of the fourth attack?

Now that the attacker is inside the system, the attacker starts implementing code injection. This can be clearly seen with the first payload $whoamI, as explained shown in the next question.

1. What is the first payload for 4th attack?

The first payload is (%27whoami%27) or ‘whoami’. This will show the name of the current user logged into the system.



1. Is there any persistence clue for the victim machine in the log file ? If yes, what is the related payload?

Yes, on the victims payload there is a URL encoded message showing the name of the hacker. When decoding the URL message (%27net%20user%20hacker%20Asd123!!%20/add%27), the result becomes ('net user hacker Asd123!! /add')

