The first course of action would be to scan the server, to check for any suspicious files. There were a total of 3 infected files, however there was one more suspicious file that was not detected by the initial scan report. After writing a detection rule, the file was successfully detected as a suspicious file as well.
Afterwards, an initial check on the Intrusion Detection System logs showed some unusual activity that was performed as the root user from a Secure Shell connection (SSH connection). A security measure was taken against this ip address to prevent it from being able to connect to the server.

Moreover, there was a new user created onto the server, titled “darklord”, which had access to the root user and all its functionalities. There was also a suspicious process that was being run in the background by the root user, which was certainly done by the intruder. The username and the background process were successfully removed from the server.
To secure the server further, gaining access to the root user account was disabled for anyone that is connecting remotely to the server using SSH, regardless of the remote user privileges. Additional steps to secure the system in general have been documented in a step by step process to secure the environment further.

In order to harden security, a scan was made onto the server, which resulted in 23 results out of a possible 588. Out of these 23 results, only one is of high severity, and can be mitigated using the additional steps previously mentioned.
Afterwards, the banner from the web server was removed, to remove the probability of an attack happening due to a publicly visible banner.
The apache web server was then modified to have an owner user and group, titled apache-user and apache-group respectively in order to improve system security.