Nykaa Internship

Security Assignment

Aaryash Raj Sinha

15th January, 2021

AIM

1. To set up an EC2 instance.
2. To set up and configure a WordPress Website on that instance.
3. To carry out the CIS hardening of the server and providing a hardening score via AWS Inspector scan or some alternative mechanism.

IMPLEMENTATION

1. The process is begun by creating an AWS EC2 micro-instance with the AMI of Ubuntu 20.04. (Security Group comprises an SSH, HTTP and HTTPS ports.)
2. Next step according to the plan was to set up a LAMP/LEMP Server and configure Wordpress on it. But before proceeding, it is advised to perform the Hardening of freshly installed OS on an instance.
3. Before beginning the Hardening process, using the InSpec compliance profile on our Ubuntu (Linux-Baseline), the Hardening Score of this freshly installed OS, is shown below.

```
Profile Summary: 27 successful controls, 28 control failures, 1 control skipped
Test Summary: 84 successful, 46 failures, 2 skipped
```

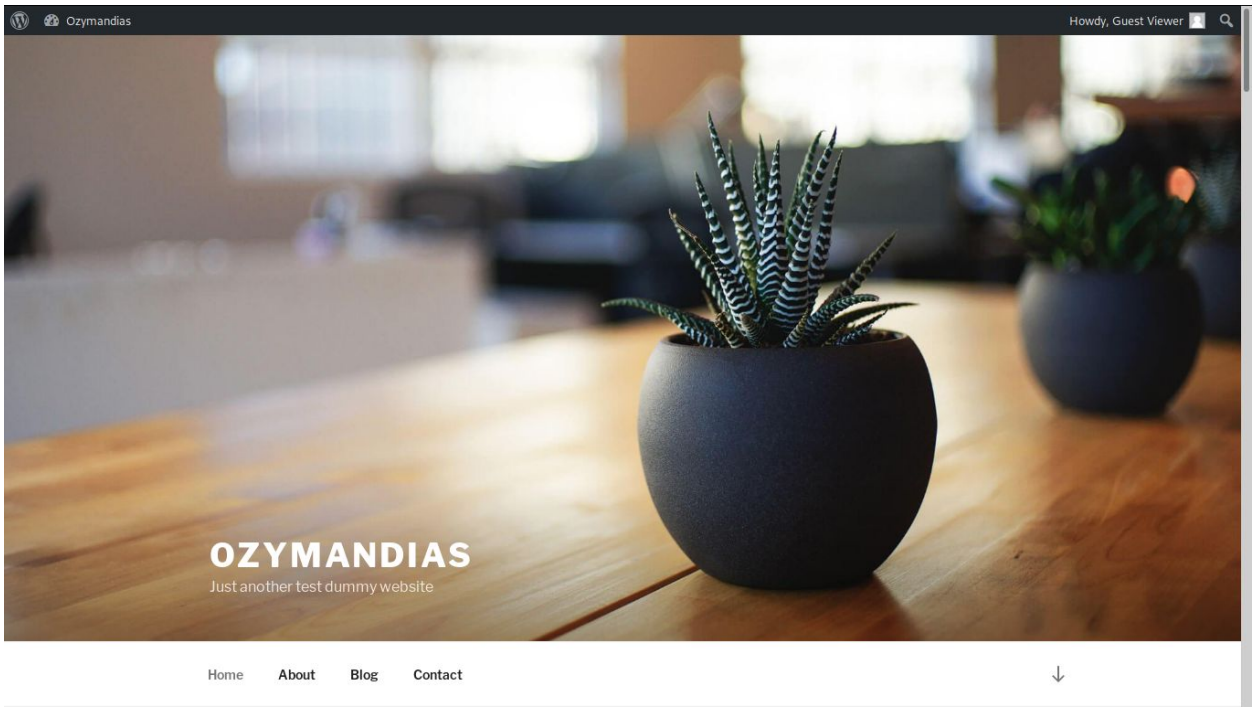
4. Proceeding with the Hardening process. Among the numerous Linux Hardening scripts available on Github, AKcryptoguy's-Server-Hardening-Script was easy to set up and helped in increasing the Hardening Score by 4. This was all about the Hardening process performed by the automated scripts.

```
Profile Summary: 29 successful controls, 26 control failures, 1 control skipped
Test Summary: 88 successful, 42 failures, 2 skipped
```

5. Moving ahead, a LEMP Server (Linux, Nginx, MySQL, PHP) on the instance is set up and the configuration of a Wordpress Website is done. A fully configured Wordpress Website is as shown below.

   Website - **http://3.7.71.238/**

   Credentials - **Viewer : PT9&r6woti^Z$)Ny)Xf4FZw***



6. On further researching, I found a blog explaining the steps to perform Stage-1 Hardening manually, which consisted mainly of,
    a) Disabling SSH root login
    b) Ensuring the working of Fail2Ban, a brute-force & intrusion prevention software.
    c) Disabling IPV6 and Hardening IPV4
    d) Enabling Unattended Security Updates

    Upon performing these above steps, the Hardening Score of our EC2 Instance increased.

```
Profile Summary: 33 successful controls, 22 control failures, 1 control skipped
Test Summary: 95 successful, 35 failures, 2 skipped
```

Initial Hardening Score: **84** Final Hardening Score: **95**