

|  |  |
| --- | --- |
| Name | W.G. Malaka Dananjaya |
| Registration Number | IT17007948 |
| Subject | Information Assurance and Auditing |
| Report | Security Audit Assignment Report |

**Nginx Security Audit**

Nginx is a secured, reliable web server even with the default setup. But there are more ways to secure Nginx further. In this document, we will use both open source and commercial tools for auditing Nginx.

In the first part of the document we will discuss how to use Wapiti open source tool to audit Nginx.

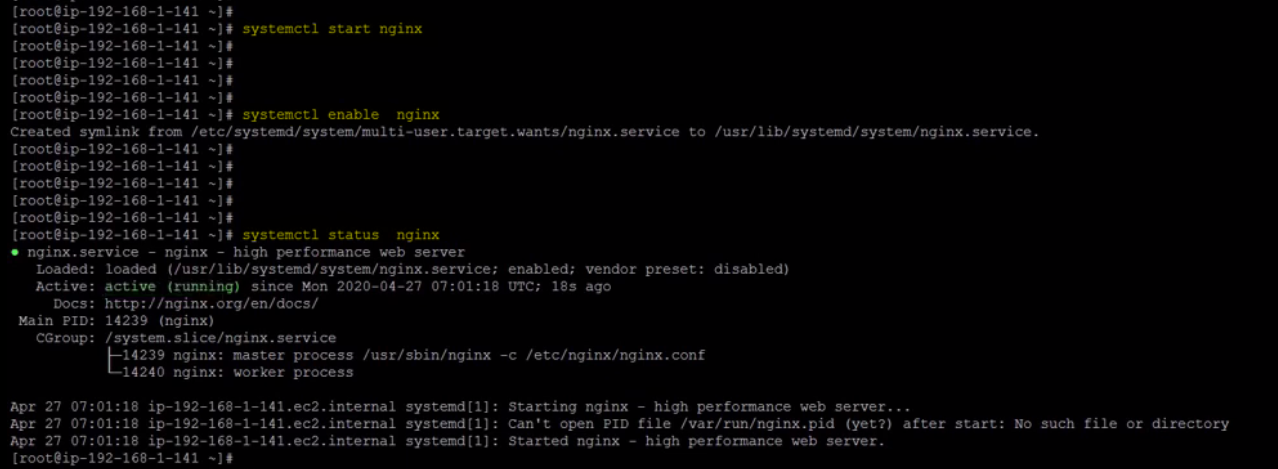
In the second part we’ll discuss how to use Barracuda vulnerability manager (commercial tool) to audit Nginx.

**Part 1 - Nginx Audit using Wapiti**

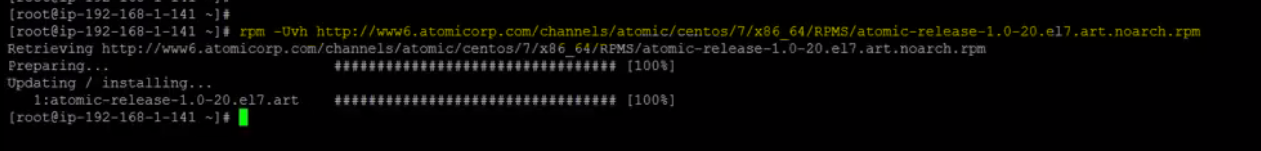
Step 1 : Install Nginx



Step 2 : Start and Enable Nginx service



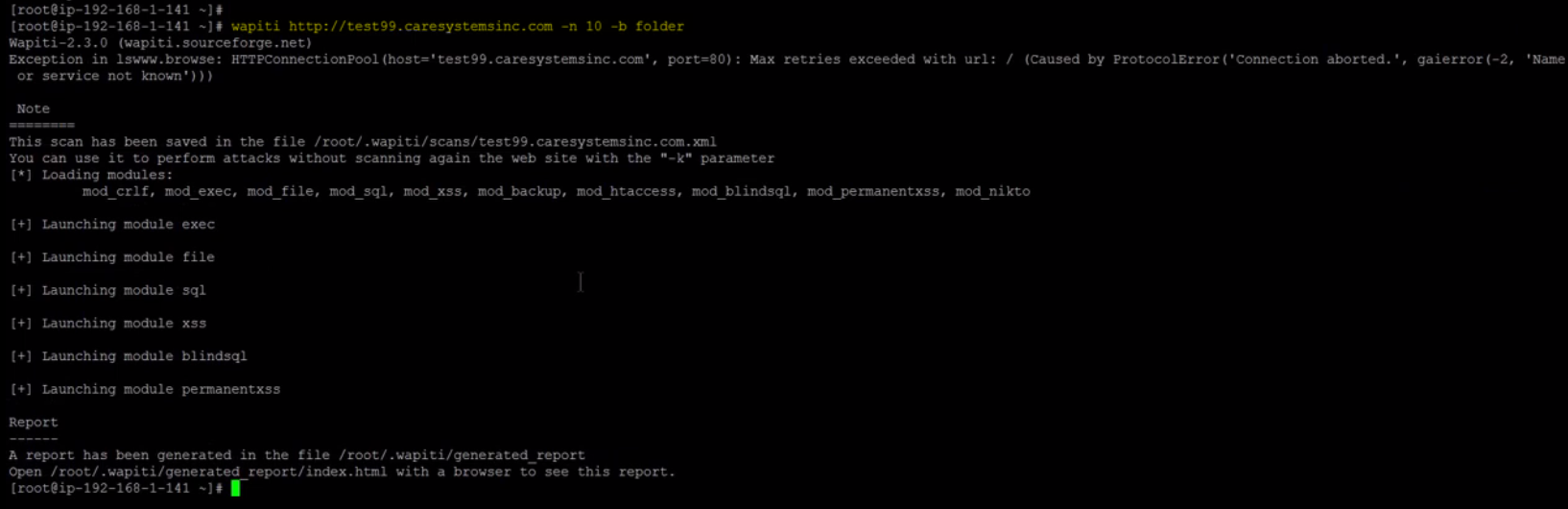
Step 3 : Install atomic release package



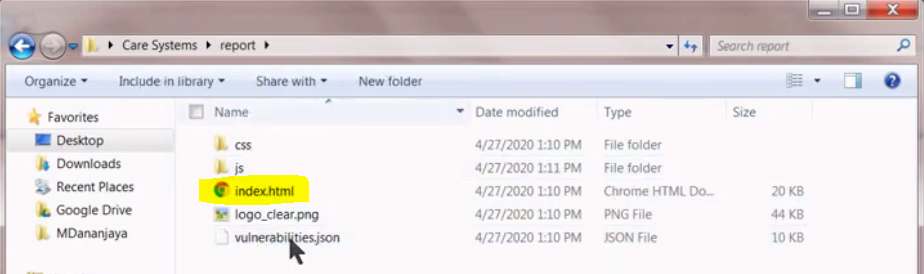
Step 4 : Install Wapiti package



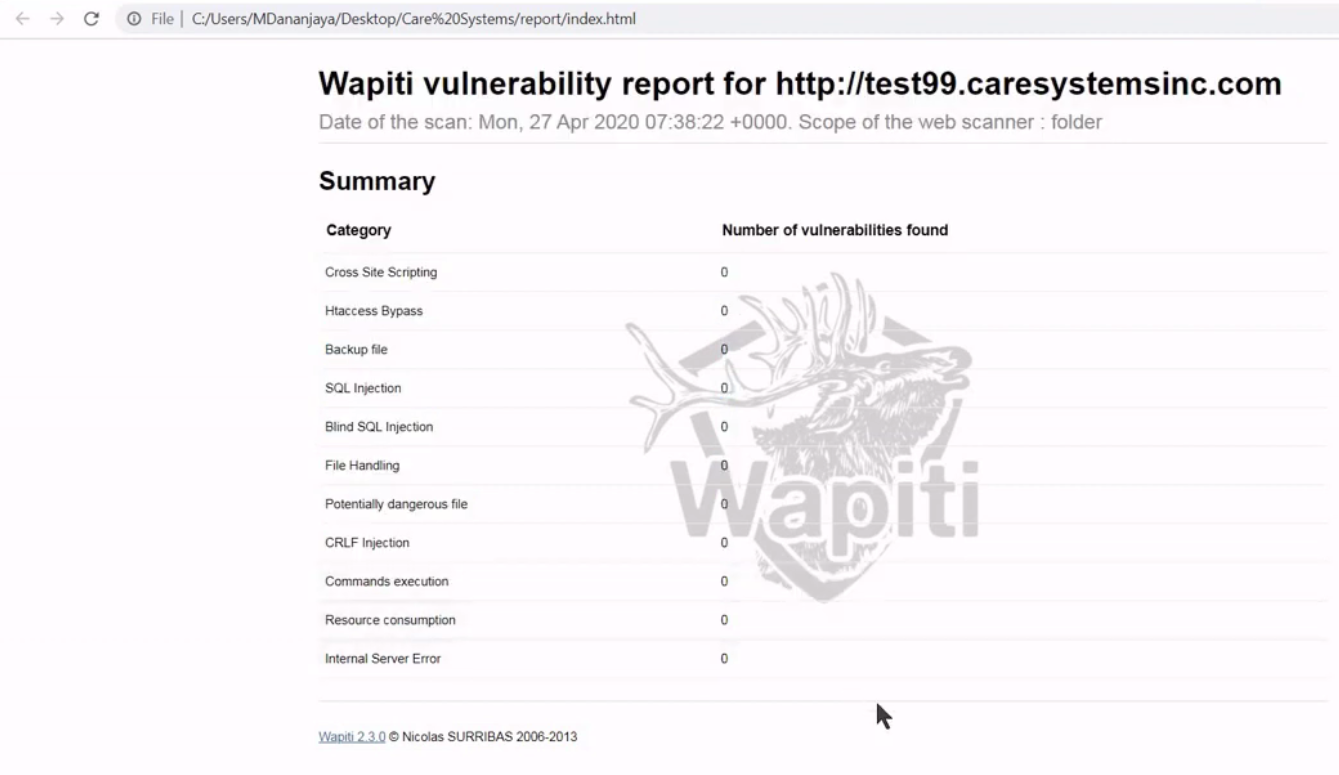
Step 5 : Execute audit using wapiti command



Step 6 : Download the generated report folder to your local machine

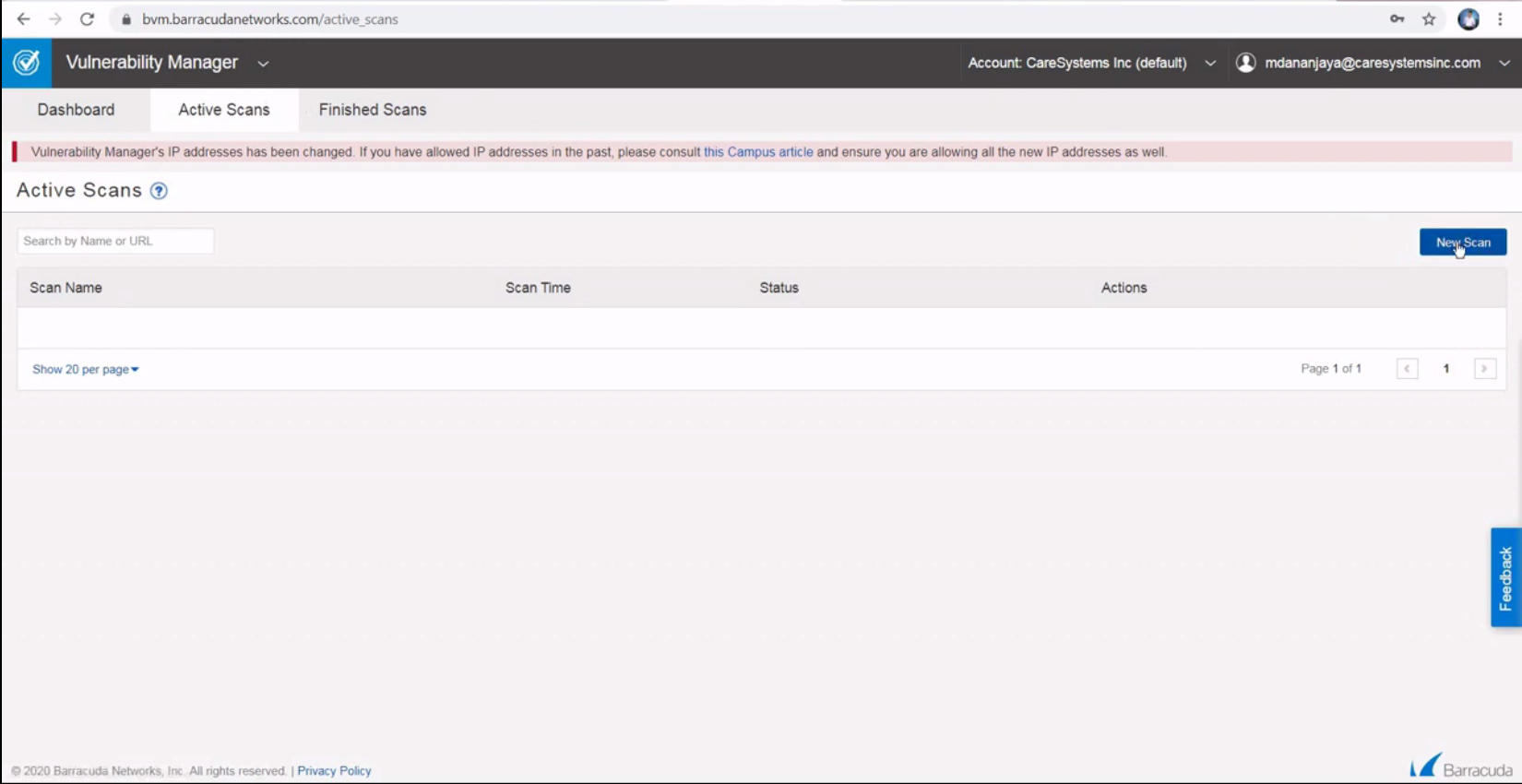


Step 7 : Open index.html file in your browser. It will display all the vulnerabilities found.

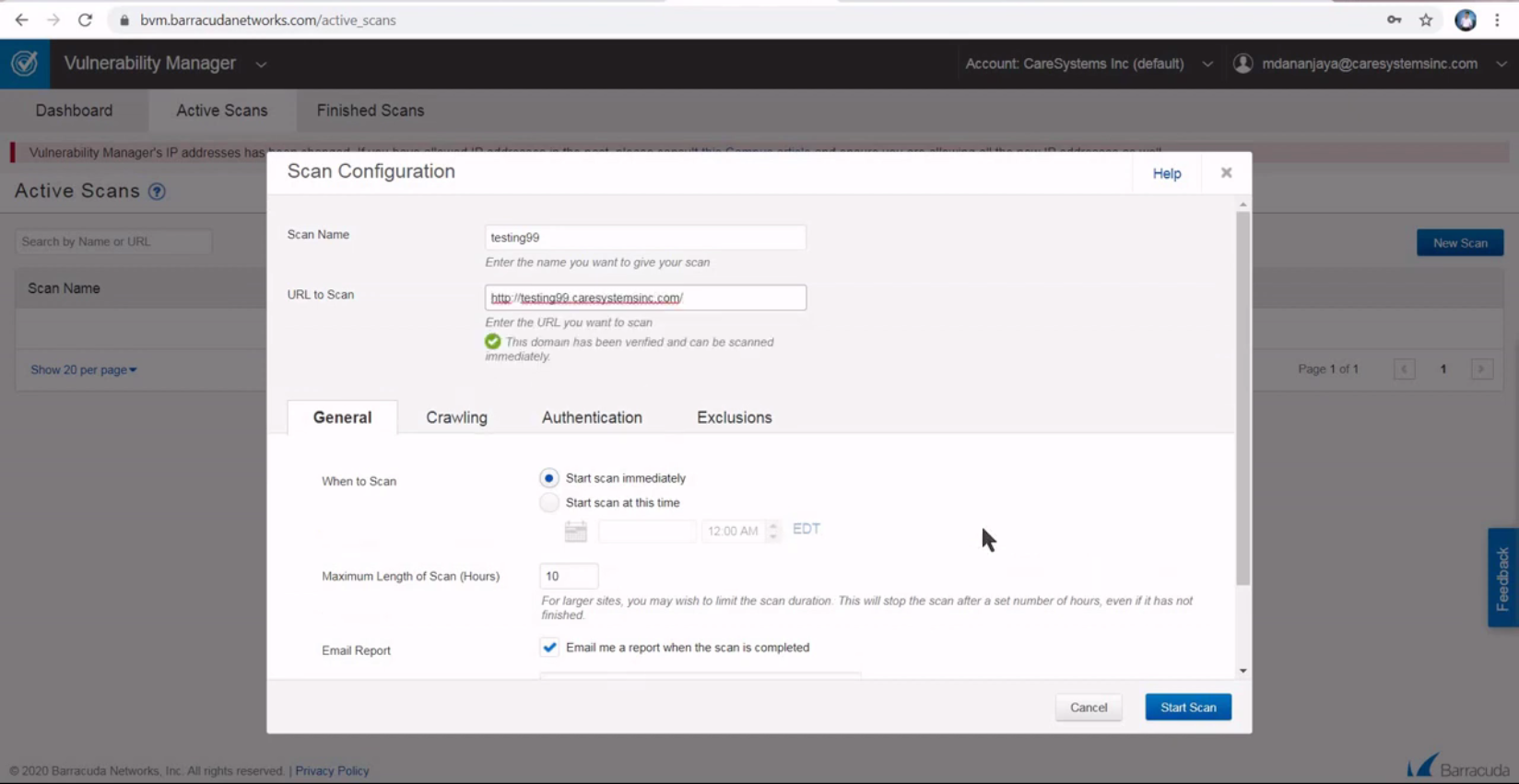


**Part 2 - Nginx Audit using BVM**

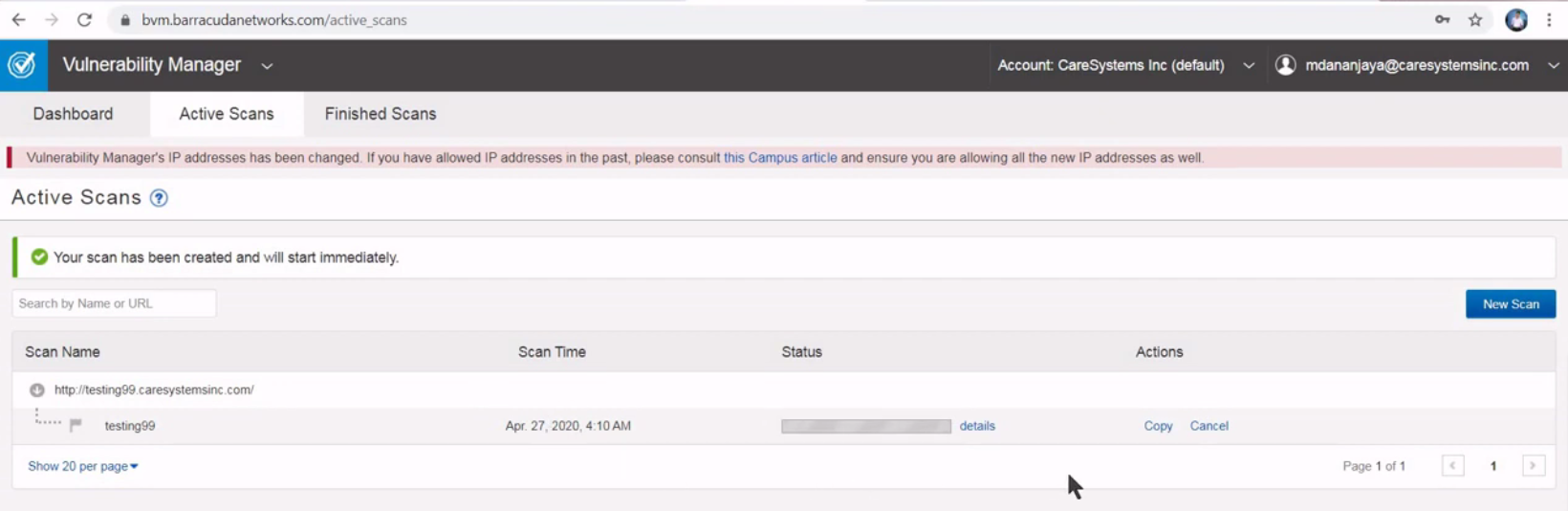
Step 1 : Login to <http://bvm.barracudanetworks.com/> with a valid account



Step 2 : Select New scan button under active scans tab. Give a scan name and the URL to the Nginx



Step 3 : Select start button and it’ll run around 5-10 minutes.



Step 4 : once scan finished click on “see finished scan” link and you can see the report.

