Logo

Description automatically generated

Using Nessus to scan for vulnerabilities in the MOP web application

Zachary Kein – 220277143

Contents

[Setting up Nessus 2](#_Toc133322791)

[Scans Completed 4](#_Toc133322792)

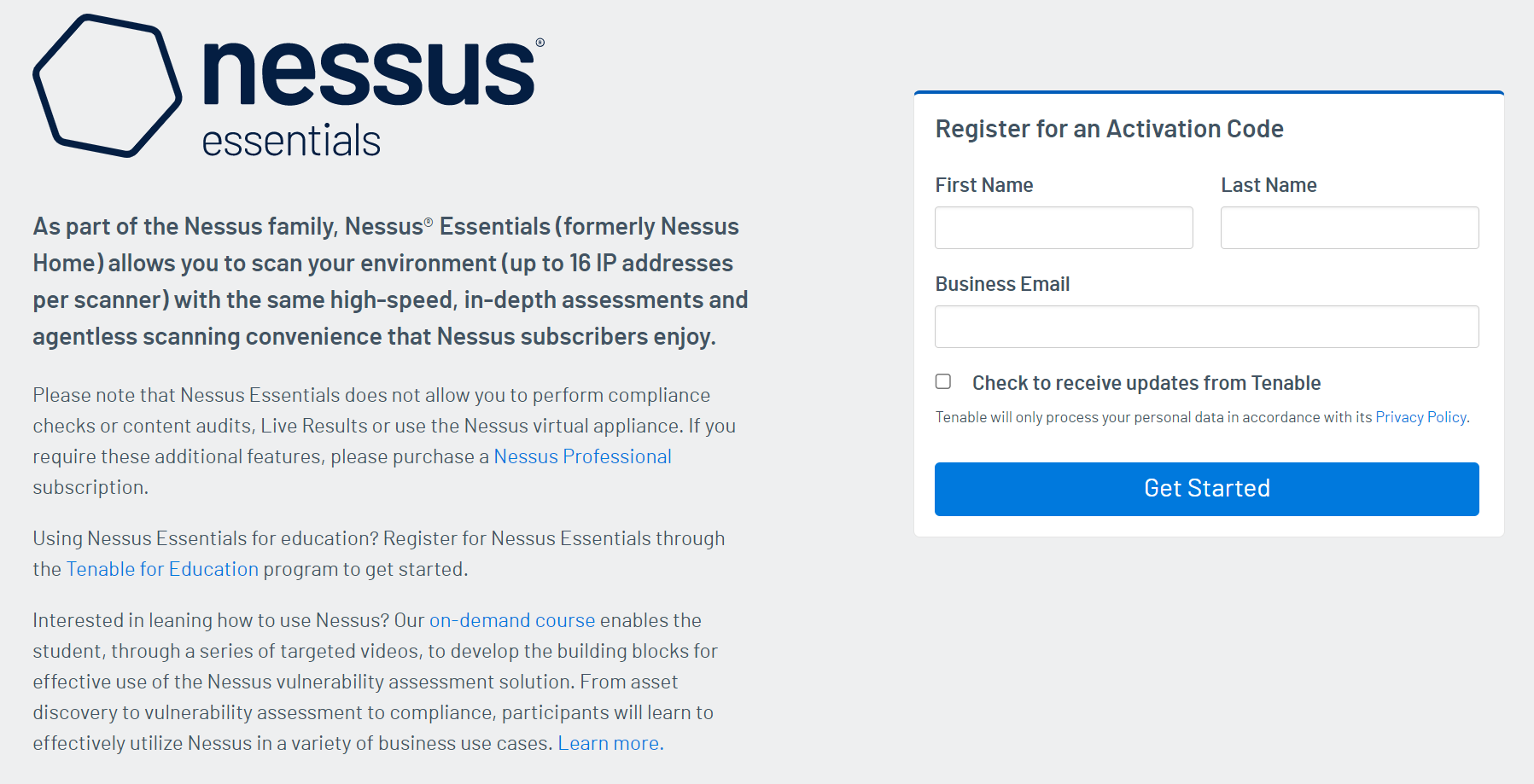
[Results 5](#_Toc133322793)

[Vulnerability Analysis 7](#_Toc133322794)

[Conclusion 10](#_Toc133322795)

# Setting up Nessus

Sign up for Nessus from [this link](https://www.tenable.com/products/nessus/nessus-essentials?tns_redirect=true) to begin the set-up process. You are unable to download Nessus without first setting up an account as it will redirect you to the download page.



After signing up for Nessus, you will be directed to a page to download the installation package. This report will be using Nessus Essentials, however Tenable offers many different versions of Nessus that can be used for different coverage of scans.

Graphical user interface, application

Description automatically generated

After installing the correct version, we will use the command ‘**sudo apt-get install libssl1.1**’ to install the required dependencies

Text

Description automatically generated

To install Nessus, navigate to the folder containing the package. In our case it will be in the Downloads folder. Then, use the command ‘**sudo dpkg -I Nessus-10.5.1-ubuntu-1404\_amd64.deb**’.

It should be noted the number after Nessus and the numbers after ubuntu may need to be changed depending on the version you have downloaded.

Text

Description automatically generated

To start Nessus, use the command ‘**sudo systemctl start nessusd.service**’.

Graphical user interface, website

Description automatically generated

Open your browser and go to ‘**https://localhost:8834/**’ to access the Nessus web interface

Graphical user interface, website

Description automatically generated

Follow the on-screen instructions to access, making sure to grab the activation code from the email you signed up with.

**Note**: While Nessus does require a paid subscription to use, they offer a 7-day free trial to test out the software and complete scans. You do not need to fill out any payment information to get the free trial you can just sign up with your email and when it finishes, you can use the same email to renew the trial, however reports will not save.

# Scans Completed

Nessus offers a wide range of scan types depending on the specific things you are looking for. It ranges from a basic network scan to looking for specific malware such as the WannaCry ransomware. I chose three scan types for this vulnerability check to check for basic vulnerabilities in case the MOP website had some small flaws that needed to be patched. I conducted a basic network scan, web app test, and TLR vulnerability scan. TLR is the Threat Report Landscape from 2022 which would highlight the issues most prevalent in web servers last year.

Graphical user interface, application

Description automatically generated

# Results

The results of the scans show that the basic network scan found 9 vulnerabilities, the web app test found 8, and the TLR scan found 3. Overall, the three scans combined found 9 unique vulnerabilities that may be impacting the server. Nessus ranks the level of concern for the vulnerabilities on a five-point scale from info being of little to no concern, and critical being of extreme importance. There were no concerning vulnerabilities found in the results as they were all in the ‘info’ level of concern, making the webapp very secure. The results can be found on this table:

|  |  |  |
| --- | --- | --- |
| **Basic Network Scan** | **Web App Test** | **TLR Vulnerability Scan** |
| Nessus SYN Scanner | HTTP Methods Allowed | Nessus SYN Scanner |
| Common Platform Enumeration | HSTS Missing from HTTPS Server |  |
| Device Type |  |  |
| HTTP Information | HTTP Information |  |
| OS Identification |  |  |
| Service Detection |  |  |
| Traceroute Information |  |  |

\*\*Red Text = Overlap in scan results

You may notice the number of vulnerabilities may not match the amount in the table. This is due to each open port being counted as a vulnerability, as well as Nessus listing the scan information as a vulnerability.

The least important scan completed was the TLR scan as it was the results were an overlap of the other two scans completed. It is important to check regardless as the different scan types may find different results.

Graphical user interface, text, application, Word, email

Description automatically generatedGraphical user interface, text, application, Word, email

Description automatically generatedGraphical user interface, text, application

Description automatically generated

# Vulnerability Analysis

This section will detail the vulnerabilities that were found in the scans. It should be noted that it will only detail each unique vulnerability as each scan had a few overlaps and solutions will only be added if they are necessary as per the results.

**Common Platform Enumeration (CPE)**

Synopsis: It was possible to enumerate CPE names that matched on the remote system.

Description: By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Risk Factor: None

**Device Type**

Synopsis: It is possible to guess the remote device type.

Description: Based on the remote operating system, it is possible to determine what the remote system type is (e.g.: a printer, router, general-purpose computer, etc).

Risk Factor: None

**Hypertext Transfer Protocol (HTTP) Information**

Synopsis: Some information about the remote HTTP configuration can be extracted.

Description: This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keepalive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Risk Factor: None

**Nessus SYN scanner**

Synopsis: It is possible to determine which TCP ports are open.

Description: This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution: Protect your target with an IP filter.

Risk Factor: None

Port 80/tcp was found to be open

Port 443/tcp was found to be open

**OS Identification**

Synopsis: It is possible to guess the remote operating system.

Description: Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Risk Factor: None

Remote operating system : AIX 5.3

Confidence Level: 65

Method: SinFP

The remote host is running AIX 5.3

**Service Detection**

Synopsis: The remote service could be identified.

Description: Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Risk Factor: None

**Traceroute Information**

Synopsis: It was possible to obtain traceroute information.

Description: Makes a traceroute to the remote host.

Risk Factor: None

For your information, here is the traceroute from 10.0.2.15 to 216.239.36.56 :

10.0.2.15

10.0.2.2

216.239.36.56

Hop Count: 2

84502 - HSTS Missing From HTTPS Server

Synopsis: The remote web server is not enforcing HSTS.

Description: The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks and weakens cookie-hijacking protections.

Solution: Configure the remote web server to use HSTS.

Risk Factor: None

The remote HTTPS server does not send the HTTP "Strict-Transport-Security" header.

**HTTP Methods Allowed (per directory)**

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each

directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities

Risk factor: none

Based on tests of each method :

- HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND

BPROPPATCH CHECKIN CHECKOUT COPY DEBUG DELETE GET HEAD INDEX

LABEL LOCK MERGE MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY OPTIONS

ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT

RPC\_IN\_DATA RPC\_OUT\_DATA SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK

UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on

# Conclusion

The scans that I was able to complete using Nessus’ wide range of tools helped to give me a great insight into the security that the MOP project already has in place.

Though I was expecting more issues to show up in the results, it is great to see that there are only extremely minor things that were picked up in the scan. Not having many major issues reduces a lot of the worry that may be had by the web dev team as they will be able to know the extent of their security.

There are not many changes that can be added from the results of these scans. There are some solutions in some of the vulnerabilities that may be a place to start but the results conclude that the risk factor is nowhere near high enough to warrant immediate action.