

# **IAA - Mini Project**

Gunasinghe M.D. IT17043342

B.Sc (Hons) Degree in Information Technology

Department of Information Technology

Sri Lanka Institute of Information Technology

Sri Lanka

May 2020

## DECLARATION

I declare that this is my own work and this proposal does not incorporate without acknowledgment of any material previously submitted for a degree or diploma in any other university or institute of higher learning and to the best of our knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgment is made in the text.

<b>Name</b>	<b>IT Number</b>	<b>Contribution</b>	<b>Date</b>
Gunasinghe M.D.	IT17043342	Network audit using “Nessus” vulnerability scanning tool in windows OS.	2020/05/04

## Table of Contents

<b>List of figures</b> .....	3
<b>Introduction</b> .....	4
Installation .....	5
Auditing Process -Set the Policy .....	8
Audting Process – Start a New Scan .....	11
References .....	17

## List of Figures

Figure 1.1 : Nessus website .....	5
Figure 1.2 : Register for product Activation Code .....	5
Figure 1.3 : Activate the product .....	6
Figure 1.4 : Loading Plugins. ....	6
Figure 1.5 : Policies .....	7
Figure 2.1 : Setup the policy .....	8
Figure 2.2 : Policy Configurations .....	9
Figure 2.3 : Authentcations. ....	10
Figure 3.1 : select the policy. ....	11
Figure 3.2 : Host selection .....	12
Figure 3.3 : scan report. ....	13
Figure 3.4 : Multiple hosts. ....	14
Figure 3.5 : Vulnerabilities .....	15
Figure 3.6 : issue and solution .....	16

## **Introduction**

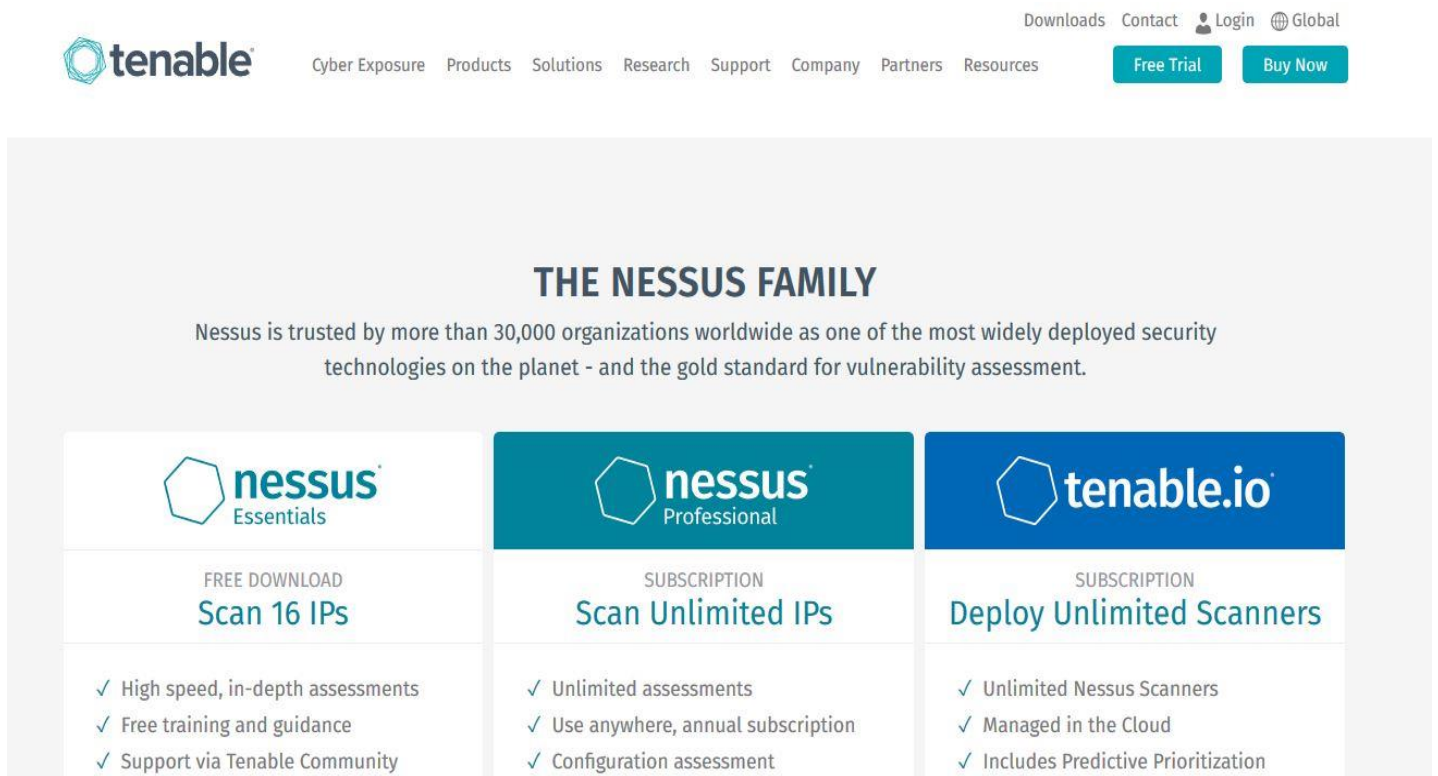
This assignment is based on Information Assurance and Auditing. Purpose of this project is to give an idea about importance of Information Auditing. [1] IT audits cover a wide range of IT processing and communication infrastructure including web services, software applications, security systems, operating systems and client-server networks and systems. The audits are generally designed to ensure there are no errors within your IT system, leaving you vulnerable for an attack.

For this assignment I've used "Nessus" and I did Basic network audit for all Networks that connected with my Laptop. It's one of the most widely used vulnerability assessment tools in the IT industry. It's easy to use and finds vulnerabilities effectively but does not penetrate them.

## 1. Installation.

Download the setup file from this site <https://www.tenable.com/products/nessus>

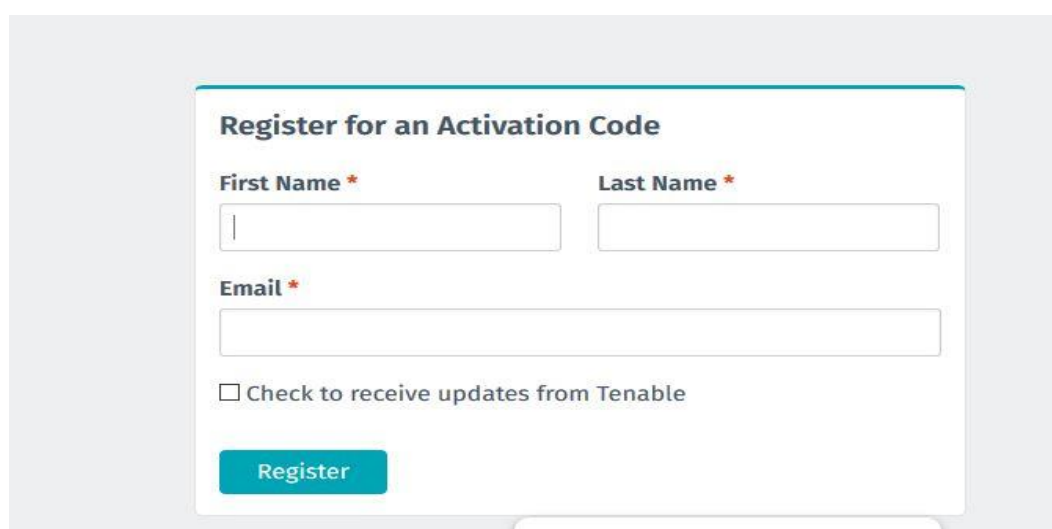
Before you download it please check your OS is 64-bit or 32-bit. They have provide different setups for each Operating System.



The screenshot shows the top navigation bar of the Tenable website with links for Downloads, Contact, Login, and Global. Below the navigation bar, the 'THE NESSUS FAMILY' section is displayed. It features three product cards:

- nessus Essentials**: FREE DOWNLOAD, Scan 16 IPs. Features include: High speed, in-depth assessments; Free training and guidance; Support via Tenable Community.
- nessus Professional**: SUBSCRIPTION, Scan Unlimited IPs. Features include: Unlimited assessments; Use anywhere, annual subscription; Configuration assessment.
- tenable.io**: SUBSCRIPTION, Deploy Unlimited Scanners. Features include: Unlimited Nessus Scanners; Managed in the Cloud; Includes Predictive Prioritization.

Figure 1.1 : Nessus website



The screenshot shows a registration form titled 'Register for an Activation Code'. It includes input fields for First Name, Last Name, and Email, each marked with a red asterisk. Below the email field is a checkbox labeled 'Check to receive updates from Tenable'. A teal 'Register' button is at the bottom of the form.

Figure 1.2 : Register for product Activation Code

As in figure 1.2 you need register with you email to get the product activation code.

When you finish the setup , “Nessus” will automatically open via localhost address through your default web browser to continue the loading plugins and setup the environment for scanning purposes.



*Figure 1.3 : Activate the product.*



*Figure 1.4 : Loading Plugins.*

It will take some time to finish the loading plugins that is needed for operations of “Nessus tool” (figure 1.4).

Once you have finished the installation process you can log in to “Nessus dashboard”. (figure 1.5) In here you can see many vulnerability test settings against different scenarios.

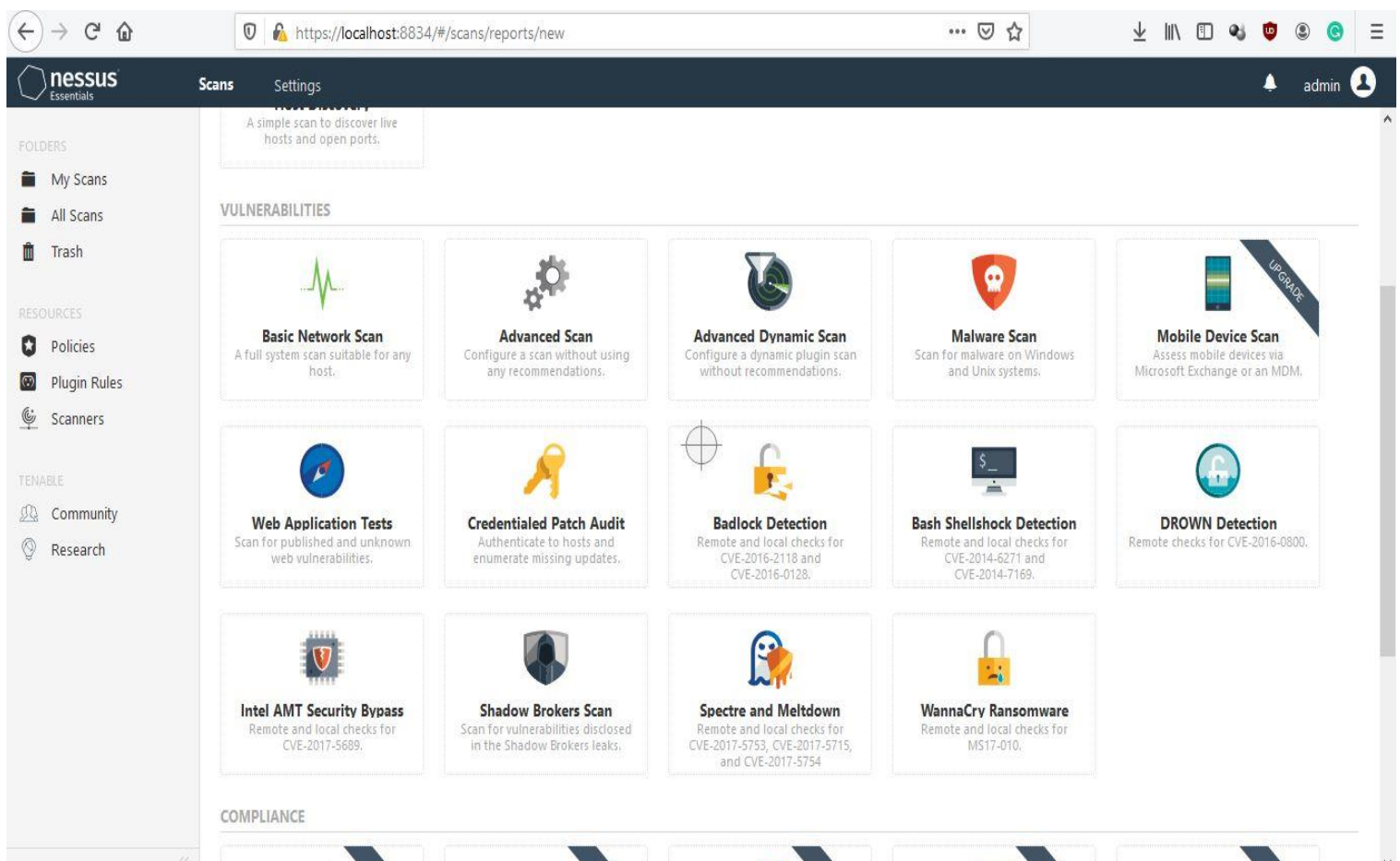


Figure 1.5 : Policies.

<https://localhost:8834/#/>

You can access this Nessus Dashboard via any web browser using this localhost address. All you have to do is just copy this url and paste it in any web browser. Then using the Nessus Credentials that you’ve given earlier in the installation process , you can log into the “Nessus” dashboard.



## 2. Auditing Process – Set the policy.

Before you start a scanning , you have to set a new policy for that scan including settings. As first step please go to **policies** in dashboard. It appears in left tab.

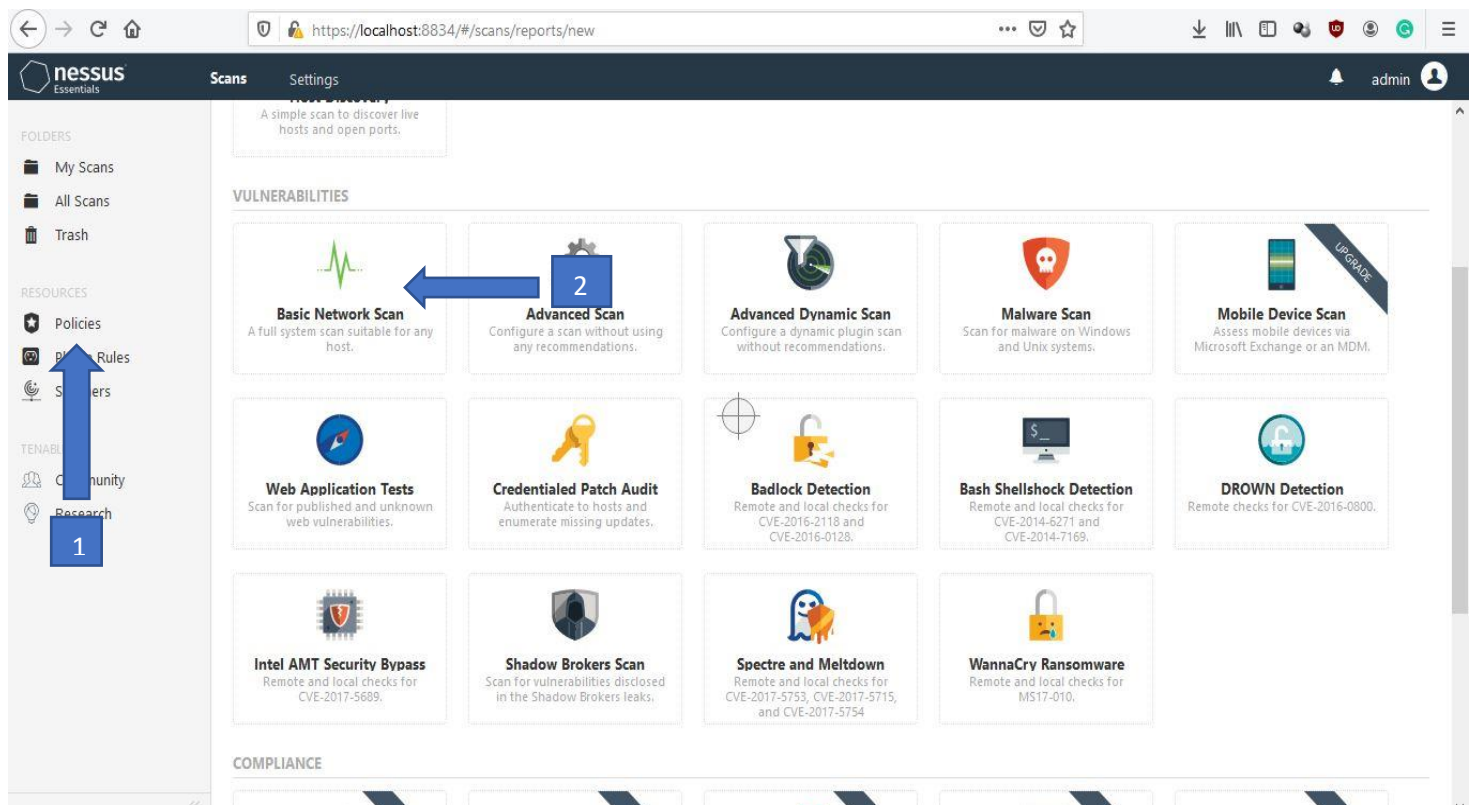


Figure 2.1 : Setup the policy

Then click “Basic Network Scan” to set new policy in Network scan. Since we are doing a Network Audit you have to set Policy before the scanning.

In next window it will display Configurations under “Basic Network Scan”. You have to give the name of the policy and Description about the scan as in figure 2.2.

The screenshot shows the Nessus Essentials interface. The top navigation bar includes the 'nessus Essentials' logo, 'Scans', and 'Settings' tabs. The user is logged in as 'admin'. The left sidebar contains 'FOLDERS' (My Scans, All Scans, Trash), 'RESOURCES' (Policies, Plugin Rules, Scanners), and 'TENABLE' (Community, Research). The main content area is titled 'Basic scan / Configuration' with a 'Back to Policies' link. It features three tabs: 'Settings' (active), 'Credentials', and 'Plugins'. Under the 'Settings' tab, there is a list of categories: 'BASIC' (selected), 'DISCOVERY', 'ASSESSMENT', 'REPORT', and 'ADVANCED'. The 'BASIC' section is expanded, showing two fields: 'Name' with the value 'Basic scan' and 'Description' with the value 'IAA - TEST Scan'. At the bottom of the configuration area are 'Save' and 'Cancel' buttons. A 'Tenable News' section is visible at the bottom left of the sidebar.

Figure 2.2 : Policy Configurations

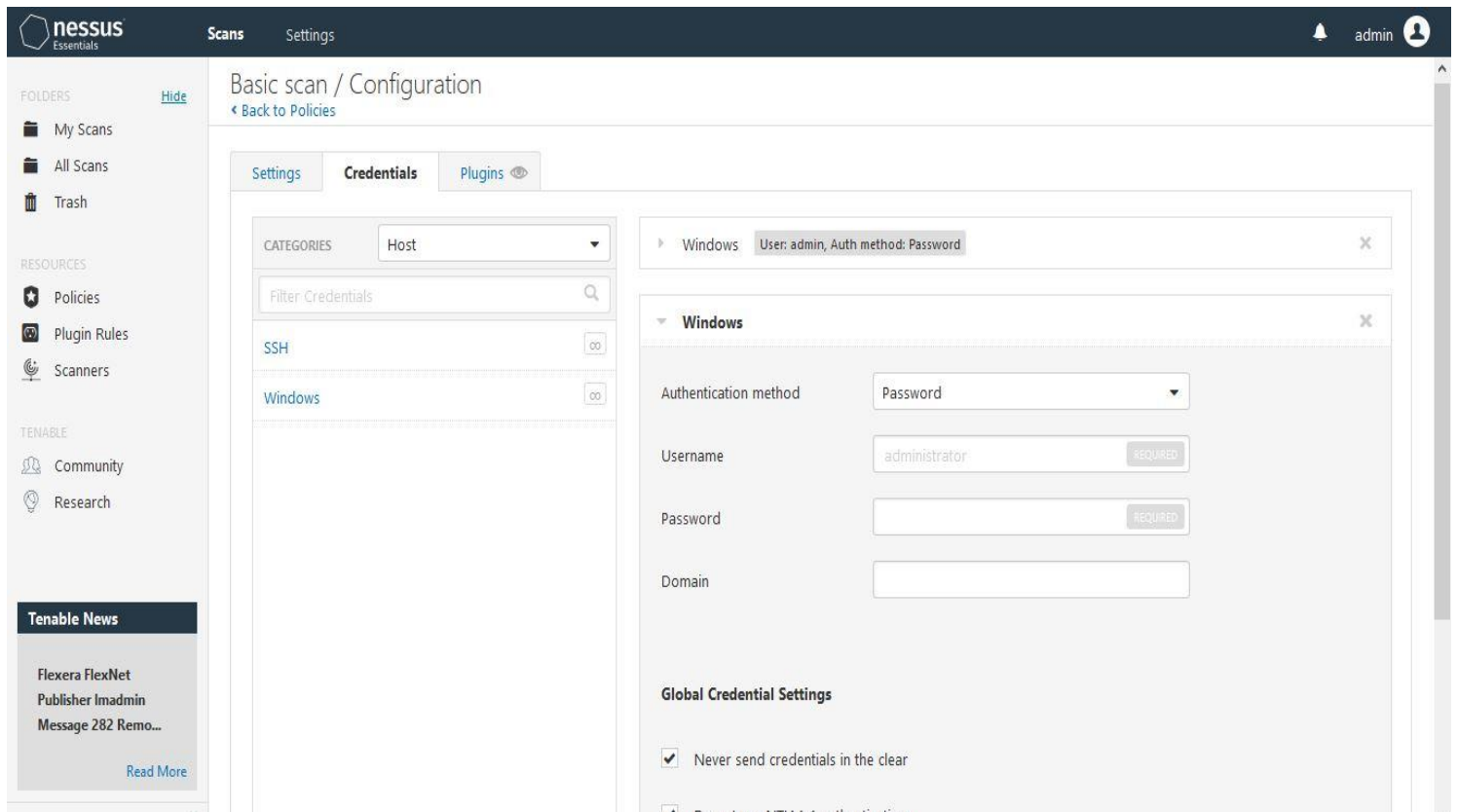


Figure 2.3 : Authentications.

(figure 2.3) Then you have to set the Authentication method for the policy. If it's **linux** machine you have to select **SSH**. This practical based on **windows 10** OS so select windows tab and you set Credentials for the authentication. Give both Username and password same as the “Nessus Dashboard Credentials” that have access to log into the dashboard.

See the Arrow in figure 2.3: in **Global Credential Settings**

Put tick to : **start the registry service during scan** and **enable administrative shares during the scan**.

Then save it.

### 3. Auditing Process – Start a New Scan

Once you set a policy, you can start new scans using that policy. According policy rules. Select new scan in “Nessus” home . In scan templates select **User defined**.

Whenever user create a new policy it's appear in **User defined tab** scan templates(figure 3.1).

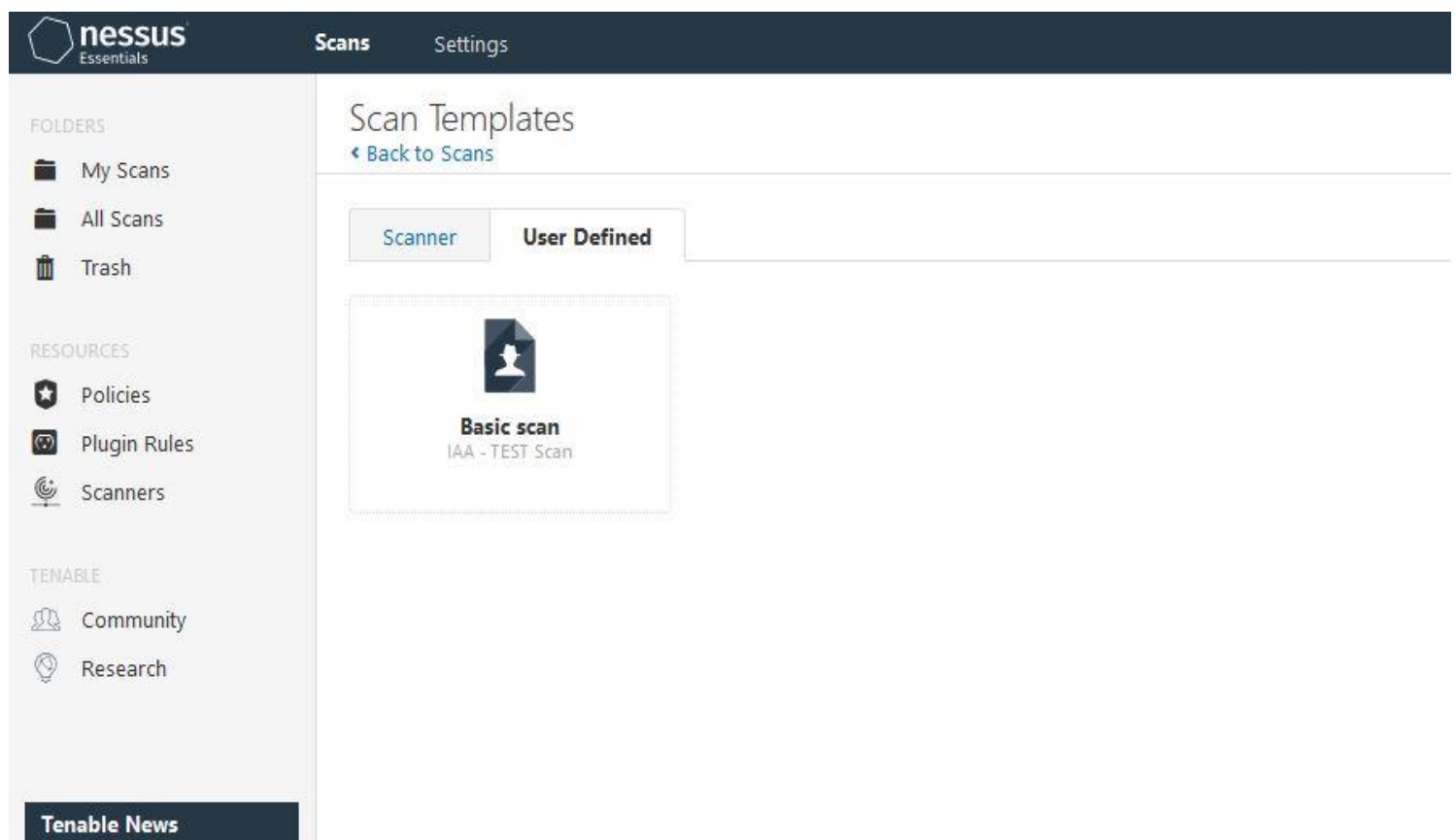


Figure 3.1 : select the policy.

That policy you've selected in previous window is configure to do basic Network Vulnerability scan.

In this window users have to give information about the scan and **most importantly** give **target hosts** to scan.(figure 3.2) Users can scan Invidual Host or Multiple hosts at the same time.

The screenshot shows a web interface for configuring a scan. On the left, a sidebar contains a 'Settings' header and a 'BASIC' section with three sub-items: 'General' (selected), 'Schedule', and 'Notifications'. The main area is titled 'Settings' and contains four input fields: 'Name' (with a 'REQUIRED' label), 'Description', 'Folder' (a dropdown menu currently showing 'My Scans'), and 'Targets' (with a 'REQUIRED' label and an example text: 'Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com'). At the bottom of the main area, there are two buttons: 'Upload Targets' and 'Add File'.

*Figure 3.2 : Host selection.*

Then save and Launch the scan using **Launch** button.

It'll take 20 to 30 minutes to complete whole scanning process. Once it completed it generates a report about the scan as in figure 3.3.

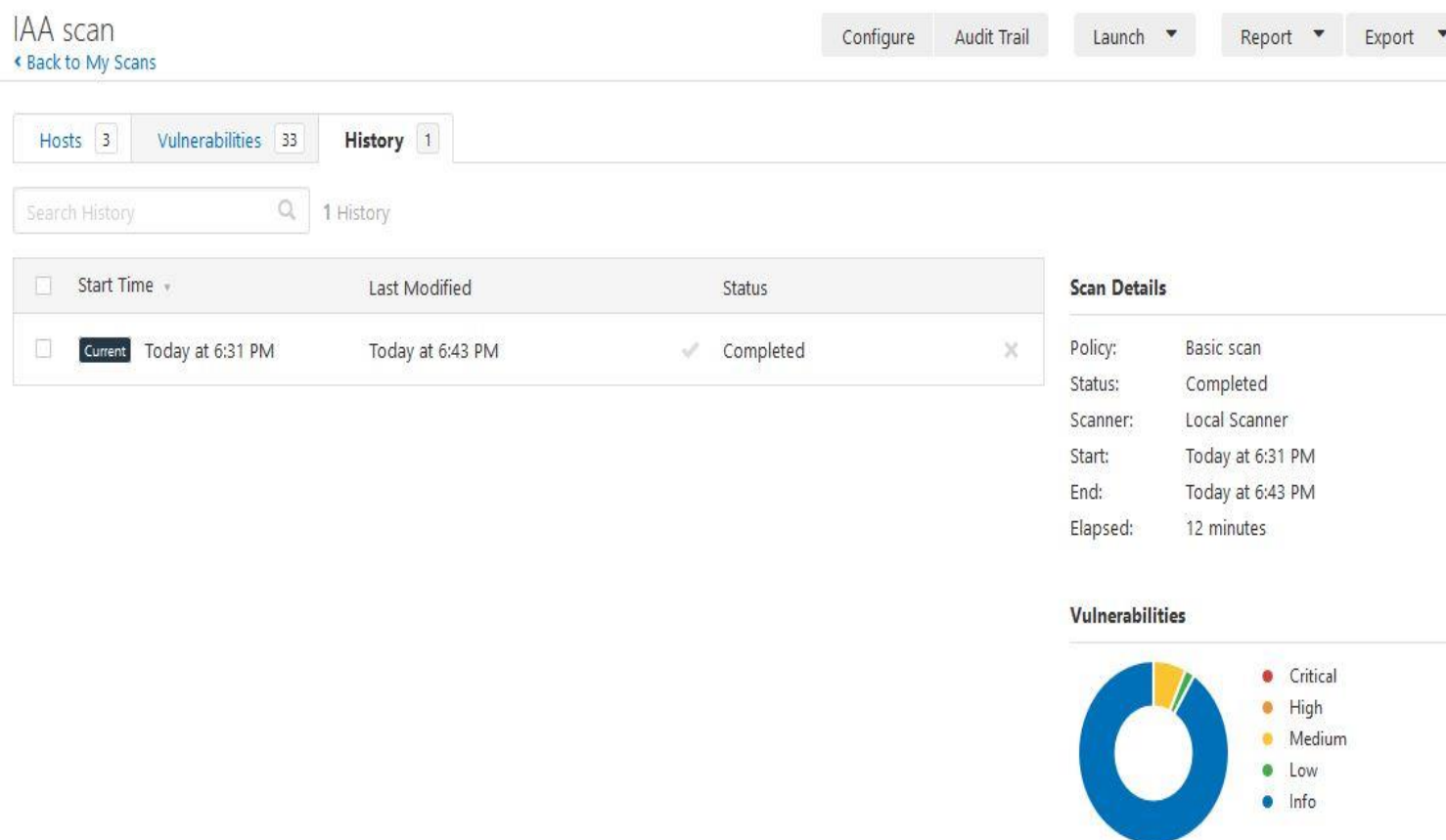


Figure 3.3 : scan report.

If you select host tab in scan report , you can see how many hosts that process have checked for vulnerabilities. In this scenario there are three hosts in this network and report show each and every vulnerabilty according to the relevant host. All the vulnerabilties are color coded and users can easily identify and give priority to fix which ones are the critical (figure 3.4).

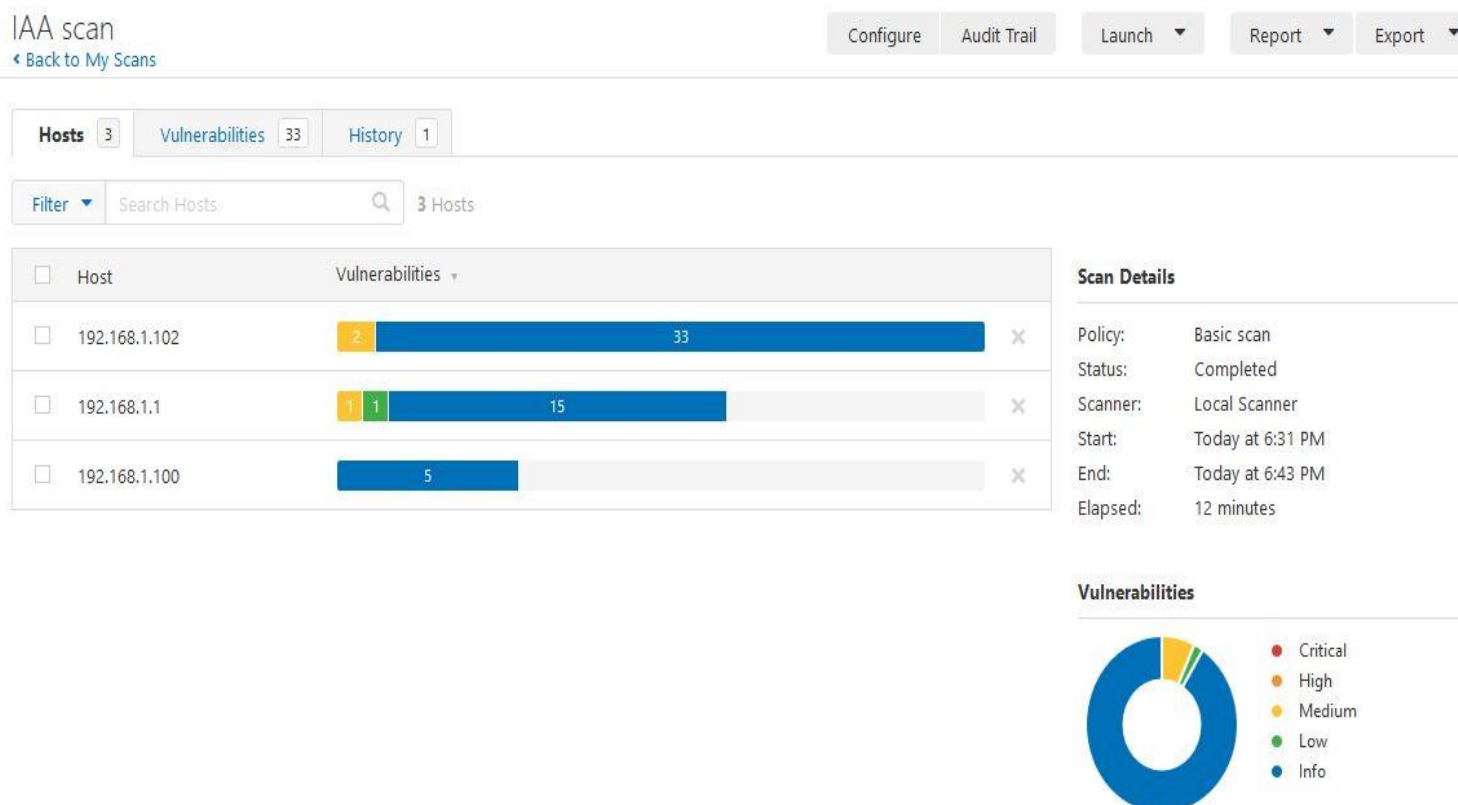


Figure 3.4 : Multiple hosts.

Check vulnerabilities using **vulnerability** tab and it'll show user to how threats that found in the scanning process. Always give high priority for critical, high and medium issues to fix soon as possible. In this window users can see full description about the issues. For example , type of the issue , how many time it occurring and which category it belongs figure 3.5.

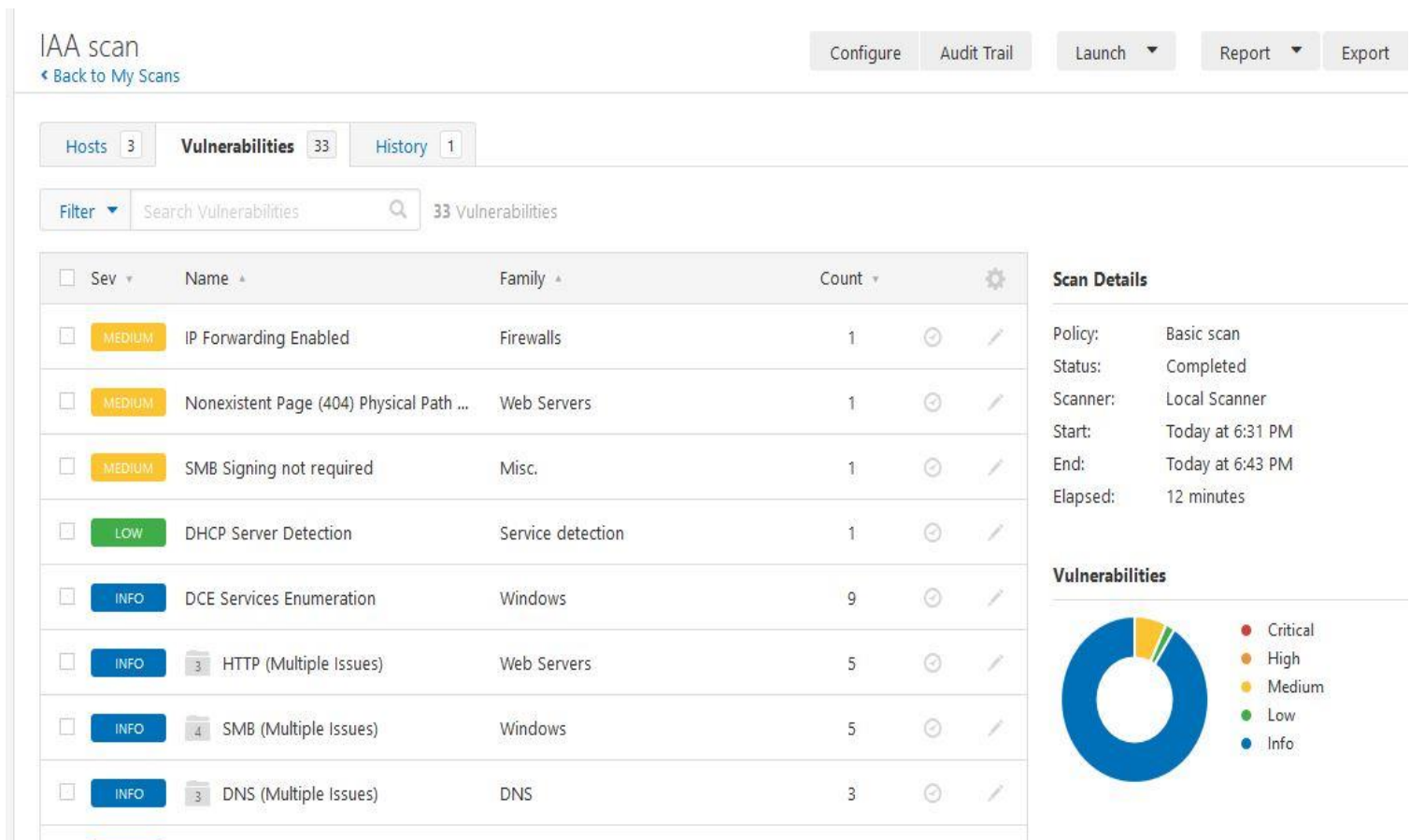


Figure 3.5 : Vulnerabilities.



Furthermore it gives possible solution for fix that issue and why it happens as in figure 3.6. Mostly due to human errors in developing a system or network. So with these informations dev teams can easily fix those issues before a 3<sup>rd</sup> party or Anonymous person will threat to a system or network.

IAA scan / Plugin #50686

[Back to Vulnerabilities](#)

Configure

Audit Trail

Launch ▼

Report ▼

Export ▼

Hosts 3

Vulnerabilities 33

History 1

MEDIUM IP Forwarding Enabled

Description

The remote host has IP forwarding enabled. An attacker can exploit this to route packets through the host and potentially bypass some firewalls / routers / NAC filtering.

Unless the remote host is a router, it is recommended that you disable IP forwarding.

Solution

On Linux, you can disable IP forwarding by doing :

```
echo 0 > /proc/sys/net/ipv4/ip_forward
```

On Windows, set the key 'IPEnableRouter' to 0 under

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters
```

On Mac OS X, you can disable IP forwarding by executing the command :

```
sysctl -w net.inet.ip.forwarding=0
```

For other systems, check with your vendor.

Plugin Details

Severity: Medium

ID: 50686

Version: 1.11

Type: remote

Family: Firewalls

Published: November 23, 2010

Modified: March 6, 2019

Risk Information

Risk Factor: Medium

CVSS Base Score: 5.8

CVSS Vector: CVSS2#AV:A/AC:L/Au:N/C:P/I:P/A:P

Reference Information

CVE: CVE-1999-0511

Figure 3.6 : issue and solution.

## References

- [1] Netcomp.com.au. 2020. *The Importance Of IT Auditing And Its Benefits – Netcomp Solutions*. [online] Available at: <<https://netcomp.com.au/blog/importance-it-auditing-and-its-benefits>> [Accessed 6 May 2020].
- [2] 2020. [online] Available at: <<https://www.youtube.com/watch?v=82x5C7Bd71U>> [Accessed 6 May 2020].
- [3] Atomi Systems, Inc. 2020. Elearning Authoring Software & Training Video Editor. [online] Available at: <<https://atomisystems.com/activepresenter/>> [Accessed 6 May 2020].