



## Chapter 5

# Vulnerability Assessment

Lab manual



**THIS DOCUMENT INCLUDES ADDITIONAL PRACTICALS WHICH  
MAY OR MAY NOT BE COVERED DURING CLASSROOM TRAINING.  
FOR MORE DETAILS APPROACH LAB COORDINATORS**

## INDEX

S. No.	Practical Name	Page No.
1	Performing vulnerability assessment using the Nessus Vulnerability Scanner	1

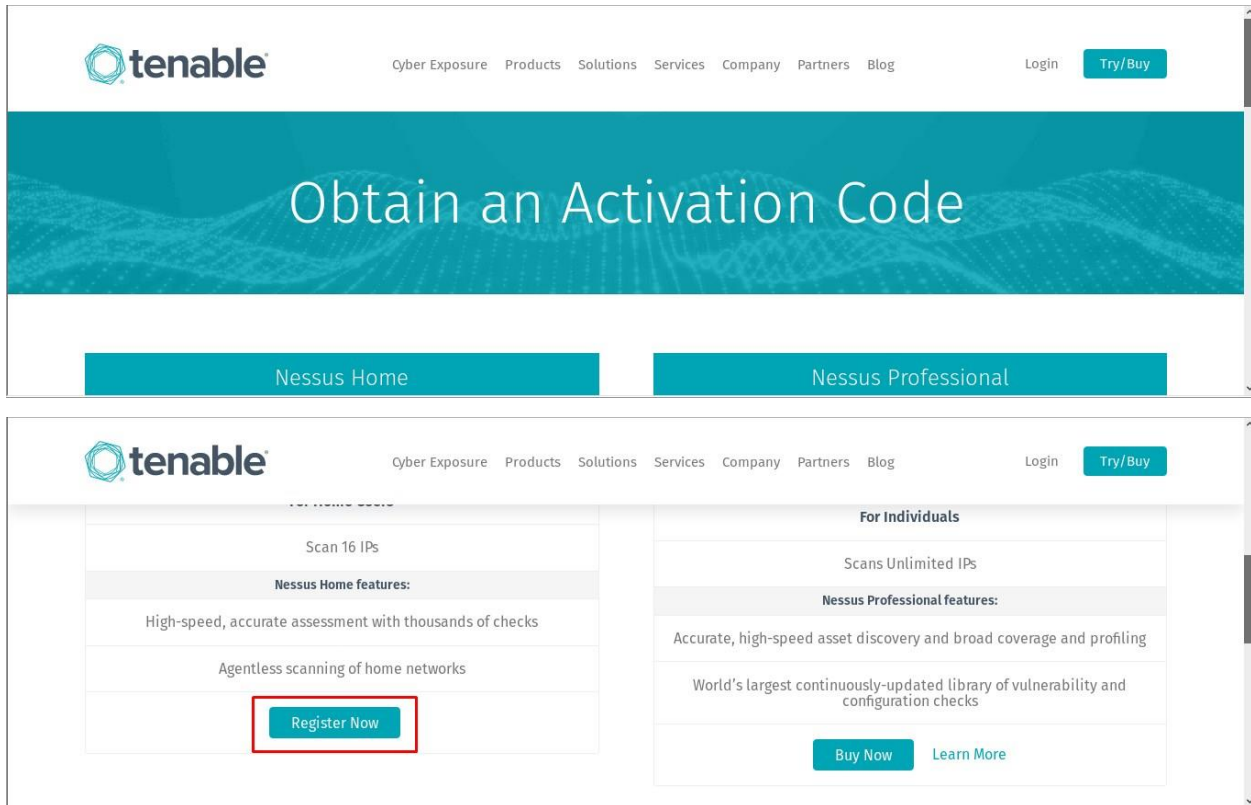
# Practical 1: Performing vulnerability assessment using the the Nessus Vulnerability Scanner.

## Step 1: Download and Install Nessus Vulnerability Scanner

Perform a simple google search to download Nessus Vulnerability Scanner or click on the following link

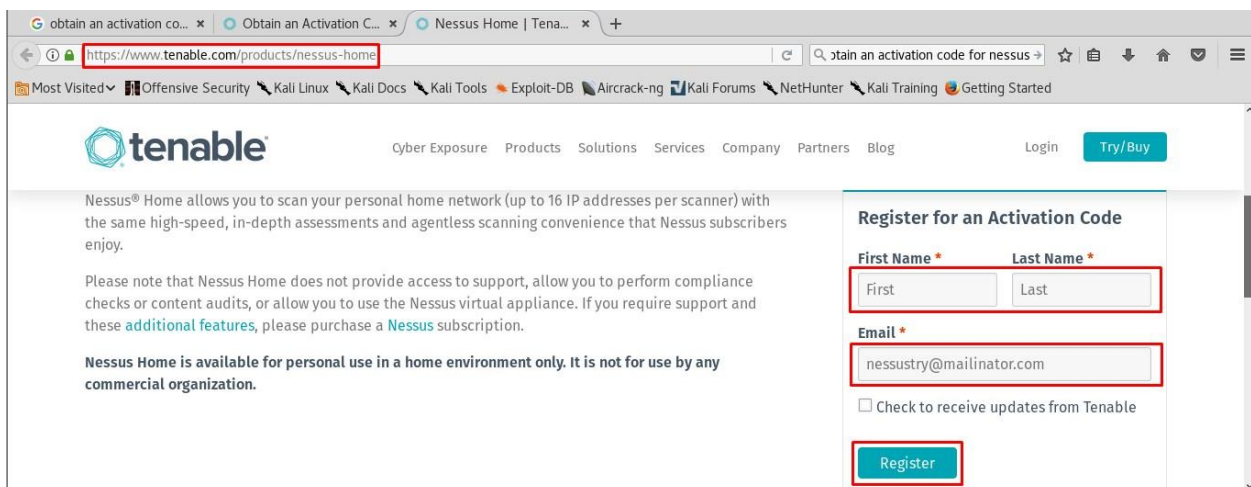
<https://www.tenable.com/products/nessus/activation-code>

Choose **Nessus Home** edition and click on register now.

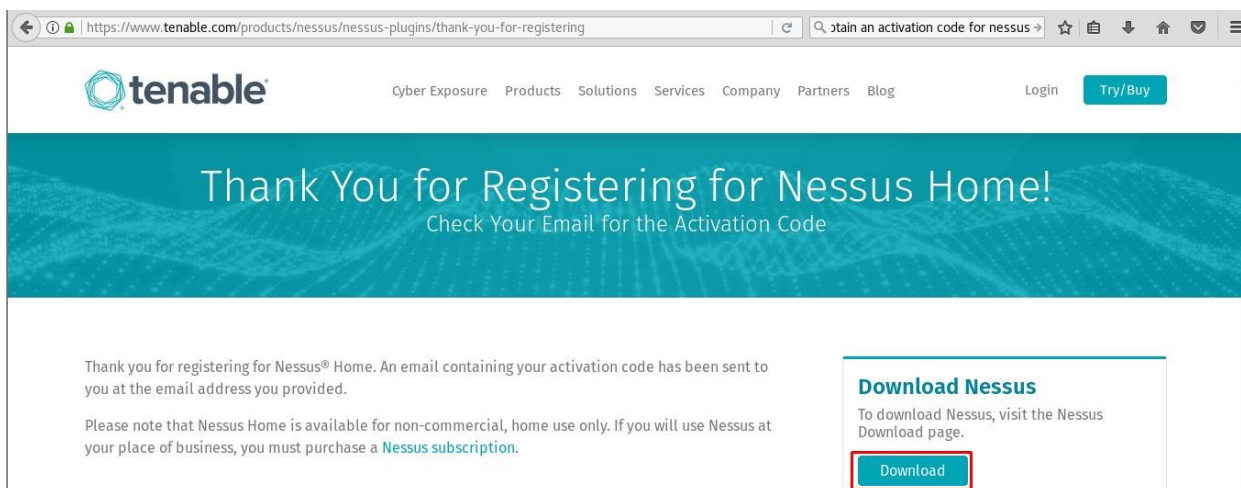


We will be redirected to the registration page, complete user registration and click **Register**.

**Note: Provide a valid email address (you will receive Nessus Activation Code).**



After registration, click on download.



Select Linux version **.deb package** (32-bit or 64-bit based on your machine compatibility). Click **Agree** to start the download.

Nessus-7.1.2-x64.msi	Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, 7, 8, 10, Server 2016 (64-bit)	<a href="#">Checksum</a>
Nessus-7.1.2-es5.x86_64.rpm	Red Hat ES 5 (64-bit) / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel)	<a href="#">Checksum</a>
Nessus-7.1.2-debian6_i386.deb	Debian 6, 7, 8, 9 / Kali Linux 1, 2017.3 i386(32-bit)	<a href="#">Checksum</a>
Nessus-7.1.2-Win32.msi	Windows 7, 8, 10 (32-bit)	<a href="#">Checksum</a>
Nessus-7.1.2.dmg	macOS (10.8 - 10.13)	<a href="#">Checksum</a>
Nessus-7.1.2-amzn.x86_64.rpm	Amazon Linux 2015.03, 2015.09, 2017.09	<a href="#">Checksum</a>
Nessus-7.1.2-debian6_amd64.deb	Debian 6, 7, 8, 9 / Kali Linux 1, 2017.3 AMD64	<a href="#">Checksum</a>
Nessus-7.1.2-es5.i386.rpm	Red Hat ES 5 i386(32-bit) / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel)	<a href="#">Checksum</a>
Nessus-7.1.2-es6.x86_64.rpm	Red Hat ES 6 (64-bit) / CentOS 6 / Oracle Linux 6	<a href="#">Checksum</a>

In the terminal, locate the **Downloads** directory and execute the following command.

**`dpkg -i Nessus-7.1.2-debian6_amd64.deb`**

```

root@kali: ~/Downloads
File Edit View Search Terminal Help
root@kali:~# cd Downloads
root@kali:~/Downloads# ls
Nessus-7.1.0-debian6_amd64.deb
root@kali:~/Downloads# dpkg -i Nessus-7.1.0-debian6_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 332952 files and directories currently installed.)
Preparing to unpack Nessus-7.1.0-debian6_amd64.deb ...
Unpacking nessus (7.1.0) ...
Setting up nessus (7.1.0) ...
Unpacking Nessus Core Components...

- You can start Nessus by typing /etc/init.d/nessusd start
- Then go to https://kali:8834/ to configure your scanner

Processing triggers for systemd (236-2) ...
root@kali:~/Downloads#
  
```

this command is used for installation of nessus

## Step 2: Nessus Configuration

Execute the following command to start Nessus

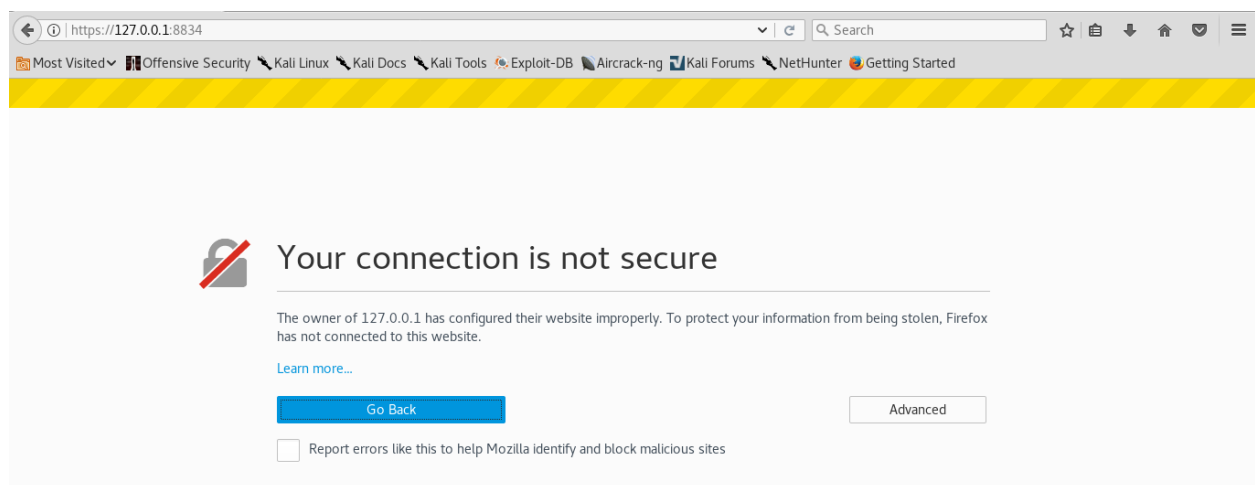
***/etc/init.d/nessusd start***

```
- You can start Nessus by typing /etc/init.d/nessusd start
- Then go to https://kali:8834/ to configure your scanner

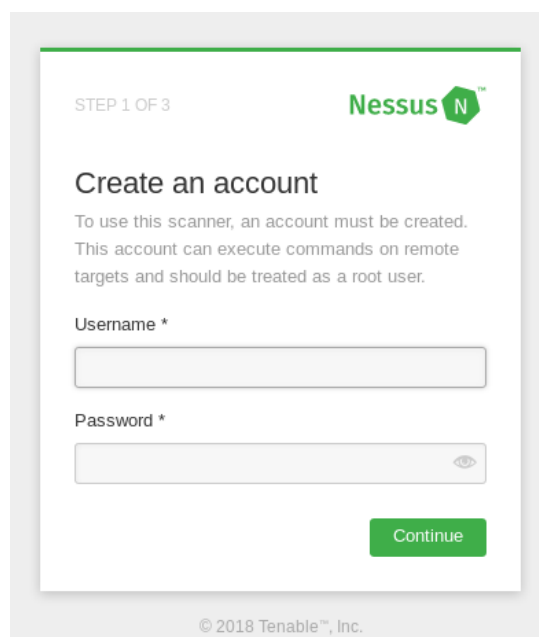
Processing triggers for systemd (236-2) ...
root@kali:~/Downloads# service nessusd start
root@kali:~/Downloads#
```

to start nessus, you can use any of these commands

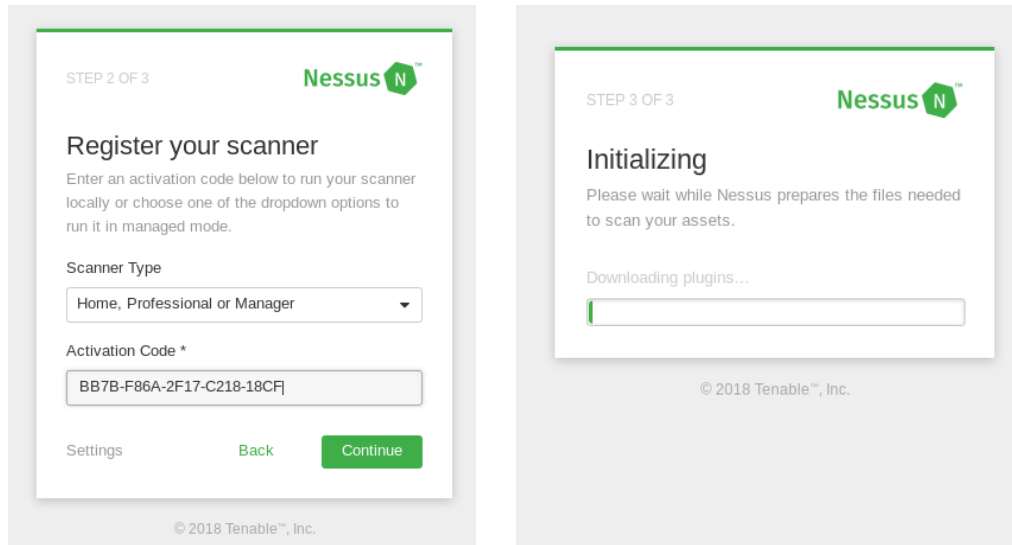
On browser open <https://127.0.0.1:8834/>



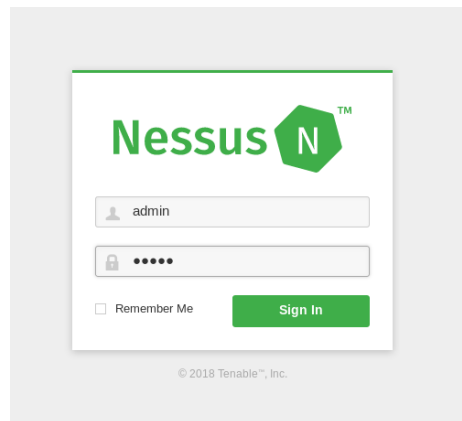
Click on **Advanced** and **Add Exceptions** to display Nessus login screen. Provide Username and Password (remember these credentials to Login to Nessus in future).



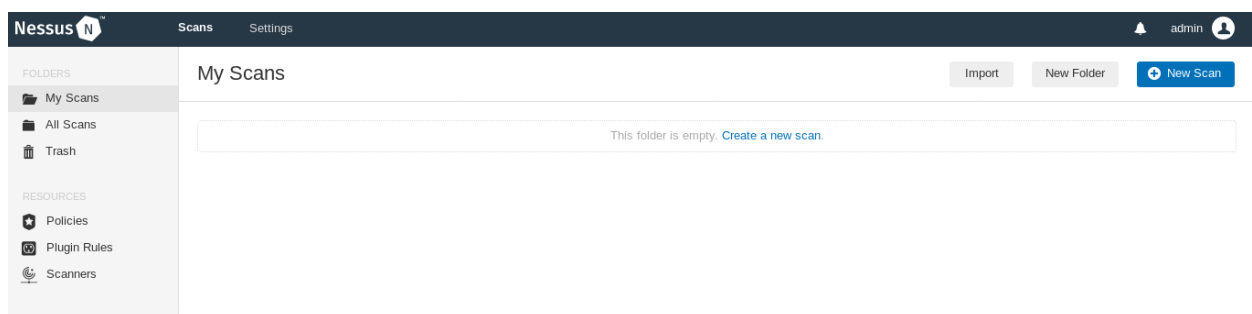
Enter **Activation Code** when prompted. Initialization process starts and takes some time to complete.



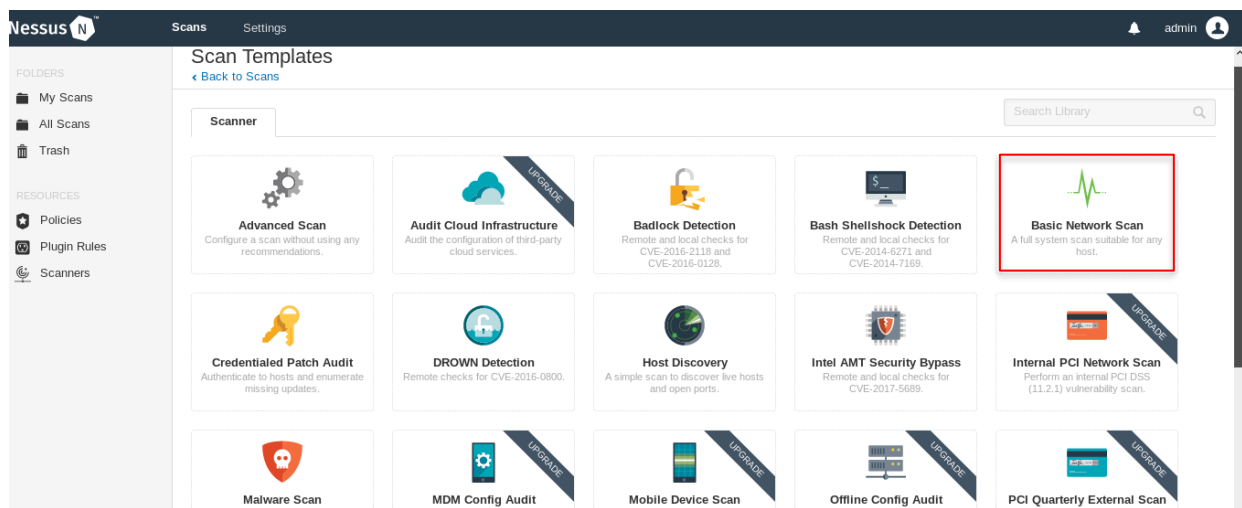
Once registration is done. We can Login to Nessus (using your credentials as created before).



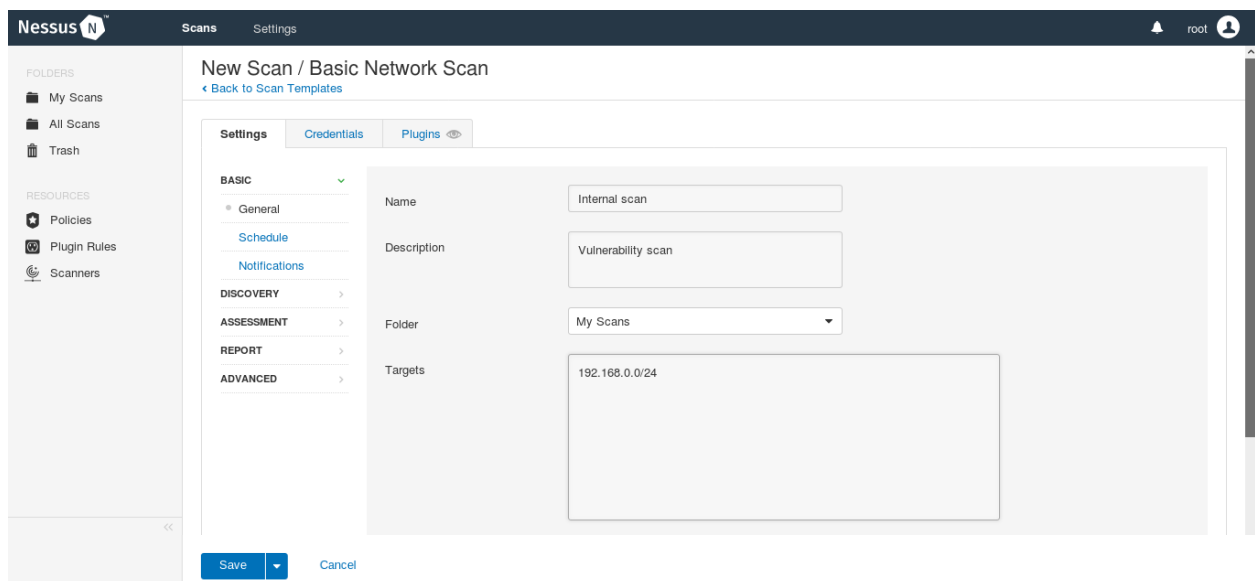
To perform a vulnerability scan, click on **New Scan** on the top-right corner of the Nessus interface.



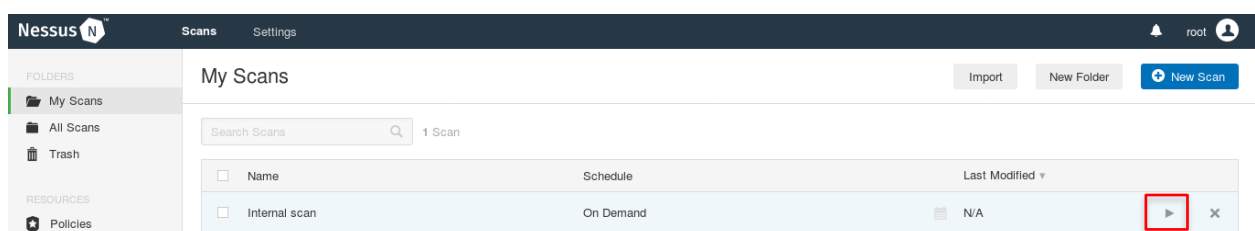
Select the type of scan that we are intended to perform on the target machine. In this case, let us choose **Basic Network Scan**.



Provide the necessary details (Name of your scan, IP address of the target are mandatory) and save the profile.



We can see that the scan name is listed under **My Scans** tab. Click on the play button to start the scan.



Click on the scan to view identified vulnerabilities

Nessus Scans Settings

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Scanners

Filter Search Vulnerabilities 93 Vulnerabilities

Sev	Name	Family	Count
CRITICAL	Microsoft Windows SMBv1 Multiple Vulnerabilities	Windows	1
CRITICAL	Microsoft Windows/Exchange SMTP DNS Lookup Ove...	SMTP problems	1
CRITICAL	MS11-030: Vulnerability in DNS Resolution Could Allow...	Windows	1
HIGH	Service Detection (HELP Request)	Service detection	3
MEDIUM	SSL Certificate Cannot Be Trusted	General	3
MEDIUM	SSL Self-Signed Certificate	General	2
MEDIUM	Unencrypted Telnet Server	Misc.	2

**Scan Details**

Name: Internal scan  
 Status: Completed  
 Policy: Basic Network Scan  
 Scanner: Local Scanner  
 Start: Today at 6:06 PM  
 End: Today at 6:27 PM  
 Elapsed: 21 minutes

**Vulnerabilities**

Click on those vulnerabilities for detailed information regarding the risk.

Nessus Scans Settings

Internal scan / Plugin #15464

Configure Audit Trail Launch Export

Vulnerabilities 33

**CRITICAL** Microsoft Windows/Exchange SMTP DNS Lookup Overflow (885881)

**Description**

The remote host is running a version of Microsoft SMTP server which fails to validate DNS response data. An attacker can exploit this flaw to execute arbitrary code subject to the privileges of the SMTP application server process.

**Solution**

Apply the bulletin referenced above.

**Plugin Details**

Severity: Critical  
 ID: 15464  
 Version: \$Revision: 1.18 \$  
 Type: remote  
 Family: SMTP problems  
 Published: October 12, 2004  
 Modified: August 30, 2017

To document the results, click on the **export** button located on the top right corner.