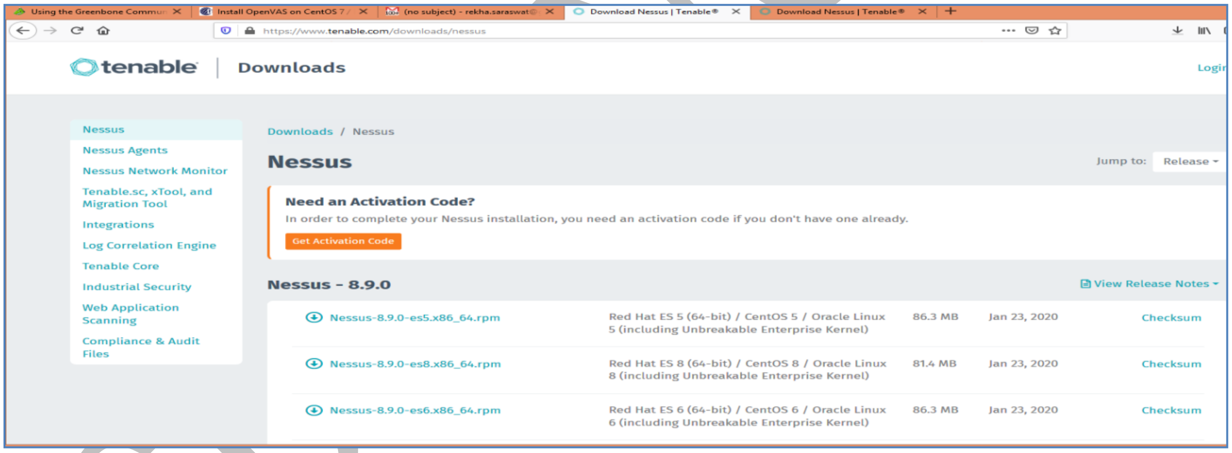
Network vulnerability scanning using NESSUS

NESSUS is a proprietary vulnerability scanner developed by Tenable, Inc It is a commercial tool. But a free version is available with limited set of capabilities to scan maximum 20 machines per user. It is a remote security scanning tool which scans a system and raises alert when it discovers any vulnerabilities which malicious hackers can use to gain access to any system connected to networks.

Download and installation:

1. Download NESSUS from https://www.tenable.com/downloads/nessus.
2. Download latest release available for windows 64
   It is supports Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, 7, 8, 10, Server 2016 (64-bit).
3. An activation code is also required to make NESSUS work after installation. Get activation code by clicking on GET ACTIVATION CODE on the download page (or by browsing https://www.tenable.com/products/nessus/activation-code)

   It requires registration. After registration the activation code is sent to the registered email id.



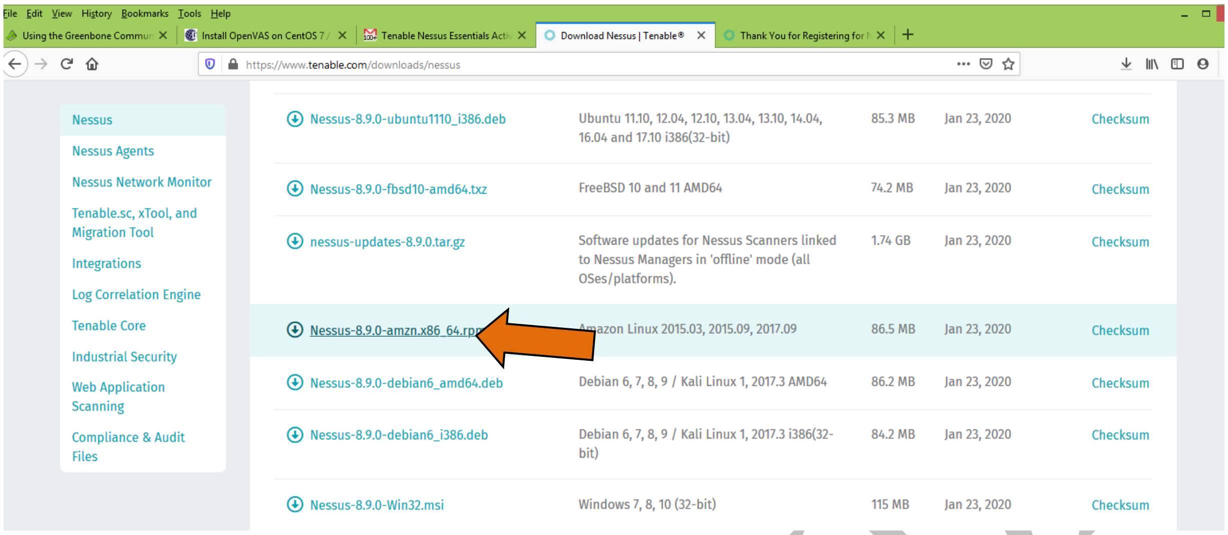
Nessus

Need an Activation Code?

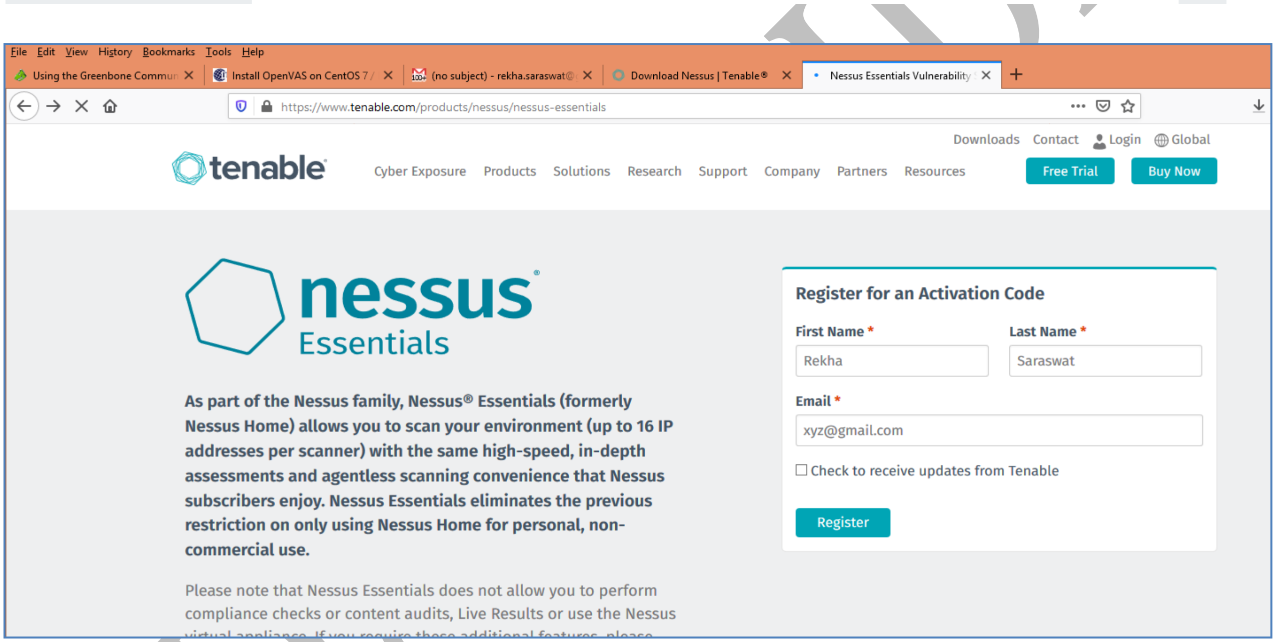
In order to complete your Nessus installation, you need an activation code if you don't have one already.

Nessus - 8.9.0

Nessus-8.9.0-es5.x86_64.rpm	Red Hat ES 5 (64-bit) / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel)	86.3 MB	Jan 23, 2020	Checksum
Nessus-8.9.0-es8.x86_64.rpm	Red Hat ES 8 (64-bit) / CentOS 8 / Oracle Linux 8 (including Unbreakable Enterprise Kernel)	81.4 MB	Jan 23, 2020	Checksum
Nessus-8.9.0-es6.x86_64.rpm	Red Hat ES 6 (64-bit) / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel)	86.3 MB	Jan 23, 2020	Checksum


File Edit View History Bookmarks Tools Help
Using the Greenbone Commun
Install OpenVAS on CentOS 7
Tenable Nessus Essentials Acti
Download Nessus | Tenable®
Thank You for Registering for
https://www.tenable.com/downloads/nessus
Nessus
Nessus Agents
Nessus Network Monitor
Tenable.sc, xTool, and Migration Tool
Integrations
Log Correlation Engine
Tenable Core
Industrial Security
Web Application Scanning
Compliance & Audit Files

Nessus-8.9.0-ubuntu1110_i386.deb	Ubuntu 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 16.04 and 17.10 i386(32-bit)	85.3 MB	Jan 23, 2020	Checksum
Nessus-8.9.0-fbsd10-amd64.txz	FreeBSD 10 and 11 AMD64	74.2 MB	Jan 23, 2020	Checksum
nessus-updates-8.9.0.tar.gz	Software updates for Nessus Scanners linked to Nessus Managers in 'offline' mode (all OSes/platforms).	1.74 GB	Jan 23, 2020	Checksum
Nessus-8.9.0-amzn.x86_64.rpm	Amazon Linux 2015.03, 2015.09, 2017.09	86.5 MB	Jan 23, 2020	Checksum
Nessus-8.9.0-debian6_amd64.deb	Debian 6, 7, 8, 9 / Kali Linux 1, 2017.3 AMD64	86.2 MB	Jan 23, 2020	Checksum
Nessus-8.9.0-debian6_i386.deb	Debian 6, 7, 8, 9 / Kali Linux 1, 2017.3 i386(32-bit)	84.2 MB	Jan 23, 2020	Checksum
Nessus-8.9.0-Win32.msi	Windows 7, 8, 10 (32-bit)	115 MB	Jan 23, 2020	Checksum


File Edit View History Bookmarks Tools Help
Using the Greenbone Commun
Install OpenVAS on CentOS 7
(no subject) - rekha.saraswat@
Download Nessus | Tenable®
Nessus Essentials Vulnerability
https://www.tenable.com/products/nessus/nessus-essentials
Downloads
Contact
Login
Global
tenable
Cyber Exposure
Products
Solutions
Research
Support
Company
Partners
Resources
Free Trial
Buy Now
nessus
Essentials

As part of the Nessus family, Nessus® Essentials (formerly Nessus Home) allows you to scan your environment (up to 16 IP addresses per scanner) with the same high-speed, in-depth assessments and agentless scanning convenience that Nessus subscribers enjoy. Nessus Essentials eliminates the previous restriction on only using Nessus Home for personal, non-commercial use.

Please note that Nessus Essentials does not allow you to perform compliance checks or content audits, Live Results or use the Nessus virtual appliance. If you require these additional features, please

Register for an Activation Code

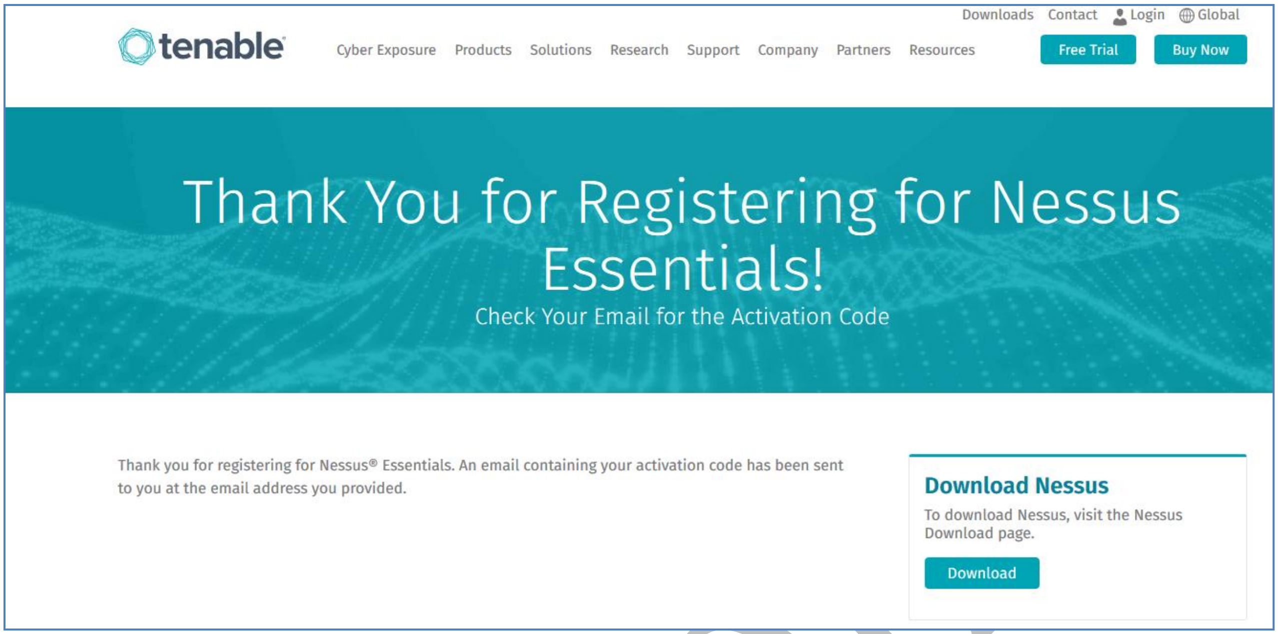
First Name * Rekha

Last Name * Saraswat

Email * xyz@gmail.com

☐ Check to receive updates from Tenable

Register



Thank You for Registering for Nessus Essentials!

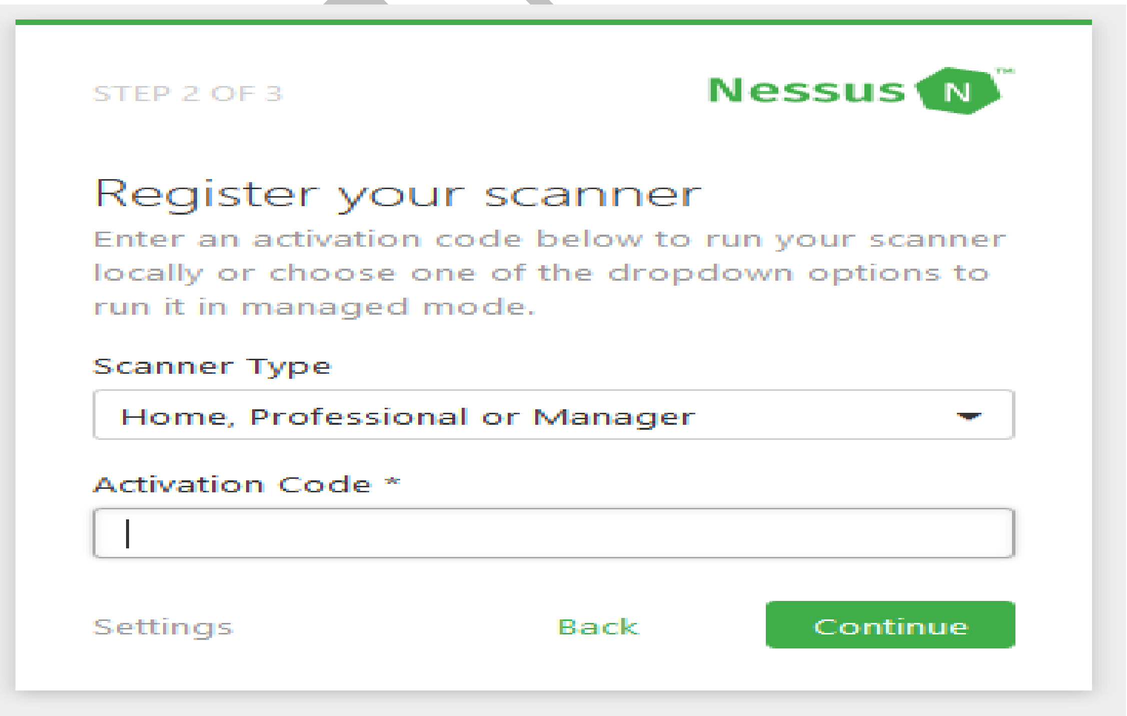
Check Your Email for the Activation Code

Thank you for registering for Nessus® Essentials. An email containing your activation code has been sent to you at the email address you provided.

Download Nessus

To download Nessus, visit the Nessus Download page.

4. Windows executable file is downloaded, which can be installed in one click.
5. After installation, web client starts with url: https://127.0.0.1:8834
6. Provide userid and password for account creation.
7. Copy activation code, received on email.



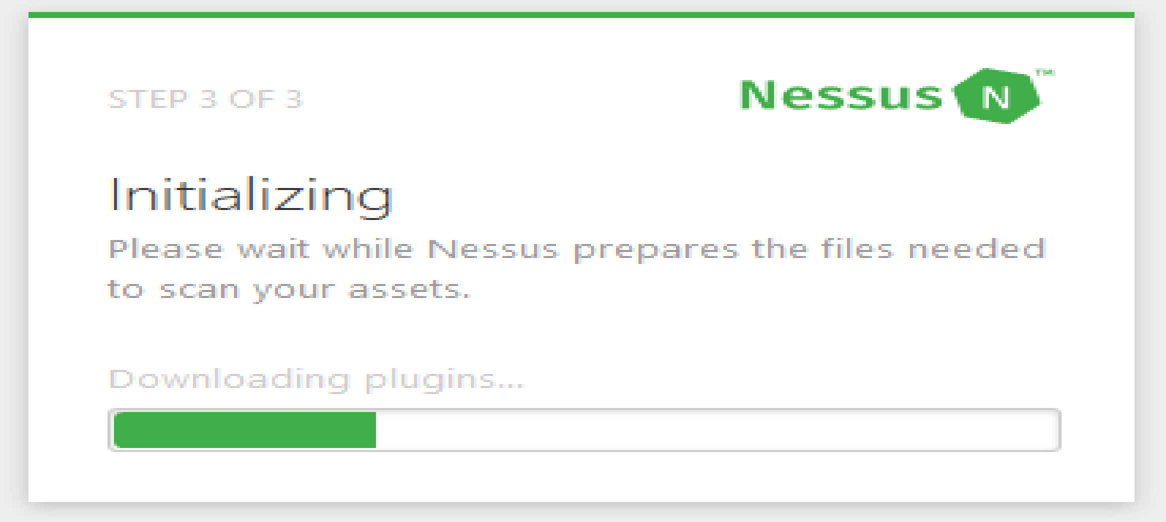
Register your scanner

Enter an activation code below to run your scanner locally or choose one of the dropdown options to run it in managed mode.

Scanner Type: Home, Professional or Manager

Activation Code *

8. Nessus completes setup and starts downloading plug-ins and initializes. This may take some time.



STEP 3 OF 3

Initializing

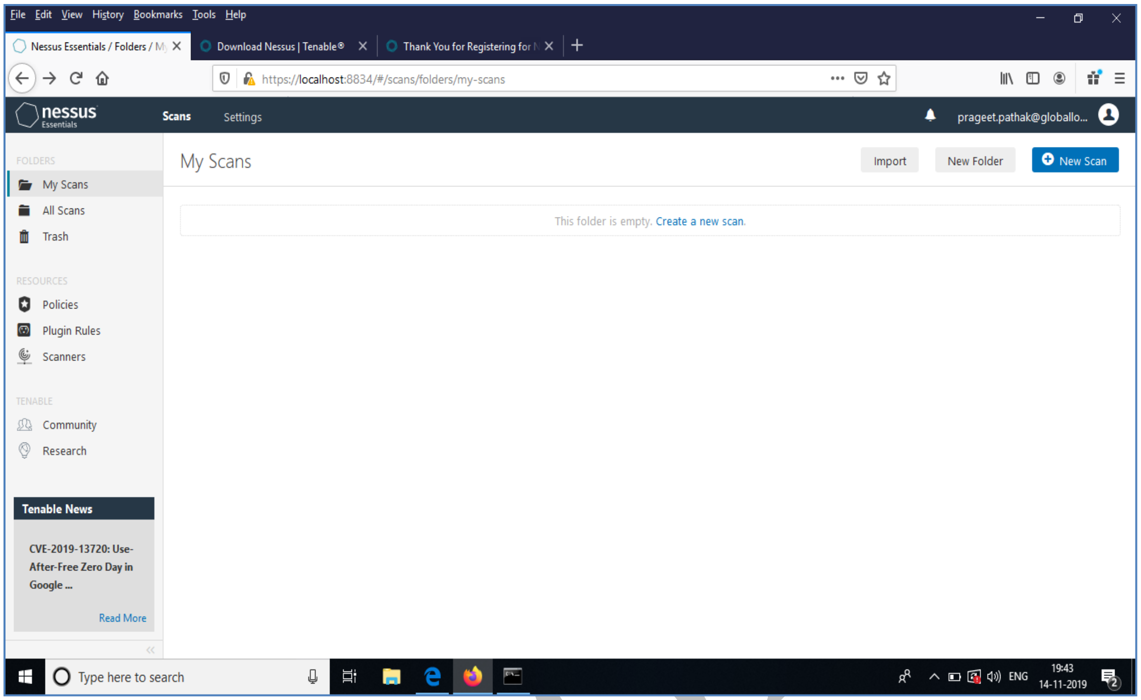
Please wait while Nessus prepares the files needed to scan your assets.

Downloading plugins...

9.After initialization, the nessus webclient must open in web browser. Sometimes the " Secure Connection error" may come. To resolve this error, open nessus in private window of your browser.

Scanning hosts with NESSUS:

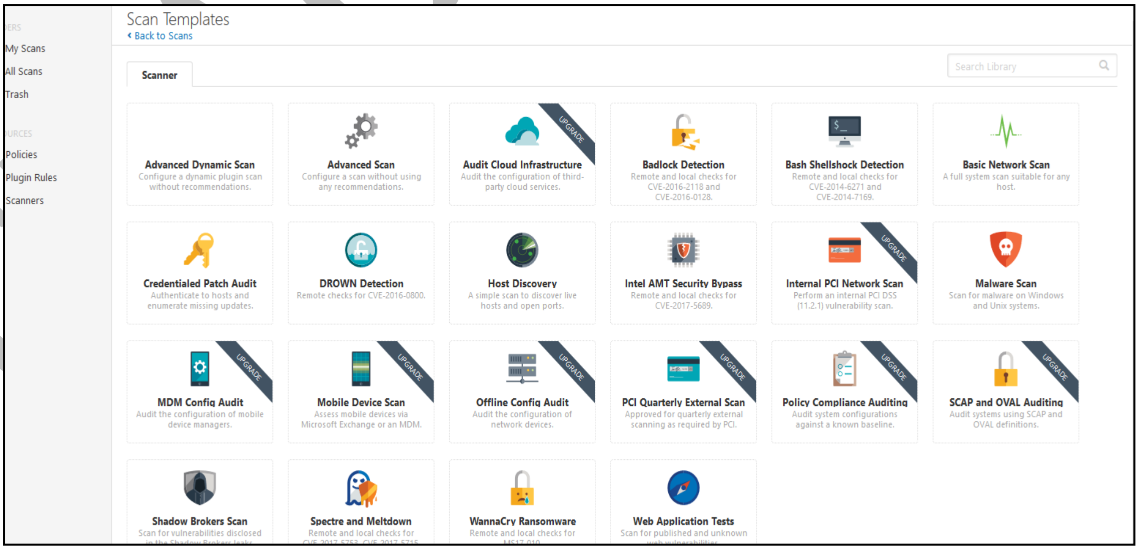
1. Once you have installed and launched Nessus, you're ready to start scanning. The home page ,when nessus starts.
2. First, you have to create a scan. To create your scan:
3. In the top navigation bar, click Scans.
4. In the upper-right corner of the My Scans page, click the New Scan button.



This folder is empty. Create a new scan.

CVE-2019-13720: Use-After-Free Zero Day in Google ...

5. Click on **new scan** to create a new scan task. Next, click the scan template you want to use. Here we use Basic Network Scan which performs a full system scan that is suitable for any host. Use this template to scan an asset, for example, you can perform an internal vulnerability scan on your systems.



Advanced Dynamic Scan Configure a dynamic plugin scan without recommendations.

Advanced Scan Configure a scan without using any recommendations.

Audit Cloud Infrastructure Audit the configuration of third-party cloud services.

Badlock Detection Remote and local checks for CVE-2016-2118 and CVE-2016-0128.

Bash Shellshock Detection Remote and local checks for CVE-2014-6271 and CVE-2014-7169.

Basic Network Scan A full system scan suitable for any host.

Credentialed Patch Audit Authenticate to hosts and enumerate missing updates.

DROWN Detection Remote checks for CVE-2016-0800.

Host Discovery A simple scan to discover live hosts and open ports.

Intel AMT Security Bypass Remote and local checks for CVE-2017-5689.

Internal PCI Network Scan Perform an internal PCI DSS (11.2.1) vulnerability scan.

Malware Scan Scan for malware on Windows and Unix systems.

MDM Config Audit Audit the configuration of mobile device managers.

Mobile Device Scan Assess mobile devices via Microsoft Exchange or an MDM.

Offline Config Audit Audit the configuration of network devices.

PCI Quarterly External Scan Approved for quarterly external scanning as required by PCI.

Policy Compliance Auditing Audit system configurations against a known baseline.

SCAP and OVAL Auditing Audit systems using SCAP and OVAL definitions.

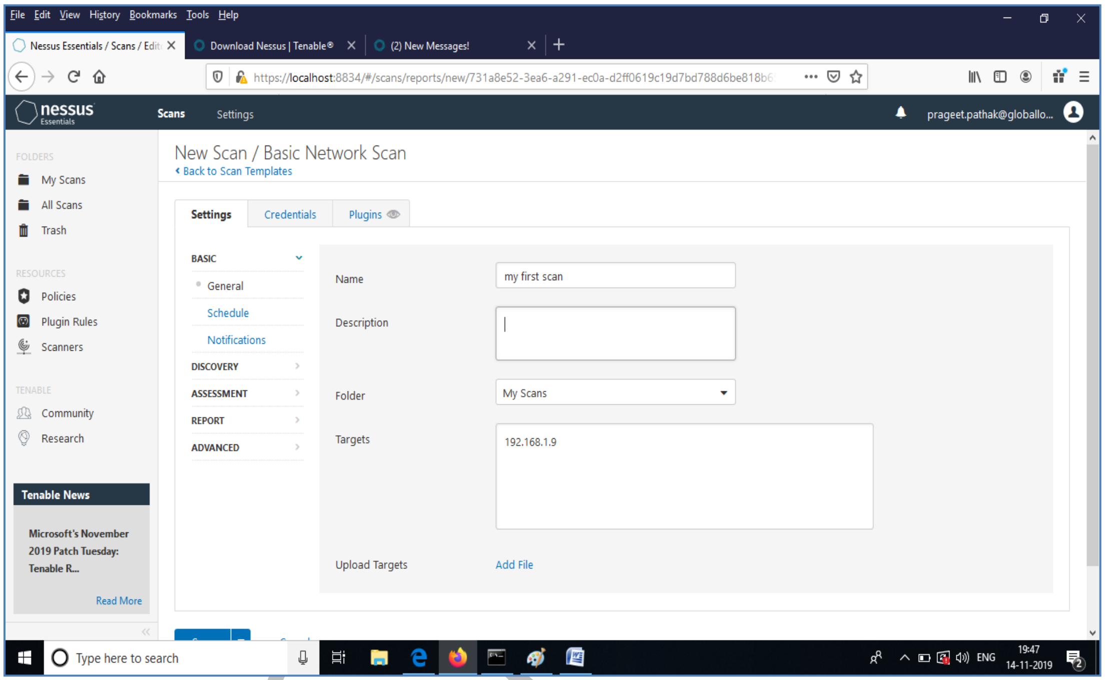
Shadow Brokers Scan Scan for vulnerabilities disclosed in the Shadow Brokers leaks

Spectre and Meltdown Remote and local checks for CVE-2017-5753, CVE-2017-5715

WannaCry Ransomware Remote and local checks for MS17-010

Web Application Tests Scan for published and unknown web vulnerabilities

6. Click on desired scan type. (The following screenshots are for Basic Network Scan). Prepare your scan by configuring the settings available for your chosen template. The Basic Network Scan template has several default settings preconfigured, which allows you to quickly perform your first scan and view results without a lot of effort. Specify the name of scan and the targets. There may be a single target or a range of targets in a CIDR notation. After Specifying the name of scan and the target IP.



New Scan / Basic Network Scan

Settings — BASIC — General

Name: my first scan

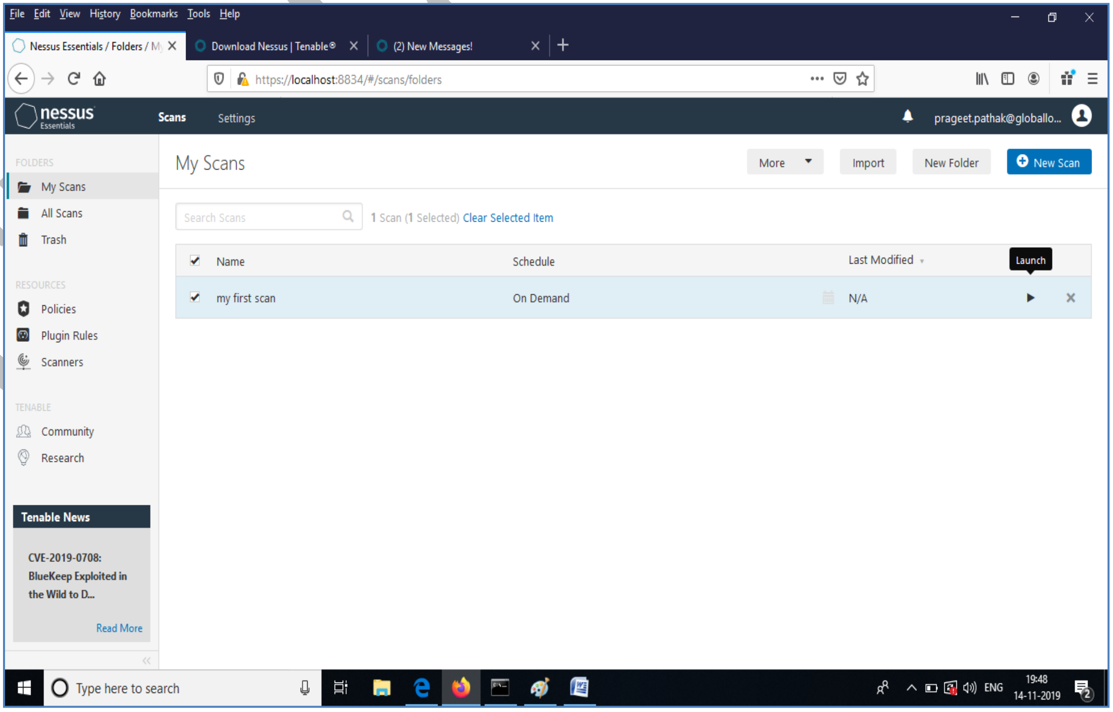
Description:

Folder: My Scans

Targets: 192.168.1.9

Upload Targets: Add File

7. Click on Save. The next page will be following.

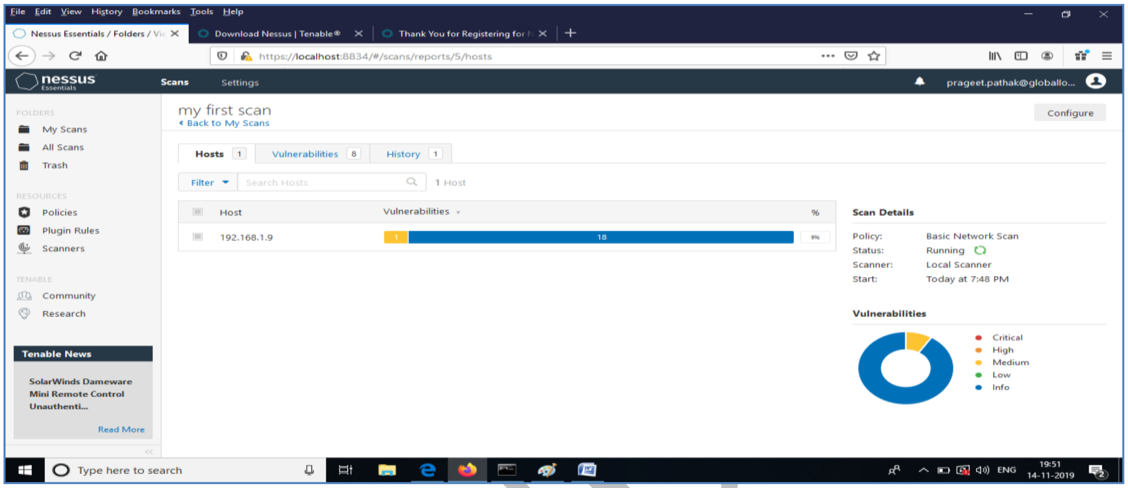


My Scans

1 Scan (1 Selected) Clear Selected Item

☑	Name	Schedule	Last Modified
☑	my first scan	On Demand	N/A

8. Click on blue arrow button to launch the scan.
9. Scan starts. The time it takes to complete a scan involves many factors, such as network speed and congestion, so the scan may take some time to run.



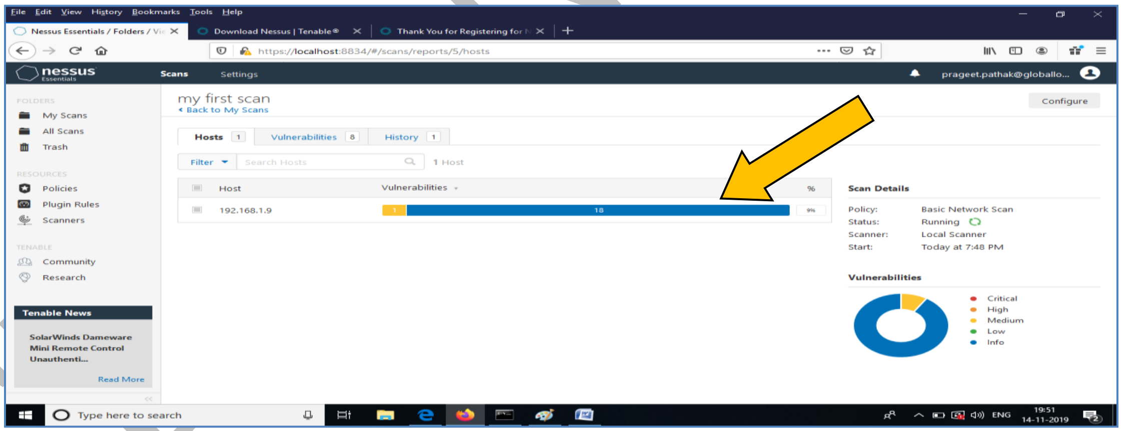
Host	Vulnerabilities	%
192.168.1.9	1 18	9%

Scan Details

Policy: Basic Network Scan
Status: Running
Scanner: Local Scanner
Start: Today at 7:48 PM

Vulnerabilities

10. By clicking on Vulnerabilities (Bar), the details of vulnerabilities can be found. Viewing scan results by vulnerabilities gives you a view into potential risks on your assets.

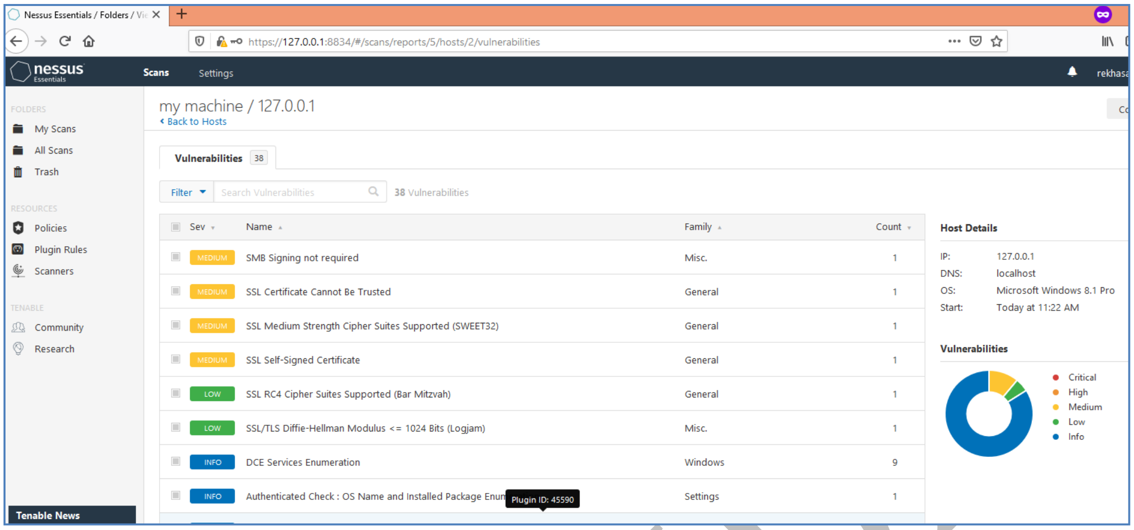


Host	Vulnerabilities	%
192.168.1.9	1 18	9%

Scan Details

Policy: Basic Network Scan
Status: Running
Scanner: Local Scanner
Start: Today at 7:48 PM

Vulnerabilities



my machine / 127.0.0.1

‹ Back to Hosts

Vulnerabilities 38

38 Vulnerabilities

Sev	Name	Family	Count
MEDIUM	SMB Signing not required	Misc.	1
MEDIUM	SSL Certificate Cannot Be Trusted	General	1
MEDIUM	SSL Medium Strength Cipher Suites Supported (SWEET32)	General	1
MEDIUM	SSL Self-Signed Certificate	General	1
LOW	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	General	1
LOW	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Misc.	1
INFO	DCE Services Enumeration	Windows	9
INFO	Authenticated Check : OS Name and Installed Package Enum	Settings	1

Host Details

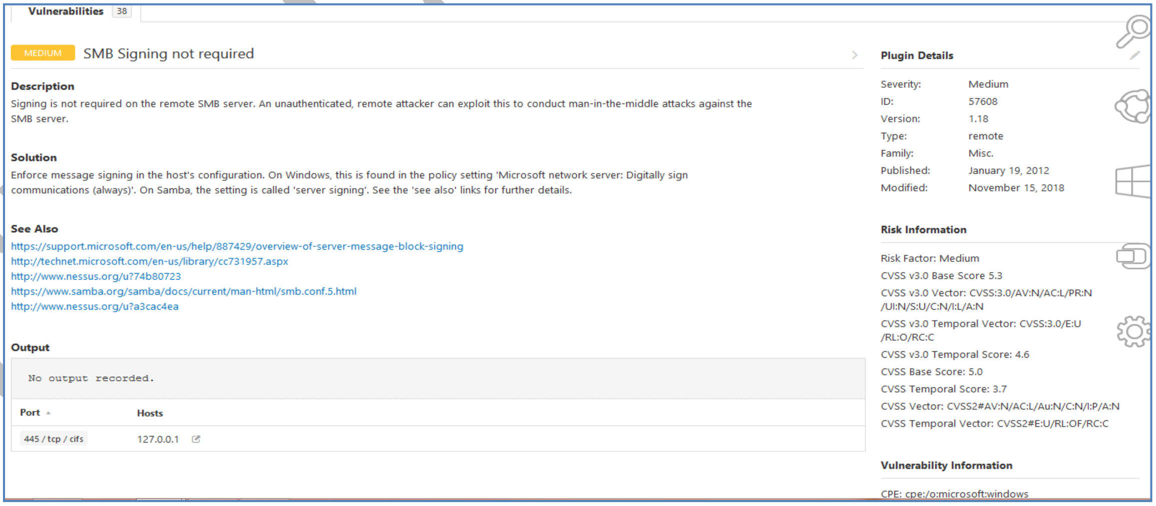
IP:	127.0.0.1
DNS:	localhost
OS:	Microsoft Windows 8.1 Pro
Start:	Today at 11:22 AM

Vulnerabilities

- ● Critical
- ● High
- ● Medium
- ● Low
- ● Info

11. By clicking on any vulnerability details can be obtained.
12. To view vulnerabilities:

    Do one of the following:
13. Click a specific host to view vulnerabilities found on that host.
14. Click the Vulnerabilities tab to view all vulnerabilities.
15. (Optional) To sort the vulnerabilities, click an attribute in the table header row to sort by that attribute.
16. Clicking on the vulnerability row will open the vulnerability details page, displaying plugin information and output for each instance on a host.


Vulnerabilities 38

MEDIUM SMB Signing not required

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

See Also

https://support.microsoft.com/en-us/help/887429/overview-of-server-message-block-signing
http://technet.microsoft.com/en-us/library/cc731957.aspx
http://www.nessus.org/u?74b80723
https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html
http://www.nessus.org/u?a3cac4ea

Output

```
No output recorded.
```

Port	Hosts
445 / tcp / cifs	127.0.0.1

Plugin Details

Severity:	Medium
ID:	57608
Version:	1.18
Type:	remote
Family:	Misc.
Published:	January 19, 2012
Modified:	November 15, 2018

Risk Information

Risk Factor: Medium
CVSS v3.0 Base Score 5.3
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C
CVSS v3.0 Temporal Score: 4.6
CVSS Base Score: 5.0
CVSS Temporal Score: 3.7
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N
CVSS Temporal Vector: CVSS2#E:U/RL:OF/RC:C

Vulnerability Information

CPE: cpe:/o:microsoft:windows