VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Information Security Management
CSE3502

Lab Assignment 1
Nessus and Information Security Policies

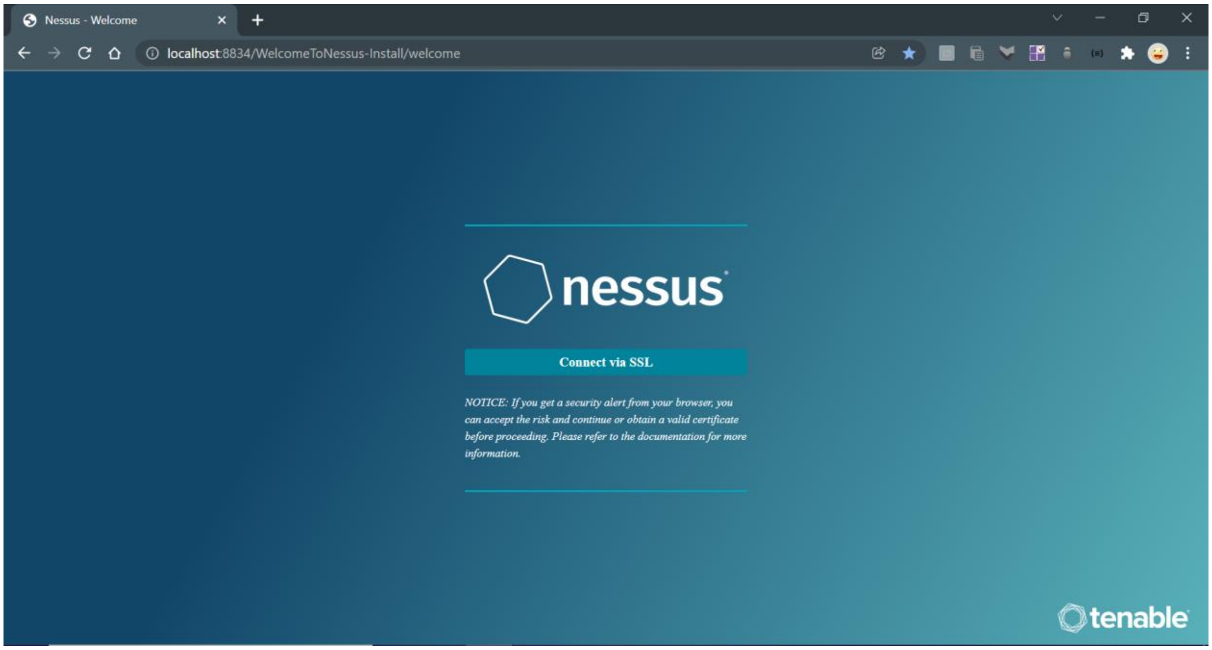
Slot : L25+L26

Name : Kulvir Singh

Register Number : 19BCE2074

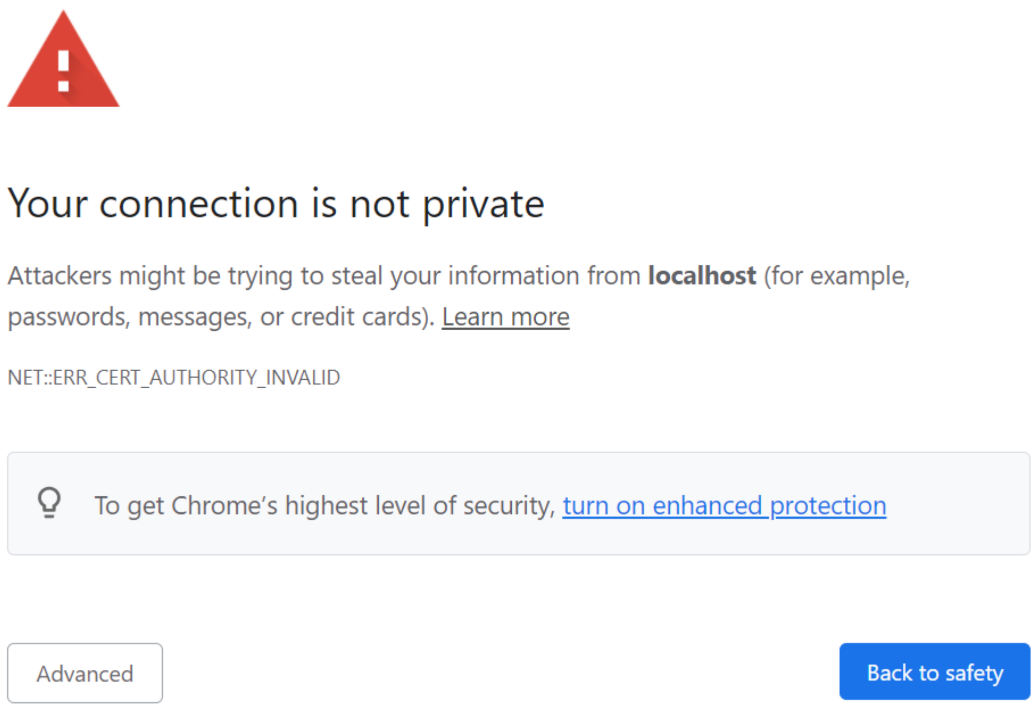
Experiment 1 : Nessus

Nessus Installation page :



NOTICE: If you get a security alert from your browser, you can accept the risk and continue or obtain a valid certificate before proceeding. Please refer to the documentation for more information.

Accepting the non-private connection :



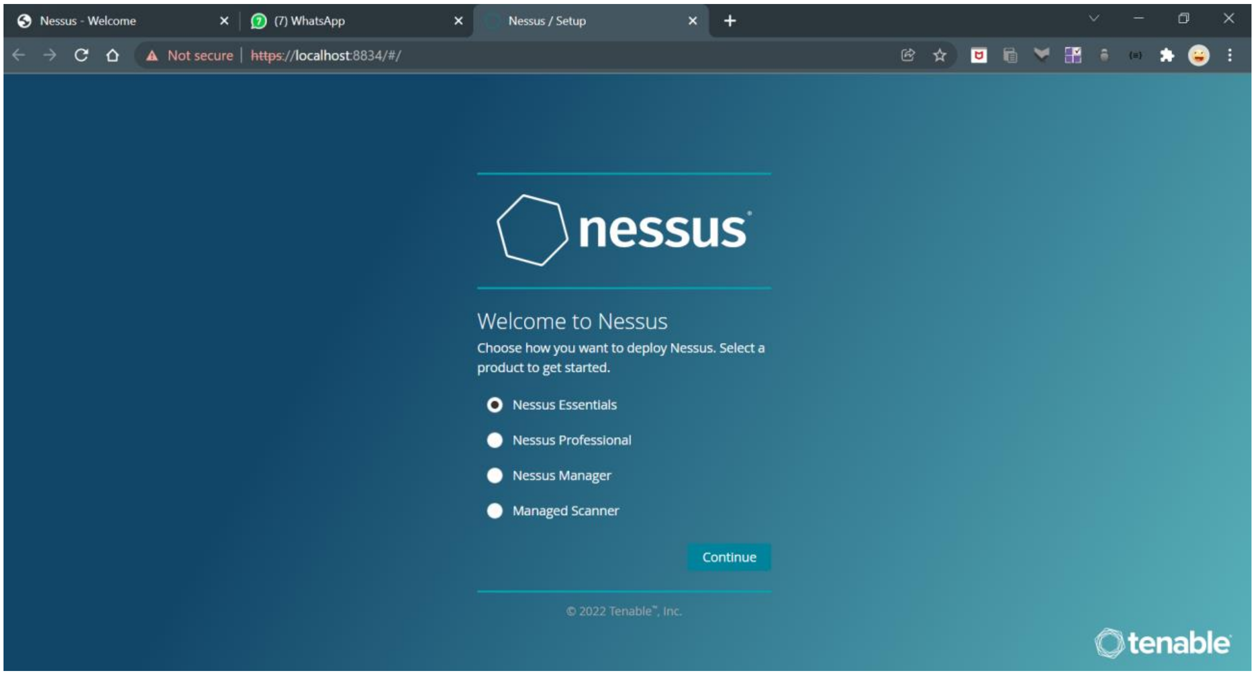
Your connection is not private

Attackers might be trying to steal your information from **localhost** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

To get Chrome's highest level of security, turn on enhanced protection

Installing nessus essentials



Welcome to Nessus

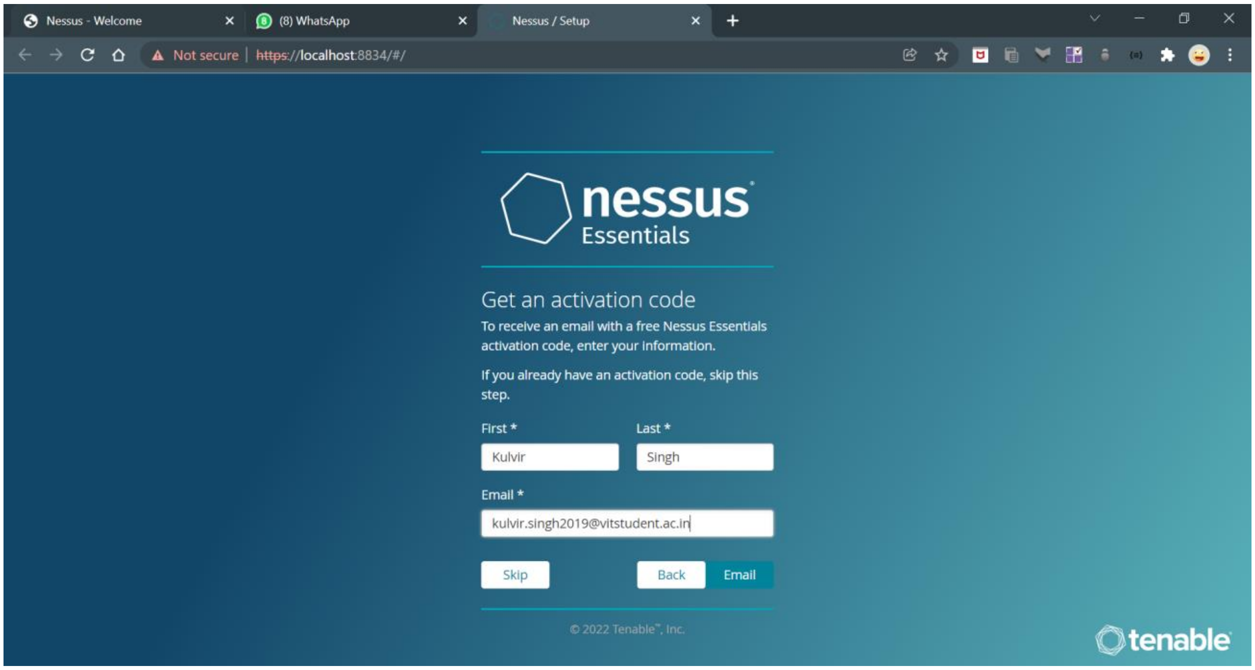
Choose how you want to deploy Nessus. Select a product to get started.

- ● Nessus Essentials
- ○ Nessus Professional
- ○ Nessus Manager
- ○ Managed Scanner

Continue

© 2022 Tenable™, Inc.

Setting up nessus



Get an activation code

To receive an email with a free Nessus Essentials activation code, enter your information.

If you already have an activation code, skip this step.

First * Kulvir

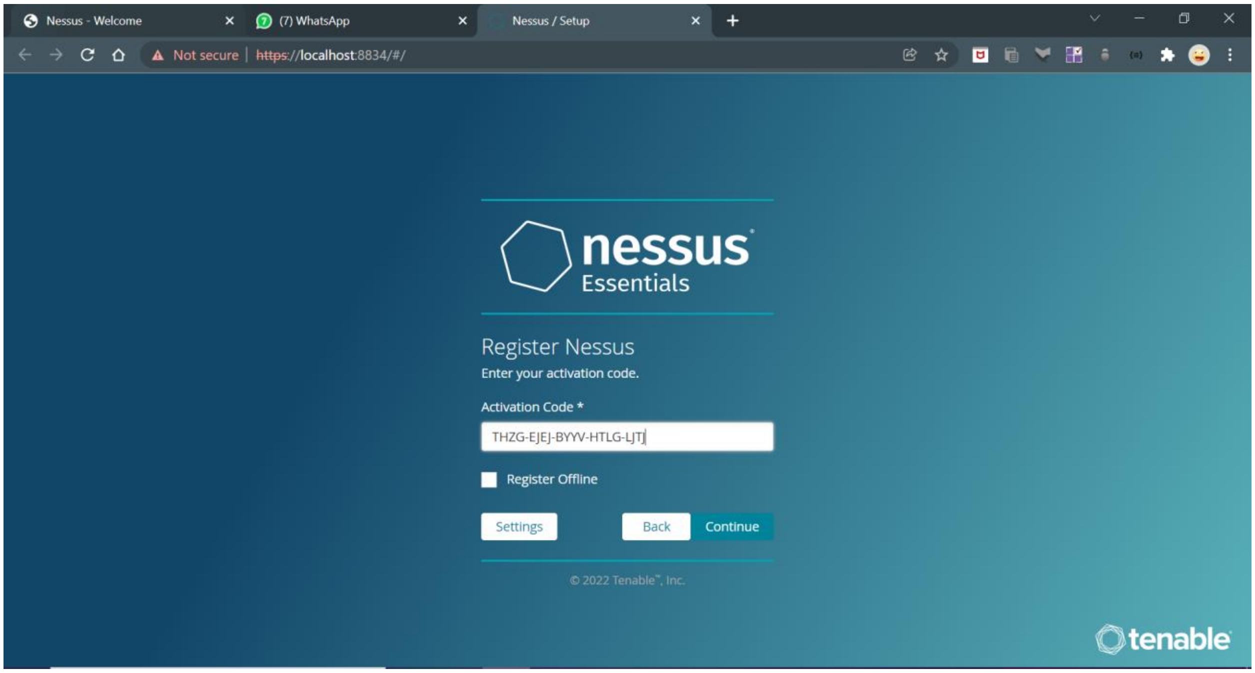
Last * Singh

Email * kulvir.singh2019@vitstudent.ac.in

Skip Back Email

© 2022 Tenable™, Inc.

Registering nessus



Register Nessus

Enter your activation code.

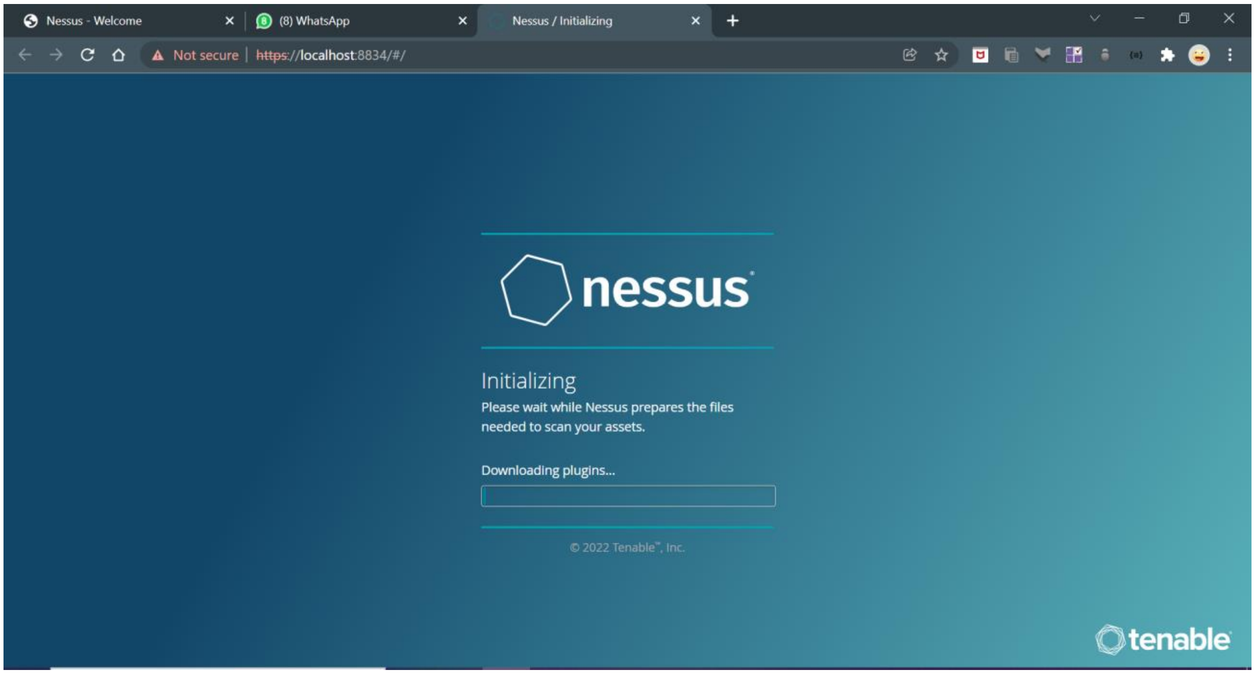
Activation Code *

THZG-EJEJ-BYVV-HTLG-LJTJ

□ Register Offline

© 2022 Tenable™, Inc.

Initialization :



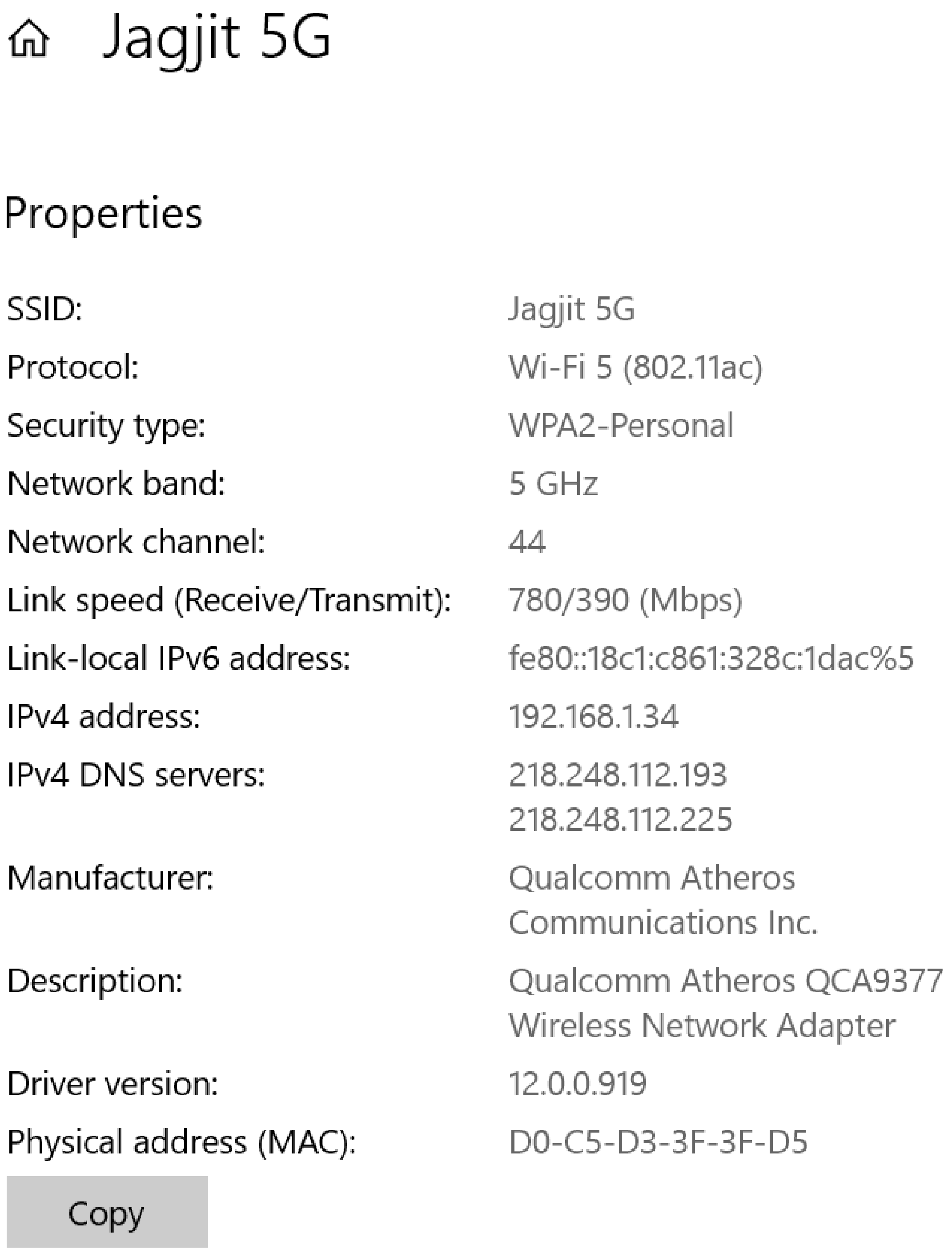
Initializing

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

Downloading plugins...

© 2022 Tenable™, Inc.

My Network IP address

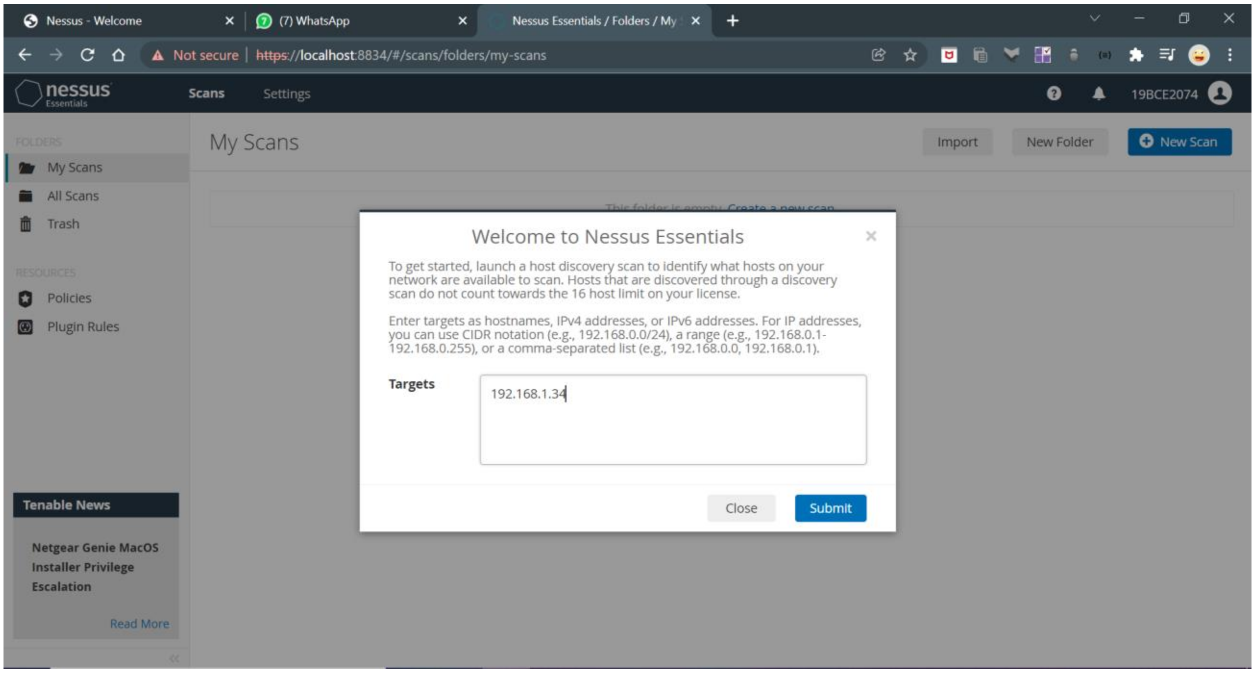


Jagjit 5G

Properties

SSID:	Jagjit 5G
Protocol:	Wi-Fi 5 (802.11ac)
Security type:	WPA2-Personal
Network band:	5 GHz
Network channel:	44
Link speed (Receive/Transmit):	780/390 (Mbps)
Link-local IPv6 address:	fe80::18c1:c861:328c:1dac%5
IPv4 address:	192.168.1.34
IPv4 DNS servers:	218.248.112.193 218.248.112.225
Manufacturer:	Qualcomm Atheros Communications Inc.
Description:	Qualcomm Atheros QCA9377 Wireless Network Adapter
Driver version:	12.0.0.919
Physical address (MAC):	D0-C5-D3-3F-3F-D5

Performing a scan for my host :



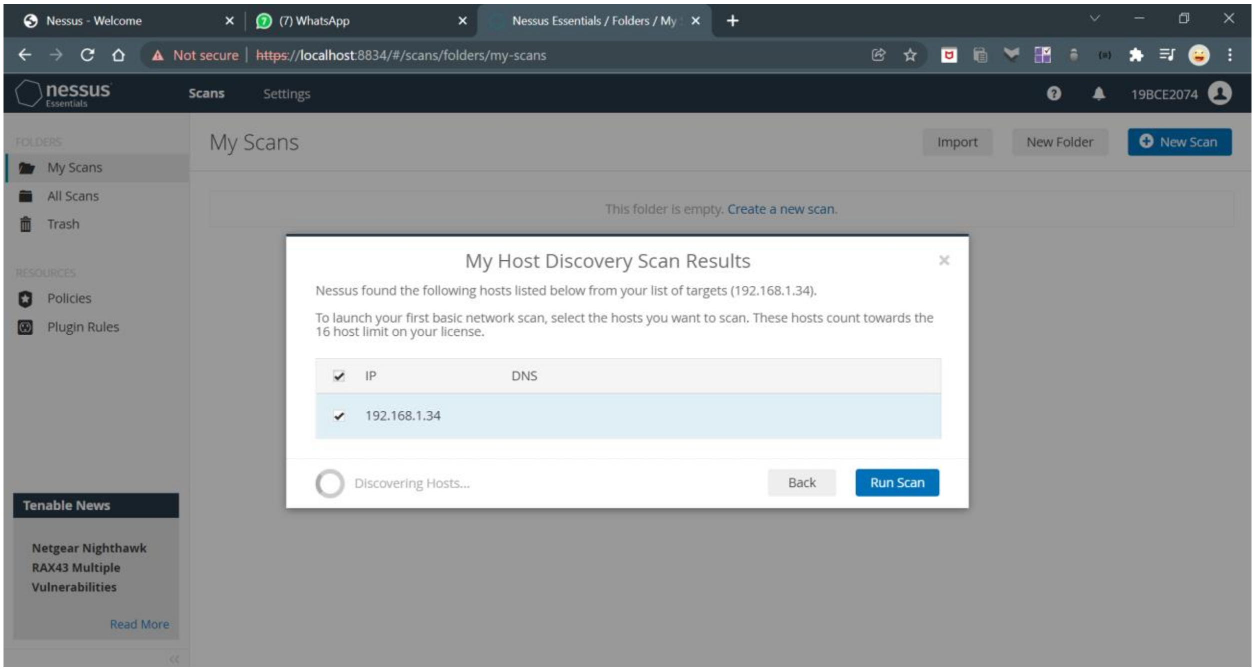
Welcome to Nessus Essentials

To get started, launch a host discovery scan to identify what hosts on your network are available to scan. Hosts that are discovered through a discovery scan do not count towards the 16 host limit on your license.

Enter targets as hostnames, IPv4 addresses, or IPv6 addresses. For IP addresses, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).

Targets: 192.168.1.34

Close | Submit



My Host Discovery Scan Results

Nessus found the following hosts listed below from your list of targets (192.168.1.34).

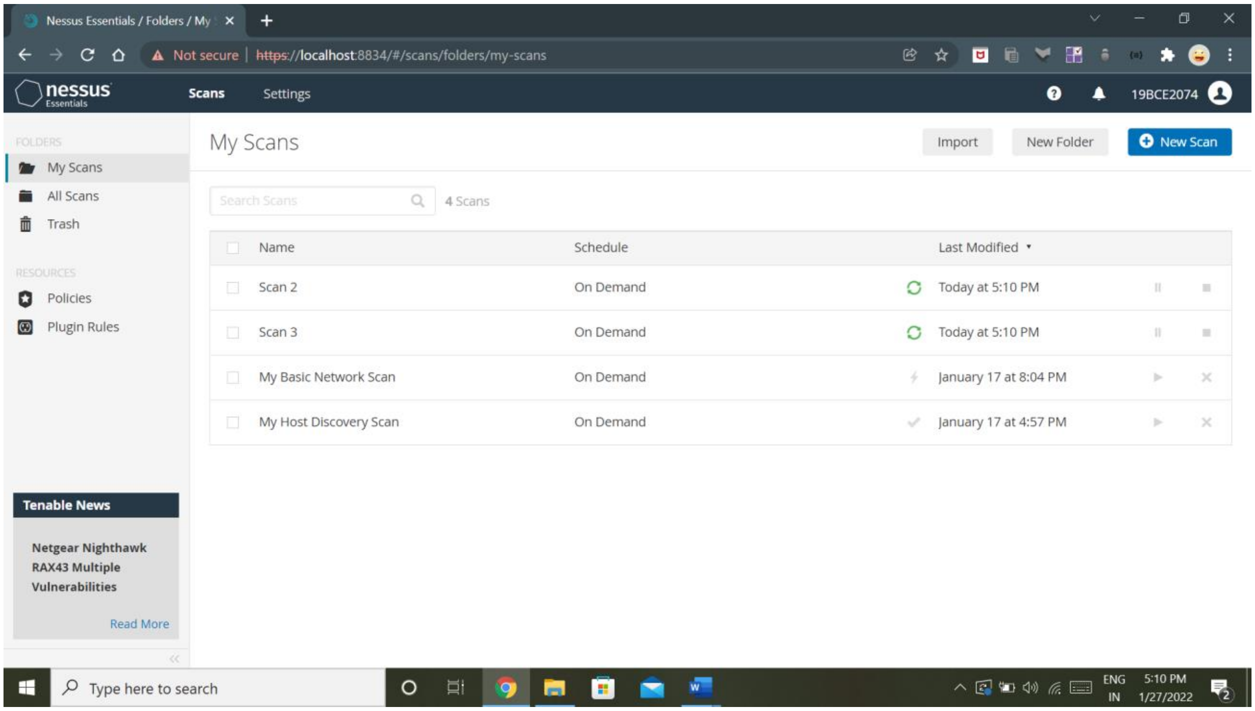
To launch your first basic network scan, select the hosts you want to scan. These hosts count towards the 16 host limit on your license.

☑	IP	DNS
☑	192.168.1.34	

Discovering Hosts...

Back | Run Scan

Performing 3 SCANS :

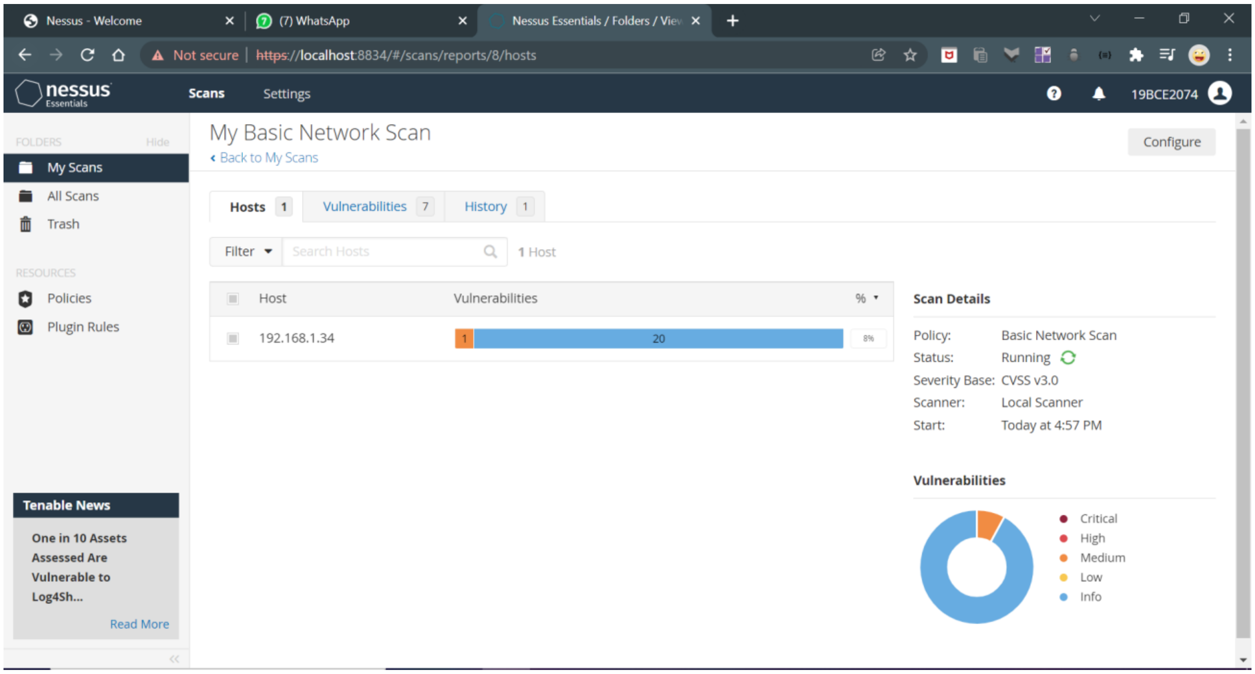


My Scans

4 Scans

Name	Schedule	Last Modified
Scan 2	On Demand	Today at 5:10 PM
Scan 3	On Demand	Today at 5:10 PM
My Basic Network Scan	On Demand	January 17 at 8:04 PM
My Host Discovery Scan	On Demand	January 17 at 4:57 PM

SCAN 1 :



My Basic Network Scan

‹ Back to My Scans

1 Host

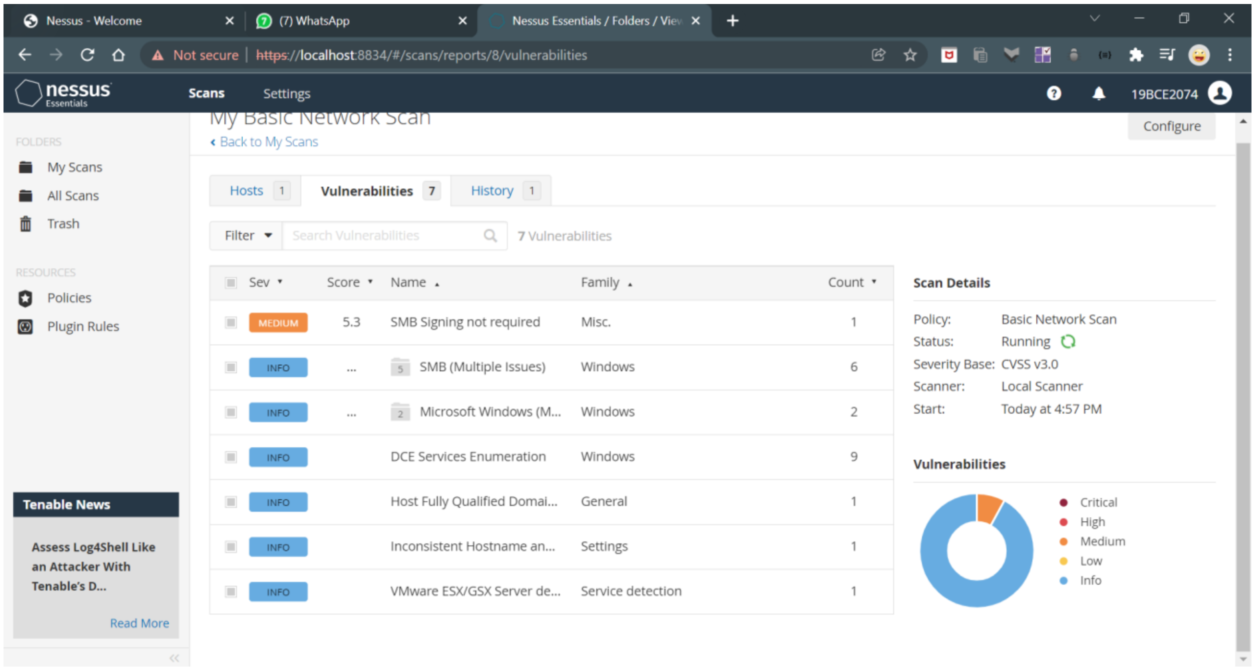
Host	Vulnerabilities	%
192.168.1.34	1 20	8%

Scan Details

Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 4:57 PM

Vulnerabilities

Vulnerabilities detected :



My Basic Network Scan
‹ Back to My Scans

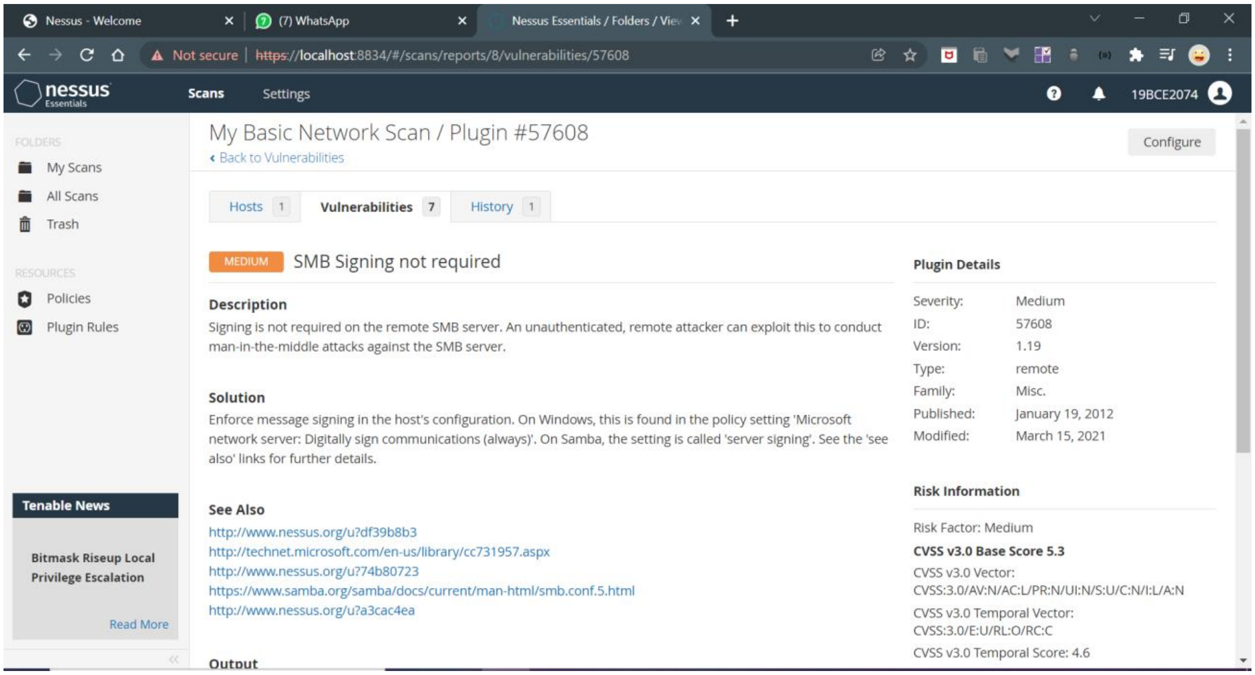
7 Vulnerabilities

Sev	Score	Name	Family	Count
MEDIUM	5.3	SMB Signing not required	Misc.	1
INFO	...	5 SMB (Multiple Issues)	Windows	6
INFO	...	2 Microsoft Windows (M...	Windows	2
INFO		DCE Services Enumeration	Windows	9
INFO		Host Fully Qualified Domai...	General	1
INFO		Inconsistent Hostname an...	Settings	1
INFO		VMware ESX/GSX Server de...	Service detection	1

Scan Details

Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 4:57 PM

Vulnerabilities



My Basic Network Scan / Plugin #57608
‹ Back to Vulnerabilities

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

http://www.nessus.org/u?df39b8b3
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

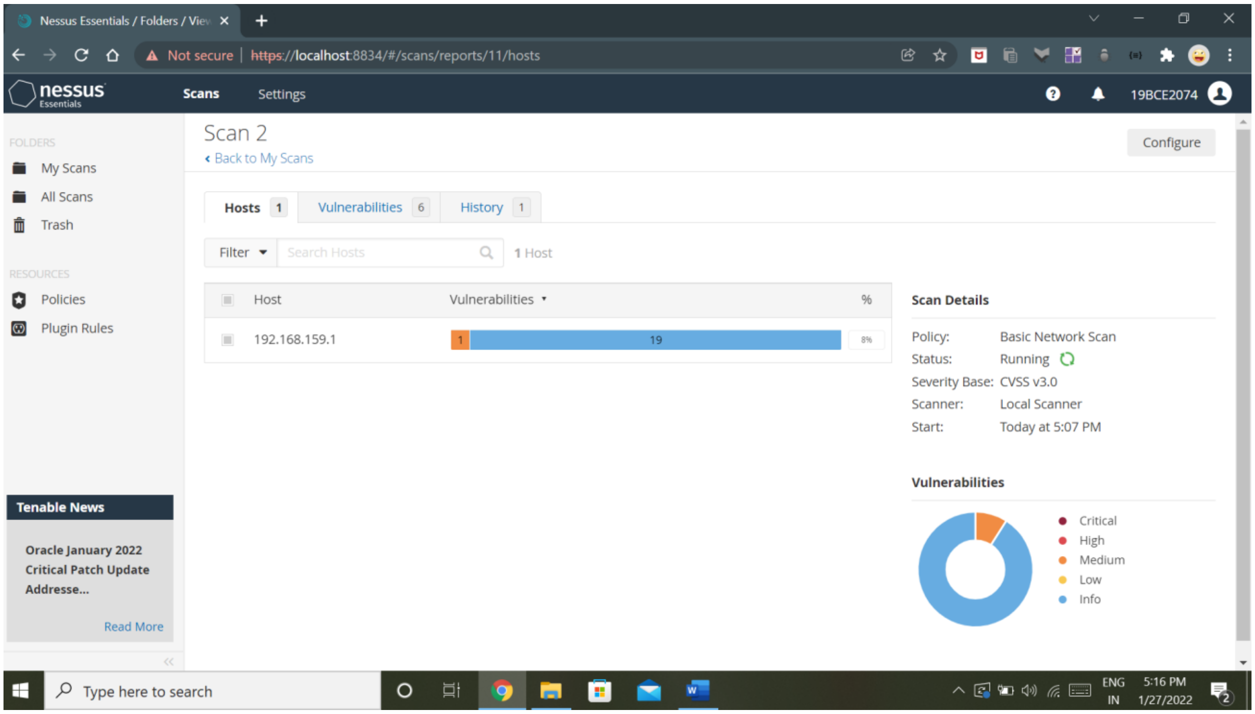
Plugin Details

Severity:	Medium
ID:	57608
Version:	1.19
Type:	remote
Family:	Misc.
Published:	January 19, 2012
Modified:	March 15, 2021

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

SCAN 2 :



Scan 2

‹ Back to My Scans

1 Host

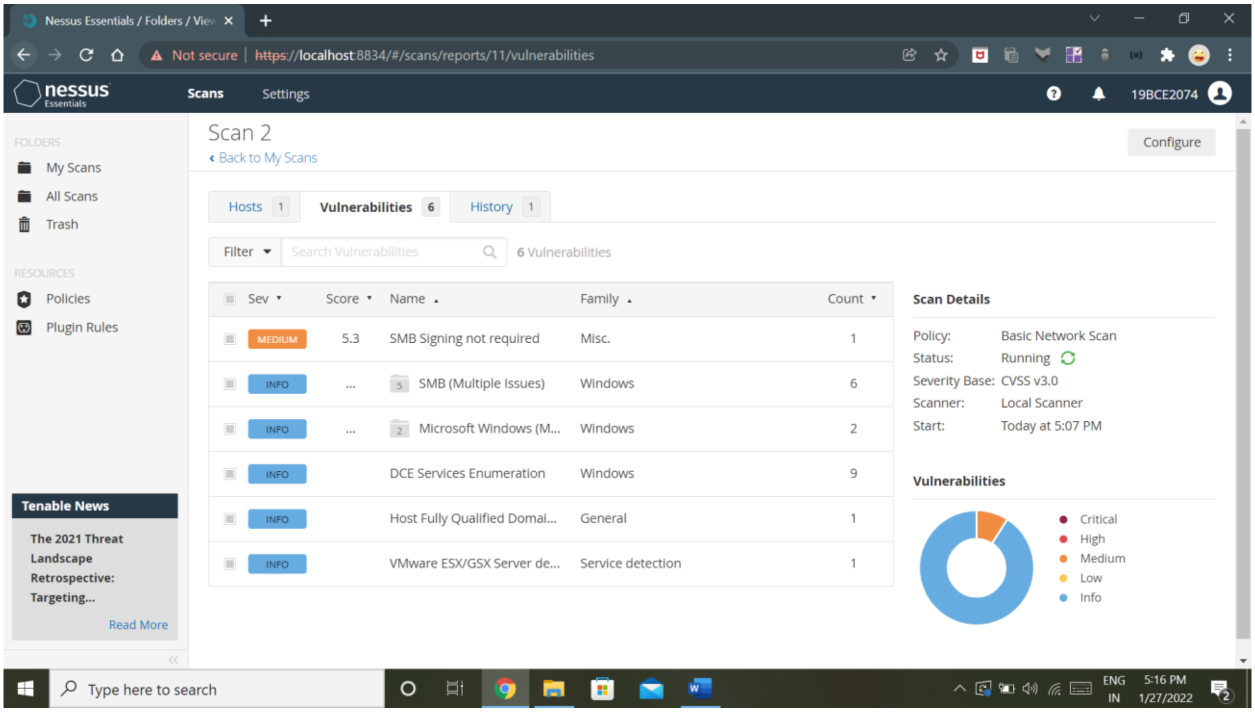
Host	Vulnerabilities	%
192.168.159.1	1 19	8%

Scan Details

Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 5:07 PM

Vulnerabilities

Vulnerabilities detected :



Scan 2

‹ Back to My Scans

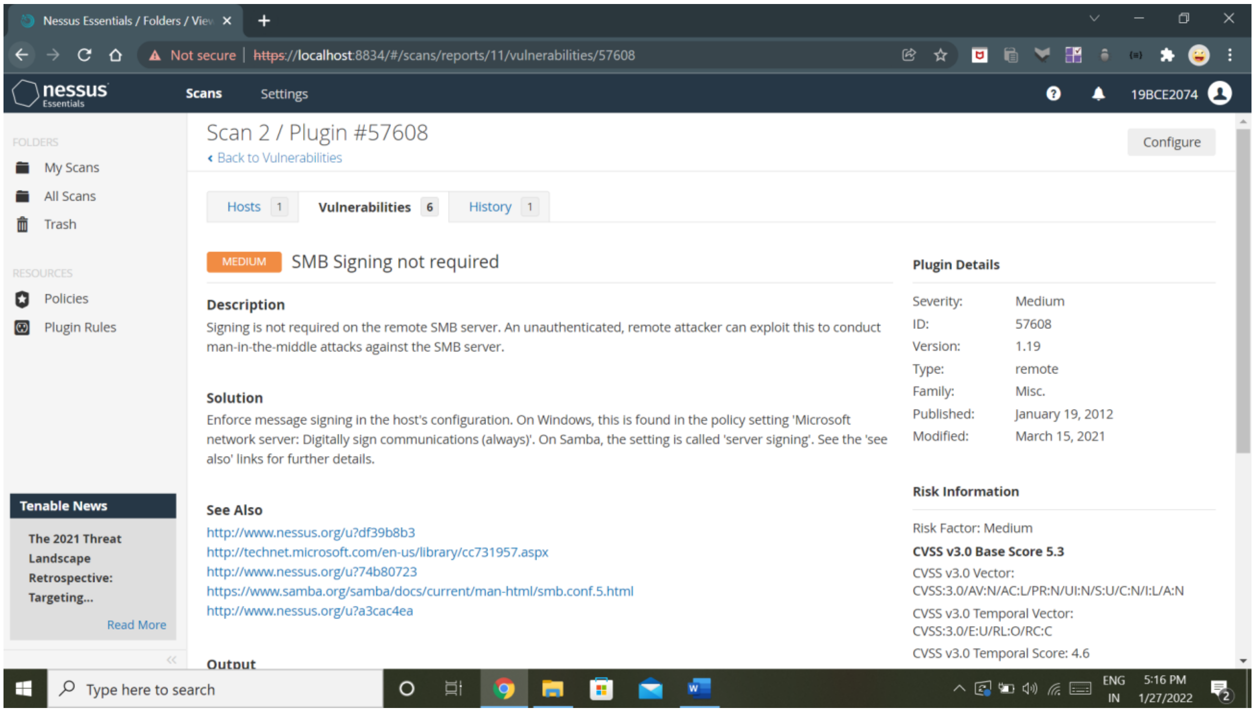
6 Vulnerabilities

Sev	Score	Name	Family	Count
MEDIUM	5.3	SMB Signing not required	Misc.	1
INFO	...	5 SMB (Multiple Issues)	Windows	6
INFO	...	2 Microsoft Windows (M...	Windows	2
INFO		DCE Services Enumeration	Windows	9
INFO		Host Fully Qualified Domai...	General	1
INFO		VMware ESX/GSX Server de...	Service detection	1

Scan Details

Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 5:07 PM

Vulnerabilities



Scan 2 / Plugin #57608

‹ Back to Vulnerabilities

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

http://www.nessus.org/u?df39b8b3
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

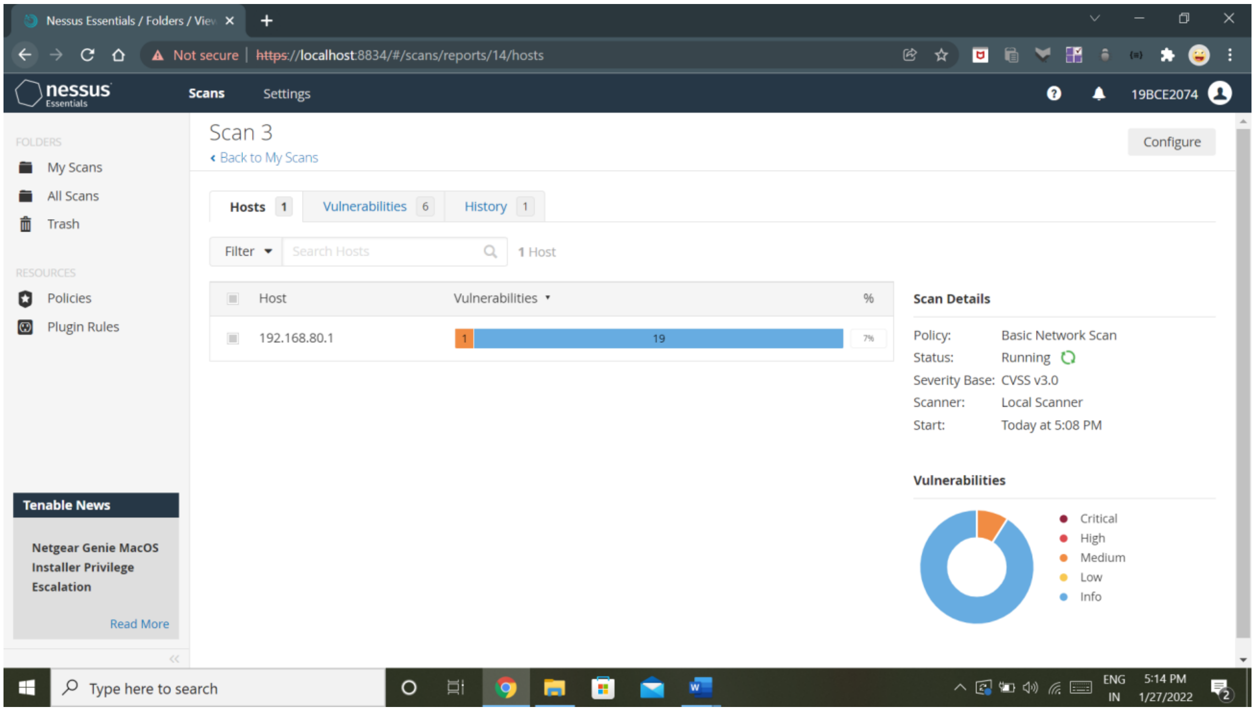
Plugin Details

Severity:	Medium
ID:	57608
Version:	1.19
Type:	remote
Family:	Misc.
Published:	January 19, 2012
Modified:	March 15, 2021

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

SCAN 3 :



Scan 3

‹ Back to My Scans

1 Host

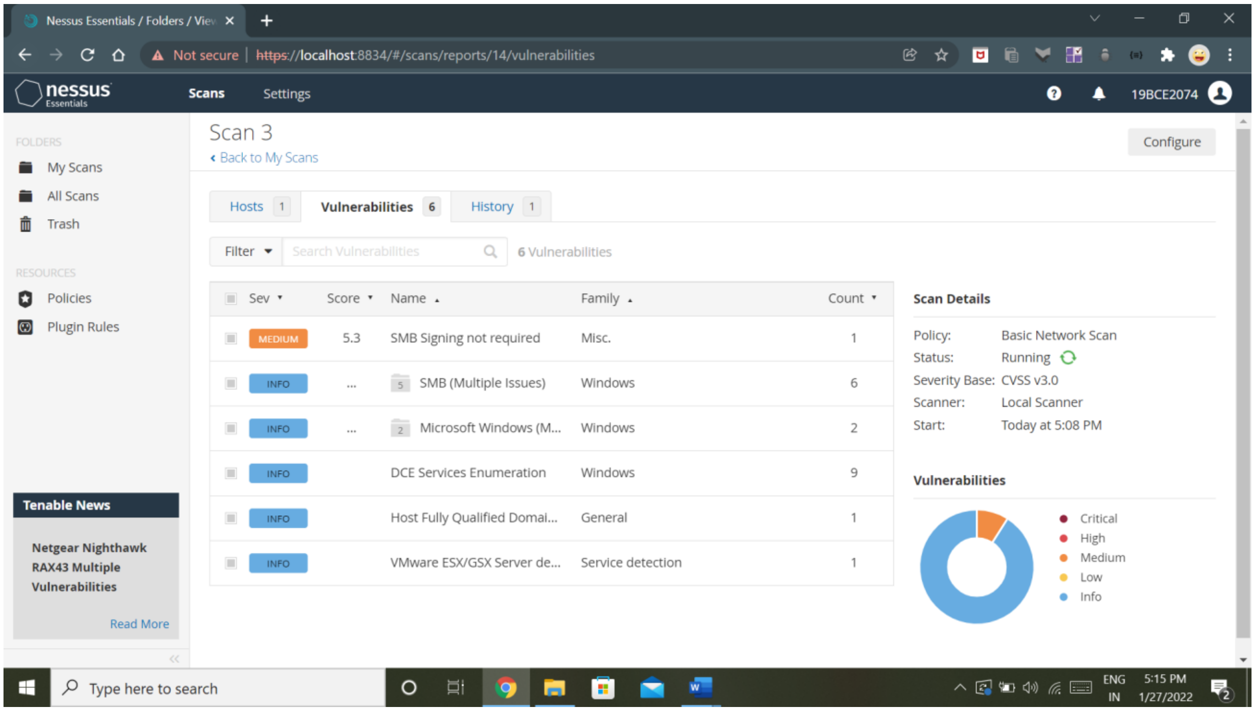
Host	Vulnerabilities	%
192.168.80.1	1 19	7%

Scan Details

Policy:	Basic Network Scan
Status:	Running
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 5:08 PM

Vulnerabilities

Vulnerabilities detected :



Scan 3

‹ Back to My Scans

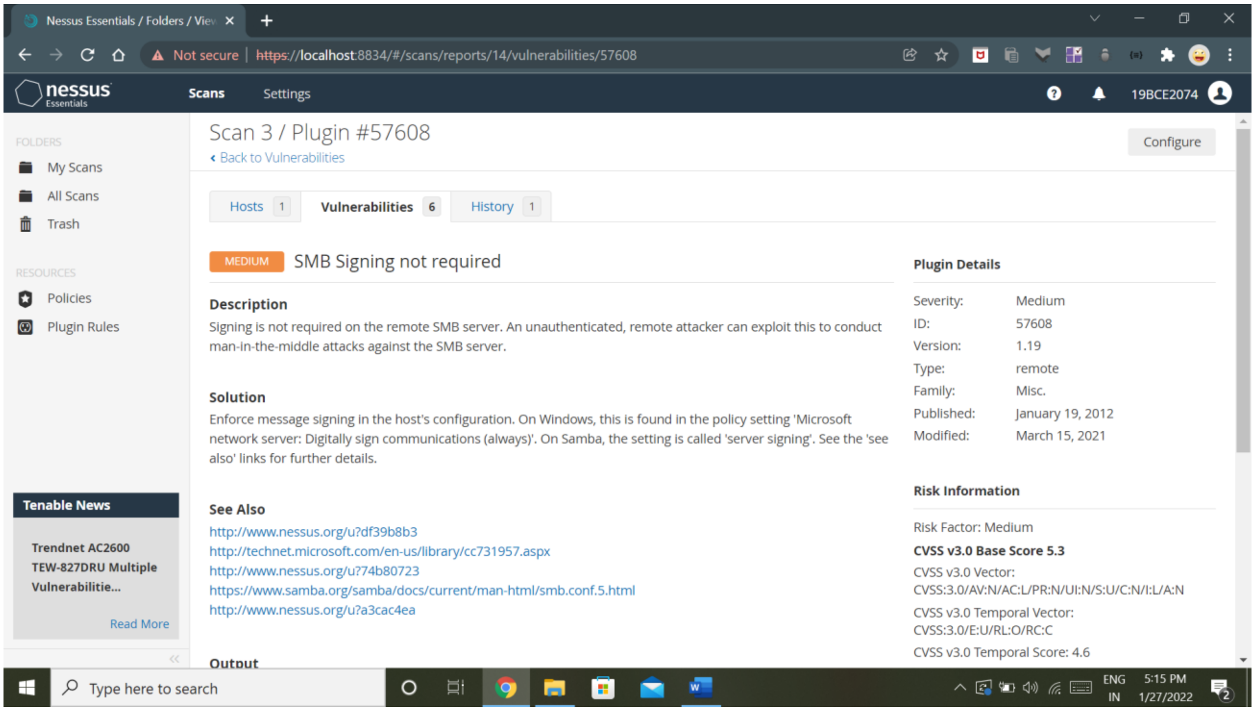
6 Vulnerabilities

Sev	Score	Name	Family	Count
MEDIUM	5.3	SMB Signing not required	Misc.	1
INFO	...	5 SMB (Multiple Issues)	Windows	6
INFO	...	2 Microsoft Windows (M...	Windows	2
INFO		DCE Services Enumeration	Windows	9
INFO		Host Fully Qualified Domai...	General	1
INFO		VMware ESX/GSX Server de...	Service detection	1

Scan Details

Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 5:08 PM

Vulnerabilities



Scan 3 / Plugin #57608

‹ Back to Vulnerabilities

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

http://www.nessus.org/u?df39b8b3
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

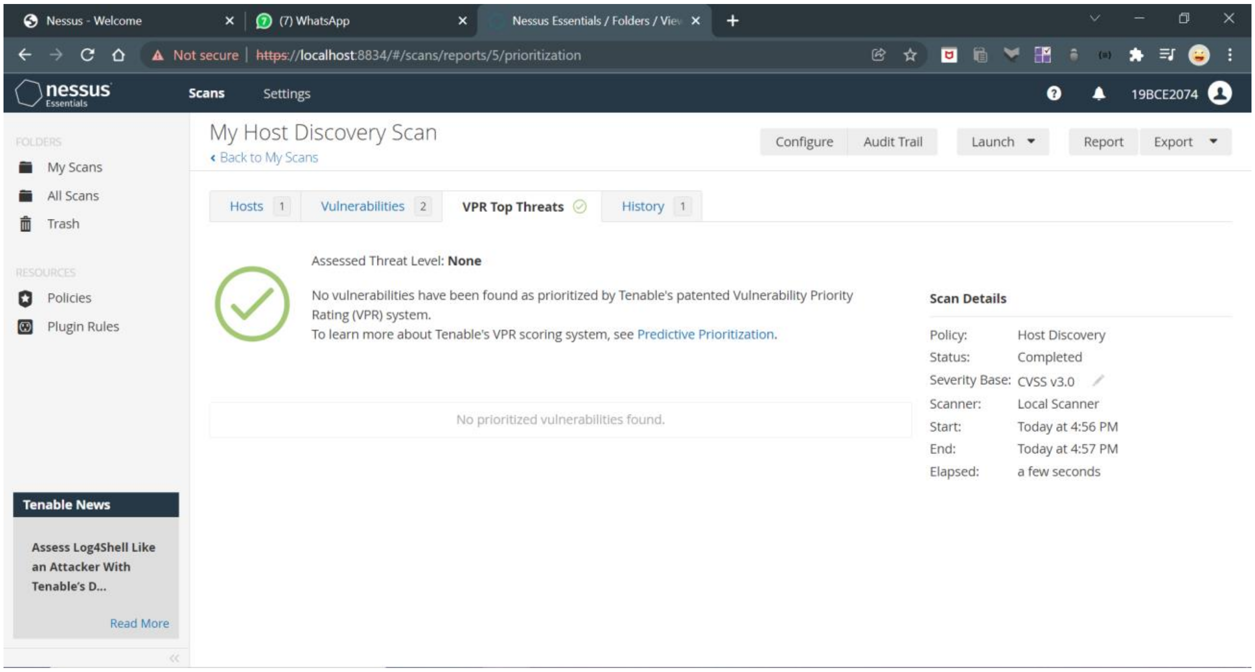
Plugin Details

Severity: Medium
ID: 57608
Version: 1.19
Type: remote
Family: Misc.
Published: January 19, 2012
Modified: March 15, 2021

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

Results for my host discovery scan



My Host Discovery Scan

‹ Back to My Scans

Assessed Threat Level: **None**

No vulnerabilities have been found as prioritized by Tenable's patented Vulnerability Priority Rating (VPR) system.
To learn more about Tenable's VPR scoring system, see Predictive Prioritization.

No prioritized vulnerabilities found.

Scan Details

Policy:	Host Discovery
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 4:56 PM
End:	Today at 4:57 PM
Elapsed:	a few seconds

Assess Log4Shell Like an Attacker With Tenable's D...

Experiment 2 :
Information Security Policy

https://drive.google.com/drive/folders/1ojN6WzJJEbQE5-nqTu0cCuDiWJdmS3xj?usp=sharing
The above google drive link contains all the 5 policies written as separate documents.
Please use the above google drive link to review the policy documents individually.
I have also attached the documents down below.

The policies that have been formulated by me are :

1. Clean Desk Policy
2. Ethics Policy
3. Incident Handling Forms – Incident Identification
4. Software Installation Policy
5. Data Breach Response Policy

Clean Desk Policy

1. Overview

A clean desk policy can be an import tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee or student leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase employee's and student's awareness about protecting sensitive information.

2. Purpose

The purpose for this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information about our employees and students, our intellectual property, our administrators and our contractors is secure in locked areas and out of site. A Clean Desk policy is not only ISO 27001/17799 compliant, but it is also part of standard basic privacy controls.

3. Scope

This policy applies to all Vellore Institute of Technology employees, students and affiliates.

4. Policy

4.1 Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.

4.2 Students are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area, that is, the classroom, lecture halls or hostels.

4.3 One must ensure proper logging out off the systems present inside the labs or other classrooms after completion of work.

4.4 Computer workstations must be locked when workspace is unoccupied.

4.5 Computer workstations must be shut completely down at the end of the work day.

4.6 Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.

4.7 File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.

4.8 Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.

4.9 Laptops must be either locked with a locking cable or locked away in a drawer.

4.10 Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.

4.11 Printouts containing Restricted or Sensitive information should be immediately removed from the printer.

4.12 Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.

4.13 Whiteboards containing Restricted and/or Sensitive information should be erased.

4.14 Lock away portable computing devices such as laptops and tablets.

4.15 Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer

All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

5. Policy Compliance

5.1 Compliance Measurement

The Department of Security and Operations will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Department of Security and Operations in advance.

5.3 Non-Compliance

An employee or student found to have violated this policy may be subject to disciplinary action, up to and including termination of employment and immediate dismissal from the Institute.

6 Related Standards, Policies and Processes

None.

7 Definitions and Terms

None.

8 Revision History

Date of Change	**Responsible**	**Summary of Change**
January 2022	Kulvir Singh (19BCE2074)	Updated and converted to new format.

Ethics Policy

6. Overview

Vellore Institute of Technology is committed to protecting employees, partners, vendors and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. When Vellore Institute of Technology addresses issues proactively and uses correct judgment, it will help set us apart from competitors.

Vellore Institute of Technology will not tolerate any wrongdoing or impropriety at any time. Vellore Institute of Technology will take the appropriate measures act quickly in correcting the issue if the ethical code is broken.

7. Purpose

The purpose of this policy is to establish a culture of openness, trust and to emphasize the employee's and consumer's expectation to be treated to fair business practices. This policy will serve to guide business behavior to ensure ethical conduct. Effective ethics is a team effort involving the participation and support of every Vellore Institute of Technology's employee. All employees should familiarize themselves with the ethics guidelines that follow this introduction.

8. Scope

This policy applies to employees, professor, students, contractors, consultants, temporaries, and other workers at Vellore Institute of Technology including all personnel affiliated with third parties.

9. Policy

4.1 Administration Commitment to Ethics

4.1.1 Senior employees, executives and the administration body within Vellore Institute of Technology must set a prime example. In any executive or administrative practice or any form of activity, honesty and integrity must be top priority for them.

4.1.2 The employees in the administrative department must have an open door policy and welcome suggestions and concerns from other employees, professors or students. This will allow the ecosystem at Vellore Institute of Technology to feel comfortable discussing any issues and will alert executives to concerns within the work force.

4.1.3 Executives must disclose any conflict of interests regard their position within Vellore Institute of Technology.

4.2 Professors' Commitment to Ethics

4.2.1 Vellore Institute of Technology professors will treat everyone fairly, have mutual respect, promote a team environment and avoid the intent and appearance of unethical or compromising practices.

4.2.2 Every professor needs to apply effort and intelligence in maintaining ethics value.

4.2.3 Professors must disclose any conflict of interests regard their position within Vellore Institute of Technology.

4.2.4 Professors will help Vellore Institute of Technology to increase student and parent satisfaction by practicing proper and efficient teaching and give a timely response to inquiries.

4.2.5 Professors should consider the following questions to themselves when any behavior is questionable:

- Is the behavior legal?
- Does the behavior comply with all appropriate Vellore Institute of Technology policies?
- Does the behavior reflect Vellore Institute of Technology values and culture?
- Could the behavior adversely affect the Institute’s reputation?
- Would you feel personally concerned if the behavior appeared in a news headline?
- Could the behavior adversely affect Vellore Institute of Technology if all professors, did it?

4.3 Students’ Commitment to Ethics

4.3.1 Vellore Institute of Technology students will treat everyone fairly, have mutual respect, promote a team environment and avoid the intent and appearance of unethical or compromising practices.

4.3.2 Every student needs to apply effort and intelligence in maintaining ethics value.

4.3.3 Students will help Vellore Institute of Technology to increase student and professor satisfaction by practicing proper mannerism inside and outside the campus.

4.3.4 Students should consider the following questions to themselves when any behavior is questionable:

- Is the behavior legal?
- Does the behavior comply with all appropriate Vellore Institute of Technology policies?
- Does the behavior reflect Vellore Institute of Technology values and culture?
- Could the behavior adversely affect the Institute’s reputation?
- Would you feel personally concerned if the behavior appeared in a news headline?
- Could the behavior adversely affect Vellore Institute of Technology if all students, did it?

4.4 Company Awareness

4.4.1 Promotion of ethical conduct within interpersonal communications will be rewarded.

4.4.2 Vellore Institute of Technology will promote a trustworthy and honest atmosphere to reinforce the vision of ethics within the company.

4.5 Maintaining Ethical Practices

4.5.1 Vellore Institute of Technology will reinforce the importance of the integrity message and the tone will start at the top. Every person related to the Institute needs consistently maintain an ethical stance and support ethical behavior.

4.5.2 One should encourage open dialogue, get honest feedback and treat everyone fairly, with honesty and objectivity.

4.5.3 Vellore Institute of Technology has established a best practice disclosure committee to make sure the ethical code is delivered to all persons related to the Institute and that concerns regarding the code can be addressed.

4.6 Unethical Behavior

4.6.1 Vellore Institute of Technology will avoid the intent and appearance of unethical or compromising practice in relationships, actions and communications.

4.6.2 Vellore Institute of Technology will not tolerate harassment or discrimination.

4.6.3 Unauthorized use of company trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company will not be tolerated.

4.6.4 Vellore Institute of Technology will not permit impropriety at any time and we will act ethically and responsibly in accordance with laws.

4.6.5 Vellore Institute of Technology employees will not use corporate assets or business relationships for personal use or gain.

10. Policy Compliance

8.1 Compliance Measurement

The Department of Welfare from Vellore Institute of Technology will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback.

8.2 Exceptions

None.

8.3 Non-Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination and immediate dismissal from the Institute.

9 Related Standards, Policies and Processes

None.

10 Definitions and Terms

None.

11 Revision History

Date of Change	Responsible	Summary of Change
January 2022	Kulvir Singh (19BCE2074)	Updated and converted to new format.

Vellore Institute of Technology, Vellore PAGE 1 OF 1

INCIDENT IDENTIFICATION FORM

DATE UPDATED:____________

General Information

Incident Detector's Information:

Name:________________________________

Designation: ____________________________

Mobile:________________________________

Alt. Mobile:_____________________________

Fax(for faculty):__________________________

VIT E-mail: _____________________________

Address/ Hostel Details: ___________________

____

Detector's Signature:_______________________

Date and Time Detected: ____________________

Location Incident Detected From: _______________

____

Additional Information:_______________________

____

____

____

Date Signed: ____________________________

Incident Summary

Type of Incident Detected:

- Denial of Service
- Malicious Code
- Unauthorized Use
- Unauthorized Access
- Espionage
- Other:______________________________
- Probe
- Hoax

Incident Location:

Site:__________________________________

Site Point of Contact:_______________________

Mobile:________________________________

Alt. Mobile:_____________________________

Fax(for faculty):__________________________

VIT E-mail: _____________________________

Address: _______________________________

____

How was the Incident Detected:_________________

____

____

____

____

____

____

____

Additional Information: ____

____

____

Prepared By:
Kulvir Singh 19BCE2074

Software Installation Policy

11. Overview

Allowing employees and students to install software on company computing devices opens the organization up to unnecessary exposure. Conflicting file versions or DLLs which can prevent programs from running, the introduction of malware from infected installation software, unlicensed software which could be discovered during audit, and programs which can be used to hack the organization's network are examples of the problems that can be introduced when employees install software on company equipment. Also provision of licensed software under company's name for personal use or practice is handled.

12. Purpose

The purpose of this policy is to outline the requirements around installation software on Vellore Institute of Technology computing devices as well as personal devices. To minimize the risk of loss of program functionality, the exposure of sensitive information contained within Vellore Institute of Technology computing network, the risk of introducing malware, and the legal exposure of running unlicensed software.

13. Scope

This policy applies to all Vellore Institute of Technology employees, students, vendors and agents with a Vellore Institute of Technology-owned devices. This policy covers all computers, servers, smartphones, tablets and other computing devices operating within Vellore Institute of Technology.

14. Policy

- Employees and students may not install software on Vellore Institute of Technology computing devices operated within the Vellore Institute of Technology network.
- Software requests must first be approved by the head of Software Development Cell of Vellore Institute of Technology and then be made to the Head of Security and Operations in writing or via email.
- Software must be selected from an approved software list, maintained by the Software Development Cell of Vellore Institute of Technology, unless no selection on the list meets the requester's need.
- The Software Development Cell of Vellore Institute of Technology will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.

15. Policy Compliance

11.1 Compliance Measurement

The Infosec team of Vellore Institute of Technology will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

11.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

11.3 Non-Compliance

An employee or student found to have violated this policy may be subject to disciplinary action, up to and including termination and dismissal from the Institute.

12 Related Standards, Policies and Processes

None.

13 Definitions and Terms

None.

14 Revision History

Date of Change	Responsible	Summary of Change
January 2022	Kulvir Singh (19BCE2074)	Updated and converted to new format.

Data Breach Response Policy

1.0 Purpose

The purpose of the policy is to establish the goals and the vision for the breach response process. This policy will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms. The policy shall be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.

Vellore Institute of Technology Information Security's intentions for publishing a Data Breach Response Policy are to focus significant attention on data security and data security breaches and how Vellore Institute of Technology's established culture of openness, trust and integrity should respond to such activity. Vellore Institute of Technology Information Security is committed to protecting Vellore Institute of Technology's employees, students, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

2.0 Scope

This policy applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information or Protected Health Information (PHI) of Vellore Institute of Technology members. Any agreements with vendors will contain language similar that protects the fund.

3.0 Policy Confirmed theft, data breach or exposure of Vellore Institute of Technology's Protected data or Vellore Institute of Technology's Sensitive data

As soon as a theft, data breach or exposure containing Vellore Institute of Technology's Protected data or Vellore Institute of Technology's Sensitive data is identified, the process of removing all access to that resource will begin.

The Board of Directors in cohesion with the Registrar office will chair an incident response team to handle the breach or exposure.

The team will include members from:

- IT Infrastructure
- IT Applications
- Finance (if applicable)
- Legal
- Communications
- Member Services (if Member data is affected)
- Human Resources
- The affected unit or department that uses the involved system or output or whose data may have been breached or exposed

- Additional departments based on the data type involved, Additional individuals as deemed necessary by the Board of Directors, Registrar or the Chancellor himself.

Confirmed theft, breach or exposure of Vellore Institute of Technology data

The Registrar and Board of Directors will be notified of the theft, breach or exposure. IT, along with the designated forensic team, will analyze the breach or exposure to determine the root cause.

Work with Forensic Investigators

As provided by Vellore Institute of Technology cyber insurance, the insurer will need to provide access to forensic investigators and experts that will determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or organizations impacted; and analyze the breach or exposure to determine the root cause.

Develop a communication plan.

Work with Vellore Institute of Technology communications, legal and human resource departments to decide how to communicate the breach to: a) internal employees, b) the staff, c) the students if necessary and d) those directly affected.

3.2 Ownership and Responsibilities

Roles & Responsibilities:

- Sponsors - Sponsors are those members of the Vellore Institute of Technology community that have primary responsibility for maintaining any particular information resource. Sponsors may be designated by any Vellore Institute of Technology Executive in connection with their administrative responsibilities, or by the actual sponsorship, collection, development, or storage of information.
- Information Security Administrator is that member of the Vellore Institute of Technology community, designated by the Board of Directors or the Chancellor, Information Technology (IT) Infrastructure, who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources in consultation with the relevant Sponsors.
- Users include virtually all members of the Vellore Institute of Technology community to the extent they have authorized access to information resources, and may include professors, students, staff, trustees, contractors, consultants, interns, temporary employees and volunteers.
- The Incident Response Team shall be chaired by Software Development Cell Head and shall include, but will not be limited to, the following departments or their representatives: IT-Infrastructure, IT-Application Security; Communications; Legal; Management; Financial Services, Member Services; Human Resources, Student Welfare.

4.0 Enforcement

Any Vellore Institute of Technology personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Any third party partner company found in violation may have their network connection terminated.

5.0 Definitions

Encryption or encrypted data – The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text;
Plain text – Unencrypted data.
Hacker – A slang term for a computer enthusiast, i.e., a person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject(s).
Protected Health Information (PHI) - Under US law is any information about health status, provision of health care, or payment for health care that is created or collected by a "Covered Entity" (or a Business Associate of a Covered Entity), and can be linked to a specific individual.
Personally Identifiable Information (PII) - Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered
Protected data - See PII and PHI
Information Resource - The data and information assets of an organization, department or unit.
Safeguards - Countermeasures, controls put in place to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Safeguards help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.
Sensitive data - Data that is encrypted or in plain text and contains PII or PHI data. See PII and PHI above.

6.0 Revision History

Version	Date of Revision	Author	Description of Changes
1.0	January, 2022	Kulvir Singh	Initial version