Don Bosco Institute of Technology, Mumbai 400070 Department of Information Technology

Experiment No. : 10

Name: Swasti Jain
Batch: B
Roll No: 24

Title: NESSUS tool

Problem Definition : Use NESSUS/ISO Kali Linux tool to scan the network for vulnerabilities.

Prerequisite : Basic Knowledge of kali linux and network scanning

Theory :
A vulnerability is a weakness or error in a system or device's code that, when exploited, can compromise the confidentiality, availability, and integrity of data stored in them through unauthorised access, the elevation of privileges, or denial of service.

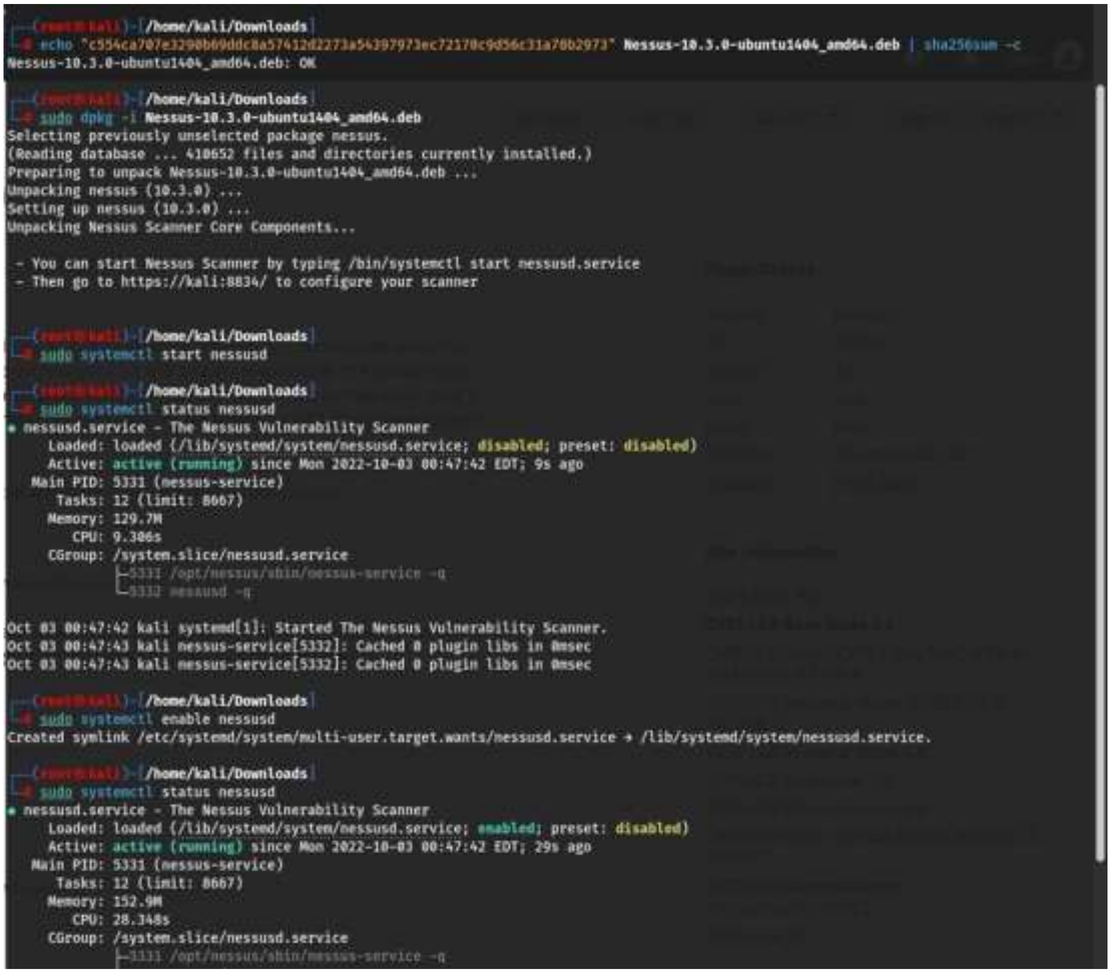
Nessus is developed by Tenable, Inc. It is a remote security scanning tool, which scans a computer for vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network.

Purpose: Vulnerability Assessment

- Vulnerability scanning is a process of identifying network, application, and securityvulnerabilities.
- In addition to identifying security loopholes, vulnerability scans also predict effectivesolutions to counter a threat or attack .
- After the scan, a report is generated. The findings in the report can then be analysedand interpreted to identify opportunities to improve security

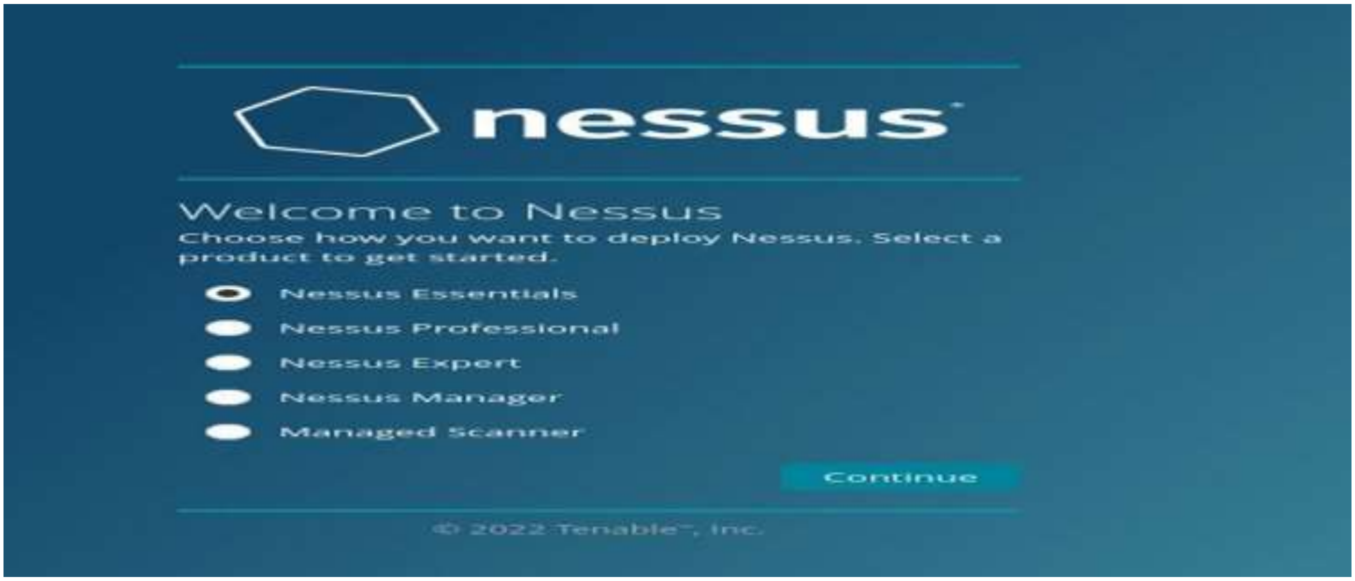
Procedure/ Algorithm :

Step 1.)Download and install Nessus



```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# echo "c554ca707e3290b69ddc8a57412d2273a54397973ec72170c9d56c31a70b2973" Nessus-10.3.0-ubuntu1404_amd64.deb | sha256sum -c
Nessus-10.3.0-ubuntu1404_amd64.deb: OK

┌──(root㉿kali)-[/home/kali/Downloads]
└─# sudo dpkg -i Nessus-10.3.0-ubuntu1404_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 410652 files and directories currently installed.)
Preparing to unpack Nessus-10.3.0-ubuntu1404_amd64.deb ...
Unpacking nessus (10.3.0) ...
Setting up nessus (10.3.0) ...
Unpacking Nessus Scanner Core Components...

 - You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
 - Then go to https://kali:8834/ to configure your scanner


┌──(root㉿kali)-[/home/kali/Downloads]
└─# sudo systemctl start nessusd

┌──(root㉿kali)-[/home/kali/Downloads]
└─# sudo systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
     Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; preset: disabled)
     Active: active (running) since Mon 2022-10-03 00:47:42 EDT; 9s ago
   Main PID: 5331 (nessus-service)
      Tasks: 12 (limit: 8667)
     Memory: 129.7M
        CPU: 9.306s
     CGroup: /system.slice/nessusd.service
             ├─5331 /opt/nessus/sbin/nessus-service -q
             └─5332 nessusd -q

Oct 03 00:47:42 kali systemd[1]: Started The Nessus Vulnerability Scanner.
Oct 03 00:47:43 kali nessus-service[5332]: Cached 0 plugin libs in 0msec
Oct 03 00:47:43 kali nessus-service[5332]: Cached 0 plugin libs in 0msec

┌──(root㉿kali)-[/home/kali/Downloads]
└─# sudo systemctl enable nessusd
Created symlink /etc/systemd/system/multi-user.target.wants/nessusd.service → /lib/systemd/system/nessusd.service.

┌──(root㉿kali)-[/home/kali/Downloads]
└─# sudo systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
     Loaded: loaded (/lib/systemd/system/nessusd.service; enabled; preset: disabled)
     Active: active (running) since Mon 2022-10-03 00:47:42 EDT; 29s ago
   Main PID: 5331 (nessus-service)
      Tasks: 12 (limit: 8667)
     Memory: 152.9M
        CPU: 28.348s
     CGroup: /system.slice/nessusd.service
             ├─5331 /opt/nessus/sbin/nessus-service -q
```

Step Two: Set Up Your Nessus Account and Activation Code



Welcome to Nessus

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

● Nessus Essentials

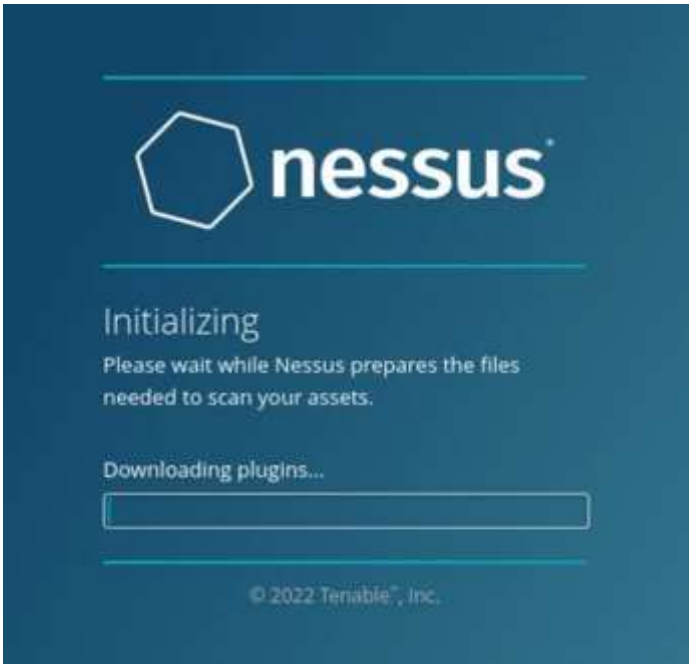
○ Nessus Professional

○ Nessus Expert

○ Nessus Manager

○ Managed Scanner

© 2022 Tenable™, Inc.



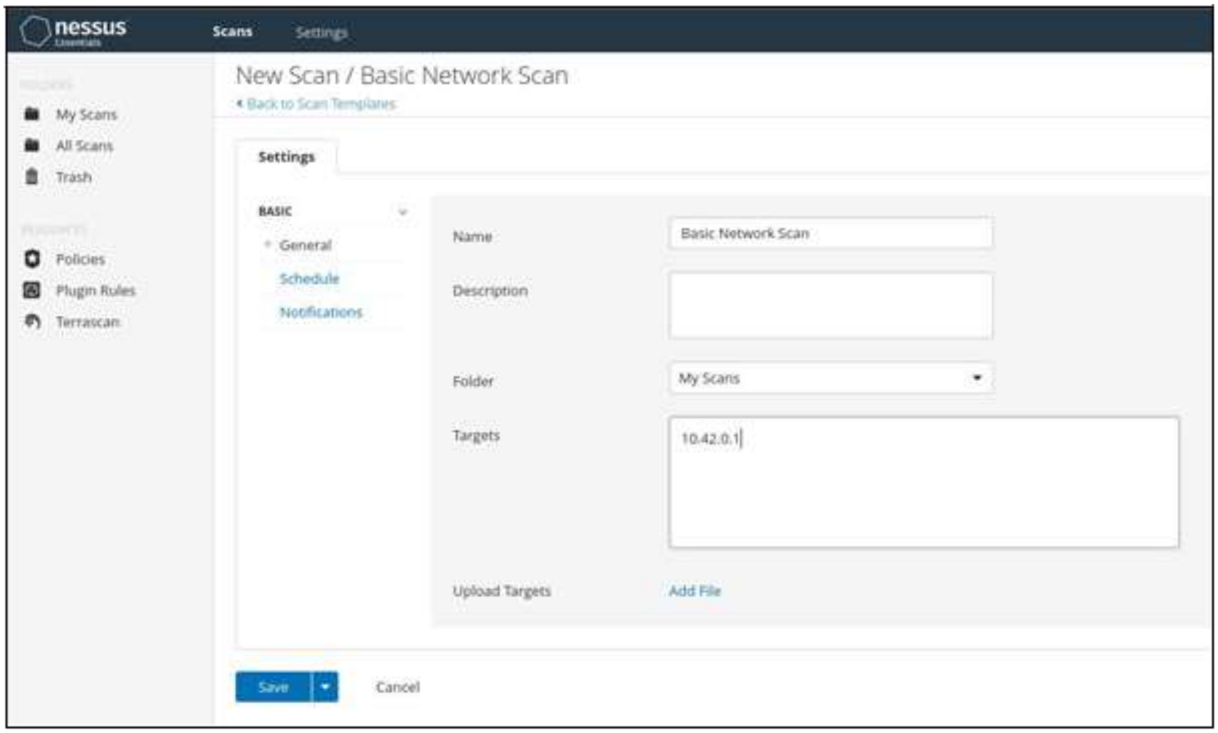
Initializing

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

Downloading plugins...

© 2022 Tenable®, Inc.

Step Three: Start a Vulnerability Scan



New Scan / Basic Network Scan

‹ Back to Scan Templates

Name: Basic Network Scan

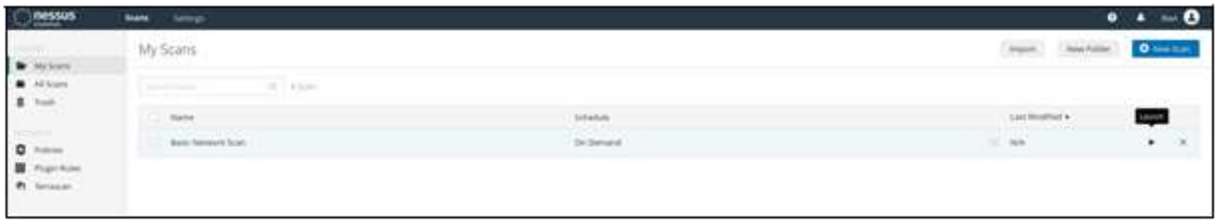
Description:

Folder: My Scans

Targets: 10.42.0.1

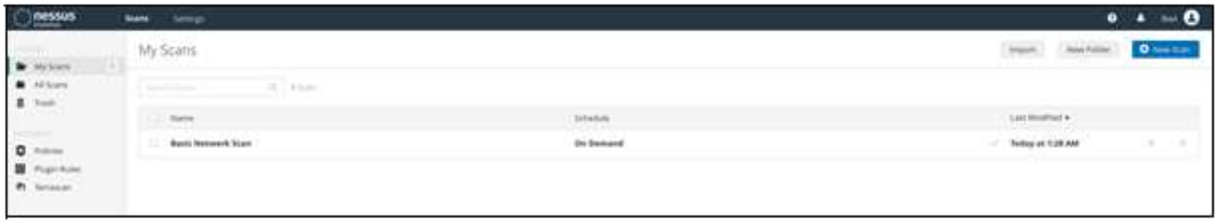
Upload Targets: Add File

Step Four: Make Sense of the Results



My Scans

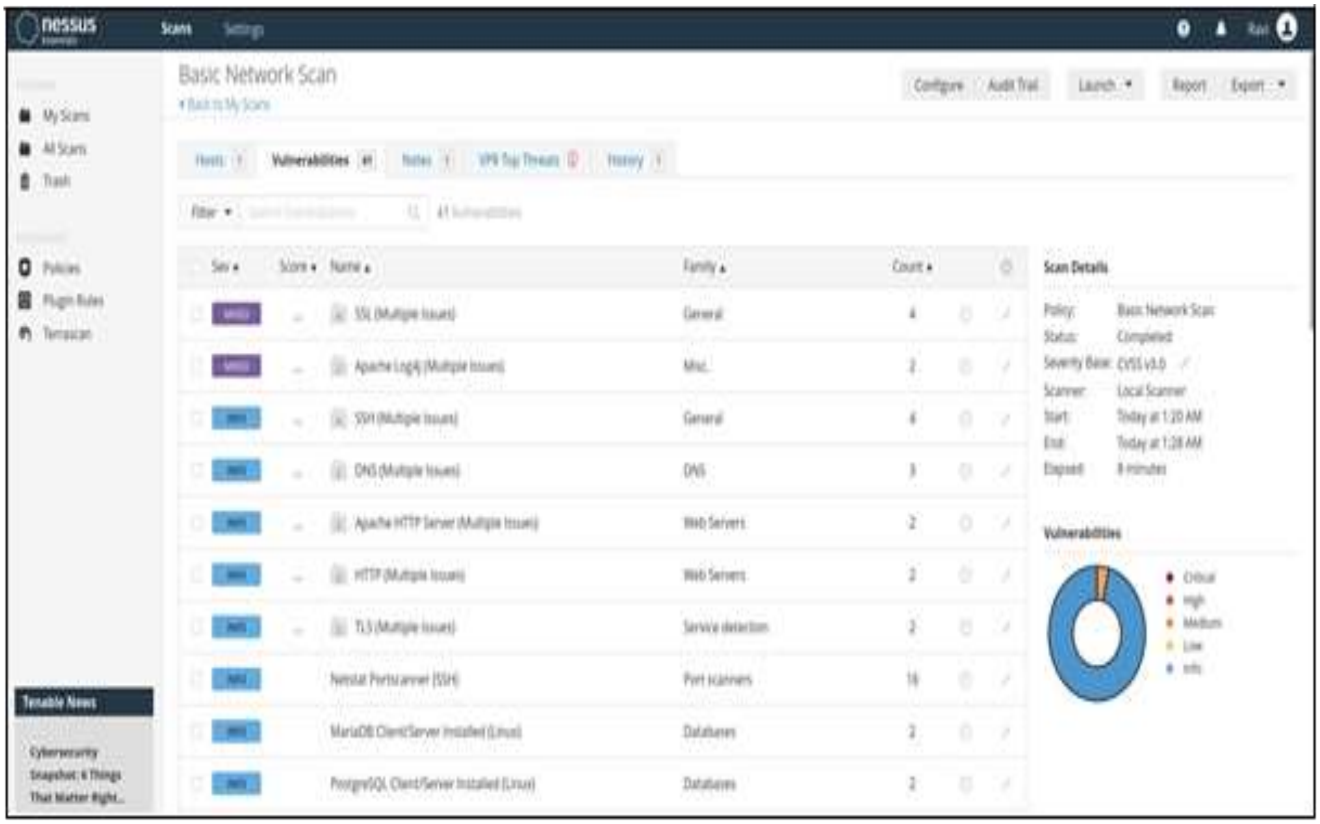
Name	Schedule	Last Modified ▾
Basic Network Scan	On Demand	N/A



My Scans

Name	Schedule	Last Modified ▾
Basic Network Scan	On Demand	Today at 1:28 AM

RESULTS:



Basic Network Scan

◂ Back to My Scans

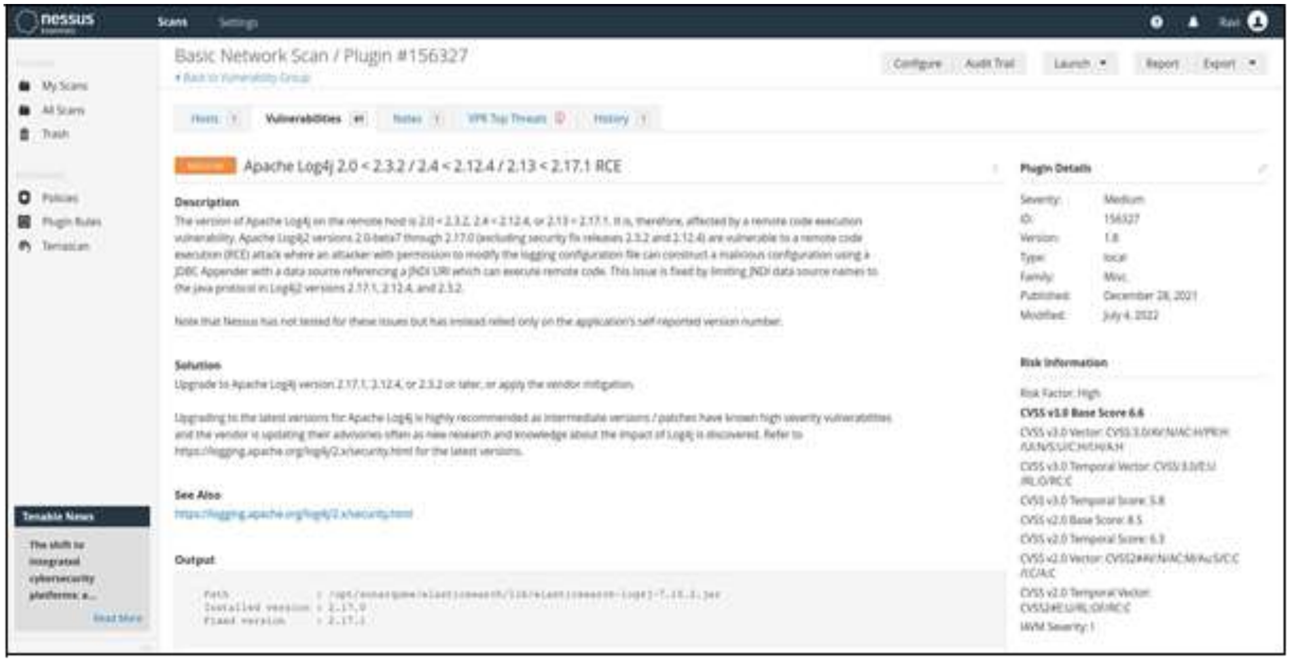
41 Vulnerabilities

Sev ▴	Score ▾	Name ▴	Family ▴	Count ▾
MIXED	...	SSL (Multiple Issues)	General	4
MIXED	...	Apache Log4j (Multiple Issues)	Misc.	2
INFO	...	SSH (Multiple Issues)	General	6
INFO	...	DNS (Multiple Issues)	DNS	3
INFO	...	Apache HTTP Server (Multiple Issues)	Web Servers	2
INFO	...	HTTP (Multiple Issues)	Web Servers	2
INFO	...	TLS (Multiple Issues)	Service detection	2
INFO		Netstat Portscanner (SSH)	Port scanners	16
INFO		MariaDB Client/Server Installed (Linux)	Databases	2
INFO		PostgreSQL Client/Server Installed (Linux)	Databases	2

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 1:20 AM
End:	Today at 1:28 AM
Elapsed:	8 minutes

Vulnerabilities



Basic Network Scan / Plugin #156327

◂ Back to Vulnerability Group

Apache Log4j 2.0 < 2.3.2 / 2.4 < 2.12.4 / 2.13 < 2.17.1 RCE

Description

The version of Apache Log4j on the remote host is 2.0 < 2.3.2, 2.4 < 2.12.4, or 2.13 < 2.17.1. It is, therefore, affected by a remote code execution vulnerability. Apache Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4) are vulnerable to a remote code execution (RCE) attack where an attacker with permission to modify the logging configuration file can construct a malicious configuration using a JDBC Appender with a data source referencing a JNDI URI which can execute remote code. This issue is fixed by limiting JNDI data source names to the java protocol in Log4j2 versions 2.17.1, 2.12.4, and 2.3.2.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache Log4j version 2.17.1, 2.12.4, or 2.3.2 or later, or apply the vendor mitigation.

Upgrading to the latest versions for Apache Log4j is highly recommended as intermediate versions / patches have known high severity vulnerabilities and the vendor is updating their advisories often as new research and knowledge about the impact of Log4j is discovered. Refer to https://logging.apache.org/log4j/2.x/security.html for the latest versions.

See Also

https://logging.apache.org/log4j/2.x/security.html

Output

```
  Path              : /opt/sonarqube/elasticsearch/lib/elasticsearch-log4j-7.16.2.jar
  Installed version : 2.17.0
  Fixed version     : 2.17.1
```

Plugin Details

Severity:	Medium
ID:	156327
Version:	1.8
Type:	local
Family:	Misc.
Published:	December 28, 2021
Modified:	July 4, 2022

Risk Information

Risk Factor: High

CVSS v3.0 Base Score 6.6

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H

CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C

CVSS v3.0 Temporal Score: 5.8

CVSS v2.0 Base Score: 8.5

CVSS v2.0 Temporal Score: 6.3

CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:S/C:C/I:C/A:C

CVSS v2.0 Temporal Vector: CVSS2#E:U/RL:OF/RC:C

IAVM Severity: I

References : https://adamtheautomator.com/install-nessus-on-kali/