Vulnerability Scan Report

Target: Localhost
Date: 25/9/2025
Tool: Nessus Essentials

Summary:

The scan was performed on the local machine to identify common security vulnerabilities. Below are the findings and recommendations.

Critical Vulnerabilities:

1. Oracle Database outdated version
    - CVSS Score: 10.0 (High)
    - Risk: No new security patches will be received
    - Fix: Upgrade to the version Oracle Database is currently supported

2. Oracle TNS Listener Remote Poisoning
    - CVSS Score: 7.3 (High)
    - Risk: Successful exploits will allow the attacker to manipulate database instances, potentially facilitating man-in-the-middle, session-hijacking, or denial of service attacks.
    - Fix: Apply the workaround in Oracle’s advisory.

3. SMB Signing not required
    - CVSS Score: 5.9 (Medium)
    - Risk: An unauthenticated, remote attacker can exploit this to conduct MITM attacks against SMB server.
    - Fix: Enforce message signing in the host’s configuration.

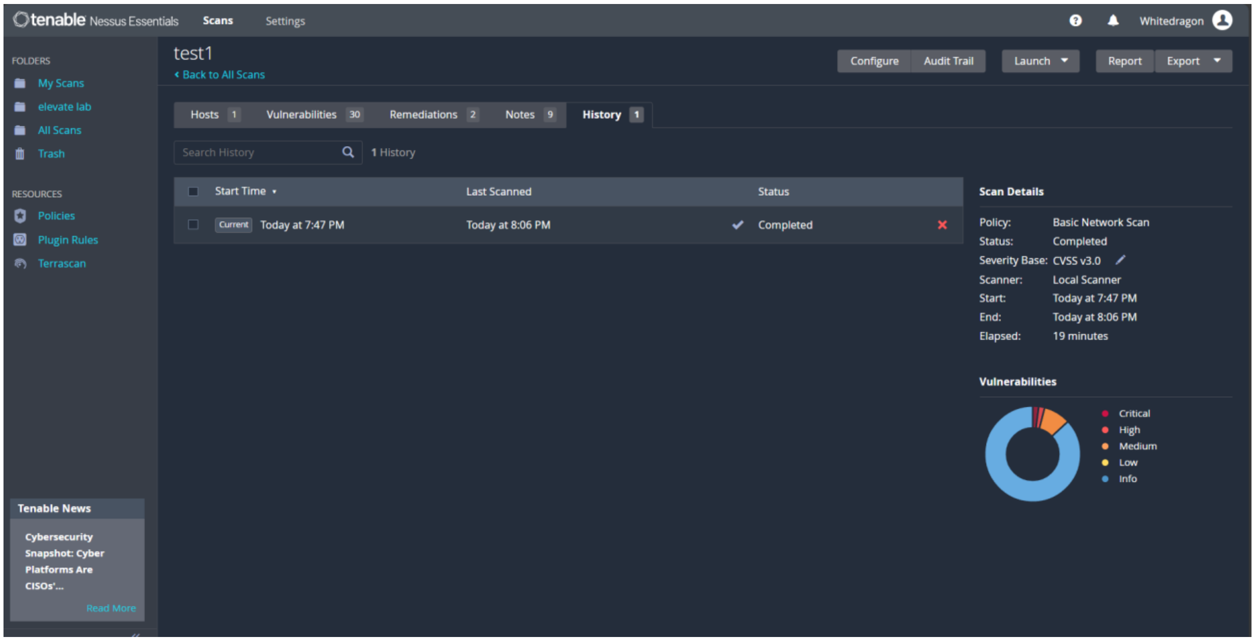
Recommendations:

- Oracle Application Express:Upgrade Application Express to at least version 4.1.1.

-Apply the workaround in oracle’s advisory
- Enable strong authentication and encryption mechanisms.
- Perform vulnerability scans monthly to maintain security posture.

Conclusion:

The scan identified outdated services and weak configurations that could be exploited by attackers. Applying the recommended fixes will significantly reduce the attack surface.



test1

‹ Back to All Scans

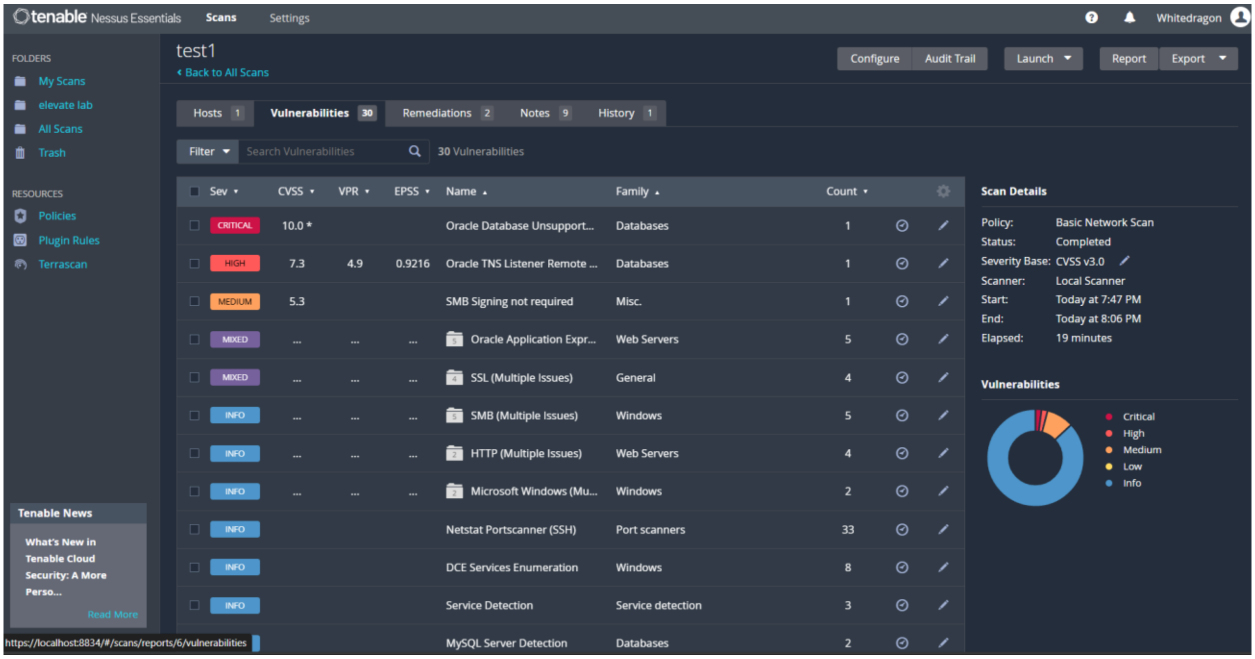
1 History

Start Time	Last Scanned	Status
Current Today at 7:47 PM	Today at 8:06 PM	✓ Completed

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 7:47 PM
End:	Today at 8:06 PM
Elapsed:	19 minutes

Vulnerabilities



test1

‹ Back to All Scans

30 Vulnerabilities

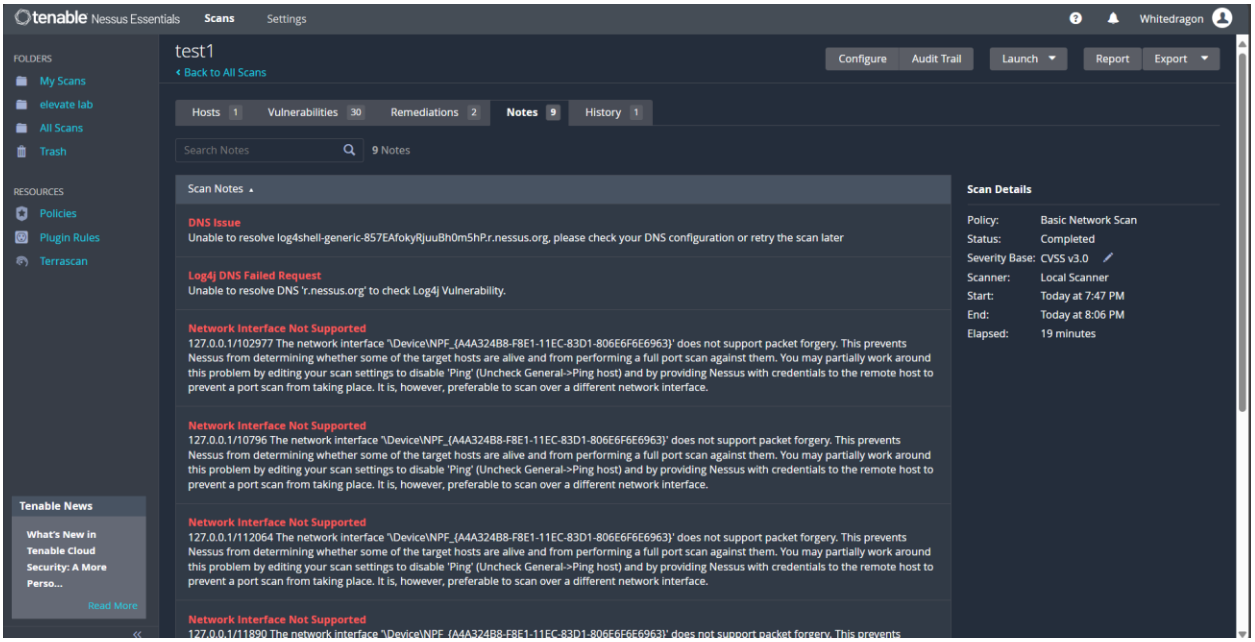
Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0 *			Oracle Database Unsupport...	Databases	1
HIGH	7.3	4.9	0.9216	Oracle TNS Listener Remote ...	Databases	1
MEDIUM	5.3			SMB Signing not required	Misc.	1
MIXED	...	...	...	5 Oracle Application Expr...	Web Servers	5
MIXED	...	...	...	4 SSL (Multiple Issues)	General	4
INFO	...	...	...	5 SMB (Multiple Issues)	Windows	5
INFO	...	...	...	2 HTTP (Multiple Issues)	Web Servers	4
INFO	...	...	...	2 Microsoft Windows (Mu...	Windows	2
INFO				Netstat Portscanner (SSH)	Port scanners	33
INFO				DCE Services Enumeration	Windows	8
INFO				Service Detection	Service detection	3
				MySQL Server Detection	Databases	2

https://localhost:8834/#/scans/reports/6/vulnerabilities

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 7:47 PM
End:	Today at 8:06 PM
Elapsed:	19 minutes

Vulnerabilities



test1

‹ Back to All Scans

DNS Issue
Unable to resolve log4shell-generic-857EAfokyRjuuBh0m5hP.r.nessus.org, please check your DNS configuration or retry the scan later

Log4j DNS Failed Request
Unable to resolve DNS 'r.nessus.org' to check Log4j Vulnerability.

Network Interface Not Supported
127.0.0.1/102977 The network interface '\Device\NPF_{A4A324B8-F8E1-11EC-83D1-806E6F6E6963}' does not support packet forgery. This prevents Nessus from determining whether some of the target hosts are alive and from performing a full port scan against them. You may partially work around this problem by editing your scan settings to disable 'Ping' (Uncheck General->Ping host) and by providing Nessus with credentials to the remote host to prevent a port scan from taking place. It is, however, preferable to scan over a different network interface.

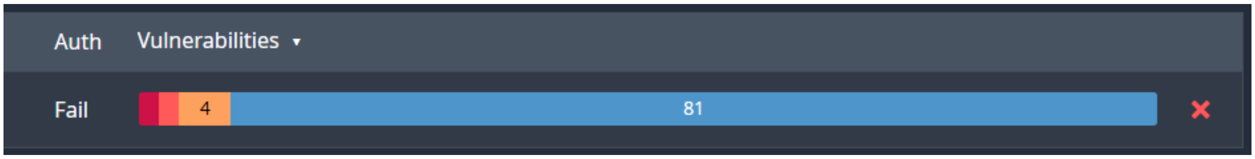
Network Interface Not Supported
127.0.0.1/10796 The network interface '\Device\NPF_{A4A324B8-F8E1-11EC-83D1-806E6F6E6963}' does not support packet forgery. This prevents Nessus from determining whether some of the target hosts are alive and from performing a full port scan against them. You may partially work around this problem by editing your scan settings to disable 'Ping' (Uncheck General->Ping host) and by providing Nessus with credentials to the remote host to prevent a port scan from taking place. It is, however, preferable to scan over a different network interface.

Network Interface Not Supported
127.0.0.1/112064 The network interface '\Device\NPF_{A4A324B8-F8E1-11EC-83D1-806E6F6E6963}' does not support packet forgery. This prevents Nessus from determining whether some of the target hosts are alive and from performing a full port scan against them. You may partially work around this problem by editing your scan settings to disable 'Ping' (Uncheck General->Ping host) and by providing Nessus with credentials to the remote host to prevent a port scan from taking place. It is, however, preferable to scan over a different network interface.

Network Interface Not Supported
127.0.0.1/11890 The network interface '\Device\NPF_{A4A324B8-F8E1-11EC-83D1-806E6F6E6963}' does not support packet forgery. This prevents

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 7:47 PM
End:	Today at 8:06 PM
Elapsed:	19 minutes



Auth	Vulnerabilities ▾
Fail	4 81 ✕