Task - 7

Hiya Sharma
21BCY10078

Date:4/9/2023

Vulnerability report-

Nessus tool-

Nessus is a remote security scanning tool, which scans a computer network and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network.

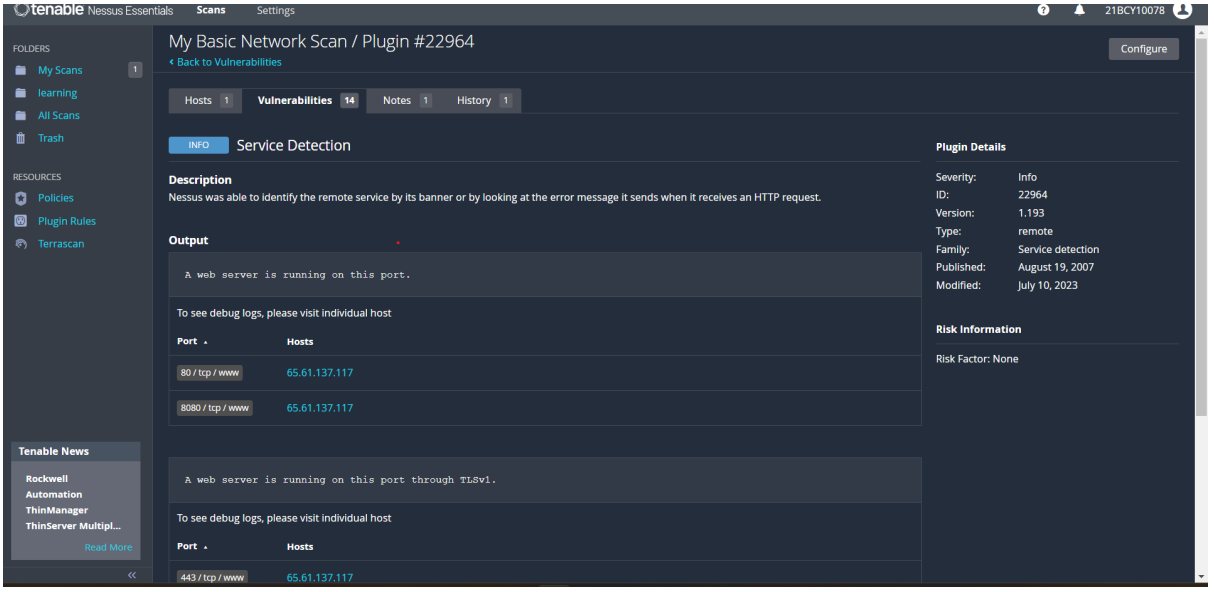
After scanning an IP address using Nessus, you can obtain a variety of valuable information and insights, including:

- Vulnerability Assessment: Nessus identifies known vulnerabilities and potential security issues present on the scanned system, services, or applications. It provides a detailed list of vulnerabilities, categorized by severity and impact.
- Risk Assessment: The tool assigns risk scores to vulnerabilities, helping you prioritize remediation efforts based on the level of risk each vulnerability poses to your system.
- Detailed Reports: Nessus generates comprehensive reports that include a summary of findings, detailed descriptions of vulnerabilities, recommendations for mitigation, and references to external resources for further information.
- CVSS Scores: Common Vulnerability Scoring System (CVSS) scores are provided for each identified vulnerability. These scores help you gauge the severity of the vulnerabilities and prioritize patching or mitigation.
- Compliance Auditing: Nessus supports compliance checks against various industry standards and regulatory requirements, such as CIS benchmarks, PCI DSS, HIPAA, and more. It helps organizations ensure compliance with specific security standards.
- Asset Discovery: Nessus can discover and enumerate devices, systems, and services running on the scanned network, providing visibility into your IT infrastructure.
- Credential-Based Scanning: When credentials are provided, Nessus can perform authenticated scans, allowing for a more accurate assessment of the system's security posture by accessing internal configuration and settings.
- Historical Data: Nessus allows you to track and compare scan results over time, helping you monitor improvements or regressions in your security posture.
- Customization: You can customize Nessus scans by specifying target IPs, ports, and specific tests or plugins to run, tailoring the assessment to your organization's needs.

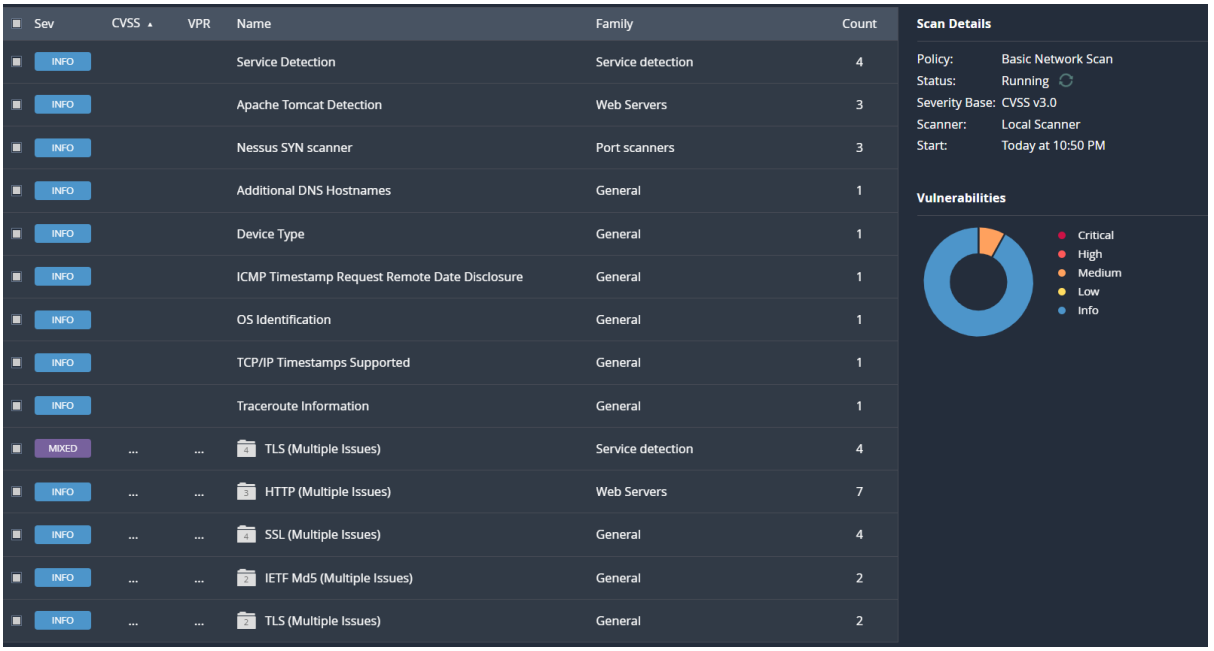
- Remediation Recommendations: Nessus often provides recommendations and guidance on how to remediate identified vulnerabilities or misconfigurations, making it easier for administrators to address security issues.

Affected URL- http://testfire.net/

IP address- 65.61.137.117



Found 14 vulnerabilities.




Back to My Scans
Hosts 1
Vulnerabilities 15
Notes 1
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
%
65.61.137.117
2
1
33
99%
Scan Details
Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 10:50 PM
Vulnerabilities
Critical
High
Medium
Low
Info