Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

Batch: B1 Roll No.: 16010121045

Experiment No. 5

Title: Use Nessus/OpenVAS and NIKTO tool to find all the vulnerabilities

Objective:
Use Nessus/OpenVAS and NIKTO tool to find all the vulnerabilities

CO	Outcome
CO2	Perform Penetration testing and vulnerability assessment on various systems

Books/ Journals/ Websites referred:

- Web Penetration Testing with Kali Linux, Joseph Muniz, Aamir Lakhani, Packt Publishing, 2013.
- Hacking Exposed 7: Network Security Secrets and Solutions, George Kurtz, Joel Scambray, and Stuart McClure, McGraw Hill, 2012.

Introduction:

Nessus/OpenVAS: Nessus and OpenVAS are both popular vulnerability scanners used by organizations to identify security vulnerabilities within their networks, systems, and applications. They work by scanning the target environment for known vulnerabilities and misconfigurations, providing valuable insights into potential weaknesses that could be exploited by malicious actors.

Features:

1. **Scanning Capabilities**: Both Nessus and OpenVAS offer comprehensive scanning capabilities, including network scanning, application scanning, and compliance auditing.
2. **Database of Vulnerabilities**: They maintain extensive databases of known vulnerabilities, which are continuously updated to ensure accurate detection of the latest threats.
3. **Customization**: Users can customize scans based on their specific requirements, such as targeting certain types of vulnerabilities or specific network segments.
4. **Reporting**: Both tools generate detailed reports that highlight identified vulnerabilities, their severity levels, and recommended remediation steps.

Nessus:

- **Commercial Solution**: Nessus is a commercial vulnerability scanner developed and maintained by Tenable, Inc. It offers a user-friendly interface and advanced features tailored for enterprise environments.
- **Scalability**: Nessus is scalable and suitable for large organizations with complex IT infrastructures.
- **Advanced Policies**: It provides advanced policy creation options, allowing users to define specific scan parameters and compliance requirements.

OpenVAS:

- **Open Source**: OpenVAS (Open Vulnerability Assessment System) is an open-source alternative to Nessus. It is developed as a collaborative project under the GNU General Public License (GPL).
- **Community Support**: OpenVAS benefits from a strong community of developers and contributors who continuously improve its functionality and update vulnerability databases.
- **Customization and Flexibility**: Being open source, OpenVAS offers greater flexibility and customization options for users who prefer to tailor the tool to their specific needs.

Nikto: Nikto is an open-source web server scanner that performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/CGIs, outdated versions of over 1250 servers, and version-specific problems on over 270 servers.

Features:

1. **Web Server Testing**: Nikto focuses specifically on testing web servers for various vulnerabilities and misconfigurations.
2. **Wide Range of Checks**: It conducts a wide range of checks, including outdated server software, server configuration issues, and potential security risks in web applications.

3. **Customizable Scanning**: Nikto allows users to customize scans by specifying target ports, specific plugins, and exclusion criteria.
4. **Reporting**: Similar to Nessus and OpenVAS, Nikto generates detailed reports that highlight identified vulnerabilities and recommended actions for remediation.

Usage and Reporting:

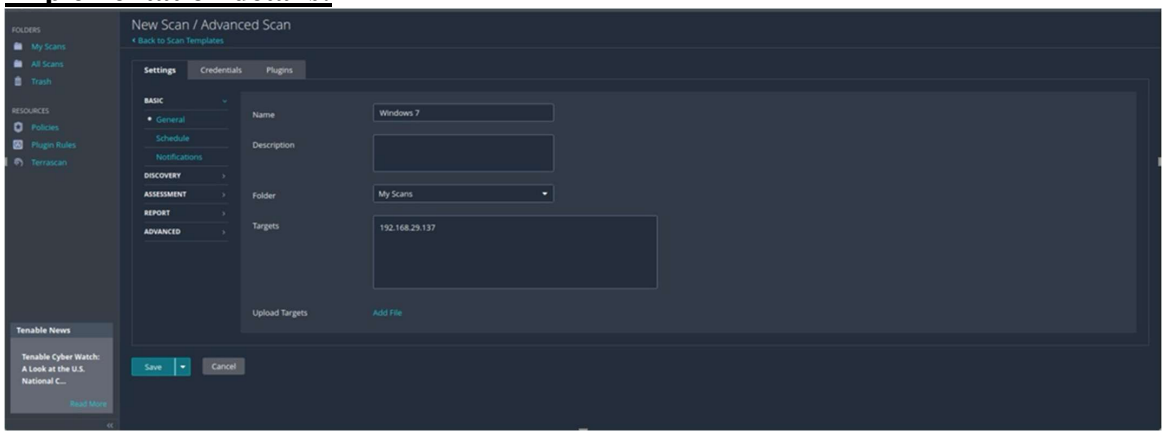
1. Scanning:

- Organizations can utilize Nessus/OpenVAS to perform network scans to identify vulnerabilities within their infrastructure, while Nikto can be used specifically for web server scanning.
- These tools employ a combination of active and passive scanning techniques to comprehensively assess the security posture of the target environment.

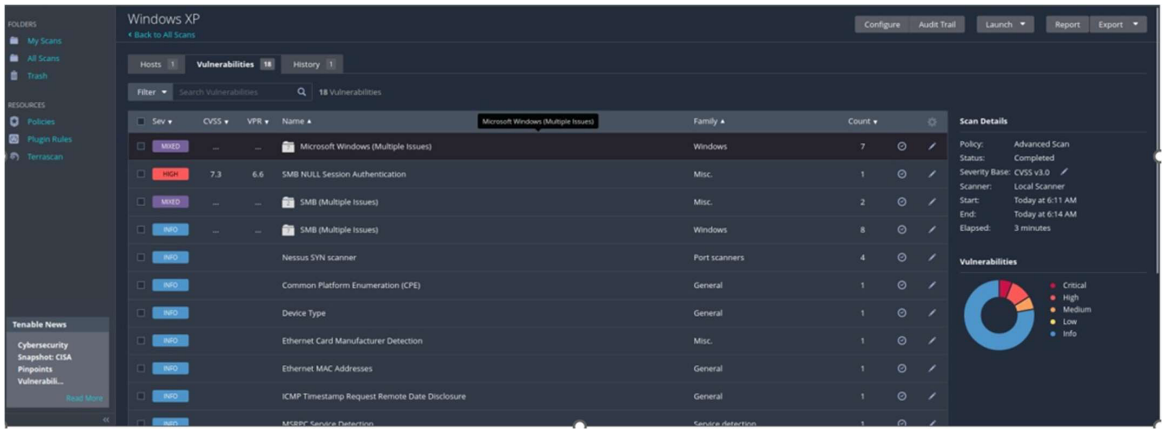
2. Analysis and Reporting:

- Once the scans are completed, Nessus/OpenVAS and Nikto generate detailed reports that categorize vulnerabilities based on severity levels (e.g., critical, high, medium, low) and provide recommendations for remediation.
- Reports typically include an executive summary, detailed findings, risk ratings, and actionable insights for addressing identified vulnerabilities.
- Organizations can use these reports to prioritize remediation efforts, allocate resources effectively, and improve their overall security posture.

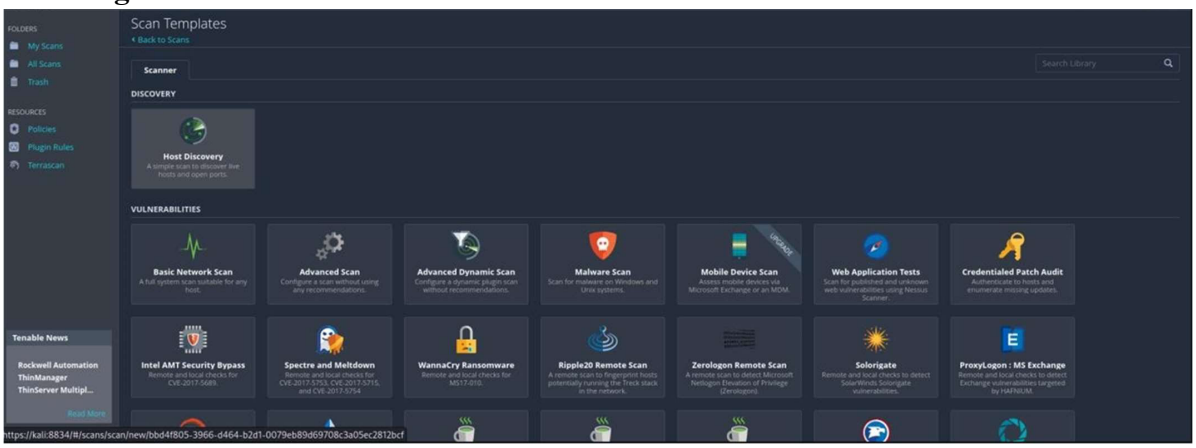
Implementation details:

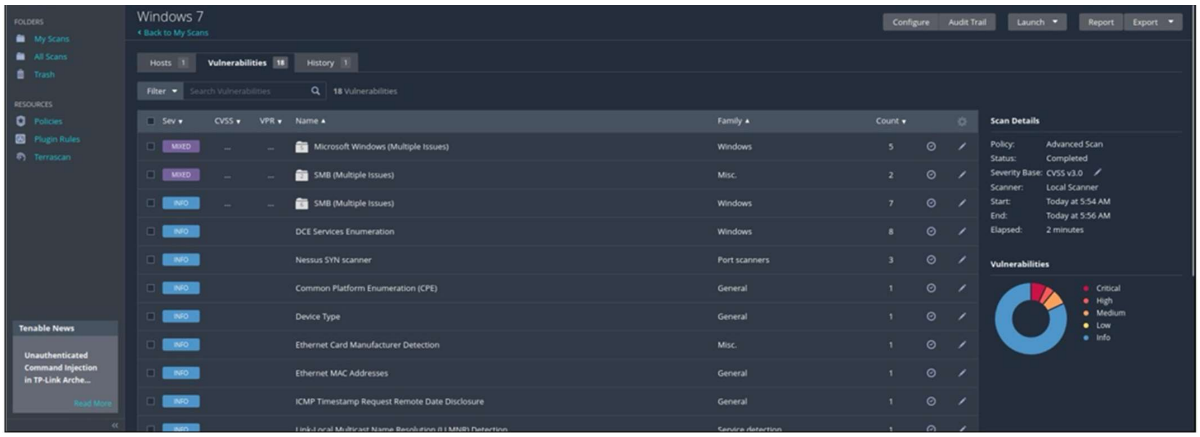


Windows XP Scan



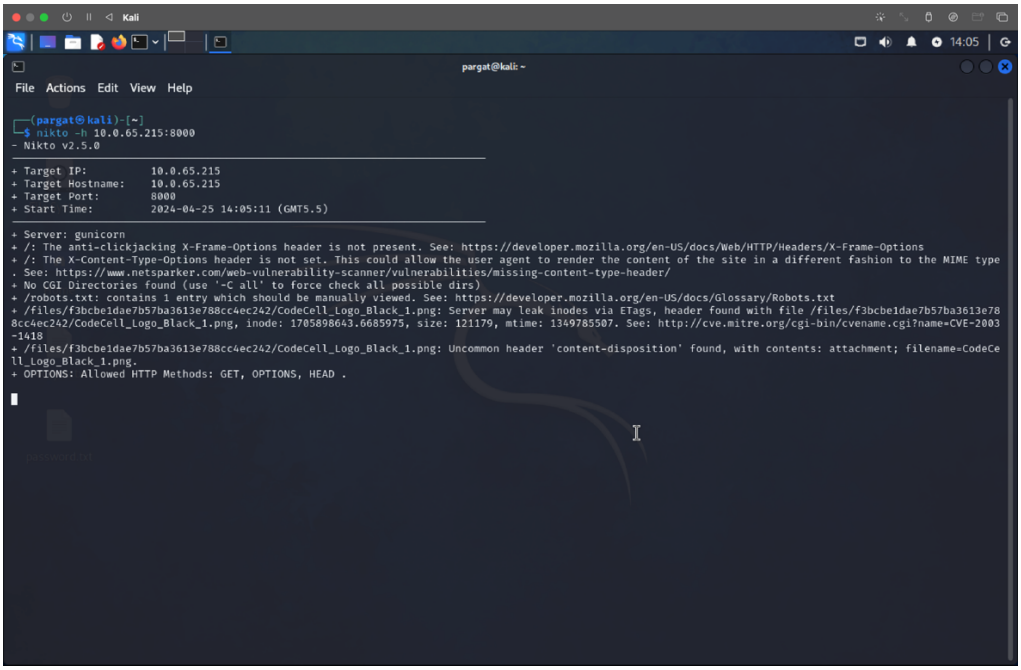
Scanning Windows 7 -

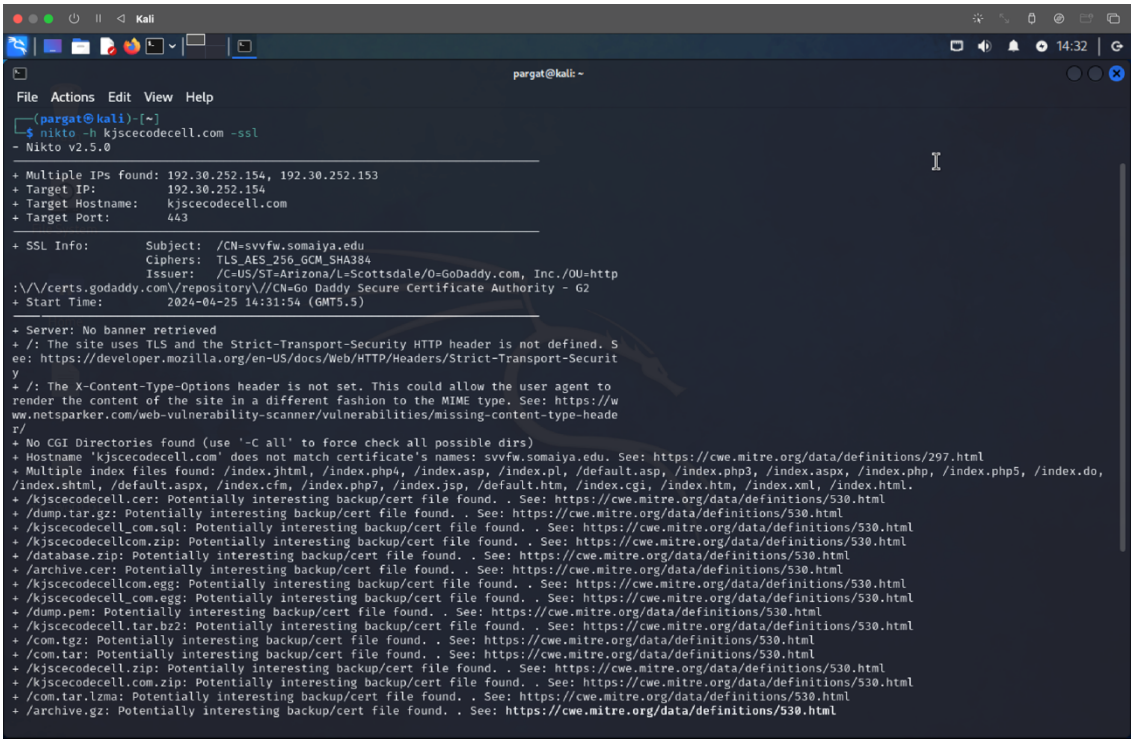




Nikto:

Normal Nikto Scan





Conclusion:

From this experiment, we have successfully studied Nessus/OpenVAS and NIKTO tool to find all the vulnerabilities with its level and generate a report for an organization