Department of Information Technology

Academic Year: 2022-23 **Semester: V**
Class / Branch: TE IT
Subject: Security Lab (SL)
Subject Lab Incharge: Prof. Apeksha Mohite

EXPERIMENT NO. 7

Aim : To study usage of NESUS/ISO Kaali Linux for scanning network vulnerabilities

Theory:

Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools. Nessus employs the Nessus Attack Scripting Language (NASL), a simple language that describes individual threats and potential attacks.

Nessus has a modular architecture consisting of centralized servers that conduct scanning, and remote clients that allow for administrator interaction. Administrators can include NASL descriptions of all suspected vulnerabilities to develop customized scans.

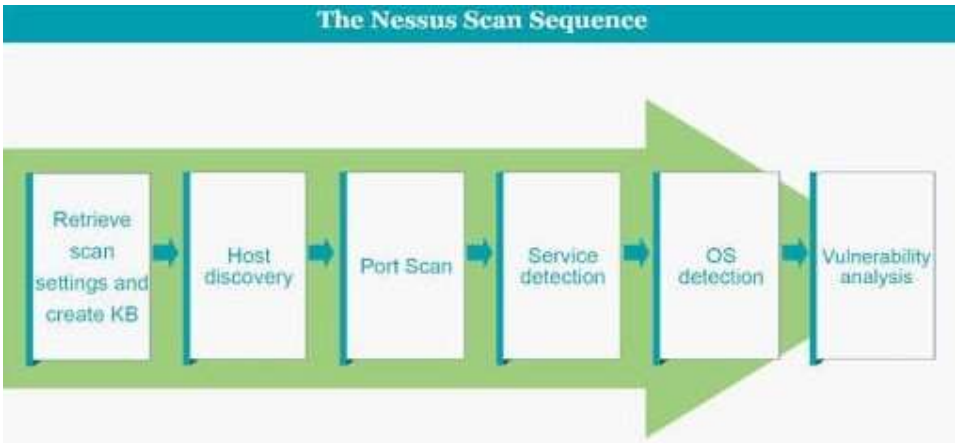
Significant capabilities of Nessus include:

- Compatibility with computers and servers of all sizes.
- Detection of security holes in local or remote hosts.
- Detection of missing security updates and patches.
- Simulated attacks to pinpoint vulnerabilities.
- Execution of security tests in a contained environment.
- Scheduled security audits.

The Nessus server is currently available for Unix, Linux and FreeBSD. The client is availablefor Unix- or Windows-based operating systems.

Parshvanath Charitable Trust's
A. P. SHAH INSTITUTE OF TECHNOLOGY
(Approved by AICTE New Delhi & Govt. of Maharashtra, Affiliated to University of Mumbai)
(Religious Jain Minority)

High speed asset discovery and scanning	Network devices including next generation firewalls, operating systems, databases, web applications, virtual and cloud environments and more
Scan multiple networks	Scan on IPv4, IPv6 and hybrid networks
Credentialed / non-credentialed	Flexible scanning options to meet different needs
Scan scheduling	Set up scans to run when and how often you want
Selective host re-scanning	After a scan, re-scan all or a subsection of previously scanned hosts



Conclusion: Thus we have studied the usage of Nessus as a Vulnerability scanning in kali linux.