Experiment- 4

Aim: Vulnerability Scanning using with Nessus

DESCRIPTION:

Nessus

Nessus is one of the many vulnerability scanners used during vulnerability assessments and penetration testing engagements, including malicious attacks. This article will focus on this vulnerability scanner, discussing the fundamentals that one needs to have before getting started with the tool, the different scanning capabilities that it provides, what it takes to run the tool and how results appear once scans are complete.

Vulnerability scanning with Nessus

Nessus performs its scans by utilizing plugins, which run against each host on the network in order to identify vulnerabilities. Plugins can be thought of as individual pieces of code that Nessus uses to conduct individual scan types on targets. Plugins are numerous and wide in their capabilities. For instance, a plugin could be launched and targeted at a host to:

1) Identify which operating systems and services are running on which ports
2) Identify which software components are vulnerable to attacks (FTP, SSH, SMB and more)
3) Identify if compliance requirements are met on various hosts

When you launch a scan, Nessus goes through a series of steps.

Step 1: Nessus will retrieve the scan settings. The settings will define the ports to be scanned, the plugins to be
enabled and policy preferences definitions.

Step 2: Nessus will then perform host discovery to determine the hosts that are up. The protocols used in host
discovery will be ICMP, TCP, UDP and ARP. You can specify these per your desires.

Step 3: Nessus then performs a port scan of each host that is discovered to be up. You can also define which
ports you will want to be scanned. Ports can be defined in ranges or individually, with valid ports ranging from
1 to 65535.

Step 4: Nessus will then perform service detection to determine the services that are running behind each port
on each host discovered

Step 5: Nessus then performs operating system detection.

Step 6: Once all the steps are complete, Nessus runs each host against a database of known vulnerabilities in an
attempt to discover which host contains which vulnerabilities.