eJPT Certification

Section: Vulnerability Assessment

09/10/2020

**­­Learning Objectives**

* Automatic vulnerability detection.
* Common tools that are used for vulnerability assessment.
* Why is this important?
  + Identify vulnerabilities and security misconfigurations.
  + Prepare yourself for the exploitation phase.
* Vulnerability assessments are faster than traditional pentests and have a lighter load on the client infrastructure. Do not need to proceed to the exploitation phase.
* Vulnerability Assessment Process:
  + Engagement
  + Information Gathering
  + Footprinting and Scanning
  + Vulnerability Assessment
  + Reporting
* Vulnerability assessment can be done both locally and remotely.
* **Vulnerability Scanners**
  + Scanners use a database of known vulnerabilities and security audits to detect vulnerabilities of a system. Scanners perform their probes on:
    - Daemons listening on TCP and UDP ports
    - Configuration files of operating systems, software suites, network devices, etc.
    - Windows registry entries.
  + OpenVAS, Nexpose, GFI LAN Guard, and Nessus are a few popular vulnerability scanners. Nessus is most popular.
* When testing a custom application, a vulnerability scanner probably wont be enough. You will have to do some testing manually.
  + Studying Custom apps means:
    - Learning and understanding its features.
    - Understanding how it exchanges data over the network.
    - Understanding how it accesses resources like database, servers, local and remote files and so on.
    - Reverse engineering its logic.

**Nessus**

* Vulnerability scanner
* Free license and also pro license
* **Architecture** 
  + Two components: client and server.
  + Client component is a web interface where we can make all of our scanning configurations
  + Server component conducts scans by sending probes to systems and apps, collecting responses and matching them against the vulnerability database.
  + Client and server can run on the same machine.
* **Port Scanning**
  + Determining which hosts are alive and scanning each host to find which ports are open.
* **Service Detection** 
  + Every port found, the scanner will probe them to find which app (name and version) is running on them.
* **Vulnerabilities and Database Lookup**
  + For each detected service (known as daemons) the scanner queries its database looking for known vulnerabilities.
  + When configuring the scanner, we are able to setup the scanner to look for specific vulnerabilities.
* **Probing**
  + During the last step, the scanner sends probes to verify the vulnerability.
    - Beware, the assessment is prone to false positives as some probes could be too mild to effectively identify a real vulnerability.