

Vulnerability Analysis

Industrial Control Systems Security Workshop
June 22-23, 2017



Vulnerability

Failure of security policies, procedures, and controls that allow a subject to commit an action that violates the security policy

Penetration Testing

- Testing to verify that a system satisfies certain constraints
- Hypothesis stating system characteristics, environment, and state relevant to vulnerability
- Result is compromised system state
- Apply tests to try to move system from state in hypothesis to compromised system state

Vulnerability

—Assessment Tools—

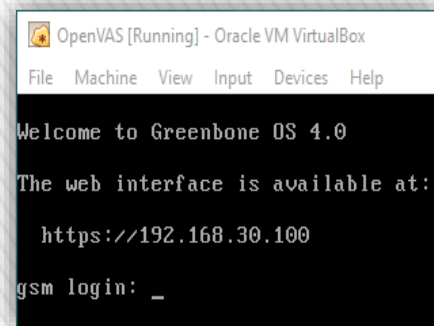
- » **Nessus** — previously open-source, free home edition
- » **OpenVas**—came from free version of Nessus but slowly being commercialized
- » **QualysGuard**—Software as a service (SaaS) tool
- » **Retina**—eEye product, scans all hosts and generates a comprehensive VA report
- » **Nexpose**— integrates easily with Metasploit, a penetration tool

OpenVas


- » Vulnerability scanning is a preliminary phase of a penetration test by discovering vulnerable items in the system or network before performing the more intrusive actions.
- » Follow the instructions at <http://openvas.org/vm.html> to import the newest version of the application
- » After you have created the virtual machine, double-click on it in VirtualBox. The virtual machine will launch in a separate window

OpenVas

- » After the virtual machine finishes booting up, it should display an IP address you will use to log into the web interface.



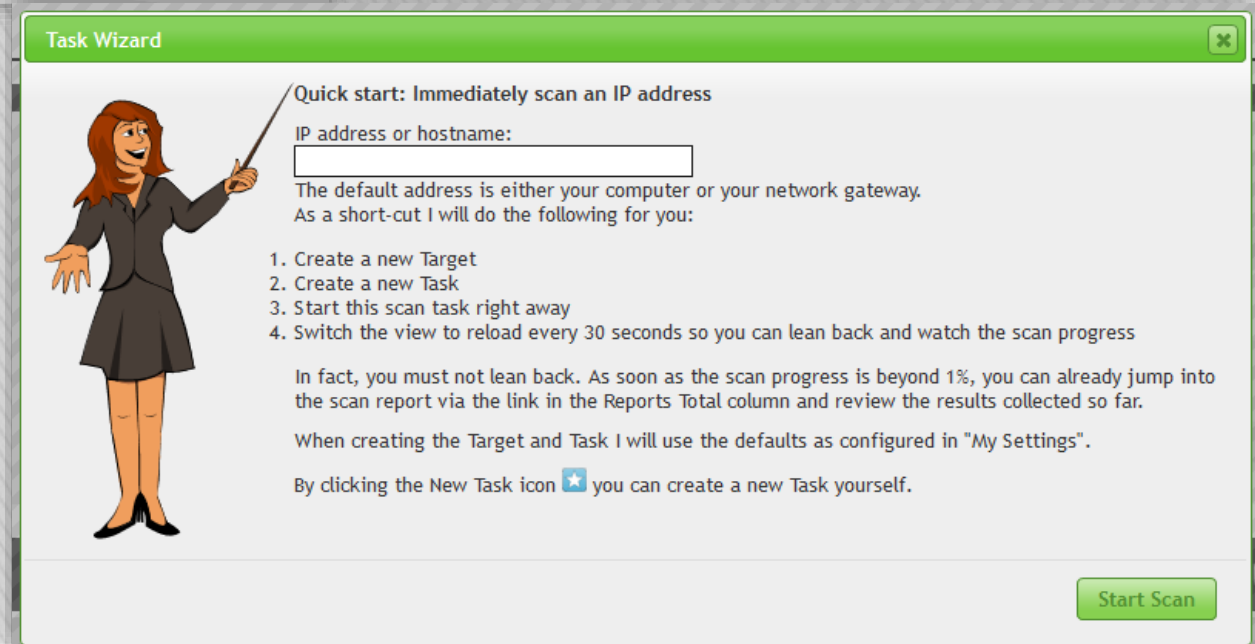
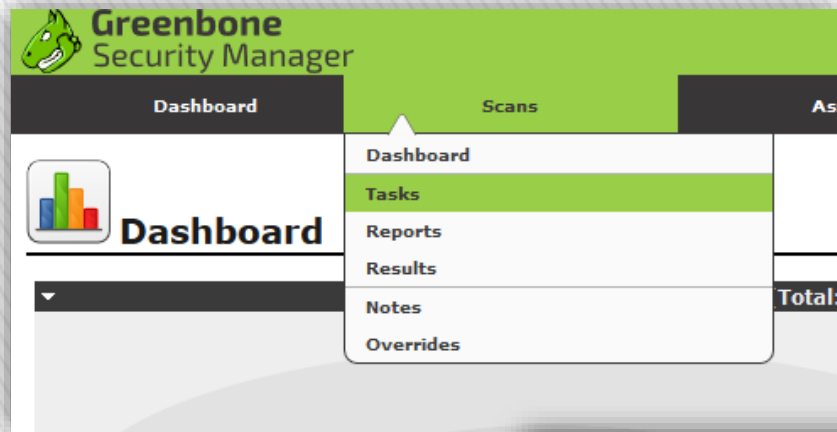
- » Open a web browser, such as Firefox or Google Chrome
- » Type the full address displayed on your virtual machine (including the "http://") into the address bar of your web browser, just as you would navigate to a web site.



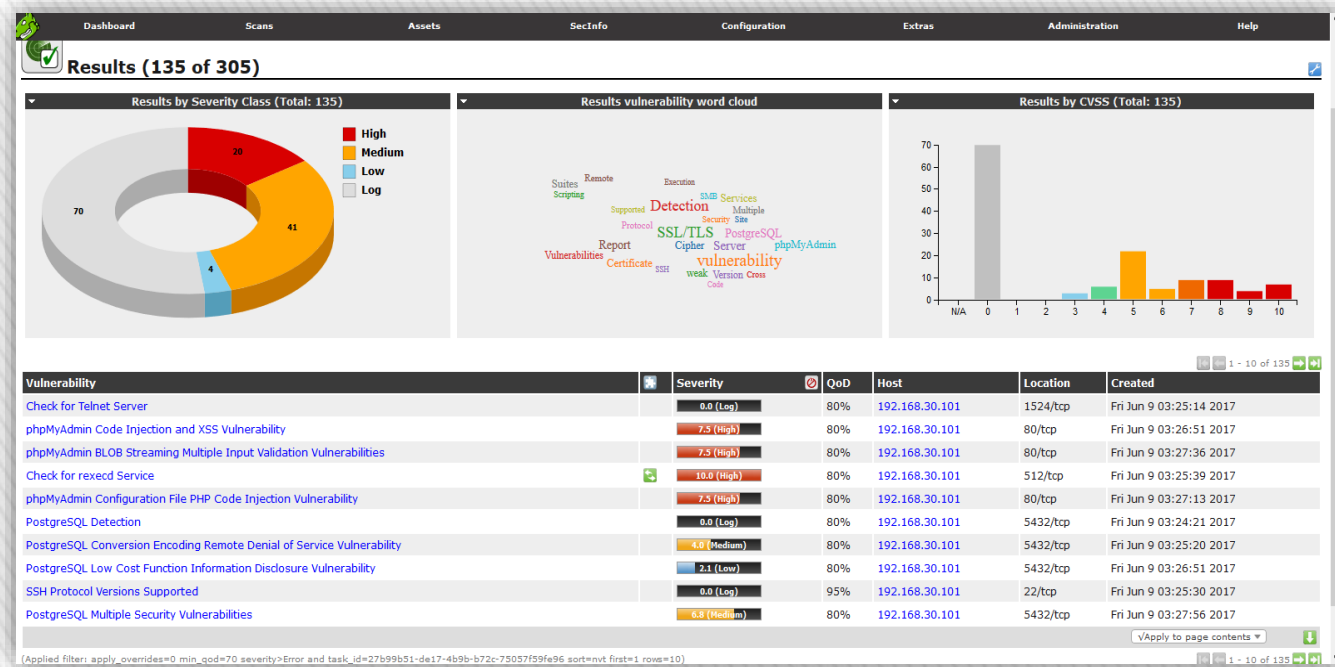
Username:

Password:

Openvas Login



Start Scan



Scan Results