**Undergraduate Program in Information Assurance Engineering**

# IA-201: Introduction to Information Assurance

Lab 6 – Vulnerability Scanning & Patching – Nessus

**Lab Objective:**

The objective of this lab is to introduce students to Nessus. Students will understand what vulnerabilities are and what risk they pose to a network. Students will understand how to scan a host and network using Nessus to find vulnerabilities and other network information.

**Laboratory Deliverable:**

1. Screenshot of vulnerabilities on Windows box.
2. Screenshot of vulnerabilities of Metasploitable box.

**Materials:**

1. Windows Virtual Machine
2. Metasploitable Virtual Machine

**Instructions:**

1. On the Windows box, go to <http://www.tenable.com/products/nessus/select-your-operating-system> and download the appropriate file for the Windows operating system.
2. Go to <http://www.tenable.com/products/nessus-home> and register a home account for your Nessus. You will need the registration code that is sent to your e-mail.
3. Install Nessus. After Nessus is installed, go to your web browser and go to your Nessus web page. If it doesn’t open automatically, enter into the URL <https://localhost:8834/> .
4. Create a user for Nessus.
5. Copy the activation code Tenable sent you and enter it into the form when it asks you.
6. Click “Download Plugins”. It will take a moment for the plugins to download.
7. Login to the Nessus web portal with the credentials you created earlier.

Nessus is a network vulnerability scanner that searches for known exploits on hosts. It will compile scan results that allows an analyst to properly assess weaknesses in a network. Nessus keeps up to date on current exploits and vulnerabilities that allow for constant current network monitoring.

1. Click on “Scan Queue” and then “New Scan”.
2. In the Name field, enter your name. Leave the Type field as “Run Now”. Add “127.0.0.1” to the Scan Targets field.
3. Click “Run Scan” now. This will take a while as it is scanning your whole system (the Windows box) for many different possible vulnerabilities.
4. Go to the “Results” page and click on the scan.
5. Click on the host “127.0.0.1”.

Take a screenshot once the full scan is complete.

What Nessus is doing is performing many tests on your local host computer. It is assessing its services and looking for vulnerabilities.

1. Click the “Netstat portscanner” and examine the ports opened on your computer.
2. Click the “Service Detection” and examine the services on your computer.
3. Startup the Metasploitable VM and login.
4. Run another scan with the name set to your name and append Metasploitable, set the policy field set to “External Network Scan” and set the Scan Targets field to the IP address of the Metasploitable VM (**192.168.107.129**). Run the scan.
5. Go to the “Results” page and click on the Metasploitable scan.
6. Click the host.

Take a snapshot of the vulnerabilities once the scan is complete.

1. Click the “Netstat portscanner” and examine the ports opened on Metasploitable.

This shows the ports that are open on the host.

1. Click the “Service Detection” and examine the services on Metasploitable.
2. Click the “TWiki rev Parameter Arbitrary Command Execution” vulnerability. Examine the synopsis, description, and solution.

This is an exploit that exists on the web server. The web server is running a web service called TWiki which has a command execution vulnerability. What this means is that an attacker could execute commands on the server without permission.

1. Click on a critical vulnerability and examine the issue.

On large scale networks, Nessus is run on a periodic basis making sure that all services are up to date and no know vulnerabilities exist. These reports make hardening servers and services much easier by compiling what the issues are and what the solutions are to fix them.

==END==

**Questions:**

1. What is Nessus?  **A network vulnerability scanner that searches for known exploits on hosts.**
2. Why is a tool like Nessus important? **It allows for constant current network monitoring**
3. How many vulnerabilities did Windows have? **35**
4. How many vulnerabilities did Metasploitable have? **0**
5. What critical leveled vulnerabilities are there on the Metasploitable box? **0**
6. What is the solution to fix each of the critical leveled vulnerabilities? **NA**
7. Do you see any non-critical vulnerabilities in the Metasploitable box that you find interesting or might pose a risk? What are they? What are the solutions to fix them?**NA**

|  |  |  |  |
| --- | --- | --- | --- |
| Requirement | **Points Allowed** | **Points Actual** | **Comments** |
|  |  |  |  |
| **Title page** | **5** |  |  |
| **Screen shots** | **5** |  |  |
| **Questions** | **10** |  |  |
| **Conclusion** | **5** |  |  |
|  |  |  |  |
| **Extra Credit** |  |  |  |
|  |  |  |  |
|  |  |  |  |
| **Total Points** | **25** |  |  |