

# Network Mapping and Vulnerability Scanning

## Objective

The purpose of this lab is to gain an understanding of some of the basic reconnaissance tools that are available to an outside attacker. Imagine that you are interested in launching an attack against some organization. Assume you have already used Whois and found the IP address range of the target organization.

Now you want to “case the joint” and gather as much information as you can about the target network including the identification of any vulnerabilities which reside on hosts within this network.

## 1.0 Map the Network

Using the tools nmap and Nessus gather information about the network. Specifically:

- IP addresses of hosts
- Open ports on the hosts
- OS on each host, including OS version
- Any potential vulnerabilities on the host which are returned by the tools.

You will first need to familiarize yourself with both nmap and Nessus in order to complete this lab. Google is your friend and there is plenty of information available on the internet. However, here are two links which will get your started:

The best resource for learning nmap can be found at:

<http://nmap.org/book/toc.html>

and the main website for Nessus is located at:

<http://www.tenable.com/products/nessus/documentation>

## 1.1 Nmap Scan

First be sure that all of your virtual machines are powered up. Your primary virtual machine for this lab will be Backtrack 5. The username is “root” with a password of “toor”

From there you can start the gui using “startx”

You should have a DHCP address assigned to your Backtrack machine. You can verify this by opening a terminal session and typing: `ifconfig`

You will use the Backtrack 5 VM as your platform to perform this reconnaissance. You will find that both nmap and Nessus are preinstalled.

Now, perform an nmap scan of 10.10.111.0/24 and document which hosts are present on this subnet. In addition, document the operating systems they are running, TCP ports which are open and the services (and versions of the services if possible) running on these TCP ports. You can do all of the above with a single nmap statement. Be sure to document the nmap statement which you used.

## **I.2 Nessus Vulnerability Scan**

We will now perform a vulnerability scan on this host using the Nessus vulnerability scanner.

In order to launch Nessus perform the following steps:


You first need to create a user account in Nessus. In order to do this select:  
Applications->Backtrack->Vulnerability Assessment->Network Assessment->Vulnerability Scanners->nessus user user add (user is misspelled as sser)

You will be prompted to create a username and password. Select what you wish. You will then be prompted as to whether you want this user to be an administration user. Answer ‘y’.

When it asks you to enter rules for the user you can leave it blank and hit <enter>

Nessus is architected in a client-server model. All communication between the client and server is secured using SSL so we next need to create a digital certificate on the server side.

Run the Nessus server by selecting:  
Applications->Backtrack->Vulnerability Assessment->Network Assessment->Vulnerability Scanners->nessus start



The Nessus server will load a number of plugins. Once this process is completed we can connect to the server by starting Firefox and changing the URL to <https://127.0.0.1:8834/>

A login page will present itself. Login as the nessus user you created,

Accept the certificate warnings (if any). In general accepting certificate warnings is never a good idea as we will demonstrate in a subsequent lab. For now trust me and accept the warnings ;)

The client will connect to the server and your Nessus environment will be ready for use.

*Perform an Nessus scan on the Windows XP host that you identified with the nmap scan. Be sure to take screen shots and capture the report of the vulnerabilities identified.*