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 gather as much information as you can about the target network including the identification of any vulnerability that resides on hosts in this network.

1. 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 vulnerability on the host that are returned by the tools.

You will first need to familiarize yourself with both *nmap* and *Nessus* in order to complete this lab. However, here are two links that will get your started:

The best resource for learning *nmap* can be found at:
http://nmap.org/book/toc.html
The main website for *Nessus* is located at:
http://www.tenable.com/products/nessus/documentation

2. [25 pts] Nmap Scan

First be sure that all of your virtual machines are powered up, starting with the external router (rtr), then the internal router (int-rtr), then the other VMs. Your primary virtual machine for this lab will be Backtrack 5 (bt5). The username is “root” with a password of “toor”.

After you login, start the gui using the command “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. Open up a terminal window and execute the nmap scan of 10.10.111.0/24 from the command line (**not the GUI**).

Document which hosts are present on this subnet as well as their respective operating systems, 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. You must document the *nmap* statement that you used.

What to Submit:

Follow the instructions and document the commands and results using screenshots in your report. Explain what is going on in each screenshot.
[5 pts] Correct nmap command to find the request details.
[5 pts] Find all open ports on all the hosts.
[5 pts] Find the OS on each host, including the OS version.
[10 pts] Potential vulnerabilities found by nmap.

3. [25 pts] 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 mispelled as sser)

You will be prompted to create a username and password. Select what you wish.
You will then be promoted 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 complete (may take a bit of time) 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 demonstrated in a subsequent lab. For now accept the warnings. The client will connect to the server and your Nessus environment will be ready for use.

Perform a 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.

4. [50 pts] Python/SCAPY Programming

Python/SCAPY is a Python module that provides detailed support for networking protocols as well as some common functions for network diagnosis. To run SCAPY, first type Python" at the command prompt, then:

```
import sys
from scapy.all import *
```

At this point you have access to all the features of Python as well as *scapy*. Try out some of the features shown in scapy.pdf to get familiar with *scapy*. If you need information on Python look at https://www.python.org/. There are many books on Python as well as many examples that can be found using Google as well as many additional modules.

1. Build a packet by stacking the following layers and give the screen-shots of the constructed packets after running on scapy. Use show() to see the fields of the packets.
   a. [5 pts] Ethernet, IP, TCP
   b. [5 pts] Ethernet, IP, UDP
2. [10 pts] Generate a set of packets for a given IP address and its subnet (example: 10.20.111.2/30) and assign each of the generated packets, the TCP destination port numbers [80, 53]. Give the screenshots of the packets generated.
3. [10 pts] Send an ICMP packet from the BT5 machine to the Windows XP machine and get the reply. Give the screenshots of the packets generated and the replys.
4. [20 pts] Implement TCP trace-route for the machine (10.20.111.2) using scapy. Do **NOT** use the build-in *traceroute* function. Give the screenshots of the packets generated.

What to Submit:

For each question, provide the source code required to construct the packet. Include screen shots of the constructed packet that’s generated. Provide description and explanation of what’s required to complete each question.