Network Mapping, Vulnerability Scanning, and Exploitation

Objective

In this lab, you will be performing networking mapping of the VLAB network, scan for vulnerabilities, and exploit a vulnerability on the Windows XP host for administrative access. You will be using *nmap*, *OpenVAS*, and *metasploit*. Imagine that you are interested in launching an attack against some organization. Assume you are already inside the network with the Kali machine.

You will first need to familiarize yourself with both *nmap*, *OpenVAS*, and *metasploit*. to complete this lab. (OpenVAS is the open source version of Nessus that we discuss in class.)

The best resource for learning *nmap* can be found at: http://nmap.org/book/toc.html
The main website for *OpenVAS* is located at: http://www.openvas.org/documentation.html

Additionally, a thorough understanding of the Metasploit Exploit Framework is required. The tool is used to perform authorized penetration testing, IDS signature detection and exploit research. Thoroughly research the Metasploit framework and familiarize yourself with its use. There are several resources available on the web. Here are a few to get you started:

http://www.offensive-security.com/metasploit-unleashed/
http://www.securitytube.net/groups?operation=view&groupId=10

1. [25 pts] Map the Network using nmap

Perform network reconnaissance using *nmap* to gather the following information for all hosts:

- IP addresses of hosts
- Open ports on the hosts
- OS on each host, including OS version
- Any potential vulnerability on the host

Be sure that all your virtual machines are powered up, which must start in order starting with the external router (rtr). Wait until the router finished booting up as it provides DHCP services, and then start the other VMs. Your primary virtual machine for this lab will be Kali Linux. The username is “root” with a password of “toor”. Enter the credentials in the GUI interface to login into Kali.

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

You will use the Kali VM as your platform to perform this reconnaissance. 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.

Tip: Use the nmap scripting engine to perform the vulnerability scan. You should be able to find the MS08-067 vulnerability using nmap.

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.

2. [25 pts] OpenVAS Vulnerability Scan

We will now perform a vulnerability scan hosts you found using nmap by using the *OpenVAS* vulnerability scanner. OpenVAS uses a server/client architecture, so you will need to start the OpenVAS server and then use a client (Firefox) to connect to it. To launch *OpenVAS*, perform the following steps:

Start *OpenVAS* service by selecting **Applications->Vulnerability Assessment->openvas service start (second option among the 3 choices).**

If the command takes a lot of time (more than 15 minutes), select Applications->Vulnerability Assessment->openvas service stop (third option) to stop the service and try starting the service again.

Once this process is started successfully(may take a bit of time) connect to the server by starting Iceweasel(a variant of Firefox) and changing the URL to https://localhost:9392 --

A login page will present itself with the credentials already entered.

NOTE: All the "blue star" symbols on the OpenVAS client page represent creating new tasks, targets, rules etc.

Firstly, select Scan->Tasks from the taskbar.

Look for a "blue star" in the top left below the taskbar. The "blue star" allows you to create new tasks.

You can use the Wizard (wand symbol) to explore how to set up scans if necessary. But keep in mind, the wizard based scan will not be accepted since it is a kind of default scan which defeats the purpose of learning to configure OpenVAS scans.
Click on the "blue star" symbol to set up your own scan. You will be prompted to add scan options. Make sure you can ping the Windows machine from the Kali machine before starting any scan.
Create a new target (Windows IP would be needed from the nmap scan) in the scan settings under "Scan Targets" using the "blue star" symbol. Familiarize yourself with the other options. Ensure all TCP ports are scanned and reasonable options and scan types are set appropriately.

Before you start a new scan, make sure you properly configure a scan configuration in **Configuration -> Scan Configs**. Explain some of your choices.

Perform an OpenVAS 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.

What to Submit:

[25 pts] Screenshot and description of how you configured your *OpenVAS* scan config from the default. Screenshot of OpenVAS results screen showing vulnerabilities found (top vulnerabilities will do).

3. [50 pts] Exploit Windows XP using metasploit

Based on the vulnerabilities found via OpenVAS, use *Metasploit* to compromise the Windows XP machine using the appropriate vulnerability based on the CVE information from OpenVAS.

Gain shell access and transfer a file of your choice from the target machine to your Kali machine. Also, perform a remote screen capture *using Metasploit* of the compromised machine. You will need to use an auxiliary module to do this. Finally, install the *persistence* Meterpreter service. Be sure to document each step you take with both screen shots and descriptions of the commands employed.
Tip: In metasploit you can use "search" keyword to find the exact vulnerability and payload you want to use

Tip 2: You can exploit any vulnerability on the WinXP machine, but MS08-067 works very well.

What to Submit:

For each task, provide a complete description of your steps, include all commands used, the reason why each command was used, and screenshots of the steps employed during your attack using the Metasploit framework. Perform screen captures of both the Metasploit and target machine, show the commands used and results to prove that you have accomplished each of the following steps:

[20 pts] Obtain shell access to the Windows XP machine using the Meterpreter payload and set all necessary metasploit options correctly.
[5 pts] Transfer a file of your choice from the target machine to your Kali machine.
[5 pts] Perform a remote screen capture of the compromised machine using Metasploit. This can be done in various ways; one way is to using an auxiliary module.
[20 pts] Install the *persistence* Meterpreter service on the Windows XP machine that will automatically connect back when the system boots. Reboot the Windows XP machine and show that it automatically connects back to the Kali machine.