Network Mapping and Exploitation

Objective

An attacker would typically compromise a network by performing port scanning, finding vulnerabilities, and then exploiting them. Common tools to perform this are *nmap*, *Nessus*, and *Metasploit*. In this lab, we will cover *nmap* and *metasploit*. We skip Nessus as it's not pre-installed in Kali Linux anymore.

You will be performing networking mapping of the VLAB network, then exploit a vulnerability on the Windows XP host for administrative access. You will be using *nmap* 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* and *metasploit*. to complete this lab.

The best resource for learning *nmap* can be found at: http://nmap.org/book/toc.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/ (Sections Introduction and Metasploit Fundamentals)
- http://www.securitytube.net/groups?operation=view&groupId=10

1. [40 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.
[10 pts] Correct nmap command to find the requested details.
[10 pts] Find all open ports on all the hosts.
[10 pts] Find the OS on each host, including the OS version.
[10 pts] Potential vulnerabilities found by nmap.

(At this point, you would then scan for vulnerabilities using Nessus, but we are skipping this step.)

2. [60 pts] Exploit Windows XP using metasploit

Based on the vulnerabilities found via nmap, use *Metasploit* to compromise the Windows XP machine.

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:

Provide a report of your work. For each task, give 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.
[10 pts] Transfer a file of your choice from the target machine to your Kali machine.
[10 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.

3. [Bonus +30 pts] Obtain admin access on the WinXP host by using a different exploit

Bonus. Find a different exploit than the one you used in part 2 and perform all the same steps. Explain how the different exploit was found.