Project 4: Penetration Test

CSE 468 Computer Network Security

Due Date: May 4, 2014 11:59PM

1 Objective

The learning objective of this project is to gain hands-on experiences with the usage and functionality of Nmap, Neussus and Metsploit. After the project, students should know how to conduct a penetration test using these tools to scan and detect vulnerabilities in target machines, and how to exploit these vulnerabilities using Metasploit framework.

2 Project Description and Tasks

The goal of the project is to compromise one or two target VMs by conducting the penetration test procedure. There are 7 public VMs you need to explore:

10.0.32.146, 10.0.32.147, 10.0.32.148, 10.0.32.149, 10.0.32.150, 10.0.32.151, 10.0.32.152

These VMs have different operating systems and host several services. You need to find out their OS version, services, and vulnerabilities using Nmap and Nessus, also try to compromise one or two VMs using available exploits in the Metasploit framework.

Perform the following tasks in your VM Gateway to finish the project:

1 Scan the public VMs using Nmap and create a table to summarize the result. The table must include the following information:

   a. Version information of their OS

   b. Open port and services

   c. Version information about each service.

2 Scan vulnerabilities in these public VMs using Nessus.

a. Create a table using the following format and populate it with one vulnerability from each serveity level.

Ip address || Vulnerability id || Severity Level || Base Score

b. For each vulnerability that you add in the table above, describe:

- How to exploit this vulnerability
- The services/program this vulnerability affects
- Solution

3 Try to gain a root access against a vulnerable VM using the Metasploit Framework (we've shown this in class). You're free to use any vulnerability and any available exploit module in Metasploit. To prove that you compromised the VM, please log in to the compromised machine and create a folder under the root (/) directory. Name the folder that you created like 'asuid_firstname'.

NOTE: You are smart! Once you get root access, please do NOT delete folders created by other students ☺

4 (Bonus) Search the Internet for the exploitation steps and modules in the Metasploit and perform a more advanced attack against a vulnerable VM. Describe how you performed this attack.

3 Project Report

You should submit a report to record detailed project process (including some major screen shots) as required on Blackboard.