Cabrillo College

Lab 8: Desktop and Server OS Vulnerabilities

This lab introduces MBSA (Microsoft Baseline Security Analyzer) and uses Metasploit to hack a vulnerable desktop PC.

Warning and Permission

Unauthorized hacking can result in prison terms, large fines, lawsuits and being dropped from this course!

For this lab you have authorization to hack the VMs in the VLab pod assigned to you.

Preparation

- Get the CIS 76 Login Credentials document. You will need usernames and passwords to log into VLab and each of the VMs. This document is on Canvas and the link is in the CIS 76 Welcome letter.
- Determine which VLab pod number you were assigned. See the link on the left panel of the class website.
- If you haven't already configured your pod in the previous labs, then follow the instructions here: https://simms-teach.com/docs/cis76/cis76-podSetup.pdf

Part 1 – Run MBSA on your EH-WinXP VM

1) Download the 32-bit version of MBSA from \\172.30.10.36\depot and install it.
2) Scan your EH-WinXP system using the default options.
3) Capture a screen shot of the results when finished.

Part 2 – Use CVE-2007-0038 to exploit your EH-WinXP VM

1) Add the vulnerability details and CVSS score from CVE Details to your report.
2) Use the Metasploit IE exploit to do a HTTP hack on your EH-WinXP VM.
3) Capture screen shots of the following for your report:
    - [EH-Kali] Loading the exploit in Metasploit.
    - [EH-Kali] Choosing the payload.
    - [EH-Kali] Showing the all required options completed.
    - [EH-Kali] Starting the exploit.
    - [EH-WinXP] Internet Explorer after browsing to your "website" on EH-Kali.
    - [EH-Kali] Listing the processes and migrating from IE to Explorer.
    - [EH-Kali] Starting and ending a victim keystroke capture.
    - [EH-Kali] Desktop showing victims captured screen with captured keystrokes.
    - [EH-Kali] Captured keystroke file contents.

Part 3 – Questions

1) From your MBSA results (Part 1), what is the most serious vulnerability with your EH-WINXP VM?
2) In Meterpreter (Part 2), why migrate from IE to Explorer?

Submit your work

1) Prepare a report using the word processor and formatting of your choice. Your report should contain the following:

    - Course name, lab assignment name, your name, and date.
    - Part 1 contents from above.
    - Part 2 contents from above.
    - Part 3 contents from above.

    As an example you can see Benji Simms' report here:
    https://simms-teach.com/docs/cis76/cis76-lab08-simben76.pdf

2) Email your report to: **risimms@cabrillo.edu**

Remember **late work is not accepted.** If you run out of time submit what you have completed for partial credit.

Grading Rubric (30 points)

6 points for Part 1 MBSA screen shot
2 points each for the Part 2 vulnerability details/score and nine screen shots.
2 points each for the Part 3 answers.