Lab 5: Vulnerability Scanning

Description

By now you should have started your documentation of the Behemoth Lab from your NMAP scans. Now we will enhance your data by using 3 vulnerability scanners.

Objectives

- Gain information on the 'low-hanging-fruit' vulnerabilities of the Behemoth
- Become familiar with Vulnerability Scanning tools
- Analyze and prioritize your findings

Scope

The Behemoth network ranges are:

- 192.168.207.2-254
- 192.168.208.1-254

Note that 192.168.207.1 is explicitly OUT OF SCOPE. It is being monitored.

Method

1. Use 3 vulnerability scanners to perform a vulnerability scan of the hosts you have already identified from Lab 3
2. Analyze the vulnerability scans and correlate this information with previous findings. Update a 'priority list' of where to focus your efforts.
3. Present your findings by updating your Behemoth final report. (This will become your final report by the end of the semester – the better it is now, the easier your life is later!)

Submission

You should submit your report to canvas before the lab deadline.

You should use the report template you have previously created. Don't worry about missing sections right now, just present your findings.

You should not submit raw vulnerability data, but rather find a way to illustrate your findings in a clear, concise and prioritized manner.

Some research will be required to prioritize your findings. Note that accuracy here is not critical, just that you have tried and provided justification for your decisions. It is fully expected that your list will change as you move through the coming labs and learn more.

Grading Rubric

50%	Pass off (to TA or instructor)
50%	Report (20 Clarity, 20 Results and Conclusions, 10 Accuracy)

Expectations

Students are expected to conduct some research in order to prioritize their results. Care should be given to presentation.

Resources

Nessus - http://www.tenable.com/products/nessus/select-your-operating-system

Nexpose - http://www.rapid7.com/products/nexpose/

Core Impact (licensed – use the licensed VM we have – note this should only be used on the IT network – license violations will get reported by Core Impact). (ftp://isos.ad.csrl.byu.edu/)

OpenVAS – Comes with Kali.