

Project 2

Due October 21st, 2003 at 4pm

Project description

Scan an experimental network called *project2* that is set in Emulab within the project CIS662. The goal is to discover internal configuration and vulnerabilities, then develop rules to protect the network.

1. If you don't yet have an Emulab account, open it by going to <http://www.emulab.net> and joining the project CIS662. Be careful to use your last name or combination of your first and last name as a chosen username
2. Carefully read Emulab documentation, especially *How to get an account on the Testbed, Getting Started Tutorial* and *FAQ*. **Make sure you understand the difference between control network and experimental network. If you don't understand this, E-mail me.**
3. Carefully read the following documentation:
 - a. Ping manpage, can be obtained by running `man ping`
 - b. Traceroute manpage, can be obtained by running `man traceroute`
 - c. Nmap manpage, can be obtained from http://www.insecure.org/nmap/data/nmap_manpage.html
 - d. Sara manpage, can be obtained from <http://www-arc.com/sara/sara8.html>

All work should be done on experiment 'project2'. Warning: Use all scanning and probing only within the experiment! Use target addresses only from 192.168.*.* range!

4. Write `my_pingsweep`, a shell script or a small program that performs a ping sweep – sends an ICMP packet to all hosts in a given range to determine whether they are alive or not. **Be sure to include address range as an argument, be sure to use 192.168.*.* range when you invoke the program!**
5. Use `my_pingsweep` to determine live hosts within the experimental network.
6. Use `traceroute` tool to discover internal topology of experimental network.
7. Use `nmap` tool to discover open ports on experimental network machines. Also try to perform TCP/IP fingerprinting. **Make sure you specify that you want to test address range 192.168.*.***
8. Use `sara` tool to discover potential vulnerabilities on experimental network machines
9. Provide a write-up containing five parts:
 - a. **Source code of my_pingsweep program and list of live machines in experimental network. Don't run this code on departmental machines!**

Discuss how you would adapt `my_pingsweep` code if you knew that machines are protected by a firewall that blocks outgoing ICMP packets. What type of firewall would this be (packet filter, stateful filter or proxy)? Is there a way for the firewall to defend against this new scanning method you devised?

- b. **A drawing of experimental network topology along with ping delays between nodes.** Discuss whether this topology is a good one. Are there any weak spots. How would you reorganize the topology if you could add more machines to make it more robust?
- c. **A list of open ports on each of the machines.** List what you have learned about open ports and OS of each machine. Imagine that a network you just scanned is the network of a small company. Discuss which services need to be running and which could be shutdown; list all assumptions you make about company's business. Is the network homogeneous or is there a lot of difference between software running on different machines. How would you improve this situation?
- d. **A list of vulnerabilities discovered on each machine.** Choose two vulnerabilities from the list and find information on the Internet about possible exploits that misuse them. Provide this information in the writeup. **Do not download, install or run exploit code.** How would you protect from possible misuse of the vulnerabilities you discovered? How about future vulnerabilities?
- e. **Comprehensive protection plan.** Based on everything you learned describe on a separate page(s) a comprehensive protection plan to protect the experimental network from intrusions. Imagine that you can do whatever necessary to bring strong security to this system – add machines, change topology, patch software, configure firewalls, run periodical checks, etc. Discuss how your protection plan improves system security. Do you see any potential problems with your solution?

Project Submission Instructions

Place the PDF or PS file containing your writeup in a folder named "YourName_project2" (naturally, replace YourName with your name, e.g. I would create a folder named JelenaMirkovic_project2). Tar and zip this folder and send it as attachment by E-mail to **sunshine@cis.udel.edu**.