CS393 - Network Security - Lab Assignment 2
Network Layout Discovery - Part II
DUE MARCH 5TH

Summary:
As you would have noticed in the last lab that traditional tools such as traceroute and tcpdump do not detect hosts that are not communicating. In a typical enterprise there could hosts that are silent, an example is a web server. A web server does not create any traffic unless someone requests some thing from it. The same applies to services too, (i.e. a server could have both ftp and http installed, but http could be silent). To detect such hosts and services running on them, a more advanced tool is required. In this Lab you will be using an automated network discovery tool called nmap, which in addition to discovering hosts in the network will also report what services are running on these hosts and some additional information about these services.

Pre-Lab:
Learn how to use nmap from: http://www.nmap.org/ . You should understand how nmap works and write a one-page report on how nmap discovers hosts and routers. We would appreciate if you use flow chart and dataflow diagrams to aid your explanation.

Lab Work:
Now comes the exciting part of this assignment. As an administrator it's your responsibility to find and fix the vulnerabilities of the services and OS's that are running on your company's servers and workstations. As we all know, often Operating Systems and services running on them have weakness and bugs; hackers take advantage of this fact to gain control of the system. There are ways you make nmap to discover services and also identify what operating system is installed. You should explore all the command line options available with nmap, if you think some option are irrelevant to this assignment then you should explain why. In your report you must provide evidence in form of screen snap shots and tcpdump to prove that you did in fact explore all possible options that can be used with nmap. Please note, if you attach unnecessary tcpdump output to your report YOU WILL LOSE POINT.

How do I investigate?
Good question. You'll find the answers hidden in the following links:

http://www.securitysearch.net/
http://www.securityportal.com/
http://www.linuxsecurity.org/resources/security_sources-1.html
http://www.ntsecurity.com/
http://www.solariscentral.org/
Estimated time to finish this lab:
Based on the amount of time it took for us to create this lab, we estimate that it will take at least 2 hours for you to finish this lab.

TIPS:
1) Do not misuse root privileges in nmap servers. Doing so will not only jeopardize the network, it will also interfere with other student who really want to learn. IF WE CATCH YOU DOING SUCH THING WE WILL TAKE IT SERIOUSL.
2) You know the network ID for the network you are scanning, which is 10.3.0.0. Form the last assignment you should have learned that scanning the whole range can cause you machine to lockup. So be smart scan in smaller chunks.
3) Do not copy man page or any other paper on nmap from the net. You will get a 0 for the next two labs if you plagiarize.

What to Hand in:
1) Pre-lab reports on nmap.
2) Hand in a report that includes all the nodes you discovered on the network with the network layout. You can map them using traceroute. Your evidence for using nmap.
3) For each node list all the services the node is running and the ports on which these services are running. Also for each unique service on the network, investigate what are the known bugs and issues and briefly summarize them.
4) Submit your report using digital drop box and also submit a hardcopy. Hardcopy can be submitted up to a day after the deadline.