CS 5434 Assignment 2

Due via CMS on Fri Oct 4th by 11:59pm

Nmap

Obtain a copy of Nmap and install it on your own laptop (or a lab machine). Use it to scan your own machine (localhost or 127.0.0.1) and determine whether any server ports are open/visible from the network. Use both the –sS scan type to initially determine open ports, and then the –A scan to get maximal information on what type of machine/software is visible from the network. Research the function of any open ports, and determine if any can be closed without affecting your use of the laptop. Close any such ports, either by turning off the affected software, or using personal firewall functionality

Write up for the T.A. which ports were open, what they do, and how/whether you disabled them.

Coding assignment

Write a C program which will use the libpcap interface (start with 'man pcap') to read packets from either a network interface, or a pcap file, and count on a per-client-ip basis the number of successful TCP handshakes, half-open connections, and reset connections. Use this to implement a portscan detector. Your data structures should be able to handle an arbitrary number of ip addresses.

Testing your code

Use tcpdump (or similar) to capture a pcap or set of pcaps covering at least 12 hours of your normal daily activity while using the computer. Use this to tune your portscan detector to be as sensitive as possible while not triggering on these pcap files of your regular usage. Then, using nmap, find the largest number of consecutive ports you can scan while not triggering your detector.

Notes

Again, it's permissible to discuss the assignment in general terms with your classmates, but you need to develop your own program and tests, so that you have done your own work and can defend it in detail in discussion with the T.A.

Reminder: "you could get in **very serious trouble** for running exploits or network reconnaissance techniques against computers and networks that aren't explicitly sanctioned in this course for educational purposes. Therefore, be careful to keep all your activity confined to computers and networks that you own personally, or lab facilities provided explicitly for the course."