Computer Science CSC 433 Intrusion Detection

Allan C Roth, PhD CISSP

Sample assignments and Projects

1. Windump Lab Assignment

Please submit a screen dump of your success with running windump on a lab or your own computer. If the screen dump does not show the commands that you entered for listening, please enter them as a text line on your submission.

I would suggest that your use the window print screen function (print screen key while holding down the alt key), and take several screen prints with different windump settings and paste them into a single MS word document with text comments

Please submit using the link below by Sept 10, 2007 and be sure to include your name on the submission

2. WireShark Lab Assignment

Please install and run Wireshark (Module 5) and collect a few seconds of traffic (enough time to get some traffic perhaps with a web page connection). Find a tcp packet and determine the TTL for that packet.

Build a filter to show only icmp traffic (new filter looking for string "icmp"-read instructions thoroughly about capture filters) and run a tracert command (command line) to some host outside your network (www.microsoft.com?) and find the TTL = 1 for one of the echo request (there are three tries for the first router)packets and the TTL =2 for the second set of requests

Submit one screen print for the three exercises above.

Submit by Sept 28, 2008

[Some of you may have trouble using wireshark on your wirelessly connected laptop. After working with this myself, I determined that my wireless adapter cannot be put in promiscuous mode and therefore captures no packets. Go into the capture options, choose your wireless adapter as the default adapter and uncheck the "capture in promiscuous mode" box. Then take a look at tcp (web site requests) or icmp (tracert, ping) traffic for your assignment]

3. Mid-Term Paper

Please choose a topic under Scanners and Scan Patterns or Attack Examples on the SANS FAQ page (scroll toward the bottom) http://www.sans.org/resources/idfaq/ and prepare a short paper on this subject. This paper should be 2-3 pages (excluding graphics and diagrams). I want you to

research this subject from more sources than just the SANS site (be sure and cite these sources) and I want the report written in your own words and not copied from web or book sources. IMPORTANT: At the end of the report, please indicate what logic an Intrusion Detection System could use to detect this kind of scan or attack. That is what might be useful in designing a "signature" that would detect this attack or scan. If you find that this Scan or Attack is completely immune from detection by an Intrusion Detection System, then choose another topic.

4. Snort Final Project

Using two computers on the same network that also can see the internet, set up Snort on one of these computers (SnortPC) with the full set of rules from snort.org. Perform the following two (2)exercises. (Note: these computers should be on a wired network, not wireless)

1. On SnortPC run snort with the full rules and then on the second computer run a full nmap scan (-v -A) against the computer running snort. Capture all alerts generated by this nmap scan and identify (in your paper show the alert text) many or all of the alerts that were generated by this nmap scan.
Repeat the above using the newt scanner against the computer running snort. Show the all the alerts generated by the newt scan.

2.On snortPC run snort in the sniffer mode (no rules folder designated in the command and -v switch verbose to print to screen) or as an alternative you could run Wireshark for a period sufficient to see some of the common benign packets that could be expected over a short period of time arriving at this computer (you could also simply surf the web to generate benign packets). After capturing this traffic for a short period of time, choose two unique benign packets you saw with the sniffer and craft two snort rules that would trigger alerts when these benign packets hit the snort computer. In these rules that you craft, insert your own name and a description in the title of the alert so it will appear in the text file when alert is tripped. You can now either simply insert these rules at the top of the full rule-set or, preferably, substitute your very small rule set for the long rule set. Run this snort configuration for a time sufficient enough to to catch several instances of these packets that would also be recorded in your alert.ids file.

Write up these exercises explaining all your steps and presenting screen prints of your command line outputs and your alert.ids files and your logic for your rule set. This report will typically be approximately 7 to 8 pages including your screen prints and text files.

Course Documents links from Blackboard--Snapshot