Final Report

Jennifer Johnson

During the summer of 2004, I worked under Dr. Wu-chang Feng on the Forensix (4N6) project at the Oregon Graduate Institute. The project recreated attacks on a computer so that we could test the Forensix system. The Forensix system is made up of a weaker honeypot front-end and a more secure back-end machine. The system calls from the honeypot are sent over a secure connection to the back-end machine and are stored on a database. At this point, one can search through the system calls using a query that represents a familiar attack to see if the machine was exploited. The team s main objective over the summer was to analyze the different methods a hacker can use to collect information on a machine and take it over.

Our first few weeks consisted of reading and researching multiple avenues of computer hacking and security breaches. By learning how attackers could break into a system, we became better familiar with ways to thwart them. We then presented our research to the lab as a series of PowerPoint slides, followed by some experimentation with various tools. A link to the slides that we prepared can be found below.

(http://www.cse.ogi.edu/sysl/projects/4N6/HackingFundamentals.ppt)

An attacker might have to do some investigative work to find out about an organization, and then scan the network to find vulnerable machines. It may also be necessary to port scan some of the machines, which would help one formulate a strategy to gain access to a machine. As we already had much information about the honeypot, we experimented instead with different tools and methods of hacking, including port scanning and war dialing. We also researched ways of maintaining access, such as rootkits.

Without the extensive research and experimentation that we were allowed to conduct with the Forensix system, we would not have learned how relatively easy it is for an attacker to breach a machine. More importantly, we were able to learn the many different types of attacks that the Forensix system was able to detect.

If the honeypot was attacked, the system calls could be analyzed with SQL queries and the attack signature would be formed. The new attack signatures would then be added to the known attack signatures.

Although attackers have the advantage in the security race, security professionals have many factors to work with making their software secure. However, troubleshooting at the critical beginning stages must be intense to avoid software errors that can (and do) allow hackers easy access to machines and information.

Without a foundation in security, software designers can severely limit the success of their products by allowing these attacks.