Jace Conflenti

Cameron Taylor

TLEN 5540

RaspberryPi Forensics

After imaging and mounting our pi disk, we analyzed the file system in an attempt to learn more about how the pi was previously used. The Pi runs Raspbian GNU/Linux 8 (Jessie), and the disk consisted of two partitions, boot and root. The latter was about half full, with about 3.9 GB of used space. There was only user account on the disk, Pi. This made analyzing the disk simpler than it would have been otherwise, because many of the which we found notable were concentrated in one place. After parsing through log files, looking at bash history, analyzing IP addresses, and investigating other intricacies of the Pi’s file system, we were able to piece together how the machine was used during the hackathon.

One of the first places we looked to get a better idea of what the user was doing on the Pi was his bash history. Here, we were able to discover some software that was installed by user, namely hostapd and iptables. Shortly after installing these programs, the user began writing some server code which we later found in their home directory. As we followed through the rest of the log, we were able to see the user continually making changes to the server code. We also saw the user use iptables a lot, primarily to open ports and accept new connections. One funny (although insignificant) thing we noticed was that the user doesn’t like to use git. Instead he/she ended up making a few renditions of the server, server1.py and server2.py. That being said, there were only very minor changes between the file versions such as accepting a port as a command line argument instead of having it hard-coded in. Our theory is that the user was using hostapd to turn the Pi’s network interface card into an access point.

Another place we looked which helped us piece together a rough timeline of events was the /var/log/syslog file. Here, we found that the Pi had an IP address of 192.168.42.10. By looking at the frequency and timestamps of various DHCP connections, we were able to determine a little bit of information about other people (connections) the Pi interacted with. For example, the IP address 192.168.42.11 appeared over five times more often in the log than the next most common IP address, ranging over a wide time frame. We think that this is the machine he was using to connect/test his server code, which also makes sense because we never found any client code on the Pi itself. Towards the end of the log, there were a few entries from 192.168.42.13 and 192.168.42.14. The time between the first of these entries and the last was about half an hour, and we think that these two addresses were trying to attack the Pi near the end of the hackathon.

After retrieving a ton of information from the file system itself, we also tried to analyze the server code written by the user. Upon first glance, it looked like a basic file server. We had previously seen a directory on the Pi account called pygames, but we didn’t think they were written at the hackathon because some of them were fairly intricate. After digging a little bit more through the server code we started to put the pieces together. It seems like the user downloaded the pygames from the internet and designed his server to be a centralized game server. It had basic commands which allowed clients to make PUT, LIST, GET, and EXIT requests. It seems like the primary use case for a client would have been to list the available games on the server, and then download one via a GET request. His code really wasn’t too complex or interesting, but we still managed to find a small vulnerability. Someone could potentially upload any kind of file with the PUT request. Although these files are never executed on the server, this could still be exploited to spread malware to other clients.