Defense Against the Dark Arts

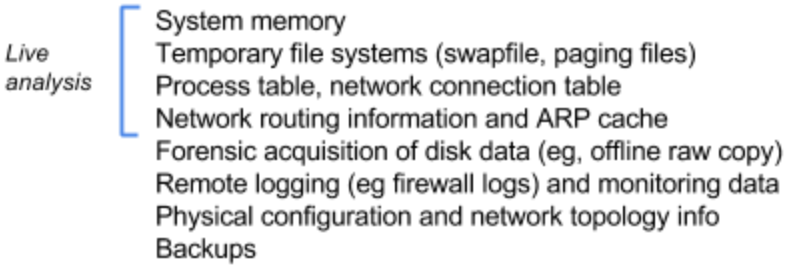
Week 2 writeup

CS373.400 Winter 2018 Shoshana Abrass abrasss@oregonstate.edu

This week's focus was on digital forensics.

I've always considered "forensics" to be a general term for investigating the impact of malware or bad actors. This week's lectures made it clear that computer forensics is a formal discipline with the specific goal of supporting law enforcement.

The workflow of forensics was described as "identify, preserve, analyze, and present" evidence of what happened. There was a lot of discussion around preserving evidence, particulary for "live forensics" which is done while the exploited system is still up and running. RFC 3227 goes into this as well, discussing the importance of not changing the system while examining it.[1] The order of volatility was particularly useful, since it also acts as a checklist of where to look for information:



Although a lot of the lecture information covered the use of specific tools (FTK, Volatility, PhotoRec, etc) to look at memory dumps or system metadata, it was clear that fundamentally, forensic analysis requires a deep understanding of system and application internals. For example one needs to be familiar with the workings of the filesystem and memory - what causes pages or filesystem blocks to be overwritten - as well as the metadata files and logs for a particular OS. I'm familiar with Linux but not Windows, so all of the tools and file locations were new to me. Fortunately NTFS seems to be similar to most modern filesystems.

Aside from the basic discipline of forensics, I was surprised to learn (implicitly) that the playing field for forensics is very unlevel. Certain tools are expansive and may therefore only be available to large companies or law enforcement. This made me wonder why there aren't more forensics tools that are, for example, paid for by government research, written by universities, and released as open source. Since we learned in week 1 that malware often follows a predictable pattern, having high quality free forensics tools seems like it would enable a wider range of professionals to identify

[1] RFC 3227, https://www.ietf.org/rfc/rfc3227.txt

new exploit. But perhaps all the people who are interested in doing this analysis (on the white hat side) are already working at one of the large security companies.

In the same vein I was surprised that forensic methods can lag far behind new technology. The lecturer made it clear the SD storage was much more difficult to investigate than hard drive storage or even live memory, because (if I understand correctly) SD devices have large blocks that must be zeroed before being written to - which means data really does get deleted. [2] [3] It's hard to tell whether the state of the art has improved since the lectures were given. Again I would expect that manufacturers of SSD devices would be producing good forensics tools, but it seems instead that security professionals try to reverse engineer how these products work.

Other notable ideas from week 2:

- Encrypted files can be decrypted <sigh>
- Passwords are stored in memory in the clear, or may be stored in the registry with weak encryption
- Accurate time correlation of events is critical for forensics
- Pen and paper are considered more trustworthy evidence than digital files in the cloud :)
- When in doubt, unplug the network (or turn off the wifi) but leave the power on
- A large amount of critical information is accessible in running memory.
- System logs are amazing

[2] Forensics wiki, link
[3] Forensic Focus: Recovering evidence from SSD drives, link