Arthur Liou
CS373

Week 2 Writeup

Prompt: Submitting a write-up of your thoughts, impressions, and any conclusions based on the material from the week. Each week will have its own assignment in the grades page.

For this week's writeup, I'm reflecting on the lectures content that we had over the two lessons (and multiple videos per lesson). We started in diving into forensic analysis, with the three steps for forensic analysis. Then we went deeper into the cycles, ensuring what to do and how to preserve evidence during it acquisition, and how this is important when dealing with legal ramifications. Handling of evidence is critical because of what law enforcement can discover and use in court to prove intent/malware/evidence/etc. Further along the lectures, we found that there are probably hundreds (if not millions!) of different sources from where we can collect and / or use as evidence.

I liked going through this week more since we went through a lot of different parts of forensic analysis and heard a lot more stories about real-world applications of this material. Also Day 2 was very informative. When I was young, I had a Windows PC and liked to tinker with software and settings, so seeing familiar actions/programs/features, such as regedit, really clicked and resonated with me as aspects of Windows PCs that I was previously familiar with, and now am / will be using to learn about cyberdefense!

Lecture Notes

Advanced Forensics Lesson 1

- Intro to this week's material and time split
- Incident response
- How to best react to incident response, Create a timeline, Analyzing memory, memory dump, book around Hacking – The Cuckoo's Nest,
- Cases for using forensics: fraud, IP theft, inappropriate child behavior, eDiscovery supporting,
- As a forensic investigator this time around, we're only proving what happened on the system. Specialty in an area, use the data to discover the facts, replicating and showing what happened
- 3 Steps
- 1) Evidence acquisition
- 2) Investigation and analysis,
- 3) Reporting results
- Minimize data loss, record everything, analyze all data collected (evidence), report findings
- Story: Don't pull the plug since also clean out memory too
- Post-modern devices, like Xbox, and PlayStation
- Always do a memory dump

- Time – is very important
- What is Evidence? Network, operating systems, databases, CD, USB, humans
- Evidence handling – preserve integrity of the evidence at all times
- The IR Process – Incident Occurs, Take Action, Remediation, Evaluation
- Legal Topics for IR & Forensic Analysts. When dealing with digital evidence, ensuring that you have access and gather all the available evidence is paramount.
- Mapping Evidence to an APT-Case - Recon, Weaponization, Deliver, Exploitation, Installation, Command and Control, Actions on Objectives
- Investigation Cycle – Verification, System Description, Evidence Acquisition. Then Cycle – Reporting Analysis, Timeline Analysis, Media Analysis, String or Byte Search, Data Recovery
- What to Acquire: Memory (virtual and physical) Drive, physical and logical (entire drive and partition), network traffic)full packet captures)
- Locard's Exchange Principle states that when any two object come into contact, there is always transference of material from each object onto the other. You can't interact with a live system without having some effect on it.
- Evidence: "Once Contaminated – stay contaminated = compromised evidence"
- Initial Response: Pull the plug or turn the machine off
- Order of volatility – when collecting evidence you should proceed from the volatile to the less volatile (see RFC 3227).
- Example order of volatility: System Memory, Temporary File Systems (swapfile / paging file), Process Table & Network Connections, Specific Process Information May Be Dumped, Network Routing Information & ARP Cache, Forensics Acquisition of Disks, Remote Logging & Monitoring Data, Physical configuration & network topology, Backups
- Live Response on Windows: Obtain volatile data (which would be lost upon shutdown), obtain the non-volatile data (time stamps, event logs, web logs, registry), Obtain any relevant, logical files – unknown executables, attacker tools
- Lab 1 – Hands On Evidence Acquisition with FTK Imager
- Memory Analysis – physical memory / RAM. A LOT can be obtained from RAM, like passwords. Analyzing memory dumps
- Strings – 'old skool': Sysinternals' strings – defaults to Unicode and ASCII, minimum length 3 characters – a lot of interesting info is not in a printable format.
- Volatility & YARA: Volatility – advanced memory forensics framework, python, plugins, free tools, malware detection tools. YARA – malware plugins for volatility, easy to write custom extensions
- Lab 2- Memory Analysis with volatility – analyzing a sample memory dump with volatility.

Advanced Forensics Lesson 2

- Core Windows Forensics
- Investigation Methodology from Day 1
- Virtually everything done in Windows refers to or is recorded into the Registry
- RegMon (sysinternals) can be used to display registry activity in real time.

- Registry access barely remains idle.
- By opening the Registry Editor (regedit), the Registry can be seen as one unified “file system”. Five most hierarchal folders are called “hives” and being with HKEY. Only two real HKU and HKLM. The other three are shortcuts or alias to branches to withint one of the two hives
- Each of the five hives is composed of keys, which contain values and subkeys
- The registry as a forensic log
- Timeine creation and analysis: once you obtain info you could check file access, creation and modify times around the period – you can get some idea of the actions taken place and correlate that with other time stamped files
- Lab 4: Creating Timeline of $MFT
- List of things to look for: relevant files, windows event logs, application config files and logs, prefetch folder.
- In many cases, the target system is a VM.
- File and directory analysis
- Data recovery – recovers files or data deleted or in slack from the system
- Lab 4 – Recovering Data (with PhotoRec)
- Case info and team work lab