Incident Response and Digital Evidence Types

Instructor: The NIST incident response cycle consists of four phases: Preparation. Detection and analysis. Containment eradication and recovery. Post-incident activity.

During the preparation phase the response team acquires and tests the necessary tools and establishes processes, procedures, and responsibilities for when an incident actually occurs.

During the second phase, detection and analysis, the response team determines the scope and scale of a potential incident and decides how to respond.

In the third phase, containment eradication and recovery, systems that are affected are quarantined or taken offline to prevent further compromise. Systems are investigated, malware is removed, vulnerabilities are patched, and business critical operations are restored. Depending on what is discovered during containment and eradication there may be a need to reanalyze the evidence to determine whether the incident has truly been contained and removed.

The final and fourth phase is the post-incident activity phase. At this time, the events that allowed the incident to occur are examined, addressed, and where possible -

mitigated. All of the knowledge gained and lessons learned throughout the response cycle should be incorporated into preparation plans for handling future incidents.

Depending on the scope and scale of the incident, several types of digital or forensic evidence can be acquired. Types of digital evidence include: volatile data, persistent data, and data that exists externally to the target system.

Volatile data is any type of data that is lost upon system shutdown, reboot, or other loss of power to the target system. Volatile data includes memory, which is one of the more crucial pieces of evidence to collect. Volatile system data might also include items like the assigned IP address, users who were logged in, existing network connections, and running processes at the time of collection.

When compared against memory analysis, volatile system data can shed light on hidden processes, files, connections, and other data loaded only in memory. Since volatile data is so fragile, it is often necessary to collect this data first to reduce the risk of loss or damage to the current state of the system.

Persistent or non-volatile data is data that is written to a disk or other device. Unlike volatile data, persistent data is typically safe from a loss of power and can be collected after volatile data is collected. Persistent

data comes in many forms, such as physical and logical disk drives, CD's, DVD's, Blu-Ray discs, flash or thumb drives, external storage devices, and even extends to devices like cell phones, cameras, and gaming systems.

There is one caveat to bear in mind when collecting persistent data and that is when the drive is believed to be encrypted. If a hard drive, for example, has local disk encryption and power is lost or the system is shut down, access to the decrypted contents may be lost forever. Whenever encryption is suspected you should collect this data while the system is powered on and you have access. Access to the data at a later time may not be guaranteed.

A third type of digital evidence is data that exists outside of the target system itself. This type of data consists of network captures or logs, system logs that may have been sent elsewhere, backup files, and even cloud data. Sometimes this data is within the scope of the incident and should be collected when appropriate.

Each incident and investigation will have its own scope. Capture as much data as is necessary but try to limit analysis only to the types of data or evidence that seems relevant and work from there.

Notices

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM18-0098