Network Forensics Investigative Methodology

Cyber Security (Parul University)

Network Forensics Investigative Methodology (OSCAR)

Like any other forensic task, recovering and analyzing digital evidence from network sources must be done in such a way that the results are both reproducible and accurate. In order to ensure a useful outcome, forensic investigators should perform our activities within a methodological framework.

The overall step-by-step process recommended in this book is as follows:

- Obtain information
- Strategize
- Collect evidence
- Analyze
- Report We refer to this methodology as “OSCAR,”

and walk through each of these steps in the following section.

1.5.1 Obtain Information Whether you’re law enforcement, internal security staff, or a forensic consultant, you will always need to do two things at the beginning of an investigation: obtain information about the incident itself, and obtain information about the environment.

1.5.1.1 The Incident Usually you will want to know the following things about the incident:

- Description of what happened (as is currently known)

- Date, time, and method of incident
- Persons involved
- Systems and data involved
- Actions taken since discovery
- Summary of internal discussions
- Incident manager and process
- Legal issues
- Time frame for investigation/recovery/resolution
- Goals This list is simply a starting point, and you will need to customize it for each incident.

1.5.1.2 The Environment

The information you gather about the environment will depend on your level of familiarity with it. Remember that every environment is constantly changing, and complex social and political dynamics occur during an incident. Even if you are very familiar with an organization, you should always take the time to understand how the organization is responding to this particular incident, and clearly establish who needs to be kept in the loop.

Usually you will want to know the following things about the environment:

- Business model

• Legal issues

• Network topology (request a network map, etc. if you do not have one)

• Available sources of network evidence

• Organizational structure (request an organizational chart if you do not have one)

• Incident response management process/procedures (forensic investigators are part of the response process and should be at least basically familiar with it)

• Communications systems (is there a central incident communication system/evidence repository?)

• Resources available (staff, equipment, funding, time)

1.5.2 Strategize

It is crucial that early on you take the time to accurately assess your resources and plan your investigation.

While this is important for any investigation, it is especially important for network forensics because there are many potential sources of evidence, some of which are also very volatile. Investigators must work efficiently.

You will want to regularly confer with others on the investigative/incident response team while planning and conducting the investigation to ensure that everyone is working

in concordance and that important developments are communicated.

An example of evidence prioritization. In this example, we list potential sources of evidence, the likely value, the likely effort to obtain it, and the expected volatility.

These values will be different for every investigation. Here are some tips for developing an investigative strategy:

• Understand the goals and time frame of the investigation.

• List your resources, including personnel, time, and equipment.

• Identify likely sources of evidence.

• For each source of evidence, estimate the value and cost of obtaining it.

• Prioritize your evidence acquisition.

• Plan the initial acquisition/analysis.

• Decide upon method and times of regular communication/updates.

• Keep in mind that after conducting your initial analysis, you may decide to go back and acquire more evidence. Forensics is an iterative process.

Figure 1–1 shows an example of evidence prioritization. In this example, the organization collects firewall logs but stores them in a distributed manner on systems that are not easily accessed.

The organization has a web proxy, which is centrally accessed by key security staff. ARP tables can be gathered from any system on the local LAN.

The table lists potential sources of evidence, the likely value for the investigation, the expected effort required to obtain the evidence, and the expected volatility. All of these values are unique to each investigation; every organization has different system configurations, data retention policies, and access procedures. Furthermore, the network equipment, investigative resources, and goals of each investigation vary widely. Based on this information, we can create our evidence spreadsheet and prioritize accordingly.

Next, we would develop a plan for evidence acquisition based on our avail□able resources.

1.5.3 Collect Evidence

In the previous step, “Strategize,” we prioritized our sources of evidence and came up with an acquisition plan. Based on this plan, we then collect evidence from each source.

There are three components you must address every time you acquire evidence:

• Document—

Make sure to keep a careful log of all systems accessed and all actions taken during evidence collection. Your notes must be stored securely and may referenced in court. Even if the investigation does not go to court, your notes will still be very helpful during analysis. Be sure to record the date, time, source, method of acquisition, name of the investigator(s), and chain of custody.

• Capture—

Capture the evidence itself. This may involve capturing packets and writ□ing them to a hard drive, copying logs to hard drive or CD, or imaging hard drives of web proxies or logging servers.

• Store/Transport—

Ensure that the evidence is stored securely and maintain the chain of custody. Keep an accurate, signed, verifiable log of the persons who have accessed or possessed the evidence. Since the admissibility of evidence is dependent upon its relevance and reliability, investigators should carefully track the source, method of acquisition, and chain of custody. It's generally accepted that a bit-for-bit image of a hard drive is acceptable in court.

For a lot of network-based evidence, the admissibility is not so clear-cut. When in doubt, take careful notes and consult legal counsel. As with any evidence gathered in the course of an

investigation, proper care must be taken to preserve evidence integrity and to document its use and disposition throughout its life cycle (from the initial acquisition to its return to its rightful owner).

As we'll see, in some cases this may mean documenting and maintaining the physical chain of custody of a network device. However, in many cases the original incarnation of the evidence being acquired will never be taken into custody.

1.5.3.1 Tips for Evidence Collection

Best practices for evidence collection include:

- Acquire as soon as possible, and lawfully
- Make cryptographically verifiable copies
- Sequester the originals under restricted custody and access (or your earliest copy, when the originals are not available)
- Analyze only the copies
- Use tools that are reputable and reliable
- Document everything you do!

1.5.4 Analyze Of course

the analysis process is normally nonlinear, but certain elements should be consid□ered essential:

• Correlation One of the hallmarks of network forensics is that it involves multiple sources of evidence. Much of this will be timestamped, and so the first consideration should be what data can be compiled, from which sources, and how it can be correlated. Correlation may be a manual process, or it may be possible to use tools to do it for you in an automated fashion. We'll look at such tools later on

• Timeline Once the multiple data sources have been aggregated and correlated, it's time to build a timeline of activities. Understanding who did what, when, and how is the basis for any theory of the case. Recognize that you may have to adjust for time skew between sources!

• Events of Interest Certain events will stand out as potentially more relevant than others. You'll need to try to isolate the events that are of greatest interest, and seek to understand how they transpired.

• Corroboration Due to the relatively low fidelity of data that characterizes many sources of network logs, there is always the problem of "false positives." The best way to verify events in question is to attempt to corroborate them through multiple sources. This may mean seeking out data that had not previously been compiled, from sources not previously consulted.

• Recovery of additional evidence Often the efforts described above lead to a widening net of evidence acquisition and analysis. Be prepared for this, and be prepared to repeat the

process until such time as the events of interest are well understood.

• Interpretation Throughout the analysis process, you may need to develop working theories of the case. These are educated assessments of the meaning of your evidence, designed to help you identify potential additional sources of evidence, and construct a theory of the events that likely transpired. It is of the utmost importance that you separate your interpretation of the evidence from fact. Your interpretation of the evidence is always a hypothesis, which may be proved or disproved.

1.5.5 Report Nothing

you'll have done to this point, from acquisition through analysis, will matter if you're unable to convey your results to others. From that perspective, reporting might be the most important aspect of the investigation. Most commercial forensic tools handle this aspect for the analyst, but usually not in a way that is maximally useful to a lay audience, which is generally necessary.

The report that you produce must be:

• Understandable by nontechnical laypeople, such as: – Legal teams – Managers – Human Resources personnel – Judges – Juries

• Defensible in detail

• Factual In short, you need to be able to explain the results of your investigation in terms that will make sense for nontechnical people, while still maintaining scientific rigor.

Executive summaries and high-level descriptions are key, but they must be backed by details that can easily be defended.