Use of Network Monitoring and Analysis Tools and Methodologies in Digital Forensic Investigations

George Chlapoutakis

Digital Forensics Group, School of Science and Technology, University of Teeside, Middlesbrough, TS1 3BA

Abstract

This paper discusses the reasons behind the adoption of Network Monitoring and Analysis tools and critically evaluates the current trend of incorporating such tools and methodologies in existing Digital Forensic software. Furthermore, the paper proposes an alternative approach to Digital Forensics investigations using Open-Source Software tools drawn from the Network Security and Digital Forensics fields. The proposed solution revolves around the creation of a customised LiveCD GNU/Linux Distribution loosely modelled after the Helix and BackTrack Network Security and Digital Forensics GNU/Linux Distributions. The resulting software allows for efficient real-time network monitoring and analysis, as well as a high degree of expandability so as to accomodate future demands and a greater degree of portability compared to standard Digital Forensic Software solutions.

1 Introduction

The process of Network Monitoring and Analysis has long been the remit of the fields of Network Administration and Network Security Engineering, assisting in both identifying network-related issues as well as revealing the presence of hostile or illegal material and individuals.

Digital Forensic Investigators, recognising the positive contribution of this process in the field of Forensic Science, have started adopting this process in the course of a criminal investigation to allow them to both monitor and

* Corresponding author.
Email address: G7133486@tees.ac.uk (George Chlapoutakis).

record criminal acts in progress as well as a tool to create a timeline and a chain of sequence in the investigation of a digital crime.

Thus, in the last few years there has been a marked increase in Network Monitoring and Analysis tools used in Digital Forensics investigations in both stand-alone software solutions [1–3] and as either internal or external parts of popular Digital Forensic toolkit solutions [4], or as specialised GNU/Linux Distributions [5].

This paper discusses this adoption of Network Monitoring and Analysis tools and methodologies by the Digital Forensics community, the reasons behind it as well as the tools and methodologies most often used as part of an Digital Forensic investigation in Section 2. The development of a GNU/Linux distribution specifically aimed at Digital Forensic Investigators is presented and discussed in Section 3. The strengths and weaknesses of this distribution are compared to those of standard Digital Forensic Software solutions in Section 4, followed by a discussion of the resulting achievements and the future work required in Section 5.

2 Network Monitoring and Analysis in Network Security and Digital Forensics

As a practice, Network Monitoring and Analysis has been used extensively in the Network Administration community to allow administrators of primarily large-scale computer networks to detect abnormalities in the flow of data across their networks.

According to Marchette [6], Network Monitoring is defined as a system designed with the purpose of monitoring the traffic both between individual computers in a network and between the computer network and the Internet in order to determine whether the network functions in a proper way through the statistical and protocol analysis of the information the system sends and/or receives.

A network monitoring system can either operate in an active way or passive way [7,8]. The prior actively injects packets of data to the network in an attempt to measure statistical information, while the latter sits on the system and captures the traffic (defined as packets of data) going through the network through the use of a sniffer module [9]. Approaches have recently been made to integrate both approaches in software-based solutions, as shown in Andreozzi et al.'s research [10].

The abilities of network monitoring and analysis systems were seen as a very potent tool in the Network Security and Intrusion Detection fields, which adopted the practice and modified the tools to capture a wider and more detailed set of information on data packets.

Passive network monitoring can allow further analysis of the content of the packets received for information regarding malicious attacks on the network in order to ascertain how the attacker is or has been trying to gain access to individual computers on the network [6]. Further analysis of the data packets can also identify the transmission of unauthorised or illegitimate content between computers or between individual computers and the Internet.

Active network monitoring, on the other hand, can identify previously hidden network resources and provide a constant map of the existing network and report on the status and availability of either services or computers conected to the network.

Finally, in the field of Network Intrusion Detection, network monitoring has been been extensively used in the Anomaly Detection, where the behavior of the characteristics of the captured data packets is compared to a set of default or otherwise called normal values and reports deviations from the normal values [11–13].

2.2 Network Monitoring and Analysis Use in Digital Forensics

From a Digital Forensic Investigator's point of view, the process of Network Monitoring and Analysis offers certain distinct advantages when used in a digital investigation.

First of all, the investigator can, through monitoring the network in real-time or through the aquisition of network monitoring tool log files, prove or disprove the hypothesis that an offence was actually commited[14]. The investigator can potentially demonstrate the sequence of network connections and actions that signified either that an incident occured or that an incident has not occured, what the incident was, what its scope was and what the target was.

The investigator can use the network monitoring logs to prove or disprove the hypothesis that the offence has been commited by a specific suspect or by a specific number of suspects by linking the information gleaned from the captured data regarding the offence to the suspect(s) [15].

An analysis of the sequence in which certain actions were performed, the cumulative result of which constitutes an offence, and the time interval between those actions as detailed in the network monitoring log files can then present the investigator with a timeline of the incident [16,14].

Prolonged real-time network monitoring of the network in which the offence is pressumed to be taken place, if a portable network evidence collector is used, as shown by Nikkel [17], and if particular attention is paid to network connections between the suspect's Internet Protocol address and other internal or external computers, can also provide evidence of an ongoing offence. This can also potentially provide an investigator with a list of accomplices to an offence, although this list can (in some cases) be provided by after the fact analysis of the network monitoring log files [16,18].

Finally, analysis of network monitoring log files gathered either in real-time or a'posteriori can provide information regarding the skill of the offender and prove or disprove the hypothesis that the offender posessed the knowledge, skills and tools to commit the offence [16,14].

2.3 The trend of integrating Network Monitoring and Analysis tools in existing Digital Forensics toolkits

Given the properties of Network Monitoring and Analysis tools and particularly the advantages they offer a Digital Forensics Investigator, the use of such tools in a digital investigation can increase the depth of analysis an investigator can perform on a computer network, as discussed in Mohay's [19] and Casey's [20] research.

As the workload and backlog digital forensics investigators increased substantially over the last few years, a faster, more automated and more efficient way for investigators to analyse digital evidence became a necessity.

This necessity resulted in proprietary digital forensics software houses either developing Network Monitoring software with more in-depth packet analysis and service discovery abilities and increased regular expression search functionalities, as in the case of NetDetector [3] or integrating Network Monitor log file monitoring and analysis solutions, natively or modularly, to their current toolkits and expanding their regular expression search functionalities accordingly, as in the case of GuidanceSoftware's EnCase Enterprise product [4].

Those software solutions posessed an increasingly in-depth, automated and thus time and cost-effective ability to include intelligence gathered during network monitoring when correlating data sources during the investigation.

In the case of stand-alone Network Monitoring and Analysis software developed for Digital Forensics Investigations, the in-depth analytical abilities are reported [20] to be far more accurate than more traditional network monitoring tools such as tcpdump [1] or solutions like Wireshark [21].

3 The Pazair GNU/Linux Forensics LiveCD Distribution

In this section the proposed solution of a GNU/Linux LiveCD distribution, Pazair GNU/Linux Forensics LiveCD, specially developed to aid in network forensics investigations is detailed.

An overview of the proposed system is given first. The requirements and considerations taken into account during the design of the proposed software solution are discussed along with further information on its implementation, after which follows a detailed discussion on the resulting distribution's strengths and weaknesses compared to standard digital forensics software.

3.1 System Overview

The proposed GNU/Linux LiveCD Distribution, Pazair GNU/Linux Forensics LiveCD is a customised LiveCD GNU/Linux Distribution based on the Ubuntu GNU/Linux distribution and is of a similar nature to the Helix [5] and BackTrack [22] Network Forensics and Network Security distributions in that it contains an assortment of both network monitoring and digital forensics tools.

However, unlike the aforementioned distributions, the emphasis of this project is on the exclusive use of Open-Source network monitoring and digital forensics software.

3.2 Design Requirements

A major requirement of the proposed system, as stated before, was for the Operating System, specifically the GNU/Linux distribution, to be highly portable and operate in a plug-and-play mode both with respect to hardware and network card detection as well as with respect to automatic connection to a wired and wireless network.

Another major requirement of the proposed system was for its framework to be highly expandable and customisable in terms of not only usage but

development.

Other design requirements that affected the design of the proposed system were a high degree of system and process stability, integrity and security.

Finally, as already stated, a requirement existed for the network monitoring and digital forensics software to be Open-Source Software.

3.3 Implementation and Results

The Pazair GNU/Linux Forensic LiveCD distribution was developed using the LiveCD version of the Ubuntu GNU/Linux distribution, version number 7.10, as the core, and the Reconstructor Ubuntu CD Creator utility [23], version number 2.7. The Ubuntu GNU/Linux distribution was chosen as it fulfilled the major design requirements for portability, expandability and hardware compatibility, as well as the reqirements for system and process stability, integrity and security.

Specifically, the requirement for portability is met through the distribution's excellent record for plug-and-play hardware and network card identification and its Restricted Drivers Manager module as well as the standard identification offered by hot and cold-plugging daemons.

The requirements for expandability and customiseability in both development and usage is met through the distribution's use of the apt-get and aptitude package managers. Furthermore, the stability and integrity requirements are met through quality assurance testing performed during the development of the core distribution, while the requirement for system and process security is met through the kernel-level patches and the AppArmor utility in the standard Ubuntu GNU/Linux Distribution.

The resulting distribution itself, while still in the early stages of development, demonstrates accurate hardware and network device detection in both desktop and laptop PCs, correctly identifying hardware and network cards, with minor performance-related issues during system booting which are regularly encountered with LiveCD distributions.

Further testing was performed to determine the distribution's ability to automatically, or with a minimum of configuration, connect to wired and wireless networks using either DHCP or Static IP address assignment. The result of these tests show that the NetworkManager module in the distribution provided very quick and very easy manual connectivity, while connections to DHCP-based networks was extremely fast and fully automated.

3.4 An evaluation of the strengths and weaknesses of the solution compared to standard Digital Forensics software

As yet, the proposed software solution as a whole has not been fully tested either under a controlled environment or in the process of a real life digital forensic examination, its design and structure, as well as the experience gained through the development of the software solution can provide some pointers as to a number of strengths and weaknesses of the proposed solution compared to other standard Digital Forensics software, open-source and proprietary alike.

Design-wise, the proposed solution has been specifically tailored to contain both network monitoring and digital forensic analysis software, but also software currently used in the network security field, such as p0f [24], ettercap [25], etherape [26], dsniff [27] and Xprobe2 [28].

The strenghts of such an design are that it allows a digital investigator to augment the process of network monitoring by, at the cost of greater complexity, using a greater variety of tools than those included in standard solutions. This allows for a much more in-depth analysis of the data packets and their attributes, some of which cannot be revealed through the simple use of network monitoring and analysis software like ethereal, as well as deal with environments where normal network monitoring tools cannot be easily, if at all, used, such as the case of network monitoring in switched environments.

From the structural point of view, a clear strength of the proposed solution is the fact that the network monitoring tools are all included in a complete and stand-alone LiveCD GNU/Linux Distribution, in essence an Operating System that can work through a CD-ROM, making the solution extremely portable .

If the added expandability and automatic hardware and networking detection capabilities are taken into account, the proposed software solution results in a much more flexible and versatile solution to current proprietary software solutions.

From a development point of view, the strength of the proposed software solution's use of the Reconstructor software allows for an extremely easy upgrade cycle and an equally extremely easy ability to further customise and incorporate new monitoring software to the current toolkit as required.

Finally, while direct comparison between Open-Source and proprietary software and Operating Systems is outside the scope of the paper, it should be added that an immense and thus far unexploited strength of the proposed software solution over standard digital forensics software is the high degree of software and process intercommunication afforded by GNU/Linux as an

Operating System. Almost every tool and every process in the proposed software solution can, through the use of programming, interpreted or scripting languages, funnel information unidirectionally or bidirectionally to other tools and processes, allowing for a great degree of automation.

4 Discussion and Further Work

The use of Network Monitoring and Analysis tools and methodologies has been applied first to the fields of Network Security and Intrusion Detection, where it has proved most useful in predicting and understanding attacks and intrusions against computers and networks, and recently to the field of Digital Forensics Science where it is already showing great promise as a powerful way to collect and analyse digital network evidence and allow investigators to have more information at their disposal.

The first part of this paper provided a detailed timeline of the evolution of Network Monitoring and Analysis and a detailed discussion on the reasons behind its adoption by Digital Forensics Investigators. In the second part of this paper, a software solution was proposed in the form of the Pazair GNU/Linux Forensic LiveCD distribution, the requirements, design, implementation and results phases of this solution detailed, and the strengths and weaknesses of the solution compared to the standard Digital Forensics software solutions currently used were discussed to a greater depth.

Further work certainly needs to be carried out to better determine, through controlled environment testing as well as through use in real investigations, the suitability of the developed software solution. Other areas where further work is can focus on is the determination of the exact level of process and data intercommunication and how programming, interpreted and scripting languages can be used to exploit this level of intercommunication.

5 References

References

[1] tcpdump, `http://www.tcpdump.org/`, Last visited: 01/3/2008.

[2] Windump, `http://www.mirrorservice.org/sites/ftp.wiretapped.net/pub/security/packet-capture/winpcap/windump/`, Last visited: 01/3/2008.

[3] NIKSUN-Incorporated, Netdetector, http://www.niksun.com/Products_NetDetector.htm, Last visited: 01/3/2008.

[4] Guidance-Software-Incorporated, Encase enterprise, http://www.guidancesoftware.com/products/airs_index.asp, Last visited: 01/3/2008.

[5] e-fence Incorporated, Helix - incident response and computer forensics livecd, http://www.e-fense.com/helix/index.php, Last visited: 01/3/2008.

[6] D. J. Marchette, Computer Intrusion Detection and Network Monitoring: A Statistical Viewpoint, Springer, 2001, Ch. 1. Introduction, p. xiii, iSBN: 0387952810.

[7] A. W. Moore, A. J. McGregor, J. W. Breen, A comparison of system monitoring methods, passive network monitoring and kernel instrumentation, SIGOPS Oper. Syst. Rev. 30 (1) (1996) 16–38.

[8] L. Cottrell, Passive vs. active monitoring, http://www.slac.stanford.edu/comp/net/wan-mon/passive-vs-active.html, Last visited: 01/3/2008 (March 2001 2001).

[9] C. Klaus, computer-security/sniffers faq, http://www.faqs.org/faqs/computer-security/sniffers/, Last visited: 01/3/2008 (July 1997 1997).

[10] S. Andreozzi, A. Ciuffoletti, D. Antoniades, M. Polychronakis, E. Markatos, P. Trimintzios, Integrated Research in GRID Computing, Springer US, 2007, Ch. On the Integration of Passive and Active Network Monitoring in Grid Systems, pp. 147–161.

[11] M. Bishop, Computer Security: Art and Science, Addison Wesley Ltd, London, 2003, iSBN: 978-0201440997.

[12] S. Axelsson, S. Goteborg, Intrusion detection systems: A survey and taxonomy, http://www.mnlab.cs.depaul.edu/seminar/spr2003/IDSSurvey.pdf, Last seen: 20/3/07 (2000a).

[13] E. Amoroso, Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, Traps, and Response, Intrusion.Net Books, New Jersey, US., 1999, iSBN: 0-9666700-7-8.

[14] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet: Second Edition, second edition Edition, Elsevier Academic Press, 2004, iSBN: 978-0-12-163104-8.

[15] T. E. Daniels, A functional reference model of passive systems for tracing network traffic, Digital Investigation 1 (1) (2004) 69–81.

[16] K. Mandia, C. Prosise, Incident Response: Investigating Computer Crime (2nd edition), McGraw-Hill Osborne, 2003, iSBN-13: 978-0072226966.

[17] B. J. Nikkel, A portable network forensic evidence collector, Digital Investigation 3 (3) (2006) 127–135.

[18] A. Ahmad, T. Ruighaver, Design of a network-access audit log for security monitoring and forensic investigation, in: Australian Computer, Network & Information Forensics Conference, 2003.

[19] G. Mohay, Technical challenges and directions for digital forensics, in: SADFE '05: Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05) on Systematic Approaches to Digital Forensic Engineering, IEEE Computer Society, Washington, DC, USA, 2005, p. 155.

[20] E. Casey, Network traffic as a source of evidence: tool strengths, weaknesses, and future needs, Digital Investigation 1 (1) (2004) 28–43.

[21] G. Combs, Wireshark, `http://www.wireshark.org/`, Last visited: 01/3/2008.

[22] Remote-Exploit.Org, Backtrack linux, `http://www.remote-exploit.org/backtrack.html`, Last visited: 01/3/2008.

[23] Reconstructor, the ubuntu cd creator, `http://reconstructor.aperantis.com/`, Last visited: 01/3/2008.

[24] M. Zalewski, p0f: Passive os fingerprinting, `http://lcamtuf.coredump.cx/p0f.shtml`, Last visited: 01/3/2008.

[25] A. Ornaghi, M. Valleri, Ettercap, `http://ettercap.sourceforge.net/`, Last visited: 01/3/2008.

[26] Etherape: a graphical network monitor, `http://etherape.sourceforge.net/`, Last visited: 01/3/2008.

[27] dsniff, `http://www.monkey.org/~dugsong/dsniff/`, Last visited: 01/3/2008.

[28] xprobe2 active os fingerprinting tool, `http://xprobe.sourceforge.net/`, Last visited: 01/3/2008.