Northeastern University

Using computer forensics in incident response methodologies

Term Paper

Information System Forensics - IA5210

Instructor: Fred Howell

Teaching Assistant: Mukund Sarma

College of Computing and Information Science

Ira Tiwari

Spring 2016

Table of contents

Abstract

This paper aims to understand incident response methodologies. This is specifically a study of how digital forensics may be integrated in to existing incident response methodologies and use forensics to better respond to and understand the incident that occurred. After a brief introduction, we move on to understand what comprises an incident in the field of information security, what are the methods used in industry and the standard techniques used for the same. I have also delved in to an overview of the digital forensic process to better understand how and which steps can be integrated into an incident response plan. Finally I present a case study of unusual activity on a network and what would be the steps taken in order to remediate such an attack.

CHAPTER 1

Introduction

An incident in the field of information security refers to an attempted or successful unauthorized access, use, disclosure, modification or destruction of information; interference with information technology operation; or violation of explicit or implied acceptable usage policy. The expanded definition of an incident involves any unlawful, unauthorized or unacceptable action involving a computer system or network. (Luttgens & Pepe, 2014) It is necessary to have an expanded definition with respect to the continuously changing landscape of both the fields of information technology and consequently, computer or digital forensics.

The field of digital forensics involves investigating an incident by recovering and investigating material found on digital devices. The incident in this case usually involves computer crime.

The term incident response can be thought of as a structured and methodical approach followed from incident detection to resolution. (Luttgens & Pepe, 2014) An incident response generally consists of an investigation team that determines what happened and performs a damage assessment, a remediation team that enhances the security of the victim and may even remove the attacker and some form of public relations, which is used to convey the process and in some cases, the status of the proceedings to senior management, business partners or even the public.

Since there are new forms of attacks on systems and incidents occurring every day, the incident response methods should also continually evolve, while also knowing previously occurred incidents and how they were handled. In this paper I aim to understand the various tools and

techniques used for the same. I aim to find out if there is a better way of doing so in any way and arrive at a possible conclusion with respect to the same.

CHAPTER 2

What comprises an incident?

As mentioned above, an incident in the world of computer security would involve any unlawful activity associated with a computer system or network. Different organizations may have different definitions of what comprises an incident. An event differs from an incident, whereas an event is “any observable occurrence on a computer system or network”, an incident would have some violation or threat to the computer security policies and principles of the organization. Organizations may even classify incidents by the severity of their occurrence and have various response teams assigned, classified by the severity of such an incident. The security policy of a company should define what comprises an incident and what needs to be done in case one occurs. (Rouse, 2005)

Examples of incidents can be a malware infection, a machine intrusion (Windows/Unix or MAC or any other as the case may be), a denial of service attack, unusual behavior observed on the network, an attack to deface the website of an organization, a social engineering attack, a phishing attack, etc.

It is of utmost importance to identify and be aware of all the attacks that an organization can be subject to. This would help in coming up with a better incident response strategy in case any of the above occur. As we can see later, there are different approaches that would need to be adopted for each of the above attacks. Being aware of as many of them as possible would help any organization in coming up with a better incident response strategy. From a security perspective,

security can always be enhanced but never perfected. Caution needs to be maintained, however, as cost impacts would also need to be considered in case of any organization.

CHAPTER 3

Incident response stages in digital forensics

The various stages associated with responding to an incident have been discussed as follows:

1. Preparation – This is before the incident occurs. The organization needs to be prepared for the worst. A stringent security policy is the best way to prepare for any incident. (Kral, 2011) Creating policies regarding user privacy expectations, established incident notification processes, development of a containment policy and creation of incident handling checklists are important aspects that can be covered at this stage. There would be different preparation methods associated with different types of incidents. Basic steps such as keeping the system updated, installing anti-virus software and applying regular patches would go a long way in securing the system or the network.

2. Identification – The next stage is to identify the actual incident. We would want to identify if an unusual activity is really an incident or more? Unusual activity could be suspicious entries in the system, excessive login attempts, unexplained user accounts and files. The incident would then need to be classified by the level of its severity. It would also be important at this stage to have good communication between the incident response team and the management. (Kral, 2011) The who, what, where and why questions should be attempted to be answered at this stage. The severity level of the incident is generally classified with a lower number severity being assigned to a higher impact incident with more harmful ramifications. Level 6 could, for example mean an

investigation incident, a level 5 could be a scan or probe and Level 1 could be unauthorized access into a system or worse, the network. As mentioned earlier, different organizations would have different definitions of what comprises an incident. Some times the risk factor would need to be taken in to account. If the asset costs more than the impact of the incident, it would sometimes be an effective and time-saving strategy to not respond to the incident at all.

3. Containment – After knowing what incident has occurred, the IR team would focus on containing the incident and the damage caused by it. There are 2 aspects when considering this – protecting other computers/networks from getting affected; determining the status of the infected computer. There could also be short-term containment, which would first be to limit the damage. A system back-up with a tool such as the FTK forensic imager would be the next step. (Kral, 2011) The steps to be taken should be decided on and taken immediately to move on to the next step. It would be a wise strategy to decide and test a containment strategy beforehand as a precautionary measure to know what to do in case an incident occurs.

4. **Investigation** – After identifying that an incident has really occurred and then containing it, there should be an investigation, examining the bit stream copies of drive data, systematic reviews of logs including those of memory, the network devices, applications and other supporting data needs to be performed. Questions such as what was accessed, who did it, what do the logs reveal should be answered at this stage. (Kral, 2011) This is the part where the expertise of the person conducting the investigation would matter. A digital forensics expert might help in analyzing the data better. There are different tools that would be needed to be used in case of different kinds of incidents. In an interview with a professional security engineer, I was told on asking that the ability to dig in and investigate the cause of the incident is a highly sought-after skill in the information security industry.

5. **Eradication** – The process of actually getting rid of the impact on the computer or the network needs to be done at this stage. It is also important at every stage to document the steps that were taken and other resources that were used. An example of the processes in this stage could be the using the original disk images to restore the system and installing any updates as required. The system could also be hardened at this stage so that another one maybe be avoided in future. (Kral, 2011) This could also be the remediation step as mentioned further. Once the attack vectors have been established and its effects contained, it is important from a business perspective to bring back the systems to normal. The larger the organization, the higher the financial impact might be for even one server not working.

6. Recovery – The stage when everything returns to normal in the organization is the recovery phase. The affected systems after being restored and patched would be brought back into the organization's production environment. Some important decisions also need to be made at this stage, such as the time and date to bring back the system to its original state; how to decide if the systems are in fact fully functional and which are the tools that will be run in order to designate them so. Any component that was compromised must be verified. It should be ensured that such a component is operational and secure, only then should it be brought back to its original use. (Pickel, 2015) This stage would also involve communicating with management teams to come up with a suitable course of action in case an internal employee or an external source is involved, as the case may be.

7. Follow up/ Lessons learned – After everything is back to normal, this is the stage to document and acknowledge the occurrence and complete any documentation that was not completed during the previous steps of the incident response plan. (Kral, 2011) Some of the questions that can be asked during this stage would include – a review of the preparation, whether or not detection was

timely, the financial impact of the incident and what should be done in future to avoid the incident altogether. Any areas of improvement can also be identified at this stage. Any documentation that was missed in previous steps would need to be completed in this step too.

CHAPTER 4

Incident response methodologies and computer forensics

Computer forensic techniques can be integrated into an established incident response plan in an organization. This chapter aims to explore the same.

The digital forensics process provides a way of doing the following with respect to the incidents which occurred in an organization:

1. Collection
2. Examination
3. Analysis
4. Reporting

The goal of performing digital forensics is to analyze the facts and data related to an event. By doing this we can gain a deeper understanding of the occurrence of such an event and it may help us prevent the same in future. The above stages have been explained below:

1. Collection – Data related to an incident is identified, labeled, recorded and collected during this stage. It is important to maintain the integrity of such data during this stage. (Kent, Chevalier, Grance, & Dang, Guide to Integrating Forensic Techniques into Incident Response, 2006) In case of a network attack, for example, this stage would involve collecting all data associated with the network traffic in order to analyze it. Tools such as wireshark and tcpdump are examples of such tools which could help us in analyzing the network traffic.

2. Examination – Forensic tools would be used at this stage to identify and extract relevant information from the collected data. (Kent, Chevalier, Grance, & Dang, Guide to Integrating

Forensic Techniques into Incident Response, 2006) In case a system has been identified which was used to conduct an attack, for example, a forensic tool such as the FTK Imager or ProDiscover could be used to create an image of the drive and then analyze the system. In case of a network intrusion, this stage would involve examining the logs, identifying the ports of attack, the source IP address etc.

3. Analysis – This stage involves analyzing the results and deriving useful information from them about the incident. It involves answering the questions of who performed the attack, what drives were targeted, what is illustrated by the logs etc. (Kent, Chevalier, Grance, & Dang, Guide to Integrating Forensic Techniques into Incident Response, 2006) Different incidents would have different approaches to analyzing the incident. A system used to conduct an attack would need to be analyzed thoroughly. In case of unusual behavior on a network, the examination and analysis stages would be similar.

4. Reporting – This step might include reporting the steps performed, determining the other actions that need to be taken and recommending any changes that need to be applied to the policies and procedures. (Kent, Chevalier, Grance, & Dang, Guide to Integrating Forensic Techniques into Incident Response, 2006) Reporting needs to be done at every stage of any incident response. Using forensic techniques would involve the same and recording all the happenings of the incident, the steps taken to remediate and further improvement that can be done would need to be documented. It proves useful in remaining aware of future incidents and steps to be taken in case one occurs.

CHAPTER 5

Examples of incidents that occurred and the methods used

To illustrate the impact of some incidents and the methods used to respond to them, a case study has been presented below:

Incident Response for malicious network behavior:

The following methods have been suggested by CERT for various stages of incident response:

1. Preparation – In preparation of a network attack, 3 things need to be taken care of:

1. Intrusion Detection Systems – It should be ensured that these are up to date, there should be contact with network and security teams so that they can respond as soon as possible in case an attack takes place. All employees should also be notified of the alert notification.

2. Network – The network access points list should be updated and available, teams should have up to date maps of the networks. Any unwarranted network points should be warranted for and closed. (CERT Societe Generale)

3. Baselining – A baseline of the network traffic flows and traffic should be maintained. (CERT Societe Generale) Establishing a baseline, while difficult, is necessary to define the "normal" behavior of the network and will help in monitoring and responding to any incidents.

The above might be considered step "zero" and it may be worth considering that the better prepared an organization is to deal with an incident, the easier and better they can handle incidents.

2. Identification – The second step or rather the first step in the incident response is to detect the incident and examine its effects. Once it has been identified, the appropriate teams may be involved.

Sources of detection can be notifications from the user, alerts from the IDS or detection by network staff. A complaint may also be recorded from an external source.

Recording of suspect network activity can be done by tools like tcpdump, wireshark, windump. A hub can be used on the LAN to capture the unusual network traffic.

Analysis of the attack would require analyzing the alerts generated by the IDS, reviewing statistics and logs of network devices. The malicious traffic would need to be analyzed. (CERT Societe Generale) This would require skill and effort on the part of the forensic examiner. One would need to identify what the unusual traffic was trying to do and which components of the network were affected by the attack. The source IP addresses, ports and protocols used need all be examined to carefully understand how the attack was conducted. (CERT Societe Generale)

At the end of this stage, the methodology of the attack conducted and the goals of the attack, if possible should have ideally been identified. With respect to computer forensics, the above steps can be thought of as a combination of the collection and examination of the network data.

3. Containment – The containment steps would have to be taken in accordance with the impact of the attack on the network. The compromised system or area could be removed from the network, unwanted connections or processes on the affected machines could be terminated, firewall rules would be needed to block the attack. (CERT Societe Generale) If needed, the business partners or senior management would need to be contacted to discuss the business impact of shutting down any affected systems. Some of the following ad-hoc measures could also be taken –

1. Restricting access to confidential files or applications on the system

2. Configure the logging abilities of the system to record more data of the incoming traffic, etc.

This step is done to mitigate the effect of the attack on the system or the nearby systems on the network. Ideally, after this step the effects of the attack should have been contained. Although digital forensics is mainly concerned with collecting and analyzing the data gathered, it is important when an incident has occurred to remediate it as soon as possible.

4. Remediation – This step is taken in order to stop the malicious behavior on the network. The following are the steps suggested:

1. Blocking the source where the attack took place

2. If it is an insider attack, the management would need to be notified of the same and appropriate action would need to be taken.

3. Similar to the above, if it was an external source that performed the attack and if it involved serious consequences, law enforcement would need to be notified. (CERT Societe Generale)

A remediation process would need to be established beforehand and tested before being implemented. Once this step has been completed, the malicious behavior should have been stopped. With respect to the discipline of computer forensics, this step, though not part of the forensic method is of great importance in the incident response cycle. Eradication of the after-effects of any incident or attack is necessary in order to mitigate its effects on the organization.

5. Recovery – This step needs to be taken in order to ensure that normal operations can be restored in the organization. The following are the steps suggested by CERT:

1. Ensuring that the network traffic is back to normal. This can be done by comparing the traffic to the baseline.

2. Re-allowing network traffic that was blocked. Any connections that were terminated can be brought back to normal, provided care has been taken to ensure that it is alright to do so.

3. Connections to the internet can be re-allowed if blocked before.

The purpose of the recovery step is to bring all operations back to normal as far as possible. It may become important in case there is a high financial impact, to reach this stage as soon as possible. Many organizations refer to this stage as “BAU” or business as usual after the incident has ended and its effects been dissolved.

6. The aftermath/lessons learned – Every step taken above should be documented every step of the way. If not already done, a report should be made and it should be ensured to include the following:

1. Cause of the issue
2. Timeline associated with the incident
3. Financial impact of the incident (CERT Societe Generale)

This report can be used to analyze what steps should be taken in order to improve the network Intrusion Detection System and lessons learnt to improve the steps taken in the incident response process. Just as in digital forensics, reporting at every stage is crucial in the incident response stage of an incident.

Tools used for network forensics

While not an exhaustive list, the following are some of the tools that can be used to conduct an investigation on a network attack:

1. Microsoft Network Monitor - Microsoft Network Monitor is a packet analyzer that captures, views and analyzes network traffic. This tool comes in handy for troubleshooting network problems. Its features include support for over 300 public and Microsoft proprietary protocols, simultaneous capture sessions, a Wireless Monitor Mode and sniffing of promiscuous mode

traffic. (Tabona, Network monitoring and analysis tools, 2015) This tool would prove useful in case of a network incident on a windows machine. This can be compared to the Wirehark tool in Kali Linux which provides similar functions of capturing packet sessions and sniffing.

2. Ethereal – It is an open source software that is widely used as a network packet analyzer. It captures live packets from the network. It displays information contained in the headers of all the protocols used in the transmission of the captured traffic. It gives us a better representation to understand the results by using a colorized display of packets belonging to different protocols. The platforms supported by Ethereal include Microsoft Windows, UNIX and Linux. (Natarajan, Allam, & Moore, 2009)

3. NetworkMiner - NetworkMiner captures network packets and then parses the data to extract files and images. This helps in reconstructing actions that a user has taken on the network – it can also do this by parsing a pre-captured PCAP file. We can enter keywords which will be highlighted as network packets are being captured. NetworkMiner is classed as a Network Forensic Analysis Tool (NFAT) that can obtain information such as hostname, operating system and open ports from hosts. (Tabona, Network monitoring and analysis tools, 2015)

4. WinPcap and AirPcap - WinPcap is a packet capture tool used to capture the packets intercepted at the network interface of a system running the Windows Operating System. It is used for link-layer network access in Windows. It includes a network statistics engine and provides support for kernel-level packet filtering and remote packet capture. AirPcap is a packet capture tool for the IEEE 802.11b/g Wireless LAN interfaces. This tool is currently available only for Windows systems. AirPcap can be used to capture the control frames (ACK, RTS, CTS), management frames and data frames of the 802.11 traffic. The AirPcap adapter captures the per-

packet power information, which can be used to detect weak signal areas and measure the transmission efficiency of the wireless devices. (Natarajan, Allam, & Moore, 2009)

5. Splunk - Splunk is a data collection and analysis platform that allows one to monitor, gather and analyze data from different sources on the network (e.g. event logs, devices, services, TCP/UDP traffic, etc). We can set up alerts to notify us when something is wrong or use Splunk's extensive search, reporting and dashboard features to make the most of the collected data. Splunk also allows you to install 'Apps' to extend system functionality. (Tabona, Network monitoring and analysis tools, 2015)

The above tools are some of the examples of tools that can be used as part of the forensic process and can be used in incident response. These may prove useful in identifying the attack that has occurred and if not contain it, would certainly help in better understanding how the attack was conducted. This information can then be used to come up with a more efficient incident response methodology.

CHAPTER 6

Conclusion

In studying the various methodologies used for incident response and the steps taken in digital forensics, I was able to better understand how these two can be integrated to formulate a more efficient incident response methodology.

Forensic investigation would prove helpful in the identification of an incident and in the final stage where we would need to examine the lessons learned in order to come up with an

efficient incident response methodology. To summarize, the steps of the incident response methodology are as follows:

1. Preparation
2. Identification
3. Containment
4. Remediation or Eradication
5. Recovery
6. Aftermath/Lessons learned

The computer forensics method involves the following steps:

1. Collection
2. Examination
3. Analysis
4. Reporting

When comparing these two methods, we can conclude that the collection and examination parts would be helpful in the identification of the incident. Analysis of the data would reveal how the attack was conducted, hence helping in the containment of the incident. The final stage, reporting is helpful in analyzing the lessons learned from the incident and how the response methods can be improved in future.

References

1. Alienvault. (n.d.). *Insider guide to incident response.* Retrieved from alienvault.com: https://www.alienvault.com/resource-center/ebook/insider-guide-to-incident-response/incident-response-tools

2. Anitian Enterprise security. (n.d.). *Incident response-digital forensics-how to build a rational response plan.* Retrieved from Sideshare: http://www.slideshare.net/andrewplato/incident-response-digital-forensics-how-to-build-a-rational-response-plan

3. Beckett, J. (n.d.). *Border wars incident response*. Retrieved from http://endpoint-intelligence.blogspot.com/2013/07/border-wars-incident-response-vs.html

4. Carnegie Mellon University. (n.d.). *Digital Intelligence Tools.* Retrieved from cert.org: http://www.cert.org/digital-intelligence/tools/

5. Carpenter, C. (n.d.). Retrieved from http://www.darkreading.com/attacks-breaches/why-digital-forensics-in-incident-response-matters-more-now/a/d-id/1318254

6. CERT Societe Generale. (n.d.). *Incident Response for unusual network behaviour.* Retrieved from https://cert.societegenerale.com: https://cert.societegenerale.com

7. Grace, S. (n.d.). *Computer incident response computer forensics overview.* Retrieved from https://www.giac.org/: https://www.giac.org/paper/gsec/569/computer-incident-response-computer-forensics-overview/101298

8. Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response.* Retrieved from nist: http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

9. King, V. J. (n.d.). *Impact of digital forensics.* Retrieved from afcea: http://www.afcea.org/events/cyber/14/documents/impactofdigitalforensics.pdf

10. Kral, P. (2011, December). *The Incident Handler's Handbook.* Retrieved from sans.org: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

11. Luttgens, J. T., & Pepe, M. (2014). Real-World Incidents. In J. T. Luttgens, & M. Pepe, *Incident Response and Computer Forensics.* Cenveo Publisher Services.

12. Natarajan, M., Allam, S. R., & Moore, L. A. (2009, April). *Tools and techniques for network forensics.* Retrieved from https://arxiv.org/ftp/arxiv/papers/1004/1004.0570.pdf

13. Pickel, F. (2015, February). *Stages of an incident response plan*. Retrieved from http://phoenixts.com/blog/7-stages-incident-response-plan/

14. Rocha, L. (n.d.). *Computer forensics and investigation methodology- 8 steps*. Retrieved from Countuponsecurity: http://countuponsecurity.com/2014/08/06/computer-forensics-and-investigation-methodology-8-steps/

15. Rouse, M. (2005, September). *Incident response*. Retrieved from searchsecurity.techtarget.com: http://searchsecurity.techtarget.com/definition/incident-response

16. Tabona, A. (2015, May). *Network monitoring and analysis tools*. Retrieved from GFI: http://www.gfi.com/blog/the-top-20-free-network-monitoring-and-analysis-tools-for-sys-admins/

17. http://www.emailtrackerpro.com

18. http://www.tamos.com

19. http://www.mandian.com

20. http://www.majorgeeks.com/index.dat_analyzer_d5259.html

21. http://www.ethereal.com