USE OF NETWORK FORENSIC MECHANISMS TO FORMULATE NETWORK SECURITY

Dhishan Dhammearatchi

Sri Lanka Institute of Information Technology Computing (Pvt) Ltd

ABSTRACT

Network Forensics is fairly a new area of research which would be used after an intrusion in various organizations ranging from small, mid-size private companies and government corporations to the defence secretariat of a country. At the point of an investigation valuable information may be mishandled which leads to difficulties in the examination and time wastage. Additionally the intruder could obliterate tracks such as intrusion entry, vulnerabilities used in an entry, destruction caused, and most importantly the identity of the intruder. The aim of this research was to map the correlation between network security and network forensic mechanisms. There are three sub research questions that had been studied. Those have identified Network Security issues, Network Forensic investigations used in an incident, and the use of network forensics mechanisms to eliminate network security issues. Literature review has been the research strategy used in order study the sub research questions discussed. Literature such as research papers published in Journals, PhD Theses, ISO standards, and other official research papers have been evaluated and have been the base of this research. The deliverables or the output of this research was produced as a report on how network forensics has assisted in aligning network security in case of an intrusion. This research has not been specific to an organization but has given a general overview about the industry. Embedding Digital Forensics Framework, Network Forensic Development Life Cycle, and Enhanced Network Forensic Cycle could be used to develop a secure network. Through the mentioned framework, and cycles the author has recommended implementing the 4R Strategy (Resistance, Recognition, Recovery, Redress) with the assistance of a number of tools. This research would be of interest to Network Administrators, Network Managers, Network Security personnel, and other personnel interested in obtaining knowledge in securing communication devices/infrastructure. This research provides a framework that can be used in an organization to eliminate digital anomalies through network forensics, helps the above mentioned persons to prepare infrastructure readiness for threats and also enables further research to be carried on in the fields of computer, database, mobile, video, and audio.

Keywords

Network Security, Network Forensics, Issues and attacks, Network forensic mechanisms, Set of Guidelines, and Recommendation.

1. BACKGROUND

Network security is a component implemented in early 1980's. However, with the sophisticated mechanisms used by the intruders' sensitive information is at risk. The Computer Emergency Response Team (CERT) Coordination Centre has shown an increase of Internet-related vulnerabilities and incidents reported to CERT over a 10-year period [1]. Supporting it, the CSI/FBI (Crime Scene Investigation/ Federal Bureau of Investigation) Computer Crime and security survey for 2006 explains the losses experienced in various types of security incidents

[13]. Case studies of anomalies in New Zealand and Russia has explained the damages done with exploit [2].

Network forensics first emerged when computer crimes grew rapidly due to the growth of the communication media. Forensic Investigation normally comes into action when an incident has happened, as a post event response. It has been supported that there are technologies that could be helped in an investigation as mechanisms that would be useful in presenting to the court as evidence. Benefits of network forensics in eliminating network security issues should be considered. Processes and procedures that need to be implemented in order to gather evidence as well as being ready for a network forensic analysis[3] [4] [5].

Confidentiality, Integrity, and Assurance (CIA) among the communication with users and applications which are involved in delivering particular services. Application layer, Transmission Control Protocol/ Internet Protocol (TCP/IP) layers, and network layer need to have separate policies to protect information crossing from one layer to another [6].

As indicated above, a study in network security which has been an active component in the past needs to be reviewed for an enhanced version. There are a number of studies conducted by many researchers in affiliating network forensics into network security which does not fulfil in targeting as a set of guidelines. Therefore a study in affiliating mechanisms used in network forensics to network security as a complete solution would be a timely study.

2. AIM

The aim of this research is to correlate mechanisms of network forensics into network security. Along with the assistance of network forensic elements it would assist to protect not only devices and users but also confidential information in an organization. It would assist the strategic, tactical, and operational managers to create guidelines in the perspective of network security.

2.1 Research Questions

Main research question
How would network forensic mechanisms be used to eradicate network security attacks?

Sub research questions

a) What are the network security issues and attacks?
b) What are the network forensic investigation mechanisms used in a network security incident?
c) How to use network forensic mechanisms to eliminate the above network security issues and attacks?

2.2Deliverables

The deliverables or the output of this research would be a report on how network forensics would be helpful in aligning network security in case of an intrusion. The main purpose of this report is to cover the scope of the project aim as shown below:

- Identify the main security issues and attacks that could be commonly seen in an organizational network security.
- Investigate the available network forensic mechanisms to investigate an incident as digital evidence.
- Map the above issues and attacks in relation to the available network forensic methods.
- Build a set of guidelines that can be used for an organization to eliminate networks security issues and attacks through network forensics.

3.0 LITERATUREREVIEWONNETWORK SECURITY AND NETWORK FORENSICS

Network forensics is a post event activity in an incident or an anomaly. When an attack or an intrusion is detected in an organization, a forensic investigator would be called upon to determine the method of intrusion, the cost affiliated with the intrusion, and to investigate the existence of any backdoor vulnerability [4]. However, it is extremely a difficult role in the real world [3]. It is potentially important in revealing possible evidence that may be lost or hidden accidently or deliberately through tools, processes, and procedures that would be timely and costly.

Globally, network security and network forensics have been managed as separate entities. However, in the recent era a network forensic readiness has been the study interest of the researchers in the field of network security and network forensics. Factors such as cost, time, inaccuracy, and inefficiency of an investigation without a proper arrangement in network security have interested the researchers in exploring this field. Separate modules of network forensic readiness have been discussed without correlating among processes, procedures, policies, tools, and standards.

3.1 Limitations and potential problems

The subject of digital forensics covers a spectrum of forensic science. Computer forensics, database forensics, mobile device forensics, network forensics, forensic video, and forensic audio would be a number of forensic sciences available. However in this research the author would only cover network forensics but with a limited association of the other forensic areas that affiliates with network forensics. The credibility of the documents reviewed was a complication that was found. The insufficient amount of research being done in this subject area made doing a literature survey difficult. Most of the researches done would only discuss one aspect of network security or network forensics where the author had to use the data extraction sheet efficiently and accurately to structure the raw data found into potential information.

3.2Network Security Issues and Attacks

Defence Advanced Research Project Agency (DARPA), USA carried out an intrusion detection evaluation program in the year 1998 at the USA Air Force Local Area network (LAN) [7]. Furthermore, 494,021 data subsets were used for the analysis and the subsets were divided into 41 different quantitative and qualitative features. However 20% of the data was isolated as normal traffic and the rest were differentiated as shown below:

- Probing;
- DOS;
- U2SU (Unauthorized access to local super user);
- R2L (Unauthorized access from a remote machine).

Figure 01 illustrates the findings in a graphical view. It would assist the reader in determining the 80% of the illegitimate data set in a categorized format. The four sectors have been illustrated by the above mentioned has shown below:

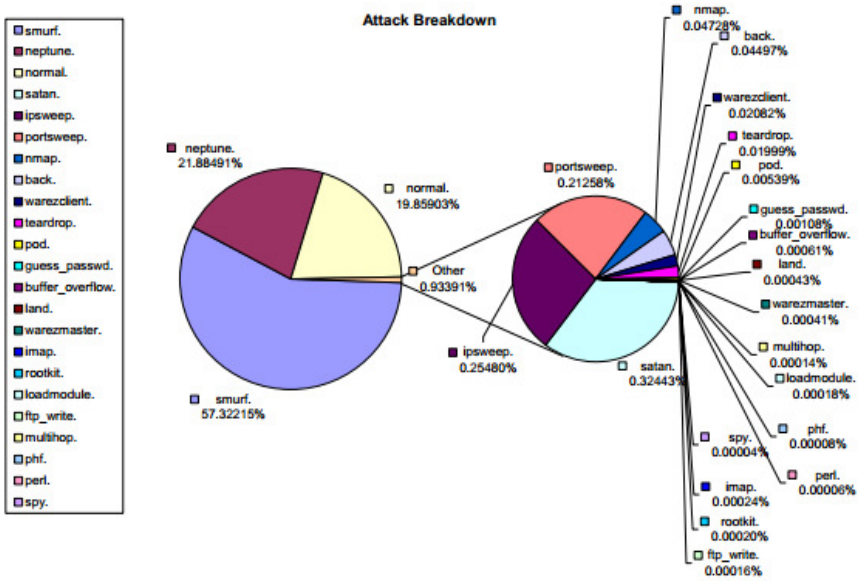

Figure 01: DARPA intrusion detection program.
(Source: https://www.utica.edu/academic/institutes/ecii/publications/articles/A04CCCB9-D778-B3D4-3C9A98DB4B0F99D1.pdf)

14 different classifications which perform individually or simultaneously in an attack [9]. Attack comprises of different activities as shown in Figure 02. An intruder needs to perform either one or several activities in each category in the given 14 classifications. In an incident identifying the attack and determining the attack structure would be essential for an organization to measure the losses affiliated and to be protected from future anomalies. The classifications shown below in figure 02 would assist the forensic investigators to conclude how, when, where, and why the incident occurred and the proactive measurements that need to be in place.Further, information has been illustrated in Appendix A.

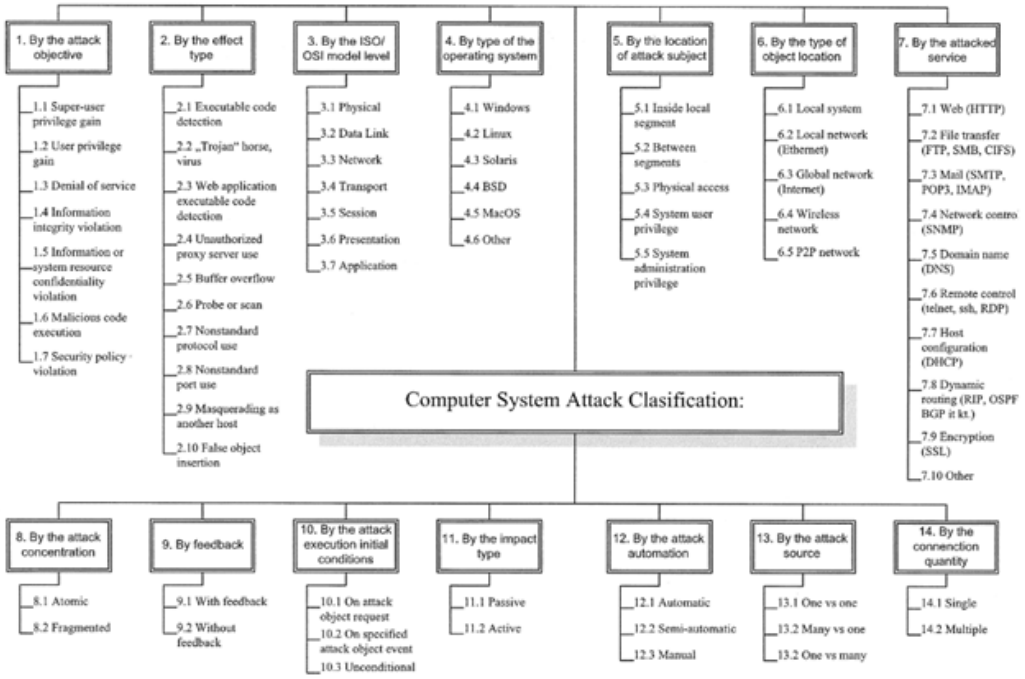

Figure 02: Computer System Attack Classification.
(Source: http://www.ee.ktu.lt/journal/2006/2/1392-1215-2006-02-66-84.pdf)

IPS (Intrusion Prevention System) is a proactive system that combines a firewall technique with IDS [10]. It would not only detect inbound traffic but also check the outbound traffic. The system examines various data records based on the pattern recognition sensor and if detected, blocks the matched data records and keeps a log. According to the above mentioned authors 69% of the enterprises use IPS to defend anomalies. IPS uses a signature technology to identify the different network traffic.

3.3 Network Forensic Mechanisms used in an incident

As illustrated in section 3.1 network forensics is a part of digital forensics. The ultimate aim of Computer Network Forensics (CNF) is to gather evidence that enables prosecution of a suspect [3]. Furthermore, the duty of the law enforcement agencies to apprehend the suspect and impose charges. However the present Network Forensic Investigation (NFI) comprises of a number of mechanisms that assist in the investigation. It contains processes, procedures, methodologies, and tools. Different researchers have different opinions on NFI but the methodology remains the same with partial changes.

As per the findings there are two considerations that need to be achieved in an investigation [10]. Those are considerations limited to workstations and considerations of a workstation on a network. Considerations limited to workstations would be applicable for the workstation on a network. The outcomes have been categorised as policies. The findings of the above mentioned description privacy protection of the user verses forensic investigation. For the relevance of the

research the author would only discuss the perspectives that are important for NFI. Presented below are the policies of the investigator's perspective:

- Build duplicate copies of the hard disk;
- Define a scope of the investigation meeting the goals of the examination;
- Acquire tokens of the packets transferred over the IP address;
- Secure the transaction logs;
- Secure event logs of the external nodes;
- Getting educated with the policies of the organization for specific action item;
- Secure backup data relevant to an investigation;
- Dispose data gathered securely.

More information has been illustrated in Appendix B.

A framework that assists in an investigation has been discussed. The framework contains a multi-tier approach to guide the investigation. As per the authors the framework combines and improves both the theoretical and practical aspects of digital investigation. Furthermore, the usability and the acceptability of the framework has been mentioned. To achieve those two components, the framework needs to incorporate phases, sub-phases, principles, and objectives. The authors mentioned above describe phases and sub-phases as steps which separate one another and are repeatable. The Principles are procedures that overlap with some or all phases and sub-phases. Objects are the goals of a process. Figure 03 illustrates a generic model of the framework that was developed. As per figure 03 there are a number of phases associated with the framework. Sub-phases can be seen inside a phase which indicates tasks of the investigation [11].

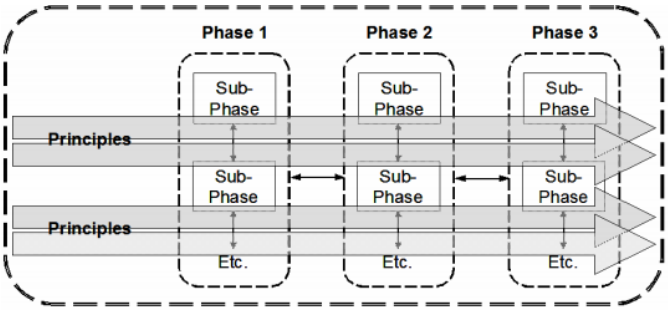

Figure 03: Generic Model of the framework
(Source: Beebe and Clark., 2005)

Data analysis sub phases to demonstrate as a framework. A data analysis sub phase could be derived as first and second tier phases. Figure 04 illustrates the first tier of the data analysis sub phase. It contains preparation, incident response, data collection, data analysis, findings, and incident closure.There are different responsibilities in different phases in the illustration of the data analysis done. Shown below are those responsibilities:

- Preparation;
- Incident Response;
- Data Collection;

- Data Analysis;
- Presenting the Findings;
- Incident Closure.

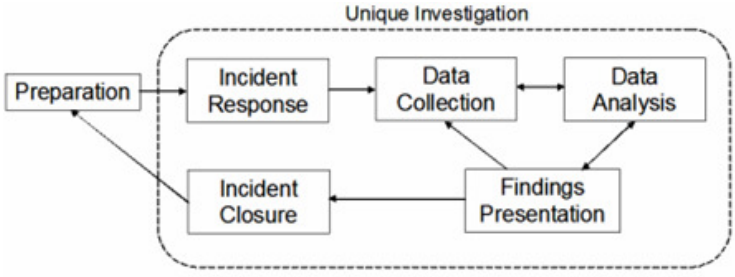

Figure 04: First-tier phase of the framework
(Source: Beebe and Clark., 2005)

Preparation is an important phase that needs better planning. Better planning improves the quality and availability of the evidence gathered minimizing costs affiliated with the investigation. Incident response consists of detection and pre-investigation response to an incident. Data and information collection which would assist in the response strategy could be positioned at the data collection in figure 04. Data analysis has been defined as a complex and time consuming phase. The data collected would be surveyed, extracted, and reconstructed during the data analysis. Findings would be evaluated repeatedly by the Data Collection, Data Analysis and Findings Presentation steps until a final outcome is reached. Communicating the findings to the management, technical personnel, legal personnel, and law enforcement would be the associated with the presentation of findings. The closure is important for almost all the stakeholders equally. It contains not only closure of the investigation but in preserving the knowledge gathered.

3.4Baseline guides used to formulate a set of guidelines

As illustrated above the outcome of the NFI is to construct evidences for the purpose of presenting it to the required personnels. Construction of the evidence, enables the appropriate entity to learn about the anomaly as well as in succeeding in decision making to either in the perspective of law or in the perspective of the organization.

According to figure 05, a framework needs to be implemented in an organization which consist a number of policies, procedures, practices, mechanisms, and awareness which bridge the goals of the systems.

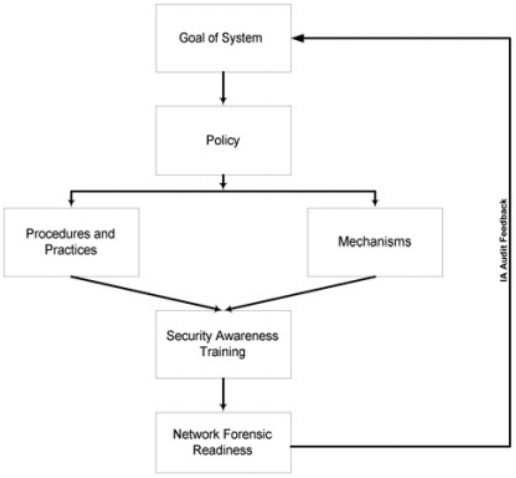

Figure 05: Embedding digital forensics framework into an organization
(Source: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.119.846&rep=rep1&type=pdf)

Development of a framework would not only assist in a NFI but in increasing the effects of network security. The framework would assist in gathering evidence as well as in providing a base to the security awareness of the organization [2]. As a result of the policies created with procedures and practices with mechanisms enables in spreading awareness about information sources throughout the organization to build network forensic ready environment. Audit feedback would contribute in evaluating whether the end outcome meets the organizational expectations of implementing the systems.

Furthermore, a life cycle which would assist in developing the framework mentioned [2]. Network Forensics Development Life Cycle (NFDLC) is based on the Information Systems Development Life Cycle (ISDLC). The NFDLC has been shown in the figure 06. There are five phases that need to be accomplish gain the benefit of NFDLC. Those are as initiation, acquisition or development, implementation, operation or maintenance, and disposition. In the initiation phase determining the aspects of the network for Digital Forensic Protection (DFP) would be evaluated. Acquisition or development would contain rules of evidence in a system developing a baseline test, performing verifications, and calibration of the test would be associated with the implementation phase. Operation or maintenance phase would cover the conduct of verification and the measurements taken based on audits. Evidence preservation and a discard mechanism would be covered under the disposition procedure. Additionally the above mentioned authors have discussed mechanisms that would assist in developing the phases of NFDLC. Risk assessment, checklists, calibration of tests, audits, and chain of custody would assist the five procedures mentioned above subsequently after the initiation procedure.

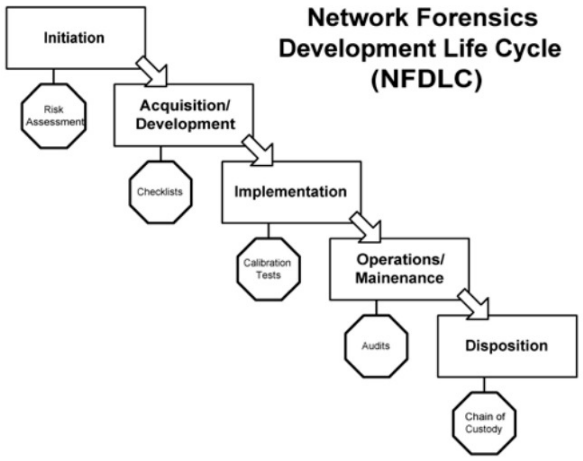

Figure 06: Network Forensic Development Life Cycle
(Source:http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.119.846&rep=rep1&type=pdf >)

An enhanced cycle that assists gathering evidence before an incident [3]. The cycle has been shown in the figure 07. The stages of the cycle are as start of data gathering before an incident, attack underway situation, analysis stage, and completion of the investigation. As mentioned before data gathering would be in process when an attack occurs. It would be more beneficial in the analysis stage rather than performing data mining after the attack. Present network monitoring tools enable in detecting anomalies based on the data gathered and in alerting the authorities while an attack is occurring rather than being discovered about an incident. The model which was discussed gives competitive advantage of the initial stage of an attack. It would enhance the accuracy and the efficiency of the investigation.

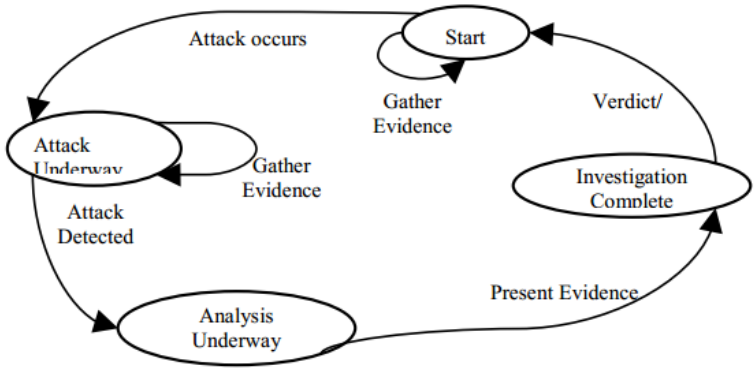

Figure 07: Enhance Network Forensic Cycle
(Source: http://home.eng.iastate.edu/~guan/course/backup/CprE-536-Fall-2004/paperreadinglist/manzano_ieee2001-westpoint.pdf)

Illustrate about retaining information that has been gathered [3]. The logs that have been gathered from devices are the key of an investigation. The logs would assist the investigators in rebuilding the scenario and in providing essential points to establish a potential case. Planning the response is a key factor that the authors have discussed. The plan contains in establishing a forensic team, an intrusion response procedure, and a formalizing investigation procedure. A CNF team should contain members of upper management, human resource, technical staff, and outside members. Furthermore, a balanced network forensic team containing the above mentioned members would cover aspects that are crucial not only in an investigation but in the daily work that needs to be done. In an incident a step by step guideline is necessary for the employees to follow. It has been covered in the intrusion response procedure. In an incident a minor mistake could remove the evidence. It would be time consuming as well as not recoverable occasionally. Through formalizing the investigation procedure would assist investigators in obtaining necessary information without been misplaced of damaged by an employee. Performing disk images of the affected, chopping logs, and limiting access to the affected system would be the activities that would be performed in the above mentioned procedure. Training the response and investigation teams would enable in gaining advantage of an analysis of a case [3].

Certifications such as ISO/IEC 27001 would assist in ensuring the CIA of the information in an organization. The certification assists an organization to build a Plan-Do-Check-Act (PDCA) which enhances the network forensic cycle. The ISO standard would evaluate risks of security breaches, the impact of security breaches, reactivity measurements towards legal action, and international acceptance. It would not only be beneficial towards protecting vital information it also gives a high credibility for the stakeholders. The ISO standard would look into topology, processes, procedure, policies, and the tool used by the organization and would support the organization to meet the industry accepted standardized method [12].

4.0 Discussion of Findings

Network security issues and attack, Network forensic mechanisms used in an incident has been analysed in the above sections. The outcome of this analysis is to further discuss to draw conclusions and recommendations as given below.

4.1Formulate a set of guidelines

It would not be possible in implementing a set of guidelines without the knowledge of the policies, procedures, processes, mechanisms, tools, and standard of the management entities and the technical entities. This research would be enhancing network security with the use of network forensics in order to take counter measures to an attack. A set of guidelines would be discussed as shown below.

As discussed in the subsection3.4implementation of embedding digital forensic framework enables in building a set of policies, procedures, practices, mechanisms, and awareness. This framework would enable in performing preparation, incident response, data collection, data analysis, presenting the findings, and incident closure.

In order to be successfully implemented the framework, NFDLC is necessary. It has been discussed in the subsection 3.3. NFDLC consists of a number of entities comprising initiation,

acquisition/development, implementation, operations/maintenance, and. The life cycle would enable in developing an enhanced network forensic cycle as discussed which would assist in gathering evidence as studied.
IPS system is a proactive system with artificial intelligence to capture known anomalies. It has been discussed in the subsection 3.2. The system would assist in delaying any intrusion that would be passing through to access the internal network. It would not only delay the intrusion but in logging the evidences and alerting the authorized would be additional components affiliated with IPS. The traffic that would be passing through would be examined using pre-built algorithm called signatures.

Certifications such as ISO/IEC 27001 would assist in ensuring the CIA of the information in an organization. The certification would assist an organization to build a PDCA which would assist the enhances network forensic cycle. Risks of security breaches, the impact of security breaches, reactivity measurements towards legal action, and international acceptance would be evaluated by the ISO standard. It would not only be beneficial towards protecting vital information it also gives a high credibility for the stakeholders. The ISO standard would look into topology, processes, procedure, policies, and the tool used by the organization and would advise in developing the organization in meeting the industry accepted standardized method.

4.2 Benefit of associating Network Forensic Mechanisms to Network Security

4R strategy could be implemented in managing a network. It has been shown in table 01. As explained resistance would prevent an attack, recognition would detect and react to an intrusion, recovery would deliver services and to restore the services, and redress would bring the responsible in a court of law.

Strategy	Tools
Resistance Ability to repel attacks	• Firewalls • User authentication • Diversification
Recognition 1) Ability to detect an attack or a probe 2) Ability to react / adapt during an attack	• Intrusion detection systems • Internal integrity checks
Recovery 1) Provide essential services during attack 2) Restore services following an attack	• Incident response • ("forensics" - *the what)* • Replication • Backup systems • Fault tolerant designs
Redress 1) Ability to hold intruders accountable in a court of law. 2) Ability to retaliate	• Forensics - *the who* • Legal remedies • Active defense

Table 01: 4R Strategies
(Source:http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.119.846&rep=rep1&type=pdf)

The 4R strategy would be beneficial in enhancing network security with network forensic mechanisms in establishing network forensic readiness. Tools that could be used with the

strategies have been illustrated in table 02. The strategy enables a network to be robust, accurate, efficient, effective, and ready to defend against an anomaly.

5.0 Conclusion

Based on the discussed, and the findings, legacy network security is obsoleting around the globe and most of the organizations are in search of a number of enhanced solutions to defend against anomalies. This research would assist managers, technical officers, and other researchers gain knowledge in converting an organization in a secure environment with less concern regarding intruders.

The author has indicated that Embedding Digital Forensics Framework, Network Forensic Development Life Cycle, Enhanced Network Forensic Cycle are a number of portfolios which would assist in developing a secure network. Through the above mentioned strategy an organization would be able to achieve the 4R Strategies. Tools such as IPS, honeypots, network management tools, firewalls would assist in achieving the 4R strategy. Furthermore the author discusses that the methodologies that would be used should comply with the industry recommendations, such as ISO/IEC 27001.

ACKNOWLEDGEMENT

My sincere thanks goes to the staff members of Sri Lanka Institute of Information Technology Computing (Pvt) Ltd as well as all the authors whom I have referred in this research paper. Without their contribution to the field would have not been possible to be successful in this research. At the same time I would like to thank University of Wolverhampton, UK in assisting me compose this paper.

REFERENCES

[1] Riordan, B. (2012) IT Security. Lecture 01: Security Trends and IT Security Losses [online].Available at <http://wolf.wlv.ac.uk>[Accessed 19 November 2012].

[2] Popovsky, B.E., Frincke, D.A., Taylor,C. A., (2007) A Theoretical Framework for Organizational Network Forensic Readiness. Journal of Computers, 2 (3), pp. 1 –11.<Available :http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.119.846&rep=rep1&type=pdf >[Accessed 10 November 2015].

[3] Yasinsac, A., Manzano, Y. (2001) Policies to Enhance Computer and Network Forensics: Workshop on Information Assurance and Security Proceedings of the 2001 IEEE . United States Military Academy, West Point 5-6 June.NY. pp. 289 – 295.<Available:http://home.eng.iastate.edu/~guan/course/backup/CprE-536-Fall-2004/paperreadinglist/manzano_ieee2001-westpoint.pdf >[Accessed : 10 November 2015]

[4] Rowlingson, R., and QinetiQ (2004) A Ten Step Process for Forensic Readiness. International Journal of Digital Evidence. 2 (3) pp. 1 – 28. <Available: http://www. ijde.org >[Accessed 28 November 2012]

[5] Garfinkel, S.L. (2010) Digital forensics research: The next 10 years, Journal of Digital Investigation, pp. S64– S73.

[6] Buchanan, W. (2011), Introduction to Security and Network Forensics, CRC Press.

[7] Mukkamala, S., Sung, A.H. (2003) Identifying Significant Features for Network Forensic Analysis Using Artificial Intelligent Techniques. International Journal of Digital Evidence [online]. 1 (4) pp. 1

– 17. <Available: https://www.utica.edu/academic/institutes/ecii/publications/articles/A04CCCB9-D778-B3D4-3C9A98DB4B0F99D1.pdf>[Accessed 10 November 2015].
[8] Paulauskas, N., Garsva,E. (2006) Computer System Attack Classification. Electronics and Electrical Engineering [online]. Vilnius Gediminas Technical University, Lithuania 2 (66) pp. 84– 87. Available at : <http://www.ee.ktu.lt/journal/2006/2/1392-1215-2006-02-66-84.pdf>[Accessed 10 November 2015].
[9] Stiawan, D., Abdullah, A.H., Idris, M.Y. (2010) The Prevention Threat Behaviour-based Signature using Pitcher Flow Architecture. International Journal of Computer Science and Network Security [online]. UniversitiTeknology, Malaysia 10 (40) pp. 289 – 294. <Available:http://eprints.unsri.ac.id/77/1/Journal_IJCSNS_edit_utm.pdf>[Accessed 10 December 2012]
[10] Srinivasan, S. (2007) Security and Privacy vs. Computer Forensics Capabilities. Journal of ISACA. , pp. 1 – 2.
[11] Beebe, N.L., Clark, J.G. (2005) A Hierarchical, Objectives-Based Framework for the Digital Investigations Process, Journal of Digital Investigation, 2 (2), pp. 146 – 166.
[12] Lambo, T. (2006) ISO/IEC 27001: The future of inforsec certification. Journal of ISSA, pp. 44–45.
[13] Internet Crime Complaint centre (2011) Internet Crime Report [online]. United States: Internet Crime Complaint centre. <Available:https://www.ic3.gov/default.aspx>[Accessed 20 January 2013].

Author

I am a Lecturer / Network Engineer with over 08 years of hands on experience who worked for Millennium Information Technologies, a subsidiary of the London Stock Exchange as well as a lecturer in SLIIT Computing (Pvt) Ltd which is a leading private university in Sri Lanka. I have been involved in many critical projects primarily in Sri Lanka, United Kingdom, and the Maldives. I have also acquired a bachelors and a masters degree with a number of professional examinations as well as being a Toastmaster with Competent Communication Status.

APPENDIX A: Network Security Issues and Attacks

Defence Advanced Research Project Agency (DARPA) findings:

Probing

Through probing the intruder would be able to scan a set of computers to gather information to build a network map as well as to identify the services available and to find known vulnerabilities for an exploit. Ipsweep, MScan, Nmap, Saint, Satan are a number of scan activities that could be seen commonly in a network.

Denial of Service Attack

DOS is an attack by an intruder in order to interrupt the services of either computers or any other device that uses memory by intensifying the usage of resource through a legitimate or unauthorized service attack. Apache2, Back, Land, Mail bomb, SYN Flood, Ping of death, Process table, Smurf, Syslog, Teardrop, and Udstorm are a number of DOS attacks that could be seen commonly in an organization.

U2SU

U2SU is an exploit done by an intruder in a system to gain a higher privilege level. Gaining root access would be the prime goal towards a disruption. Firstly the intruder would obtain a normal user account and would be manoeuvring towards the root level by

exploiting the vulnerabilities in the system. Eject, Ffbconfig, Fdformat, Loadmodule, Perl, Ps, and Xterm are a number of commonly seen attacks in this category.

R2L
R2L is a commonly seen attack in a network where the intruder gains access to a user machine which he is not privileged to access. After gaining access the intruder would use the machine for malicious act in a network. Dictionary, FTP_write, Guest, Imap, Named, Phf, Sendmail, Xlock, and Xsnoop would be a number of commonly seen attacks in this category.

For the benefit of the reader the author would explain the activities through an example as shown below:

Brief explanation of the system attack
A number of confidential reports were leaked from an organization.

Possible point of leakage
A breach on the Chief Executive Officer's (CEO) electronic mail.

Attack performed by the intruder

I. Probing and scanning the network
II. Identifying a list of devices, services, and types of operating systems
III. Making a map of the network
IV. Distinguish the attack methodology
V. Initialize a user account for the devices
VI. Performing the attack

The intruder would be probing and scanning a network in order to identify the devices and the services in the organization. Through the above mentioned activity the intruder would be able to recognize and gather information such as device types and operating systems affiliated with the devices. It has been shown in the attack objective, effect type, and ISO/OSI model level in the figure 02. Secondly the intruder would be able to identify a map of devices in the network and segregate a pathway for the intrusion. It has been shown in the type of operating system and location of attack subject in the figure 02. The intruder would gain local access to the devices through a normal user and manoeuvre to a super user. It has been shown in the type of object location, attacked services, attack concentration, and feedback in figure 02. The intruder would be taking passive measurements till initializing the attack. It has been shown in attack execution initial conditions, by impact, attack automation, attack source, and the connection quality.

APPENDIX B: Network Forensic Investigation Mechnisms used in an Incident

The findings of Srinivasan (2007):

- Build duplicate copies of the hard disk
  Important evidence needs to be stored with a hash signature in the ownership of the possessor. The duplicate copies needs to be with the investigators where one copy of left unchanged for the purpose of building new copies and the other to perform investigations.

- Define a scope of the investigation meeting the goals of the examination
  Information that is not relevant to the investigation should not be associated with the search of evidence. Decryption of sensitive information related to other organizations and individuals should not be examined which would violate the privacy right. The court would not accept data gathered by unauthorized mean.
- Acquire tokens of the packets transferred over the IP address
  Hashed information of the tokens such as sender/receiver would be essential in protecting the user privacy right. In case of an intruder the token would be classified as unknown.
- Secure the transaction logs
  Logs that were created relevant to a particular network status would be critical information for the investigators. If the information been corrupted it would not be possible in recreating the scenario.
- Secure event logs of the external nodes
  If the intrusion occurs from outside the organization the logs that are created would be vital information for the investigators. As specified in the above bullet point if the information been corrupted it would not be possible in recreating them.
- Getting educated with the policies of the organization for specific action item
  The policy implementation and the action taken should match in terms of an intrusion. Policies and action taken should not violate the privacy right. The investigators need to be educated if the policies do match with consistent action taken.
- Secure backup data relevant to an investigation
  Information that is in backup storages would be at high risk in an intrusion. An intruder could retrieve information from backup storages violating privacy rights.
- Dispose data gathered securely
  Data gathered in an investigation would be in a format that would indicate various relationships. This information would assist in developing the scenario if placed on the wrong hands.

Data analysis phases:

Preparation

- Measure risk considering vulnerabilities;
- Build an information preservation plan;
- Build an Incident Response Plan;
- Build technical capabilities;
- Educate personnel;
- Gather information about the hosts and the network devices;
- Build a framework to secure the evidence gathered;
- Build a legal activity plan.

Incident Response

- Detect the anomaly;
- Report the anomaly to the authorities;
- Verify the incident;
- Document the damage and review the logs and network topologies;

- Build strategies regarding the spread of the intrusion, damage, recovery, and investigation regarding the business, technical, political, legal, and other aspects;
- Coordinating with management, legal, human, and law enforcements;
- Build the investigation plan for data collection and analysis.

Data Collection

- Build a plan to obtain data from the incident response;
- Obtain evidence from applicable sources in the network;
- Acquire evidence from the applicable sources of hosts
- Acquire evidence from the applicable sources of removable media;
- Install network monitoring tools;
- Certify the integrity and authenticity of the digital evidence;
- Build a plan to package, transport, and store the evidence.

Data Analysis

- Manage the collect information relevant to the incident from the collected data;
- Assign personals based on the individual skill levels to recognize the evidence as a data survey process;
- Build a data extraction technique;
- Build a report through an examination, analysis, and event reconstruction.

Presenting the Findings

- Reconstruct the findings of the data analysis.

Incident Closure

- Critical review of the investigation to identify the lessons learned;
- Manage and build an appropriate evidence disposable plan;
- Secure the information related to the incident.