A Systematic Study on Incident Process Methodology in Cyber Forensics

Karthik Konar.

(a)MCA Student, Dept. of Computer Engineering, NMIMS Mukesh Patel School of Technology Management & Engineering, Vile Parle(West) Mumbai.

Abstract: *Nowadays usage of data hiding techniques such as encryption and steganography by smarter criminals results in some difficulty to find evidence against the criminals, people consider cyber forensics to be a detective work but it is more concerned with handling sensitive data more responsibly and with more confidentiality, take precaution, not to corrupt data and maintain the integrity of the data, stay with the regulations and guidelines of evidence. There are 4 steps involved in computer forensics they are a collection of data, an examination of data, analysis of data, reporting of evidence.*

The purpose of this paper is to provide a general overview of incident process methodology which includes various phases such as pre-incident, detection of an incident, initial response, formulate response strategy, investigate the incident, reporting, resolution.

Abbreviations: CSIRT-Computer Security Incident Response Team.

Keywords-Incident process methodology, incident management, data collection in cyber forensics.

I.INTRODUCTION

Incident process methodology is responsible for managing the lifecycle of all Incidents irrespective of their origination. The goals for the incident management process are to restore normal service operations as soon as possible, minimize the impact on business operations, protect the organization's reputation and assets.

Incident process methodology consists of various phases .in the first phase i.e in the pre-incident phase both the organization as well as the computer security incident response team is prepared to handle as well as prevent attacks that can occur.

In the detection of the incident phase, any unauthorized or illegal things that affect the organization, computer network are identified.

The initial response phase consists of interviewing system administrators and business unit personnel, reviewing intrusion detection reports and network logs, reviewing network topology, and access control lists.

In the formulated response strategy phase an appropriate response strategy is formulated, given the circumstances of the incident.

The investigation phase involves determining who, what, when, where, how, and why surrounding an incident.

In the reporting phase a report is created which precisely describes all the details of the incident in such a way that it is understandable to the decision-makers.

The resolution phase consists of executing host-based, network-based, and procedural countermeasures to keep an incident from creating additional harm.

II. DETAILED EXPLANATION

Who are the persons involved in the incident response process?

There are 2 persons involved in the incident response process. They are :

(1)The organization.

(2)CSIRT(computer security incident response team).

INCIDENT PROCESS METHODOLOGY:

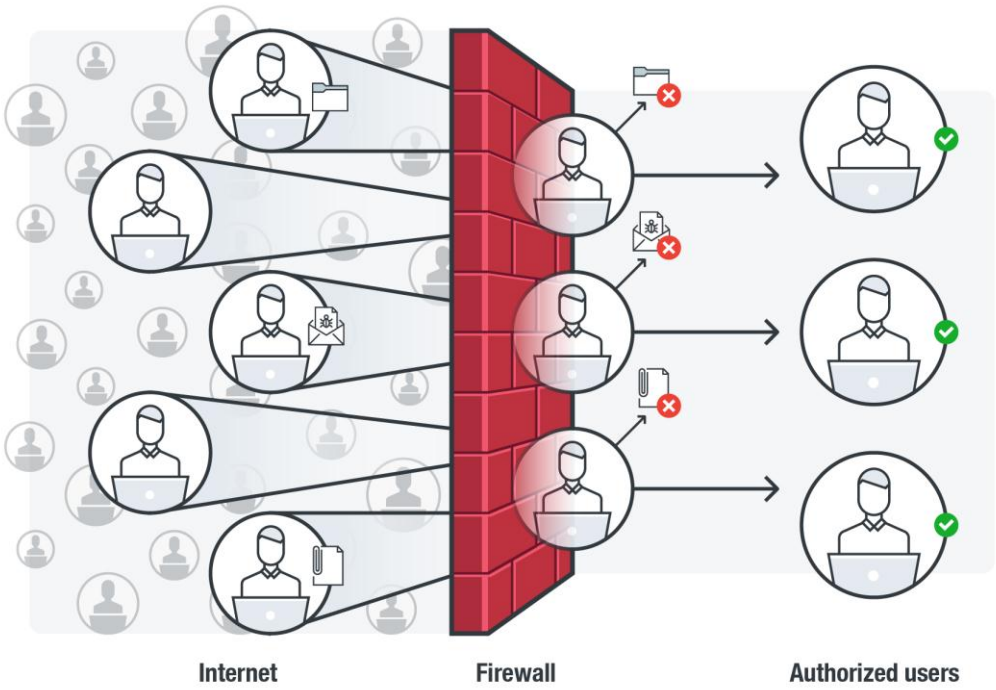
Incident process methodology consists of the following steps:

(1)Pre-incident:

In this phase the organization as well as the CSIRT(computer security incident response team) is prepared to handle as well as prevent attacks that can occur.

(a) Preparing the organization consists of the following:

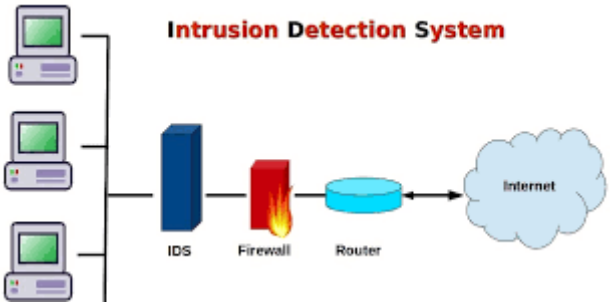
(i) Apply host and network-based security measures.



For eg: Building a firewall will allow only authorized users to enter the network, unauthorized users will not get access to enter the network.

(ii)Training end-users.

(iii)Hiring an intrusion detection system.



(iv) Create strong access control.

(v) Perform a timely vulnerability examination.

(vi) Ensuring backups are performed regularly.

(b) Preparing the CSIRT consists of the following:

(i)The hardware and software required to investigate computer incidents.

(ii)Documentation like forms, and reports required to investigate incidents.

(iii)ideal guidelines and operating tactics to implement response techniques.

(iv)Training required to perform the incident response to staff or employees.

(2)Detection of incident

Whenever any unauthorized thing happens which involves an organization or computer network or data processing unit, the computer security incidents are identified.

End-users may document the incident through 3 ways:

(a)Their immediate supervisor.

(b) Company help desk.

(c) Incident hotline controlled by the Information Security entity

To record an incident an initial checklist is prepared.

The checklist must include the following:

(a) Current date and time of the incident.

(b) Who reported the incident?

(c) Nature of the incident.

(d) When the incident happened.

(e) What hardware/software are involved?

(3)Initial Response.

This phase does the following tasks:

(a)interviewing system administrators and business unit personnel.

(b)Reviewing intrusion detection reports and network-based logs to identify data that would support that an incident has happened.

(c)Reviewing network topology and access control list to determine if an attack can be ruled out.

(4)Formulate Response Strategy

In this phase the main goal is to formulate appropriate response strategies given the circumstances. political, technical, legal, and business factors that surround the incident are taken into consideration.

All the following circumstances are taken into consideration:

(a) Estimated dollar loss.

(b) Network downtime and its impact on operations.

(c) User downtime and its impact on operations.

(d)Whether or not your organization is legally compelled to take certain actions.

(e)Public announcement of the incident and its effect on the organization's reputation/business.

(f)Some factors are needed while deciding the resources required for investigating an incident.

Legal Action:

There are 2 legal choices available:

(1)To file a civil complaint.

(2)To notify law enforcement.

Law enforcement involvement will result in reducing the autonomy that the organization has in dealing with an incident.

The following standards have to be considered while identifying whether or not to include law enforcement in the incident response:

(a)Does the damage/cost of the incident merit a criminal referral?

(b)Is it likely that civil or criminal action will accomplish the outcome desired by your

organization?

(c)Has the reason for the incident been reasonably established?

(d)Does your organization have proper documentation and an organized report that will be conducive to an effective investigation?

ADMIN:

The following are the actions that an admin can perform to discipline an internal employee.

(a)Letter of scolding.

(b)Immediate dismissal.

(c)Mandatory leave of absence for a particular period.

(d)Reassignment of job duties.

(e)Temporary reduction in pay.

(f) Public/private apology

(g)Withdrawal of certain privileges.

5. Investigate Incident:

Investigating an incident involves who, where, what, how involving an incident. Computer security investigation is involved in 2 phases:

(1)Data collection.

Data collection consists of the following:

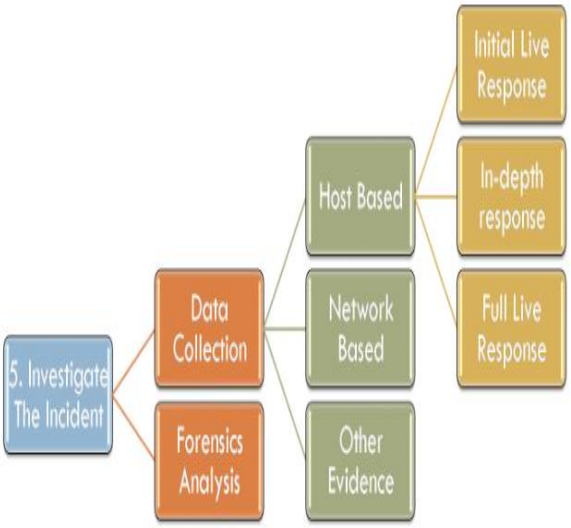
(a)collection of host-based data.

(b)collection of network-based data.

(c)collection of data from other evidence.

(2)Forensic analysis.

The main aim of forensic analysis is to review all the collected data. The review includes log files review, system configuration files, trust relationships, web browser history files, email messages and their attachments, installed applications, and graphic files.



DATA COLLECTION:

Data collection consists of the gathering of facts and clues, the data you gather can help you form your conclusions.

The data collected can be partitioned into 3 stages:

(a)Host-based information.

It consists of logs, records, documents, and any other information that is obtained from the system and not obtained from the network-based nodes. Host data collection can be performed in 2 ways:

(i)live data collection.

(ii)forensic duplication.

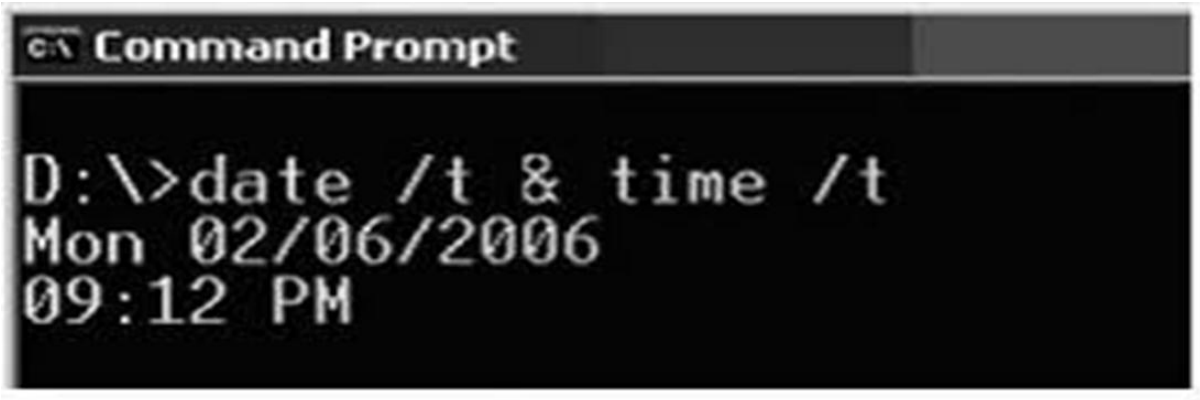
In a few cases, the evidence that is required to recognize an incident is temporary or lost when the victim/relevant system is powered down. Such type of volatile data can contain critical information which helps to understand the nature of the incident. This is known as a live response.

There are 3 types of live responses:

(a)**Initial live response:**

The initial live response collects only volatile data from the victim/relevant system.

For eg:



(b)**In-depth response.**

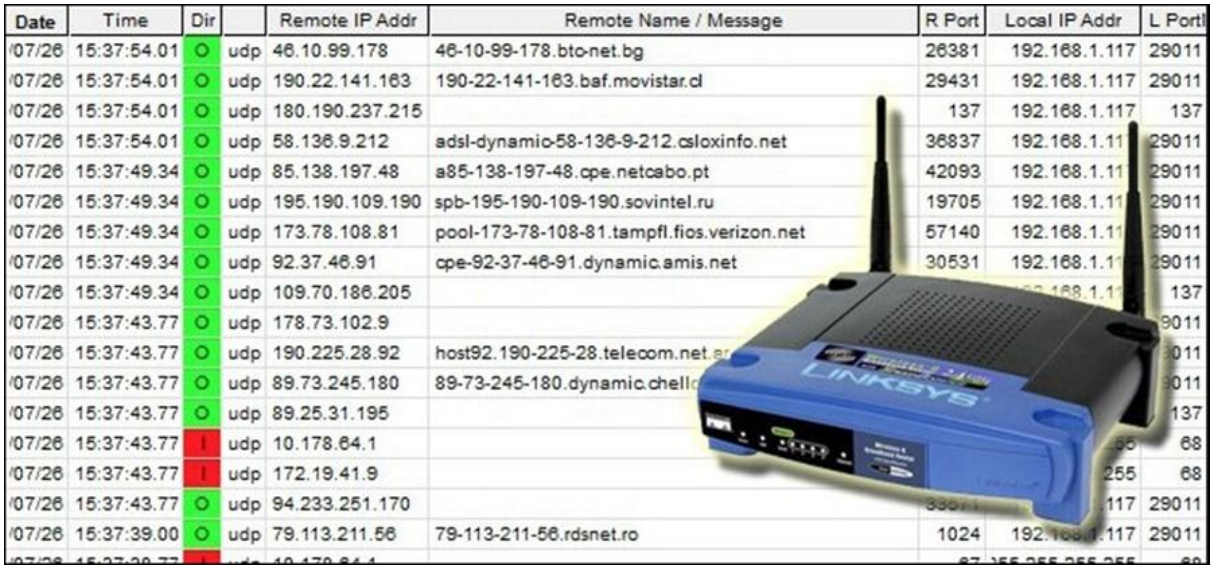
In this response the computer security incident response team collects additional information from the target/victim system. Even non-volatile information is collected from the target/victim system which consists of log files that can help determine the nature of the incident.

(c)**Full-live response.**

In full live response a full investigation is performed on a live system.

(b)Network-based evidence.

It consists of information gathered from the sources such as Intrusion detection system logs, Router logs, firewall logs, and authentication server.



Date	Time	Dir		Remote IP Addr	Remote Name / Message	R Port	Local IP Addr	L Port
/07/26	15:37:54.01	O	udp	46.10.99.178	46-10-99-178.bto-net.bg	26381	192.168.1.117	29011
/07/26	15:37:54.01	O	udp	190.22.141.163	190-22-141-163.baf.movistar.cl	29431	192.168.1.117	29011
/07/26	15:37:54.01	O	udp	180.190.237.215		137	192.168.1.117	137
/07/26	15:37:54.01	O	udp	58.136.9.212	adsl-dynamic-58-136-9-212.csloxinfo.net	36837	192.168.1.11	29011
/07/26	15:37:49.34	O	udp	85.138.197.48	a85-138-197-48.cpe.netcabo.pt	42093	192.168.1.11	29011
/07/26	15:37:49.34	O	udp	195.190.109.190	spb-195-190-109-190.sovintel.ru	19705	192.168.1.11	29011
/07/26	15:37:49.34	O	udp	173.78.108.81	pool-173-78-108-81.tampfl.fios.verizon.net	57140	192.168.1.11	29011
/07/26	15:37:49.34	O	udp	92.37.46.91	cpe-92-37-46-91.dynamic.amis.net	30531	192.168.1.11	29011
/07/26	15:37:49.34	O	udp	109.70.186.205				137
/07/26	15:37:43.77	O	udp	178.73.102.9				9011
/07/26	15:37:43.77	O	udp	190.225.28.92	host92.190-225-28.telecom.net.ar			9011
/07/26	15:37:43.77	O	udp	89.73.245.180	89-73-245-180.dynamic.chello			9011
/07/26	15:37:43.77	O	udp	89.25.31.195				137
/07/26	15:37:43.77	I	udp	10.178.64.1			55	68
/07/26	15:37:43.77	I	udp	172.19.41.9			255	68
/07/26	15:37:43.77	O	udp	94.233.251.170			117	29011
/07/26	15:37:39.00	O	udp	79.113.211.56	79-113-211-56.rdsnet.ro	1024	192.168.1.117	29011

The above figure shows information about router logs.

(c)other evidence

It consists of information obtained from the people. It follows the traditional investigative techniques to collect evidence. You get other evidence when you collect personnel files, interview employees, etc.

(6)Reporting

It is one of the biggest challenges in the entire process.in the phase a report is created which precisely describes the details of the incident which is understandable to the decision-makers.There are some guidelines that one needs to follow while creating reports. They are as follows:

(a)Document immediately:

Document all investigative steps and conclusions which are necessary to document as early as possible It results in time-saving and ensures that it can be communicated more clearly to others at any time.

(b)write concisely and clearly:

Write down everything in simple language. Try to avoid shortcuts.

(c)Use a standard format.

Use a standard format for your report and stick to it.

(d)Use editors.

Recruit professional editors to read your reports.

(7)Resolution

The main aim of the resolution is to execute host-based,network-based evidence and procedural countermeasures to keep an incident from creating additional harms and to give back your organization to a protected, solid operational status. The following activities are involved here :

(a)Identify your organization's top needs.

(b)Restore any affected or compromised systems.

(c)Track progress on all corrections required.

(d)Determine if there are basic or systemic reasons for the incident that needs to be addressed.

III. OBSERVATION

Phase No	Phase Name	Consists of	Remarks
1	Pre-Incident	(a)preparing the organization (b)preparing the CSIRT.	Pre-incident phase mainly focuses on preparing the organization as well as preparing the CSIRT
2	Detection of Incident	Initial checklist which contains all necessary details of the incident	In the Detection of the incident phase, the computer security incident is identified.
3	Initial Response	Collection of data.	The main task of this phase is to review network-based evidence.
4	Formulate Response Strategy	(a)identifying the impact of the incident on the organization. (b)Legal actions that can be taken against the culprit. (c)identifying actions that can be taken to discipline internal employees.	The main goal of this phase is to determine the appropriate response strategy considering the circumstances of the incident.

5	Investigate Incident	(a)Data Collection (b)Forensic analysis	This phase involves determining who, what, when, where, how, and why surrounding an incident.
6	Reporting	Guidelines for writing a good report.	This phase involves the creation of report in a manner that it is understandable to the decision-makers
7	Resolution	Results are obtained by executing host-based,network-based evidence.	This phase mainly focuses on measures that can be implemented to keep an incident from creating additional harm to the organization.

Table 1.1 Overview of incident process methodology.

Sr no:	Data collection types:	Consists of:	Remarks:
1	Host-based	Logs, records, documents and any other information that can be obtained from the system	Host-based data mainly consists of volatile information that can contain critical information.
2	Network-based	Information gathered from intrusion detection system logs, firewall logs, router logs, etc.	Network-based information permits an organization to accomplish several tasks such as Confirm or dispel suspicions surrounding an alleged computer.
3	Other-Evidence	Information collected from personnel files, interview employees, interview witnesses, interview character witnesses, and document the information gathered.	Other-Evidence consists of information obtained from the people.

Table 1.2 Types of data collection.

Host-based data collection is done in 2 ways:

(1)live data collection.

It consists of 3 types.

Sr No.	Name	Remarks.
1	Initial live response	Collects only volatile data from the target/victim system
2	In-depth response	Collect additional information such as non-volatile information from systems such as log files.
3	Full-live response	It is a full investigation of the live system.

Table 1.3 types of live data collection.

(2)forensic duplication.

IV. EXPERIMENTATION PERFORMED.

To apply host-based and network-based security measures, we created a network on cisco packet tracer consisting of the hub, personal computers, and a server, and a firewall was enabled in the server so that only authorized systems to get the data.ie. the experiment main aim was to configure the firewall on the server

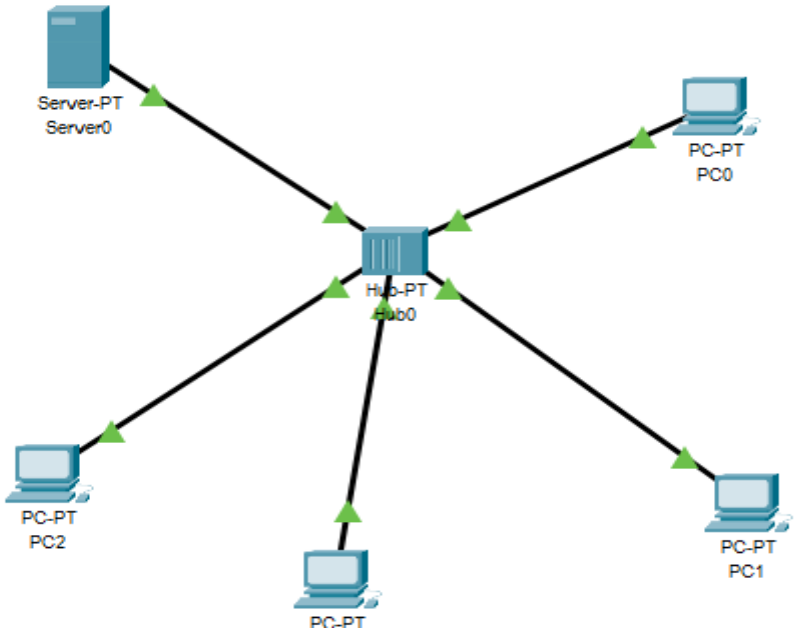


Fig 1.1 Network created using cisco packet tracer.

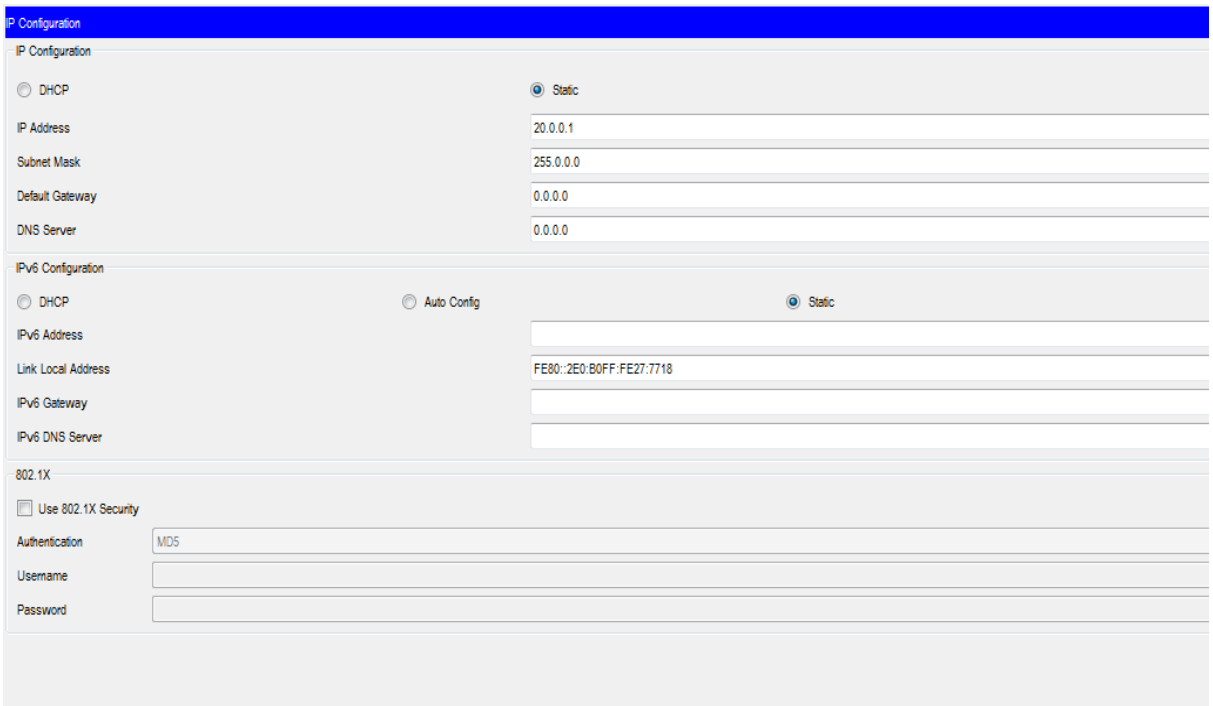


Fig 1.2 Server configuration.

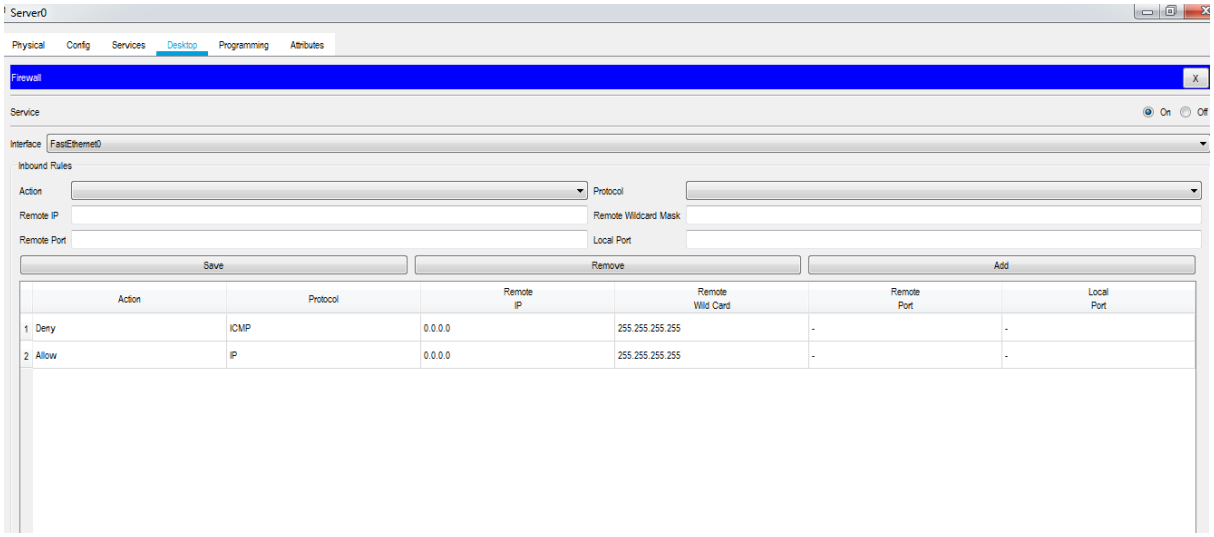


Fig 1.3 Firewall configuration.

(we have disabled the internet control message protocol but have enabled internet protocol meaning all the systems connected with the hub will get their IP address using DHCP protocol and all systems connected to the hub will be able to interact with each other but not directly with the server.)

The main aim behind configuring the firewall on the network was to distinguish between authorized and unauthorized users, so that data will be transmitted only to the authorized users who are registered on the server.

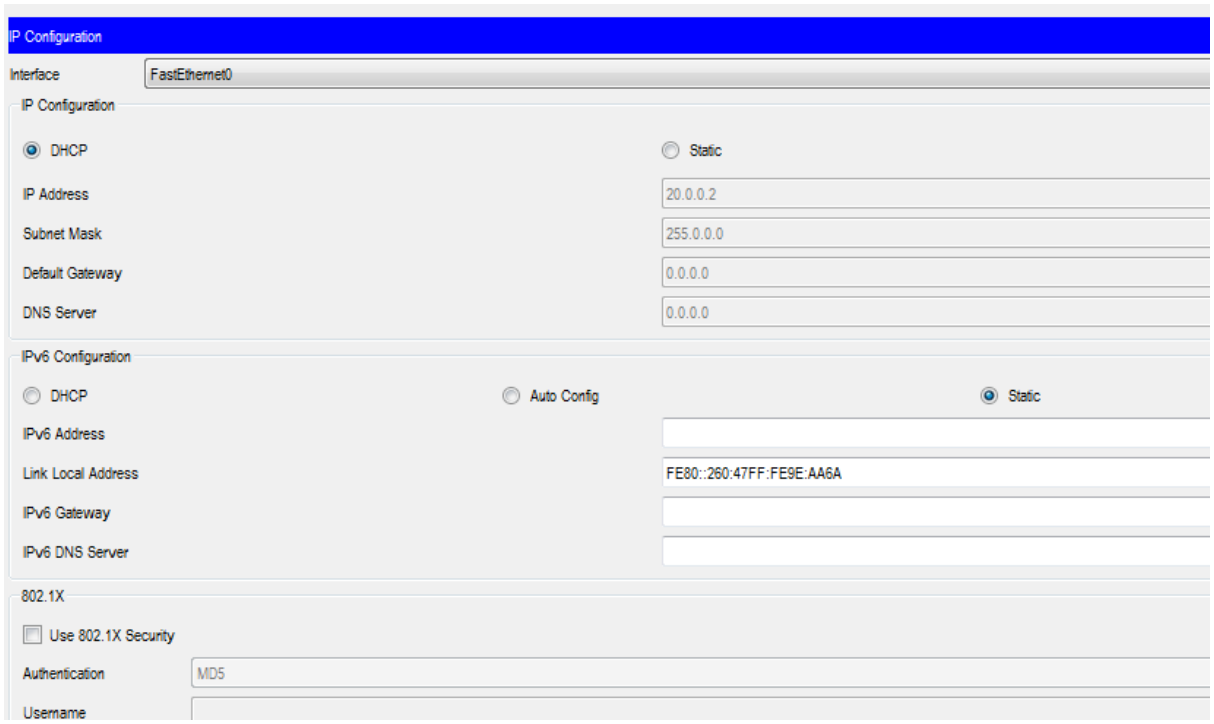


Fig 1.4 IP configuration of one of the systems obtained from the DHCP.

V. RESULTS OBTAINED.

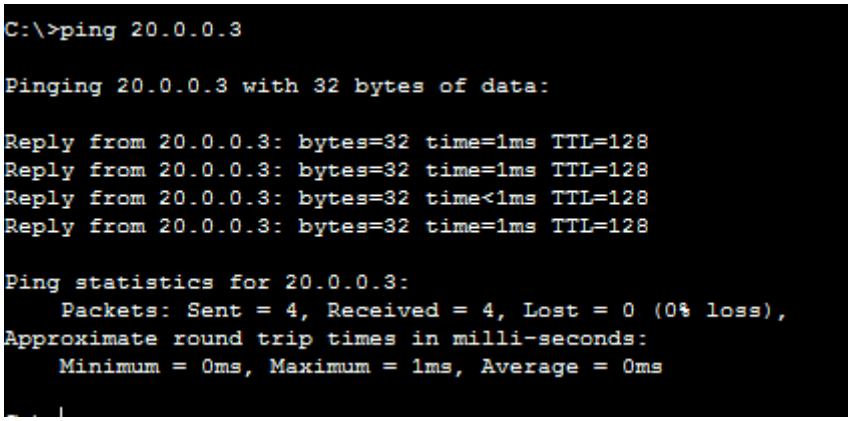


Fig 1.5 shows that the connection is successfully established from one system to another.

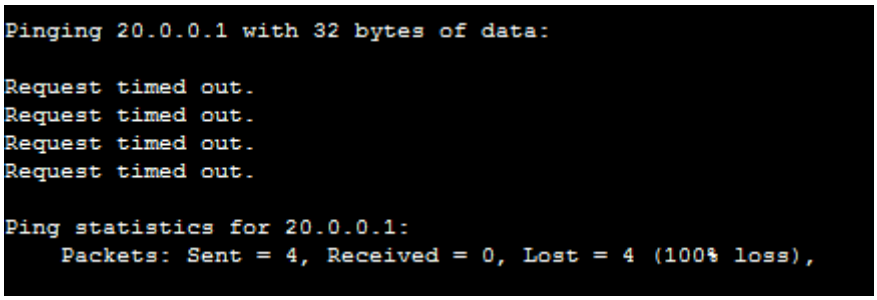


Fig 1.6 shows that connection is not successfully established when trying to communicate from one system to the server because we have disabled the ICMP protocol while configuring the firewall in the server.

VI. CONCLUSION

This paper provides a detailed overview of incident process methodology in cyber forensics. The experimentation performed proves that the addition of a firewall in your server acts as a great security measure to prevent any intruder entry into your network.

VII. ACKNOWLEDGEMENT

I would like to thank Mr.Krishna Samdani(Assistant Professor,Mukesh Patel School of Technology Management &Engineering) for his support .Also ,I acknowledge the contribution of NMIMS University to provide this wonderful opportunity and good facilities to carry out this work.

REFERENCES

[1]Karen Scarfone, Paul Hoffman 'Guidelines on Firewalls and Firewall Policy' NIST Special Publication 800-41 Revision 1

[2]ITSM Process Description Office of Information Technology Incident Management

AUTHOR

Karthik Konar is a first year student pursuing MCA from SVKM NMIMS Mukesh Patel School of Technology Management And Engineering(MPSTME), Mumbai, India. His passion for research led him to gain interest in exploring new domains such as artificial intelligence, wireless sensor networks, Cyber forensics. He has published 2 research papers in the fields of wireless sensor networks, artificial intelligence.