Network Forensic Analysis with Efficient Preservation for SYN Attack

Deepali Avasthi
Amity University
Lucknow-226070, India

ABSTRACT
In Now-a-days Internet has removed physical distance among individuals for communication and also provides the platform for cyber crimes. Attacker attacks on protocol and steal information, so it is necessary to find out the attackers. Network Forensic is basically about monitoring, capturing, analysing the network traffic and investigating the security policy violations. Main goal of Network Forensic is to discover the source of attacker and provide evidence to identify the attackers. This paper proposes a simple architecture of network forensic for SYN attack and it is also provide efficient preservation. We are using self embedded watermark provide integrity and at the time of watermark it requires security key which will provide authenticity . It ensures the efficient preservation. It uses various open source port scanning tool such as Nmap, Advance port scanner, free port scanner and also capturing tool as Snort.

General Term
Network forensic

Keywords
Port scanning, SYN packets, FIFO ,snort, nmap

1. INTRODUCTION
Continuous improvement in information technology, networking and communication giving us advantages and increasing our dependence on computer as well as on Internet. Internet provides a lot of services. Organisations have daily transaction on Internet so network security is very essential. That is a big issue in organisational environment. Due to dependency of company on web services on Internet and Internet is source of cyber crimes.

Computer users need proper security to save and protect their valuable information from hackers, when the system is connected with Internet. Several techniques are developed to secure network infrastructure and communication over Internet, such as firewalls for prevention; Intrusion detection system and antivirus for detection but now organisation are interested to trace and follow up the attacker. Increasing cyber crimes gives the birth of new branch as forensic science or computer forensic.

Computer forensic is a technique of recognising, collecting, storing , analyzing and showing the result as evidence in a legal way.

Network forensic is investigation technique that capture, store and analyze network packets for investigative purpose.

Network forensic is science that deals with capturing, recording and analysing the network traffic for detecting and investigating network traffic. Network forensic is next step of network security. Network security defends system against attack by attackers whereas Network forensic system collects the proof of integrity as evidence of attack. [1]In network forensic system network traffic can be captured either in "catch it as you can" form means capture all network packets ,It will require a large amount storage to store data, or "stop, look, and listen" i.e " in filtered form".[10]

Network forensics is the area of using forensic science to the network environment to find out the source of attack/cyber crimes. The main goal is to mark suspicious activity from network data and calculate the damage that is occur or could be in future [3]. Network forensics is defined as "the use of scientifically proven techniques to collect, fuse, identify, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of facilitating or furthering the reconstruction of events to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations"[4]. Network forensics is the science that deals with capture, recording, and analysis of network traffic for detecting intrusion and investigating them[5].

Network forensics is basically about monitoring, capturing, analyzing the network traffic and investigating the security policy violations. Forensic specialist monitors the network continuously and stores a copy of all or the relevant packets, depending upon the policy, in a prescribed format for future analysis. These stored packets information is further analyzed, either manually or by using different approaches, to find if there is an anomaly in the network and if that anomaly is an attack. If any attack is found, the type of attack is determined and the source of the attack is investigated. Forensic specialists can attribute the attacker by proper monitoring, capturing, and analysis of the network traffic and by proper investigation.

Main goal is to discover the source of attacker and provide evidence to identify the attackers. Attackers checks whether any port (SMTP, FTP, HTTP) is open or not, if port is open then he may proceed for attack. Attackers use denial-of-service (Dos) attack.

Our objective is analysis of port scanning attack and discovers the source of attacker.

1.1 Motivation
The large numbers of fresh DDoS attacks are affecting security in organisations that is very hard to recognise and become undetected until the event happen. Companies have to be painstaking in recognising and opposing attempt to weaken their sites.

This year (2011-12) various attacks again Mastercard, Visa, Sony are on toplist.

1. In 2010, WikiLeaks release US Defence Department secrets. Also released diplomatic cables leak from US embassies. In 2011, WikiLeaks release prison file leak and secret of spy file.

   In 2009 ACMA blacklist the WikiLeaks sites for all Australians, that is removed in last 2009.

   In 2010 US library of congress is blocked. FBI, US Army, Deptt of justice considered criminally prosecuting WikiLeaks. [17]

2. In June 2011, Lulz Security (LulzSec) involve in DDoS attack against the SOCA, At the same time Reston Virginia facility of Swiss web hosting service also raided by LulzSec for information on undiscovered target. CIA website also suffered from distributed denial-of-service(DDoS) attacked by LulzSec and also changed the password of a numbers of users of the United States Senate to make anyone unsafe on Internet. In June 2011 LulzSec claimed for attack against Sony pictures for data with name, email, password, address of many peoples.

3. Hackers targeted the Sony Play station by recruiting people to joining the Geohot and participate where as participation was free to anyone. Many customers suffer If they click then PC will be targeted.[6]

4. Hong Kong stock market aimed for DDoS attack affecting multiple companies and individuals financially.

2. PORT SCANNING

Network scanning is to scan the network i.e. to obtain the information of the host or the network. The purpose of network scanning is to obtain the networking information of a particular host by knowing IP address, routing, domain name and system information as operating system etc. Port is a process/application specific address of destination/source endpoints for communication purpose. Port is identified by a 16 bit number known as port number of range 0 to 65,535.
Port numbers are divided into three ranges

- Well Known Ports: Ports range from 0 to 1023 are well known ports. eg port *25 for* SMTP, *port 20 for* FTP , port *80* for HTTP.
- Registered Ports: Ports range from 1024 to 49151 maintains official list. eg port 5010 for Yahoo! Messenger
- Private or Dynamic Ports: Ports range from 49152 to 65535, can be used by any process. These are also known as ephemeral ports.[7]
- Port scanning is identifying active machines, information gathering and finding whether hosts are open or not. Port scan shows that there are chances of occurrence of attack in near future. Port scanning is same as knocking the door and determines what systems are listening & reachable from the Internet.

The ports of a machine can be scanned in following ways

- SYN scan: To a particular destination Port so many packets with SYN flag are moved and establish three way handshake if port is open with reply SYN/ACK flag indicator. SYN Scan is half opening scanning because here complete TCP connection is not maintained.
- TCP connect scan: A lot of connections are maintained by connect() system call with victim at different port. A connection established and shows port is open if connect() returns true otherwise port is closed. TCP connect scan is a complete connection.
- ACK scan: To a particular destination so many packets with ACK flag are moved and get the result for an open port with reply SYN/ACK flag indicator.
- FIN scan: To a particular destination so many packets with FIN flag (without SYN/ACK packets) are moved and destination reply RST shows the port is closed. Open port always ignores the packets.

3. RELATED WORK & LITERATURE SURVEY

In 2001, Palmer in Digital Forensic Research Workshop (DFRWS) proposed a framework for dealing with network environment having various steps from Identification of packets, Analysis ,observation are presented, taking Decision about the packets and result are documented for future investigation **(Palmer G. , 2001)[4]**

In 2002, An abstract digital forensic model was proposed by adding two more steps in DFRWS framework by Reith et al . These two more steps were preparation, approach strategy and returning the evidence (Reith et al., 2002). This model has following steps: Identification, Preparation and approach strategy, Preservation, Collection, Examination, Analysis, Presentation and Returning evidence.[18]

In 2003, A new incident response methodology was by Mandia and Procise where an initial response phase based on data or information collected to access the incident and to express the response phase in a clear way are added. Working of investigation phase is to collect the traffic then apply analysis. In last reporting phase shows the improvements and changes (Mandia K, et al. ,2003).

In 2003, Carrier and Spafford proposed an Integrated digital investigation process model with phases: Ready, survey, search, collection, process, reconstruction and documentation The goal of these phases is to ensure that the personal and infrastructure are able to fully support an investigation when an incident occurs.Ready phase shows the readiness of operations infrastructure, next phases survey, search, collection combined and process the data ,then analyze the data and records the evidence.

In 2004, An investigation process model come in existence by Casey and Palmer where assessment phase to validate the incident and decision phase about to continue the investigation or not are added with common phases.

In 2004 Ciardhuain proposed a cyber crime investigation model by combining phases of all existing model. It performs full investigation having steps of awareness, authorization and planning.

In 2004, A new model by enhancing Integrated digital investigation process model of Carrier and Spafford ,2003 by adding two new phases traceback and dynamite.

In 2005, Ren and Jin proposed first generic model for network forensic having steps Capture, copy, transfer, analysis, investigation and presentation.In 2009, A generic framework based on digital forensic models was developed by Pilli E S having various phases. This generic process model has steps :

Preparation of placing network security, Detection of unauthorized events , Incident response on attack identified ,Collection of traffic data, Storing of original data as backup , Examination of obtained integrated large data, Analysis of attack patterns ,Investigation of the path of attacker, and Presentation of observations for legal requirement in understandable format (Pilli E S, et al. ,2010)

All existing frameworks are sown in easy to understandable (tabular) form in Table. 1

Table 1: Tabular representation of existing frameworks with proposed phases

YEAR	AUTHOR	PROPOSED MODEL	PHASES OF PROPOSED MODEL
2001	**Palmer G**	**First framework for forensic science in the network environment**	**Identification, Preservation , Collection, Examination ,Analysis, Presentation and Decision**
2002	**Reith et al.**	**Abstract digital forensic model**	**Identification , Preparation & approach strategy, Preservation , Collection, Examination ,Analysis, Presentation and Returning evidence**
2003	**Mandia K, Procise C**	**Incident response model**	**Incident preparation, detection of incident, initial response, formulate response strategy, investigation and reporting**
	Carrier and Spafford	**Integrated digital investigation process model**	**Readiness, survey, search , collection, process, reconstruction , documentation**
2004	**Ciardhuain**	**Extended model of cyber crime investgation**	**Awareness, Authorization, Planning, Collection, Examination, Presentation and Dissemination**
	Casey and Palmer	**Investigative process model**	**Incident alerts , Assessment , Identification , Preservation, Recovery, Harvesting , Reduction Organization and search, Analysis ,Persuasion and testimony**
	Baryamureeba , Tushabe	**Enhanced digital investigation process model**	**Readiness, survey, search , collection, traceback, dynamite process, reconstruction , documentation**
2005	**Ren and Jin**	**First general purpose model for network forensics**	**Capture, copy, transfer, analysis, investigation and presentation**
2009	**Pilli E S, Joshi R C, Niyogi R**	**Generic framework**	**Preparation, Detection, Incident response, Collection, Preservation, Examination, Analysis, Investigation, Presentation**

4. PROPOSED WORK

This framework tells attackers can use various port scanning tools as Advance port scanner, Free port scanner, Angry IP scanner, Nmap etc. and victim host can use capture tools like Snort.

4.1 Nmap

Nmap ("Network Mapper") is open source utility for network security auditing. It is called security scanner. It is used to discover host on network, it creates "map" of network. Nmap uses IP packets to determine various characteristics of network such as available host on the network, services provided by hosts, operating systems (and OS versions), firewalls are in use, and other. Zenmap is official Graphic User Interface for Nmap. Nmap mainly runs on Linux, also on Windows, Solaries, BSD etc.[11]

Basic Nmap commands are

- Nmap port scanning

  # nmap -v -sT local host

- Nmap TCP SYN (half open) scanning

  # nmap -v -sS local host

- Nmap TCP FIN scanning

  # nmap -v -sF local host

- Nmap TCP NULL scanning

  # nmap -v -sN local host

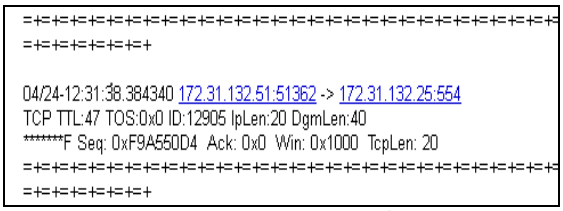
4.2 Port Scanner

Port scanner is a software application used by administrator to check security of network and also by attackers to check or identify running services on hosts. A Port scan is an attack of sending request from client to range of server port address on host for finding active port and knowing vulnerability of that services. [7]

4.2.1 Free Port Scanner

FreePortScanner is a small Windows application by which users can scan specific ports on a given IP. It needs the port numbers and the IP the user wishes to scan. All the fields are at the top of the main window, the rest of the window is used by the results of the scan having IP address, port number , status and description. FreePortScanner is easy to use, so help file is completely missing from the FreePortScanner package. FreePortScanner provide entire ranges to be scanned, not only specific ports.[12]

4.2.2 Advance Port Scanner



Advance Port Scanner is easy-to-use, fast and small port scanner for Win 32 platform. It can scan ports very fast, Also it can perform scans on predefined port ranges, description of common ports available here[13].

Features of Advance Port Scanner

- It gives fast and stable port scanning.
- It is fully configurable port scan.
- It can export scan results.

4.2.3 Angry IP Scanner

Searching for addresses with known properties of computer networks is a practice that is used by both network administrators and hackers. Administrators need to scan their own networks to check status of computers and network devices ,find spare addresses in statically-addressed networks, check for recently identified holes in order to patch them, and much more things. Angry IP Scanner (or simply *ipscan*) is open-source and multi-platform network scanner. It is designed to be fast and easy-to-use. It runs on *Linux*, *Windows*, and *Mac OS X.[14]*

4.3 PROPOSED ARCHITECTURE OF NETWORK FORENSIC SYSTEM

Proposed Architecture of Network Forensic System has three modules Collection and Preservation module, Analysis module, Presentation module as shown in figure 1. The working of system is to collect the packets from network interface, analyze the useful packet and present the information of suspicious addresses.

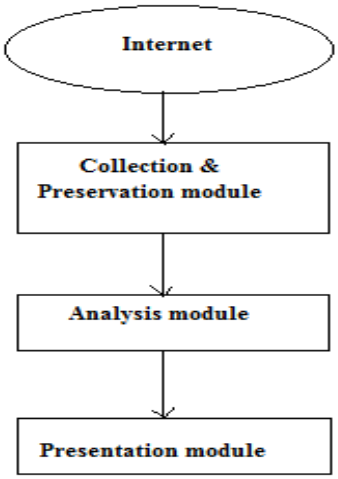


Figure 1: Proposed Architecture of Network Forensic System

4.3.1 Collection and Preservation module

The main task of Collection and Preservation module is to capture all network traffic from network interface for network forensic analysis. This module collects all packets which are passing by network interface of host system and transfer it to UNIX inter process communication FIFO. Working of FIFO is that data has been read by once, it is discarded from FIFO automatically. We capture packets from network interface by using Snort tool,[15] output of Snort is redirected to FIFO. Command used for capturing and redirecting packets is ' **snort -v try.txt**' . A format of captured packet is given in figure 2.

Figure 2. A captured packet

In this module filtering only TCP packets will results in less storage space of hard disk as compared to capture and store all packets passing through network interface.

Previously we use encryption for confidentiality or hash function for storage of network traces to maintain integrity but

now in this module text is converted in to image providing confidentiality, use of self embedded watermark provide integrity and at the time of watermark it requires security key which will provide authenticity [16]

4.3.2Analysis module

The analysis module takes as input the captured and collected data stored in host system. **T**his module choose only TCP packets for analysis. It considered attack via port scanning method. TCP-SYN, TCP-ACK, TCP-FIN methods are identified by S, R, F flags in packets. A data structure **ipdetail** is prepared with following fields:

- Relevant machine address: Shows IP address that request for connection with host.
- Port Count: total number of ports for which connection is requested.
- Date: Date at which connection request occur.
- Initial time: Time when first connection request is sent.
- Finish time: Time when last connection request is sent.

Following algorithm is used for analysis of packets which are captured from network traffic

1. Catch all packets that have attacked the host computer using the utility snort (intrusion detection system) in a text file. Use command snort –v > try.txt
2. Store first line of file in array(a) , second line in array(b) and third line in array(c).
3. If b[0]= 'T' , b[1]= 'C' , b[2]= 'P'
   then checkline(c).
   else goto step 6.
4. If c[7] ='S' then it is SYN packet that attacked the computer.
5. If count > 3 then mark the packet suspicious .
6. Repeat step 2 for whole file EOF.
7. Print all suspicious and other parameters

4.3.3 Presentation module

On the basis of port count value by analysis module, machines are either suspicious or normal. Decision of suspiciousness of machines depends on the value which is greater than threshold value that is predefined. This module shows the analysis module output if having port scanning attack. Suspicious machine details are total number of packets, total meaningful packets, port count value, date, start time, time of last request are displayed as observation in a predefined format.

4.4 EXPERIMENTAL RESULT

Implementation is used for efficient preservation and analysis. To implement collection and preservation module, Snort is used from command line to capturing network traffic from network interface.

Analysis module is implemented by running user defined codes on terminal in Nmap, where a data structure "ipdetail" contains information of total packets.

A small network set-up of two hosts, each having the operating system Ubuntu, One hosts having IP address 172.31.132.98 is used to launch port scanning attack on the Victim host having IP address 172.31.132.25 shown in fig.3

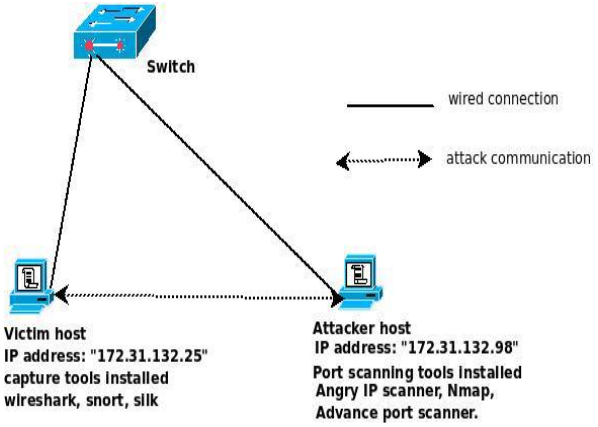


Figure 3: Attack perform by single attacker

Table 2: for single attacker

Victim IP address	172.31.132.25
Attacker IP address	172.31.132.98
Date	4/24/11
Starting Time of attacker	04:06:55
End Time of attacker	04:08:13

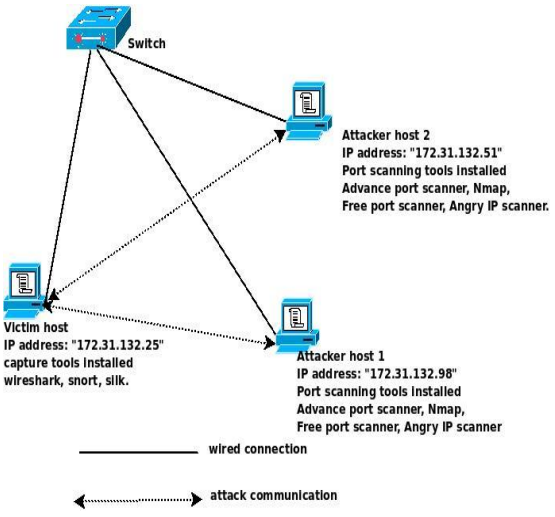


Figure 4: Attack perform by two attackers

In a small network two hosts having different IP address were used to launch port scanning attack on the victim host having IP address 172.31.132.25' shown in figure 4. We used snort to collect the packet captures in the victim system

Table 3: For two attackers

Victim IP address	172.31.132.25
Attacker 1 IP address	172.31.132.51
Attacker 2 IP address	172.31.132.98
Date	4/24/11
Starting Time of attacker 1	5:16:20
Starting Time of attacker 2	5:17:01
End Time of attacker 1	05:16:21
End Time of attacker 2	05:17:20

Following figure (figure 5) gives the results of packets after analysis, that machine sending connection request is suspicious or normal

Fig 5: Comparison with previous work

Proposed work discovers the source of attackers. This network forensic model is capable to discover more than one source of attackers. If various attackers are scanning the host machine then proposed model will discover and provide the details of attackers.

5. CONCLUSION

This framework discovers the source of attackers. Results shows that it will work properly if more than one attackers are scanning the host machine using Nmap. It provides efficient preservation for network forensic system. By this proposed framework integrity, confidentiality, authenticity all security requirement can be maintained. If same type of incidents occurs in future, they can be solved easily.

6. ACKNOWLEDGMENT

I am thankful to my God Bade Maharaj ji and my brother Rama Kant Misra for spiritual support. I would like thank to Vimal Kumar who has given several tips and suggestions towards development of the framework.

7. REFERENCES

[1] E. S. Pilli, R. C. Joshi and R. Niyogi. Network forensic frameworks: Survey and research challenges. In Digital Investigation, In Press, corrected proof, 2010.

[2] Atul Kant Kaushik, Emmanuel S. Pilli and R. C. Joshi. Network forensic system for port scanning attacks. In 2nd International Advance Computing Conference (IACC),Thapar University, Patiala, India, pages 310-315. IEEE 2010.

[3] R. Chandran. Network Forensics. Know Your Enemey: Learning about Security Threats, Second Edition, Ed. L. Spitzner, Addison Wesley Professional, pages 281 -325, 2004.

[4] G. Palmer. A Road Map for Digital Forensic Research In in proceedings of 1st Digital Forensic Research Workshop (DFRWS 2001), Utica, New York, pages 27-30 ,LNCS Springer August 2001.

[5] A. Yasinsac and Y. Manzano. Policies to Enhance Computer and Network Forensics. In IEEE Workshop on Information Assurance and Security,, United States Military Academy, West Point, New York, June 2001, pages 289-295, 2010.

[6] Consumer electronic and IT products available at www.sony.co.in

[7] Port computer networking at http://en.wikipedia.org/wiki/Port_(computer_networking

[8] Mandia K, Procise C. Incident response and computer forensics. New York: Osborne McGraw-Hill; 2003.

[9] Casey E, Palmer G. The investigative process. In: Casey E, editor. Digital evidence and Computer crime. Elsevier Academic Press; 2004.

[10] S.Garfinkel, "Network Forensics:Tapping the Internet" http//www.oreillynet.com/pub/a/network/2002/04/26/nettap.html

[11] **N**etwork **Map**per) is a security scanner at en.wikipedia.org/wiki/Nmap

[12] Software free scanner download at http://www.softpedia.com/get/Network-Tools/Network-IP-Scanner/FreePortScanner

[13] Advance Port Scanner V 1.3 http://www.radmin.com/products/previousversions/portscanner.php

[14] Angry IP Scanner available on http://www.angryip.org/w/Home

[15] Snort, Snort® is an open source network intrusion prevention and detection system (IDS/IPS) on www.snort.org

[16] Vimal Kumar, Akhilendra Pratap Singh, Anjani K. Rai , Manoj Wairiya: Self Alteration Detectable Image Log File for Web Forensics. In International Journal of Computer Applications, 2011

[17] WikiLeaks, WikiLeaks is a not-for-profit media organization on www. wikileaks.org

[18] M. Reith, C. Carr and G. Gunsch. An examination of digital forensic models. In International Journal of Digital Evidence, , volume:1, Issue:3 pages 112, Fall 2000.