Network Forensics an emerging approach to an network analysis.

[1]Abhishek Srivastav
M.S. in Cyber Law & Information Technology
Indian Institute of Information Technology,
Allahabad, India
Abhiit02@gmail.com

[2]Irman Ali
M.S. in Cyber Law & Information Technology
Indian Institute of Information Technology,
Allahabad, India
Ali.cs09@gmail.com

Abstract: Network forensic is a new growing approach to a network security. Digital forensic applies the forensic procedure to electronic or digital evidence. This digital forensic process involves systematically collecting and analyzing digital information for use as evidence in court. Network forensics is a branch of digital forensics that focuses on the monitoring and analysis of network traffic. Network forensics is the process of gathering and examining raw data of network and systematically tracking and monitoring traffic of network to make sure of how an attack took place. Network forensic will help in identifying unauthorized access to computer systems and networks, and searches for evidence if it will happen. In this paper, we are focusing on network forensics, the steps to perform network forensics, various network forensic tools, comparison chart, and emerging area of network forensics.

Keywords: network forensics, digital forensic, network forensic tools

Introduction :

Network forensics is the process of collecting , recording, and examining of network events for finding the source of security attacks. It helps in identifying unauthorized access to computer systems, and searches for evidence in case of such an occurrence. Network forensics is in fact to investigate, at a network level, things taking place or that have taken place across an IT system. There are three parts of network forensics: [2] Intrusion detection

- Logging
- Correlating the intrusion detection and logging[2]

The main goal of network forensics is to provide enough evidence to allow the criminal perpetrator to be successfully prosecuted. The practical application of Network Forensics could be in areas such as hacking, email investigation, fraud detection , insurance companies, data the, defamation, narcotics trafficking, credit card cloning, software piracy, electoral law, obscene publication, perjury, murder, sexual harassment, and discrimination.

Network Forensics Systems Can Be Of Two Kinds

"**Catch-it-as-you-can**" systems, in which all packets passing through certain traffic point are captured and written to storage with analysis being done subsequently in batch mode. This approach requires large amounts of storage.[3]

"**Stop, look and listen**" systems, in which each packet is analyzed in a rudimentary way in memory and only certain information saved for future analysis. This approach requires a faster processor to keep up with incoming traffic. [3]

Developing Standard Procedures for Network Forensics: network forensics is a long , tedious process, and unfortunately trail can go cold quickly. A standard procedure often used in network forensics Is as follows.

- Always use a standard investigation image for system on a network. This image is not a bit stream image but an image(dd) containing all the standard application used. You should also have the MD5 and SHA-1 hash values off all application and os files.[1]
- When an intrusion incident happens ,make sure the vulnerability has been fixed to prevents othr attacks from taking advantage of the opening.
- Attempt to retrieve all volatile data such as RAM and running processes, by doing a live acquisition before turning the system off.

- Acquire the Compromised drive and make a forensic image of it.
- Compare files on the forensic image to the original installation image compare hash values of coomon files , such as Win.exe and standards DLLs and ascertain whether they have changed.

EMERGING NETWORK FORENSICS AREAS

Network forensics has important roles to play in new and developing areas related to social networking, data mining and digital imaging, and data visualization.

Social networks :

Social networking sites such as Google+, Facebook, Twitter, and YouTube have expanded astronomically in recent years, but because the success of such sites depends on the number of users they attract, there is pressure on developers to design systems that encourage behavior that increases both the number of users and their connections. Security has not been a high priority, leading to the emergence of inevitable security risks. Obviously, there is a need for network forensic tools that address such an important area of usage, but to date, only traditional digital and network forensic tools are available.

Data mining:

Forensic profiles can be created using data mining technology, which provides a way to discover relevant patterns, thus generating profiles from large quantities of data. Although there has been significant work in the areas of extracting and analyzing digital evidence from physical devices such as hard disks, less work has been reported on data mining in portable storage devices such as flash drives, cell phones, digital cameras, radio frequency identification devices, compact disks, and iPods.

The extraction of historical data from supervisory control and data acquisition (SCADA) systems, which are widely used to monitor and control equipment in various industries such as oil and gas refining, water and waste control, and transportation, is an important area that draws on the combination of data mining and network forensics. There is currently no generic model for understanding the processes necessary to gather digital evidence from SCADA systems. However, such a model is needed to enable incident response, intelligence gathering, digital evidence collection and legal action against system intruder. There is a distinct difference between the process of network forensics-based data mining investigations (where time-based data is analyzed to detect potential malware intrusion) and incident recovery and response (where the key purpose is to respond to an alarm and implement recovery). Some work has been done to incorporate the use of decision trees as well as naive Bayesian, a priori, and neural network techniques. Recently proposed architectures also incorporate mechanisms for monitoring process behavior, analyzing trends, and optimizing plant performance.

Digital imaging and data visualization:

Researchers have developed numerous state-of-the-art tools to assist in conducting digital crime investigations. However, digital investigations are increasingly complex and time-consuming due to the amount of data involved. The visualization of data obtained from such investigations is a new and developing area and has the potential to display significant volumes of data where the dimensionality, complexity, or volume prohibits manual analysis. Data visualization is the graphical interpretation of

high-dimensional data, which is particularly appropriate for obtaining an overall view and locating important aspects within a dataset. This is useful in network forensics because the data encountered in digital investigations is often significant in size, multidimensional, and complex. Consequently, obtaining an overall view can help digital investigators obtain a better understanding of the data and identify important aspects to assist in the recovery of appropriate digital evidence.

Network forensic tools :

Network forensic can be done by using different types tools which can be categorized as the following:

- Using network tools
- Using UNIX/LINUX tools
- Using packet sniffer
  Using network tools : A variety of tools are available for network administrators to perform remote shutdowns, monitor device use, and more. The following are the list describes a few examples of the powerful windows tolls available at Sys internals
- Regimen shows all registry data in real time
- Process Explorer shows what files , registry keys, and dynamic link libraries are loaded at a specific time.
- Handle shows what files are open and which processes are using these files
- Philemon shows file system activity.

Using Unix /Linux tools: Knoppix security tools distribution is a bootable Linux CD intended for computer and network forensics. A few of the Knoppix-std tools include the following.

Dcfldd- the u.s. DOD computer forensics lab version of the DD command

Memfetch- forces a memory dump

Snort- a popular IDS that perform packet capture and analysis in real time.

Oinkmaster – helps manage snort rules so that you can specify what items to ignore as regular **traffic** and what items should raise alarms

John – the latest version of john the ripper, a password cracker

Chntpw – enables you to reset passwords on a windows computer , including the administrator password.

Tcpdump and ethereal – packet sniffers.[1]

Using packet sniffers : packet sniffers are devices and/or software placed on a network to monitor traffic. Most network administrators use sniffers for increasing security and tracking bottlenecks. However, attackers can use them to obtain information illegally. On tcp/ip networks, sniffers examine packets , hence the term "packet sniffers."

Most packet sniffers work at layer 2 or layer 3 of the osi model. To understand what's happening on a network, often you have to look at the higher layers by using custom software that comes with switches and routers, however.

Methodology

Task performed by network forensics tools: all network forensics tool perform some specific task. These task are combined into five major categories, each with sub functions for further refining data analysis and recovery.

- Acquisition
- Validation and discrimination
- Extraction
- Reconstruction
- Reporting

Acquisition : the first task in network forensics investigation , is making a copy of the original drive. Sub function in the acquisition category include the following **:**

- Physical copy of data
- Logical copy of data
- Data acquisition format
- Command line acquisition
- GUI acquisition
- Remote acquisition
- Verification

Validation and discrimination : the process of validating data is what allows discrimination of data. Many forensics software vendors offer three methods for discriminating data values. These are the sub functions of the validation and discrimination function

- Hashing
- Filtering
- Analyzing file headers

Extraction : The Extraction process is the recovery process in an investigation of cyber crime and is the most challenging of all tasks to master. The following sub functions of extraction are used in investigation.

- Packet viewing
- Keyword Searching
- Decompressing
- Carving
- Decrypting
- Bookmarking

Reconstruction: The purpose of having a reconstruction feature in a forensics tool is to re create a suspect drive to show what happened during a crime or an incident**.** These are the sub functions of reconstruction.

- Disk to disk Copy
- Image to Disk Copy
- Partition to Partition copy
- Image to Partition copy

Reporting : To complete a digital forensics analysis and examination , you need to make a report. These are the sub functions of the reporting function

- Log Reports
- Report Generator

Network Forensic Analysis Process:

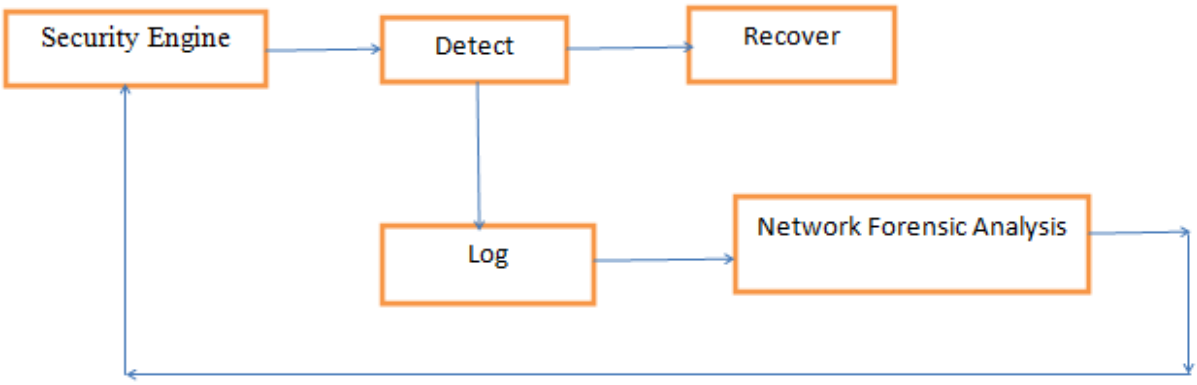

Figure: Network Forensic Analysis process

Functional Point Analysis:

Tools	Features and Advantages	Attributes
Wireshark	Widely used network traffic analysis tool, forms basis of network forensic studies.	Filter & collect
Driftnet	Listen to network traffic and picks out images used in backtrack version 5	Filter & collect
Tcpdump	Command line Network packet analyzer that supports network forensic Analysis.	Filter & collect
Kismet	Network detector, network packet sniffer, and intrusion-detection system for wireless LANs	Filter & collect
Xplico	A network forensic analysis tool that allows for data extraction from traffic captures; used in Backtrack version 5	Filter & collect
NetworkMiner	A network forensic analysis tool that can be used as a passive network sniffer/packet-capturing tool	Filter & collect
Ngrep	Simple, low level network traffic debugging tool.	Filter & collect
Solera DS	Appliance for live network forensics, application classification, metadata extraction, and analysis tools	Filter & collect, Reassembly of data stream
NetIntercept	Appliance for network forensics, monitoring, and analysis	Filter & collect, Reassembly of data stream, Correlation of data, Application layer view
Netwitness	Addresses network forensic analysis, insider threat, data leakage protection, compliance verification, designer malware, and 0-day detection	Filter & collect, Reassembly of data stream, Correlation of data, Application layer view, Log Analysis
RSA EnVision	Provides live network forensics analysis, log management, network security surveillance, data leakage protection	Filter & collect, Reassembly of data stream, Correlation of data, Application layer view, Log Analysis
Forensic & Log Analysis GUI	Log file analysis combined with network forensics, the Python implementation	Log Analysis
Dragon IDS	Provides network, host intrusion detection and network forensic capture analysis	Filter & collect, Reassembly of data stream, Correlation of data, Log Analysis
Infinistream	Appliance for network forensics, incident analysis combined with session reconstruction and playback	Filter & collect, Reassembly of data stream, Correlation of data
Savant	Appliance for live forensic analysis, surveillance, network analysis, and critical infrastructure reporting	Filter & collect, Reassembly of data
Snort	Widely used, popular tool for network intrusion detection and prevention, as well as for network forensic analysis	Filter & collect
Honey D	Improves cyber security by providing mechanisms for traffic monitoring, threat detection, and assessment	Filter & collect
Omnipeek	Low-level traffic analyzer for network forensics	Filter & collect, Reassembly of data stream ,Log Analysis
EtherApe	Graphical network monitor for capturing, network traffic	Filter & collect
Flow-Tools	Software package for collecting and processing NetFlow data from Cisco and Juniper routers	Filter & collect, Log Analysis
Fenris	Suite of tools for code analysis, debugging, protocol analysis, reverse engineering, network forensics,	Filter & collect

	diagnostics, security audits, vulnerability research	
DeepNines	Provides real-time identity-based network defense for content and applications, along with basic network forensics	Filter & collect
Argus	Used for network forensics, nonrepudiation, detecting very slow scans, and supporting zero-day attacks	Filter & collect, Log Analysis
Netstumble	Widely used wireless LAN analysis tool for devices and network traffic analysis	Filter & collect
Airmon-ng	Widely used suite of low-level traffic analysis tools for wireless LANs; used in Backtrack version 5	Filter & collect, Reassembly of data stream, Correlation of data, Log Analysis
Ettercap	Packet capture, ARP poisoning, Network protocol analysis & security auditing.	Filter & collect

Conclusion:

Network Forensic is the procedure that makes sure of investigation of attacks performed in the network or network devices. In this paper we concluded a matrix for analyzing various network forensics tools. The data analysis steps of network forensic process is the core for investigating any security breach in network. Unlike digital forensics, which collects information from a computer and disk of computer or other storage devices, network forensics collects both traffic and information about which ports it used to access the network. It is impractical that a single tool will be used for any investigation in generally it is observe that combinations of tools are used for investigation process. Form analyzing various past statistics it is found that Network forensics has crucial roles to play in new and developing areas that is related to social networking, data mining and digital imaging, and data visualization.

References:

[1] http://browse.feedreader.com/c/Cyber_Attacks_Vulnerabilities_Advisories_IT_Security_Research_Latest_IT_Security/233307330 , data accessed, jan 26, 2014.
[2] http://www.bitpipe.com/rlist/term/type/white+paper/Network-Forensics.html, data accessed, jan 26, 2014.
[3] http://searchsecurity.techtarget.com/definition/network-forensics, data accessed, jan 26, 2014.