Operating System Based Analysis of Security Tools for Detecting Suspicious Events in Network Traffic

Fasee Ullah and Waqas Tariq

Department of Computer Sciences, City University of Science & Information Technology
Peshawar, Pakistan

Abstract

Computer networks have important role regarding communication between the machines. Providing finite number of connections could be a little difficult to secure every connection from security hazards. Researchers have proposed many solutions for possible security hazards and known attacks but unfortunately it does not provide consolation up to satisfactory extents. Security engineers tried their best to scan the network for possible security hazards but attackers also have a very dedicated community, trying to find the best techniques for network intrusion attempts.

Many tools are designed for avoiding intrusion attempts, but we are still far away from optimal solution. This paper presents some of appropriated tools which are still in use for network security, anomaly detection, network intrusion detection and port analyzing.

Keywords: *Security; Operating System; Network intrusion; Attacks;*

1. Introduction

Computer network is the basic source of connecting machines. In between any machine we have some incorporated important data. When the machines are connected to the global network (Internet), the meaning full data is illegally accessed [1]. This kind of unauthentic and unauthorized access could lead Denial Of Service (DOS) attack [1] and [9]. In any organization for availability communication, connectivity between machines and resource sharing etc network and internet is used. Any machine connected to a network can be caused an eye over it and the important data inside the machine could be accessed illegally by the hackers [5]. Operating system is meant to obey the defined set of instructions in form of DLL (Dynamic Link Library) and .conf (configuration) files but these files are susceptible of changing instruction between them. UNIX systems are susceptible to thread in form of unauthorized user, intruders, worms, viruses and logic booms as well as failure and bugs [1]. In Microsoft Windows 7,360 altered and different forms of malevolent software targets has been discovered [7]. Technical user believes that the foot prints of the attackers are all recorded in security logs, attacker can be traced but unfortunately it is a volatile statement the security logs can be erased [1]. Tools for such intrusions detection are designed for technical user; installation and maintenance of tools for network intrusion detection and traffic analyzing are almost impossible for non-technical user. In this paper we discussed merits and demerits of tools for traffic analyzing, anomaly detection and other security event handling.

In the rest of this paper, section 2 describes Literature review; Section 3 describes critical review and section 4 describes conclusion and future work.

2. Literature Review

One of the most appropriate tool for the file integrity checks and Intrusion Detection (ID) written for UNIX environment is tripwire [1]. According to author, every computer system has some valuable data in it; usually that particular data is targeted by attackers. Intruders could modify the operating system configuration files for ease of future entry [1]. The system logs could be erased to clear the foot prints of the attackers, it can discourage future detection; Compromised security could lead to Denial of Service (DOS) attack [1]. Author proposed Tripwire tool for solution, by which administrator can have a closer look at file system integrity and administrator can sense unauthorized modifications in form of reports. The scenario of the tripwire operation is simple; it generate a Tw.conf (Tripwire configuration) file which contains all of the information about the current file system integrity and stores that file in database after configured time it checks the present files and match it with Tw.conf and then creates a tripwire report. A weakness of this

solution is that hacker can listen to the ports one by one and then analyzes which port of the system is being secured by tripwire. It is a comparatively simple job to shun attaching that particular port of the system [8].

[2] Introduces the immersive network monitoring system; for situational awareness in respect with retrospective analysis of the network traffic. According to author immersive network monitoring is based on internal attacks but the major principal is not to detect well identified forms of attacks that can be sense routinely. The primary goal is to enable detection of unauthorized attacks [2]. Authors designed algorithm for negotiated problems and then anticipated informs of Immersive Network Monitoring based tools. This system contains several modules for fast data collecting; a fast and robust database system; a highly efficient data purifying and handling pipe line; a time controlling system for time management; 3D animation based representation of domain, for understanding of user [2].Weakness is that it is a complex tool to configure it.

[3] has designed a tool for security analysts for situational awareness. It shows graphs for illustration of class B IP network, with a quick visualization of current state of network called NVisionIP. The author proposed a tool which is very best in detecting worm infection, compromised system attack, misuse attack, port based attack and Denial of Service attack [3]. The deployment scenario of NVisionIP is to record the NetFlow of data, which can be send by multiple routers; flow are recorded in all routers within the network and send to UDP to an essential data gathering where it congeries the NetFlow data in form of report, recorded NetFlow can then be presented in front of security analysts in form of picture that what is happening throughout the network. For further situational awareness traditional Intrusion Detection Systems (IDSys) take place [3]. Whenever anomaly practice configuration is sensed a notification is raised in form of email to the administrative authority perhaps the intrusion get recorded in logs [3]. Some weaknesses of NVisionIP are dependency of IDSys in proposed system and according to [1] the log files can be modified so the statement is volatile.

Weaknesses of [1,2,3] is port security because the crackers find the forwarded ports by port listening and then attack the computer system the finest identified denial of service attack is “SYS flood” it contains stream of TCP SYN packets which are observed by listening TCP ports at the victim. According to [9] most of attackers prefer numerous ports comparatively solitary port and some of them are dispersing throughout the domain. The primary step of securing the network is to find the best security for ports. One of the very appropriate tool for port security is [4] which summarize the statistics of motion for TCP ports; it helps to uncover the interesting security events by visualization. Intruders regularly probe the ports, and observing for the undefended ports that can be explored to achieve access to the victim’s machine [4]. In [1], [2], [3] they consider ports for security consolation but ports are the basic source used by crackers to target the computer system. Where [4] is designed for special consideration on TCP ports which makes it different and efficient from others. It provides an image of the traffic and the significant structures of data flow on network (for e.g. Port number, time, protocol etc.). The whole process of generating significant image of the network traffic movements is not exclusively different; because there are other tools that function correspondingly as PortVis (such as SeeNet, NvisionIP, Spinning the cube of potential Doom etc.) [4]. Solution is designed by consideration of port based attacks or worm attacks, distributive denial of service attack (many systems attack one system) and TTL walking attack. Scenario of visualizing the traffic is systematically disciplined in [4], it gives the complete detail of protocol, port number, hour of the report, session count and all of the important features; [4] provide a tool that converts non-concise network data in to significant graphs to represents the data.

[5] Presents tool for visualization of unusual suspicious traffic within the network of Abilene backbone (Internet 2 backbone for high performance). one aspect of proposed tool is statistical intrusion and anomaly detection method that allows networks to be observed for unknown attacks for which attack signatures are not been deployed yet [5]. Visualization technique of tools has originated much practice in network monitoring [5]. Intensive care for the flows ultimately is an excellent attribute of tool to identify Denial Of Service (DOS) attack and slammer worm attack [5]. Proposed frame work consists of sensors which play a very important role as software or hardware in recording the data, the verified data can be of subjectively high dimension [5]. For understanding the scenario of the sensor data representation it is to understand three basic questions. Where are the sensors? What traffic statistics is recorded? What are the dimensions? Sensors can be placed at any tangible or intangible intellectual environment hardware or software .i.e. routers, IP address perhaps source or destination ports. Sensors measure the statistics of data flow across the network. Sensors can distribute the territory of traffic by further detail as source or destination IP address, ports analyzed, time ratio etc. Solution is very mature

for security but some weaknesses of this proposed frame work is that it is very complex to understand by non-technical user as well as platform dependency, proposed solution is based on Abilene backbone network.

[6] Presents for an animated 3-D graphs and cubes to be plot on X, Y and Z-axis of the coordinates for visualization of network events. It displays traffic in three dimensional cubes which uses source and destination address as well as port numbers for each dimension. Internet is hostile network environment; every system connected to internet is unsafe, perhaps it is regularly scan and attacked by many techniques [6] and [8]. For present situation author(s) recommend InetVis to keep obscurity fine and avoiding future attacks. [4] and [6] are similar in the mean of consideration about the port analyzing. In [6] it is dedicated Y-axis for the destination port (TCP and UDP) visualization. Scanning the ports of the victim's machine is the very common major step for intrusion [8]. [6] Provides visualization for ports (TCP and UDP) which is very important feature of the tool and that make it very effective in security perspective among others. [6] Visualization of the network is divided in to three parts; First part for destination address (home address) plotting on horizontal X-axis by destination IP addresses; Second part for source address (external internet address) on Z-axis and the third part for the port(s) (TCP and UDP) plotted on vertical Y-axis.

[7] Presents a network visualization tool for detail analysis of data flow on the network and for investigating the network motions of host on network. Frame work of this paper is prepared under the consideration of problematic visual analysis of the communication, the data flow among host territory and the global network (internet). The problem is highlighted as the data flow between the machines across the network is essentially complex to analyze but it is to deal with data frames captured in intangible real time environment which also surrounds a complex association between the communication connections which may moreover be altering in time. The problem is tackled by conceptualizing TCP/IP protocol. According to authors the software architecture of [7] is TCP/IP protocol on network layer provides the source and destination address while the transport layer is responsible for capturing the source and destination port detail, in addition it incorporates statistics about the protocol (TCP or UDP) along with packet level detail. Using TCP/IP protocol, in architecture by [7] makes the proposed tool very efficient. Transport layer and application layer of TCP/IP protocol worth many positive aspects to the tool [10]. Transport layer of the TCP/IP protocol is responsible for facilitating connectivity from one end to another end (process to process) across the internet and both TCP and UDP are based on the concept of ports to facilitate connectivity. Tool investigates ports for discovering susceptibilities [10]. In application layer headers and data provides a great deal of information about the nature of attacks.

3. Critical Review

In literature review we have analyzed different tools with their merits and demerits. In the critical review section we depict tabular representation of previous studied tools in literature review section with their complete information as shown in table 1.

This information will provide a brief description about the security tools with a brief summary, identified problems, and proposed solution of identified problem, security services, reliability of tools and weaknesses or limitations of the proposed tools.

Table 1: Summary of Various Discussed Tools in Literature Review

Author(s)	*Name of Proposed Tool*	*Summary*	*Identified Problem(s)*	*Proposed Solutions*	*Data used*	*Implemented*	*Limitations*
G.H.kim& E .H. Spafford 1995	Tripwire	Tool for file integrity checking & intrusion detection.	Leakage attack & denial of service attack	Tripwire; to sense authorized modificatio ns	YES	YES	Attacker(s) can determine which port is been used as tripwire
M.Fisk, S.A.Smith,P.M.Webe r&T.P.Caudell 2003	Immersive Network Monitoring based tool(s	Tool for situational awareness in respect with retrospective analysis	Internal attack(s) &unauthoriz ed attack(s)	Algorithm for Immersive network monitoring	YES	YES	Complex configuration

K.Lakkaraju, W.Yurick& A.J. Lee 2003	NVisionIP	Tool for Graph representation of class B IP network	Compromise system attack, misuse attack port base attack(s) & denial of service attack	Anomaly pattern deduction & sudden notification	YES	YES	Intrusion detection system dependency & log files can be modified
J.Mcpherson, K-liu.Ma, P.Krystosk, T.Bartoletti&M.Christensen 2004	PortVis	Tool for summarizing the information activity on each TCP port	Port base attack(s) or worm attack , distributive denial of service attack & TTL waking attack	Image of traffic and important features (port number, time, protocol etc.)	YES	YES	Complex configuration and less user friendly
N. Patwari, Alfred O &A.Pacholski 2005	Manifold learning based	Tool for visualization of anomalous traffic in Abilene (internet 2 backbone)	Denial of service attack & slammer worm attack	Deployment of sensors for statistics and dimension	YES	YES	Platform dependency & very complex in maintains
J-P.Van, Riel & Barry Irwin 2006	InetVis	Tool for animated 3-D scatter plot visualization of network	Port based attack(s) & future or undefined attack(s)	Visualization of network with destination address, destination IP, source IP and port number etc.	YES	YES	Less user friendly
Daniel A. Keim, F.Mansmann, J.Schneidewind&T.Schreck 2006	Radial traffic analyzer	Scalable visualization toolkit for packet level analysis	Future or undefined attack(s), out ring attack, denial of service attack & worms or viruses	Architecture based on TCP/IP model	YES	YES	------

4. Conclusion and Future Work

Security is the basic need of every standalone system to a group of computer systems across the network. It is negotiated above different tools using different techniques with some merits and demerits according to the nature of the practice. Tools for security of the networks are developing rapidly by doing certain amendment in present tools as they become the need of network.

Future work will be mainly focused on port based authentication of suspicious traffic as we have studied that ports are the very basic source for intruders to target the machine, so the future work will be focusing on special consideration on ports and port based attacks by analyzing previous tools. A tool would be proposed for standalone machine with user friendly controls of ports as the present tools are very complex to understand and configure by non-technical user. Current tools provide security for known attacks in a dedicated network environment; future work will be contributed to standalone machines for further

betterment and achievements.

References

[1] G. H. Kim and E. H. Spafford, "The Design and Implementation of Tripwire: A File System Integrity Checker", Technical Report CSD–TR–93–071, In ACM 47907–1398, page1-18, February 23, 1995.

[2] M Fisk, S. A. Smithy, P. M. Webery, S. Kothapallyz and T. P. Caudell, "Immersive Network Monitoring",PAM2003 – Passive and Active Measurement, NLANR/MNA (National Laboratory for Applied Network Research / Measurement and Network Analysis Group). page 1-10, 2003.

[3] K. Lakkaraju, W. Yurcik, A. J. Lee, "NVisionIP: NetFlow Visualizations of System State for Security Situational Awareness", CCS Workshop on Visualization and Data Mining for Computer Security (VizSEC/DMSEC), October 29, 2004.

[4] J McPherson, K.Ma, PKrystosk, T Bartoletti, M Christensen,"PortVis: A Tool for Port Based Detection of Security Events", ACM Workshop on Visualization and Data Mining for Computer Security, page 73-81, October 29, 2004.

[5] NPatwari, Alfred O, A.Pacholski, "Manifold Learning Visualization of Network Traffic Data", In SIGCOMMMineNet, page 191–196, Aug. 2005.

[6] J. Pierre and B. Irwin, " InetVis, a Visual Tool for Network Telescope Traffic Analysis", Afrigaph '06: Proceedings of the 4th international conference on Computer graphics, virtual reality, visualization and interaction in Africa, ACM press, page 85-89, 25–27 January 2006.

[7] D. A. Keim, F.Mansmann, J.Schneidewind and T.Schreck, "Monitoring Network Traffic with Radial Traffic Analyzer", IEEE Symposium on Visual Analytics Science And Technology, page 123-127,October 31 - November 2 2006.

[8] C.Muelder, Kwan-Liu M and T.Bartoletti, "Interactive Visualization for Network and Port Scan Detection", Proceedings of RAID, September, 2005.

[9] D. Moore, Geoffrey M and S. Savage, "Inferring Internet Denial-of-Service Activity" , In Proceedings of the USENIX Security Symposium, Aug. 2001.

[10] G. Conti and K. Abdullah, "Passive Visual Fingerprinting of Network Attack Tools", ACM Workshop on Visualization and Data Mining for Computer Security (VizSec/DMSec), October 29, 2004.

[11] Tyrone Grandison and EvimariaTerzi, "Intrusion Detection Technology", IBM Almaden Research Center, page 1-7, September 7, 2007.

Mr. Fasee Ullah is a lecturer in the Department of Computer Sciences, City University of Science & IT. He has teaching as well as research experience, His specialization Areas are: Sensor Networks, Security, WiMAX, MANET and Routing Protocols. Currently he has an official reviewer of IEEE and ICCTD conferences. He has done his MS (IT) from SZABIST – Pakistan.

Mr. Waqas Tariq has worked as a researcher for the first time under the supervision of Mr. Fasee Ullah. Currently he is studying BS (Software Engineering) from City University of Science & IT. His area of interest is Network System Security and Software Engineering.