Network Security Analysis Using Cloud Based Intrusion Detection Systems

Aditya Anil Balapure
Department of Computer Science and Engineering
Jaypee Institute of Information Technology Noida, India.
aditya.anil.balapure@gmail.com

Eshan Aggarwal
Department of Computer Science and Engineering
Jaypee Institute of Information Technology Noida, India.
aggarwaleshan@gmail.com

Alok Aggarwal
Department of Computer Science and Engineering
Jaypee Institute of Information Technology Noida, India.
alok.aggarwal@jiit.ac.in

***Abstract*—With the advancement of Internet technologies there is need to track down and prevent suspicious traffic. The rise in the internetwork and intra-network activities by means of smart-phones and tablets is taking network communication to the next level. The advancements in smart-phones is opening a gateway for the next level vulnerabilities and attacks on the network which now contains a collection of smart-phones, tablets, laptops and personal computers. High percentage of newly generated attacks and intrusion techniques has indeed spurred up the need of a unified defense mechanism which can be deployed as a platform. The focus of this paper is to introduce before the type of these defense mechanisms known as intrusion detection techniques over a cloud platform, to prevent the vulnerabilities and provide resistance from the newly developed attacks and loop holes for smart-phones, tablets and personal computers. Since nowadays smart-phones and tablets have the same system architecture as personal computers and hence is vulnerable to security threats. These intrusion detection systems are intelligently developed systems which monitor both intrusions and misuse of the network. In this paper we would propose a cloud based Intrusion Detection System which provides Unified Threat management system for all types of networking devices.**

***Keywords* – Intrusion Detection System, Snort, iptables, mobile devices.**

I. Introduction

INTRUSION DETECTION SYSTEMS is a robust system in both hardware and software form designed to detect possible malicious activity and inspection of incoming and outgoing traffic. These systems must be capable of accurately differentiating normal and acceptable user behavior and a potentially unsafe or suspected behavior. Basically these systems make use of a database which contains attack signatures. The continuously monitored traffic is monitored under these systems and is matched with the signature database in the back-end. In the case if a match is detected the malicious traffic is dropped and reported. Net goal of the Intrusion Detection System is to collect data about the system, their behavior in order to facilitate recovery in case of a failure and log events and identify the sources and techniques involved in the attack. Snort engine will also be used to monitor the traffic. Snort is capable of examining the TCP packet flow across the network.

Smart-phones and tablets are increasingly changing the scenario how people work. Despite the computational and storage resource limitations in hand held devices the system can perform an in-depth analysis on these devices, since the major vulnerability scan would take place only in the cloud. The latest hand-held devices are mostly based on Android and are able to run applications based on Java. A recent study by OnlineMarketing Trends shows that Android tablets and smart-phones have a market capture of around 50% [9]. This has given rise to new types of attacks and methods of penetration aimed on these mobile devices. In fact a large number of malwares and viruses have been specially developed to exploit vulnerabilities in such devices [8]. As history suggests smart-phones malwares like Geinimi Trojan, 3D Anti-Terrorist, SMS Android Trojan, spread and populate through the Bluetooth and Wireless Fidelity transfer modes. Such threats cause interruption in the network and therefore disrupt services.

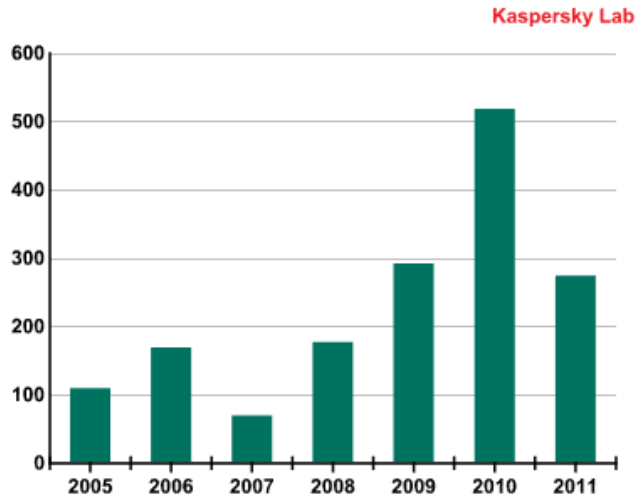
Top security reports and statistics suggest that there has been a 400% increase in Android malware attacks since 2010, a report by Juniper Networks Global Threat Center Research [8]. Not only this, the report also suggests same results for other hand-held devices of Blackberry's Research in Motion and Nokia's Symbian Operating System.

The solutions in the past for such mobile devices encountered several limitations in practice. Many of such methods involve running of Host Based Intrusion Detection System techniques

on these devices [10]. These schemes fail to provide effective protection as they are low on storage, memory and power resources. Also, these systems are based on detecting malware/intrusions by signature matching. Hence it requires a large database storage and protection for newly created threat detection which may not exist in the database. Another segment of these intelligent systems are Network Based Intrusion Detection Systems which removes the above problems in some respects [11]. Also an aspect which needs to be focused on is the automated recovery from these attacks in that case in which there has been a hacking attempt by a hacker.

In this paper we have built upon a cloud based intrusion detection system to provide comfort to this critical issue of security to these mobile hand-held devices. We plan to build a robust system which would give unified intrusion free network communication. We aim to achieve real time secure network transmissions, hassle free usage to the technically unskilled users, light resource utilization for quicker response time. This system will provide behavioral, signature and anomaly based Intrusion Detection and prevention in accordance with National Vulnerability Database.

Fig 1: Vulnerability reports till April, 2011 by Kaspersky Labs.



II. SYSTEM DESIGN

The proposed design aims to remove the need to deploy large resource consuming intrusion detection systems, as such not exhausting the physical resources of the smart hand-held devices and tablets. This system targets a scenario in which the intrusion detection would be deployed over the cloud and would be given as software as a service. We tend to develop plans in which we would customize our software for different clients over static Internet protocol addresses. The basic idea is to deploy various virtual machines with the software for each company/client which would include his whole network in the background. We plan to also implement a mechanism of proxy/reverse proxy for faster Internet browsing and logging. Suppose a company's technical head wants to reduce the security implementation cost and also hardens his security he could happily go for this cloud based system. This would enable this company to have hassle free network communications over various channels such as mobiles, smart-phones, tablets, laptops and other devices. The cloud based Intrusion Detection System would connect to the company's server from where the network communication would take place involving Network Address Translations. This removes the need for a specific hardware based intrusion detection system, reduces power consumption and also reduces the technical management workforce. Also the policy implementation and hardening of the system would be properly discussed with the client company for customized hardening of their intrusion detection systems. This also reduces maintenance downtime.

This proposed framework would provide intrusion detection and response capabilities to the registered users. This system would actually work on a behavioral analysis and the powerful servers keep filtering the traffic for any vulnerability using the National Vulnerability Database (nvd.nist.gov) so far the best vulnerability database internationally. This system would forward the legitimate traffic to the company servers which would be connected to the users of mobile devices and personal computers. This system would also keep a replica(backup) of the machines attached to it and would continuously monitor the changes from the current state of the device to the state stored in the cloud server.

In case if any vulnerability or misbehavior activity is encountered the smart intrusion detection would sense the alert and try to block it. In case if it fails to stop the penetrating malware it would send a real time alert to that particular device. This would result in real time risk management rather than simply logging the traffic for the administrator's review. The user would have an option to switch back to the most recent malware free virtual image (backup) already present on the cloud server. This would handle the problem of zero downtime and hassle free recovery of the infected system.

The Proxy and Reverse Proxy Mechanism would also come into play for better speed and caching of the data and of the device for review, if found mischievous. This setup would also keep the identity of each user system private and only the Internet protocol address of the cloud based intrusion detection

system would be visible.

Fig 2: Proposed system design and modeling of cloud based Intrusion Detection System.

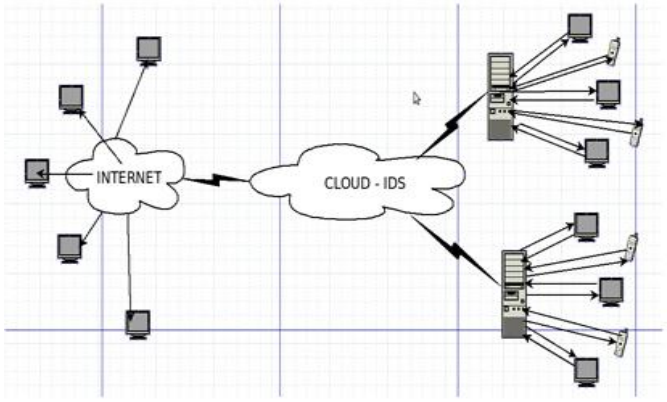


Figure 2 actually demonstrates the actual architecture of the whole system. The actual implementation would need for the user/company to apply for our cloud based Intrusion detection software service and we would create a customized cloud environment for them as per their requirements. Also in addition when the clients/users would connect to the network for the first time using their devices, automatically an add-on of the Java module would be installed on their systems which would enable the cloud based service to keep track and sync with the user attached device in the network. The proxy and the reverse proxy mechanism would also come in play for faster caching of the data. This cloud based implementation of the intrusion detection system would be a very robust, light and secure way to protect multiple device communications, also it would be involving the types of signature based detection, behavioral based detection and real time signature detection. Also this would remove the problem of outdated signatures which is there in some intrusion detection systems.

The mechanism in place for such mixed signature detection would be use of a collection of open source tools and Java based module which would send real time optimized response to the end user.

III. IMPLEMENTATION

We have basically worked out the whole system architecture using the open source Linux system tools and active attack detection Java based module. The working system has been evolved from a three stage development process. The first stage involves packet filtering using Iptables/Ipchains module based on Linux kernel version 2.6.35.14. We have implemented the proper rules customized as per plan for each user of our service as per the needs. The first emphasis has been put on checking the ports which are the first points for attacks. By customizing the iptables rule we can only/block the particular services which a user would want for him. This would be the first steps to curb various attacks aimed at the service.

The second in line of defense for attack detection would be using the Snort engine. The filtered traffic would now pass through the snort attack detection engine to detect various active and passive attacks. With the help of Snort we will be able to analyze and monitor live traffic and TCP packet flow along with anomalies in the network. Hence we would have a second line of defense analysis tool for signature based attack detection. This would take care of attacks such as operating system fingerprinting attempts, common gateway interface, buffer overflows, server message block probes and stealth port scans.

The third in line of defense against the attackers would be our Java based module for active attack detection and blocking. This would be built on platform using Java netfilter libraries for various attack detection techniques such as ICMP flooding, Ping of Death and the vulnerability detection engine from the National Vulnerability Database. Also a small Java based client would deploy on the mobile/tablet platforms for alarm generation in case of vulnerability detection. This would avoid deploying heavy software such as anti-viruses which decrease the processing rate of these hand-held devices.

ATTACK ANALYSIS

CVE#	Program	Language	Attack Type	Attack Description
CVE-2011-2694	Samba	C	Cross site scripting	Script Injection
CVE-2008-1668	Wu-ftpd	C	Format String	Authentication without password
CVE-2005-1953	pico-server	C	Buffer Overflow	Command execution via URL

CAN-2003-0486	PHP for Drupal	PHP	Cross site scripting	Web script injection
CAN-2005-0258	Ajax in PHP	PHP	Command Injection	SQL Injection
CVE-2011-1720	Postfix mail server	UNIX	Denial Of service	Arbitrary Code Execution

I. Table 1 : National Vulnerability Database usage

IV. CONCLUSION

In this paper we have introduced a unified threat management system aimed at delivering high secure networks and system infrastructure. This is 2research based architecture and technique which has been developed keeping in mind the growing era of smart-phones and shift in industrial means of communications and work flow. Our long term emphasis would be on rapid enterprise level deployment and testing of this system for response analysis and effectiveness.

V. REFERENCES

[1] Bhisham Sharma, Karan Bajaj : "Packet Filtering using IP Tables in Linux", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue

[2] Vyas Sekar , Ravishankar Krishnaswamy , Anupam Gupta , Michael K. Reiter : "Network Wide Deployment of Intrusion And Prevention Detection Systems" , ACM CoNEXT 2010, November 30 – December 3 2010, Philadelphia, USA.

[3] Emmanuel Hooper :"An Intelligent Intrusion Detection and Response System Using Network Quarantine Channels: Firewalls and Packet Filters", International Conference on Multimedia and Ubiquitous Engineering, 2007.

[4] Masayoshi Mizutani , Keiji Takeda , Jun Murai : "Behavior Rule based Intrusion Detection", CoNEXT Student Workshop'09, December 1, 2009, Rome, Italy.

[5] 2011. Iptables Concepting : http://linuxcommand.org/man_pages/iptables8.html

[6] Sara Mirzaie, "Preventing of SYN Flood attack with iptables Firewall", 2010 Second International Conference on Communication Software and Networks.

[7] Amir Houmansadr, Saman A. Zonouz, and Robin Berthier : "A Cloud-based Intrusion Detection and Response System for Mobile Phones", IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshop, 2011.

[8] 2011. "Mobile malware development continues to rise, Android leads the way". : www.globalthreatcenter.com/?p=2492

[9] 2011. "Global mobile phone market share" : www.onlinemarketing-trends.com/2011/02/globalmobile-market-share.html

[10] A. Boukerche and M.S.M.A.Notare : "Behavior-based Intrusions Detection in mobile phone system". Jour. Paral. And Dist. Comp., 62(9) : 1476-1490, 2002.

[11] J.Cheng, S.H.Wang, H.Yang and S.La.Smartsiren : "Virus detection and alert for smart-phones". In Mobisys, pages 258-271, New York, NY, USA, 2007.ACM

[12] Bhisham Sharma, Karan Bajaj : "Packet Filtering using IP Tables in Linux". International Journal of Computer Science Issues, Vol. 8, Issue 4, No 2, July 2011.