PROACTIVE NETWORK SECUIRTY TO DETERMINE INTERNET ATTACKS

[1]Munish Sharma, [2]Er.Tajinder Kaur

[1]M.Tech Scholar, [2]Assistant Professor
PTU Regional Center, SBBSIET (India)

ABSTRACT

In this paper we will implement a linux based Design and framework for determining internet attack and to analyze the activity that will be logged by Honey--pot and attack report generation.(pie-chart wise,Port--wise,attack wise et.).

Keywords: Pie Chart , Port Wise, Protocol Type, Snort

I INTRODUCTION

Internet is becoming the most favourable media for communication .Every industry or a company are completely dependable on internet. As it is very efficient to use internet for transferring data.Companies are expending a large amount of capital for securing their Network . As the most vital thing for their company is their data.For Securing our Data and network we are using Antivirus ,Firewall,VPN and IDS Intrusion detection system.These are the four basic pillars for security.[1]

Types of Attacks

- Virus
- Worm
- Trojans
- Spyware
- Adware
- Root kits

Security Systems

Presently we are working with security systems those are reactive in nature. Means they react only when attacker make an attack. After then our security systems start their working. But still they fail .Presently we are having antivirus, firewall, VPN and IDS for securing our networks.

Antivirus

Antivirus is a software and it is basic security tool used at user end.These mostly rely on signature based detection where executable files are matched against a signature base database of known Virus. These are successful for known viruses or signatures if updated regularly ,they are unable to protect users from remote

port attacks directed at user application from internet[1].A latest survey shows that 25% of users disabled their antivirus software because they believe this software have negative impact on their pc performance[13].

Firewal

It is also a good measure to protect our network. It inspects the packets and stop the bad packets from entering our network or we can say that it attempts to block the bad traffic. But the major drawback of firewall is that it is unable to recognize the attack also [1].In these days firewall are available in systems at the time of purchase.

Virtual Private Network (VPN)

It is also count as an important measure to protect our network**.**VPN creates a secure seperate path between insecure systems but VPN fails to protect network resources[1].

Intrusion Detection System (IDS)

Intrusion detection system is totaly a reactive .It does not stop the attacks.It works only after attacks occurred.

Proactive Network Security

Countermeasures like firewall , antivirus or any anti things all are reactive security tools. They works only after being attacked. For protecting our network we have to regular vigilance to our system to get highest level of security. Daily vigilance is the key but is not possible to watch your network all the time[1]. For resolving this major concern we have develop some proactive tools that we should protect our networks our take some necessary action when we got any threat. In this paper we will develop such a system using Honeypot technology to protect our network.

Honeypot

Honeypot is a system that is made to attract the attackers and then to observe their activities .By making such a system we can protect our actual data and the system shown to attacker can be observed and counter measures can be taken without any information to attackers.The importance of honeypot lies in the information collected by it.In this paper we will work honeypot that act as defense mechanism proactively to protect the network. To divert the attention of attacker ,to capture new viruses or worms for future study ,to buid attacker's profile and to identify new vulnerabilities and riskd of operating systems are the main functions of Honepot [1].

Classification of Honeypots

Low interaction Honeypot:I n low interaction honeypot we attacker only get limited access of system. Example nepenthes, honeyd etc

High Interaction Honeypot : In High interaction honeypot we give full freedom to attacker to interact with our system and their every event will be logged**.**example ;argos,HiHat,Honeybow.

II LITRATURE REVIEW OF RELATED WORKANTIVIRUS

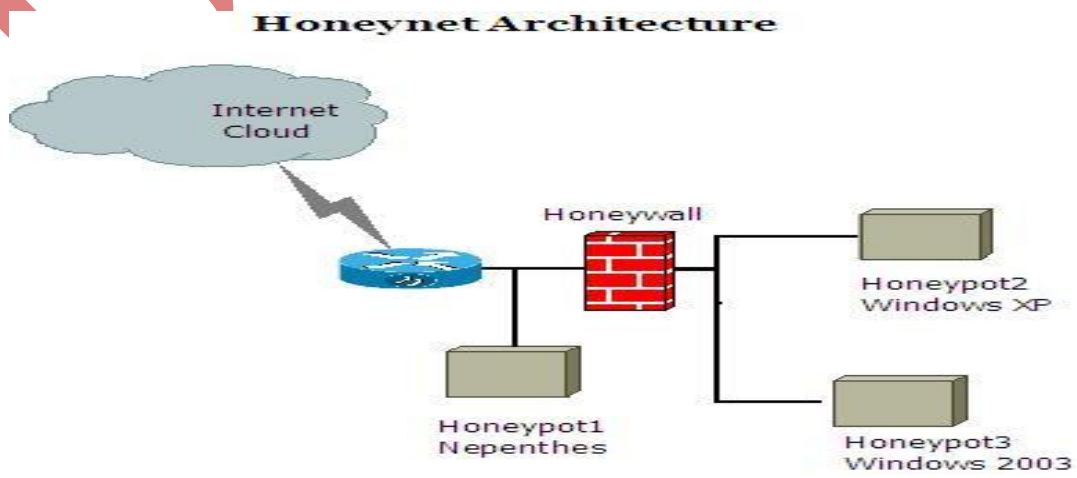
- **Antivirus** proposed a Network Intrusion Testbed using Honeypots .This study aims to create a interface that will make the configuration of Honeypot easier. Use a Honeypot configuration that will be tested over a small network and analyze the activity that will be logged by Honeypot.
- **Kim** et proposed in 2012 a agent based Honeypot framework or protecting a server in organization. He shows in his framework, how agents remove malicious processes.
- **Abhay nath** et in 2011 presented a solution in which he addresses the issue of a huge log size,which consumes a lot of space, which creates a problem when they are processed.
- **Fahim** et in 2009 proposed a method for establishing a virtual Honeynet on Vmware server running Honewall CDROM roo.This special technique was implemented in order to enhance the data capture mechanisms on linux based honeypot to efficiently generate reports.
- **Tupakula** et in 2011 proposed a security architecture to deal with attacks on virtual machines at fine granular level.
- **Kumar** et in 2012 proposed hybrid framework fro malware collection and detection using both of the honey technologies known as client and server Honeypots .
- **Masood mansoori and ray hunt** in 2011 proposed an ISP based notification and detection system to maximize the efficiency of client Honeypots in protection of end users.

III OBJECTIVES

The objective of proposed work is to develop proactive network security framework to determine internet attacks. To fulfill the objective, following steps are implemented.

- To study of Proactive Network security Tools and techniques.
- To design and develop a linux based framework using honeypot technology for determining Internet attacks.
- To analyze the activity that will be logged by honeypot and attack report generation.

IV DESIGN



V METHODOLOGY USED

The Proposed work completes through the following steps

- Platform Creation using virtualization and installation of linux operating system as base operating system.
- Instalation of virtual Box tools to create multiple operating systems on single base machine.
- Installation of unpatched operating system with latest vulnerabilities
- Configuration development to record the activities of invader.
- Network Configuratio and accesibilty on base machine as well as on virtual machine(depends on number of honeypots).
- Ip address setting and assignment
- Network port configurations.
- Applications bind with specific ports.
- Incorporation of Signature based detection techneques with honeypots.
- Network Attack Capuring through Honeypots and storage of attack data.
- Signature based classification through data processing engine
- Statisical Report generation
- Port wise Distribution
- Attack wise Distribution
- Persentage distribution of attacks.
- Pie charts of attacks.
- Bar charts of attacks.etc.
- Distribution of collected attacks based on SNORT(Intrusion Detection System).

VI RESULTS

In the implementation of proactive network security setup , we will collect, analyze and defend our network from unknown network attacks. we have created a vitual honeynet framework using Low intereaction honeypot and high intereaction honeypot.With the help of our framework attack traces can be collected for the further investigations for interfering the attackers report and behavior. We also tried to develop online mechanism using some automated code and scripts to generate some statistics of the attack report which is very useful for system

and network administrators to defend their network or take some proactive actions against attacks.We have generated a Statisical report of attack data as given below**.**

- Firstly report on Distribuiton of attack data.
- Distribution of Classification method.
- Distribution of event by destination port and events by hour.
- Popularity of one source host.
- Distribution by protocols.

Events: These are the types of attacks such as mysql injections,smtp attacks etc.

Methods: Classification methods means class of exploitation like bad traffic,sensitive data stealing etc.

ATTACK DATA STATISTICS (Generated with NIDS alerts)

6.1 Distribution of Attack Methods

%	No	IP Source	Attack	Severity
27.42	17	177.x.x.x	OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc NetrpPathCanonicalize path canonicalization stack overflow attempt {tcp}	high
27.42	17	177.x.x.x	OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc NetrPathCanonicalize overflow attempt {tcp}	high
12.90	8	116.x.x.x	OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc NetrPathCanonicalize overflow attempt {tcp}	high
12.90	8	115.x.x.x	OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc NetrpPathCanonicalize path canonicalization stack overflow attempt {tcp}	high
6.45	4	116..x.x.x	OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc NetrpPathCanonicalize path canonicalization stack overflow attempt {tcp}	high
6.45	4	196.x.x.x	OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc NetrPathCanonicalize overflow attempt {tcp}	high
3.23	2	91.x.x.x	MALWARE-OTHER lovegate attempt {tcp}	high
3.23	2	91..x.x.x	OS-WINDOWS DCERPC NCACN-IP-TCP ISystemActivator RemoteCreateInstance attempt {tcp}	low

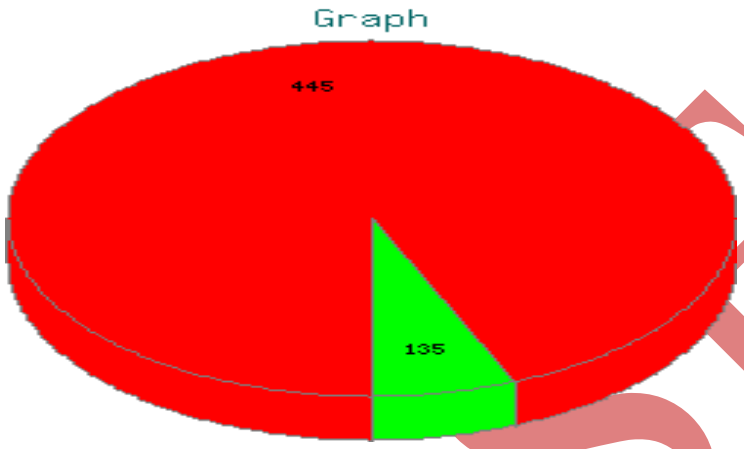
6.2 Distribution of Classification Method

%	No	Classification	Severity
93.55	58	Attempted Administrator Privilege Gain	high
3.23	2	A Network Trojan was Detected	high
3.23	2	Generic Protocol Command Decode	low

6.3 Distribution of Event by Destination Port

%	No	Destination Port
93.55	58	445
6.45	4	135

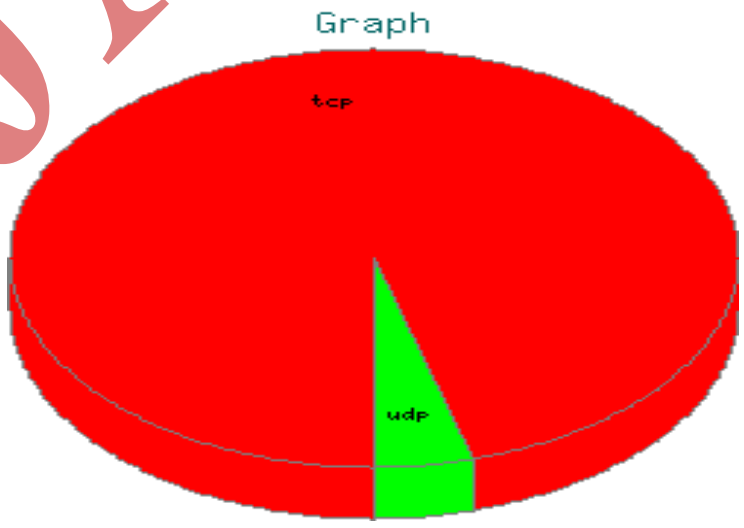
In this graph we shown the events by destination port.In this graph port no. 445 is sending 93.55% of attacks and port no. 135 is sending 6.45 % of events.



6.4 Distrubution by Protocol Type.

%	No	Protocols
95.52	64	tcp
4.48	3	udp

This graph shows that which protocol the attacker is using mostly to spread virus.As shown in graph 95.52% of attacks are through TCP protocol and small amount of attacks 4.48 % through UDP protocol.This type of distribution is called Protocol type distribution.



6.5 Popularity of One Source Host

%	No	IP Source	Resolve	Domain
23.88	16	23.xxx.xxx.xx	unresolved	Unresolved
17.91	12	123.xx.xx.xxx	unresolved	Unresolved
14.93	10	22x.xxx.xx.xx	unresolved	Unresolved
13.43	9	2xx.xx.xx.xx	unresolved	Unresolved
7.46	5	1xx.xxx.xx.x	unresolved	Unresolved
5.97	4	7x.xx.xxx.xx	unresolved	Unresolved

VII FUTURE SCOPE

Apart from the development of honeynet in virtual enviorment ,the single window web interface is missing in our current development.We propose to develop the GUI gor attack data categorization and summarization of attacks for the end users. We also propose to integrate the active components to browse actively the malicious web pages and to collect client side attacks which exploits the client side applications.Apart from GUI development for single window operation and configuration management of virtual honeynet ,we also propose to distributed deployment of honeynet sensors,collect the distributed attack data ,correlate the data and determine the coordinated attacks in variousl locations.To determine the coordinated attacks ,we also trying to implement the machine learning algorithms into honeynet data to infer the intelligent information.

REFERENCES

[1] Study on Network Intrusion Detection Based on Proactive mechanism by Munish sharma & ER.Tajider Kaur in 2014..

[2] R. Danford, ―2nd Generation Honeyclients‖ , SANS InternetStorm Center,2006 http://handlers.dshield.org/rdanford/pub/Honeyclients_Danford_SANS 06.pdf

[3] Cheswick, B. (1990), An Evening with Berferd in which a cracker is Lured, Endured, and Studied: Citeseer.

[4] Ramaswamy, C. and R. Sandhu. (1998), Role-based access control features in commercial database management systems: Citeseer.

[5] Skoudis, E., and Zeltser, L., "Malware: Fighting Malicious Code", Prentice Hall,2003, Page 3, ISBN = 978-0131014053.

[6] [Provos, N., McNamee, D., Mavrommatis, D. W., K and Modadugu, N., the Ghost In The Browser Analysis of Web-based Malware. 2007. [Online]. Available at:http://www.usenix.org/events/hotbots07/tech/full_papers/provos/provos.pdf [Accessed 11 Feb 2009]

[7] Secure Browsing | Malware Protection | Secunia. (2010), "Secunia Yearly Report - 2010". Available from:secunia.com/gfx/pdf/Secunia_Yearly_Report_2010.pdf.

[8] Secunia. (2010), "Research Reports, Factsheet by Browser - 2010". [Cited 2011 5 - January]; Available from: http://secunia.com/resources/factsheets/2010_browsers/.

[9] VirtualBox. (2004). Sun VirtualBox® User Manual. Available:http://www.virtualbox.org/manual/UserManual.htmlLast accessed 20 July 2008.

[10] Sanjeev Kumar, at al, Hybrid Honeypot Framework for Malware Collection and Analysis, ICIIS-2012, IIT Chennai

[11] www.honeyclient.org

[12] en.wikipedia.org/wiki/Client_honeypot

[13] www.honeynet.org

[14] Trustwavehttps://www.trustwave.com/securebrowsing/

[15] Detection and Analysis of Drive-by-Download Attacks and Malicious JavaScript Code www.cs.ucsb.edu/~vigna/.../2010_cova_kruegel_vigna_Wepawet.pdf

[16] Prophiler: A Fast Filter for the Large-Scale Detection of Malicious Web Pages www.cs.ucsb.edu/.../2011_canali_cova_kruegel_vigna_Prophiler.pdf

[17] Xiaoyan Sun, Yang Wang, JieRen, Yuefei Zhu and Shengli Liu, “Collecting Internet Malware Based on Client-side Honeypot”, 9th IEEE International Conference for Young Computer Scientists (ICVCS 2008), pp. 1493 – 1498, 2008.

[18] Secunia. (2010), "Factsheets by Windows Operating System - 2010". 20 - March - 2011]; Availablefrom: http://secunia.com/resources/factsheets/2010_win_os/.

[19] PcPitstop. (2010), "The State of PC Security". 20 - December 2010]; Available from:http://techtalk.pcpitstop.com/2010/05/13/the-state-of-pc-security/.

[20] YaserAlosefer, Analysing Web-based Malware Behaviour through Client HoneypotsCardiff University School of Computer Science & Informatics, Feb-2012