IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Volume 12, PP 41-44

Survey on Security Using Honeypot

Ashka Ashani[1], Deesha Nirmal [2], Viral Doshi[3], Nikita Patil[4]

[1]*Student, Department Of Computer Engineering, Atharva College Of Engineering, Mumbai, India*
[2]*Student, Department Of Computer Engineering, Atharva College Of Engineering, Mumbai, India*
[3]*Student, Department Of Computer Engineering, Atharva College Of Engineering, Mumbai, India*
[4]*Assistant Professor, Department Of Computer Engineering, Atharva College Of Engineering, Mumbai, India*

Abstract : *With The Recent Advancements In Cyber Attack And Ready Available Internet Connection Security Has Become More And More Of An Issue. Here, Honeypots Can Be Used To Ensure Security. Honeypot Uses Deception To Trap The Attacker And Also Logs Details About The Attacker. The Purpose Of The Paper Is To Give An In Depth Idea About What Honeypot Is And How It Can Be Deployed On A Network For Protecting From Malicious Usage Of Any Sensitive Data. It Also Focuses On The Various Attacks That Can Occur On The System.*

Keywords – *Honeypot, Honeynet, Intrusion Detection System.*

I. INTRODUCTION

Advances In Technology And Human Dependency On Them Are Rapidly Increasing Gradually. Apart From This, The Number Of Devices Connected To A Network Is Also On Its Peak. With These Ever Changing Technologies, Threats Are Also Increasing Day By Day. Therefore For Any Network Administrator It Becomes At Most Necessary To Protect The Systems And System Data On A Network From Any Attackers.

There Are Possibilities Of Many Loopholes In A Network. A Hacker Tries To Detect These Vulnerabilities In The Network And Then Attack It In Order To Get The Access Of Important And Confidential Information Stored On The Network. The Hacker Can Also Manipulate The Sensitive Information Or Can Delete The Important Records. Hackers Can Attack Using Various Types Of Attacks Such As Denial Of Service Attack, Brute Force Attack, Phishing Attack, IP Spoofing And Many More. These Potential Attacks Can Manipulate The System Data Or Use It For Malicious Activities.

There Are Various Technologies Developed For Preventing The Systems From These Attacks. One Of Such Technology Is The Intrusion Detection System. The Intrusion Detection System Runs In The Background And Monitors The System And Detects Any Malicious Activities On It. Intrusion Detection System Can Be Classified Into Two Types One Which Just Notifies Or Alerts The Network Administrator About Any Intrusion Detected And The Other Type Lets The Network Administrator To Take Action Against The Intruder. [1]However It Does Not Obtain Information About The Attackers. Another Drawback Of The Intrusion Detection System Is That In Case Of Heavy Traffic On The Network, It Is Difficult To Determine Which Packets Are Deviated. Intrusion Detection System Is Mainly Suitable For Small Scale Network Where Preventing Data Breach Is Secondary Purpose.

Honeypot Is A System Which Is Deployed On A Network In Order To Detect Malicious Activities And Protect The System From Various Attacks. Honeypot Detects Malicious Activities And Tries To Deceive The Attacker. The Attacker Thinks That The System Which Is Being Attacked Is A Real System Whereas It Is A Trap Created By The Honeypot. [2]In This Process The Honeypot Tries To Obtain The Information About The Attacker And Also Prevent The Network From The Attacks. In Other Terms, Honeypot Is Basically A Decoy Or A Trap.

This Paper Gives An Overview Of Honeypot And Its Application In Real Time Systems. The Objective Of This Paper Is To Represent The Various Trends And Opportunities For Honeypot Researchers.

II. BASIC THEORY

A Honeypot Is A Machine Or A System That Is Usually Designed With The Aim Of Detecting And Trapping Any Attempt To Penetrate Into An Experimental System. [3]It Acts As Masquerade To The Attacker. If The Attacker Breaks Into The System Or Server, Then The Honeypot Which Resembles The Original Server Will Be Assaulted By The Attack, While The Actual System Remains Safe And Untouched As A Server Behind The Honeypot. [4]For Those Who Are Not Experienced Attackers, They Tend To Think That They Have Easily Managed To Hack The System / Server. However, All Actions, Tools, And Techniques Used In The Attack Have Been Recorded For Study By The System Administrator Concerned Through The Data And Information Presented By The Honeypot.

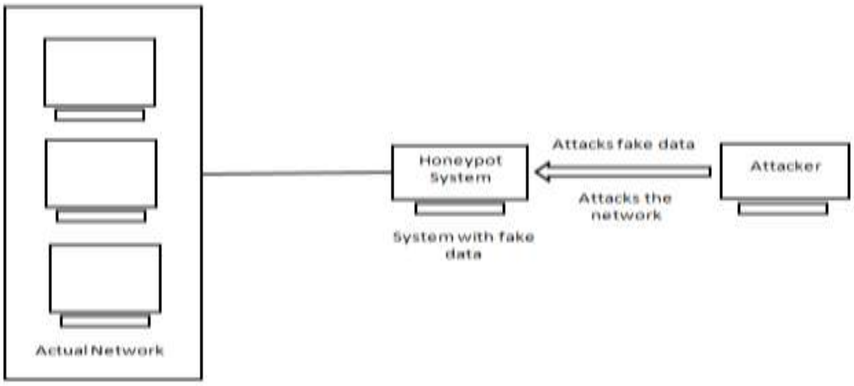

Fig 1.1 Basic Working Of Honeypot System

Fig 1.1 Shows Basic Working Of Honeypot System. [5]Any Malicious User Will Be Redirected To A Fake Server So That The Actual Network Remains Unaffected. Simillary, Legitimate Users Of The Network Will Be Able To Access Network Services As They Won't Be Redirected To Honeypot Trap.

[6]According To Their Use And Their Involvement, Honeypots Can Be Classified As Production And Research Honeypots.

Production Honeypot -

Production Honeypots Are Primary Honeypots Which Can Detect The Attacks And Provide A Warning To The Attackers. These Type Of Honeypots Are Easy To Deploy And Provide Least Information About The Attacks And Attackers.

Research Honeypot -

Research Honeypots Are High Level Honeypot Which Are Used By Researchers Or Professionals. These Honeypots Are Capable Of Logging Information About The Intruder As Well As The Techniques Used By The Intruder. These Honeypot Gather As Much Information As Possible. They Provide Information Which Can Be Used For Statistical Study Or Investigation.

Level Of Interaction

Honeypot Can Be Implemented In Three Different Levels Depending Upon Its Interaction And Way Of Handling Network Security.

1. Low Level Interaction:

Honeypot Designed To Operate At Low Level Interaction Is The Most Simplest Honeypot. A Low Level Interaction Honeypot Just Tries To Record Or Log Information About The Attacker. But The Drawback Here Is, The Attacker Can Easily Recognize A Honeypot At This Level.

2. Medium Level Interaction:

As Compared To Low Level Honeypot, A Medium Level Honeypot Cannot Be Recognized Easily. Medium Level Honeypot Are More Complex Than Low Level Interaction Honeypot But Long-Delayed.

3. High Level Interaction:

High Level Interaction Are Complex To Set Up As They Involve Real Time Operating System. Honeypot At This Level Misguides The Hacker To A Fake System.

Honeynet

[7] In A Network, If There Are Too Many Honeypots Deployed Then It Is Known As A Honeynet. Typically, A Honeynet Is Used For Monitoring And/Or More Diverse Network In Which One Honeypot May Not Be Sufficient. The Purpose Of Honeynet Is To Better Understand The Hacker's Behavior And Methodologies. They Allow Hacker To Be Easily Identified.

III. Proposed System

The Purpose Of The Proposed System Is To Design A Honeypot On A Network And Check The Efficiency By Attacking The Same.

Following Are The Steps For Extraction Procedure Of Honeypot.

1. Identify Any Attack On The System And To Log Source And Target Information.
2. Redirecting The Intruder To The Honeypot.
3. Extracting The Attacker's Information.
4. Ban Attacker From The Network.
5. Generating Records And Statistical Data.

IV. Expected Results

The System Will Monitor The Network And Prevent It From Malicious Activities And Attacks. Honeypot Will Be Deployed On The Network Which Will Check Whether The Person Entering The Network Is A Legitimate User Or An Attacker. If The User Is Legitimate, He Will Be Given Access To The Actual System Else He Will Be Redirected To A Fake Server. Meanwhile, Honeypot Server Will Try To Obtain The Methodologies Used By The Attacker As Well As The Attacker's Information.

V. Conclusion

As Our Dependence On Computers And Network Constantly Increases, Comprehensive Network Security Is Of Tremendous Importance. A First Requirement To Be Able To Better Protect Networks Assets Is To Gain A Detailed Understanding Of Malicious Threats. There Are Innumerable Options Available Today To Access Any Sensitive Information Maliciously. Therefore, To Counter Such Attacks The Concept Of Honeypot Has Been Precisely Invented To Fill This Task. This System Gave Us An Opportunity To Study Honeypot And IDS System In Detail. It Is Important For Organizations To Secure Their Digital Assets By Detecting And Preventing Vulnerabilities Before They Are Exploited. Honeypot System Generates Less Number Of Alarms Than IDS. Hence It Can Be Concluded That Combination Of Honeypot And Intrusion Detection System Can Be Suitably Used As Most Efficient System To Ensure System Security.

Acknowledgement

We Gratefully Acknowledge The Assistance Provided To Us By The Following Authorities In The Completion Of Our Project Titled "SECURITY USING HONEYPOT." We Take This Opportunity To Express Our Profound Gratitude And Deep Regards To Our Guide Prof. Nikita Patil Having An Immensely Busy Work Schedule, We Never Found Any Of Our Request Of Help And Guidance To Her Being Turned Down. We Are Sincerely Grateful To Her For His Exemplary Guidance, Monitoring And Constant Encouragement Throughout The Course Of This Project. We Would Like To Take The Opportunity To Thank The Head Of Department Of Computer Engineering, Prof. Mahindra Patil For Permitting Us To Pursue This Project. A Number Of People Contributed Their Time And Efforts In Making This Project A Success. We Would Like To Thank Everyone Who Contributed Their Effort And Sharing Time For Our Work And Encouraging Us To Continue. In Particular, We Are Greatly Indebted To Our Guide For His Valuable Suggestion And Moral Support Without Which This Project Would Not Have Been Possible. Last But Not The Least, We Are Thankful To Our Friends Who Inspired And Encouraged Us Throughout.

References

[1] Hibatul Wafi, Andrew Fiade, Nashrul Hakiem, Rizal Broer Bahaweres, "Implementation Of A Modern Security Systems Honeypot Honey Network On Wireless Networks", 20 17 International Young Engineers Forum (YEF··ECE) Caparicil, Porlugal, May 5 , 2017 IEEE

[2] Janardhan Reddy Kondra, Santosh Kumar Bharti, Sambit Kumar Mishra, "Honeypot-Based Intrusion Detection System: A Performance Analysis", Computing For Sustainable Global Development (Indiacom), 2016 3rd International Conference On 16-18 March 2016 **INSPEC :** 16426743

[3] Ronald M. Campbell, Keshnee Padayachee,Themba Masombuka, "A Survey Of Honeypot Research: Trends And Opportunities", The 10th International Conference For Internet Technology And Secured Transactions (ICITST-2015), 978-1-908320-52/0/$31.00 ©2015 IEEE

[4] Akshay A. Somwanshi, Prof. S.A. Joshi, "Implementation Of Honeypots For Server Security", International Research Journal Of Engineering And Technology (IRJET) E-ISSN: 2395 -0056 Volume: 03 Issue: 03 | Mar-2016, P-ISSN: 2395-0072

[5] Jiqiang Zhai, Keqi Wang, Research On Applications Of Honeypot In Campus Network Security, Measurement, Information And Control (MIC), 2012 International Conference On 18-20 May 2012, 10.1109/MIC.2012.6273260, **INSPEC:** 13064684

[6] Yogendra Kumar Jain, Surbhi Singh, "Honeypot Based Secure Network System", International Journal On Computer Science And Engineering (IJCSE) ISSN : 0975-3397 Vol. 3 No. 2 Feb 2011 612

[7] Anas Abd Almonim Nour Albashir, "Detecting Unknown Vulnerabilities Using Honeynet", Anti-Cybercrime (ICACC), 2015 First International Conference On 10-12 Nov 2015, 10.1109/Anti-Cybercrime 2015.7351929

[8] Irwan Sembiring, Satya Wacana, "Implementation Of Honeypot To Detect And Prevent Distributed Denial Of Service Attack"; Proc. Of 2016 3rd Int. Conf. On Information Tech., Computer, And Electrical Engineering (ICITACEE), Oct 19-21st, 2016, Semarang, Indonesia

[9] Https://Www.Networkworld.Com/Article/3234692/Lan-Wan/Increase-Your-Network-Security- Deploy-A-Honeypot.Html, Last Accessed 21/01/18, 08:34 Pm

[10] Https://Ethics.Csc.Ncsu.Edu/Abuse/Hacking/Honeypots/Study.Php, Last Accessed 27/01/18, 04:40 Pm

[11] Http://Searchsecurity.Techtarget.Com/Definition/Honeynet, Last Accessed 28/01/18, 02:40 Pm