International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

Intrusion Detection in Network using Honeypot Technology

[1] Mrs. B. Sathyabama, [2]Dr. V. Kavitha, [3]Mrs. S. Subhasini,, [4]J. Sudharson
[1] Assistant Professor, [2] Professor, [3]Assistant professor, [4]PG Studnet
[1, 2, 4]Department of MCA, [3]Department of BCA, Hindusthan College of arts and science,

***Abstract:** The network security is the issue which rose due to self-configuring and decentralized nature of the network. The malicious nodes may join the network due to which various type of active and passive attacks are possible in the network. The passive type of attack is the type of attack in which malicious nodes do not affect the network performance. The active type of attacks is the attacks in which malicious nodes reduce networks performance in terms of various parameters. The black hole, wormhole, sinkhole, Sybil etc are the various type of active attacks which reduce network. In recent times, various techniques have been proposed which detect malicious nodes from the network. To improve the security of the network, techniques of the data encryption, intrusion detection systems are proposed in recent times. This paper mainly aims to detect the bad traffic and attackers by deploying Honetpot Technology to improve the network security of the enterprise. This paper shows that how Honeypot works in real-time environment and how it responds when any unwanted activity occurs in the network.*
***Keywords:** Network attackers, False positives, Bad traffic, Illicit activity, Intrusion-detection.*

I. INTRODUCTION

Today, Honeypots are still in their infancy, developed and used primarily by researchers and security enthusiasts. A handful of commercial products are available, and organizations are beginning to deploy open-source honeypots and their more robust iterations, such as Honeyd. But honeypots are not widely deployed. Honeypot technology is moving ahead rapidly, and, in a year or two, honeypots will be hard to ignore. New developments will advance the lab technology with the catchy name to a full-fledged, enterprise-level security tool.

II. DETECTION WIZARDRY

Honeypot will look only for “bad” traffic. And looks for convergence with existing technology to help transform the intrusion detection crapshoot into a good bet. Honeypots can fill the growing gaps left by conventional IDSes, which suffer from false positives and a lack of alert intelligence. That's not to say honeypots will replace IDSes. Each technology has its strengths and limitations. In this scenario, both technologies will log to a central database, correlating information. The honeypot will reduce false positives by identifying attacks for which the IDS doesn't have signatures.

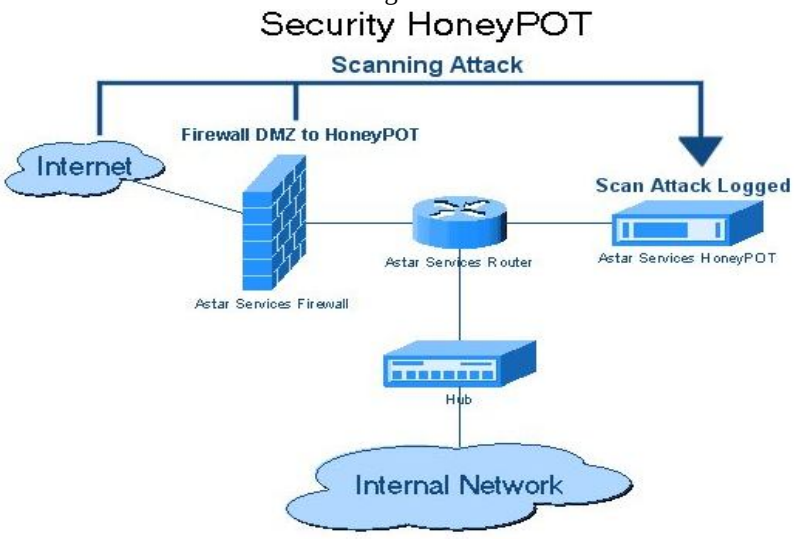

Fig 2.1: HoneyPOT

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

On the other hand, IDS sensors address the fact that honeypots can't monitor all network activity. Symantec's honeypot, Decoy Server, works with the company's IDS solution, ManHunt. Attackers then interact with these real operating systems and applications. This information is fed into a central system, where it's combined with data from ManHunt.

III. IDSES Vs HONEYPOTS

A. IDSes and honeypots differ fundamentally in the way they attempt to detect malicious traffic. IDSes have the advantage of monitoring all traffic, flagging threats through a combination of known attack signatures and statistical anomalies. The flip side of this is the sheer volume of information IDSes produce--gigabytes of data. Some large organizations may have to deal with more than 100,000 alerts a day, many of them false alarms.

B. Hackers can slip through network defenses by using encryption or IPv6 tunneling. IDSes are useless against this kind of traffic. But it's a different story if hackers connect to a honeypot using, say, SSH, IPv6 or the encoded (and not yet commonly used) Network Voice Protocol. First of all they're up to no good, because nice people don't connect to honeypots. Once inside, every actionwill be captured, including toolkits, keystrokes and communications. As more and more legitimate traffic is encrypted and uses IPv6 tunneling, organizations will begin to turn to honeypots to complement their IDSes.

C. Honeypots are less comprehensive, but more discerning. Honeypots only report the connections they receive--and most of these will be real attacks. This means that, the organization has far less, but more precise information to analyze, allowing to more quickly identify and respond to attacks.

D. Honeypots detect and capture new attacks or methods. That means regardless of the tactics used, honeypots will most likely detect and capture the activity. Examples of these attacks discovered by honeypots include the Solaris and Samba exploits.

IV. HOW HONEYD DETECTS AN ATTACKERS

Honeypot deployment can be complex and time-consuming. Because each Honeyd addresses only the relative handful of connections it receives. One solution being developed is the open-source Honeyd (Fig 1), which monitors unused IP space, instead of a single IP address. Any traffic or connection attempt made to an unassigned IP address is most likely unauthorized or illicit activity. This exponentially increases a Honeyd ability to detect unauthorized activity.

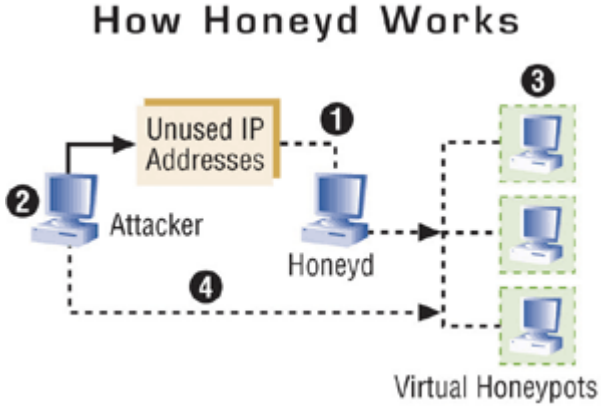

Fig4.1: Process of Honeyd

When someone attempts to communicate with an unused IP, Honeyd , which is installed on a single computer, creates a virtual Honeyd that interacts with the attacker. It also has the capability to detect activity on any TCP/UDP port, even if the connection is encrypted or uses IPv6 to tunnel traffic.

V. HONEYPOT FARMS

A honeypot here, a honeypot there,not exactly scalable security. But in the near future, clustering will enable organizations to easily and quickly deploy honeypot technology globally. While developments such as Honeypot address, the scalability issue to some extent, honeypot farms promise to be a breakthrough technology. Instead of deplying honeypot on organization’s networks, a hardware device which monitors unused IP addresses can be deployed. Similar to Honeyd, it redirects all attacker traffic to a single cluster of honeypots (Fig 2).

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

Honeypot farms will simplify administration by locating all honeypots in one location, where they can be monitored. For example, a major auto manufacturer wants to deploy honeypots on all of its networks around the world. That's a logistical nightmare. But with farms, all the honeypots are physically located at the company's headquarters and maintained by security specialists. Admins will simply deploy devices on the local networks to redirect unauthorized traffic to the farm. So, instead of bringing the honeypot to the attacker, attackers in the future will be directed to the honeypot.

NetBait provides a service where it will deploy redirectors on internal network. Attackers are then redirected to NetBait's honeypot farm, where their every action is detected and recorded. Or, if an organization prefers, it can maintain its own honeypot farm, using the NetBait solution to redirect attackers.

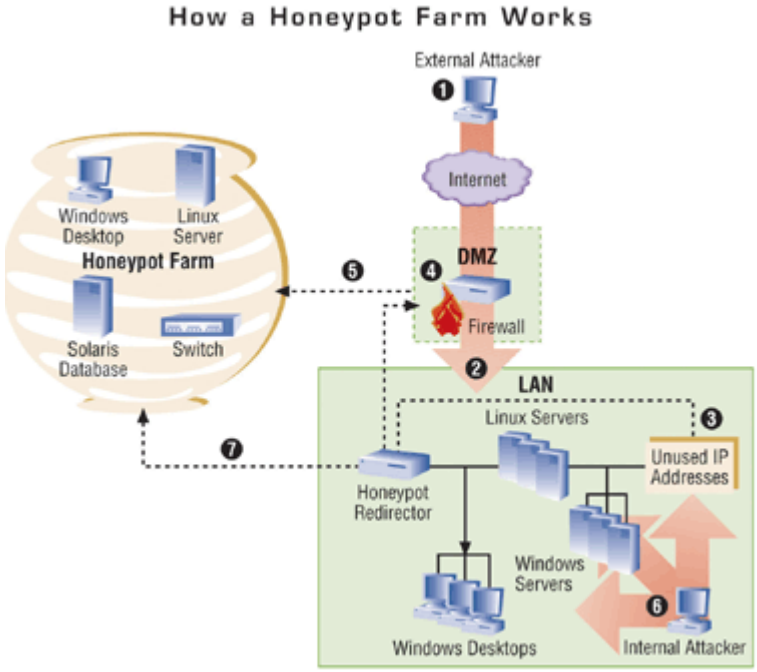

Fig5.1: Process of Honeypot

When the attacker probes a monitored IP address, the appliance will simply redirect the connection to the honeypot farm. There's no routing, hence no time to live (TTL) decrement of the IP packet, and no proxying. At the most, there may be some latency, which would be difficult to detect.

These farms could be highly sophisticated. Instead of deploying software (such as Honeyd) that emulates computers and services, the honeypots could be real computers running real applications. For example, Honeyd's virtual computer will emulate a service, such as FTP or HTTP. An attacker may be able to figure out which services are emulated--it's very difficult to provide the full functionality of an FTP server without an actual server. The real computers in a honeypot farm will be far more difficult for an attacker to figure out.

Further, security personnel can learn a lot more if they give the bad guys real OSes and apps to play with. For example, instead of just detecting an employee scanning internal networks for file shares, a honeypot on a farm could identify the person doing the scanning, what files they are looking for and perhaps even what they intend to do with those files. The honeypot farms could be highly customized based on the type of threats you're concerned about.

VI. DYNAMIC CONFIGURATION

In the near future, honeypots will be able to "learn" about networks and configure themselves, making them a lot easier to deploy in large numbers. Honeypot technology, like most security technologies, can be time consuming to install and configure.

This will be a quantum leap from the early honeypot implementations, such as Honeyd or Deception Toolkit, which are distributed in source code and have to be compiled and manually installed and configured. Point-and-click GUIs in Windows-based honeypots, such as NetSec's Specter and KeyFocus' KFSensor are making the job easier, but getting honeypots up and running is a lot of work.

It is to be configured, for example, which IP addresses to be monitored, what operating systems to be emulated and which services to be detected by honeypot. Future honeypots will dynamically make these decisions for the enterprise.

Imagine that, a honeypot appliance is simply deployed on the network of the enterprise. The power plug and network cable(or wireless card) are to be connected and then the honeypot do the rest. Using techniques such as passive fingerprinting, the honeypot appliance will monitor all the traffic on the network, learning what IP addresses are active--and which are unused--what systems are bound to those IP addresses, what services are being used, and by whom. The honeypot could determine not only the operating system of each computer on the network, but potentially the patch level and applications on each system like Apache Web server1.28 on a Linux 2.4.18 kernel, or, perhaps, Windows XP Pro running IIS 6.0.

Once the appliance identifies the makeup of the network, it would dynamically configure virtual honeypots across the unused IP space. These honeypots would mirror the makeup of the network, blending into an environment, whether a Microsoft shop with Win2K systems or running nothing but Solaris. It could even emulate devices such as routers, switches or wireless access points.

VII. WORKING TOGETHER

Each of these technologies will advance the state of the art on its own. When they are together to work, honeypots will really hit the working process.Imagine the honeypot farm, with an appliance redirecting scans of unused IP addresses. Now dynamic configuration can be added. But instead of configuring virtual honeypots, now configure real honeypots in the farm, mirroring the network environment.

The redirectors would have the intelligence to know what honeypots to direct the attackers to. For example, if the organization is made up mainly of Windows-based computers, the redirectors can detect and direct attackers to Windows-based honeypots. If the environment changes (perhaps with Linux servers deployed internally), the redirectors can dynamically identify these changes. The data collected by these dynamically configured honeypot farms can be leveraged to enhance other security technologies. For example, honeypot logs can be correlated with other system logs, IDS alerts and firewall logs. This will produce a far more comprehensive picture of the activity within an organization, and dramatically reduce the number of false positives.

VIII. CONCLUSION

Attacks on websites and databases are increasing day-by-day rapidly. Because the network attackers are gradually grown in these present days. No one is fail-safe for the security of their enterprise's data. But the technology world keeps on producing the solutions for every issue. There must be some system to detect those attacks on the databases. The enterprise can avoid the network attacking, traffics and hackings by using these technologies like Honeypots. To use honeypot for these systems special care should be given like after applying honeypot the system must look realistic and is capable for generate logs for all suspicious entries. Honeypot is a useful tool for entice and trapping attackers, capturing information. Security is the essential element of any organization web sites, but though the security provided by the honeypots based on hardware setups are very expensive for small and medium scaled organization.

REFERENCES

[1] Cole, Eric; Northcutt, Stephen. "Honeypots: A Security Manager's Guide to Honeypots".
[2] Lance Spitzner (2002). Honeypots tracking hackers. Addison-Wesley. pp. 68–70. ISBN 0-321-10895-7.
[3] Katakoglu, Onur (2017-04-03). "Attacks Landscape in the Dark Side of the Web" (PDF). acm.org. Retrieved 2017-08-09.
[4] "Deception related technology – its not just a "nice to have", its a new strategy of defense – Lawrence Pingree". 28 September 2016.
[5] Litke, Pat. "Cryptocurrency-Stealing Malware Landscape". Secureworks.com. SecureWorks. Retrieved 9 March 2016.
[6] "Bitcoin Vigil: Detecting Malware Through Bitcoin". cryptocoins news. May 5, 2014.
[7] Edwards, M. "Antispam Honeypots Give Spammers Headaches". Windows IT Pro. Retrieved 11 March 2015.
[8] "Sophos reveals latest spam relaying countries". Help Net Security. Help Net Security. 24 July 2006. Retrieved 14 June 2013.
[9] "Honeypot Software, Honeypot Products, Deception Software". Intrusion Detection, Honeypots and Incident Handling Resources. Honeypots.net. 2013. Retrieved 14 June2013.
[10] dustintrammell (27 February 2013). "spamhole – The Fake Open SMTP Relay Beta". SourceForge. Dice Holdings, Inc. Retrieved 14 June 2013.
[11] Ec-Council (5 July 2009). Certified Ethical Hacker: Securing Network Infrastructure in Certified Ethical Hacking. Cengage Learning. pp. 3–. ISBN 978-1-4354-8365-1. Retrieved 14 June 2013.
[12] "Secure Your Database Using Honeypot Architecture". www.dbcoretech.com. August 13, 2010. Archived from the original on March 8, 2012.
[13] "Deception Toolkit". All.net. All.net. 2013. Retrieved 14 June 2013.
[14] "Cisco router Customer support". Clarkconnect.com. Retrieved 2015-07-31.
[15] "Know Your Enemy: GenII Honey Nets Easier to deploy, harder to detect, safer to maintain". Honeynet Project. Honeynet Project. 12 May 2005. Retrieved 14 June 2013.