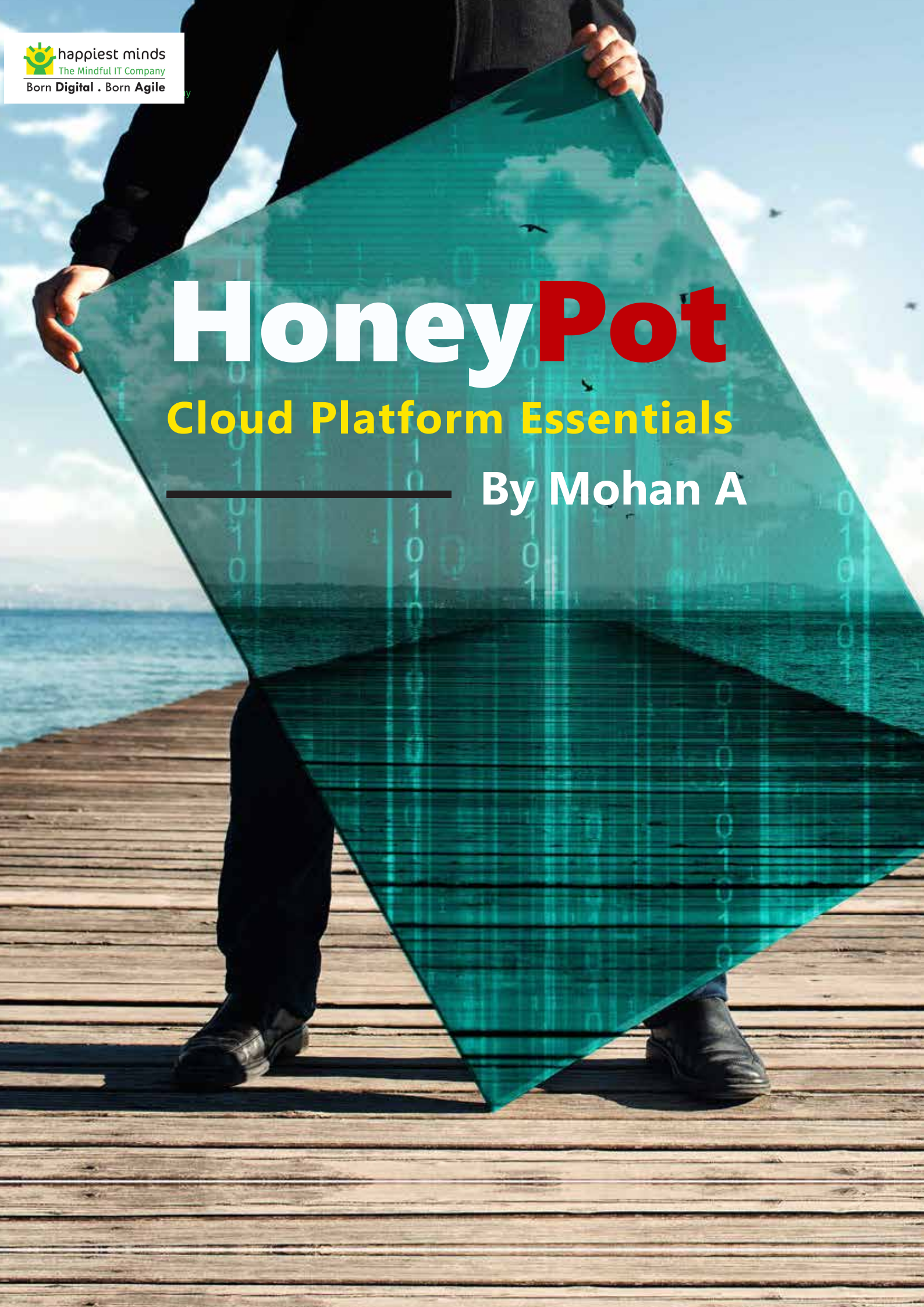
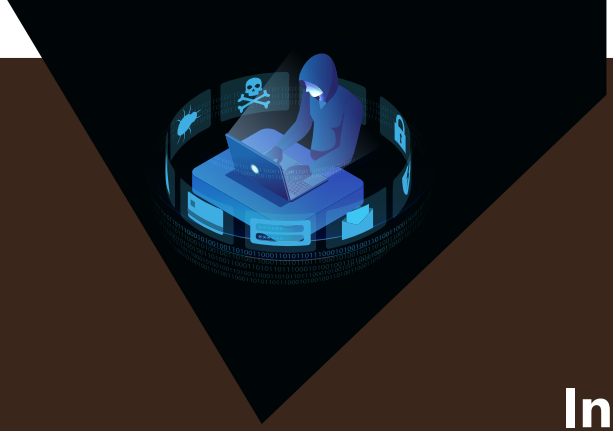
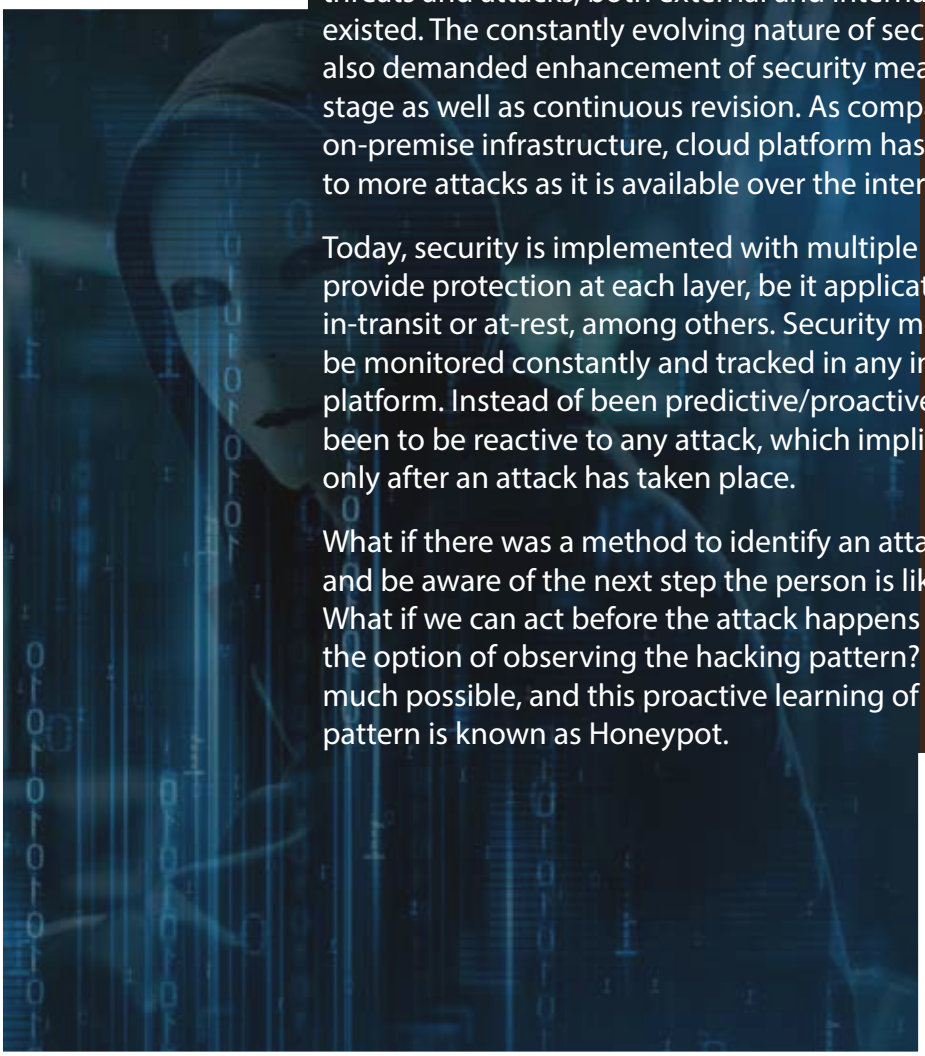

happiest minds
The Mindful IT Company
Born Digital . Born Agile
HoneyPot
Cloud Platform Essentials
By Mohan A

Contents



Introduction

Security has always been a vital component for any industry and a critical factor in Information Technology. Physical, VM or Cloud, no matter which era we belong to - security risks, threats and attacks, both external and internal – have always existed. The constantly evolving nature of security risks has also demanded enhancement of security measures at each stage as well as continuous revision. As compared to on-premise infrastructure, cloud platform has been subject to more attacks as it is available over the internet.



Today, security is implemented with multiple devices to provide protection at each layer, be it application, physical, in-transit or at-rest, among others. Security measures must be monitored constantly and tracked in any infrastructure platform. Instead of been predictive/proactive, the trend has been to be reactive to any attack, which implies that we react only after an attack has taken place.

What if there was a method to identify an attacker's strategy and be aware of the next step the person is likely to take? What if we can act before the attack happens and even have the option of observing the hacking pattern? Yes, this is very much possible, and this proactive learning of an attack pattern is known as Honeypot.

Honeypot

Honeypot is the emulated environment of a system or application, where one intentionally sets up infrastructure in which a system or an application is vulnerable to an attack. The intention of such a system is to gain information regarding the attacking methods, which could subsequently be used for understanding the attacking patterns. By tricking the attacker to think it as an actual system, this emulated environment provides a great way of studying attacking patterns. Honeypots can be built in a VM or a physical system, depending on the individual's choice. The best Honeypot would be a system with the most interactive configuration to emulate a real system, which would trick the attacker to completely believe that he is attacking a real system/infrastructure.

The intention of such a system is to gain information regarding the attacking methods, which could subsequently be used for understanding the attacking patterns.

Honeypot can serve companies well in their endeavor to comprehend an attacking strategy. For example, a software company could use Honeypot on their newly devel-oped software or application to understand the security threats and loopholes associated with it. All they need to do is to set up an emulated system, isolated from their production network, and keep it accessible for an attacker.

All they need to do is to set up an emulated system, isolated from their production network, and keep it accessible for an attacker

Once a hacker tries to sniff into these simulated systems, it makes it easier for the security team to monitor, track and learn the attacking strategy as well as any vulnerable application that may be available in their production system. This will, in turn, enable the team to secure the production system appropriately, thereby proactively securing their product.

Need for Honeypot

Honeypot provides multiple benefits as compared to traditional security products. However, this does not imply that traditional security products can be replaced with Honeypot, as each of them serves a different purpose and are implemented for different situations.

Some of the benefits of Honeypot are described below:

1

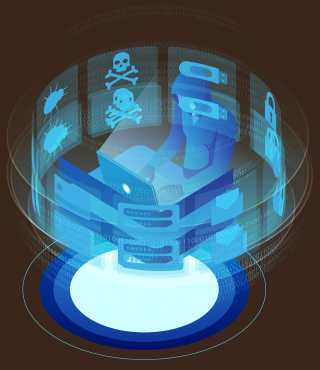
Studying the Attacker:
The emulated environment (Honeypot) will not just let you study the vulnerable application that gets attacked but also lets you read the attacker's mind. It simply means that that you get to know which specific data/information the attacker is looking for and what steps he/she would take to compromise those systems.

2

Notify about Vulnerabilities:
Monitoring the attack patterns gives a clear picture to the company's security team regarding systems that are most vulnerable. This enables an organization to fix those vulnerabilities and prevent any future attack on a production/live setup.

3

Keeps the attacker busy
Honeypot keeps the production network safer by consuming the attacker's time as the person will be engaged in attacking simulated systems.

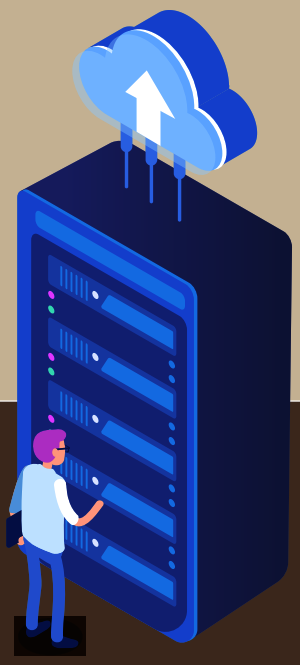


Security on Cloud

As Cloud is considered to be the most attackable platform since it hosted on a public network, it demands a proactive approach from cloud providers and the companies hosting their services, to ensure that their application, system, data, etc., are secure. The ideal way to secure these systems is by safeguarding the traffic with cloud ACL's, Instance Level Security, and making use of traditional security mechanisms such as IDS/IPS, Nextgen Firewalls, AV, etc. However, these security systems will only let you prevent an attack. It will not allow you to predict an attack beforehand.

Honeypot in Cloud

Setting up honeypot on the cloud lets an organization recognize the attacker's behavior and enables one to gauge the most vulnerable application running in the environment. Honeypot provides vital information for the security team about the attack and the possible targets, which can be used to secure those targets.

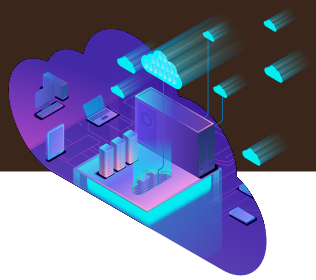


Procedure – Setup Honeypot in Cloud

1. **Honeypot Software**
   Choose the list of applications or servers that you would want to emulate in the honeypot. For example, you can select a new application to understand how it is likely to get attacked. Multiple open source software such as "Honeynet Project", "Honey Stick", "Web Application honeypot", etc., are available for hosting a honeypot.

2. **Installation**
   Once the Honeypot software has been selected, you can install it the virtual system in the cloud.

3. **Build a Honeypot Environment**
Set up an isolated network to host a honeypot because once the honeypot system is compromised by an attacker, he/she should not get access to the production networks.



4. **Honeypot Configuration**
Setup up an interaction level between low and high. The higher the interaction level, the higher are the chances of getting the attacker tricked to believe it is a real system.

5. **Set the Trap**
Enable the necessary port to get attacked for studying the attack pattern.

6. **Start Observing**
Provide complete visibility to the security team to track and monitor activities in the environment.

Disadvantage of Honeypot

Though honeypot lets us study the attacker's behavior and attack forms, it has the following disadvantages.

1. If the attacker succeeds in compromising the honeypot system, he/she may get access to the network and try to attack other systems in that network. And, if honeypot is in the same production network, it is very likely that the production system will also be attacked.

2. Honeypot in the cloud also poses a threat to get attacked by other Virtual Networks because no one is sure how the underlying cloud connectivity is set up. It will be risky if the underlying cloud connectivity could be used to attack other instances in the cloud.

Conclusion

With the increase in the number of threats and attacks in the industry, traditional security products are no longer sufficient. Learning the next move of an attacker at an early stage will keep the application/network safe. Cloud is a good platform to implement and monitor the Honeypot to study and be aware of the attacks.

Mohan Alagar

Certified Network Specialist from Palo Alto, Amazon Web Service, Juniper and Cisco networks Engineer with 9+ years of IT experience, Including 7 years of Networking Security Specialist and 5 years of Novell Technologies and . Skill set and expertise with Amazon Web Service, Palo Alto firewalls, Juniper Firewalls, Cisco ASA, Cisco Routers and Switches, Cloud Websense Proxy, Novell eDirectory, Novell ZENworks, iPrint, Identity Manager, and SuSE Linux. Roles performed are Juniper TAC, Novell Technical Support, Senior Engineer and Tech Lead. Worked with clients like Infosys, Juniper, HP, Novell, TMF Groups, Bestinet, Freedom, SUD Life and Ascend Learning. I have published several Technical Information Document (TID) for Novell. I am Certified - Palo Alto Certified Network Security Engineer (PCNSE), Amazon Web Service (AWS - Associate), Juniper Networks Certified Internet Specialist (JNCIS-FWV), Cisco Certified Network Associate - Security (CCNA-Security), Cisco Certified Network Associate - Routing and Switching (CCNA R&S).

About Happiest Minds Technologies

Happiest Minds, the Mindful IT Company, applies agile methodologies to enable digital transformation for enterprises and technology providers by delivering seamless customer experience, business efficiency and actionable insights. We leverage a spectrum of disruptive technologies such as: Big Data Analytics, AI & Cognitive Computing, Internet of Things, Cloud, Security, SDN-NFV, RPA, Blockchain, etc. Positioned as "Born Digital . Born Agile", our capabilities spans across product engineering, digital business solutions, infrastructure management and security services. We deliver these services across industry sectors such as retail, consumer packaged goods, edutech, e-commerce, banking, insurance, hi-tech, engineering R&D, manufacturing, automotive and travel/transportation/hospitality.

Headquartered in Bangalore, India Happiest Minds has operations in USA, UK, The Netherlands, Australia and Middle East.

To know more about our offerings. Please write to us at **business@happiestminds.com**