1.A brief history and evolution of honeypots:

1. INTRODUCTION:

For every consumer and business that is on the Internet, viruses, worms, and crackers are but a few security threats.The systems can only react to or prevent attacks but they cannot give us information about the attacker, the tools used or even the methods employed.

Hence, Honeypots are a novel approach to network security and security research alike.

Honeypots are closely monitored decoys that are employed in a network to study the trail of hackers and to alert network administrators of a possible intrusion. Honeypots provide a cost-effective solution to increase the security posture of an organization. Nowadays, they are also being extensively used by the research community to study issues in network security.

1.1 History of Honeypots:

Honeypots have played a significant role in computer security, and their evolution can be traced back to the late 1980s. Here's a brief history and evolution of honeypots:

1. Early Years (Late 1980s - Mid-1990s):

The concept of honeypots originated with Clifford Stoll's book, "The Cuckoo's Egg," published in 1989. Stoll, an astronomer turned system administrator, created a honeypot to track a hacker infiltrating his systems. However, the term "honeypot" was coined by Lance Spitzner in the mid-1990s.

2. Research and Development (Late 1990s - Early 2000s):

In the late 1990s, honeypot research gained momentum. Researchers began experimenting with different types of honeypots and methodologies. The focus was on gathering information about attackers, their techniques, and their motives. Some notable early honeypot projects include "Honeynet Project" by Lance Spitzner and "LaBrea Tarpit" by Tom Liston.

3. Production Honeypots (Early 2000s):

As the concept of honeypots matured, the first production-grade honeypots were developed. These honeypots were designed for deployment in real-world environments and focused on capturing and analyzing attacks. Projects like "Honeyd" by Niels Provos and "KFSensor" by Dario Ferrante were among the early production honeypots.

4. Honeypots for Intrusion Detection (Mid-2000s):

Honeypots began to be used as intrusion detection tools. By deploying honeypots alongside production systems, organizations could detect and respond to attacks more effectively. Honeypots helped in identifying new attack techniques and vulnerabilities, enabling the improvement of overall security defenses.

5. Diversity and Interaction (Late 2000s - Early 2010s):

Honeypot diversity increased during this period. Different types of honeypots emerged, including high-interaction and low-interaction honeypots. High-interaction honeypots provided a complete emulated environment for attackers, while low-interaction honeypots emulated specific services or protocols. This diversity allowed researchers to collect more detailed information about attackers' activities.

6. Threat Intelligence and Deception (2010s):

Honeypots became integral to threat intelligence. By analyzing data collected from honeypots, security professionals gained insights into emerging threats, attacker behavior, and trends. Deception technologies, which use honeypot-like techniques, also emerged during this period to lure and deceive attackers away from critical systems.

7. Virtualization and Cloud-Based Honeypots (Mid-2010s - Present):

Virtualization and cloud computing brought new possibilities to honeypot deployment. Virtualized honeypots allowed for efficient resource allocation and easy deployment in various environments. Cloud-based honeypots

leveraged the scalability and accessibility of cloud platforms, enabling organizations to deploy honeypots globally.

8. Modern Honeypot Ecosystem (Present):

Today, the honeypot ecosystem has evolved into a sophisticated network of tools, frameworks, and projects. Honeypots are used for various purposes, including threat intelligence, intrusion detection, malware analysis, and attacker profiling. Open-source projects like "Cowrie," "Dionaea," and "Glastopf" have gained popularity, providing flexible and scalable honeypot solutions.

The evolution of honeypots continues as security professionals adapt to new threats and technologies, ensuring that honeypots remain effective tools for understanding and mitigating cyber risks.

2. Cybersecurity breaches and trends

A **data breach** is a security violation, in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen, altered or used by an individual unauthorized to do so. Other terms are **unintentional information disclosure**, **data leak**, information leakage and **data spill**. (source wikipedia)

2.1 Types of security breaches

There are a number of types of security breaches depending on how access has been gained to the system:

- An exploit attacks a system vulnerability, such as an out of date operating system. Legacy systems which haven't been updated, for instance, in businesses where outdated and versions of Microsoft Windows that are no longer supported are being used, are particularly vulnerable to exploits.
- Weak passwords can be cracked or guessed. Even now, some people are still using the password 'password', and 'pa$$word' is not much more secure.
- Malware attacks, such as phishing emails can be used to gain entry. It only takes one employee to click on a link in a phishing email to allow malicious software to start spreading throughout the network.
- Drive-by downloads use viruses or malware delivered through a compromised or spoofed website.
- Social engineering can also be used to gain access. For instance, an intruder phones an employee claiming to be from the company's IT helpdesk and asks for the password in order to 'fix' the computer.

2.2 Examples of a security breach

When a major organization has a security breach, it always hits the headlines. Security breach examples include the following:

- Equifax - in 2017, a website application vulnerability caused the company to lose the personal details of 145 million Americans. This included their names, SSNs, and drivers' license numbers. The attacks were made over a three-month period from May to July, but the security breach wasn't announced until September.
- Yahoo - 3 billion user accounts were compromised in 2013 after a phishing attempt gave hackers access to the network.

- eBay saw a major breach in 2014. Though PayPal users' credit card information was not at risk, many customers' passwords were compromised. The company acted quickly to email its users and ask them to change their passwords in order to remain secure.
- Dating site Ashley Madison, which marketed itself to married people wishing to have affairs, was hacked in 2015. The hackers went on to leak a huge number of customer details via the internet. Extortionists began to target customers whose names were leaked; unconfirmed reports have linked a number of suicides to exposure by the data breach.
- Facebook saw internal software flaws lead to the loss of 29 million users' personal data in 2018. This was a particularly embarrassing security breach since the compromised accounts included that of company CEO Mark Zuckerberg.
- Marriott Hotels announced a security and data breach affecting up to 500 million customers' records in 2018. However, its guest reservations system had been hacked in 2016 - the breach wasn't discovered until two years later.
- Perhaps most embarrassing of all, being a cybersecurity firm doesn't make you immune - Czech company Avast disclosed a security breach in 2019 when a hacker managed to compromise an employee's VPN credentials. This breach didn't threaten customer details but was instead aimed at inserting malware into Avast's products.

A decade or so ago, many companies tried to keep news of security breaches secret in order not to destroy consumer confidence. However, this is becoming increasingly rare. In the EU, the GDPR (General Data Protection Regulations) require companies to notify the relevant authorities of a breach and any individuals whose personal data might be at risk. By January 2020, GDPR had been in effect

for just 18 months, and already, over 160,000 separate data breach notifications had been made - over 250 a day.

2.3 What to do if you experience a security breach

As a customer of a major company, if you learn that it has had a security breach, or if you find out that your own computer has been compromised, then you need to act quickly to ensure your safety. Remember that a security breach on one account could mean that other accounts are also at risk, especially if they share passwords or if you regularly make transactions between them.

- **If a breach could involve your financial information, notify any banks** and financial institutions with which you have accounts.
- **Change the passwords on all your accounts**. If there are security questions and answers or PIN codes attached to the account, you should change these too.
- **You might consider a credit freeze.** This stops anyone using your data for identity theft and borrowing in your name.
- **Check your credit report to ensure you know if anyone is applying for debt using your details**.
- **Try to find out exactly what data might have been stolen.** That will give you an idea of the severity of the situation. For instance, if tax details and SSNs have been stolen, you'll need to act fast to ensure your identity isn't stolen. This is more serious than simply losing your credit card details.
- **Don'trespond directly to requests from a company to give them personal data after a data breach;** it could be a social engineering attack. Take the

time to read the news, check the company's website, or even phone their customer service line to check if the requests are legitimate.

- **Be on your guard for other types of social engineering attacks.** For instance, a criminal who has accessed a hotel's accounts, even without financial data, could ring customers asking for feedback on their recent stay. At the end of the call, having established a relationship of trust, the criminal could offer a refund of parking charges and ask for the customer's card number in order to make the payment. Most customers probably wouldn't think twice about providing those details if the call is convincing.
- **Monitor your accounts for signs of any new activity**. If you see transactions that you don't recognize, address them immediately.

2.4 How to protect yourself against a security breach

Although no one is immune to a data breach, good computer security habits can make you less vulnerable and can help you survive a breach with less disruption. These tips should help you prevent hackers breaching your personal security on your computers and other devices.

- Use strong passwords, which combine random strings of upper and lower-case letters, numbers, and symbols. They are much more difficult to crack than simpler passwords. Don't use passwords that are easy to guess, like family names or birthdays. Use a Password Manager to keep your passwords secure.
- Use different passwords on different accounts. If you use the same password, a hacker who gains access to one account will be able to get into all your other accounts. If they have different passwords, only that one account will be at risk.
- Close accounts you don't use rather than leaving them dormant. That reduces your vulnerability to a security breach. If you don't use an account, you might never realize that it has been compromised, and it could act as a back door to your other accounts.
- Change your passwords regularly. One feature of many publicly reported security breaches is that they occurred over a long period, and some were not reported until years after the breach. Regular password changes reduce the risk you run from unannounced data breaches.
- If you throw out a computer, wipe the old hard drive properly. Don't just delete files; use a data destruction program to wipe the drive completely, overwriting all the data on the disk. Creating a fresh installation of the operating system will also wipe the drive successfully.

- Back up your files. Some data breaches lead to the encryption of files and a ransomware demand to make them available again to the user. If you have a separate backup on a removable drive, your data is safe in the event of a breach.
- Secure your phone. Use a screen lock and update your phone's software regularly. Don’t root or jailbreak your phone. Rooting a device gives hackers the opportunity to install their own software and to change the settings on your phone.
- Secure your computer and other devices by using anti-virus and anti-malware software.Kaspersky Antivirus is a good choice to keep your computer free from infection and ensure that hackers can't get a foothold in your system.
- Be careful where you click. Unsolicited emails which include links to websites may be phishing attempts. Some may purport to be from your contacts. If they include attachments or links, ensure they're genuine before you open them and use an anti-virus program on attachments.
- When you're accessing your accounts, make sure you're using the secure HTTPS protocol and not just HTTP.
- Monitoring your bank statements and credit reports helps keep you safe. Stolen data can turn up on the dark web years after the original data breach. This could mean an identity theft attempt occurs long after you've forgotten the data breach that compromised that account.
- Know the value of your personal information and don't give it out unless necessary. Too many websites want to know too much about you; why does a business journal need your exact date of birth, for instance? Or an auction site your SSN?

You'd never dream of leaving your house door open all day for anyone to walk in. Think of your computer the same way. Keep your network access and your personal data tightly secured, and don't leave any windows or doors open for a hacker to get through.

3.1 Importance of Honeypots for an organization’s security strategy

Honeypots are very important for every company ,
Honeypot helps company to protect company secret ,
Most important security strategy is given below in detail.

1. Early Threat Detection:
Honeypots serve as early warning systems by attracting and capturing attackers in a controlled environment. They are designed to mimic real systems and services, making them attractive targets for potential attackers. By monitoring honeypots, organizations can detect attacks at an early stage, before they reach production systems. This early detection allows security teams to initiate incident response procedures promptly, minimizing potential damage and reducing the time an attacker has to compromise critical assets.

2. Attack Analysis and Understanding:
Honeypots provide an opportunity for organizations to closely observe and study attacker behavior. By capturing and analyzing the activities within a honeypot, security professionals can gain valuable insights into attacker techniques, tools, and motives. They can observe the types of attacks attempted, the methods used, and the vulnerabilities targeted. This knowledge helps organizations improve their

overall security defenses by identifying weaknesses, implementing appropriate countermeasures, and enhancing incident response capabilities.

3. Identification of Zero-Day Attacks:

Zero-day attacks refer to vulnerabilities or exploits that are unknown to the public or the software vendor. Honeypots can be used as bait to identify attempts to exploit such vulnerabilities. Since honeypots are isolated and closely monitored, any attempts to exploit vulnerabilities unique to the honeypot environment can be quickly identified. This enables organizations to gain early insight into zero-day attacks, understand their impact, and develop effective mitigation strategies.

4. Deception and Misdirection:

Honeypots serve as decoys, diverting attackers away from critical systems and assets. By strategically placing honeypots within the network, organizations can create an additional layer of defense. Attackers who interact with honeypots waste their time and resources on non-production systems, increasing the chances of their activities being detected. Honeypots confuse and delay attackers, providing security teams with more time to respond, investigate, and mitigate attacks on real systems.

5. Threat Intelligence and Forensics:

The data collected from honeypots provides valuable threat intelligence. By analyzing the activities and techniques employed by attackers within honeypots, organizations can gain insights into emerging threats, attack trends, and indicators of compromise (IOCs). This intelligence can be used to update security controls, improve intrusion detection systems, and enhance incident response capabilities.

Honeypots also assist in forensic investigations by providing a controlled environment for capturing and preserving evidence related to attacks.

6. Insider Threat Detection:
Honeypots can be utilized to detect and mitigate insider threats within an organization. By monitoring honeypot activity, security teams can identify suspicious behavior or unauthorized access attempts by internal employees. Honeypots can help detect insider threats who may be attempting to exploit vulnerabilities or gain unauthorized access to sensitive information. This allows organizations to take appropriate actions, such as conducting internal investigations, implementing stricter access controls, and providing targeted security awareness training.

7. Training and Skill Development:
Honeypots offer a platform for security professionals to gain hands-on experience in analyzing and responding to real-world attacks. By actively managing and monitoring honeypots, security personnel can enhance their skills in incident response, malware analysis, threat hunting, and vulnerability assessment. Honeypots provide a safe and controlled environment for security teams to test new techniques, practice incident response procedures, and develop effective strategies for protecting critical systems.

By incorporating honeypots into their security strategy, organizations can benefit from early threat detection, gain insights into attacker behavior, identify and mitigate zero-day attacks, divert and confuse attackers, gather threat intelligence, detect insider threats, and enhance the skills of their security teams. Honeypots

serve as valuable tools in understanding, mitigating, and defending against a wide range of cyber threats.

4.1 An overview of the various types of honeypots

Honeypots are classified based on their deployment and the involvement of the intruder.

Based on their deployment, honeypots are divided into :

1. Research honeypots- These are used by researchers to analyze hacker attacks and deploy different ways to prevent these attacks.
2. Production honeypots- Production honeypots are deployed in production networks along with the server. These honeypots act as a frontend trap for the attackers, consisting of false information and giving time to the administrators to improve any vulnerability in the actual system.

Based on interaction, honeypots are classified into:

1. **Low interaction honeypots:**Low interaction honeypots gives very little insight and control to the hacker about the network. It simulates only the services that are frequently requested by the attackers. The main operating system is not involved in the low interaction systems and therefore it is less risky. They require very fewer resources and are easy to deploy. The only disadvantage of these honeypots lies in the fact that experienced hackers can easily identify these honeypots and can avoid it.
2. **Medium Interaction Honeypots:** Medium interaction honeypots allows more activities to the hacker as compared to the low interaction honeypots.

They can expect certain activities and are designed to give certain responses beyond what a low-interaction honeypot would give.

3. **High Interaction honeypots:**A high interaction honeypot offers a large no. of services and activities to the hacker, therefore, wasting the time of the hackers and trying to get complete information about the hackers. These honeypots involve the real-time operating system and therefore are comparatively risky if a hacker identifies the honeypot. High interaction honeypots are also very costly and are complex to implement. But it provides us with extensively large information about hackers.

   Most common uses of honeypot are given below:

   - Web honeypot
   - Network honeypot
   - Mobile honeypot

There are also different types of web network,mobile honeypots present.

5.1 What is a Honeynet?

A Honeynet is a type of security system that can be used to detect, respond to, and prevent malicious activities on a network. It is comprised of several components, including honeypots, honeywalls, honeydumps and honeyagents. Honeypots are decoy systems that are designed to attract and identify malicious actors. A honeywall is used to monitor network traffic and divert malicious actors to the honeypot instances. Security teams can use these decoy systems or servers deployed alongside production systems within their networks as enticing targets for attackers in order to investigate attacker behavior patterns. Honeydumps are databases that store information about malicious activity on the network while

honeyagents are software programs that detect and respond quickly and efficiently when potential threats arise.

5.2 Benefits of Honeynets

Honeynets offer a range of benefits to organizations, including improved network security, faster threat detection and response times, and reduced risk of data loss or compromise. Setting up and managing honeynets is also relatively easy, as they require minimal maintenance and can be automated for optimal performance. Additionally, honeynets are cost-effective solutions that can help organizations save time and money.

Honeypots are decoy systems designed to look like vulnerable systems in order to attract malicious actors. There are several types of honeypots available depending on the design and deployment model chosen. High-interaction honeypots provide a wealth of information but also introduce additional risk into the network. Honeynets consist of multiple interconnected honeypots which allow for vast amounts of data to be collected for analysis. Server-based honeypots can be placed on the internet so that attackers come directly to them with little direct value in protecting your network from threats.

Organizations benefit from using honeynets as they help protect networks from malicious actors while reducing the risk of data loss or compromise. Honeynets also enable faster threat detection and response times which helps organizations save time and money in the long run due to their cost-effectiveness compared with other security solutions available on the market today. Furthermore, setting up and managing a honeynet is relatively easy as it requires minimal maintenance while being able to automate processes for optimal performance at all times

5.3 How Do Honeynets Work?

Honeynets are a powerful tool for detecting and responding to malicious activity on a network. They work by monitoring network traffic for suspicious behavior or

malicious activity, and then responding accordingly. Honeynets are designed to be as unobtrusive as possible, so they can run in the background without interfering with normal operations. The primary purpose of honeynets is to test network security by inviting attacks, which can be done using a honeywall that monitors and analyzes network traffic for suspicious or abnormal activity. When unusual or malicious activity is detected, the honeynet will provide alerts and reports while also blocking access to servers or networks if necessary. Intrusion detection is an important part of this process, which involves monitoring events occurring in a computer system or network and analyzing them for signs of possible incidents. The MBSAP methodology provides seven functional layers that form the basis for communication among computers over networks; these layers can easily be applied to systems requiring protection from sensitive data and processes. With all these features combined, honeynets offer organizations an effective way of detecting threats before they become serious problems.

Conclusion

In conclusion, honeynets are an invaluable tool for protecting networks from malicious actors. They are designed to detect, respond to, and prevent threats quickly and efficiently. Furthermore, they are relatively inexpensive and easy to set up and maintain. Honeypots can be used in conjunction with firewalls and other security solutions to create a comprehensive defense against cyber attacks. Organizations should also train their employees in security principles as well as protect information, computers, and networks from cyber attacks. Additionally, organizations should consider implementing the MBSAP framework for secure network architecture design. By using these tools together organizations can ensure that their networks are secure and protected from malicious activity.

REFERENCE

1. http://www.123seminarsonly.com/Seminar-Reports/012/53599210-Honey-Pots.pdf (introduction)
2. https://chat.openai.com/ (A brief history and evolution of honeypots)
3. https://en.wikipedia.org/wiki/Data_breach
4. https://www.kaspersky.com/resource-center/threats/what-is-a-security-breach (all about security breaches).
5. https://www.geeksforgeeks.org/what-is-honeypot/ (types of honeypots)
6. https://www.privacysense.net/terms/honeynet/ (All about honeynet)