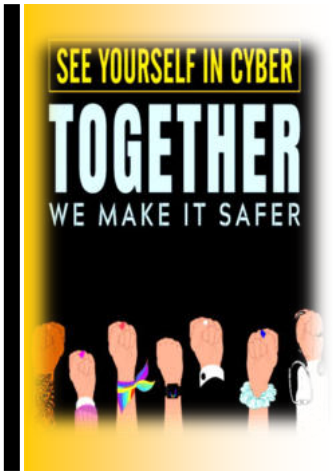
Vol I Issue 8

Cybersecurity Digest

Bi-weekly update by the CISO Section of Meghalaya Rural Bank

Newsletter Date : 01-01-2025

Honeypots



In cybersecurity honeypots are decoy servers or systems that are deployed next to systems your organization actually uses for production. Honeypots are designed to look like attractive targets, and they get deployed to allow IT teams to monitor the system's security responses and to redirect the attacker away from their intended target.

There are various honeypots, and they can be set up according to what your organization needs. Because they appear to be legitimate threats, honeypots act like a trap, enabling you to identify attacks early and mount an appropriate response. This honeypot meaning points to some of the ways they can be used to direct attackers away from your most important systems. While the attacker falls for the bait, you can gather crucial intelligence about the type of attack, as well as the methods the attacker is using.

A honeypot works best when it appears to be a legitimate system. In other words, it must run the same processes your actual production system would run. It should also contain decoy files the attacker will see as appropriate for the targeted processes. In many cases, it is best to put the honeypot behind the firewall protecting your organization's network. This enables you to examine threats that get past the firewall and prevent attacks engineered to be launched from within a compromised honeypot. As the attack ensues, your firewall, positioned between the honeypot and the internet, can intercept it and eliminate the data.

How do Honeypots work?

In many ways, a honeypot looks exactly like a genuine computer system. It has the applications and data that cyber criminals use to identify an ideal target. A honeypot can, for instance, pretend to be a system that contains sensitive consumer data, such as credit card or personal identification information. The system can be populated with decoy data that may draw in an attacker looking to steal and use or sell it. As the attacker breaks into the honeypot, the IT team can observe how the attacker proceeds, taking note of the various techniques they deploy and how the system's defenses hold up or fail. This can then be used to strengthen the overall defenses used to protect the network.

Honeypots use security vulnerabilities to lure in attackers. They may have ports that are vulnerable to a port scan, which is a technique for figuring out which ports are open on a network. A port left open may entice an attacker, allowing the security team to observe how they approach their attack.

Honeypotting is different from other types of security measures in that it is not designed to directly prevent attacks. The purpose of a honeypot is to refine an organization's intrusion detection system (IDS) and threat response so it is in a better position to manage and prevent attacks.

SALAMI ATTACK

A salami attack is a fraudulent technique used by cybercriminals to steal small amounts of money or data from multiple victims, gradually accumulating a significant gain for themselves. It is a deceptive and subtle form of hacking that can go unnoticed for a long time, making it difficult to detect and trace back to the perpetrator.

A salami attack derives its name from slicing thin and indiscernible pieces, just as a salami slicer slices the meat thinly without arousing suspicion. Similarly, cybercriminals in a salami attack carry out their malicious activities stealthily, making it challenging for victims and investigators to identify and stop the breach.

The origin of salami attacks can be traced back to the early days of the digital age when financial systems became increasingly interconnected. As technology advanced, so did the methods employed by cybercriminals, leading to the emergence of salami attacks as a sophisticated technique for financial gain.

Real-Life Examples of Salami Attack

Salami attacks have been carried out in various industries, targeting both individuals and organizations. One notable example occurred in banking, where cybercriminals manipulated financial transactions by rounding off decimal points. By siphoning off the fractions of rupees, the attackers accumulated significant sums over time, all while remaining undetected.

Another salami attack occurred in the e-commerce industry. Cybercriminals exploited vulnerabilities in the payment systems of online retailers, making small alterations to purchase amounts. These seemingly insignificant changes went unnoticed by customers, but the attackers accumulated substantial profits by skimming off a fraction of each transaction.

> Ever spotted a weird, tiny charge on your bank statement? It might have only been a couple of rupees, and you wrote it off as an error. But what if it wasn't? Or maybe it was the first step in an elaborate cybercrime strategy called a salami attack?

Citibank : SALAMI Attack

The Citibank hack was the first significant cybercrime involving banks. In 1994, Russian computer programmer Vladimir Levin tricked Citibank's computers into transferring money to his account. He then used the money to buy goods and services in various locations around the world. Levin pleaded guilty in January 1998, admitting that he had hacked into Citibank's systems and obtained the customer information.

Although Levin did not steal any money directly, he did gain control of funds belonging to others. Citibank denied that anyone within the bank helped Levin carry out the crime. However, no one has ever claimed responsibility for Levin's actions.

According to published reports (Citigroup), Citibank's internal systems detected suspicious activity involving two wire transfer requests totaling $26,800 and $304,000. When bank personnel contacted the Federal Bureau of Investigation, they could trace the source of the funds to an account belonging to Michael R. Levin, a resident of New York City. Telephone records showed that Levin had used his home telephone number to make the fraudulent requests. In addition, investigators determined that Levin had transferred money out of the United States through Western Union offices in Moscow, Russia.