Seminar Topic

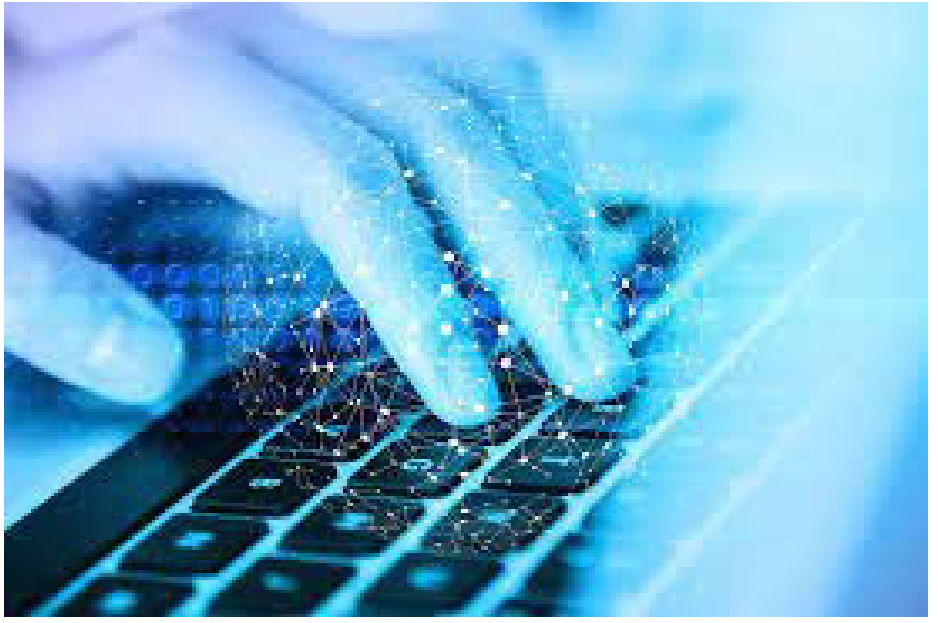
Honey Trap

Group Members

- ***Belim Toufique***
- ***Abhishek Yadav***
- ***Haamid Khan***
- ***Suyog Bokefode***

What is a Honey Trap ?

- It is defined as a computer system on the Internet that is expressly set up to attractand "***trap***" people who attempt to ***penetrate*** other person's computer systems. Honeypot is a trap; an electronic bait. It is a computer or network resources that appear to be a part of the network.



What is a Honey Trap ?

- But have been deployed as a honeypot can be as simple as a single computer running a program to listen on any number of ***ports***; ***when a connection is made,the program logs the source IP and alerts the owner with an e-mail.***

How does a Honey Trap Work ?

- Honey pots work by ***monitoring*** and/or ***controlling*** the intruder during their use ofthe honey pot. A critical element to any honeypot is ***data capture***, the ability to log, alert, and capture everything the bad guy is doing. Most honeypot solutions, such as Honeyd or Specter, have their own logging and alerting capabilities.

How does a Honey Trap Work ?

- It is highly recommend deploying ***Snort*** with any honeypot deployment. Snort is an ***OpenSource IDS*** system that will not only detect and alert any attacks against your honeypot, but it can capture the ***packets*** and ***packet payloads*** involved in the attack.

The Idea of Honey Pots

- To learn how ***intruders*** probe and attempt to ***gain access*** to your systems and gain insight into attack methodologies to better protect real production systems.
- To gather ***forensic information*** required to aid in the apprehension orprosecution of intruders.

Email Trap

- **Email traps** or spam traps place a fake email address in a hidden location where only an automated address harvester will be able to find it. Since the address isn't used for any purpose other than the spam trap, it's 100% certain that any mail coming to it is spam.

Email Trap

- All messages which contain the same content as those sent to the spam trap can be automatically blocked, and the source IP of the senders can be added to a ***denylist***.

Decoy database

- A **decoy database** can be set up to monitor software vulnerabilities and spot attacks exploiting insecure system architecture or using SQL injection, SQL services exploitation, or privilege abuse.

Malware honeypot

- A **malware honeypot** mimics software apps and APIs to invite malware attacks. The characteristics of the malware can then be **analyzed** to develop anti-malware software or to close vulnerabilities in the API.

Spider honeypot

- A **spider honeypot** is intended to trap webcrawlers ('spiders') by creating web pages and links only accessible to crawlers. Detecting crawlers can help you learn how to block malicious bots, as well as ad-network crawlers.

What’s the use of HoneyPot ?

By monitoring traffic coming into the **honeypot** system, you can assess:

- ***Where the cybercriminals are coming from!***
- ***The level of threat!***
- ***What modus operandi they are using!***
- ***What data or applications they are interested in!***
- ***How well your security measures are working to stop cyberattacks!***

Benefits

- Using a honeypot has several advantages over trying to spot intrusion in the real system. For instance, by definition, a honeypot shouldn't get any ***legitimate*** traffic, so any activity logged is likely to be a probe or intrusion attempt.

Benefits

- That makes it much easier to spot patterns, such as similar IP addresses (or IP addresses all coming from one country) being used to carry out a ***network sweep***. By contrast, such tell-tale signs of an attack are easy to lose in the noise when you are looking at high levels of legitimate traffic on your ***core network.***

Benefits

- The big advantage of using honeypot security is that these **malicious** addresses might be the only ones you see, making the attack much **easier** to identify.

Dangers of Honey Pot

- While honeypot cybersecurity will help chart the **threat environment**, honeypots won't see everything that is going on - only activity that's directed at the honeypot. Just because a certain threat hasn't been directed against the honeypot, you can't assume it doesn't exist; it's important to keep up with **IT security news**, not just rely on honeypots to notify you of the threats.

Dangers of Honey Pot

- Once a honeypot has been '**fingerprinted**', an attacker can create spoofed attacks to distract attention from a real exploit being targeted against your production systems. They can also feed bad information to the honeypot.

Conclusion

- Overall, the benefits of using **honeypots** far outweigh the risks. Hackers are often thought of as a distant, invisible threat - but using honeypots, you can see exactly what they're doing, in **real time**, and use that information to stop them getting what they want.

Thank you