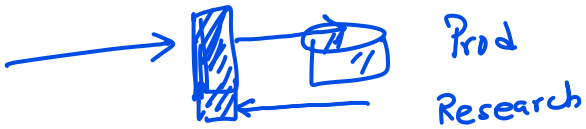
Honeypots

What is a honeypot?

Honeypots are decoy systems or servers deployed alongside production systems within your network. When deployed as enticing targets for attackers, honeypots can add security monitoring opportunities for blue teams and misdirect the adversary from their true target. Honeypots come in a variety of complexities depending on the needs of your organization and can be a significant line of defense when it comes to flagging attacks early. This page will get into more detail on what honeypots are, how they are used, and the benefits of implementing them.

Honeypot basics

There are many applications and use cases for honeypots, as they work to divert malicious traffic away from important systems, get an early warning of a current attack before critical systems are hit, and gather information about attackers and their methods. If the honeypots don't actually contain confidential data and are well-monitored, you can get insight on attacker tools, tactics, and procedures (TTPs) and gather forensic and legal evidence without putting the rest of your network at risk.



For a honeypot to work, the system should appear to be legitimate. It should run processes a production system is expected to run, and contain seemingly important dummy files. The honeypot can be any system that has been set up with proper sniffing and logging capabilities. It's also a good idea to place a honeypot behind your corporate firewall—not only does it provide important logging and alerting capabilities, but you can block outgoing traffic so that a compromised honeypot cannot be used to pivot toward other internal assets.

In terms of objectives, there are two types of honeypots: research and production honeypots. Research honeypots gather information about attacks and are used specifically for studying malicious behavior out in the wild. Looking at both your environment and the wider world, they gather information about attacker trends, malware strains, and vulnerabilities that are actively being targeted by adversaries. This can inform your preventative defenses, patch prioritization, and future investments.

Production honeypots, on the other hand, are focused on identifying active compromise on your internal network and tricking the attacker. Information gathering is still a priority, as honeypots give you additional monitoring opportunities and fill in common detection gaps around identifying network scans and lateral movement. Production honeypots sit with the rest of your production servers and run services that would typically run in your environment. Research honeypots tend to be more complex and store more types of data than production honeypots.

Honeypot complexity varies

Within production and research honeypots, there are also differing tiers depending on the level of complexity your organization needs:

1. **Pure honeypot:** This is a full-scale, completely production-mimicking system that runs on various servers. It contains "confidential" data and user information, and is full of sensors. Though these can be complex and difficult to maintain, the information they provide is invaluable.

2. **High-interaction honeypot:** This is similar to a pure honeypot in that it runs a lot of services, but it is not as complex and does not hold as much data. High-interaction honeypots are not meant to mimic a full-scale production system, but they do run (or appear to run) all the services that a production system would run, including a proper operating system. This type of honeypot allows the deploying organization to see attacker behaviors and techniques. High-interaction honeypots are resource-intensive and come with maintenance challenges, but the findings can be worth the squeeze.

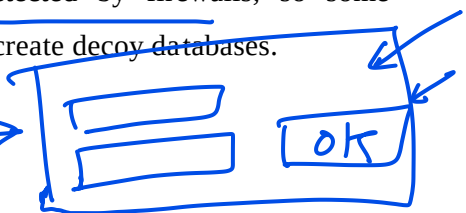
3. **Mid-interaction honeypot:** These emulate aspects of the application layer but do not have their own operating system. They work to stall or confuse attackers so that organizations have more time to figure out how to properly react to an attack.

4. **Low-interaction honeypot:** This type of honeypot is the most commonly deployed in a production environment. Low-interaction honeypots run a handful of services and serve as an early warning detection mechanism more than anything. They are easy to deploy and maintain, with many security teams deploying multiple honeypots across different segments of their network.

Different types of honeypots

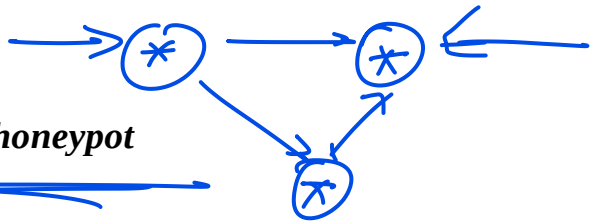
Several honeypot technologies in use include the following:

1. **Malware honeypots:** These use known replication and attack vectors to detect malware. For example, honeypots (e.g., Ghost) have been crafted to emulate as a USB storage device. If a machine is infected by malware that spreads via USB, the honeypot will trick the malware to infect the emulated device.
2. **Spam honeypots:** These are used to emulate open mail relays and open proxies. Spammers will test the open mail relay by sending themselves an email first. If they succeed, they then send out large quantities of spam. This type of honeypot can detect and recognize this test and successfully block the massive volume of spam that follows.
3. **Database honeypot:** Activities such as SQL injections can often go undetected by firewalls, so some organizations will use a database firewall, which can provide honeypot support to create decoy databases.



Client honeypots: Most honeypots are servers listening for connections. Client honeypots actively seek out malicious servers that attack clients, monitoring for suspicious and unexpected modifications to the honeypot. These systems generally run on virtualization technology and have a containment strategy to minimize risk to the research team.

Honeynets: Rather than being a single system, a honeynet is a network that can consist of multiple honeypots. Honeynets aim to strategically track the methods and motives of an attacker while containing all inbound and outbound traffic.



Benefits of a honeypot

Honeypots offer plenty of security benefits to organizations that choose to implement them, including the following:

They break the attacker kill chain and slow attackers down

As attackers move throughout your environment, they conduct reconnaissance, scan your network, and seek misconfigured and vulnerable devices. At this stage, they are likely to trip your honeypot, alerting you to investigate and contain attacker access. This allows you to respond before an attacker has the chance to successfully exfiltrate data from your environment. Malicious actors can also spend a significant amount of time trying to work on the honeypot instead of going after areas that have real data. Diverting their attack to a useless system wastes cycles and gives you early warning of an attack in progress.

They are straightforward and low-maintenance

Modern honeypots are not only easy to download and install, but can provide accurate alerts around dangerous misconfigurations and attacker behavior. In some cases, your team might even forget that a honeypot was ever deployed until someone starts poking around your internal network. Unlike intrusion detection systems, honeypots do not require known-bad attack signatures and fresh threat intel to be useful.

They help you test your incident response processes

Honeypots are a low-cost way to help you increase your security maturity, as they test whether your team knows what to do if a honeypot reveals unexpected activity. Can your team investigate the alert and take appropriate countermeasures?

Honeypots shouldn't be your entire threat detection strategy, but they are another layer of security that can be helpful in discovering attacks early. They are one of the few methods available to security practitioners to study

real-world malicious behavior and catch internal network compromise. Want to learn more about other types of tech that can boost your blue team defenses? Check out our page on deception technology.