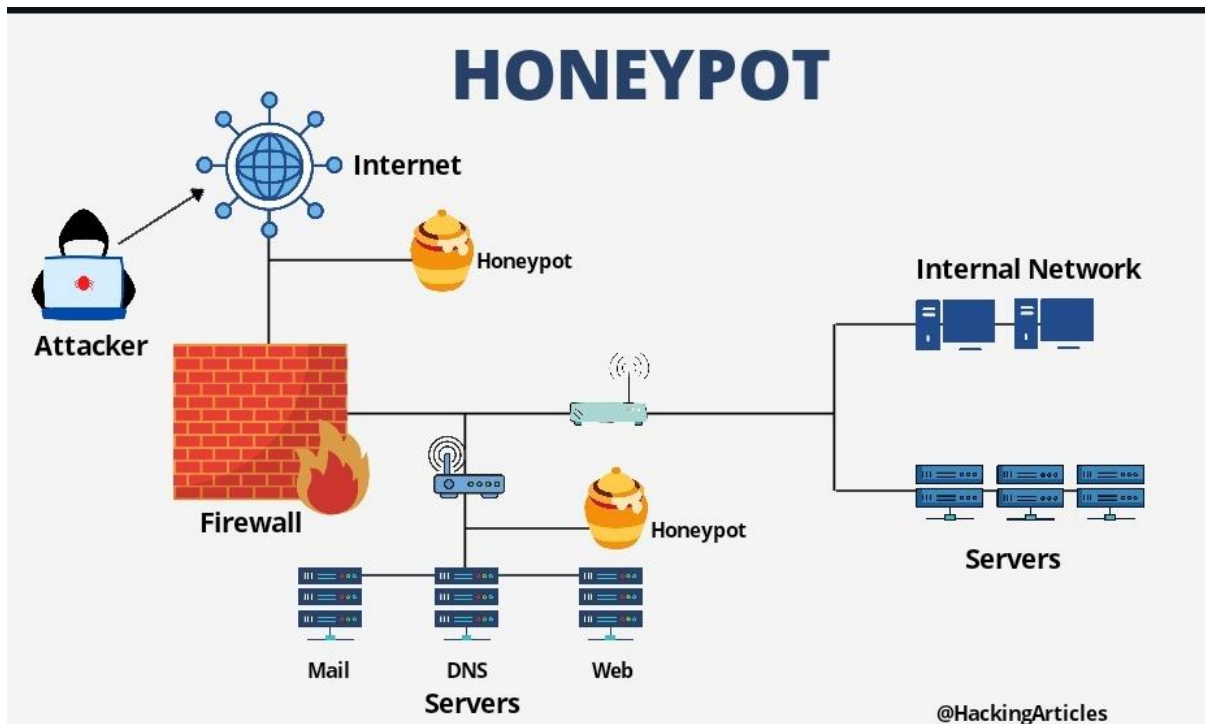


ITEC442 IOT & Cyber Security

Week 5-6 – Honeypot



What is a Honeypot?

A honeypot is a network-attached system set up to act as a decoy, luring in potential attackers to reveal their malicious activity and provide an opportunity for organizations to observe and track them.

Honeypots can be used to gain a better understanding of the tactics and tools used by attackers, to identify new threats, and to monitor the activity of known threats. They can also be used to distract and mislead attackers away from more valuable resources.

There are several different types of honeypots, ranging from simple decoy systems that are used to detect and track basic attacks, to complex systems that are designed to emulate entire networks and systems in order to lure in and track advanced attackers.

Production vs. Research Honeypots

There are two primary types of honeypot designs:

- **Production honeypots**—serve as decoy systems inside fully operating networks and servers, often as part of an intrusion detection system (IDS). They deflect criminal attention from the real system while analyzing malicious activity to help mitigate vulnerabilities.
- **Research honeypots**—used for educational purposes and security enhancement. They contain trackable data that you can trace when stolen to analyze the attack.

Types of Honeypot Deployments

There are three types of honeypot deployments that permit threat actors to perform different levels of malicious activity:

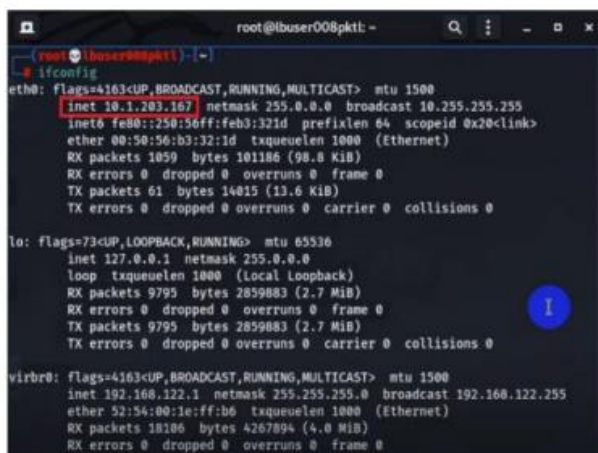
- **Pure honeypots**—complete production systems that monitor attacks through bug taps on the link that connects the honeypot to the network. They are unsophisticated.
- **Low-interaction honeypots**—imitate services and systems that frequently attract criminal attention. They offer a method for collecting data from blind attacks such as botnets and worms malware.
- **High-interaction honeypots**—complex setups that behave like real production infrastructure. They don't restrict the level of activity of a cybercriminal, providing extensive cybersecurity insights. However, they are higher-maintenance and require expertise and the use of additional technologies like virtual machines to ensure attackers cannot access the real system.

Simulating Honeypot:

1. From the left sidebar, click the **Terminal** icon to open its window.
2. In the **Terminal** window, execute the following command:

```
ifconfig
```

Note: Note down the **inet IP** of the **eth0** router; it will be required later.



```
root@t0user008pkt: -  
(root@t0user008pkt) ~  
# ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 10.1.203.167 netmask 255.0.0.0 broadcast 10.255.255.255  
    inet6 fe80::250:56ff:feb3:321d prefixlen 64 scopeid 0x20<link>  
    ether 00:50:56:b3:32:1d txqueuelen 1000 (Ethernet)  
    RX packets 1059 bytes 101186 (98.8 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 61 bytes 14015 (13.6 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 9795 bytes 2859883 (2.7 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 9795 bytes 2859883 (2.7 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
virbr0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.122.1 netmask 255.255.255.0 broadcast 192.168.122.255  
    ether 52:54:00:1e:ff:b0 txqueuelen 1000 (Ethernet)  
    RX packets 18106 bytes 4267894 (4.0 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0
```

Figure 1: The inet IP address

3. In the **Terminal** window, execute the following commands to manage the directory (**Note:** Execute one command at a time.):

```
1. cd pentbox-1.8/  
2. ./pentbox.rb
```

4. In the **Terminal** window, when asked to select the **Network tools** option, type **2** and press the **Enter** key.
5. In the **Terminal** window, when asked to select the **Honeypot** option, type **3** and press the **Enter** key.
6. In the **Terminal** window, type **2** and press the **Enter** key for manual configuration.
7. In the **Terminal** window, type **443** and press the **Enter** key to open the port.
8. Type the false message as **Caught You!!** and press the **Enter** key.
9. In the **Terminal** window, type **y** and press the **Enter** key to save the log.
10. Press the **Enter** key to save the log file in the default location.
11. In the **Terminal** window, type **n** and press the **Enter** key for not activating the beep sound.

My Reflection:

Honeypots are a useful tool for organizations seeking to improve their cybersecurity posture and protect their systems and data from malicious actors. By setting up decoy systems and luring in attackers, organizations can gain valuable insights into the tactics and tools used by attackers, identify new threats, and track the activity of known threats.

However, honeypots also have their limitations. They are only effective if they are properly configured and maintained, and if they are used as part of a larger cybersecurity strategy. Honeypots can also be resource-intensive, as they require ongoing monitoring and maintenance to ensure they are effective.

Overall, honeypots can be a useful addition to an organization's cybersecurity arsenal, but they should not be relied upon as the sole means of protecting systems and data. A comprehensive and proactive approach to cybersecurity, including measures such as strong passwords, regular software updates, and employee training, is essential for effectively protecting against cyber threats.

References:

<https://www.imperva.com/learn/application-security/honeypot-honeynet/>

https://www.kau.edu.sa/files/611/researches/54209_24619.pdf