

CET139 – Emerging Technologies

Honeypot Technologies

A short history and introduction



**University of
Sunderland**

Dr Neil Eliot / Mr Adam Robson

neil.eliot@sunderland.ac.uk / adam.robson@sunderland.ac.uk

Learning Outcomes

- To:
 - Understand where they came from.
 - Understand why they exist.
 - Understand what types are there.
 - Understand how we use them at the University!

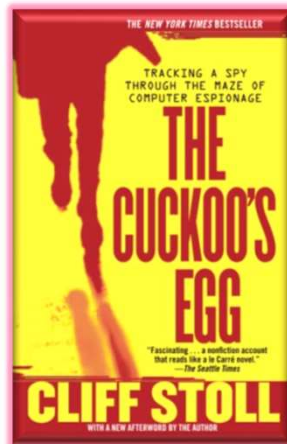
A brief history of honeypots

- Sometimes cybersecurity is described as the same crimes just brought up to date, but what about the technologies we use?
- Consider these:
 - “During the cold war (1947-1991) Russia used ‘Mozhno Girls’ to spy on foreign officials by seducing them.”
 - “honeypot is a cybersecurity mechanism that uses a manufactured attack target to lure cybercriminals.”

Entrapment!

A brief history of honeypots

- The basic idea came from two publications:
 - *The Cuckoo's Egg* (1989 – reissued 2005)
 - *An evening with Breford* (1991)



<https://www.amazon.co.uk/Cuckoos-Egg-Tracking-Computer-Espionage/dp/1416507787>



<http://www.cheswick.com/ches/papers/berferd.pdf>

A brief history of honeypots

- “*The Cuckoos Egg*”
 - Is about the experience of catching a computer hacker who was searching for company secrets.
- “*An Evening with Breford*”
 - Is about how a computer hacker moved through deliberately configured traps set by his colleagues so they could catch them.

In effect “*An Evening with Breford*” is also the first documented case of an **internal threat**!

An **internal threat** refers to the risk of somebody from the inside of a company exploiting a system in a way that causes damage or allows data to be stolen.

So what is a honeypot then?

- Dictionary definition:
 - a container for honey.
 - something which attracts people in great numbers.
 - an attractive ***thing used to lure people into performing a particular action*** or visiting a particular location.

<https://www.crowdstrike.com/cybersecurity-101/honeypots-in-cybersecurity-explained/>

What does ChatGPT have to say?



what is a honeypot



A honeypot is a computer security mechanism that is used to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. Typically, a honeypot consists of a computer, data, or a network site that appears to be part of a network, but is actually isolated and monitored, and which seems to contain information or a resource of value to attackers. When someone attempts to access the honeypot, the activity is logged and analyzed, providing information about the attacker's methods and tools, and allowing the organization to improve its security.



<https://openai.com/blog/chatgpt/>

So what is a honeypot then?

- “A honeypot is a cybersecurity mechanism that uses a manufactured attack target to lure cybercriminals away from legitimate targets. They also gather intelligence about the identity, methods and motivations of adversaries.”

This definition covers both types of honeypots!

There's more than one type!

- Currently honeypot technologies fall into two broad categories:
 - Production Honeypots
 - High interaction
 - Medium interaction
 - Low interaction
 - Research Honeypots
 - Pure
 - High interaction



Commercial organisations

A magenta arrow points from the 'Production Honeypots' category to this box.



Educational and Cybersecurity organisations

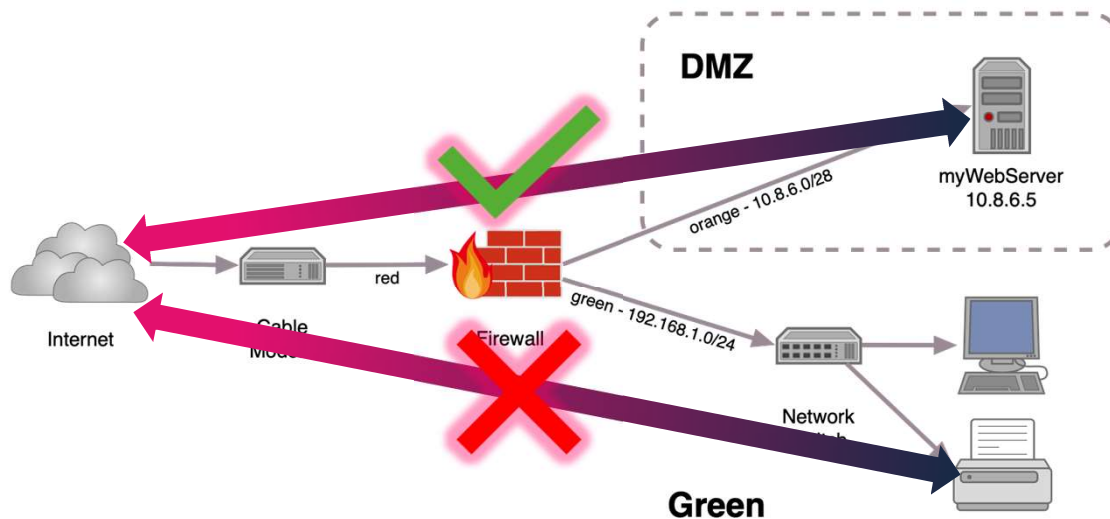
A magenta arrow points from the 'Research Honeypots' category to this box.

Production honeypots

- High interaction can be:
 - Fully functional scaled down version of a system with fake data.
 - Deployed into a live environment (not quite).
 - A demilitarized zone of a network (DMZ).
 - This is usually implemented via a firewall.
 - Used to distract attackers from the live systems.
 - Usually an automated bot.

Production honeypots

- What is a demilitarized zone (DMZ)?
 - It's a section of a network that is segregated from the internal networks and systems and is usually used for public facing services.



DIRECTED LEARNING:

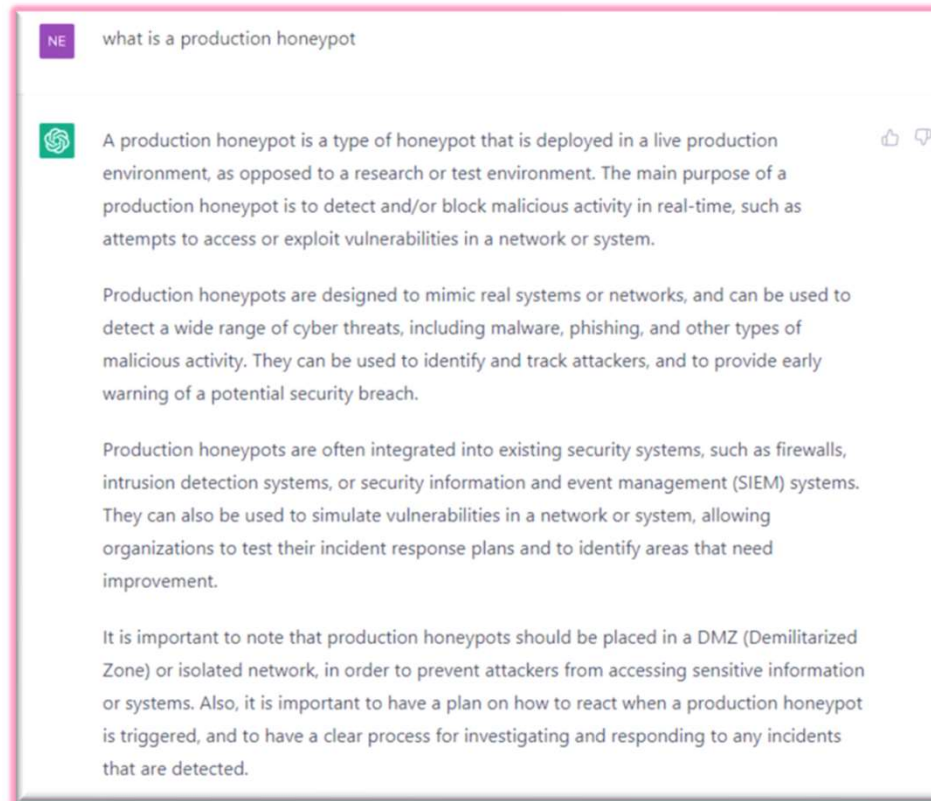
What are the red, orange, green, yellow, blue zones with respect to firewall technology configurations?

<https://wiki.ipfire.org/configuration/firewall/rules/dmz-setup>

Production honeypots

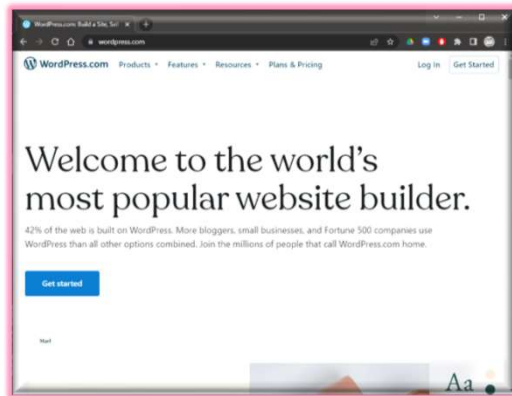
- Low/Medium interaction
 - Usually simulate services and applications rather than being the actual.
 - Limited number of services per pot.
 - Web e.g. Wordpot
 - Small
 - Small scale servers with limited capacity and speed.
 - Specifically designed to log activity.
- Medium/High
 - Usually simulate services and applications rather than being the actual.
 - Multiple services per pot i.e. more general purpose.
 - Cowrie

What does ChatGPT have to say?



Lets have a little look at wordpot

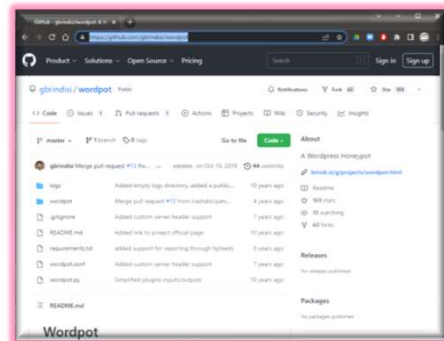
- Firstly, what is **Wordpress**.
 - **Wordpress** is an extensible framework for developing websites based on themes and plugins which requires minimal knowledge of web development and allows the user to concentrate on the content and functional requirements.
 - They claim 42% of the web uses **WordPress!**



<https://wordpress.com/>

Lets have a little look at wordpot

- **Wordpot** is a **Wordpress** honeypot which detects probes for plugins, themes, timthumb (image resizing script) and other common files used to fingerprint a **Wordpress** installation.
- **Wordpot** isn't an installation of **Wordpress**. It mimics a **Wordpress** installation and logs the activity when it is being access.
- It is an adopted component of **Kali Linux**.



<https://github.com/gbrindisi/wordpot>
<https://www.kali.org/>

Lets have a little look at wordpot

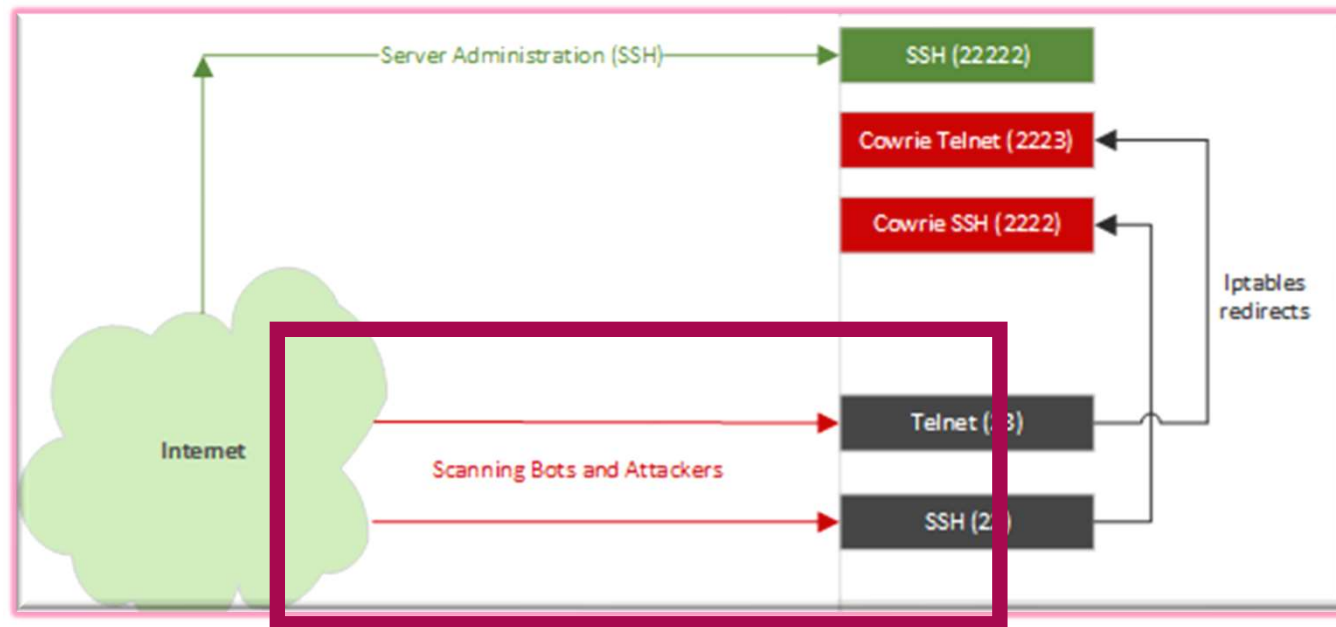
```
Honeypot started on 10.5.14.10:8080
10.5.14.1 probed for the admin panel with path: /
10.5.14.1 probed for the login page
10.5.14.1 tried to login with username test and p
10.5.14.1 tried to login with username  and passw
10.5.14.1 tried to login with username asdf and p
10.5.14.1 tried to login with username asdf and p
10.5.14.1 tried to login with username asf and pa
10.5.14.1 tried to login with username sdf and pa
10.5.14.1 tried to login with username sdf and pa
10.5.14.1 tried to login with username test123 an
10.5.14.1 tried to login with username test and p
10.5.14.1 tried to login with username test and p
10.5.14.1 probed for the admin panel with path: /
10.5.14.1 probed for the login page
10.5.14.1 tried to login with username uitm and p
10.5.14.1 tried to login with username efwegwteg
10.5.14.1 tried to login with username qewrwqerqw
10.5.14.1 tried to login with username qwerq and
10.5.14.1 tried to login with username qwerqw and
```


Lets have a little look at cowrie

- Cowrie is a medium to high interaction SSH and Telnet honeypot designed to log brute force attacks and the shell interaction performed by the attacker.
 - In medium interaction mode (shell) it emulates a UNIX system in Python.
 - In high interaction mode (proxy) it functions as an SSH and telnet proxy to observe attacker behaviour to another system.

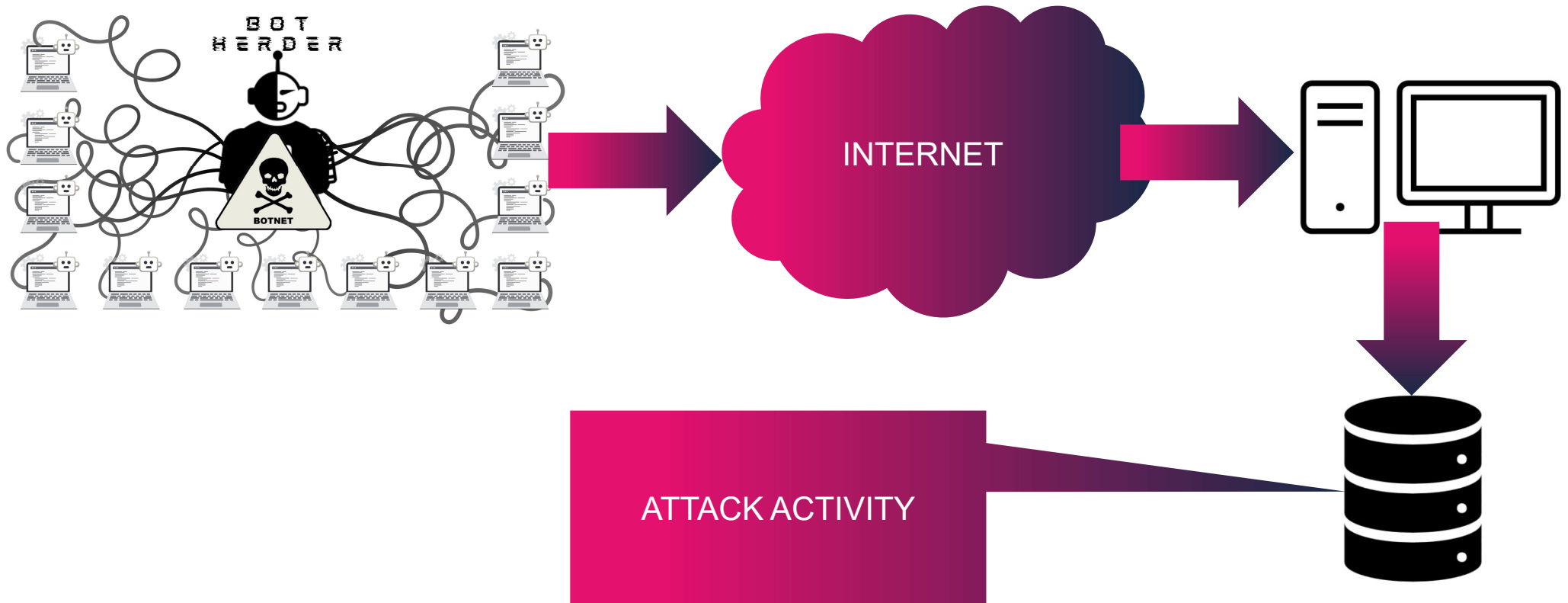
<https://github.com/cowrie/cowrie>

Lets have a little look at cowrie

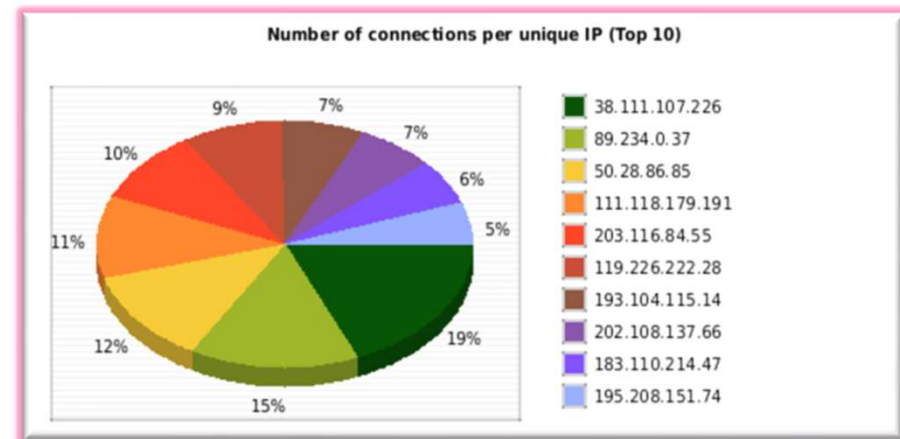
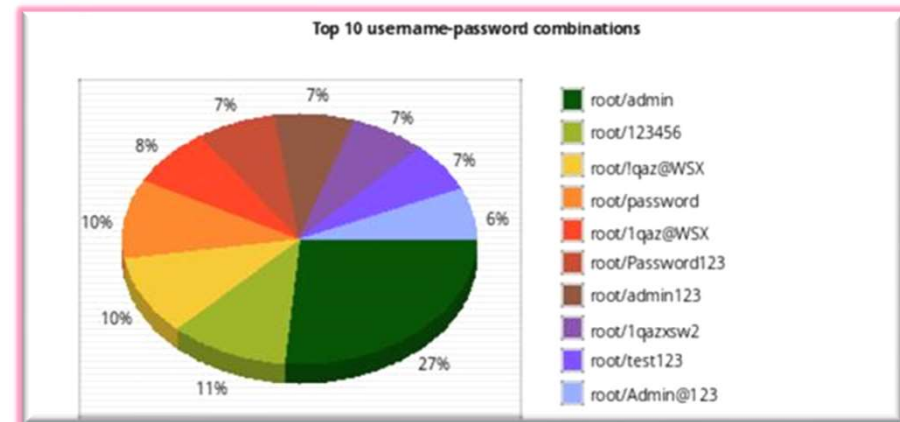
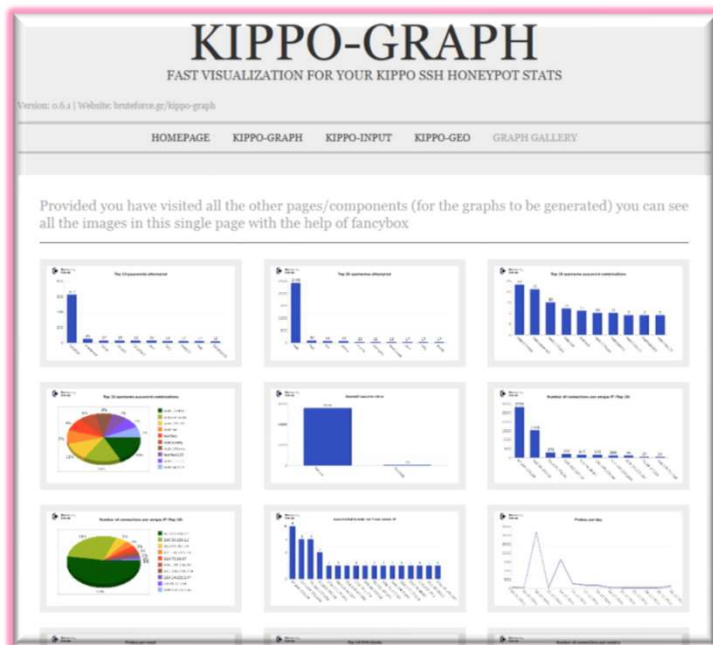


<https://cowrie.readthedocs.io/en/latest/index.html>

Lets have a little look at cowrie



Lets have a little look at cowrie

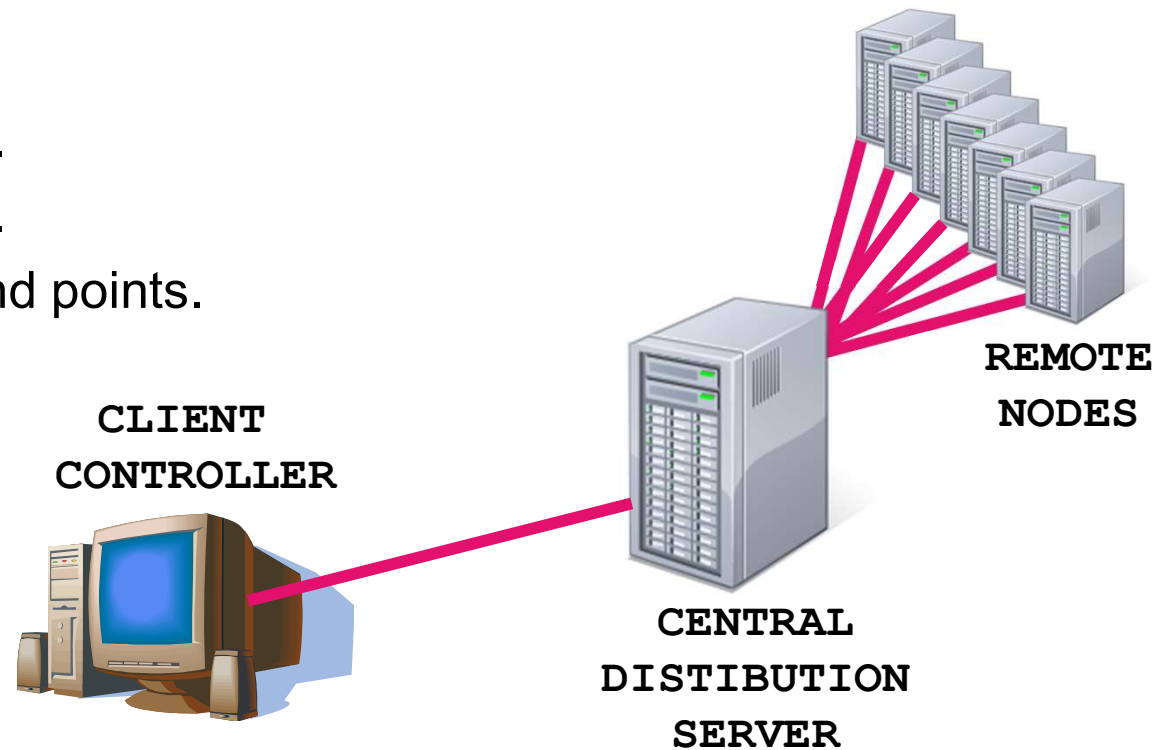


Lets have a little look at cowrie



How do we scale them up?

- Honey Nets
 - Central Controller.
 - Distributed nodes.
 - Low interaction end points.



<https://github.com/pwnlandia/mhn>

Research honeypots

- Small scale version of a generic infrastructure.
- Extensible so as to allow additional services and applications to be implemented.
- Purpose is to allow researches to analyse attack types.
- Generally deployed into a sandboxed laboratory environment.
 - Can be standalone or limited internet access.
- Usually very insecure to allow complete analysis of attacks and attack tools.

What does ChatGPT have to say?

NE


what is a research honeypot






A research honeypot is a type of honeypot that is specifically designed for the purpose of research and studying various types of cyber threats, such as malware, phishing, or other types of malicious activity. Research honeypots are set up to mimic real systems or networks and are used to collect data and information about the methods, techniques, and tools that attackers use to gain unauthorized access. The data collected by research honeypots can be used to improve security and threat detection systems, as well as to develop new security strategies and countermeasures. Research honeypots can also be used to study the behavior of attackers, such as which vulnerabilities they tend to exploit, and to identify trends in the types of attacks that are occurring.



What does ChatGPT have to say?

 draw a diagram of a research honeypot



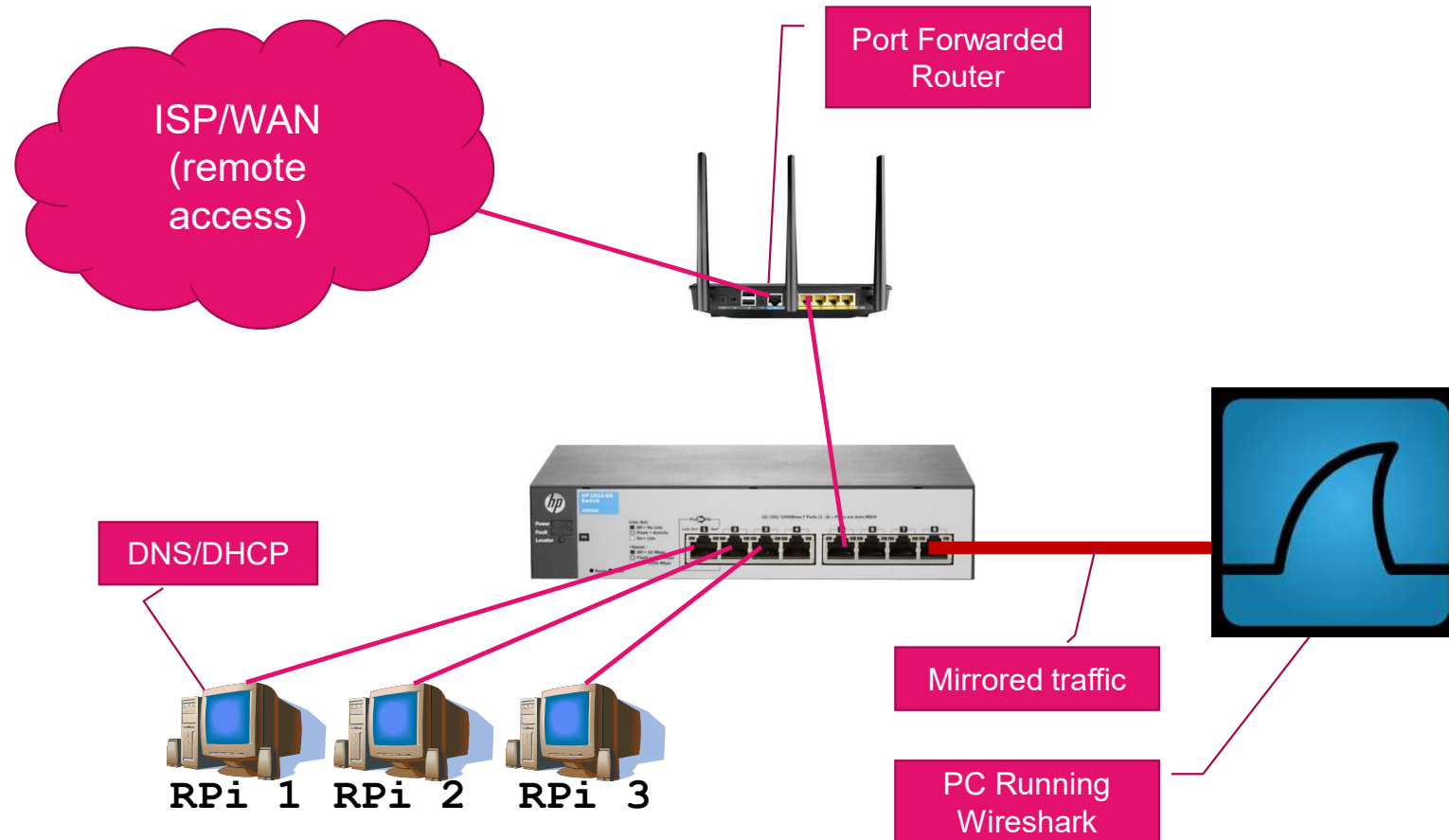
I am sorry, as a language model AI, I am not able to draw a diagram. However, I can describe  

the general architecture of a research honeypot.

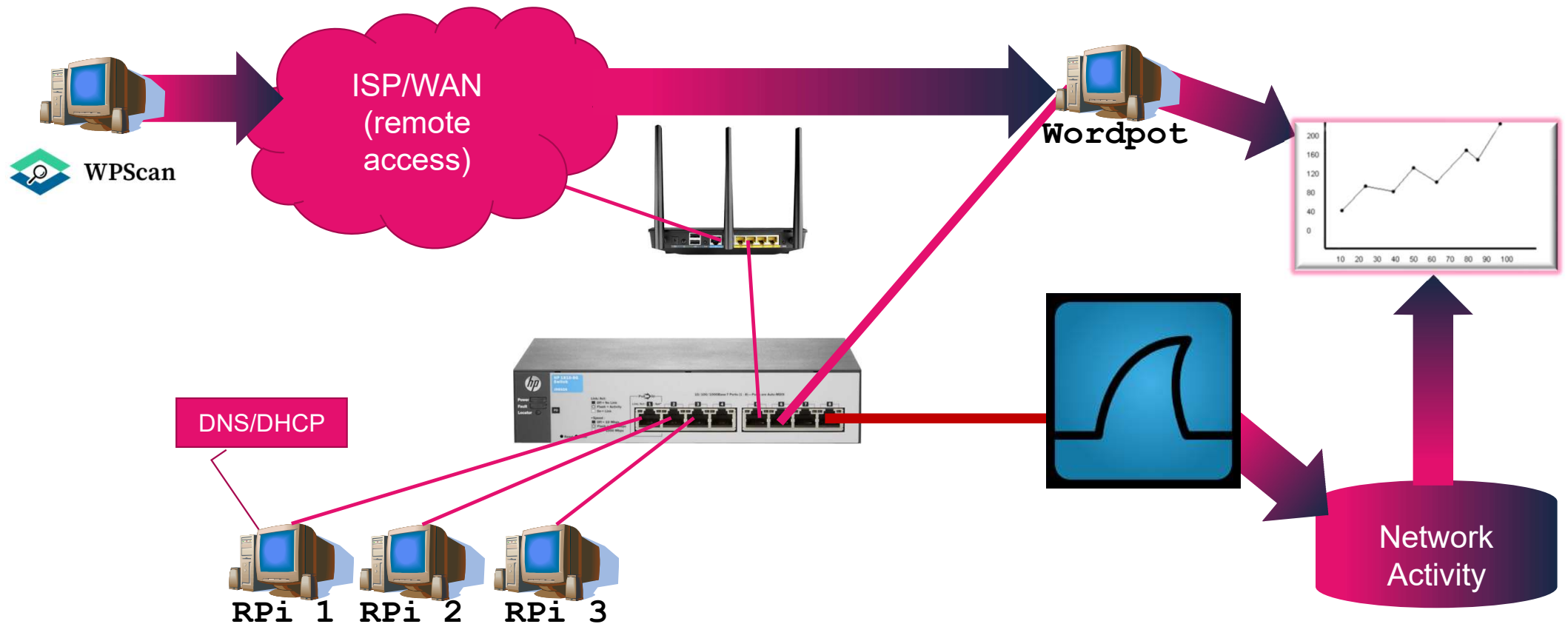
A typical research honeypot architecture includes several components:

1. The honeypot itself: This is the system or network that is set up to mimic a real environment and attract attackers. It may consist of one or more virtual machines or servers.
2. The monitoring system: This component is responsible for collecting data on the activity that occurs on the honeypot, such as traffic logs, system logs, and other types of data. This data is then analyzed to identify patterns or signs of malicious activity.
3. The data collection system: This component is responsible for storing and organizing the data that is collected by the monitoring system. This data can be used for further analysis and research.

Generalised research honeypot



Generalised research honeypot



What do we use hear at the University

- Virtualised research honeypots (VMWare)



- Physical small scale research honeypots (RPi Clusters)



Summary

- To:
 - Understand where they came from.
 - Understand why they exist.
 - Understand what types are there.
 - Understand how we use them at the University!

Now you need to do some research!