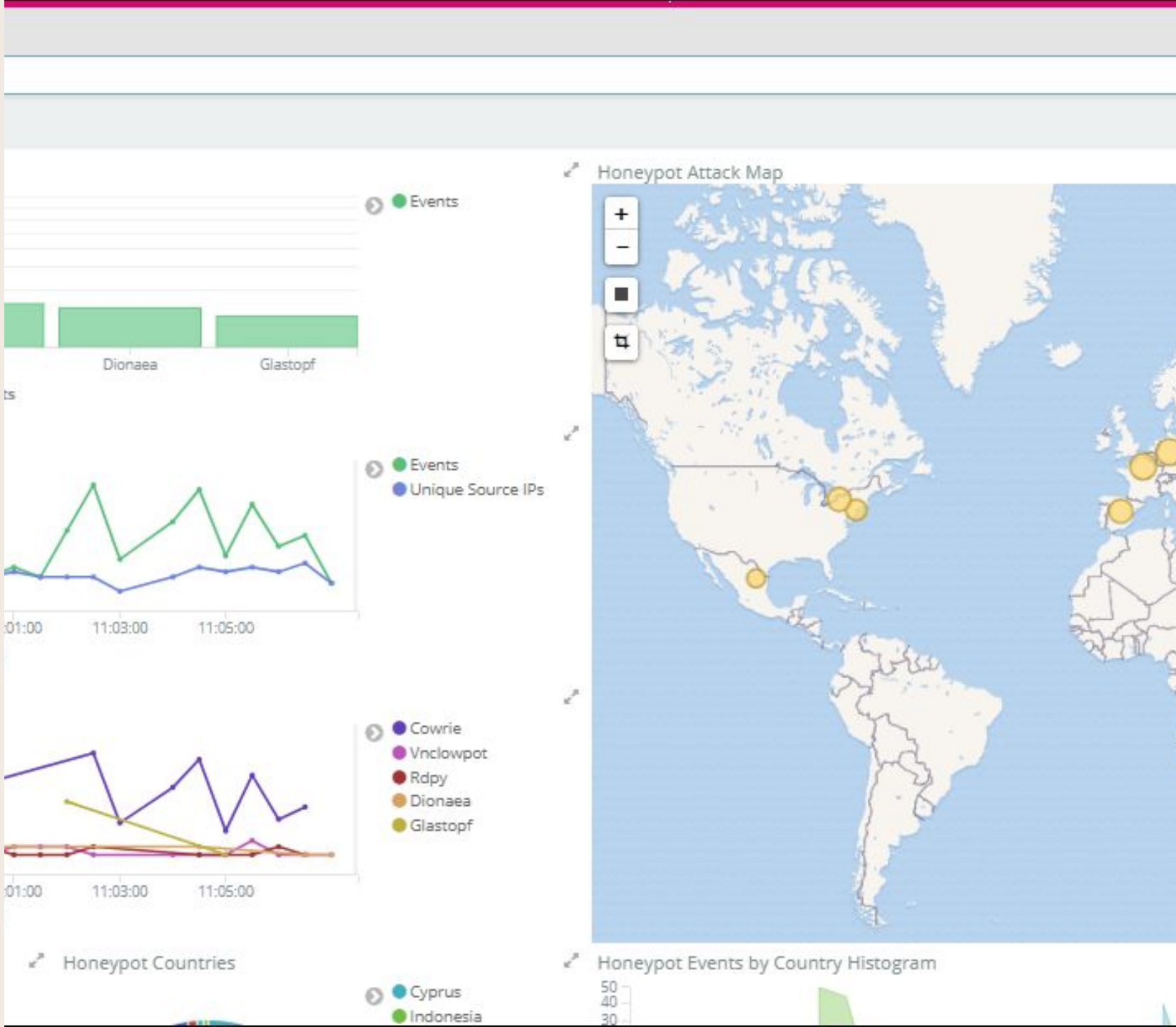
PERJASA SESSION 2021

Analisa Kaedah Serangan Siber Menggunakan Honeypot

CONTENT

- What is honeypot
- Honeynet
- What is T-Pot
- T-Pot Components / Sensor
- How it work
- System Placement
- Demo



WHAT IS HONEYPOT

- Definition:
  - Computer term: (Wikipedia) – is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. Consist of data seem legitimate and contain valuable resource to attackers but actually isolated and monitored.(“baiting”).

- Purposes:
  - Admin can watch the attacker exploit the vulnerabilities of the system, learning where the system has weakness that need to be redesigned.
  - Attacker can be caught and stop while trying to obtain access to the system.
  - Studying the hackers/attackers activities, developer/designers can better create more secure system that are potentially vulnerable in the future.

WHAT IS HONEYPOT

- 2 categories Honeypot type:
  - **Production** – is one used within an organization's environment to help mitigate the risk.
    - To assist an organization in protecting its internal IT Infrastructure.
    - Help to reduce the risk and secure the organization by policing its IT environment to identify attack.
    - The implementation and deployment are relatively easy
    - Are like the police.
  - **Research** – add value to research in computer security by providing a platform to study the threat
    - Implementation and deployment are complex.
    - Design to collect as much information as possible about the attackers/hackers and their activity
    - Primary task – to research the threat organization may face.
    - Are like CSI (the police intelligence counterpart)

WHAT IS HONEYPOT

- 3 Honeypot classification:
  - **Low-interaction honeypots (LiH)**
    - The easiest to install, configure, deploy and maintain – simple design and basic functionality.
    - Emulate variety of services and have the lowest level of risk.
    - Emulate several running services like telnet, SSH, FTP – honeypot capture and collect the login attempt but there is no real operating system for attacker to logon.
  - **Medium-interaction Honeypot (MiH)**
    - More advanced than **LiH.**
    - Also do not have real operating system
    - The services provided more sophisticated technically.
    - The risk also increases especially with regards to vulnerability.

WHAT IS HONEYPOT

- **High-interaction honeypots (HiH)**
  - A complex solution and involve the deployment of real operating system and applications.
  - Capture extensive amount of information.
  - Allowing attacker/hackers to interact with real system – full extent of their behavior can be studied and recorded.
  - E.g : Honeynets and Sebek.
  - Time consuming to design, manage and maintain.
  - Posses a huge risk but the information and evidence gathered for analysis is very large.
  - What we can learn – tools that hackers use, exploits type, vulnerability they love to exploit, hackers/attackers knowledge (the way they surfing their way through operating system and how they interact with the system.

WHAT IS HONEYPOT

- Honeypot & Function: (https://github.com/paralax/awesome-honeypots)
  - **Low-interaction honeypots (LiH)**
    - Honeyd (2003) – simple network emulation tools (evolved to Nepenthes)
    - Dionaea – capture attack payload and malware (Nepenthes successor)
    - Glastopf – Web attack (port 80)
    - Conpot – SCADA/ICS systems
    - Thug – crawl and evaluate potentially malicious web sites.
  - **Medium-interaction Honeypot (MiH)**
    - MultiPot – capture shellcode and payload (listening on multiple vulnerable and backdoor ports)
    - Mwcollectd – malware collection daemon.
    - Amun (**LiH & MiH)** – vulnerability emulation honeypot.
  - **High-interaction honeypots (HiH)**
    - Sshhipot – MiTM SSH Honeypot

WHAT IS HONEYPOT

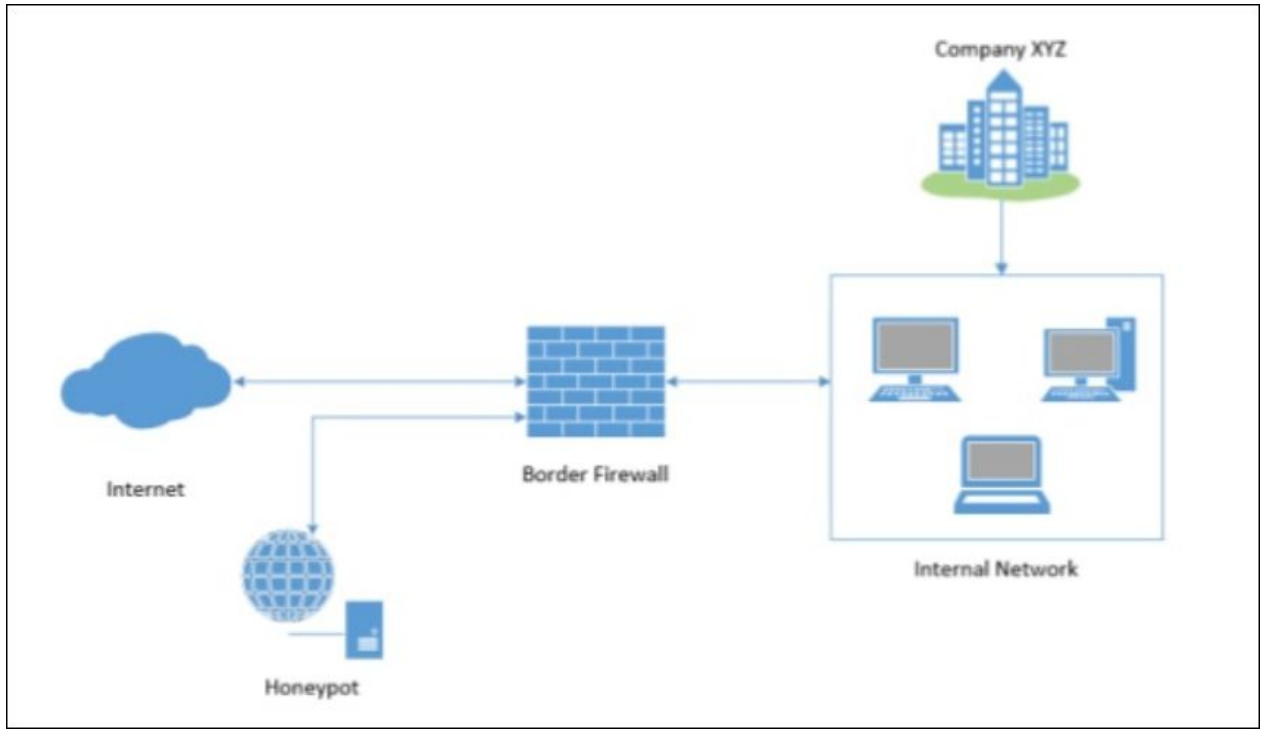
Degree of involvement	Low	Medium	High
Installation and configuration effort	Easy	Medium	Difficult
Deployment and maintenance effort	Easy	Medium	Difficult
Information Gathering	Limited	Medium	Extensive
Level of Risk	Low	Medium	High

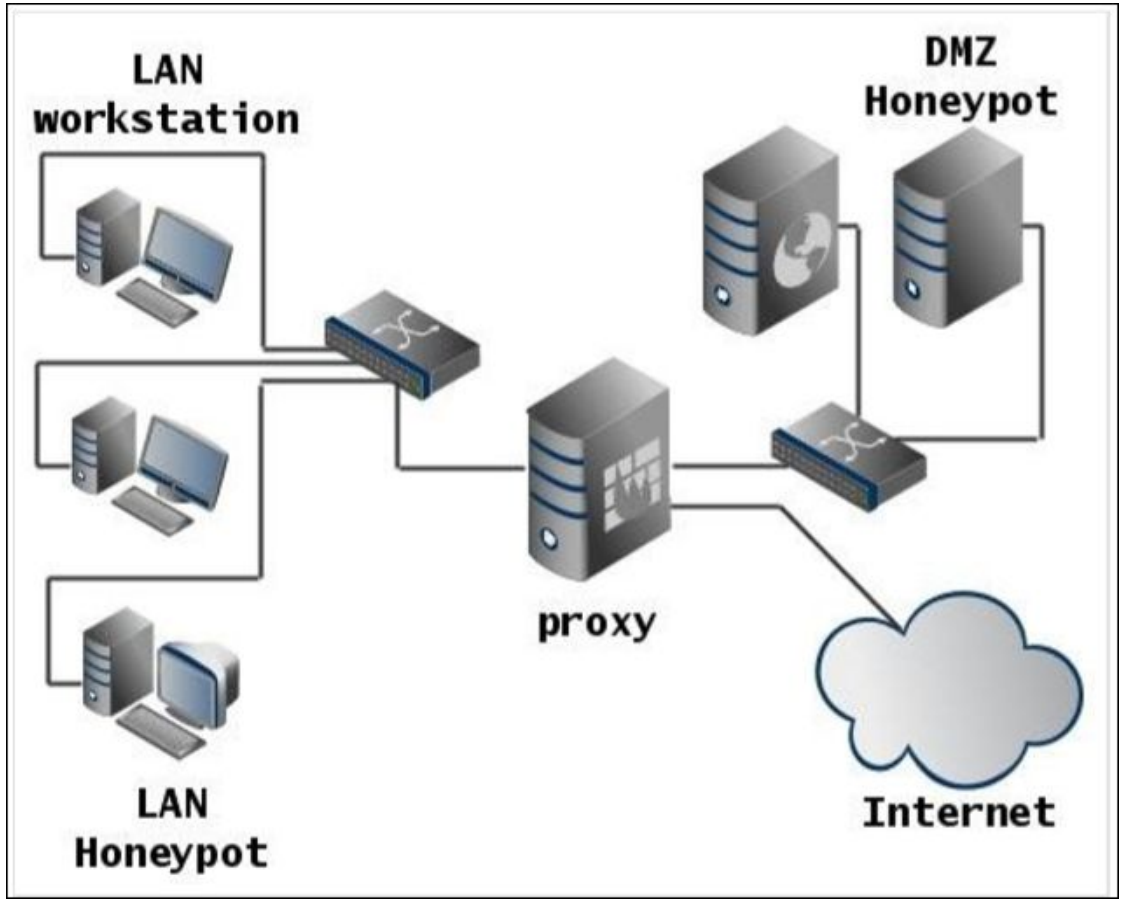
HONEYPOT : ADVANTAGES & DISADVANTAGES

- **Advantages:**
- Focused (small data sets)
- Help reducing false positive
- Help to catch unknown attack (false negative)
- Can capture encrypted activity (e.g Sebek)
- Work with IPv6
- Are very flexible
- Require minimal resources.
- simplicity

- **Disadvantages:**
- Field of view limited (focused)
- Risk (low, medium or high)

HONEYPOT INFRASTRUCTURE





HONEYNET : IS ARCHITECTURE NOT A PRODUCT

- **Definition:**
- 2 or more honeypots on a network
- Used for monitoring a larger and/more diverse network.
- Honeynet & honeypot – as part of larger network intrusion detection systems.
- A honey farm – a centralized collection of honeypots and analysis tool.
- Honeynet concept began in 1999 – when Lance Spitzner (Honeynet Project Founder) published the paper "To build a honeypot".

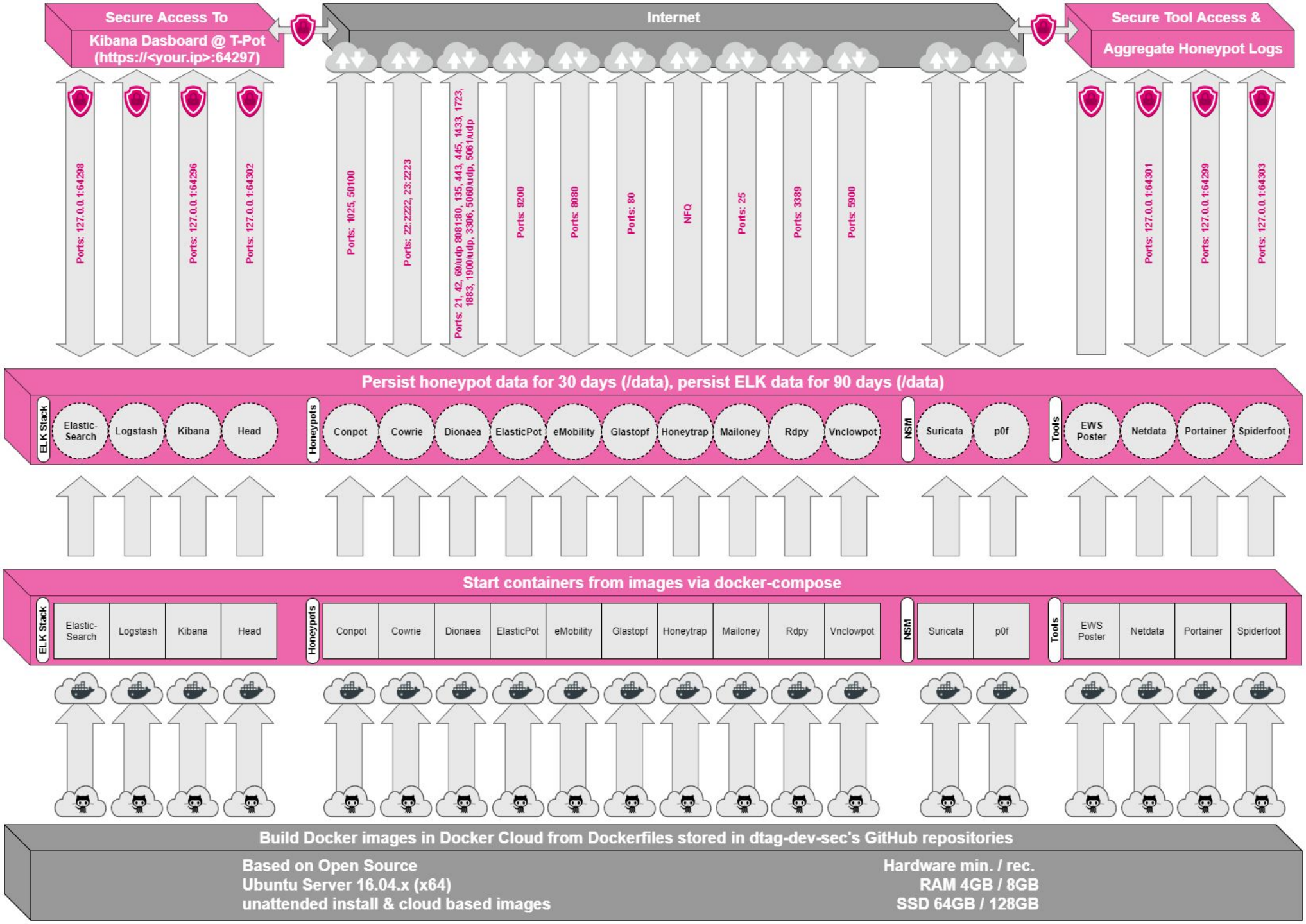
- **How it's works:**
- Monitoring, capturing and analyzing all the packet entering or leaving through networks
- All traffic is entering or leaving through the Honeynet is naturally suspect.
- E.g – Modern Honey Network (MHN) – open source Honeynet Management Platform. (https://threatstream.github.io/mhn/)
- https://hq.honeynet.asia/ui/honeymap/

WHAT IS T-POT

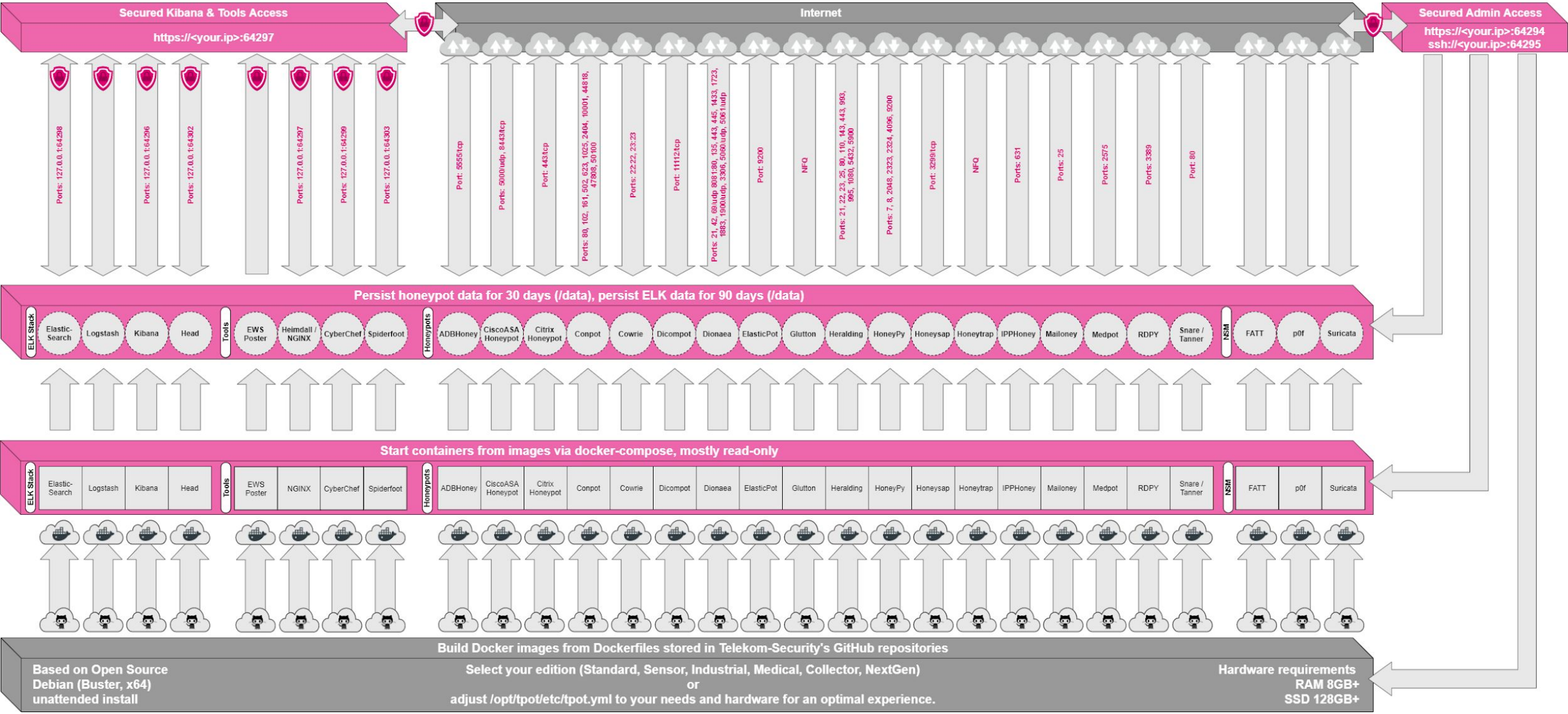
- T-Pot – Multi-Honeypot Platform: - Deutsche Telekom's honeypot project
- http://sicherheitstacho.eu/start/main (community data submission)
  - T-Pot is based on Ubuntu Server (T-Pot 17.10 runs on 16.04 LTS)
    - T-Pot 20.06 runs on Debian (Stable)
  - Honeypot daemons and support component have been paravirtualized using docker and docker-compose.
    - Allow developers to run multiple honeypot daemon on the same network interface and very low maintenance.
  - Dockerized version of honeypots : conpot, cowrie, Dionaea, elasticpot, emobility, glastopf, honeytrap, mailoney, rdpy and vnclowpot

- Tools:-
  - Suricata – network security monitoring engine
  - ELK stack – visualize all event captured by T-Pot
  - Elasticsearch Head – web front end interaction with ELK Search cluster.
  - Netdata – real-time performance monitoring
  - Portainer – web based UI for docker
  - Wetty – web based SSH Client.
  - Spiderfoot – open source intelligence automation tools.
  - Link - https://dtag-dev-sec.github.io/mediator/feature/2017/11/07/t-pot-17.10.html
    - https://github.com/telekom-security/tpotce

T-POT – ARCHITECTURE



CURRENT - T-POT ARCHITECTURE



T-POT – COMPONENTS / SENSORS

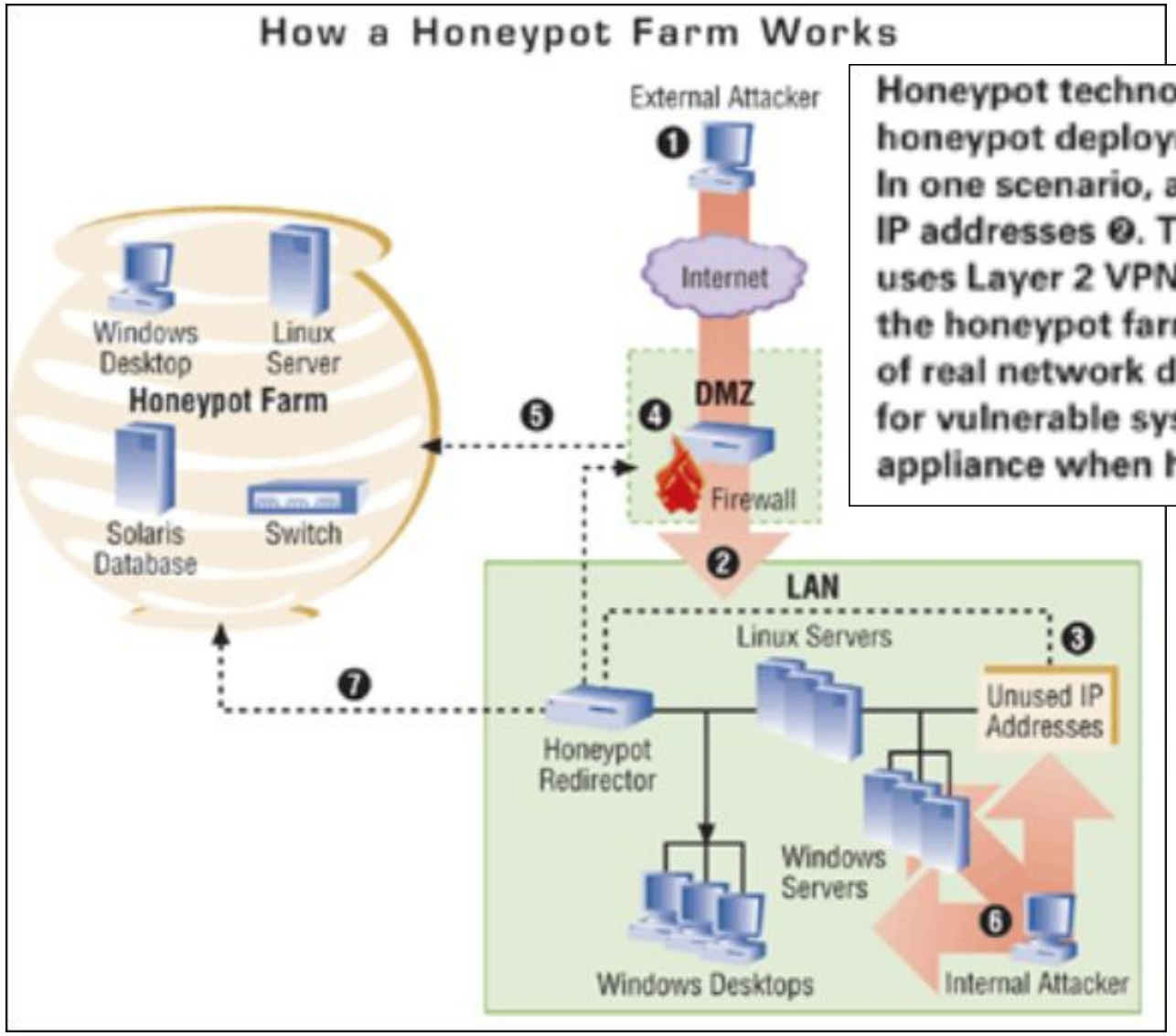
Bil	Sensor	Fungsi / Keterangan
1.	Suricata	Bertindak seperti intrusion detection (IDS), mengesan dan memantau serangan ke atas rangkaian.
2.	Conpot	Analisa ancaman berkaitan dengan system berkaitan infrastruktur industry seperti SNMP, IPMI, SCADA (Port : 81,102,502, 161 (UDP))
3.	Cowrie	Merekodkan serangan brute-force (DDoS) (Port: 22 (SSH))
4.	Dionaea	Perangkap payloads attack, malware, shellcode dan TLS (Port: 21 (FTP), 42 (WINS), 135, 443 (HTTPS), 445 (SMB), 1433 (MSSQL), 3306(MySQL), 5060(SIP), 5061(SIP TLS), 8081(EMC Backup), 69 (TFTP).
5.	Elasticpot	Serangan ke ELK server (Port: 9200)
6.	Emobility	Port 8080, yang selalu digunakan oleh system yang mempunyai antaramuka web untuk kawalan berpusat.
7.	Glastopf	Port 80, memerangkap trafik serangan ke atas laman web.
8.	Honeytrap	Port 25 (SMTP), 110 (Pop3), 139(NetBios Session), 3389 (RDP) 4444 (listener port Oracle WebCenter), 4899(RAT) 5900 (VNC) 21000 (IRTrans)
9.	Mailoney	A low-interaction SMTP honeypot (Port: 25, 465, 587) - https://github.com/awhitehatter/mailoney
10.	Rdpy	A low-interaction RDP (Remote Desktop Protocol) honeypot (https://github.com/citronneur/rdpy)
11.	vnclowport	A low-interaction VNC honeypot. (https://github.com/magisterquis/vnclowpot)

T-POT – CURRENT COMPONENTS / SENSORS

T-POT 20.06 RUNS ON DEBIAN (STABLE)

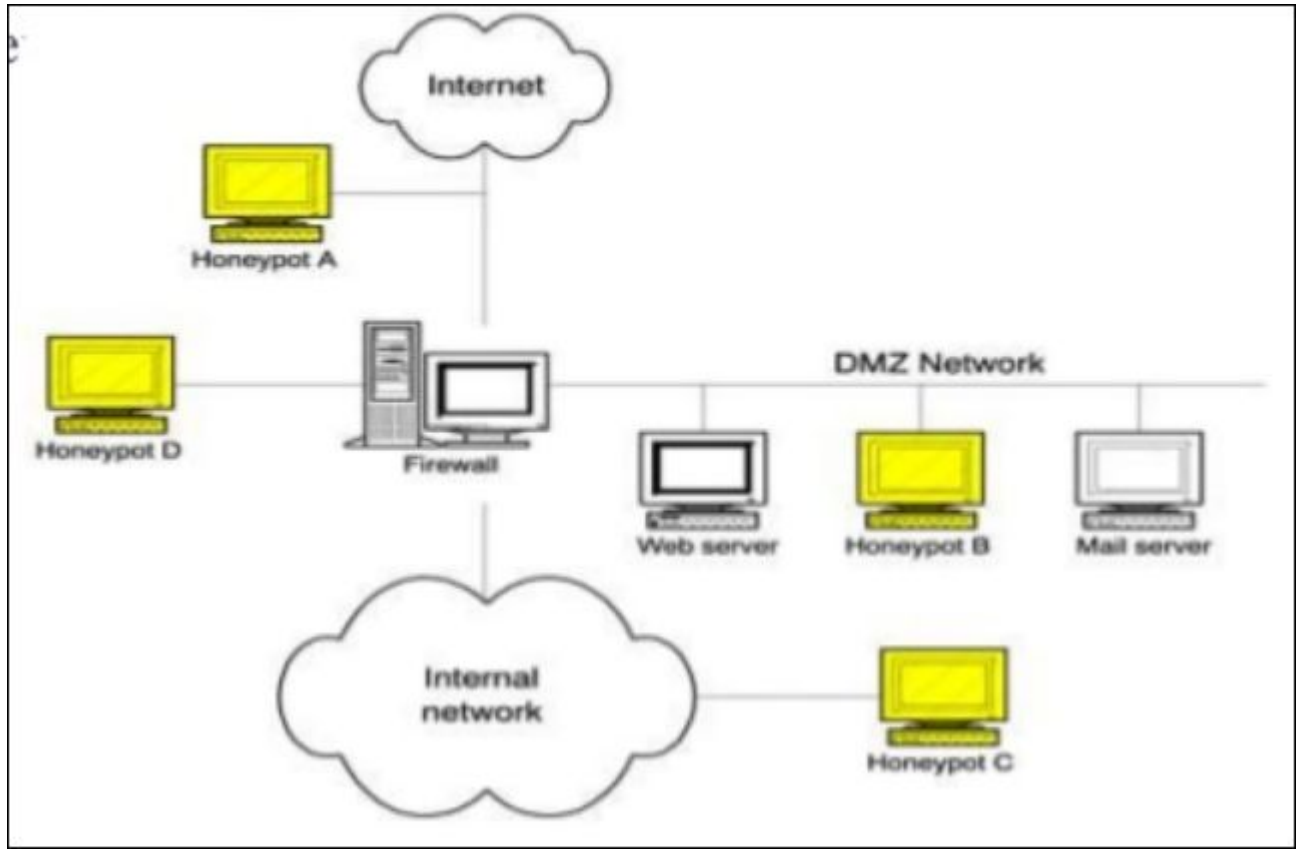
- adbhoney – android debug bridge over TCP/IP
- ciscoasa – CISCO ASA (CVE-2018-0101, a DoS & remote code execution vulnerability)
- citrixhoneypot – detect and log CVE-2019-19781 scan and exploitation attempts
- dicompot – digital imaging and communications in medicine (DICOM) honeypot
- glutton – ssh & TCP Proxy (MITM between attacker and server to log everything in plain text
- heralding – collects crendentials (protocols: ftp, telnet, ssh, http, https, pop3,pop3s, imap, imaps, smtp, vnc, postgresql, socks5)
- honeypy - A low interaction honeypot with the capability to be more of a medium interaction honeypot
- honeysap - low-interaction research-focused honeypot specific for SAP services
- Ipphoney - A honeypot for the Internet Printing Protocol
- Medpot – HL7 FHIR (Fast Health Interoperability Resources) Heatlhcare Interoperability
- Snare / Tanner – web application honeypot sensor (successor of Glastopf)

HOW IT'S WORK



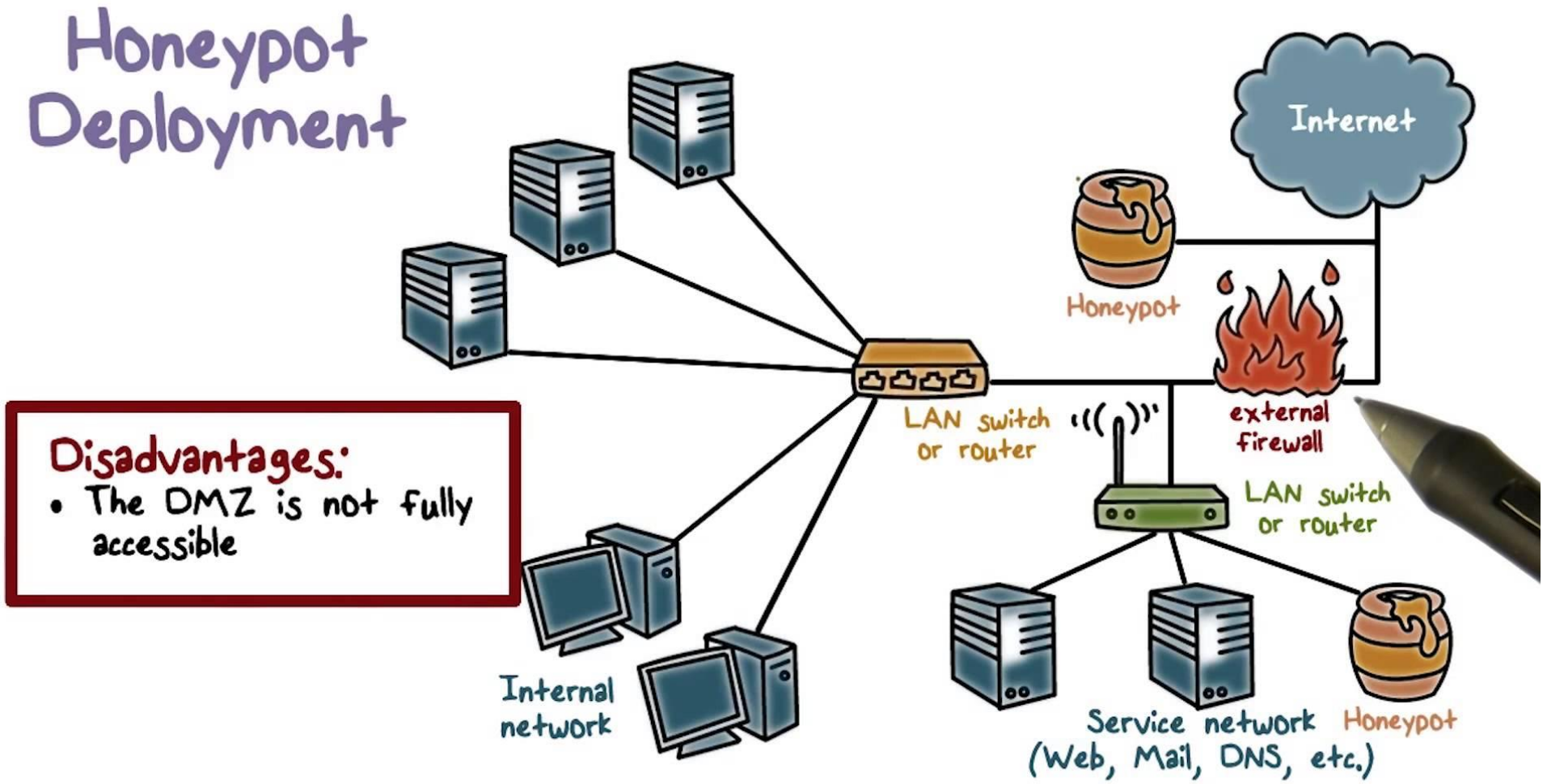
Honeypot technology under development will eventually allow for large-scale honeypot deployments that redirect suspected attack traffic to honeypot farms. In one scenario, an external attacker ❶ penetrates the DMZ and scans network IP addresses ❷. The redirection appliance ❸ monitors all unused addresses, and uses Layer 2 VPN technology to enable the firewall ❹ to redirect the intruder to the honeypot farm ❺, which may have honeypot computers mirroring all types of real network devices. Similarly, an internal attacker ❻, scanning the network for vulnerable systems (such as open file shares) is redirected ❼ by the honeypot appliance when he probes unused IP addresses.

T-POT – SYSTEM PLACEMENT



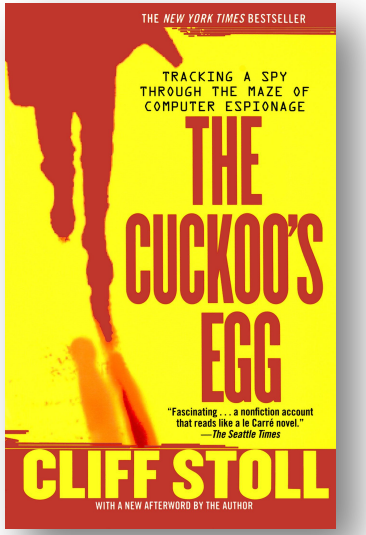
- Reachable through the Internet (if not then will capture internal network only)
- In front of the Firewall (Internet)
- DMZ (De-militarized Zone)
- Behind the firewall (NAT) – Internal & External
- multi-VLAN : put sensor on every VLAN and push log to main (master).

T-POT – SYSTEM PLACEMENT



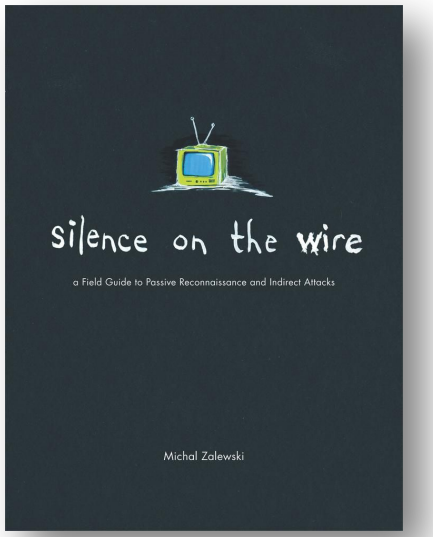
BOOKS

- The Cuckoo's Egg: Tracking A spy through the maze of computer espionage – Cliff Stoll (2005)



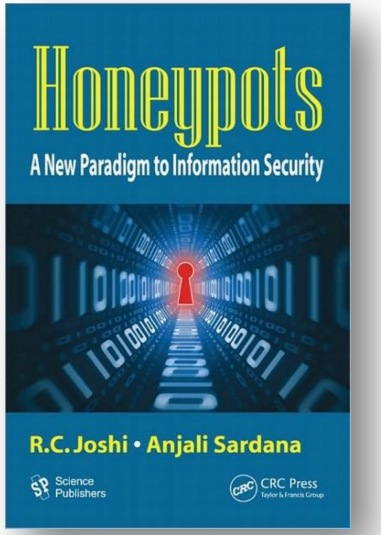
- Silence on the wire: A Field Guide to Passive Reconnaissance and Indirect Attack –

  Michal Zalewski (2005)



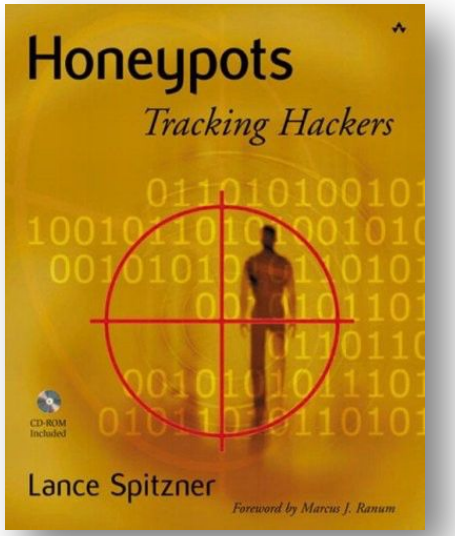
- Honeypot: A New Paradigm to Information Security –

  R.C Joshi & Anjali Sardana (2011)

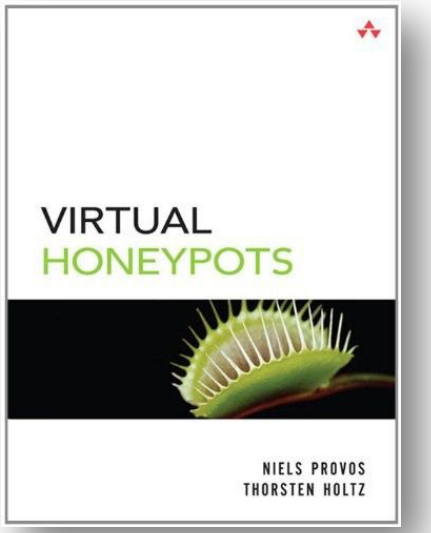


- Honeypot: Tracking Hackers –

  Lance Spitzner (2003)

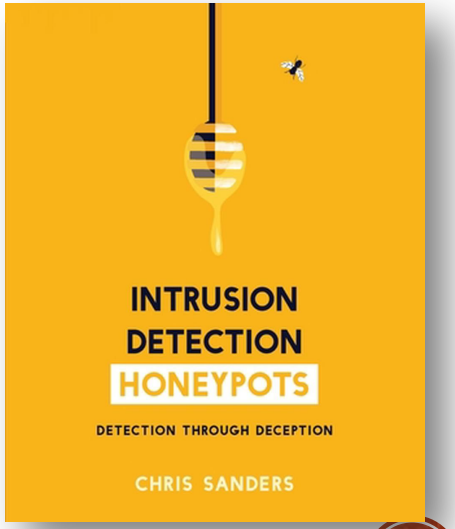


- Virtual Honeypots : From Botnet Tracking to Intrusion Detection (2007)



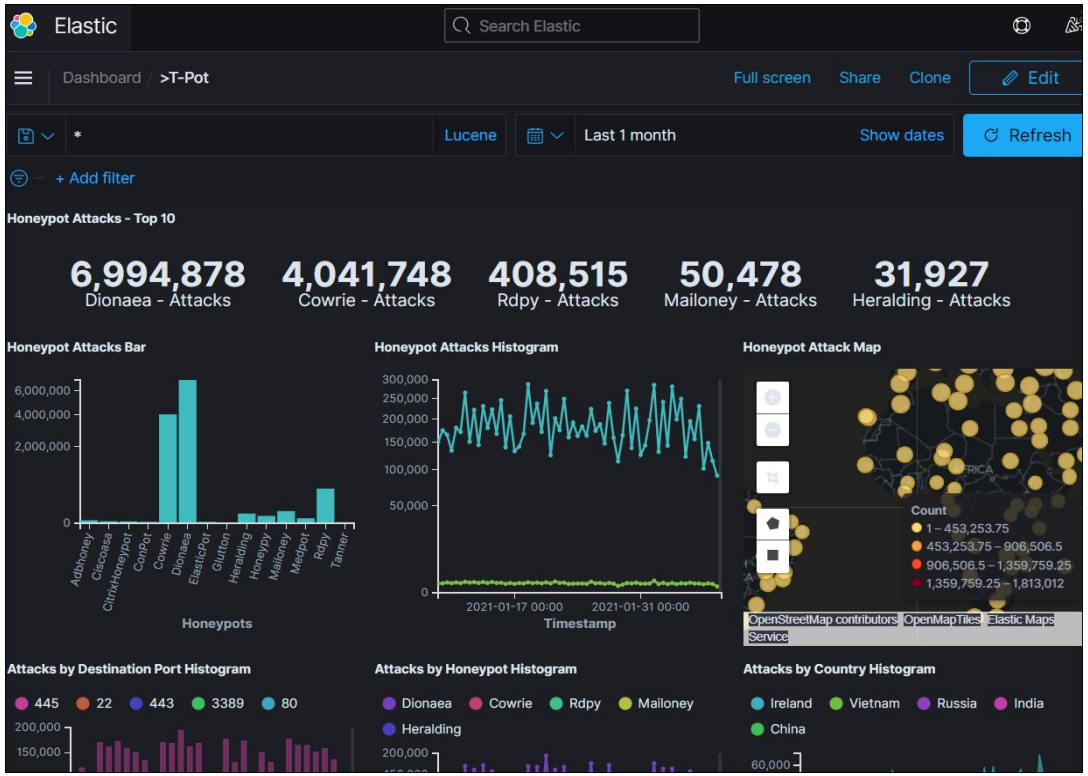
- Intrusion Detection Honeypots: Detection Through Deception –

  Chris Sanders (2020)

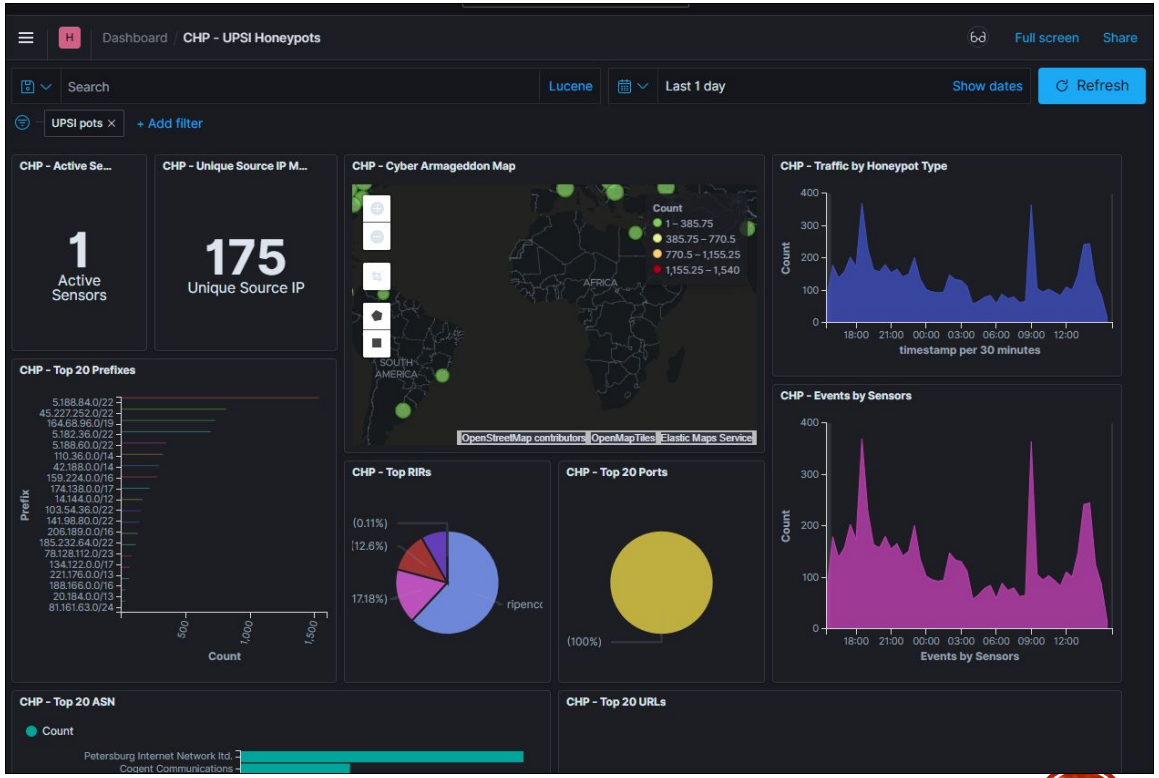


HONEYPOT - UPSI

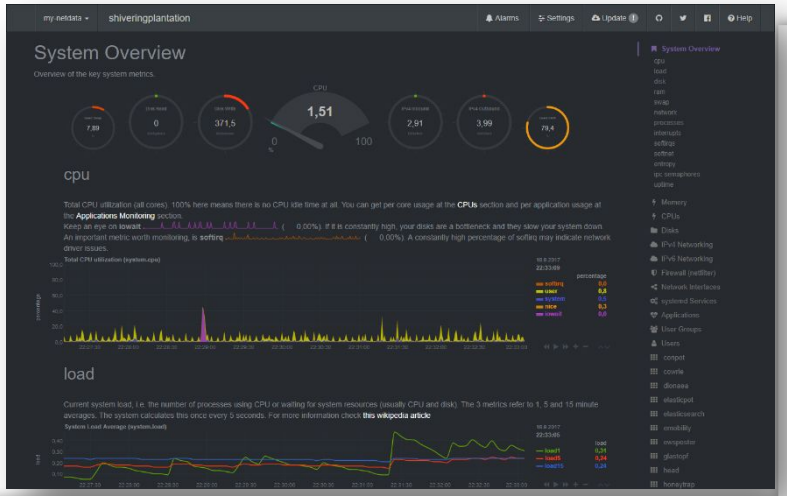
- T-Pot Honeypot Deployment

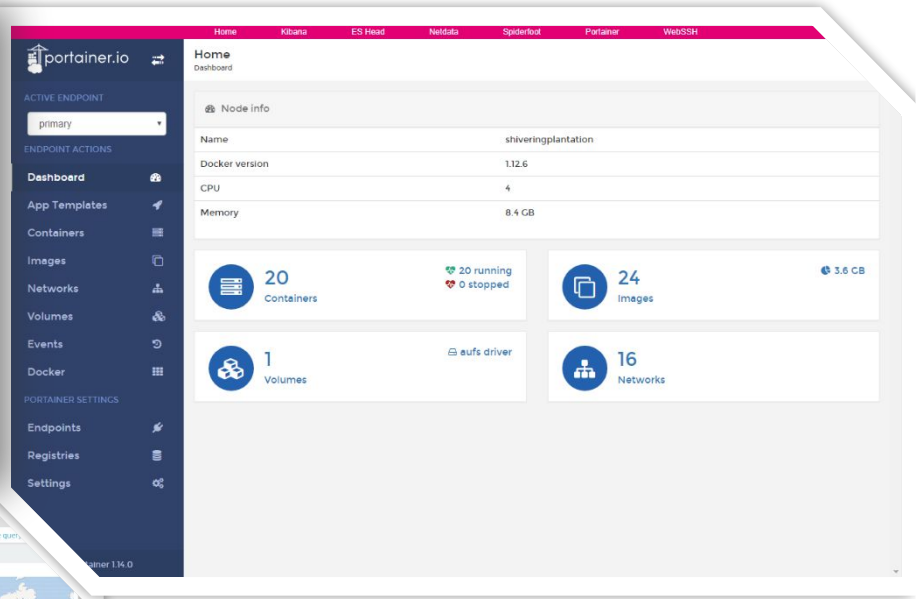


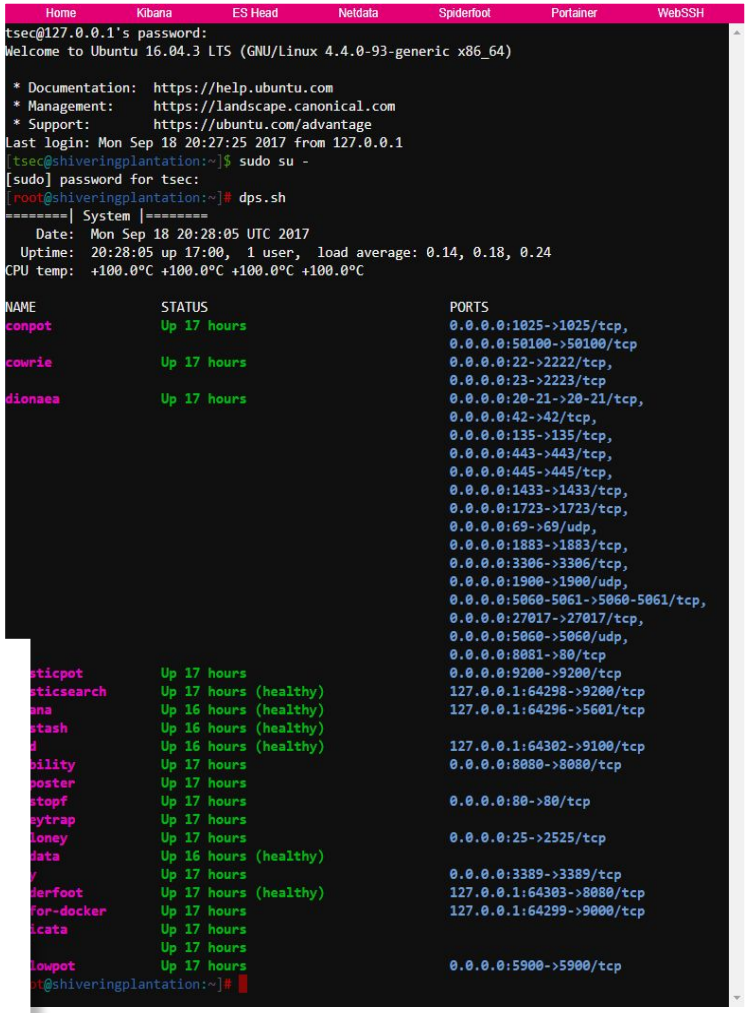
- APNIC Collaboration

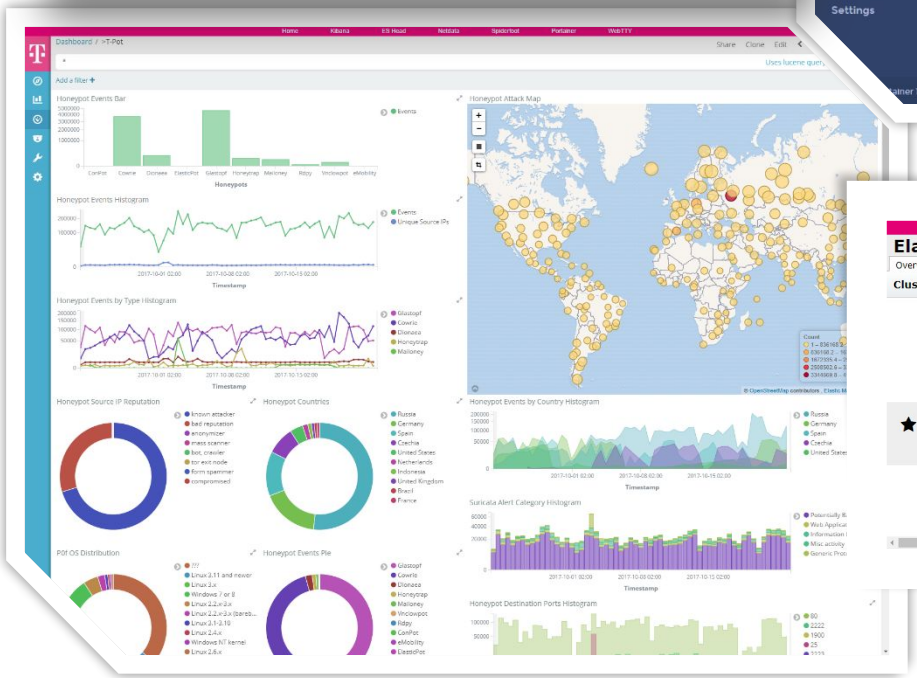


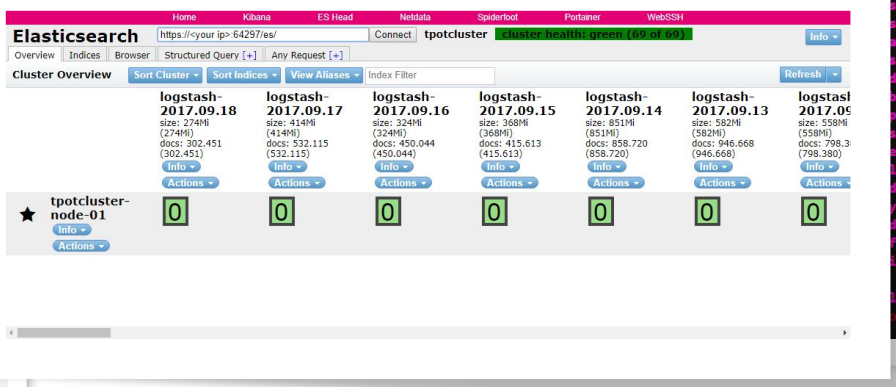
DEMO


my-netdata
shiveringplantation
Alarms
Settings
Update
Help
System Overview
Overview of the key system metrics.
CPU
1,51
cpu
load


Home
Kibana
ES Head
Netdata
Spiderfoot
Portainer
WebSSH
portainer.io
ACTIVE ENDPOINT
primary
ENDPOINT ACTIONS
Dashboard
App Templates
Containers
Images
Networks
Volumes
Events
Docker
PORTAINER SETTINGS
Endpoints
Registries
Settings
Home
Dashboard
Node info
Name
shiveringplantation
Docker version
1.12.6
CPU
4
Memory
8.4 GB
20
Containers
20 running
0 stopped
24
Images
3.6 GB
1
Volumes
aufs driver
16
Networks


Home
Kibana
ES Head
Netdata
Spiderfoot
Portainer
WebSSH
tsec@127.0.0.1's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-93-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
Last login: Mon Sep 18 20:27:25 2017 from 127.0.0.1
[tsec@shiveringplantation:~]$ sudo su -
[sudo] password for tsec:
[root@shiveringplantation:~]# dps.sh
========| System |========
Date: Mon Sep 18 20:28:05 UTC 2017
Uptime: 20:28:05 up 17:00, 1 user, load average: 0.14, 0.18, 0.24
CPU temp: +100.0°C +100.0°C +100.0°C +100.0°C
NAME STATUS PORTS
conpot Up 17 hours 0.0.0.0:1025->1025/tcp, 0.0.0.0:50100->50100/tcp
cowrie Up 17 hours 0.0.0.0:22->2222/tcp, 0.0.0.0:23->2223/tcp
dionaea Up 17 hours 0.0.0.0:20-21->20-21/tcp, 0.0.0.0:42->42/tcp, 0.0.0.0:135->135/tcp, 0.0.0.0:443->443/tcp, 0.0.0.0:445->445/tcp, 0.0.0.0:1433->1433/tcp, 0.0.0.0:1723->1723/tcp, 0.0.0.0:69->69/udp, 0.0.0.0:1883->1883/tcp, 0.0.0.0:3306->3306/tcp, 0.0.0.0:1900->1900/udp, 0.0.0.0:5060-5061->5060-5061/tcp, 0.0.0.0:27017->27017/tcp, 0.0.0.0:5060->5060/udp, 0.0.0.0:8081->80/tcp
ticpot Up 17 hours 0.0.0.0:9200->9200/tcp
sticsearch Up 17 hours (healthy) 127.0.0.1:64298->9200/tcp
ana Up 16 hours (healthy) 127.0.0.1:64296->5601/tcp
stash Up 16 hours (healthy)
d Up 16 hours (healthy) 127.0.0.1:64302->9100/tcp
bility Up 17 hours 0.0.0.0:8080->8080/tcp
poster Up 17 hours
stopf Up 17 hours 0.0.0.0:80->80/tcp
eytrap Up 17 hours
loney Up 17 hours 0.0.0.0:25->2525/tcp
data Up 16 hours (healthy)
Up 17 hours 0.0.0.0:3389->3389/tcp
derfoot Up 17 hours (healthy) 127.0.0.1:64303->8080/tcp
for-docker Up 17 hours 127.0.0.1:64299->9000/tcp
icata Up 17 hours
Up 17 hours
lowpot Up 17 hours 0.0.0.0:5900->5900/tcp
t@shiveringplantation:~]#


Dashboard / >T-Pot
Honeypot Events Bar
Honeypot Attack Map
Honeypot Events Histogram
Honeypot Events by Type Histogram
Honeypot Source IP Reputation
Honeypot Countries
Honeypot Events by Country Histogram
Suricata Alert Category Histogram
P0f OS Distribution
Honeypot Events Pie
Honeypot Destination Ports Histogram


Home
Kibana
ES Head
Netdata
Spiderfoot
Portainer
WebSSH
Elasticsearch
https://<your ip>:64297/es/
Connect
tpotcluster
cluster health: green (69 of 69)
Info
Overview
Indices
Browser
Structured Query [+]
Any Request [+]
Cluster Overview
Sort Cluster
Sort Indices
View Aliases
Index Filter
Refresh
logstash-2017.09.18
size: 274Mi (274Mi)
docs: 302.451 (302.451)
logstash-2017.09.17
size: 414Mi (414Mi)
docs: 532.115 (532.115)
logstash-2017.09.16
size: 324Mi (324Mi)
docs: 450.044 (450.044)
logstash-2017.09.15
size: 368Mi (368Mi)
docs: 415.613 (415.613)
logstash-2017.09.14
size: 851Mi (851Mi)
docs: 858.720 (858.720)
logstash-2017.09.13
size: 582Mi (582Mi)
docs: 946.668 (946.668)
Info
Actions
tpotcluster-node-01
0