

Monitoring Intrusions with HONEYAPPS

Spenser Reinhardt

<https://github.com/honeyappsproject/presentations>



Celebrating a
decade
of guiding
security
professionals.

SECURE360 
conference



@Secure360 or
#Sec360

www.Secure360.com

Who am I?

- Spenser Reinhardt (@c0mmiebstnd)
- Github: commiebstnd \ sreinhartd \ honeyappsproject
- Docker: commiebstnd \ sreinhartd \ honeyappsproject
- Co-Founder \ Lead Developer – Honeyapps
- Lead Developer \ Security Lead – Nagios-Plugins
- Def Con NOC Goon
- Capture the Flag Challenge Creator



Celebrating a decade of guiding security professionals.

SECURE360 
conference



@Secure360 or
#Sec360

www.Secure360.com

HONEYAPPS

Plan of Attack

- Terminology
- Where We've Been
- Where We're Going
- How Do Honeypots Help Improve Security Posture
- How Does HoneyApps Fit in My Org
- Videos



Celebrating a decade of guiding security professionals.

SECURE360 
conference



@Secure360 or
#Sec360

www.Secure360.org

HONEYAPPS

Terminology

Github – Code versioning system and storage

50 commits 8 branches 0 releases 2 contributors

branch: master **Docker-Honeynet** / +

This branch is 35 commits ahead of commiebstrd:master Pull Request Compare

checkins from dev branches, logfile

N sreinhart authored 2 days ago latest commit 35a112c68a

conpot	conpot - more tee testing	2 days ago
dionaea	checkins from dev branches, logfile	2 days ago
glastopf	checkins from dev branches, logfile	2 days ago
honeybrid	checkins from dev branches, logfile	2 days ago
kippo	checkins from dev branches, logfile	2 days ago
scripts	Completing folder cleanup and fork.	2 days ago
templates	Completing folder cleanup and fork.	2 days ago
thug	checkins from dev branches, logfile	2 days ago
README.rdoc	README.rdoc - initializing repo	3 months ago



Celebrating
decade of
geometric
security
prof

Secure360
conference

Terminology

Docker – Containerized application build and deployment

AUTOMATED BUILD REPOSITORY

Updated 2 days, 2 hours ago

sreinhardt / honeynet

Pull this repository

docker pull sreinhardt/honeynet

No description set

☆ 0 💬 0 📦 0

Information

Dockerfile

Build Details

Tags

▶ Start a Build

Build Details

[Edit Build Details](#)

Type	Name	Dockerfile Location	Tag Name
Branch	kippo	/kippo/	kippo-dev
Branch	honeybrid	/honeybrid/	honeybrid-dev
Branch	glastopf	/glastopf/	glastopf-dev
Branch	thug	/thug/	thug-dev
Branch	dionaea	/dionaea/	dionaea-dev
Branch	conpot	/conpot/	conpot-dev
Branch	master	/kippo/	kippo
Branch	master	/honeybrid/	honeybrid

Build Details

[Source Project Page](#)

[Source Repository](#)

Properties

🕒 2014-09-20

15:33:01

👤 sreinhardt

Settings

[Description](#)



Celeb
decad
of gui
secur
profes

CURE360
conference

🐦 @Secure360 or
#Sec360

www.Secure360.

HONEYAPPS

Terminology

Rust

- Modern C\C++ replacement
- Memory safety without garbage collection
- Implicit immutability, explicit mutability
- Rich Typesystem
- Strong functional programming influence

"Rust is a systems programming language that runs blazingly fast, prevents almost all crashes*, and eliminates data races."

* In theory. Rust is a work-in-progress and may do anything it likes up to and including eating your laundry. Control / Performance
Safety C C++ Rust Go Java ML Haskell



Celebrating a
decade
of guiding
security
professionals.

SECURE360 
conference



@Secure360 or
#Sec360

www.Secure360.org

HONEYAPPS

Terminology

Cargo – Automated build and dependency tracker for Rust

docker 0.0.33

About This Package
Docker Remote API binding in Rust

Last Updated
11 days ago

Authors
• [Graham Lee](#)

License
Apache-2.0

Keywords
[docker](#)

Owners
[View](#)

Cargo.toml
`docker = "0.0.33"`

Links
[Homepage](#)
[Documentation](#)
[Repository](#)

Dependencies
[unix_socket](#) *0.3.2
[rustc_serialize](#) *0.3.14
[openssl](#) *0.6.2

Versions
[0.0.33](#) Apr 30, 2015
[0.0.32](#) Apr 29, 2015
[0.0.31](#) Apr 28, 2015
[0.0.30](#) Apr 26, 2015
[0.0.29](#) Apr 26, 2015
[show all 33 versions](#)

Stats Overview

Downloads all time	Versions published
424	33

Showing stats for **All Versions**



Celebrating a decade of guiding security professionals.

SECURE360 
conference



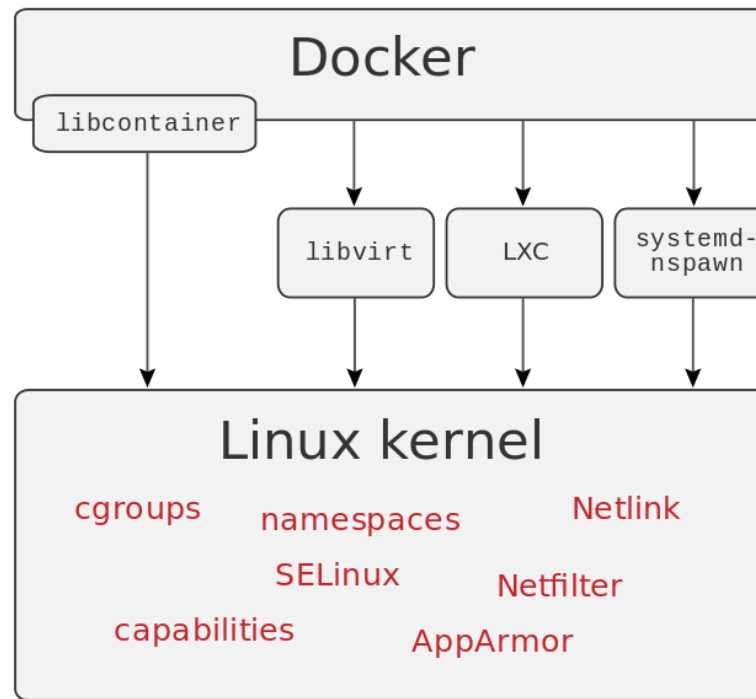
@Secure360 or
#Sec360

www.Secure360.

HONEYAPPS

Terminology

Containers – OS level virtualization and isolation method for deploying applications.



Celebrating a
decade
of guiding
security
professionals.

SECURE360 
conference



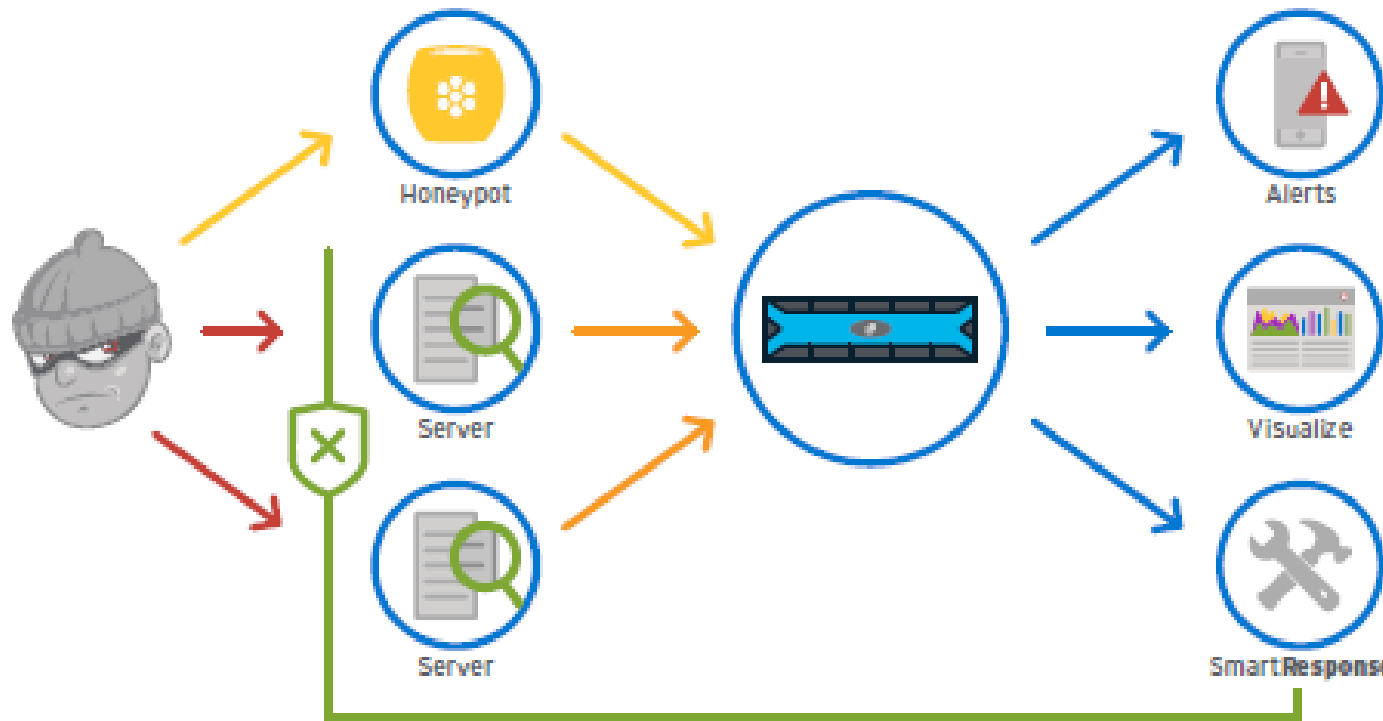
@Secure360 or
#Sec360

www.Secure360.com

HONEYAPPS

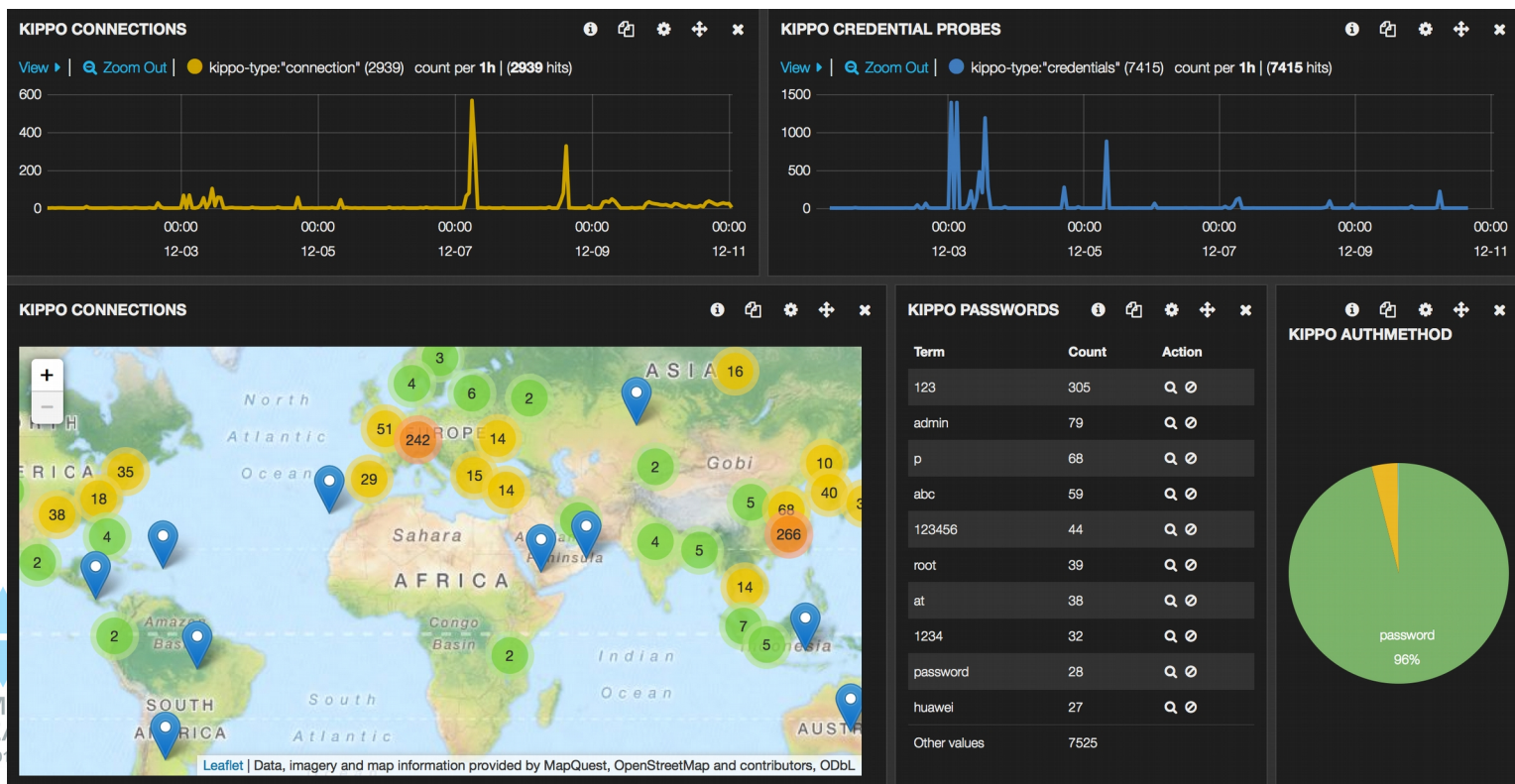
Terminology

Honeytrap - System designed to attract and detect malicious actions and actors.



Terminology

Elk Stack – Centralized log collection and parsing, deep search, and data analytics and visualizations.



@Secure360 or
#Sec360

www.Secure360.

HONEYAPPS



Where We've Been

- Nagios Core – Maintain honeypots, execute remote scripts.
- Nagios Log Server – Retain and visualize attack and log data.
- Nagios Network Analyzer – Capture netflow traffic.
- Docker – Honeypot containment and execution.
- Suricata – Signature based detection of attacks.
- Honeynet Project – Various honeypots.



Celebrating a
decade
of guiding
security
professionals.

SECURE360 
conference

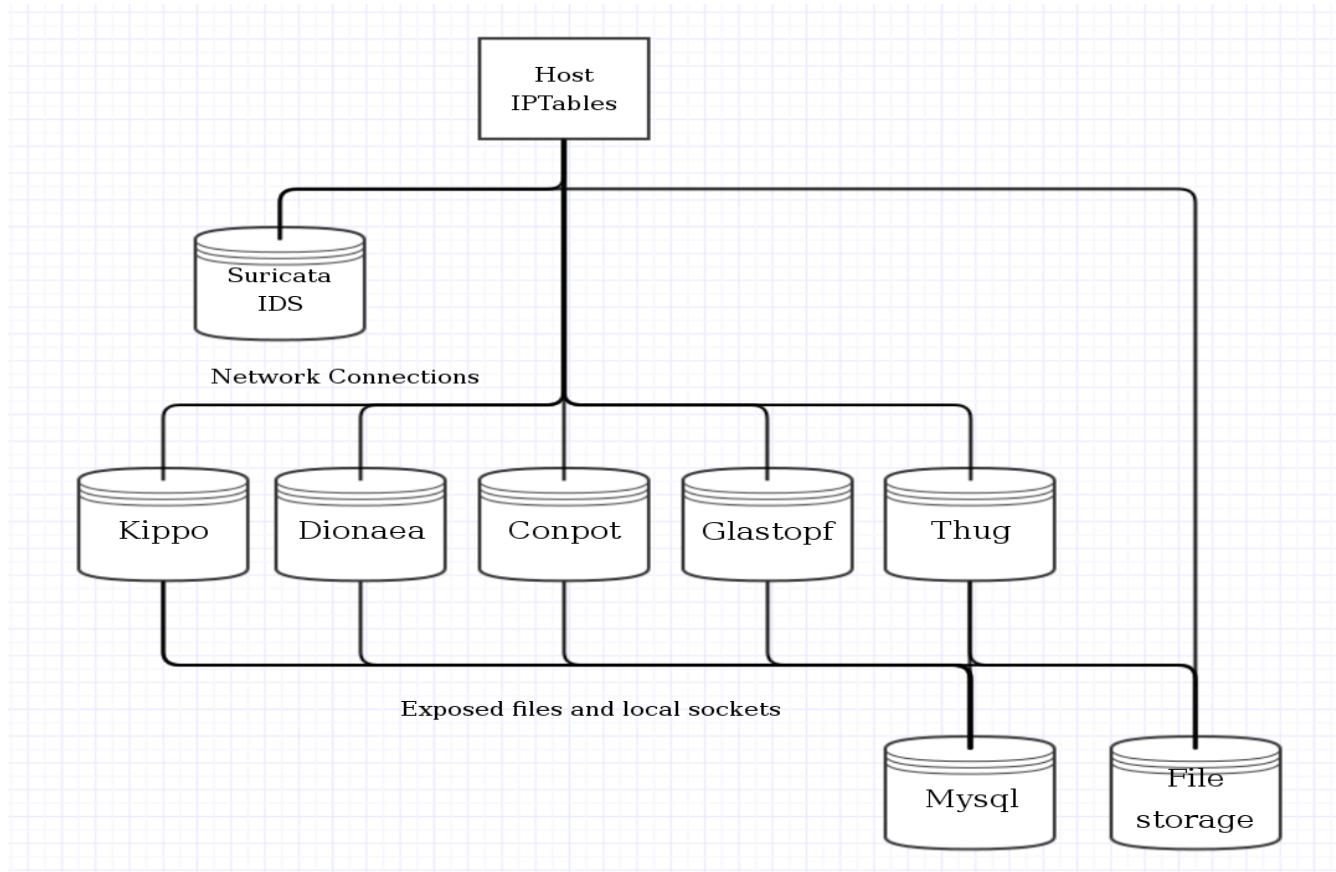


@Secure360 or
#Sec360

www.Secure360.com

HONEYAPPS

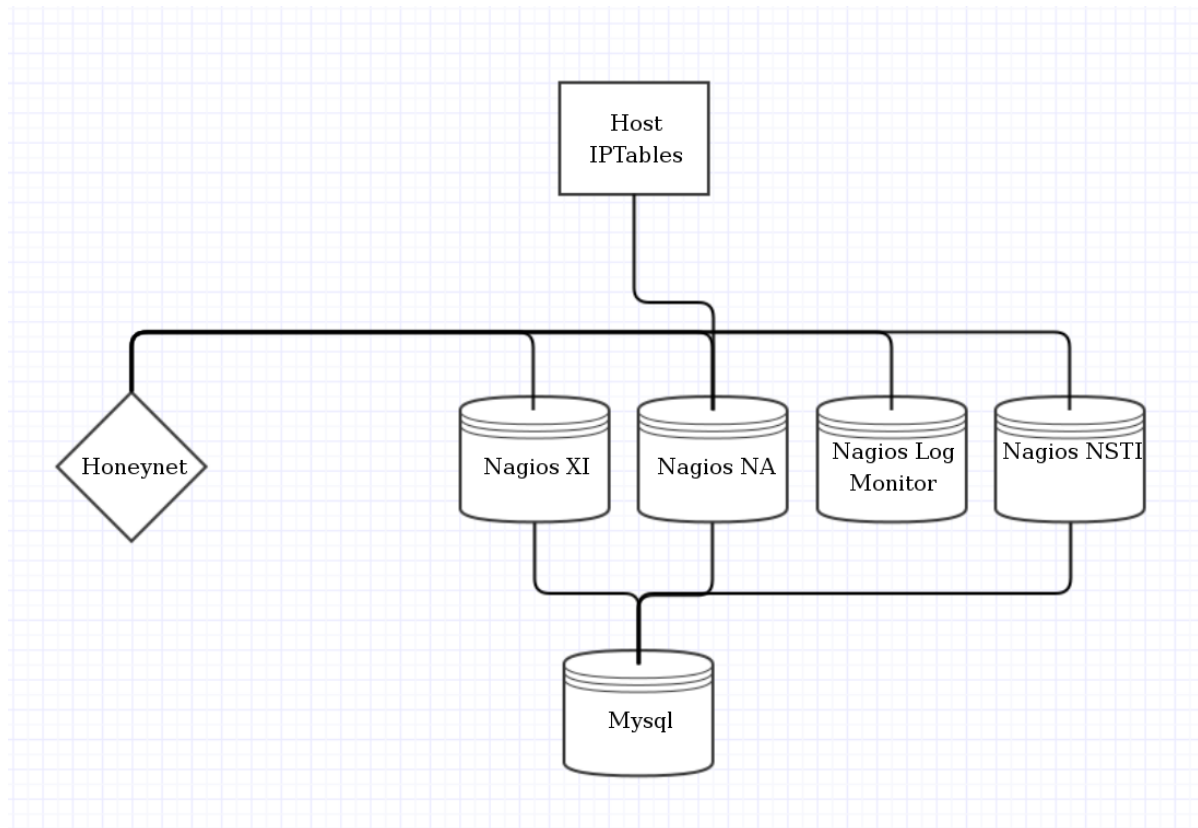
Where We've Been



Celebrating a
decade
of guiding
security
professionals.

SECURE360 
conference

Where We've Been



Celebrating a
decade
of guiding
security
professionals.

SECURE360 
conference



@Secure360 or
#Sec360

www.Secure360.com

HONEYAPPS

Where We're Going

- HoneyApps Director
 - Centralized management interface
 - Control, logging, honeypot daemon isolation.
 - Simple flat file and web interface configuration.
 - Memory and thread safe build language.
 - Repeatable build and test environments, publicly available.
- Overall Project
 - Revert on crash honeypots.
 - Fast deployment with automatic configuration pushes.
 - Deployment via Docker containers and VMware images.
 - HPfeeds\HPfriends integration via native rust implementation
 - Integration and correlation with third-party tools. (import & export)
 - Enterprise supported open-source project



Celebrating a
decade
of guiding
security
professionals.

SECURE360 
conference

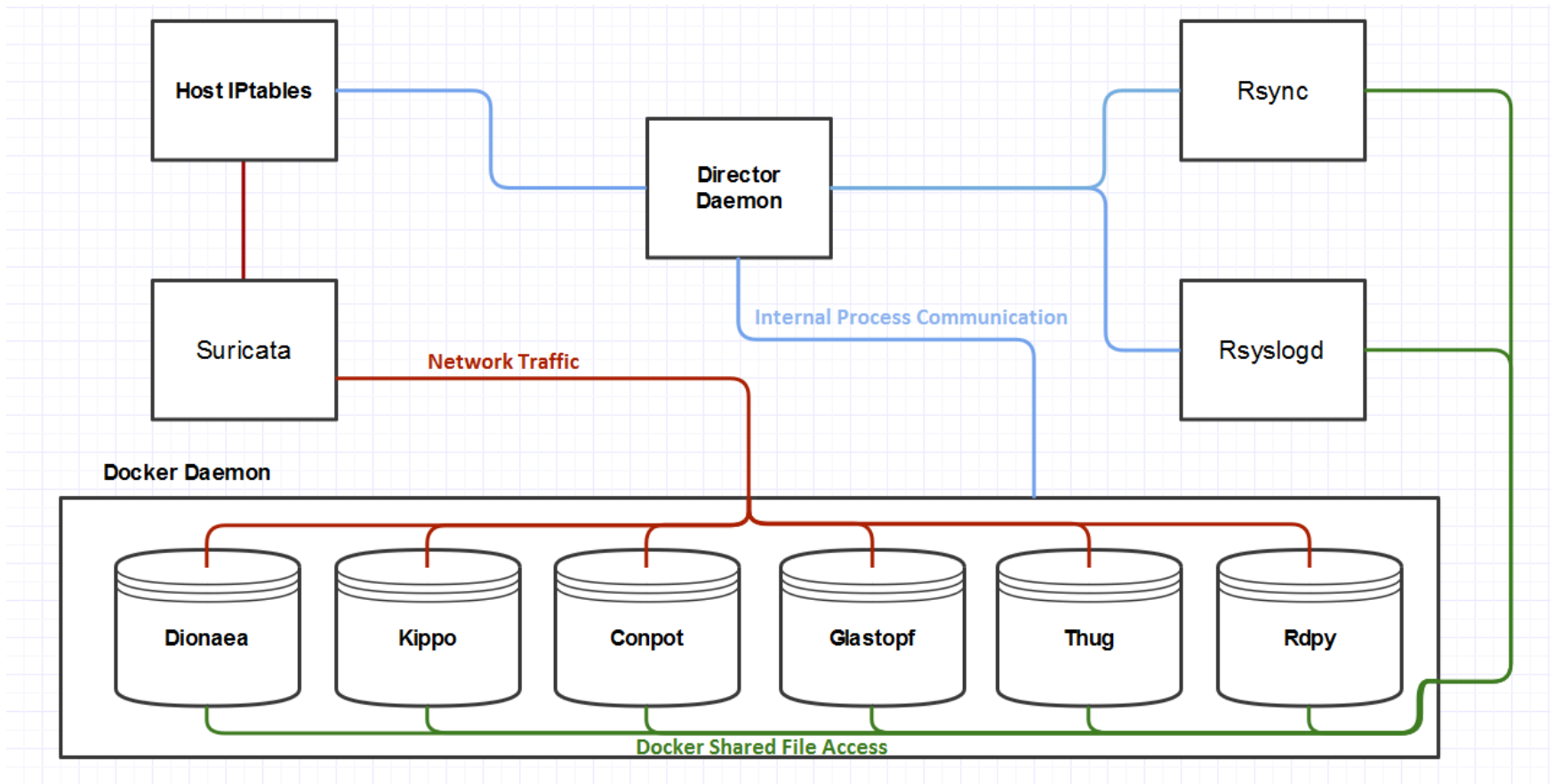


@Secure360 or
#Sec360

www.Secure360.org

HONEYAPPS

Director Worker



Celebrating a
decade
of guiding
security
professionals.

SECURE360 
conference

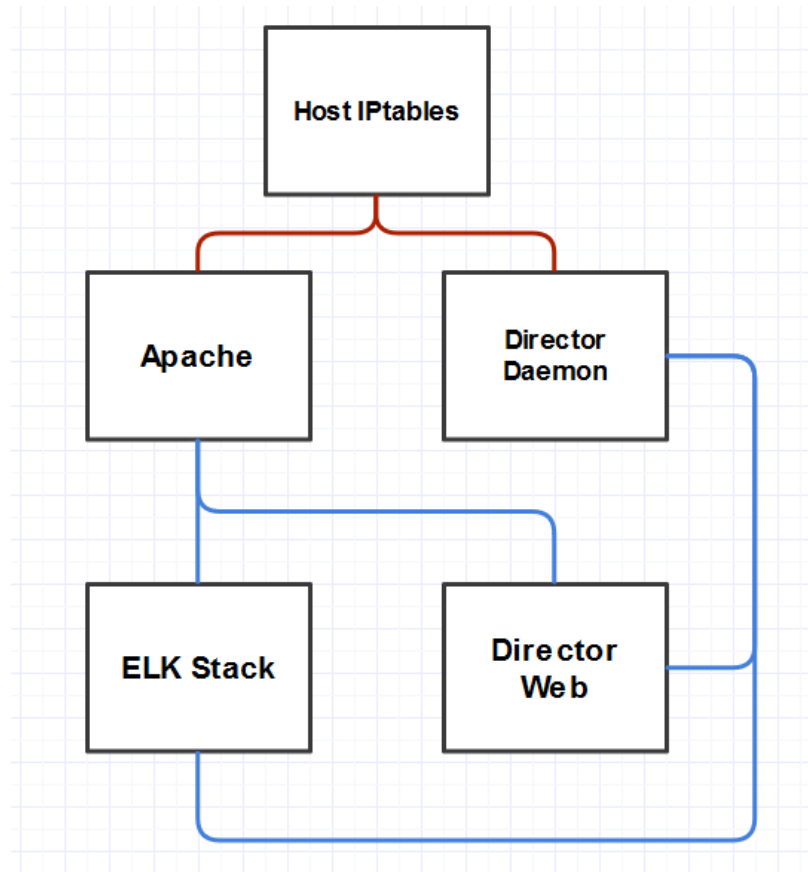


@Secure360 or
#Sec360

www.Secure360.com

HONEYAPPS

Director Primary



Celebrating a decade of guiding security professionals.

SECURE360 
conference

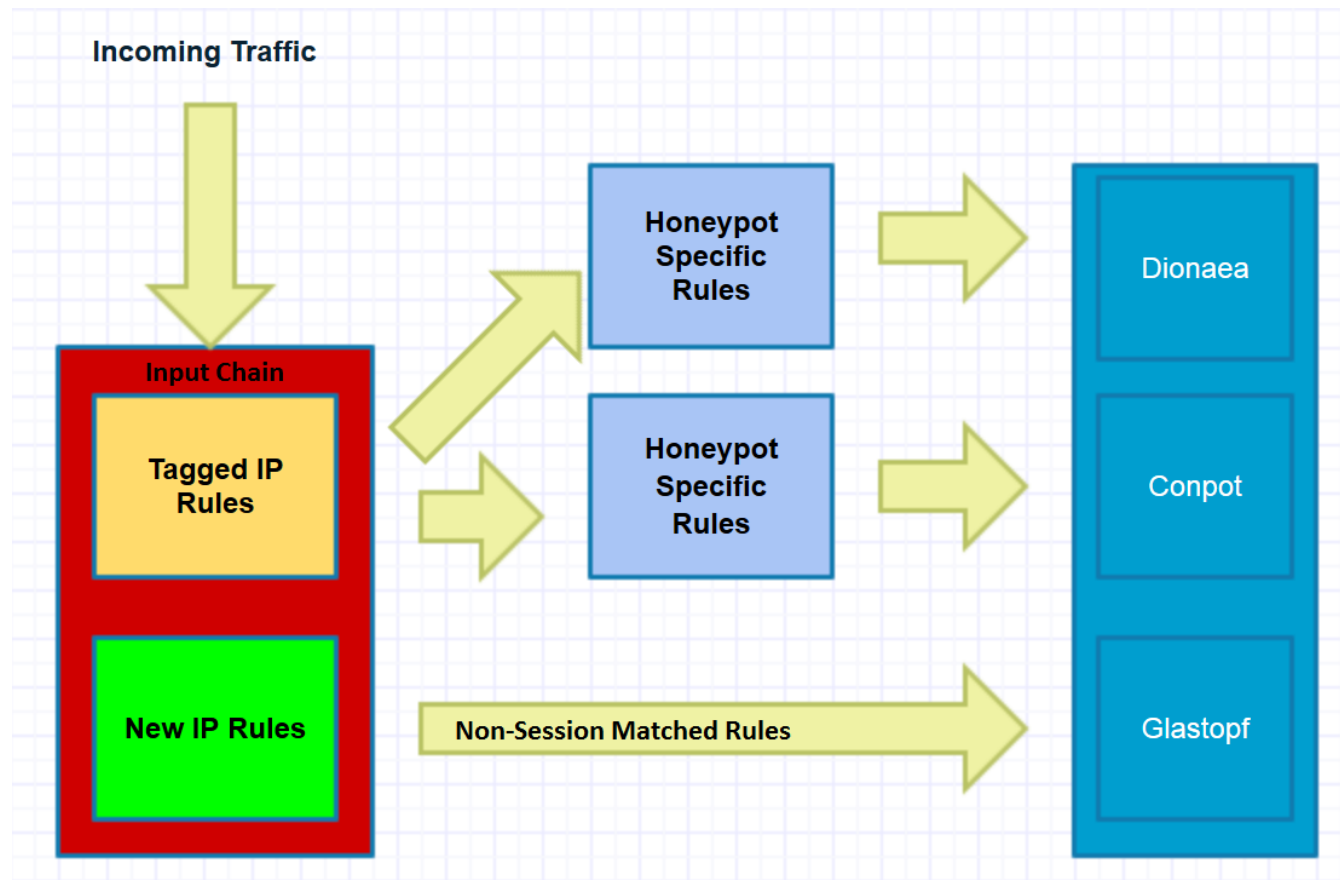


@Secure360 or
#Sec360

www.Secure360.com

HONEYAPPS

Dynamic IPtables Rules

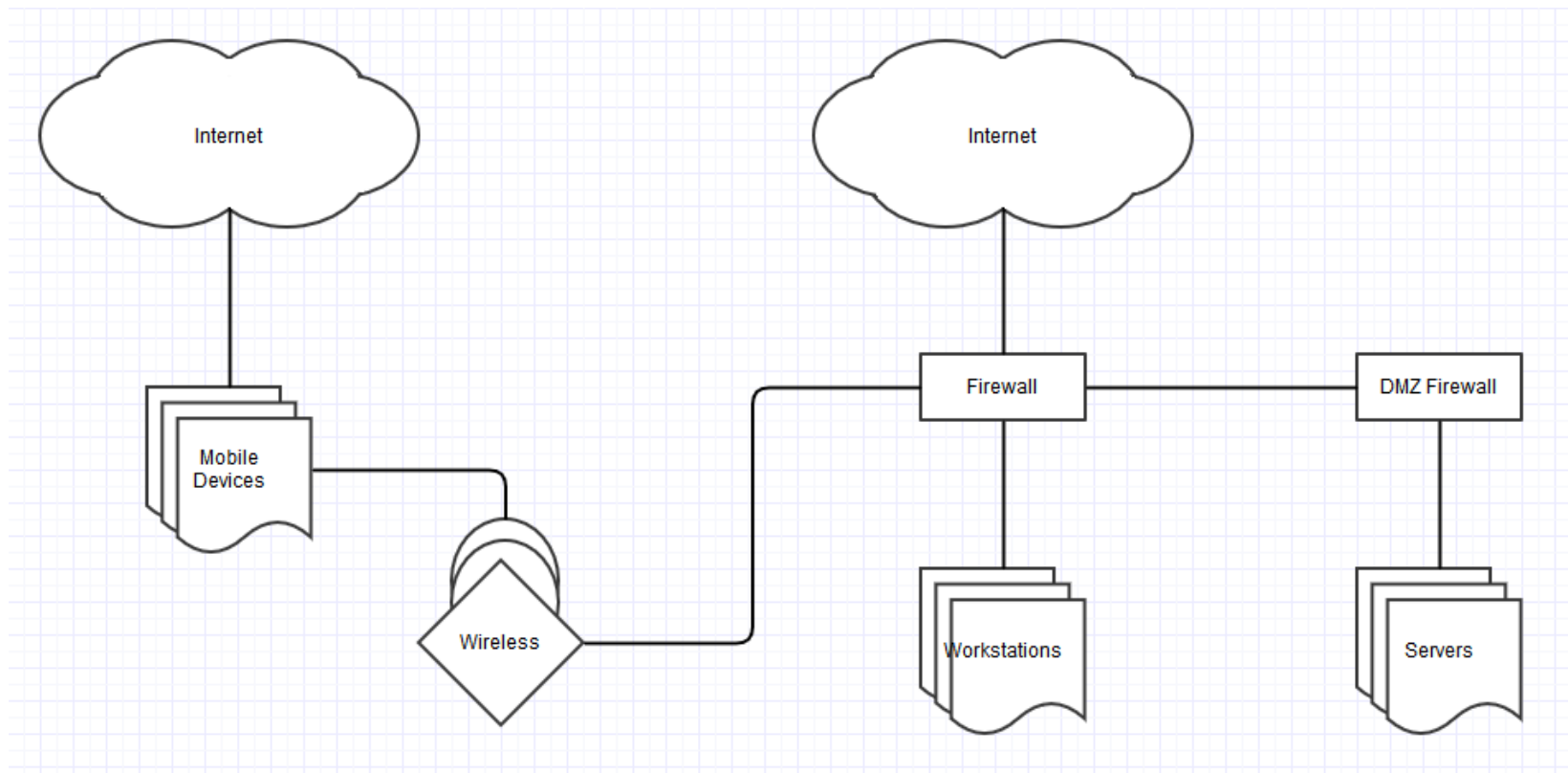


Celebrating a decade of guiding security professionals.

SECURE360 
conference

HONEYAPPS

Modern Network Layouts



Celebrating a
decade
of guiding
security
professionals.

SECURE360 
conference

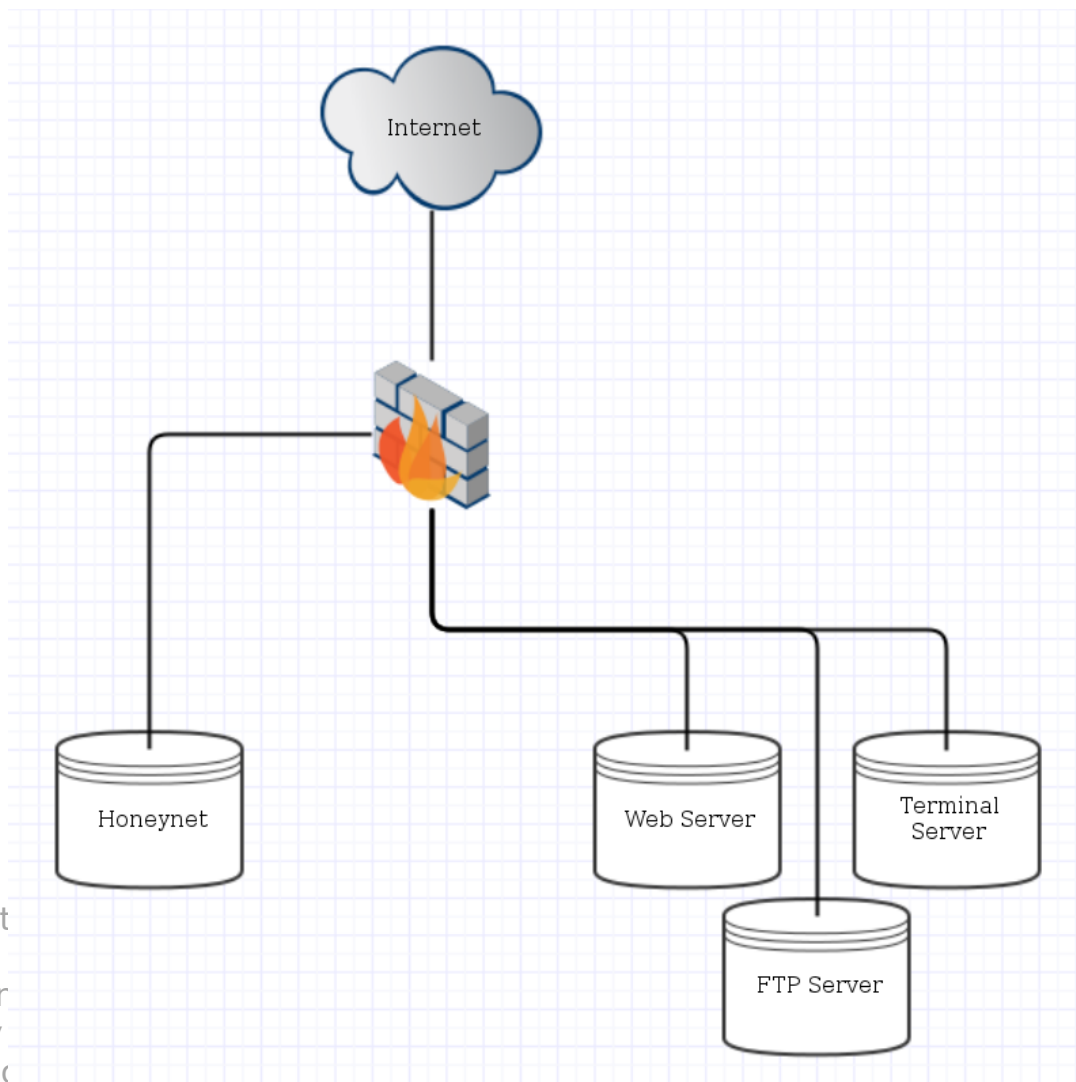


@Secure360 or
#Sec360

www.Secure360.com

HONEYAPPS

Server Honeypot Layout



Celebrating
decade of guiding
security
professionals

CURE360 
conference

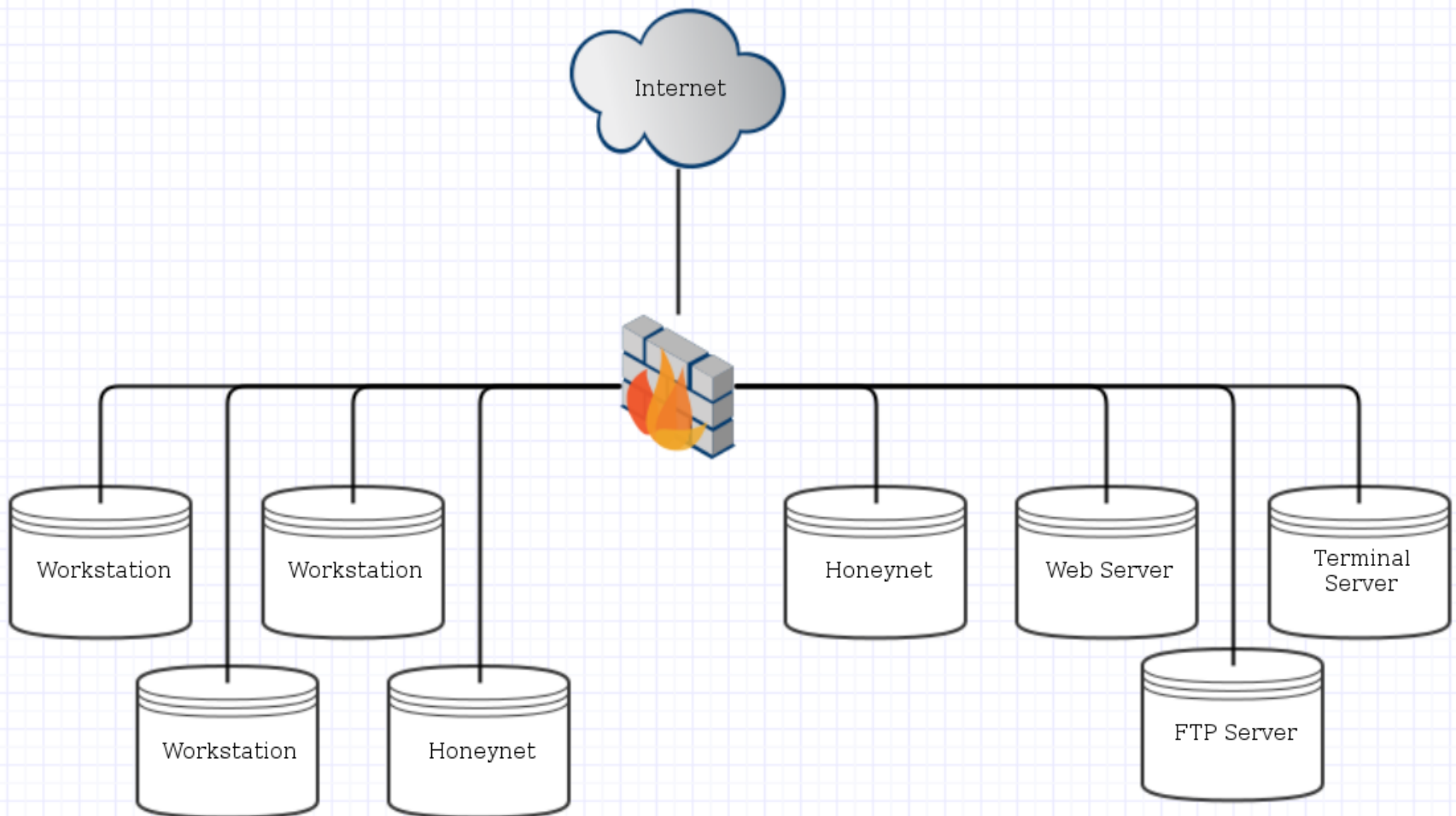


@Secure360 or
#Sec360

www.Secure360.org

HONEYAPPS

Workstation Honeypot Layout



Plan of Attack

- Terminology
- Where We've Been
- Where We're Going
- How Do Honey pots Help Improve Security Posture
- How Does HoneyApps Fit in My Org
- Videos



Celebrating a decade of guiding security professionals.

SECURE360 
conference



@Secure360 or
#Sec360

www.Secure360.com

HONEYAPPS

Dionaea Honeyypot

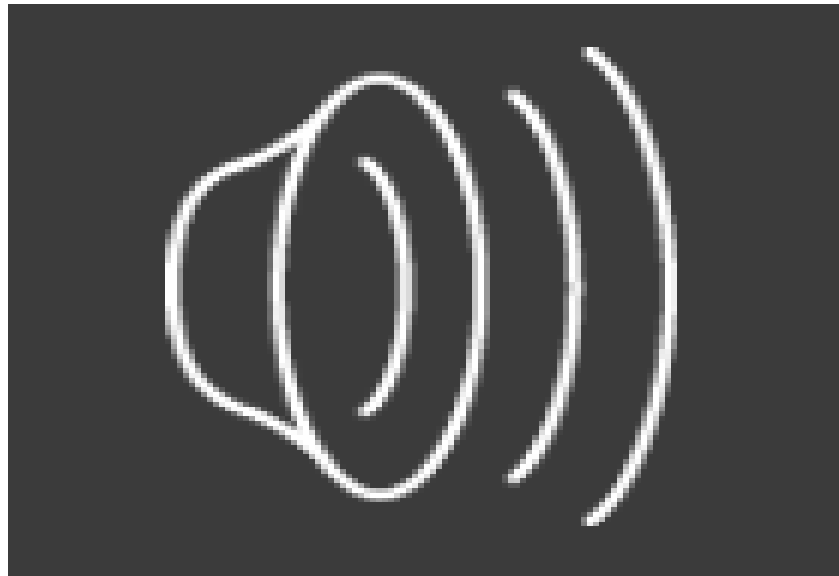
- General purpose honeypot
- Expandable through plugins and modules
- Full shellcode emulation
- Detects attacks on ports:
 - 21(ftp)
 - 69(tftp)
 - 135(emap)
 - 445(smb)
 - 1443(mssql)
 - 3306(mysql)
 - 5060-5061(sip)
 - 63001-64000(ftp)
- Automated control and deployment with Director



Celebrating a
decade
of guiding
security
professionals.

SECURE360 
conference

Dionaea Attacks



Celebrating a
decade
of guiding
security
professionals.

SECURE360 
conference

 @Secure360 or
#Sec360

www.Secure360.com

HONEYAPPS

Glastopf Honeypot

- Web application specific honeypot
- Detects attacks on ports:
 - 80 (http)
 - 443 (https)
- Full PHP emulated virtual environment
- Emulated sql backend
- Automated control and deployment with Director



Celebrating a
decade
of guiding
security
professionals.

SECURE360 
conference

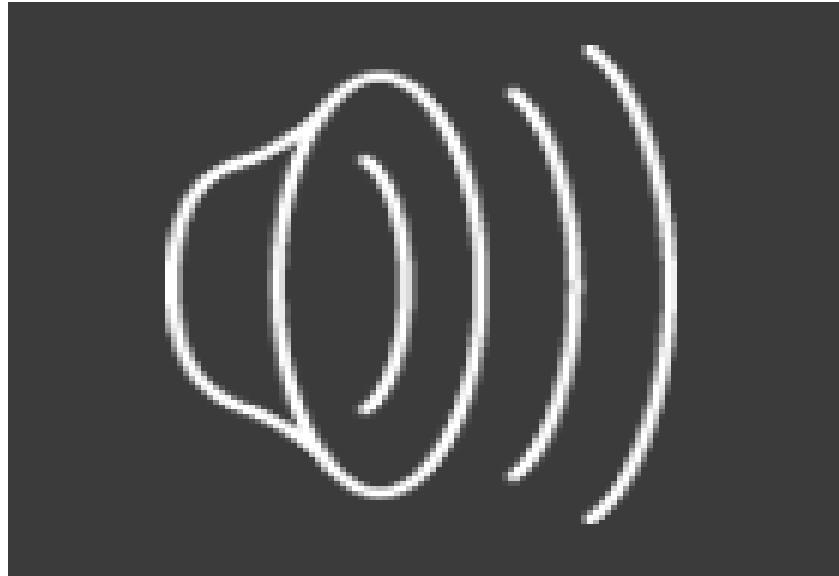


@Secure360 or
#Sec360

www.Secure360.com

HONEYAPPS

Glastopf Attacks



Celebrating a
decade
of guiding
security
professionals.

SECURE360 
conference



@Secure360 or
#Sec360

www.Secure360.com

HONEYAPPS

Conpot Honeypot

- Industrial Control Systems(ICS)
Supervisory Control and Data
Acquisition (SCADA)
- Defaults to building device control
system
- Full Shellcode emulation
- Detects attacks on ports:
 - 80 (http)
 - 161 (snmp)
 - 503 (modbus)
- Automated control and deployment with
Director



Celebrating a
decade
of guiding
security
professionals.

SECURE360 
conference

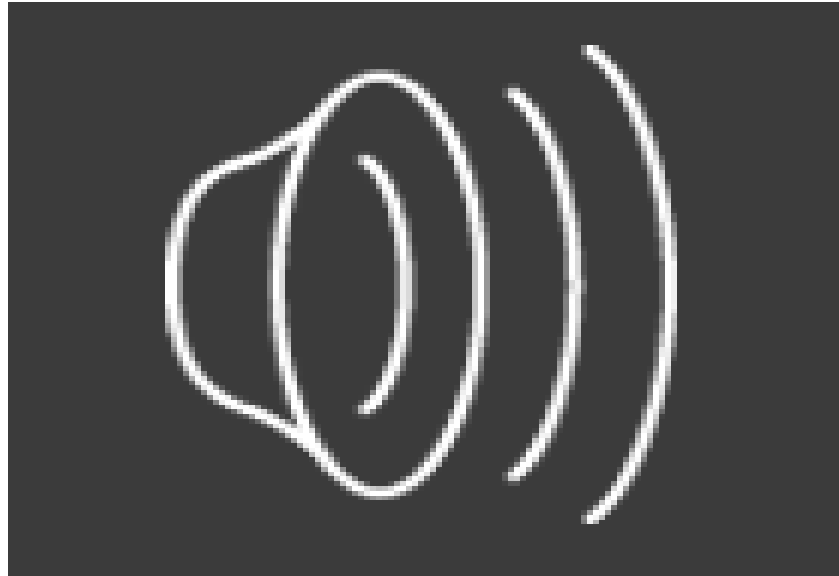


@Secure360 or
#Sec360

www.Secure360.org

HONEYAPPS

Conpot Attacks



Celebrating a
decade
of guiding
security
professionals.

SECURE360 
conference



@Secure360 or
#Sec360

www.Secure360.com

HONEYAPPS

Kippo Honeypot

- SSH specific honeypot
- Full virtual shell emulation
- Daemon attack emulation
- Detects attacks on port:
 - 22 (ssh)
- Automated control and deployment with Director



Celebrating a
decade
of guiding
security
professionals.

SECURE360 
conference

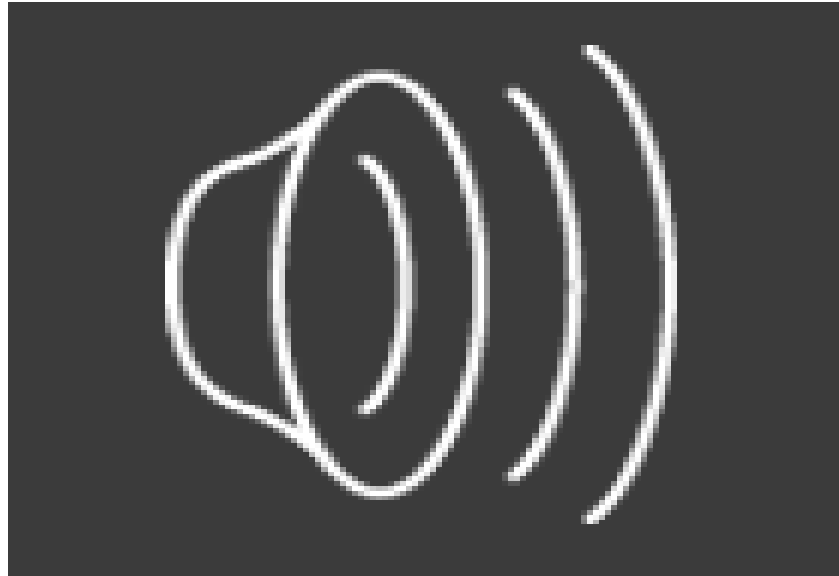


@Secure360 or
#Sec360

www.Secure360.com

HONEYAPPS

Kippo Attacks



Celebrating a
decade
of guiding
security
professionals.

SECURE360 
conference

 @Secure360 or
#Sec360

www.Secure360.com

HONEYAPPS

RDPy Honeypot

- Remote Desktop Protocol honeypot and mitm
- Record & replay screen, mouse interaction, and keys
- Man-in-the-middle to live Windows hosts
- Detects attacks on port:
 - 3389 (ms-rdp)
- Automated control and deployment with Director



Celebrating a
decade
of guiding
security
professionals.

SECURE360 
conference

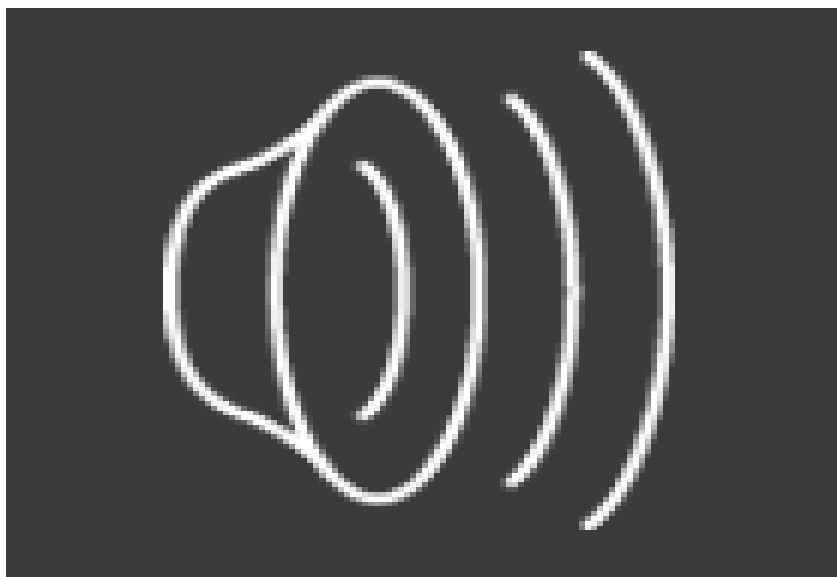


@Secure360 or
#Sec360

www.Secure360.com

HONEYAPPS

RDPy Attacks



Celebrating a
decade
of guiding
security
professionals.

SECURE360 
conference

 @Secure360 or
#Sec360

www.Secure360.com

HONEYAPPS

Thug HoneyPot

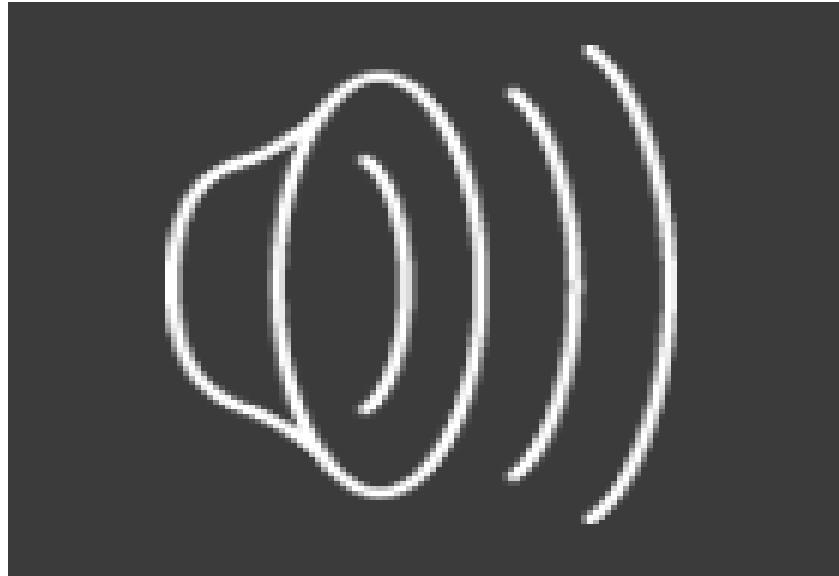
- Low interaction honeyclient
- W3C DOM compliant
- Google V8 Javascript Engine
- Libemu\Pylibemu shellcode emulation
- 8 IE, 15 Chrome, 3 Firefox, & 5 Safari user-agents and personalities
- No active ports, is feed uri's to connect and analyze
- Automated control and deployment with Director



Celebrating a
decade
of guiding
security
professionals.

SECURE360 
conference

Thug Attacks



Celebrating a
decade
of guiding
security
professionals.

SECURE360 
conference

 @Secure360 or
#Sec360

www.Secure360.com

HONEYAPPS

Conclusion & Questions

Personal:

@c0mmiebstrd

Docker.com/u/sreinhardt – Docker.com/u/commiebstrd

Github.com/commiebstrd – github.com/commiebstrd

HoneyApps:

@honeyappsproj

Docker.com/u/honeyappsproject

Github.com/honeyappsproject

www.honeyapps.net

HONEYAPPS



Celebrate
decade
of guiding
security
professionals.

SECURE360 
conference

 @Secure360 or
#Sec360

www.Secure360.
com

HONEYAPPS