Honeypots in the Cloud

Shishir P., Sivasubramanian R., Josh S., Stephen B., Rebecca L.

Agenda

Introduction

Background

Experimental Setup

Results

Conclusion

Future Work

Overview

- What we did:
  - Set up honeypots in several different clouds
- Goals:
  - Where do attacks come from?
  - What kind of attacks are being made?
  - Are there differences across cloud providers?
- Findings:
  - Most attacks come from China and US
  - Most attacks on SSH and HTTP
  - Reviewed honeypots for cloud setting

Introduction

- Motivation
  - Cloud security important!
  - Not many studies about traffic captured by honeypots in cloud instances
  - Most cloud honeypots done in EC2

- Related Work
  - Honeypots in networks
  - "Honeypots: Tracking Hackers" - Lance Spitzner
  - http://blog.infosanity.co.uk/ - Andrew Waite

Agenda

Intro

Background

Experimental Setup

Results

Conclusion

Future Work

Honeypots

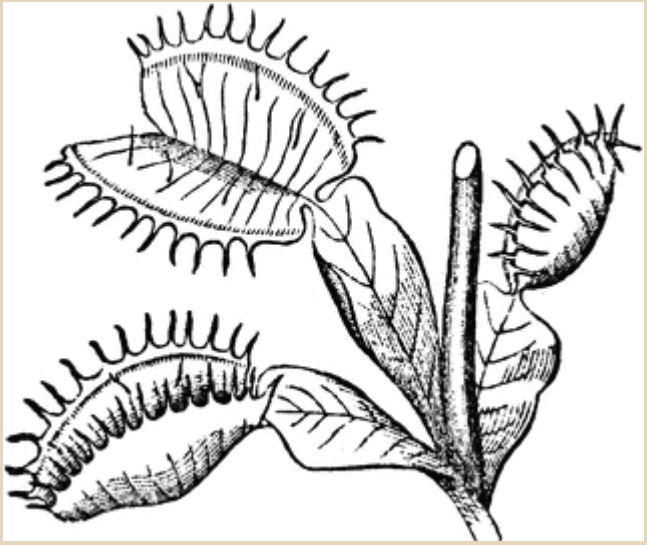
- Honeypot basics
  - Used to detect malicious or erroneous traffic
  - Emulates vulnerabilities and logs attacker behaviour

Types of Honeypots

- Low Interaction
  - Simulate services, passively log connections
- Medium Interaction
  - Simulate services, and respond to attacker
- High Interaction
  - Simulate entire system

Dionaea

- Low interaction
- Emulates vulnerable Windows system
- Logs attempted exploits
- Captures automated malware
- Protocols
  - SMB, HTTP, FTP, TFTP
  - MSSQL, MySQL, SIP



Kippo

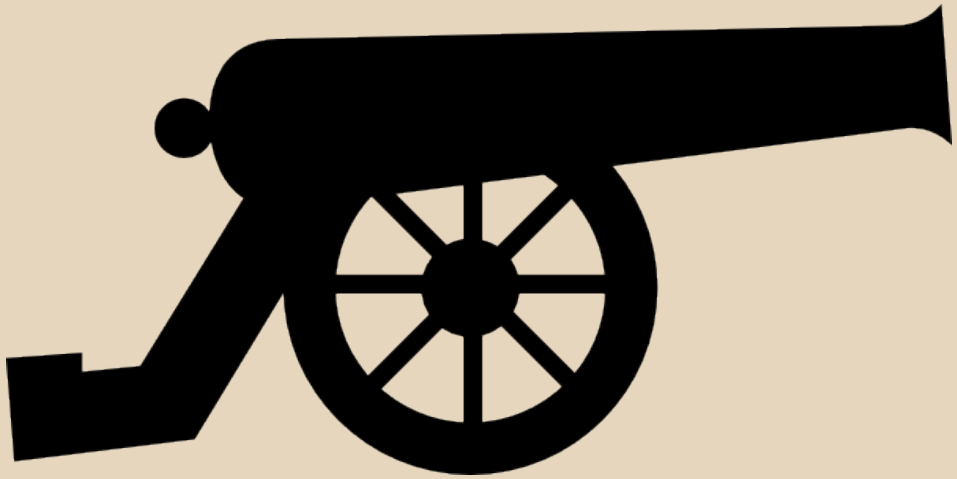
- Medium interaction
- SSH honeypot
- Logs attempted logins
- Logs shell commands
- Emulates:
  - shell
  - filesystem

Amun

- Low interaction
- Capture autonomous spreading malware
- Log shellcode and downloads
- Extensible through custom XML modules

Artillery

- Low interaction
- Automatically blacklists ip addresses that attempt to connect
- Monitors file system and emails changes
- Detects and derails SSH Brute Force Attacks



Glastopf

- Low Interaction
- A web server which emulates thousands of vulnerabilities
- Trick attacker to attempt exploits such as SQL injection and file inclusion attacks.
- Respond in ways that the attacker expects

Other Honeypots

- Honeyd
  - Capable of emulating different OS's or even entire networks of hosts
  - Uses DHCP, incompatible with cloud infrastructure
- HiHat
  - High-Interaction PHP Honeypot
  - Received no attacks
- Artemissa
  - High-Interaction VoIP Honeypot
  - No longer maintained

Agenda

Intro

Background

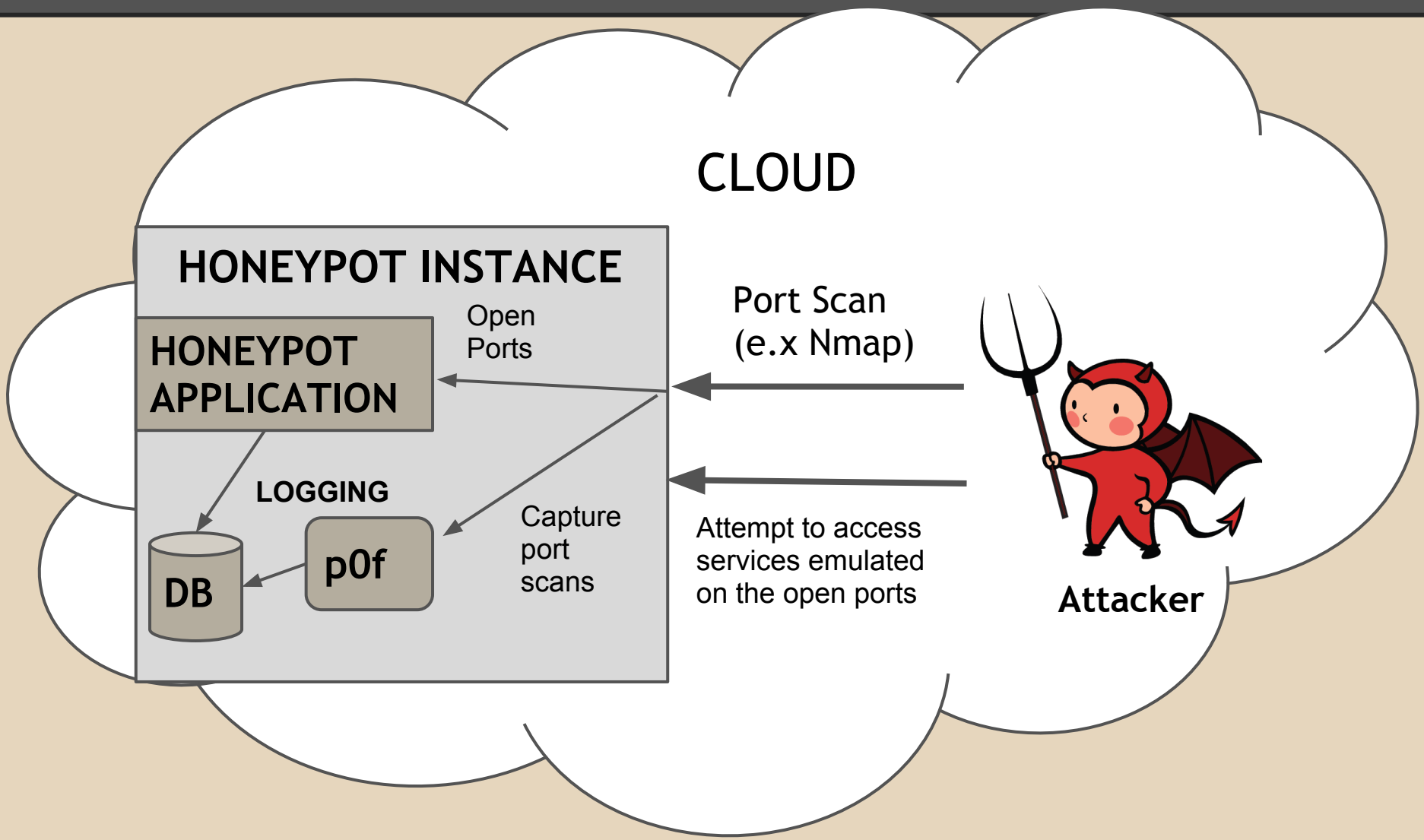
Experimental Setup

Results

Conclusion

Future Work

Experimental Setup - Infrastructure



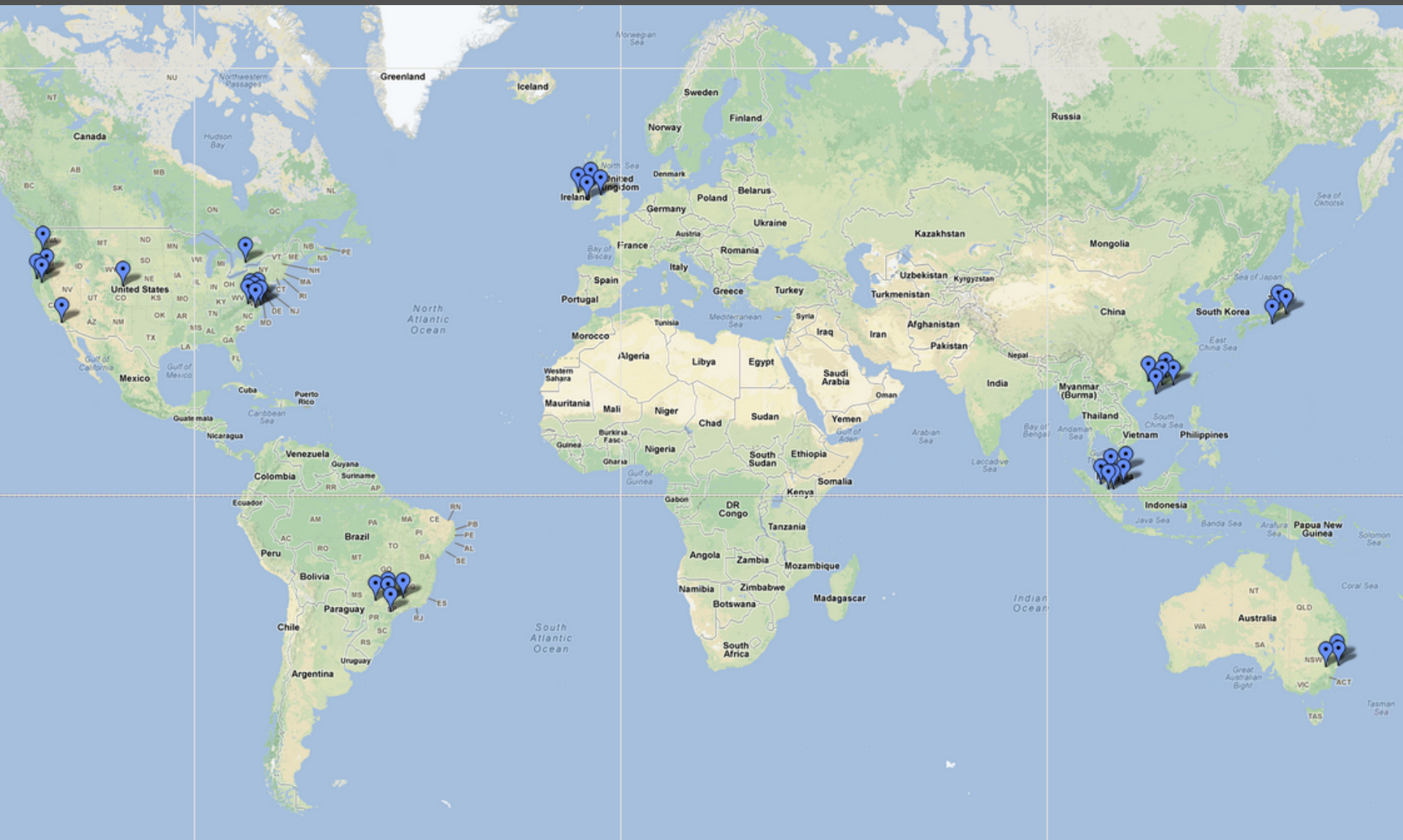
Fingerprinting Tool

- p0f
  - Installed on every instance
  - Version 2.08 available for ubuntu.
  - Passively captures attacker information:
    - IP
    - OS
    - Location

Experimental Setup

- 42 Honeypots:
  - Amazon EC2 (22)
  - Windows Azure (14)
  - IBM Smartcloud (5)
  - ElasticHosts (1)

Cloud Instance Locations



Cloud details

Cloud	OS	Access
EC2	Ubuntu Server 12.04 LTS	Private Key
Azure	Ubuntu Server 12.04 LTS	SSH with Password
IBM Smartcloud	Redhat Enterprise Linux 6.3 64-bit	Private Key
ElasticHosts	Ubuntu 12.04 LTS	SSH with Password

Agenda

Intro
Background
Experimental Setup
Results
Conclusion
Future Work

HoneyWeb - Architecture

DIONAEA | KIPPO | AMUN | ARTILLERY | GLASTOPF

LOG EXTRACTOR → LOG PARSER → DATABASE

Results

See Know Thy Hacker

Challenges

- Limitations of free accounts on clouds
- Attackers not interested in exploiting micro instances
- Low interaction honeypots not as enticing to attackers
- Little success for windows-based honeypots
- Poor honeypot documentation
- Tools like p0f don't have latest ubuntu packages for quick installation

Agenda

Intro
Background
Experimental Setup
Results
Conclusion
Future Work

Attacker Profile

- Most attacks from:
  - China
  - US
- Most commonly attempted user:
  - root
- Most commonly attempted passwords:
  - "" (Blank string)
  - 123456
- Most commonly attacked services:
  - SSH
  - HTTP

Attacker Profile Cont'd

- Most common known attacker OS
  - Linux 2.6
  - Windows 2000 SP4
- Most common attacker connection protocol
  - ethernet/modem

Attacker Behavior

- Most common attack pattern:
  - w : see all logged in users
  - cat /proc/cpuinfo : see system resources
  - exit or launch attacks
- Downloads:
  - Worms:
    - Conficker / Downadup / Kido

Cloud Conclusions

- Similarities
  - Attacker location
  - SSH login username/password

- Differences
  - Attackers use newer OS on Azure than EC2 - indicated by % of unknown OS
  - Greater number of Windows-based attackers on Azure

Honeypot Review

1. Kippo ☆☆☆☆☆
2. Dionaea ☆☆☆☆☆
3. Amun ☆☆☆
4. Artillery ☆☆
5. Glastopf ☆

Future Work

- Larger instances with more resources
- Other paid clouds
- Windows OS Instances
- Non-cloud instance for baseline comparison

Thank you!
Questions?