LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

HEALTH SECTOR CYBERSECURITY COORDINATION CENTER

HC3

Using Honeypots for Network Intrusion Detection

10/22/2020

Report #: 202010221030

Agenda

- Introduction
- Honeypot History
- Honeypot Characteristics
- Honeypot Types
- Honeypot Goals
- Honeypots for Intrusion Detection
- Honeypot Logging and Monitoring
- Honeypot Risks and Mitigations
- Conclusion
- References
- Questions

Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

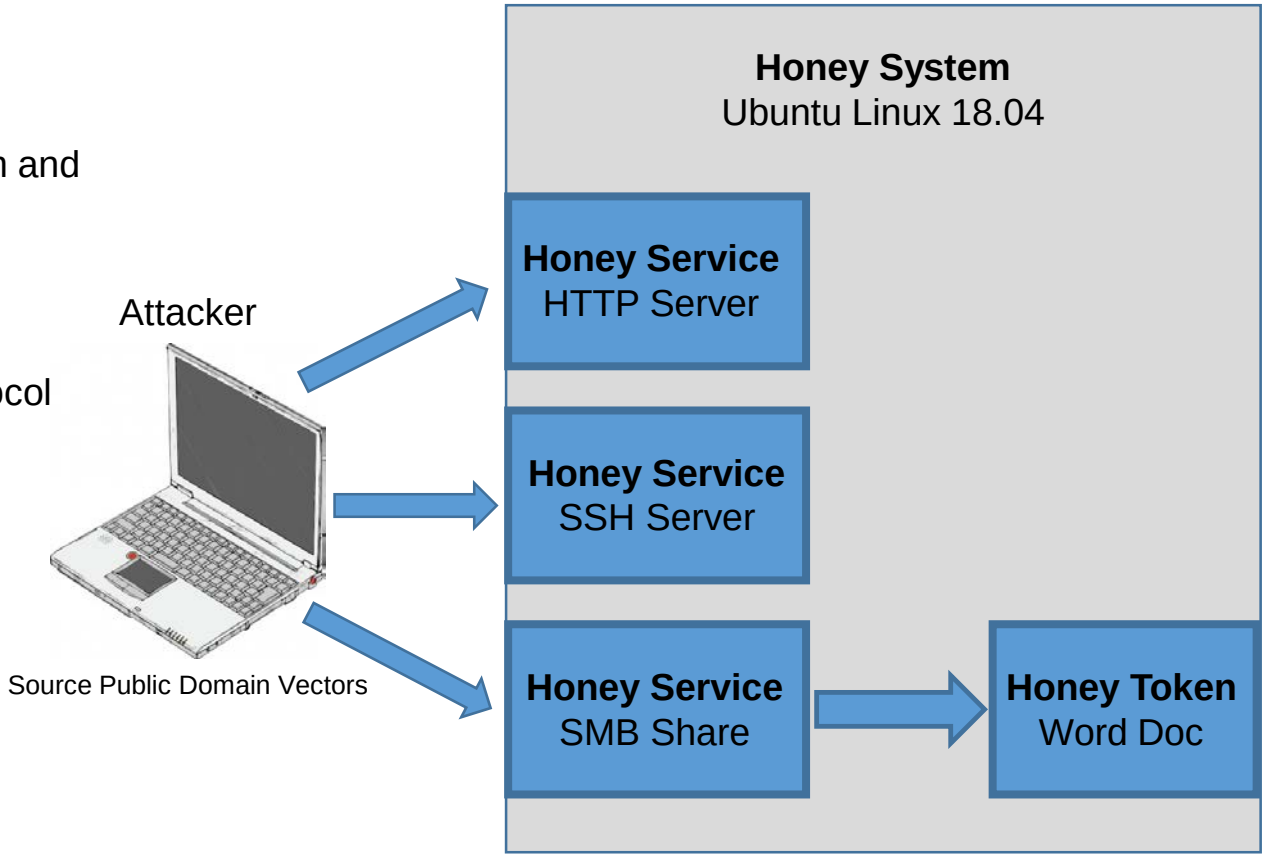
What is a honeypot?

"A security resource whose value lies in being probed, attacked, or compromised." – Lance Spitzner

Source: EC Council

Honeypot Types

- ***Honey System***
  - Imitates operating system and services.
- ***Honey Service***
  - Imitates software or protocol functions.
- ***Honey Tokens***
  - Imitates data.



Source Public Domain Vectors

Source: Intrusion Detection Honeypots

Honeypot History

1989
"The Cuckoo's Egg"

1991
"An Evening with Berferd"

1997
Deception Toolkit

1999
CyberCop Sting

2000
The Honeynet Project

2003
Honeyd

2014
Deception-based Technology Boom

Present
80+ free open source honeypot tools

Honeypot Characteristics

Honeypots are:

- ***Deceptive***
  - They appear to be something they are not.
- ***Discoverable***
  - Located on a network where an attacker is likely to find them.
- ***Interactive***
  - The honeypot will respond to a range of stimuli from low to high interactivity.
- ***Monitored***
  - Any interaction with a honeypot is logged and triggers an alert.

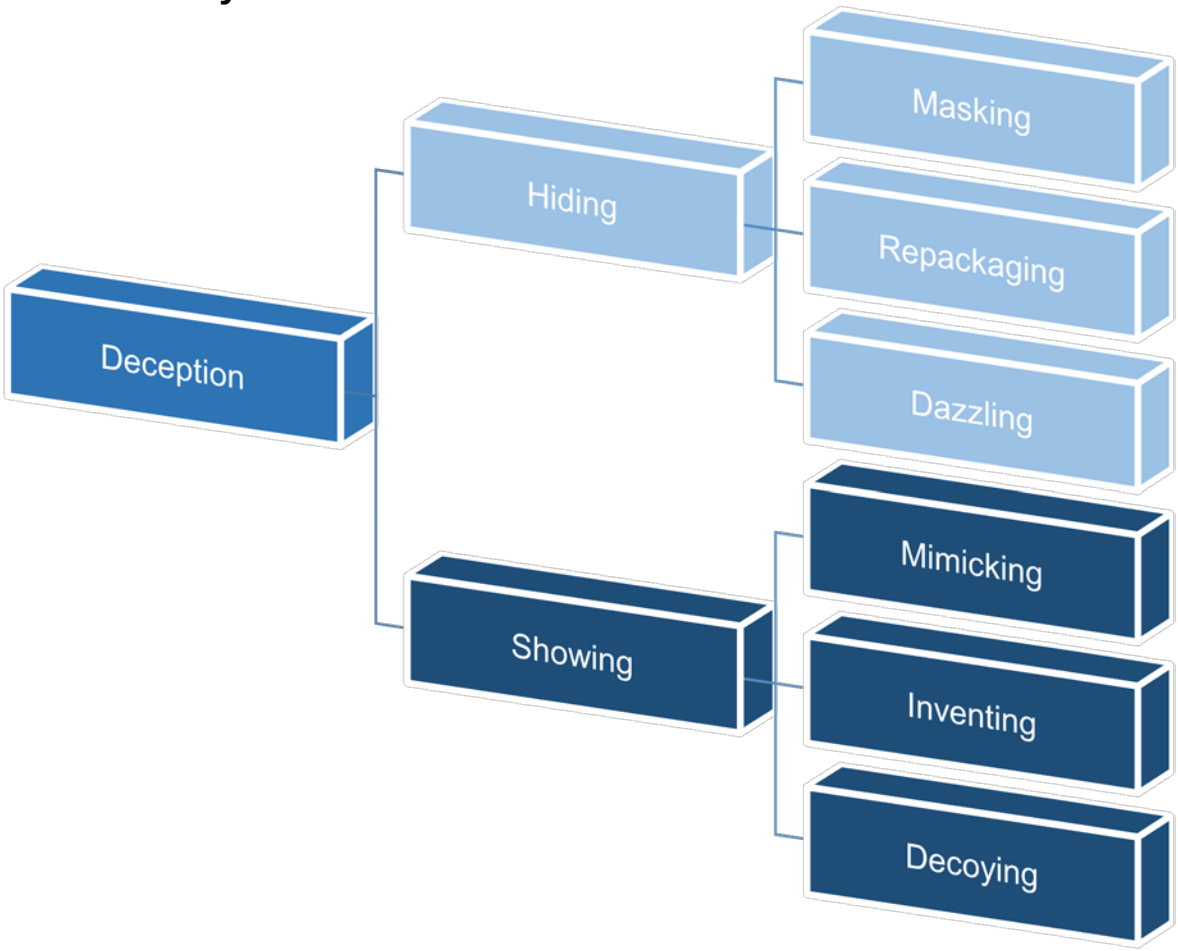
Source: StickPNG

Source: Photos.com

Source: Amazon.com

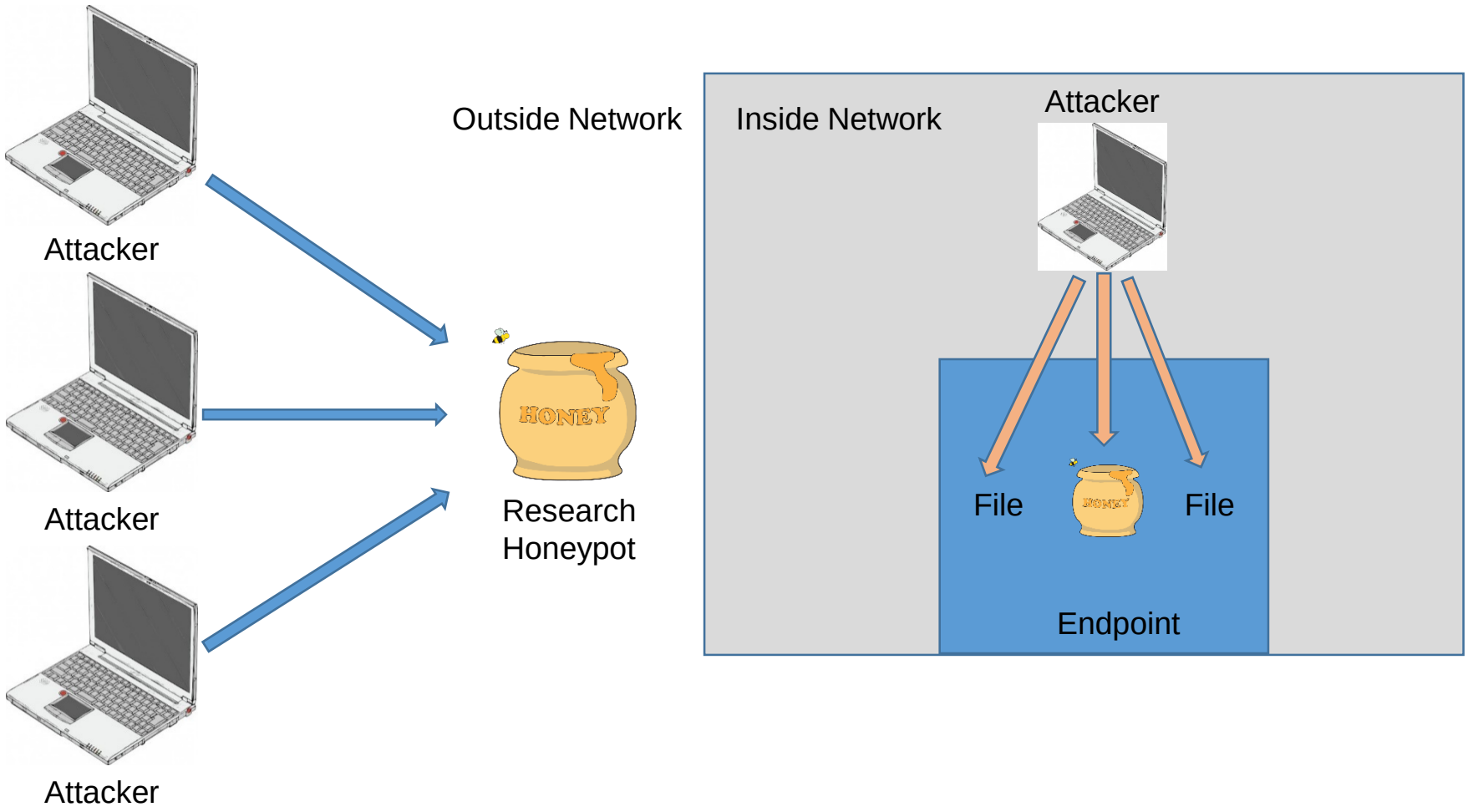
Source: Physical Security Online

Whaley's Deception Taxonomy

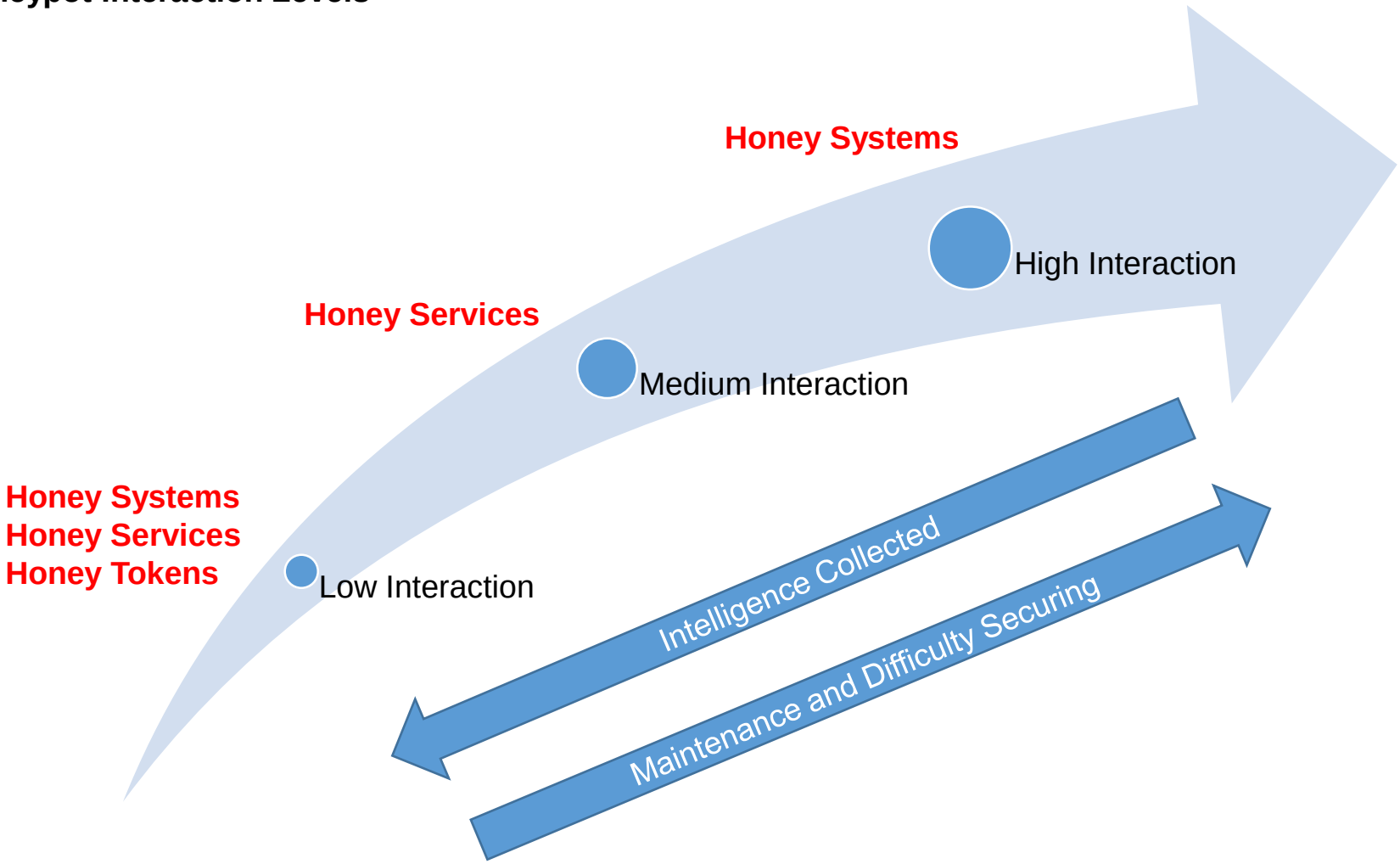


Source: Intrusion Detection Honeypots

Honeypot Discoverability



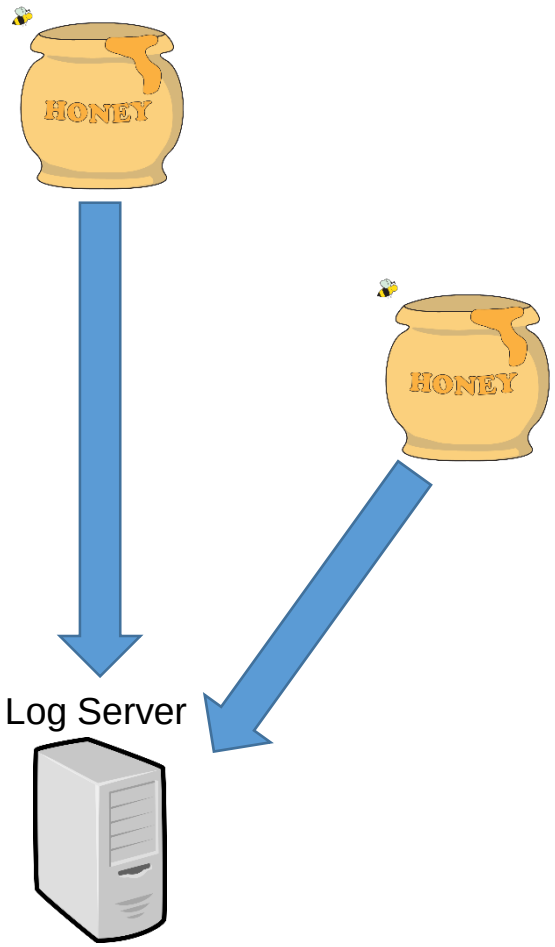
Honeypot Interaction Levels



Monitoring and Logging Honeypots

Questions to ask…

1. What log formats does the honeypot provide?
2. What log formats does the logging server accept?
3. What tool will I use to send logs over the network from the honeypot?
4. What tool will I use to receive the logs sent to the logging server?
5. How will I filter and parse the honeypot logs for useful analysis?



Source: Clipart Library

Honeypot Goals

- ***Research***
  - Goal is to learn about attackers' tactics, techniques and procedures

Source: Medical News Today

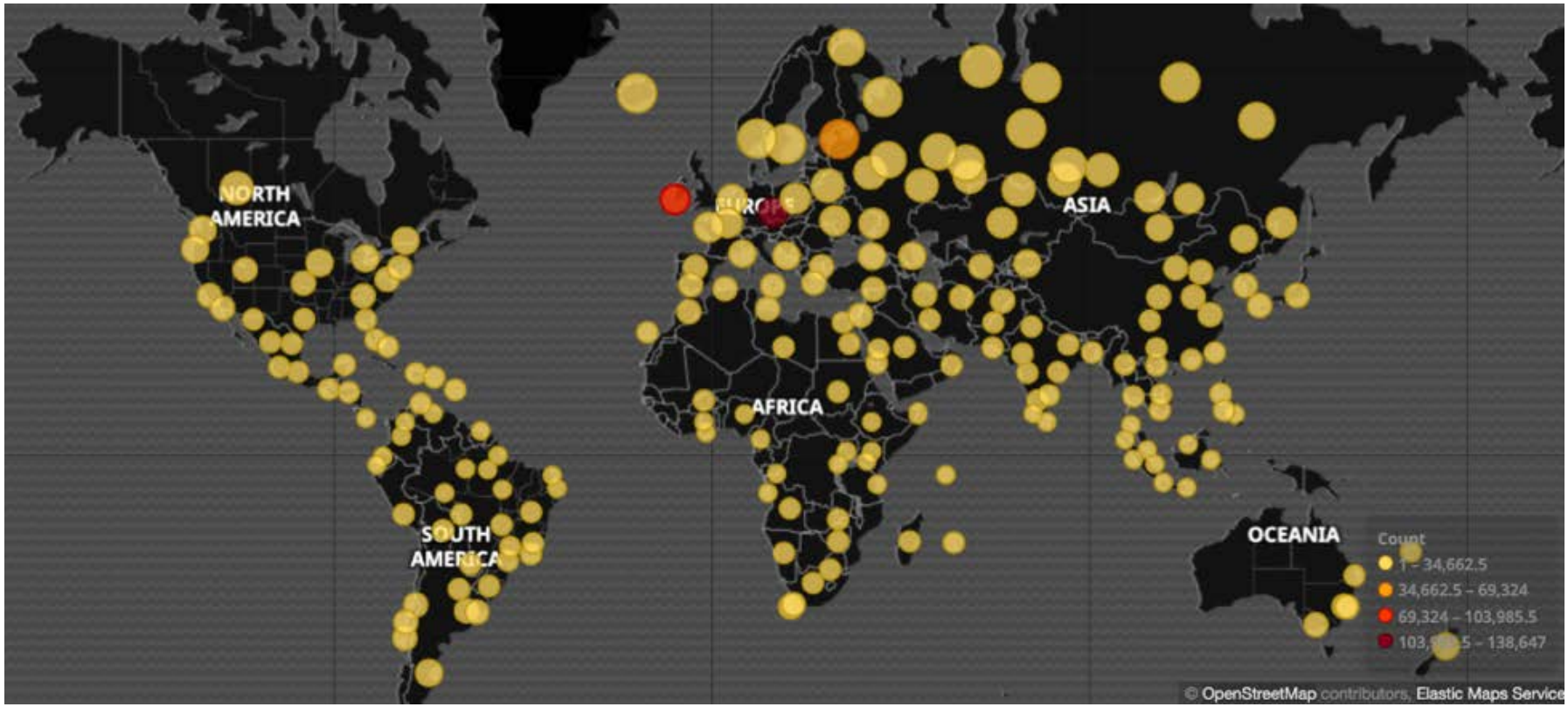
- ***Resource Exhaustion***
  - Goal is to waste the attackers' time for as long as possible

Source: National Geographic

- ***Intrusion Detection***
  - Goal is to be alerted to an attacker's presence on the network, as nothing legitimate should be interacting with it

Source: WebStockReview

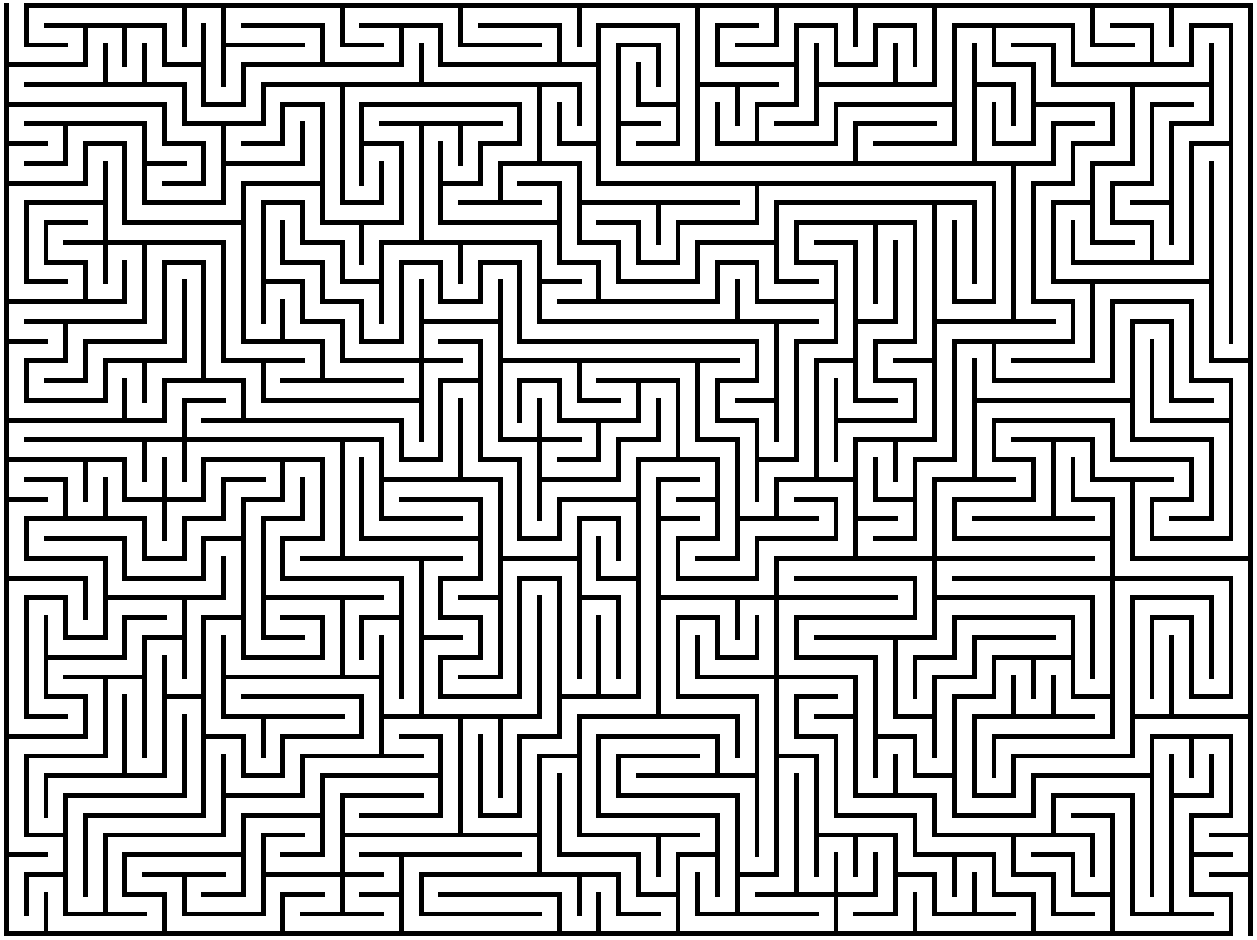
Research Honeypots



Source: Digital Shadows

Honeypot Goals: Resource Exhaustion

Resource Exhaustion Honeypots



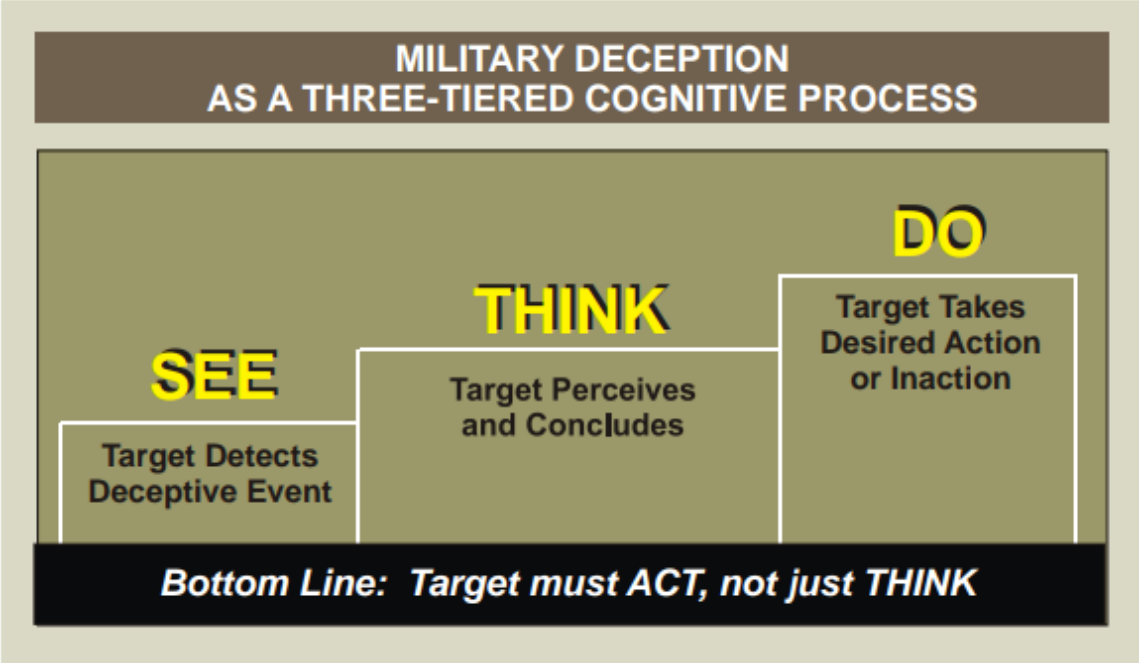
Source: Stack Overflow

Intrusion Detection Honeypots

Source: Australian Broadcasting Corporation

See – Think – Do Deception Methodology

- ***See***
  - The attacker needs to see the honey system, service, or token
- ***Think***
  - The attacker must think the honey system, service, or token is worth taking the time to explore or interact with
- ***Do***
  - The attacker must do something with the honey system, service, or token, generating an alert



Source: JP 3-13.4, Military Deception

Honeypot Placement Within the Network

- ***See***
  - Where will an attacker be to see a honeypot?
  - Where will they want to pivot to and find more honeypots waiting for them?
  - What would they consider valuable in the network where additional honeypots could be placed?
- ***Think***
  - How do you make a honeypot important enough to interact with?
  - Do you make it stand out, or blend in?
- ***Do***
  - How much functionality do you give the honeypot so the attacker will interact with it?

Source: Wikimedia Commons

! All honeypot IP addresses should be included on vulnerability scanners and penetration testing, so that lists avoid false positive alerts.

Medical Device Honeypot Use Case

Medical Device Honeypot Data	
Honeypots	10
Successful logins (SSH/Web)	55,416
Successful exploits (Majority were MS08-067)	299
Dropped malware samples	24

Honeypot Risks and Mitigations

Risk	Mitigation
Using honeypots in place of other security tools	Use with other enterprise security tools
Honeypots aren't alerting on intruders	Use with other enterprise security tools
Honeypots can be detected by attackers and manipulated	Their interaction has already been alerted on
High-interaction honeypots can provide attackers a pivot point	Position high-interaction honeypots outside the network, where they can't interact with internal systems

Conclusion

- **Honeypots are generally found in the form of:**
  - Honey Systems
  - Honey Services
  - Honey Tokens

- **To be effective, all honeypots must be:**
  - Deceptive
  - Discoverable
  - Interactive
  - Monitored

- **Honeypots are primarily used for:**
  - Research
  - Resource Exhaustion
  - Intrusion Detection

Reference Materials

References

- Sanders, C. (2020). *Intrusion Detection Honeypots: Detection Through Deception.* Chris Sanders.
- Intrusion Detection Honeypots: Detection Through Deception - Chris Sanders – PSW #668
  - https://www.youtube.com/watch?v=m8i02Hr_g6s
- Stoll, C. (1990). *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage.* Pocket Books.
- An Evening with Berferd In Which a Cracker is Lured, Endured, and Studied.
  - http://cheswick.com/ches/papers/berferd.pdf
- Joint Publication 3-13.4, Military Deception
  - https://info.publicintelligence.net/JCS-MILDEC.pdf
- Strand, J. (2017). *Offensive Countermeasures: The Art of Active Defense.* John Strand
- Black Hills Information Security – Projects
  - https://www.blackhillsinfosec.com/projects/
- Active Defense Harbinger Distribution
  - https://www.activecountermeasures.com/free-tools/adhd/
- Canary Tokens
  - https://docs.canarytokens.org/guide/
- OpenCanary
  - https://opencanary.readthedocs.io/en/latest/

References (cont.)

- How You Can Set up Honeytokens Using Canarytokens to Detect Intrusions
  - https://zeltser.com/honeytokens-canarytokens-setup/
- The Honeynet Project
  - https://www.honeynet.org/about/
- Best Honeypots for Detecting Network Threats
  - https://securitytrails.com/blog/top-20-honeypots
- What is a honeypot?
  - https://usa.kaspersky.com/resource-center/threats/what-is-a-honeypot
- Epidemic: Researchers Find Thousands of Medical Systems Exposed to Hackers
  - https://securityledger.com/2015/09/epidemic-researchers-find-thousands-of-medical-systems-exposed-to-hackers/
- Honeypots Illustrate Scores of Vulnerabilities in Medical Devices
  - https://threatpost.com/honeypots-illustrate-scores-of-vulnerabilities-in-medical-devices/116280/
- Web Labyrinth
  - https://github.com/mayhemiclabs/weblabyrinth
- Artillery
  - https://github.com/BinaryDefense/artillery
- Cowrie
  - https://github.com/cowrie/cowrie

Questions

Upcoming Briefs

- QakBot/Qbot Malware (10/29)
- SMB-Based Attacks Targeting Healthcare (11/05)

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to **HC3@HHS.GOV**.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV** or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**

About Us

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently impacting threats via the HHS OIG

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing document and presentation that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic or want to join our listserv? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.

Contact

Health Sector Cybersecurity Coordination Center (HC3)

(202) 691-2110

HC3@HHS.GOV