

# Catching More Flies

Spotting the Adversary With Honey Techniques

Matthew Gracie  
BSidesROC  
March 18, 2023

Who Am I And What Am I Talking About?

Detection Engineering

Vs.

Deception Engineering



**Chris Sanders** 🔍 🧠 ✅  
@chrissanders88



See-Think-Do 🧠

If you know where someone will look, you can control what they see. Put something valuable there, and you control what they think. Provide an opportunity for interaction and you can control what they do.

9:15 AM · Jan 23, 2023 · **1,241** Views

# Enterprise tactics

Tactics represent the "why" of an ATT&CK technique or sub-technique. It is the adversary's tactical goal: the reason for performing an action. For example, an adversary may want to achieve credential access.


Enterprise Tactics: 14

ID	Name	Description
TA0043	Reconnaissance	The adversary is trying to gather information they can use to plan future operations.
TA0042	Resource Development	The adversary is trying to establish resources they can use to support operations.
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.
TA0003	Persistence	The adversary is trying to maintain their foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005	Defense Evasion	The adversary is trying to avoid being detected.
TA0006	Credential Access	The adversary is trying to steal account names and passwords.
TA0007	Discovery	The adversary is trying to figure out your environment.
TA0008	Lateral Movement	The adversary is trying to move through your environment.
TA0009	Collection	The adversary is trying to gather data of interest to their goal.
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.
TA0010	Exfiltration	The adversary is trying to steal data.
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

# Prerequisites

- Asset Inventory
- Centralized Logging
- Alerting Function
- Incident Response Plan

# Canarytokens



AWS keys ▼

Provide an email address or webhook URL (or both space separated)

Reminder note when this token is triggered, like: AWS keys placed on Jim's laptop

Fill in the fields above

# Canarytokens

## Canarytoken triggered

### ALERT

An HTTP Canarytoken has been triggered by the Source IP [REDACTED]

#### Basic Details:

Channel	HTTP
Time	2023-02-22 20:23:09 (UTC)
Canarytoken	vmftuufubslqn9ipzvju5wy29
Token Reminder	AWS Canarytoken Test
Token Type	aws_keys
Source IP	[REDACTED]
User Agent	aws-cli/1.18.69 Python/3.8.10 Linux/5.4.0-136-generic botocore/1.16.19

#### Canarytoken Management Details:

Manage this Canarytoken [here](#)

More info on this token [here](#)

Powered by: [Thinkst Canary](#)



# Canarytokens

- AWS Keys
- Azure Credentials
- Office Documents
- DNS Lookups
- Windows EXEs
- Web Redirects
- Credit Cards
- Wireguard Profiles
- And many more...

# Honeydocs

- Build a temptingly named file and put it on a file share – something like PAYROLL\_DATA.XLS
- Take the hash of the file
- Write a Zeek Intel rule for the hash
- Write an endpoint alerting tool for the hash

# Honeycreds

- Create a domain account named WEBADMIN or something similar
- Give it no valid login hours
- Put the credentials in a honeydoc somewhere
- OR seed the credentials in memory on a sampling of machines using Runas<sup>1</sup>
- Write an alert to detect logins from the account

# Other Honey Techniques

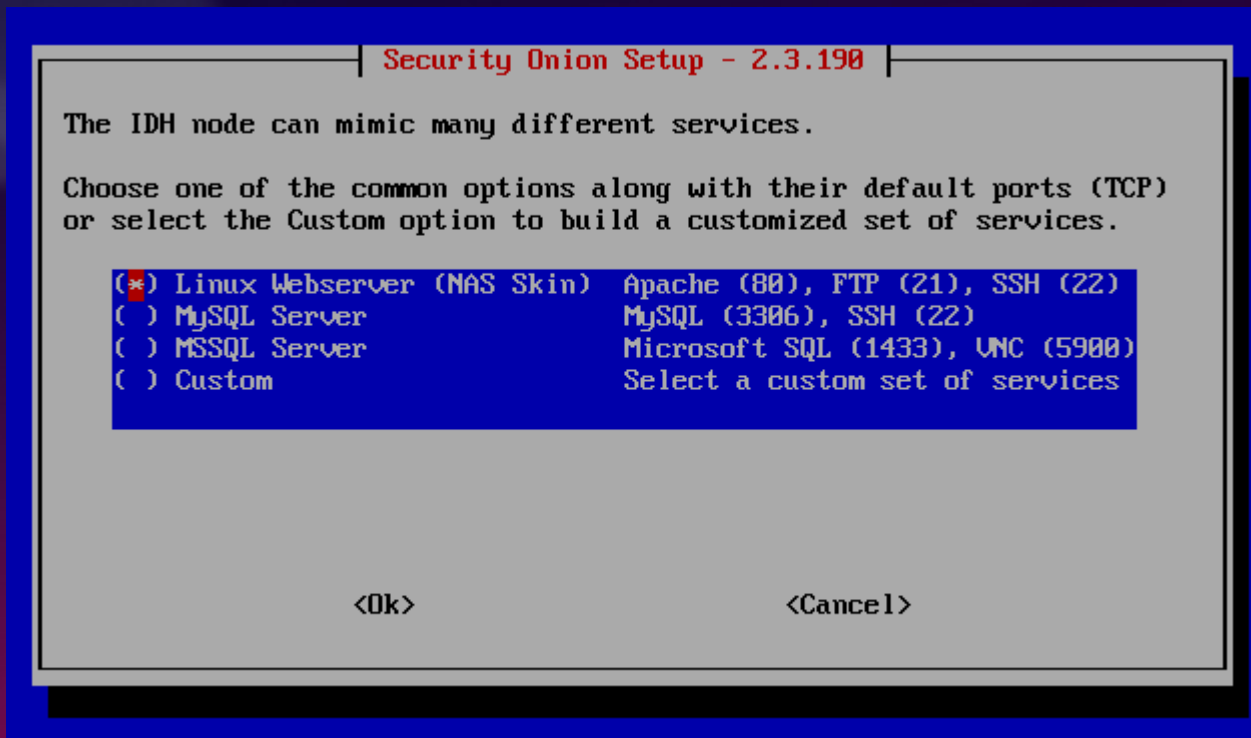
There are some interesting possibilities out there for threat-informed deception engineering:

- Windows Process Killed canary<sup>2</sup>
- Windows Uninstaller canary<sup>3</sup>

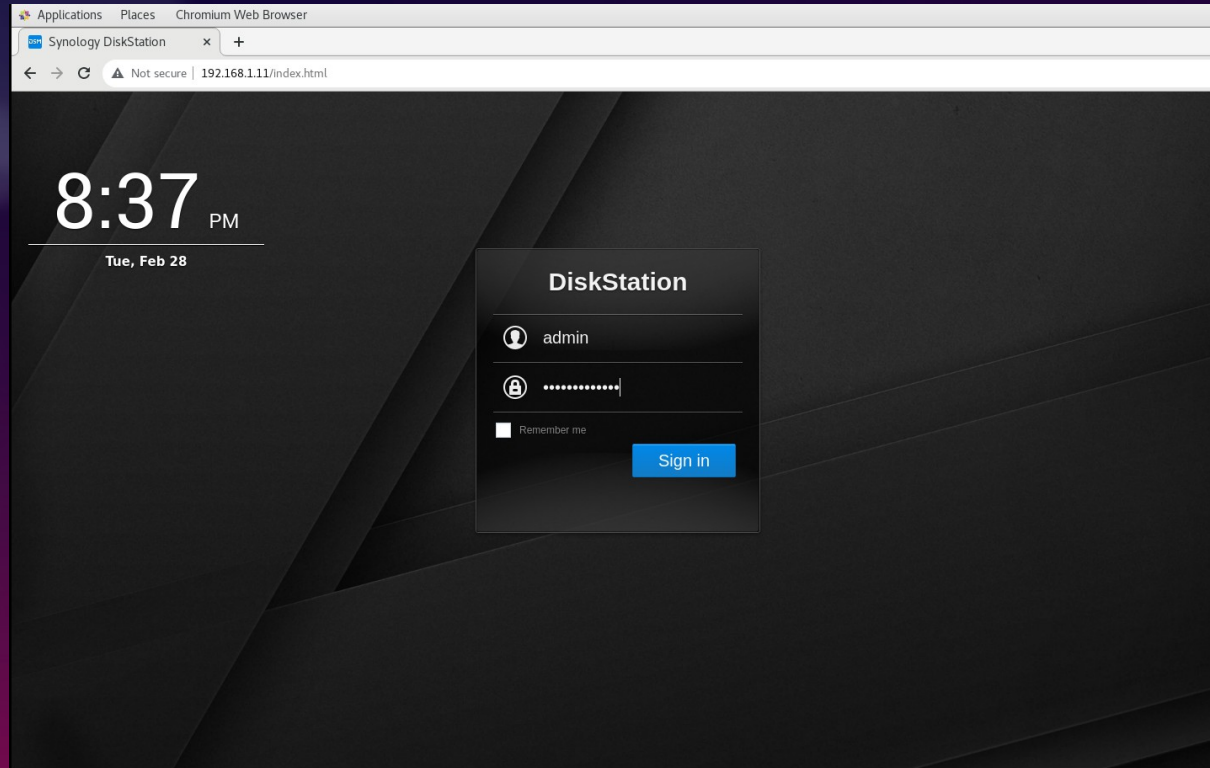
# Intrusion Detection Honeypots

- What if the whole server was a trap?
- Different than a research honeypot
- Emulate a production server configuration
- Raise alerts when there is interaction
- Security Onion IDH nodes are based on Thinkst Opencanary platform

# Intrusion Detection Honeypots



# Intrusion Detection Honeypots



# Intrusion Detection Honeypots

The screenshot displays the Security Onion Alerts web interface. The left sidebar contains navigation links: Overview, Alerts, Dashboards, Hunt, Cases, PCAP, Grid, Downloads, and Administration. The main content area is titled 'Alerts' and shows a list of alerts. The interface includes a search bar, a 'Group By' dropdown, and a 'Filter Results' button. The alerts are displayed in a table with columns for Count, rule.name, event.module, and event.severity\_label. Two alerts are shown, both with a count of 1 and a severity of 'critical'. The first alert is 'SO IDH - HTTP Accessed' and the second is 'SO IDH - HTTP Login Attempt'. The interface also shows a 'Fetch Limit' of 500 and a 'Rows per page' of 50. The footer indicates the version is 2.3.210 and includes copyright information for Security Onion Solutions, LLC.

Security Onion Alerts

Overview Alerts Dashboards Hunt Cases PCAP Grid Downloads Administration

Alerts

Options

Total Found: 2

Search: Group By Name, Module

Last 24 hours

Fetch Limit: 500

Filter Results

Count	rule.name	event.module	event.severity_label
1	SO IDH - HTTP Accessed	playbook	critical
1	SO IDH - HTTP Login Attempt	playbook	critical

Rows per page: 50 1-2 of 2

Version: 2.3.210 © 2023 Security Onion Solutions, LLC Terms and Conditions




# Conclusion



**SwiftInSecurity**  
@SwiftOnSecurity



To defeat attackers, you gotta bring them down to your level, and just beat the  out of them with it. It's your god damn network.

7:26 PM · Jun 12, 2019



**David Weston (DWIZZLE)**   
@dwizzzleMSFT



Don't play their game, make them play yours.

2:07 PM · Sep 21, 2019

# Questions?



@InfosecGoon



infosecgoon@roadflares.org



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

# Links

1 - <https://logrhythm.com/blog/using-honeywords-to-make-password-cracking-detectable/>

2 - <https://research.nccgroup.com/2021/03/04/deception-engineering-exploring-the-use-of-windows-service-canaries-against-ransomware/>

3 - <https://research.nccgroup.com/2021/03/16/deception-engineering-exploring-the-use-of-windows-installer-packages-against-first-stage-payloads/>