PHISHING BAIT

UNDERSTANDING AND DEMONSTRATING REAL-WORLD PHISHING ATTACKS

Presented By:

ELI DAVID AND AZSANTE HAWKINS

June 9, 2025

INTRODUCTION TO PHISHING

WHAT IS PHISHING?

- A method of tricking users into revealing sensitive data.
- Often done through fake websites, emails, or messages.
- One of the most common and effective cyber threat

COMMON PHISHING TECHNIQUES

Spear Phishing

- A highly targeted form of phishing.
- Attacker customizes emails or messages using specific details about the victim (name, job title, contacts).
- Often appears to come from a trusted source, such as a colleague or supervisor.

Whaling

- A specialized type of spear phishing aimed at high-level executives or key decision-makers.
- Attacks often mimic urgent business requests, like wire transfers or document sign-offs.
- Success can lead to significant financial or identity damage.

COMMON PHISHING TECHNIQUES

Smishing

- Phishing conducted through SMS or messaging apps.
- Messages may include malicious links, fake alerts, or requests for login details.
- Frequently impersonates delivery services, banks, or tech support.

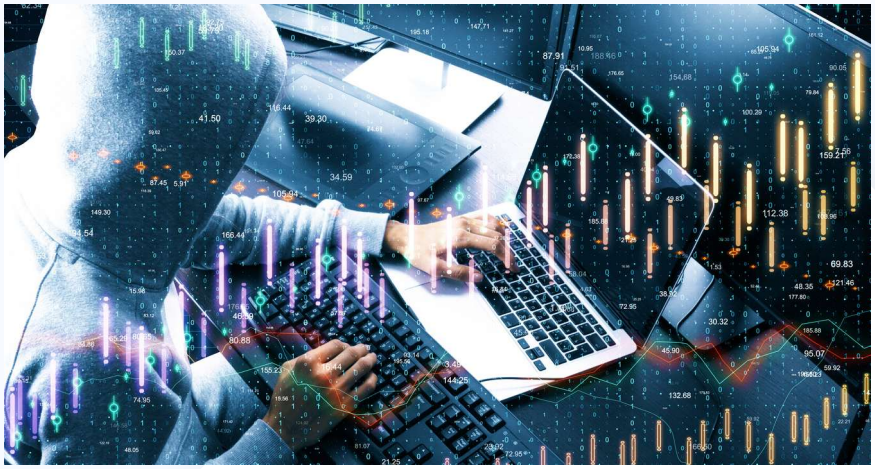
Vishing

- Voice phishing via phone calls.
- Attackers may pose as government agents, bank officials, or tech support.
- Goal is to verbally extract sensitive information like account credentials or social security numbers.

WHY IT MATTERS

WHY IS PHISHING SO DANGEROUS?

- Exploits human trust and behavior
- Often leads to data breaches, financial loss, and identity theft
- Users tend to reuse passwords across multiple accounts



CYBERSECURITY'S ROLE

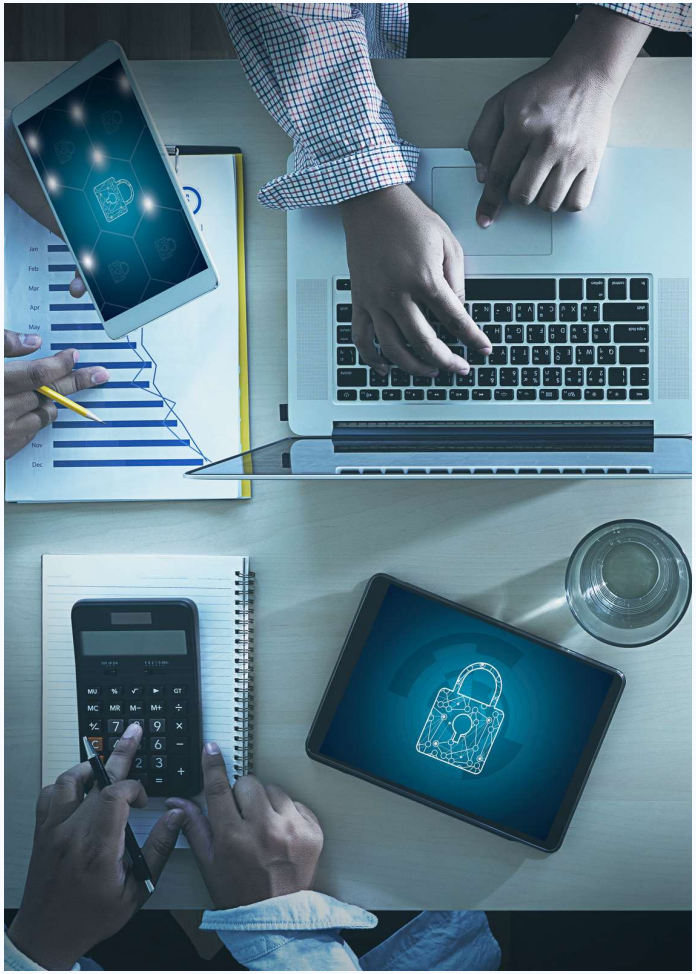
OUR JOB IN CYBERSECURITY

- Detecting and preventing phishing attempts
- Training users to recognize suspicious activity
- Using tools like MFA and email filtering
- Maintaining system security and data integrity

PROJECT OBJECTIVE

PURPOSE OF OUR PROJECT

- ☑ Demonstrate how phishing attacks are executed
- ☑ Raise awareness about common tactics
- ☑ Show how stolen credentials can be misused
- ☑ Promote education and prevention



TOOLS USED

TOOLS FOR THE ATTACK SIMULATION

SOCIAL-ENGINEER TOOLKIT (SET)

For cloning websites

KALI LINUX

The operating system used

DNS SPOOFING

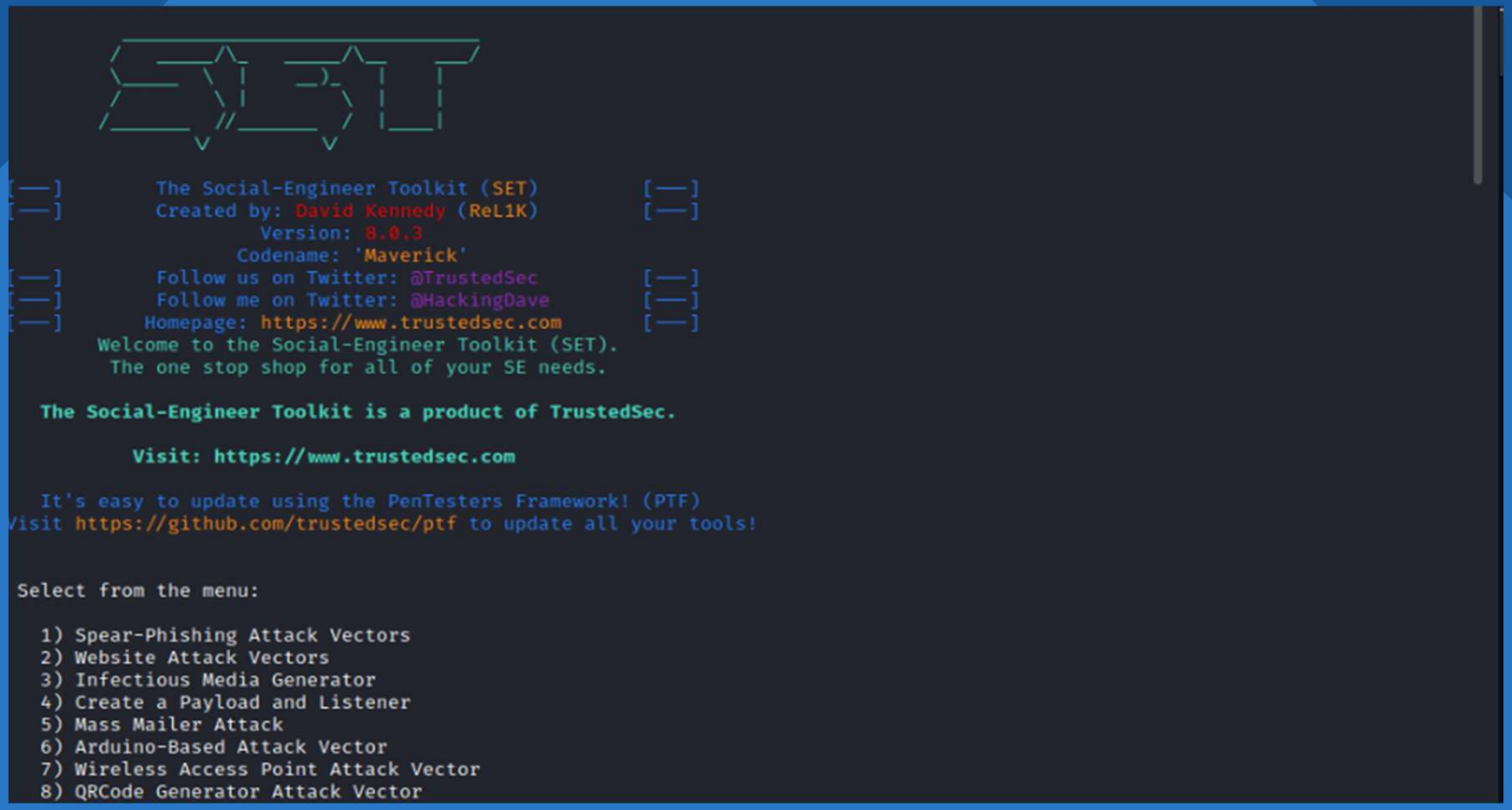
Redirected victims to a fake site

ATTACK SCENARIOS

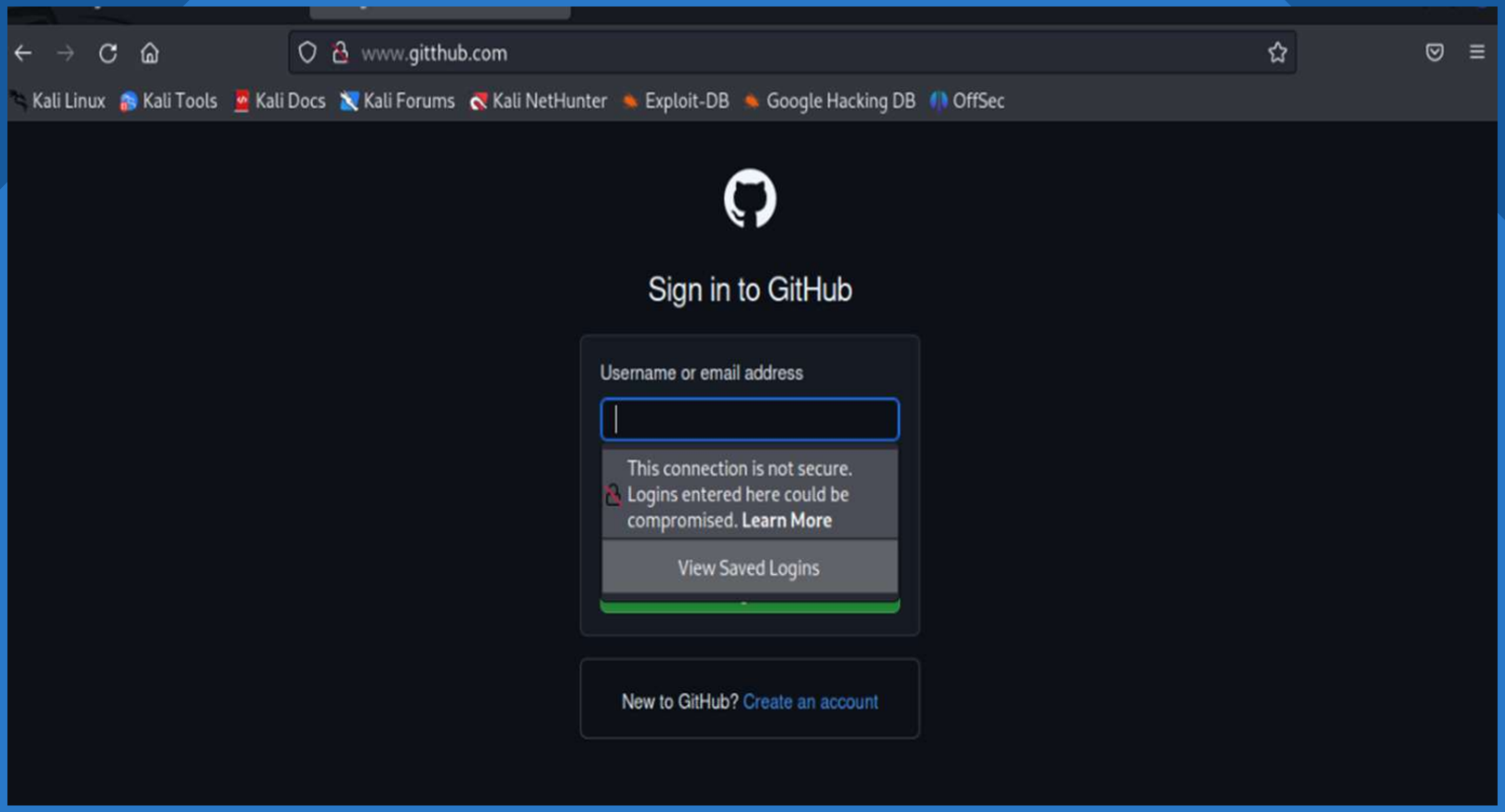
HOW WE DID IT

- Cloned LinkedIn login page using SET
- Used DNS spoofing to reroute github.com to our fake site
- Created a phishing email with a malicious link
- Sent email to a fictional executive (John Doe)
- Collected credentials entered on the fake page

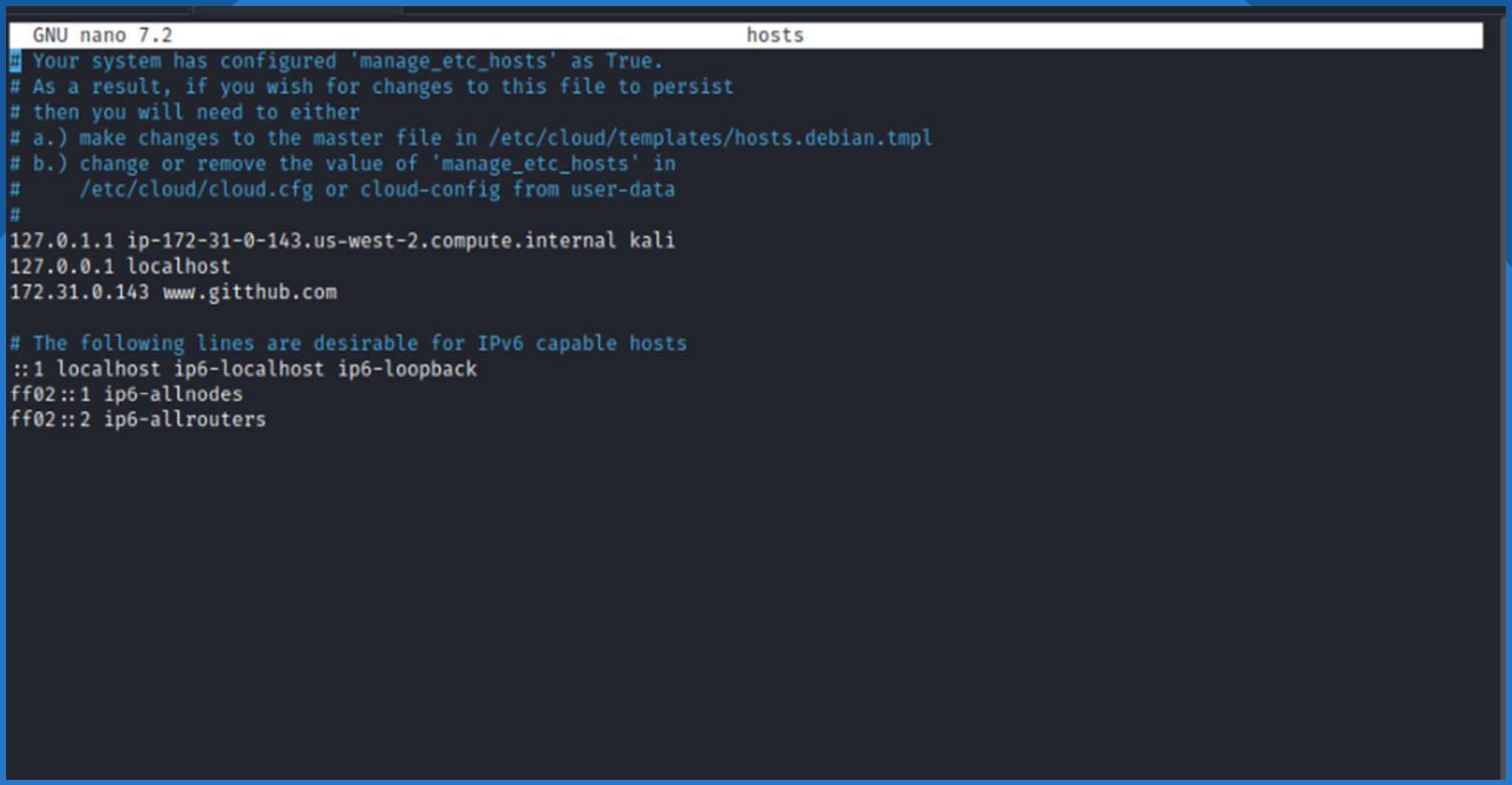
SOCIAL ENGINEERING TOOL



CLONED WEBSITE (SET)



DNS SPOOFING



EMAIL DRAFT

Audit Please Loggin Inbox ×

Azsante Hawkins <azsantehawkins33@yahoo.com> 5:51 PM (4 minutes ago)

to me

Hi [Azsante],

As part of our ongoing internal security audit, we're asking all administrators to verify their access credentials through our secure portal.

Please log in at your earliest convenience to complete the verification process:

gittub.com *(Secure Internal Access Only)*

This is a routine measure to ensure compliance with our updated infrastructure access policies. If you encounter any issues accessing the portal or have questions, reach out to [IT/Security contact] immediately.

Thank you for your prompt attention to this matter.

Best regards,

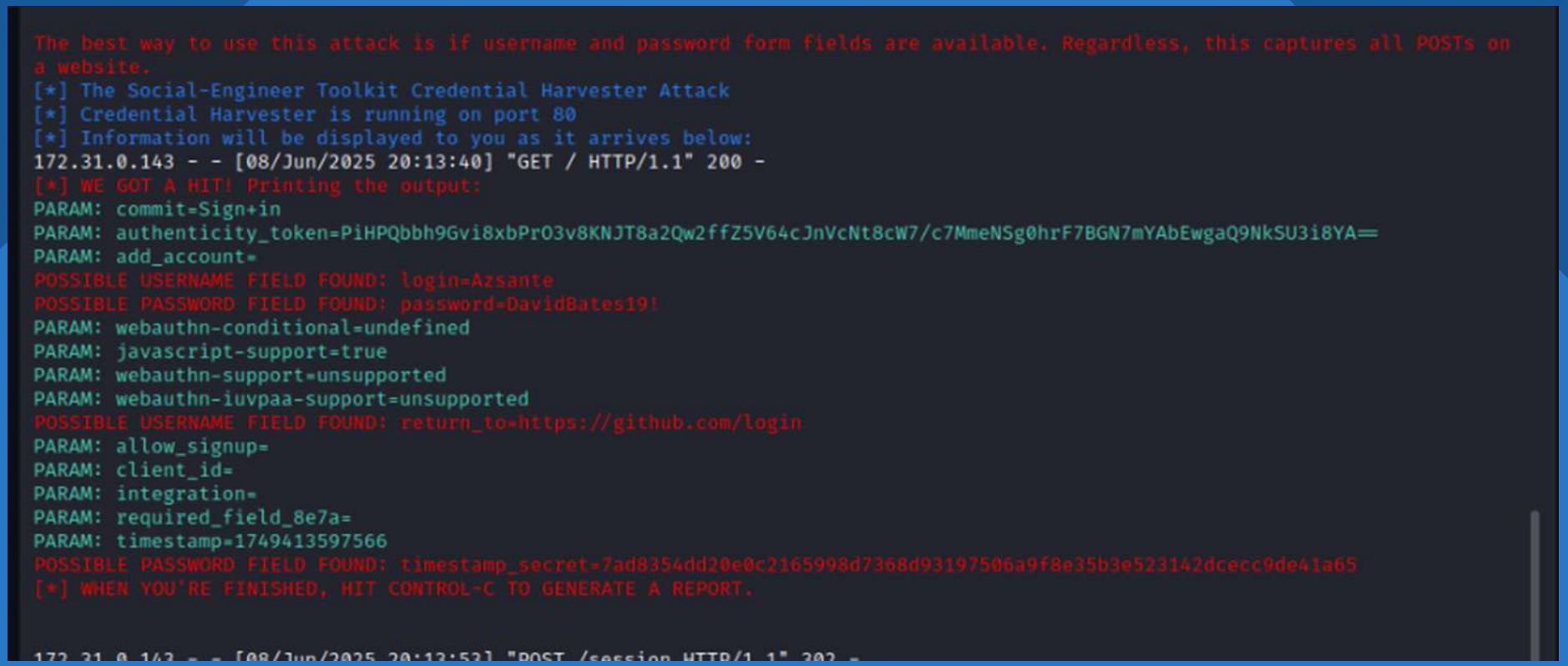
[Darnell Hawkins]

Chief Executive Officer

GitHub

[darnellhawkins@gitthub.com]

COLLECTION OF INFORMATION



REAL WORLD IMPACT

THE CONSEQUENCES

- Stolen Credentials - Access to multiple systems
- Targeted Individuals (e.g., executives) = Higher Risk
- Breaches can be fast and far-reaching

DEFENSE AND PREVENTION

HOW TO PROTECT AGAINST PHISHING

- Never click suspicious links
- Use strong, unique passwords
- Enable multi-factor authentication
- Conduct regular cyber security training

CONCLUSION

WHAT WE LEARNED

Key Takeaways

- Phishing remains a major threat due to human error
- Tools like SET are easily available to attackers
- Awareness and training are the best defense
- Stay vigilant, stay secure