SET

SOCIAL ENGINEER TOOLKIT

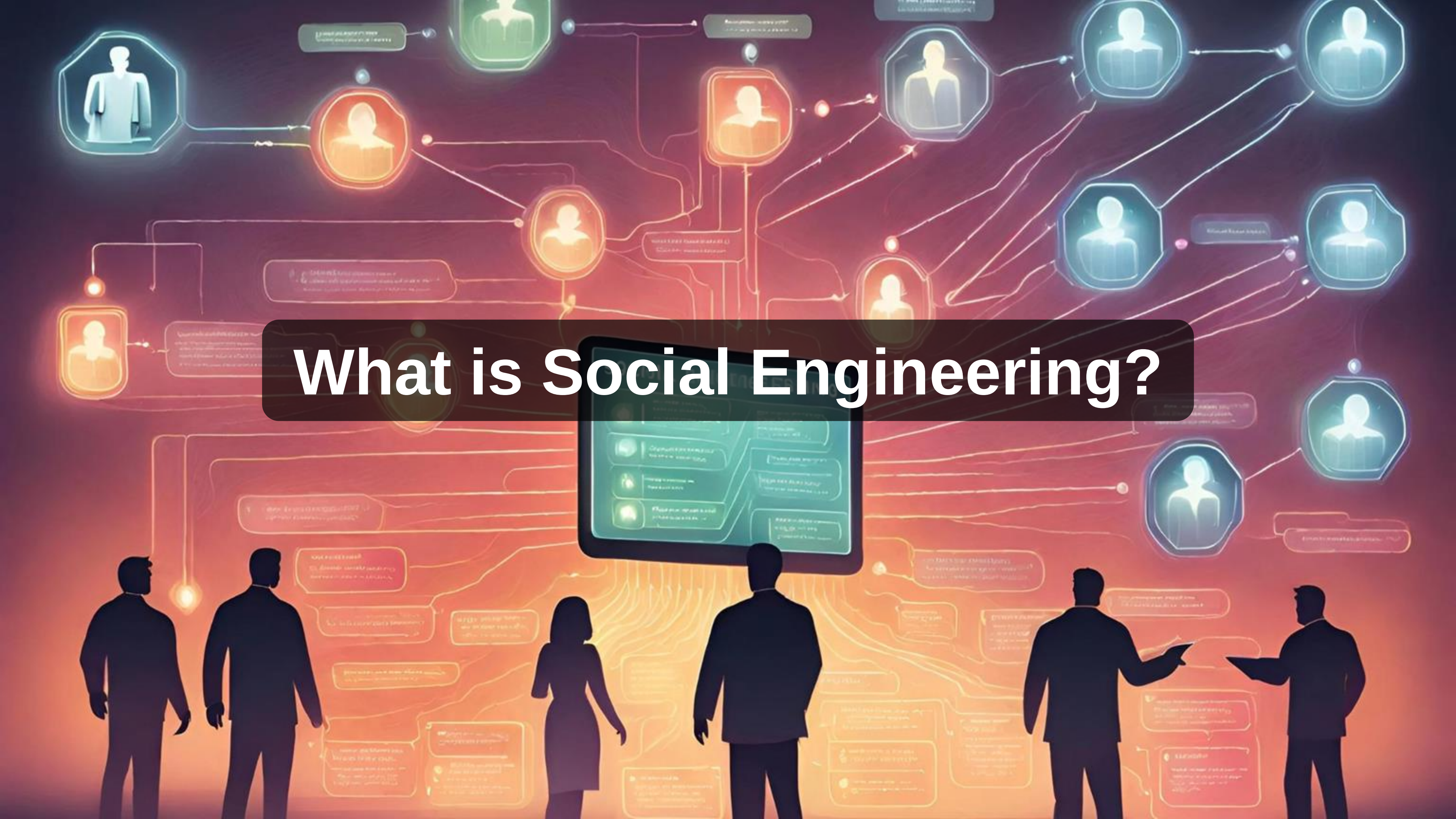
BY: ETHAN CANTRELL, COLLIN JANECKA, CARLOS BROWN, JOSEPH FAUNCE

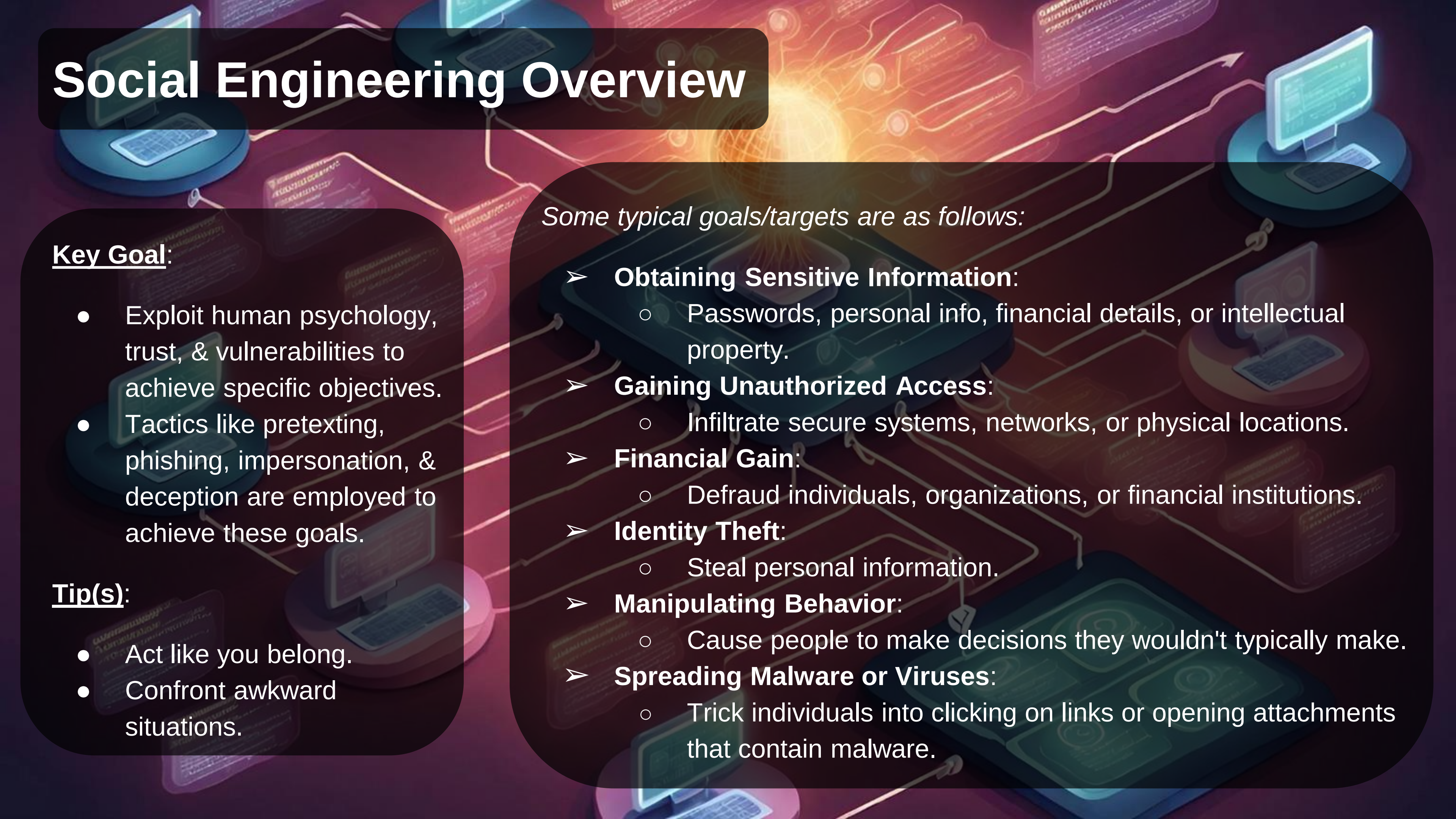
Goal

- The objective is to present specific tools within SET.
- Illustrate the tools’ potential application in a social engineering campaign.
- This presentation focuses on tools that do not involve the production or distribution of materials or outputs that could raise data concerns.

This approach is underpinned by a conscientious acknowledgment of the legal ramifications associated with particular aspects of the Social Engineering Toolkit.

What is Social Engineering?





Social Engineering Overview

<u>Key Goal</u>:

- Exploit human psychology, trust, & vulnerabilities to achieve specific objectives.
- Tactics like pretexting, phishing, impersonation, & deception are employed to achieve these goals.

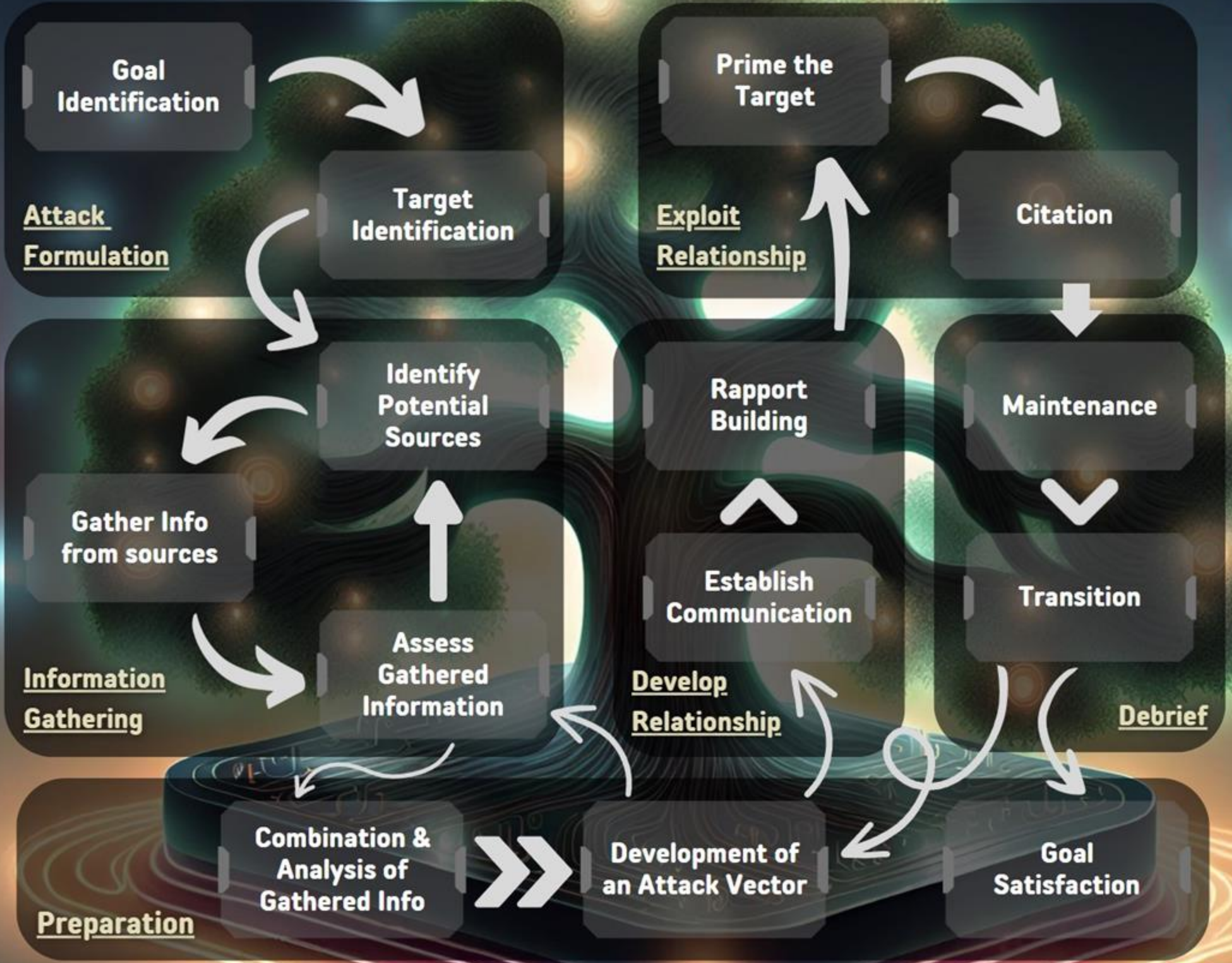
<u>Tip(s)</u>:

- Act like you belong.
- Confront awkward situations.

Some typical goals/targets are as follows:

- ➢ **Obtaining Sensitive Information**:
  - ○ Passwords, personal info, financial details, or intellectual property.
- ➢ **Gaining Unauthorized Access**:
  - ○ Infiltrate secure systems, networks, or physical locations.
- ➢ **Financial Gain**:
  - ○ Defraud individuals, organizations, or financial institutions.
- ➢ **Identity Theft**:
  - ○ Steal personal information.
- ➢ **Manipulating Behavior**:
  - ○ Cause people to make decisions they wouldn't typically make.
- ➢ **Spreading Malware or Viruses**:
  - ○ Trick individuals into clicking on links or opening attachments that contain malware.

Social Engineering Campaign Strategy



Attack Formulation

Goal Identification

Target Identification

Information Gathering

Identify Potential Sources

Gather Info from sources

Assess Gathered Information

Preparation

Combination & Analysis of Gathered Info

Development of an Attack Vector

Develop Relationship

Establish Communication

Rapport Building

Exploit Relationship

Prime the Target

Citation

Debrief

Maintenance

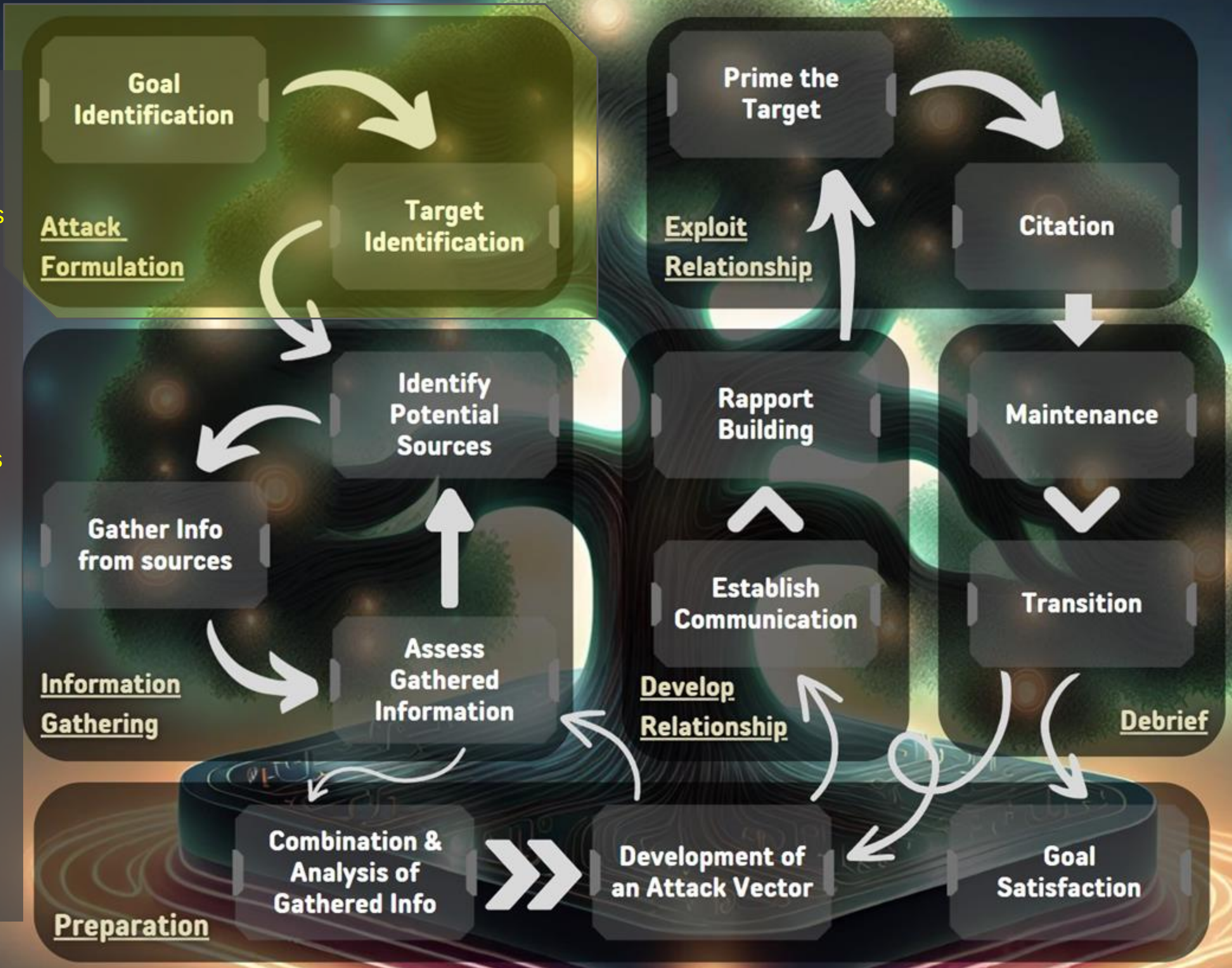
Transition

Goal Satisfaction

Social Engineering Campaign Strategy

Potential Target(s):

- General GitHub Users
- GitHub Developers
- Contributors and/or Collaborators
- Admin Privilege Users
- Users in Sensitive Industries
- GitHub Employees



Attack Formulation

Goal Identification

Target Identification

Information Gathering

Identify Potential Sources

Gather Info from sources

Assess Gathered Information

Preparation

Combination & Analysis of Gathered Info

Development of an Attack Vector

Develop Relationship

Establish Communication

Rapport Building

Exploit Relationship

Prime the Target

Citation

Debrief

Maintenance

Transition

Goal Satisfaction

Social Engineering Campaign Strategy

Potential Sources:

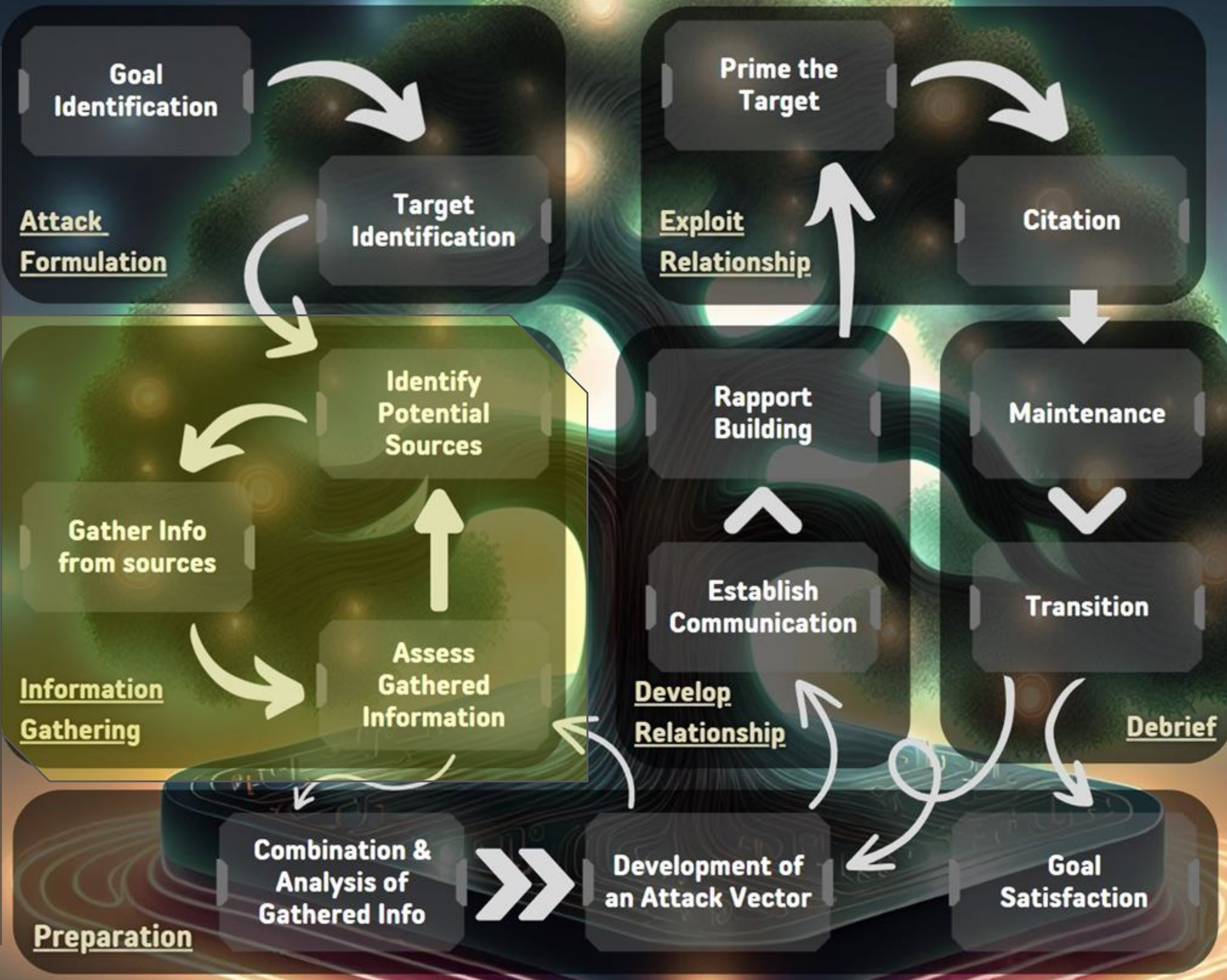
- Publicly Available Information
- Users with relevant data

Source Information:

- Used to Build Target Profile

Info Assessment:

- Data Evaluation
- Establish Relevance
- Further Exploitation



Attack Formulation

Goal Identification

Target Identification

Information Gathering

Identify Potential Sources

Gather Info from sources

Assess Gathered Information

Exploit Relationship

Prime the Target

Citation

Develop Relationship

Rapport Building

Establish Communication

Debrief

Maintenance

Transition

Preparation

Combination & Analysis of Gathered Info

Development of an Attack Vector

Goal Satisfaction

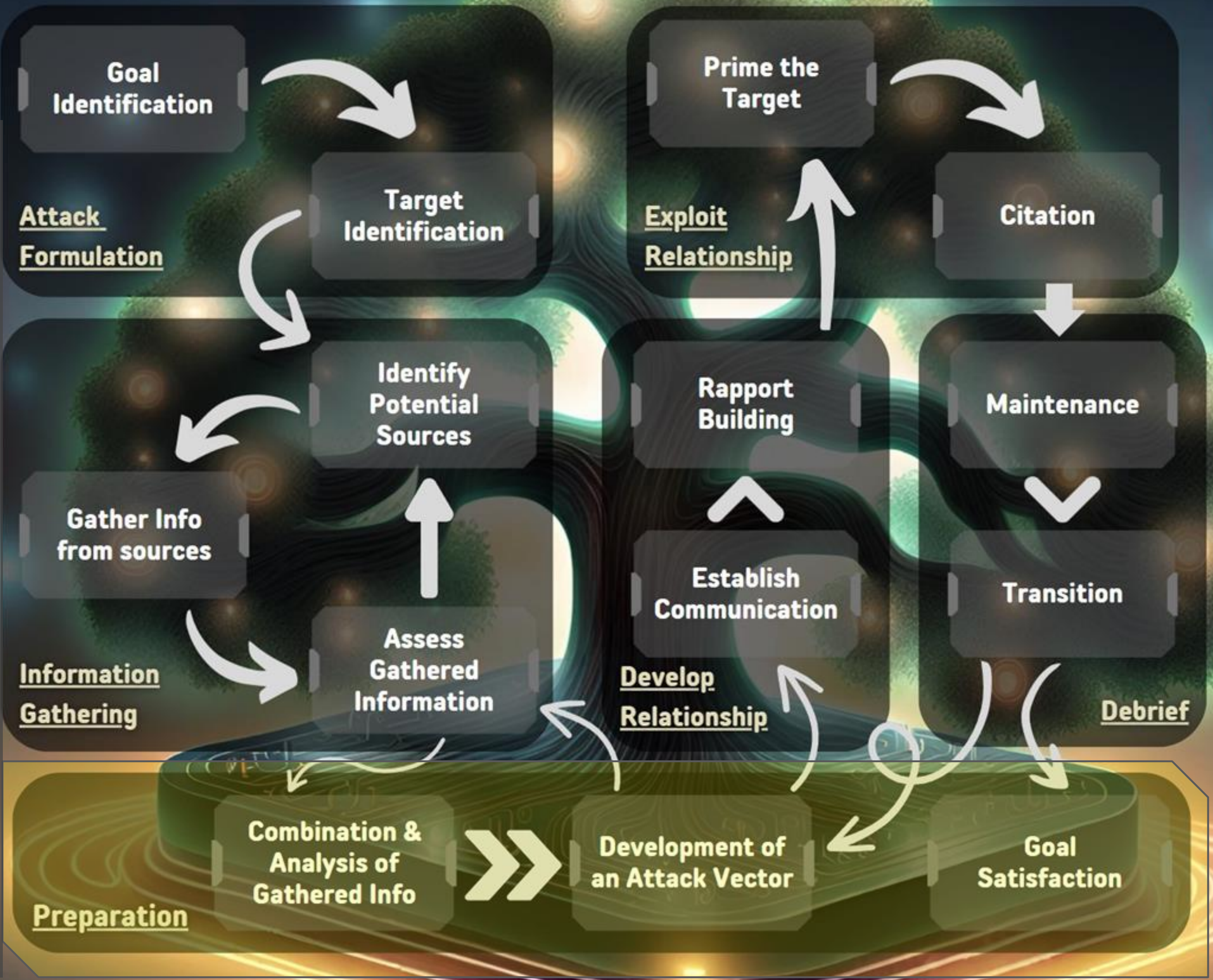
Social Engineering Campaign Strategy

Combine & Analyze:

- ➢ Identify Weak Points
- ➢ Understand Operational Environment
- ➢ Profile the Target
- ➢ Map Potential Attack Vectors

Develop an Attack:

- ➢ Tailor to Align with Target
- ➢ Psychology Manipulation
- ➢ Define Path to reach Goal



Attack Formulation

Goal Identification

Target Identification

Information Gathering

Identify Potential Sources

Gather Info from sources

Assess Gathered Information

Exploit Relationship

Prime the Target

Citation

Develop Relationship

Rapport Building

Establish Communication

Debrief

Maintenance

Transition

Preparation

Combination & Analysis of Gathered Info

Development of an Attack Vector

Goal Satisfaction

Goal Satisfaction:

- ➢ Gaining Access
- ➢ Information Extraction
- ➢ Influencing Behavior
- ➢ Mitigating Risks

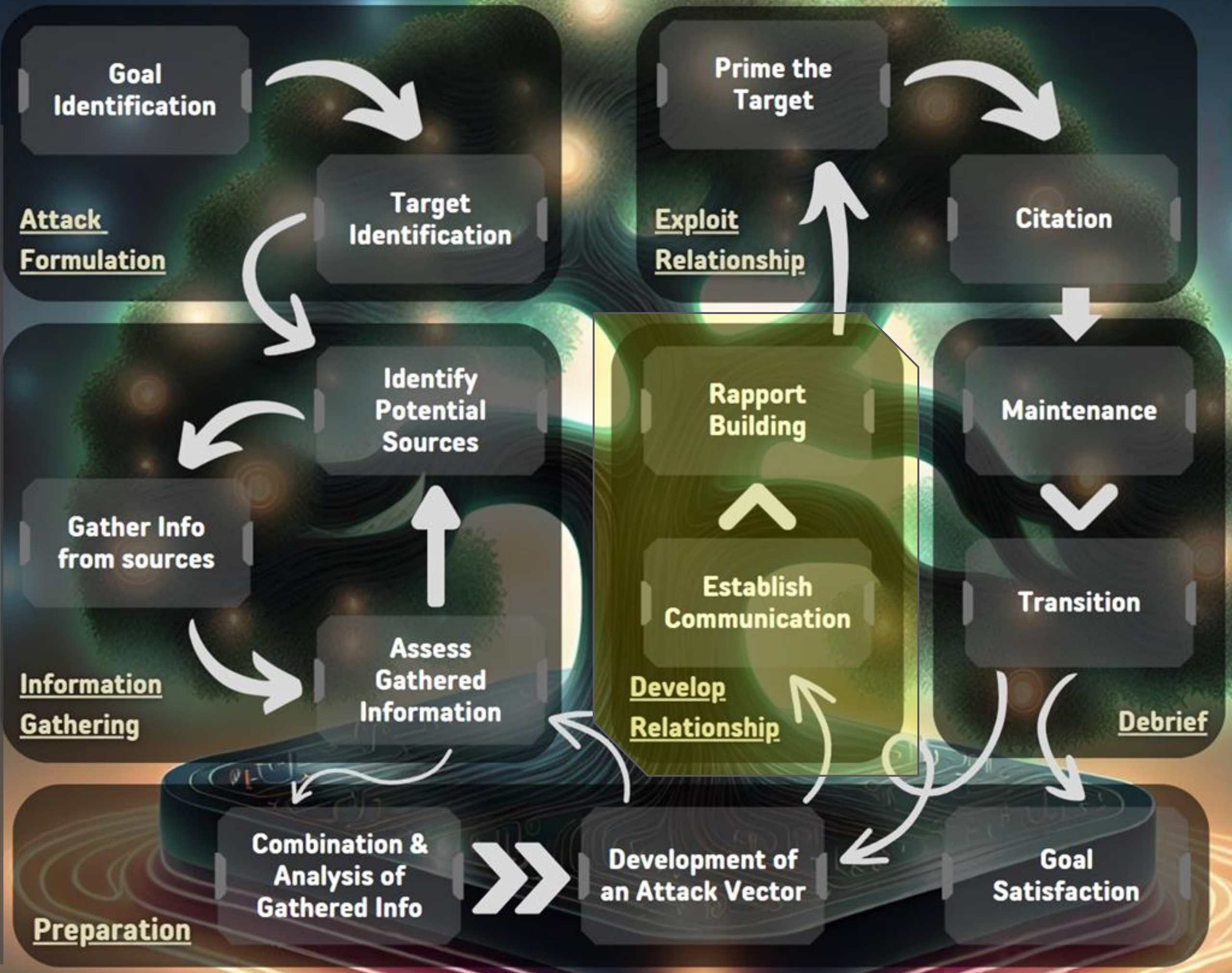
Social Engineering Campaign Strategy

Establish Coms:

- Contact Method
- Initial Contact
- Strategic Timing

Building Rapport:

- Natural Engagement
- Active Listening
- Empathy
- Consistency & Reciprocity
- Emotional Appeal



Attack Formulation

Goal Identification

Target Identification

Information Gathering

Identify Potential Sources

Gather Info from sources

Assess Gathered Information

Preparation

Combination & Analysis of Gathered Info

Development of an Attack Vector

Goal Satisfaction

Develop Relationship

Establish Communication

Rapport Building

Exploit Relationship

Prime the Target

Citation

Debrief

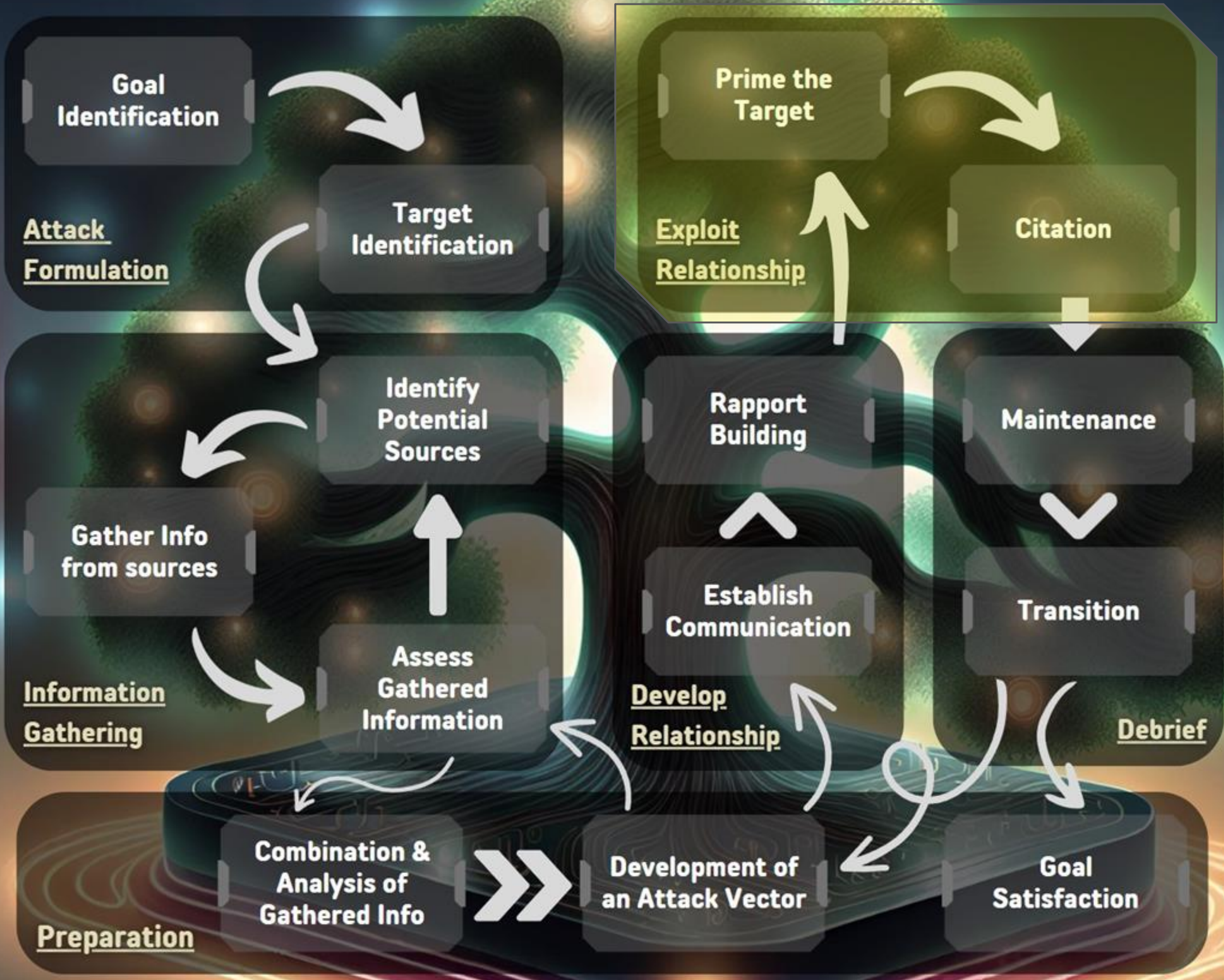
Maintenance

Transition

Social Engineering Campaign Strategy

Target Priming:

- ➢ Positive Framing
- ➢ Alignment with Beliefs
- ➢ Problem-Solution Approach
- ➢ Urgency & Necessity



Attack Formulation

Goal Identification

Target Identification

Information Gathering

Identify Potential Sources

Gather Info from sources

Assess Gathered Information

Preparation

Combination & Analysis of Gathered Info

Development of an Attack Vector

Develop Relationship

Establish Communication

Rapport Building

Exploit Relationship

Prime the Target

Citation

Debrief

Maintenance

Transition

Goal Satisfaction

Citation:

- ➢ Name-Dropping
- ➢ Fake Credentials
- ➢ Impersonation
- ➢ Appeal to Expertise

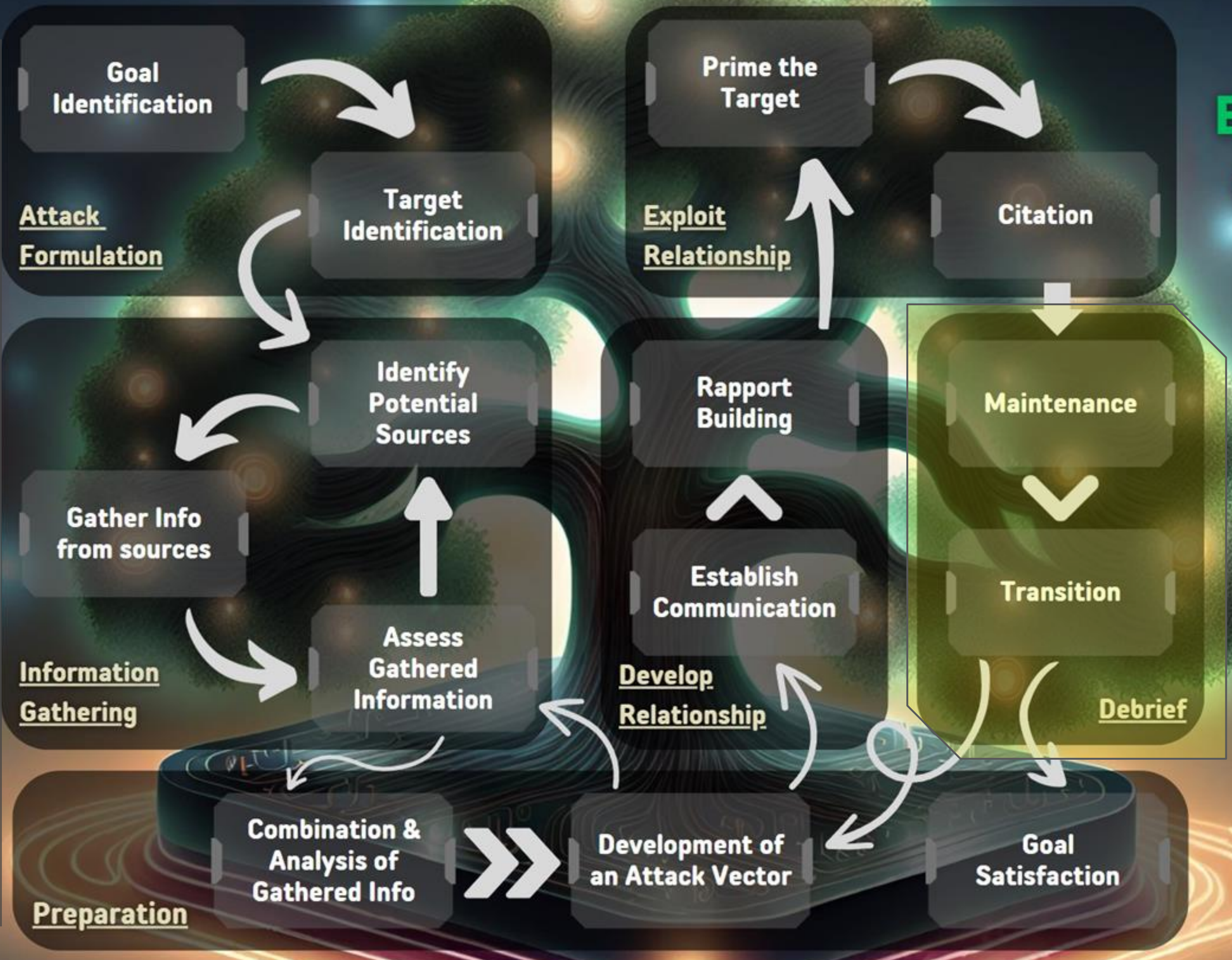
Social Engineering Campaign Strategy

Maintenance:

- ➢ Regular Contact
- ➢ Reinforce Trust
- ➢ Provide Feedback
- ➢ Address Concerns
- ➢ Maintain Pretense

Transition:

- ➢ Information Extraction
- ➢ Minimize Suspicion
- ➢ Complete Defined Goal(s)



Attack Formulation

Goal Identification

Target Identification

Information Gathering

Identify Potential Sources

Gather Info from sources

Assess Gathered Information

Preparation

Combination & Analysis of Gathered Info

Development of an Attack Vector

Develop Relationship

Establish Communication

Rapport Building

Exploit Relationship

Prime the Target

Citation

Debrief

Maintenance

Transition

Goal Satisfaction

Social Engineering Campaign - Example

GitHub Campaign

Goal: Deceive GitHub users into revealing their login credentials by posing as GitHub Support.

- ➢ **Prep**:
  - ○ Gather user information.
  - ○ Create spoofed email:
    - ■ support@ghubsecurityupdate.com
- ➢ **Contact**:
  - ○ Send phishing email, posing as the GitHub Security Team.
  - ○ Inform user(s) of a critical security update, required to to safeguard account.
- ➢ **Phishing Website**:
  - ○ Email linked to a cloned GitHub login page.
    - ■ QR Code attack is also viable here.
- ➢ **Credential Harvesting**:
  - ○ Unsuspecting users input their credentials.
    - ■ Info is collected & stored for future unauthorized use.

Continued

- ➢ **Confirmation & Redirection**:
  - ○ After inputting their credentials, users may believe they’ve completed the security verification.
    - ■ Users redirected to the official GitHub site.
- ➢ **Use of Stolen Credentials**:
  - ○ Unauthorized access to GitHub user accounts.
  - ○ Further exploitation for malicious purposes:
    - ■ Data theft.
    - ■ Spreading malware.
    - ■ Conduct further attacks.

The Social Engineering Toolkit (SET)

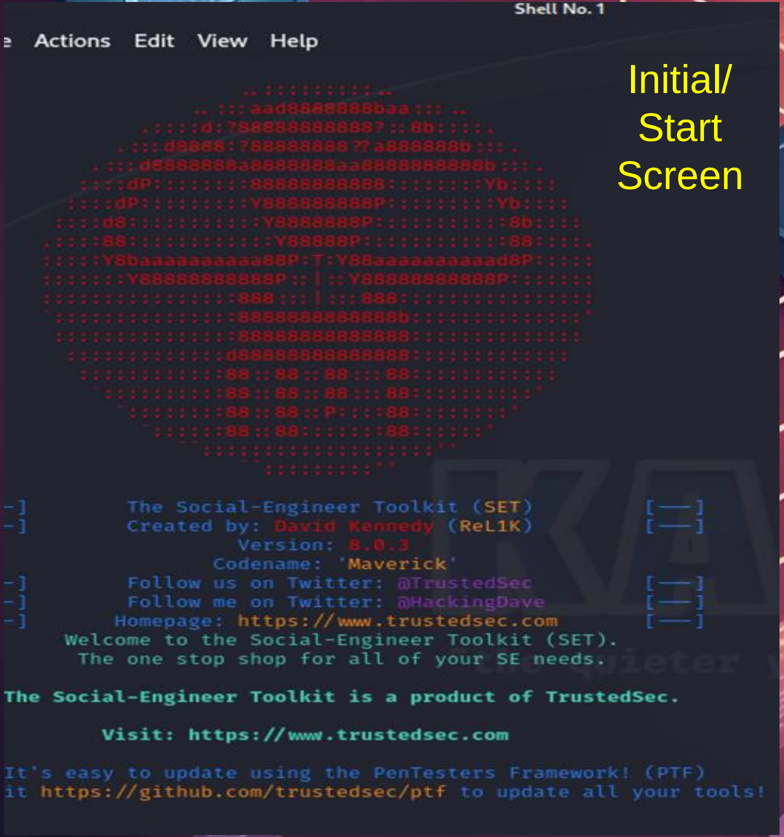
SET Description

- The Social Engineering Toolkit (SET) is a collection of tools integrated into Kali Linux, designed to target the human factor of cybersecurity.
- Open-source Python toolkit, freely available, encompassing a wide array of tools that facilitate diverse strategies for a social engineering campaign.
- SET also incorporates penetration testing attack vectors, in the form of Fast-Track.

Some of the tools within SET include:

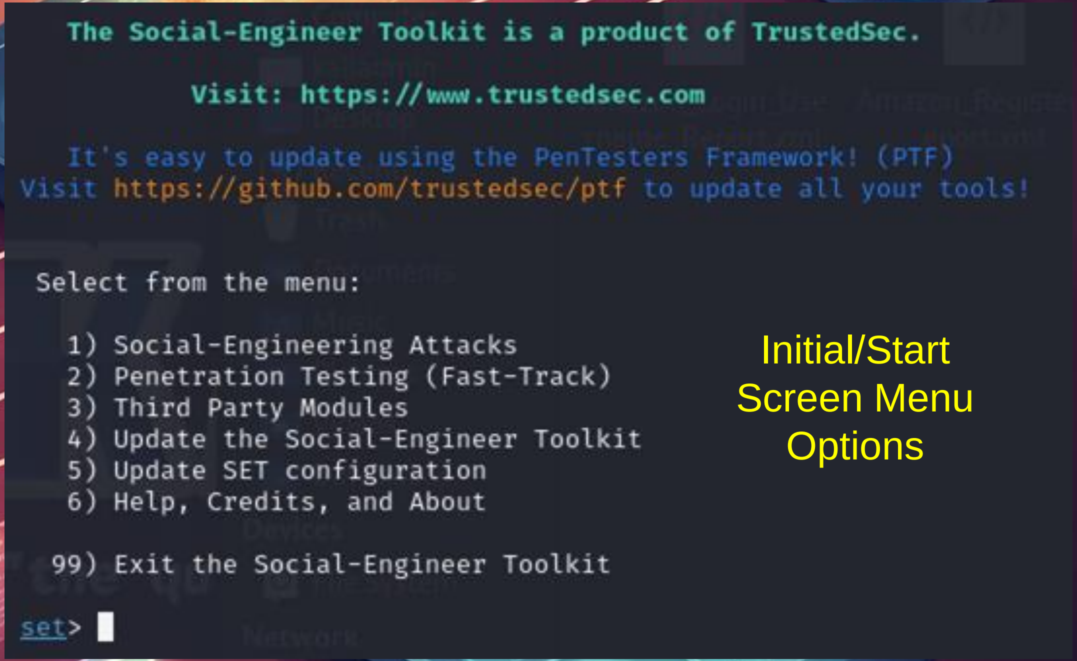
- Spear-Phishing Attacks
- Website Attacks
- Mass Mailing Attacks
- QRCode Attacks
- Powershell Attacks
- Creating Payloads & Listeners
- Arduino-Based Attacks
- Infectious Media Generator

Social Engineering Toolkit (SET) - Dashboard



```
-]          The Social-Engineer Toolkit (SET)          [---]
-]          Created by: David Kennedy (ReL1K)          [---]
                     Version: 8.0.3
                  Codename: 'Maverick'
-]          Follow us on Twitter: @TrustedSec          [---]
-]          Follow me on Twitter: @HackingDave         [---]
-]         Homepage: https://www.trustedsec.com        [---]
     Welcome to the Social-Engineer Toolkit (SET).
      The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

         Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
it https://github.com/trustedsec/ptf to update all your tools!
```

Initial/ Start Screen



```
   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 
```

Initial/Start Screen Menu Options

Pros & Cons of SET

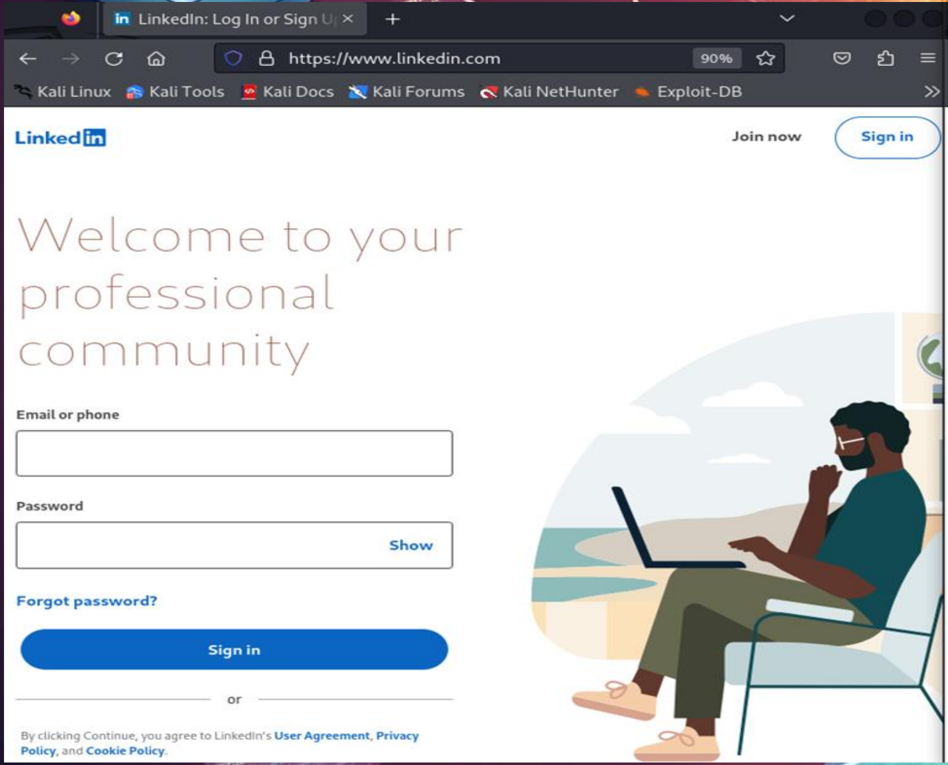
Pros: ✓

- **Versatility**: A diverse selection of specialized tools is available, & designed to address specific needs.
- **User-Friendly Interface**: Provides a menu-driven, user-friendly interface making it widely accessible.
- **Community Support**: With 2+ million downloads, SET has a strong user-base & community support.
- **Educational Value**: Can be used for educational purposes, helping individuals understand social engineering tactics & their mitigations.
- **Open Source**: SET is freely available, & its code can be inspected & modified by users, contributing to transparency & trust.

Cons: X

- **Legal & Ethical Concerns**: Unauthorized use can lead to criminal charges, & using it for malicious purposes is unethical.
- **Risk of Data Misuse**: Harvested data can be used for malicious activities, posing data risk.
- **Buggy**: Often requires application relaunch for the toolkit to properly function.
- **Prior Knowledge Needed**: Good understanding of social engineering, networking, & cybersecurity principles.
- **Platform Specific**: Primarily designed for Linux distributions. A less straightforward set-up is needed for macOS & Windows configurations.

Website Cloning & Credential Harvesting



LinkedIn: Log In or Sign Up

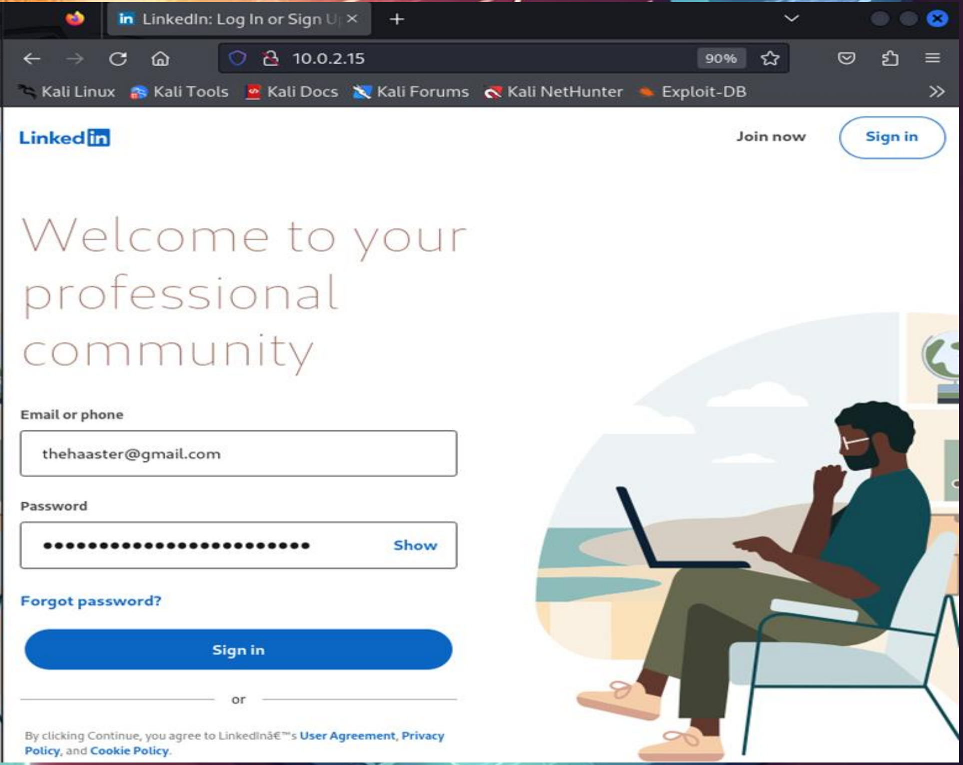
https://www.linkedin.com

Welcome to your professional community

Email or phone

Password

By clicking Continue, you agree to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy.



LinkedIn: Log In or Sign Up

10.0.2.15

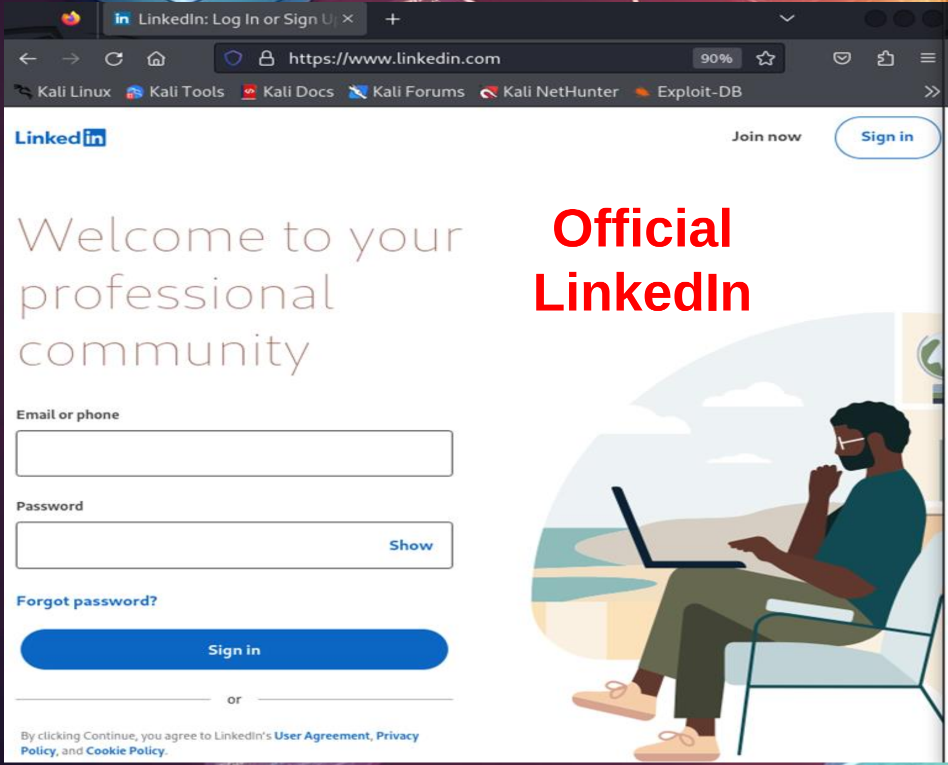
Welcome to your professional community

Email or phone: thehaaster@gmail.com

Password: ••••••••••••••••••••••••

By clicking Continue, you agree to LinkedInâ€™s User Agreement, Privacy Policy, and Cookie Policy.

Website Cloning & Credential Harvesting



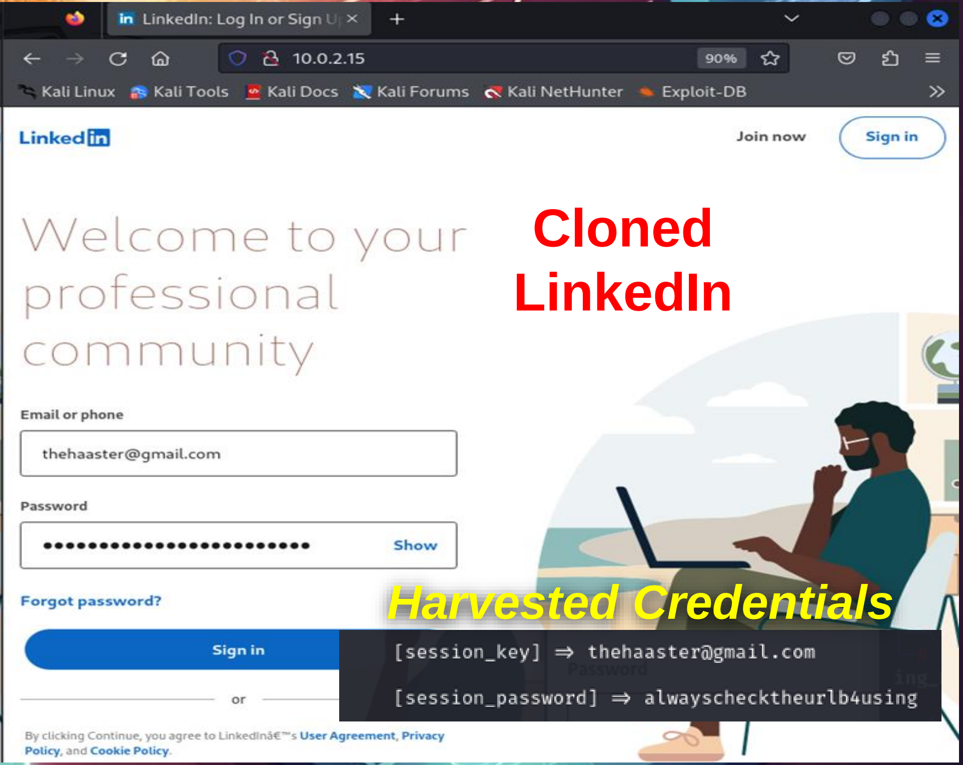
Official LinkedIn

Welcome to your professional community

Email or phone

Password

By clicking Continue, you agree to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy.



Cloned LinkedIn

Welcome to your professional community

Email or phone: thehaaster@gmail.com

Password: ••••••••••••••••••••••••

By clicking Continue, you agree to LinkedInâ€™s User Agreement, Privacy Policy, and Cookie Policy.

Harvested Credentials

```
[session_key] ⇒ thehaaster@gmail.com
[session_password] ⇒ alwayschecktheurlb4using
```

Attack of the Clones

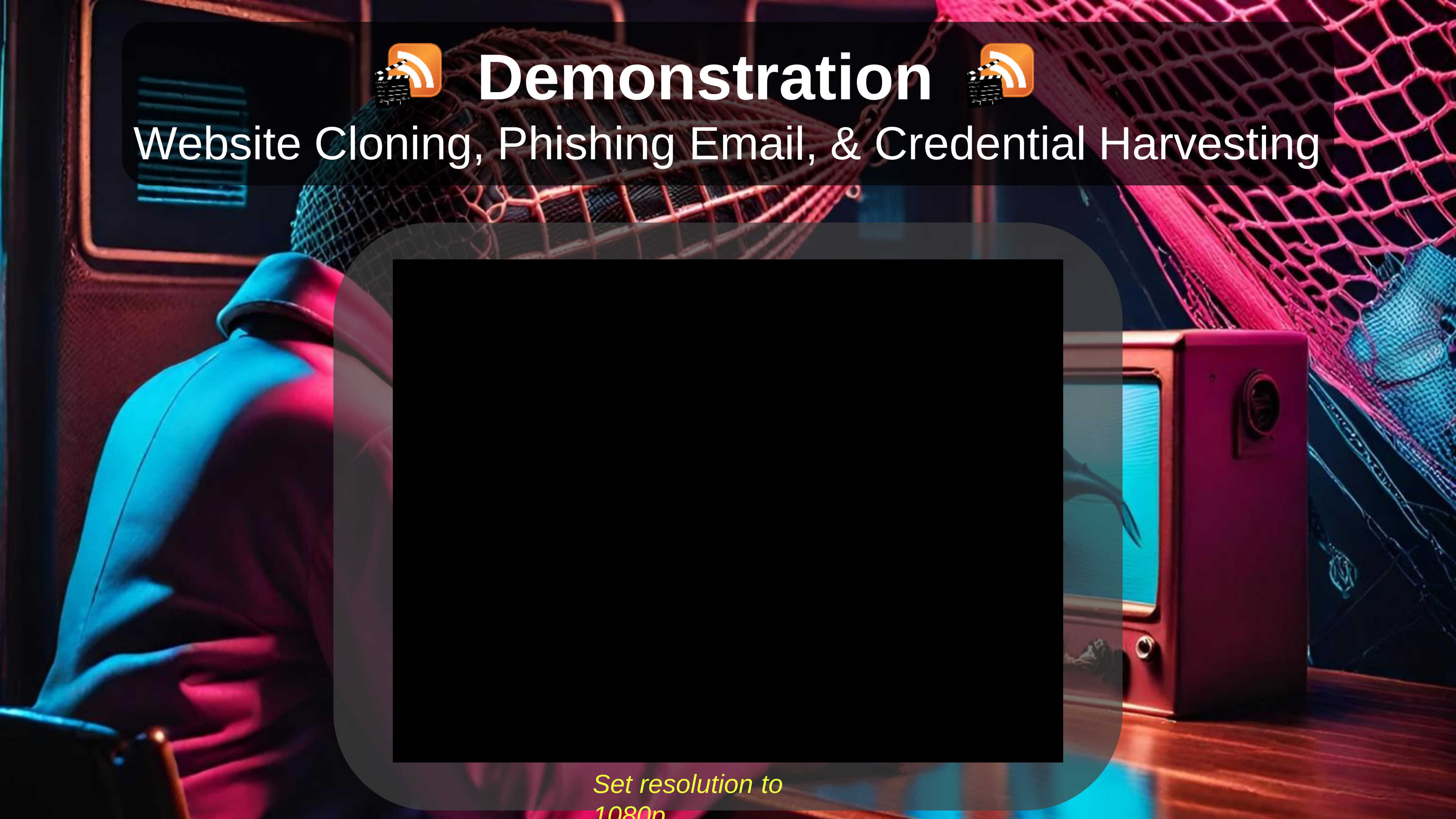
- Leverages Credential Harvester techniques to clone a website's login page, using both username & password fields.
    - For optimal usage, both the username & password fields should be on the same page.
    - Illustrated with Google as an example.
- Collects user credentials & other sensitive information, to be employed later for malicious purposes.
    - Credit Card info
    - Username/Passwords
    - Emails
    - etc

What we did.

- Used a cloned website in a phishing email
    - Cloned google website
    - Sent cloned site to emails with link attached
    - Gathered Potential Targets

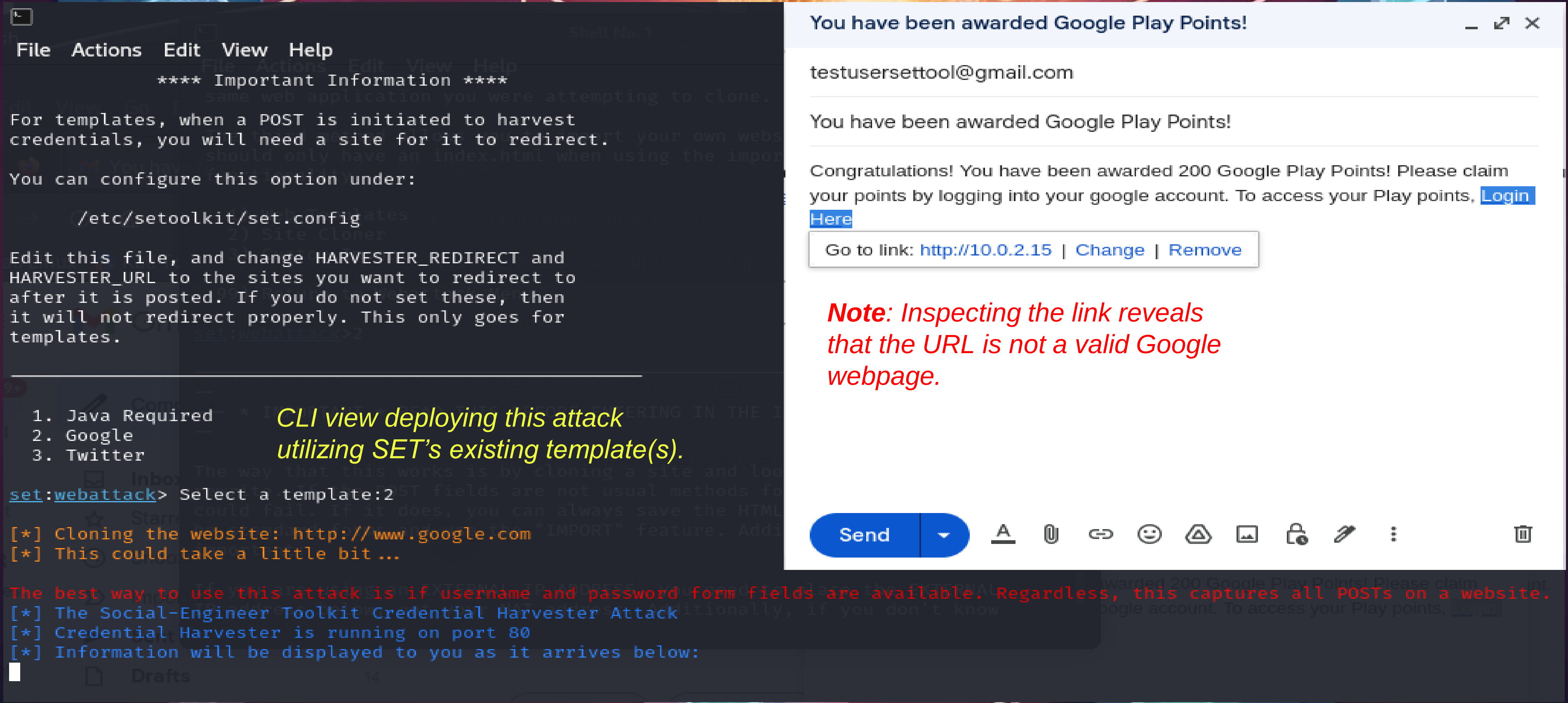
🎬 Demonstration 🎬

Website Cloning, Phishing Email, & Credential Harvesting



Set resolution to 1080p

Phishing Email linking to Cloned Website



```
                 **** Important Information ****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under:

      /etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

_______________________________________________________

  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template:2

[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

CLI view deploying this attack utilizing SET's existing template(s).

You have been awarded Google Play Points!

testusersettool@gmail.com

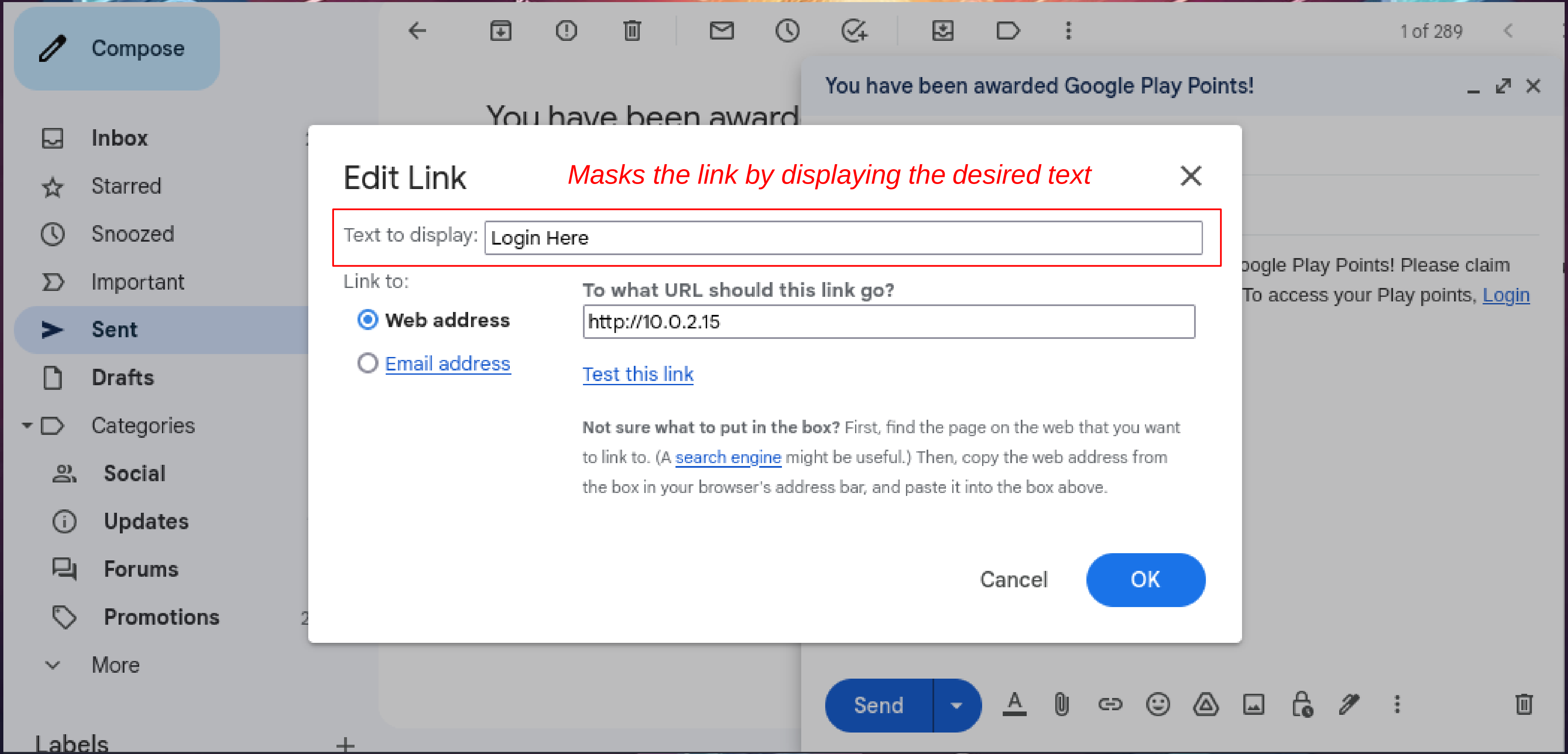
You have been awarded Google Play Points!

Congratulations! You have been awarded 200 Google Play Points! Please claim your points by logging into your google account. To access your Play points, Login Here

Go to link: http://10.0.2.15 | Change | Remove

***Note**: Inspecting the link reveals that the URL is not a valid Google webpage.*

Email Attack - Concealing the URL



Masks the link by displaying the desired text

Edit Link

Text to display: Login Here

Link to:

● Web address

○ Email address

To what URL should this link go?

http://10.0.2.15

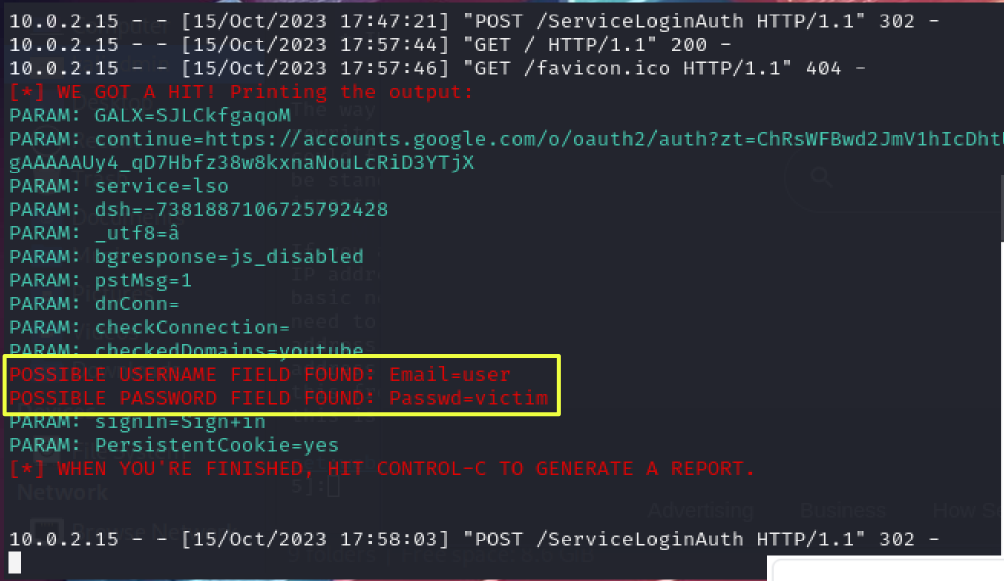
Test this link

Not sure what to put in the box? First, find the page on the web that you want to link to. (A search engine might be useful.) Then, copy the web address from the box in your browser's address bar, and paste it into the box above.

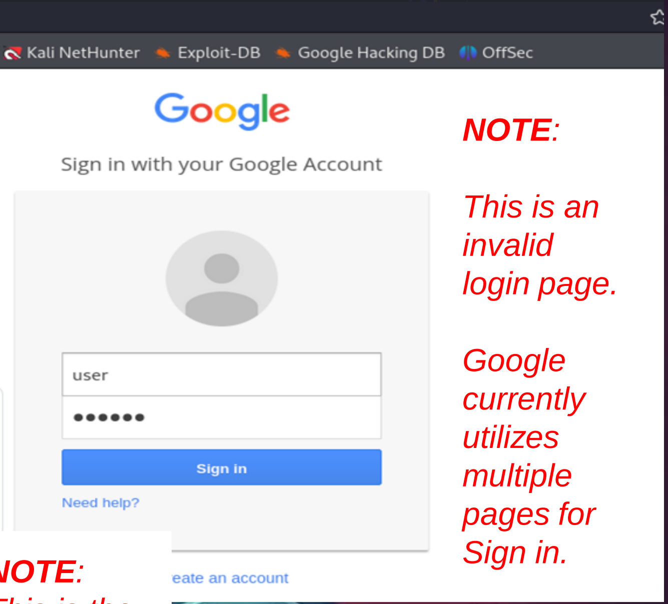
Cancel OK

You have been awarded Google Play Points!

ogle Play Points! Please claim
To access your Play points, Login



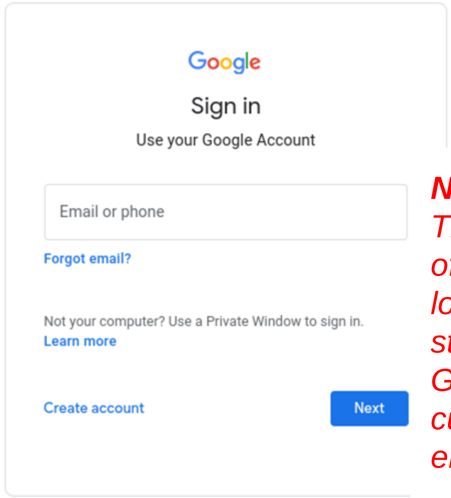
```
10.0.2.15 - - [15/Oct/2023 17:47:21] "POST /ServiceLoginAuth HTTP/1.1" 302 -
10.0.2.15 - - [15/Oct/2023 17:57:44] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [15/Oct/2023 17:57:46] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4
gAAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=user
POSSIBLE PASSWORD FIELD FOUND: Passwd=victim
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

10.0.2.15 - - [15/Oct/2023 17:58:03] "POST /ServiceLoginAuth HTTP/1.1" 302 -
```



NOTE:

This is an invalid login page.

Google currently utilizes multiple pages for Sign in.



NOTE:
This is the official login page style which Google currently employs.

Credential Harvesting using the Google cloning website template.

Mitigation Strategies

Social engineering stands as a multifaceted challenge, encompassing various techniques & attack vectors that adversaries employ to manipulate human behavior for their advantage.

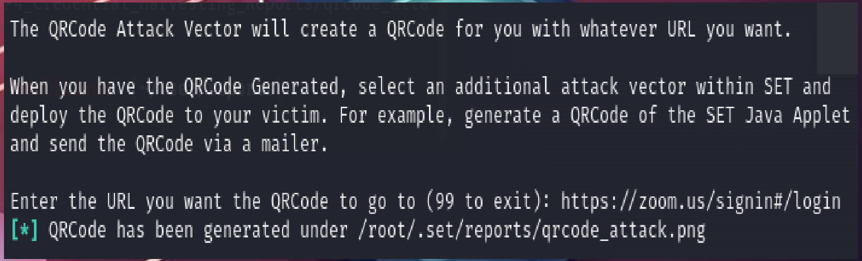
A comprehensive defense against this involves a combination of the following mitigation strategies:

- Use Multi-Factor Authentication (MFA).
- Verify the Sender’s Email.
- Check SSL certificates.
- Foster Positive Security-aware Culture.
- Employee Training & Awareness.
- Strict Access Control.
- Email Filtering & Spam Detection.
- Regular Security Audits.
- Network Segmentation.
- Regular Software Updates & Patches

QR Code Attack

- Why use QR code attacks?
  - Common practice in modern society, appearing on:
    - Product labels,
    - Advertisements,
    - Tickets,
  - Offers a convenient & rapid way to access information, websites, or apps by simply scanning the code with a smartphone.
  - Many users may not be aware of the potential risks associated with QR codes.
  - Attacks can bypass email filters presenting the code as a pdf
- Common use cases:
  - Website links, Contact info, Wifi configs, App downloads, tickets/boarding passes, payments/transactions, geolocation data, & product information.

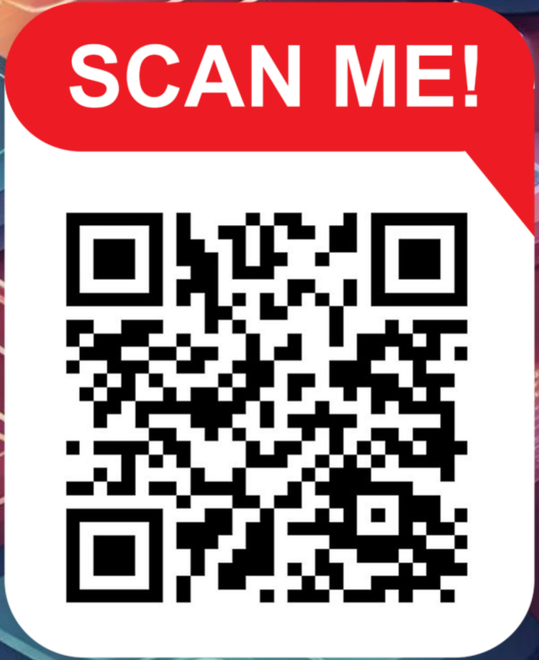
- What could be done:
  - Make a QR code of a cloned website targeting mobile users.
- What can you lose
  - Logins and Passwords
  - Credit Card information
  - Social Security
- What can you see
  - New Contact / “Friend”
  - Composed Email
  - Opens malicious website
  - Malicious downloads

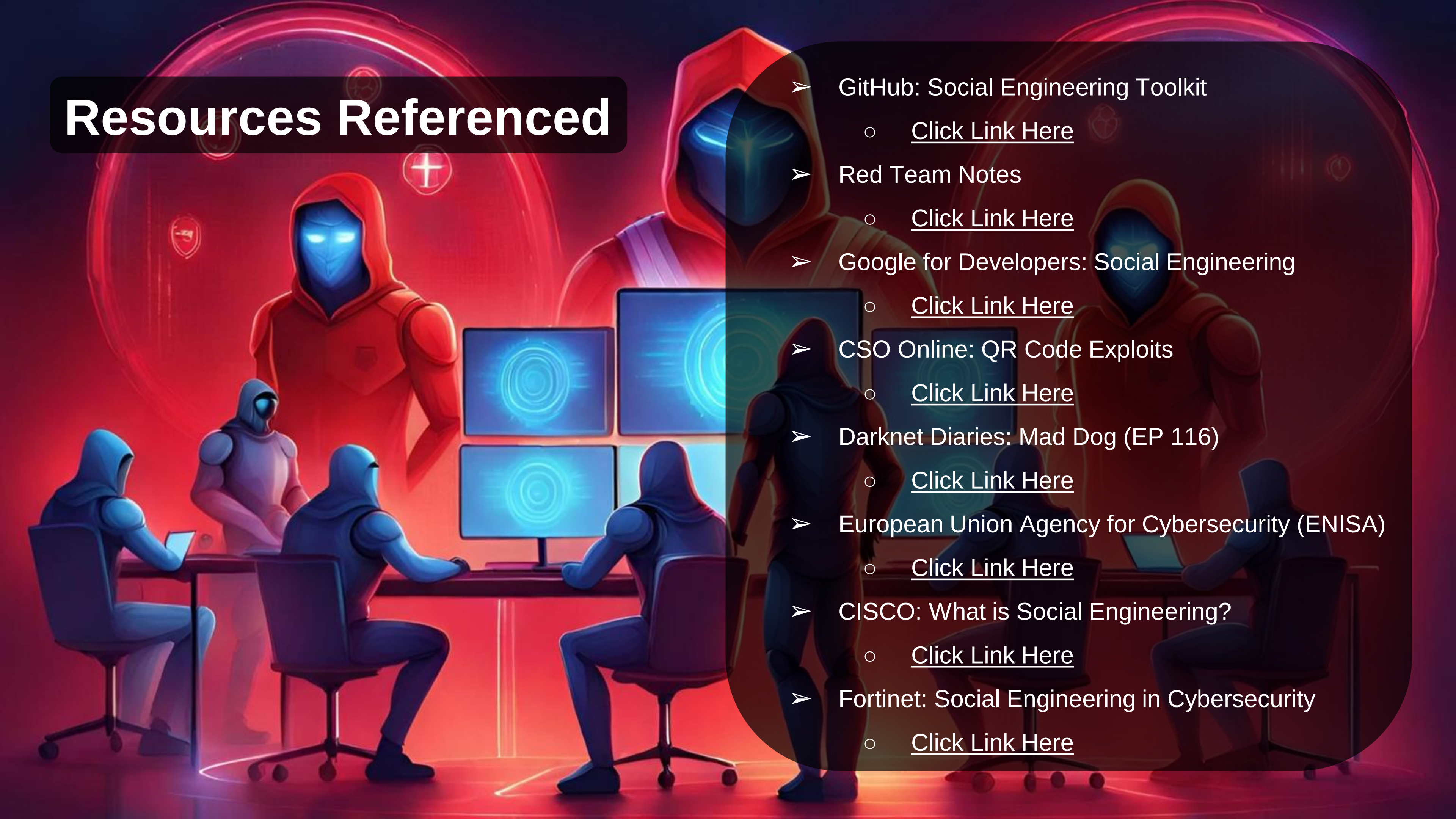


```
The QRCode Attack Vector will create a QRCode for you with whatever URL you want.

When you have the QRCode Generated, select an additional attack vector within SET and
deploy the QRCode to your victim. For example, generate a QRCode of the SET Java Applet
and send the QRCode via a mailer.

Enter the URL you want the QRCode to go to (99 to exit): https://zoom.us/signin#/login
[*] QRCode has been generated under /root/.set/reports/qrcode_attack.png
```

Malicious QR Code Mitigations

- Refrain from scanning QR codes from unverified or unfamiliar sources.
- Before scanning, verify the source.
    - Ensure the code is from a legitimate entity.
        - Check URL Previews.
- Exercise user education & awareness.
- Implement URL filtering & scanning solutions to detect & block malicious websites linked.
- Keep all software up-to-date to benefit from security enhancements.
- Check for tampering on physical objects.





Resources Referenced

- GitHub: Social Engineering Toolkit
  - Click Link Here
- Red Team Notes
  - Click Link Here
- Google for Developers: Social Engineering
  - Click Link Here
- CSO Online: QR Code Exploits
  - Click Link Here
- Darknet Diaries: Mad Dog (EP 116)
  - Click Link Here
- European Union Agency for Cybersecurity (ENISA)
  - Click Link Here
- CISCO: What is Social Engineering?
  - Click Link Here
- Fortinet: Social Engineering in Cybersecurity
  - Click Link Here