**Phishing Campaign Simulation Report: Credential Harvesting Analysis and Training Recommendations**

**Executive Summary**

This report details a simulated credential harvesting phishing campaign, outlining the attack methodology, potential success vectors, and crucial recommendations for employee training to mitigate such threats. The simulation leverages the Social Engineering Toolkit (SET) to clone a Google login page and craft deceptive emails designed to harvest user credentials. The findings emphasize the importance of vigilance, password management, and awareness training to protect against phishing attacks.

**Attack Simulation Methodology**

1. **Setup**:
   * The Social Engineering Toolkit (SET) was used to conduct a credential harvesting attack.
   * A Google website template was cloned using SET's "Website Templates" option.
   * The attacker's machine IP address was configured to host the cloned website.
2. **Cloned Website Testing**:
   * The cloned website was accessed via the attacker's IP address in a web browser to ensure functionality.
   * Test credentials entered on the cloned site were successfully captured, confirming the effectiveness of the credential harvester.
3. **Phishing Email Crafting**:
   * A new, seemingly legitimate Google account (e.g., "[systemprotection.alert@gmail.com](mailto:systemprotection.alert@gmail.com)") was created to send the phishing email.
   * The content of a genuine Google email was copied and pasted into a new email draft.
   * The sender information was modified to appear innocuous (e.g., "System Alert").
4. **Phishing Email Deployment**:
   * The newly created Google account was accessed via Gmail on the Kali machine.
   * The victim's email address was set as the recipient.
   * Links within the email were modified to redirect to the credential harvesting website.
5. **URL Masking**:
   * The attacker's IP address was converted to its decimal equivalent using an online tool like **dnshcheck.org/ip-to-decimal.php**.

*An****IP to Decimal Converter****transforms an IP address into its decimal equivalent, allowing it to be used in URL masking techniques for phishing attacks.*

* + Masked URLs were created using the format **$http://www.google.com@decimal\_ip$**. The **@** symbol is used to hide the malicious link.
  + All relevant links in the email were replaced with the masked URLs, ensuring any click redirects the victim to the cloned site.

**Potential Success Vectors**

* **Deceptive Email Content**: The simulation highlighted how easily a legitimate email can be copied and used for malicious purposes.
  + The created email contained no apparent typos or suspicious elements, increasing the likelihood of deceiving recipients.
* **Browser Vulnerabilities**: The demonstration indicated that while Firefox may provide a warning about the redirect, Chrome might not, potentially making the attack more effective on Chrome users.
* **URL Masking**: Masking techniques effectively concealed the true destination of the links, making the phishing attempt less obvious to the average user.
  + Even when hovering over the link, it displayed **$www.google.com$** with random characters, further misleading the victim.

**Analysis of Potential Success Rates**

Based on the simulation, the success rate of such a phishing campaign could be significant, particularly among users who:

* Use Chrome as their primary browser without advanced security extensions.
* Are not trained to recognize URL masking techniques.
* Rely on visual cues (e.g., logos, familiar layout) without verifying the authenticity of the sender and links.

**Recommendations for Employee Training**

To mitigate the risks associated with phishing attacks, the following training recommendations are crucial:

1. **Phishing Awareness Training**:
   * **Recognizing Phishing Attempts**: Educate employees on how to identify phishing emails, including inspecting sender addresses, looking for inconsistencies, and being wary of urgent or unusual requests.
   * **Real-World Examples**: Use real-world examples and case studies to illustrate the sophistication of modern phishing techniques.
   * **Interactive Simulations**: Conduct regular phishing simulations to test employees' ability to recognize and report phishing attempts.
2. **URL Analysis Training**:
   * **Hover-Over Verification**: Teach employees to hover over links to verify the destination URL before clicking.
   * **URL Masking Awareness**: Educate on techniques like URL masking and how to identify suspicious URLs, including those with IP addresses or unusual characters.
   * **IP to Decimal Conversion**: Explain how IP addresses can be converted to decimal format and used in deceptive URLs.
3. **Password Management Best Practices**:
   * **Strong, Unique Passwords**: Enforce the use of strong, unique passwords for all accounts.
   * **Password Managers**: Encourage the use of password managers to generate and store complex passwords securely.
   * **Password Reuse Prevention**: Emphasize the importance of not reusing passwords across multiple sites to prevent widespread compromise.

*Using the same password for multiple accounts means that once a hacker obtains your password from one site, they can use it to access any other accounts where you use the same password, including Google, company accounts, Netflix, and other online services*

1. **Reporting Mechanisms**:
   * **Easy Reporting System**: Implement an easy-to-use system for employees to report suspected phishing emails.
   * **Feedback and Updates**: Provide regular feedback and updates to employees on the latest phishing trends and techniques.
2. **Continuous Education**:
   * **Regular Training Sessions**: Conduct regular training sessions to reinforce phishing awareness and best practices.
   * **Stay Informed**: Keep employees informed about the latest phishing tactics and trends through newsletters, alerts, and workshops.

**Conclusion**

The simulated phishing campaign demonstrates the potential effectiveness of credential harvesting attacks and the importance of comprehensive employee training. By implementing the recommended training measures, organizations can significantly reduce their vulnerability to phishing attacks and protect sensitive information. Continuous education and vigilance are essential to maintaining a strong security posture against evolving cyber threats.