Document Reference: PRTU-1
Document Name: Phishing Incident Response Red Team Usecases

Effective Date: 29 April 2024
Expiry Date: 29 April 2025

Phishing Red Team Usecases

Redback Operations

Document Owner: Liya Thomas
Next Review Date: 17 June 2024

Last Modified By: Liya Thomas
Last Modified on: 14 April 2024

Document Reference: PRTU-1
Document Name: Phishing Incident Response Red Team Usecases

Effective Date: 29 April 2024
Expiry Date: 29 April 2025

Version	Modified By	Approver	Date	Changes made
0.1	Liya Thomas		14 April 2024	First Draft
1.0	Liya Thomas	Joel Daniel	29 April 2024	Approved for Publishing

Table of Contents

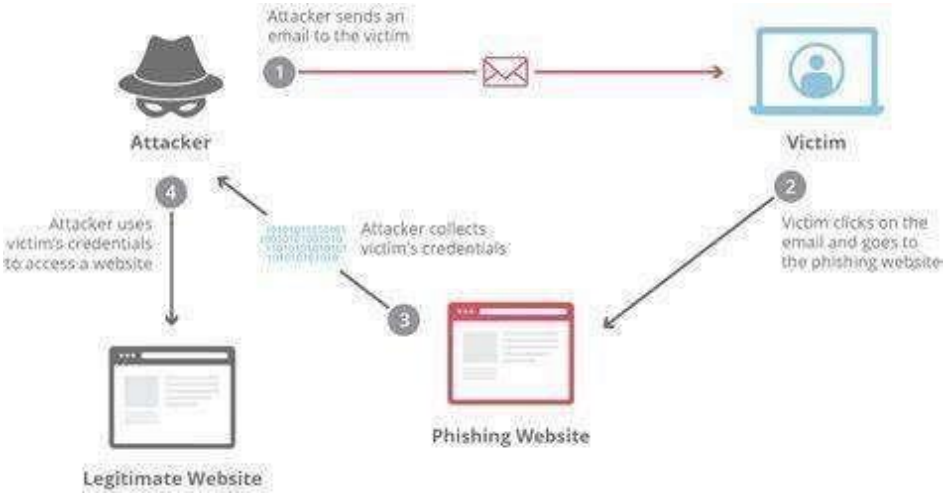
1 Introduction:

Phishing attacks are persistent threats in today's digital world, posing a significant risk to organizations worldwide.

The Red Team Phishing Simulation Playbook is a vital resource designed to equip organizations with a comprehensive strategy for executing simulated phishing attacks.

By evaluating and fortifying an organization's defenses against evolving phishing threats, this playbook plays a pivotal role in enhancing cybersecurity.

2 Email Phishing Simulation:



2.1 Objective:

Our goal is to evaluate the robustness of an organization's email security measures against phishing attempts.

2.2 Steps:

Craft Persuasive Phishing Emails:

Craft emails that closely resemble legitimate communications from trusted sources. These emails should be convincing and compelling, aiming to deceive recipients into taking action.

Embed Malicious Links or Attachments:

Insert malicious links or attachments within the phishing emails strategically. These links or attachments should entice recipients to divulge sensitive information or download malware.

Employ Techniques for Success:

Utilize various tactics to enhance the effectiveness of the phishing campaign. This may include email spoofing, creating a sense of urgency, or leveraging psychological triggers to increase the likelihood of recipients falling for the scam.

2.3 Tools and Techniques:

Social Engineering Toolkit (SET):

SET provides a range of attack vectors, including email spoofing, credential harvesting, and attachment-based attacks. It enables the replication of trusted sources and facilitates the creation of convincing phishing emails through psychological manipulation techniques.

Gophish:

Gophish is a versatile phishing framework that streamlines the process of creating and executing phishing campaigns. It offers customizable email templates, tracking capabilities, and detailed analytics, making it easier to assess the effectiveness of the simulation.

Customized Email Templates:

Tailoring phishing email templates to mimic the branding and communication style of reputable organizations enhances authenticity and increases the likelihood of successful deception.

Email Spoofing Tools:

Tools like "SendEmail" or custom scripts enable the spoofing of email addresses, making phishing emails appear legitimate. Email spoofing enhances the credibility of the attack, making it more likely for recipients to trust the message.

URL Obfuscation Techniques:

Besides URL shorteners, advanced obfuscation techniques like URL encoding and redirect chains can disguise malicious links, making them harder to detect by email security filters.

Payload Delivery Mechanisms:

Deploying weaponized documents or exploit kits increases the impact of phishing attacks by exploiting software vulnerabilities or manipulating user behavior to deliver malware payloads.

3 Spear Phishing Simulation:

3.1 Objective: Target specific individuals or departments within an organization to assess their susceptibility to personalized phishing attacks.

3.2 Steps:

Conduct Thorough Reconnaissance: Gather personal information to craft highly personalized phishing emails.

Tailor Phishing Emails: Customize phishing emails with relevant information to enhance credibility and effectiveness.

Deploy Personalized Phishing Emails: Send tailored phishing emails, leveraging social engineering tactics to increase engagement.

3.3 Tools and Techniques:

Gathering Information: Using tools like Maltego or Recon-ng, we meticulously gather personal details from various online platforms, including social media profiles and public databases. This thorough approach helps us build detailed profiles of our targets, empowering us to create highly personalized and convincing phishing campaigns.

Crafting Personalized Emails: Armed with a wealth of information, we tailor our email campaigns meticulously to each recipient. We not only include their name, position, or recent activities but also delve into their interests and preferences, ensuring that our messages resonate personally. This personalized touch enhances the credibility and effectiveness of our emails.

Social Manipulation: Our email communications go beyond personalization; they utilize persuasive language to exploit recent events or job roles relevant to the recipient. By tapping into their emotions and professional context, we create a sense of urgency or necessity, compelling them to take actions that benefit us. This strategic approach maximizes the success of our phishing endeavors

4 Whaling (CEO Fraud) Simulation:

4.1 Objective: Evaluate an organization's resilience against CEO fraud attacks by targeting high-profile individuals like CEOs or senior managers.

4.2 Steps:

Identify High-Profile Targets: Identify executives with access to sensitive information or financial resources.

Create Sophisticated Phishing Emails: Craft convincing emails impersonating trusted connections or business partners.

Include Requests for Sensitive Information: Request sensitive information or financial transactions in the emails to simulate CEO fraud scenarios.

4.3 Tools and Techniques:

Crafting Deceptive Emails: In our pursuit of sophisticated deception, we meticulously analyze the target's communication habits and organizational structure. This enables us to create emails that not only mirror the tone and mannerisms of authoritative figures within the company but also leverage their understanding of internal procedures, making our phishing attempts highly persuasive.

Spoofing Domains: To bolster the credibility of our phishing emails, we employ advanced tactics to spoof the sender's domain. This goes beyond simply registering domains similar to trusted sources. Instead, we replicate the exact email addresses of familiar contacts or reputable organizations, ensuring our emails blend seamlessly with genuine correspondence. By doing so, we effectively sidestep email security filters, significantly increasing our chances of success.

Creating Urgent Appeals: Our emails are strategically crafted to instill a sense of urgency, prompting recipients to act swiftly without hesitation. By emphasizing the urgency of the requested information or transaction and employing authoritative language, we exploit psychological triggers that drive immediate compliance. This ensures that targets are compelled to respond promptly, furthering our objectives in the phishing campaign.

5 Vishing (Voice Phishing) Simulation:

5.1 Objective: Assess an organization's awareness and response to voice-based phishing attacks.

5.2 Steps:

Use Automated Voice Calls or Prerecorded Messages: Utilize automated calls or messages to simulate phishing attempts.

Request Sensitive Information: During the calls, request sensitive information or financial transactions under the guise of legitimate organizations.

Mimic Trusted Phone Numbers: Spoof trusted phone numbers to enhance the credibility of the phishing attempts.

5.3 Tools and Techniques:

Voice Manipulation: Utilizing platforms like Asterisk or FreePBX, we meticulously tailor automated voice calls or prerecorded messages to deceive our targets. By adjusting tone, cadence, and speech patterns, our aim is to instill a sense of authenticity, thereby boosting engagement and compliance.

Caller ID Spoofing: Employing advanced methods, we manipulate caller ID details to ensure our calls appear to be from known and trusted sources recognized by the target. This deceptive strategy bolsters the credibility of our phishing endeavors, minimizing suspicion and heightening the success rate of our social engineering efforts.

Scripted Messages: Within our repertoire, we have finely crafted, pre-recorded scripts meticulously designed to emulate official correspondence. By replicating the language, urgency, and tone of authentic messages, we bolster the legitimacy of our phishing attempts, significantly increasing the likelihood of target compliance.

6 Smishing (SMS Phishing) Simulation:

6.1 Objective: Evaluate an organization's resilience to SMS-based phishing attacks targeting mobile devices.

6.2 Steps:

Send Text Messages with Malicious Links: Send SMS containing malicious links or requests for sensitive information.

Mimic Trusted Sources: Mimic trusted sources such as banks or government agencies in the messages.

Create a Sense of Urgency: Generate a sense of urgency in the messages to prompt immediate responses.

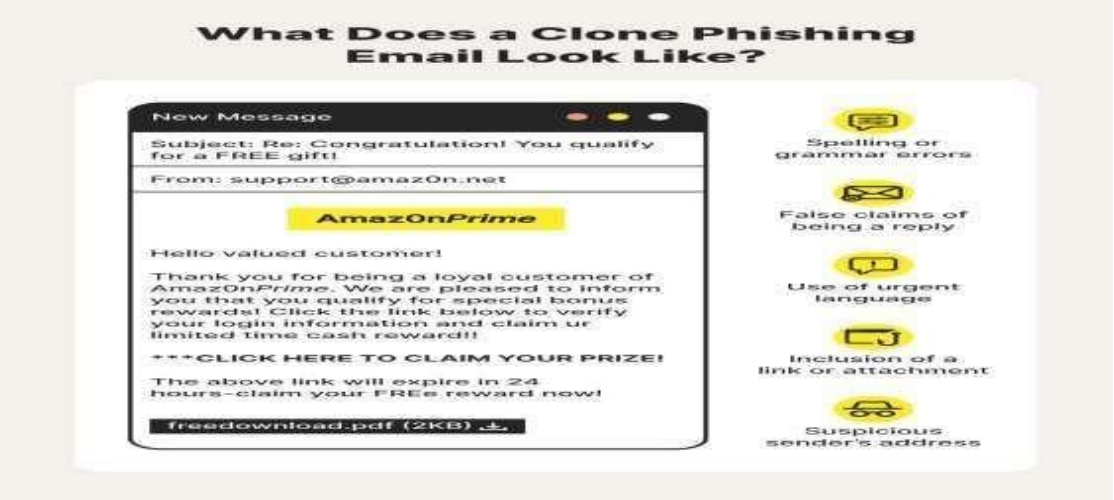
6.3 Tools and Techniques:

Text-based Deception: Utilizing SMS spoofing services, we adeptly conceal our identity, dispatching messages that mimic those from trusted sources, enhancing our phishing efforts.

Tailored Messages: Our SMS campaigns feature meticulously crafted templates tailored to diverse scenarios, including urgent requests for account verification or financial transactions, maximizing recipient engagement and response rates.

Link Masking: To obfuscate malicious links, we employ URL shorteners like Bitly or TinyURL, heightening the probability of recipients clicking on them unwittingly, thereby facilitating successful phishing attempts.

7 Clone Phishing Simulation:



7.1 Objective: Test an organization's ability to detect and mitigate phishing emails that mimic legitimate correspondence.

7.2 Steps:

Identify Authentic Emails: Identify authentic emails within the organization or from trusted sources to serve as templates.

Create Clone Emails: Make slight modifications to replicate legitimate emails, enabling the creation of convincing phishing attempts.

Send Clone Emails to Targeted Individuals: Assess awareness and response by sending clone emails to targeted individuals.

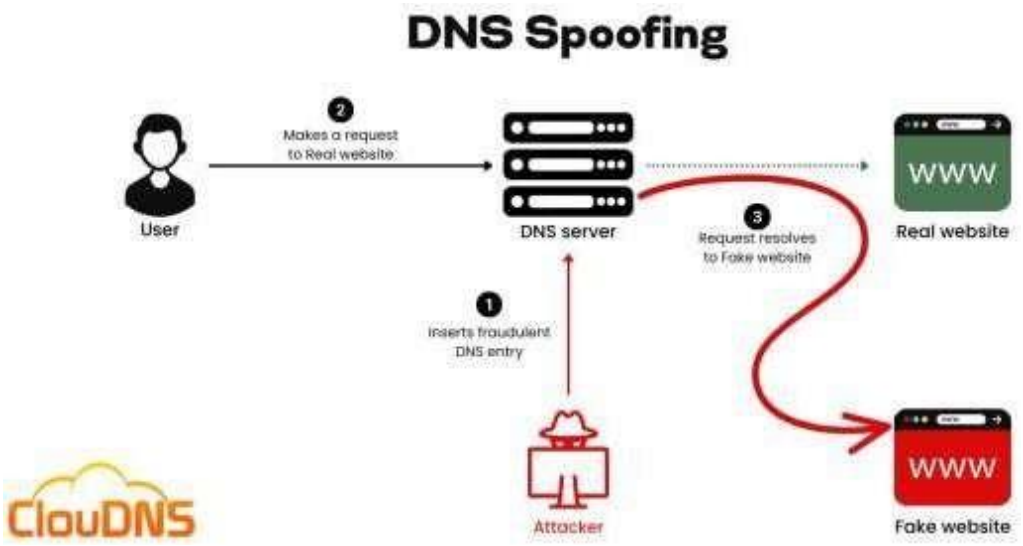
7.3 Tools and Techniques:

Email Replication: Leveraging tools such as GoPhish, we meticulously replicate authentic emails with subtle modifications, ensuring our clone phishing attempts are highly convincing and indistinguishable from legitimate correspondence.

Content Analysis: Through meticulous examination of previous emails, we discern patterns and content that can be replicated, significantly boosting the authenticity and success rate of our phishing campaigns.

Phishing Platforms: We harness the capabilities of sophisticated platforms equipped with customization features to streamline the creation and dissemination of clone phishing emails, optimizing our efforts for maximum impact and efficacy.

8 DNS Spoofing Simulation:



8.1 Objective: Assess an organization's preparedness against DNS manipulation-based phishing attacks.

8.2 Steps:

Modify DNS Records: Alter DNS records to reroute users from legitimate sites to malicious ones under the attacker's control.

Phish for Data: Create fake login pages or forms on the malicious sites to deceive users into providing credentials or sensitive information.

Data Harvesting: Capture the information entered by users on these fake pages for malicious use.

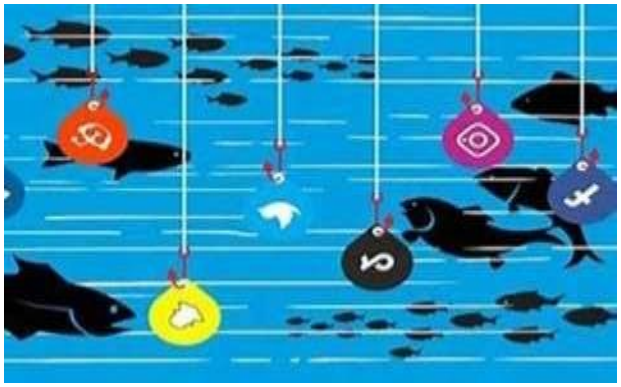
8.3 Tools and Techniques:

DNS Spoofing Tools: Employing software like dnsspoof or Ettercap, we manipulate DNS responses to reroute users from legitimate websites to malicious ones under our control. This deceptive tactic allows us to intercept unsuspecting users' traffic and exploit their interactions with fraudulent web pages.

Fake Web Pages: Our strategy involves meticulously crafting replicas of authentic login pages or forms on malicious websites, meticulously designed to deceive users into divulging sensitive information. By closely mimicking the appearance and functionality of legitimate sites, we enhance the effectiveness of our phishing campaigns.

Data Interception: Leveraging packet sniffing tools such as Wireshark, we intercept and capture sensitive information transmitted over the network. Through this methodical approach, we gain access to valuable data, including usernames, passwords, and financial details, enabling us to exploit the vulnerabilities of our targets.

9 Angler Phishing Simulation:



9.1 Objective: Evaluate how susceptible an organization is to phishing attacks via compromised websites or applications.

9.2 Steps:

Identify Vulnerable Websites: Find sites or apps with security weaknesses allowing the injection of malicious content.

Redirect Users: Employ tactics like hijacked ads or fake login pages to steer users to the compromised sites.

Capture Credentials: Prompt users to input login details or sensitive data on fake pages, capturing this information for misuse.

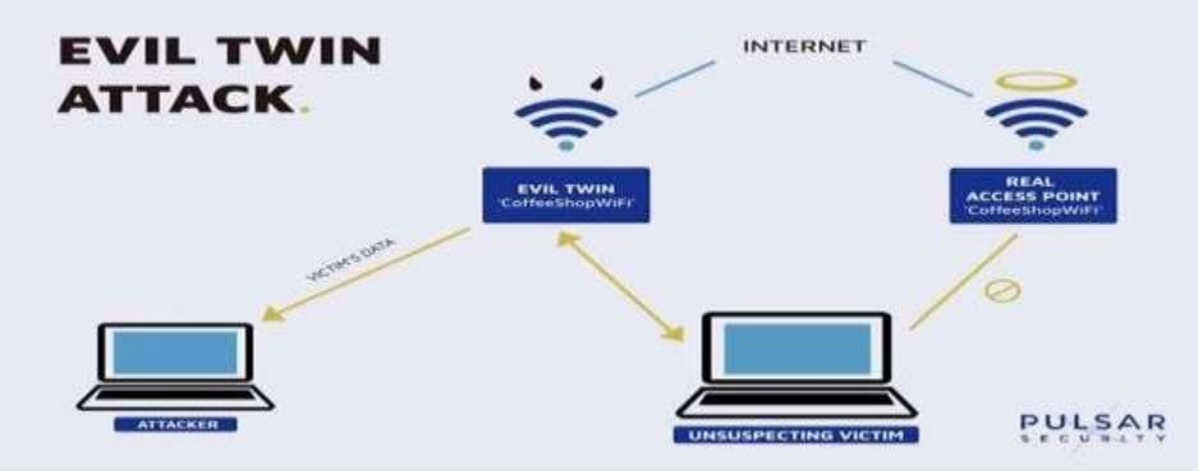
9.3 Tools and Techniques:

Exploit Kits: We employ tools like Blackhole or Angler to capitalize on weaknesses within websites or applications, exploiting security vulnerabilities. These kits automate the process, enabling us to launch attacks efficiently and effectively, increasing the likelihood of successful infiltration.

Malicious Redirection: By tampering with URLs or advertisements, we divert users to compromised sites under our control. This manipulation heightens the risk of users interacting with malicious content, facilitating unauthorized access to sensitive information.

Credential Harvesting: Through techniques like keylogging or form grabbing, we illicitly capture user credentials and sensitive data. This clandestine approach enables us to steal valuable information without the user's knowledge.

10 Evil Twin Phising Simulation



10.1 Objective: Assess awareness and response to Wi-Fi-based phishing attacks.

10.2 Steps:

Set Up Rogue Wi-Fi Hotspots: Create rogue Wi-Fi hotspots mimicking legitimate networks to lure users.

Entice Users to Connect to Rogue Hotspots: Attract users with free or unsecured Wi-Fi access.

Intercept and Capture Sensitive Information: Capture sensitive information transmitted over compromised Wi-Fi connection.

10.3 Tools and Techniques:

Rogue Wi-Fi Networks: Leveraging Wi-Fi Pineapple devices, we establish deceptive Wi-Fi hotspotsmirroring authentic networks, enticing unsuspecting users to connect.

Traffic Interception: Employing packet sniffing tools such as Wireshark, we intercept and scrutinize network traffic, extracting critical data like usernames and passwords for unauthorized access.

Social Manipulation: Through enticing offers of free or unsecured Wi-Fi access, coupled with the emulation of genuine network appearances, we coax users into connecting to our rogue hotspots, amplifying our ability to exploit their vulnerabilities.

11 Conclusion:

The Red Team Phishing Simulation Playbook provides a comprehensive framework for executing simulated phishing attacks across various vectors.

By implementing these simulations and leveraging recommended tools and techniques, organizations can identify vulnerabilities, enhance their security posture, and mitigate the risks associated with phishing attacks.

Continuous testing, refinement, and employee education are crucial for effectively defending against the evolving threat landscape, safeguarding assets, data, and reputation from malicious actors.

12 Reference Image

Phising - https://cdn.vectorstock.com/i/preview-1x/08/11/cyber-crime-banner-vector-21210811.jpg

Email Phising - https://th.bing.com/th/id/OIP.LAHAzuJWME5T4cYt-G3liAAAAA?rs=1&pid=ImgDetMain

Spear Phising Simulation https://www.kindpng.com/picc/m/17-175089_phishing-spear-phishing-cycle-diagram-phishing-diagram-hd.png

Whaling (CEO Fraud) Simulation https://assets-global.website-files.com/620d42e86cb8ec4d0839e59d/6230ec85282a1d26a199de19_61ca0f33167ad578cc0b8cd9_Fraud-Detection-and-Prevention-Diagram.png

Vishing (Voice Phishing) Simulation https://www.ringcentral.com/gb/en/blog/wp-content/uploads/2021/04/root-cause-of-phishing-640x480.png

Smishing (SMS Phishing) Simulation-https://blog.pulsarsecurity.com/hs-fs/hubfs/BlogTemplate_EvilTwin-1.jpg?width=1500&name=BlogTemplate_EvilTwin-1.jpg

Clone Phising Simulation - https://now.symassets.com/content/dam/norton/global/images/non-product/misc/tlc/what-is-clone-phishing.png

DNS spoofing Simulation - https://www.cloudns.net/blog/wp-content/uploads/2022/04/DNS-Spoofing.png

Angler Phishing - https://th.bing.com/th/id/OIP.jDWMszekEwVd31QoFxF01gHaE4?rs=1&pid=ImgDetMain

Evil Twin Phising https://blog.pulsarsecurity.com/hs-fs/hubfs/BlogTemplate_EvilTwin-1.jpg?width=1500&name=BlogTemplate_EvilTwin-1.jpg