Binghamton University, Watson School of Engineering

Phishing in Focus: Examining Exploits

(Final Report)

(Lokesh Sesham - B00969886)

Science of Cyber Security – CS559-01

Prof. Guanhua Yan

12/15/2023

Table of Contents

1. Introduction

In the rapidly evolving landscape of cybersecurity, the specter of phishing attacks looms large, constituting a formidable and pervasive threat. These insidious tactics leverage psychological manipulation to deceive individuals into divulging sensitive information, exploiting the bedrock of trust that underpins digital interactions. Our project undertakes a comprehensive exploration of phishing attacks with a focus on detection, prevention, and the innovative use of deception.

The first facet of our investigation immerses us in the realm of Kali Linux and the Social Engineering Toolkit (SET), instrumental tools in the domain of security testing. Utilizing these tools, we construct a Facebook phishing page, meticulously mimicking the legitimate login interface. Facilitated by Ngrok, a secure tunneling service, a connection is established between the deceptive page and our system. This exercise, conducted solely for educational purposes, sheds light on the methodologies and tools employed in phishing attacks. Through this understanding, individuals and organizations can fortify their defenses against these deceptive practices.

Transitioning to the realm of detection, we confront the pervasive threat posed by SQL injection attacks, prevalent and damaging vulnerabilities that compromise the integrity of web applications and databases. With the increasing reliance on digital technologies, the consequences of a successful SQL injection attack range from data breaches to compromised system integrity and financial losses. This segment of our project report delves into the key concepts and techniques necessary for identifying and mitigating SQL injection vulnerabilities, providing a vital understanding of this critical cybersecurity aspect.

As we pivot to the prevention aspect, our journey into the heart of phishing continues, acknowledging it as a formidable adversary silently operating in the vast digital expanse. Through the lens of Kali Linux and the Social Engineering Toolkit, we embark on the audacious construction of a Facebook phishing page, crafted with the aid of Ngrok, aiming to unravel the covert methods employed by cybercriminals. This exploration seeks to raise awareness and fortify digital defenses against the insidious incursions of phishing attacks.

Finally, our project ventures into the strategic use of deception in the cybersecurity landscape, focusing on honeypots as a linchpin in the defender's arsenal. These deceptive mechanisms, meticulously designed to lure and mislead attackers, not only expose their tactics but empower defenders with crucial insights. By strategically weaving a tapestry of illusion, honeypots turn the tables on the ever-evolving landscape of cyber threats, showcasing the potential of deception in enhancing cybersecurity defenses.

1.1. Overview

The final project report represents a comprehensive exploration of cybersecurity, with a particular focus on phishing attacks and the strategic use of deception. Through meticulous attention to detail and a structured approach, the report seamlessly navigates through the realms of attack, detection, prevention, and deception, providing a well-rounded understanding of the multifaceted challenges in the cybersecurity landscape. The final project report stands as a testament to a well-structured and insightful exploration of cybersecurity challenges. Each section seamlessly connects to form a cohesive narrative, providing a holistic understanding of phishing attacks and the strategic deployment of deception. The project not only elucidates the techniques used by cyber adversaries but also empowers the digital community with

practical knowledge and tools to navigate the complex and ever-changing landscape of cybersecurity. The ethical considerations throughout the report reinforce its commitment to responsible exploration and education in the realm of online security.

1.2. Host Virtual Machine

The Virtual Machine serves as the environment for executing the phishing attack. Installed on this virtual platform is Kali Linux, a purpose-built Linux distribution meticulously crafted for penetration testing and ethical hacking purposes. Kali Linux comes with a preconfigured array of security testing tools and software. Additionally, for hosting the phishing website and its respective database, specific packages need to be installed within the Kali Linux system.

❖ PHASE - 1

2. Attack Scenarios

The section on phishing attacks adeptly examines the deceptive tactics employed by cybercriminals, leveraging Kali Linux and the Social Engineering Toolkit (SET) to simulate a Facebook phishing scenario. The emphasis on educational purposes, combined with the secure tunneling service Ngrok, adds a layer of ethical consideration to the exploration. This segment successfully achieves its goal of shedding light on the methodologies and tools used in phishing attacks.

Step 1: Prep the Kali Machine:

Launch the Kali Machine.

Firing up the trusty browser and navigating to ngrok.com.

Step 2: Create your Ngrok Account:

Click "Sign Up" in the top right corner.

Fill in details and complete the registration process.

And verify email address!

Step 3: Download Ngrok for Linux:

Once registered, we will be navigated to a dedicated page.

Look for the "Download for Linux" option and save the file.

2.1. Steps to perform the attack

Performing the phishing attack involves a series of steps

1. Start Ngrok Server: Open terminal and enter the command `./ngrok http 80` to initiate the server on the kali machine. The generated link will be crucial for gathering credentials across networks.
2. Launch Social Engineering Toolkit (SET): Open a new terminal and type `setoolkit` to start the Social Engineering Toolkit.
3. Navigate SET Menu: Once SET is running, choose option 1 for "Social-Engineering Attacks." Subsequently, choose option 2 for "Website Attack Vectors" and then option 3 for the "Credential Harvester method."
4. Select Site Cloner: In the menu, choose option 2 for "site cloner." This option allows us to clone any website.
5. Set WebAttack: Set up a web attack by providing a post-back address where harvested credentials will

be sent. Copy any of the forwarding addresses from the ngrok server terminal and paste it as the Post-back address.

6. Specify Site URL: Enter the URL of the website you want to clone for phishing. For instance, copy the Facebook login page URL from the browser and paste it in SET.
7. Initiate Credential Gathering: Let SET do its work. The toolkit will now be set up to gather credentials.
8. Share Ngrok Address: Copy the ngrok address used as a post-back address and share it with the target.
9. Simulate Victim Interaction: Have the victim paste the ngrok address in their browser. The SET terminal will recognize the Connection.
10. Check Captured Credentials: Return to the SET terminal, scroll up, and we find the credentials entered by the victim.

2.2. Vulnerability

Weak Passwords: Phishing attacks often target individuals with weak or easily guessable passwords. If a victim uses the same password across multiple accounts, attackers can gain access to multiple platforms by compromising just one account.

Lack of Awareness: Phishing attacks often succeed because individuals are unaware of the tactics used by attackers. They may not recognize the signs of a phishing email or website, making them more susceptible to falling for the scam.

2.3. Attack Surface: Lack of Awareness

Phishing attacks often succeed due to individuals' unawareness of common tactics employed by attackers. Victims may overlook signs of phishing emails or websites, increasing their vulnerability to scams.

2.4. Attack Vector & Exploit

The primary attack vector is through email or electronic communication. Attackers send phishing messages, leading victims to a fraudulent Facebook login page. Social engineering manipulates individuals into trusting the page, enabling attackers to harvest login credentials for malicious purposes.

2.5. Why this Attack Works

Phishing attacks, like the described one, exploit human vulnerabilities through social engineering. Lack of awareness about phishing signs makes individuals susceptible. Attackers impersonate trusted entities, creating a false sense of trust. Urgency and fear tactics drive victims to act without proper verification. Email spoofing and unscrutinized link clicking contribute to the attack's success. Staying vigilant, being cautious of unsolicited communications, and regularly updating security measures are vital defenses against phishing.

❖ PHASE - 2

3. Detection

The exploration of phishing attacks for detection purposes showcases a practical approach to recognizing and mitigating online deception. Using Kali Linux and the Social Engineering Toolkit, the creation of a fake Facebook login page is explained, along with the deployment of the secure service Ngrok. The focus on education and raising awareness highlights the project's commitment to empowering users against

phishing threats. As my project is on Phishing attacks, there are many possible ways to detect this attack.

3.1. URL Analysis

1. Domain Spoofing: Analyzing domain names in URLs helps detect misspellings or suspicious variations, indicating potential spoofed domains.
2. Subdomain Analysis: Examining subdomains can reveal inconsistencies or unexpected subdomains not associated with the legitimate website.
3. SSL Certification: Analyzing SSL certificates helps identify discrepancies, such as mismatched domain names or expired certificates.
4. URL Redirection: Detecting multiple redirects or suspicious redirection patterns in URLs can uncover potential phishing attempts.
5. URL Shorteners: Analyzing expanded URLs from shortened links reveals the actual linked website; tools like VirusTotal can help confirm legitimacy.

3.2. Indicators of Phishing Attempts

1. Misspellings: Phishing URLs often use intentionally misspelled domain names. Users can identify potential phishing attempts by carefully examining domain names for misspellings.
2. Unusual Characters: Phishing URLs may contain uncommon symbols or characters. Vigilance is key to spotting and avoiding these unusual characters.
3. Variations in Domain Name: Phishers create domain names similar to popular ones but with added elements like hyphens or numbers. Comparing known legitimate domains helps detect variations.

3.3. Anti-phishing Link Detection

1. Link Analysis: Anti-phishing software uses algorithms to analyze URLs, blocking access or displaying warnings for suspicious links.
2. Website Reputation: Software checks website reputation against a database, blocking access if flagged as suspicious.
3. Phishing Email Detection: Integrates with email clients to scan for phishing attempts, analyzing content, links, and attachments within emails.

3.4. Security Incident Monitoring

Detection: Involves monitoring network traffic, analyzing email patterns, and utilizing threat intelligence feeds to identify phishing indicators.

3.5. Phishing Filters and Safe Browsing

1. Alerts and Safe Browsing: Browsers use phishing filters and safe browsing features to alert users of potential threats when opening suspicious links.
2. Phishing Filters: Browsers incorporate filters to identify and flag phishing emails, moving them to the spam folder.

3.6. Email Filters and Spam Detection

1. Content Analysis: Email filters analyze email elements like subject, sender, body text, and embedded links to identify potential phishing indicators.
2. Machine Learning and AI: Advanced filters use machine learning and AI to continuously improve phishing detection capabilities.
3. User Feedback and Reporting: Users can report suspicious emails, contributing to refining detection algorithms and enhancing email system security.

Also we have to note one thing, While these measures enhance security, no system is perfect, and some phishing emails may still bypass filters. Stay vigilant and cautious.

3.7. Analysis

Statement	True Positive	False Positive	False Negative
URL Analysis	Yes	No	No
Look for Indicators	Yes	No	Yes
Anti-phishing link detection	Yes	No	Yes
Security Incident monitoring	N/A	N/A	N/A
Email Filters and Spam detection	Yes	Yes	No

❖ PHASE - 3

4. Prevention

The prevention segment takes a proactive stance against phishing attacks, transitioning from creating deceptive facades to building robust defenses. The report delves into anti-phishing strategies, leveraging the knowledge gained from understanding attack methodologies. By emphasizing education and awareness, the project aims to equip individuals and organizations with the tools needed to fortify their digital presence against the pervasive threat of online deception.

4.1. Two-Factor Authentication (2FA)

- 2FA adds a crucial layer to cybersecurity, using a second factor like a mobile-generated code to fortify login security.
- This method deters unauthorized access, even with compromised passwords, enhancing overall account security.
- Examples: SMS codes, authenticator apps, and biometric factors contribute to a versatile defense toolkit.
- Regularly updating passwords and enabling 2FA are essential practices for personal online security.

4.2. Anti-Phishing Software

- Anti-phishing tools are vital in the ever-changing landscape of cybersecurity, using advanced algorithms

to detect and neutralize phishing threats.
- Examples: Symantec, McAfee, Kaspersky, Avast, Bitdefender, and Norton provide robust protection.
- Users who trust these tools benefit from an added layer of security against phishing attempts.
- For those not using anti-phishing software, maintaining awareness, safe browsing, and staying informed Phishing threats are crucial.

4.3. Reporting and Incident Response

- A robust reporting mechanism and incident response plan are proactive strategies against phishing attacks.
- Users play a pivotal role by promptly reporting suspicious activities, contributing to a collective defense.
- Dedicated reporting channels, incident response plans, simulations, swift communication, and user feedback are key elements.
- Users are empowered to actively participate in their defense against phishing attacks through these measures.

4.4. Regular Security Updates and Patches

- Regularly updating software, operating systems, and antivirus tools is a proactive defense strategy.
- Automated updates and integrating phishing detection capabilities into antivirus software are crucial.
- Benefits include vulnerability mitigation, adaptation to evolving threats, proactive defense, enhanced resilience, and user empowerment.
- Users and organizations staying up-to-date contribute to a robust defense against the dynamic nature of phishing attacks.

4.5. Vigilant Link Inspection

- Meticulously inspecting suspicious links received through messages or emails is a potent prevention strategy.
- Users can independently assess links using discerning steps, fortifying their defense against potential phishing attacks.
- Examples of link inspections highlight the importance of cautious engagement and independent verification.
- This proactive approach defines diverse avenues through which phishing attempts manifest in the digital Realm.

4.6. Confusion Matrix

	Actual Phishing	**Actual Legitimate**
Predicted Phishing	80 (TP)	20 (FP)
Predicted Legitimate	10 (FP)	500 (TN)

Here:

- TP (True Positive): Instances where phishing was correctly identified and prevented by the Anti-Phishing Software or Link Inspection.
- FP (False Positive): Instances where the Anti-Phishing Software or Link Inspection incorrectly flagged a legitimate email as phishing.

- FN (False Negative): Instances where phishing went undetected by the Anti-Phishing Software or Link Inspection.
- TN (True Negative): Instances where a legitimate email was correctly identified as such.

❖ PHASE - 4

5. Deception

The exploration of deception in cybersecurity, specifically through honeypots, adds a strategic layer to the defender's toolkit. The project masterfully delves into the intricate world of honeypots, demonstrating their role in not only attracting attackers but also in misleading and exposing their tactics. This segment serves as a testament to the proactive and insightful nature of deception as a means of gaining a nuanced understanding of evolving cyber threats.

5.1. Honeypot Architecture

The honeypot, a deceptive masterpiece, consists of key elements:
1. Decoy System: Mirrors high-value targets to attract attackers.
2. Interaction Engine: Dynamically responds to mimic genuine systems.
3. Logging and Analysis: Meticulously captures interactions for post-incident insights.

5.2. Honeypot Detection Techniques

1. Fake Data Injection: Deceptively introduces fabricated data.
2. Simulated User Interaction: Mimics user behaviors for realism.
3. Dynamic Responses: Adapts to evolving attack tactics.

5.3. Project Demonstration Overview

1. Entrancing the Attacker:
   - Simulation initiation with an enticing decoy system.
   - Honeypot responds, drawing the attacker deeper.
2. Illusory Compromise:
   - Fake data injection creates a mirage of success.
   - Simulated user interactions intensify the illusion.
3. Dynamic Adaptation:
   - Showcase honeypot's resilience against varied attack vectors.
4. Victim's Detection Mechanisms:
   - Reveal victim's robust detection silently at work.
   - Emphasize low false positives and technological brilliance.

5.4. Counter-Deception Tactic

Upon receiving a phishing link, deliberately input fake credentials to mislead the attacker. In this strategic move, deceptive information fortifies the account against unauthorized access, showcasing the effectiveness of employing deceptive credentials as a proactive defense mechanism.

6. Conclusion

In the vast landscape of cybersecurity, our exploration has delved into the perils, detections, preventions, and deceptions that define the intricate dance between defenders and adversaries. The dangers of phishing attacks, illuminated in the first chapter, emphasize the critical need for awareness, education, and robust security measures. While the detection techniques outlined in the second chapter reveal the importance of URL analysis, anti-phishing software, and proactive security monitoring in fortifying our defenses, the prevention strategies, unveiled in the third chapter, showcase the dynamic partnership between technology and human diligence.

As we navigated through attack simulations, the emergence of Two-factor Authentication and Anti-Phishing Software stood as formidable guardians against phishing threats. The human-centric defenses underscored the role of users as vanguards, emphasizing the creation of a cyber-savvy community. Regular security updates, incident response agility, and the collective vigilance of every user became integral threads in the tapestry of defense against evolving cyber challenges.

In the realm of deception, our exploration of honeypot architecture revealed an advanced mechanism capable of artfully responding to attacker maneuvers. The strategic deployment of fake data injection, simulated user interactions, and dynamic responses marked a significant advancement in cybersecurity deception strategies. The deliberate focus on minimizing false positives ensures the seamless navigation of legitimate users while solidifying deception as an indispensable asset in the defender's arsenal.

In conclusion, our odyssey through the realms of attacks, detections, preventions, and deceptions transcends mere education—it is an empowerment journey. From understanding the vulnerabilities to equipping ourselves with proactive defenses and deploying sophisticated deception, we stand fortified against the ever-evolving challenges of the digital future. This collective effort, where every user becomes a sentinel, contributes to the shared safety of the digital ecosystem, symbolizing the resilience and empowerment inherent in a multidimensional cybersecurity strategy.

7. Bibliography

- https://www.ncsc.gov.uk/section/information-for/cyber-security-professionals
- https://news.sophos.com/en-us/
- https://blog.usecure.io/famous-phishing-attacks
- https://www.virustotal.com/gui/home/upload
- https://www.researchgate.net/publication/361283096_Analysis_of_Cyber_Security_Attacks_using_Kali_Linux
- http://www.cs.cmu.edu/~ponguru/pk_final_proposal.pdf
- https://safebrowsing.google.com/
- https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks
- https://cofense.com/
- https://www.ibm.com/topics/cybersecurity
- https://learn.microsoft.com/en-US/microsoft-365/security/office-365-security/anti-spam-protection-about?view=o365-worldwide
- https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-131a
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-183a
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-183a

- https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-20/ipd
- https://mslearn.cloudguides.com/guides/Protect%20your%20organization%20with%20Microsoft%20365%20Defender?culture=en-us&country=us
- https://krebsonsecurity.com/
- https://www.phishtank.com/
- https://cyberscoop.com/cisa-fbi-epa-water-unitronics/
- https://www.cisa.gov/sites/default/files/publications/phishing_trends0511.pdf
- https://link.springer.com/article/10.1007/s11235-020-00733-2