Binghamton University, Watson School of Engineering

Phishing in Focus: Examining Exploits

(Deception)

(Lokesh Sesham - B00969886)
Science of Cyber Security – CS559-01
Prof. Guanhua Yan
12/08/2023

Contents

1. Introduction

In the dynamic landscape of cybersecurity, the strategic use of deception has become a linchpin in the defender's arsenal. This project delves into the sophisticated realm of honeypots, a deceptive mechanism meticulously crafted to not only lure attackers but to convincingly mislead them into believing their phishing endeavor was triumphantly successful. Unbeknownst to the attacker,the victim, armed with a vigilant honeypot, skillfully detects and prevents the malicious incursion. Through the artful orchestration of sending fabricated or misleading data back to the attacker, the honeypot weaves a tapestry of illusion, ensnaring the assailant in a carefully laid trap. This multifaceted deception not only exposes the attacker's tactics but also empowers the defender with crucial insights, turning the tables on the ever-evolving landscape of cyber threats.

2. Honeypot Architecture

In the intricate dance between attackers and defenders in the cybersecurity arena, the deployment of a honeypot stands as a strategic masterpiece. The architecture of this deceptive mechanism is meticulously designed to mimic a vulnerable system or service, strategically positioned within the Victim's environment to lure potential attackers. Crafted with precision, the honeypot beckons assailants towards a decoy system, artfully responding to their actions with seemingly authentic data and interactions. This section explores the components of this cunning architecture, unraveling the intricate layers that make up an effective honeypot.

Components:

1. **Decoy System**

   At the heart of the honeypot lies the decoy system, a carefully crafted entity that mirrors a high-valued target. Whether simulating a database server housing sensitive information or emulating a login portal for critical systems, the decoy system entices attackers to engage, believing they have found a vulnerable point of entry.

2. **Interaction Engine**

   Driving the illusion of compromise is the interaction Engine, an intelligent mechanism that dynamically responds to the attacker's actions. This adaptive engine tailors its behavior based on the attacker's techniques, enhancing the authenticity of the honeypot's responses and interactions. By adeptly mimicking the subtleties of a genuine system, the interaction Engine ensnares the attacker deeper into the deceptive web.

3. **Logging and Analysis**

   The honeypot architecture relies on meticulous Logging and Analysis, capturing every interaction for in-depth post-incident insights. This strategic asset unveils evolving attacker tactics and tools, crafting an extraordinary symphony in cybersecurity deception. It's a nuanced dance where illusion meets analysis, empowering defenders in the adversarial landscape.

3. Honeypot Detection Techniques

In the realm of cybersecurity deception, the effectiveness of a honeypot lies in its ability to convincingly deceive attackers. This section delves into the sophisticated techniques employed by the honeypot, weaving a tapestry of deception that not only traps attackers but also provides defenders with valuable insights into adversarial methodologies.

1. **Fake Data Injection**
   A masterstroke in the art of the deception, fake data injection involves surreptitiously introducing fabricated credentials or the data into the decoy system. The aim is to make the attacker believe their actions were successful, leading them into a false sense of accomplishment.
   Example:
   An attacker attempts to extract user credentials. In response, the honeypot artfully injects a set of fictitious but plausible usernames and passwords, creating the illusions of a successful data breach.
2. **Simulated User Interaction**
   To elevate the illusion of compromise, the honeypot engages in simulated user interactions on the fake system. These interactions may include mimicking user behaviors such as accessing files, opening applications, or engaging in dialogues with the attacker, fostering the belief of a genuinely compromised environment.
   Example:
   The attacker triggers a simulated user session where the honeypot convincingly performs tasks that resemble legitimate user actions, reinforcing the notion of a successful infiltration.
3. **Dynamic Responses**
   In the ever-evolving landscapes of cyber threats, adaptability is key. Honeypots employ dynamic responses, intelligently adjusting their reactions based on the attacker's behavior. This adaptability ensures resilience against variations in attack vectors, making the deception robust and enduring.
   Example:
   As the attacker modifies their approach, the honeypot astutely recognizes the change and dynamically adjusts its responses. This strategic flexibility maintains the illusion of compromise, regardless of the evolving tactics employed by the attacker.
   In the intricate dance of deception, these techniques form the backbone of the honeypot's ability to create a convincing illusion. By understanding and implementing these nuanced strategies, defenders not only cofound attackers but also gain a deeper comprehension of the shifting sands of adversarial intent.

4. Project Demonstration

The project demonstration serves as the grand stage where the intricate choreography of cybersecurity unfolds, revealing the prowess of an advanced honeypot in the face of a simulated attacker. This section meticulously engineers a symphony of deceptive maneuvers, emphasizing the illusory compromise orchestrated by the honeypot and the astute vigilance of the victim's detection mechanisms that shield against tangible harm.

Project Demonstration Overview

In this dynamic portrayal, the objective is to immerse the audience in a scenario where an attacker engages with the honeypot, believing in the success of their malicious endeavor. The honeypot, a technological maestro, seamlessly responds to the attacker's actions, artfully injecting fake data, mimicking user interactions, and dynamically adjusting its tactics to thwart different attack vectors.

Honeypot Execution Procedure for Deception Steps:

1. Entrancing the Attacker

Initiating the Simulation: Introduce a crafted scenario where an attacker, enticed by the allure of a seemingly vulnerable system, initiates a phishing attack on the honeypot.
Interaction Initiation: The honeypot, disguised as an enticing decoy system, responds to the attacker's initial interactions, drawing them further into the deceptive web.

2. Illusory Compromise

Fake Data Injection: As the attacker attempts to extract sensitive information, the honeypot adeptly injects fabricated yet plausible data, creating a mirage of successful compromise.
Simulated User Interaction: Showcase the honeypot engaging in user-like behaviors, such as accessing files or initiating communication, intensifying the illusion of a genuine compromise.

3. Dynamic Adaptation

Variation in attack Vectors: Introduce changes in the attacker's tactics, highlighting the honeypot's ability to dynamically adapt its responses to maintain the illusion of compromise.
Resilience in Deception: Emphasize how the honeypot remains resilient against evolving attack strategies, showcasing its capacity to stay one step ahead of the attacker.

4. Victim's Detection Mechanisms

Unveiling the Reality: At a strategic juncture, reveal that the victim's robust detection mechanisms have been silently at work, distinguishing between genuine and malicious interactions.
Preventing Real Compromise: Showcase instances where the honeypot's orchestration of fake data and simulated interactions did not lead to any actual compromise due to the victim's vigilant defenses.

Key Emphases:

Low False Positives: Throughout the demonstration, underscore the significance of low false positives, showcasing how the honeypot accurately discerns malicious intent without flagging legitimate interactions.
Technological Brilliance: Highlight the technological sophistication of the honeypot, portraying it as an intelligent entity capable of not just deceiving but outsmarting the attacker.
User Empowerment: Conclude the demonstration by emphasizing the empowerment gained through a deceptive yet vigilant cybersecurity approach, where users and systems actively thwart potential threats.

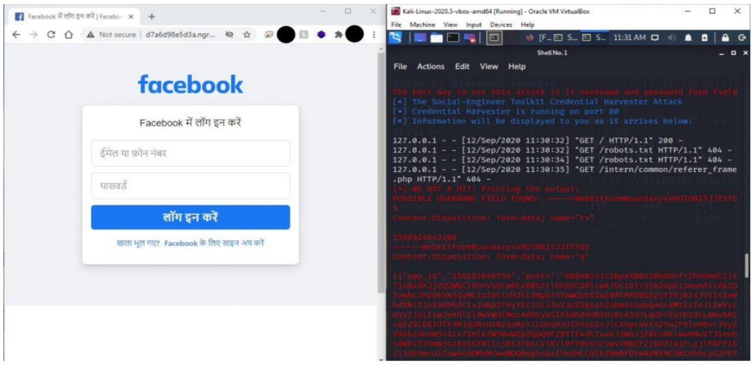
This grand narrative of illusion and defense not only illustrates the capabilities of an advanced honeypot but elevates the significance of a proactive and resilient cybersecurity strategy in the contemporary digital landscape.

5. Counter-Deception Tactic

Enhancing Security with Fake Credentials

In this process, upon receiving a phishing link, I deliberately input fake credentials. This strategic move creates an illusion for the attacker, leading them to believe they have successfully obtained genuine login details. However, I remain secure as I have provided deceptive information, fortifying my account against unauthorized access.

In the presented scenario, upon accessing the phishing link provided by the attacker, denoted as "d7a6d98e5d3a.ngrok.io," I intentionally fabricated input credentials. This strategic maneuver leads the attacker to believe that they have successfully compromised my account, falling under the assumption that I entered genuine login details. However, the reality unfolds as I have meticulously set up a honeypot, securing my account with deceptive information and outsmarting the attacker's malicious intentions.

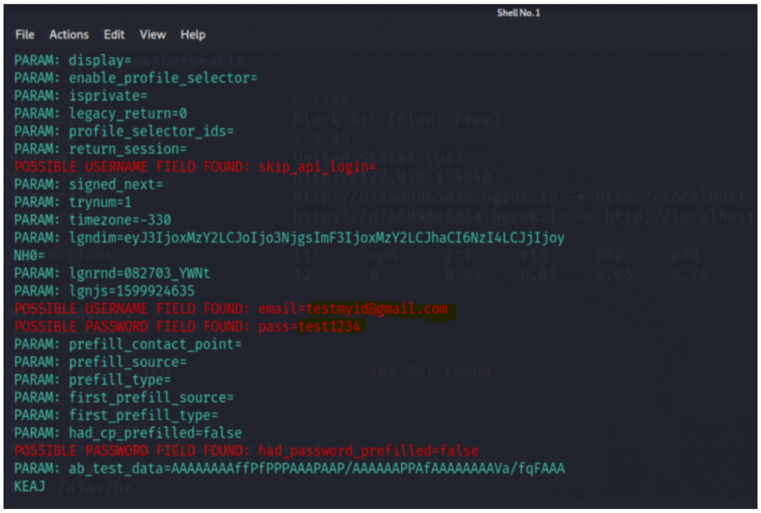

Facebook में लॉग इन करें | Facebook
Not secure | d7a6d98e5d3a.ngr...
facebook
Facebook में लॉग इन करें
ईमेल या फ़ोन नंबर
पासवर्ड
लॉग इन करें
खाता भूल गए? · Facebook के लिए साइन अप करें
Kali-Linux-2020.3-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
11:31 AM
Shell No.1
File Actions Edit View Help

```
The best way to use this attack is if username and password form field
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:

127.0.0.1 - - [12/Sep/2020 11:30:32] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [12/Sep/2020 11:30:32] "GET /robots.txt HTTP/1.1" 404 -
127.0.0.1 - - [12/Sep/2020 11:30:34] "GET /robots.txt HTTP/1.1" 404 -
127.0.0.1 - - [12/Sep/2020 11:30:35] "GET /intern/common/referer_frame
.php HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: ------WebKitFormBoundaryxV0DTOBI5JJI5TG
5
Content-Disposition: form-data; name="ts"

1599924643208
------WebKitFormBoundaryxV0DTOBI5JJI5TG5
Content-Disposition: form-data; name="q"

[{"app_id":"256281040558","posts":"KB94WIsIc2NyaXB0X3BhdGhfY2hhbmdlIix
[illegible]
```



```
PARAM: display=
PARAM: enable_profile_selector=
PARAM: isprivate=
PARAM: legacy_return=0
PARAM: profile_selector_ids=
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=-330
PARAM: lgndim=eyJ3IjoxMzY2LCJoIjo3NjgsImF3IjoxMzY2LCJhaCI6NzI4LCJjIjoy
NH0=
PARAM: lgnrnd=082703_YWNt
PARAM: lgnjs=1599924635
POSSIBLE USERNAME FIELD FOUND: email=testmyid@gmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=test1234
PARAM: prefill_contact_point=
PARAM: prefill_source=
PARAM: prefill_type=
PARAM: first_prefill_source=
PARAM: first_prefill_type=
PARAM: had_cp_prefilled=false
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
PARAM: ab_test_data=AAAAAAAAffPfPPPAAAPAAP/AAAAAAPPAfAAAAAAAAVa/fqFAAA
KEAJ
```

In this strategic move, the credentials I submitted during the interaction with the phishing attempt are intentionally false. This calculated measure ensures my safety and security, as the attacker, misled by the deceptive information, remains unaware of the actual login details. Thus, my account is shielded against my unauthorized access, underscoring the effectiveness of employing deceptive credentials as a proactive defense mechanism.

5. Confusion Matrix:

	Actual Positive	Actual Negative
Predicted Positive	True Positive	False positive (Low)
Predicted Negative	False Negative	True Negative

1. **True Positive:**
   - The honeypot successfully identifies the attacker's malicious actions, even when the attacker varies their tactics.
   - Occurs during the stages of the demonstration where the honeypot responds to the attacker's interactions with fake data injection, simulated user interactions, and dynamic adaption.
2. **True Negative:**
   - The victim's detection mechanisms correctly identify benign interactions with the honeypot, even when the attacker introduces variations in their attack.
   - Occurs when the victim's detection mechanisms unveil the reality, distinguishing between genuine and malicious interactions, preventing real compromise.
3. **False Positive:**
   - The honeypot incorrectly flags a legitimate interaction as malicious, but with low frequency due to its ability to handle variations in the attack.
   - This might occur if the honeypot, in its dynamic adaption, mistakenly interprets a genuine user interaction as an attack, but the occurrence is minimized.
4. **False Negative:**
   - The victim's detection mechanisms fail to identify malicious actions, allowing the attacker to proceed undetected, even when introducing variations.
   - This could occur if the attacker employs highly sophisticated tactics that temporarily evade the victim's detection mechanisms.

6. Conclusion

This project underscores the strategic imperative of deploying deception in the cybersecurity realm. Through the implementation of an adept honeypot, capable of artfully responding to attacker maneuvers, organizations can glean critical insights into malicious tactics without exposing themselves to actual threats. The meticulous integration of fake data injection, simulated user interactions, and dynamic responses in this advanced honeypot marks a significant advancement in cybersecurity deception strategies. The deliberate focus on minimizing false positives ensures that legitimate users navigate unimpeded, solidifying this deception mechanism as an indispensable asset in the defender's arsenal.

7. Bibliography

1. https://krebsonsecurity.com/
2. https://www.phishtank.com/
3. https://cyberscoop.com/cisa-fbi-epa-water-unitronics/
4. https://ieeexplore.ieee.org/abstract/document/5260965?casa_token=MgMx6eR_tJwAAAAA:q9LS_58EVB80aVCqMOH_qvGdumDXVOIySvHnBvt30k2ZeVmKdp-L8iMgQ0JQIbw0uPW8VyQj
5. https://www.researchgate.net/profile/Shabnam-Sharma-2/publication/329716781_Study_on_Phishing_Attacks/links/5ef9867a92851c52d6069bf2/Study-on-Phishing-Attacks.pdf
6. https://link.springer.com/article/10.1007/s11235-020-00733-2
7. https://www.cisa.gov/sites/default/files/publications/phishing_trends0511.pdf