國立臺灣師範大學資訊工程學系

113 資訊專題研究（一）期中書面報告

釣魚攻擊與防禦的紅藍對抗實踐

Phishing Attack and Defense: A Practical Red-Blue Team Exercise

指導教授官振傑教授

學生李曜宇撰

中華民國 113 年 10 月

摘要

在現代網路安全領域，釣魚攻擊仍然是最主要且有效的入侵手段之一，尤其是在高階持續性威脅（APT）攻擊中。攻擊者透過精心設計的釣魚郵件，引誘目標點擊惡意連結或下載惡意附件，從而取得系統的初始訪問權限。本專題旨在深入研究釣魚攻擊的技術和策略，透過紅方滲透演練實踐釣魚攻擊的方法，並隨後開發藍方的防禦措施。最終，我們將實現一個完整的紅藍對抗環境，以驗證攻擊和防禦策略的有效性，為企業和組織提供實用的安全建議。

1 背景

隨著數位化進程的加快，企業和組織對於網路安全的需求日益增加。然而，釣魚攻擊作為一種常見且有效的網路攻擊手段，仍然在全球範圍內造成了巨大的安全威脅。根據最新的網路安全報告，釣魚攻擊在各種攻擊手段中佔有相當大的比例，尤其是在高階持續性威脅（APT）攻擊中，釣魚郵件常常作為第一步，幫助攻擊者突破企業防線並深入系統內部。

根據《PHISHING ACTIVITY TRENDS REPORT 4th Quarter 2023》[1]，APWG 在 2023 年觀察到近五百萬次的釣魚攻擊，具體數量為 4,987,809 次，這使得 2023 年成為有記錄以來釣魚攻擊最嚴重的一年，超越了 2022 年的 4.7 百萬次攻擊。這一數據顯示，釣魚攻擊的規模和頻率持續上升，攻擊手法也愈發多樣化和精密化。

APT 攻擊通常具有長期滲透和高度隱秘的特點，其目的是取得持續的系統控制權限，並進行數據竊取或破壞性操作。釣魚攻擊作為 APT 的起點，通常依賴於社交工程技巧來騙取受害者的信任，讓他們主動點擊惡意連結或下載惡意軟體，這使得傳統的防禦機制難以有效偵測。

在這樣的背景下，如何有效地識別和防禦釣魚攻擊成為了網路安全領域的一個重要課題。雖然現有的安全工具能夠一定程度上防止常規的釣魚攻擊，但對於精心策劃的攻擊，尤其是 APT 背景下的攻擊，防禦效果仍然有限。因此，本研究希望從紅方和藍方的雙重角度，深入探討釣魚攻擊的實踐過程及對應的防禦措施。

2 研究動機

隨著網路技術的發展，企業和組織面臨的網路安全威脅日益嚴峻。APT 攻擊者通常利用釣魚郵件作為入侵的起點，因其成功率高且難以防範。然而，許多安全團隊對於釣魚攻擊的理解僅停留在理論層面，缺乏實際的攻防經驗。

為了更深入地理解釣魚攻擊的手法和防禦策略，我們決定從紅方（攻擊者）的角度出發，親自實踐釣魚攻擊的全過程。透過這種方式，我們可以更清晰地了解攻擊者的思維模式和技術手段。隨後，我們將站在藍方（防禦者）的立場，設計和實施針對性的防禦措施。最終，我們希望建立一個完整的紅藍對抗環境，模擬真實的攻擊和防禦場景，提升我們對於網路安全的實踐能力。

3 研究問題

1. 如何有效地設計和實施釣魚攻擊，突破目標的安全防線？
    - 釣魚郵件的內容和形式如何設計才能提高成功率？
    - 目標系統和用戶的哪些弱點可以被利用？
    - 在進行釣魚攻擊時，如何避免被防禦系統偵測？
2. 如何開發有效的防禦措施，預防和偵測釣魚攻擊？

- 哪些技術和策略可以提升釣魚郵件的偵測率？
- 用戶教育在防禦釣魚攻擊中起到什麼作用，如何有效實施？
- 如何建立一套完整的應對流程，在釣魚攻擊發生時迅速響應？

3. 如何構建一個紅藍對抗環境，以驗證攻擊和防禦策略的有效性？

- 紅藍對抗的場景如何設計，才能真實模擬實際的網路攻擊？
- 如何評估紅方攻擊和藍方防禦的效能和效果？
- 在對抗過程中，如何持續改進攻擊和防禦策略，達到最佳效果？

4. 成功釣魚後，紅方會進行哪些駭客行為？

- 一旦獲得系統初始訪問權限，紅方如何進一步擴展其控制範圍？
- 紅方常見的後續攻擊行為包括哪些，例如橫向移動、數據竊取等？
- 如何設計防禦措施來針對紅方在成功釣魚後的進一步行動？

4 預期成果

透過本研究，我們期望能夠：

1. 掌握釣魚攻擊的實際操作技能，瞭解攻擊者的手法和思維方式。
2. 開發一套針對釣魚攻擊的防禦措施，包括技術手段和用戶教育策略。
3. 構建一個完整的紅藍對抗環境，模擬真實的攻防場景，驗證我們的攻擊和防禦策略。
4. 提供詳細的實驗報告和安全建議，為企業和組織提升網路安全水平提供參考。

我們的研究最終希望能夠提升自身和他人對於釣魚攻擊和防禦的實踐能力，為網路安全領域的發展貢獻一份力量。

5 研究方法

1. 紅方滲透演練：學習並實踐釣魚攻擊的各種技術，包括社交工程、郵件偽造、惡意軟體開發等。在合法合規的前提下，對預設的目標系統進行釣魚攻擊測試。
2. 藍方防禦實施：基於紅方的攻擊手法，設計相應的防禦策略和技術措施。例如，配置郵件過濾器、開發釣魚郵件偵測工具、制定用戶培訓計劃等。
3. 紅藍對抗測試：建立一個模擬環境，讓紅方和藍方進行對抗測試。通過多次迭代，不斷改進攻擊和防禦策略。
4. 結果分析與報告：記錄對抗過程中的發現和經驗，分析攻擊和防禦的效果，並撰寫詳細的報告。

6 結論

透過本專題的實踐，我們將深入了解釣魚攻擊的全貌，從攻擊者和防禦者的雙重視角出發，提升對網路安全的理解和應對能力。我們相信，這種實踐經驗對於未來從事網路安全工作具有重要的價值。

References

[1] APWG, “PHISHING ACTIVITY TRENDS REPORT 4th Quarter 2023,” APWG, 2023.