ArgusHack

White Paper

産品白皮書

L.K.C.
Leukocyte-Lab

Introduction

資安威脅是全球性的議題，駭客透過新開發的攻擊手法以及自動化工具，輕鬆執行即可獲取海量的資訊。例如「釣魚郵件」是你絕對聽過的攻擊手法，對駭客組織早已是家常便飯的起手式，但在資安意識尚未普及的現今，仍是成功率極高的敲門磚。

面對驚濤駭浪的資安威脅，資安體系的建立是無可避免的，這包含資安設備投資、危機應變守則、人員資安意識培訓，其中最有效又容易達成的第一步，通常是從資安設備的投資開始。不過，容易被許多人忽略的是，資安設備的投資從來不是場軍備競賽，購入五花八門的資安設備，並不會和「安全」兩個字劃上等號。

具有資安意識的團隊，要能夠根據自身環境配置資安設備，讓所有設備適得其所。有趣的事情來了，每天吃的肉品需要通過安全驗證；消防設備需要通過專業檢測，有關安全的議題可不能自吹自擂，當一切都好似妥善的時候，要如何知道，你真的已經準備好了？

第三方驗證－以最客觀的角度執行資安檢測

資安檢測中，第三方驗證的存在有其絕對必要性，常見方案有弱點掃描、滲透測試、紅隊演練，能定期做到上述三者的團隊，已經有前段班的表現水準。然而，現實面告訴我們，這其中仍有駭客可入侵的空窗期。

舉例來說，紅隊演練確實成效良好，但不可忽略的是時程較長的演練週期，畢竟駭客可不會等你準備好才進攻，面對這樣的網路威脅，永遠不會有準備好的一天。資安團隊能做到的，就是確保威脅發生的當下，資安建設有堅守自己的工作崗位，將風險最大限度地降低。

抗體疫苗－在威脅來臨前做好萬全準備

無窮無盡的資安威脅，就像流行性傳染疾病一般，除了每年固定出現的流感，還有可能突變成未知的病毒。為避免過度暴露在威脅下，透過注射疫苗的概念獲得抗體，當更強勁的攻擊侵襲時，才能避免重大傷亡。

然而，在資安建設的第三方驗證上，真有像疫苗般的存在嗎？

網路世界的疫苗

入侵與攻擊模擬

Breach and Attack Simulation

入侵與攻擊模擬 (Breach and Attack Simulation, BAS)，經由 Gartner 解釋，是能夠在有限的風險下提供連續測試，並可用於警告 IT 和業務利益相關者，有關安全狀況方面的現有差距，或驗證安全基礎結構、安全規劃和防禦技術是否按期運行。

BAS 是一種資安驗證的解決方案，存在目的並非要取代既有第三方驗證。以較低的成本為受測環境提供持續性測試，補足傳統驗證方案週期間的空隙，達到相輔相成，進而優化整個驗證流程。

Red-Team 演練

資安專家進行

時程較長

演練成本高

協助企業找出資安建設不足

已有成熟資安建設與量能，進一步找出弱點

BAS 進行方式

高度自動化進行

時程短

演練成本低

快速驗證資安建設

累積資安量能，驗證資安建設，讓紅隊發揮最大價值

網路戰爭の機動要塞

ArgusHack

Next-Gen Breach & Attack Strategy Platform

ArgusHack (AGH) 是台灣第一套自行研發的 BAS 軟體，其中，我們把「Simulation」的概念替換成「Strategy」，重新定義為「入侵與攻擊演練策略平台」，進而擴大 BAS 在使用情境上的可能性。

我們打造了 ArgusHack-APT 與 ArgusHack-Center，分別對應不同的資安成熟度層級，無論在哪個階段皆能協助企業的資安量能不斷向前邁進。

ArgusHack APT

先進戰役重現

高效奠定精實基礎

能重現駭客戰役的 ArgusHack-APT，透過重現「真實攻擊」相較於僅模擬攻擊的 BAS，能達到更高效力的演練成果；自動化的靈活演練，讓企業高校奠定精實資安基礎。

ArgusHack Center

攻擊演練中心

持續積累資安能量

透過 ArgusHack-Center，除了定期更新的演練劇本與手法外，也能納入第三方滲透測試與紅隊演練報告中的測試手法，除了豐富企業的演練內容外，更能精準預防企業可能遭受的潛在攻擊。

ArgusHack

APT 先進戰役重現

檢視資安建設不足

熟練資安應變操作

驗證資安規劃成效

提升資安威脅經驗

適用情境：Red-Team 前

適用資安成熟度：B、C、D

成本：約 10 ~ 20% 紅隊演練成本

對於資安團隊的健全與否，最能直接驗證的方式，就是發動一場真實的駭客攻擊。在真實環境不受攻擊演練影響的前提下，透過靶機模擬真實的受測環境。針對已知的駭客組織攻擊手法進行演練，資安建設的問題將一目了然，資安團隊更能從演練中汲取駭客攻擊思維，作為演練後的檢討依據。

此外，每次的演練結果都能結合 MITRE ATT&CK、MITRE D3FEND 框架，產出有效的資安策略改善與投資依據，不論從設備、人員、投資面向來看，對資安團隊皆可獲得一定成效的幫助。

為什麼資安團隊需要入侵與攻擊演練？

許多資安團隊並不清楚自身的資安體系所位於的階級，並且會在這樣的狀態下執行紅隊演練，而紅隊演練就像是專家間的對決，紅、藍方各自為陣，但如果兩方勢力不均時，會發生什麼事呢？

常見的情況是，藍方花費了大筆資金投入紅隊演練，但由於自身資安體系尚未健全，除了輕易地被紅方攻下，演練中也無法完整記錄、監測到攻擊流量，而演練後所取得的修繕建議，也和投入成本不成正比。

入侵與攻擊演練就像是一套培訓資安團隊的解決方案，透過無數次的演練，可以觀察到體系中所欠缺的設備，資安團隊亦可不斷修正政策，讓資安設備符合預期地去監測與回報，也讓成員更熟悉告警與日誌的判讀。

當資安體系得到全方面的升級後，資安團隊有更多實力與紅隊抗議，此時從紅隊演練中能獲取更多經驗，從各方面讓紅隊演練效益最大化。

將每一分資安投資花在刀口。

如同剛出新手村即花錢挑戰最終魔王，花費大量金錢卻僅得到少量經驗值。過早採用紅隊演練也是，無法有效觀察與防禦紅隊時花費大量投資，卻無法有效的學習與成長。

我們認為，透過於企業環境內重現固定且真實的演練提升資安建設的健全度與資安團隊的熟練度，再進一步採用紅隊演練有效提升資安免疫力才是最經濟實惠的資安投資。

我們的優勢

一般而言，BAS 可用來復現駭客攻擊手法，並提供該項漏洞的持續性驗證。AGH-APT 的優勢則是在虛擬環境走過一套完整的「劇本」，這表示，從開始到結束都有脈絡可循，透過分析每一個通過與阻擋的步驟，讓資安團隊能更細膩的調整應對守則。

How it works

如同消防演習的概念，在不影響真實環境的情況，擬定一套完整有邏輯的情境。演習人員會用各種方式讓警鈴作響，而不是放一把火將建築物點燃。警鈴作響後，演習的民眾則會開始演練疏散的流程。

相同的道理，我們攻擊「靶機」製造流量，進而觸發資安設備響應，而不是直接讓客戶的伺服器癱瘓。

70% 節省
資安設備驗證時間

300% 提升
資安演練學習成果

ArgusHack

Center 先進戰役重現

檢視資安建設不足

熟練資安應變操作

驗證資安規劃成效

提升資安威脅經驗

適用情境：導入紅隊演練後

適用資安成熟度：A、B

成本：約 25 ~ 35% 紅隊演練成本

兼備「真實」與「即時」的特性，如同網路作戰指揮中心一般，隨時都能發動攻擊演練。

無論是 Zero-Day 或既有 One-Day 的漏洞，都可以編撰劇本執行自動化測試演練。高度可客製化的特性，也可以配合受測環境進行調整。此外，更可協同滲透測試、紅隊演練，將相關資訊製成劇本，即可達成自動化複測，隨時驗證修繕後的成效，更減少相關的人力成本。

系統內儲備常見漏洞與測試工具模組，搭載自動匹配與建議攻擊手法的功能，使用者可輕易執行簡易的攻擊演練。資安團隊亦可彈性設計各種演練劇本，並透過自動化攻擊重放功能，於多次複測中不斷校正，最終完成屬於企業的專屬劇本。

那麼多的第三方測試為何要用 ArgusHack？

一般而言，BAS 可用來復現駭客攻擊手法，並提供該項漏洞的持續性驗證。

AGH-Center 系統已納入多種攻擊漏洞手法、工具，並提供多種程式語言的編寫介面，使有能力編寫的資安人員更能彈性應用。除了 BAS 本身具備的持續性驗證，更可將其作為一種滲透、紅隊工具使用。

由 AGH-Center 所提供的持續性測試服務，首先將從原廠團隊進行入侵與攻擊演練，針對測試環境取得環境資訊，這包含硬體配置、網路架構、IP 網段等.....。

而這樣的入侵與攻擊演練，亦可作為一種滲透測試，並產出第三方驗證的正式報告。

透過人工初步的入侵與攻擊演練後，針對受測環境獲取更細膩的資訊，編寫可應用的攻擊流程與漏洞利用，能並客製化專屬於受測環境的劇本。

最終，利用屬於受測環境的客製化劇本，可以無限次、無指定時間，隨時對自身環境開始複測。

在不改變環境架構的情況下，劇本不但可以持續使用，更可週期性擴編，不斷擴大與豐富劇本內容。

一樣的第三方驗證，我們省去複測的人力、時間、服務成本。

一樣的第三方驗證，我們客製化您的專屬演練劇本。

一樣的第三方驗證，我們隨時間不斷的進步與擴大。

其他運用方式

無限次複測方案

基於客戶所提供的滲透測試、紅隊演練或攻擊演練等資安報告，將報告中所揭露之攻擊手法編撰成入侵與攻擊演練劇本，讓客戶可自行用於自動化複測與重複性演練中。

吸收各方紅隊、滲透資源

透過收集不同的的滲透測試與紅隊演練，將報告中所揭露之攻擊手法編撰成入侵與攻擊演練劇本，持續擴大 AGH-Center 軍火庫。