RAPID7 PRODUCT BRIEF

metasploit®

測試您的安全防禦

Rapid7的滲透測試解決方案Metasploit 可提高滲透測試人員的效率，驗證漏洞、網路釣魚和更廣泛的社交工程，並提高受測單位的安全意識

了解對手的行動有助於您更充分地準備防禦措施

Metasploit為您提供了由超過200,000名用戶和貢獻者所組成的社群支援的洞察力：它是全球最具影響力的滲透測試解決方案。 透過 Metasploit，您可以發現防禦中的弱點，專注於最高風險，並改善您的安全結果。

了解你的弱點

模擬真實世界的攻擊，以便在惡意攻擊者發現之前找到你的弱點。 Metasploit與其開源框架無縫整合，讓您可以使用相關偵察模組，從而節省您的工作並加速測試。 使用攻擊者技術來逃避防毒程式，查找弱點憑據，並在整個網路中進行透通測試。

使用世界上最大的源碼漏洞審查資料庫

Rapid7 由 Metasploit Framework開源項目提供對攻擊者心態，當前向量和方法的獨特見解。 Rapid7與使用社群合作，每周定期添加新的攻擊參數，目前正在積累超過2,300個漏洞和超過3,300個模組和有效負載。

針對您的防禦的模擬真實攻擊

Metasploit有效的避開防病毒程式，並使您能夠運用超過330多個高效能模組，從受感染機器中發現外洩數據。 一旦一台設備受到攻擊，透過Credential Domino MetaModule或簡易的VPN數據透視深入挖掘您的網路，並了解攻擊者可以進行多遠。

發現弱點和使用憑據

測試您的網路是否存在弱密碼和過期重複密碼。 除了破解操作系統帳戶之外，Metasploit還可以針對超過 15種帳戶類型（包括資料庫，Web 伺服器和遠端管理程式）進行暴力攻擊。

070717

Rapid7 has worked with the user community to amass more than 2,300 exploits and more than 3,300 modules and payloads.

優先考慮最重要的事情

找到你的弱點只完成防禦工作的一半。作為滲透測試人員，您的工作是進行全面評估並告知如何降低違規風險。Metasploit 允許您查明攻擊鏈中的弱點連結，然後使用 Top Remediation Reports 並透過 InsightVM 或 Nexpose無縫地整合驗證漏洞並確定其優先級別。

精確定位攻擊鏈中的弱點連結

現今網路之攻擊手法更加複雜; 對手正在使用多種組合技術好更快地破壞您的系統。使用Metasploit，您可以從對手的角度模擬攻擊，並輕鬆找出最大的安全風險。

與Rapid7 InsightVM和Nexpose進行無縫地整合驗證漏洞

當其他單位質疑弱點掃描結果的有效性時，請證明漏洞會使系統和數據面臨風險。您將獲得補救措施並與設備相關者建立公正信譽。Metasploit 和 InsightVM（或Nexpose）的整合，提供了單一供應商驗證解決方案，可簡化漏洞優先級劃分和補救報告。

提高您的成效

作為一名滲透測試員，您無需浪費時間在等待。Metasploit 允許您透過大規模運行滲透測試更快地完成合規性計劃來加速改進系統漏洞。 此外，您還可以模擬網路釣魚活動，以獲取憑據，提供有效資訊及提高內部安全意識。

大規模運行滲透測試程序

使用傳統的指令工具進行評估並在100多台主機的網路中管理資料是相當具有挑戰性的工作。Metasploit可以擴展支援數千台主機在每個測試項目中，並可支援多個同步滲透測試人員。您可使用任務鏈，資源腳本和MetaModule自動執行滲透測試步驟，以提高工作效率。

使用複雜的社交工程測試和滲透使用者設備

使用Metasploit Pro的網路釣魚模組向成千上萬的用戶發送和追踪電子郵件。只需單擊一下即可複製Web應用程式登錄頁面，以通過測量社交工程通路中每個步驟的轉化率來獲取憑據，提供有效資訊並進行內部安全意識培訓。

更快地完成合規性計劃

完整報告產出以顯示您的發現並根據PCI DSS和FISMA等法規對其資訊進行分類。此外，用戶可以驗證為保護系統而實施的補償控制是否可操作且有效。更棒的是， Metasploit 自動記錄網路和應用程式評估中的操作和發現，以節省手動建構報告所花費的寶貴時間。

“ Metasploit Pro 中的開發模塊非常棒。它使我不必手動記錄這麼多，節省了大量的工時。”

- Tim Lawrence, IT Security Analyst
AutomationDirect