DDoS 攻擊模擬測試報告

時間:2024.9.20

參與人員：資訊部人員 2 人

攻擊模擬前準備	模擬攻擊類型	攻擊響應驗證	攻擊緩解測試	測試後恢復	注意事項
一、測試環境搭建 1.部署獨立測試網路，隔離生產環境 2.攻擊模擬工具： A.OWASP ZAP（漏洞掃描與攻擊模擬） B.ApacheBench（HTTP 洪泛攻擊模擬） 3.流量監控工具： A.Wireshark（實時流量分析） B.Netstat（連接狀態監測）	一、攻擊類型： HTTP Flood（層 7 應用層攻擊） 二、攻擊工具： ApacheBench 三、攻擊指令： bash ab -n 10000 -c 100 http://目標服務器 IP/ -n：總請求數（10,000 次） -c：併發請求數（100 個）	一、 防火牆行為觀察 1.是否觸發速率限制（如每秒請求數閾值） 2.異常流量是否被自動攔截（基於規則或 AI 學習） 3.狀態檢測（如 TCP 連接跟踪）是否生效	一、手動干預驗證 1.封禁攻擊源 IP（使用防火牆規則） 2.驗證封禁後流量是否下降 二、自動化防護測試 1.啟用 DDoS 防護模組（如 Palo Alto Cortex XDR） 2.驗證流量清洗設備（如 F5 BIG-IP）是否正常工	一、重置防火牆配置 二、清理測試數據 三、生成測試報告 1.攻擊類型與流量規模 2.防火牆攔截效率 3.業務受影響程度 4.優化建議（調整規則）	一、合法性：確保獲得書面授權，避免觸犯網路安全法規。 二、風險控制：從低流量攻擊開始逐步加壓，防止業務中斷。 三、監控覆蓋：攻擊期間需實時監控網路、伺服器和防火牆狀態。

二、防火牆配置 1.備份當前防火牆規則與閾值設定 2.啟用詳細日誌記錄： A.流量類型（HTTP/HTTPS） B.源 IP 地址 C.攻擊特徵（如異常請求速率） 三、協調通知 1.通知維運與安全團隊測試計劃 2.確認業務系統可承受短暫流量衝擊		二、日誌分析 1.統計被攔截的攻擊流量特徵（如源IP、請求類型） 2.檢查誤報 / 漏報情況（如正常業務是否被阻斷） 三、業務影響評估 1.伺服器響應時間變化（使用 JMeter 監測） 2.網路頻寬利用率（超過 80% 視為異常） 3.服務可用性（HTTP	作		

		200/503 狀態碼比例）			