滲透測試實務應用

Code Review & HostVA tools

洪睿宸, 邵靖翔

Slide here!

Code Review: Bearer

- Bearer CLI 是一種靜態應用程式安全測試 (SAST) 工具，可掃描原始程式碼並分析資料流，以發現、過濾安全性和隱私風險並確定其優先順序。
- 目前支援：JavaScript/TypeScript (GA)、Ruby (GA)、PHP (GA)、Java (Beta)、Go (Beta)、Python (Alpha)
- Pros: 安裝快速、CLI
- Cons: 沒有好看的report

Code Review: Bearer

檢測出多種風險、歸類並依照風險等級排序

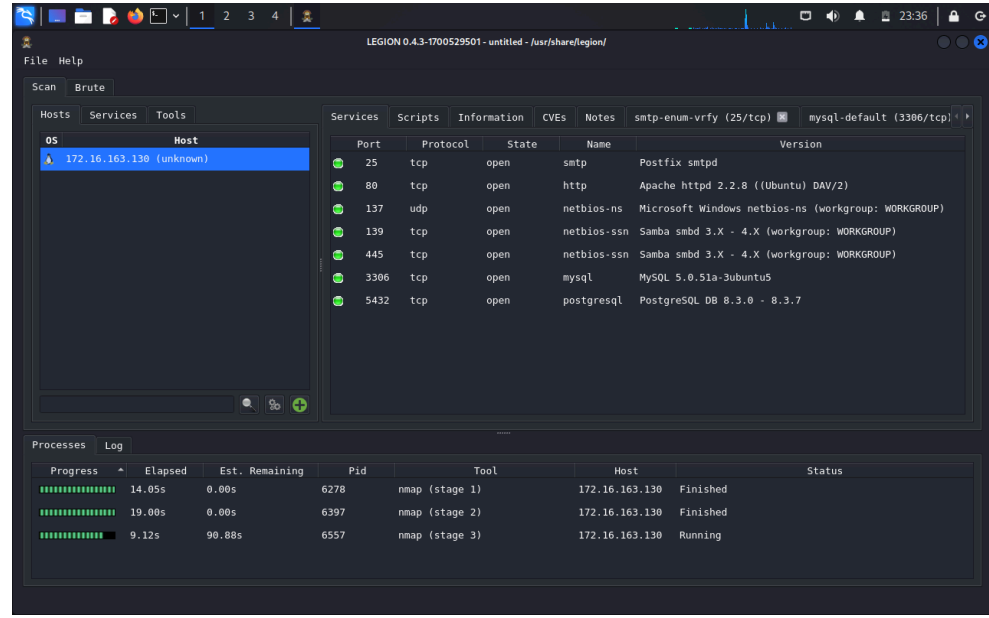
以檢測Vulnerable-Code-Snippets為例，共檢測出87個風險

其中0個為critical、49個為high、18個為low、17個warning

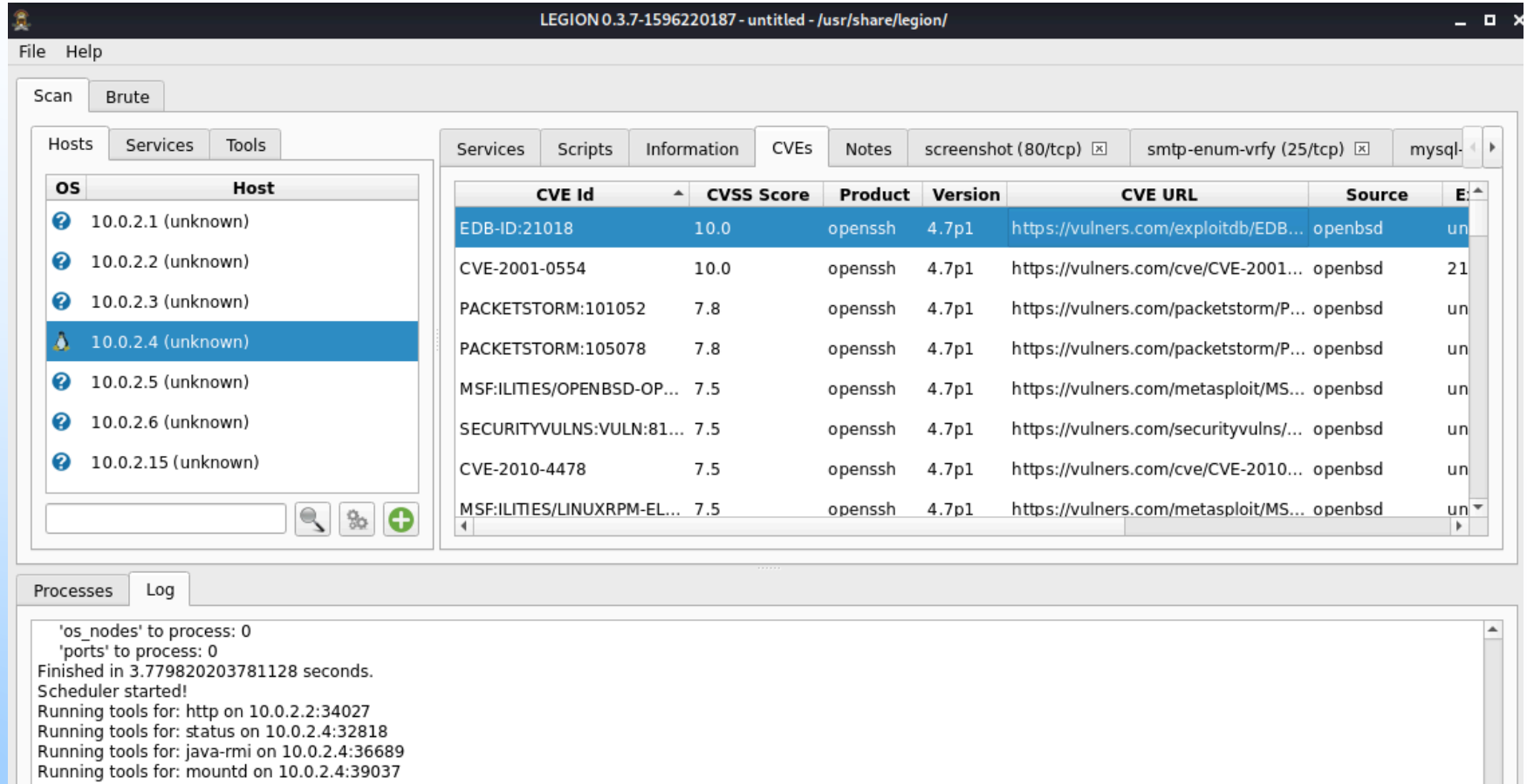
Host VA: Legion

Legion是一個開源的半自動網路滲透測試工具，適合用來進行探索 可以識別網路中的設備並對暴露出的目標設備進行攻擊

會利用Nikto、whataweb、sslyzer、vulners、SMBenum、 NMAP、THC Hydra、Shodan的自動化程序來進行掃描



Host VA: Legion



Thanks for Listening