

الاعضاء: سعود المري - راشد حمد - سعود العامري
- عبد العزيز الهاجري - راشد عبد الله اللبده

اسم المشروع : Recon v2 اسم الفريق: NetScouts

التحدي

المحتوى

- الحاجة إلى أداة موحدة تساعد مختبري الاختراق على جمع معلومات مفصلة عن الأهداف بسرعة وكفاءة.
- وجود أدوات متعددة تؤدي وظائف متفرقة مما يؤدي إلى التشتت وتأخير سير العمل في المهام الأمنية.
- أهمية توفير تقرير شامل بعد الاستطلاع لاستخدامه في العروض أو كجزء من التقييم الأمني.

المنهجية

المحتوى

- تطوير أداة شاملة بلغة Python تجمع أبرز مهام الاستطلاع في أداة واحدة.
- استخدام مكتبات خارجية مثل whois, shodan, requests, و nmap لتنفيذ وظائف متعددة.
- تنظيم الأداة من خلال قائمة رئيسية (CLI) تسهل على المستخدم اختيار المهمة المطلوبة.
- تقسيم الأداة إلى وحدات: مثل بحث WHOIS ، استعلام DNS ، المسح عبر Shodan، تحديد المنافذ المفتوحة، جمع العناوين الفرعية، إلخ.
- توفير مخرجات قابلة للحفظ والاستخدام في تقارير تحليلية.

الحل

المحتوى

أداة الاستطلاع المتقدمة تقوم بتنفيذ ما يلي:
استعلامات WHOIS للكشف عن تفاصيل النطاق.
جمع العناوين الفرعية باستخدام واجهات برمجة تطبيقات عامة.
استعلامات Shodan للكشف عن الخدمات المكشوفة.
مسح المنافذ باستخدام Nmap.