# جدول أدوات تحليل الحزم والمراقبة في اختبار الاختراق

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| اسم الأداة | كيف تعمل الأداة | سبب اختيارها | وظيفتها | نتائجها المتوقعة |
| Wireshark | أداة رسومية لتحليل حركة مرور الشبكة تقوم بالتقاط الحزم واستعراضها بشكل مفصل. | لأنها توفر واجهة سهلة لفهم وتحليل الترافيك بدقة. | تحليل البروتوكولات والتقاط الحزم وفهم محتوياتها. | فهم سلوك الشبكة، واكتشاف التهديدات أو التسريبات أو التكوينات الخاطئة. |
| tcpdump | أداة سطر أوامر تلتقط حزم الشبكة وتعرضها مباشرة أو تحفظها للمعالجة. | لأنها خفيفة وسريعة وتعمل في بيئات لا تدعم الواجهات الرسومية. | تحليل الحزم مباشرة من التيرمنال. | رصد الحزم وفهم الاتصالات الشبكية بشكل مباشر وسريع. |
| Ettercap | أداة لتنفيذ هجمات التنصت (Sniffing) والتلاعب بالحزم في الشبكات المحلية. | لأنها فعالة في اختبارات MITM على الشبكات الداخلية. | تنفيذ هجمات Man-in-the-Middle وجمع البيانات. | التقاط كلمات المرور، إعادة توجيه الجلسات، وتحليل سلوك المستخدم. |