# جدول أدوات الحماية والمراقبة في الشبكات

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| اسم الأداة | كيف تعمل الأداة | سبب اختيارها | وظيفتها | نتائجها المتوقعة |
| Arpwatch | يراقب تغييرات عناوين MAC المرتبطة بعناوين IP في الشبكة ويرسل تنبيهات عند حدوث تغييرات غير متوقعة. | للكشف المبكر عن هجمات انتحال الهوية (ARP Spoofing). | مراقبة الشبكة وتسجيل تغييرات عناوين MAC/IP. | الكشف عن أي نشاط مريب في الطبقة الثانية وإرسال تنبيهات تلقائية. |
| Snort IDS | نظام كشف التسلل يعمل بتحليل الترافيك الشبكي ومطابقته مع قواعد لاكتشاف التهديدات. | لأنه مفتوح المصدر وفعال في كشف الهجمات المعروفة وغير المعروفة. | كشف التهديدات وتحليل الحزم وتوليد تنبيهات أمنية. | تحديد الهجمات ومحاولات التسلل وتسجيلها بشكل مفصل. |
| iptables | أداة في أنظمة Linux لإعداد قواعد الجدار الناري والتحكم في الترافيك الوارد والصادر. | لأنه مرن وقابل للتخصيص ويعمل على مستوى النواة. | إدارة الجدار الناري وتصفية الترافيك. | حظر أو السماح بالاتصالات حسب السياسات المحددة. |
| fail2ban | يراقب ملفات السجلات ويمنع عناوين IP التي تحاول الدخول غير المصرح به مرارًا. | لتقليل محاولات التخمين والهجمات العشوائية على الخدمات. | حماية من هجمات brute-force على SSH وخدمات أخرى. | منع الوصول المؤقت أو الدائم لعناوين IP المشبوهة. |