جدول اختبار الاختراق - شبكة الرعاية الصحية (الجزء 2)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| رقم | المرحلة | الأداة المستخدمة | الهدف (IP/جهاز) | النتيجة | ملاحظات / هل تم تسجيله؟ |
| 8 | هجوم كلمة المرور | Hydra | 192.168.130.10 (SSH) | تم الكشف عن بيانات دخول ضعيفة | لم يُسجل في الجدار الناري |
| 9 | تصيّد داخلي | Bettercap | شبكة الضيوف | تم التقاط بيانات اعتماد HTTP | تم تسجيل النشاط كـ MITM |
| 10 | محاولة رفع ملف ضار | curl + Netcat | Web Server (DMZ) | تم منع الاتصال على البورت 4444 | تم تسجيله في IPS |
| 11 | التنصت على الترافيك | Wireshark | VLAN 120 | تم التقاط بعض الحزم غير مشفرة | غير مسجّل لأنه Passively |
| 12 | اختبار بروتوكول DNS | dig, dnsenum | 192.168.150.1 | تم استرداد معلومات DNS حساسة | لم يتم تسجيله |
| 13 | تحليل الشبكة التحتية | arp-scan | كل الشبكة | تم اكتشاف عناوين MAC غير موثوقة | لم يُسجل في الجدار |
| 14 | فحص SSL | sslscan | 192.168.200.20 | تم العثور على دعم لـ SSLv3 | تم التنبيه في FortiGate |