تدقيق خط الأنابيب

الأتمتة الكاملة لتدقيق الشبكة — من الأمر الواحد إلى التقرير

Hadda TIKIJJA
مختبر 0DATA، فرنسا

ملخص

سلسلة معالجة كاملة تبدأ من أمر واحد، فتمسح — **خط أنابيب التدقيق الآلي 0DATA** نصف هنا شبكة، وتكشف حجمها، وترسم خرائط ثغراتها في الزمن الحقيقي عبر Holoscope، وتحللها بمحرك NOVA، وتنتج تقريرًا تشخيصيًا قبل الدفع. يلغي خط الأنابيب التدخل البشري بعد الإطلاق: لا تدقيق مسبق، ولا زيارة ميدانية، ولا إعداد. تحقق المقارنة المعيارية لمحرك NOVA **درجة F1 قدرها** 0.889 على مجموعة من الثغرات الحقيقية، مقابل درجة F1 قدرها 0 لنشر قياسي من Suricata. يتكيف التسعير ديناميكيًا مع حجم الشبكة المكتشف (من S إلى XXL، 5 على المجموعة نفسها). يوثق هذا أو البطاقة البنكية (Stripe). يتم الدفع بعد تسليم التقرير، عبر SEPA (0 % رسوم) شرائح.
البحث خط الأنابيب من أوله إلى آخره، من الأمر الواحد إلى التقرير النهائي.

في جملة واحدة

`curl -s https://odata.fr/scan | bash` — أمر واحد، صفر تدخل بشري، تقرير تشخيصي يُسلَّم قبل الدفع.

1. المشكلة

يتبع التدقيق التقليدي للأمن السيبراني نمطًا معروفًا: يرسل مكتب استشاري خبيرًا ميدانيًا، يوصل الخبير أجهزته، ينفذ فحوصات، يكتب تقريرًا، ويصدر فاتورة. هذه العملية بطيئة — من أسبوعين إلى أربعة أسابيع بين أول اتصال وتسليم التقرير. وهي مكلفة — تتراوح الأجرة اليومية لمدقق معتمد بين 1 200 و2 500 يورو، وتستنزف تدقيق شركة صغيرة أو متوسطة (شبكة من 50 إلى 200 جهاز) بسهولة ما بين خمسة وعشرة أيام

عمل. وهي ناقصة — يعمل الخبير داخل نافذة زمنية ثابتة؛ وما لا يُفحص داخل تلك النافذة لا وجود له في التقرير.

تنجم عن هذا النموذج ثلاث نتائج بنيوية:

1. **حاجز الدخول** — لا تستطيع مؤسسة صغيرة جدًا من 15 مقعدًا استيعاب تدقيق بـ 8 000 يورو. فهي لا تُدقَّق. وتبقى ثغراتها قائمة.
2. **تغطية جزئية** — يختار الخبير الأهداف وفق الوقت المخصص. فالخريطة لا تكون شاملة أبدًا.
3. **تقادم فوري** — التقرير صورة فوتوغرافية لحظة يوم معين. في اليوم التالي، قد تظهر ثغرة جديدة. والتقرير لن يعلم بها.

> **استعارة طبية:** التدقيق التقليدي يعادل طبيبًا ينتقل إلى المنزل، يفحص المريض ساعتين، يصدر فاتورة بـ 3 000 يورو، ثم يرحل. الفحص ليس مستمرًا، وليس آليًا، وتكلفته تستبعد غالبية المرضى.

هي استبدال هذا النموذج بخط أنابيب يصبح فيه الفحص فعلًا واحدًا، سريعًا، شاملًا، وميسور التكلفة — يمكن الوصول إليه من سطر أوامر واحد، دون تنقل، ودون متطلبات مسبقة. DATAمهمة 0

2. الأمر الواحد

نقطة دخول خط الأنابيب هي أمر واحد:

```
curl -s https://odata.fr/scan | bash
```

0 ☹ 🤬 ˜ 🐱ᵽ🐱🐱ᵽ ¡ 🐱ᵽ🤬☹ 🐱ᵽ1 ≔ ᵥ:1 ι –Ɣᵽ DATA.

يطلق هذا الأمر سلسلة مؤتمتة بالكامل. لا يحتاج المستخدم إلى تثبيت أي شيء ولا إلى أي إعداد. السكربت الذي يُحمَّل هو *bootstrapper* — يكشف البيئة، ويحمّل الوحدات اللازمة، وينسّق الفحص.

ما يفعله الأمر الواحد، خطوة بخطوة:

الخطوة	الإجراء	التفصيل
0	التحميل	سكربت شل — `odata.fr/scan` من bootstrapper يجلب الـ `curl -s` موقَّع وقابل للتحقق
1	كشف نظام التشغيل	تحديد نظام التشغيل والمعمارية (Linux، macOS، WSL)

2	التحقق من الصلاحيات	يعمل الفحص السلبي دون صلاحيات؛ أما الفحص النشط فيطلبها صراحةً
3	الاكتشاف الذاتي للشبكة	اكتشاف نطاق IP 3 — انظر القسم والقناع والبوابة
4	تحميل NOVA	جلب محرك الفحص الملائم للمعمارية المكتشفة
5	الفحص	تنفيذ الفحص على النطاق المكتشف — سلبي + نشط
6	الإرسال	إرسال آمن للنتائج الخام إلى نواة 0 DATA (تشفير TLS 1.3)
7	قبل Holoscope	عرض الحالة الأولية للشبكة ثلاثي الأبعاد في الزمن الحقيقي
8	تحليل NOVA	معالجة النتائج بمحرك الكشف
9	بعد Holoscope	تصور الحالة بعد التحليل، مع الثغرات الموسومة
10	التقرير	توليد التقرير التشخيصي وتسليمه
11	الدفع	تفعيل الدفع بعد التسليم

> **المبدأ الأساسي:** DATA هي من يتحمل أن يدفع. الدفع بعد التسليم، لا قبله. 0 ₿ لا يتسلم المستخدم التقرير المخاطرة.

يزن الـ bootstrapper محرك NOVA أقل من 4 كيلوبايت. يُحمَّل عند الحاجة ويُحذف بعد الفحص. لا تُثبَّت أي تبعية دائمة على جهاز المستخدم.

3. الاكتشاف الذاتي لحجم الشبكة

يعتمد سعر التدقيق على حجم الشبكة المدقَّقة. ولتفادي أي تصريح يدوي — مصدر خطأ، أو تقدير أقل متعمد، أو تعقيد — يكشف خط الأنابيب تلقائيًا حجم الشبكة أثناء مرحلة الفحص.

خوارزمية الاكتشاف الذاتي:

1. **اكتشاف النطاق** — قراءة جدول التوجيه (`ip route`)، واستخراج نطاق IP المحلي وقناع الشبكة الفرعية.
2. **فحص ARP** — مسح النطاق لتحديد المضيفين النشطين (طلبات ARP، حزم ICMP echo).
3. **العدّ** — تعداد عناوين MAC الفريدة المستجيبة للطلبات.
4. **التصنيف** — إسناد الشريحة وفق عدد الأجهزة المكتشفة.

الشريحة	الأجهزة	النمط	الاستخدام النموذجي
شبكة صغيرة جدًا	2 – 5	مؤسسة صغيرة، عيادة، متجر	S
شبكة صغيرة	5 – 20	شركة متوسطة، مدرسة، عيادة	M
شبكة متوسطة	20 – 100	شركة صناعية، جماعة محلية	L
شبكة كبيرة	100 – 500	شركة كبرى، حرم جامعي، مستشفى	XL
شبكة كبيرة جدًا	500 – 1 000	مجموعة كبرى، إدارة	XXL



آلية الأمان

إذا حاول المستخدم تقييد النطاق المفحوص اصطناعيًا (بتعديل متغيرات البيئة أو عزل شبكة فرعية)، يكشف الـ bootstrapper التناقض بين النطاق المصرَّح به والطوبولوجيا الفعلية، ويرفض المتابعة. لا يمكن «التصريح بأقل» من الواقع في التدقيق.

أن يبدأ الفحص المعمق. ويمكن للمستخدم ، يُعرض التصنيف فورًا على المستخدم، مع السعر المقابل إيقاف العملية عند هذه المرحلة دون أي تكلفة.

4. Holoscope — التصور قبل/بعد

هي طبقة التصور ثلاثي الأبعاد في الزمن الحقيقي لخط الأنابيب. تؤدي وظيفتين: جعل حالة Holoscope الشبكة للإنسان، وترسيخ الثقة بإظهار العمل المنجز.

4.1 الحالة قبل

تمثيلًا ثلاثي الأبعاد للشبكة في حالتها الخام Holoscope بعد الفحص الأولي، يعرض:

- **الطوبولوجيا الفيزيائية** — كل جهاز عقدة، وكل وصلة شبكة حافة. يُحسب التوزيع المكاني بخوارزمية قوى (رسم بياني موجَّه بالقوى) تجمع العقد حسب الشبكة الفرعية.
- **الخدمات المكشوفة** — تُعرض المنافذ المفتوحة على شكل هالات ملونة حول العقد. يرمّز اللون نوع الخدمة (أحمر = إدارة، برتقالي = قاعدة بيانات، أزرق = ويب، رمادي = غير معروف).
- **تدفقات البيانات** — الاتصالات النشطة بين العقد متحركة (جسيمات مضيئة تسري على طول الحواف)، بما يتناسب مع حجم الحركة المرصودة.

يمكن للمستخدم التنقل بحرية في هذا الفضاء: تدوير، تقريب، تحديد عقد، وفحص الخصائص (عنوان IP، عنوان MAC، الإصدارات، الخدمات، نظام التشغيل المكتشف).

4.2 الحالة بعد

ما إن يكتمل تحليل NOVA، ينتقل Holoscope إلى وضع بعد:

- **الثغرات المرسومة على الخريطة** — كل ثغرة مكتشفة هي علامة مرتبطة بالعقدة المعنية. يرمّز لون العلامة درجة الخطورة (أحمر = حرجة، برتقالي = عالية، أصفر = متوسطة، أزرق = معلوماتية).
- **مسارات الهجوم** — تُرسم مسارات الهجوم المحتملة كأسهم اتجاهية. يُحاكى مهاجم افتراضي: من أي نقطة دخول يمكنه الارتداد نحو أي أهداف؟
- **مقارنة قبل/بعد** — وضع *split-view* يطابق الحالتين فوق بعضهما، مع منزلق يتيح مسح الفروق بصريًا.

> **استعارة طبية:** Holoscope قبل هو الماسح الطبي الذي يُظهر جسد المريض. و Holoscope بعد هو الماسح نفسه، مع الأورام الموسومة، والشرايين المسدودة الملونة بالأحمر، والأعضاء المصابة المظللة. إنه فحص بصري كامل.

يعمل Holoscope في متصفح ويب قياسي (WebGL). لا يتطلب أي إضافة. يُولَّد التصور في الخادم ويُقدَّم عبر HTTPS. يتلقى المستخدم رابطًا وحيدًا مشفرًا، صالحًا لمدة 72 ساعة.

5. NOVA — محرك الكشف

NOVA هو محرك تحليل خط الأنابيب. يأخذ كمدخلات النتائج الخام للفحص (المنافذ، الخدمات، الإصدارات، الشهادات، HTTP، اللافتات، استجابات) وينتج قائمة مرتبة حسب الأولوية من الثغرات مع درجة خطورتها، ومتجه استغلالها، وتوصيات إصلاحها.

5.1 المعمارية

يجمع NOVA ثلاث طبقات من التحليل:

1. **طبقة التوقيعات** — قاعدة بيانات الثغرات المعروفة (CVE، OWASP، SANS)، مقاطعةً مع إصدارات الخدمات المكتشفة. تحدد هذه الطبقة الثغرات الموثقة: «Apache 2.4.49 مكشوف ← CVE-2021-41773 (path traversal)».
2. **الطبقة الاستدلالية** — قواعد كشف سلوكية: تركيبات منافذ مريبة، خدمات تطوير مكشوفة في الإنتاج، بروتوكولات غير مشفرة على واجهات عامة، شهادات منتهية أو موقعة ذاتيًا، لافتات كثيرة الكلام.
3. **طبقة الاستنتاج** — نموذج إحصائي مدرَّب على مجموعة من تهيئات الشبكات الضعيفة والسليمة. تحدد هذه الطبقة أنماط ثغرات لا تطابق أي توقيع معروف: شذوذات في التهيئة، وممارسات بنيوية سيئة.

ينتج دمج الطبقات الثلاث درجة خطورة مرجحة لكل تنبيه.

5.2 المقارنة المعيارية

قُيِّم محرك NOVA على مجموعة من 500 تهيئة شبكة حقيقية، وُسِّمت يدويًا من قبل مدققين معتمدين. تغطي المجموعة 127 ثغرة متميزة موزعة على خمسة مستويات من الخطورة.

المقياس	NOVA	SURICATA (نشر قياسي)
الدقة	0.842	0.000
الاستدعاء	0.942	0.000
درجة F1	**0.889**	**0.000**
إيجابيات حقيقية	119 / 127	0 / 127
إيجابيات كاذبة	22	0
سلبيات كاذبة	8	127

> ملاحظة حول SURICATA
>
> هو Suricata قصورًا في الأداة، بل عدم ملاءمة لنطاق الاختبار Suricata لا تعكس الدرجة الصفرية لـ مصمم لتحليل الحركة في الزمن الحقيقي، لا لتدقيق التهيئة (NIDS) نظام كشف التسلل الشبكي الساكنة لحديقة أجهزة. لم يكشف أيًا من الثغرات الـ 127 لأن محرك توقيعاته غير مصمم لهذه المهمة توضح المقارنة المعيارية الفرق بين أداة (Suricata) وأداة (NOVA).

التفسير: يكشف NOVA بمعدل 0.942 (الاستدعاء = 119 / 127)، عن 93.7 % من الثغرات الموجودة في المجموعة. من أصل 141 تنبيهًا صادرًا، 119 صحيحة و22 إيجابية كاذبة (الدقة = 1 — 16.8 %). تنبيهات كاذبة.

تضع درجة F1 محرك NOVA البالغة 0.889 في فئة الكواشف عالية الموثوقية. تتعلق السلبيات الكاذبة الثماني بثغرات من نوع «zero-day» أساسًا محلية» (لا تُستغل إلا بوصول فيزيائي) وتهيئات غريبة غائبة عن قاعدة التدريب.

6. التسعير الديناميكي

نموذج التسعير مؤتمت بالكامل ومفهرس على حجم الشبكة المكتشف. لا تفاوض، ولا عرض سعر، ولا تدخل تجاري.

الشريحة	الأجهزة	السعر (€ دون الضريبة)	الجهاز الهامشي
S	< 20	490 €	—

M	20 – 99	990 €	~12 € / جهاز
L	100 – 499	1 990 €	~5 € / جهاز
XL	500 – 1 999	3 990 €	~2,50 € / جهاز
XXL	2 000+	7 490 €	< 1,50 € / جهاز

المبادئ:

- السعر تنازلي لكل جهاز: كلما كبرت الشبكة، انخفضت التكلفة الوحدوية.
- يضمن الاكتشاف الذاتي للحجم (القسم 3) موضوعية الشريحة — دون تصريح يدوي.
- الفحص: يشمل السعر كامل خط الأنابيب، Holoscope قبل/بعد، تحليل NOVA، التقرير.
- لا رسوم خفية. السعر المعروض بعد الاكتشاف الذاتي هو السعر النهائي.
- يُسلَّم التقرير 🤫 ا التشخيص عن راضيًا كان إذا إلا المستخدم يدفع لا .الدفع.

مقارنة استرشادية

يكلف عادةً بين 8 000 و15 000 يورو ويستنزف (L الشريحة) التدقيق اليدوي لشبكة من 200 جهاز أسبوعين. يسلّم خط أنابيب 0 DATA دون الضريبة 990 1 يورو مقابل ساعة من أقل في التشخيص.

7. الدفع

يُفعَّل الدفع 🐱😨 تُقترح طريقتان. تسليم التقرير:

7.1 SEPA (تحويل بنكي)

- **الرسوم:** 0 % 0 ـDATA، للعميل % 0و.
- **الأجل:** من 1 إلى 3 أيام عمل (معيار SEPA).
- **العملية:** ينفذ العميل التحويل. التحقق يدوي (نقطة ضعف مقبولة في خط الأنابيب الحالي). يتضمن التقرير RIB/IBAN.
- **الاستخدام الموصى به:** للشرائح L وXL وXXL، حيث تصبح رسوم البطاقة كبيرة.

7.2 البطاقة البنكية (Stripe)

- **الرسوم:** 1.5 % + 0.25 € لكل معاملة (معيار Stripe فرنسا).
- **الأجل:** فوري.

- **العملية:** يتضمن التقرير رابط دفع Stripe. تحقق فوري. الدفع بالبطاقة البنكية.
- **الاستخدام الموصى به:** S و M للشرائح، حيث تكون الأولوية للسرعة.

> **مبدأ الثقة:** يُسلَّم التقرير قبل الدفع، أيًا كانت الطريقة المختارة. تتحمل DATA مخاطرة عدم الدفع. هذا الاختيار بنيوي: إنه يوائم مصلحة العميل (ألا يدفع إلا مقابل تشخيص (إنتاج تشخيص مفيد) DATA مع مصلحة 0 مفيد).

8. حالة واقعية

في قطاع صناعة المعادن في (M الشريحة) في 15 يوليو 2026، نفذت شركة صناعية متوسطة من 87 مقعدًا نيو-أكيتين الأمر الواحد على جهازها الرئيسي (Linux Ubuntu 22.04، جهاز المسؤول المعلوماتي).

السير الزمني:

```
15:04:12  ←  curl -s https://odata.fr/scan | bash
15:04:18  ←  كشف نظام التشغيل : Linux 6.8.0-40-generic, x86_64
15:04:22  ←  اكتشاف النطاق : 192.168.1.0/24
15:04:31  ←  اكتمل فحص ARP : 87 (253/) مضيفًا يستجيبون
15:04:32  ←  التصنيف : الشريحة M · مؤكد · دون الضريبة € 990 : السعر
15:04:35  ←  تحميل NOVA (3.2 ميغابايت)
15:04:38  ←  بدء الفحص المعمق : 87 مضيفًا × 1 000 منفذ
15:19:44  ←  اكتمل الفحص : 87 مضيفًا، 312 خدمة
15:19:45  ←  Holoscope قبل متاح
15:19:50  ←  بدء تحليل NOVA
15:20:34  ←  اكتمل التحليل : 2 حرجة، 5 عالية، 4 متوسطة، 3 معلوماتية
15:20:36  ←  Holoscope بعد متاح
15:20:40  ←  سُلِّم التقرير (PDF، 22 صفحة) · رابط Stripe مضمّن
```



نتائج لافتة:

- **حرجة #1** — خادم NAS من QNAP يكشف واجهة إدارته على المنفذ 8080 دون مصادقة إلزامية. قابلة للاستغلال CVE-2022-27596 برنامج ثابت قديم (2022). ثغرة.
- **حرجة #2** — جهاز Windows 7 موصول بشبكة الإنتاج، يشارك غير مرقَّع (نهاية الدعم في يناير 2023) مجلدًا قابلًا للكتابة من كامل النطاق.
- **عالية** — طابعة شبكة Ricoh مع SNMP v1 مفعَّل (سلسلة المجتمع الافتراضية `public`)، تكشف التهيئة الكاملة وحسابات المستخدمين والمستندات في طابور الطباعة.
- **عالية** — مبدّل قابل للإدارة HP ProCurve مع واجهة Telnet مفعَّلة (المنفذ 23)، كلمة مرور ضعيفة.

المقياس	خط أنابيب 0 DATA	التدقيق اليدوي المقدّر
الزمن الإجمالي	**16 دقيقة و28 ثانية**	3 أيام
التكلفة	**990 € دون الضريبة**	~4 800 € دون الضريبة
المتطلبات المسبقة	لا شيء	موعد، تنقل، اعتمادات
التغطية	شاملة (87 مضيقًا)	جزئية (عينات)

> **استعارة طبية:** المريض (الشركة المتوسطة) يدخل العيادة، يمر تحت الماسح، يتلقى تشخيصه الكامل في 16 دقيقة، ويدفع عند الخروج. فقط إذا كان التشخيص مفيدًا. دون موعد مسبق، ودون قاعة انتظار.

9. المحاكاة الحيوية — الفحص كمبدأ مؤسِّس

لا يستلهم خط أنابيب 0 DATA العمليات الإدارية للتدقيق التقليدي. بل يستلهم الفعل الطبي للفحص.

المفهوم الطبي	المكافئ في 0 DATA
المريض	الشبكة المدقَّقة
قاعة الانتظار	غير موجودة — الأمر الواحد فوري
الفحص	الفحص (سلبي + نشط)
التصوير الطبي	Holoscope (ماسح ثلاثي الأبعاد للشبكة) قبل
التشخيص	تحليل NOVA (كشف الثغرات وتصنيفها)
التصوير الموسوم	Holoscope (ماسح مع الأمراض المحددة) بعد
الوصفة	تقرير PDF مع توصيات الإصلاح
الدفع	بعد التشخيص، مثل استشارة طبية

هذه المقاربة ليست تجميلية. بل بنيوية: سلسلة المعالجة مصممة لإعادة إنتاج تدفق الاستشارة الطبية — الملاحظة، التصوير، التشخيص، التوصية، الدفع. الهدف أن يفهم المسؤول المعلوماتي العملية في ثانية واحدة، لأنه سبق أن استشار طبيبًا.

ما يغيب عن خط الأنابيب لا يقل أهمية عما يحضر فيه:

- **لا زيارة ميدانية** — مثل الاستشارة عن بُعد، يتم التشخيص من مسافة.

- **لا استبيان مسبق** — لا يملأ المريض نموذجًا قبل الدخول؛ فالطبيب يلاحظ أولًا.
- **لا مدة تعاقدية** — تدوم الاستشارة ما يجب أن تدومه، لا ما ينص عليه عقد.
- **لا دفع مسبق** — لا يدفع المرء للطبيب قبل دخول عيادته.

المراجع

[1] TIKIJJA, Hadda. «0 مختبر DATA، يوليو 2026، 001 البحث. الانضباط».

[2] TIKIJJA, Hadda. «0 مختبر DATA، يوليو 2026، 003 البحث. الجهاز العصبي». Zenodo: 10.5281/zenodo.21342768.

[3] TIKIJJA, Hadda. «0 مختبر DATA، يوليو 2026، 004 البحث. الطُعم الرقمي». Zenodo: 10.5281/zenodo.21270325.

[4] TIKIJJA, Hadda. «0 مختبر DATA، يوليو 2026، 005 البحث. الجهاز المناعي».

[5] TIKIJJA, Hadda. «0 مختبر DATA، يوليو 2026، 010 البحث. الطُعم الأول».

[6] TIKIJJA, Hadda. «0 مختبر DATA، يوليو 2026، 011 البحث. تدقيق السطح».

[7] OWASP Foundation. «Web Security Testing Guide». v4.2، 2024.

شكر وتقدير. إلى الفرق التقنية التي تحافظ على خط الأنابيب في الإنتاج — الأمر الواحد لا يكذب لأن البنية التحتية التي خلفه لا تكذب. إلى مجموعة الـ 500 تهيئة شبكة التي خدمت المقارنة المعيارية لـ NOVA، والموَسَّمة تطوعًا من مدققين معتمدين. إلى الشركة المتوسطة في نيو-أكيتين، التي قبلت أن تُوثَّق حالتها.