CONCEPT

تحليل حزم الشبكة باستخدام Wireshark: التقاط الحركة وتأخير TCP وتشخيص الأعطال

10 – 14 مايو 2027

لندن - فندق أربع نجوم في وسط لندن



تحليل حزم الشبكة باستخدام Wireshark: التقاط الحركة وتأخير TCP وتشخيص الأعطال

المرجع: 18164_629 **التاريخ:** 10 – 14 مايو 2027 **المكان:** لندن - فندق أربع نجوم في وسط لندن **الرسوم:** SAR 25300

مقدمة:

يحسم تحليل حزم الشبكة الجدل الذي يعقب كل شكوى من بطء التطبيقات: هل التأخير في الشبكة أم في الخادم أم عند العميل؟ وحين تغيب أدلة التتبع تتبادل الفرق الاتهامات وتعيد تشغيل الأجهزة وتغلق بلاغات تعود للظهور بعد أيام. تدرب هذه الدورة من كور كونسبت المهندسين على اختيار نقاط الالتقاط الصحيحة وتصفية ملفات التتبع الكبيرة بمحلل الحزم مفتوح المصدر Wireshark، وقراءة تبادلات Ethernet وIP وTCP وDNS وDHCP وHTTP وTLS لتحديد المصدر الفعلي للتأخير. ويخرج المشاركون بتقرير تشخيص على مستوى الحزم لحادثة بطء تطبيق.

أهداف الدورة:

- اختيار نقطة الالتقاط وطريقته عبر المنفذ المعكوس أو موزع الشبكة أو الالتقاط على المضيف بما يسجل الحركة اللازمة للتحقيق دون فقد إطارات
- بناء مرشحات الالتقاط والعرض وقواعد التلوين والأعمدة المخصصة لتقليص ملف تتبع كبير إلى المحادثات المرتبطة بالبلاغ
- تفسير مصافحات TCP ونوافذ الاستقبال وإعادات الإرسال وزمن الذهاب والعودة للفصل بين تأخير الشبكة وتأخير الخادم والعميل
- تحليل تبادلات DNS وDHCP وHTTP ومصافحة TLS لتحديد أعطال تحليل الأسماء وتخصيص العناوين والطلب والاستجابة وإنشاء الجلسات
- إعداد خطوط أساس لحركة المرور بالرسوم البيانية للإدخال والإخراج وإحصاءات المحادثات لاكتشاف السلوك غير الطبيعي بسرعة
- كتابة تقرير تشخيص على مستوى الحزم يبين السبب الجذري وأدلة التتبع والإجراء التصحيحي لحادثة بطء تطبيق

الفئة المستهدفة:

- مهندسو تشغيل الشبكات الذين يحققون في انقطاع الاتصال وفقد الحزم وازدحام الوصلات في شبكات المباني ومراكز البيانات
- مهندسو الأنظمة والخوادم المطالبون بإثبات التأخير من جهة المضيف أو استبعاده عند بطء استجابة التطبيقات
- مهندسو مكاتب الخدمة والدعم المتقدم الذين يتولون بلاغات الأداء التي تعجز عنها الفرق الأخرى
- مهندسو دعم التطبيقات الذين يتتبعون تبادلات العميل والخادم أثناء الإصدارات والحوادث
- فرق مراقبة الشبكات التي تحدث خطوط أساس حركة المرور وتحقق في تنبيهات أدوات قياس الأداء

محاور الدورة:

اليوم 1: استراتيجية الالتقاط ونقاط الالتقاط وإدارة ملفات التتبع

- بنية محلل الحزم: مكتبة الالتقاط ووحدات تشريح البروتوكولات وأداة الالتقاط من سطر الأوامر
- اختيار نقطة الالتقاط: جهة العميل وجهة الخادم والنقاط الوسيطة
- المنافذ المعكوسة SPAN وRemote SPAN مقابل موزعات الشبكة السلبية ثنائية الاتجاه
- الوضع المختلط والمخازن الحلقية وطول الاقتطاع وفحص الحزم المفقودة
- إدارة ملفات التتبع: الدمج والتقطيع ومراجع الزمن وإخفاء البيانات قبل المشاركة

اليوم 2: المرشحات وتشريح Ethernet وIP وTCP وبيئة عمل المحلل

- صيغة مرشحات الالتقاط مقابل صيغة مرشحات العرض مع التعبيرات القائمة على الحقول
- قواعد التلوين والأعمدة المخصصة وملفات تهيئة المحلل
- تشريح إطار Ethernet II ووسم 802.1Q مع فحص طلبات ARP وردودها
- فحص ترويسة IPv4: زمن البقاء TTL وأعلام التجزئة وعلامات DSCP
- حقول ترويسة TCP والمصافحة الثلاثية وخيار تحجيم النافذة وفق RFC 7323

اليوم 3: مختبر أداء TCP وإعادات الإرسال وتحليل زمن الانتظار

- قياس زمن الذهاب والعودة وسلوك مهلة إعادة الإرسال وفق RFC 6298
- لوحة معلومات الخبير: الإقرارات المكررة وإعادات الإرسال السريعة والمقاطع خارج الترتيب
- اكتشاف الفقد بآلية RACK ومراحل التحكم في الازدحام وفق RFC 5681 وRFC 8985
- تحليل النافذة الصفرية وامتلاء النافذة والبايتات قيد النقل برسوم تدفق TCP
- أعمدة فرق الزمن للفصل بين زمن العبور في الشبكة وزمن معالجة الخادم وتأخير العميل

اليوم 4: بروتوكولات التطبيقات وقراءة مصافحة TLS وتشخيص بطء التطبيقات

- توقيت استعلامات DNS وردودها وعمليات البحث الفاشلة وأنماط إعادة المحاولة لدى المحلل
- تسلسل الاكتشاف والعرض والطلب والإقرار في DHCP وتتبعات فشل الإيجار
- توقيت طلبات HTTP واستجاباتها ورموز الحالة ومخططات تنزيل العناصر
- قراءة مصافحة TLS: رسالة Client Hello وServer Hello وتبادل الشهادات ورسائل التنبيه
- نظرة على الالتقاط اللاسلكي: وضع المراقبة واختيار القناة وإطارات إعادة المحاولة في 802.11

اليوم 5: مختبر خطوط الأساس وتقرير التشخيص على مستوى الحزم

- بناء خط الأساس بالرسوم البيانية للإدخال والإخراج: الإنتاجية ومعدل الحزم وزمن الاستجابة
- إحصاءات المحادثات ونقاط النهاية والتسلسل الهرمي للبروتوكولات لرصد الحالات الشاذة
- مختبر حالة: التقاط متعدد النقاط لحادثة بطء تطبيق أعمال
- سلسلة أدلة السبب الجذري: حزم مشروحة ورسوم بيانية وجداول توقيت
- عرض تقرير التشخيص على مستوى الحزم ومناقشته مع الزملاء

المهارات التي ستكتسبها:

- تخطيط نقاط الالتقاط
- بناء مرشحات العرض
- تشخيص تدفقات TCP
- إسناد زمن التأخير إلى مصدره
- تفسير تبادلات البروتوكولات
- إعداد خطوط أساس حركة المرور
- توثيق أدلة التتبع
- فحص الإطارات اللاسلكية

لماذا تحضر هذه الدورة:

- العودة بتقرير تشخيص على مستوى الحزم مبني على التقاط متعدد النقاط لحالة بطء تطبيق
- إنهاء تبادل الاتهامات بين فرق الشبكات والخوادم والتطبيقات بعرض أدلة توقيت مأخوذة من السلك مباشرة
- العمل على ملفات تتبع حقيقية في المختبر كل يوم بدلا من مشاهدة عروض توضيحية
- تبادل أساليب الالتقاط مع مهندسين يديرون شبكات في المكاتب والمستشفيات والمصانع ومراكز الاستضافة

الخاتمة:

تحل مشكلات بطء التطبيقات والأعطال المتقطعة أسرع حين يستطيع المهندس أن يبين بدقة أين يضيع الوقت داخل المحادثة. تنتقل الدورة من نقاط الالتقاط وإدارة ملفات التتبع إلى المرشحات وتشريح Ethernet وIP وTCP، ثم إلى تحليل إعادات الإرسال وزمن الانتظار، فتتبع DNS وDHCP وHTTP وقراءة مصافحة TLS والالتقاط اللاسلكي. ويبني اليوم الأخير خطوط أساس لحركة المرور ويطبقها في مختبر حالة متعدد النقاط، ليخرج بتقرير تشخيص على مستوى الحزم جاهز للمشاركة مع مالكي التطبيقات.