



## دورة التحقيق في حركة الشبكة باستخدامreshark



## دورة التحقيق في حركة الشبكة باستخدام Wireshark

المرجع: 158751\_772 التاريخ: 29 أغسطس - 2 سبتمبر 2027 المكان: مسقط الرسوم: Euro 5700

### نظرة عامة

دورة التحقيق في حركة الشبكة باستخدام Wireshark دورة متوسطة لمدة 5 أيام لمحلي الشبكات ومحققى مراكز العمليات ومستجيبى الحوادث ومهندسي البنية التحتية وفرق العمليات السيبرانية، ويعود المشاركون منها بدفتر تحقيق لحركة الشبكة. يمارس المشاركون تخطيط التقاط الحزم وتحليل مرشحات Wireshark وتحليل محادثات TCP ومراجعة بيانات البروتوكولات وفرز الحركة المشبوهة وإعادة بناء الخط الزمني للحدث. وتميز الدورة أدلة الحزم عن أمن الشبكات العام. تطور أجائل للتدريب قدرات التحقيق في حركة الشبكة.

### الفئة المستهدفة

- وظائف تحليل الشبكات المسؤولة عن تفسير سلوك الحزم وأداء الخدمات
- وظائف العمليات الأمنية المسؤولة عن فرز نشاط الشبكة المشبوه
- وظائف الاستجابة للحوادث المسؤولة عن إعادة بناء أدلة الشبكة
- وظائف هندسة البنية التحتية المسؤولة عن تشخيص أعراض البروتوكولات والاتصال
- وظائف العمليات السيبرانية المسؤولة عن توثيق نتائج حركة الشبكة

تفترض الدورة أن المشاركين يستطيعون تفسير عنوانة TCP/IP والمنافذ والبروتوكولات الشائعة ومخططات الشبكات، وتستبعد الاستغلال الهجومي والهندسة العكسية للبرمجيات الخبيثة واختراق الشبكات اللاسلكية ومعمارية الأمن العامة.

### الإدارات والقطاعات المستهدفة

تدعم الدورة الإدارات والقطاعات التي تشغل الخدمات الشبكية أو تراقبها أو تحقق فيها.

- عمليات الشبكات والأمن في القطاع المصرفي
- ضمان خدمات الاتصالات
- مراقبة البنية التحتية للطاقة والمرافق
- عمليات تقنية الرعاية الصحية
- خدمات الشبكات والأمن المدارة



## أهداف التعلم

بنهاية هذه الدورة، سيتمكن المشاركون من:

- تطبيق تخطيط لالتقاط الحزم قائم على الأدلة
- استخدام مرشحات الالتقاط والعرض بدقة
- تحليل البروتوكولات والمحددات وسلوك TCP
- تشخيص أعراض الأداء من أدلة الحزم
- ترتيب الحركة المشبوهة وإعادة بناء الخطوط الزمنية
- بناء دفتر تحقيق لحركة الشبكة

## جدول الدورة

### اليوم 1: تخطيط أدلة الحزم وحفظها

- خريطة اختيار نقاط مراقبة الشبكة
- خطة نطاق الالتقاط الحزم والأدلة
- إعداد واجهات الالتقاط في Wireshark
- أسلوب تصميم مرشحات الالتقاط والتحقق منها
- سجل سلامة ملفات PCAP وملاحظات القضية

### اليوم 2: التنقل في الحركة وترشيحها

- سير قوائم الحزم والتفاصيل والبايتات في Wireshark
- منشئ حقول مرشحات العرض ومعاملاتها
- مصفوفة إحصاءات نقاط النهاية والمحددات
- مراجعة تسلسل البروتوكولات وتوزيع الحركة
- أسلوب المراجع الزمنية ومحاذاة ملفات الالتقاط



### اليوم 3: تحليل سلوك البروتوكولات

- مخطط مصافحة TCP وحالة الجلسة
- جدول أدلة إعادة إرسال TCP وفقد الحزم
- ورقة تحليل استعلامات DNS واستجاباتها
- خريطة معاملات HTTP وبيانات الكائنات
- مراجعة مصافحة TLS وبيانات الشهادات

### اليوم 4: التحقيق في الشذوذ والحوادث

- أسلوب فرز معلومات الخبراء في Wireshark
- إعادة بناء المحادثة بأداة Follow Stream
- مصفوفة أنماط الاتصال المشبوه
- ورقة الخط الزمني لحادث الشبكة
- سجل الثقة في النتائج والتفسيرات البديلة

### اليوم 5: ممارسة التحقيق في حركة الشبكة

- تمرين: التحقق من نطاق التقاط الحزم
- تمرين: بناء مرشحات لسؤال شبكي
- تمرين: تشخيص أعراض TCP والبروتوكولات
- تمرين: إعادة بناء نشاط حركة مشبوهة
- المشروع الختامي: دفتر تحقيق لحركة الشبكة

### التمارين التطبيقية

تستخدم الدورة أنشطة مقترحة من شبكات المصارف والاتصالات والطاقة والرعاية الصحية والخدمات المدنية.

- نشاط مقترح: اختيار نقاط المراقبة وتحديد نطاق الالتقاط وحفظ سجل أدلة PCAP.
- نشاط مقترح: بناء مرشحات التقاط وعرض تجيب عن أسئلة تشغيلية محددة.
- نشاط مقترح: ربط بيانات TCP وDNS وHTTP وTLS بفرضية أداء أو أمن.
- نشاط مقترح: جمع المحادثات والخطوط الزمنية وأحكام الثقة والنتائج في دفتر تحقيق.



## الأسئلة الشائعة

### لمن تناسب دورة التحقيق في حركة الشبكة باستخدام Wireshark، وماذا تفترض؟

تناسب وظائف الشبكات والعمليات الأمنية والاستجابة للحوادث والبنية التحتية والعمليات السيبرانية، وتفترض الإلمام بعنوانات TCP/IP والمنافذ والبروتوكولات الشائعة ومخططات الشبكات.

### كيف يختلف التحقيق في حركة الشبكة باستخدام Wireshark عن تدريب أمن الشبكات العام؟

يركز التحقيق باستخدام Wireshark على أدلة الحزم والمحددات وسلوك البروتوكولات والخطوط الزمنية والنتائج، بينما يغطي أمن الشبكات العام المعمارية والضوابط والإدارة والسياسات.

### ما الفرق بين مرشحات الالتقاط ومرشحات العرض في Wireshark؟

تحدد مرشحات الالتقاط الحزم التي يجري جمعها، بينما تختار مرشحات العرض الحزم الظاهرة من ملف التقاط قائم دون حذف بقية الحزم الملتقطة.

### كيف يساعد Wireshark في تشخيص أعراض أداء TCP؟

يساعد Wireshark المحللين على فحص المصافحة وتسلسل الحزم والإقرارات وإعادة الإرسال ومؤشرات الفقد والتوقيت وسلوك النوافذ وإحصاءات المحادثات ضمن سياق الشبكة.

### كيف يوثق المحللون نتائج حركة الشبكة المشبوهة؟

يوثق المحللون نطاق الالتقاط والتوقيعات والمرشحات ونقاط النهاية والمحددات وأدلة البروتوكولات والتفسيرات البديلة والثقة والقيود والإجراءات اللازمة للتأكيد أو التصعيد.

## الخاتمة

يعود المشاركون بدفتر تحقيق لحركة الشبكة يربط قرارات الالتقاط والمرشحات وأدلة البروتوكولات والمحددات والخطوط الزمنية وأعراض الأداء والنشاط المشبوه والنتائج المدعومة. يحول الدفتر الحزم المنفصلة إلى سير تحقيق قابل للتتبع. ويدعم التحليل المنسق بين وظائف الشبكات والبنية التحتية والعمليات الأمنية والاستجابة للحوادث.