CONCEPT

التحليل الجنائي للذاكرة وتحليل البرمجيات الخبيثة: 3

Volatility وقواعد YARA والخط الزمني لأنظمة Windows

التحليل الجنائي للذاكرة وتحليل البرمجيات الخبيثة: Volatility 3 وقواعد YARA والخط الزمني لأنظمة Windows

مقدمة:

يحدد التحليل الجنائي للذاكرة وتحليل البرمجيات الخبيثة ما إذا كان نطاق الاختراق قد حدد بدقة أم عولج جزئيا فقط. فكثير من فرق الاستجابة تعيد تثبيت الجهاز قبل التقاط الذاكرة العشوائية، وتغفل الشيفرات المحقونة التي لم تكتب على القرص، وتسلم مركز العمليات الأمنية قيم تجزئة عامة بدلا من قواعد كشف تصمد أمام إعادة تجميع العينة. تمنح هذه الدورة من كور كونسبت الفاحصين روتينا مخبريا قابلا للتكرار: جمع البيانات المتطايرة، وتحليل صور الذاكرة بإطار Volatility 3، وإعادة بناء الخط الزمني لأنظمة Windows، وفرز الملفات التنفيذية المشبوهة بأمان داخل بيئة معزولة. ويعد المشاركون تقرير فحص الجهاز المخترق وحزمة تسليم قواعد الكشف.

أهداف الدورة:

- جمع الذاكرة العشوائية وغيرها من البيانات المتطايرة من جهاز Windows يعمل وفق ترتيب التطاير مع تسجيل قيم التجزئة وملاحظات الفاحص
- تحليل صور الذاكرة بإضافات Volatility 3 لكشف العمليات الدخيلة والشيفرات المحقونة واتصالات الشبكة وآليات البقاء
- إعادة بناء نشاط المهاجم من السجل وسجلات الأحداث وملفات Prefetch وآثار نظام الملفات في خط زمني موحد
- فرز الملفات التنفيذية المشبوهة من خصائصها الثابتة وسلوكها داخل بيئة معزولة دون تشغيل أي عينة على أنظمة الإنتاج
- تحويل نتائج الفحص إلى مؤشرات اختراق وقواعد YARA يستطيع مركز العمليات الأمنية نشرها واختبارها
- كتابة تقرير فحص يبين النتائج ودرجة الثقة وحدود التحليل للقارئ التقني والإداري

الفئة المستهدفة:

- فرق الاستجابة للحوادث التي تعزل الأجهزة المخترقة وتقرر ما يجب جمعه قبل المعالجة
- محللو مستوى التصعيد في مراكز العمليات الأمنية الذين يحققون في تنبيهات تشير إلى اختراق يدوي مباشر
- الفاحصون الجنائيون الذين يعالجون صور الأجهزة ولقطات الذاكرة في القضايا الداخلية
- مهندسو الكشف الذين يحولون نتائج الفحص إلى قواعد كشف للأجهزة الطرفية والشبكة
- محللو استخبارات التهديدات الذين يثرون المؤشرات المستخرجة من العينات ويتشاركونها مع فرق الدفاع

محاور الدورة:

اليوم 1: مسار التحليل الجنائي والاستجابة للحوادث وسلامة الأدلة وتجهيز المختبر

- مراحل NIST SP 800-86 دليل دمج التقنيات الجنائية في الاستجابة للحوادث: الجمع والفحص والتحليل وإعداد التقارير
- ترتيب التطاير وقائمة قرارات المستجيب الأول
- تجزئة الأدلة وملاحظات الفاحص وسجل الحيازة للقطات الأجهزة
- بناء مختبر تحليل معزول: اللقطات الافتراضية والشبكة المقصورة على المضيف وقواعد التعامل مع العينات
- مراجعة جاهزية فحص الأجهزة المخترقة: القياس عن بعد وفترات الاحتفاظ وفجوات أدوات الجمع

اليوم 2: جمع البيانات المتطايرة وتحليل الذاكرة بإطار Volatility 3

- التقاط الذاكرة الحية وملفات الإسبات وملفات تفريغ الأعطال بوصفها مصادر للذاكرة
- جداول الرموز في Volatility 3 وبنية الإضافات والتحقق من صورة الذاكرة
- مطابقة قوائم العمليات: الفروق بين مخرجات pslist psscang pstreeg
- مراجعة مقابس الشبكة وأسطر الأوامر والمكتبات المحملة في الذاكرة
- كشف حقن الشيفرات والعمليات المجوفة بالإضافة malfind

اليوم 3: آثار أنظمة Windows وتحليل الخط الزمني الموحد

- ملفات السجل: مفاتيح التشغيل التلقائي والخدمات وأدلة Amcacheg ShimCache
- قنوات سجلات أحداث Windows لتسجيل الدخول وإنشاء العمليات وتثبيت الخدمات
- ملفات Prefetch والاختصارات LNK وقوائم الانتقال دليلا على التنفيذ
- جدول الملفات الرئيسي في NTFS وسجل USN وفحص التلاعب بالطوابع الزمنية
- بناء الخط الزمني الموحد بأداتي log2timeline Plasog وتقنيات التصفية

اليوم 4: فرز البرمجيات الخبيثة لفرق الدفاع ومحتوى الكشف

- مراجعة الخصائص الثابتة: ترويسات PE والدوال المستوردة والسلاسل النصية والإنتروبيا وعلامات الضغط
- مراقبة السلوك في البيئة المعزولة: شجرة العمليات ونشاط الملفات والسجل والشبكة
- مؤشرات مقاومة التحليل والتهرب من البيئة المعزولة وطريقة توثيقها
- استخراج مؤشرات الاختراق وتقييم جودتها وتحديد موقعها على هرم المؤشرات
- كتابة قواعد YARA واختبار الإنذارات الكاذبة والتوافق مع YARA-X

اليوم 5: حالة الفحص المخبري وحزمة تسليم قواعد الكشف

- نظرة عامة على التحليل الجنائي للأجهزة المحمولة: أنواع الاستحواذ والنسخ الاحتياطية وحدود بيانات التطبيقات
- حالة مخبرية: جهاز سرقت منه بيانات الاعتماد مع محمل مقيم في الذاكرة
- حالة مخبرية: تعقب آليات البقاء في السجل والخدمات والمهام المجدولة
- صياغة تقرير فحص الجهاز المخترق مع عبارات درجة الثقة
- مراجعة حزمة تسليم قواعد الكشف: المؤشرات وقواعد YARA واستعلامات التعقب لمركز العمليات الأمنية

المهارات التي ستكتسبها:

- جمع البيانات المتطايرة
- تحليل صور الذاكرة
- تفسير آثار أنظمة Windows
- إعادة بناء الخط الزمني
- الفرز الثابت للبرمجيات الخبيثة
- تحليل السلوك في البيئة المعزولة
- كتابة قواعد الكشف
- كتابة التقارير الجنائية الرقمية

لماذا تحضر هذه الدورة:

- العودة بتقرير فحص الجهاز المخترق وحزمة تسليم قواعد الكشف مبنيين على حالة مخبرية كاملة
- قضاء معظم وقت كل يوم في العمل المباشر على صور الذاكرة وآثار الأقراص والعينات المخبرية بدلا من العروض النظرية
- كشف الشيفرات المحقونة وآليات البقاء التي يغفلها فحص القرص وحده وبرامج مكافحة الفيروسات
- مقارنة ممارسات الفحص مع مستجيبين وفاحصين من قطاعات المالية والطاقة والاتصالات والخدمات العامة

الخاتمة:

لا يغلق ملف الاختراق إلا حين يعرف الفريق ما الذي تم تشغيله وكيف بقي وكيف يكتشف في المرة القادمة. تنتقل الدورة من مسار NIST SP 800-86 وسلامة الأدلة، إلى جمع الذاكرة العشوائية وتحليلها بإطار Volatility 3، ثم إلى آثار أنظمة Windows والخط الزمني الموحد، ففرز البرمجيات الخبيثة من منظور دفاعي وكتابة قواعد YARA. ويطبق اليوم الأخير هذا الروتين على حالات مخبرية تنتهي بتقرير فحص الجهاز المخترق وحزمة تسليم قواعد الكشف جاهزين لمركز العمليات الأمنية.