دورة التحقيق الجنائي في الذاكرة المتطايرة والبرمجيات الخبيثة

12 – 16 أبريل 2027

أديس أبابا

AGILE LEADERS
Training Center

دورة التحقيق الجنائي في الذاكرة المتطايرة والبرمجيات الخبيثة

المرجع: 223988_770 **التاريخ:** 12 – 16 أبريل 2027 **المكان:** أديس أبابا **الرسوم:** Euro 4500

نظرة عامة

دورة التحقيق الجنائي في الذاكرة المتطايرة والبرمجيات الخبيثة دورة متوسطة لمدة أسبوع لمحللي الأدلة الرقمية ومستجيبي الحوادث ومحللي البرمجيات الخبيثة ومحققي مراكز العمليات وفرق الجرائم السيبرانية، ويعود المشاركون منها بملف قضية للتحليل الجنائي للذاكرة. يمارس المشاركون جمع الذاكرة الآمن للأدلة وتحليل الذاكرة المتطايرة وفرز البرمجيات الخبيثة وكشف حقن العمليات وربط الخط الزمني للهجوم. وتستبعد الدورة تحليل الأقراص والهندسة العكسية العامة. تطور أجايل للتدريب قدرات التحقيق في أدلة الذاكرة.

الفئة المستهدفة

- وظائف الأدلة الرقمية المسؤولة عن جمع آثار النظام المتطايرة وفحصها
- وظائف الاستجابة للحوادث المسؤولة عن التحقيق في الأجهزة المخترقة
- وظائف تحليل البرمجيات الخبيثة المسؤولة عن فرز سلوك التشغيل المشبوه
- وظائف العمليات الأمنية المسؤولة عن تصعيد تنبيهات الأجهزة والشبكات
- وظائف التحقيق في الجرائم السيبرانية المسؤولة عن توثيق الأدلة التقنية

تفترض الدورة أن المشاركين يستطيعون التعامل مع أنظمة Windows وتفسير آثار العمليات والشبكات والأمن الأساسية، وتستبعد تصوير الأقراص وتفكيك الشيفرة وتطوير الاستغلال وإدارة قيادة الحوادث المؤسسية.

الإدارات والقطاعات المستهدفة

تدعم الدورة الإدارات والقطاعات التي تحقق في اختراق الأجهزة ونشاط البرمجيات الخبيثة.

- العمليات الأمنية والتحقيق في الاحتيال بالقطاع المصرفي
- الدفاع السيبراني في الطاقة والمرافق
- الاستجابة للحوادث في الاتصالات
- التحقيق الرقمي في الجهات العامة
- خدمات الأمن المدارة والأدلة الرقمية

AGILE LEADERS
Training Center

أهداف التعلم

بنهاية هذه الدورة، سيتمكن المشاركون من:

- تطبيق أساليب آمنة للأدلة عند جمع الذاكرة المتطايرة
- تحليل العمليات والوحدات والمقابض وآثار التنفيذ
- تشخيص حقن الشيفرة والجذور الخفية وآثار سرقة بيانات الاعتماد
- ربط أدلة الشبكة والاستمرارية والخط الزمني
- ترتيب الآثار المشبوهة لفرز البرمجيات الخبيثة في الذاكرة
- بناء ملف قضية قابل للدفاع للتحليل الجنائي للذاكرة

جدول الدورة

اليوم 1: جمع الأدلة المتطايرة وحفظها

- خريطة مصادر الأدلة المتطايرة وأولوياتها
- أسلوب الجمع الحي الأقل تدخلا
- مصفوفة اختيار أداة التقاط الذاكرة
- سجل ملاحظات الجمع والتحقق من قيمة التجزئة
- قائمة سلامة صورة الذاكرة والتعامل معها

اليوم 2: تأسيس خط أساس حالة التشغيل

- سير تعريف صورة الذاكرة باستخدام Volatility 3
- خريطة شجرة العمليات وعلاقات الأصل والفرع
- جرد الوحدات المحملة والمكتبات الديناميكية
- أسلوب تحليل المقابض المفتوحة وكائنات النظام
- مراجعة سجل الأوامر وآثار وحدة التحكم

AGILE LEADERS
Training Center

اليوم 3: كشف البرمجيات الخبيثة في الذاكرة

- مصفوفة مؤشرات حقن العمليات
- أسلوب فرز مناطق الذاكرة القابلة للتنفيذ
- قائمة كشف الجذور الخفية وخطافات النواة
- فحص آثار سرقة بيانات الاعتماد
- سجل أدلة البرمجيات الخبيثة المقيمة في الذاكرة

اليوم 4: ربط النشاط وبناء النتائج

- خريطة آثار المقابس واتصالات الشبكة
- ورقة ربط مؤشرات الاستمرارية
- أسلوب ربط مراجع السجل والملفات
- جدول إعادة بناء الخط الزمني للهجوم
- مصفوفة الثقة في النتائج والتفسيرات البديلة

اليوم 5: ممارسة التحقيق في الذاكرة

- تمرين: التحقق من صورة ذاكرة ملتقطة
- تمرين: تتبع سلسلة عمليات مشبوهة
- تمرين: تشخيص أدلة الحقن وسرقة بيانات الاعتماد
- تمرين: ربط آثار الشبكة والاستمرارية والخط الزمني
- المشروع الختامي: ملف قضية للتحليل الجنائي للذاكرة

التمارين التطبيقية

تستخدم الدورة أنشطة مقترحة من تحقيقات الأجهزة في المصارف والطاقة والاتصالات والجهات العامة.

- نشاط مقترح: توثيق التقاط ذاكرة حية والتحقق من صورة الدليل الناتجة.
- نشاط مقترح: التمييز بين علاقات التشغيل المعتادة وسلوك العمليات والوحدات المشبوه.
- نشاط مقترح: ربط حقن الشيفرة واتصالات الشبكة ومؤشرات الاستمرارية وآثار بيانات الاعتماد بفرضية تحقيق.
- نشاط مقترح: جمع الآثار والخطوط الزمنية وأحكام الثقة وملاحظات التقرير في ملف قضية.

AGILE LEADERS
Training Center

الأسئلة الشائعة

لمن تناسب دورة التحقيق الجنائي في الذاكرة والبرمجيات الخبيثة، وماذا تفترض؟

تناسب وظائف الأدلة الرقمية والاستجابة للحوادث وتحليل البرمجيات الخبيثة والعمليات الأمنية والتحقيق السيبراني، وتفترض خبرة عملية بأنظمة Windows والآثار الأمنية الشائعة.

كيف يختلف التحليل الجنائي للذاكرة المتطايرة عن التحليل الجنائي الرقمي العام؟

يفحص التحليل الجنائي للذاكرة حالة التشغيل الحية الملتقطة، بينما يمتد التحليل الجنائي الرقمي العام إلى مصادر أوسع مثل وسائط التخزين والأجهزة المحمولة والسجلات السحابية وبيانات التطبيقات.

لماذا يعد جمع الذاكرة الآمن للأدلة مهما في تحقيقات البرمجيات الخبيثة؟

يعد الجمع الآمن مهما لأن التقاط الذاكرة الحية يغير حالة النظام، ولذلك يقلل المحققون الأثر ويوثقون الإجراءات ويحافظون على سلامة الدليل ويشرحون التغييرات الناتجة.

ماذا يكشف تحليل حقن العمليات في الذاكرة المتطايرة؟

يكشف تحليل حقن العمليات مناطق قابلة للتنفيذ وعلاقات عمليات غير معتادة ووحدات مشبوهة وتغييرات في حماية الذاكرة وسلوكا قد لا يبقى ظاهرا على القرص.

كيف يقوي ربط الخط الزمني للهجوم نتائج تحليل ذاكرة البرمجيات الخبيثة؟

يقوي الربط النتائج عبر وصل العمليات ونشاط الشبكة ومؤشرات الاستمرارية والأوامر وآثار بيانات الاعتماد في تسلسل يدعم فرضية التحقيق أو يناقضها.

الخاتمة

يعود المشاركون بملف قضية للتحليل الجنائي للذاكرة يضم سجلات الجمع وآثار التشغيل وقرارات الفرز وأدلة الخط الزمني والنتائج المدعومة. يحول الملف ملاحظات الذاكرة المنفصلة إلى سير تحقيق قابل للتتبع. ويدعم المراجعة التقنية وقرارات الحوادث والتقارير القابلة للدفاع بين فرق الأدلة الرقمية والعمليات الأمنية.