CONCEPT

اختبار الاختراق والاختراق الأخلاقي: تحديد النطاق ومنهجيات الاختبار وكتابة التقارير

12 – 16 يوليو 2027

دبي - فندق خمس نجوم في وسط الأعمال

اختبار الاختراق والاختراق الأخلاقي: تحديد النطاق ومنهجيات الاختبار وكتابة التقارير

المرجع: 380_13381 **التاريخ:** 12 – 16 يوليو 2027 **المكان:** دبي - فندق خمس نجوم في وسط الأعمال **الرسوم:** SAR 19500

مقدمة:

يفقد اختبار الاختراق والاختراق الأخلاقي المصرح به قيمته في كثير من الأحيان قبل إرسال أول طلب فحص: نطاق يغفل أصولا حرجة، وتفويض مكتوب غامض، وقواعد اشتباك لا تراعي مخاطر بيئة الإنتاج، وتقارير تنقل مخرجات الماسحات دون تقييم للخطورة من منظور الأعمال ودون خطة لإعادة الاختبار. تعد هذه الدورة من كور كونسبت مهندسي الأمن وفرق الدفاع ومدققي تقنية المعلومات لتنفيذ اختبارات الاختراق المصرح بها وتكليف جهات تنفيذها وفق PTES ودليل OWASP لاختبار أمن الويب و800-115 SP NIST، ضمن مختبر معزول. ويبني المشاركون حزمة مهمة اختبار الاختراق التي تضم التفويض والنطاق وخطة الاختبار والتقرير المقيم وفق CVSS وسجل إعادة الاختبار.

أهداف الدورة:

- إعداد التفويض المكتوب وحدود النطاق وقواعد الاشتباك بما يحمي الجهة المختبرة وفريق الاختبار معا
- تخطيط مهمة الاختبار وفق مراحل PTES ومراحل التخطيط والاكتشاف والهجوم وإعداد التقارير في 800-115 NIST SP، مع اختيار تغطية الصندوق الأسود أو الرمادي أو الأبيض
- تنفيذ جمع المعلومات وتحليل الثغرات وحالات اختبار تطبيقات الويب من دليل OWASP لاختبار أمن الويب داخل مختبر مضبوط
- تقييم تعرض الشبكات وخدمات الدليل وتصعيد الصلاحيات على مستوى المفاهيم، وتوثيق الأدلة بمعيار يمكن الدفاع عنه
- تقييم خطورة النتائج باستخدام CVSS v4.0 وكتابة تقرير اختبار اختراق تنفيذي وفني مع توصيات المعالجة
- إدارة موردي اختبار الاختراق الخارجيين، والتحقق من المعالجة بإعادة الاختبار، وإغلاق النتائج في سجل متابعة

الفئة المستهدفة:

- مهندسو الأمن الذين ينفذون تقييمات الثغرات الداخلية واختبارات الاختراق المصرح بها
- موظفو فرق الدفاع ومراكز العمليات الأمنية الذين يتحققون من قدرات الرصد والاستجابة أمام نشاط مهاجم محاكى
- مدققو تقنية المعلومات الذين يراجعون نطاق اختبار الاختراق وأدلته ونتائجه ضمن أعمال التوكيد
- مديرو الأمن الذين يكلفون موردي الاختبار الخارجيين ويملكون سجل النتائج
- مالكو البنية التحتية والتطبيقات الذين يعتمدون نوافذ الاختبار ويعالجون نقاط الضعف المبلغ عنها

محاور الدورة:

اليوم 1: أسس الاختبار المصرح به والحدود القانونية وتحديد نطاق المهمة

- الفرق بين اختبار الاختراق وفحص الثغرات وتمرين الفريق الأحمر: الغرض والعمق
- خطاب التفويض المكتوب والحدود القانونية ومدونة سلوك المختبر
- مرحلة التفاعلات السابقة للمهمة في PTES: استبيان النطاق وحصر الأصول والاستثناءات
- قواعد الاشتباك: نوافذ الاختبار وضمانات بيئة الإنتاج وشروط الإيقاف وجهات التصعيد
- اختيار تغطية الصندوق الأسود والرمادي والأبيض ومراجعة نضج الاختبار في الوضع الحالي

اليوم 2: منهجيات الاختبار وخطة اختبار المهمة

- أقسام PTES السبعة من جمع المعلومات الاستخبارية إلى ما بعد الاستغلال
- مراحل التخطيط والاكتشاف والهجوم وإعداد التقارير في NIST SP 800-115
- فئات دليل OWASP لاختبار أمن الويب WSTG ومعرفات حالات الاختبار
- مقاييس الأمن التشغيلي في OSSTMM بوصفها منهجية مقارنة
- بناء خطة اختبار المهمة: ربط المنهجية وحالات الاختبار ومصفوفة التتبع

اليوم 3: جمع المعلومات وتحليل الثغرات وحالات اختبار تطبيقات الويب

- جمع المعلومات السلبي والنشط: البصمة العامة وسجلات DNS وحصر الخدمات باستخدام Nmap
- سير عمل تحليل الثغرات: التحقق من مخرجات الماسحات واستبعاد الإيجابيات الكاذبة
- مختبر: حالات اختبار WSTG للمصادقة والتفويض وإدارة الجلسات على تطبيق تدريبي
- مختبر: حالات اختبار WSTG للتحقق من المدخلات ومنطق الأعمال وواجهات API على تطبيق تدريبي
- معايير توثيق الأدلة: لقطات شاشة مؤرخة وسجلات الطلبات ويومية نشاط المختبر

اليوم 4: مفاهيم اختبار الشبكات وخدمات الدليل وتصعيد الصلاحيات والأدلة وتقييم الخطورة

- اختبار تجزئة الشبكة الداخلية ومراجعة خدمات الإدارة المكشوفة
- مسارات الهجوم على خدمات الدليل: التفويض الضعيف والحسابات الخاملة وصلاحيات المجموعات المفرطة
- فئات تصعيد الصلاحيات على أجهزة Windows وLinux وأسبابها الجذرية في الإعدادات
- التعامل مع الأدلة وتقليل البيانات والإتلاف الآمن لمخرجات الاختبار
- تطبيق مقاييس Base Threatg وSupplementalg في CVSS v4.0 على نتائج الاختبار

اليوم 5: إعداد التقارير والإشراف على الموردين وإعادة الاختبار وحزمة المهمة

- هيكل تقرير اختبار الاختراق: الملخص التنفيذي وسرد مسار الهجوم والنتائج الفنية
- مختبر: كتابة النتائج بدرجات CVSS-BTE وتوصيات المعالجة
- اختيار مورد الاختبار الخارجي: اعتماد CREST وكفاءة المختبرين ومراجعة بيان العمل
- خطة إعادة الاختبار للتحقق من المعالجة ومعايير إغلاق سجل النتائج
- تجميع حزمة مهمة اختبار الاختراق ومراجعتها بالنقد المتبادل بين الأقران

المهارات التي ستكتسبها:

- تحديد نطاق المهمة
- صياغة قواعد الاشتباك
- تنفيذ حالات اختبار تطبيقات الويب
- استطلاع سطح الهجوم
- التحقق من الثغرات
- إدارة أدلة الاختبار
- تقدير خطورة النتائج وفق CVSS
- الإشراف على موردي الاختبار

لماذا تحضر هذه الدورة:

- العودة بحزمة مهمة اختبار الاختراق التي تضم خطاب التفويض والنطاق وقواعد الاشتباك وخطة الاختبار والتقرير المقيم وفق CVSS وسجل إعادة الاختبار
- تنفيذ حالات اختبار WSTG عمليا على تطبيق تدريبي في مختبر معزول بدلا من القراءة عن فئات الهجمات
- مساءلة عروض الموردين وتقاريرهم بفهم واضح لما يجب أن يغطيه الاختبار الموثوق وما يقدمه من أدلة
- مقارنة ممارسات الاختبار والتوكيد مع مهندسي أمن وموظفي مراكز عمليات ومدققين من قطاعات المصارف والطاقة والخدمات الحكومية والتقنية

الخاتمة:

لا تتجاوز فائدة اختبار الاختراق المصرح به جودة نطاقه وأدلته ومتابعته. ينتقل الأسبوع من التفويض القانوني وتحديد النطاق وقواعد الاشتباك، إلى منهجيات PTES وNIST SP 800-115 ودليل OWASP لاختبار أمن الويب، ثم إلى جمع المعلومات والتحقق من الثغرات وحالات اختبار تطبيقات الويب في المختبر. ويتناول بعد ذلك مفاهيم الشبكات وخدمات الدليل وتصعيد الصلاحيات والتعامل مع الأدلة وتقييم الخطورة وفق CVSS v4.0، ويختتم بكتابة التقارير والإشراف على الموردين وإعادة الاختبار وحزمة مهمة اختبار الاختراق لكل مشارك.