CONCEPT

دورة أمن الشبكات: جدران الحماية والشبكات الافتراضية الخاصة VPN وأنظمة كشف التسلل ومنعه IDS/IPS والتحكم في الوصول NAC

10 – 21 مايو 2027

دبي - فندق خمس نجوم في وسط الأعمال



دورة أمن الشبكات: جدران الحماية والشبكات الافتراضية الخاصة VPN وأنظمة كشف التسلل ومنعه IDS/IPS والتحكم في الوصول NAC

المرجع: 23805_1438 **التاريخ:** 10 – 21 مايو 2027 **المكان:** دبي - فندق خمس نجوم في وسط الأعمال **الرسوم:** SAR 38610

مقدمة:

دورة أمن الشبكات في جدران الحماية والشبكات الافتراضية الخاصة VPN وأنظمة كشف التسلل ومنعه IDS/IPS والتحكم في الوصول NAC دورة عملية مدتها أسبوعين لمهندسي الشبكات ومهندسي الأمن ومسؤولي جدران الحماية، تنتهي بحزمة تصميم وتدقيق لشبكة مقسمة إلى مناطق أمنية. تعمل مؤسسات كثيرة بشبكات مسطحة وقواعد جدران حماية قديمة مليئة بالاستثناءات المفتوحة وحساسات غير مضبوطة، فيتنقل المهاجم بحرية بعد تجاوز المحيط دون أن يرصده أحد. يهيئ المرشحون الموجهات والمبدلات أو جدران الحماية في عملهم اليومي، وتقدم الأيام كلها في صورة مختبر تطبيقي على أدوات مفتوحة المصدر لا ترتبط بمورد معين. وتقدم كور كونسبت هذه الدورة في أمن الشبكات.

أهداف الدورة:

- رسم مسارات الهجوم على الشبكة وتصميم المناطق الأمنية وموقع المنطقة منزوعة السلاح DMZ وسياسات التجزئة الدقيقة وفق مبادئ الثقة الصفرية
- بناء قواعد جدران الحماية وترجمة عناوين الشبكة NAT وصيانتها على جدران الحماية ذات الحالة وجدران الجيل التالي وفق إرشادات NIST SP 800-41
- تهيئة أنفاق VPN بين المواقع عبر IPsec والوصول عن بعد عبر TLS مع المصادقة بالشهادات والمصادقة متعددة العوامل
- نشر حساسات كشف التسلل ومنعه IDS/IPS بأداتي Snort أو Suricata ومراقبة Zeek وضبطها لخفض الإنذارات الكاذبة مع الحفاظ على تغطية الكشف
- فرض التحكم في الوصول إلى الشبكة وفق IEEE 802.1X وحماية الشبكات اللاسلكية وتقوية المبدلات والموجهات استنادا إلى CIS Benchmarks
- تدقيق إعدادات أجهزة الشبكة وفحص ثغراتها وإدارة ضبط التغيير بما يبقي سياسة جدران الحماية وخطوط الأساس محدثة

الفئة المستهدفة:

- مهندسو الشبكات المسؤولون عن تصميم الشبكات الموجهة والمبدلة واللاسلكية في المؤسسات وتعديلها
- مهندسو الأمن المسؤولون عن ضوابط المحيط وبوابات VPN وحساسات كشف التسلل
- مسؤولو جدران الحماية المكلفون بتغييرات القواعد وترجمة العناوين والمراجعات الدورية للسياسات
- موظفو عمليات البنية التحتية المسؤولون عن تقوية أجهزة الشبكة وتحديثها وإدارتها
- موظفو التحقق الفني المسؤولون عن مراجعة إعدادات أجهزة الشبكة وسجلات التغيير

محاور الدورة:

اليوم 1: مشهد التهديدات الشبكية ومبادئ البنية الآمنة

- مسارات الهجوم على الشبكة من الاستطلاع إلى التنقل الجانبي
- أساليب انتحال العناوين والتنصت وهجمات الوسيط
- طبقات الدفاع المتعدد عبر المحيط والنواة والأجهزة الطرفية
- التقاط حركة الهجوم في المختبر بأداة Wireshark
- خط الأساس الحالي لأمن الشبكة وخريطة الأصول المكشوفة

اليوم 2: تجزئة الشبكة والمناطق الأمنية والمنطقة منزوعة السلاح DMZ وتصميم الثقة الصفرية

- نموذج المناطق الأمنية بمستويات الثقة وقنوات العبور
- خيارات موقع المنطقة منزوعة السلاح للخدمات المتاحة للجمهور
- التجزئة بالشبكات المحلية الافتراضية VLAN وجداول VRF مقارنة بالتجزئة الدقيقة
- تطبيق مبادئ الثقة الصفرية على التدفقات الداخلية في الشبكة
- مصفوفة التجزئة لتحديد التدفقات المسموحة بين المناطق

اليوم 3: أنواع جدران الحماية وتصميم القواعد وترجمة العناوين في المختبر

- سياسة جدران الحماية واختيار التقنية وفق NIST SP 800-41 لإرشادات جدران الحماية
- مقارنة قدرات مرشحات الحزم وجدران الحماية ذات الحالة وجدران الجيل التالي
- مختبر pfSense لبناء الواجهات والأسماء المستعارة وقواعد المناطق
- ترتيب القواعد والرفض الافتراضي وأعراف تسمية الكائنات
- تهيئة ترجمة عنوان المصدر والوجهة وإعادة توجيه المنافذ

اليوم 4: مختبر الشبكات الافتراضية الخاصة بين المواقع وللوصول عن بعد

- أنماط أنفاق IPsec وبروتوكول ESP وروابط الأمن
- تفاوض IKEv2 بالمفاتيح المشتركة مسبقا مقارنة بالشهادات الرقمية
- بناء نفق IPsec بين بوابتي pfSense في موقعين
- الوصول عن بعد عبر VPN بتقنية TLS مع المصادقة متعددة العوامل
- قرارات تقسيم النفق وتشخيص أعطال VPN بالتقاط الحزم

اليوم 5: دراسة حالة الأسبوع الأول لمراجعة قواعد جدران الحماية وتنظيفها

- تحليل استخدام القواعد بعدادات المطابقة وسجلات جدار الحماية
- تحديد القواعد المحجوبة والمكررة والمفرطة في السماح
- معالجة قواعد السماح المفتوح وإعادة كتابتها بمبدأ أقل الصلاحيات
- سير عمل إعادة اعتماد القواعد مع مالكي الأعمال ومدد صلاحيتها
- مراجعة تصميم المحيط المقسم للأسبوع الأول ونقده بين المشاركين

اليوم 6: نشر أنظمة كشف التسلل ومنعه IDS/IPS وضبطها بأداتي Suricatag Snort

- خيارات موقع حساسات كشف التسلل الشبكية مقارنة بحساسات المضيف
- منع التسلل داخل مسار الحركة مقارنة بالنشر السلبي عبر TAP وSPAN
- صياغة قواعد Suricata ومتغيراتها وإدارة مجموعات القواعد
- ضبط التواقيع والعتبات وكبت الإنذارات الكاذبة
- سجلات المراقبة الأمنية للشبكة في Zeek لتحليل البروتوكولات

اليوم 7: التحكم في الوصول إلى الشبكة NAC ومعيار IEEE 802.1X وأمن الشبكات اللاسلكية

- أدوار طالب الوصول والموثق وخادم المصادقة في IEEE 802.1X
- سياسات RADIUS مع EAP-TLS وهوية الأجهزة المستندة إلى الشهادات
- تجاوز المصادقة بعنوان MAC وتسجيل الضيوف للأجهزة غير المدارة
- تقييم حالة الجهاز وقواعد العزل في شبكة VLAN للحجر
- حماية الشبكات اللاسلكية المؤسسية وكشف نقاط الوصول الدخيلة

اليوم 8: تقوية الأجهزة والإدارة الآمنة وبوابات أمن DNS والبريد الإلكتروني

- تطبيق CIS Benchmarks للتقوية المرجعية على إعدادات المبدلات والموجهات
- أمن المنافذ ورقابة DHCP Snooping والفحص الديناميكي لبروتوكول ARP
- تصميم شبكة إدارة منفصلة عبر SSH وSNMPv3
- تصفية DNS وتقوية خوادم الحل وكشف أنفاق DNS
- بوابة أمن البريد الإلكتروني وفحوص SPF وDKIM وDMARC

اليوم 9: سجلات الشبكة وفحص الثغرات وضبط التغيير وتدقيق الإعدادات

- جمع سجلات Syslog وتدفقات NetFlow لحالات الكشف الشبكي
- فحص ثغرات أجهزة الشبكة بأداتي Nmap وOpenVAS
- طلبات تغيير جدران الحماية وتصنيف مخاطرها وسجلات اعتمادها
- فحص انحراف الإعدادات عن قوالب الأجهزة المعتمدة
- مؤشرات أمن الشبكة لنظافة القواعد ومدة سد الثغرات

اليوم 10: مختبر ختامي لبناء شبكة مقسمة وتدقيقها

- مختبر ختامي لتصميم المناطق وتطبيق سياسات pfSense
- مختبر ختامي لتهيئة نفق IPsec وبوابة الوصول عن بعد
- مختبر ختامي لحساس Suricata والتحكم في الوصول وفق 802.1X
- مختبر ختامي لتدقيق الإعدادات وفق CIS Benchmarks
- استكمال حزمة تصميم أمن الشبكة المقسمة وتدقيقها

المهارات التي ستكتسبها:

- تصميم المناطق الأمنية
- إدارة قواعد جدران الحماية
- تهيئة بوابات VPN
- ضبط تواقيع كشف التسلل
- التحكم في الوصول عبر المنافذ
- تقوية أجهزة الشبكة
- تقييم ثغرات الشبكة
- تدقيق إعدادات الأجهزة

لماذا تحضر هذه الدورة:

- تسليم قائد أمن الشبكات حزمة تصميم أمن الشبكة المقسمة وتدقيقها، وتضم المناطق وسياسة جدران الحماية وVPN والحساسات والتحكم في الوصول ونتائج التدقيق
- تحديد قواعد جدران الحماية الواجب إلغاؤها ومواقع حساسات IDS/IPS والوقت المناسب لتفعيل المنع داخل مسار الحركة
- تجنب الاختراقات وملاحظات التدقيق والأعطال الناتجة عن القواعد المفتوحة والحساسات غير المضبوطة والمبدلات والموجهات غير المقواة
- نقل قوائم مراجعة القواعد وخطوط أساس التقوية وإعدادات مختبر Suricatag pfSense إلى فرق تشغيل الشبكة

الخاتمة:

بعد العودة إلى العمل يسلم المشارك قائد أمن الشبكات ومجلس اعتماد التغيير حزمة تصميم أمن الشبكة المقسمة وتدقيقها، وتضم مصفوفة المناطق والتدفقات وسياسة جدران الحماية وVPN وإعدادات IDS/IPS و802.1X وخطوط أساس التقوية ونتائج التدقيق. ويعتمد عليها القائد في تحديد المقاطع المسطحة التي تقسم أولا، والقواعد التي تلغى، ومواقع الحساسات. وبعد أول دورة لإعادة اعتماد القواعد أو فترة لضبط الحساسات يراجع الفريق القواعد المحذوفة ونسب الإنذارات الكاذبة ومحاولات الأجهزة المحجوبة وملاحظات التدقيق المفتوحة مقارنة بالحزمة.

الأسئلة الشائعة:

ما الذي يحتاج المشارك إلى معرفته قبل دورة أمن الشبكات في جدران الحماية وVPN وIDS/IPS؟

يكفي أن يهيئ المشارك الموجهات أو المبدلات أو جدران الحماية في عمله، وأن يفهم عنونة IP والتوجيه والشبكات المحلية الافتراضية ومنافذ TCP وUDP. وتفيده الألفة بسطر الأوامر، لأن كل يوم يتضمن عملا تطبيقيا على Suricatag pfSense وWiresharkg وأدوات مفتوحة المصدر أخرى.

بم تختلف دورة أمن الشبكات عن دورة أساسيات الشبكات أو دورة العمليات الأمنية؟

تفترض الدورة أن المشارك يبني الشبكات فعلا، وتعلمه تأمينها بالتجزئة وقواعد جدران الحماية وVPN وIDS/IPS وNAC والتقوية. أما دورات الأساسيات فتعلم العنونة والتوجيه، ودورات العمليات الأمنية تركز على فرز التنبيهات والاستجابة للحوادث لا على هندسة الضوابط.

هل يكفي جدار حماية من الجيل التالي لأمن الشبكات دون IDS/IPS وNAC؟

لا يكفي. فجدار الجيل التالي يتحكم في الحركة بين المناطق، لكنه لا يرى كل تدفق داخلي ولا يصادق الأجهزة عند منفذ المبدل ولا يغني عن حساسات تسلل مضبوطة. والضوابط المتعددة والتجزئة والمراجعة المنتظمة للقواعد تضيف عمقا يواجهه المهاجم بعد تجاوز المحيط.

ماذا يعود به المشارك من دورة أمن الشبكات في جدران الحماية وVPN وIDS/IPS وNAC؟

يعود المشارك بحزمة تصميم أمن الشبكة المقسمة وتدقيقها، وفيها مصفوفة المناطق والتدفقات وسياسة جدران الحماية وVPN وإعدادات IDS/IPS وX802.1 وخطوط أساس التقوية ونتائج تدقيق المختبر الختامي، جاهزة للتكييف مع شبكة مؤسسته.