قبيلة الهاكر الفريق الأحمر

تفاصيل وإجابات من الخطوط الأمامية

جميل حسين طويله

www.cyberpedia.site

قبيلة الهاكر الفريق الأحمر

تفاصيل وإجابات من الخطوط الأمامية

"لدينا أذنان وفم واحد حتى نتمكن من الاستماع ضعف ما نتحدث "

يُنسب هذا الاقتباس إلى الفيلسوف اليوناني Epictetus

محاولة عيش هذه الحكمة أمر قد لا أتقنه أبداً

عندما كنت صغيراً، كنت أظن أنني أعلم كل شيء وكنت أجادل كثيراً لأكون على صواب حتى عند مواجهة الحقائق التي أظهرت بشكل قاطع أنني كنت مخطئاً، كنت ذلك الطفل الذي لا يرفع يده لأي سؤال في الفصل الدراسي ولكن هذا السلوك المتمثل بالاعتقاد بأنني كنت أذكى شخص على وجه الأرض قد تم سحقه عندما أصبحت بعمر أكبر وخاصة أثناء دراستي الجامعية وعندما بدأت في أول عمل لي تخلصت من كبريائي وبدأت بطرح المزيد من الأسئلة وبدأت بأخذ مقولة "لا يوجد شيء اسمه سؤال غبي" على محمل الجد ومنذ ذلك الحين بدأت بطرح الأسئلة والأهم من ذلك بدأت بالاستماع إلى ما قاله الآخرون، الأمر الذي غير حياتي ومسيرة تعليمي وإلى هذا اليوم ما زلت أقرأ كل ما يمكنني الحصول عليه وأظل قريباً من الخبراء المتقنين لمجالاتهم وحصلت على معظم الإجابات على اسئلتي المحيرة من قراءة الكتب وهذا الأمر قادني للوصول لعمل ناجح في مجال الأمن السيبراني.

وعندما يسألني الناس كيف وصلت إلى هنا أقول لهم:

" وصلت لأنني أطرح اسئلة واقرأ من الكتب أكثر من أي شخص آخر"

في هذه السلسلة الممتعة جداً سألنا عدد من الخبراء في مجال الأمن السيبراني أكثر من عشرين سؤال حول كيفية بدايتهم في هذا المجال وكيف حققوا النجاح وسنشارك معكم إجابات مجموعة من خبراء الاختراق العاملين في مجال الحماية الهجومية Offensive Security أو ما يعرف باسم الفريق الأحمر Red Teaming

قبل أن نبدأ، اسمحوا لي أن أوضح بسرعة ما هو الفريق الأحمر

الفريق الأحمر:

الفريق الأحمر هو تخصص في الأمن السيبراني يتم من خلاله اختبار اختراق الشبكات والتطبيقات والأنظمة للعثور على نقاط الضعف والثغرات التي قد تؤدي إلى اختراق النظام وفي بعض الأحيان، يُسمح للفرق الحمراء باستغلال الأنظمة للتحقق من أن الثغرة حقيقية ويمكن للفرق الحمراء أيضاً تنفيذ هجمات مادية أو حتى القيام بهجمات الهندسة الاجتماعية

الفريق الأزرق:

وبالجهة الأخرى هناك الفريق الأزرق المسؤول عن مراقبة الشبكات والأنظمة والتطبيقات وأنظمة منع الاختراق والتأكد من سرية جميع الأصول وسلامتها وتوافرها والاستجابة للحوادث والقيام بعمليات التحليل الجنائي الرقمي

في يومنا الحالي تجمع المنظمات بين الفرق الحمراء والزرقاء وأحياناً تستخدم مصطلح الفريق الأرجواني

الخبير الأول Marcus J. Carey:

Twitter: @marcusjcarey

https://www.linkedin.com/in/marcuscarey/

ماركوس هو خبير في الأمن السيبراني ومؤسس لشركة ناشئة لديه خبرة أكثر من 25 عاماً في العمل بحماية البيانات الحكومية والتجارية الحساسة، بدأ حياته المهنية في مجال الأمن السيبراني في دراسة علم التشفير في البحرية الأمريكية ومن ثم قدم العديد من الخدمات لوكالة الأمن القومي الاميركية (NSA)

كيف كانت بدايتك مع الفريق الأحمر؟

الشيء المضحك في رحلتي للعمل في الفريق الأحمر هو أنني لم أكن من الناحية التقنية متخصص في هذا المجال حتى طردت من العمل واضطررت لتغطية نفقاتي وحصلت على عمل في شركة استشارية في الساحل الشرقي تقوم باختبار الاختراق وتطوير المنتجات.

تمكنت من اكتساب مهارات الفريق الأحمر من خلال العمل في مركز الدفاع ضد الجريمة الإلكترونية DC3 – Defense Cyber Crime Center وفي تلك الفترة قمت بالبحث وبالتدريس وبتطوير مناهج الدورات وتمكنت من الوصول إلى جميع أدوات الفريق الأحمر التي يمكنك تخيلها، بالإضافة إلى لكل أدوات التحليل الجنائي الرقمي

الموجودة على هذا الكوكب، أنا محظوظ للغاية لأنني كنت في تلك المناصب والتي ساعدتني لألعب هذا الدور ضمن الفريق الأحمر.

" في يومنا الحالي تهيمن الأدوات مفتوحة المصدر على مساحة الفريق الأحمر، مما يجعل الأمر ممكناً لعدد أكبر من الأشخاص للتعرف عليها واستخدامها"

الحظ هو عندما تلتقي الاستعدادات بالفرصة المناسبة، إنه لأمر مزعج أنه تم تسريحي من عملي ولكن كان من الجيد أنني امتلك مهارات الفريق الأحمر لدفع الفواتير.

ما هي أفضل طريقة للحصول على عمل في الفريق الأحمر؟

من غير المألوف أن يبدأ الناس مباشرة في وظائف الفريق الأحمر وأفضل طريقة هي اكتساب المهارات الأساسية مثل كيف يعمل الإنترنت وأنظمة التشغيل وهندسة البرمجيات والبدء في دور ضمن الفريق الأزرق، في البداية سيسمح لك هذا الدور باكتساب خبرة في الأمن السيبراني والتواصل مع الأشخاص من المحيط المطلوب ويمكنك التواصل من خلال هذا الدور عبر الأحداث المحلية ومؤتمرات الأمن السيبراني الإقليمية.

كيف يمكن اكتساب مهارات الفريق الأحمر دون الوقوع في مشاكل قانونية؟

أوصي باستخدام الأنظمة الافتراضية Virtual Machines وتطبيقات الويب التي تحتوي على ثغرات أمنية لاستخدامها عند محاولة التعلم في المنزل، يوجد العديد منها، كن حذراً عندما تقوم بإعداد بيئة الاختبار وتأكد من إعداد كرت الشبكة للنظام الذي يحوي على ثغرات ليكون خلف NAT أو غير متصل بالإنترنت لأن هذا الأمر قد يؤدي لتعريض جهازك للاختراق.

إذا لم يكن لديك إذن من مالكي النظام وقمت باستخدام أدوات الاختبار ضد هذا النظام فمن المحتمل أنك ستنتهك بعض القوانين وإذا كنت تحاول الانضمام إلى للفريق الأحمر فحاول استغلال الأنظمة التي تمتلكها فقط أو الأنظمة التي لديك إذن كتابي صريح يُسمح لك من خلاله باستغلالها.

لماذا لا نتفق على ما هو الفريق الأحمر؟

أعتقد أنه من الطبيعة البشرية أننا نرغب في الاختلاف عن بعضنا البعض ولا سيما في بيئة تنافسية مثل مجتمع الأمن السيبراني.

ما تعلمته هو أن هناك طرقاً عديدة لحل المشاكل وفي كثير من الأحيان ننتهي بنفس الحلول لنفس المشاكل التي نراها وينتهي بنا الأمر إلى وجود حلول مختلفة لنفس الأمر وهذا يثبت صحة القول المأثور "لا توجد أفكار جديدة تحت الشمس"

ما هو الأمر الذي لا يفهمه الآخرون حول التواجد في الفريق الأحمر؟ وما أكثر الأكاذيب السامة التي سمعتها فيما يتعلق بالفرق الحمراء أو الزرقاء أو البنفسجية؟

هناك صراع طبيعي بين الفريق الأحمر والفريق الأزرق ناتج عن مزيج من التجارب السيئة وسوء الفهم.

أعتقد أن الأمر السيء يأتي أحياناً من أشخاص يرتكبون أخطاء مدمرة مثل إزالة السيرفرات أو ترك البرامج الضارة على أجهزة النقاط النهاية والمشكلة هي أن الجميع يسمع قصص رعب عن الفريق الأحمر ولكن ليس هناك الكثير من البيانات التي تدعم هذا الأمر.

متى يجب تقديم فريق أحمر رسمي لبرنامج الحماية الخاص بالمؤسسة؟

أعتقد أن كل فرد في مجال تكنولوجيا المعلومات وهندسة البرمجيات يجب أن يعرف كيفية بناء وتأمين واختراق أي شيء مسؤول عنه، رؤيتي المجنونة هي لأن الجميع معرض للتهديد ولست بحاجة إلى أن يكون لديك فريق أحمر للاستفادة من مهارات الفريق الأحمر، أنا دائما أقول "القيام بهجمات أكثر من قبل الفريق الأحمر يؤدي لقلق أقل من ناحية الحماية".

كيف تفسر قيمة العمل الجماعي للفريق الأحمر لعميل أو منظمة مترددة أو غير تقنية؟

أعتقد أن أفضل طريقة للقيام بذلك هي توضيح حقيقة أنه على الرغم من أن الفريق الأحمر يلعب دوراً عدائياً إلا أن أهداف الفريق الأحمر الداخلية والخارجية تتماشى مع أننا جميعاً نريد حماية البيانات الحساسة والأنظمة الهامة وللحفاظ على الثقة بمرور الوقت، يجب أن تتجنب الفرق الحمراء الظهور أمام الفرق الزرقاء أو أصحاب المصلحة الداخليين ولا يمكنك القيام بذلك إلا من خلال العمل بشكل وثيق كفريق، لا يتطلب الأمر سوى تجربة سيئة واحدة لإفساد هذه العلاقات.

ما هو أقل عنصر تحكم في الحماية من وجهة نظرك؟

مضاد الفيروسات

هل سبق لك أن أوصيت بعدم القيام بمشاركة الفريق الأحمر؟

أوصي بأن تبدأ المنظمة بإدارة نقاط الضعف وإدخال السياسة الخاصة بالحماية والحوكمة في اللعبة، أرى عدداً كبيراً جداً من المؤسسات التي تجري عمليات "اختبار الاختراق" للامتثال، أضع هذه الكلمات بين علامات الاقتباس لأن المؤسسات عادة ما تحصل على فحص محدود النطاق للثغرات الأمنية.

ما هو عنصر التحكم الأكثر أهمية أو الأسهل من حيث التنفيذ والذي يمكن أن يمنعك من اختراق نظام أو شبكة؟

تقييد الامتيازات الإدارية للمستخدمين النهائيين.

لقد رأيت بنفسي كيف أن هذا الأمر يقلل بشكل كبير من الهجمات الناجحة على الشبكة، ينطبق هذا التحكم البسيط على المؤسسات من أي حجم ومن السهل تنفيذ تقييد الامتيازات وتوسيع نطاق هذا الأمر.

لماذا تعتقد أنه من المهم الالتزام بالاتفاقية المسبقة للاختبار؟

الفرق الوحيد بين الشخص الجيد والشخص السيئ هو أن الشخص الجيد يتبع القواعد، انتهاك قواعد الاتفاقية المسبقة أو ما يعرف باسم قواعد الاشتباك rules of engagement يكسر الثقة بين الفرق وإذا انتهكت قواعد الاشتباك فقد تخالف القانون أيضاً.

هل تم كشفك في أي من عمليات اختبار اختراق وكيف تعاملت مع هذا الأمر؟

من أكثر الأشياء المحرجة التي فعلتها على الإطلاق فيما يتعلق بالفريق الأحمر هو امتلاك ذاكرة USB كان اسم وحدة التخزين الخاصة بها ماركوس كاري واكتشف برنامج التحليل الجنائي الرقمي الجهاز الذي يحمل اسمي.

لن أرتكب هذا الخطأ مرة أخرى، أنا أشارك هذه القصة حتى لا يحدث لك ذلك.

ما هو أكبر مأزق أخلاقي واجهته أثناء عملك على هدف معين؟

أكبر مأزق أخلاقي هو استخدامي للخداع في التصيد الاحتيالي والهندسة الاجتماعية

والسبب في ذلك أنك قد تسبب ضرراً فعلياً للأشخاص وسبل عيشهم ويتطلب مني هذا الأمر دائماً وجود عدد قليل من المديرين التنفيذيين في النطاق حتى لا تتمكن الإدارة من إلقاء اللوم على موظفيها وفي بعض الأحيان كنت أخفي هوية الشخص الذي تعرض للخطر حتى لا يقع في أي مشاكل محتملة.

كيف يعمل أعضاء الفريق الأحمر معاً لإنجاز المهمة؟

إذا كنت تعمل مع فريق فإن التواصل والاتصال هي العناصر الأكثر أهمية، قم بتقسيم العمل وتأكد من توثيق كل ما تفعله، الثقة مهمة أيضاً، لأنني قد واجهت مواقف يفقد فيها أعضاء الفريق الثقة بزملائهم في الفريق

أوصي أيضاً باستخدام الأدوات التعاونية حتى يتمكن الجميع من رؤية ما يفعله زملائهم في الفريق، الشفافية دائماً تفوز بالإضافة لأمر آخر وهو عدم الخوف من طلب المساعدة فإذا كان زميلك في الفريق خبيراً في أمر معين فما عليك سوى طلب المساعدة منه.

ما هو أسلوبك في استخلاص المعلومات ودعم الفرق الزرقاء بعد اكتمال العملية؟

الاحتراف هو المفتاح

نظراً لأننا جميعاً بشر، يمكن أن تلعب المشاعر دوراً عند استخلاص المعلومات للفرق الزرقاء الداخلية والخارجية، أخبرهم دائماً أنك في نفس الفريق بهدف انجاز المهمة الكبيرة وإذا قمت بذلك بشكل صحيح فسيكون لديهم خطة مفصلة لكيفية تصحيح أي مشكلات تم اكتشفتها.

الجزء الصعب هو عندما تساعد شخصاً ما ثم تعود في المستقبل وتجد أن نفس المشكلة ما زالت موجودة، لا تغضب وحاول التعامل مع هذا الموقف بشكل احترافي من خلال تقديم الحلول والمساعدة.

"يمكنك أن تقود الحصان إلى الماء ولكن لا يمكنك أن تجعله يشرب"

إذا كنت ستنتقل إلى الفريق الأزرق فما هي خطوتك الأولى للدفاع بشكل أفضل ضد الهجمات؟

أنا فريق أزرق مدى الحياة ولكنني أحياناً فريق أحمر.

الخطوة الأولى لامتلاك القدرة على الدفاع ضد الهجمات هي وضع السياسة واتباعها

أكرر: اتبعها

لا يطبق الناس السياسات لأنها تبدو مرهقة، يجب النظر إلى السياسة الأمنية مثل الخريطة، قد لا تكون في المكان الذي تنص السياسة على وجودك فيه ولكن إذا لم يكن لديك خريطة فلن تصل إلى وجهتك أبداً

ما هي بعض النصائح العملية لكتابة تقرير جيد؟

نصيحتي هي عدم إعادة اختراع العجلة فهناك الكثير من الموارد المتاحة لوصف نقاط الضعف والاستغلالات، لا تتردد في الحصول على المحتوى من NIST, CVSS or MITER ATT & CK والاستشهاد بها كمراجع لأن الاستشهاد بهذه المصادر كمراجع يعزز في الواقع مصداقية نتائجك وتقريرك.

استخدم المعرفات الخاصة بالثغرات مثل CVSS للمساعدة في تسجيل نقاط الضعف التي تجدها كما أن MITER ATT&CK مفيد لمناقشة تقنيات الاستغلال والحلول المقترحة، إذا كنت تستخدم هذه الموارد فسيكون من السهل كتابة التقرير ويسهل على العميل الوثوق به.

كيف تضمن أن تكون نتائجك ذات قيمة للأشخاص الذين يحتاجون إلى سرد كامل؟

أعتقد أنه من المهم استخدام شيء يخبر كلا الجانبين كامل التفاصيل

أنا أحب التعامل مع أمور مثل MITER ATT&CK Framework و إطار عمل الأمن السيبراني NIST Framework يمكنك استخدام هذه الأمور لقياس قدراتك الفعلية

ومن الممكن أن تكون فعالاً في مجال الأمن السيبراني دون إتقان جميع المهارات ولكن من المهم أن تكون قادراً على التعلم.

كيف توصي بإدخال تحسينات على الحماية بخلاف الإشارة إلى المواضع التي تكون فيها غير كافية؟

أحاول دائماً العثور على بعض الأمور التي يجب على المنظمات تطبيقها بشكل صحيح والحصول على نتائج ملموسة من خلالها مثل تطبيق المصادقة الثنائية وطول كلمة السر وتطبيق التحديثات التلقائية.

هناك طريقة أخرى للمساعدة بصفتك عضواً في الفريق الأحمر وهي فهم طرق إصلاح المشاكل، سواء على النظام أو على الشبكة أو في التعليمات البرمجية التي تساعدك لبناء صداقات وعلاقات عديدة، لقد جلست جنباً إلى جنب مع مديري العديد من الأنظمة لمساعدتهم في كتابة أوامر لتقوية الحماية الخاصة بأنظمتهم وهذا الأمر مهم وخاصةً إذا كنت تعمل ضمن فريق أحمر داخل الشركة.

ما هي المهارات الغير تقنية التي تبحث عنها عند تعيين أعضاء الفريق الأحمر بعد إجراء مقابلات معهم؟

التعاطف، هو مهارة عظيمة يجب امتلاكها عندما تنقل أخباراً سيئة.

بصفتك عضواً في الفريق الأحمر سيتعين عليك تقديم بعض الأخبار السيئة بين الحين والآخر، ضع نفسك مكان الشخص الآخر وتعامل مع هذا الأمر بعاطفة وحكمة.

ما الذي يميز لاعبي الفريق الأحمر الجيد ليكونوا قادرين على التعامل مع المشاكل بشكل مختلف؟

أعتقد أن أعضاء الفريق الأحمر الجيدين يدرسون ويعرفون كيف تعمل كل التقنيات وقادرين على التعامل مع مختلف الأمور.

ذكرت التعاطف من قبل كما يمكن لعضو الفريق الأحمر الجيد أن يضع نفسه في عقلية مسؤول النظام أو مهندس الشبكة أو مطور البرامج وأن يحل المشاكل التي يواجهها ودائماً ما يكون لاعب الفريق الأحمر الجيد متعطش لتحسين مهاراته ومساعدة الآخرين على القيام بذلك وحل المشاكل

الخبير الثاني David Bell:

Twitter: @operant

يشغل ديف حالياً منصب مدير الفريق الأحمر لشركة GE – General Electric حيث يقود عمليات المشاركة مع الأصول الإستراتيجية في العديد من الصناعات في جميع أنحاء العالم وقبل انضمامه إلى هذه الشركة، أمضى ديف 10 سنوات مع الفريق الأحمر للبحرية الأمريكية، حيث خطط وقاد ونفذ العديد من عمليات الاختبار ضد جميع فروع الجيش الأمريكي والعديد من الوكالات الحكومية وحتى شركاء التحالف.

ديف هو أيضاً من قدامى المحاربين في البحرية الأمريكية، حيث أمضى 10 سنوات في مجتمعات الاستخبارات والبرامج العسكرية الخاصة

كيف كانت بدايتك مع الفريق الأحمر؟

لقد بدأت في عام 2006 مع الفريق الأحمر للبحرية الأمريكية كمقاول وكنت قد أمضيت وقتها حوالي ستة أشهر في العمل الليلي كمحلل لأنظمة كشف الاختراق مع شركة مقاولات أخرى وقبل ذلك كنت في الخدمة الفعلية في البحرية ومعظم فترة خدمتي كانت في استخبارات الإشارات.

قضيت الكثير من الوقت قبل انفصالي عن البحرية في الدراسة للحصول على الشهادات الخاصة باختراق الشبكات وكان ذلك كافياً لدخولي إلى هذا المجال والآن أنا مدير الفريق الأحمر في شركة GE

ما هي أفضل طريقة للحصول على عمل ضمن الفريق الأحمر؟

هذا السؤال يُطرح علي بشكل دائم وما زلت أجد صعوبة في الإجابة عليه.

ليس هناك "طريقة صحيحة" لتصبح عضواً في الفريق الأحمر، لقد عملت مع رجل ذكي جداً وقد قاد الجرافات في وقت من الأوقات، أشير لهذا الأمر لإظهار أن القدرة على التفكير كمهاجم هي أمر بالغ الأهمية وهذا الأمر لا يمكن تعليمه، يمكننا تعليم المهارات التقنية ولكن العقلية تأتي من الفطرة، إذا كان لدى شخص ما العقلية الصحيحة فإن نصيحتي هي متابعة التدريب والحصول على الشهادات والمشاركة في مسابقات CTF – Capture The Flag كل هذه الأمور تشير إلى أن المرشح ملتزم وسيواصل العمل وتعطيني فكرة عن كيفية أداء المرشح كجزء من الفريق وأقترح أيضاً البدء بوظائف أخرى في مجال الأمن السيبراني مثل تحليل الهجمات أو التعامل والاستجابة للحوادث الأمنية

كيف يمكن لشخص أن يكتسب مهارات الفريق الأحمر دون الوقوع في مشاكل قانونية؟

لا ينبغي أن يكون هذا الأمر مشكلة بعد الآن وخاصة بعد توفر الكثير من فرص التدريب سواء عبر الإنترنت أو من خلال الحضور بشكل شخصي.

توفر المنصات السحابية بيئات تعلم فعالة وغير مكلفة من الناحية المادية ولهذا السبب لم نعد بحاجة إلى شراء معدات قديمة لبناء مختبر منزلي.

لماذا لا نتفق على ما هو الفريق الأحمر؟

كوني قادم من مجتمع الفريق الأحمر العسكري الأمريكي فلدي وجهة نظر قوية جداً حول إساءة استخدام هذا المصطلح وغيره من المصطلحات ذات الجذور العسكرية.

من المغري إلقاء اللوم على التسويق الصناعي في هذا الأمر ولكنها في الحقيقة مشكلة مجتمعية، اختبار الاختراق هو نظام منفصل عن الفريق الأحمر ، كما أن هناك فرق كبير بين الفرق الحمراء الداخلية والفرق الحمراء الاستشارية و يمكن أن تتسبب هذه الاختلافات في إرباك العملاء الذين يريدون فقط أفضل أمر وفق الميزانية المتوفرة لديهم.

ما هو الأمر الذي لا يفهمه بقية العاملين في مجال أمن المعلومات حول التواجد في الفريق الأحمر؟

ما أكثر الأكاذيب السامة التي سمعتها فيما يتعلق بالفرق الحمراء أو الزرقاء أو البنفسجية؟

قد تكون عمليات الفريق الأحمر مملة نوعاً ما لإنه عمل تحليلي مفصل ولكنه أيضاً عمل مذهل للعقل وتتخلله لحظات من الابتهاج المطلق والأدرينالين العالي.

يرى معظم الناس النقاط البارزة فقط في استخلاص المعلومات لأن لديهم مفاهيم خاطئة من المشاهد المعروضة في أفلام هوليوود.

متى يجب تقديم فريق أحمر رسمي إلى برنامج الحماية في المؤسسة؟

غالباً ما أخبر الناس أنهم لا يحتاجون إلى مشاركة الفريق الأحمر حتى يتمكنوا من فهم هذا العمل وبمجرد أن تشعر المنظمة أنها تتفهم جميع التهديدات ولديها تعامل جيد مع الأمور فقد حان الوقت لفريق أحمر جيد لتحدي هذه الافتراضات.

كيف تفسر قيمة العمل الجماعي للفريق الأحمر لعميل أو منظمة مترددة أو غير تقنية؟

لا أستطيع أن أؤكد هذا بما فيه الكفاية، يتعين على الفريق الأحمر فهم ما يهاجمونه في سياق العمل الذي يدعمونه ولهذا السبب يجب فهم طبيعة الأعمال وإظهار هذا الفهم سيقطع شوطاً طويلاً نحو بناء الثقة والشراكة الحقيقية مع العميل.

ما هو أقل عنصر تحكم في الحماية تراه مطبقاً؟

البحث عن الثغرات ونقاط الضعف.

على الرغم من أن هذا الأمر يعتبر وظيفة حماية مهمة، إلا أنني نادراً ما أرى أنها تتم بشكل صحيح وخاصة إذا كانت المؤسسة لا تحتفظ بجرد دقيق للأصول فكيف يمكن أن يتوقعوا أن يكونوا قادرين على فحص كل ما لديهم؟

هل سبق لك أن أوصيت بعدم القيام بمشاركة الفريق الأحمر؟

نعم! في كثير من الأحيان

لقد اكتشفت أنه بينما يطلب العديد من العملاء مشاركة الفريق الأحمر فإنهم غالباً ما يبحثون (دون قصد) عن اختبار تطبيق ويب أو شكل آخر من اختبار الاختراق محدود النطاق وفي هذه الحالات أقوم بتوجيههم لفريق آخر يمكنه تلبية احتياجاتهم بشكل أفضل

قد يرى البعض هذا الأمر على أنه "خسارة عمل" ولكنني أرى أنه بناء للثقة مع العملاء.

ما هو عنصر التحكم الأكثر أهمية أو الأسهل من حيث التنفيذ والذي يمكن أن يمنعك من اختراق نظام أو شبكة؟

نادراً ما تحتاج أجهزة النقاط النهاية إلى القدرة على التواصل مع بعضها البعض عبر الشبكة ويجب أن يؤدي حظر هذا النوع من حركة البيانات أو مراقبته إلى قطع شوط طويل نحو الحد من الحركة الجانبية للمهاجم للتوسع في الهجوم والوصول لأجهزة جديدة داخل الشبكة.

ضع في اعتبارك أن المهاجم يسعى وراء البيانات الموجودة في قاعدة البيانات وما إلى ذلك ويستخدم ما يسمى بالحركة الجانبية للوصول لهذه الأنظمة الخاصة بقواعد البيانات والحصول على الأذونات أو الصلاحيات اللازمة لذلك ولهذا السبب عندما أقلل من هذه الحركة قدر الإمكان فإني أمنع المهاجمين من القيام بذلك.

لماذا تعتقد أنه من المهم الالتزام باتفاقية حدود الاختبار؟

تُستخدم اتفاقية حدود الاختبار أو ما يسمى بقواعد الاشتباك Rules of Engagement لتحديد كيفية إجراء المهمة المطوبة تحديد نطاقها وبمن يجب الاتصال في حالة الطوارئ وأي بنود أخرى ذات أهمية .

تعتبر قواعد الاشتباك ROE شبكة الأمان الأساسية لكل من الفريق الأحمر والعميل وإذا انحرف الفريق الأحمر عن هذه القواعد فقد تتعطل الأنظمة أو يمكن إنشاء ظروف أخرى غير آمنة ومع ذلك، يمكن أن تحدث الحوادث (بالفعل تحدث) لذا فإن قواعد الاشتباك الجيدة ستحدد عمليات الإبلاغ عن تلك الحوادث وسيكون الفريق الأحمر صادقاً تماماً بشأن ما حدث.

إذا تم ضبطك في أي عملية اختبار اختراق أو عمل آخر فكيف تتعامل مع هذا الموقف؟

لم أقم مطلقاً بعمليات اختبار اختراق و لكنني كنت جزءاً من العديد من مشاركات الفريق الأحمر بما في ذلك عمليات استغلال للشبكات السلكية واللاسلكية وحتى عمليات الاختبار المادية داخل مكان العمل.

إحدى قصصي المفضلة هي عندما تم ضبطي أنا وزميلي في الفريق أثناء محاولة إقناع بعض الأفراد العسكريين بالسماح لنا بتوصيل محرك أقراص USB صغير، سمع ضابط رفيع المستوى المحادثة من الغرفة المجاورة واندفع على الفور لمواجهتنا وكان يرتجف من الغضب

وأخبرنا:

"الفريق الأحمر فعل هذا بي العام الماضي ولن تفعل ذلك مرة أخرى!"

لم يكن لدي أي فكرة عما كان يتحدث عنه ولكنني كنت أعلم أن لدي خيارين: إما أن أتراجع وأعترف بأنني تم الإمساك بي أو يمكنني الحفاظ على هذه الشخصية والتفاعل بنفس الطريقة التي قد يتخذها أي شخص آخر في هذا الموقف، اخترت الخيار الثاني وبدأت في الصراخ بأنني لا أقبل هذه الاتهامات وأنني كنت أحاول القيام بعملي فقط.

أخذنا هذا الضابط إلى مسؤول الأمن الخاص به و أخبره أن بطاقات التعريف (المزورة في الواقع) تبدو طبيعية بالنسبة لهم و بينما غادر الضابط الأول الغرفة لاسترداد مفتاح التشفير لهاتفه (حتى يتمكن من الاتصال بـ "رئيسي") أوضحت لضابط الأمن أن لدينا أذن تفويض في السيارة ويمكننا احضاره لتبرير هذا العمل.

ما هو أكبر مأزق أخلاقي واجهته أثناء عملك على هدف معين؟

أن يُطلب منك "استهداف" أفراد معينين، هذا أمر مخيف بعض الشيء.

أفضل عدم القيام بذلك وسأجادل دائماً ضد هذا الأمر، ليس لدي مشكلة في استهداف أدوار أو مناصب معينة داخل المنظمة ومع ذلك، طالما أن هناك نموذجاً قوياً للتهديد يبرر ذلك.

أحد الأمثلة عندما طُلب مني إلقاء نظرة على صفحات وملفات وسائل التواصل الاجتماعي للمديرين التنفيذيين وعائلاتهم وهنا يجب أن تكون الضوابط الدقيقة في مكانها وأن يُمنح الإذن الصريح قبل أن أقوم بمهام مثل هذه.

كيف يعمل أعضاء الفريق الأحمر معاً لإنجاز المهمة؟

غالباً ما تكون القدرة على العمل كفريق متماسك هي ما يميز الفرق عالية الفعالية عن الفرق الأخرى ويجب أن يكون كل عضو في الفريق مهم وماهر وموهوب ولكن لا يوجد عضو في الفريق يتمتع بمهارات عالية بحيث يمكنه من خلالها إكمال العمل بدون مساعدة زملائه في الفريق.

التوثيق التفصيلي له أهمية قصوى أثناء عمل الفريق الأحمر، يدفع العميل مقابل المعلومات الواردة في التقرير والمشتقة من التسجيل المفصل لكل عمل تم إجراؤه أثناء المهمة الفعلية.

ما هو أسلوبك في استخلاص المعلومات ودعم الفرق الزرقاء بعد اكتمال العملية؟

يجب أن تكون عملية استخلاص المعلومات مخصصة للجمهور دائماً ويجب أن يحصل المدافعون على تقرير تقني متعمق يرشدهم خلال مسار الهجوم من البداية إلى النهاية ويجب تحديد وقت كافي للأسئلة ويجب أن يكون الفريق الأحمر مستعداً لأي تقارير متابعة للأشخاص الرئيسيين الذين لم يتمكنوا من الحضور لسبب ما، كما أشجع الفرق على أن تكون متاحة لإجراء اختبارات مصغرة أو أشكال أخرى من الدعم لتمكين المدافعين من التعلم من المشاركة ويجب أن يعكس التقرير ذلك ويجب أن تذكر الحقائق دون غرور وأن تدرك أن بعض الناس سيكونون محرجين.

إذا كنت ستنتقل إلى الفريق الأزرق فما هي خطوتك الأولى للدفاع بشكل أفضل ضد الهجمات؟

الوقاية هي الأمر الأفضل ولكن الكشف أمر لا بد منه.

ستكون خطوتي الأولى هي فهم مصادر البيانات المتاحة والتأكد من أنها في متناول المدافعين، لقد اشتكى العديد من المدافعين من التحميل الزائد للبيانات ولكن في كل عملية شاركت فيها ظهر نوع من النقاط العمياء وكلما زادت البيانات المتاحة للأتمتة والاستعلامات اليدوية، زاد احتمال اكتشاف الهجوم.

ما هي بعض النصائح العملية لكتابة تقرير جيد؟

إلتزم بالحقائق وارسم صورة واضحة لمسار الهجوم ولا تستخدم المصطلحات المعقدة وقدم مراجع خاصة بمعرفات الثغرات CVE أو الأدلة التقنية الأخرى.

التقرير هو المنتج الذي تقدمه وهذا هو ما يدفع الزبون من أجله ولا يوجد شيء آخر مهم غيره، لذا عليك القيام بذلك بشكل صحيح في كل مرة وإذا كانت هناك أسئلة إضافية بعد المتابعة فأجب عنها بسرعة وبدقة وقم بتدوينها في تقريرك التالي.

كيف تضمن أن تكون نتائج برنامجك ذات قيمة للأشخاص الذين يحتاجون إلى سرد كامل للتفاصيل؟

سيختلف هذا الأمر مع كل مؤسسة ولكن الطريقة الجيدة للبدء هي تحديد العملاء الحقيقيين للفريق الأحمر.

يختلف العملاء عن أصحاب المصلحة ويصبح هذا التمييز مهماً عند محاولة تحديد الأولويات للعمل والتقارير وبمجرد تحديد العملاء وأصحاب المصلحة الحقيقيين يجب أن تبدأ قيادة الفريق الأحمر في تكييف اتصالاتهم مع هؤلاء الأفراد ويجب أن تكون التقارير في المستوى الصحيح من التفاصيل وأن تجيب بوضوح على كل الأسئلة المتوقعة قبل أن يتم طرحها.

يتطلب هذا الأمر تعلم وفهم الأعمال وفهم كيف تتناسب التكنولوجيا التي قام فريقك بتقييمها للتو مع تلك العمليات وبالتالي تأثير إجراءات فريقك على العمل ككل.

كيف توصي بإدخال تحسينات على الحماية بخلاف الإشارة إلى المواضع التي تكون فيها غير كافية؟

غالباً ما يُطلب من الفرق الحمراء تقديم توصيات لتحسين الحماية والأمان، تقدم الفرق الحمراء نظرة سريعة على بيئة العمل و من المحتمل ألا يكون لدى الفرق الحمراء أي فكرة عن سبب ظهور البيئة بالشكل الذي تبدو عليه ولكن من شبه المؤكد أنه تم اتخاذ قرارات في مرحلة ما لسبب خاص بالعمل بهدف تصميم وبناء البيئة بهذه الطريقة المعينة.

تتمثل إحدى الطرق الفعالة أخذ تلك الأمور في الاعتبار ويجب أن يجلس الفريق الأحمر مع الفرق المسؤولة عن تنفيذ الإصلاحات والسير في مسار الهجوم من البداية إلى النهاية، يساعد هذا الأمر مسؤولي الشبكة في إلقاء نظرة خاطفة على عقل المهاجم، كما يساعد الفريق الأحمر على فهم التحديات التي يواجهها أصحاب الشبكة وبعد ذلك، يمكن إجراء عصف ذهني لعمليات التخفيف المحتملة ووضعها على رأس الجدول مما يؤدي إلى الحصول توصيات عالية الجودة يمكن تنفيذها بالفعل ويمكن للفريق الأحمر العودة في وقت لاحق وإعادة اختبار البيئة لمعرفة ما إذا كانت الإصلاحات الموصى بها تعمل على النحو المنشود.

ما هي المهارات الغير تقنية التي تبحث عنها عند تعيين أحد أعضاء الفريق الأحمر أو أثناء إجراء مقابلات معهم؟

عندما أتحدث إلى المرشحين أقوم بالبحث عن المواقف الإيجابية والدوافع الداخلية القوية وغالباً ما يجد العاملون في الفريق الأحمر أنفسهم غارقين في عمليات التحليل والتي يمكن أن تحدد نتائجها نجاح عملهم، لذلك من المهم أن يكون المرشحون قادرين على تحفيز أنفسهم على الاستمرار وعدم تضيع الهدف وعدم الشكوى من أنهم "لا يقومون بأشياء رائعة" عادةً ما يكون عمل الفريق الأحمر مملاً جداً، باستثناء لحظات الأدرينالين العالي عند الحصول على النتائج الرائعة، لذلك يحتاج المرشحون إلى إعطاء الانطباع بأن لديهم الصبر والتصميم على إنجاز المهام المطلوبة.

ما الذي يميز لاعبي الفريق الأحمر الجيد عندما يتعاملون مع مشكلة ما بشكل مختلف؟

أعضاء الفريق الأحمر الجيدون قادرون على التفكير والتخطيط والتصرف كمهاجم وغالباً ما يُشار إلى هذه القدرة على أنها عقلية المهاجم، لكنها تتعلق بأسلوب حياة أكثر من كونها مجرد شيء يمكن تشغيله أو إيقاف تشغيله حسب الحاجة، على سبيل المثال: بمجرد أن يتم تدريب فريق العمل الأحمر الجيد وإجراء عمليات اختراق مادية فإن هؤلاء العناصر سيقومن بشكل اعتيادي وبدون وعي برصد كل مبنى يدخلونه و سيقومون وبشكل تلقائي بتدوين موقع وزاوية الكاميرات ومكان عناصر الأمن ونوع وحالة الأقفال على الأبواب والنوافذ وما إلى ذلك، كل هذه الأمور تتم دون التفكير في الأمر وينطبق الشيء نفسه على أعضاء الفريق الأحمر أثناء العمل على لوحة المفاتيح، سيطورون قدرة فطرية على الشعور بنقاط الضعف والثغرات ويفهمون بشكل حدسي ليس فقط كيفية استغلالها ولكن ما إذا كان ينبغي عليهم استغلالها لتعزيز أهدافهم النهائية.

يصعب تحديد هذه الجودة في المرشحين بل ويصعب التعبير عنها بالكلمات ومع ذلك، فقد رأيت نتائج جيدة عند قيام المرشحين بإظهار مواهبهم في تحديات المهارات خلال المراحل الأخيرة من عملية المقابلة.

تخبرنا الطريقة التي يتعامل بها المرشح مع المشاكل في بيئة افتراضية عالية الضغط عما إذا كانت عقلية المهاجم موجودة بالكامل لديه أو تحتاج إلى تطوير أو ببساطة غير

موجودة، لا يمكن لأي شخص أن يفكر بهذه الطريقة ولا يمكن للجميع أن يكونوا في الفريق الأحمر.

لا بأس بذلك، لقد رأيت أشخاصاً أذكياء جداً يكافحون مع هذا الجانب ولكن بعد ذلك استمروا في بناء وظائف ناجحة في جوانب وتخصصات أخرى في الأمن السيبراني.

الخبير الثالث Paul Brager:

Twitter: @ProfBrager

نظراً لكونه قائداً فكرياً وخبيراً في مجتمع الأمن السيبراني لأكثر من 25 عاماً، يتمتع بول بخبرة عميقة في تقييم البنية التحتية الحيوية لأصول المصانع (الأنظمة الصناعية) وأجهزة انترنت الأشياء IoT وتأمينها والدفاع عنها ويسعى بصفته متحدثاً وباحثاً شغوفاً إلى المضي قدماً في الأمور الخاصة بحماية أنظمة التحكم الصناعية – ICS Industrial Control Systems وإدارة التهديدات وقد شارك وقدم العديد من المقابلات والمنشورات والندوات عبر الإنترنت والتي قدمت إرشادات ونظرة ثاقبة حول استراتيجيات البنية التحتية الحيوية و الدفاع السيبراني.

لدى بول شغف بتوجيه الأشخاص الذين يتطلعون إلى المساهمة في تقدم الصناعة وتعزيز التنوع داخل المجتمع السيبراني.

كيف كانت بدايتك مع الفريق الأحمر؟

بدايات فريقي الأحمر (مثل معظم التجارب في هذا المجال) جاءت من الضرورة.

عندما كنت أعمل في شركة كانت تستخدم نظام التشغيل Windows 95 نعم Windows 95 لا تستغرب كان هذا الأمر في منتصف التسعينيات وأثناء عملي كنت بحاجة إلى بعض المهارات لتنفيذ الأعمال المطلوبة مني وبدأت اتعلم بعض تقنيات الاختراق الخاصة بأنظمة التشغيل وعندها كنت بحاجة إلى بعض المعرفة بنظام Linux وإلى معرفة كيفية عمل الأقراص والتقسيمات داخل نظام Windows وكنت أمضي ساعات طويلة في بناء (وإعادة بناء) البرامج الخاصة بعمليات نظام التشغيل Windows

95 وبالفعل تمكنت بنجاح من الوصول إلى آلية عمل Windows 95 واستعادة الكود المصدري القيم الذي كان سيكلف الشركة شهوراً في التطوير.

ما هي أفضل طريقة للحصول على وظيفة ضمن الفريق الأحمر؟

هذا الأمر يعتمد على السؤال التالي: ما هو عمل الفريق الأحمر ؟

اختبار الاختراق بشكل كامل؟ اختبار الاختراق ضد فئات معينة من الأصول وبعبارة أخرى ضد أنظمة التحكم الصناعية ICS؟

أفضل طريقة للحصول على وظيفة في الفريق الأحمر هي أن تفهم أولاً ما الذي تريد القيام به ثم بناء مجموعة من المهارات التقنية لتتماشى مع ما يستلزمه هذا الأمر وبالتأكيد فإن الخبرة هي المفتاح هنا ولكن ليس بشكل دائم ففي بعض الأحيان تكون المعرفة الأولية والدراية بالأمور الأساسية أمر كافي.

كيف يمكن لشخص أن يكتسب مهارات الفريق الأحمر دون الوقوع في مشاكل قانونية؟

في يومنا الحالي من السهل اكتساب مهارات الفريق الأحمر دون الوقوع في مشاكل قانونية، العديد من الأدوات التي نحتاجها هي مفتوحة المصدر ويمكن الحصول عليها بسهولة وينطبق هذا الأمر أيضاً على الوصول إلى العديد من أنظمة التشغيل التي قد تكون أهدافاً محتملة، لقد فتح عالم المحاكاة الافتراضية الباب أمام إنشاء مختبرات افتراضية يمكن تدميرها وإعادة بنائها دون أي تأثير على أي شخص آخر غيرك بالطبع

وبالإضافة إلى ذلك، هناك العديد من المنصات القابلة للاختراق المتاحة لاختبار المهارات والقدرات المختلفة مثل Hack The Box

لماذا لا نتفق على ما هو الفريق الأحمر؟

كما هو الحال مع العديد من الأمور في مجال الأمن السيبراني، هناك دائماً اعتقاد ضمني عند مناقشة ما هو الفريق الأحمر، يعتقد البعض أن الفريق الأحمر هو مجرد فريق للهجوم ويعتقد البعض الآخر أن الفريق الأحمر هو أكثر قوة ومنهجية من ذلك بكثير وبالنسبة لي أعتقد أن هذا الأمر يعتمد في النهاية على منظور الجمهور بالنسبة لأولئك الذين يعملون في بيئة الشركات، يعطي الفريق الأحمر اسماً أكثر أناقة لاختبار الاختراق لغرض غير ضار وهو يولد إحساساً بالبنية والمنهجية التي تعزز القدرات الأمنية الهجومية للكشف عن نقاط الضعف القابلة للاستغلال.

ما هو الأمر الذي لا يفهمه بقية العاملين في مجال أمن المعلومات حول التواجد في الفريق الأحمر؟

ما أكثر الأكاذيب السامة التي سمعتها فيما يتعلق بالفرق الحمراء أو الزرقاء أو البنفسجية؟

التواجد في فريق أحمر لا يجعل الشخص شريراً أو ضاراً وبدلاً من ذلك، فإن ما يثيرهم في مجال الأمن السيبراني يميل إلى أن يكون امتلاك القدرات الهجومية.

يعد البحث عن نقاط الضعف القابلة للاستغلال واكتشافها أمراً شاقاً ومضنياً والقدرة على القيام بذلك وتوضيح النتائج بطريقة قابلة للفهم يعد فناً أكثر من كونه علماً.

أكثر الأكاذيب السامة التي سمعتها حتى الآن هي أن متخصصي الأمن السيبراني يتناسبون تماماً مع واحدة من ثلاث مجموعات: الفريق الأحمر والفريق الأزرق والفريق الأرجواني، يعطي هذا الأمر تصوراً بأن محترفي الأمن السيبراني هم مترابطون وهذا ببساطة ليس صحيحاً على الإطلاق.

يجب أن يفهم أعضاء الفريق الأحمر كيف يمكن إحباط محاولات الاختراق أو اكتشافها وأن يتوصلوا إلى تدابير مضادة لتقليل احتمالية حدوث ذلك ويجب أن يفهم أعضاء الفريق الأزرق لحد ما، طريقة تفكير المهاجمين والأسلوب المتبع والتقنيات المستخدمة في الهجمات ليتمكنوا من تطوير إجراءات مضادة بشكل أفضل.

معظم متخصصي الأمن السيبراني هم ظلال من اللون الأرجواني، حيث يكون اللون الأحمر أو الأزرق أكثر اعتماداً على التقارب والنضج في هذا المجال.

متى يجب تقديم فريق أحمر رسمي إلى برنامج الحماية للمؤسسة؟

يمكن إدخال فريق أحمر رسمي في برنامج الحماية في أي وقت، تعتمد قيمة وفائدة القيام بذلك إلى حد كبير على ما يمكن اكتسابه من تمارين الفريق الأحمر فإذا كان القصد هو فهم سطح التهديد وإلى أي درجة يكون البرنامج (أو جزء من البرنامج) ضعيفاً فمن المعقول إشراك خدمات الفريق الأحمر في وقت مبكر من مرحلة تطوير البرنامج كأداة لوضع إطار أفضل للمخاطر الكلية وبالمثل، يمكن أن تكون مشاركة الفريق الأحمر الرسمي جزءاً من استراتيجية الحماية الشاملة ودورة الحياة لإعادة تقييم قوة عناصر التحكم وقدرة المؤسسة على الاكتشاف والاستجابة.

كيف تفسر قيمة العمل الجماعي للفريق الأحمر لعميل أو منظمة مترددة أو غير تقنية؟

قد يكون الضغط من أجل تكوين فرق حمراء داخل المؤسسة أمراً صعباً وخاصةً إذا لم ينضج برنامج الحماية في المؤسسة بعد تقييم الضعف أو إدارة الثغرات الأمنية. بالإضافة إلى ذلك، إذا لم تستثمر المنظمة بشكل كافي في الضوابط أو الموارد فقد يكشف الفريق الأحمر عن نقاط الضعف التي لم تُدرج في الميزانية والتي لا توجد موارد كافية لمعالجتها، مما يؤدي إلى تفاقم المشكلة.

كان نهجي دائماً هو تأطير فكرة الفريق الأحمر كوظيفة لإدارة المخاطر أو التخفيف منها، يسمح العمل الجماعي للفريق الأحمر للمؤسسة بالعثور على ثغرات قد تكون ضارة أو محفوفة بالمخاطر في وضعها الأمني قبل أن يستغلها المهاجمون، مما يقلل من التأثير المحتمل على سمعة الشركة و العملاء والمساهمين.

ما هو أقل عنصر تحكم حماية تراه مطبقاً؟

مع العدد الهائل من المنتجات والخدمات والقدرات الأمنية المتوفرة في السوق، يجب أن تدعم جميعها مفهومين رئيسيين: الكشف والاستجابة ومع ذلك، فإن العديد من المؤسسات الأمنية ليست مجهزة بالموظفين بشكل مناسب لاستهلاك جميع البيانات المتاحة لها من هذه الأدوات والعمل وفقاً لها.

أدوات اكتشاف التهديدات تقدم فائدة أقل من المتوقع منها لأنها لا تزال تتطلب ارتباطاً بالبيئة التشغيلية، الأمر الذي يتطلب ضمنياً كوادر بشرية، حتى مع الأتمتة والتنسيق بين جدران الحماية و أنظمة كشف ومنع الاختراق IDS / IPS وأنظمة إدارة

الأحداث الأمنية SIEM فإن الاستفادة من معلومات التهديد بشكل صحيح يتطلب موارد أخرى أو تدخل للعنصر البشري.

هل سبق لك أن أوصيت بعدم القيام بمشاركة الفريق الأحمر؟

يمكن للعميل أو المؤسسة دائماً الاستفادة من أي شكل من أشكال نشاط "الفريق الأحمر" حتى لو كان مجرد اختبار اختراق بسيط.

في حياتي الاستشارية، أوصي عموماً بعدم العمل الكامل للفريق الأحمر إذا كان هناك عدم نضج كبير واضح في برنامج أمان المنظمة أو إذا تعذر تسوية قواعد الاشتباك لإجراء عمل الفريق الأحمر بأمان، ما تم التوصية به في الماضي هو نهج أكثر تدريجياً، يتبع نطاقاً محدوداً من الأهداف ثم يتوسع تدريجياً مع زيادة النضج الأمني للمؤسسة.

ما هو عنصر التحكم الأكثر أهمية أو الأسهل من حيث التنفيذ والذي يمكن أن يمنعك من اختراق نظام أو شبكة؟

يمكن أن يكون التدريب على الوعي الأمني أحد أسهل وأهم عناصر التحكم التي تعزز الوضع الأمني العام للمؤسسة.

يمكن أن يكون سلوك المستخدم هو الفرق بين مشهد التهديد المُدار والمشهد الجامح وفي كثير من الحالات، سيرى المستخدم النهائي الحوادث قبل الحماية، لذا يجب تثقيف المستخدمين وتمكينهم من ممارسة النظافة الإلكترونية الجيدة وبالإضافة إلى ذلك يمكن الاستفادة من بعض ضوابط الحماية المعتمدة على خدمات الحوسبة السحابية لتعويض التكاليف العالية للبنية التحتية، إذا كان ذلك يمثل عائقاً،

هذا الأمر مفيد للشركات الصغيرة والمتوسطة الحجم ذات الموظفين أو الميزانيات المحدودة.

لماذا تعتقد أنه من المهم الالتزام بقواعد اتفاقية الاختبار؟

يتم وضع اتفاقية الاختبار أو ما يعرف باسم قواعد الاشتباك كعلامات خارجية لأي فريق أحمر أو لأي عملية اختبار اختراق لإنها توفر بشكل أساسي الغطاء العلوي للأنشطة التي قد تسبب ضرراً أو انقطاعاً عن الخدمة، حتى لو كان ذلك بشكل غير مقصود وبالإضافة إلى ذلك، يمكن أن تكون قواعد الاشتباك هي بطاقة "الخروج من السجن" في حالة حدوث شيء ما بشكل جانبي وقد يؤدي الانحراف عن هذه القواعد إلى تعرضك لقضايا المسؤولية القانونية وقد يكون هذا الأمر مدمراً لحياتك المهنية.

إذا تم ضبطك في عملية اختبار اختراق فكيف تتعامل مع هذا الموقف؟

كان لدي تجربة سابقة عند القيام باختبار اختراق بشكل مادي لأحد العملاء وأهمل الراعي إخطار أمن الموقع عن تواجدي وبعد الوصول إلى المرفق من خلال باب مفتوح، كنت أسير عبر المنشأة بقبعة صلبة لأبدو على أنني عامل إصلاح وقد تم القبض عليه من قبل أمن الموقع والشرطة المحلية ومما زاد الطين بلة، أن جهة الاتصال الخاصة بي لم تكن متاحة عندما اتصلوا لتأكيد أنني مصرح لي بإجراء اختبار الاختراق وبعد ساعتين اتصلت الجهة المسؤولة أخيراً وتم إطلاق سراحي.

ما هو أكبر مأزق أخلاقي واجهته أثناء عملك على هدف معين؟

أكبر مأزق أخلاقي واجهته هو التعثر في ذاكرة التخزين المؤقت للحساب أو السجلات المالية أو معلومات تحديد الهوية الشخصية في مكان لا ينبغي أن يكونوا فيه وتم إعلامي من قبل الراعي بعدم الكشف عن التفاصيل للأفراد المتأثرين حتى اكتمال العملية والتي قد تستغرق عدة أيام

بالنسبة لي، هناك بعض الاكتشافات التي تحظى بالأولوية وتحتاج إلى اتخاذ إجراء بشأنها على الفور ولا سيما عندما يتعلق الأمر بمعلومات التعريف الشخصية أو المعلومات المالية وفي هذه الحالة، كان الراعي يحاول إثبات نقطة لعضو آخر في الإدارة ولم يكن لديه أي اعتبار تقريباً لما تم اكتشافه.