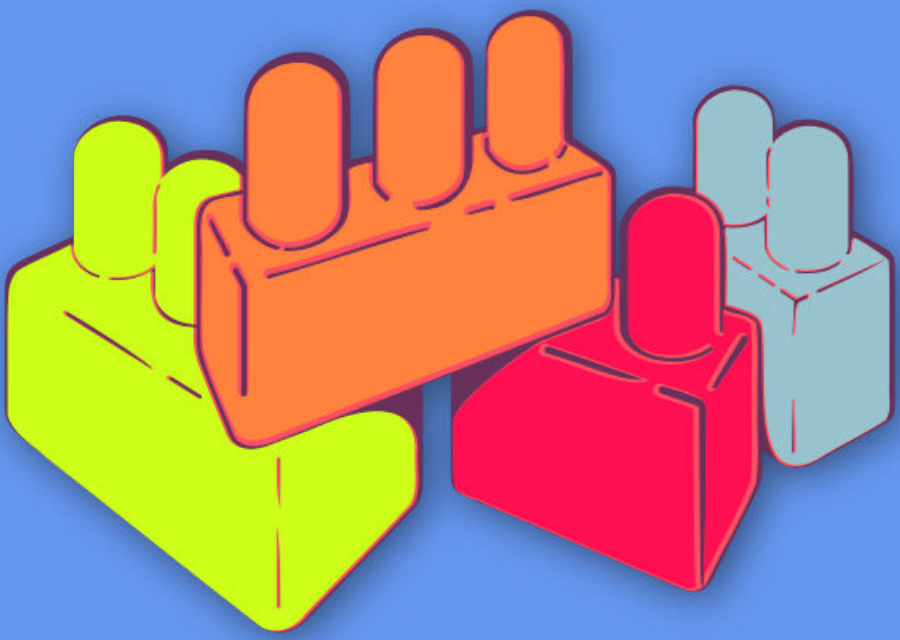

أسس الأمن الرقمي | الجولة الثانية

أسس الأمن الرقمي،الجولة الثانية

INSTITUTE FOR
WAR & PEACE REPORTING

© 2019– Institute For War And Peace Reporting

https://iwpr.net/

نَسب المُصنَّف - الترخيص بالمثل 4.0 دولي

https://creativecommons.org/licenses/by-sa/4.0/deed.ar

المحتويات

باب ١

التخزين والتشفير

- **الأهداف:** في هذه الجلسة، ستشددن على أهمية القيام بنسخ احتياطية للبيانات بشكلٍ دوري، وستناقشن كيفية منع التلاعب أو الوصول غير المسموح به لمعلومات المشاركات.
- **الطول:** 90 دقيقة
- **المعرفة المطلوبة:**
  - معرفة مفاهيم الأمن الرقمي الأساسية و/أوتدريب مسبق
  - تعريف بمسألة التشفير (التشفير)
  - كيفية حماية حاسوبكن (أسس الأمن الرقمي،الجولة الأولى)
- **جلسات/تمارين ذات صلة:**
  - كيفية حماية حاسوبكن[١]
  - الخصوصية[٢]
  - الحملات الآمنة على الإنترنت[٣]

---

[١] https://vrr.im/ac95
[٢] https://vrr.im/819e
[٣] https://vrr.im/8e6b

- تعريف بمسألة التشفير[٤]

- **المواد اللازمة:**
  - شرائح (فيها النقاط المفتاحية الواردة أدناه)
  - حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
  - نسخ مطبوعة عن نموذج النسخ الإحتياطي (أدناه)
  - مفاتيح يو إس بي أو نوع آخر من وسائط التخزين (لكل مشاركة)
- **التوصيات:** المشاركات في هذه الجلسة ستستخدمن إما برمجية "فيراكريبت" veracrypt أو "ماك كيبر" mackeeper (بحسب النظام التشغيلي الخاص بهن) للتدرّب على تشفير النسخ الاحتياطية للبيانات ووسائط التخزين – لتوفير الوقت، فكرن في الطلب من المشاركات تنزيل أي من هذه البرمجيات مسبقًا. بشكلٍ عام، ولا سيما للمبتدئات، لا ينصح بإجراء المشاركات لعملية تشفير شاملة للقرص الصلب على حاسوبهن الآن – عوضًا عن ذلك، يتوجب عليهن إختبار برمجيتي "فيراكريبت" أو "ماك كيبر" على وسيط تخزين خارجي (من قبيل مفتاح يو إس بي) باستخدام ملفات مزيّفة حضّرنها خصيصًا لهذه الجلسة. إذ حتمًا لا ترغبن في التعرّض لخطر فقدان إحدى المشاركات لإمكانية الوصول إلى أي بيانات خلال التدريب عن طريق الخطأ!

إدارة الجلسة

الجزء الأوّل – نسخ البيانات الاحتياطية والتخطيط

١. إسألن المشاركات – كم مرّة في السنة يقمن بنسخ احتياطية لملفاتهن؟ شاركن أمثلة عن الممارسات الفضلى في مجال إنشاء نسخ احتياطية للبيانات، من قبيل الإحتفاظ بالنسخة الاحتياطية في مكان آمن منفصل عن حاسوبهن، وإنشاء نسخ احتياطية لمعلوماتهن بشكلٍ دوري ومتكرر، بحسب للمعلومات التي يُنشأ لها نسخ احتياطية، والتفكير أيضًا في تشفير القرص الصلب أووسيط التخزين حيث سيقمن بتخزين البيانات.

[٤] https://vrr.im/f5d4

٢. شاركن مع المشاركات نموذج تنظيم النسخ الإحتياطي الوارد أدناه، وأطلبن منهن البدء بملئه بشكلٍ فرديّ. إشرحن للمجموعة أن الإستعانة به طريقة مفيدة لوضع سياسة شخصية خاصة بإنشاء نسخ احتياطية للبيانات – يمكنهن الإستعانة بهذا النموذج بعد التدريب، كمورد مفيد في متابعة مكان تخزينهن للبيانات وعدد المرّات التي يجب فيها إنشاء نسخ احتياطية للبيانات.

نموذج تنظيم النسخ الإحتياطي

- نوع المعلومات
- الأهمية/القيمة
- ما وتيرة إنتاجها أوتغييرها؟
- كم عدد المرات التي يجب فيها إنشاء نسخ احتياطية لها؟

الجزء الثاني – تشفير التخزين والنسخ الاحتياطية

٣. بعد أن تنتهي المشاركات من ملء نموذج تنظيم النسخ الاحتياطية، أطلبن منهن مراجعة أنواع المعلومات (إلى جانب أهميتها وقيمتها) الموجودة على لائحتهن مجددًا – أثناء قيامهن بذلك، أطلبن منهن التفكير في ما قد يحدث في حال وصلت هذه المعلومات إلى أحد خصومهن، أوفي حال فقدن هذه المعلومات كلها. ما أثر ذلك عليهن شخصيًا وعلى منظمتهن؟

٤. والآن، قدّمن مفهوم التشفير للمجموعة – إشرحن لهن أنهن على الأرجح يجدن التشفير مرات عدّة في حياتهن اليومية، فهو مستخدم بطرق مختلفة في أدوات ومنصات مختلفة. على سبيل المثال، يمكنكن الإشارة إلى أن "إيتش تي تي بي إس" هو نفسه شكل من أشكال تشفير البيانات "المتنقلة" (البيانات المنتقلة من النقطة "أ" إلى النقطة "ب") في حين أنهن في هذه الجلسة، ستناقشن تشفير البيانات "الثابتة" (أي البيانات المخزّنة في مكان واحد).

٥. ذكرن المشاركات بأنه طلب منهن تنزيل إما برمجية "فيراكريبت" أو برمجية "ماك كيبر" على حواسيبهن. إمنحن المشاركات الوقت اللازم لتثبيت هذه الأدوات وإختبارها،

بواسطة وسيط تخزين خارجي (من قبيل مفاتيح يو إس بي) وملفات مزيّفة حضّرنها خصيصًا لهذه الجلسة. لا ينصح بإجراء عملية تشفير شاملة لقرص الحاسوب الصلب الآن، لا سيما للمشاركات المبتدئات - إذ حتمًا لا ترغبن في التعرّض لخطر فقدان إحدى المشاركات لإمكانية الوصول إلى أي بيانات خلال التدريب عن طريق الخطأ!

المراجع

- https://securityinabox.org/en/guide/veracrypt/windows/
- https://securityinabox.org/en/guide/veracrypt/mac
- https://securityinabox.org/en/guide/veracrypt/linux

باب ٢

لنعد إلى خانة الصفر(إعادة الضبط)!

- **الأهداف:** تعزز هذه الجلسة فكرة أنه "ليس للأدوات والتكنولوجيا سطوة سحرية خارقة علينا!" ستقدن المشاركات هنا في عملية سترفع من مستوى قدراتهن هي عملية "البدء من خانة الصفر" عبر إعادة ضبط أجهزتهن من أجل البدء بإستخدامها وكأنها جديدة.
- **الطول:** 90 دقيقة
- **الشكل:** جلسة
- **مستوي المهارة:** متوسط
- **المعرفة المطلوبة:**
  - معرفة مفاهيم الأمن الرقمي الأساسية و/أوتدريب مسبق
  - تعريف بمسألة التشفير (التشفير)
  - التخزين والتشفير (أسس الأمن الرقمي،الجولة الثانية)
- **جلسات/تمارين ذات صلة:**
  - وجهات النظر الشخصية حيال الأمن[١]
  - البرمجيات الخبيثة والفيروسات[٢]

---

[١] https://vrr.im/9339
[٢] https://vrr.im/47e5

- الخصوصية[٣]
- المزيد من الهويات الإلكترونية![٤]
- التخزين والتشفير[٥]

• **المواد اللازمة:**
- شرائح (فيها النقاط المفتاحية الواردة أدناه)
- مفاتيح يو إس بي مجهّزة بنظامي تايلز وأوبونتو Ubuntu القابلين لإعادة التشغيل.

• **التوصيات:** فكرن في جلب مفاتيح يو إس بي مجهّزة بنظام تشغيل لكل مشاركة على أن يحتفظن بها؛ وإلّا جهزن حاسوبًا لتتدرب المشاركات عليه (أو إثنين في حال عرضتن نظامي تايلز وأوبونتو التشغيليين) - وحتى لو كان الهدف من النشاط تشغيل نظامي تايلز أو أوبونتو من مفتاح يو إس بي مجهّز بنظام تشغيل، عوضًا عن تثبيته، قد لا تشعر بعض المشاركات بالإرتياح لإستعمال حاسوبهن الخاص لإختباره. من الممكن أيضًا تغيير ذلك بحيث يسهل إدخاله إلى أي جلسة مخصصة لناشطات لا يخفن من شيء في ورشتكن التدريبية، يرغبن في تغيير الأنظمة التشغيلية بالكامل من ماك أو ويندوز إلى نظام كنظام أوبونتو من شركة لينوكس linux.

إدارة الجلسة

الجزء الأوّل - تبديد الخرافات

الجزء الأوّل - تبديد الخرافات

١. إبدأن الجلسة بشرح الهدف من هذه الجلسة: إعادة تأكيد قدرة الإنسان على التحكم بالتكنولوجيا، وتبديد فكرة أن الأجهزة الرقمية لها "قوى خارقة" تسيطر من خلالها على مستخدميها. في حال قدمتن جلسة وجهات النظر الشخصية حيال الأمن للمشاركات، يمكنكن تذكيرهن بما يلي من التأكيدات الختامية:

[٣] https://vrr.im/819e
[٤] https://vrr.im/e9f7
[٥] https://vrr.im/0ccc

ليس للأدوات والتكنولوجيا سطوة سحرية خارقة علينا! نحن من يقرر ما يمكنها الوصول إليه، وفي حال طرأ أي حادث، يمكننا دومًا إعادة ضبطها!

الجزء الثاني – ما الذي نعنيه فعليا بإعادة الضبط؟

٢. كررن للمجموعة هذا التأكيد من المرحلة السابقة، وشددن على الجملة الأخيرة منه "يمكننا دومًا إعادة ضبطها" – ماذا يعني ذلك؟ إشرحن لهن ذلك عبر تقديم السيناريو التالي:

لعلكن في إحدى محطات مسيرتكن مع الأمن الرقمي، شعرتن أنكن تقمن بكل شيء بالطريقة الخاطئة.

تنظرن إلى حاسوبكن – هو مليء بالبرمجيات المقرصنة والأفلام والبرامج التلفزيونية المنزّلة عبر منصة "تورينت" والملفات الأخرى المبعثرة التي لا تتذكرن حتى أنكن نزّلتنها.

إستخدمتن مفاتيح اليو إس بي من دون تمييز – على حاسوبكن المحمول، وعلى حواسيب وآلات طباعة في مقاهي إنترنت، وربما لا تقمن دائمًا بإخراجها بالطريقة الصحيحة حين تنتهين من استخدامها.

ربما إنفصلتن مؤخرًا عن شخصٍ ما تعرفن جيّدًا أنه/ها كان يفتح حاسوبكن في غيابكن – وربما قام/ت بتخمين كلمة السرّ أو حتى أعطيتنه/ها إياها بأنفسكن.

والآن، تشعرن بأنكن فقدتن السيطرة – من يعرف ما نوع الفيروسات الموجودة على قرصكن الصلب، أو من يا ترى له القدرة على الوصول إلى معلوماتكن؟

ولكن على فكرة، ذلك ليس مشكلة كبيرة! لم يفت الأوان بعد لفتح صفحة جديدة. هل ترغبن في فتح صفحة جديدة؟ هذه الجلسة معدّة خصيصًا لكنّ إذًا!

٣. والآن، بعد أن قرأتن السيناريو الوارد أعلاه لتحديد السياق، يمكنكن شرح ما يعني مصطلح إعادة الضبط في هذا السياق: أي البدء من خانة الصفر عبر إعادة ضبط جهازكن أو حاسوبكن إلى حالته وإعداداته الأصليّة، وبالتالي منح أنفسكن "صفحة بيضاء" لمسيرة الأمن الرقمي الخاصة بكن.

لا تنسين تذكير المشاركات أن هذه الجلسة ستفسّر لهن كيفية إجراء عملية إعادة ضبط – لن يتوجب عليهن إجراء عملية إعادة ضبط خلال الجلسة، أو حتى خلال التمرين. فقد تترتب نتائج سيئة جدًا عن عملية إعادة الضبط في حال لم تكن المشاركات جاهزات لها، أو في حال لم يقمن بإجراء نسخ إحتياطية لبياناتهن مؤخرًا – وقد يحتجن لحواسيبهن المحمولة بما أنهن يرغبن حاليًا بالمحافظة على قدرتهن على الوصول إلى بياناتهن إلى أن يصبحن جاهزات أكثر لإجراء عملية إعادة الضبط. ولكن، خلال هذه الجلسة ستتاح للمشاركات فرصة التدرّب بواسطة أنظمة تشغيل بديلة على حواسيبهن، وهذا ما يشكّل محطة تحضيرية مهمة في حال قررن إجراء عملية إعادة ضبط لاحقًا.

الجزء الثالث – التحقق: هل تحتجن لإنشاء نسخ إحتياطية؟

٤. يفضّل أن تكنّ قد قدمتن قبل الآن جلسة التخزين والتشفير للمشاركات بما أنها تتناول نقاطًا مهمة في مجال إنشاء نسخ احتياطية للبيانات. بكل الأحوال، قبل أن تبدأن بالجزء الخاص بالممارسة التطبيقية من هذه الجلسة، قمن بعملية تحقق سريعة مع المجموعة حول إنشاء نسخ إحتياطية لبياناتهن.

إختياري: كتذكير سريع بجلسة التخزين والتشفير، إسألن المشاركات - كم مرّة في السنة يقمن بنسخ إحتياطي لملفاتهن؟ شاركن أمثلة عن الممارسات الفضلى في مجال إنشاء نسخ إحتياطية للبيانات، من قبيل الإحتفاظ بالنسخة الإحتياطية في مكان آمن منفصل عن حاسوبهن، وإنشاء نسخ إحتياطية لمعلوماتهن بشكلٍ دوري ومتكرر، بحسب المعلومات التي يُنشأ لها نسخ إحتياطية، والتفكير أيضًا في تشفير القرص الصلب أو وسيط التخزين حيث سيقمن بتخزين البيانات.

الجزء الرابع – إعادة الضبط وإعادة التشغيل Resetting & Rebooting

٥. قبل البدء بالجزء الخاص بالممارسة التطبيقية من هذه الجلسة، لابد من تناول مسألة مهمة هي العلاقة بين إعادة التشغيل وإعادة الضبط فربما إستخدم هذان المصطلحان من

دون تمييز بينهما طوال هذه الجلسة:

يدلّ هذان المصطلحان إلى عمليتين تشبه بعضهما إلى حدٍ كبير بالمعنى العام، ولكن ذكرن المشاركات أن كلمة "إعادة الضبط" تستخدم هنا للدلالة على مفهوم "فتح صفحة جديدة" في سياق هذه الجلسة. عملية إعادة التشغيل هي عملية تقنية تجريها حواسيبهن خلال عملية إعادة فتحها؛ هي عملية مهمة أيضًا يجب فهمها من أجل الممارسة التطبيقية لأنظمة التشغيل البديلة التي ستجرى في الجزء التالي من الجلسة.

٦. لمزيد من التوضيح للفكرة الواردة أعلاه، قدمن أنظمة تشغيل تايلز وأوبونتوإلى جانب تقديم بعض المعلومات التقنية القيّمة للمشاركات التي ستكون مفيدة في الجزء التالي من الجلسة. إشرحن ما الذي يجعل من تايلز وأوبونتو نظامين بديلين عن أنظمة التشغيل الأخرى مثل ماك أو إس ووينـدوز – في هذه الجلسة، سيركز الجزء الخاص بالممارسة التطبيقية على تشغيل هذين النظامين التشغيليين من مفتاح يو إس بي.

الجزء الخامس – الأنظمة التشغيلية الحيّة

٧. قد يطرح عليكن سؤالاً من قبيل: كيف يمكننا إستخدام النظام التشغيلي الجديد على حواسيبنا المحمولة من دون التخلّص من الذي نستخدمه الآن؟ ماذا سيحدث لبياناتنا؟ عليكن الآن إغتنام هذه الفرصة لشرح بعض المصطلحات للمشاركات قد تساعدهن على فهم كيفية عمل تايلز وأوبونتو في سياق هذه الجلسة بشكلٍ أوضح:

النظام الحي Live System

النظام الحيّ هو نظام تشغيلي يمكن تشغيله مباشرة من وسيط تخزين خارجي مثل مفتاح يو إس بي أو شريحة ذاكرة. نظام تايلز التشغيلي هو مثال عن الأنظمة الحيّة؛ ومن الممكن إعداد أوبونتوللعمل كنظام حيّ، وهو "نسخة" أخرى عن النظام التشغيلي المستند إلى نظام لينوكس الذي يستعين به نظام تايلز.

لينوكس Linux

لينوكس نظام تشغيلي شبيه بنظامي ويندوز وماك، إلا أن الفرق الرئيسي بينه وبينهما هو أنه موزع كبرمجية مجانية ومفتوحة المصدر. ولذلك، تتوفر نسخ مختلفة كثيرة مستندة إلى نظام لينوكس – نظام ديبيان Debian، هو إحدى النسخ الأكثر شعبية وهو يشكّل أساس نظام تايلز.

الجهاز القابل للتشغيل Bootable Device

أجهزة التشغيل (أو القابلة للتشغيل) هو جهاز أو قرص يمكن للحاسوب تحميل ملفات منه للتمكن من العمل. على سبيل المثال، على معظم الحواسيب يعتبر القرص الصلب جهاز التشغيل الذي يتم من خلاله تحميل نظام التشغيل (مثل ويندوز) عند تشغيل الحاسوب. بالإضافة إلى الأقراص الصلبة، تعتبر الوسائط كالأقراص المدمجة CD وأقراص الدي في دي DVD وشرائح الذاكرة ومفاتيح اليو إس بي من الأجهزة القابلة للتشغيل.

نظام الإدخال والإخراج الأساسي (Basic Input/Output System Bios)

نظام الإدخال والإخراج الأساسي BIOS هو البرمجية الأولى التي تشغلها معظم الحواسيب حيت يتم تشغيلها. يستخدم هذا النظام لإجراء عمليات إختبار ذاتية على الأنظمة والأجهزة لضمان عملها بشكلٍ سليم، ومن أجل تفعيل تسلسل التحميل للبرمجيات (كالأنظمة التشغيلية) الموجودة على الأجهزة القابلة للتشغيل المتوفرة. يتمتع نظام الإدخال والإخراج بواجهة تفاعلية، ولكن لا يمكن للمستخدمين الوصول إليها إلا إذا قاموا بخطوة محددة خلال إقلاع الجهاز للوصول إليه مباشرة.

تسلسل التشغيل

تسلسل التشغيل، الذي يمكن الوصول إليه من خلال نظام الإدخال والإخراج (أو واجهة البرنامج الثابت الممتد UEFI) أثناء إقلاع حاسوبٍ ما، هو لائحة بالأجهزة القابلة للتشغيل على حاسوبٍ ما – يستخدم لتحديد التسلسل الذي يحاول الحاسوب وفقه تحميل المعلومات من هذه الأجهزة. عادةً القرص الصلب في الحاسوب هو الجهاز الأوّل في تسلسل التشغيل، ومنه يتم تحميل نظام التشغيل. ولكن من الممكن تغيير تسلسل التشغيل ليُحمّل معلومات من أجهزة خارجية قابلة للإزالة أوّلاً كأقراص الدي في دي أو مفاتيح اليو إس بي.

الجزء السادس – الممارسة التطبيقية

٨. للبدء بالجزء المخصص للممارسة التطبيقية من هذه الجلسة، قسمن المشاركات إلى مجموعتين على الأقل. قدمن لكل مجموعة حاسوبًا ليجربن عليه تشغيل نظام أوبونتو أو تايلز من مفتاح يو إس بي معدّ مسبقًا؛ أو، في حال توفر لديكن العدد الكافي من مفاتيح اليو إس بي المعدّة مسبقًا لكل المشاركات، عندها سيتمكنّ من التدرّب كل واحدةٍ على حدة (في هذه الحالة، ستقمن بجعل الجميع يتدربن على إستخدام إما نظام تايلز وإما نظام أوبونتو)

٩. على حاسوبكن المحمول، وبواسطة جهاز عرض، وجهن المشاركات عند إجرائهن لعملية إعادة تشغيل حواسيبهن وإطلاق نظام تايلز/أوبونتو خلال تسلسل تشغيل نظام الإدخال والإخراج. وأثناء قيامكن بذلك، إحرصن على شرح الفوارق بين نظامي تايلز وأوبونتو لكي تفهم المجموعة بشكلٍ أفضل كيفية استخدامها في عملية "إعادة الضبط" الخاصة بهن.

١٠. إختتمن الجلسة بمناقشة كيف يمكن أن تكون عملية إعادة الضبط بواسطة تايلز أو أوبونتو خيارًا لفتح "صفحة جديدة" على حواسيب المشاركات في حال التعرّض لهجوم برمجيات خبيثة أو أي فقدان آخر للسيطرة، ولكن إحرصن أيضًا على ذكر أنواع أخرى

من الهجمات التي لا ينفع فيها هذا الحلّ بشكلٍ فعال، كالعنف على الإنترنت.

المراجع

- https://tails.boum.org/
- http://www.ubuntu.com