مقدمة في الأمن السيبراني

مدخل إلى الأمن السيبراني و الشبكات و أنظمة التشغيل

هذه المادة هي نتاج عدة أشهر من البحث كان الدافع وراءها الحيرة
التي واجهتها حينما قررت الدخول في مجال الأمن السيبراني حيث
لم أجد مرجعاً واضحاً يتطرق الى هذا الموضوع بشمولية كاملة.

إذا كنت تريد تطوير الكتيب أو لديك ملاحظات او اسئلة فراسلني على :

الفهرس

المقدمة

بسم الله الرحمن الرحيم

هذه المادة موجة للمتخصصين في المجال التقني أو من يريد دخول مجال الأمن السيبراني من الناحية التقنية لا الإدارية أو الأكاديمية أو غيرها، إنما هو لمن يريد أن يتخصص في الناحية الفنية التطبيقية في مجال الأمن السيبراني حيث أنه يحتوي على دراسة الأمور الفنية و إرشادات لكيفية البدء في بعض التخصصات في الأمن السيبراني و كيفية الوصول إلى مدخل التخصص بمقدمة يسيرة مناسبة للمبتدئين .. أما التخصصات الإدارية مثل الحوكمة و إدارة المخاطر و ما إلى ذلك.. فهذه التخصصات لم يتم التطرق لها بشكل مباشر و إنما تم ذكر بعض الأمور عنها.

تنويه : مجمل محتويات هذه المادة هو مما جمع أو ترجم من مقالات موجودة .. و هو نتاج بحث و ليس من تأليفي، و ما كتبته بنفسي قليل إذا ما تم مقارنته بالمنقول و المترجم .. و هذه المادة هي خلاصة تساؤلات و بحوث و إستشارات امتدت إلى ما يقارب عدة أشهر.

تنويه : ستحتاج منك قراءة هذه المادة و الإطلاع على محتوياتها من (مقالات و مقاطع فيديو و صور) إلى عدة أيام .. لكن اقترح أن تأخذ تصور عام عن الماده ثم تبدأ فيها من البداية و تأخذ وقتك في القراءة و البحث و التعلم.

بذل القائم على هذا العمل أقصى جهوده لتحقيق مستوى عالٍ من الجودة، إلا أنه لا يتحمل أي مسؤولية و لا يوفر أيّ ضمانات صريحة أو ضمنية تجاه ما قد ينجم عن استخدام أو سوء استخدام ما ورد في هذه المادة.

هذا كان اجتهادي فإن أصبت فمن الله و إن أخطأت فمن نفسي و الشيطان.

و الله ولي التوفيق

Creative Commons

يخضع هذا الكتاب لرخصة المشاع البداعي (creative commons) نَسب المُصنَّف ، غير تجاري ، الترخيص بالمثل 4.0 دولي (CC BY-NC-SA 4.0) لك مطلق الحرية في:

- المشاركة — نسخ وتوزيع ونقل العمل لأي وسط أو شكل.
- التعديل — المزج، التحويل، والإضافة على العمل.

بموجب الشروط التالية:

نَسب المُصنَّف — يجب عليك نَسب العمل لصاحبه بطريقة مناسبة، وتوفير رابط للترخيص، وبيان إذا ما قد أُجريت أي تعديلات على العمل. يمكنك القيام بهذا بأي طريقة مناسبة، ولكن على ألا يتم ذلك بطريقة توحي بأن المؤلف أو المرخِّص مؤيد لك أو لعملك.

غير تجاري — لا يمكنك استخدام هذا العمل لأغراض تجارية.

الترخيص بالمثل — إذا قمت بأي تعديل، تغيير، أو إضافة على هذا العمل، فيجب عليك توزيع العمل الناتج بنفس شروط ترخيص العمل الأصلي.

منع القيود الإضافية — يجب عليك ألا تطبق أي شروط قانونية أو تدابير تكنولوجية تقيد الآخرين من ممارسة الصلاحيات التي تسمح بها الرخصة.

أهلا بك.. أتمنى أن تكون هذه المادة ✍ خفيفةً عليك ..

و لكن قبل أن ننطلق في المسار التقني ..

أريد إثراء معلوماتك قليلاً عن الأمن السيبراني 🕮 ..

ألم تتسائل ما هو الأمن السيبراني؟... و ما فائدته و ما تاريخه؟... و ما هي أبعاده السياسية؟ .. و كيف أستفيد منه 😐 ؟؟ و الكثيييير الكثير من الأسئلة التي سنجيب عليها في هذه المادة بإذن الله.

مفهوم الأمن السيبراني و تاريخه و علاقته بالسياسة تاريخياً في هذا المقال استمتع يا صديقي

أتمنى بأن المقال لم يكن طويلا عليك ⏳ .. دعنا لا نطيل الحديث و نبدأ في القسم الأخر..

الأمن السيبراني تقنياً..

قد يعتقد الكثير بأن تخصص أمن المعلومات هو فقط للمخترقين و الإختراقات مثل الأفلام التي كلها إثارة .. لكن يجب أن تعلم أن هذا التخصص كبير جداً و يندرج تحته العديد من التخصصات مثل : اختبار الإختراق و التحليل الجنائي الرقمي.. و سوف نتعرف في هذه المادة على بعض التخصصات المندرجة تحت تخصص الأمن السيبراني

نبدأ هنا > بعرض شرائح عن "مفهوم الأمن السيبراني و عناصر أمن المعلومات و أنواع الهجمات و البرمجيات الخبيثة و التشفير" .. من اعداد د.أيمن الحربي (الإطلاع عليه مهم)

كما أريد أن أضيف إلى معلوماتك أن الأمن السيبراني ليس كياناً قائماً بذاته، و إنما هو عبارة عن مجموعة من الإجراءات و العمليات التي تستخدم لحماية أشياء كالشبكات و البرمجيات و أنظمة التشغيل و غيرها.. و بهذا نعرف أنه من البديهي أن يكون تعلم الأمن السيبراني مرحلة ثانية بعد دراسة أحد مجالات الحاسب (مثل : علوم الحاسب ، هندسة الحاسب ...) و هذا يدعونا للحديث عن المسارات التقنية للأمن السيبراني من حيث وظائفها.

ينقسم مجال الأمن السيبراني إلى ثلاث مسارات رئيسية

- **Offense** > و يشمل إختبارالإختراق بأنواعه (**Pen Test**)
- **Defense** > و يشمل أمن الشبكات & إدارة الأنظمة و الخوادم و قواعد البيانات (**Network Security & Administration**)
- **Analysis** > و يشمل التحليل الجنائي الرقمي و الاستجابة للحوادث & تحليل البرمجيات الخبيثة و الهندسة العكسية (**Digital Forensic / Incident Response (DFIR)** & **Malware Analysis / Reverse Engineering**)

هناك أكثر من منهجية لمساعدة المبتدئين في الدخول إلى مجال الأمن السيبراني، احرص دائماً على اختيار المنهجية القائمة على الأساس السليم و من الأمثلة على ذلك؛ سلسلة مقاطع على اليوتيوب للمهندس Muhammad Alharmeel > إبدأ بالمقطع الثاني أولاً

في هذه المادة، سنعتمد منهجية المراحل الثلاث:-

- المرحلة الأولى : أساسيات علوم الحاسب
- المرحلة الثانية : أساسيات الأمن السيبراني
- المرحلة الثالثة : التخصص في أحد مسارات الأمن السيبراني

لكن قبل أن نبدأ يجب التنويه على أن اللغة الأنجليزية مهمة جداً في المجال التقني عموماً و في مجال الأمن السيبراني خصوصاً، لإحتياج المبتدئ في المجال إلى كتابة التقارير و القراءة والبحث في الأنترنت و ما إلى ذلك من أمور مهمة.
من المصادر الجيدة لتعلم اللغة الأنجليزية اكاديمية English Place

عزيزي المبتدئ: الشهادات هي مجرد جسر عبور للمقابلة الوظيفية و ستسأل في المقابلة عن ما تعرفه لقياس مهاراتك فلا تحرج نفسك (لا تجمع شهادات بدون معرفة)

التفاصيل المتعلقة باي شهادة أو دورة لن يتم ذكرها في هذه المادة، و يمكن لمن يرغب معرفتها و ضع اسم الشهادة/الدورة في محركات البحث و الحصول على االعديد من النتائج.

المرحلة الأولى : أساسيات علوم الحاسب الأساسية

إذا كانت مهارتك في استخدام الكمبيوتر ضعيفة، فيجب عليك تعلم أساسيات الحاسب، كأن تدرس محتوى تعليمي مخصص للمبتدئين (مثل دورة: A+) قبل أن تبدأ في أي شيء اخر.

البرمجة؛ مثل لغات : Java , C++ , C , Python , JS , PHP (قد تحتاج إلى أكثر من لغة و قد لا تحتاج إلى أي منها !!)

- أساسيات بعض أنظمة التشغيل الدارجة (Linux & Windows) مثل كورسات: MCSA , Linux+
- أساسيات الشبكات؛ مثل كورسات : CND , CCNA , Network+

بعض الشهادات المذكورة حتى الآن ليس لها قيمتة تذكر في سوق العمل كشهادة احترافية و إنما تم ذكرها للفائدة الكبيرة الموجودة في مناهجها، كاحتوائها على أساسيات و تدرج مناسب للمبتدئين، لكن هذا كله لا يفيد إذا لم يصحب بتطبيق عملي !!

البرمجة :-

قد تتسائل .. لماذا أحتاج إلى تعلم البرمجة في مجال الأمن السيبراني؟ و هل من الممكن العمل في المجال دون تعلمها؟ إن كان الأمر كذلك، فأي لغةٍ أتعلم ؟ ستجد جواباً لهذه التساؤلات في مقال:" البرمجة و أهميتها في أمن المعلومات" للأستاذ تكناوي.

لمن يرغب في البدء في تعلم البرمجة، تحتوي منصة يوتيوب والعديد من المنصات الأخرى على محتوى رائع (باللغة الإنجليزية) لكن المحتوى العربي فيها متواضع. إذا كان المتعلم لا يجيد اللغة الإنجليزية، فمنصة فلكس كورسز تقدم محتوى (يعد من الأفضل في الساحة العربية حتى تاريخ هذه المادة).

يقسم المختصون في مجال الأمن السيبراني حسب حاجتهم إلى البرمجة إلى ثلاث أقسام :

1. مستخدمي الأدوات: هؤلاء لا يحتاجون إلى تعلم البرمجة، فقط يحتاجون إلى إتقان كيفية استخدام الأدوات.
2. معدلي الأدوات: هؤلاء يحتاجون معرفه جيدة أو متوسطة في البرمجة، تمكنهم من التلاعب بالنصوص البرمجية لتتوافق مع حاجتاهم.
3. صانعي الأدوات: هؤلاء يحتاجون معرفة ممتازة في البرمجة، لإنشاء أدوات جديدة لأهداف محددة.

أنظمة التشغيل :-

ما هي أنظمة التشغيل ؟ موقع سلامتك ويكي فصل في الشرح عن أنظمة التشغيل و تاريخها و بعض أنواعها في بطريقة مميز جداً >> هنـا <<

لكن قد يتبادر إلى ذهنك سؤال.. أي نظام تشغيل هو الأفضل ؟ و قد يفيدك النقاش هنا في الإجابة عن سؤالك.. و إذا أردت معرفة سبب انتشار نظام ويندوز، فإليك النقاش التالي..

و لكن لا تنسى أنه من الممكن أن تستخدم أكثر من نظام تشغيل في كمبيوتر واحد بعدة طرق مختلفة .. لأنك **غالباً ستحتاج إلى معرفة استخدام و إدارة أكثر من نظام في مجال الأمن السيبراني.**

مصادر عربية لتعلم نظام التشغيل GNU/Linux

مدونة أخونا أبو تيم

من ممكن أن تتعلم استخدام وإدارة سيرفرات GNU/Linux في فلكس كورسز (مدفوع لكن أنصح به)

من المهم أن تتعلم **shell scripting** و هذه دورة مقدمة من الأستاذ : عبدالمجيب الحميد

تنويه : يعد التمكن من استخدام و إدارة نظام GNU/Linux من أهم الأمورالتي يحتاجها المتخصص في مجال الأمن السيبراني. في بداية التعلم، يفضل البدء باستخدام التوزيعات البسيطة المناسبة للمبتدئين قبل الانتقال إلى توزيعات GNU/Linux الإحترافية مثل (Kali أو parrot).

* بالرغم من أهمية تعلم نظام GNU/Linux إلا أنه في بعض الحالات القليلة قد يكفي المتخصص بنظام ويندوز ☺

الشبكات :-

في هذه الروابط، ستجد إجابة هذا السؤال "من أين ابدأ وكيف أبدأ في مجال الشبكات ؟" (بعض المعلومات في هذا المقطع غير محدثه) المقاطع : 1 2 3 4 سلسلة مهمة جداً، يشكر عليها المهندس عادل الحميدي، في هذه المرحلة، **يكفي فقط الاطلاع** على هذه الشهادات الموجودة في المقاطع السابقة.

للبدء في المجال، ينصح بشدة مشاهدة أحد دورات **Network+** و **CCNA** في اليوتيوب مع التطبيق في أحد برامج المحاكاة مثل: **Packet Tracer** (قد يكون اكثر مناسبة للمبتدئين) أو **Gns3** أو حتى **eve-ng** (ابحث في اليوتيوب عن طريقة استخدام البرنامج) و من الممكن أن تساعدك سلسلة الفيديوهات هذه على الممارسة العملية.

إن كان لديك القدرة المادية فبإمكانك بناء المعمل الخاص بك (Switch + Router + Firewall)

بعض المصادر المفيدة للبدء في دراسة الشبكات :-

- قناة المهندس : **حسن صالح** مفيدة جداً في مجال الشبكات.
- ملخص أساسيات الشبكات من إعداد : **ماتركس**.
- شرائح عرض تحتوي على بعض المعلومات عن بروتوكول الـ **HTTP** و أهميته في عالم الويب من إعداد : **هيثمان الحربي**.

هذه فقط بعض الأساسيات و لا تغني عن باقي العلوم الموجودة في مجال الحاسب عموماً مثل التشفير و الخوارزميات و هيكلة البيانات و قواعد البيانات و ما إلى ذلك من أمور لا يتسع المجال لذكرها و لذا اكتفيت بذكر الأشياء التي لابد من تعلمها (برمجة ، أنظمة تشغيل ، شبكات).

بعض الشهادات المذكورة حتى الآن ليس لها قيمتة تذكر في سوق العمل كشهادة احترافية و إنما تم ذكرها للفائدة الكبيرة الموجودة في مناهجها، كاحتوائها على أساسيات و تدرج مناسب للمبتدئين، لكن هذا كله لا يفيد إذا لم يصحب بتطبيق عملي !!

المرحلة الثانية : أساسيات الأمن السيبراني

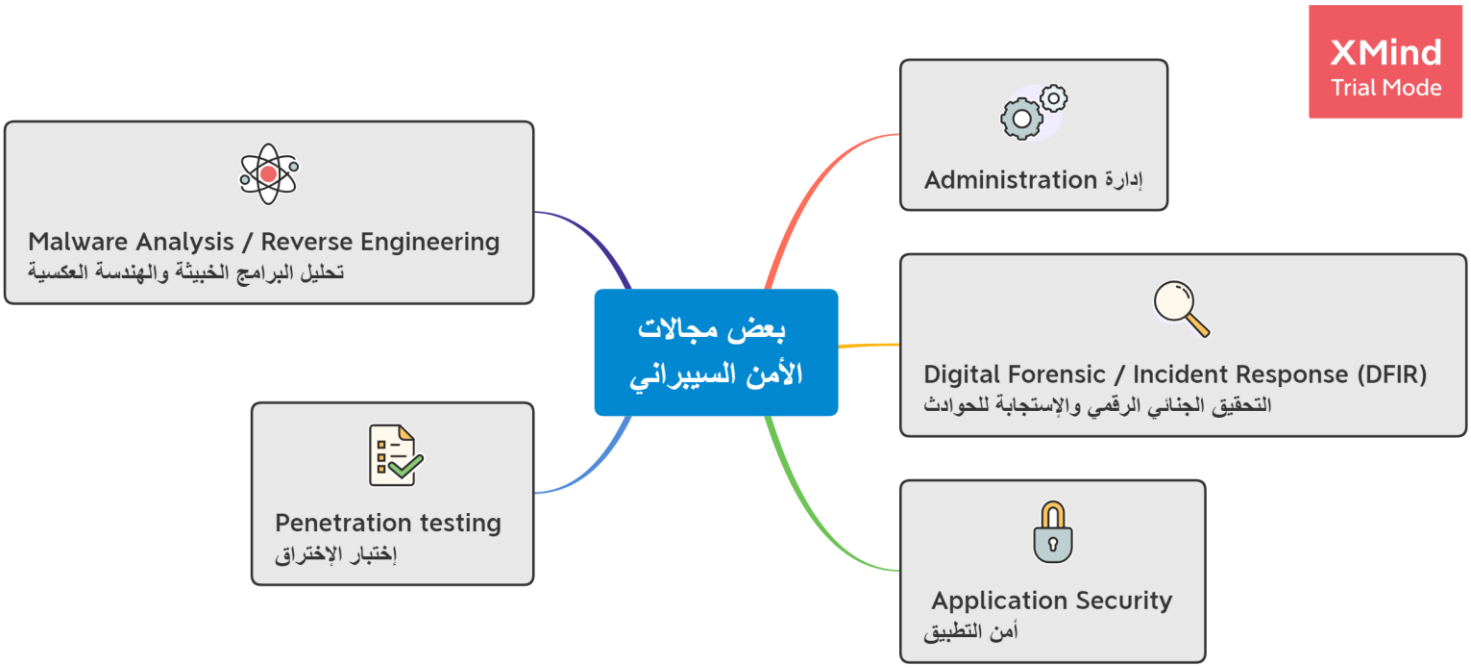
من المهم قبل التخصص في أحد مجالات الأمن السيبراني أن تأخذ بعض الدورات العامة لتكون ملماً بالمفاهيم الأساسية التي توسع معرفتك و تيسر لك التقدم مستقبلًا بإذن الله.. مثل كورسات : **CSCU** , **Security+** أو حتى **GSEC**

إذا كنت في هذه المرحلة تبحث عن وظيفة سريعة في المجال، فمن الممكن أن تكون الشهادات التالية مفيدة لك : **C|EH** و **CISSP** و **CISM** ، نظراً للاهتمام الذي توليه بعض أقسام الموارد البشرية في بعض الشركات بهذه الشهادات.

من المهارات التي يحتاجها المبتدئ والمتمرس في مجال الأمن السيبراني: مهارات البحث كيف و أين وعمّا تبحث و متى يجب أن توقف البحث، فمثلاً، مختبر الإختراق يجمع المعلومات عن الهدف و بقدر جمعه تتحدد سهولة الإختراق أو حتى إمكانيته، أيضاَ، باستخدام مهارات البحث يكون المحلل الجنائي الرقمي قادر على الوصول إلى تفاصيل قد يعجز عن الوصول إليها إن لم يتقن هذه المهارة.

المرحلة الثالثة : التخصص في أحد تخصصات الأمن السيبراني

(هذه ليست جميع التخصصات و لكن المشتهرمنها، يمكن الاطلاع على تلخيص إطار سيوف صفحة 34 أو إطار سيوف السعودي للمزيد من التفاصيل)



الحقيقة أن كل تخصص يستحق إفراد كتاب خاص به و لكن المقام لا يسمح بالإطالة لذا سنأخذ نبذة عن كل تخصص بشكل مختصر

في هذه المرحلة (**المرحلة الثالثة**) بعض الروابط و الشروحات ستكون باللغة الأنجليزية لشح المراجع العربية، و هنا يتبين لنا ضرورة أن يكون الفرد قادراً على ممارسة اللغة الأنجليزية في هذة المرحلة من التخصص.

في الفترة التي ستحتاجها لتعلم الأساسيات من الممكن أن تكون قادراً على تحديد المجال المناسب لك (و إن لم يكن أحد الخمس مجالات السابق ذكرها)

Administration

(إدارة)

5	4	3	2	1

مستوى الصعوبة

مسؤول الأمن (**security administrator**) هو الشخص المسؤول عن فريق الأمن السيبراني. وعادة ما يكون مسؤول عن تثبيت و إدارة وصيانة الحلول الأمنية للمؤسسات.

يقوم مسؤول الأمن أيضًا بكتابة وثائق سياسات الأمان والتدريب حول الإجراءات الأمنية للزملاء، كما أنه مسؤول عن النظام بشكل عام.

عندما يقوم مسؤولي الشبكة و الأنظمة بإعداد النظام و صيانته ، يتراجع مسؤولي الأمان خطوة إلى الوراء للحصول على رؤية شاملة للأمان. بدلاً من التركيز على الأجهزة و البرامج، فإنهم يعملون للدفاع عن النظام ككل و الحفاظ عليه آمناً من التهديدات.

قد يكون من مهام مسؤول الأمن الأعمال التالية:

- الدفاع عن الأنظمة ضد الوصول غير المصرح به و التعديل و التدمير.
- مسح و تقييم الشبكة بحثًا عن نقاط الضعف.
- مراقبة حركة مرور الشبكة بحثًا عن نشاط غير عادي.
- تكوين و دعم أدوات الأمان مثل جدران الحماية و برامج مكافحة الفيروسات و أنظمة إدارة الترقيع.
- تنفيذ سياسات أمن الشبكة و أمن التطبيقات و التحكم في الوصول و حماية بيانات الشركة.
- تدريب زملائه الموظفين على الإجراءات الأمنية و رفع وعيهم الأمني.
- تطوير و تحديث الأعمال و بروتوكولات التعافي من الكوارث بإستمرار.

المرجع : مدونة موقع CompTIA

من أقسام التخصص :-

- إدارة **أنظمة التشغيل:**
  - لينكس.
  - ويندوز.
- إدارة **الشبكات.**
- إدارة **السيرفرات.**
- إدارة **قواعد البيانات.**

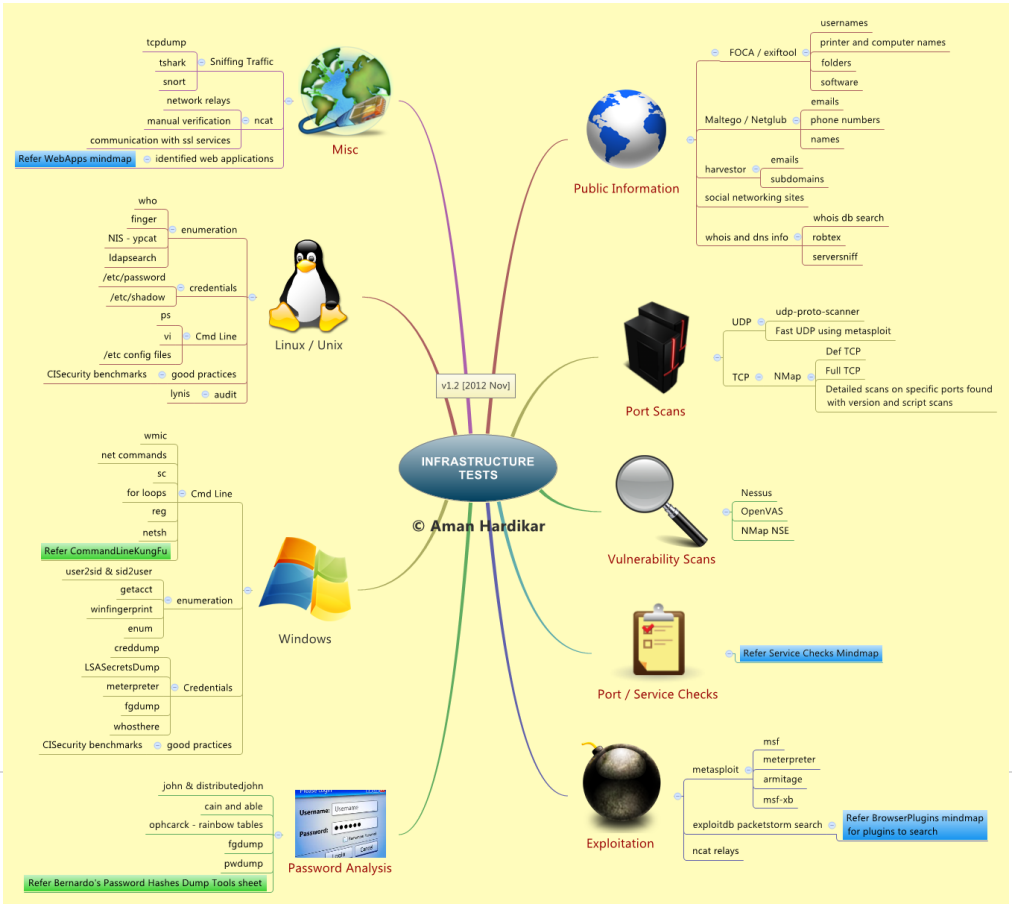
و غيرها..

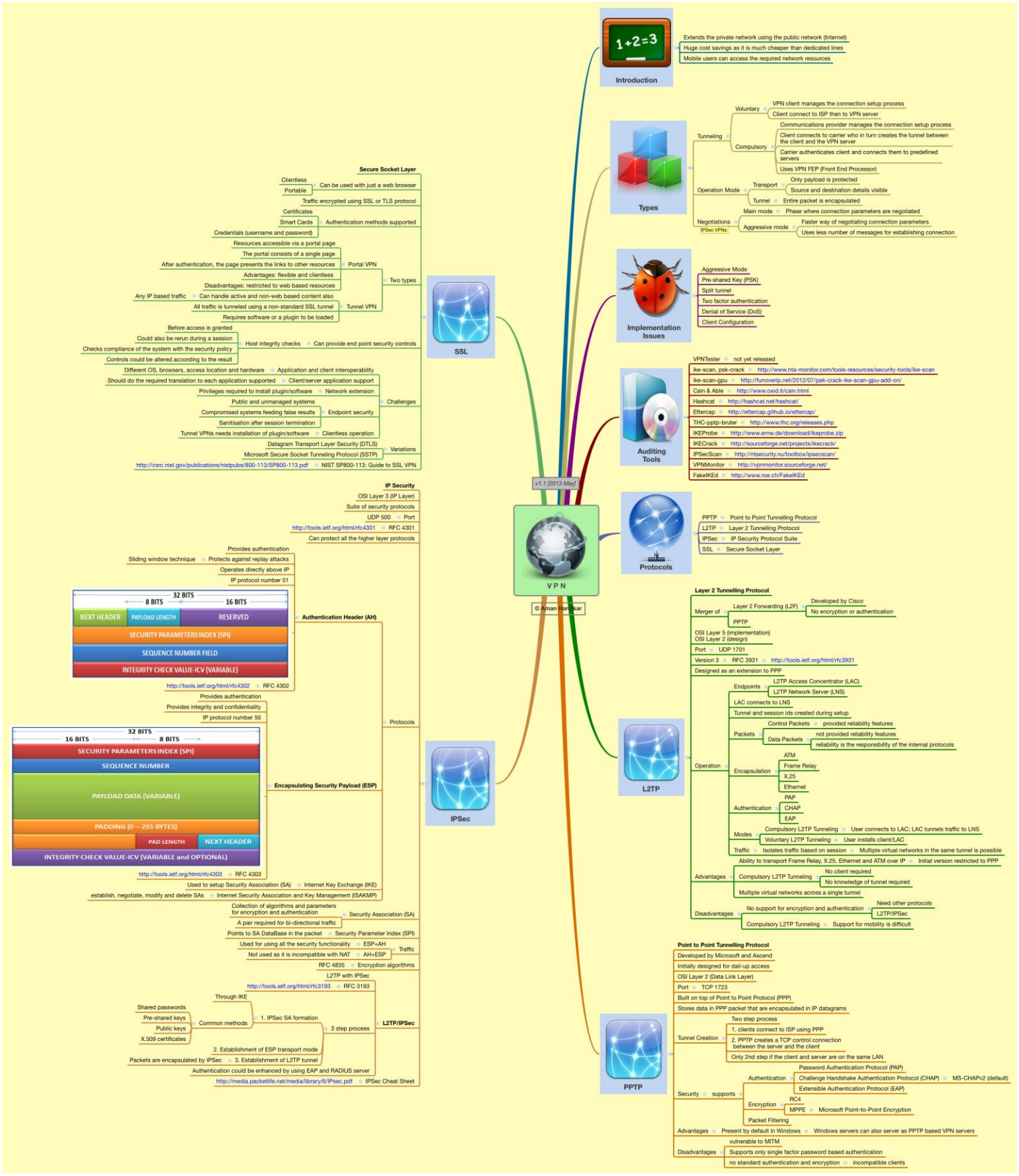
من المسميات الوظيفية التابعة للتخصص:-

- مدير الأمن - Security manager
- مدير أمن المعلومات - Information security manager
- مسؤول أمن الشبكة - Network security administrator
- مسؤول أمن الأنظمة - Systems security administrator
- ضابط أمن نظم المعلومات - Information systems security officer
- مسؤول أمن تكنولوجيا المعلومات - IT security administrator

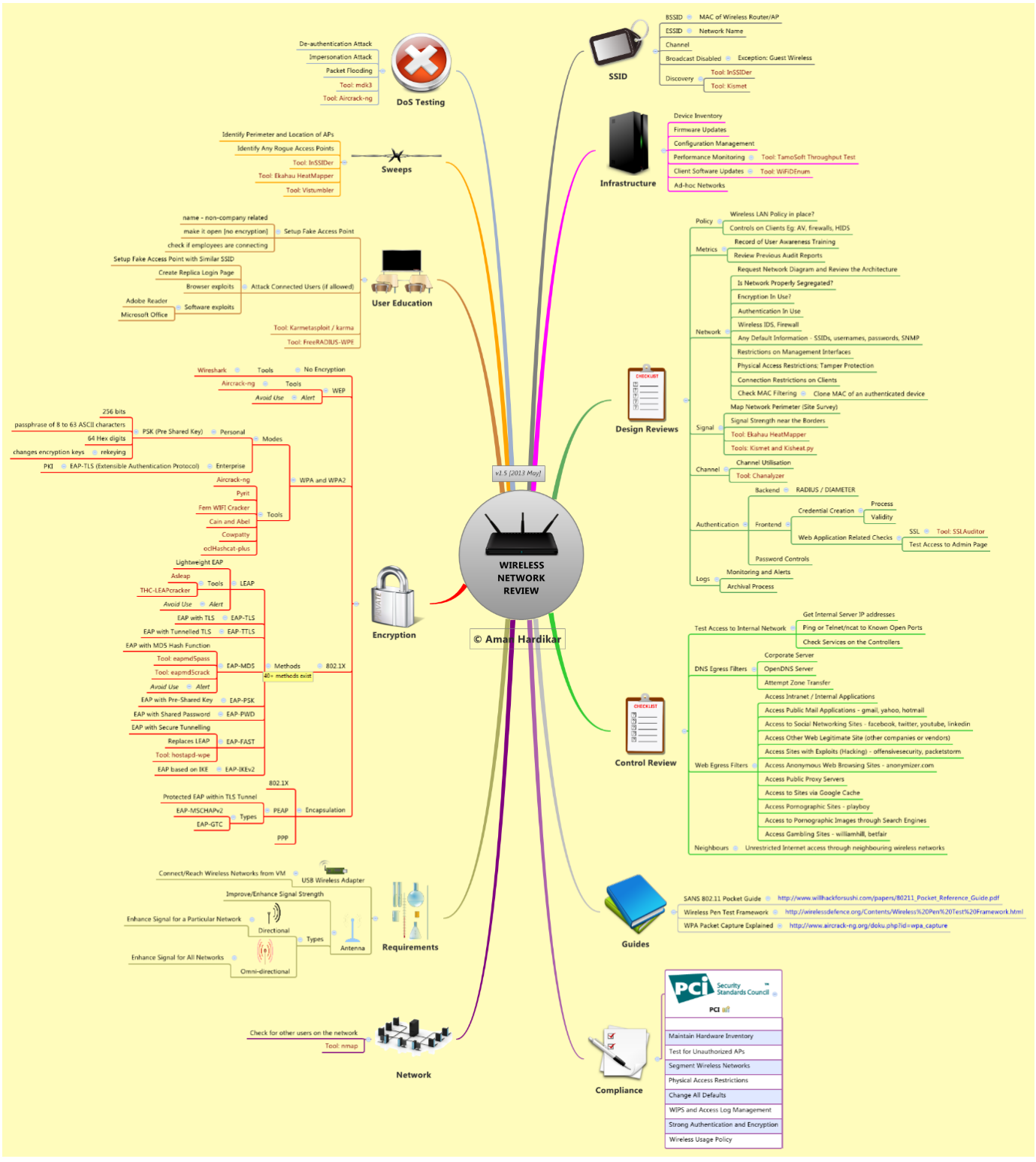
أدوات و خرائط (MAPs & Tools)

بعض الأدوات المهمة هنا





الصورة بجودة أعلى و الروابط في الصورة هنا



الصورة بجودة أعلى و الروابط في الصورة هنا

شهادات ودورات

عزيزي المبتدئ: الشهادات هي مجرد جسر عبور للمقابلة الوظيفية و ستسأل في المقابلة عن ما تعرفه لقياس مهاراتك فلا تحرج نفسك (لا تجمع شهادات بدون معرفة)

لينكس(GNU/Linux) : دورة فليكس كورسز (ينصح بها للمعرفة العملية) كما توجد دورة Linux+ لكن أغلب الشهدات في هذا المجال مقدمة من شركة RedHat ستجد خارطة شهدات الشركة في صفحة 52

ويندوز (Windows) : جميع الشهدات مقدمة من شركة Microsoft مثل شهادة MCSA و MCSE ستجد خارطة شهادات الشركة صفحة 46

الشبكات (Network) : (راجع **أساسيات الشبكات**) من الممكن أن تبدأ بدورة Network+ و بعد هذه المرحلة من الأفضل أن تبحث عن الشركة المقدمة لـ أجهزة/خدمات الشبكات في المنشأة التي تنوي العمل بها.. و تأخذ أحد مسارات التدريبية التي تقدمها تلك الشركة، من الأمثلة على الشركات: Cisco ، FireEye ، Juniper.

لكن لو احترت أو لم تستطع معرفة أي المسارات أنسب لك، فمن الأفضل أن تأخذ دورات شركة Cisco حيث أنها الأكثر انتشاراً.. و لكن لا تقلق، فمهما كان المسار الذي أتبعته، ستجد أنك في الغالب ستكون على قدر عالي من الكفاءة التي تمكنك من التعامل مع معظم أنظمة باقي الشركات، حيث أن المفهوم العام واحد.. **انظر إلى خارطة شهادات شركة Cisco في صفحة 47**

مسار مقترح للشهادات:

الشركة	اسم الشهادة كامل	اسم الشهادة المختصر
Cisco	Cisco Certified Network Associate	CCNA
Microsoft	Microsoft Certified Solutions Associate	MCSA
Microsoft	Microsoft Certified Solutions Expert	MCSE
Cisco	Cisco Certified Network Professional	CCNP Enterprise
Cisco	Cisco Certified Network Professional Security	CCNP Security
RedHat		
Microsoft	Microsoft Azure	
AWS	AWS Certified Advanced Networking	
AWS	AWS Certified Security	

نبذة تعريفية عن التحليل الجنائي الرقمي:-

تعرف موسوعة ويكيبيديا التحليل الجنائي الرقمي (المعروف أحيانًا باسم علم الطب الشرعي الرقمي) هو فرع من فروع علم التحليل الجنائي يشمل استرداد المواد الموجودة في الأجهزة الرقمية و التحقيق فيها ، و غالبًا ما يتعلق بجرائم الكمبيوتر .تم استخدام مصطلح التحليل الجنائي الرقمي في الأصل كمرادف للتحليل الجنائي الحاسوبي و لكنه امتد ليشمل التحقيق في جميع الأجهزة القادرة على تخزين البيانات الرقمية . تعود جذورها إلى ثورة الحوسبة الشخصية في أواخر السبعينيات و أوائل الثمانينيات ، تطور النظام بطريقة عشوائية خلال التسعينيات ، و لم تظهر السياسات الوطنية إلا في أوائل القرن الحادي و العشرين.

نبذة تعريفية عن الإستجابة للحوادث:-

هي الممارسة المنظمة للإستجابة لحوادث الأمن السيبراني. يتم تنظيم هذه الممارسات في خطة محكمة تحدد الخطوات والأدوات التي يجب على المنظمة إتباعها خلال وقوع الحادث.

يمكن لهذه الخطة أن تختلف بين جهة وأخرى ، و لكنها على الأقل يجب أن تغطي 6 خطوات رئيسية:
1- الإعداد 2-الإكتشاف 3-الإحتواء 4-الإستئصال 5- الإستعادة 6- الدروس المستفادة

يجب أن نضع في عين الإعتبار أن كل خطوة من هذه الخطوات تحتاج إلى أتمته لذا يتم استخدام بعض الأدوات المختصة في التحليل الجنائي الرقمي لتساعدنا على جمع البيانات واستيعابها .. بينما تستخدم أدوات أخرى للوصول لأهداف أخرى مثل، إجراءات الإستجابة الفعلية .. كما يوجد أدوات أخرى أيضا تساعد في تحقيقات تفصيلية معقدة في الحوادث الأمنية.

الجدير بالذكر هنا أن معظم الأدوات المجانية توفر حلاً لجزء فقط من عملية الإستجابة للحوادث ، لذا في الغالب ستحتاج إلى الجمع بين عدة أدوات للوصول إلى أفضل النتائج بالسرعة المطلوبة.

للمزيد من التفاصيل

أقسام التخصص + بعض التفاصيل

و التحليل الجنائي الرقمي له فروع كثيرة و نذكر منها:

- التحليل الجنائي الرقمي **لأجهزة الحاسب.**
- التحليل الجنائي الرقمي **لقواعد البيانات.**
- التحليل الجنائي الرقمي **للشبكة.**
- التحليل الجنائي الرقمي **للويب.**
- التحليل الجنائي الرقمي **لأجهزة الجوال.**

و المزيد من التفاصيل في الصورة التالية

Forensics (Digital)
© Aman Hardikar

File System Forensics
- Intro
  - file system holds all the files
  - boot sectors and partitions need to be identified / marked
- Tools
  - TSK (The Sleuth Kit)
  - GUI for Sleuthkit – PTK
  - scalpel
  - foremost
- Extra Tools

Disk Imaging
- Intro
  - an exact copy of the hard disk should be taken
  - this includes free space replication also
  - Copy should be in a format supported by other analysis tools
  - copier should have forensic features like hash calculations to maintain/prove integrity
- Tools
  - FTK Imager
  - guymager
- Encrypted Disks
  - to identify encryption used
  - Encrypted Disk Detector
  - Encryption Analyzer
- Hardware Copier
  - faster and efficient
  - forensic features like write protect
- Remote Imaging
  - agent based remote live forensics tool – grr
  - full memory and disk based access
  - remote forensics tool based on nbd protocol – nbdserver
- Extra Tools
  - disk duplication tools – dd dcfldd rdd
  - linux command line version of Encase's disk imaging tool – LinEn

Mac Forensics
- Intro
  - tools to examine Mac OSX machines
- Tools
  - Volafox – memory
  - TSK – filesystem
- Extra Tools
  - Mac Memory Reader – memory

Timeline
- Intro
  - to create a timeline for identifying the files affected at a certain point in time
- Tools
  - Plaso / log2timeline
  - 4n6time / l2t_Review

Toolkit
- SIFT (SANS Investigative Forensic Toolkit)
- Autopsy
- DFF
- Sysinternals
- Data Recovery Tools
- md5deep and hashdeep
  - md5deep: compute MD5, SHA-1, SHA-256, Tiger, or Whirlpool hashes
  - hashdeep: compute, match, and audit hashsets
- ssdeep
- Misc
  - Tools
    - automated image forensics tool – Ghiro
    - file comparison tool – codecompare
    - mac address lookup script – macl.pl
    - create vm from raw disk image – Live View
    - vmdk file analysis – VMDK Forensic Artifact Extractor
  - Extra Tools
    - file comparison tool – winmerge

eMail Analysis
- Intro
  - tools to analyse emails
- Tools
  - smtpcat
  - Exchange EDR Viewer
- Extra Tools
  - ost, pst and eml viewers
  - Mail Viewer

Unix and Linux Forensics
- Intro
  - tools to examine Unix and Linux machines
  - Supports BSD, Solaris and Linux – TSK
- Tools
  - filesystem
    - Autopsy
    - data carving tool to recover files based on foremost – scalpel
    - foremost
  - memory
    - memdump
    - volatility
- Extra Tools
  - viewer for ext partitions on Windows – Explore2fs
  - outdated. TSK recommended – TCT

Windows Forensics
- Intro
  - tools to examine Windows machines
- Tools
  - memory
    - DumpIt
    - Volatility
  - filesystem
    - TSK
    - scalpel
  - artifacts
    - Vinetto – thumbs.db
    - pref.pl – prefetch
    - VSCToolset / ShadowExplorer – volume shadow copy
    - Rifiuti – recycle bin
    - GrokEVT / Evtxtools – event logs
    - MS LogParser
    - restore points
    - liblnk – lnk files
    - scheduled tasks
    - JumpLister – jump lists
    - other artifacts
  - native / Microsoft
    - Sysinternals
  - collection
    - multiple smaller tools for acquisition – Triage IR
    - Autopsy
    - collect files of interest – ircollect

Registry Forensics
- Intro
  - registry holds all configuration settings of OS and software
  - Hives
- Tools
  - regripper
  - Registry Decoder
  - regshot
  - recovers contents from deleted registry keys – RegSlack
  - UserAssist
- Extra Tools
  - registryasxml
  - runs on windows, linux ans osx – yaru

Methodology
- Incident Handling
- Incident Response

Links, Blogs and Study
- Forensics Wiki – http://www.forensicswiki.org/
- SANS – http://computer-forensics.sans.org/

Browser/Internet Forensics
- Intro – tools and resources to analysis Internet related software/evidence
- Tools
- Extra Tools
  - FireFoxForensics
  - ChromeForensics
  - FacebookSaver – save facebook profile
- Links – http://www.browserforensics.com/

IOC
- Description
  - Indicators of Compromise
  - XML data
  - an artefact observed on a network or in operating system that with high confidence indicates an intrusion
- Structure
- Standards
  - The Incident Object Description Exchange Format – RFC 5070
  - Cyber Observable eXpression (CybOX) – http://cybox.mitre.org/ / https://github.com/CybOXProject
  - Structured Threat Information eXpression (STIX) – http://stix.mitre.org/
  - Trusted Automated eXchange of Indicator Information (TAXII) – http://taxii.mitre.org/
  - Malware Attribute Enumeration and Characterization (MAEC) – http://maec.mitre.org/
- Databases
  - IOC Bucket – http://iocbucket.com/
  - ForensicArtifacts – http://ioc.forensicartifacts.com/
  - Snort Rules / Signatures – http://www.snort.org/vrt
  - OpenIOC – http://www.openioc.org/
- Tools
  - IOC Finder
  - IOC Editor
  - IOCextractor

Log Analysis
- Intro – Used to correlate the various incident on the network
- Tools
  - Splunk
  - PyFLAG
- Extra Tools
  - AWStats
  - webalizer
  - Highlighter

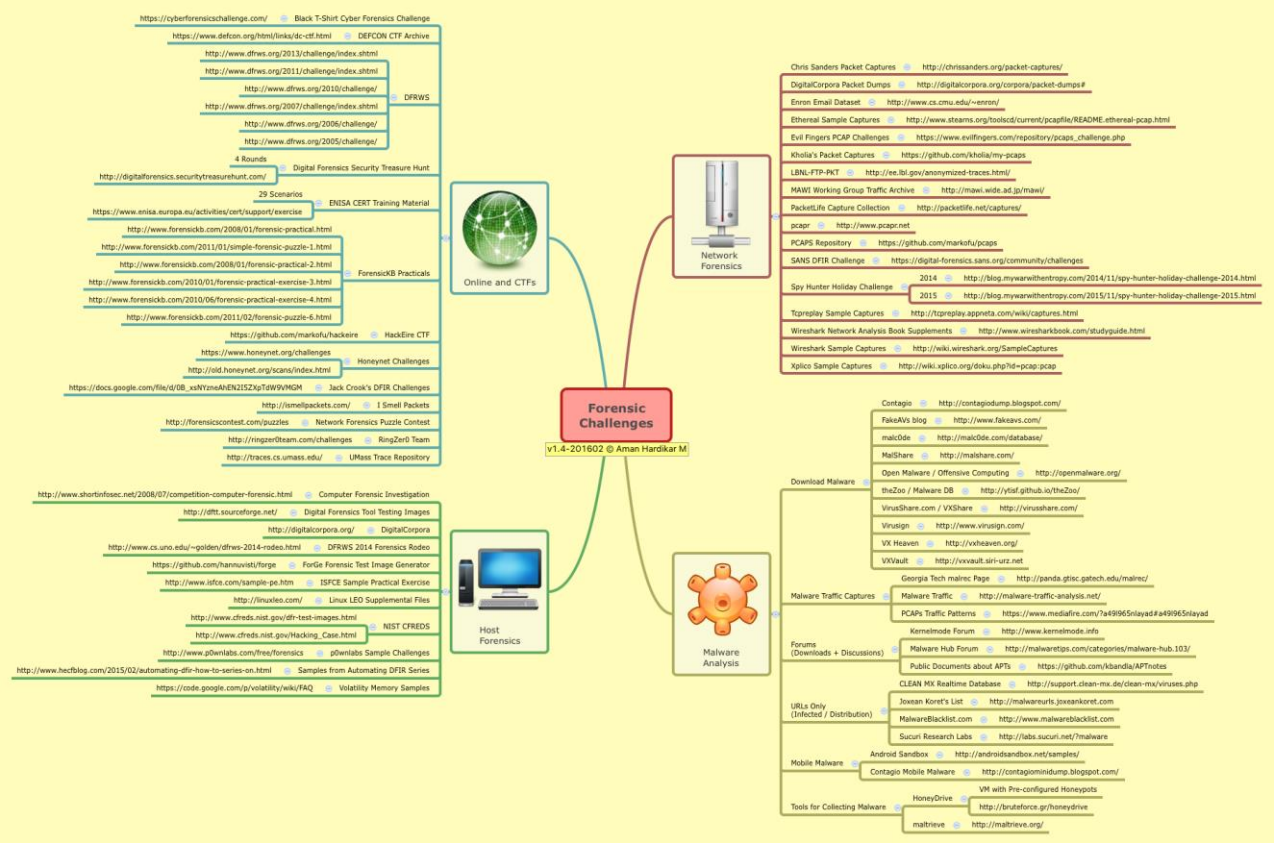
Memory Analysis
- Intro
  - Memory/RAM holds huge amount of information
  - Should be captured for a fast analysis of the system
  - Normally holds process, registry, file and internet/browser information
- Tools
  - DumpIt – Saving copy of the Memory (RAM)
  - Volatility – Analysis of Memory
    - Supports Windows OS and Linux
    - Can also convert hibernation and crash dumps files to binary for analysis
  - Volafox – Analysis of Memory
    - Mac OSX and BSD
- Extra Tools
  - Memoryze (MemoryDD.bat) – Saving copy of the Memory
  - win32dd / win64dd – Saving copy of the Memory
    - Supports acquisition via network
  - Redline – Analysis of Memory
    - Windows OS
  - WinPMem – Acquire physical memory
    - Windows OS
  - Mac Memory Reader – Acquire physical memory
    - Mac OSX 10.4 to 10.8
  - hibr2bin – Convert hibernation file to binary file
    - x86 - Windows OS (XP/Vista)
  - dmp2bin – Converts crash dumps to binary file
    - x86
- Help – SANS Memory Forensics Cheat Sheet

Network Forensics
- Intro
  - Network generally contains the clues of the compromise
  - URLs of the destination and the data being sent
- Tools
  - Netwitness – network traffic analysis/dissection tool
    - filter traffic based of various parameters
  - tshark – command line version of wireshark
    - can specify number of packets or size of pcap for capture
- Extra Tools
  - Network Miner – similar to netwitness
  - Wireshark – packet sniffing and analysis tool
    - follow tcp stream to see the full conversation
  - tcpdump – command line packet sniffer
  - Moloch – PCAP browsing, searching, and exporting
  - NfSen – analysing the netflow of the traffic
  - Snort/Sguil – ids/packet capture tool
    - alerts on signature matches
    - new signature could be tested
  - Suricata – ids/ips/nsm tool
    - can detect protocols
    - can be used to extract files from the traffic
  - OSSIM – Open-source SIEM tool

Mobile Forensics
- Intro – tools and references to examine mobile and embedded devices
- Tools
  - Santoku Linux
  - AFLogical
  - iPBA2
  - iPBD
  - Oxygen Forensic Suite
- Extra Tools – iBrowse
- References
  - FAT64 filesystem forensics
  - Chip-Off_Forensics – http://www.forensicswiki.org/wiki/Chip-Off_Forensics

أدوات ، معامل ، الالآت (Machines , Labs , Tools)

توجد الكثير من الأدوات في الصورة السابقة



الصورة بجودة أعلى و الروابط في الصورة هنا

عزيزي المبتدئ: الشهادات هي مجرد جسر عبور للمقابلة الوظيفية و ستسأل في المقابلة عن ما تعرفه لقياس مهاراتك فلا تحرج نفسك (لا تجمع شهادات بدون معرفة)

الشركة	اسم الشهادة كامل	اسم الشهادة المختصر
CompTIA	Cybersecurity Analyst	CySA+
EC-Council	Certified Ethical Hacker	CEH
EC-Council	Certified Forensic Hacking Investigator	CHFI
GIAC	Certified Incident Handler	GCIH
GIAC	Certified Intrusion Analyst	GCIA
GIAC	Certified Forensic Analyst	GCFA
GIAC	Certified Forensic Examiner	GCFE
GIAC	Reverse Engineering Malware	GREM
GIAC	Network Forensic Analyst	GNFA
EnCase	Certified Examiner	EnCE
	Certified Computer Examiner	CCE
	Certified Forensic Computer Examiner	CFCE

المصدر

و من المهم أن تطلع على شهادات هذا التخصص في مسارات دورات الشركات خصوصا eLearnSecurity صفحة 48

Applications Security (AppSec)
(أمن التطبيقات)

5	4	3	2	1

مستوى الصعوبة

نبذة تعريفية عن التخصص:-

يعرف موقع "VMware" أمن التطبيقات بأنه: عملية تطوير و إضافة واختبار ميزات الأمان داخل التطبيقات لتحصين الثغرات الأمنية ضد التهديدات مثل الوصول غير المصرح به و التعديل، كما يصف الإجراءات الأمنية على مستوى التطبيقات، و التي تهدف إلى منع سرقة أو اختطاف البيانات أو النصوص البرمجية داخل التطبيقات. تشمل العملية، احتمالات نشوء الثغرات الأمنية أثناء تطوير التطبيقات وتصميمها ، كما أنها تتضمن أنظمة و أساليب لحماية التطبيقات بعد نشرها .

قد يتضمن أمن التطبيقات: الأجهزة والبرامج و الإجراءات التي تحدد نقاط الضعف الأمنية أو تقللها. يعد جهاز التوجيه (و الذي من مهامه، منع أي شخص من عرض عنوان IP الخاص بجهاز الكمبيوتر من الإنترنت) شكلاً من أشكال أمن تطبيقات الأجهزة. في العادة، تكون مقاييس الأمان على مستوى التطبيق مضمنة في البرنامج ، مثل جدار الحماية للتطبيق (و الذي من مهامه، تحديد الأنشطة المسموح بها والمحظورة بدقة). يمكن أن تستلزم الإجراءات أشياء مثل، العمليات الدورية لأمن التطبيقات و التي تتضمن بروتوكولات مثل الإختبار المنتظم.

أقسام التخصص:-

- أمن تطبيقات **الويب**.
- أمن تطبيقات **الجوال**.
- أمن تطبيقات **سطح المكتب**.

و غيرها..

أدوات ، معامل (Lab , Tools)

معمل (يقدم الموقع خدمات اخرى)

بعض الادوات و الشروحات المفيدة

شهادات ودورات

عزيزي المبتدئ: الشهادات هي مجرد جسر عبور للمقابلة الوظيفية و ستسأل في المقابلة عن ما تعرفه لقياس مهاراتك فلا تحرج نفسك (لا تجمع شهادات بدون معرفة)

الشركة	اسم الشهادة الكامل	اسم الشهادة المختصر
GIAC	GIAC Certified Web Application Defender	GWEB
GIAC	GIAC Web Application Penetration Tester	GWAPT
OWASP (Open Web Application Security Project)		
eLearnSecurity	Web Application Penetration Testing	WAPT
eLearnSecurity	Web Application Penetration Testing eXtreme	WAPTX
Whitehat Security		
Veracode		

المصدر: شبكة نكرة

Penetration testing (pen Testing) : اختبار الإختراق

5	4	3	2	1

مستوى الصعوبة

يعد مختبر الإختراق (**penetration tester**, or **pen tester**) ، من اصحاب القبعات البيضاء أو "مخترق أخلاقي". و على الرغم من أنه يجب عليه التفكير كمخترق غير أخلاقي (صاحب قبعة السوداء) ، فإن الهدف النهائي هو مساعدة المنظمات على تحسين ممارساتها الأمنية لمنع الأضرار، كالسرقة أو التدمير و يستهدف مختبر الإختراق أنظمة التشغيل و الأنظمة المضمنة و الهواتف و الحواسيب، كما يستهدف أيضا التقنيات الناشئة مثل، أنترنت الأشياء (IoT) و غيرها.

بعض مسؤوليات مختبر الإختراق:-

- تطبيق الأدوات المناسبة لاختبار الإختراق.
- إجراء اختبارات الهندسة الإجتماعية و مراجعة الأمن المادي عندما يقتضي الامر.
- مواكبة أحدث طرق الإختبار و القرصنة.
- جمع البيانات و نشر منهجية الإختبار.
- تحديد وتقييم و إدارة نقاط الضعف.
- تقديم إقتراحات لتحسين الأمان و إعداد الإستجابات التقنية لأسئلة الأمان.

المرجع : مدونة موقع CompTIA

و أحب أن أنوه على جزئية عادةً ما يخطئ فيها الناس :-

PT ≠ vulnerable hunting & PT ≠ Red Teaming

ولكن تعني : PT = penetration testing

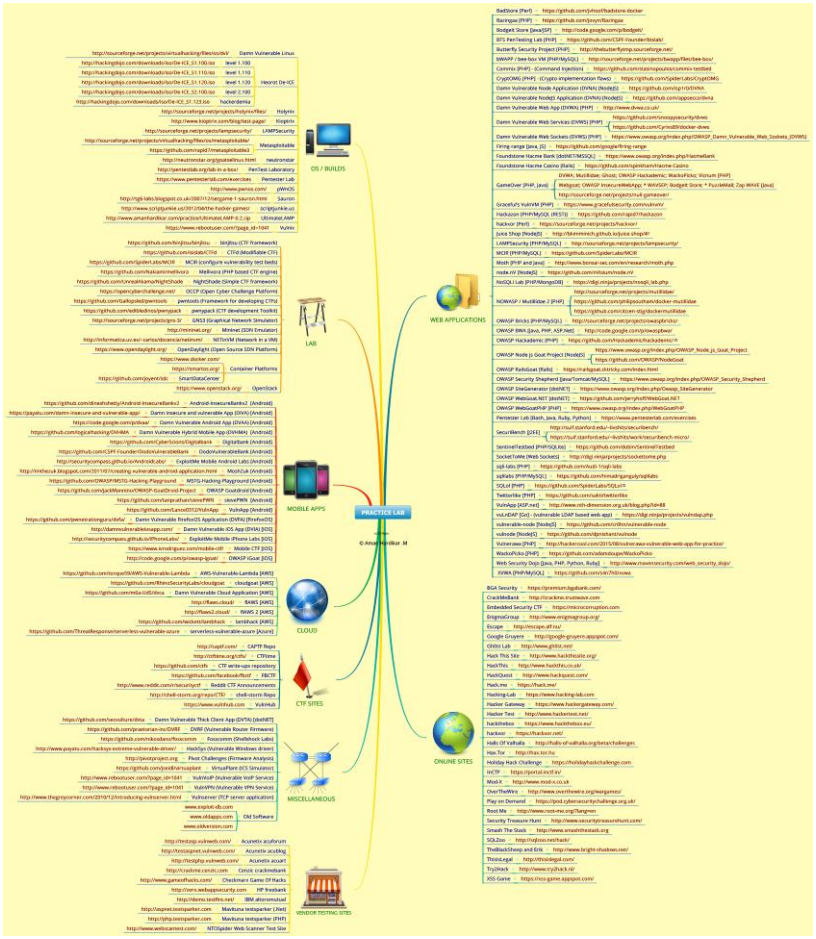
أقسام التخصص:-

- اختبار اختراق **تطبيقات ويب.**
- اختبار اختراق **تطبيقات جوال.**
- اختبار اختراق **الشبكات.**
- اختبار اختراق **أنظمة تشغيل.**

و غيرها..

أدوات ، معامل ، الآلآت (Machines , Labs , Tools)

من المهم الاطلاع على هذا الكتيب (قد تحتاج إلى تحميله لرؤية بعض الصور بوضوح) و مجتمع incyber (حيث يحتوي على ملفات و معلومات و أدوات و شروحات و العديد من الأشياء عن : PenTest , BugBounty , SOC) ... كلاهما من إعداد الأستاذ: مالك الدوسري



الصورة بجودة أعلى و الروابط في الصورة هنا

شهادات و دورات

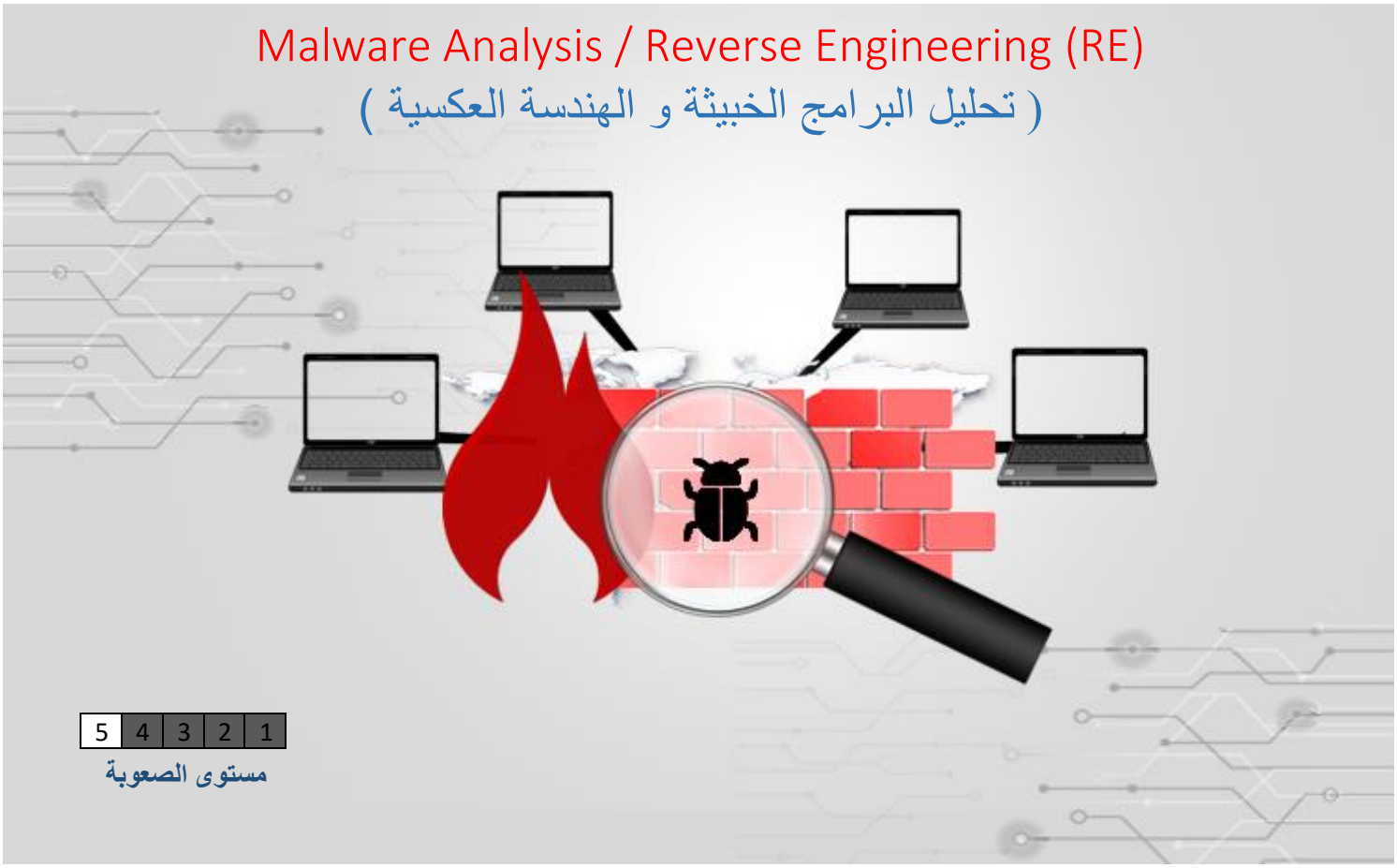
عزيزي المبتدئ: الشهادات هي مجرد جسر عبور للمقابلة الوظيفية و ستسأل في المقابلة عن ما تعرفه لقياس مهاراتك فلا تحرج نفسك (لا تجمع شهادات بدون معرفة)

اسم الشهادة المختصر	اسم الشهادة الكامل	الشركة
OSCP		Offensive Security
OSCE		Offensive Security
PTP	Penetration Testing Professional	eLearnSecurity
GPEN	GIAC Certified Penetration Tester	GIAC
GXPN	GIAC Exploit Researcher and Advanced Penetration Tester	GIAC
CoreLan Team		

المصدر: شبكة نكرة

أو يمكنك إتباع مسار أحد الشركات المذكورة في اخر هذا المحتوى مثل eLearnSecurity

Malware Analysis / Reverse Engineering (RE)
(تحليل البرامج الخبيثة و الهندسة العكسية)



5	4	3	2	1

مستوى الصعوبة

البرمجيات الخبيثة :

البرمجيات الخبيثة ((malicious Software (Malware و هي برامج أو ملفات صممت بطريقة معينة لتلحق الضرر بالبرامج و الأنظمة، بل و قد يصل ضررها إلى أجزاء الكمبيوتر، وهذا لا شك له تداعيات خطيرة منها الإقتصادي و السياسي و البيئي و غيرها.

هناك أنواع كثيرة من البرمجيات الضارة تختلف سلوكياتها و أهدافها و مدى الضرر الذي يمكن أن تسببه، من الأمثله على هذا : **الديدان** ، **الفيروسات** ، **أحصنة طروادة** ، **فيروسات الفدية** ، **برامج التجسس** ، **برمجيات الإعلانات** ، **الجذور الخفية** و أنواع أخرى..

يمكن لبرنامج ضار وحيد القيام بعدة مهام، مثل: **سرقت البيانات** أو **حذفها** أو **تشفيرها** أو **التعديل عليها** أو حتى **إضافة الأنظمة إلى شبكة روبوت (botnet)** و مراقبتها دون علم المستخدم بذلك.

و للمزيد عن البرمجيات الخبيثة إليك هذا المقال (أو مجموعة المقالات إن أحببت التفصيل في كل نوع)

الهندسة العكسية :

الهندسة العكسية (Reverse engineering – وتسمى أيضا backwards engineering أو back engineering) وهي العملية التي يتم من خلالها تفكيك شيء اصطناعي للكشف عن تصميماته أو هندسته المعمارية أو برمجته أو من أجل المعرفة.

كما يمكن تطبيق الهندسة العكسية في مجالات هندسة الكمبيوتر و الهندسة الميكانيكية و الهندسة الإلكترونية و هندسة البرمجيات و الهندسة الكيميائية و بيولوجيا الأنظمة.

المصدر

لتبسيط الفكرة دعنا نفترض أنني أعطيت متذوق حلويات قطعة من الكعك و طلبت منه اكتشاف مكوناتها (زيت ، بيض ، دقيق ، سكر ...) فتحليله لطعم الكعك ومحاولته اكتشاف الوصفة (دون علم مسبق) يعد هندسة عكسية (و لو أن الكعك ليس شيء علمي و لا هندسي ☺)

لا أحد يمكنه تغطية جميع الجوانب في هذا المجال لأنه يمكن تطبيقه على عدد كبير جداً من العلوم و هذا يتخطى حدود معرفة الإنسان الواحد ولكن بإمكان مجتمع أو دولة مثل الصين مثلا أن يبرع في كثير من مجالاته وقد فعلوا

لتتعرف أكثر عن الهندسة العكسية انظر هذا المقال في ويكيبيديا أو هذا المقال في موقع "Engineering 360"

و هنا شرائح عرض عن الهندسة العكسية للبرمجيات و هنا شرح للشرائح **(بالعربي)**

بما أن المقام لا يتسع للتفصيل في المجال فسأقتصر هنا على الحديث عن "تحليل البرمجيات الخبيثة و هندستها عكسيا"

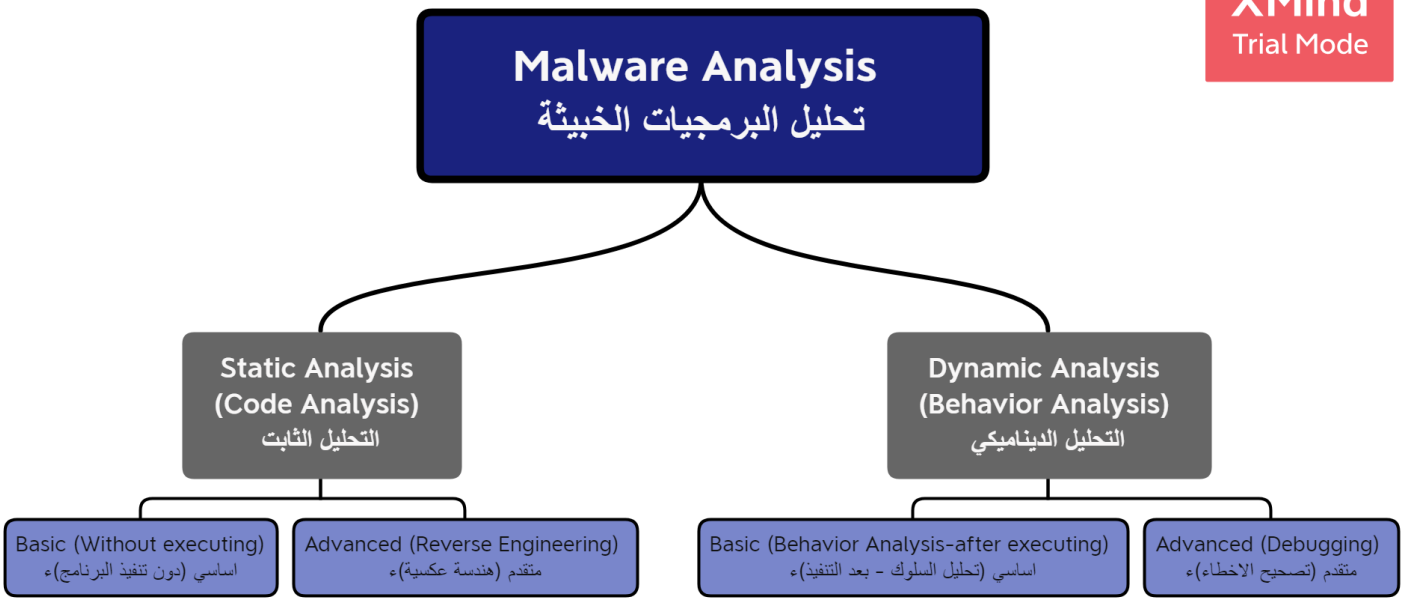
نبذة تعريفية عن التخصص (الهندسة العكسية و تحليل البرامج الخبيثة)

هو فن تشريح البرمجيات الخبيثة لفهم كيفية عملها أو لرصدها أو لتعطيلها أو للتخلص منها لتصدي لها مستقبلاً. يتطلب العمل في هذا المجال معرفة واسعة في مجال تقنية المعلومات عموماً ومن الشركات التي تهتم في هذا المجال، شركات برامج الحماية مثل : كاسبرسكاي ، نورتن و غيرها ..

حتى لا نطيل .. هذا مقطع **عظيم جداً** بعنوان : "Malware Analysis " للمهندس وجدي عصام .. تكلم فيه عن الطرق و المراحل و الأدوات و البرامج و البيئات الإفراضية لتحليل البرمجيات الخبيثة (رابط المكتبة المذكور في الفيديو و الموجودة على Github تجده مع الأدوات بالأسفل)

نظراً لضيق الوقت، اضطُر المهندس وجدي إلى الاختصار و عدم الحديث بشكل مفصل عن تحليل البرمجيات الضارة و هندستها عكسياً و عن التحليل الجنائي للذاكرة و أتمنت هذه العمليات.

ليكون فهم الموضوع أسهل .. هذه خارطة ذهنية لمساعدتك على فهم تفاصيل الموضوع ..

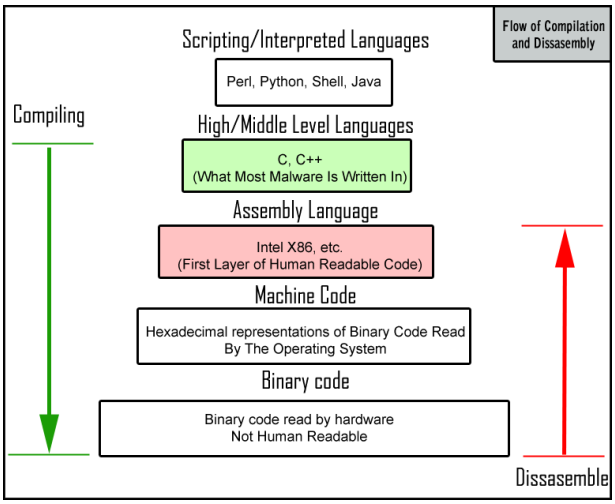


مصادر : مقال و مرجع و مقال

مقال عن "Basic Static Analysis" و من الجيد قراءة هذا الكتاب

كيف تتم هندسة البرمجيات الخبيثة عكسياً ؟

سابقاً كان الموضوع معقد ويحتاج إلى عدد من المختصين .. لكن مع تطور العلوم التقنية أصبح بإمكان شخص واحد بإستعمال الأدوات الجاهزة و لغات التجميع "Assembly languages" أداء دور كل هؤلاء المختصين



و كما ترى في الصورة التالية :

فإن عملية ترجمة الكود البرمجي "Compilation" تتم من الأعلى إلى الأسفل (من لغة يفهمها الأنسأن مثل: java , python أو C إلى لغة الكود الثنائي 0 ، 1 "Binary")

و حيث أنه يتم عادةً كتابة الكود بلغة مثل C ثم تترجم "compiled" بالطريقة المذكورة سابقاً فحينها لا يمكن فهم الكود وسنحتاج إلى إعادتها إلى لغة يمكن للأنسان فهمها، ويمكن عمل ذلك عن طريق أداة تسمى "Decompiler" ولكن في في الغالب لن تنفع معنا هذه العملية أو سيكون من الأفضل استعمال أداة تسمى "Disassembler". هناك عدة أسباب لاستخدام هذه الأداة، منها.. تسهيل فهم البرنامج أو استعادة الـ"source code" و أسباب أخرى.. **و بما أننا سنستخدم في الغالب أداة الـ"disassembler" فسنحتاج إلى معرفة لغات التجميع** (تسمى عملية إرجاع الكود من اللغة الثنائية إلى لغات التجميع "Disassembly" و إرجاع الكود إلى لغة مثل java أو C تسمى "decompilation")

المصادر: Malware Analysis and Detection Using Reverse Engineering Technique ، malwarebytes Labs

و في الختام إليك بعض المواضيع و التقنيات التي ستساعدك في احتراف هذا المجال :

Principles and Fundamental Concepts:

- Assembly languages and program compilation
- Binary code and ELF/PE data representations
- Static binary analysis and disassembly
- Dynamic execution analysis

Attacks and Existing Malware:

- Malware behavior (e.g., control flow hijacking)
- Anti-reverse engineering and obfuscation
- Return-oriented programming
- Web-based malware and social engineering

Analyses and Security Defenses:

- Symbolic execution and taint tracking
- Runtime memory forensics
- Behavioral detection signatures
- Security hardening (ASLR, DEP, and CFI)

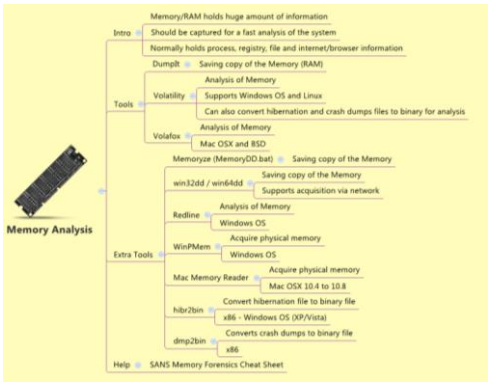
أدوات ، معامل ، الالآت (Machines , Labs , Tools)

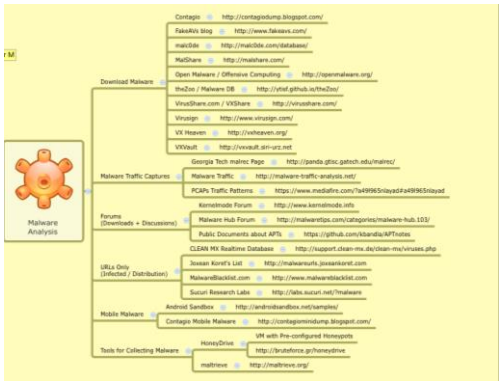
المكتبة المذكورة في شرح المهندس هنا

بعض **الأدوات و المصادر** هنا

بعض **المراجع للهندسة العكسية** هنا

طريقة إنشاء **معمل خاص** هنا





الصورة بجودة أعلى و الروابط في الصورة هنا

شهادات و دورات

هنا **دورة** عبارة عن جزئين الهندسة العكسية 101 و 102 (مفيدة جداً و فيها معامل)

هنا **سلسلة من المقالات** بعنوان "Hacking — Best OF Reverse Engineering "

هنا **سلسلة** أخرى بعنوان "Practical Malware Analysis "

الشهادات

Reverse Engineering Malware (GREM) GIAC

Reverse Engineering Professional (REP) eLearnSecurity

الشهادتين في الأعلى لم اجل غيرهما و بحسب ما وصلت إليه من نتائج بعد البحث فهذا المجال تحديداً يعتمد على المهارات أكثر من الشهادات.

بعض المقالات المفيدة في مجال الأمن السيبراني:

- مقالة على موقع **نتاوي** بعنوان "كيف تصبح هكر أخلاقي"
- مقالة بعنوان "تكتيك الفريق الأحمر و الأزرق و الأرجواني"
- مقالة بعنوان "How to became a hacker"
- مقالة بعنوان "How Every Operating System Keeps You Safe" و ترجمت و اختصرت.. هنا
- مقالة بعنوان "ماهو Bug Bounty"

بعض المواقع و الأدوات المفيدة في مجال الأمن السيبراني:

- مقطع > يحتوي على عدة مواقع و أدوات.
- hackerEnv > منصة عربية سعودية من إبداع مجموعة من الشباب.
- Nakerah Network
- Pentester Academy
- vuln hub
- reversing.kr
- w3challs
- I O
- hacksplaining
- alf.nu
- hacker 101 ctf
- hack.me
- pentestit
- OverTheWire
- hellbound hackers
- root me
- komodo
- attack defense

- بعض الكتب عن الشبكات وانظمة التشغيل وأشياء اخرى رفعتها على Google Drive هنا
- الكثير من الكتب و الفيديوهات و الكورسات بهذا المستودع الضخم The-Art-of-Hacking لمختلف التخصصات في مجال الأمن السيبراني.
- أكثر من **400 كتاب** متاحة للتنزيل مجاناً من سبرنجر Springer Text books

قناتي على اليوتيوب (تحتوي على مجموعة من المقاطع المفيدة في مجال التقنية عموماً)

المسميات الوظيفية في مجال أمن المعلومات و الأمن السيبراني : (وفق إطار سيوف)

معمارية الأمن السيبراني والبحث والتطوير

تنفيذ اعمال التصميم والمعمارية والبحوث والتطوير في مجال الأمن السيبراني.

أ- معمارية الأمن السيبراني

تصميم أنظمة الأمن السيبراني ومكوناته التابعة لنظم وشبكات تقنية المعلومات، والإشراف على تطويرها وتنفيذها.

1- مصمم معمارية الأمن السيبراني

تصميم نُظم وشبكات الأمن السيبراني، والإشراف على إعداداتها وتطويرها وتنفيذها

2- أخصائي الحوسبة السحابية الأمنة

تصميم نُظم الحوسبة السحابية الأمنة وتنفيذها وتشغيلها، مع تطوير سياسات السحابة الأمنة.

ب- البحث والتطوير في الأمن السيبراني

القيام بأعمال البحث والتطوير في مجال الأمن السيبراني.

1. أخصائي تطوير أمن النظم
تصميم أمن نُظم المعلومات وتطويره واختباره وتقييمه في كافة مراحل تطوير تلك النُظم.

2. مطور الأمن السيبراني
تطوير برمجيات الأمن السيبراني وتطبيقاته ونُظمه ومنتجاته.

3. مقيم البرمجيات الأمنة
تقييم أمن تطبيقات الحاسب وبرمجياته وشفراته أو برامجه، مع تقديم نتائج قابلة للتطبيق.

4. باحث الأمن السيبراني
إجراء الأبحاث العلمية في مجال الأمن السيبراني.

5. أخصائي علم البيانات للأمن السيبراني
استخدام نماذج رياضية ومنهجيات وعمليات علمية لتصميم وتنفيذ خوارزميات وأنظمة لاستخلاص استنتاجات ومعارف الأمن السيبراني من مصادر متعددة لمجموعة بيأنات واسعة النطاق.

6. أخصائي الذكاء الاصطناعي للأمن السيبراني

استخدام نماذج الذكاء الاصطناعي وتقنياته (شاملا أساليب التعلم الآلي) لتصميم وتنفيذ خوارزميات وأنظمة لأتمتة وتحسين كفاءة وفعالية مهام الأمن السيبراني.

القيادة وتطوير الكوادر

قيادة وتطوير فرق عمل الأمن السيبراني وأعمالها ، وتطوير كوادر الأمن السيبراني.

أ- القيادة

الإشراف على فرق الأمن السيبراني وأعمالها، وإدارتها وقيادتها.

1. رئيس إدارة الأمن السيبراني

إدارة أعمال الأمن السيبراني داخل المنظمة، ووضع الرؤية والتوجه بشأن الأمن السيبراني، والاستراتيجيات والموارد والأنشطة ذات العلاقة وتقديم المرئيات لقيادة المنظمة حيال أساليب الإدارة الفعّالة لمخاطر الأمن السيبراني للمنظمة.

2. مدير الأمن السيبراني

إدارة الأمن السيبراني للوظائف والنُظم المعلوماتية داخل المنظمة .وقيادة الأمن السيبراني سواء على مستوى فريق أو وحدة أو وظيفة على المستوى المؤسسي.

3. مستشار الأمن السيبراني

تقديم الرأي والمشورة لقيادة المنظمة وقادة وفرق الأمن السيبراني في مواضيع الأمن السيبراني.

ب- تطوير الكوادر

تطبيق معارف ومهارات الأمن السيبراني ومنهجيات تعليم وتطوير الموارد البشرية لتطوير مهارات كوادر الأمن السيبراني وإدارتها والحفاظ عليها وتحسينها.

1. مدير الموارد البشرية للأمن السيبراني

تطوير الخطط والاستراتيجيات والإرشادات داخل المنظمة لدعم تطوير كوادر الأمن السيبراني وإدارتها.

2. مطور المناهج التعليمية للأمن السيبراني

تطوير وتخطيط وتنسيق وتقييم برامج التعليم والتدريب للأمن السيبراني والمناهج ومحتوياتها وطرقها وأساليب تقديمها، حسب الاحتياجات التعليمية.

3. مدرب الأمن السيبراني
تعليم الأفراد وتدريبهم وتطويرهم واختبارهم في موضوعات الأمن السيبراني.

الحوكمة والمخاطر والالتزام والقوانين

تطوير سياسات الأمن السيبراني للمنظمة، وحوكمة هياكل الأمن السيبراني وعملياته، وإدارة مخاطر الأمن السيبراني، وضمأن الالتزام بمتطلبات إدارة المخاطر والأمن السيبراني للمنظمة والمتطلبات القأنونية ذات الصلة.

أ- الحوكمة والمخاطر والالتزام

حوكمة هياكل الأمن السيبراني وعملياته، وإدارة مخاطر الأمن السيبراني، وضمأن تلبية متطلبات إدارة المخاطر والأمن السيبراني للمنظمة لكافة نُظم وتقنيات المعلومات. وكذلك تطوير سياسات الأمن السيبراني داخل المنظمة وتحديثها.

1. أخصائي مخاطر الأمن السيبراني
تحديد مخاطر الأمن السيبراني للمنظمة وتقييمها وإدارتها لحماية أصولها المعلوماتية والتقنية وفقًا لسياسات وإجراءات المنظمة، وكذلك القوأنين والأنظمة ذات العلاقة.

2. أخصائي الالتزام في الأمن السيبراني
ضمأن التزام برنامج الأمن السيبراني للمنظمة بالمتطلبات والسياسات والمعايير المعمول بها.

3. أخصائي سياسات الأمن السيبراني
تطوير سياسات الأمن السيبراني وتحديثها، لدعم متطلبات الأمن السيبراني بالمنظمة ومواءمتها.

4. مقيم ضوابط الأمن السيبراني
تحليل ضوابط الأمن السيبراني وتقييم فاعليتها.

5. مدقق الأمن السيبراني
تصميم عمليات التدقيق للأمن السيبراني وتنفيذها وإدارتها بهدف تقييم مدى التزام المنظمة بالمتطلبات والسياسات والمعايير والضوابط المعمول بها، وإعداد تقارير التدقيق وتقديمها للأطراف ذات الصلاحية.

ب- القوأنين وحماية البيانات

ضمأن التزام المنظمة بقوأنين وتنظيمات الأمن السيبراني وحماية البيانات.

1. أخصائي قأنون الأمن السيبراني
   تقديم الخدمات القأنونية بشأن الموضوعات ذات الصلة بالقوأنين والأنظمة السيبرانية.

2. أخصائي الخصوصية وحماية البيانات
   دراسة هيكلة البيانات الشخصية وقوأنين وأنظمة الخصوصية المعمول بها، مع تحليل مخاطر الخصوصية، وتطوير برنامج المنظمة للمواءمة مع ضوابط الخصوصية وحماية البيانات والسياسات الداخلية، والإشراف على تنفيذها، مع دعم استجابة المنظمة لحوادث الخصوصية أو حماية البيانات.

الحماية والدفاع

تحديد تهديدات وثغرات نُظم وشبكات تقنية المعلومات، وتحليلها ومراقبتها والتعامل معها وإدارتها، واستخدام التداب ر الدفاعية، والمعلومات التي تم الحصول عليها من مصادر متنوعة، للإبلاغ عن الأحداث والاستجابة للحوادث.

أ- الدفاع

استخدام أدوات المراقبة والتحليل لتحديد الأحداث وتحليلها والكشف عن حوادث الأمن السيبراني.

1. محلل دفاع الأمن السيبراني
   استخدام البيانات التي تم استخلاصها من مجموعة أدوات الدفاع السيبراني لتحليل الأحداث الواقعة داخل المنظمة بهدف الكشف عن التهديدات والتعامل معها

2. أخصائي البنية التحتية للأمن السيبراني
   فحص وتنصيب وصيأنة الأجهزة والبرمجيات المستخدمة للدفاع وحماية الأنظمة والشبكات من التهديدات السيبرانية وتشغيلها والإشراف عليها.

3. أخصائي الأمن السيبراني
   تقديم الدعم العام للأمن السيبراني، والمساعدة في مهام الأمن السيبراني.

ب- الحماية

استخدام أدوات المراقبة والتحليل لتحديد الأحداث وتحليلها والكشف عن حوادث الأمن السيبراني.

1. أخصائي التشفير
تطوير أنظمة التشفير وخوارزمياته، وتقييمها وتحليلها وتحديد نقاط ضعفها وسبل تحسينها.

2. أخصائي إدارة الهوية والوصول
إدارة هوية الأفراد والكيأنات، وصلاحيات وصولهم إلى الموارد من خلال تطبيق أنظمة وعمليات التعريف والتوثيق والتصريح.

3. محلل أمن النظم
تطوير أمن النظم واختباره وصيأنته، وتحليل أمن العمليات والأنظمة المدمجة.

ت-تقييم الثغرات

اختبار نُظم وشبكات تقنية المعلومات، وتقييم التهديدات والثغرات.

1. أخصائي تقييم الثغرات
تقييم ثغرات النُظم والشبكات، وتحديد مواطن أنحرافها عن الإعدادات المقبولة أو السياسات المعمول بها، وقياس فاعلية البنية الدفاعية متعددة الطبقات ضد الثغرات المعروفة.

2. أخصائي اختبار الإختراقات
أداء محأولات اختراق مصرح لها لأنظمة الحاسبات أو الشبكات والمنشآت المادية باستخدام أساليب تهديد واقعية لتقييم حالتها الأمنية وكشف الثغرات المحتملة.

ث- الاستجابة للحوادث

مباشرة الحوادث السيبرانية وتحليلها والاستجابة لها.

1. أخصائي استجابة للحوادث السيبرانية
مباشرة الحوادث المتعلقة بالأمن السيبراني وتحليلها والاستجابة لها.

2. أخصائي التحليل الجنائي الرقمي
جمع الأدلة الرقمية وتحليلها، والتحقيق في حوادث الأمن السيبراني لاستخلاص معلومات مفيدة لمعالجة ثغرات النُظم والشبكات.

3. أخصائي تحقيقات الجرائم السيبرانية
تعريف الأدلة وجمعها وفحصها والحفاظ عليها، باستخدام أساليب تحرٍ واستقصاء موثقة ومقننة.

4. أخصائي الهندسة العكسية للبرمجيات الضارة
تحليل البرمجيات الضارة (عن طريق تفكيكها وإعادتها إلى صيغة برمجية مفهومة)، وفهم طريقة عملها وتأثيرها وغرضها، وتقديم توصيات للوقاية منها والاستجابة للحوادث الناتجة عنها.

ج- إدارة التهديدات

جمع وتحليل المعلومات عن التهديدات والبحث عن التهديدات غير المكتشفة، وتقديم رؤى قابلة للتطبيق لدعم عمليات اتخاذ القرار في الأمن السيبراني.

1. محلل معلومات التهديدات السيبرانية
جمع معلومات عن التهديدات السيبرانية من مصادر مختلفة وتحليلها لتكوين فهم وإدراك عميقين للتهديدات السيبرانية، وخطط المخترقين، والأساليب والإجراءات المتبعة، لاستنباط وتوثيق مؤشرات من شأنها مساعدة المنظمات في الكشف عن الحوادث السيبرانية والتنبؤ بها، وحماية النُظم والشبكات من التهديدات السيبرانية.

2. أخصائي اكتشاف التهديدات السيبرانية
البحث الاستباقي عن التهديدات غير المكتشفة في الشبكات والنُظم، وتحديد مؤشرات الإختراق، وتقديم التوصيات للتعامل معها.

أنظمة التحكم الصناعي والتقنيات التشغيلية

تنفيذ أعمال الأمن السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية.

أ- أنظمة التحكم الصناعي والتقنيات التشغيلية

القيام بأعمال الأمن السيبراني المتعلقة بالحوكمة وإدارة المخاطر، ومتابعة الالتزام، والتصميم والتطوير، والتشغيل والإشراف، والحماية والدفاع في نظم التقنيات التشغيلية التي تشمل نُظم التحكم الصناعي، ونُظم التحكم الإشرافي وحيازة البيانات

1. مصمم معمارية الأمن السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية
تصميم نُظم وشبكات الأمن السيبراني في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية والإشراف على إعداداتها وتطويرها وتنفيذها.

2. أخصائي البنية التحتية للأمن السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية
فحص وتنصيب وصيانة الأجهزة والبرمجيات المستخدمة للدفاع وحماية الأنظمة والشبكات من التهديدات السيبرانية في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية وتشغيلها والإشراف عليها.

3. محلل دفاع الأمن السيبراني الأنظمة التحكم الصناعي والتقنيات التشغيلية
استخدام البيانات، التي تم جمعها من مجموعة متنوعة من أدوات الأمن السيبراني لتحليل الأحداث الواقعة في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية بهدف الكشف عن تهديدات الأمن السيبراني والتعامل معها.

4. أخصائي مخاطر الأمن السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية
تحديد مخاطر الأمن السيبراني في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية وتقييمها وإدارتها، مع تقييم وتحليل فاعلية ضوابط الأمن السيبراني القائمة، وتقديم الملاحظات والتوصيات بناء على تلك التقييمات.

5. أخصائي استجابة للحوادث السيبرانية لأنظمة التحكم الصناعي والتقنيات التشغيلية
مباشرة حوادث الأمن السيبراني وتحليلها والاستجابة لها في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية.

المرجع إطار سيوف السعودي

من الممكن أن تساعدك الصورة التالية في تطوير مسيرتك المهنية : (**ليس لها علاقة بإطار سيوف**)

A GUIDE TO CYBER SECURITY CAREER DEVELOPMENT

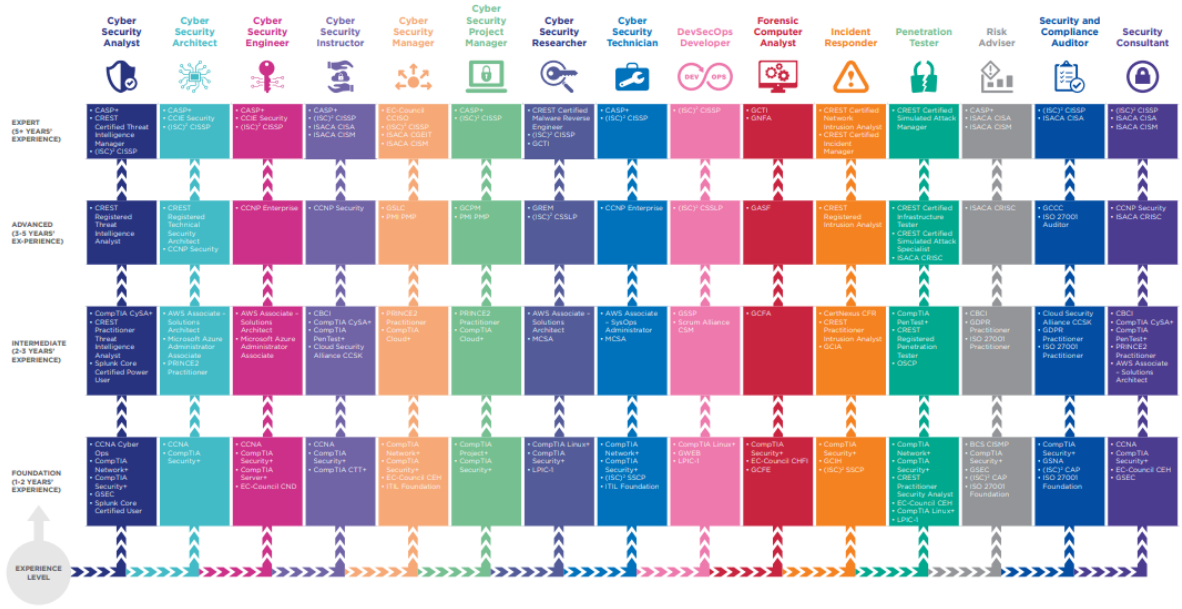
DIGITAL WORLD
SHAPE IT

Skills Development Scotland

Looking to upskill your knowledge and climb up the Cyber Security ladder?

Confused by the industry certifications landscape and trying to decide which one is right for you?

Check out our handy guide to Cyber Security Professional Certifications currently available in Scotland (as of June 2019)



أسماء بعض الشهادات والدورات والشركات التي تقدمها

مقسمة حسب مستوى الخبرة (للمزيد راجع قسم الشركات في الاسفل)

يوجد العديد من الشركات لم يتم وضعها في الجدول تجدها في قسم الشركات أسفل الصفحة .. مثل :
eLeanSecurity و Offensive Security و RedHat والمزيد

اسم الشهادة/الدورة	الاسم كامل	الشركة
Beginner / Foundational مبتدئ / تأسيسي		
A+		CompTIA

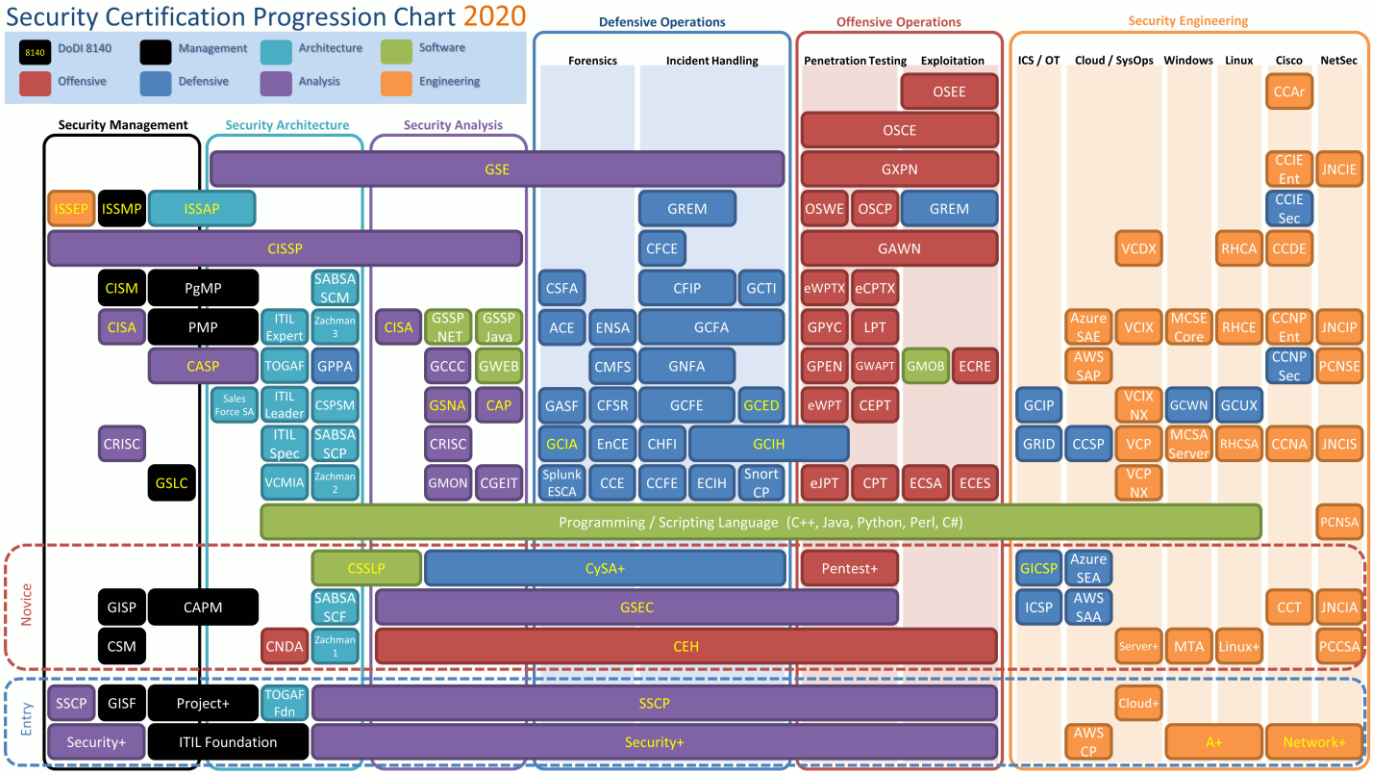
INTERMEDIATE متوسط		
Network+		CompTIA
Security+		CompTIA
Server+		CompTIA
CCNA	Cisco Certified Network Associate	CISCO
C|EH	Certified Ethical Hacker	EC-COUNCIL
C|HFI	EC Council Certified Incident Handler	EC-COUNCIL
GCIH	GIAC Certified Incident Handler	GIAC

GISP	**GIAC Information Security Professional**	
GSEC	**GIAC Security Essentials**	
MCSA	**Microsoft Certified Solutions Associate**	

ADVANCED متقدم		
CSA+(CySA+)	**Cyber Security Analyst+**	
Pen Test+		
CCDP	**Cisco Certified Design Professional**	
CCNP	**Cisco Certified Network Professional**	
CISA	**Certified Information Systems Auditor**	
CSSLP	**Certified secure software lifecycle professional**	
MCSE Core Infrastructure	**Microsoft Certified Solutions Expert**	
GSLC	**GIAC Security Leadership Certification**	
GCED	**GIAC Certified Enterprise Defender**	

EXPERT خبير		
CASP+	**CompTIA Advanced Security Practitioner**	CompTIA
CCIE	**Cisco Certified Internetwork Expert**	cisco
SCYBER	**Cisco Cybersecurity Specialist**	cisco
CGEIT	**Certified in the Governance of Enterprise IT**	ISACA Trust in, and value from, information systems
CISM	**Certified Information Security Manager**	ISACA Trust in, and value from, information systems
CISSP	**Certified Information Systems Security Professional**	(ISC)²

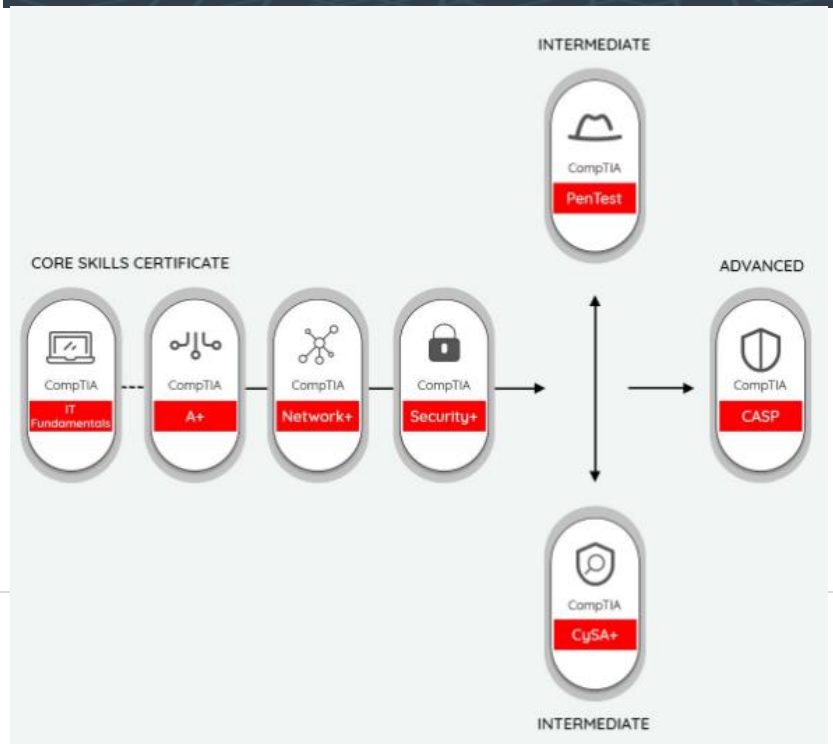
من الممكن أن تكون الصورة التالية مفيدة و أكثر ترتيب من الجداول السابقة :



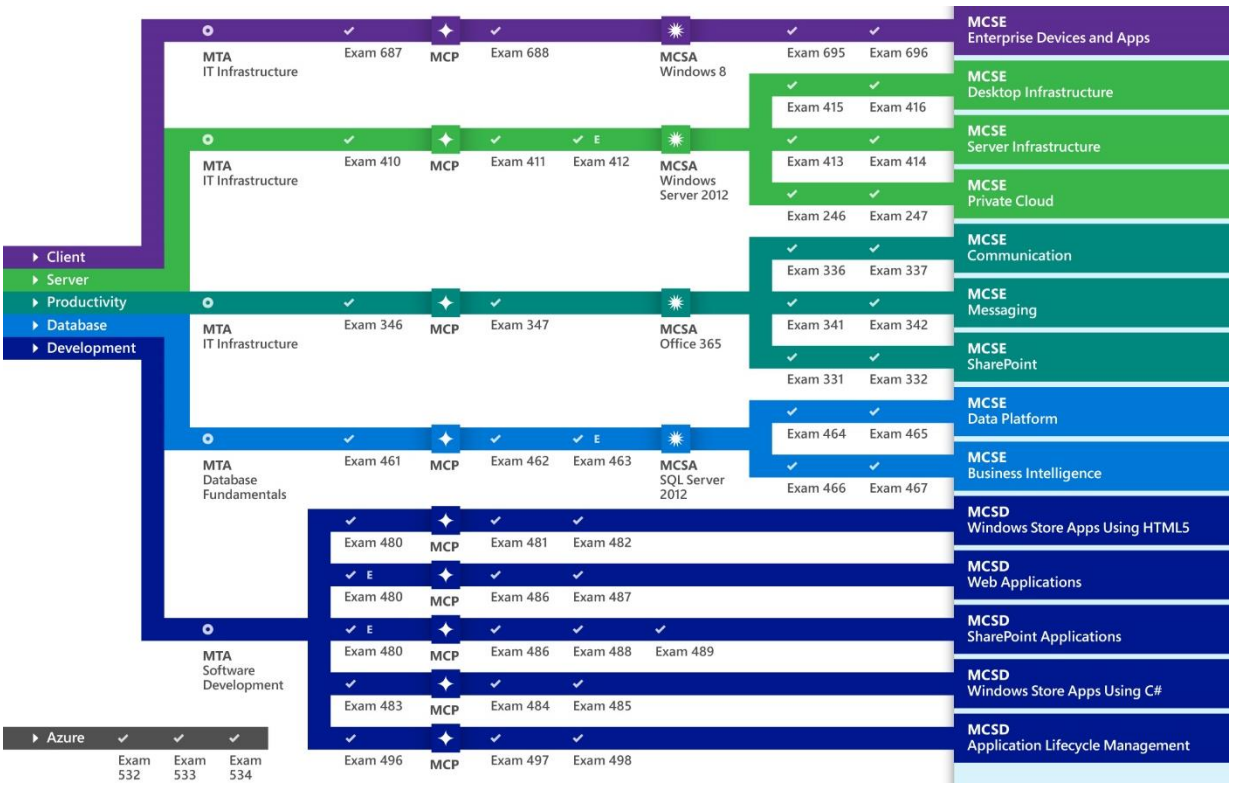
بعض مسارات عدد من الشركات المتخصصة في الأمن السيبراني و نظم التشغيل و الشبكات.

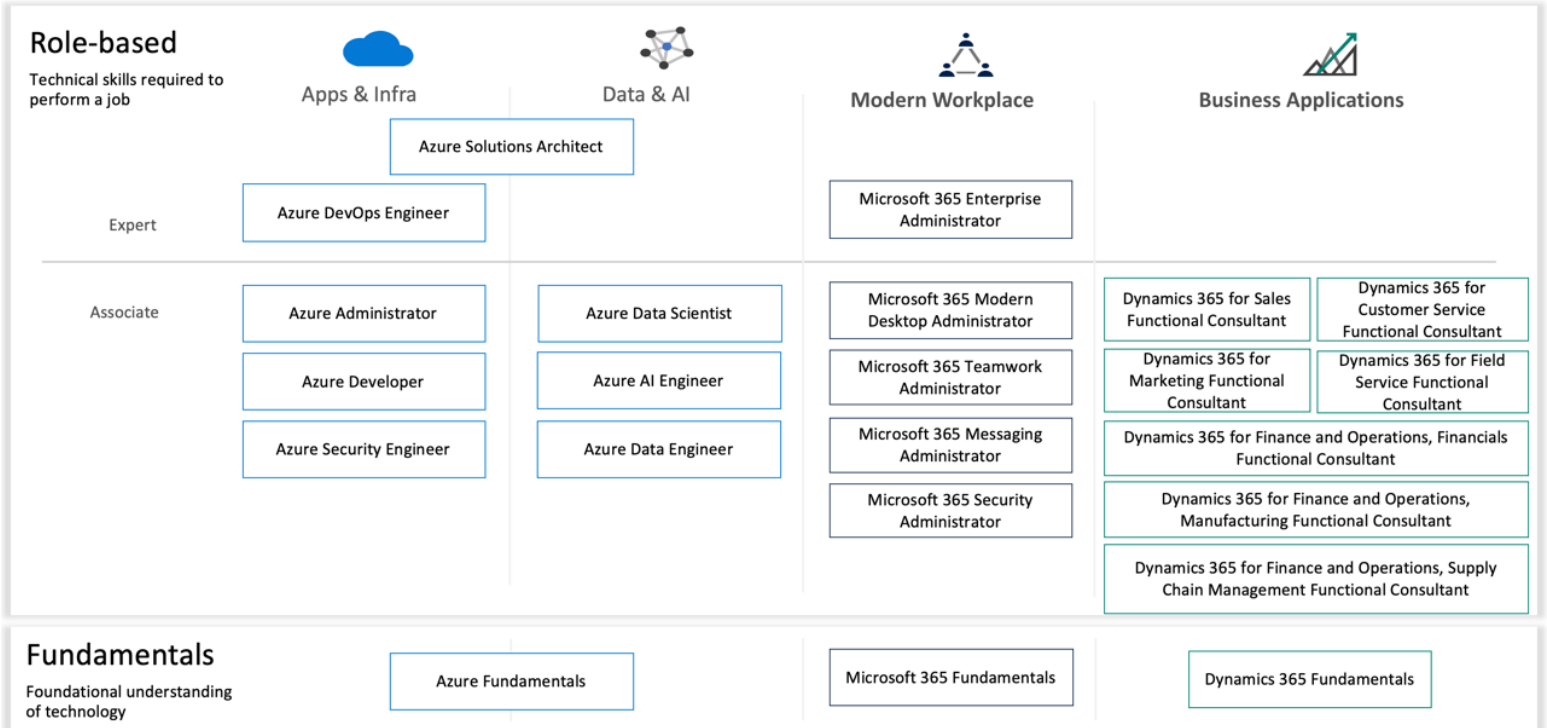
CompTIA

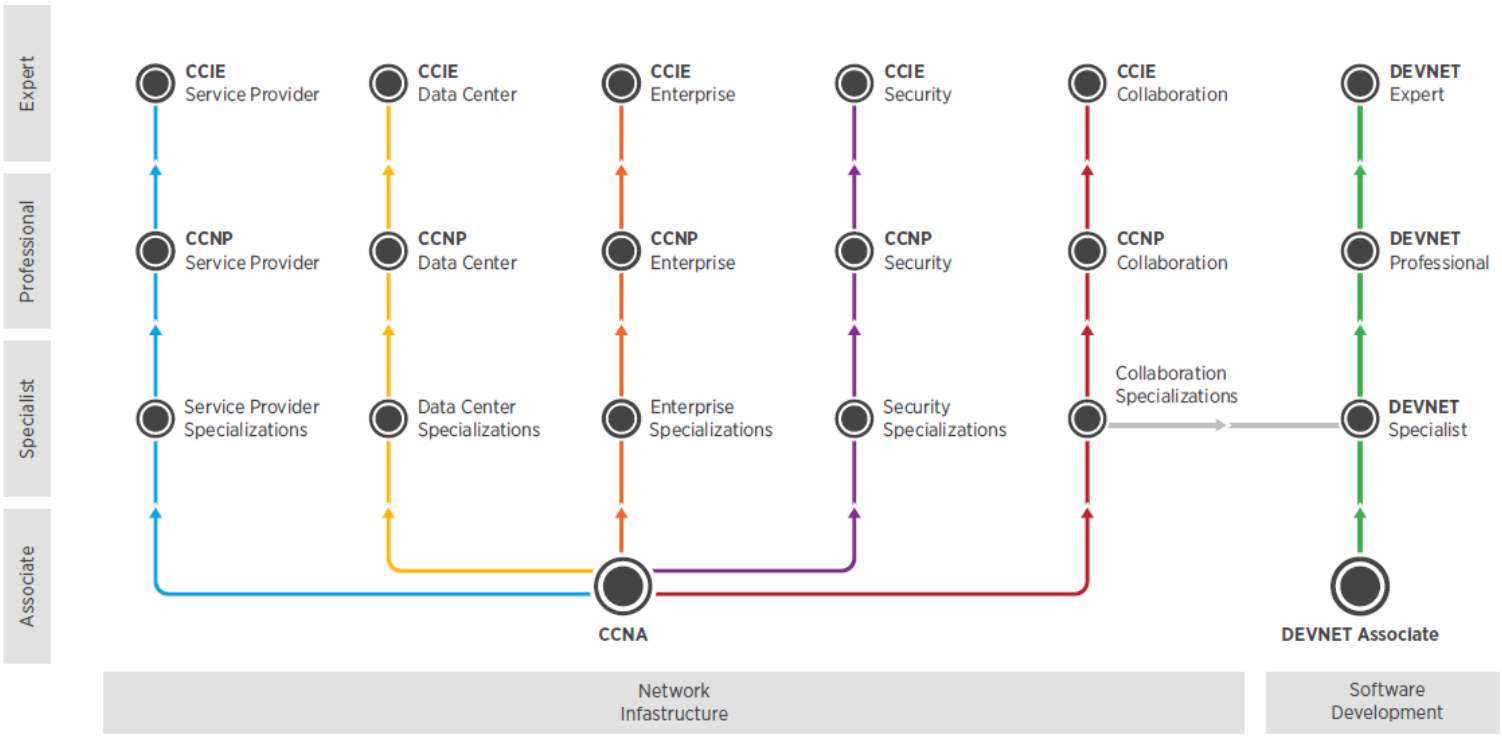
مسار الأمن السيبراني

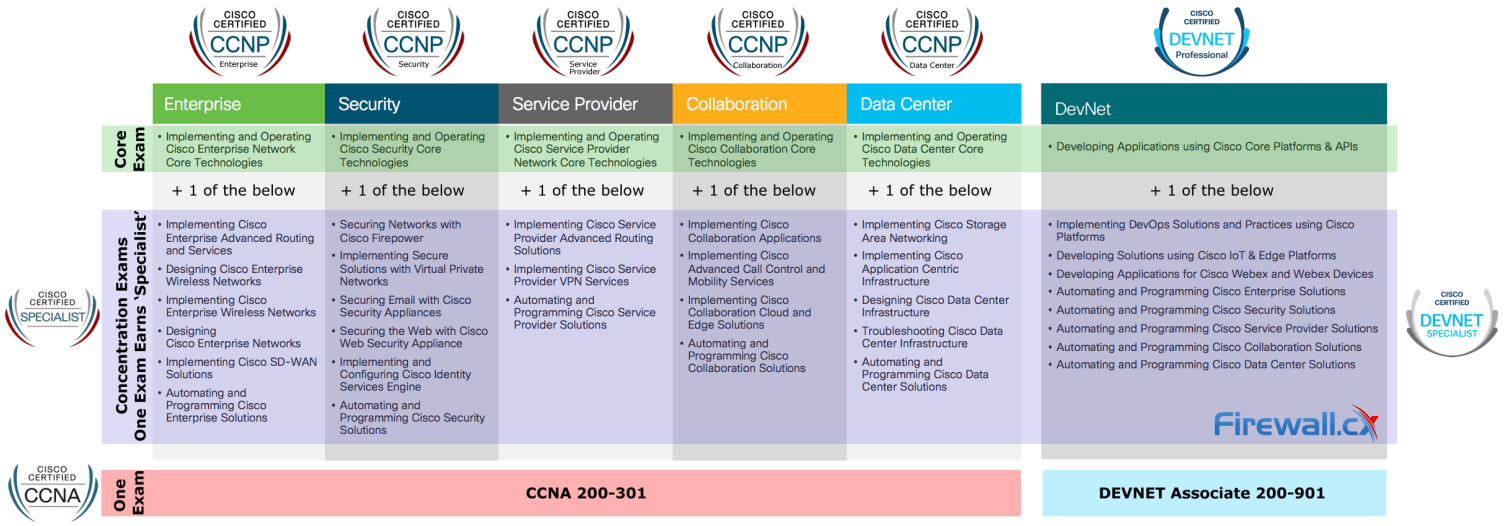


Microsoft


Client
Server
Productivity
Database
Development
Azure
MTA
IT Infrastructure
Exam 687
MCP
Exam 688
MCSA
Windows 8
Exam 695
Exam 696
MCSE
Enterprise Devices and Apps
Exam 415
Exam 416
MCSE
Desktop Infrastructure
MTA
IT Infrastructure
Exam 410
MCP
Exam 411
Exam 412
MCSA
Windows
Server 2012
Exam 413
Exam 414
MCSE
Server Infrastructure
Exam 246
Exam 247
MCSE
Private Cloud
Exam 336
Exam 337
MCSE
Communication
MTA
IT Infrastructure
Exam 346
MCP
Exam 347
MCSA
Office 365
Exam 341
Exam 342
MCSE
Messaging
Exam 331
Exam 332
MCSE
SharePoint
Exam 464
Exam 465
MCSE
Data Platform
MTA
Database
Fundamentals
Exam 461
MCP
Exam 462
Exam 463
MCSA
SQL Server
2012
Exam 466
Exam 467
MCSE
Business Intelligence
Exam 480
MCP
Exam 481
Exam 482
MCSD
Windows Store Apps Using HTML5
Exam 480
MCP
Exam 486
Exam 487
MCSD
Web Applications
MTA
Software
Development
Exam 480
MCP
Exam 486
Exam 488
Exam 489
MCSD
SharePoint Applications
Exam 483
MCP
Exam 484
Exam 485
MCSD
Windows Store Apps Using C#
Exam 496
MCP
Exam 497
Exam 498
MCSD
Application Lifecycle Management
Exam
532
Exam
533
Exam
534

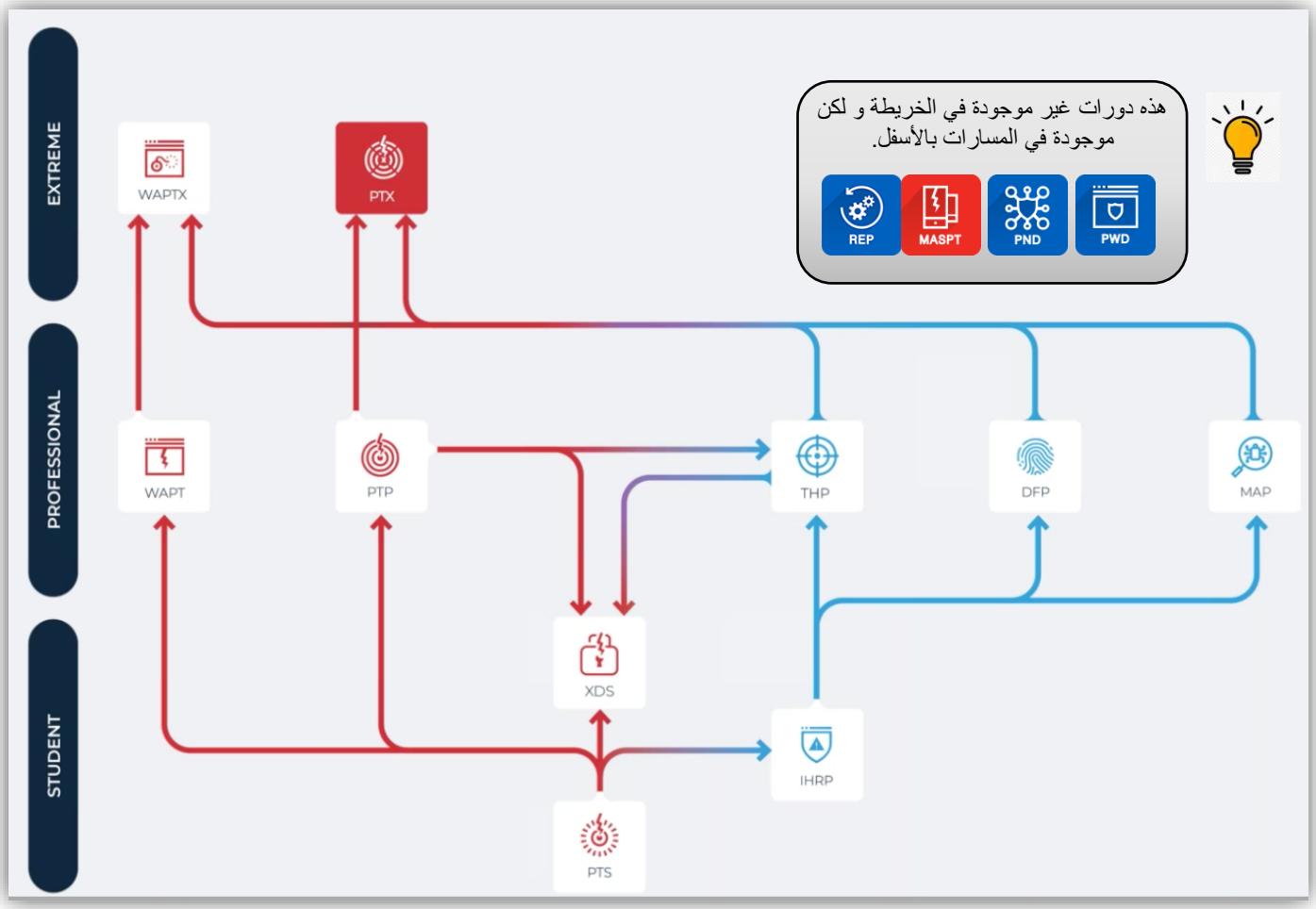

Role-based
Technical skills required to perform a job
Apps & Infra
Data & AI
Modern Workplace
Business Applications
Azure Solutions Architect
Expert
Azure DevOps Engineer
Microsoft 365 Enterprise Administrator
Associate
Azure Administrator
Azure Data Scientist
Microsoft 365 Modern Desktop Administrator
Dynamics 365 for Sales Functional Consultant
Dynamics 365 for Customer Service Functional Consultant
Azure Developer
Azure AI Engineer
Microsoft 365 Teamwork Administrator
Dynamics 365 for Marketing Functional Consultant
Dynamics 365 for Field Service Functional Consultant
Azure Security Engineer
Azure Data Engineer
Microsoft 365 Messaging Administrator
Dynamics 365 for Finance and Operations, Financials Functional Consultant
Microsoft 365 Security Administrator
Dynamics 365 for Finance and Operations, Manufacturing Functional Consultant
Dynamics 365 for Finance and Operations, Supply Chain Management Functional Consultant
Fundamentals
Foundational understanding of technology
Azure Fundamentals
Microsoft 365 Fundamentals
Dynamics 365 Fundamentals


Expert
Professional
Specialist
Associate
CCIE Service Provider
CCIE Data Center
CCIE Enterprise
CCIE Security
CCIE Collaboration
DEVNET Expert
CCNP Service Provider
CCNP Data Center
CCNP Enterprise
CCNP Security
CCNP Collaboration
DEVNET Professional
Service Provider Specializations
Data Center Specializations
Enterprise Specializations
Security Specializations
Collaboration Specializations
DEVNET Specialist
CCNA
DEVNET Associate
Network Infastructure
Software Development


CISCO CERTIFIED CCNP Enterprise
CISCO CERTIFIED CCNP Security
CISCO CERTIFIED CCNP Service Provider
CISCO CERTIFIED CCNP Collaboration
CISCO CERTIFIED CCNP Data Center
CISCO CERTIFIED DEVNET Professional
Enterprise
Security
Service Provider
Collaboration
Data Center
DevNet
Core Exam
Implementing and Operating Cisco Enterprise Network Core Technologies
Implementing and Operating Cisco Security Core Technologies
Implementing and Operating Cisco Service Provider Network Core Technologies
Implementing and Operating Cisco Collaboration Core Technologies
Implementing and Operating Cisco Data Center Core Technologies
Developing Applications using Cisco Core Platforms & APIs
+ 1 of the below
Concentration Exams One Exam Earns 'Specialist'
Implementing Cisco Enterprise Advanced Routing and Services
Designing Cisco Enterprise Wireless Networks
Implementing Cisco Enterprise Wireless Networks
Designing Cisco Enterprise Networks
Implementing Cisco SD-WAN Solutions
Automating and Programming Cisco Enterprise Solutions
Securing Networks with Cisco Firepower
Implementing Secure Solutions with Virtual Private Networks
Securing Email with Cisco Security Appliances
Securing the Web with Cisco Web Security Appliance
Implementing and Configuring Cisco Identity Services Engine
Automating and Programming Cisco Security Solutions
Implementing Cisco Service Provider Advanced Routing Solutions
Implementing Cisco Service Provider VPN Services
Automating and Programming Cisco Service Provider Solutions
Implementing Cisco Collaboration Applications
Implementing Cisco Advanced Call Control and Mobility Services
Implementing Cisco Collaboration Cloud and Edge Solutions
Automating and Programming Cisco Collaboration Solutions
Implementing Cisco Storage Area Networking
Implementing Cisco Application Centric Infrastructure
Designing Cisco Data Center Infrastructure
Troubleshooting Cisco Data Center Infrastructure
Automating and Programming Cisco Data Center Solutions
Implementing DevOps Solutions and Practices using Cisco Platforms
Developing Solutions using Cisco IoT & Edge Platforms
Developing Applications for Cisco Webex and Webex Devices
Automating and Programming Cisco Enterprise Solutions
Automating and Programming Cisco Security Solutions
Automating and Programming Cisco Service Provider Solutions
Automating and Programming Cisco Collaboration Solutions
Automating and Programming Cisco Data Center Solutions
Firewall.cx
CISCO CERTIFIED SPECIALIST
CISCO CERTIFIED DEVNET SPECIALIST
CISCO CERTIFIED CCNA
One Exam
CCNA 200-301
DEVNET Associate 200-901


Associate Level
Specialist Level
Professional Level
Expert Level
Engineering
CISCO CERTIFIED CCNA
CISCO CERTIFIED SPECIALIST
CISCO CERTIFIED CCNP
CISCO CERTIFIED CCIE
Software
CISCO CERTIFIED DEVNET Associate
CISCO CERTIFIED DEVNET SPECIALIST
CISCO CERTIFIED DEVNET Professional
Future Offering
CISCO CERTIFIED DEVNET Expert

دورات شركة eLearnSecurity يتم أخذها في موقع ine (مسار الأمن السيبراني) و يتم أخذ الشهادة عليها بعد الاختبار في موقع الشركة



هذه دورات غير موجودة في الخريطة و لكن موجودة في المسارات بالأسفل.

NETWORK PENTESTER

WEB APPLICATION PENTESTER

PURPLE TEAM MEMBER

ADVANCED PENTESTER

ENTERPRISE DEFENDER

INCIDENT RESPONDER

غير موجودة في أي مسار

يقدم موقع ine دورة **PTS** مجاناً (لكن لديك وصول محدود للمعامل)

مكنك الحصول على الدورة عبر التسجيل في الموقع هنا ثم تأكيد تفعيل الحساب عبر رسالة الايميل التي ستصلك بعد التسجيل

الان انت جاهز للبدأ كل ما عليك هو التوجه لصفحة الدورة وتسجيل الدخول ثم زبدأ التعلم ☺

OFFENSIVE security

للحصول على أحد الشهادات من شركة Offensive Security
لابد من إنهاء الدورة و اجتياز الاختبار الخاص بالشهادة

مثلا : إذا أردت الحصول على شهادة OSCP فلابد من أن تكمل دورة PWK ثم تجتاز اختبار الـ 24 ساعة الخاص بالشهادة

COURSES AND CERTIFICATIONS

Offensive Security certifications are the most well-recognized and respected in the industry. Courses focus on real-world skills and applicability, preparing you for real-life challenges. Online, live, and in-house courses available.

OVERVIEW AND PRICING

START HERE	ADVANCED FOR WEB	ADVANCED FOR PENTEST	NETWORK SECURITY	EXPERT LEVEL FOR EXPLOIT DEVELOPERS
PENETRATION TESTING WITH KALI LINUX (PWK)	ADVANCED WEB ATTACKS & EXPLOITATION (AWAE)	EVASION TECHNIQUES AND BREACHING DEFENSES (PEN-300)	WIRELESS ATTACKS (WIFU)	ADVANCED WINDOWS EXPLOITATION (AWE)
				
OSCP	OSWE	OSEP	OSWP	OSEE

EVERYTHING STARTS WITH PWK

Penetration Testing with Kali Linux (PWK) is a self-paced online course. Students learn the latest ethical hacking tools and techniques to become effective penetration testers. Learning materials include:

- A course guide
- Video lectures
- Active student forums
- Access to a virtual penetration testing lab

Students learn to conduct a penetration test from start to finish and practice techniques safely and legally. The course offers hands-on experience within a target-rich, diverse, and vulnerable network environment.

To earn the coveted OSCP certification, students must complete PWK and pass a 24-hour exam.

FREE RESOURCES: Offensive Security also provides free, open source courses that focus on introductory topics. Check out Kali Linux Revealed and Metasploit Unleashed.

للمزيد من المعلومات عن التدريب و الشهادات :
موقع الشركة

PENETRATION TESTING | WEB APPLICATION | EXPLOIT DEVELOPMENT

Course	Description	
	**PEN-200** PENETRATION TESTING WITH KALI LINUX PEN-200 is our foundational penetration testing course. Students learn the latest tools and techniques, and practice them in a virtual lab.	$999+ EARN YOUR OSCP Difficulty: ●●●○○
	**PEN-210** OFFENSIVE SECURITY WIRELESS ATTACKS PEN-210 trains students to audit, compromise, and secure wireless devices. Get greater insight into the wireless security field with topics like packet interaction and complex WPA attack techniques.	$450 EARN YOUR OSWP Difficulty: ●●●○○
	**PEN-300** EVASION TECHNIQUES AND BREACHING DEFENSES Take your penetration testing skills to the next level. PEN-300 teaches advanced pentesting techniques, including bypassing security mechanisms and evading defenses.	$1299+ EARN YOUR OSEP Difficulty: ●●●●○

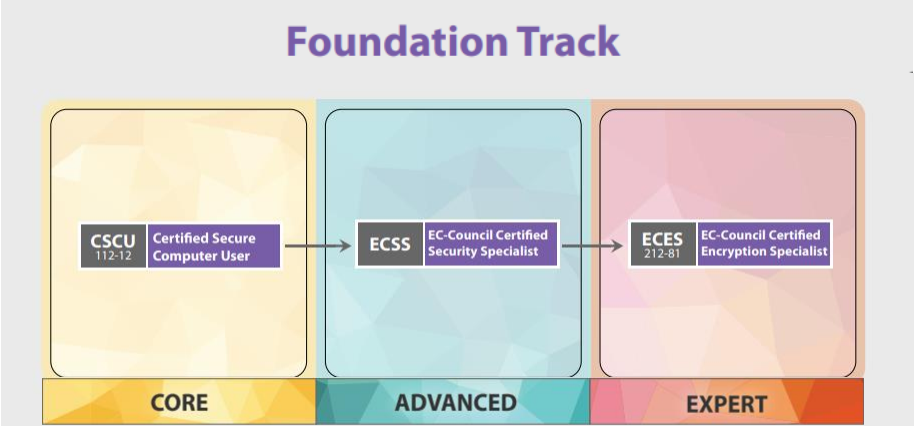
PENETRATION TESTING | WEB APPLICATION | EXPLOIT DEVELOPMENT

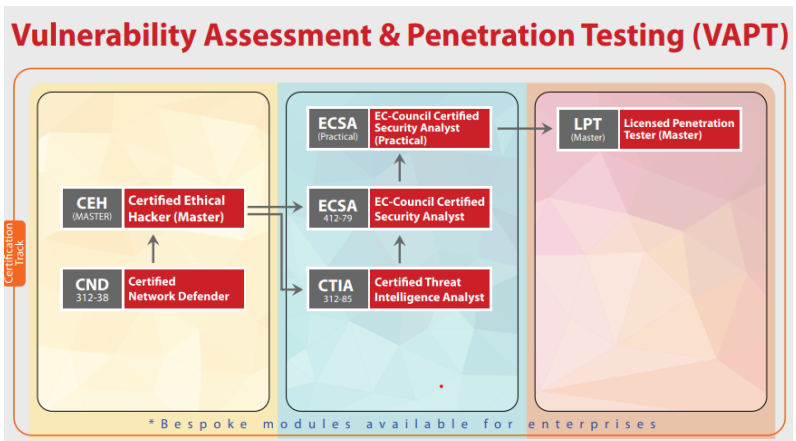
Course	Description	
	**WEB-300** ADVANCED WEB ATTACKS AND EXPLOITATION Specialize in web application security with WEB-300. From XSS attacks to advanced SQL injections, learn how to exploit and secure web apps using white box pentesting methods.	$999+ EARN YOUR OSWE Difficulty: ●●●●○

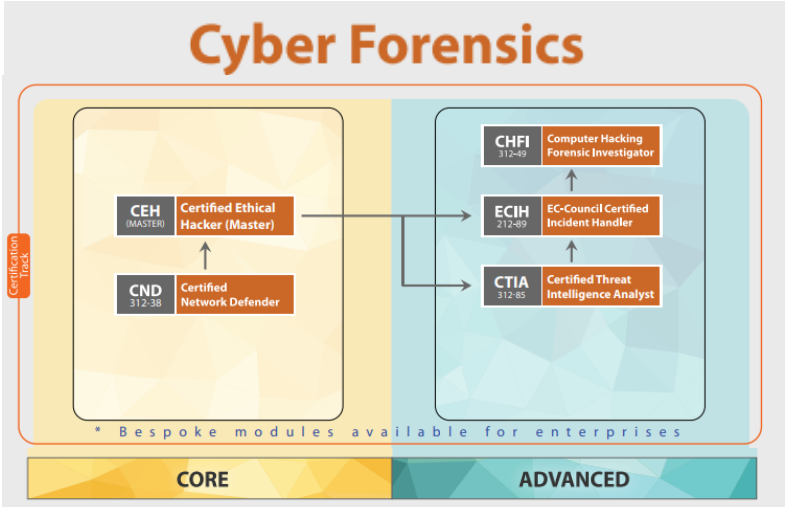
PENETRATION TESTING | WEB APPLICATION | EXPLOIT DEVELOPMENT

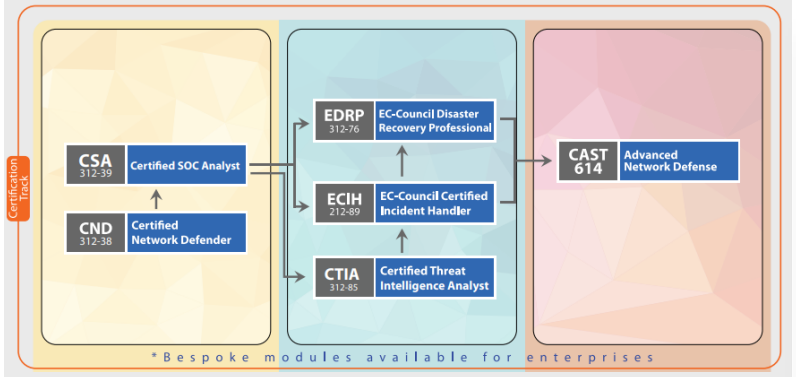
Course	Description	
	**EXP-401** ADVANCED WINDOWS EXPLOITATION EXP-401 is the most difficult course offered by Offensive Security. Tackle advanced topics such as DEP and ASLR evasion, heap spraying, function pointer overwrites, and more.	EARN YOUR OSEE Difficulty: ●●●●●

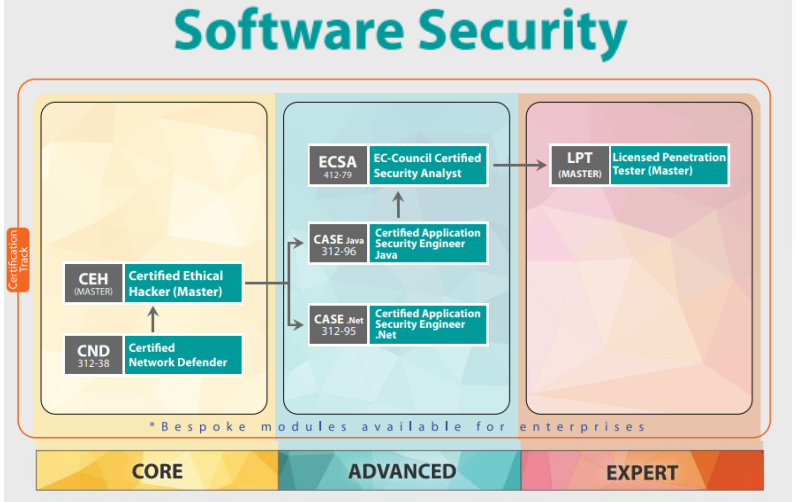
EC-COUNCIL







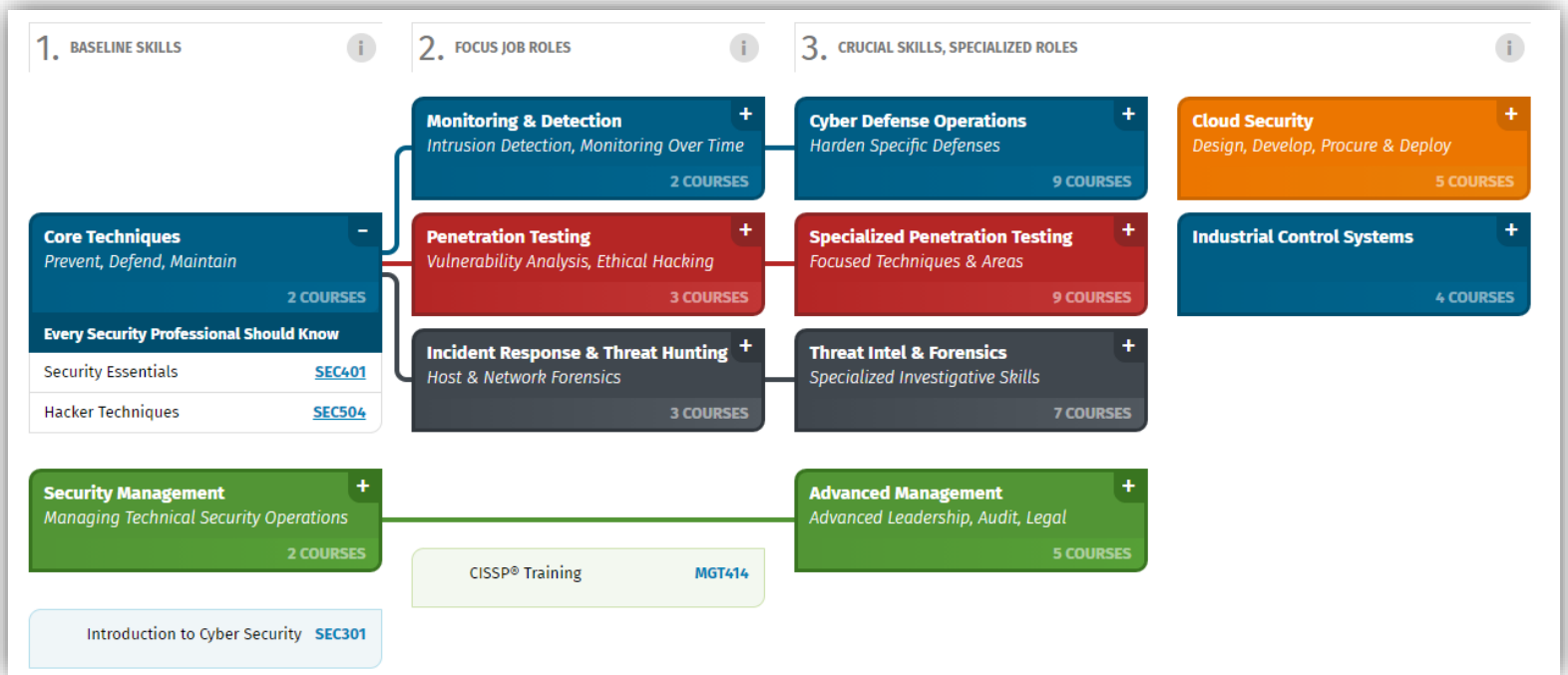




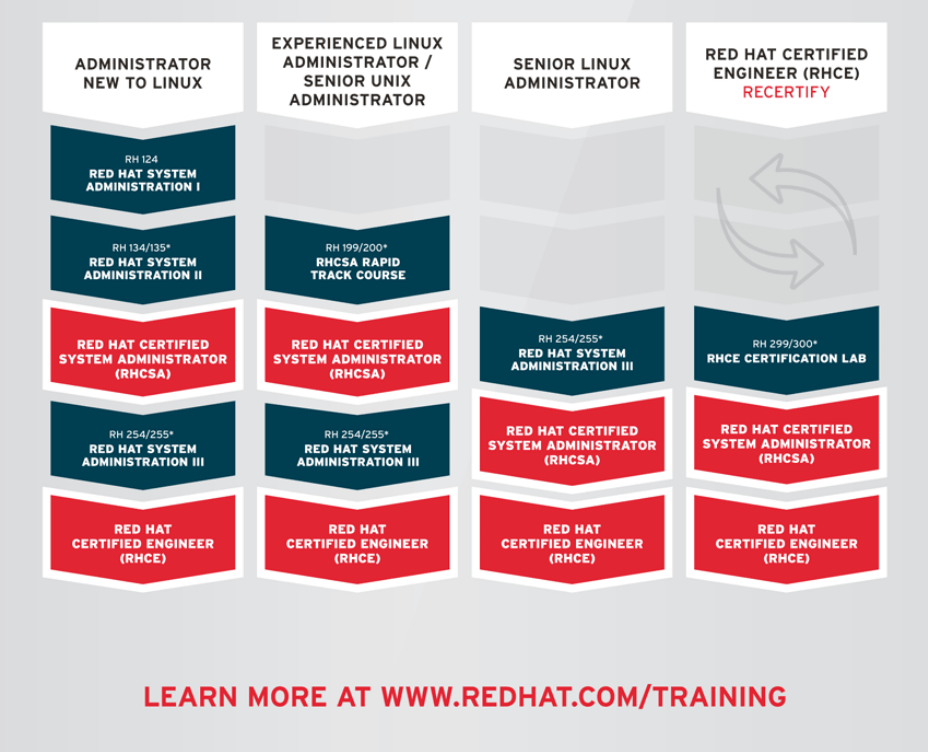
للمزيد من المعلومات عن التدريب و الشهادات : ملف من الشركة

قامت شركة SANS المعروفة بالتدريب في مجال الأمن السيبراني بتشكيل برنامج "شهادة ضمان المعلومات العالمية" (GIAC) ليصبح جهة الاعتماد التي تقدم شهادات للدورات التدريبية الخاصة بها

للمزيد من المعلومات عن التدريب و الشهادات: [موقع الشركة]



للمزيد من المعلومات عن التدريب و الشهادات: موقع الشركة



للمزيد من المعلومات عن التدريب و الشهادات: موقع الشركة

للمزيد من المعلومات عن التدريب و الشهادات: موقع الشركة

INSPIRING A SAFE AND SECURE CYBER WORLD.

CISSP - Certified Information Systems Security Professional

Summary: The most-esteemed cybersecurity certification in the world. The CISSP recognizes information security leaders who understand cybersecurity strategy, as well as hands-on implementation. It shows you have the knowledge and experience to design, develop and manage the overall security posture of an organization. Are you

SSCP - Systems Security Certified Practitioner

Summary: A global IT security certification. The SSCP recognizes your hands-on, technical abilities and practical experience. It shows you have the skills to implement, monitor and administer IT infrastructure using information security policies and procedures — ensuring the confidentiality, integrity and availability of data.

CCSP - Certified Cloud Security Professional

Summary: The premier cloud security certification. One of the hottest certifications on the market today. The CCSP recognizes IT and information security leaders who have the knowledge and competency to apply best practices to cloud security architecture, design, operations and service orchestration. It shows you're on the forefront of

CAP - Certified Authorization Professional

Summary: An information security certification aligning with the Risk Management Framework (RMF). The CAP recognizes your knowledge, skills and abilities to authorize and maintain information systems within the RMF. It proves you know how to formalize processes to assess risk and establish security documentation.

CSSLP - Certified Secure Software Lifecycle Professional

Summary: A global, vendor-neutral certification to recognize those with leading software and application security skills. The CSSLP recognizes your expertise and ability to incorporate security practices — authentication, authorization and auditing — into each phase of the SDLC.

HCISPP - HealthCare Information Security and Privacy Practitioner

Summary: A global healthcare security certification. It bridges healthcare information security and privacy like no other certification! The HCISPP recognizes your knowledge and ability to successfully implement, manage or assess security and privacy controls for healthcare and patient information. It proves you have a strong foundation in healthcare risk, security and privacy, and you understand important healthcare regulations.

CISSP - ISSAP - Information Systems Security Architecture Professional

Summary: Elite, specialized credentials that build upon the CISSP. These are optional pursuits for CISSPs who wish to prove their subject matter mastery. The CISSP Concentrations recognize your evolving expertise in information security architecture, engineering or management. As a CISSP-ISSAP, you prove your expertise developing, designing and analyzing security solutions. You also excel at giving risk-based guidance to senior management in order to meet organizational goals.

CISSP - ISSEP - Information Systems Security Engineering Professional

Summary: Elite, specialized credentials that build upon the CISSP. These are optional pursuits for CISSPs who wish to prove their subject matter mastery. The CISSP Concentrations recognize your evolving expertise in information security architecture, engineering or management. As a CISSP-ISSEP, you show your keen ability to practically apply systems engineering principles and processes to develop secure systems.

CISSP - ISSMP - Information Systems Security Management Professional

Summary: Elite, specialized credentials that build upon the CISSP. These are optional pursuits for CISSPs who wish to prove their subject matter mastery. The CISSP Concentrations recognize your evolving expertise in information security architecture, engineering or management. As a CISSP-ISSMP, you excel at establishing, presenting and governing information security programs. You also demonstrate deep management and leadership skills.

Associate of (ISC)² - Associate of (ISC)²

Summary: A unique designation to validate your skills and rapidly advance toward certification. The Associate of (ISC)² proves your knowledge in cybersecurity.

ISACA®
Trust in, and value from, information systems

CISA - Certified Information Systems Auditor

The CISA certification is world-renowned as the standard of achievement for those who audit, control, monitor and assess an organization's information technology and business systems. The recent quarterly IT Skills and Certifications Pay Index (ITSCPI) from Foote Partners ranked CISA among the most sought-after and highest-paying IT certifications. This certification is a must have for entry to mid-career IT professionals looking for leverage in career growth.

CRISC - Certified in Risk and Information Systems Control

ISACA's Certified in Risk and Information Systems Control™ (CRISC®) certification indicates expertise in identifying and managing enterprise IT risk and implementing and maintaining information systems controls. Gain instant recognition and credibility with CRISC and boost your career! If you are a mid-career IT professional with a focus on IT and cyber risk and control, CRISC can get you the leverage you need to grow in your career.

CISM - Certified Information Security Manager

ISACA's Certified Information Security Manager® (CISM®) certification indicates expertise in information security governance, program development and management, incident management and risk management. If you are a mid-career IT professional aspiring to senior management roles in IT security and control, CISM can get you the visibility you need.

CGEIT - Certified in the Governance of Enterprise IT

ISACA's Certified in the Governance of Enterprise IT® (CGEIT®) is unique and framework agnostic. It is the only IT governance certification that can give you the mindset to assess, design, implement and manage enterprise IT governance systems aligned with overall business goals. Get visibility at the executive level with CGEIT!

CSX-P - Cybersecurity Practitioner Certification

CSX®-P remains the first and only comprehensive performance certification testing one's ability to perform globally validated cybersecurity skills spanning five security functions – Identify, Protect, Detect, Respond, and Recover – derived from the NIST Cybersecurity Framework. CSX-P requires that candidates demonstrate critical cybersecurity skills in a live, proctored, virtual environment that assesses their analytical ability to identify assets and resolve network and host cybersecurity issues by applying the foundational cybersecurity knowledge and skills required of an evolving cyber first responder. For more information, see the CSX-P Exam Content Outline.

CDPSE - Certified Data Privacy Solutions Engineer

Modern privacy laws and regulations require organizations to implement privacy by design and by default into IT systems, networks, and applications. To do so, privacy professionals must partner with software developers, system and network engineers, application and database administrators, and project managers to build data privacy and protection measures into new and existing technology environments.

Available AWS Certifications

aws certified
Updated May 2019

Professional

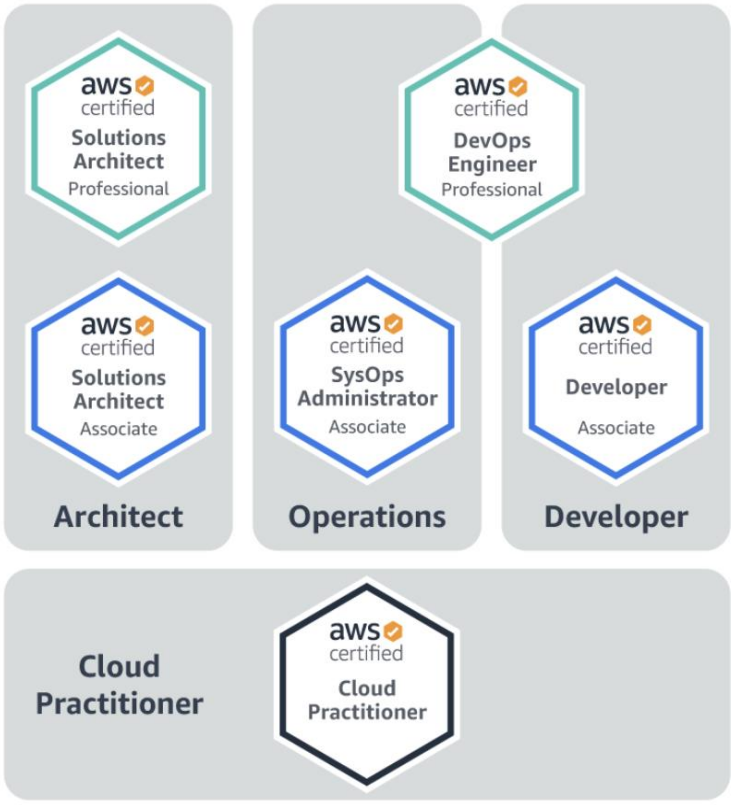
Two years of comprehensive experience designing, operating, and troubleshooting solutions using the AWS Cloud

Associate

One year of experience solving problems and implementing solutions using the AWS Cloud

Foundational

Six months of fundamental AWS Cloud and industry knowledge



Specialty

Technical AWS Cloud experience in the Specialty domain as specified in the **exam guide**

الخاتمة

أخيراً: لا تتردد في تعلم شيء معين (شبكات ، برمجة ، أنظمة تشغيل ، الإنجليزية ، ..) لأن التردد سيضيع وقتك و جهدك و لكن خصص وقتاً معيناً (أسبوعين مثلاً) للبحث و الإستفسار و شاور أهل الخبرة ثم صل الإستخارة و أبدأ فوراً بعد إنتهاء تلك المدة حتى لو لم تكن مستعداً تماماً .. لأنك مهما ارتكبت من الأخطاء في البداية فإنك مع الوقت سوف تصحح مسارك بنفسك وتلاحظ أن الأخطاء ستقل تدريجاً و هذا أفضل بكثير من إضاعة الوقت في التردد.

"و مُشَتَّتُ العَزَماتِ يُنفِقُ عُمرَهُ *** حَيرانَ لا ظَفَرٌ وَ لا إخفاقُ"

في الختام،، أرغب في التنويه على أن الموضوع يحتاج إلى طويل و صبر و إجتهاد، لذا فإياك أن تيأس و تستسلم أمام الصعاب و سترى نتائج عظيمة بإذن الله

تم بحمد الله في : 1442/05/21 الموافق 2021/01/15

آخر تحديث : لا يوجد