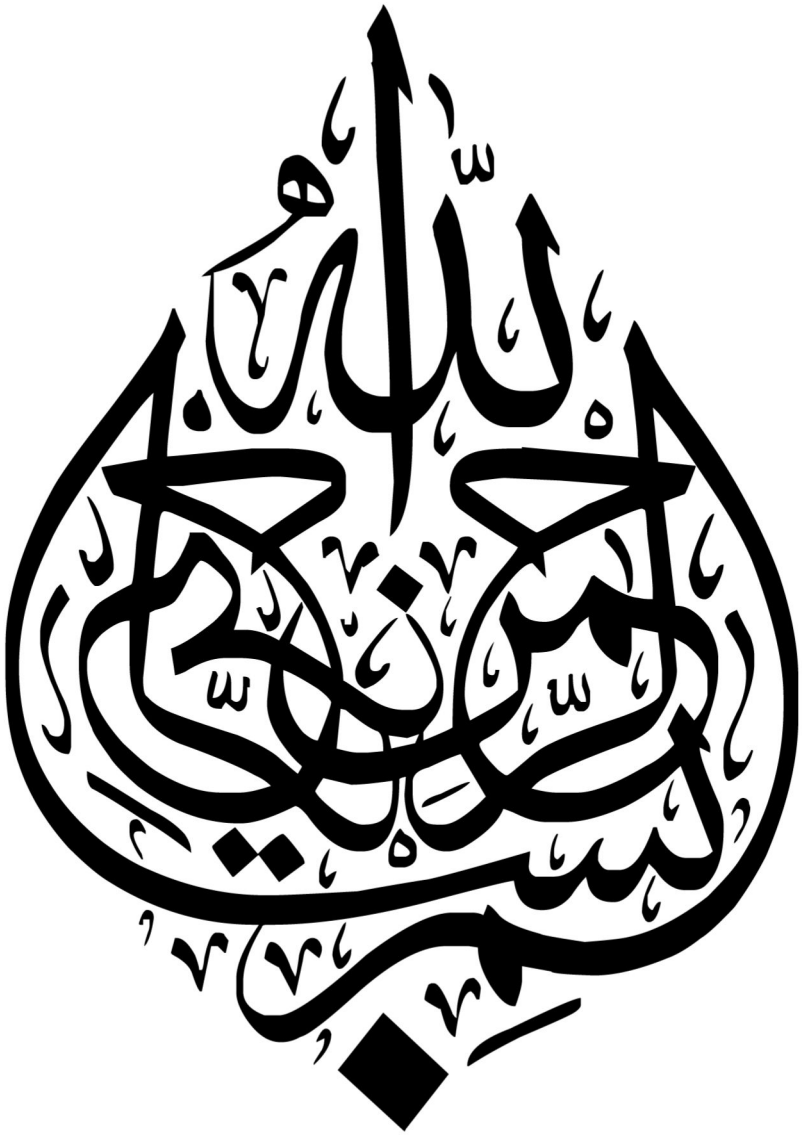
أسئلة و أجوبة عن الهاكرز

كتابة: عبد المهيـــــمن الآغا

تنسيق على شكل كتاب: مدونة علوم



في كل يوم أفتح به ايميلي أشاهد العديد من الأسئلة المتكرّرة التي تصلني بشكل مستمر عن طريق المدونة, البعض يسألني كيف يصبح هاكر ومن أين يجب أن يبدأ وآخر يستفسر عن ضرورة تعلّم البرمجة ولغة البرمجة التي يجب أن يتعلّمها وفائدة استخدام نظام لينوكس بالاضافة للعديد من الأسئلة الأخرى.. غالبا كنت أرسل هاؤلاء الأشخاص للمقال الذي كتبه Eric S. Raymond بعنوان How to become a hacker يوجد له ترجمة عربية أيضا لكنها قديمة بعض الشيء. من خلال تصفحي للانترنت واستماعي لآراء البعض لاحظت أن الكثيرين من الأشخاص لا يعلمون الوصف الصحيح للقب هاكر ولا يعلمون من هو الهاكر أساساً.

بصراحة لم أكن أريد أن أكتب عن هذا الموضوع فالمقال الذي كتبه رايموند أكثر من كافي لكن بسبب كثرة هذه النوعية من الأسئلة وتكرار الردود التي أرسلها دائما قررت أن أكتب هذا الموضوع بعد صياغته بطريقة أخرى ومن وجهة نظر شخصيّة! الموضوع طويل بعض الشيء ونظري بحت! عكس الطابع الذي أفضّله والذي اعتدت على كتابته في المدونة لذلك أنصح أن قرائته بتأني عندما تمتلك الوقت الكافي.

في البداية من هو الهاكر؟

- في وسائل الاعلام وعند أغلبية مستخدمي الانترنت الهاكر هو الشخص الذي يخترق الأجهزة والمواقع, من يسرق المعلومات ويبرمج الفايروسات وغالبا يتم تصويره على أنه الشخص الشرير الذي يستمتع بايذاء الآخرين.
- في الجهة المقابلة يأتي رايموند وغيره من الهاكرز ليقولوا أن من يقوم بهذه الأفعال ليسوا هاكرز بل هم مخربين (Crackers) لأن الهاكرز الحقيقيين هم المبرمجين الذين أوصلوا نظام لينوكس لما هو عليه الآن والخبراء الذين يستمتعون بحل المشاكل (تمكّنهم خبرتهم من الاختراق واكتشاف الثغرات لكنهم لا يستخدموها في التخريب).

لمن لا يعلم.. الهاكرز مقسومين لثلاث أصناف:
1. White Hat Hackers: أصحاب القبعات البيضاء ويعرفوا أيضا بالـ Ethical Hackers أو الهاكر الأخلاقي. هذا الشخص يملك خبرات ومهارات الهاكرز وهو قادر على اختراق الأنظمة والشبكات بنفس الأسلوب والأدوات التي يستخدمها المخترقين لكنّه يستغل خبرته في الأمور الجيدة كأن يبلّغ الشركات عن وجود ثغرة في احدى منتجاتها أو يعمل Penetration Tester أو مسؤول الحماية في احدى الشركات.

2. Black Hat Hackers: أصحاب القبعات السوداء وحسب وجهة نظر رايموند يجب اطلاق لقب Crackers عليهم وليس Hackers فهاؤلاء الأشخاص يستغلون معرفتهم وخبراتهم في الأمور التخريبية ويخترقون المواقع والسيرفرات بغرض المتعة واثبات

الوجود أو لغايات أخرى غالبا تكون غير شرعية كالابتزاز وسرقة المعلومات أو اختراق مواقع الشركات بغرض تدمير سمعتها...

3. Gray Hat Hackers: أصحاب القبعات الرماديّة, يمكننا القول أنهم هاكرز أخلاقيين أيضاً وهم يشبهون الصنف الأول (أصحاب القبعات البيضاء) كثيراً لكن بنفس الوقت قد يقوموا ببعض الاختراقات بغرض التحدي مثلاً أو لاثبات وجود ثغرة أو في حال مخالفة إحدى مبادئه أو لايصال رسالة معيّنة...

الآن ماذا نستنتج؟ الأصناف الثلاثة السابقة هم "هاكرز" يملكون الخبرة والمعرفة التي تمكّنهم من الاختراق لكن المبادئ التي يسيرون عليها والغايات مختلفة..!

أما الأشخاص الذين يدّعون أنهم هاكرز فيطلق عليهم لقب أطفال الهاكرز, Script Kiddies أو Lamers وغالباً نجد هذا النوع منتشر بالمنتديات, يقوم بالأعمال التخريبية بشكل "همجي", يسير على مبدأ من يخترق أكثر هو الأقوى! غالباً نجدهم يبحثون عن الشهرة عن طريق اختراق الأجهزة والمواقع الضعيفة بشكل عشوائي. السؤال الذي يطرح نفسه هو طالما أن هاؤلاء الأشخاص تمكنوا من الاختراق لماذا ليسوا هاكرز؟ ببساطة لأنهم لا يملكون أي معرفة علمية! فهم يجيدون استخدام بعض البرامج والأدوات واستغلال الثغرات الجاهزة التي برمجها واكتشفها الهاكرز "الحقيقيين" لكنهم ليسوا قادرين على برمجة أدواتهم واكتشاف ثغراتهم الخاصة وليسوا قادرين على تطوير طرق وأساليب جديدة أي أنهم عبارة عن "مستخدمين" فقط.

دائماً أقول وأكرر لقب هاكر ليس بسيط ليتم اطلاقه على أي شخص! فلتصبح مبرمج يكفي أن تتعلم لغة برمجة واحدة وتبدأ البرمجة بها, لتصبح مصمم يكفي أن تجيد استخدام برنامج أو اثنين في التصميم, لتصبح مدير سيرفرات يكفي أن تعلم كيف تتعامل مع سيرفر ويندوز أو لينوكس مثلاً, أما لتصبح هاكر عليك أن تجيد جميع الأمور السابقة بنفس الوقت! قبل أن تصبح هاكر عليك أن تكون مستخدم محترف قادر على ايجاد طريقك وحل المشاكل التي تصادفك فكيف ستتمكن من اختراق نظام ان لم تكن مستخدم محترف له تعلم كيف يعمل هذا النظام وما هي أسراره ونقاط ضعفه؟ كيف ستتمكن من اكتشاف ثغرة وبرمجة استغلال لها اذا لم تكن تعلم كيف تبرمج؟ لتكون هاكر عليك أن تكون أذكى من المبرمج الذي وقع بالخطأ الذي أدى للثغرة وأكثر معرفة من مدير السيرفر الذي اخترقت نظامه, الأغلبيّة يظنوا أن معرفة استخدام بعض الأدوات واستغلال الثغرات الجاهزة تجعل من الشخص هاكر! لكن هذا الأمر ليس صحيح فالهاكر هو من بنى خبرته على علم ومعرفة حقيقية.

لماذا تريد أن تصبح هاكر؟

يجب عليك أن تسأل نفسك هذا السؤال وتفكّر به جيّداً, اسأل نفسك ماذا تريد أن تصبح؟

وكم هي المسافة المستعد لسيرها لتصبح "هاكر"؟ اذا كنت تريد تعلّم اختراق الأجهزة والمواقع فقط ليقول الآخرين عنك أنك هاكر أو لأنك تظن أن اختراقك للمواقع سيجعل الآخرين يحترموك ويخافون منك فاعلم أن ما ستقوم به هو مضيعة للوقت! قد تستطيع خلال فترة زمنية قصيرة أن تخترق بعض الأجهزة والمواقع الضعيفة لكن هذا لن يجلب لك الاحترام الذي تبحث عنه, اذا لم تكن ترغب باحتراف مجال الهاكر وتحمّل الأمور المترتبة على ذلك أنصحك ألا تبدأ وألا تضيع وقتك من الأساس.
أما اذا كنت تريد أن تصبح هاكر حقيقي أو اخترت الحماية والاختراق كمجال مهني تريد احترافه فيجب أن تعلم أن الطريق الذي اخترته طويل وليس بالبساطة التي يتصوّرها البعض. فبذلك أنت ستحتاج لتعلم واحتراف العديد من الأمور المختلفة بنفس الوقت بدءً من الشبكات, ادارتها وحمايتها مروراً باحتراف لينوكس وأنظمة التشغيل المختلفة انتهاءً بالبرمجة, اكتشاف الثغرات والهندسة العكسية وقد تصل للهندسة الاجتماعية وأساليب التلاعب بالأشخاص أيضا! الحقيقة لا أحد يستطيع أن يصبح هاكر بين يوم وليلة أو خلال بضعة أيام أو حتى شهور فتعلّم جميع الأمور التي ذكرتها سابقاَ ليس بالبساطة التي قد يتصوّرها البعض ويحتاج صبر واصرار كبيرين.

من أين وكيف أبدء؟

فعليّاً لا يوجد خطوات محددةّ أو تسلسل يجب أن تسير عليه لتصبح هاكر لكن يجب أن تعلم أنه من الضروري أن تكون البداية صحيحة فهي التي ستحدد ماذا ستصبح لاحقاً! الكثيرين من الهاكرز يبدأون بشكل خاطئ وأغلبهم كان Lamer قبل أن يصبح Hacker فتجدهم يبدؤون بتعلم كيفية سرقة الايميلات باستخدام الصفحات المزوّرة ثم الانتقال لاختراق الأجهزة عن طريق استخدام Key loggers وبرامج جاهزة تستخدم لهذا الغرض مثل Bifrost و Poison Ivy وغيرهم من البرامج الأخرى بعد ذلك يتطوّر هاؤلاء الأشخاص قليلاً ويتعلمون كيف يتم استغلال ثغرات المتصفح التي تحتوي على جملة "ضع رابط الباتش هنا!!!" ثم ينتقلون لاختراق المواقع عن طريق تعلم استغلال بغض ثغرات لغة php مثل SQL Injection وتعلّم استخدام "الشيل" (php shell) مثل C99, r57 وغيرهم من الأدوات. لكن غالباً يتوقّف هاؤلاء الأشخاص عند هذا الحد لاعتقادهم أنهم أصبحوا هاكرز وبسبب انشغالهم باختراق المواقع الضعيفة بشكل عشوائي (لغايات ومبادئ مختلفة) والتسابق لتجميع أكبر عدد من الأجهزة المخترقة والسير على مبدأ من يخترق أكثر هو الأقوى!! وحسب ما لاحظت قد يهتم بعضهم باختراق الشبكات بغرض التجسس عليها عن طريق استخدام بعض أدوات الـ Sniffers وتطبيق هجمات ARP/DNS Spoofing وبعضهم يتعّلم كسر تشفير شبكات الوايرلس وآخرين يستخدمون مشروع ميتاسبلويت لاختراق الأجهزة الغير محدّثة بالشكبة وكل ذلك باستخدام برامج وأدوات جاهزة لا أحد منهم يعرف مبدأ عملها وكيف برمجت أساساً!!
على ماذا حصلنا الآن؟ ببساطة نحن لم نحصل على هاكر بل على شخص يجيد استخدام

على ماذا حصلنا الآن؟ ببساطة نحن لم نحصل على هاكر بل على شخص يجيد استخدام أدوات الهاكرز لكنه لا يملك أي معرفة علمية! حسب ما لاحظت قلّة قليلة يفكّرون بتطوير أنفسهم أكثر ويتجهون للطريق الصحيح عن طريق تعلّم البرمجة واكتشاف الثغرات, احتراف نظام لينوكس, تعلّم الهندسة العكسية, ادارة الشبكات, الحماية... وبذلك يبدأ هذا الشخص بالسير على الطريق الصحيح ليصبح هاكر ويدرك لاحقاً أن ما كان يقوم به سابقاً عبارة عن "لعب أطفال" لكن بعد أن يكون قد ضيّع شهور وسنين من عمره في الاختراق العشوائي بدون جدوى تذكر.
تعلّم مبادئ الشبكات واحتراف التعامل مع أنظمة التشغيل وتعلّم البرمجة أمر ضروري ليصبح الشخص هاكر لأنها الأساس, بعد ذلك يأتي تعلّم استخدام الأدوات التي يستخدمها الهاكرز ثم تعلم استخدام أنظمة الحماية لتعرف كيف تتخطاهم عند الحاجة وهذا يتطلّب دراسة موسّعة وتعلّم الأمور المنخفضة المستوى وأدق التفاصيل عنها مثلاً في الشبكات لتتعلّم كيف تستخدم نظام لحماية الشبكة أنت بحاجة لاجادة ادارة سيرفر لينوكس أو ويندوز مثلا ومعرفة بكيفية عمل الشبكات أولاً, عندما تفكّر بتعلّم طرق لتخطي أنظمة الحماية أنت بحاجة لاحتراف هذا النظام ودراسة مبدأ عمله وقوانية ثم دراسة بروتوكول TCP/IP والأمور المنخفضة المستوى في تحليل الـ Packets وهكذا في كل أمر تريد احترافه والتوسّع به... ستحتاج لتعلّم العديد من الأمور بنفس الوقت لتحترف شيء واحد.
لاحظ أنه عندما تبدأ في مجال الهاكر يجب أن تعلم أنه لا يوجد توقّف! لأن عالم الحماية والاختراق يتطوّر بسرعة كبيرة ويجب عليك تحديث معلوماتك, البرامج والأدوات المستخدمة بالاضافة للأساليب التي نستخدمها أولاً بأول والا بعد مرور أقل من سنة واحدة لن يكون هناك قيمة فعليّة للأمور التي تعلمتها سابقاً.

لماذا يجب أن أحترف استخدام نظام لينوكس؟

الهاكر ليس مرتبط بنظام تشغيل محدد وبجميع الأحوال يجب عليك أن تتعلم كيف تتعامل مع أكثر من نظام تشغيل ونظام جنو/لينوكس هو الأكثر أهميّة. ليس لأنه لينوكس وليس لأني من مستخدمي هذا النظام أو تعصّب كما يعتقد البعض بل لأنه يشكّل بيئة العمل الأفضل للهاكرز فهو يحتوي على جميع البرامج والأدوات التي ستحتاجها في عملك أضف الى ذلك أن بعض البرامج والأدوات لا تعمل الا على نظام لينوكس وبشكل عام لغات البرمجة التفسيريّة مثل Python , Perl , Ruby تعمل بشكل أفضل على نظام لينوكس من ويندوز وهذا يعني أن الأدوات التي برمجت بهذه اللغات بكل تأكيد ستعمل على نظام لينوكس بشكل أفضل! كما أن نظام لينوكس منتشر بشكل كبير خصوصا في مجال السيرفرات والشبكات وعندما أقول يجب تعلّم نظام لينوكس أنا لا أقصد معرفة أساسيات النظام وتعلم تنفيذ بضعة أوامر وحسب بل أقصد الوصول لدرجة الاحتراف فيه! نظام لينوكس سيعلّمك الكثير من الأمور التي كنت تجهلها في نظام ويندوز وباقي الأنظمة الأخرى, ستتعلم كيف يعمل النظام وكيف ترتبط الأمور مع بعضها وهذه

المعلومات مفيدة لك كهاكر! "فعليّاً كل شيء تتعلمه بمجال الكمبيوتر سيفيدك بالهاكر بطريقة أو بأخرى" أما السبب الجوهري لاستخدام نظام لينوكس هو أنه نظام حر ومفتوح المصدر (قد لا تكون مبرمج قادر على تطوير النظام لكن يكفي أن تعلم أن آلاف الخبراء من المبرمجين اطلعوا على الكود المصدري قبلك وآلاف غيرهم يعملون على تحسينه وتطويره بشكل مستمر) هذا يعني أن نظام لينوكس والبرامج المفتوحة المصدر بشكل عام أأمن وأكثر موثوقية من البرامج والأنظمة المغلقة المصدر وهذا الأمر يجب أن تنتبه له جيداً..!

عل كل حال لا أريد تحويل الموضوع لأي نظام أفضل وأنا لست من النوع الذي يتعصّب لشيء ويطلق أحكاماً بدون تجربة مطوّلة وشخصيا أنا مقتنع تماما أن كل نظام يتميز عن الآخر ببعض الأمور لكن نظام لينوكس يتفوّق على ويندوز بالمجال الذي اخترناه ولذلك من المهم احترافه.

هل يجب أن أستغني عن ويندوز؟

لا يوجد أي ضرورة لذلك واستخدامك لنظام لينوكس لا يعني أن نظام ويندوز بهذا السوء! فنظام ويندوز هو الأكثر انتشاراً بين المستخدمين هذا يعني ضرورة احترافك التعامل مع نظام ويندوز قبل التفكير باستخدام غيره! كما أن بعض البرامج الاحترافية (غالباً تجارية) التي نستخدمها في الـ Penetration Testing تعمل على نظام ويندوز فقط ولا يوجد لها اصدارات للأنظمة الأخرى وكهاكر يجب أن تستفيد من أغلب الأدوات والبرامج الموجودة (ان كانت مجانية أو تجارية) بأقصى درجة ممكنة ولذلك يجب أن توفّر بيئة العمل المناسبة لهذه الأداوت ان كان نظام التشغيل لينوكس, ويندوز أو أي نظام آخر وتذكّر دائماً أن النظام وسيلة وليس غاية! فنحن لا نحتاج النظام بحد ذاته بقدر حاجتنا للبرامج والأدوات التي تعمل عليه. يمكن تنصيب النظامين على نفس الجهاز أو تخصيص جهازين منفصلين لكل نظام أو حتى استخدام نظام ويندوز عند الحاجة لاحدى برامجه فقط عن طريق احدى برامج الأنظمة التخيّلية المتوفرة لنظام لينوكس مثل Virtual Box أو VMware وبهذه الحالة ستحصل على نظام ويندوز وجميع برامجه داخل نظام لينوكس (شخصياً أجد هذا أفضل الحلول في حال اعتمدت لينوكس كنظام أساسي في جهازك).

لماذا تعلّم البرمجة أمر ضروري؟

لأنك ستحتاجها في العديد من الأمور لكن للدقة درجة الاحترافية ستختلف بحسب التخصص الذي تريد أن تحترفه. الهاكر ليس قسم واحد بل هو بحر بحد ذاته ويوجد له

تخصصات فاذا أردت أن تكون Penetration Tester مثلا بهذه الحالة مهمتك ستكون اختبار امكانية اختراق النظام عن طريق استخدام نفس البرامج والأدوات التي يستخدمها الهاكرز (تركيزك سيكون على الـ Vulnerability Assessment) وهنا كل ما تحتاجه من البرمجة معرفة بسيطة في حال احتجت لبرمجة استغلال ثغرة أو تعديل استغلال مبرمج مسبقاً أو لبرمجة أداة تقوم بمهمة معيّنة تحددها أو لتقوم ببعض المهام بشكل أوتوماتيكي وهذا ضروري لاختصار الوقت طبعاً. أما اذا أردت اكتشاف ثغرات تطبيقات الويب في سكريبتات PHP مثلاً بهذه الحالة يجب عليك تتعلّم أساسيات هذه اللغة والتركيز على الجانب الأمني المتعلّق بكيفية تعامل السكريبت مع مدخلات المستخدم, فلترتها, ادخالها لقواعد البيانات وعرضها ثم ستتطوّر أكثر وتنتقل لثغرات Clinet Side-Attack وبهذه الحالة سيصبح هدفك المستخدم وليس السكريبت بحد ذاته لذلك قد تضطّر لتعلم أساسيات لغة Javascript وتعلم مبدأ عمل ثغرات XSS و CSRF مثلاً ثم تنتقل لتعلم اكتشاف ثغرات المتصفّح والبرامج والخدمات بشكل عام وهذا هو الجزء الأصعب لأنك انتقلت لمرحلة مختلفة تماماً عن لغة php وأنواع الثغرات السابقة وهذه المرحلة تتطلّب منك معرفة قويّة باللغات المنخفضة المستوى مثل لغة C و Assembly بالاضافة لاجادة الهندسة العكسية Reverse Engineering والتعامل مع برامج التنقيح (Debugging) وتتبع الأخطاء مثل IDA Pro , OllyDBG , DDD , GDB... عليك أن تعلم كيف يتعامل البرنامج والنظام مع الذاكرة, لماذا ومتى حدث Buffer Overflow مثلا وهل نستطيع استغلال هذا الخطأ للتحكم بسير البرنامج وتشغيل Shellcode يمكننا من اختراق النظام أم أنها ستؤدي لتوقفه عن العمل فقط, هل يستخدم النظام تقنيات تمنعنا من استغلال الثغرات وما هي التقنيات التي نستطيع استخدامها لتخطي الحماية وتطوير الاستغلال؟... كل هذا ان دل على شيء فهو يدل على أن البرمجة ضرورية بل ضرورية جداً وكلما تطوّر مستواك في مجال الحماية والاختراق ستحتاج لاحتراف البرمجة أكثر.

أي لغة برمجة يجب أن أختار؟

لغات البرمجة كثيرة واختيار لغة البرمجة المناسبة قد بكون محيّر للكثيرين, شخصياً لا أنصح بالبدء بلغة C/C++ أو Assembly لأن هذه الغات منخفضة المستوى وهذا يعني أنها أصعب في التعلم وستحتاج مدة ليست بالقصيرة حتى تصبح قادر على البرمجة والانتاج بها لكن لا تنسى أنهم لغات ضرورية بنفس الوقت وستحتاج لتعلمهم عاجلاً أم آجلا (حتى ان اخترت أن تكون Penetration Tester يجب أن تتعلم الأساسيات على الأقل وعندما تقرأ كود مصدري لاحدى البرامج يجب أن تعلم كيف تتبّعه وترجع للمكتبات المستخدمة لتعرف ماذا يفعل) وبنفس الوقت أنصح بالابتعاد عن اللغات الضعيفة أو المرتبطة بنظام تشغيل واحد مثل Visaul Basic وكبداية أنصح وبشدة تعلّم احدى اللغات التفسيرية مثل Perl, Python, Ruby... لأنك ستحتاجها كثيراً وتسهّل عليك الكثير من الأمور كما أنها تغنيك عن أغلب لغات البرمجة الأخرى وتستطيع باستخدامهم برمجة

أي شيء تريده تقريباً. طبعاً لا أستطيع أن أقول أي لغة برمجة هي الأفضل لأن المقارنة بين لغات البرمجة بشكل عام أمر خاطئ فكل لغة تتميز عن غيرها ببعض الأمور لكن ان أتيتم لرأيي الشخصي سأستبعد بيرل وأختار لغة روبي أو بايثون فاللغتين بقوّة بعض تقريباً مع العلم أن لغة روبي أسهل قليلاً من بايثون ومفهومة بشكل أكبر لكن بايثون مستخدمة بشكل أكثر ومجتمعها أكبر وتأتي منصّبة بشكل افتراضي في أغلب توزيعات نظام لينوكس أما بالنسبة للغة بيرل فلقد كانت الخيار الأول للهاكرز في السنين الماضية لكن الآن أتوقع أن الوضع اختلف قليلاً.
بعد تعلّمك لاحدى اللغات التفسيرية السابقة سيكون من السهل عليك الانتقال للغة الأخرى وتعلمها لكن نصيحة اكتسبتها من تجربة شخصية لا تضيّع وقتك بالانتقال من لغة برمجة الى أخرى الا اذا كانت لغة البرمجة التي تتعلّمها غير قادرة على تحقيق ما تريد. لا تستمع للمهاترات التي تتكلم عن أي لغة برمجة أفضل وأي لغة هي الأقوى!

كيف أطوّر نفسي ومن أي أحصل على المساعدة؟

بالنسبة لي أفضّل ألا أسأل ولا أطلب المساعدة من أحد الا بالحالات القصوى! قد يجد البعض أن هذه النصيحة غريبة لكن ان أتيتم للحقيقة لا شيء سيجعلك هاكر الا اتباع النصيحة السابقة, في كثير من المواضيع التي أكتبها في مدونتي أجد شخص واحد طرح أكثر من 10 أسئلة (كل أمر ينفّذه, كل خطوة يقوم بها, كل رسالة خطأ تظهر له يكتب سؤالاً عنها!!) موضوع طرح الأسئلة لا يزعجني لكن بالطريقة التي يتبعها هذا الشخص (الاطعام بالملعقة) لن تحقق له الفائدة بالقدر التي ستحققها التجربة والاعتماد على نفسه. قد أكون موجود اليوم وأستطيع الاجابة على بعض الأسئلة أو قد يجد غيري يجيبه ويعطيه الحل على الجاهز لكن من يعلم ماذا سيحدث غداً؟ الهاكر هو الشخص القادر على حل المشاكل هذا يعني أنه يملك خبرة كبيرة في مجالات مختلفة وهذه الخبرة لن تأتي من طرح الأسئلة واحداً تلو الآخر أو الاعتماد على الآخرين في حل المشاكل! بل تأتي من القراءة, البحث الطويل والتجراب المتكرّرة. اعتمد على نفسك في ايجاد الحلول, إن واجهتك مشكلة في الشبكة, نظام التشغيل أو حتى في احدى البرامج والأدوات التي تستخدمها. حاول التفكير بالحل وجرّب أساليب وطرق مختلفة, اقرأ الوثائق وملفات المساعدة المرفقة (رغم أن أكثرها ممل لكن غالباً ستجد الحل فيها), في حال يأست ابدأ بالبحث عن أشخاص واجهوا نفس المشكلة وما هي الأمور التي قاموا بتنفيذها لحل المشكلة (نسخ رسالة الخطأ والبحث عنها في Google ليس بهذه الصعوبة!), جرّب الحل/الطريقة المطروحة مرة واثنتين وثلاثة و مئة! لا تكتفي بالحل فقط بل حاول أن تفهم سبب المشكلة ولماذا هذا الحل هو المفتاح. في حال لم تجد جواب (غالبا ستجد الا في بعض الحالات النادرة والأمور المتقدمة) اعرض المشكلة في احدى المنتديات أو المواقع المتخصصة مع ضرورة ذكر كافة التفاصيل ونتائج البحث

والتجارب التي قمت بها (لا أحد يحب أن يساعد شخص يريد كل شيء جاهز ولم يكلّف نفسه عناء البحث!!) ثم ناقش الأمر معهم حتى تجد الحل الصحيح للمشكلة. في حال يأست لم تتوصّل لحل يأتي دور مراسلة شخص مختص بهذه الأمور أو مبرمج الأداة التي حدثت بها المشكلة. في كثير من الأوقات أقضي ساعات وأيام كاملة لحل مشكلة وبنفس الوقت أنا أعرف شخص متأكد أنه قادر على حلها خلال دقائق لكني لا أفضّل أن ألجئ اليه مباشرة الا اذا كنت أحتاج الحل بشكل سريع أو اذا يأست من ايجاد الحال الصحيح.

هل يوجد مواقع محدّدة أنصح بها؟

كثير من الأشخاص يسألوني هذا السؤال ويعتقدون أني أملك مواقع سريّة لكن الواقع لا يوجد شيء من هذا! أنا لا أعتمد على مواقع محددة بل أعتمد على Google في كل شيء تقريباً, عندما أقول لأحد استخدم جوجل هذا لا يعني أني لا أريد مساعدته لكنه الواقع (لماذا أحصر نفسي في موقع محدد اذا كان Google يظهر لي أفضل المواقع بحسب الموضوع الذي أبحث عنه؟) المضحك أن البعض أصبح يستخدم كلمة Private دون وعي ودون أن يعلم معناها! فأصبحنا نرى برنامج له موقع Private و ثغرة صدرت وانتشر استغلالها من عدة أشهر Private وأصبحت طريقة استخدام احدى الأدوات Private ووو... مع العلم أن كل ذلك موجود على الانترنت وبشكل علني!! أغلب الأمور التي تعلمتها وتعلّمها غيري عن طريق المصادر الموجودة في الانترنت بالاضافة للتجربة والخبرة التي تأتي مع مرور الوقت بعد ذلك عندما يتخطى الشخص مرحلة التعلّم ويبدأ بالاكتشاف وتطوير أساليب جديدة كأن يكتشف ثغرة في احدى خدمات نظام لينوكس ولا يبلّغ عنها أو ينشر كود الاستغلال فيمكننا القول أنه يملك ثغرة برايفت.
بالنسبة لي أنا أكتب في مدونتي وفي موقع iSecur1ty حيث ستجد فيهم العديد من المواضيع والمقالات بالاضافة لشروحات الفيديو التي ستعلّمك الكثير من الأمور بشكل صحيح. أما بالنسبة لمنتديات الهاكر الموجودة حالياً فأنا لا أتابع أي منهم وبعد قيامي بجولة سريعة لاحظت أن أغلب المواضيع التي تكتب فيهم تطرح المعلومة بشكل خاطئ أو يكون الموضوع منقول من بعض المواقع الأخرى أو قديم جداً و في أحسن الأحوال يكون الموضوع مترجم حرفياً من بعض المواقع الانكليزية!!

أخيراً.. كون الموضوع متشعّب ويناقش عدّة فقرات وطويل نوعاً ما فمن المحتمل أن أكون وقعت بأخطاء في بعض التعابير أو أنقصت احدى الأمور, لذلك قد أقوم بتعديل هذا الموضوع وتنقيحه واضافة بعض الفقرات عليه بين الحين والآخر.

تنسيق مدونة علوم

http://www.33loum.blogspot.com