@A.DEVE.LOPMENT

أسرار الإختراق

رحلة المخترق من تحديد الهدف إلى
دخول النظام.

علي الوائلي

المقدمة

هل سألت نفسك يوماً عن الخطوات التي يتبعها الهكر عندما يقوم بالإختراق؟ أم هي مجرد محاولات عشوائية بعضها ينجح والآخر يفشل؟، في الحقيقة هم يتبعون خطوات معينة، توجد خمس خطوات متعارف عليها يتبعها معظم المخترقين حول العالم.

بعد قراءتك لهذا الكتاب ستكون لديك خلفية واضحة عن طريقة الإختراق وعن خطوات الإختراق، هذه الخلفية ستساعدك في استيعاب كل ماتتعلمه عن مجال أمن المعلومات والإختراق الأخلاقي، وكذلك سيساعدك كثيراً في ربط كل ما تتعلمه.

خطوات الإختراق

كما قلنا توجد خمسة خطوات يتبعها معظم المخترقين حول العالم، سنتطرق إلى جميع هذه الخطوات بالتفصيل.

لنفترض أنك تريد إختراق موقع اسمه "example.com" أخلاقياً، إلى الآن لا تملك معلومات عن الموقع غير الاسم.

الخطوة الأولى: Reconnaissance

وتعني الإستطلاع، وهي عبارة عن جمع معلومات عن الموقع من خلال محرك البحث أو حسابات منصات التواصل الإجتماعي. قد تستصغر من هذه الخطوة، ولكنها من أهم الخطوات، ماذا ستفعل بدون هذه المعلومات؟

تستطيع القيام بهذه المهمة يدوياً ولكنك ستستغرق الكثير من الوقت، لذلك يفضل أن تستخدم بعض الأدوات التي ستسهل وتسرع العملية، أين تجد هذه الأدوات؟ بالطبع تستطيع البحث عن هذه الأدوات والتي تسمى OSINT tools، ولكن يوجد موقع إلكتروني جمع لك هذه الأدوات:

osintframework.com

ركز على منصة تويتر ولينكدان، Twitter & Linkedin، لأنها في العادة تحتوي على الكثير من المعلومات المفيدة والتي ستوصلك إلى ثغرات تستغلها في الخطوات القادمة.

حتى باقي المنصات مفيدة، لا تهملها.

الخطوة الثانية: Scanning

وتعني المسح، تقوم بمسح الموقع لجمع بعض المعلومات المهمة مثل معلومات الإتصال التي تخص شبكات الكمبيوتر، ولكن ما الفرق بين هذه المرحلة والتي قبلها؟ صحيح أنك تقوم بجمع المعلومات في كلتا المرحلتين، ولكن في المرحلة الأولى تقوم بجمع معلومات متاحة للجميع في الإنترنت.

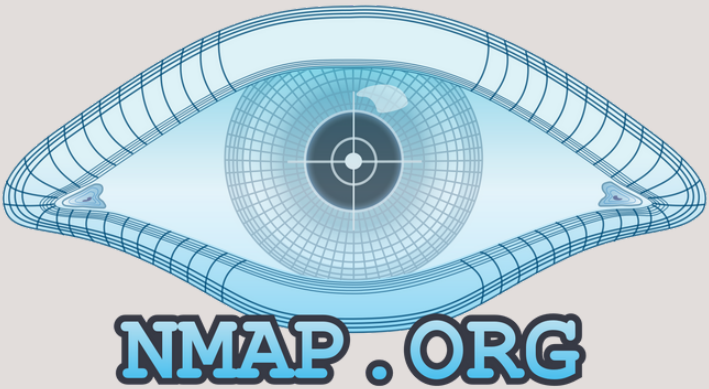
أما المعلومات التي تجمعها في هذه المرحلة عبارة عن معلومات حساسة خاصة بالموقع وتعرضك للمساءلة القانونية وقد تصل إلى السجن.

ما الذي تحتاجه لجمع هذه المعلومات؟ تحتاج إلى معرفة عامة بشبكات الكمبيوتر،

كذلك تحتاج إلى تعلم استخدام أدوات المسح الخاصة بهذه المرحلة والتي تعمل (معظمها) على نظام التشغيل لينكس.

بإختصار، لتقوم بهذه المرحلة يجب عليك تعلم هذه المواضيع:

- لينكس وتوزيعاته، خاصة كالي لينكس.
- شبكات الكمبيوتر.
- بعض الأدوات مثل nmap.



الخطوة الثالثة: Gaining access

وتعني دخول النظام، ولكن كيف ستدخل للنظام؟ عن طريق المعلومات والثغرات التي حصلت عليها من خلال المرحلتين السابقتين.

أحد السيناريوهات التي تكررت عند دخول المخترقين على الأنظمة هي استغلال أحد الموظفين من خلال التحايل عليه أو ابتزازه، لذلك عند قيامك بالمرحلتين السابقتين لا تقتصر فقط على المعلومات الخاصة بالموقع أو المنظمة، لا تهمل الموظفين ومن يستطعيون الدخول على النظام كذلك.

ملاحظة: الغرض من هذا الكتاب التعليم، استخدم الفائدة من الكتاب في دخول عالم الإختراق الأخلاقي.

الخطوة الرابعة: Maintaining

وتعني الصيانة، ولكن ما الذي يحتاج إلى صيانة؟ الطريقة التي تدخل بها للنظام تحتاج إلى صيانة بمعنى التأكد من فعاليتها، كذلك يفضل أن تجد طريقة أخرى إحتياطية للدخول إلى النظام.

في الغالب العثور على المدخل الأول أصعب من الثاني والثالث، لأنك في الثاني والثالث تكون قد دخلت للنظام مسبقاً.

ولكن لماذا تريد البقاء داخل النظام لفترة طويلة؟ هذا السؤال تعتمد إجابته على سؤال آخر، لماذا اخترقت النظام من الأساس؟ في كثير من الأحيان لن تحصل على مبتغاك من الإختراق بعد دخولك للنظام مباشرة، قد تستغرق العملية بعض الوقت.

الخطوة الخامسة: Covering tracks

وتعني إخفاء الأثر، ولكن هل تحتاج إلى إخفاء الآثار إذا اخترقت النظام بشكل أخلاقي؟ نعم، تحتاج إلى تحديد هل إذا كان إخفاء الآثار في النظام سهل أم صعب، لأنه يستحيل وجود موقع خالي من الثغرات بنسبة 100%، فأقلها اذا اخترق النظام، تستطيع إيجاد المخترق.

كيف تتعلم الإختراق؟
في البداية تحتاج إلى أساسيات متعلقة بالكمبيوتر (Hardware)، ثم يفضل أن تتعلم عن البرمجة، لغة واحدة من لغات البرمجة.

بعدها انتقل إلى أنظمة التشغيل وتعلم لينكس وتوزيعاته. بعدها قم بالتعلم على شبكات الكمبيوتر.

تابع الحساب لمزيد من المعلومات.

هذا الكتاب من إصدار حساب:

Instagram: @a.deve.lopment

الحساب خاص بمحتوى البرمجة والأمن السيبراني، كذلك تجد كتب عربية في متجر الحساب، الكتب هي:

- بوابتك لعالم البرمجة.
- لينكس للجميع.
- مقدمة في الشبكات.
- طريقة Proxychains للإختباء.

هذه الكتب ستساعدك وتسهل عليك تعلم مجال الأمن السيبراني والبرمجة.


The End