مقدمة إلى مسار مختبر الاختراق (Introduction to the Penetration Tester Path)

هذا الدرس هو بمثابة بوابة الدخول إلى مسار "مختبر الاختراق (Penetration Tester)". يُعد هذا المسار نقطة انطلاق ممتازة للمبتدئين في منصة أكاديمية (HTB Academy) أو في صناعة أمن المعلومات بشكل عام. الهدف من هذا الدرس هو إعطاؤك نظرة شاملة عن مراحل اختبار الاختراق وكيف تترابط هذه المراحل مع بعضها البعض لتشكيل الصورة الكاملة.

1. ماذا يشمل هذا المسار؟

هذا المسار مصمم ليناسب الجميع، سواء كنت مبتدئاً يطمح لدخول المجال، أو محترفاً يسعى لتطوير مهاراته من منظور مختلف.

- يغطي المسار المفاهيم الأساسية التي تحتاجها للنجاح في: اختبار الاختراق الخارجي (External Penetration Tests)، واختبار الاختراق الداخلي (Internal Penetration Tests) سواء للشبكات أو الدليل النشط (Active Directory)، بالإضافة إلى تقييم أمان تطبيقات الويب (Web Application Security Assessments).
- ستعيش تجربة عملية تغطي جميع مراحل العملية، بدءاً من الاستطلاع وجمع المعلومات (Reconnaissance and Enumeration) وصولاً إلى التوثيق وكتابة التقارير (Documentation and Reporting).
- المسار يختتم بمشروع نهائي عبارة عن محاكاة لاختبار اختراق حقيقي.
- بنهاية المسار، ستكون مسلحاً بالمهارات العملية والعقلية اللازمة لإجراء تقييمات أمنية احترافية ضد شبكات حقيقية بمستوى أساسي إلى متوسط.

2. فلسفتنا في التعلم: الفهم قبل الأدوات

> **ملاحظة توضيحية:** تخيل أنك تتعلم قيادة السيارة. نحن لن نعلمك فقط كيف تضغط على دواسة الوقود (تشغيل الأدوات)، بل سنعلمك كيف يعمل المحرك من الداخل (فهم الثغرة)!

- **التعلم بالممارسة (Learn by doing):** نعتمد على نهج يركز على التطبيق العملي، والاستخدام القانوني والأخلاقي للمهارات.
- **فهم الجذور:** كل وحدة دراسية تتعمق في شرح "السبب (Why)" وراء كل ثغرة والأساليب المستخدمة، بدلاً من مجرد أن تكون درساً تعليمياً لكيفية استخدام أدوات النقر المباشر (point-and-click tools).
- **الذاكرة العضلية (Muscle Memory):** من خلال التدريب على مئات الأمثلة العملية والأمثلة التطبيقية، ستبني "ذاكرة عضلية" تساعدك على تكرار الخطوات وتطبيق المنهجيات بثقة في أي تقييم، بغض النظر عن حجم بيئة العمل.
- **تقديم الحلول:** عندما نفهم الخلل الأساسي (Underlying flaw)، سنتمكن من تقديم نصائح علاجية وإصلاحية أكثر دقة لعملائنا.

3. الأخلاقيات والقانون: خط أحمر!

> **تشبيه مبسط:** مهارات الاختراق هي مثل "مفتاح ماستر" يمكنه فتح أي باب. امتلاكك للمفتاح لا يعني أن يحق لك فتح منازل الآخرين دون إذنهم المسبق!

مهنة اختبار الاختراق (Penetration Testing) هي من المهن القليلة التي يُسمح لك فيها بالقيام بأفعال ضد شركة قد تُعتبر غير قانونية في ظروف أخرى، ولكن **فقط** خلال فترة زمنية مصرح بها للاختبار.

- **المسموح به للتدريب:** يمكنك استخدام تقنيات الاستخبارات مفتوحة المصدر (OSINT) بشكل سلبي لجمع المعلومات، بشرط استخدام محركات البحث وقواعد البيانات العامة فقط دون فحص البنية التحتية للشركة. كما يمكنك التدرب في بيئاتنا المعزولة (Labs) التي توفرها المنصة بشكل آمن وقانوني.
- **الممنوع (الخط الأحمر):** القيام بأي عمليات فحص (Scanning) أو تفاعل مع أنظمة أي مؤسسة دون الحصول على موافقة خطية صريحة (Explicit written consent) ضمن وثيقة نطاق العمل (Scope of Work) يُعد مخالفة للقانون وقد يؤدي إلى اتخاذ إجراءات قانونية وجنائية ضدك.
- **البديل القانوني للتدريب الواقعي:** إذا كنت جاهزاً للتدرب على أهداف حقيقية، يمكنك المشاركة في برامج مكافآت الثغرات (Bug Bounty Programs) عبر منصات مثل (HackerOne) و (Bugcrowd). تذكر دائماً قراءة قواعد الاشتباك (Rules of Engagement) ونطاق العمل الخاص بكل برنامج قبل البدء.

4. المبدأ الأساسي: "لا تسبب ضرراً (Do No Harm)"

- عملاؤنا يضعون ثقة كبيرة فينا عندما يسمحون لنا بدخول شبكاتهم وتشغيل أدوات قد تسبب فوضى أو انقطاعاً في الخدمة، مما يؤدي إلى خسارة الأرباح.
- يجب أن نعمل بمبدأ "لا تسبب ضرراً"، وأن نؤدي جميع مهام الاختبار بطريقة حذرة ومدروسة.
- **اسأل نفسك دائماً:** هل تشغيل كود استغلال معين (Exploit PoC) قد يؤدي إلى تعطل خادم أو أكثر؟. مجرد أنك تستطيع تشغيل أداة معينة، لا يعني أنه يجب عليك ذلك!.
- **القاعدة الذهبية:** عند الشك في أي شيء أثناء التقييم، استشر مديرك والعميل، واحصل على موافقة خطية قبل المتابعة. وثّق، وثّق، وثّق (Document, document, document).

5. نظرة على منهج المسار (Syllabus)

يحاكي المسار عملية اختراق حقيقية لشركة وهمية تُدعى (Inlanefreight)، ويتم تقسيم العملية إلى عدة مراحل رئيسية. يُنصح بشدة دراسة الوحدات بالترتيب لأن المفاهيم تُبنى على بعضها البعض:

1. **المقدمة (Introduction):** تتضمن فهم عملية اختبار الاختراق وكيفية البدء.
2. **الاستطلاع وجمع المعلومات (Reconnaissance & Enumeration):** وتشمل فحص الشبكة باستخدام أداة (Nmap)، وجمع المعلومات من تطبيقات الويب (Information Gathering - Web Edition).
3. **الاستغلال والتحرك الجانبي (Exploitation & Lateral Movement):** مثل تنفيذ هجمات كلمات المرور (Password Attacks)، واستغلال الدليل النشط (Active Directory Enumeration & Attacks).
4. **استغلال تطبيقات الويب (Web Exploitation):** استغلال ثغرات شائعة مثل الحقن بلغة (SQL Injection) والبرمجة عبر المواقع (Cross-Site Scripting - XSS).
5. **ما بعد الاستغلال (Post-Exploitation):** تقنيات رفع الصلاحيات (Privilege Escalation) على أنظمة (Linux) و (Windows).
6. **كتابة التقارير والمشروع النهائي (Reporting & Capstone):** توثيق النتائج والتواصل مع العميل، ثم إجراء اختبار اختراق وهمي شامل لشبكة الشركة.