



المقال الأسبوعي لنادي الأمن السيبراني

الاستطلاع وجمع المعلومات في مجال الأمن السيبراني

يعتبر الاستطلاع وجمع المعلومات (Reconnaissance and Gathering Information) من أهم المراحل في عملية اختراق أنظمة الأمان السيبراني. يقوم المهاجمون السيبرانيون بتنفيذ هاتين العمليتين لاكتشاف الثغرات واستغلالها في هجماتهم المستقبلية.

الاستطلاع: رحلة استكشاف الهدف

عملية الاستطلاع تتضمن جمع المعلومات حول الهدف المستهدف، سواء كانت جهازاً أو شبكة أو منظومة. يعتمد المهاجمون على تقنيات استطلاع متنوعة لاكتشاف الثغرات وتحديد نقاط الضعف في الأهداف. يتم تقسيم الاستطلاع إلى استطلاع نشط واستطلاع سلبي.

الاستطلاع النشط (Active Reconnaissance)

في الاستطلاع النشط، يتم استخدام أدوات تكنولوجيا المعلومات لجمع المعلومات. يمكن استخدام الماسحات (Scanners) والأدوات المتخصصة لاستخراج المعلومات المتاحة من الأهداف المستهدفة. يمكن أن تشمل هذه الأدوات اكتشاف الخدمات المفتوحة (Open Ports) والثغرات الأمنية في الأنظمة المستهدفة. يمكن استخدام أدوات مثل Nmap وNessus وOpenVAS لتحقيق ذلك.

الاستطلاع السلبي (Passive Reconnaissance)

من ناحية أخرى، الاستطلاع السلبي (Passive Reconnaissance) يتمثل في جمع المعلومات دون التفاعل المباشر مع الهدف. يتم ذلك عن طريق مراقبة ورصد الأنشطة المتعلقة بالهدف، مثل جمع المعلومات من وسائل الاتصال المفتوحة مثل المواقع العامة والمنشورات وشبكات التواصل الاجتماعي. يمكن للمهاجمين استخدام هذه المعلومات لتحديد نقاط الضعف المحتملة. بمجرد الانتهاء من عملية الاستطلاع، يجب تحليل وتقييم المعلومات المجمعة. يتم استخدام التحليل لتحديد الثغرات والمشاكل المحتملة في الأنظمة المستهدفة، وتحديد المواقع التي يمكن استغلالها في الهجمات المستقبلية.

جمع المعلومات: تحويل البيانات إلى قوة

تعتبر عملية جمع المعلومات من الخطوات الحاسمة في استطلاع وجمع المعلومات. تهدف هذه العملية إلى الحصول على المزيد من التفاصيل والمعلومات الحساسة التي يمكن استغلالها في الهجمات السيبرانية.

جمع المعلومات يتطلب استخدام مجموعة متنوعة من الأدوات والتقنيات. يشمل ذلك البحث عبر الإنترنت (Open Source Intelligence) والاستخبارات المفتوحة (OSINT) وفحص الأثر الرقمي (Digital Footprinting) وتحليل حركة البيانات (Packet Sniffing) والهندسة الاجتماعية (Social Engineering) ومهاجمة الشبكة (Network Scanning) واستخدام الأدوات الخاصة بالتجسس.

من خلال جمع المعلومات، يتمكن المهاجمون السيبرانيون من تحديد ثغرات الأمان ونقاط الضعف والمتسللين المحتملين في الأنظمة المستهدفة. يمكنهم أيضًا تحديد أهداف المستهدف واستخلاص المعلومات الحساسة التي يمكن استغلالها لصالحهم.

المصادر: <https://www.sans.org/white-papers/33248> ، The Web Application Hacker's Handbook