تعتبر كلمات المرور الدفاع الأخير ضد وقوعنا ضحيا في أيدي المهاجمين، على الرغم من وجود تقنيات أخرى مثل البطاقات الذكية و أجهزة التحقق و العلامات الحيوية مثل بصمة اليد و العين ، الا ان كلمة المرور لا زالت حتى الأكثر شيوعا في عمليات التحقق من الهوية.

تعتبر كلمات المرور ضعيفة نسبياً لسببين،

السبب الأول انها من اختيار المستخدم بشكل تام، فقد يقوم المستخدم باختيار كلمات مرور هشة وضعيفة مثل 123456. على الرغم من وجود أدوات تجبر المستخدمين على اختيار كلمات مرور صعبة، الا ان المستخدم يحتال ويختار الطريق الاسهل للمخترقين دائما مثل تكرار الأحرف أو الأرقام.

السبب الثاني، انه بالرغم من اختيار كلمات مرور صعبة، إلا طرق الهجوم ازدادت كفاءة في الآونة الاخيرة. فقد أصبح المهاجمين يستخدمون أدوات تستطيع تخمين كلمات المرور بشكل تلقائي.

في الأسفل نستعرض كيفية الهجوم على كلمات المرور للمستخدمين

الهجوم الفيزيائي يحدث هذا الهجوم عندما يحصل المهاجم على فرصة الوقوف على الجهاز، حيث يقوم المهاجم بتركيب قطعة صغيرة تقوم بتخزين كلمات نقرات لوحة المفاتيح للضحية، حينها يستطيع المهاجم استخلاص كلمات المرور وارقام الحسابات البنكية أيضا. أو يقوم المهاجم بإرسال برمجية خبيثة للضحية تقوم بنفس الغرض. المعاينة المستمرة وتفحص جهاز الكمبيوتر وتحديث برنامج مكافح الفيروسات يقي من هذا الهجوم.

التنصت على أجهزة الشبكة طريقة أخرى لسرقة كلمات المرور، فعندما يقوم الضحية باستخدام انترنت غير امن كالموجود في المقاهي والأسواق أو زيارة مواقع لا تستخدم بروتوكولات التشفير في مواقعها، يكون تدفق الشبكة غير مشفر ويستطيع المهاجم استخلاص كلمات المرور منه.

كلمات المرور الشائعة طريقة أخرى للمهاجمين لتخمين كلمة المرور، فالمهاجم يستخدم قائمة تحتوي على الملايين من كلمات المرور ويقوم باستخدام أدوات تستطيع تجربة كل كلمات المرور بشكل تلقائي حتى تصل الى نتيجة.

في النهاية، استخدام كلمات مرور قوية تحتوي على أرقام وحروف ورموز وليست شائعة، تحمي من سرقة كلمات المرور. تذكر دائما عزيزي القارئ ان كلمة المرور هي اخر خطوط الدفاع لحمايتك من الوقوع ضحية في أيدي المهاجمين.

تحياتي

محمد الدريس

@iAbudrees