تمرین سری چهارم امنیت(فصل های 7 و 8 کتاب)

1. فرض کنید دارای چندین حساب کاربری در اماکن مختلف مانند بانک و غیره هستید و باید برای هر حساب پسوردی را انتخاب کنید. اگر تعداد حساب­های کاربری شما زیاد باشد، مسلماً به ذهن سپردن پسوردهای مختلف سخت خواهد بود و نیز اگر از یک پسورد یکسان برای همه حساب­ها استفاده کنید نیز، احتمال حمله به تمامی حساب های شما بسیار بالا خواهد رفت. راهی را پیشنهاد کنید که دو مشکل مطرح شده را حل کند.
2. در یک سیستم فرضی، همه پسوردها 8 کارکتری هستند که برای هر کاراکتر، 64 انتخاب متفاوت می­تواند وجود داشته باشد. پسوردها همگی Hash شده و در فایلی به گنجایش 256 پسورد در سیستم ذخیره شده­اند. فرض کنید ترودی برنامه­ای در اختیار دارد که می­تواند 64 پسورد بر ثانیه را تست نماید. ترودی همچنین دیکشنری در اختیار دارد که شامل 230 پسورد معمول استفاده شده است و احتمال آنکه پسوردی از سیستم فرضی در دیکشنری موجود باشد برابر با 4/1 می­باشد. به سوالات زیر پاسخ دهید:

الف) چند پسورد متفاوت قابل ایجاد شدن است؟

ب) چه مدت(به صورت میانگین) طول می­کشد تا ترودی پسورد ادمین سایت را کرک کند؟

ج) با چه احتمالی حداقل یک پسورد از میان 256 پسورد موجود در فایل، در دیکشنری یافت خواهد شد؟

د)ترودی چه مقدار کار باید انجام دهد تا بتواند هریک از پسوردهای موجود در فایل را پیدا کند؟

3) MAC کامپیوتر را به عنوان " آنچه که داریم " در Authentication بررسی کنید؟

از فصل 8 سوالات 16 ، 26 ، 28، 33 را حل کنید

مهلت تحویل تکالیف تا ساعت 23:59 روز 16 اردیبهشت 93