دانشکده مهندسی کامپیوتر

استاد درس: دکتر ابوالفضل دیانت

بهار ۱۴۰۳

تمرین اول

درس امنیت

گزارش تمرین

ملیکا محمدی فخار - ستاره باباجانی

۹۹۵۲۲۰۸۶ - ۹۹۵۲۱۱۰۹

۱ جواب سوال ۱

همانطور که می دانیم، حمله ی Brute force یا جستجوی فراگیر نوعی از حملات است که در آن تمامی ترکیب های ممکن از حروف یک گذرواژه تا زمان یافتن رمز اصلی امتحان می شوند. البته که حجم بالایی از رخدادهای نفوذ اطلاعاتی در دهه نود شمسی با استفاده از این رویکرد انجام گرفته است، اما فرایند رمزنگاری با استفاده از این حمله ازجمله فرایندهای طولانی به حساب می آید. البته که اینجور کارها عمدتا به کامپیوترها سپرده می شود تا فرایند امتحان کردن حالات مختلف را به صورت خودکار انجام دهند.

انواع مختلفی از این نوع حملات

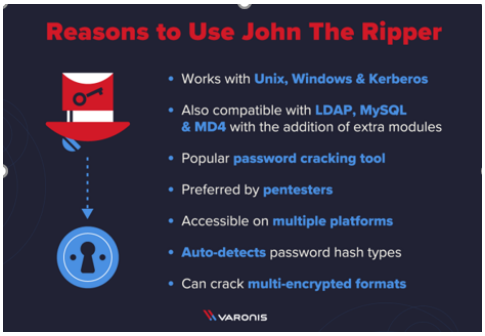
- حملات ساده Force Brute (simple Attacks)
- حملات معکوس Force Brute (Reverse Attacks)
- حملاتی از نوع دستکاری اعتبار (Credential Stuffing)
- حملات دیکشنری (Dictionary Attacks)
- حملات هیبریدی (Hybrid Attacks)

منابع مورد نیاز این حمله با افزایش طول کلید به صورت خطی افزایش پیدا نمی کنند. بلکه بصورت نمایی افزایش می یابند. بدیهی است انتخاب رمزهای طولانی تر و پیچیده تر، عملیات force Brute را وادار به آزمایش موارد بیشتری می کند که زمان موردنیاز برای بررسی تمام حالت ها نیز افزایش می یابد.

چند نمونه از ابزارهای رایج که از این حمله استفاده می کنند را می توان به صورت زیر اشاره کرد:

- Rainbow crack
- ripper the John
- Aircrack-ng

به عنوان نمونه، چند مزیت و دلیل برای استفاده از ابزار Ripper the John را می توان در تصویر زیرمشاهده نمود:



شکل ۱: مزیت و دلیل استفاده از Ripper the John

با توجه به اطلاعات آماری جمع آوری شده حدود ۵درصد از حملات سایبری از نوع Brute-force هستند که درصد بسیار پایینی است. معمولا سیستم های حمله کننده می توانند حدود ۱۰هزار تا یک میلیارد رمز را در ثانیه آزمایش کنند که بستگی که پردازنده و سخت افزار سیستم حمله کننده دارد.

زمان مورد نیاز برای پیدا کردن یک رمز به موارد زیر بستگی دارد:

- تعداد کاراکترهای به کاررفته در رمز
- تنوع حروف به کاررفته در رمز
- قدرت رمز سیستم حمله کننده
- قدرت رمز سیستم هدف

بود. در یک کیبورد استاندارد حدود ۹۴ کاراکتر داریم که در مجموع می توانند ۲میلیارد رمز ۸ حرفی به وجود بیاورند که تعداد حالات بسیار زیادی هست و چک کردن تمام این حالت ها زمانبر هست. به طور کلی می توانیم بگوییم با افزایش طول رمز، سرعت شکستن آن رمز به طور نمایی افزایش پیدا می کند و رشد می کند. به عنوان نمونه، شکستن رمزی با تعداد ۱۲۸بیت با استفاده از این روش، نیاز به بررسی 2^{128} حالت دارد که میلیاردها سال طول خواهد کشید.

** نمونه از مدل‌های پرقدرت CPU :

Intel Core i۹-۱۱۹۰۰K:

یکی از پرقدرت‌ترین پردازنده‌های مرکزی از شرکت Intel دارای ۸ هسته و ۱۶ رشته اجرایی است. این دستگاه می تواند حدود ۱۷۰۰ به بالا امتیاز (در قسمت Geekbench ۵ Single-Core Score Benchmark:) کسب کند.

AMD Ryzen ۹ ۵۹۵۰X:

یک پردازنده قدرتمند از شرکت AMD دارای ۱۶ هسته و ۳۲ رشته اجرایی است. این دستگاه می تواند حدود ۲۵۰۰۰ به بالا امتیاز (در قسمت Benchmark Geekbench ۵ Single-Core Score) کسب کند.

** نمونه از مدل‌های پرقدرت GPU:

NVIDIA GeForce RTX ۳۰۹۰:

یک کارت گرافیکی بسیار پرقدرت از NVIDIA دارای ۱۰،۴۹۶ هسته CUDA و ۲۴ گیگابایت حافظه GDDR۶X است. این دستگاه می تواند حدود ۱۵۰۰۰ به بالا امتیاز (در قسمت :Benchmark ۳DMark Spy Time) کسب کند.

AMD Radeon RX ۶۹۰۰ XT:

یکی دیگر از کارت‌های گرافیکی قدرتمند از AMD دارای ۵،۱۲۰ هسته جریانی و ۱۶ گیگابایت حافظه GDDR۶ است. این دستگاه می تواند حدود ۱۱۰۰۰ به بالا امتیاز (در قسمت Su- ۸k Optimized Benchmark: Unigine perposition) کسب کند.

۲ جواب سوال ۲

الگوریتم Double Transposition یکی از الگوریتم‌های رمزنگاری کلاسیک بوده است که توسط آلمان در طول جنگ جهانی اول (World War I) مورد استفاده قرار می‌گرفت. این الگوریتم از مبانی ساده‌ای برای رمزنگاری متن استفاده می‌کند و از ترتیب دو مرحله‌ای برای انجام عملیات رمزنگاری و رمزگشایی تشکیل شده است.

توضیح مختصر الگوریتم Double Transposition به شرح زیر است:

۱.۲ مرحله ی اول : رمزنگاری Row Transposition:

۱. متن اصلی را به یک جدول با ستون‌ها و ردیف‌ها تبدیل می‌کند.
۲. ردیف‌های جدول را بر اساس کلید مشخص مرتب می‌کند.
۳. متن رمزگشایی شده را به صورت ردیف به ردیف خوانده و بازیابی می‌کند.

۲.۲ مرحله ی دوم: رمزنگاری Column Transposition:

۱. متن اصلی را به یک جدول با ستون‌ها و ردیف‌ها تبدیل می‌کند.
۲. ستون‌های جدول را بر اساس کلید مشخص مرتب می‌کند.
۳. متن رمزگشایی شده را به صورت ستون به ستون خوانده و بازیابی می‌کند.

۳.۲ مرحله ی سوم: رمزنگاری و رمزگشایی:

برای رمزنگاری یک متن، متن اصلی به مرحله اول و سپس به مرحله دوم تبدیل می‌شود. برای رمزگشایی، مراحل برعکس انجام می‌شوند. الگوریتم Double Transposition به عنوان یکی از الگوریتم‌های رمزنگاری ساده و قدیمی شناخته می‌شود و مزایای مختصری دارد. از جمله مزایا می‌توان به سادگی اجرا و قابلیت تنوع کلید اشاره کرد. با این حال، امروزه این الگوریتم به عنوان یک الگوریتم امن برای استفاده در موارد مهم و حساس معمولاً مورد تایید نیست. الگوریتم‌های رمزنگاری پیشرفته‌تر و امن‌تری برای حفظ امنیت اطلاعات استفاده می‌شوند.

۳ جواب سوال ۳

این روش برای شکستن رمزنگاری های جانشینی بسیار مناسب است. مبنای کار آن تکرار حروف در الفبای انگلیسی است. ابتدا تکرار هر حرف الفبا در متن رمزه شده را به دست می آوریم. سپس تکرار حروف الفبای انگلیسی در متن های بزرگ را به دست می آوریم و براساس تعداد تکرار مرتب میکنیم. سپس میان این دو لیست یک نگاشت برقرار میکنیم. این روش تا حد خوبی میتواند مسئله ما را رمزگشایی کند. اما به جواب مطلق درست نخواهد رسید. در روش رمز نگاری مستوی، هر حرف با یک ضرب و جمع با عدد، به یک حرف دیگر نگاشت خواهد شد. البته بعد از ضرب و سپس جمع، باید باقیمانده عدد حاصل را بر ۲۶ محاسبه کنیم تا حرفی از بین حروف الفبای انگلیسی بدست آید. برای انجام این کار ابتدا یک دیکشنری که کلید آن جفت (a،b) است و هرvalue آن لیستی از کلمات رمز گشایی شده است ساخته میشود. سپس برای تمام مقادیر ممکن وa b متن را رمزگشایی میکند و با استفاده از کتاب خانه های موجود (که برای زبان پایتون از nltk استفاده میکنیم) کلمات معنادار پیدا میشوند. و کلمات معنادار به دیکشنری اضافه میشوند. نتیجه بعد از تست همه حالات به صورت زیر است:

G IS EXPECTED TO SUPPORT DATA RATES OF TERABYTE PER SECOND THIS LEVEL OF CAPACITY AND LATENCY WILL BE UNPRECEDENTED AND WILL EXTEND THE PERFORMANCE OF G APPLICATIONS ALONG WITH EXPANDING THE SCOPE OF CAPABILITIES IN SUPPORT OF INCREASINGLY NEW AND INNOVATIVE APPLICATIONS ACROSS THE REALMS OF WIRELESS CONNECTIVITY COGNITION SENSING AND IMAGING G HIGHER FREQUENCIES WILL ENABLE MUCH FASTER SAMPLING RATES IN ADDITION TO PROVIDING SIGNIFICANTLY BETTER THROUGHPUT AND HIGHER DATA RATES THE COMBINATION OF SUB MM WAVEE G WAVE LENGTHS SMALLER THAN ONE MILLIMETER AND THE USE OF FREQUENCY SELECTIVITY TO DETERMINE RELATIVE ELECTROMAGNETIC ABSORPTION RATES IS EXPECTED TO LEAD TO POTENTIALLY SIGNIFICANT ADVANCES IN WIRELESS SENSING TECHNOLOGY ADDITIONALLY WHERE AS THE ADDITION OF MOBILE EDGE COMPUTING IS A POINT OF CONSIDERATION AS AN ADDITION TO G NETWORKS MOBILE EDGE COMPUTING WILL BE BUILT IN TO ALL G NETWORKS EDGE AND CORE COMPUTIN G WILL BE COME MUCH MORE SEAMLESSLY INTEGRATED AS PART OF A COMBINED COMMUNICATIONS COMPUTATION INFRASTRUCTURE FRAMEWORK BY THE TIME G NETWORKSA REDEPLOYED THIS WILL PROVIDE MANY POTENTIAL ADVANTAGES AS G TECHNOLOGY BE COMESOPE RATIONAL INCLUDING IMPROVED ACCESS TO ARTIFICIAL INTELLIGENCE CAPABILITIES