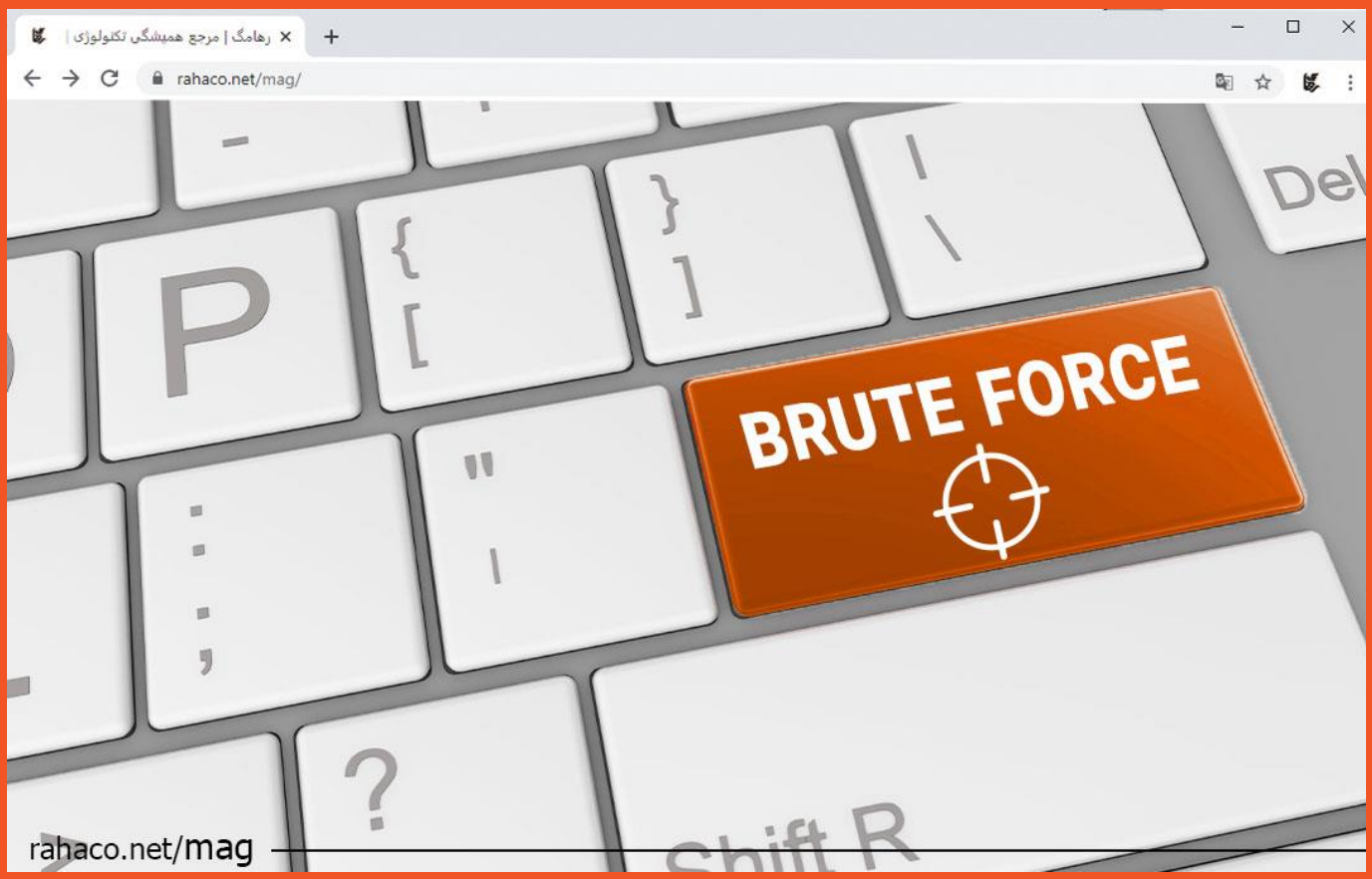
مجله رهاکو

RAHA MAG

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک 12
www.rahaco.net کدپستی1583616414 تلفن :02154521



فهرست

آشنایی با انواع حملات بروت فورس

سرقت اطلاعات با ارزش و محرمانه، یکی از چالش‌هایی است که در حال حاضر تقریبا همه افراد جامعه به طور مستقیم یا غیر مستقیم درگیر آن هستند. اما دارندگان کسب و کارهای آنلاین و بزرگ، نگرانی بیشتری نسبت به دیگر افراد دارند. حملات بروت فورس، یکی از قدیمی‌ترین روش‌های سرقت اطلاعات با ارزش و محرمانه است که همچنان در حال توسعه و پیشرفت می‌باشد. هر روز با پیدایش تکنولوژی‌های نوین، روش‌های جدیدی برای پیشگیری و مقابله با آن‌ها نیز به وجود می‌آیند.

حملات بروت فورس، که توسط هکرها انجام می‌شود، یک نوع حمله کرکینگ است. در این نوع حمله هکر تلاش می‌کند تا رمز عبور کاربر را شناسایی کند. برای انجام این عملیات هکر از نرم‌افزارهایی با قدرت پردازش بالا استفاده می‌کند. به عبارت دیگر هکر با میلیون‌ها ترکیب نام کاربری و رمز عبور، به سایت هدف حمله می‌کند. در این فرایند فرد هکر ممکن است با موفقیت یا شکست مواجه شود. بنابراین این حملات کاملا به شانس وابسته هستند و احتمال موفقیت هکر ۱۰۰ درصد نیست.

توضیح کلی درباره حملات بروت فورس

بروت فورس (Brute Force) یک روش سایبری است که در آن تمامی ترکیب‌ها و ترتیب‌های ممکن برای رمزگشایی یا دسترسی به یک سیستم یا حساب کاربری امتحان می‌شود. در این روش تمامی کلمات عبور محتمل، شماره‌های ممکن یا داده‌های مختلف با استفاده از نرم‌افزارهای خاص و یا ابزارهای سفارشی تست می‌شوند تا رمزگشایی موفقیت آمیز صورت بگیرد.

بروت فورس یک روش قدرتمند است، اما به دلیل نیاز به زمان و منابع بسیار زیاد، در بسیاری از موارد کاربردی نیست. این روش معمولا در سیستم‌ها یا حساب‌های کاربری با رمزهای عمومی و قوی مورد استفاده قرار می‌گیرد. به عنوان مثال در حملات بر روی سیستم‌های وب، یک حمله بروت فورس ممکن است از طریق تلاش برای حدس زدن رمز عبور حساب کاربری و امتحان کردن تمامی ترکیب‌های ممکن انجام شود.

روش‌های امنیتی برای مقابله با حملات بروت فورس

برای مقابله با حملات بروت فورس، روش‌های امنیتی متعددی وجود دارد، مانند: تعیین محدودیت تعداد تلاش‌ها، استفاده از رمزهای عمومی پیچیده و طولانی‌تر، اعمال تاخیر بین تلاش‌ها و استفاده از مکانیزم‌های تشخیص حملات مشترک مانند تشخیص و پیشگیری از حملات ورود بدون مجوز.

بروت فورس از روش‌های دیگری نیز استفاده می‌کند مانند: واژه نامه‌ها، فهرست‌ها و دیکشنری‌هایی که معمولا شامل کلمات رایج، اسامی و داده‌های دیگر هستند. این روش نیز ممکن است برای شکستن رمزها مورد استفاده قرار گیرد، به ویژه در صورتی که رمز انتخابی کاربران ضعیف باشد و در واژه نامه وجود داشته باشد.

همانطور که می‌توان حدس زد، بروت فورس یک روش زمان‌بر و منابع محاسباتی زیادی می‌طلبد، زیرا باید تمامی ترکیب‌های ممکن را بررسی کند. برای مقابله با حملات بروت فورس، اغلب مجموعه‌های رمزنگاری از روش‌های امنیتی مانند: محدودیت تعداد تلاش‌ها در ورودی کاربر، استفاده از الگوریتم‌های پیچیده‌تر و طولانی‌تر رمزها و استفاده از عملیات امنیتی اضافی مانند شناسایی دو مرحله‌ای استفاده می‌کنند تا شکستن رمز با بروت فورس به طور عملی غیرممکن شود.

نحوه انجام حملات بروت فورس

برنامه ریزی حملات بروت فورس معمولا توسط فرد یا گروهی از هکرها انجام می‌شود. آن‌ها ممکن است از ابزارها و نرم‌افزارهای خاصی استفاده کنند که برای تلاش متعدد بر روی رمزهای عبور مورد نظر طراحی شده‌اند. این ابزارها معمولا قواعد مشخصی برای انتخاب رمزهای عبور بر اساس اقلام مختلف مانند: حروف بزرگ و کوچک، اعداد و نمادها دارند و با تلاش متعدد و انتهایی برای پیدا کردن رمز عبور در برنامه‌ها یا سیستم‌های هدف اقدام می‌کنند.

در صورتی که رمز عبور یک کاربر به صورت رمزنگاری شده در سایت‌ها ذخیره شده باشد، هکران برای کشف آن از روش‌های مختلفی استفاده می‌کنند. این شامل اجرای حملات دیکشنری بر روی رمزهای ذخیره شده، استفاده از جداول رمزنگاری شده (rainbow tables)، استفاده از رمزگشایی نیرومند (brute-force decryption) و سایر تکنیک‌هایی است که در نهایت هدف آن‌ها کشف رمز عبور می‌باشد.

برای مقابله با حملات بروت فورس، اهمیت استفاده از رمزهای عبور قوی و پیچیده که شامل ترکیبی از حروف بزرگ و کوچک، اعداد و نمادها باشند، بسیار ضروری است. همچنین استفاده از رمزهای منحصر به فرد برای هر حساب کاربری و فراهم کردن ابزارهای دو مرحله‌ای تایید هویت (مانند کد ارسالی به تلفن همراه) می‌تواند امنیت حساب کاربری را تقویت کند.

انواع حملات بروت فورس

با اینکه قبل‌تر گفتیم موفقیت در حملات بروت فورس بسیار شانسی می‌باشد اما قابل ذکر است که این حملات قطعا با برنامه ریزی دقیق و مشخصی انجام می‌شوند که شامل 5 مرحله اصلی می‌شوند که در ادامه به توضیح درباره این روش‌ها می‌پردازیم.

حمله بروت فورس دیکشنری

در این نوع از حملات در واقع هکر نام کاربری شخص مورد نظر را دارد و به دنبال پسورد آن است. در اصل ساده‌ترین نظمی که یک حمله بروت فروس داراست. همین داشتن نام کاربری و دنبال پسورد گشتن است که این نوع حمله را دیکشنری می‌نامند. البته نکته قابل توجه این است که حمله دیکشنری مختص به بروت فورس نیست بلکه نیازهای مختلف یک هکر را برآورده می‌کند.

نوعی از حملات که به آن‌ها حملات بروت فورس یا حملات دیکشنری می‌گویند، هدفشان یافتن نام کاربری و پسورد صحیح برای ورود به حساب کاربری یا سیستم مورد نظر است. این حملات به شکل ساده‌ترین الگوی حملات هستند و هکرها تلاش می‌کنند با استفاده از لیستی از نام‌ها و رمزهای عبور متعدد (که به آن‌ها دیکشنری گفته می‌شود) وارد حساب کاربری یا سیستم مورد نظر شوند.

حملات دیکشنری هرگونه رمز عبور ممکن را امتحان نمی‌کنند، بلکه بر اساس لیستی از کلمات یا عبارات رایج و پر استفاده در دسترس هستند. این نوع حملات در واقع یک تلاش سیستماتیک برای شکستن رمز عبور است.

حمله دیکشنری می‌تواند برای برآورده کردن نیازهای مختلف هکران استفاده شود و نه تنها به حملات بروت فورس بر روی پورت‌های مشخص محدود نمی‌شود.

برای مقابله با حملات دیکشنری استفاده از رمز عبور قوی و مجموعه‌ای از اقدامات امنیتی مانند: اعمال سیاست‌های پسورد پیچیده، استفاده از شماره‌های تصادفی، قفل شدن حساب کاربری پس از تعداد تلاش‌های ناموفق و استفاده از ابزارهای تشخیص حملات می‌تواند مفید باشد. همچنین آموزش کاربران درباره روش‌های انتخاب رمز عبور قوی و جلوگیری از استفاده از رمزهای ضعیف نیز اهمیت دارد.

حمله بروت فورس معکوس

حمله بروت فورس معکوس یکی از عجیب‌ترین حملات بروت فورس است. زیرا در این نوع حمله هکر رمز عبور را دارد و به دنبال نام کاربری است. (دقیقا نقطه مقابل حمله قبلی) در واقع در این نوع حملات ممکن است هکر پسوردهای یک مجموعه را از طریقی به دست اورده و اکنون نیازمند دریافت نام‌های کاری آن مجموعه باشد. که در این صورت از حمله بروت فورس استفاده می‌کنند.

حمله بروت فورس ساده

حمله بروت فورس ساده یکی از قدیمی‌ترین و ساده‌ترین روش‌های حمله به رمز عبور است و به طور معمول برای شکستن رمزهای عبور ساده و ضعیف مورد استفاده قرار می‌گیرد. این نوع حمله به وسیله‌ی امتحان کردن تمام ترکیب‌های ممکن از حروف الفبا، اعداد و سایر کاراکترها به صورت متوالی، به طور کاملا مکرر و تکراری، به رمز عبور مورد نظر پیش می‌رود.

حمله بروت فورس ساده به ویژه برای رمزهای عبور ضعیفی که مانند "123456" یا "password" هستند، بسیار موثر است. اغلب افرادی که رمز عبور قوی‌تری انتخاب نمی‌کنند یا برای حساب‌های حیاتی‌شان از رمزهای قوی استفاده نمی‌کنند، در معرض خطر هستند. به دلیل سادگی این روش حمله و وجود رمزهای عبور ضعیف در جامعه افرادی که نیاز به نفوذ به حساب‌های دیگران دارند، اغلب از این روش استفاده می‌کنند.

برای مقابله با حمله بروت فورس ساده، بهتر است از رمزهای عبور قوی و مطمئن استفاده کنید. رمزهای عبور قوی باید دارای ترکیب حروف بزرگ و کوچک، اعداد و کاراکترهای خاص باشند و به صورت تصادفی انتخاب شوند. همچنین، از تکنیک‌های دو فاکتوره‌ی تایید هویت و محدود کردن تعداد تلاش‌های اشتباه ورود به حساب کاربری استفاده کنید. با این کار می‌توانید خود را در برابر حملات بروت فورس ساده محافظت کنید.

حمله بروت فورس ترکیبی

حمله بروت فورس ترکیبی (Combination Brute Force Attack) یک نوع حمله رمزگشایی است که از دو روش حمله دیکشنری (Dictionary Attack) و ساده (Brute Force Attack) استفاده می‌کند. این نوع حمله به منظور شکستن رمزهای عبور ترکیبی استفاده می‌شود. پسوردهای ترکیبی شامل حروف الفبا (بزرگ و کوچک)، اعداد و کاراکترهای دیگر مثل نمادها و علائم خاص هستند.

نتیجه گیری

بروت فورس یک روش حمله در حوزه امنیت فناوری اطلاعات است که در آن، تمامی ترکیب‌های ممکن برای یک رمز یا رمزگشایی را به طور سریع بررسی می‌کند تا رمز را کشف کند. این روش اغلب برای شکستن رمزهای رمزنگاری ورودی کاربران، مانند: رمزهای عبور و رمزهای مورد استفاده در سیستم‌های کامپیوتری، استفاده می‌شود.

در حملات بروت فورس تمامی ترکیب‌های ممکن برای تشکیل رمز به صورت خودکار توسط یک کامپیوتر یا نرم‌افزار مخصوص بررسی می‌شود. این ترکیب‌ها می‌توانند شامل: اعداد، حروف الفبا، نمادها و حروف بزرگ و کوچک باشند. بسته به طول رمز و مجموعه مجاز از نمادها و حروف، زمان لازم برای شکستن رمز با استفاده از بروت فورس ممکن است بسیار طولانی شود.