**۷ روش متداول حملات پسورد:**

۱. حملات Brute Force

این حمله یکی از رایج ترین و ساده ترین روش های حمله به پسورد برای هکرها است. بسیاری از هکرهای تازه کار دقیقا از این روش استفاده می کنند.

در یک حمله Brute Force یک هکر با استفاده از یک ابزار تمام ترکیبات ممکن را برای رمز عبور چک میکند. این شیوه به صورت تست پسوردهای ساده به پیچیده انجام میشود .

فراموش نکنید که اگر یک هکر به لیست کارمندان شما دسترسی پیدا کند  حدس زدن نام کاربری این فرآیند را ساده تر میسازد.

۲. حملات دیکشنری

در این نوع حمله هکرها با استفاده از لیست پسوردهای متداول سعی تلاش برای بدست آوردن پسوردها را انجام میدهند. در مقایسه حمله دیکشنری با Brute Force میشه به این نکته اشاره کرد که حمله دیکشنری هوشمندانه تر ، و حمله Brite Force کور کورانه تر انجام میشود.

همچنین ، حملات دیکشنری  به چند عامل اصلی روانشناسی کاربران متکی است. به عنوان مثال: کاربران تمایل دارند رمزهای عبور کوتاه را انتخاب کنند و کلمات عبور خود را از کلمات متداول تولید کنند. بنابراین حمله دیکشنری  با کلمات متداول و تغییرات آنها آغاز می شود (اضافه کردن شماره ها در انتها ، جایگزین کردن حروف با اعداد و غیره).

۳. حملات فیشینگ

شیوه کلاسیک و البته قدیمی هکرها ، نفوذگران به ندرت نیاز به استفاده از سایر روشهای حمله رمز عبور دارند. میپرسید چرا ؟ چون اونها میتونن از کاربر درخواست کنند تا اطلاعات اکانتشو بدهد!

معمولاً هکرها حملات فیشینگ خود را تحت عنوان خدمات قانونی و معروف انجام میدهند .این ایمیل ها ، کاربران را به صفحات ورود جعلی هدایت میکند. البته برای طبیعتی تر بودن درخواست هکرها پیشنهادهای بیسار جذاب و یا حتی تهدیدآمیزی را به ایمیلهای خود اضافه می کنند مانند: فروش با ۹۰% تخفیف! و یا : احتمال لغو سرویس. این کار کاربران را مجبور می کند قبل از توجه دقیق ، اطلاعات حساب خود را تحویل دهند.

همچنین ، یک نوع حمله فیشینگ حمله مهندسی اجتماعی است. این حملات هویتی از قوانیت اجتماعی محیط کار برای فریب کاربران استفاده می کند. هکرها می توانند خود را به عنوان تیم فناوری اطلاعات معرفی کنند و مستقیماً از کاربران بخواهند کلمات عبور خود را تحویل دهند.

مهندسی اجتماعی به هکرها این امکان را می دهد که فقط با نگاه کردن به رسانه های اجتماعی ، اطلاعات مربوط به کاربران را بدست بیاورند. از این گذشته ، بسیاری از گذرواژه‌ها شامل نامهای تولد اشخاص و یا نام حیوانات خانگی هستند که کاربران این اطلاعات را به راحتی به هکرها هدیه میدهند.

۴. حمله Rainbow Table

شرکتها اغلب رمزهای عبور کاربران خود را hash می کنند. هش مستلزم تبدیل رمزهای عبور به رشته های رمزنگاری شده و تصادفی می باشد تا از سوء استفاده از آنها جلوگیری شود. اگر هکرها نتوانند کلمه عبور را بخوانند ، نمی توانند از آنها سوء استفاده کنند.

به نظر می رسد هشینینگ یک روش امنیت است. این درست است. به عنوان مثال ، یک جدول رنگین کمان لیستی از هش های از پیش محاسبه شده را گردآوری می کند. این لیست پاسخ های ریاضیاتی را برای همه ترکیب های ممکن رمز عبور برای الگوریتم های هش را دارد.

۵. حملات Man In the Middle

در این حمله نفوذگران با استفاده از جعل هویت یک وب سایت و یا برنامه خود را در وسط ارتباط قرار میدهند و اطلاعات تبادل شده را مانیتور میکنند.این امر به آنها اجازه می دهد تا اعتبار کاربر و سایر اطلاعات حساس وی را جمع آوری کنند. حملات (MITM) اغلب با حملات [مهندسی اجتماعی](https://cynetco.com/social-engineering/) که کاربران را به یک سایت جعلی فریب می دهند تسهیل می شود.

۶. حملات رهگیری ترافیک

در این حمله هکرها از نرم افزاری مانند packet sniffers برای نظارت بر ترافیک شبکه و ضبط گذرواژه ها در هنگام عبور استفاده می کنند. این نرم افزارها  مشابه با متدهای شنود اطلاعات داده های مهم را نظارت و ضبط می کند. بدیهی است ، اگر اطلاعات تبادل شده مانند گذرواژه‌ها ، رمزگذاری نشده باشد کار آسانتر است. اما حتی اطلاعات رمزگذاری شده نیز بسته به قدرت استفاده از روش رمزگذاری مورد استفاده ، قابل رمزگشایی هستند.

۷. حملات Keylogger

در نهایت ، حملات keylogger در این شیوه هکر برنامه ای را در نقاط سیستم کاربران برای ردیابی کلیه فعالیت های کاربر نصب می کند.

بنابراین هرچه کاربران شامل نام کاربری و رمزعبورهای خود تایپ کند جمع آوری شده و به مقصد از پیش تعیین شده ارسال میشود تا هکرها آنها را مورد استفاده قرار دهند. از نظر فنی این روش زیر مجموعه بدافزارها یا ویروس دیجیتال قرار دارد ، بنابراین ابتدا باید نقاط پایانی کاربران (اغلب از طریق بارگیری فیشینگ) آلوده شود.

حتی قویترین رمزهای عبور نیز نمی توانند شما را در مقابل این حملات پسورد سایبری مستقر در گذرواژه محافظت کنند. بنابراین شرکت شما چه کاری می تواند انجام دهد؟

چگونه می توان از روش های متداول حملات پسورد جلوگیری کرد؟

در مرحله اول، شرکت شما باید با واقعیت هایی روبرو شود: پسوردها در برابر روشهای حمله پسورد بسیار آسیب پذیر هستند. در حقیقت ، هر شکلی از تأیید هویت تک عاملی ، کل ساختار IT شما را در مقابل هکرها آسیب پذیر می سازد.

به جای تکیه بر امنیت پسوردها ، سازمان شما باید از  راه کارهای احراز هویت چند عاملی (MFA) استفاده کند. احراز هویت چندعاملی Multifactor لایه های مختلفی از امنیت را در هر حساب کاربری قرار می دهد. این عوامل موارد مختلفی از قبیل زمان درخواست دسترسی و محل جغرافیایی کاربر را کنترل می کند. همچنین ، می تواند احراز هویت بیومتریک را در خود جای دهد.

نکته مهم این است که: تأیید هویت چند عاملی اثربخشی روشهای حمله رمز عبور را کاهش می دهد. البته ممکن است به طور کامل مانع از همه هکرها نشود ، اما آنها موفقیت آنها را بسیار سخت میسازد.