# [(Password Spraying Attacks)](https://authin.ir/password-spraying-attacks/)

حمله اسپری کردن رمز عبور نوعی حمله سایبری [بروت فورس](https://authin.ir/brute-force-attack/) است که در آن مجرم سایبری سعی می کند با استفاده از لیستی از گذرواژه های رایج و قابل حدس مانند “123456” رمز عبور کاربر شناخته شده را حدس بزند. این فرآیند اغلب خودکار است و به آرامی در طول زمان رخ می دهد تا غیرقابل تشخیص باقی بماند.

به زبان ساده، حمله اسپری کردن رمز عبور زمانی اتفاق می افتد که مهاجمان با امتحان گذرواژه هایی که احتمالاً کاربران از آنها استفاده می کنند، به حساب قربانی دسترسی پیدا می کنند. این حمله را نباید با حمله پر کردن اعتبارنامه اشتباه گرفت زیرا در این روش مهاجمان از اعتبارنامه هایی که قبلاً در معرض خطر قرار گرفته اند برای حساب های مشابه سایر سرویس ها استفاده می کنند.

اسپری گذرواژه یک روش رایج است که مجرمان سایبری برای دسترسی غیرمجاز به سیستم‌های کامپیوتری از آن استفاده می‌کنند. به عنوان مثال، گزارش هزینه نقض داده های سال ۲۰۲۰ موسسه IBM نشان داد که ۱۹ درصد از تمامی نقض داده ها ناشی از اعتبارنامه های ضعیف یا به خطر افتاده بودند. همچنین گزارش تخلف داده های 2020  Verizon نشان داد که بیش از 80 درصد از همه نقض های مربوط به هک شامل روشهای بروت فورس مانند اسپری کردن رمز عبور است.

## اسپری کردن رمز عبور چگونه کار میکند؟

مجرمان سایبری می توانند از رمزگشایی رمز عبور برای دسترسی غیرمجاز به سیستم های شما استفاده کنند، زیرا افراد اغلب برای ایمن کردن حساب های خود از گذرواژه های واضح (رمزهایی که حدس زدن آنها آسان است) استفاده می کنند. در ادامه شرح خواهیم داد که گذرواژه های واضح چگونه این حمله را امکان پذیر می کنند.

### 1. مجرمان سایبری لیستی از نام های کاربری ایجاد یا خریداری می کنند.

در حال حاضر بیش از 15 میلیارد اعتبارنامه در دارک وب برای فروش وجود دارد. بنابراین برای شروع حمله اسپری کردن رمز عبور، مجرمان سایبری اغلب با خرید لیستی از نام های کاربری سرقت شده از سازمان های دیگر اقدام می کنند.

با این حال اغلب، مجرمان سایبری نیز لیست خود را با استفاده از الگوهایی که آدرس ایمیل شرکت (مثلا lastname.firstname@yourcompany.com) دنبال می کند را همراه با لیستی از افرادی که در آن شرکت کار می کنند (مثلا از طریق LinkedIn) ایجاد می کنند.

**1**) در **K**nown **P**laintext only **A**ttack (**KPA**) : مهاجم فقط یه P داره و C متناظرشو ، فقط همین دوتا ، مثلا :

123->202cb962ac59075b964b07152d234b70  
123->F9C3746B8AF2FF60B09D99F20BAC3F0C

مهاجم فقط خط اولو داره (مثلا) یا مهاجم فقط مثال دومو داره ، P که عدد 123 هست و C که عبارت رمز شده اون هست ، در این مورد معمولا الگریتم هم پیدا نیس ولی ما میتونیم اونو پیدا کنیم ولی هدف بیشتر بدست اوردن کلیده (در این دو مثال من در اولی ، با یه الگریتمی عدد123 رو هش کردم و در عبارت دوم امدم و عدد 123 رو با یه کلیدی تبدیلش کردم به یه عبارت رمز شده) حالا هکر باید در مثال اول الگریتمشو پیدا کنه که مثلا میره همرو تست میکنه میفهمه عه md5 عه و دومی هم میره تلاش میکنه میبینه عه الگریتم AES-EBC عه با این کلید "abcdefghijklmnop" با یه کلیدی که طولش 16 کاراکتره یعنی میشه 128 بیتی

**2**) در حالت known **C**iphertext **O**nly **A**ttack (**COA**) : مهاجم فقط یه C داره و دیگه هیچی نداره :)

SHA256 hash : 1f7285b0a2d5e803d550c3ff9e18c867f7cdde6ef187582a7dfdc8217d365553  
Gqzq0pMzZDc=

مثلا الان یه چالش فارنزیک یا پنتست هست که شما میخوای به یه سیستم ورود کنی و پسورد اون سیستمو دامپ کردی و حالا میخوای کرک کنی ، مثلا این پسورد (این حالا از خانواده SHA بوده یا مثلا پسورد میتونه NTLM و... باشه) ، الگریتم ممکنه معلوم نباشه و اونم شاید مجبور شید پیدا کنید

یا در مثال بعدیش یه پیامیه و رسیده به ما که هیچ دیدی نداریم ، و میخوایم بازش کنیم (مثل پیام هایی که در جنگ ها ردوبدل میشه) مثلا در اینجا میدونیم که پیامی که ما داریم فرمت base64 هست ولی نمیدونم که الگریتمش des هست و کلیدش"abcdegf" و میخوایم این دوتارو پیدا کنیم

**3**) در **C**hosen **P**laintext **A**ttack (**CPA**) : ما میتونیم هر P ای که دوس داریمو بدیم و C نظیر و متقابلشو بگیریم ، در این روش الگریتم معلومه ولی کلید معلوم نیست و ما دنبال کلیدیم (یا مستقیم میخوایم به الگریتم حمله کنیم)

1:c4ca4238a0b923820dcc509a6f75849b  
2:c81e728d9d4c2f636f067f89cc14862c  
3:eccbc87e4b5ce2fe28308fd9f2a7baf3  
12:c20ad4d76fe97759aa27a0c99bff6710  
123:202cb962ac59075b964b07152d234b70  
...  
..  
.  
1:Vo5IelNXdtA=  
2:3/PLtQjbT7g=  
3:LK8BU9y0EWw=  
12:PXgjzko+UtI=  
123:pD8/onth+Fc=  
1:y6X5W9eGklc=  
2:nabFk0JtZLs=  
3:3XVi1Gw4WzA=  
12:RHNTRs4XIuo=  
123:ViiG13HwpTw=  
...  
..  
.

مثلا در اینجا ما امدیم و الگریتمو داریم که مثلا 5 تا مثال اول همگی با الگریتم هشینگ md5 هش شدن و ما هی تست میکنیم مقادیر مختلفی رو تا مثلا به Collision برسیم

یا مثلا در 10 تا مثال پایین ما میاییم و با الگریتم DES و با کلید های مختلف عبارت های مختلف رو رمز میکنیم و میرسیم به اینکه خب اون الگریتم چطوری عمل میکنه و .. مثلا 5 تا عبارت اول کلیدشون "a" بوده و 5 تای دوم "A" بوده

**4**) در  **C**hosen **C**iphertext **A**ttack (**CCA**) : مهاجم یه C داره و اونو میده و A رو میگیره (به هر روشی) و اینطوری به کلید میخواد پی ببره (این روش کم کارامد ترین روشه)

lvg8PFW22PA=

مثلا اینجا ما یه عبارت داریم و میخوایم به کلید این پی ببریم ، مثلا فرض کنید ما دونفر داریم که باهم دارن ارتباط برقرار میکنن ، فرد 1 داره با فرد 2 ارتباط برقرار میکنه ، در این حین یه فردی هم داره به این مکالمه گوش میکنه و امکان تغییر بسته هارو داره ، حالا در اینجا فرد 1 پیامی رو میفرسته به فرد 2 تحت این عنوان " Khoor Pb Iulhqg "و مهاجم که داره این وسط گوش میکنه میاد و پیامو به این تغییر میده " Helxo Op Jkfiens " (یه متن رندوم و شانسی) و وقتی پیام میرسه به فرد 2 و اون بازش میکنه میرسه به این "Khoar Rs Mnilhqv " و حالا اینجا  فرد دو میاد و تلفن میزنه به فرد 1 یا روی همون ارتباط بهش میگه این چه وضعشه ؟ منظورت از "Khoar Rs Mnilhqv " چیه ؟ بدون اطلاع به من کلیدو تغییر دادی؟

و مهاجم اینجا میفهمه که "Helxo Op Jkfiens" با کلید ناشناس میشه "Khoar Rs Mnilhqv"

Helxo Op Jkfiens - > Khoar Rs Mnilhqv

و میره مثلا در الگریتم سزار میبینه عه این کلیدش میشه 3 ، حالا میاد و پیام اصلی ای که بین اون دوتا رودبدل شده که "Khoor Pb Iulhqg" بوده رو با الگریتم سزار با کلید 3 رمز گشایی میکنه و میرسه به این " Hello My Friend "

این ساده ترین شکله ، دیگه خودتون گسترشش بدید

5 ) در این حالت **A**daptive **C**hosen **P**laintext/**C**iphertext **A**ttack (**ACPA**)(**ACCA**) : مهاجم یه P داره و با اضافه کردن جزء جزء یه سری چیزا به یه C میرسه و اینطوری میخواد به کلید یا و الگریتم پی ببره ، یا برعکس C رو داره و جز جز کم میکنه تا بره به P یا الگریتم و کلیدو پیدا کنه و بفهمه

مثال دقیق برای این موضوع ندارم و این نوع حمله برای الگریتم های قدیمی بیشتر کاربرد داشته

**نکته**: مثلا روش Brute Force معمولا برای **KPA**و **COA**کاربرد داره ، جایی که مهاجم میتونه صحت حدسو بررسی کنه

**نکته**: اگر براتون سوال پیش امده که فرق بین COA و CCA چیه ، باید بهتون بگم که در COA هدف معمولا P هست و در CCA هدف معمولا کلید هست

## حملات آنلاین غیرفعال (Passive Online Attacks)

حملات آنلاین غیرفعال  را شنود پسوردها در یک شبکه کابلی یا بی سیم نیز می نامند . حملات آنلاین غیرفعال توسط کاربر هدف قابل تشخیص نمی باشد . پسورد در طی پروسه تشخیص هویت کپچر شده و با لیست کلمات یا فایل دیکشنری مقایسه می شود .

پسوردهای اکانت کاربری معمولا هنگامی که در شبکه ارسال می شوند هش یا رمزنگاری می شوند تا از دسترسی غیرمجاز و استفاده از آن ممانعت بعمل آید . اگر که پسورد توسط رمزنگاری یا هش محافظت شود , ابزارهای خاصی به منظور شکستن این رمزها توسط هکرها به کار گرفته می شود . (کرک کردن پسوردها جلوتر آموزش داده خواهد شد) .

یک نوع دیگر از حملات آنلاین غیرفعال با نام Man in the Middle) MITM) یا همان شخصی در میان یا به عبارتی شخص واسط می باشد . در حمله MITM هکر به عنوان یک واسط فرایند درخواست های تشخیص هویت و شناسایی را انجام داده و به سرور هدایت می کند . به این وسیله با قرار دادن یک شنودگر در بین سرور و کلاینت , هکر قادر است تا اتصالات بین هر دو طرف را شنود کرده و کپچر کند .  
یک Replay Attack نیز جزو حملات آنلاین غیرفعال است . این حمله زمانی اتفاق می افتد که هکر به عنوان واسط شنودگر پسورد را به سمت سرور فرستاد و پروسه تشخیص هویت را اجرا می کند ولی این بار پسورد را کپچر کرده و بسته های تشخیص هویت را برای استفاده های بعدی نگه می دارد . به این شیوه هکر نیاز ندارد که پسورد را بشکند یا دانش شناسایی پسورد رمزشده را پیدا کند بلکه تنها پسورد را کپچر کرده و در استفاده های بعدی به کار می گیرد .

## حملات آنلاین فعال (Active Online Attacks)

حملات آنلاین فعال شامل چه انواعی هستند ؟ راحت ترین راه برای رسیدن به سطح دسترسی ادمین به یک سیستم حدس زدن یک پسورد ساده با این فرض است که ادمین از یک رمز ساده استفاده کرده است . حدس پسورد جزو  حملات آنلاین فعال  است . این حمله بر عامل انسانی که ممکن است پسوردهای ضعیف بسازد و یا از کلمات خاصی در آن استفاده کند دلالت دارد . در دروس قبلی وقتی که فاز سرشماری را توضیح دادیم , آسیب پذیری سرشماری نت بایوس (NetBIOS Enumeration) و سرشماری نشست های نال (Null Sessions Enumeration) را یاد گرفتید . فرض کنید که پورت 139 tcp باز است . موثر ترین شیوه برای نفوذ به یک سیستم NT یا ویندوز 2000 حدس زدن پسورد آن است . این شیوه از طریق تلاش برای اتصال به یک مسیر اشتراک مخفی که قبلا شرشماری شده مثل IPC$ یا C$ و امتحان یک ترکیبی از نام کاربری و کلمه عبور انجام می شود . رایج ترین اکانت ادمین به کار رفته Administrator , Sysadmin با رمز عبور password یا حتی پسورد نال (یعنی بدون پسورد) می باشد . هکر در ابتدا تلاش می کند تا به مسیر پیش فرض Admin$ یا C$ دسترسی پیدا کند . برای دسترسی به پوشه مخفی C: دستور زیر را در خط فرمان ویندوز وارد کنید (که آدرس آیپی هدف را باید جایگزین آن کرد) :

\\ip\_address\c$

برنامه های خودکار می توانند به سرعت فایل های دیکشنری , لیست کلمات یا هر ترکیب ممکنی از حروف را ایجاد کنند و سپس با استفاده از آنها به منظور لاگین به سیستم استفاده کنند . بیشتر سیستم ها از این نوع حمله ممانعت کرده . چگونه ؟ از طریق قرار دادن نهایت تعداد تلاش ها برای ورود پسورد و پس از دفعات خاص از حدس اشتباه پسورد , اکانت را برای مدت زمان محدودی که در پالیسی تعریف می شود , قفل می کند . در دو بخش زیر توضیح خواهیم داد که چگونه هکرها حدس خودکار پسورد را انجام می دهند و اقدامات متقابل با آن چیست ؟

## شیوه حدس پسورد

به منظور بالا بردن سرعت حدس یک پسورد , هکرها از ابزارهای خودکار استفاده می کنند . یک پروسه آسان برای انجام حدس خودکار پسورد استفاده از دستورات Shell بر اساس استاندارد NET USE است . برای ایجاد یک اسکریپت خودکار که این کار را برای شما انجام دهد , مراحل زیر را طی کنید :

* با استفاده از نوتپد یک فایل نام کاربری و رمز عبور ساده بسازید . ابزارهای خودکار همچون Dictionary Generator به منظور ایجاد این لیست در دسترس هستند .
* فایل ایجاد شده را در داخل درایو C: با نام credentials.txt ذخیره کنید .
* از این فایل در دستور زیر استفاده کنید :
* C:\> FOR /F “token=1, 2\*” %i in (credentials.txt)
* دستور زیر را به منظور تلاش برای لاگین به مسیر مخفی اشتراکی استفاده کنید :
* net use \\targetIP\IPC$ %i /u: %j

## **حمله Brute force چیست؟**

حمله Brute Force یکی از روشهای هکرها برای یافتن رمزهای عبور میباشد. معمولا این کار توسط نرم افزار های مخصوصی انجام میشود. در این حمله هکرها هیچ اقدامی برای رمزگشایی پسورد نمی کنند؛ بلکه با استفاده از نرم افزارهایی سعی در حدس زدن پسورد و بررسی تمام حالات ممکن برای یافتن پسورد صحیح مینماید. در صورتی که رمز پیچیده و طولانی باشد، این کار بسیار زمانبر خواهد شد.

این نوع حملات به دو فاکتور زمان زیاد و قدرت پردازش بالا احتیاج دارد و خوشبختانه تا حدودی این دو مورد بازده هکرها را پایین آورده است. اما هکرها با این دو مشکل چگونه برخورد کردند؟

با ما همراه باشید تا در ادامه نحوه عملکرد Brute Force و روشهای مقابله با این حملات را بررسی نماییم.

**قدرت پردازش بالا**: فرایند رمزگشایی، عملیات محاسباتی پیچیده ای هستند و برای انجام آن، نیاز به قدرت بالای سیستم نرم افزاری کامپیوتر می باشد. از آنجا که کامپیوتر هایی با سخت افزار های بهتر و در نتیجه سرعت پردازش بیشتر روانه بازار شده اند، در نهایت این عملیات و حمله ها سریعتر و موثرتر واقع شده اند.

شاید تصور کنید که حمله Brute force بار زیادی روی CPU ایجاد میکند؛ اما بد نیست بدانید موثرترین سخت افزار برای حملات Brute force، کارت گرافیک یا (GPU) میباشد.

**زمان زیاد:** در این نوع حملات همه حالت های ممکن پسورد بصورت ترکیبی از کاراکتر ها شامل جایگشت های مختلف اعداد، حروف کوچک، بزرگ و کاراکترهای خاص بررسی میشود. این بررسی معمولا با یک کاراکتر شروع شده و پس از بررسی تمام حالات یک کاراکتری، بررسی تمامی موارد دو کاراکتری، سه کاراکتری و... شروع شده و این روند تا زمان کشف پسورد مربوطه، ادامه خواهد یافت. از نظر تئوری این روش در نهایت به جواب خواهد رسید، بطور مثال اگر پسورد مربوطه 6 رقمی 123456 باشد، به راحتی طی زمان نسبتا کوتاهتری، توسط این روش قابل حدس زدن خواهد بود.

اما تصور کنید که رمز مربوطه، بسیار طولانی و پیچیده باشد؛ در اینصورت این فرایند بسیار زمان بر و طولانی خواهد شد.

با توجه به پیچیدگی رمز و الگوریتم هایی که استفاه شده است ممکن است، بین چند ساعت، چند روز، چند ماه و یا حتی چندین سال زمان ببرد.

هکرها برای بهبود این روش و سریعتر پیدا شدن پسورد مورد نظر از روش Dictionary Attack استفاده میکنند. در این روش به جای بررسی تمام حالت های ممکن تنها عبارت و کلماتی که به طور معمول برای پسوردها استفاده میگردد،(نظیر اسامی اشخاص و یا مکان ها و...) و یا پسورد های ساده ای که توسط کاربران مبتدی استفاده میگردد (نظیر password،123456،abc123،qwerty و....) بررسی میشود ، این روش بسیار کارآمدتر خواهد بود و شانس یافتن پسورد را زیاد کرده و در عین حال زمان کمتری صرف میشود.

**راه های جلوگیری از حملات Brute force**

حملات Brute force میتواند به صورت آنلاین و یا آفلاین باشد.

**حملات Brute force آنلاین:**

چنانچه Brute force روی اکانت های آنلاین، مانند اکانت های ورود به کنترل پنل سایت ها، ورود به حساب کاربری ایمیل ها و ... انجام شود، با توجه به موارد امنیتی ارائه شده در سرورها، از حمله هکر ها جلوگیری به عمل می آید. بدین صورت که هر کاربر در بازه ی زمانی مشخصی، تنها مجاز است به تعداد دفعات محدود(معمولا 3 یا 4 بار)، اقدام به وارد کردن نام کاربری و پسورد اشتباه کند. چنانچه تعداد دفعات بیشتر از این مقدار گردد، IP کاربر جهت جلوگیری از حملات Brute forceو هک شدن، توسط فایروال ها مسدود میگردد.

به عنوان مثال پس از چندین بار اشتباه وارد شدن پسورد در اکانت جیمیل، جیمیل برای اطمینان از وارد نشدن پسورد توسط روبات ها، کد Captcha نمایش خواهد داد که این اقدام نیز از حملات Brute force جلوگیری می نماید.

بنابراین در صورت رعایت شدن نکات امنیتی ازسمت سرور ها، این حملات در برابر سرویس های آنلاین، بازدهی خوبی نخواهند داشت. (در سرورهای تاژان این نکات امنیتی رعایت شده است.)

**حملات Brute force آفلاین:**

در حالت دیگر تصور کنید که هکر فایل مربوط به پسوردهای رمزگذاری شده را بدست آورده باشد و یا اقدام به دانلود کردن این فایل ها بر روی کامپیوتر خود کرده باشد؛ در این حالت نحوه رمزگذاری اطلاعات را روی سیستم خود دارد و هر چند بار که بخواهد بدون محدودیت، میتواند پسورد های مختلف را امتحان نماید. در صورتی که فایل در اختیار هکرها قرار گیرد، عملا به هیچ وجه نمی توان از این حملات جلوگیری نمود.

پس چنانچه حتی از الگوریتم های پیچیده و نرم افزارهای مطمئنی نظیر [KeePass](https://sazmanhost.com/KB/341/keepass-%DA%86%DB%8C%D8%B3%D8%AA-%D9%88-%DA%86%DA%AF%D9%88%D9%86%D9%87-%DA%A9%D8%A7%D8%B1-%D9%85%DB%8C-%DA%A9%D9%86%D8%AF-%D8%9F)، برای نگهداری پسورد های خود استفاده میکنید، میبایست آنها را در جایی امن نگهداری نمایید و مطمئن باشید کسی غیر از خود شما به آن دسترسی نخواهد داشت.

**چگونه از اطلاعات خود در برابر این حملات محافظت کنیم؟**

عملا میتوان گفت روشی برای مقابله کامل با این نوع حملات وجو ندارد؛ اما میتوان به نحوی احتمال یافتن پسورد از طریق این حملات را به حداقل رساند. برخی از این روش ها به شرح زیر می باشد:

* چنانچه سرویسی بر روی اینترنت دارید که نیاز به لاگین کردن و ورود پسورد دارد، مطمئن باشید که سرورهای مربوطه، موارد امنیتی جهت جلوگیری از این حملات را رعایت کرده باشند.
* از رمزهای پیچیده و طولانی استفاده نمایید، رمز ها میبایست شامل حروف بزرگ و کوچک و اعداد و کاراکتر های خاص باشند.
* از کلمات معنی دار و قابل حدس در رمزهای عبور استفاده ننمایید.
* از الگوریتم های رمزگذاری پیچیده مانند SHA-512 استفاده نمایید، از الگوریتم های رمزگذاری قدیمی و یا ضعیف استفاده نکنید. در صورت استفاده کردن از الگوریتم های پیچیده و جدید به طور چشمگیری سرعت حملات Brute force را کاهش میدهد.
* پسوردهای خود را در نرم افزارهایی مانند [KeePass](https://sazmanhost.com/KB/341/keepass-%DA%86%DB%8C%D8%B3%D8%AA-%D9%88-%DA%86%DA%AF%D9%88%D9%86%D9%87-%DA%A9%D8%A7%D8%B1-%D9%85%DB%8C-%DA%A9%D9%86%D8%AF-%D8%9F)نگهداری نمایید، در این صورت هم پسوردهای پیچیده خود را فراموش نمیکنید و به راحتی به آنها دسترسی خواهید داشت و همچنین امنیت این نرم افزار در برابر اینگونه حملات بسیار بالا میباشد.
* در نهایت اطلاعات رمزگذاری شده خود را در جای امن**ی ترجیحا روی سیستم دیگر**نگه دارید که هکرها به آن دسترسی نداشته باشند.