
بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

عنوان :

Brute Force

نام استاد : استاد کریمی

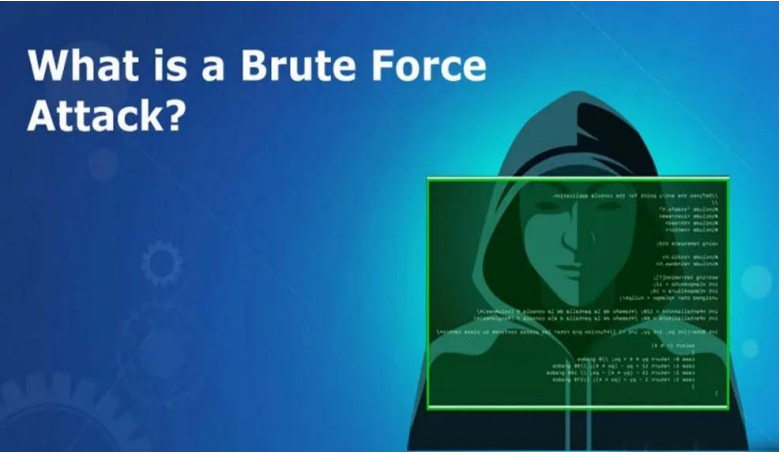
نام دانشجو : محمد حسین مسعودی پور

فهرست

- تعریف حمله ی Brute Force
- انواع مختلف آن
- روش های مقابله در برابر این حمله
- پیاده سازی حمله ی Brute Force

حمله بروت فورس
به زبان ساده:

وقتی همکلاسی قدیمیت رو می‌بینی



حمله Brute Force چیست؟

- حمله بروت فورس (Brute Force) یک روش آزمون و خطا برای رمزگشایی اطلاعات لاگین و بازکردن کلیدهای رمزگذاری‌شده و به عبارتی دسترسی غیرمجاز به سیستم‌ها است.
- حملات بروت فورس به جای استفاده از استراتژی‌های عقلانی از توسل به زور استفاده می‌کنند.
- در روند این حمله احتمال نصب بدافزار، خاموش‌کردن برنامه‌های وب یا نفوذ به داده‌ها هم وجود دارد.
- مدت زمان حملات بروت فورس متفاوت است؛ ممکن است شکستن رمزهای عبور ضعیف تنها چند ثانیه و رمزهای قوی ساعت‌ها یا روزها طول بکشد.

انواع مختلف حملات Brute Force

- حمله لغت‌نامه‌ای (Dictionary Attack)
- حمله پرکردن اعتبارنامه (Credential Stuffing)
- حمله بروت فورس معکوس (Reverse Brute Force)

انواع مختلف حملات Brute Force

- **حمله لغت‌نامه‌ای (Dictionary Attack):**
  - نوعی حمله سایبری است که در آن هکرها برای شکستن رمز عبور از لیستی از کلمات رایج و معمولی استفاده می‌کنند. هکرها با امتحان کردن این کلمات به عنوان رمز عبور، سعی در دسترسی به حساب‌های کاربری دارند

انواع مختلف حملات Brute Force

❖ حمله پرکردن اعتبارنامه (Credential Stuffing) :

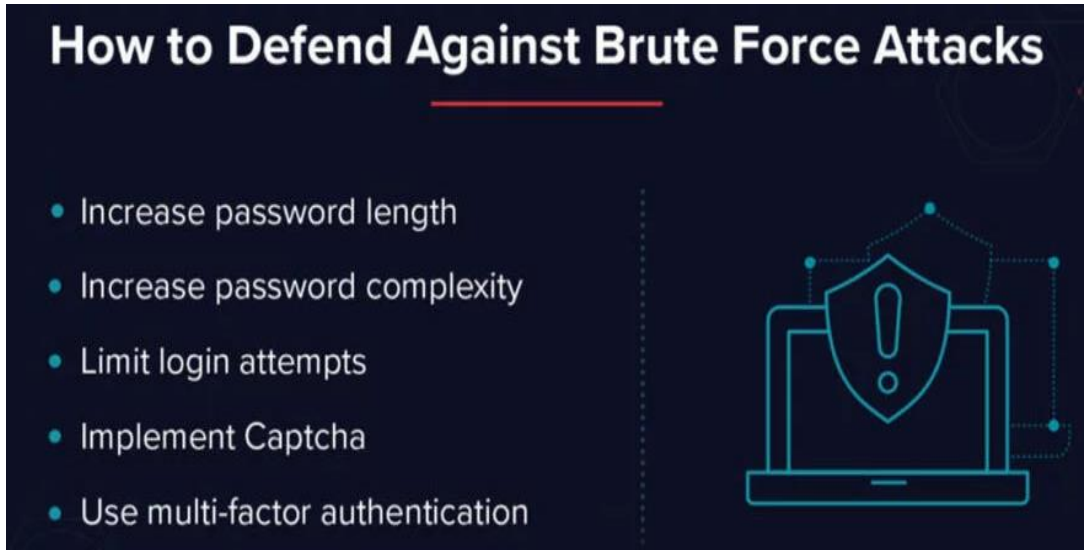
- ❖ یک نوع حمله سایبری است که در آن هکرها از نام‌های کاربری و رمزهای عبور دزدیده شده از یک سرویس برای دسترسی به حساب‌های کاربران در سرویس‌های دیگر استفاده می‌کنند.
- ❖ این حمله به دلیل استفاده مجدد کاربران از رمزهای عبور مشابه در سرویس‌های مختلف موفقیت‌آمیز است.

انواع مختلف حملات Brute Force

- **حمله بروت فورس معکوس (Reverse Brute Force) :**
  - نوعی حمله سایبری است که در آن هکرها یک رمز عبور رایج یا لو رفته را برای تعداد زیادی از نام‌های کاربری امتحان می‌کنند تا به حساب‌هایی که از آن رمز عبور استفاده می‌کنند، دسترسی پیدا کنند.

بهترین راهکارهای محافظت در برابر حملات بروت فورس چیست؟

- **سخت‌تر کردن رمز عبور:**
  - پیچیده‌تر کردن رمز عبور باعث طولانی‌تر شدن زمان لازم برای رمزگشایی گذرواژه می‌شود.
  - برای این منظور می‌توانید قوانین مدیریت رمز عبور مانند حداقل طول عبارت رمز و استفاده اجباری از کاراکترهای خاص را اعمال کنید.



بهترین راهکارهای محافظت در برابر حملات بروت فورس چیست؟

- **محدود کردن لاگین‌های ناموفق:**
  - یک راه دیگر برای محافظت از سیستم‌ها و شبکه‌ها، اجرای قوانینی است که پس از چندبار تلاش ناموفق برای لاگین، مانع دسترسی کاربر می‌شوند.

- **رمزگذاری و هشینگ (Hashing):**
  - استفاده از رمزگذاری ۲۵۶ بیتی و هشینگ پسورد، زمان و قدرت محاسباتی مورد نیاز برای اجرای حمله بروت فورس را به‌طور تصاعدی افزایش می‌دهد.
  - در هش‌کردن رمز عبور، رشته‌ای از کاراکترها در یک پایگاه داده جداگانه ذخیره و به گونه‌ای هش می‌شوند که ترکیب‌های رمز عبور مشابه، مقدار هش متفاوتی داشته باشند.

بهترین راهکارهای محافظت در برابر حملات بروت فورس چیست؟

- **پیاده‌سازی کپچا (CAPTCHA):**
  - کپچاها در عین حال که مانعی بر سر راه ابزارهای حمله بروت فورس هستند؛ سیستم‌ها، شبکه‌ها و وب‌سایت‌ها را در دسترس کاربران انسانی نگه می‌دارند.

- **اجرای احراز هویت دوعاملی (2FA):**
  - استراتژی Two-Factor Authentication نوعی احراز هویت چندعاملی است که با اجرای دو شکل از تایید هویت، لایه امنیتی اضافی را برای ورود به سیستم ایجاد می‌کند.
  - به‌طور مثال کاربران اپل برای ورود به یک دستگاه جدید باید اپل آیدی خود را به همراه یک عدد شش رقمی نمایش‌داده‌شده در یکی از دستگاه‌های قبلی‌شان وارد کنند.

پیاده سازی Brute Force

Kali Linux

- Kali Linux یک سیستم‌عامل متن‌باز مبتنی بر Debian است که برای جرم‌شناسی دیجیتال و تست نفوذ طراحی شده است که توسط Offensive Security توسعه داده شده است.

- این سیستم‌عامل شامل مجموعه‌ای گسترده از ابزارهای امنیتی و هک اخلاقی، مانند Hydra، Metasploit و Nmap می‌باشد.

- Kali Linux قابلیت اجرا بر روی انواع پلتفرم‌ها از جمله کامپیوترهای دسکتاپ، لپ‌تاپ‌ها و حتی دستگاه‌های موبایل را داراست.

پیاده سازی Brute Force

Hydra

- Hydra یک ابزار قدرتمند برای کرک کردن رمزهای عبور است که به ویژه در تست نفوذ و هک اخلاقی استفاده می‌شود که این ابزار در Kali Linux گنجانده شده است.

- این ابزار می‌تواند حملات brute-force از نوع dictionary را بر روی پروتکل‌های مختلف مانند FTP، SSH، HTTPو بسیاری دیگر انجام دهد.

پیاده سازی Brute Force

Metasploit

- Metasploit یک چارچوب متن‌باز است که به‌طور گسترده توسط هکرهای اخلاقی، تیم‌های امنیتی و پژوهشگران برای شناسایی و رفع آسیب‌پذیری‌ها به کار می‌رود.

- این ابزار توسط Rapid7 نگهداری می‌شود و به محققان امنیت اجازه می‌دهد تا نقاط ضعف سیستم‌ها و شبکه‌ها را شناسایی و بهره‌برداری کنند.

- این ابزار از زبان‌های برنامه‌نویسی مانند Ruby استفاده می‌کند و قابلیت یکپارچه‌سازی با ابزارهای دیگر را دارد.

جمع بندی

- **حمله بروت فورس (Brute Force Attack)** یکی از روش‌های قدیمی مجرمان سایبری برای به دست آوردن رمز عبور سیستم‌ها، اکانت‌ها و شبکه‌ها است.
- مهاجم آنقدر ترکیب‌های احتمالی گذرواژه را امتحان می‌کند تا در نهایت موفق به شناسایی رمز عبور صحیح شود.
- به همین دلیل اولین راهکار پیشنهادی برای محافظت در برابر حملات بروت فورس، استفاده از پسوردهای پیچیده و طولانی است.
- البته بهتر است برای ایجاد امنیت سایبری بیشتر از ترکیبی از استراتژی‌ها مانند محدود کردن لاگین‌های ناموفق، هشینگ، پیاده‌سازی کپچا و احراز هویت دوعاملی استفاده شود.
- بعلاوه سازمان‌ها می‌توانند با استفاده از ابزارهای رایج حمله بروت فورس مانند Hydra ، Hashcat، Aircrack-ng و John the Ripper امنیت شبکه را تست کنند.

پایان