به نام خدا

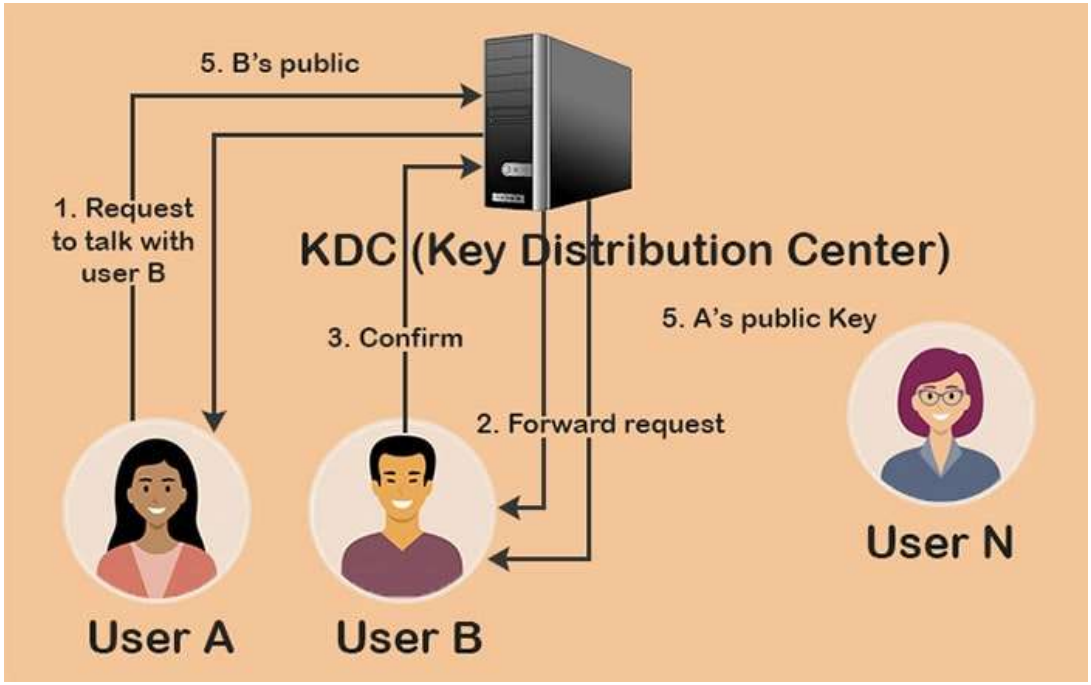
اسماعیل زارع

Kerberos کربروس چیست؟

Kerberosیا کربروس یک پروتکل امنیتی برای احراز هویت در شبکه است که برای کاربران مجاز امکان ورود به شبکه پس از تایید هویت را فراهم می آورد Kerberos .برای محافظت از خدمات شبکه توسط پروژه آتنا ارائه شده و در دانشگاه MIT توسعه یافته است . پروتکل برمبنای پروتکل کلید متقارن Needham –Schroeder است. نام این پروتکل Kerberosیا سربروس از اساطیر یونان گرفته شده‌است، که به سگ سه سر نگهبان جهنم معروف بود.

ویژگی های اصلیKerberos

- ایمن است . هرگز پسورد را ارسال نمی کند مگر اینکه رمزنگاری شده باشد.
- به ازای هر نشست تنها یک بار لاگین نیاز است . اعتبارنامه هایی که در زمان لاگین تعریف می شوند در ادامه کار بین منابع عبور داده شده تا نیاز به لاگین اضافی نباشد.
- این مفهوم وابسته به یک سیستم سوم شخص با نام مرکز توزیع کلید یا همان KDC یا Key Distribution Center می باشد.
- این پروتکل احرازهویت دوجانبه و متقابل را انجام می دهد . به این صورت که کلاینت هویت خود را برای سرور اثبات می کند و سرور هم متقابلا هویت خود را برای کلاینت اثبات می کند.



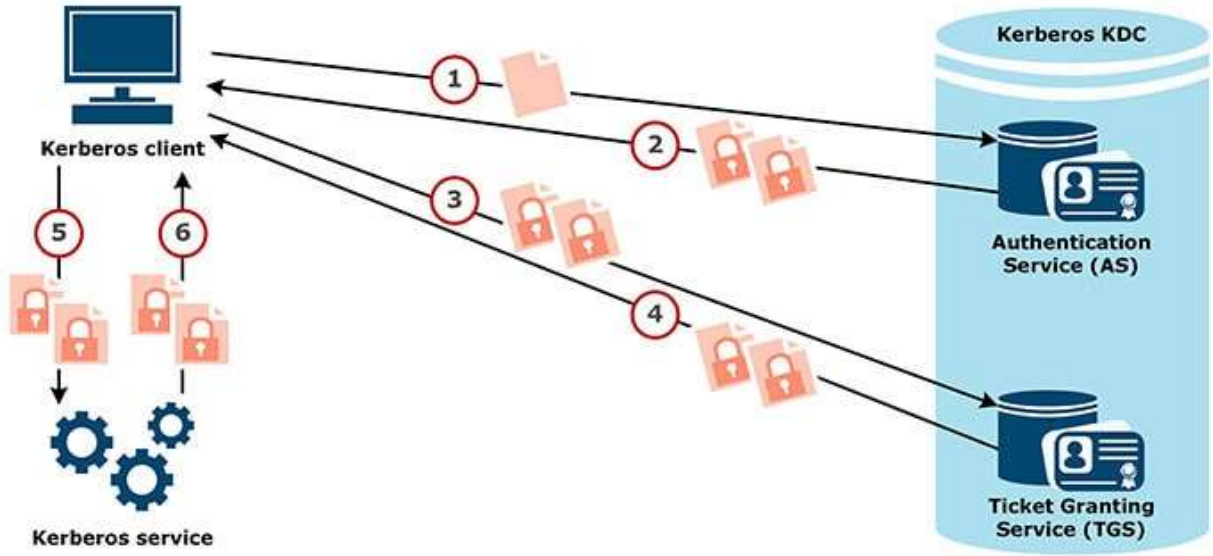
نحوه ی کار Kerberos

کاربران تیکت یا بلیط هایی را ازمرکز توزیع کربروس (KDC) دریافت می کنند و پس از آن هنگامی که ارتباط با شبکه فراهم شد کاربران این بلیط ها را به سرور ارائه می کنند و در صورت تایید مجوز ورود به شبکه فراهم می شود. بلیط های کربروس اعتبار کاربران شبکه را نشان می دهند.قبل از این که ارتباط امنی در شبکه برقرار شود پروتکل کربروس یک مکانزیم برای تایید دو طرفه اطلاعات بین موجودیت های شبکه فراهم می کنند. اگرچه این ارتباط امن بین سرورها نیز می تواند به وجود آید اما بر اساس این مستندات این دو موجودیت کاربر و سرور نامیده می شوند.

در پروتکل امنیتی کربروس کاربر و سرور به عنوان اصول امنیتی در نظر گرفته می شوند.پروتکل کربروس فرض می کند که معادلات بین کاربر و Server بر روی یک شبکه محافظت نشده قرار دارد به گونه ای که بیشتر کاربران و بسیاری از سرورها از امنیت کافی برخوردار نیستند و بسته هایی که از طریق شبکه در حال جابجایی هستند می توانند نظارت و دستکاری شوند. محیط فرضی پروتکل امنیتی کربروس مانند اینترنت امروزی است که هکرها می توانند در نقش سرورها و یا کاربران ظاهر شوند و به راحتی ارتباطات بین سرور و کاربر را مورد نظارت و دستکاری قرار دهند.

روش کار در الگوریتم کربروس:

به این صورت است که وقتی کاربری به یک شبکه Kerberos وارد می شود ، یک پیغام درخواست به سرور مربوط به نام و کلمه عبور حساب خود می فرستد. آن سرور با یک TGT که بر مبنای کلمه عبور سرویس گیرنده رمزنگاری شده است جواب می دهد . محض دریافت TGT از کاربر درخواست می شود که کلمه عبور خود را وارد کند و سپس از آن کلمه عبور برای رمزگشایی TGT استفاده می کند. چون در واقع فقط یک کاربر باید دارای کلمه عبور درست باشد ، این روند به عنوان احراز هویت عمل می کند. اگر رمزگشایی TGT با موفقیت انجام شود ، کاربر می تواند یک درخواست ، حاوی یک کپی رمزنگاری شده از TGT به یک سرور TGS، که الزاماً همان سرور احراز هویت اول نمی باشد ، بفرستد و به منابع شبکه دسترسی پیدا کند.



سرور TGS بعد از رمزگشایی TGT و تشخیص وضعیت کاربر یک بلیط سرور (Server Ticket) ایجاد می کند و به برای او می فرستد. این بلیط ، کاربر را قادر می سازد برای مدت زمان محدودی به یک سرور مشخص دسترسی داشته باشد. این بلیط همچنین حاوی یک کلید نشست (Session key) می باشد که کاربر و سرور از آن می توانند برای رمزنگاری داده های در حال انتقال بین خود استفاده کنند. کاربر در صورت نیاز به یک منبع ، بلیط سرور را به آن سرور می فرستد. سرور بعد از رمزگشایی آن بلیط ، امکان دستیابی به منبع مورد نظر را فراهم می کند.

چه تفاوتی بین Kerberos و NTLM وجود دارد؟

قبل از کربروس مایکروسافت از یک فناوری احراز هویت به‌نام NTLM (NT Lan Manager) استفاده می‌کرد که یک پروتکل احراز هویت چالش–پاسخ بود. کامپیوتر یا کنترل‌کننده دامنه گذرواژه‌ها را بررسی و هش گذرواژه را برای استفاده مداوم ذخیره می‌کرد. بزرگ‌ترین تفاوت این دو سیستم در احراز هویت ثالث و توانایی رمزنگاری قدرتمندتر کربروس است. کربروس در مقایسه با NTLM از یک لایه امنیتی اضافی در فرآیند احراز هویت استفاده می‌کند. این روزها سیستم‌های مبتنی بر NTLM را می‌توان در عرض چند ساعت هک کرد. به بیان ساده NTLM یک فناوری قدیمی و به تعبیری منسوخ شده است که نباید برای محافظت از داده‌های حساس از آن استفاده کرد.

کربروس هک‌پذیر است؟

بله .زیرا یکی از متداول‌ترین پروتکل‌های احراز هویت است و هکرها هم چند راه برای نفوذ به آن ابداع کرده‌اند. اغلب این هک‌ها بر مبنای آسیب‌پذیری‌ها، گذرواژه‌های ضعیف یا بدافزارها (یا برخی اوقات هر سه مورد) انجام می‌شوند .کربروس به روش‌های زیر هک می‌شود:

- رد کردن بلیط: فرآیندی که در آن یک کلید نشست جعل می‌شود و این کلید جعلی به عنوان یک مدرک هویتی معتبر در اختیار منبع قرار می‌گیرد.
- بلیط طلایی: یک بلیط که برای دسترسی مدیریتی برای کاربر صادر می‌شود.
- بلیط نقره‌ای: یک بلیط جعلی که برای دسترسی به یک سرویس صادر می‌شود.
- Credential stuffing/ Brute force: تلاش‌های خودکار پی در پی برای حدس زدن یک گذرواژه
- خنثی کردن رمزگذاری با Skeleton Key Malware: یک بدافزار که می‌تواند کربروس را دور بزند، اما حمله باید از طریق دسترسی مدیریتی انجام شود.
- حمله DCShadow: یک حمله جدید در مکانی که حمله‌کنندگان دسترسی کافی به شبکه دارند تا بتوانند از کنترل‌کننده دامنه اختصاصی خود برای نفوذ بیشتر استفاده کنند.

کربروس منسوخ خواهد شد؟

کربروس تا منسوخ شدن فاصله زیادی دارد و با وجودی که هکرها توانایی نفوذ به آن‌را دارند ثابت کرده که یک پروتکل کنترل دسترسی امنیتی قابل قبول است. اصلی‌ترین مزیت کربروس توانایی استفاده از الگوریتم‌های رمزنگاری قوی برای محافظت از گذرواژه‌ها و بلیط‌های احراز هویت است. با کامپیوترهای امروزی هر نوع حمله جست‌جوی فراگیر (Brute Force) به پروتکل رمزنگاری AES که کربروس از آن استفاده می‌کند و درهم شکستن آن به زمانی معادل با طول عمر خورشید نیاز دارد. بدون شک کربروس به هر شکلی که ارائه شود تا مدت زمان نسبتا طولانی قابل استفاده است.