تونل‌سازی امن DNS با رمزنگاری متقارن

هدف

هدف این پروژه ساخت یک سیستم ارتباطی امن و مخفیانه است که در آن کلاینت (Agent) داده‌های رمزنگاری‌شده را از طریق DNS queries به سرور ارسال می‌کند. این پروژه استفاده از symmetric cryptography (مثلاً AES) برای محافظت از داده‌ها در حین انتقال را نشان می‌دهد.

اجزای پروژه

1. **Agent (کلاینت):**
   - به‌عنوان فرستنده داده عمل می‌کند.
   - داده را با استفاده از symmetric key (مثلاً AES-256) رمزنگاری می‌کند.
   - تکه‌های رمزنگاری‌شده را با استفاده از Base32 یا Base64 کدگذاری می‌کند تا در DNS labels جا بگیرند.
   - هر تکه را به‌صورت بخشی از یک DNS query ارسال می‌کند.
   - پیام‌های acknowledgment را پیاده‌سازی می‌کند (Agent می‌داند که آیا سرور دریافت کرده یا نه).
   - یک sequence number اضافه می‌کند تا ترتیب درست و اعتبار پیام تضمین شود.
2. **Server (گیرنده):**
   - یک custom DNS server اجرا می‌کند.
   - به DNS queries با دامنه‌ی تونل مانند tunnel.yourdomain.com گوش می‌دهد.
   - داده را از subdomain کوئری استخراج می‌کند.
   - هر تکه را decode و سپس با استفاده از کلید متقارن decrypt می‌کند.
   - فایل یا پیام اصلی را به ترتیب درست بازسازی می‌کند.
3. **Crypto Module (مشترک بین Agent و Server)**
   - از AES (CBC یا GCM) برای رمزنگاری و رمزگشایی استفاده می‌کند.
   - کلید به‌صورت دستی پیکربندی شده و از قبل به اشتراک گذاشته شده است.
   - مدیریت padding، تولید IV یا nonce و یکپارچگی رمزنگاری را انجام می‌دهد.
   - انتقال امن داده‌ها از طریق کانال DNS را تضمین می‌کند.

🔁 جریان ارتباط (مثال):

1. Agent داده را می‌خواند (مثلاً یک پیام یا فایل).
2. داده به تکه‌هایی تقسیم می‌شود.
3. هر تکه:
   - با AES رمزنگاری می‌شود
   - با Base32 کدگذاری می‌شود
   - به‌صورت DNS query ارسال می‌شود
4. سرور:
   - DNS query را دریافت می‌کند
   - زیر دامنه را استخراج می‌کند
   - آن را decode و decrypt می‌کند
   - داده‌ی اصلی را بازسازی می‌کند

💡 سناریوی کاربردی:

فرض کنید در محیطی هستید که اتصال‌های خروجی شبکه محدود شده‌اند، اما DNS همچنان مجاز است. در این شرایط، DNS tunneling می‌تواند برای دور زدن این محدودیت‌ها استفاده شود. در این پروژه، این مفهوم را به همراه حفظ محرمانگی با استفاده از symmetric encryption پیاده‌سازی کنید.

📂 خروجی‌های مورد انتظار:

1. کد Agent (ارسال DNS queries رمزنگاری‌شده)
2. کد Server (دریافت، رمزگشایی و بازسازی داده)
3. ماژول Crypto (مبتنی بر AES، قابل استفاده مجدد)
4. فایل README.md شامل:
   - نحوه اجرای هر جزء
   - نحوه پیاده‌سازی رمزنگاری و DNS tunneling
5. گزارش (PDF) شامل:
   - معماری پروژه
   - نمودار جریان ارتباط
   - جزئیات کلیدی رمزنگاری
6. ویدیو دمو برای نمایش انتقال داده از طریق DNS