Subdomain Enumeration 4

Advanced Method with Certificates

- طبعا اتعلمنا طرق كتير عشان نجيب ال subdomains لحد مازهقنا بس في فكره كويسه برا الصندوق تعالي اقولك عليها
- قبل ما اقولك حابب اعرفك حاجه اكيد انت عارف ان ال ssl وال tls certs بيكونو خاصين للاسم الشركه او البراند مش للموقع مش فاهم؟ تعالي افهمك
- تخيل معايا لو في شركه اسمها x.com ساعات هيا بيكون عندها a.com و b.com وساعات subdomains ده اكيد بس هنا هما كلهم تحت نفس الاداره او نفس اسم الشركه اللي هو x فا ساعتها كل ال subdomains والمواقع التابعه ليها فا هما كل دول هيكونو ليهم نفس ال ssl cert زي ما قولتلك فوق
- يعني مثلا wikipedia ده اسم الشركه تمام؟ عندها مواقع زي wikipedia.com او wikimedia.com هنا الشهاده لاسم wekipidia مش للموقع اي حاجه تابعه ليك يا باشا تاخد نفس شهادتك

ازاي اعرف ابحث عن ال subdomains باستخدام الcertificates

- عندنا موقع جميل اوي اسمه crt.sh ده يا باشا بتحطلو اسم الشركه اللي واخده الشهاده تعالي هوريك ازاي

- دي مثلا شهادة لشركة america airlines بص فوق كده عند خانة ال organization مكتوب فيها اسم الشركه ودي اللي هتكتبها فالسيرش علي موقع crt.sh وهو هيجيبلك اي حاجه مرتبطه بالشركه