Subdomain Enumeration 3

- طبعا احنا اتعلمنا طرق كتير عشان نجيب ال subdomains بس في طريقة غيرهم بس مش مفيده اوي وهقولك ليه دلوقتي

Amass

- اداة ال Amass كانت زمان كويسه جدا انما دلوقتي بقت بطيئه وبتاخد وقت عشان تجيب ال subdomain

```
amass intel -active -cidr 128.89.421.16/32
```

- الكوماند ده مثال بسيط كده لو بدور علي subdomains باستخدام ال amass
- حد هيقولي انت بتستعبطنا ياعم؟ فين الdomain او ال ip بتاع الموقع اصلا هقولك ماهو ال amass لأنهم ال amass بتدور علي ال subdomains باستخدام ال CIDR او ASN بتاع الشركه

`amass => tool name` intel => mode of search

`active => mode of recon` -cidr => option of search (ASN)-`

Subdomains Filtering

- انا دلوقتي مثلا معايا subdomains كتير عاوز اصفيهم لأني اكيد فيهم subdomains كتير duplicated فا عندي طريقتين عشان نشيل المتكرر

++Notepad

- من خلال البرنامج ده علي الويندوز هقدر اني اشيل ال duplicate

anew tool

- دي تول بتكون علي كالي لينكس بتنزلها من جيت هب

```
cat subdomains.txt | anew
```

- علاطول هيروح شايلك ال duplicate