**Exploring Subdomain Vulnerabilities Netflix**

Tujuan saya melakukan ini meningkatkan kesadaran pemilik domain atau organisasi tentang risiko keamanan subdomain, terutama terkait *subdomain takeover* dan juga memberikan panduan kepada pemula atau penggiat keamanan siber tentang cara melakukan subdomain enumeration dan analisis kerentanannya.

**Information ghatering**

Disini saya melakukan passive information gathering, dimana disini crt.sh berguna untuk menemukan subdomain yang mungkin tidak terdokumentasi. Dan censys digunakan untuk menemukan data terkait domain, termasuk subdomain dan sertifikat.

crt.sh

A screenshot of a computer

Description automatically generated

censys

A screenshot of a computer

Description automatically generated

**Pelaksanaan**

Disini saya menggunakan subfinder untuk menghasilkan daftar subdomain yang ditemukan dan outputnya disimpan di file subdomain.txt.

A screenshot of a computer

Description automatically generated

Lanjut disini saya menggunakan assetfinder untuk enghasilkan daftar subdomain tambahan dari sumber alternatif dan outputnya di simpan di file subdomain1.txt.

A screen shot of a computer screen

Description automatically generated



.

Disini dengan command (sort -u subdomain.txt subdomain1.txt > mainsubdomain.txt) yang dimana sort -u untuk menggabungkan isi file subdomain.txt dan subdomain1.txt, lalu menghapus duplikasi. Outputnya adalah mainsubdomain.txt, yang merupakan daftar subdomain unik. Dan juga untuk command cat subdomain.txt | wc -l, cat subdomain1.txt | wc -l, cat mainsubdomain.txt | wc -l itu untuk menghitung jumlah baris dalam setiap file.

A screen shot of a computer program

Description automatically generated

Lanjut disini saya menggunakan httpx-toolkit untuk memastikan subdomain yang ditemukan benar-benar aktif dan dapat digunakan untuk langkah selanjutnya.

A screen shot of a computer

Description automatically generated

Terakhir disini saya menggukan subzy untuk mendeteksi potensi kerentanan takeover untuk subdomain yang ditemukan.

A screen shot of a computer

Description automatically generated

