Script para Subdomain Takeover

+ Fazemos a validação consultando os endereços na internet

+ Endereços não encontrados ou que deram erro são bons indícios de um vetor de ataque com subdomain takeover

+ O comando host ---subdominio--- n retorna nada qnd o subdo está inativo, mas o host -t cname mostra pra onde ele apontava antes

+ Montando o script: [subtakeover.sh]

```
#!/bin/bash
for palavra in $(cat cat.txt); do
host -t cname $palavra$1 | grep "alias for"
done
```

+ Caso o link seja endereçado ao site da amazon, podemos criar uma conta gratuita no site dela e na hora de registrar um domínio gratuito, fazemo-lo com exatamente o nome do domínio que achamos