Wide scope methodology

BY UNCLE RAT

Agenda

- Summary
- Strategy
  - Subdomain enum
  - Httprobe
  - Vulnerability scanning
  - Custom templates
- Basic attack plan
- Where to go from here

Summary

Summary

1. Do subdomain enumeration on as much sources as possible
2. Check which subdomains are live
3. Run a vulnerability scanner
4. Write new templates for our scanner
5. Scan all the existing subdomains for new vulnerabilities
6. Scan new subdomains found for existing templates
7. Automate the whole thing
    1. VPS recommended for stability

Strategy

Strategy – Subdomain enumeration

- What is it?
  - Grab as much subdomains as we can
  - From as much sources as we can
    - Such as google dorking
    - Such as shodan
    - Such as crt.sh
    - …
  - The more sources, the bigger of a chance to find a unique subdomain

Strategy – Subdomain enumeration

- How to do it
  - Run all the tools you can find
    - https://github.com/projectdiscovery/subfinder
    - https://dnsdumpster.com/
    - https://www.shodan.io/
    - https://github.com/fwaeytens/dnsenum/
    - https://github.com/tomnomnom/assetfinder
    - https://crt.sh/
    - amass
    - findomain

Strategy – Subdomain enumeration

- What is our result
  - A list of subdomains
  - That may or may not be up
  - That we can use for our next steps

Strategy – httprobe

- What is it?
  - Checking which of the subdomains from our list is live
- How do we do it?
  - https://github.com/tomnomnom/httprobe
- What is our result?
  - A list of subdomains that we know are live

Strategy – Vulnerability scanning

- What is it?
  - We will automatically fire requests
  - We will then check the results
  - Very basic idea with huge potential
  - See video: How custom nuclei templates can help us in recon

Strategy – Vulnerability scanning

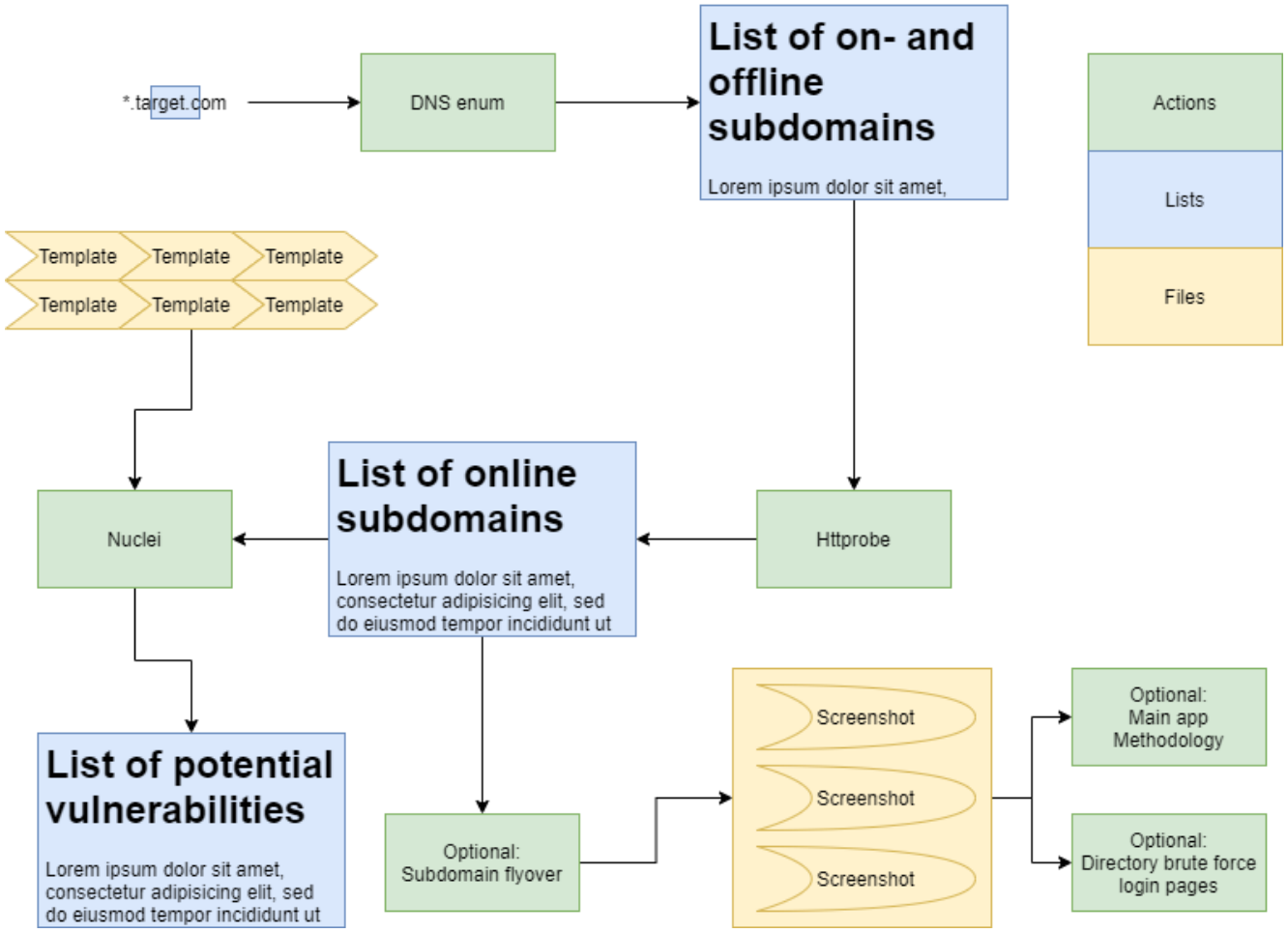
- How to do it?
  - Run nuclei vulnerability scanner on the list of existing subdomains
  - Verify any potential report
- What is our result?
  - A list of potential vulnerabilities we need to verify

Strategy – Custom templates

- What is it?
  - Nuclei vulnerability scanner uses templates
  - These are simple yaml files
  - In it's most basic form
    - Define metadata
    - Define requests that need to be made
    - Define checks that need to happen
- How to do it
  - Templating Guide - Nuclei - Community Powered Vulnerability Scanner (projectdiscovery.io)

Basic attack plan

Basic attack plan



Where to go from here

- Create a cronjob that will pick up any list in a certain folder and run nuclei on it
- Write all your subdomain lists to that folder
- Add subdomain brute forcing to your process
- Write your own templates for nuclei
- Auto scan all your existing domains with new nuclei templates