



BUG BOUNTY SUBDOMAIN RECON



BEST TOOLS & METHODS USED BY BUG HUNTERS



TOOLS USED

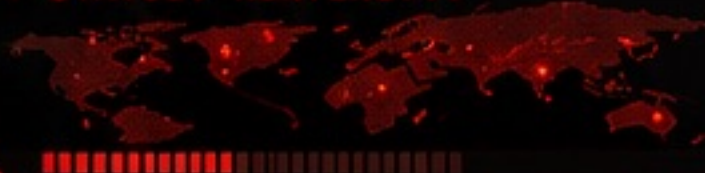
- BURP SUITE**
Web proxy, scanner and security testing platform
- CAIDO**
Modern proxy for faster interception and analysis
- SUBFINDER**
Fast passive subdomain enumeration
- AMASS**
In-depth network mapping and asset discovery
- ASSETFINDER**
Find subdomains via passive sources
- HTTPX**
Probe HTTP services, tech detect, screenshot, filter
- DNSX**
Fast DNS resolver and subdomain validation
- KATANA**
Modern web crawler for JS and API discovery
- GAU (GETALLURLS)**
Fetch URLs from AlienVault Open Threat Exchange
- WAYBACKURLS**
Fetch historical URLs from Wayback Machine
- NAABU**
Fast port scanner for large-scale recon
- AQUATONE**
Screenshot generator for visual recon
- NUCLEI**
Fast vulnerability scanner with extensive templates
- SHODAN**
Search engine for internet-connected devices
- SECURITYTRAILS**
Historical DNS and subdomain intelligence
- CRT.SH**
Certificate Transparency search for subdomains
- GITHUB**
Search code, configs, and domains in repositories
- CENSYS**
Internet scanning and asset discovery
- CHAOS**
Passive DNS database from ProjectDiscovery



METHODS USED

- PASSIVE SUBDOMAIN ENUMERATION**
Using public sources, APIs, and databases to find subdomains
- ACTIVE SUBDOMAIN ENUMERATION**
Directly querying and brute forcing to discover subdomains
- DNS BRUTEFORCING**
Using wordlists to brute force subdomains via DNS
- PERMUTATION SCANNING**
Generating permutations to find hidden subdomains
- CERTIFICATE TRANSPARENCY SEARCH**
Using CT logs to find new and old subdomains
- JAVASCRIPT ENDPOINT ANALYSIS**
Extracting subdomains and endpoints from JS files
- API DISCOVERY**
Finding hidden APIs, endpoints and services
- HISTORICAL URL COLLECTION**
Collecting old URLs from archives and public sources
- HTTP PROBING**
Checking alive hosts, status codes and technologies
- PORT SCANNING**
Discovering open ports and running services
- SCREENSHOT RECONNAISSANCE**
Capturing screenshots to identify interesting assets
- TECHNOLOGY FINGERPRINTING**
Detecting technologies, frameworks and servers
- ASN ENUMERATION**
Mapping subdomains to ASNs and organizations
- CLOUD ASSET DISCOVERY**
Finding cloud buckets, storage, and misconfigurations
- KUBERNETES DISCOVERY**
Finding exposed K8s dashboards and assets
- CI/CD ASSET DISCOVERY**
Finding CI/CD pipelines and related assets
- FAVICON HASH HUNTING**
Using favicon hashes to find related subdomains
- REVERSE IP LOOKUP**
Finding other domains hosted on the same IP
- WAYBACK MACHINE ANALYSIS**
Analyzing archived data for hidden endpoints
- CONTENT DISCOVERY**
Discovering hidden files, backups and directories
- VULNERABILITY SCANNING**
Scanning subdomains for known vulnerabilities
- AI-ASSISTED RECON**
Using AI tools to analyze and prioritize assets
- ATTACK SURFACE MAPPING**
Mapping all assets, services and entry points
- PARAMETER DISCOVERY**
Finding hidden parameters in URLs and requests
- HIDDEN ENDPOINT EXTRACTION**
Extracting hidden routes and internal endpoints
- GRAPHQL ENUMERATION**
Discovering GraphQL endpoints and brute forcing queries
- SECRET SCANNING**
Finding exposed keys, tokens and secrets
- SOURCE MAP ANALYSIS**
Analyzing source maps to discover hidden code and endpoints

> RECON MODE: ACTIVE
> TARGET: ODAY EVERYWHERE
> STATUS: HUNTING...



> INFORMATION IS POWER
> ENUMERATE EVERYTHING
> TRUST NOTHING

