HUNT (HUNT-A-DAY)

SCOPE

Target:

domain.tld [Main Domain]
*.domain.tld [Wildcard]

RECON 00

Subdomain Enum [https://github.com/Dheerajmadhukar/subnzZ] :

```
#assetfinder
assetfinder --subs-only $target | grep -v '\*' | rev | cut -d. -f1-3 | rev | sort -u | tee 1st-Starget-subs.txt > /dev/null

#subfinder
subfinder -d $target -silent | grep -v '\*' | rev | cut -d. -f1-3 | rev | sort -u | tee -a 1st-Starget-subs.txt > /dev/null

#amass
amass enum -norecursive -noalts -passive -d $target -config /mnt/c/Users/nix/Desktop/Amass_Config.ini | grep -v '\*' | rev | cut -d. -f1-3 | rev | sort -u | tee -a 1st-Starget-subs.txt > /dev/null

#Findomain
findomain -t $target -q | grep -v '\*' | rev | cut -d '.' -f1-3 | rev | sort -u | tee -a 1st-Starget-subs.txt > /dev/null

#Second Level - Sub Enum...
cat 1st-all-subs.txt | xargs -P 50 -I@ sh -c "assetfinder --subs-only '@' | grep -v '\*| tee -a 2nd-subs.txt > /dev/
null"
cat 1st-all-subs.txt | xargs -P 50 -I@ sh -c "subfinder -d '@' -silent | grep -v '\*\' tee -a 2nd-subs.txt > /dev/null"

#securitytrails
curl -s "https://api.securitytrails.com/v1/domain/$target/subdomains" --header "Accept: application/json" --
header "apikey: <API_KEY>" | jq -r '.subdomains' | grep -v '\[\]' sed 's/\"//g' sed -r 's/\/g' | sed -z 's/\n/.$target\
n/g' | awk '{print $1}' | sort -u > $target-sectrails_domains.txt

#CRT.SH
curl -s "https://crt.sh/?q=%25.$target&output=json" | jq -r '.[].name_value' 2>/dev/null | sed 's/\*\./g' | sort -u |
grep -o "\w+.$target" > $target-crt_domains.txt

#WAY-ARCHIVE
curl -s "http://web.archive.org/cdx/search/cdx?url=*.$target/*&output=text&fl=original&collapse=urlkey" | sed -
e 's_https*://__' -e 's/\/.*//' -e 's/:.*//' -e 's/^www\.//' |sort -u > $target-warchive_domains.txt

#DNS-BUFFER
curl -s "https://dns.bufferover.run/dns?q=.$target" | jq -r .FDNS_A[] 2>/dev/null | cut -d ',' -f2 | grep -o "\w.*$
target" | sort -u > $target-dnsbuffer_domains.txt
curl -s "https://dns.bufferover.run/dns?q=.$target" | jq -r .RDNS[] 2>/dev/null | cut -d ',' -f2 | grep -o "\w.*$target" |
sort -u >> $target-dnsbuffer_domains.txt
curl -s "https://tls.bufferover.run/dns?q=.$target" | jq -r .Results 2>/dev/null | cut -d ',' -f3 |grep -o "\w.*$target"|
sort -u >> $target-dnsbuffer_domains.txt

#Threatcrowd
curl -s "https://www.threatcrowd.org/searchApi/v2/domain/report/?domain=$target"|jq -r '.subdomains' 2>/dev/
null |grep -o "\w.*$target" > $target-threatcrowd_domains.txt

#HackerTarget
curl -s "https://api.hackertarget.com/hostsearch/?q=$target"|grep -o "\w.*$target"> $target-hackertarget_
domains.txt

#Certspotter
curl -s "https://certspotter.com/api/v0/certs?domain=$target" | jq -r '.[].dns_names[]' 2>/dev/null | grep -o "\w.*$
target" | sort -u > $target-certspotter_domains.txt

#anubisdb
curl -s "https://jldc.me/anubis/subdomains/$target" | jq -r '.' 2>/dev/null | grep -o "\w.*$target" > $target-
anubisdb_domains.txt

#virustotal
curl -s "https://www.virustotal.com/ui/domains/$target/subdomains?limit=40"|jq -r '.' 2>/dev/null |grep id|grep -
o "\w.*$target"|cut -d "" -f3|egrep -v " " > $target-virustotal_domains.txt

#alienvault
curl -s "https://otx.alienvault.com/api/v1/indicators/domain/$target/passive_dns"|jq '.passive_dns[].hostname'
2>/dev/null |grep -o "\w.*$target"|sort -u > $target-alienvault_domains.txt

#urlscan
curl -s "https://urlscan.io/api/v1/search/?q=domain:$target"|jq '.results[].page.domain' 2>/dev/null |grep -o "\
w.*$target"|sort -u > $target-urlscan_domains.txt

#threatminer
curl -s "https://api.threatminer.org/v2/domain.php?q=$target&rt=5" | jq -r '.results[]' 2>/dev/null |grep -o "\w.*$1"|
sort -u > $target-threatminer_domains.txt

#entrust
curl -s "https://ctsearch.entrust.com/api/v1/certificates?fields=subjectDN&domain=$target&includeExpired=
false&exactMatch=false&limit=5000" | jq -r '[].subjectDN' 2>/dev/null |sed 's/cn=//g'|grep -o "\w.*$target"|sort -
u > $target-entrust_domains.txt

#riddler
curl -s "https://riddler.io/search/exportcsv?q=pld:$target"| grep -o "\w.*$target"|awk -F, '{print $6}'|sort -u > $
target-riddler_domains.txt
curl -s "https://riddler.io/search/exportcsv?q=pld:$target"|cut -d ',' -f6|grep $target|sort -u >>$target-riddler_
domains.txt

#dnsdumpster
cmdtoken=$(curl -ILs https://dnsdumpster.com | grep csrftoken | cut -d " " -f2 | cut -d "=" -f2 | tr -d ";")
curl -s --header "Host:dnsdumpster.com" --referer https://dnsdumpster.com --user-agent "Mozilla/5.0 (X11;
Ubuntu; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0" --data "csrfmiddlewaretoken=$cmdtoken&
targetip=$target" --cookie "csrftoken=$cmdtoken; _ga=GA1.2.1737013576.1458811829; _gat=1" https://
dnsdumpster.com > dnsdumpster.html
cat dnsdumpster.html|grep "https://api.hackertarget.com/httpheaders"|grep -o "\w.*$target"|cut -d "/" -f7|sort -
u > $target-dnsdumper_domains.txt
rm dnsdumpster.html

#rapiddns
curl -s "https://rapiddns.io/subdomain/$target?full=1#result" | grep -oaEi "https?://[^\"\'\<]+" | grep $target | cut -
d "/" -f3 | sort -u | grep -v "\*" > $target-rapiddns_domains.txt

#choas
org=$(echo $target | cut -d. -f1)
curl -sSIL "https://chaos-data.projectdiscovery.io/index.json" | grep "URL" | sed 's/"URL": "//;s/",//' | grep "$org" |
while read host do;do curl -sSIL "$host" > /dev/null;done && for i in `ls -1 | grep .zip$`; do unzip $i > /dev/null;
done && rm -f *.zip && cat $org*.txt | grep -v "\*" > $target-choas_domains.txt

#GitHub Subdomains
github-subdomains -raw -t $git_api -d $target | grep -v "\*" > $target-github_domains.txt

sort -u *_domains.txt -o subdomains.txt
cat subdomains.txt | rev | cut -d . -f 1-3 | rev | sort -u | grep -v "$[blank][^$]" > root_subdomains.txt

cat top-subs-100000.txt | cut -d'.' -f2| grep -v "\# Generated\|\*" > /tmp/top-subs.txt
DNScewl --tL root_subdomains.txt -p /tmp/top-subs.txt --level=0 --subs --no-color > subs-prepend-list.txt

bash puredns resolve subs-prepend-list.txt -r resolvers.txt -w premut-subs_domains.txt
```

RECON 01

Waybackurls Leaks [https://github.com/Dheerajmadhukar/back-me-up] :

```
cat subs.txt | xargs -P 800 -I X bash -c "echo 'X' | waybackurls | tee -a waybackurls.txt > /dev/null"
cat $target | gauplus --random-agent --subs -t 5000 | anew -q waybackurls.txt
cat waybackurls.txt | cut -d'?' -f1 | cut -d'=' -f1 > filtered.txt

grep -iaE "([^.]+)\.sig(s|[^.]+)\.xip\.[0-9]+$|([^.]+)\.xip[0-9]+$|([^.]+)\.xipls-z[A-Z]{0-9]+$|([^.]+)\.xip\.[a-z]A-Z]{0-
9]+$|([^.]+)\.ras(1|[^.]+)\.tar$|([^.]+)\.tar\.gz$|([^.]+)\.tgz$|([^.]+)\.sql$|([^.]+)\.db$|([^.]+)\.sqlite$|([^.]+)\.gwg$\.
tst$|([^.]+)\.mysql\.txt$|([^.]+)\.gz$|([^.]+)\.config$|([^.]+)\.log$|([^.]+)\.hak$|([^.]+)\.backup$|([^.]+)\.hak$|([^.]+)\.
crt$|([^.]+)\.cdat$|([^.]+)\.eml$|([^.]+)\.java$|([^.]+)\.lst$|([^.]+)\.key$|([^.]+)\.passwd$|([^.]+)\.p$|([^.]+)\.pwd$|([^.]+)\.
mysql-connect$|([^.]+)\.jar$|([^.]+)\.cfg$|([^.]+)\.dir$|([^.]+)\.orig$|([^.]+)\.bz2$|([^.]+)\.old$|([^.]+)\.vbs$|([^.]+)\.
img$|([^.]+)\.inf$|([^.]+)\.sh$|([^.]+)\.py$|([^.]+)\.vbproj$|([^.]+)\.mysql-connect$|([^.]+)\.war$|([^.]+)\.gql$|([^.]+)\.
psql$|([^.]+)\.cpt$|([^.]+)\.vhd$|([^.]+)\.webinf$|([^.]+)\.inf$|([^.]+)\.cgi$|([^.]+)\.temp$|([^.]+)\.inc$|([^.]+)\.
webproj$|([^.]+)\.xsql$|([^.]+)\.raw$|([^.]+)\.lnc$|([^.]+)\.lck$|([^.]+)\.nzs$|([^.]+)\.rc$|([^.]+)\.html\.cgs$|([^.]+)\.gz$|([^.]+)\.
env$|([^.]+)\.yml$" filtered.txt | sort -u | httpx -silent -follow-redirects -threads 800 -mc 200 > leaks.txt
```

RECON 02

Waybackurls Filtration :

```
grep -vE "robots.txt$|robots.txt\/$|.gif|.jpg|.jpeg|.css|.tiff|.ico|.png|.svg|.ttf|.woff|.woff2|.eot|.pdf|" waybackurls.txt |
sort -u > clean_wbu.txt

#SSRF/OpenRedirect/LFI/RFI/RCE/
cat clean_wbu.txt| grep -E '\/.*=(\/\/|%2f%2f|\.\w+\/|\w+(%3A|:)(\/\/|%2F)|%2F[\.\w]+\.\w{2,4}[^\w])'>waybackdata/multi-
checks.txt

#EXTRAS
cat clean_wbu.txt | unfurl --unique keys >waybackdata/keys.txt
cat clean_wbu.txt | grep -P "\w+\.js(\?|$)" | sort -u >waybackdata/jsurls.txt
cat clean_wbu.txt | grep -P "\w+\.php(\?|$)" | sort -u >waybackdata/phpurls.txt
cat clean_wbu.txt | grep -P "\w+\.aspx(\?|$)" | sort -u >waybackdata/aspxurls.txt
cat clean_wbu.txt | grep -P "\w+\.jsp(\?|$)" | sort -u >waybackdata/jspurls.txt

#Cross-Site Scripting (XSS)

grep -iaE "\?q=|\?s=|\?search=|\?id=|\?lang=|\?keyword=|\?query=|\?page=|?keywords=|\?year=|\?view=|\?
email=|\?type=|\?name=|\?p=|\?month=|\?image=|\?list_type=|\?url=|\?terms=|\?categoryid=|\?key=|\?fl=|\?
begindate=|\?enddate=" clean_wbu.txt | tee xss.txt

#SQL Injection Parameters

grep -iaE "\?id=|\?page=|\?dir=|\?search=|\?category=|\?file=|\?class=|\?url=|\?news=|\?item=|\?menu=|\?lang=|\?
name=|\?ref=|\?title=|\?view=|\?topic=|\?thread=|\?type=|\?date=|\?form=|\?join=|\?main=|\?nav=|\?region=|
clean_wbu.txt | tee sqli.txt

#Local File Inclusion (LFI) Parameters

grep -iaE "\?cat=|\?dir=|\?action=|\?board=|\?date=|\?detail=|\?file=|\?download=|\?path=|\?folder=|\?prefix=|\?
include=|\?page=|\?inc=|\?locate=|\?show=|\?doc=|\?site=|\?type=|\?view=|\?content=|\?document=|\?layout=|\?
mod=|\?conf=" clean_wbu.txt | tee lfi.txt

#Open Redirect Parameters

grep -iaE "\?next=|\?url=|\?target=|\?rurl=|\?dest=|\?destination=|\?redir=|\?redirect_uri=|\?redirect_url=|\?
redirect=|redirect|/cgi-bin/redirect.cgi|\?out|//out|\?\?view=|/login\?to=|\?image_url=|\?go=|\?return=|\?
returnTo=|\?return_to=|\?checkout_url=|\?continue=|\?return_path=" clean_wbu.txt | tee open_redirect.txt

#Remote Code Execution (RCE) Parameters [GET Based]

grep -iaE "\?cmd=|\?exec=|\?command=|\?execute=|\?ping=|\?query=|\?jump=|\?code=|\?req=|\?do=|\?func=|\?
arg=|\?option=|\?load=|\?process=|\?step=|\?read=|\?function=|\?req=|\?feature=|\?exe=|\?module=|\?payload=|\?
run=|\?print=" clean_wbu.txt | tee rce.txt

#Server-Side Request Forgery (SSRF) Parameters

grep -iaE "\?dest=|\?redirect=|\?uri=|\?path=|\?continue=|\?url=|\?window=|\?next=|\?data=|\?reference=|\?
site=|\?html=|\?val=|\?validate=|\?domain=|\?callback=|\?return=|\?page=|\?feed=|\?host=|\?port=|\?to=|\?out=|\?
view=|\?dir=" clean_wbu.txt | tee ssrf.txt
```

RECON 03

HTTP/2 Request Smuggling : [https://github.com/BishopFox/h2csmuggler]

```
cat waybackurls.txt | urldedupe -m "x.qs,ne" | unfurl -u format %s://%d%p | awk -F "/" '{print $1 "#" $3 "/" $4}' |
grep "^https:\/\/" --color=no | sort -u > h2c_urls.txt

python3 h2csmuggler.py --scan-list h2c_urls.txt --test --threads 800 2>/dev/null | grep " Success!"|tee h2c-
success.txt>/dev/null
```

RECON 04

HTTP Request Smuggling : [https://github.com/defparam/smuggler]

```
cat h2c_urls.txt | xargs -P 200 -I X bash -c "python3 smuggler.py -u 'X' -q --no-color -t 10" | tee HTTP-
smuggling-payloads.txt

cat h2c_urls.txt | xargs -P 200 -I X bash -c "python3 smuggler.py -u 'X' -m 'GET' -q --no-color -t 10" | tee -a
HTTP-smuggling-payloads.txt

cat h2c_urls.txt | xargs -P 200 -I X bash -c "python3 smuggler.py -u 'X' -m 'DELETE' -q --no-color -t 10" | tee -a
HTTP-smuggling-payloads.txt

cat h2c_urls.txt | xargs -P 200 -I X bash -c "python3 smuggler.py -u 'X' -m 'PUT' -q --no-color -t 10" | tee -a
HTTP-smuggling-payloads.txt
```

RECON 05

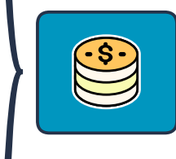
WAF/CDN Bypass : [https://github.com/Dheerajmadhukar/Lilly]

```
cat alive.txt | xargs -I %% bash -c 'echo "%%/favicon.ico" > favicon_targets.txt

cat favicon_targets.txt | xargs -I %% bash -c 'curl %% -k -s -o /dev/null -w "%% "%{http_code}\n" -X GET | grep
200" > favicon_urls.txt

cat favicon_urls.txt | awk '{print $1}' xargs -I %% bash -c "echo %% ; curl -s -L -k %% | python3 -c 'import mmh3,
sys,codecs; print(mmh3.hash(codecs.encode(sys.stdin.buffer.read(),\"base64\")))'"> hash.txt

cat hash.txt | awk 'NR%2{printf "%s ",$0;next;}1' | awk '{print $2}' | grep -v "^0$" | tee favicon_hash.txt

for hashh in $(cat favicon_hash.txt);do shodan search http.favicon.hash:$hashh --fields ip_str,port --
separator " " | grep -v 'Error' | awk '{print $1 ":" $2}' > favicon_ips.txt;done

cat favicon_ips.txt | grep -v ":\/" | httpx -threads 500 -silent | interlace -threads 100 -c "echo _target_ ; curl --
insecure -v _target_ 2>&1 | awk 'BEGIN{ cert=0 } /^\* SSL connection/{ cert=1 } /^\*/{ if (cert) print }'" --silent |
grep "https:\/\/\|CN=\|issuer: " | tee all_certs.txt
```

RECON 06

Template based Scanning with Nuclei : [https://github.com/projectdiscovery/nuclei]

```
HEADER="User-Agent: <Custom-Agent>"

cat alive.txt | nuclei -silent -H "$HEADER" -t technologies -retries 1 -timeout 3 -c 100 -rate-limit 100 -o nuclei_
output/technologies.txt

cat alive.txt | nuclei -silent -H "$HEADER" -t exposed-tokens -retries 1 -timeout 3 -c 100 -rate-limit 100 -o
nuclei_output/tokens.json

cat alive.txt | nuclei -silent -H "$HEADER" -t exposures -retries 1 -timeout 3 -c 100 -rate-limit 100 -o nuclei_
output/exposures.json

cat alive.txt | nuclei -silent -H "$HEADER" -t cves -retries 1 -timeout 3 -c 100 -rate-limit 100 -o nuclei_output/
cves.json

cat alive.txt | nuclei -silent -H "$HEADER" -t default-logins -retries 1 -timeout 3 -c 100 -rate-limit 100 -o nuclei_
output/default_creds.json

cat alive.txt | nuclei -silent -H "$HEADER" -t dns -retries 1 -timeout 3 -c 100 -rate-limit 100 -o nuclei_output/dns.
json

cat alive.txt | nuclei -silent -H "$HEADER" -t exposed-panels -retries 1 -timeout 3 -c 100 -rate-limit 100 -o
nuclei_output/panels.json

cat alive.txt | nuclei -silent -H "$HEADER" -t misconfiguration -retries 1 -timeout 3 -c 100 -rate-limit 100 -o
nuclei_output/misconfigurations.json

cat alive.txt | nuclei -silent -H "$HEADER" -t vulnerabilities -retries 1 -timeout 3 -c 100 -rate-limit 100 -o nuclei_
output/vulnerabilities.json

cat alive.txt | nuclei -silent -H "$HEADER" -t takeovers -retries 1 -timeout 3 -c 100 -rate-limit 100 -o nuclei_
output/takeovers.json

cat alive.txt | nuclei -silent -H "$HEADER" -t miscellaneous -retries 1 -timeout 3 -c 100 -rate-limit 100 -o nuclei_
output/miscellaneous.json
```



If you LIKE it.

https://twitter.com/Dheerajmadhukar

https://www.linkedin.com/in/dheerajtechnolegends/

https://medium.com/@dheerajkmadhukar

https://www.instagram.com/me_dheeraj/