HACKTHEBOX

INFORMATION GATHERING - WEB EDITION

CHEAT SHEET

WHOIS

Command	Description
`export TARGET="domain.tld"`	Assign target to an environment variable.
`whois $TARGET`	WHOIS lookup for the target.

DNS Enumeration

Command	Description
`nslookup $TARGET`	Identify the `A` record for the target domain.
`nslookup -query=A $TARGET`	Identify the `A` record for the target domain.
`dig $TARGET @<nameserver/IP>`	Identify the `A` record for the target domain.
`dig a $TARGET @<nameserver/IP>`	Identify the `A` record for the target domain.
`nslookup -query=PTR <IP>`	Identify the `PTR` record for the target IP address.
`dig -x <IP> @<nameserver/IP>`	Identify the `PTR` record for the target IP address.
`nslookup -query=ANY $TARGET`	Identify `ANY` records for the target domain.
`dig any $TARGET @<nameserver/IP>`	Identify `ANY` records for the target domain.

Command	Description
`nslookup -query=TXT $TARGET`	Identify the `TXT` records for the target domain.
`dig txt $TARGET @<nameserver/IP>`	Identify the `TXT` records for the target domain.
`nslookup -query=MX $TARGET`	Identify the `MX` records for the target domain.
`dig mx $TARGET @<nameserver/IP>`	Identify the `MX` records for the target domain.

Passive Subdomain Enumeration

<table>
<tr><th>Resource/Command</th><th>Description</th></tr>
<tr><td><code>VirusTotal</code></td><td>https://www.virustotal.com/gui/home/url</td></tr>
<tr><td><code>Censys</code></td><td>https://censys.io/</td></tr>
<tr><td><code>Crt.sh</code></td><td>https://crt.sh/</td></tr>
<tr><td><code>curl -s https://sonar.omnisint.io/subdomains/{domain} | jq -r '.[]' | sort -u</code></td><td>All subdomains for a given domain.</td></tr>
<tr><td><code>curl -s https://sonar.omnisint.io/tlds/{domain} | jq -r '.[]' | sort -u</code></td><td>All TLDs found for a given domain.</td></tr>
<tr><td><code>curl -s https://sonar.omnisint.io/all/{domain} | jq -r '.[]' | sort -u</code></td><td>All results across all TLDs for a given domain.</td></tr>
<tr><td><code>curl -s https://sonar.omnisint.io/reverse/{ip} | jq -r '.[]' | sort -u</code></td><td>Reverse DNS lookup on IP address.</td></tr>
<tr><td><code>curl -s https://sonar.omnisint.io/reverse/{ip}/{mask} | jq -r '.[]' | sort -u</code></td><td>Reverse DNS lookup of a CIDR range.</td></tr>
<tr><td><code>curl -s "https://crt.sh/?q=${TARGET}&output=json" | jq -r '.[] | "\(.name_value)\n\(.common_name)"' | sort -u</code></td><td>Certificate Transparency.</td></tr>
<tr><td><code>cat sources.txt | while read source; do theHarvester -d "${TARGET}" -b $source -f "${source}-${TARGET}";done</code></td><td>Searching for subdomains and other information on the sources provided in the source.txt list.</td></tr>
</table>

Sources.txt

```
baidu
bufferoverun
crtsh
hackertarget
otx
projecdiscovery
rapiddns
sublist3r
threatcrowd
trello
urlscan
vhost
virustotal
zoomeye
```

Passive Infrastructure Identification

Resource/Command	Description
`Netcraft`	https://www.netcraft.com/
`WayBackMachine`	http://web.archive.org/
`WayBackURLs`	https://github.com/tomnomnom/waybackurls
`waybackurls -dates https://$TARGET > waybackurls.txt`	Crawling URLs from a domain with the date it was obtained.

Active Infrastructure Identification

Resource/Command	Description
`curl -I "http://${TARGET}"`	Display HTTP headers of the target webserver.
`whatweb -a https://www.facebook.com -v`	Technology identification.
`Wappalyzer`	https://www.wappalyzer.com/
`wafw00f -v https://$TARGET`	WAF Fingerprinting.
`Aquatone`	https://github.com/michenriksen/aquatone

Resource/Command	Description
`cat subdomain.list | aquatone -out ./aquatone -screenshot-timeout 1000`	Makes screenshots of all subdomains in the subdomain.list.

Active Subdomain Enumeration

Resource/Command	Description
`HackerTarget`	https://hackertarget.com/zone-transfer/
`SecLists`	https://github.com/danielmiessler/SecLists
`nslookup -type=any -query=AXFR $TARGET nameserver.target.domain`	Zone Transfer using Nslookup against the target domain and its nameserver.
`gobuster dns -q -r "${NS}" -d "${TARGET}" -w "${WORDLIST}" -p ./patterns.txt -o "gobuster_${TARGET}.txt"`	Bruteforcing subdomains.

Virtual Hosts

Resource/Command	Description
`curl -s http://192.168.10.10 -H "Host: randomtarget.com"`	Changing the HOST HTTP header to request a specific domain.
`cat ./vhosts.list | while read vhost;do echo "\n********\nFUZZING: ${vhost}\n********";curl -s -I http://<IP address> -H "HOST: ${vhost}.target.domain" | grep "Content-Length: ";done`	Bruteforcing for possible virtual hosts on the target domain.
`ffuf -w ./vhosts -u http://<IP address> -H "HOST: FUZZ.target.domain" -fs 612`	Bruteforcing for possible virtual hosts on the target domain using `ffuf`.

Crawling

Resource/Command	Description
`ZAP`	https://www.zaproxy.org/
`ffuf -recursion -recursion-depth 1 -u http://192.168.10.10/FUZZ -w /opt/useful/SecLists/Discovery/Web-Content/raft-small-directories-lowercase.txt`	Discovering files and folders that cannot be spotted by browsing the website.
`ffuf -w ./folders.txt:FOLDERS,./wordlist.txt:WORDLIST,./extensions.txt:EXTENSIONS -u http://www.target.domain/FOLDERS/WORDLISTEXTENSIONS`	Mutated bruteforcing against the target web server.