**--- Red Team Recon Technique : Link**

**--Key Techniques--**
* Ip address
* DNS info
* OSINT
* Nerwork Info

**Commands**

host <website>
nslookup <website>
traceroute <website>
dnsrecon -d <website>
wafw00f <website>
dig <website>
dig <website> NS
dig <website> ANY
whois <website>
whatweb <website>
theHarvester -d ABC -b google,linkedin,bing
theHarvester -d ABC -b google,linkedin,bing,twitter,yahoo,sublist3r
sublist3r -d <website>
site:*.bbc.com -site:www.bbc.com
dnsrecon -d <website> -t axfr
fierce --domain <website>
knockpy <website>
knockpy <website> -w /usr/share/seclists/Discovery/DNS/shubs-stackoverflow.txt
nikto -h <website>
recon-ng

**Links**

https://github.com/ajinabraham/CMSScan
https://github.com/1N3/Sn1per
https://github.com/owasp-amass/amass
https://dnsdumpster.com/
https://sitereport.netcraft.com/
https://chrome.google.com/webstore/detail/wappalyzer-technology-pro/gppongmhjkpfnbhagpmjfkannfbllamg
https://addons.mozilla.org/en-US/firefox/addon/wappalyzer/
https://chrome.google.com/webstore/detail/builtwith-technology-prof/dapjbgnjinbpoindlpdmhochffioedbn
https://addons.mozilla.org/en-US/firefox/addon/builtwith/
https://offsec.tools/
https://map.malfrats.industries/
https://osintframework.com/

**1. Waybackmachine**: We can use this tool to actually look into some sensitive files which might exist sometimes before.

**2. Knockpy**: We have this tool to actually start enumerating subdomains with different API keys.

**3. Sublist3r:** This is tool we use to enumerate subdomains again because this tools try to find subdomains using OSINT.

**4. DnsDumpster:** is a free domain research online tool that can discover hosts related to a domain. It helps to find out subdomains, HTTP headers, banner grabbing, MX Records, DNS Servers , TXT Records etc. It helps a lot in gathering information about the target.

**5. Netcraft:** This a website which monitor uptime of every website available online. Netcraft gives you some more information about the websites like NetBlocks, OS name, Site reports which includes site title, site rank, site description and many more things. Netcraft is also a good online tool for recon.

**6. Crt.sh:** This is a website which has certificates transparency logs of every website. It will give you some details about certificate issuer name, and some other useful stuff.

**7. Yougetsignal:** This is kind of network tools website which can sometimes help you to check the reverse IP domain lookup check

**8. IP Range Finder:** This can help you to have a clear image of from where to where the IP address of particular domain covers. We can do this with the help of https://bgp.he.net/

**9. Whois:** Whois records are used to gather some useful kind of information.

**10. Censys.io :** It's a public search engine which you can use to find some IP or subdomains which are available on internet which can have critical vulnerabilities.

**11. Domain Profiler:** The best thing about domain profiler is that, that it will give you the details of Email hosting, DNS hosting and Domain registrar of the target website.

**12. Photon:** This is a tool which can help you gather many critical info like some key text files, Secret Keys and more thing.

**13. VirusTotal:** We can use this website to find some external links of our target. 14. Linkfinder: to discover endpoints and their parameters in JavaScript files.

**15. Retire.Js :** This is a burp suite extension which will automatically scan javascript link you find from linkfinder to find vulnerability in them.

**16. Dig to Check CNAME:** You can use this to verify that is subdomain is ready to takeover

**17. Arjun:** This is used to find hidden parameters for your target.

apt-get install knockpy > knockpy <website>
apt-get install sublist3r > sublist3r -d <website> -o target.txt > cat target.txt | grep admin
apt-get install photon > photon -u <website> --keys --dns
apt-get install arjun > arjun -u <website>

https://dnsdumpster.com/
https://osint.sh/subdomain/
https://pentest-tools.com/information-gathering/find-subdomains-of-domain
https://subdomainfinder.c99.nl/
https://hackertarget.com/find-dns-host-records/

https://mxtoolbox.com/ReverseLookup.aspx
https://hackertarget.com/reverse-ip-lookup/
https://www.yougetsignal.com/tools/web-sites-on-web-server/
https://reverseip.domaintools.com/
https://www.nslookup.io/reverse-ip-lookup/
https://viewdns.info/reverseip/
https://dnschecker.org/reverse-dns.php
https://bgp.he.net/
https://search.censys.io/
https://github.com/jpf/domain-profiler
https://github.com/GerbenJavado/LinkFinder
https://toolbox.googleapps.com/apps/dig/