FOOTPRINTING:

WGET MIRRORING:

- wget –help
- wget google.com
- wget --morror --convert-link --adjust-extension --no-parent --page-requisites --execute robots=off url
- wget -mkEpnp url

HTTrack Mirroring:

- Httrack

Whois Lookup:

- Web search: [https://lookup.icann.org/lookup]

DNS DUMPSTER:

- Web search: [https://dnsdumpster.com]

TRACEROUTE ANALYSIS:

- Win: tracert /?
- tracert google.com
- tracert -h 5 google.com [-h hops I put 5]
- web search: path analyzer pro software for windows

MALTEGO:

OSINT FRAMEWORK:

THE HARVESTER:

- theHarvester –help
- theHarvester -d google.com -b google,bing
- theHarvester -d google.com -b google -l 50
- theHarvester -d facebook.com -b dnsdumpster -100 -n
- is binary version is not stable so u can dwnld 2.7 stable release [https://github.com/laramies/theHarvester/releases]
- dwnld zip file > extract > ls > chmod +x theHarvester.py > python theHarvester.py

- python theHarvester.py -d facebook.com -b all -l 300 -h facebook.html

WhatWeb:

- Web search https://github.com/urbanadventurer/WhatWeb
- Git clone it
- ls,cd WhatWeb
- whatweb
- whatweb -h
- whatweb google.com
- whatweb -v google.com
- whatweb -a 3 -v google.com
- whatweb -v -a 3 google.com –log-verbose=whatweb.txt

WAPPALYZER (EXTENSION):

SUBLIST3R:

- Clone github
- Python3 sublist3r.py -d google.com
- Python3 sublist3r.py -d google.com -o output.txt
- Python3 sublist3r.py -d google.com -v -b -t 5

FIND SUBDOMAINS:

- Web search pentest-tools.com
- Web search virustotal.com

NETDISCOVER:

- It is a network discovering tools
- netdiscover

NIRSOFT:

- Web search https://www.nirsoft.net/countryip/

GOOGLE DORKS:

1. inurl: php [only php related url show]
2. inurl: php?id= [sql inj related web]
3. allinurl: www.google.com [wo websites show hoga jismain www.google.com hoga must]

4. intitle: facebook login [website ka title hoga facebook login related]
5. site: google.com [all google sites show]
6. ethical hacking filetype:pdf [file type]
7. intext: ethical hacking [content a ethical hacking related sites show]
8. link: google.com [indirectly link on google.com like us web site per google.com ka link rahega]
9. define: hacking [define hacking definition]
10. info: google.com [origin page/main index]
11. related: cyber security [cs related]
12. indexof: ethical hacking [directory listening]

ex:- intitle: facebook filetype: pdf [title facebook related && filetype pdf]

SCANNING:

ANGRY IP SCANNER:

- web search win: https://www.github.com/angryip/ipscan

NMAP:

- man nmap
- nmap -h
- nmap 192.168.75.133
- nmap -v 192.168.75.133
- nmap -p22 192.168.75.133
- nmap -p0-1023 192.168.75.133
- nmap -sV 192.168.75.133
- nmap 192.168.75.133 > /root/Desktop/nmap.txt
- nmap -sV 192.168.75.133 >> /root/Desktop/nmap.txt
- nmap -oG - -vv -sV 192.168.75.133 > /root/Desktop/nmap.txt [-o output, -G graphical]
- nmap -Pn 192.168.75.133 [-Pn I know machine alive so I don't want to ping because many times losses nmap 1st discovered target alive yes/no then scan ports is it by default so I know target is alive and I don't want check victim is alive yes/no only I want scan port nmap run fast optimized]
- namp -F 192.168.75.133 [simple popular ports check]
- nmap 192.168.75.0-255
- nmap -vv 192.168.75.0/24

- nmap -f 192.168.75.133 [packet fragement small part so firewall ids ips not drop]
- nmap –mtu 16 192.168.75.133 [maximum transmission unit 16 bytes bypass ids]
- nmap -D RND:16 192.168.75.133 [random src ip se scan]
- nmap -S 192.168.75.100 -e eth0 192.168.75.133 [I put my new src ip fake]
- nmap -sI 192.168.75.100 -e eth0 192.168.75.133 [zombie scan -sI zombie machine ip need which I spoof and machine need alive]
- nmap –source-port 65 192.168.75.133 [src port chng]
- nmap –spoof-mac 0 192.168.75.133 [mac spoof]
- nmap -sT -PN –spoof-mac 0 192.168.75.133 [mac spoof and o/p]
- nmap --data-length 40 192.168.75.133 [data small part]
- nmap -sT 192.168.75.133
- nmap -sS 192.168.75.133
- nmap -sA 192.168.75.133
- nmap -sU 192.168.75.133
- nmap -sN 192.168.75.133
- nmap -sF 192.168.75.133
- nmap -sX 192.168.75.133

PORT SCANNING WITH HPING3:

- man hping3
- hping3 --scan 0-1023 192.168.75.133
- hping3 --scan 0-1023 -s 192.168.75.133 [syn scan]
- hping3 --scan 0-1023 -F 192.168.75.133
- hping3 --scan 0-1023 -R 192.168.75.133 [rst reset scan]
- hping3 --scan 0-1023 -U 192.168.75.133
- hping3 --scan 0-1023 -FUP 192.168.75.133
- hping3 --traceroute 192.168.75.133
- hping3 --tr-stop 192.168.75.133
- hping3 --scan 0-1023,2000-3000 192.168.75.133
- hping3 --scan 80 -FUP 192.168.75.133

PORT SCANNING WITH PENTEST-TOOLS:

- web: https://pentest-tools.com

COLASOFT PACKET BUILDER:

- web: https://colasoft.com/packet_builder/
- it is a software for windows
- custom packet builder

BANNER GRABBING WITH ID SERVE:

Web : windows: https://www.grc.com/id/idserve.htm

BANNER GRABBING WITH NETCRAFT:

Web : https://sitereport.netcraft.com

Web: (browser extension)netcraft anti-phishing extension by netcraft ltd

BANNER GRABBING WITH NETCAT:

- nc
- q
- man nc
- nc -nv 192.168.75.133 80
- HTTP/1.1 200
- nc -nv 192.168.75.133 22
- nc -nv 192.168.75.133 21

NESSUS VULNERABILITY SCANNER:

Web: https://www.tenable.com/products/nessus

Dwnld and login 1st

- dpkg -i Nessus-8.9.0-debian6_amd64.deb
- service nessusd start
- web: https://localhost:8834
- advanced
- accept the risk and continue
- default value
- login
- email activation key
- login
- 192.168.1.0/24

NMAP SCRIPTING ENGINE:

- ls -l /usr/share/nmap/scripts
- nmap -h
- ls -l /usr/share/nmap/scripts | grep ssh [filter only ssh file]
- nano /usr/share/nmap/scripts/ssh-brute.nse
- nmap -sC -p22 192.168.75.133 [default scripts run]
- nmap --script =ssh-brute.nse 192.168.75.133

NIKTO WEB VULNERABILITY SCANNER:

- nikto –help
- nikto -h testphp.vulnweb.com
- nikto -h testphp.vulnweb.com -o nikto_scan -F txt -p 80

OPENVAS:

Web: https://www.openvas.org

apt-get install openvas

go to kali logo search: openvas initial setup (run)

openvas-start

web: https://127.0.0.1:9392

terminal: openvasmd –create-user (username put any) testuser

auto generate passwd copy it and login

WP SCAN WORDPRESS:

- wpscan –help
- wpscan –url http://192.168.1.7/wordpress
- wpscan –url http://192.168.1.7/wordpress --enumerate u
- wpscan –url http://192.168.1.7/wordpress -U admin -P /root/Desktop/wordlist.txt
- wpscan –url http://192.168.1.7/wordpress --enumerate u -o /root/Desktop/wp_output.txt
- wpscan –url http://192.168.1.7/wordpress --enumerate u -o /root/Desktop/wp_output -f json

NETWORK TOPOLOGY MAPPER:

Web: https://www.solarwinds.com/network-toppology-mapper

Win dwnlds

SPICEWORKS NETWORK MAPPER:

Web: https://www.spiceworks.com/free-network-mapping-software

LAN STATE PRO:

Web: https://www.10-strike.com/lanstate/downlad.shtml

ENUMERATION:

WORKING WITH NETBIOS AND ENUMERATION:

- Cmd: nbtstat
- Cmd: nbtstat -A 192.168.1.6
- Now use Terminal
- Smbclient
- Smbclient -L 192.168.1.6 [if smb login is on and doesnot set passwd then you can login and get info]
- nmap -p445 -A 192.168.1.6 [smb enumeration]
- ls /usr/share/nmap/scripts | grep smb
- nmap --script=smb-enum-users 192.168.1.6
- nmap --script=smb-enum-shares 192.168.1.6

SMTP ENUMERATION:

- telnet 192.168.75.133 25 [25 smtp default port]
- now I want to main so now follow my cmmnd
- MAIL FROM:anashbhawnani@gmail.com
- VRFY ansh(user name)
- VRFY root
- VRFY bin [status code 550 then you understand it is not exist]
- VRFY daemon [if status code 252 then you understand that this user name is exist]
- Now you can try bruteforced this account because now you know username
- RCPT TO:root(user name mail received wala)

METASPLOIT USE:

- Msfconsole
- Search smtp
- Use auxiliary/scanner/smtp/smtp_enum
- Show options
- Set RHOST 192.168.75.133
- Exploit

DNS ZONE TRANSFER USING HOST COMMAND:

- host -t ns zonetransfer.me [-t query is ns then domain is zonetransfer.me]
- host -h
- host -l zonetransfer.me nsztm1.digi.ninja. [domain,nameserver example nsztm1.digi.ninja]

NSLOOKUP TOOLS:

- man nslookup
- nslookup google.com [you get default A record]
- nslookup [now,you get nslookup prompt.now I use it]
- set type=a [record type you want]
- google.com [domain]
- set type=ns
- google.com
- set type=cname
- google.com
- set type=mx
- google.com

DNS ZONE TRANSFER USING NSLOOKUP:

WINDOWS CMD:

- nslookup [you get a prompt]
- server nsztm1.digi.ninja. [set a name server]
- set type=any
- ls -d zonetransfer.me [-d for domain I put a sample]

DIG COMMAND ON LINUX:

- dig -h
- dig google.com
- dig google.com -t ns [-t type record]
- dig google.com -t ns +short
- dig google.com -t mx
- dig google.com -t mx +short
- dig google.com -t aaaa [ipv6 record]
- (dig is mainly use zone transfer a)

DNS ZONE TRANSFER USING DIG COMMAND:

- dig axfr @nsztm1.digi.ninja. zonetransfer.me [I need full record so use axfr,then put mt ns @example,then domain (test)]

PORT SCANNING: MASSCAN(BONUS PART):

- sudo masscan-- version
- sudo masscan -p0-1023 10.0.0.0/20 --rate 15000 [this is a random ip range]
- sudo masscan -p0-1023 192.168.164.135 --rate 15000 [disclamer rate value <=15000 use]
- man masscan
- sudo masscan -p0-1023 192.168.164.135 --rate 15000 -v
- sudo masscan -p0-1023 192.168.164.135 --rate 15000 -oB masscan.binary
- {-oB B for binar,X for xml, L for list,G for grepable,J for json}
- Sudo masscan --readscan masscan.binary
- Sudo masscan --readscan masscan.binary -oX masscan.xml
- Sudo masscan --readscan masscan.binary -oG masscan.grepable
- Cat masscan.grepable
- grep /open/ masscan.grepable [filter only open ports show]
- sudo masscan -p0-1023 10.10.54.61 -v -i tun1 [openvpn THM ip scan ports]

NMAP MORE CMMNDS:

Nmap -Pn -F IP [-F is for FAST SCAN DEFAULT 100 PORTS}

Nmap -Pn -F -sV -O IP [-O FOR OS]

Nmap -Pn -F -T4 -sV -O -sC IP

Nmap -sn 10.10.10.0/24 [no port scan only show up hosts]

Cd /usr/share/nmap/scripts

Ls -la /usr/share/nmap/scripts | grep smb

Ls -la /usr/share/nmap/scripts | grep -e “mongodb”

Nmap -sS -sV –script=mongodb-info -p- -T4 IP