Information Gathering

- **httprint :**

- **whatweb :**
  command line tool , use -v option for a clean output

- **Sherlock :**
  Takes a username and searches for it in many databases

- **Badkarma :**
  Network reconnaissance toolkit

- **Wayback machine :**
  Gets older version of websites

- **Whois :**
  Gets info about domain (database about domain , who bought , when , why , ips , ISP , DNS , ..)
  whois.domaintools.com

- **netcraft :**
  shows webserver and history os information ,server version , uptime stats , ip address owner , host provider.

- **whois :**
  WHOIS normally runs on TCP port 43.
  You can perform *Whois* queries by using the whois *nix command or by installing the Sysinternal Whois utility.
  whois.domaintools.com

- **Maltigo :**

- **Amass :**
  amass enum -brute -d target.com
  https://github.com/OWASP/Amass

- **Google Dorks:**
  https://www.exploit-db.com/google-hacking-database
  https://github.com/BullsEye0/google_dork_list
  https://support.google.com/websearch/answer/2466433?hl=es&rd=1
  https://antoniogonzalezm.es/tag/intitleindex-of-microsoft-iis-server-at/

- **netcat**
  nc 192.168.102.136 80 (check server field)
  HEAD / HTTP/1.0
  press enter two times, search for server headers, X-Powered-By

SubDomain Enumeration :

- **sublist3r**
- **net craft**

- Netcraft : https://searchdns.netcraft.com/

- Google : http://www.googleguide.com/advanced_operators_reference.html
  site:.microsoft.com
  site:.microsoft.com **-inurl:www**. **--> include in the results**
  site:.microsoft.com **-site:www.microsoft.com** **--> remove from results**

- Crawling/Bruteforce

- Some Tools
  dnsrecon: https://github.com/darkoperator/dnsrecon
  subbrute: https://github.com/TheRook/subbrute
  fierce: https://github.com/davidpepper/fierce-domain-scanner
  Nmap: http://nmap.org/book/man-host-discovery.html
  dnsenum: https://code.google.com/archive/p/dnsenum/downloads
  knock: https://github.com/guelfoweb/knock
  theHarvester: https://github.com/laramies/theHarvester --> can get from linkedin

Webserver Fingerprinting :

- wappalyzer
- netcraft
- netcat

Look for the following:
Serverversion
Uptimestats
IP address owner
Host provider
Webserverversion
Installedmodules
Web enabled devices (routers, cable modems, etc.)

The most important feature of these tools is that they do not solely rely on the service banner.
They are capable of fingerprinting the web server version even when the banner or the HTTP response header have been manually obfuscated / altered using security modules (mod_security...).

look at cookies
PHP = PHPSESSID=XXXXX
.NET = ASPSSESSIONIDYYYY=XXXXX
JAVA = JSESSION=XXXXX

URL rewriting is done on Apache with the **mod_rewrite** module or **.htaccess**.
it is better to use the url that deoesnt need rewriting

ISP's, hosting and IP addresses.

(u can jump to step 5)
1 - nslookup <subdomain>.com
2- nslookup www.<subdomain>.com
3- save those ip's
4- use tools to uncover the ISPs, netblock (CIDR):
arin.net

whois.domaintools.com
ripe.net

5- netcraft does all the above
https://sitereport.netcraft.com/
https://sitereport.netcraft.com/?url=http://www.google.com

Dns Enumeration :

Query for some of the IP addresses that we found:

- **nslookup :**
  nslookup google.com
  nslookup -type=PTR <ip>
  nslookup -querytype=ANY google.com

- **recon-ng** :
  module load hackertarget
  options set SOURCE <domain>
  run

- **shodan :**
  https://github.com/jakejarvis/awesome-shodan-queries

- **Domaintools :**

- **Dig (for zone transfers):**
  dig @nameserver axfr mydomain.com

Records we can find
(SOA) Start of Authority
Indicates the beginning of a zone and it should occur first in a zone file.
There can be only one SOA record per zone. Defines certain values for the zone such as a serial number and various expiration timeouts

(NS) Name Server
Defines an authoritative name server for a zone. Defines and delegates authority to a name server for a child zone.
NS Records are the GLUE that binds the distributed database together.

(A) Address
The A record simply maps a hostname to an IP address.
Zones with A records are called 'forward' zones

(PTR) Pointer
The PTR record maps an IP address to a Hostname.
Zones with PTR records are called 'reverse' zones.

CNAME
The CNAME record maps an alias hostname to an A record hostname.

(MX) Mail Exchange
The MX record specifies a host that will accept email on behalf of a given host.
The specified host has an associated priority value.
A single host may have multiple MX records.
The records for a specific host make up a prioritized list.

Virtual hosts

a website that shares an IP address with one or more other virtual hosts.

Fingerprinting framework and applications

Our first step in this case will be to consider the overall scope of the application:

- What is it for?
- Does it allow user registration?
- Does it have an administration panel?
- Does it take input from the user?
- What kind of input?
- Does it accept file uploads?
- Does it use JavaScript or Ajax or Flash? And so on.

Virtual host enumeration :

same host mapped to two domains

- use reverse lookup

Browser Extensions :

- **Wappalyzer :**
  wshows all technologies that the server uses that it can detect.
- **whoisrun :**
- **Hunter :**
  gets all email addresses related to this domain
- **whatweb :**

What is enumeration : https://resources.infosecinstitute.com/what-is-enumeration/#gref

Enumeration is defined as a process which establishes an active connection to the target hosts to discover potential attack vectors in the system, and the same can be used for further exploitation of the system.
Enumeration is used to gather the below

- Usernames, Group names
- Hostnames
- Network shares and services
- IP tables and routing tables
- Service settings and Audit configurations
- Application and banners
- SNMP and DNS Details