3. Module Information Gathering

Recommended to use a map to save and overview the results.

Gathering information about the target

-> `Whois tool` or `whois.domaintools.com` -> to get infos about the target

-> `nslookup $hostname` -> tools to translate hostname to ip
-> `nslookup -type=PTR $ip` -> translate ip to hostname
-> `nslookup -querytype=ANY $hostname` -> to query the DNS server for the whole record associated to hostname

Target ISP's

-> to find target ISP's (these information should be in the report, because it's useful to map the attack surface)

1. We use **nslookup **to get the ip's of the domain and subdomains if needed: `nslookup $hostname`
2. We use `arin.net` / `whois.domaintools.com` / `ripe.net` to uncover the target ISP's another easy way is to use: `netcraft.com` -> to show the target ip and its ISP.

Infrastructure

Discovering what **kind of web server** of the **version of the web server** will be a hint about the Target OS.

- IIS version 6.0 is by default on windows server 2003
- IIS version 7.0 supports on windows server 2008
- IIS version 8.0 supports on windows server 2012

These hints are 90% right.

Fingerprinting the Webserver

`netcat` / `httprint` / `whatweb` / `wappalyzer` / `netcraft.com` / `BuiltWith`

-> Cookie: (langauge the website uses)

- PHP - PHPSESSID=XXXX
- .NET - ASPSESSIONID=XXXX

- JAVA - JSESSION=XXXX

Enumerating Subdomains

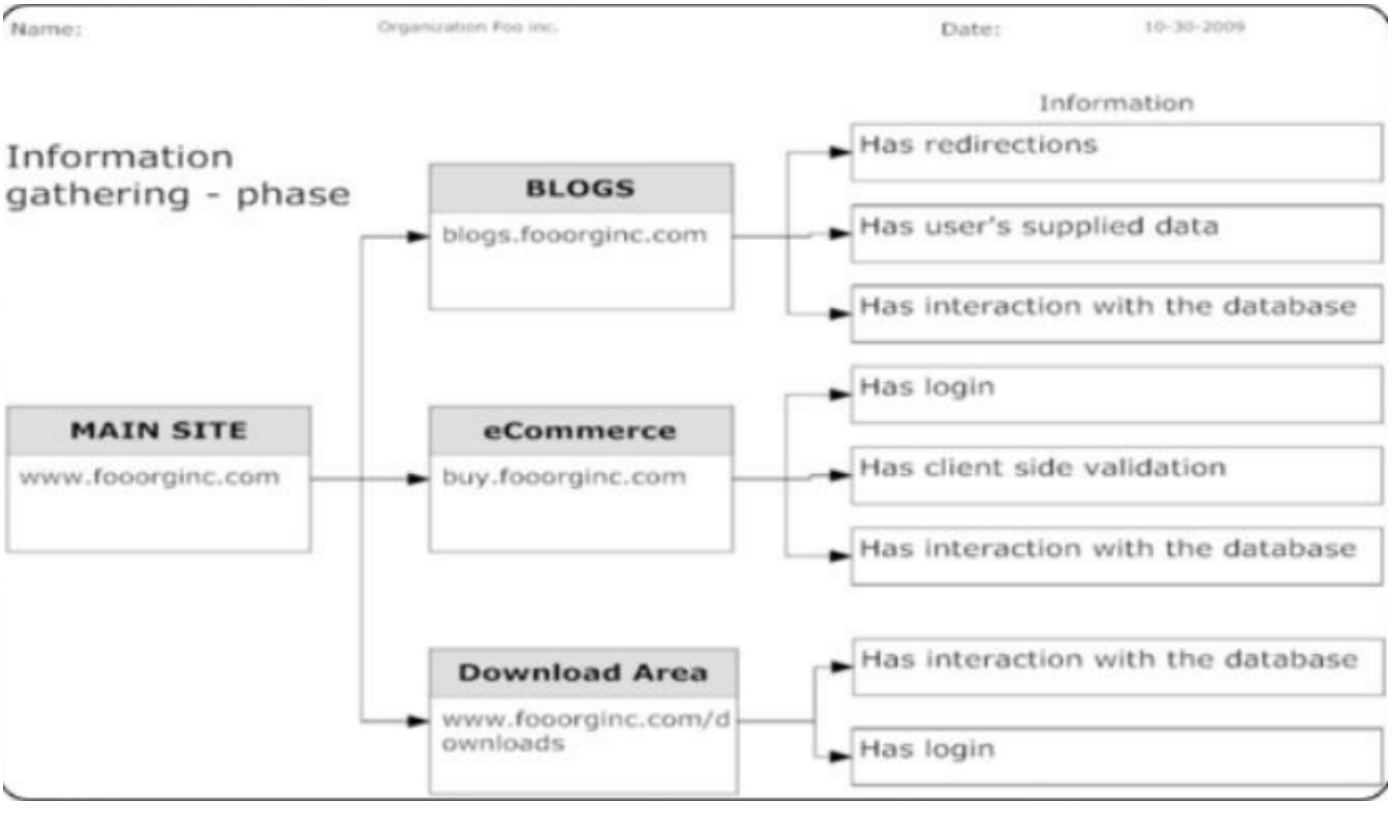
- google: `site:.target.com -inurl:www. -site:www.target.com`
- sublist3r
- dnsrecon: `dnsrecon -d $target`
- subbrute: `subbrute -h -s subs.txt $target`
- fierce: `fierce -dns $target` -> to get the Virtual Hosts
- knock
- theharvester: `theharvester -d $target -l 200`
- Zone Transfer:
  -> on windows:
  `nslookup -type=NS $target` -> to get the Name server of the target domain.
  `nslookup` -> `server "NS of the target"` -> `ls -d $target`
  -> on linux:
  `nslookup -type=NS $target`
  `dig @NS_of_target axfr $target`

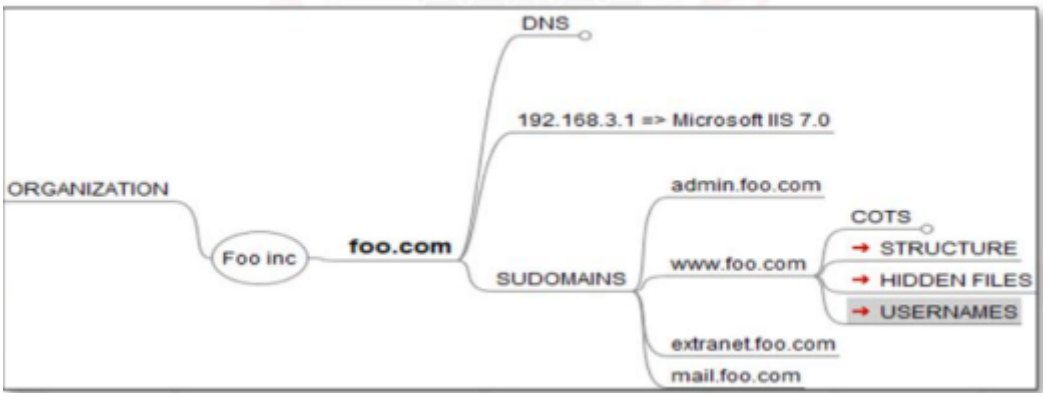
Firgerprinting Frameworks and applications

`buildwith`, `source-code`, `wappalyzer`, `read headers`

Custom: Browse the website run burpsuite in the background, spider the host.

Try to keep the gathered information well organized:





Enumerating Resources:

To find subdomains, website structure, hidden files, configuration files, and any leaked because of misconfiguration

Tools: `Burpsuite`, `dirsearch`, `ffuf`

A good list of back up files extension follows:

- bak
- bac
- old
- 000
- ~
- 01
- _bak
- 001
- inc
- Xxx

Google Hacking:

- `"index of" bak`
- `intitle:"Apache HTTP Server" intitle:"documentation" site:target.com`
- `filetype:"bak"` or `filetype:"inc"`
- `intitle:login` - to try SQLi

Shodan